UNIVERSIDAD POLITECNICA DE PUEBLA

INGENIERIA EN TECNOLOGIAS DE LA INFORMACION

Hospital ABC México

Proyecto de Interconexión de Redes

P R E S E N T AN

Joseph Diego Moysen Ramirez

Paola Xiqui García

Diana Laura Miualtecalt Rodriguez

Maestra de asignatura

Gudelia Pilar Pérez Conde

Resumen

Este proyecto tiene como finalidad diseñar e implementar una red moderna y escalable en el Hospital ABC Santa Fe, una institución médica de alta especialidad conformada por cuatro edificios principales. El objetivo es dotar al hospital de una infraestructura de red robusta, eficiente y segura, capaz de soportar las crecientes demandas tecnológicas de servicios médicos, administrativos y de comunicación. Para lograrlo, se contempla la segmentación lógica mediante VLANs, el uso de VLSM para un aprovechamiento óptimo de direcciones IP, así como la implementación de políticas de seguridad con listas de control de acceso (ACLs). Además, se integrarán redes inalámbricas de alta cobertura, dispositivos de videovigilancia, servidores esenciales como NTP, DHCP y DNS, y se garantizará la redundancia en enlaces críticos para asegurar la continuidad del servicio. Esta infraestructura permitirá mejorar la atención al paciente, optimizar los procesos internos del hospital y asegurar tanto la información como la operación diaria del centro médico, preparándolo para futuras expansiones tecnológicas.

Abstract

This project aims to design and implement a modern, scalable network at ABC Santa Fe Hospital, a high-specialty medical institution composed of four main buildings. The goal is to provide the hospital with a robust, efficient, and secure network infrastructure capable of supporting the growing technological demands of medical, administrative, and communication services. To achieve this, the project includes logical segmentation using VLANs, optimal IP address utilization through VLSM, and the implementation of security policies using access control lists (ACLs). In addition, high-coverage wireless networks will be deployed, along with surveillance devices and essential servers such as NTP, DHCP, and DNS. Redundant links will also be established to ensure continuous service. This infrastructure will enhance patient care, optimize internal hospital processes, and ensure the security of both information and daily operations—while also preparing the facility for future technological expansions.

Índice General

Índice de Figuras 4
Índice de Tablas 10
Introducción 13
Problemática 14
Justificación 15
Objetivos de Negocio 16
Objetivo General 17
Metodología 18
Resultados 20
Recomendaciones de seguridad 154
Plan de mantenimiento preventivo y correctivo 157
Referencias 158
Anexos 160

Índice de Figuras

1.1.1 Recorrido Virtual | TC 22
1.1.2 Recorrido Virtual | CNOR 23
1.1.3 Recorrido Virtual | CT 24
1.1.4 Recorrido Virtual | CGOP 26
2.5.1 Vista General – Conexión entre edificios 43
2.5.2 Torre Central | Nivel Plaza – Conexión entre dispositivos 44
2.5.3 Torre Central | Planta Baja – Conexión entre dispositivos 46
2.5.4 Torre Central | Piso 1 – Conexión entre dispositivos 47
2.5.5 Centro de Neurología | Planta Baja – Conexión entre dispositivos 48
2.5.6 Centro de Neurología | Piso 1 – Conexión entre dispositivos 49
2.5.7 Torre de Consultorios | Piso 1 – Conexión entre dispositivos 50
2.5.8 Torre de Consultorios | Piso 2 – Conexión entre dispositivos 51
2.5.9 Centro de Gineco | Planta Baja – Conexión entre dispositivos 52
2.5.10 Centro de Gineco | Piso 1 – Conexión entre dispositivos 53
2.6.1 Diagrama físico TC | NP – Archivo clínico 54
2.6.2 Diagrama físico TC | PB – Caja de Medicos 54
2.6.3 Diagrama físico TC | P1 - Asuntos Medicos 55
2.6.4 Diagrama físico CT | P1 - Consultorios 56
2.6.5 Diagrama físico CT | P2 - Consultorios 56
2.6.6 Diagrama físico CNOR | PB - 57
2.6.7 Diagrama físico CNOR | P1 – 57
2.6.8 Diagrama físico CGOP | PB - 58
2.6.9 Diagrama físico CGOP | P1 - 58
3.1.1 Conexión entre routers centrales 59
4.1.1 Configuracion TC | TC_R_NP 75
4.1.2 Configuracion TC | TC_R_PB 76
4.1.3 Configuracion TC | TC_R_P1 77
4.1.4 Configuracion TC | TC_SW_NP 78
4.1.5 Configuracion TC | TC_SW_PB 79

4.1.6 Configuracion TC | TC_SW_P1 80
4.1.7 Configuracion CT | CT_R_P1 81
4.1.8 Configuracion CT | CT_R_P2 82
4.1.9 Configuracion CT | CT_SW_P1 83
4.1.10 Configuracion CT | CT_SW_P2 84
4.1.11 Configuracion CNOR | CNOR_R_PB 85
4.1.12 Configuracion CNOR | CNOR_R_P1 86
4.1.13 Configuracion CNOR | CNOR_SW_PB 87
4.1.14 Configuracion CNOR | CNOR_SW_P1 88
4.1.15 Configuracion CGOP | CGOP_R_PB 89
4.1.16 Configuracion CGOP | CGOP_R_P1 90
4.1.17 Configuracion CGOP | CGOP_SW_PB 91
4.1.18 Configuracion CGOP | CGOP_SW_P1 92
4.1.19 VLANS | Torre Central | TC_SW_NP 93
4.1.20 VLANS | Torre Central | TC_SW_PB 93
4.1.21 VLANS | Torre Central | TC_SW_P1 94
4.1.22 VLANS | Torre de Consultorios | CT_SW_P1 94
4.1.23 VLANS | Torre de Consultorios | CT_SW_P2 95
4.1.24 VLANS | CNOR | CNOR _SW_PB 95
4.1.25 VLANS | CNOR | CNOR _SW_P1 96
4.1.26 VLANS | CGOP | CGOP _SW_PB 96
4.1.27 VLANS | CGOP | CGOP _SW_P1 97
4.1.28 Modo Troncal | Torre Central | TC_SW_NP 98
4.1.29 Modo Troncal | Torre Central | TC_SW_PB 98
4.1.30 Modo Troncal | Torre Central | TC_SW_P1 99
4.1.31 Modo Troncal | Torre de Consultorios | CT_SW_P1 99
4.1.32 Modo Troncal | Torre de Consultorios | CT_SW_P2 100
4.1.33 Modo Troncal | CNOR | CNOR _SW_PB 100
4.1.34 Modo Troncal | CNOR | CNOR _SW_P1 101
4.1.35 Modo Troncal | CGOP | CGOP _SW_PB 101
4.1.36 Modo Troncal | CGOP | CGOP _SW_P1 102

4.2.1 Conectividad TC | Nivel Plaza a Planta Baja 103
4.2.2 Conectividad TC | Nivel Plaza a Piso 1 103
4.2.3 Conectividad TC | Nivel Plaza a Internet 103
4.2.4 Conectividad TC | Nivel Plaza a Torre de Consultorios 104
4.2.5 Conectividad TC | Nivel Plaza a CNOR 104
4.2.6 Conectividad TC | Nivel Plaza a CGOP 104
4.2.7 Conectividad TC | Planta Baja Torre de Consultorios 105
4.2.8 Conectividad TC | Planta Baja a CNOR 105
4.2.9 Conectividad TC | Planta Baja a CGOP 105
4.2.10 Conectividad TC | Planta Baja a Internet 106
4.2.11 Conectividad TC | Piso 1 Torre de Consultorios 106
4.2.12 Conectividad TC | Piso 1 a CNOR 107
4.2.13 Conectividad TC | Piso 1 a CGOP 107
4.2.14 Conectividad TC | Piso 1 a Internet 107
4.2.15 Conectividad CT | Piso 1 a Piso 2 108
4.2.16 Conectividad CT | Piso 1 a Internet 108
4.2.17 Conectividad CT | Piso 1 a Torre Central 108
4.2.18 Conectividad CT | Piso 1 a CNOR 109
4.2.19 Conectividad CT | Piso 1 a CGOP 109
4.2.20 Conectividad CT | Piso 2 a Piso 1 109
4.2.21 Conectividad CT | Piso 2 a Internet 110
4.2.22 Conectividad CT | Piso 2 a Torre Central 110
4.2.23 Conectividad CT | Piso 2 a CNOR 110
4.2.24 Conectividad CT | Piso 2 a CGOP 111
4.2.25 Conectividad CNOR | Planta Baja a Piso 1 111
4.2.26 Conectividad CNOR | Planta Baja a Internet 111
4.2.27 Conectividad CNOR | Planta Baja a Torre Central 112
4.2.28 Conectividad CNOR | Planta Baja a Torre de Consultorios 112
4.2.29 Conectividad CNOR | Planta Baja a CGOP 112
4.2.30 Conectividad CNOR | Piso 1 a Planta Baja 113
4.2.31 Conectividad CNOR | Piso 1 a Planta Baja 113

4.2.32 Conectividad CNOR | Piso 1 a Torre Central 113
4.2.33 Conectividad CNOR | Piso 1 a Torre de Consultorios 114
4.2.34 Conectividad CNOR | Piso 1 a CGOP 114
4.2.35 Conectividad CGOP | Planta Baja a Piso 1 114
4.2.36 Conectividad CGOP | Planta Baja a Internet 115
4.2.37 Conectividad CGOP | Planta Baja a Torre Central 115
4.2.38 Conectividad CGOP | Planta Baja a CNOR 115
4.2.39 Conectividad CGOP | Planta Baja a Torre de Consultorios 116
4.2.40 Conectividad CGOP | Piso 1 a Planta Baja 116
4.2.41 Conectividad CGOP | Piso 1 a Internet 116
4.2.42 Conectividad CGOP | Piso 1 a Torre Central 117
4.2.43 Conectividad CGOP | Piso 1 a CNOR 117
4.2.44 Conectividad CGOP | Piso 1 a Torre de Consultorios 117
4.3.1 Servicio DNS | TC a Server_TC 118
4.3.2 Servicio DNS | CT a Server_TC 118
4.3.3 Servicio DNS | CNOR a Server_TC 119
4.3.4 Servicio DNS | CGOP a Server_TC 119
4.3.5 Servicio Netflow | Server_TC 120
4.3.6 Servicio Netflow | Server_CT 120
4.3.7 Servicio Netflow | Server_CNOR 120
4.3.8 Servicio Netflow | Server_CGOP 121
4.3.9 Servicio Syslog | Server_TC 122
4.3.10 Servicio Syslog | Server_CT 122
4.3.11 Servicio Syslog | Server_CNOR 123
4.3.12 Servicio Syslog | Server_CGOP 123
4.3.13 Servicio DHCP | Server_TC 124
4.3.14 Servicio DHCP | Server_CT 124
4.3.15 Servicio DHCP | Server_CNOR 125
4.3.16 Servicio DHCP | Server_CGOP 125
4.3.17 Servicio PAT | TC a Internet 126
4.3.18 Servicio PAT | CT a Internet 126

4.3.19 Servicio PAT | CNOR a Internet 126
4.3.20 Servicio PAT | CGOP a Internet 127
4.3.21 Servicio HTTP | TC 128
4.3.22 Servicio HTTP | CT 128
4.3.23 Servicio HTTP | CNOR 128
4.3.24 Servicio HTTP | CGOP 129
4.3.25 Servicio HTTPS | TC 130
4.3.26 Servicio HTTPS | CT 130
4.3.27 Servicio HTTPS | CNOR 131
4.3.28 Servicio HTTPS | CGOP 131
4.3.29 Servicio NTP | TC 132
4.3.30 Servicio TC_R_NP | TC_R_PB | TC_R_P1 132
4.3.31 Servicio TC_SW_NP | TC_SW_PB | TC_SW_P1 133
4.3.32 Servicio NTP | CT 134
4.3.33 Servicio CT_R_P1 | CT_R_P2 134
4.3.34 Servicio CT_SW_P1 | CT_SW_P2 135
4.3.35 Servicio NTP | CNOR 136
4.3.36 Servicio CNOR_R_PB | CNOR_R_P1 136
4.3.37 Servicio CNOR_SW_PB | CNOR_SW_P1 137
4.3.38 Servicio NTP | CGOP 138
4.3.39 Servicio CGOP_R_PB | CNOR_R_P1 138
4.3.40 Servicio CGOP_SW_PB | CNOR_SW_P1 139
5.2.1 Conectividad Entre VLAN de TC 141
5.2.2 Conectividad VLAN TC a VLAN CT 141
5.2.3 Conectividad VLAN TC a VLAN CNOR 142
5.2.4 Conectividad VLAN TC a VLAN CGOP 142
5.2.5 Conectividad VLAN TC a VLAN CT 142
5.2.6 Conectividad VLAN TC a VLAN CNOR 143
5.2.7 Conectividad VLAN TC a VLAN CGOP 143
5.2.8 Conectividad VLAN TC a VLAN CT 144
5.2.9 Conectividad VLAN TC a VLAN CNOR 144

5.2.10 Conectividad VLAN TC a VLAN CGOP 144
5.2.11 Conectividad VLAN CT a VLAN CT 145
5.2.12 Conectividad VLAN CT a VLAN TC 145
5.2.13 Conectividad VLAN CT a VLAN CNOR 145
5.2.14 Conectividad VLAN CT a VLAN CGOP 146
5.2.15 Conectividad VLAN CT a VLAN CT 146
5.2.16 Conectividad VLAN CT a VLAN TC 147
5.2.17 Conectividad VLAN CT a VLAN CNOR 147
5.2.18 Conectividad VLAN CT a VLAN CGOP 147
5.2.19 Conectividad VLAN CNOR a VLAN CNOR 148
5.2.20 Conectividad VLAN CNOR a VLAN TC 148
5.2.21 Conectividad VLAN CNOR a VLAN CT 148
5.2.22 Conectividad VLAN CNOR a VLAN CGOP 149
5.2.23 Conectividad VLAN CNOR a VLAN CNOR 149
5.2.24 Conectividad VLAN CNOR a VLAN TC 149
5.2.25 Conectividad VLAN CNOR a VLAN CT 150
5.2.26 Conectividad VLAN CNOR a VLAN CGOP 150
5.2.27 Conectividad VLAN CGOP a VLAN CGOP 150
5.2.28 Conectividad VLAN CGOP a VLAN TC 151
5.2.29 Conectividad VLAN CGOP a VLAN CNOR 151
5.2.30 Conectividad VLAN CGOP a VLAN CT 151
5.2.31 Conectividad VLAN CGOP a VLAN CGOP 152
5.2.32 Conectividad VLAN CGOP a VLAN TC 152
5.2.33 Conectividad VLAN CGOP a VLAN CNOR 152
5.2.34 Conectividad VLAN CGOP a VLAN CT 153

Índice de Tablas

2.1.1 Tabla de precios 33
2.3.1 VLSM Torre Central | NP 35
2.3.2 VLSM Torre Central | PB 35
2.3.3 VLSM Torre Central | P1 35
2.3.4 VLSM CNOR | PB 36
2.3.5 VLSM CNOR | P1 36
2.3.6 VLSM CT | P1 36
2.3.7 VLSM CT | P2 36
2.3.8 VLSM CGOP | PB 37
2.3.9 VLSM CGOP | P1 37
2.4.1 Torre Central | Nivel Plaza 38
2.4.2 Torre Central | Planta Baja 39
2.4.3 Torre Central | Planta Baja 39
2.4.4 CNOR | PB 40
2.4.5 CNOR | P1 40
2.4.6 CT | P1 41
2.4.7 CT | P2 41
2.4.8 CGOP | PB 42
2.4.9 CGOP | P1 42
2.5.1 Tabla de direcciones IP (Red) | Torre Central a Torre de Consultorios 43
2.5.2 Tabla de direcciones IP (Red) | Torre Central a Centro de Neurología 43
2.5.3 Tabla de direcciones IP (Red) | Centro de Neurología a Centro de Gineco 43
2.5.4 Tabla de direcciones IP (Red) | Centro de Gineco a Torre de Consultorios 44
2.5.5 EIGRP1 TC | NP 44
2.5.6 OSPF2 TC | NP 45
2.5.7 OSPF4 TC | NP 45
2.5.8 EIGRP2 TC | PB 46
2.5.9 OSPF2 TC | PB 46
2.5.10 EIGRP3 TC | P1 47

2.5.11 OSPF4 TC | NP 47
2.5.12 EIGRP6 CNOR | PB 48
2.5.13 OSPF8 CNOR | PB 48
2.5.14 EIGRP7 CNOR | P1 49
2.5.15 OSPF8 CNOR | P1 49
2.5.16 EIGRP4 CT | P1 50
2.5.17 OSPF6 CT | P1 50
2.5.18 EIGRP5 CT | P2 51
2.5.19 OSPF6 CT | P2 51
2.5.20 EIGRP8 CGOP | PB 52
2.5.21 OSPF10 CGOP | PB 52
2.5.22 EIGRP9 CGOP | P1 53
2.5.23 OSPF10 CGOP | P1 53
3.1.1 Conexiones de Router (1) | Torre Central 59
3.1.2 Conexiones de Router (2) | CNOR 59
3.1.3 Conexiones de Router (3) | CNOR 59
3.1.4 Conexiones de Router (4) | CGOP 60
3.1.5 Conexión de dispositivos | Torre central | Nivel Plaza 60
3.1.6 Conexión de dispositivos | Torre central | PB 61
3.1.7 Conexión de dispositivos | Torre central | Piso 1 62
3.1.8 Conexión de dispositivos | Torre de Consultorios | Piso 1 62
3.1.9 Conexión de dispositivos | Torre de Consultorios | Piso 2 63
3.1.10 Conexión de dispositivos | CNOR | Planta Baja 63
3.1.11 Conexión de dispositivos | CNOR | Piso 1 64
3.1.12 Conexión de dispositivos | CGOP | Planta Baja 64
3.1.13 Conexión de dispositivos | CGOP | Piso 1 65
3.2.1 Torre Central | Nivel Plaza 66
3.2.2 Torre Central | Planta Baja 67
3.2.3 Torre Central | Piso 1 68
3.2.4 Torre de Consultorios | Piso 1 69
3.2.5 Torre de Consultorios | Piso 2 70

3.2.6 Centro de Neurología, Ortopedia y Rehabilitación | Planta Baja 71
3.2.7 Centro de Neurología, Ortopedia y Rehabilitación | Piso 1 72
3.2.8 Centro de Gineco-Obstetricia y Pediatría | Planta Baja 73
3.2.9 Centro de Gineco-Obstetricia y Pediatría | Planta Baja 74
5.1 Validación del funcionamiento de todos los servicios de la red 140
6.1.1 Políticas de acceso para mitigar las vulnerabilidades 154
6.1.2 Sistemas de control de seguridad 155
6.1.3 Medidas de recuperación ante desastres naturales, etc 156
7.1.1 Cronograma de actividades 160
7.1.2 Tabla de características | Router 163
7.1.3 Tabla de Ventajas | Router 164
7.1.4 Tabla de Caracteristicas | Switch 165
7.1.5 Tabla de Caracteristicas | Servidor 171

Introducción

El Hospital ABC, también conocido como **Centro Médico ABC**, es una institución privada de salud de alta especialidad que se ha consolidado como uno de los referentes médicos más importantes de México y América Latina. Con una trayectoria de más de 135 años, su compromiso con la excelencia médica, la innovación tecnológica y la atención centrada en el paciente lo posicionan como un líder en el sector salud.

Este proyecto está enfocado en el **Campus Santa Fe**, una de las dos sedes del hospital (junto con Observatorio), ubicado en la zona poniente de la Ciudad de México, específicamente en **Avenida Carlos Graef Fernández No. 154, Santa Fe, Álvaro Obregón, C.P. 05330**. Esta sede combina infraestructura hospitalaria de vanguardia con servicios especializados, y opera bajo los más altos estándares internacionales de calidad, certificados por Joint Commission International (JCI).

El campus Santa Fe cuenta con múltiples instalaciones que incluyen torres de hospitalización, consultorios, áreas de cirugía, centros especializados en cáncer, neurología, ortopedia, ginecología, pediatría, imagenología, rehabilitación, así como **laboratorios clínicos, banco de sangre, farmacia 24 horas, cafetería, estacionamientos y módulos de aseguradoras**, todo integrado dentro de un entorno hospitalario inteligente y altamente interconectado.

Dada la complejidad y criticidad de sus operaciones, el diseño de la red de datos en el Hospital ABC representa un desafío técnico importante. Esta red debe garantizar **conectividad continua, alta disponibilidad, seguridad de la información médica, soporte para equipos biomédicos, integración con IoT hospitalario**, y compatibilidad con plataformas de gestión clínica y expediente electrónico.

En este proyecto se desarrollará una propuesta de red robusta y escalable, alineada a las necesidades específicas del Hospital ABC – Campus Santa Fe, considerando tanto su infraestructura actual como su proyección de crecimiento tecnológico.

Problemática

El Hospital ABC en su sede de Santa Fe es uno de los centros médicos privados más prestigiosos de México, y cuenta con una amplia infraestructura tecnológica, médica y administrativa que opera de forma constante. Sin embargo, a pesar de su nivel de innovación clínica, **la infraestructura de red actual presenta diversas deficiencias técnicas que limitan su eficiencia, escalabilidad y seguridad**.

Entre los principales problemas detectados se encuentran:

1. **Sobrecarga en la red local (LAN)** por el creciente número de dispositivos conectados simultáneamente (sistemas médicos digitales, computadoras del personal, cámaras de seguridad, sistemas de gestión hospitalaria y dispositivos móviles), lo cual genera **latencia, interrupciones intermitentes y pérdida de rendimiento en servicios críticos**.
2. **Ausencia de una segmentación lógica (VLANs)** que separe los diferentes tipos de tráfico (médico, administrativo, visitantes, videovigilancia), lo que **aumenta el riesgo de saturación, pérdida de información y vulnerabilidad a ataques**.
3. **WiFi de visitantes mal aislada y sin controles de seguridad**, lo que representa un **potencial punto de entrada para amenazas externas o accesos no autorizados**.
4. **Falta de un sistema de monitoreo centralizado** que permita observar en tiempo real el rendimiento de la red, identificar cuellos de botella y reaccionar a incidentes de forma oportuna.

Solución propuesta por el Equipo

Con base en el análisis de los problemas mencionados, proponemos el rediseño estructurado de la infraestructura de red del Hospital ABC (Santa Fe), enfocado en los siguientes puntos clave:

1. **Implementación de una red segmentada por VLANs**, separando lógicamente los entornos médicos, administrativos, visitas, videovigilancia y dispositivos IoT, para mejorar la seguridad y evitar congestión de tráfico.
2. **Instalación de una red WiFi de visitantes completamente aislada**, con portal cautivo, autenticación controlada y firewall intermedio, protegiendo la red interna y limitando el ancho de banda por dispositivo.
3. **Implementación de un sistema de monitoreo de red centralizado**, utilizando herramientas como Zabbix, PRTG o NetFlow, para detectar anomalías, administrar el tráfico y optimizar el rendimiento en tiempo real.
4. **Diseño modular y escalable**, que permita añadir nuevos dispositivos, áreas o servicios médicos en el futuro sin tener que rediseñar la red por completo.
5. **Control de acceso basado en roles (ACLs avanzadas y AAA)**, refuerza la seguridad, evita accesos no autorizados a recursos sensibles como servidores de expediente clínico.

Justificación

La solución planteada responde a la necesidad urgente de modernizar y optimizar la red del Hospital ABC, para asegurar una **operación continua, segura y eficiente** en todas sus áreas. Dado que el hospital maneja información sensible, sistemas médicos conectados y comunicación crítica entre unidades, **una infraestructura de red moderna es fundamental para su correcto funcionamiento**.

Con la nueva segmentación por VLANs y la implementación de QoS, **el tráfico médico tendrá siempre prioridad**, evitando retrasos o desconexiones en servicios vitales como monitoreo de pacientes, quirófanos conectados o registros electrónicos. La sustitución de equipos legacy reducirá fallos, mejorará la velocidad de transmisión y aumentará la compatibilidad con nuevas tecnologías médicas.

A través del monitoreo en tiempo real y el aislamiento de redes no críticas como la WiFi de visitantes, **se reducirá el riesgo de ciberataques, accesos no autorizados o saturación de la red**, protegiendo así los datos confidenciales y garantizando una operación segura.

Finalmente, esta solución sienta las bases para el crecimiento futuro del hospital, permitiéndole **escalar su infraestructura digital sin tener que reconstruir desde cero**, adaptándose fácilmente a la incorporación de nuevas tecnologías, servicios, áreas médicas o dispositivos conectados

Objetivos de Negocio

Garantizar la continuidad operativa del hospital mediante una infraestructura de red confiable y redundante, que asegure la disponibilidad de los servicios digitales incluso ante fallos técnicos o caídas parciales del sistema.

Objetivo General

Diseñar e implementar una infraestructura de red moderna, segura, escalable y segmentada para el Hospital ABC – Campus Santa Fe, que permita optimizar el rendimiento de los servicios médicos, administrativos y tecnológicos, garantizando la continuidad operativa, la protección de datos sensibles y la capacidad de crecimiento institucional a futuro.

Objetivos específicos

1. **Desarrollar una red WiFi segura para visitantes**, totalmente aislada de la red interna, con autenticación controlada y límites de ancho de banda para evitar interferencias en los servicios principales del hospital.

Metodología

Para el desarrollo de este proyecto se empleó la metodología **PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize)** de Cisco, un enfoque estructurado que permite planear, diseñar e implementar soluciones de red robustas y escalables. A continuación, se describe detalladamente cada fase y las acciones realizadas por el equipo durante su aplicación:

Prepare (Preparación)

En esta etapa inicial se realizó una revisión virtual de las instalaciones del Hospital ABC Santa Fe. Se identificaron los departamentos clave de cada torre y piso, priorizando aquellas áreas con mayor demanda tecnológica. Durante esta fase también se detectaron las necesidades particulares por zona (conectividad, videovigilancia, acceso inalámbrico, etc.), se registraron los dispositivos y servicios requeridos por cada área, y toda la información fue debidamente documentada como base para las siguientes etapas.

Plan (Planeación)

Se procedió al diseño lógico de la red, segmentando los espacios mediante subredes definidas con la técnica de VLSM (Variable Length Subnet Mask). Asimismo, se establecieron las políticas de red necesarias para garantizar la eficiencia, seguridad y priorización del tráfico (por ejemplo, políticas de QoS y aislamiento de tráfico por VLAN). En esta fase también se realizó una estimación de dispositivos necesarios y servicios de red, incluyendo investigación de precios y elaboración de cotizaciones preliminares, todo debidamente documentado.

Design (Diseño)

Durante esta fase se desarrollaron dos tipos de diagramas fundamentales:

- El **diagrama físico**, que muestra la ubicación de los dispositivos dentro del plano del hospital.
- El **diagrama lógico**, que representa la topología, conexiones y estructura general de la red.

También se definieron las **VLANs por área y función**, las **listas de control de acceso (ACLs)** necesarias para gestionar permisos y seguridad, y se construyó la **tabla IP** asignando direcciones de forma eficiente y organizada. Toda esta información quedó consolidada en la documentación técnica del diseño.

Implement (Implementación)

Se utilizó **Cisco Packet Tracer** como entorno de simulación para llevar a cabo la implementación de la red. Se configuraron los dispositivos principales (routers, switches, access points simulados, servidores), se asignaron direcciones IP y VLANs, se implementaron ACLs para controlar el tráfico, y se probaron los servicios básicos como DHCP, DNS, NAT, HTTP/HTTPS, entre otros. Finalmente, se realizaron pruebas de conectividad entre dispositivos y entre VLANs para validar el correcto funcionamiento.

Operate (Operación)

En esta etapa se verificó que todos los servicios y configuraciones funcionaran correctamente. Se hicieron pruebas de comunicación entre áreas, validación de políticas de acceso (ACLs), y pruebas de rendimiento básico del sistema. Además, se simuló el **monitoreo de tráfico** dentro de Packet Tracer para analizar la estabilidad de la red, detectar posibles errores y aplicar mejoras al diseño si era necesario.

Optimize (Optimización)

Para concluir, se elaboró el **informe final del proyecto**, integrando toda la documentación generada en las fases anteriores. Se incluyeron capturas de pantalla del simulador, justificaciones técnicas para cada decisión de diseño, las conclusiones generales del proyecto, y los anexos correspondientes como planos, scripts de configuración, y cotizaciones. Esta fase garantiza que el trabajo quede completamente organizado y listo para su presentación o escalamiento.

Resultados

Fase 1

1.1 Recorrido virtual o físico por el hospital

El Hospital ABC Santa Fe se encuentra estructurado en distintos edificios y torres distribuidos por especialidad y funcionalidad, lo cual permite segmentar los servicios médicos, administrativos y de atención al público. A través de un recorrido virtual por sus instalaciones, se identificaron los principales edificios que componen la infraestructura del hospital y las áreas clave que alberga cada uno.

Torre Central

Es el núcleo principal del hospital, donde convergen servicios generales, administrativos y médicos de alta complejidad. Se compone de las siguientes áreas:

Nivel Plaza:

- Clínica ABC Amistad
- Archivo Clínico
- Cafetería
- Central de Mezclas
- Centro Cardiovascular
- Farmacia Intrahospitalaria
- Fisiología Pulmonar e Inhaloterapia
- Medicina Preventiva
- Restaurante
- Tecnología de la Información

Planta Baja:

- Atención al Público
- Banco de Sangre
- Sucursales bancarias
- Caja General
- Caja de Médicos
- Cajeros Automáticos
- Farmacias Especializadas
- Laboratorio Clínico
- Medicasa
- Módulos de Informes
- Módulos de Aseguradoras

- Radiología e Imagen Molecular
- Cafetería
- Tienda de Regalos de las Damas Voluntarias
- Urgencias

Primer Piso:

- Admisión
- Asociación Médica
- Asuntos Médicos
- Caja de Médicos
- Centro Urológico
- Cirugía Ambulatoria / Quirófanos
- Unidad de corta estancia (dentro de UCA)
- Endoscopía
- Unidad de Hemodiálisis

Segundo Piso:

- Cirugía - Habitaciones de la 201 a la 228
- Neurofisiología

Tercer Piso:

- Caja Hospitalización
- Hospitalización
- Habitaciones de la 301 a la 309
- Terapia Intensiva
- Cubículos del T01 al T08
- Terapia Intermedia
- Habitaciones de la 350 a la 362

1.1.1 Recorrido Virtual | TC

Torre central

Centro de Neurología, Ortopedia y Rehabilitación

Edificio especializado en atención neurológica y rehabilitación, con áreas de hospitalización y consulta.

Planta Baja:

- Atención al Público
- Consultorios del 070 al 073
- Medicina Física y Rehabilitación
- Módulo de Informes

Primer Piso:

- Aulas de Usos Múltiples
- Centro Neurológico
- Consultorios del 150 al 159
- Puente de conexión con estacionamiento
- Sala de Rezo Judío
- Time Share CENOR

Segundo Piso:

- Aulas de Usos Múltiples
- Cajas de Médicos
- Caja de Hospitalización Neurología
- Neurología - Habitaciones de la 274 a las 297

Tercer Piso:

- Caja Hospitalización Ortopedia
- Ortopedia - Habitaciones de la 374 a la 399
- Rehabilitación intensiva

1.1.2 Recorrido Virtual | CNOR

Centro de Neurología

Torre de consultorios

Estructura destinada a atención ambulatoria, con múltiples consultorios distribuidos por especialidades.

Primer Piso:

- Consultorios del 101 al 116

Segundo Piso:

- Consultorios del 201 al 224

Tercer Piso:

- Consultorios del 301 al 325

Cuarto Piso:

- Consultorios del 401 al 425

Quinto Piso:

- Consultorios del 501 al 525

1.1.3 Recorrido Virtual | CT

Torre de consultorios

Centro de Gineco-Obstetricia y Pediatría

Edificio enfocado en la atención materno-infantil, hospitalización y servicios especializados en neonatología y cuidados intensivos.

Planta Baja:

- Gineco-obstetricia
- Atención al Público
- Auditorios
- Cajas de Médicos
- Caja Hospitalización
- Oficina Damas Voluntarias
- Dirección
- Módulo de Informes
- Pediatría
- Consultorios del 1 al 5
- Auditoría de ingresos

Primer Piso:

- Cuneros Fisiológicos

- Gineco-Obstetricia
- Habitaciones de la 101 a la 121
- Salas de labor y LPR
- Toco-Cirugía
- Unidad de Terapia intensiva e intermedia Neonatal

Segundo Piso:

- Ginecología - Habitaciones de la 240 a la 251
- Laboratorio DIAGEN (Cons. 201)
- Pediatría - Habitaciones de la 256 a la 269
- Subdirección de Enfermería
- Talento Humano
- Unidad de Cuidados Intensivos de Pediatría - Cubículos 270 y 271
- Unidad de Vigilancia Epidemiológica Hospitalaria
- Calidad

Tercer Piso:

- Consultorios del 330 al 343

1.1.4 Recorrido Virtual | CGOP

Centro de Gineco-Obstetricia y pediatría

1.2 Identificación de departamentos claves

En esta fase se identificaron **áreas estratégicas** dentro de cada edificio del hospital, seleccionando únicamente aquellas **con alta densidad de usuarios, operaciones críticas, y gran demanda de conectividad de red**

Torre Central

- **Nivel Plaza**: Tecnología de la Información, Farmacia, Clínica ABC Amistad, Archivo Clínico, Cafetería, Restaurante.
- **Planta Baja**: Atención al público, Sucursal Bancaria, Caja general, Caja de médicos, Módulos de aseguradoras, Cafetería, Tienda de regalos de las Damas voluntarias.
- **Piso 1**: Admisión, Asuntos médicos, Caja de médicos, etc.

Centro de Neurología, Ortopedia y Rehabilitación

- **Planta Baja**: Consultorios, Medicina Física, Atención al Público, Módulos de informes.
- **Piso 1**: Centro Neurológico, Consultorios, Time Share CENOR, Aulas de usos múltiples.

Torre de consultorios

- **Piso 1 y Piso 2**: Consultorios 101–116 y 201–224.

Se hizo la selección del piso 1 y 2 ya que son en donde mayormente transcurre gente

Centro de Gineco-Obstetricia y Pediatria

- **Planta Baja**: Auditorios, Caja de médicos, Oficina de damas voluntarias, Modulo de informes, Pediatría, Auditoria de ingresos.
- **Piso 1**: Cunero Fisiológicos, Gineco-Obstetricia, Habitaciones 101 – 121

1.3 Detección de necesidades tecnológicas en cada área.

Torre Central

Enfoque: Núcleo operativo, administrativo, clínico y de atención inmediata al paciente.

Nivel Plaza

Por qué son clave:

- **Tecnología de la Información:** Aquí estará el centro de operación tecnológica (servidores, switches, controladores), por lo tanto, es crítico en términos de infraestructura de red.
- **Clínica ABC Amistad:** Son áreas donde se genera y consulta información clínica en línea, requieren acceso constante al expediente electrónico.
- **Farmacia Intrahospitalaria y Central de Mezclas:** Dependen de conectividad para órdenes médicas digitales y trazabilidad de medicamentos.
- **Cafetería y Restaurante:** Necesitan red para TPV, cámaras IP y, si se habilita, Wi-Fi para usuarios y personal.
- **Archivo Clínico:** Punto clave para el manejo y digitalización de historiales, requiere conectividad con servidores y alta seguridad.

Planta Baja

Por qué son clave:

- **Atención al Público y Módulos de Informes:** Son el primer punto de contacto del paciente; requieren red para registro y validación de datos.
- **Caja General y Sucursales Bancarias:** Operaciones financieras que deben estar protegidas y conectadas constantemente.
- **Cajeros Automáticos / Tienda:** Conexión segura a sistemas externos y cámaras por seguridad.
- **Cafetería:** Punto de alto tráfico, ideal para cámaras de vigilancia y red para puntos de venta.

Piso 1

Por qué son clave:

- Admisión: **Conectividad constante para ingreso y alta de pacientes al sistema.**
- Caja de Médicos y Asociación Médica: **Áreas administrativas médicas que requieren infraestructura estable.**

Centro de Neurología, Ortopedia y Rehabilitación

Enfoque: Hospitalización crítica y consultas especializadas.

Planta Baja

Por qué son clave:

- **Atención al Público y Módulo de Informes:** Necesitan red para agendamiento, control de citas y gestión de pacientes.
- **Consultorios:** Uso constante de expediente electrónico.
- **Rehabilitación:** Uso de dispositivos IoT y requerimiento de cámaras de seguridad para control de áreas comunes.

Piso 1

Por qué son clave:

- **Consultorios:** Como en otros pisos, requieren red por expediente electrónico, impresión de recetas, acceso a imágenes.
- **Time Share:** Oficinas médicas compartidas que requieren conexión segura.
- **Puente y Sala de Rezo:** Importantes para vigilancia por cámaras IP, especialmente en horarios de baja afluencia.

Torre de Consultorios

Enfoque: Atención ambulatoria individualizada.

Piso 1 y 2

Por qué son clave:

- Cada consultorio opera como una unidad autónoma, con su propia agenda, historia clínica, impresora, dispositivos médicos conectados.
- Tráfico constante de pacientes requiere red estable.
- Ideal para segmentar red por VLAN por consultorio y vigilancia común en pasillos.

Centro de Gineco-Obstetricia y Pediatría

Enfoque: Atención materno-infantil, hospitalización, cuidados intensivos.

Planta Baja

Por qué son clave:

- **Consultorios y Pediatría:** Manejo clínico con conectividad al sistema
- **Cajas y Auditoría:** Flujo financiero y administrativo necesita red estable.
- **Auditorio y Dirección:** Red para presentaciones, coordinación interna, cámaras de control.

Piso 1

Por qué son clave:

- **Habitaciones y Cuneros:** Necesitan cámaras, red para expedientes y Wi-Fi para personal.
- **Salas de Labor:** Monitoreo continuo, equipos conectados, necesidad de red dedicada y segura.

1.4 Registro de dispositivos y servicios requeridos por área.

Torre Central / Cantidad de dispositivos

Implementacion de: DHCP, Syslog, Netflow, Tacacs+ para dispositivos [Routers, Switches] y loT para cámaras

Total: 3 Routers, 3 Switches, 11 APs, 3 Controladores Wi-Fi, 20 PCs, 20 Teléfonos, 12 Cámaras, 4 UPS, 2 Servidor, 1 Gabinete.

Nivel Plaza

- Router, Switch, Servidor, 2 UPS
- 8 PCs, 7 Teléfonos, 5 APs, 1 WC
- 4 Cámaras

Planta Baja:

- Router, Switch, 1 UPS
- 6 PCs, 7 Teléfonos, 3 APs, 1 WC
- 4 Cámaras

Piso 1:

- Router, Switch, 1 UPS
- 6 PCs, 6 Teléfonos, 3 APs, 1 WC
- 4 Cámaras

Centro de Neurología, Ortopedia y Rehabilitación

Implementacion de: DHCP, Syslog, Netflow, Tacacs+ para dispositivos [Routers, Switches] y loT para cámaras

Total: 2 Routers, 2 Switches, 8 APs, 2 Controladores Wi-Fi, 9 PCs, 9 Teléfonos, 8 Cámaras, 2 UPS, 1 Servidor, 1 Gabinete.

Planta Baja:

- Router, Switch, 1 UPS
- 5 PCs, 5 Teléfonos, 4 APs, 1 WC
- 4 Cámaras

Piso 1:

- Router, Switch, 1 UPS
- 4 PCs, 4 Teléfonos, 4 APs, 1 WC
- 4 Cámaras

Torre Consultorios

Implementacion de: DHCP, Syslog, Netflow, Tacacs+ para dispositivos [Routers, Switches] y IoT para cámaras

Total: 2 Routers, 2 Switches, 8 APs, 2 Controladores Wi-Fi, 10 PCs, 10 Teléfonos, 6 Cámaras, 2 UPS, 1 Servidor, 1 Gabinete.

Piso 1:

- Router, Switch, 1 UPS
- 5 PCs, 5 Teléfonos, 4 APs, 1 WC
- 3 Cámaras

Piso 2:

- Router, Switch, 1 UPS
- 5 PCs, 5 Teléfonos, 4 APs, 1 WC
- 3 Cámaras

Centro de Gineco-Obstetricia y Pediatría

Implementacion de: DHCP, Syslog, Netflow, Tacacs+ para dispositivos [Routers, Switches] y IoT para cámaras

Total: 2 Routers, 2 Switches, 8 APs, 2 Controladores Wi-Fi, 15 PCs, 15 Teléfonos, 15 Cámaras, 2 UPS,1 Servidor, 1 Gabinete.

Planta Baja:

- Router, Switch, 1 UPS
- 8 PCs, 8 Teléfonos, 4 APs, 1 WC
- 8 Cámaras

Piso 1:

- Router, Switch, 1 UPS
- 7 PCs, 7 Teléfonos, 4 APs, 1 WC
- 7 Cámaras

Fase 2

2.1 Investigacion de precios y elaboración de cotizaciones

2.1.1 Tabla de precios

Concepto	Unidad / Modelo	Cantidad	Precio Unitario MXN	Subtotal
Router	Cisco 8x rj-45, 4x sfp	9	$53,000	$477,000
Switch PoE+	Cisco CBS220-48P-4G-NA	9	$20,500	$184,500
Access Points	Ubiquiti U6-Lite	35	$3,500	$122,500
Controlador Wi-Fi (Wirreless)	Ubiquiti Cloud Key G2+	9	$5,500	$49,500
PCs	HP ProDesk 400 G7	35	$12,000	$420,000
Cámaras loT	Hikvision DS-2CD2046G2-I	41	$1,480	$60,680
Servidor	Dell PowerEdge R250	5	$33,669	$134,676
UPS	APC SMT1500C	10	$17,000	$170,000
Cableado Cat6	Bobinas 305m + canaletas	13	$2,600	$33,800
Cableado Fibra Optica	Monomodo OS2 Rollo 400m	4	$16,00	$64,000
Modulo SFP	GLC-LH-SMD	9	$210	$1,890
Conector LC	LC-UPC Duplex Monomodo – OP – ACLCUD	20	$21	$420
Conector RJ-45	Panduit CJ6X88TGIW-Cat6A	25	$370	$9,250
Patch panels, faceplates,	Varios	—	—	$25,000
Gabinete de red	Tripp Lite SR18UB SmartRack	9	$20,000	$180,000
Telefono IP PoE+	Grandstream GXP1620	30	$790	$23,700
Total				$1,956,914

2.2 Definicion de políticas de red

1. Acceso del departamento de TI:

- **Permitir** acceso completo desde la VLAN del Departamento de TI a:
    1. Todos los dispositivos de red (routers y switches).
    2. Servidores.
    3. Cámaras de seguridad.
- **Permitir** protocolos como:
    1. SSH (puerto 22).
    2. HTTPS (puerto 443).
    3. HTTP (puerto 80).
    4. Telnet (solo si es estrictamente necesario, no recomendado).

2. Acceso desde áreas públicas:

- **Permitir únicamente** el acceso a Internet (navegación web).
    1. Protocolos permitidos: HTTP (puerto 80), HTTPS (puerto 443), DNS (puerto 53).
- **Denegar completamente** el acceso a:
    1. Routers.
    2. Switches.
    3. Servidores.
    4. Cámaras de seguridad.
- **Denegar explícitamente** el uso de:
    1. SSH (puerto 22).
    2. Telnet (puerto 23).
    3. RDP (puerto 3389).
    4. FTP (puerto 21), etc.

3. Acceso desde el área de administración:

- **Permitir** acceso a los **archivos del sistema** ubicados en los servidores designados para gestión administrativa.
- **Restringir** el acceso a dispositivos de red y cámaras.
- **Permitir** protocolos como:
    1. SMB/CIFS (puerto 445 o 139 si usan recursos compartidos).
    2. HTTPS y HTTP para acceso a portales de gestión.
    3. DNS y navegación por Internet según sea necesario.

2.3 Segmentacion de red por subredes VLSM

Red Padre: 120.32.0.0

2.3.1 VLSM Torre Central | NP

Vlan	Red	Mascara	Broadcast	Rango
10	120.32.0.0	24	120.32.0.255	0.1-0.254
11	120.32.1.0	24	120.32.1.255	1.1-1.254
12	120.32.2.0	25	120.32.2.127	2.1-2.126
13	120.32.2.128	26	120.32.2.191	2.129-2.190
14	120.32.2.192	26	120.32.2.255	2.193-2.25
15	120.32.3.0	28	120.32.3.15	3.1-3.14
16	120.32.3.16	28	120.32.3.31	3.17-3.30
17	120.32.3.32	28	120.32.3.47	3.33-3.46

2.3.2 VLSM Torre Central | PB

Vlan	Red	Mascara	Broadcast	Rango
18	120.32.4.0	24	120.32.4.255	4.1-4.254
19	120.32.5.0	26	120.32.5.63	5.1-5.62
20	120.32.5.64	26	120.32.5.127	5.65-5.126
21	120.32.5.128	28	120.32.5.143	5.129-5.142
22	120.32.5.144	28	120.32.5.159	5.145-5.158

2.3.3 VLSM Torre Central | P1

Vlan	Red	Mascara	Broadcast	Rango
23	120.32.6.0	25	120.32.6.127	6.1-6.126
24	120.32.6.128	26	120.32.6.192	6.129-6.192
25	120.32.6.192	28	120.32.6.207	6.193-6.206
26	120.32.6.208	28	120.32.6.223	6.209-6.222

2.3.4 VLSM CNOR | PB

Vlan	Red	Mascara	Broadcast	Rango
30	120.32.7.0	24	120.32.7.255	7.1-7.254
31	120.32.8.0	24	120.32.8.255	8.1-8.254
32	120.32.9.0	25	120.32.9.255	9.1-9.254
33	120.32.10.0	25	120.32.10.127	10.1-10.126
34	120.32.10.128	28	120.32.10.143	10.129-10.142
35	120.32.10.144	28	120.32.10.159	10.145-10.158
36	120.32.10.160	28	120.32.10.175	10.161-10.174

2.3.5 VLSM CNOR | P1

Vlan	Red	Mascara	Broadcast	Rango
37	120.32.11.0	24	120.32.11.255	11.1-11.254
38	120.32.12.0	24	120.32.12.255	12.1-12.254
39	120.32.13.0	25	120.32.13.255	13.1-13.126
40	120.32.13.128	28	120.32.10.127	13.129-13.142
41	120.32.13.144	28	120.32.10.143	13.145-13.158

2.3.6 VLSM CT | P1

Vlan	Red	Mascara	Broadcast	Rango
50	120.32.14.0	24	120.32.14.255	14.1-14.254
51	120.32.15.0	24	120.32.15.255	15.1-15.254
52	120.32.16.0	24	120.32.16.255	16.1-16.254
53	120.32.17.0	24	120.32.17.255	17.1-17.254
54	120.32.18.0	28	120.32.18.15	18.1-18.14
55	120.32.18.16	28	120.32.18.31	18.17-18.30
56	120.32.18.32	28	120.32.18.47	18.33-18.46

2.3.7 VLSM CT | P2

Vlan	Red	Mascara	Broadcast	Rango
57	120.32.19.0	24	120.32.19.255	19.1-19.254
58	120.32.20.0	24	120.32.20.255	20.1-20.254
59	120.32.21.0	24	120.32.21.255	21.1-21.254
60	120.32.22.0	28	120.32.22.15	22.1-22.14
61	120.32.22.16	28	120.32.22.31	22.17-22.30

2.3.8 VLSM CGOP | PB

Vlan	Red	Mascara	Broadcast	Rango
70	120.32.23.0	24	120.32.23.255	23.1-23.254
71	120.32.24.0	24	120.32.24.255	24.1-24.254
72	120.32.25.0	24	120.32.25.255	25.1-25.254
73	120.32.26.0	25	120.32.26.127	26.1-26.126
74	120.32.26.128	28	120.32.26.143	26.129-26.142
75	120.32.26.144	28	120.32.26.159	26.145-26.158
76	120.32.26.160	28	120.32.26.175	26.161-26.174

2.3.9 VLSM CGOP | P1

Vlan	Red	Mascara	Broadcast	Rango
77	120.32.27.0	24	120.32.27.255	27.1-27.254
78	120.32.28.0	24	120.32.28.255	28.1-28.254
79	120.32.29.0	24	120.32.29.255	29.1-29.254
80	120.32.30.0	28	120.32.30.15	30.1-30.14
81	120.32.30.16	28	120.32.26.31	30.17-30.30

2.4 Definicion de VLANS

2.4.1 Torre Central | Nivel Plaza

VLAN	Nombre	Descripción
10	AtencionPublico_TC_NP	Red destinada a módulos de atención al público (recepción, informes). Conectividad para PCs de atención al usuario.
11	Invitados_TC_NP	VLAN para acceso de visitantes con restricciones, acceso a internet aislado de la red interna.
12	AdministracionDispositivos_TC	Red para administrar switches, access points y otros dispositivos de red gestionables.
13	TecnologiaInformatica_TC	VLAN dedicada al equipo de TI para gestión de infraestructura, mantenimiento y soporte técnico.
14	Administrativa_TC	Segmento de red para equipos del personal administrativo del hospital. Maneja sistemas internos, reportes y operaciones.
15	Telefonos_TC_1	Red IP exclusiva para teléfonos en el nivel plaza, permitiendo VoIP segura.
16	Servidores_TC	Red exclusiva para la conexión de servidores críticos de Torre Central. Asegura segmentación y alto rendimiento.
17	Camaras_TC_1	Segmento para cámaras de videovigilancia del nivel plaza, aislado para tráfico de video.

2.4.2 Torre Central | Planta Baja

VLAN	Nombre	Descripción
18	AtencionPublico_TC_PB	Red para atención al público en planta baja: recepción, cajas, información médica.
19	Administrativa_TC_2	Equipos del personal administrativo en esta planta (gestión interna y médica).
20	CajaMedicos_TC_PB	VLAN dedicada a los módulos de cobro y caja para personal médico.
21	Telefonos_TC_2	Red IP para teléfonos VoIP en planta baja.
22	Camaras_TC_2	Red exclusiva para cámaras de seguridad en planta baja.

2.4.3 Torre Central | Planta Baja

VLAN	Nombre	Descripción
23	Medicos_TC_P1	Red para estaciones de trabajo del personal médico en consultorios o áreas clínicas del primer piso.
24	Administrativa_TC_3	Red para el personal administrativo en áreas internas del piso 1.
25	Telefonos_TC_3	VLAN de telefonía IP para este nivel.
26	Camaras_TC_3	Red de videovigilancia en piso 1, tráfico segmentado para monitoreo.

2.4.4 CNOR | PB

VLAN	Nombre	Descripción
30	Invitados_CNOR	Red controlada de acceso para familiares y visitantes.
31	AdministracionDispositivos_CNOR	VLAN para gestionar switches, APs y cámaras IP de la zona.
32	Consulotrios_CNOR_PB	Red de consultorios médicos, dispositivos clínicos y PCs para consulta y registro.
33	Medicos_CNOR_PB	VLAN para estaciones de trabajo y dispositivos de médicos especialistas.
34	Telefonos_CNOR_1	Red IP para comunicación por VoIP en planta baja.
35	Servidores_CNOR	Red exclusiva para servidores locales del CNOR, con seguridad reforzada.
36	Camaras_CNOR_1	Red de cámaras de videovigilancia conectadas al sistema de monitoreo central.

2.4.5 CNOR | P1

VLAN	Nombre	Descripción
37	Aulas_CNOR_P1	Red para aulas y salas de capacitación del personal médico. Incluye proyectores, laptops y PCs.
38	Consultorios_CNOR_P1	Red de consultorios médicos del piso 1, acceso a expedientes clínicos y sistemas hospitalarios.
39	RezoJudip_CNOR_P1	VLAN dedicada a la sala de rezo, con dispositivos para transmisión, control ambiental o multimedia.
40	Telefonos_CNOR_2	Red de VoIP del primer piso.
41	Camaras_CNOR_2	Red de cámaras de vigilancia en esta planta.

2.4.6 CT | P1

VLAN	Nombre	Descripción
50	Administraciondispositivos_CT	VLAN para gestión de infraestructura de red (APs, switches, cámaras).
51	Invitados_CT_P1	Red para familiares, pacientes o proveedores con acceso a internet limitado.
52	Consultorios_CT_P1	Estaciones de trabajo y dispositivos clínicos para la atención médica.
53	Consultorios2_CT_P1	Expansión de red para más consultorios del mismo nivel.
54	Telefonos_CT_P1	Red de teléfonos IP para el personal de este piso.
55	Servidores_CT	Red de servidores internos que apoyan a los consultorios médicos.
56	Camaras_CT_1	Segmento de cámaras de videovigilancia en piso 1.

2.4.7 CT | P2

VLAN	Nombre	Descripción
57	Consultorios_CT_P2	Estaciones de médicos y personal clínico del segundo nivel.
58	Consultorios2_CT_P2	Consultorios adicionales con necesidades similares al anterior.
59	Invitados_CT_P2	Red abierta con restricciones para visitantes en el segundo piso.
60	Telefonos_CT_2	VLAN de telefonía IP para esta planta.
61	Camaras_CT_2	Tráfico de videovigilancia del piso 2.

2.4.8 CGOP | PB

VLAN	Nombre	Descripción
70	AtencionPublico_CGOP_PB	PCs de atención al público en recepción y áreas de admisión.
71	AdministracionDispositivos_CGOP	Red de gestión de infraestructura de red del edificio.
72	Invitados_CGOP	Acceso para familiares o visitantes, aislado de la red hospitalaria.
73	Administrativa_CGOP_1	Dispositivos administrativos, sistemas de gestión y archivos médicos.
74	Telefonos_CGOP_1	Red IP de telefonía para personal en planta baja.
75	Camaras_CGOP_1	Cámaras de vigilancia de planta baja, tráfico separado para monitoreo.
76	Servidores_CGOP	Red de servidores que gestionan servicios médicos y administrativos locales.

2.4.9 CGOP | P1

VLAN	Nombre	Descripción
77	Habitaciones_CGOP_P1	Red para habitaciones de hospitalización
78	Habitaciones_CGOP_2	Segmento adicional para habitaciones, posiblemente otra ala o sección.
79	Invitados_CGOP_P1	Red para visitantes en el primer piso.
80	Telefonos_CGOP_2	Comunicación IP para habitaciones o áreas clínicas.
81	Camaras_CGOP_2	Cámaras de videovigilancia en el primer piso del CGOP.

2.5 Diseño lógico de la red (Topología Lógica)

2.5.1 Vista General – Conexión entre edificios

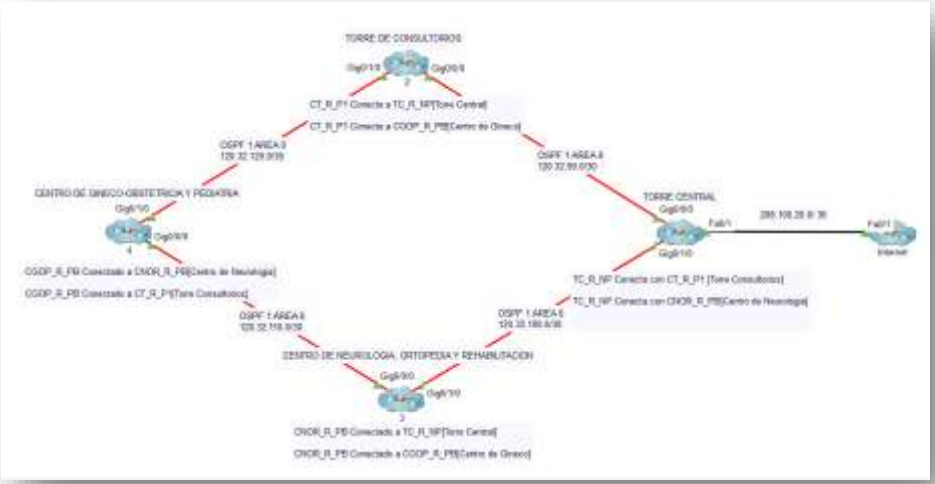


Ilustración 1

2.5.1 Tabla de direcciones IP (Red) | Torre Central a Torre de Consultorios

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 1	TC_R_NP	120.32.90.0	G0/0/0	120.32.90.1	30
	CT_R_P1		G0/0/0	120.32.90.2	30

2.5.2 Tabla de direcciones IP (Red) | Torre Central a Centro de Neurología

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 1	TC_R_NP	120.32.100.0	G0/1/0	120.32.100.1	30
	CNOR_R_PB		G0/1/0	120.32.100.2	30

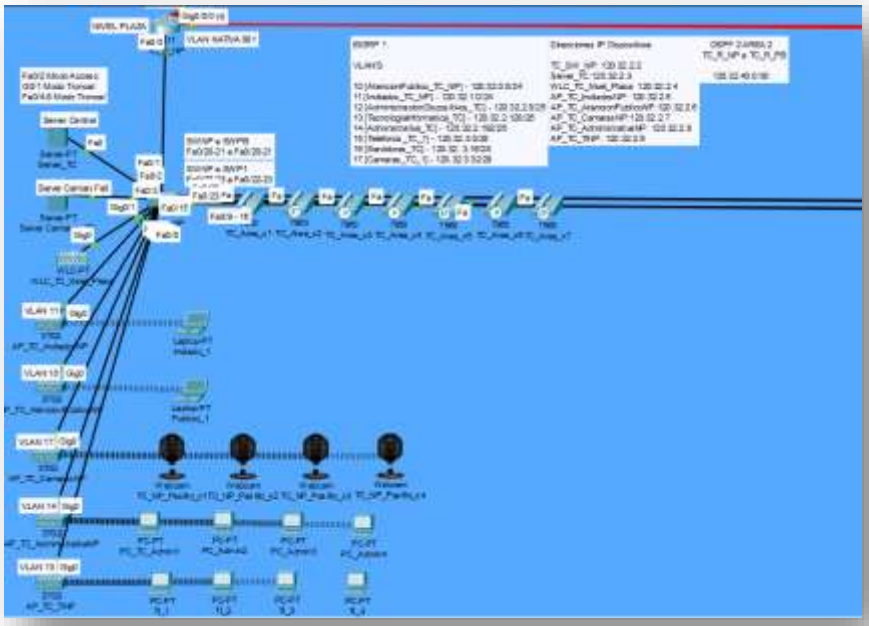
2.5.3 Tabla de direcciones IP (Red) | Centro de Neurología a Centro de Gineco

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 1	TC_R_NP	120.32.110.01	G0/0/0	120.32.110.1	30
	CGOP_R_PB		G0/0/0	120.32.110.2	30

2.5.4 Tabla de direcciones IP (Red) | Centro de Gineco a Torre de Consultorios

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 1	CT_R_P1	120.32.120.0	G0/1/0	120.32.120.1	30
	CGOP_R_PB		G0/1/0	120.32.120.2	30

2.5.2 Torre Central | Nivel Plaza – Conexión entre dispositivos



En esta ilustracion se muestra la torre central nivel plaza y todos los dispositivos que hayen este nivel, se observa un router, un switch, dos servidores (uno para camaras y el otro para telefonos) un WLC, 5 AP, 8 pcs, 4 camaras de vigilancia, 2 laptops y 7 telefonos.

2.5.5 EIGRP1 TC | NP

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 1	10	AtencionPublico_TC_NP	120.32.0.0	24
	11	Invitados_TC_NP	120.32.1.0	24
	12	AdministracionDispositivos_TC	120.32.2.0	25
	13	TecnologiaInformatica_TC	120.32.2.128	26
	14	Administrativa_TC	120.32.2.192	26
	15	Telefonos_TC_1	120.32.3.0	28
	16	Servidores_TC	120.32..3.16	28
	17	Camaras_TC_1	120.32.3.32	28

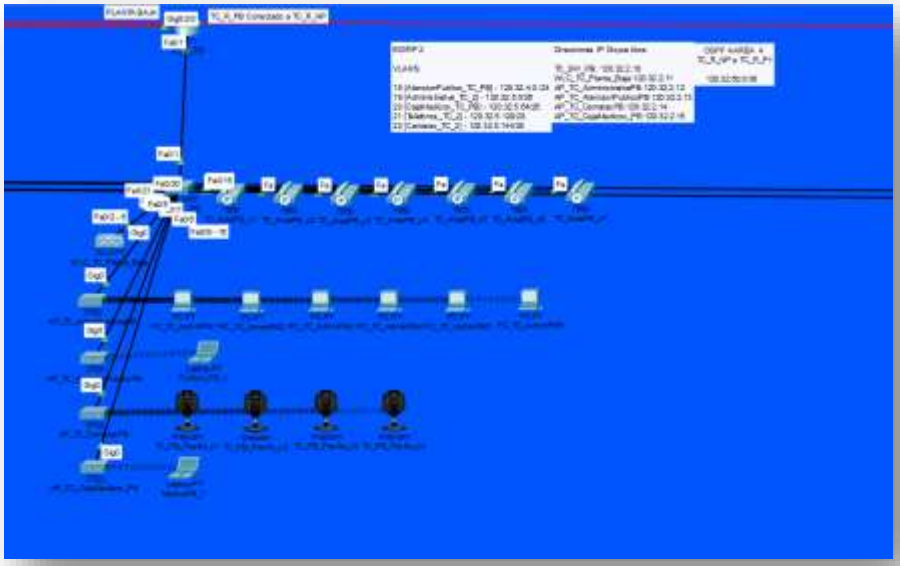
2.5.6 OSPF2 TC | NP

OSPF 2	Dispositivos	Red	Interfaz	Direccion IP	Mascara
	TC_R_NP	120.32.40.0	G0/2/0	120.32.40.1	30
	TC_R_PB		G0/2/0	120.32.40.2	30

2.5.7 OSPF4 TC | NP

OSPF 4	Dispositivos	Red	Interfaz	Direccion IP	Mascara
	TC_R_NP	120.32.50.0	G0/3/0	120.32.50.1	30
	TC_R_P1		G0/3/0	120.32.50.2	30

2.5.3 Torre Central | Planta Baja – Conexión entre dispositivos



En esta ilustracion se muestra la torre central (Planta baja) y todos los dispositivos que se encuentran en esta planta, se observa un router, un switch, un WLC, 4 AP, 2 laptops, 6 pcs, 4 camaras, y 7 telefonos.

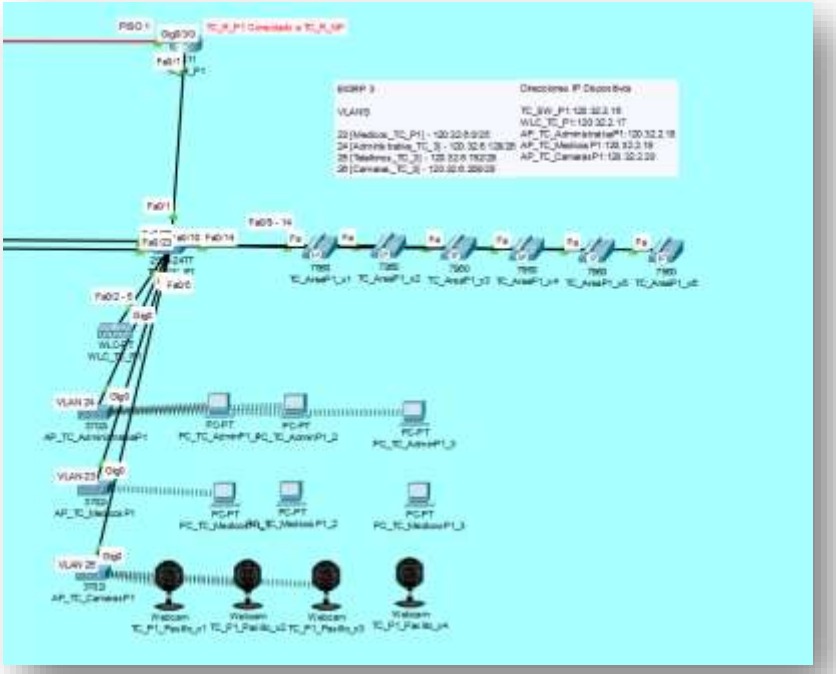
2.5.8 EIGRP2 TC | PB

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 2	18	AtencionPublico_TC_PB	120.32.4.0	24
	19	Administrativa_TC_2	120.32.5.0	26
	20	CajaMedicos_TC_PB	120.32.5.64	26
	21	Telefonos_TC_2	120.32.5.128	28
	22	Camaras_TC_2	120.32.5.144	28

2.5.9 OSPF2 TC | PB

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 2	TC_R_NP	120.32.40.0	G0/2/0	120.32.40.1	30
	TC_R_PB		G0/2/0	120.32.40.2	30

2.5.4 Torre Central | Piso 1 – Conexión entre dispositivos



En esta ilustracion se muestra la torre central (Piso 1) y todos los dispositivos que se encuentran en esta planta, se observa un router, un switch, 6 telefonos, 1 WLC, 3 AP, 6 pc's, y 4 camaras.

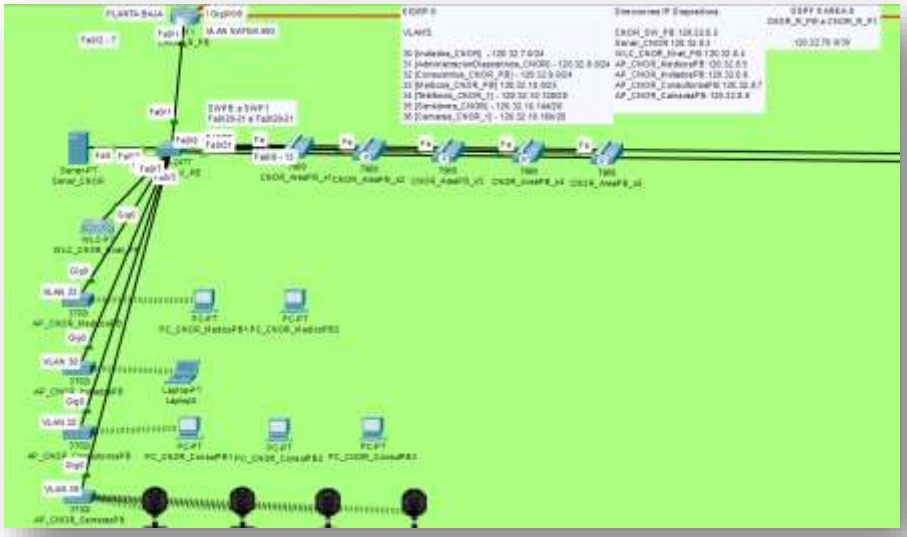
2.5.10 EIGRP3 TC | P1

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 3	23	Medicos_TC_P1	120.32.6.0	25
	24	Administrativa_TC_3	120.32.6.128	26
	25	Telefonos_TC_3	120.32.6.192	28
	26	Camaras_TC_3	120.32.6.208	26

2.5.11 OSPF4 TC | NP

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 4	TC_R_NP	120.32.50.0	G0/3/0	120.32.50.1	30
	TC_R_P1		G0/3/0	120.32.50.2	30

2.5.5 Centro de Neurología | Planta Baja – Conexión entre dispositivos



En esta ilustracion se muestra el centro de Neurologia (Planta baja) y todos los dispositivos que se encuentran en esta planta, se observa 1 router, 1 servidor, 1 switch, 5 telefonos, 1 WLC, 4 AP, 5 pc's(2 medicos, 3 consultorios),1 laptop, y 4 camaras.

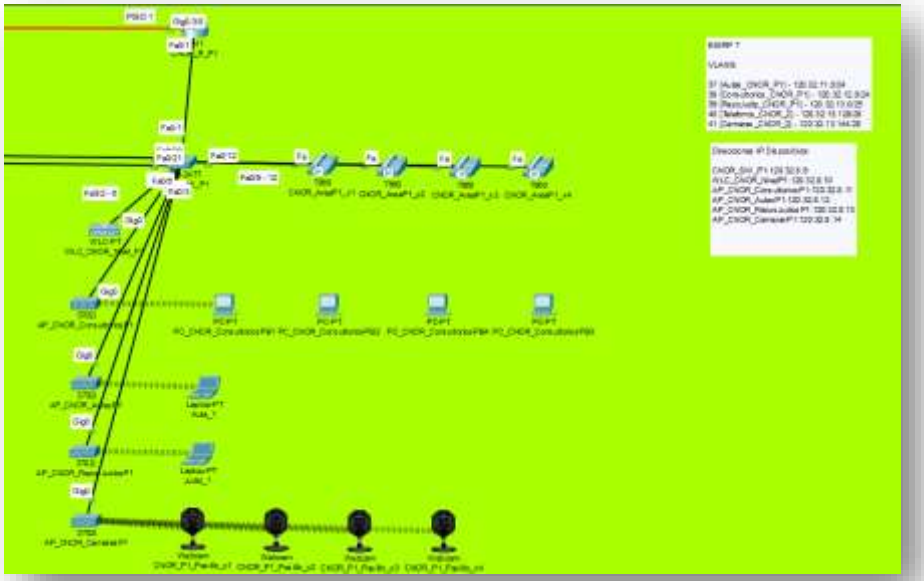
2.5.12 EIGRP6 CNOR | PB

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 6	30	Invitados_CNOR	120.32.7.0	24
	31	AdministracionDispositivos_CNOR	120.32.8.0	24
	32	Consulotrios_CNOR_PB	120.32.9.0	24
	33	Medicos_CNOR_PB	120.32.10.0	25
	34	Telefonos_CNOR_1	120.32.10.128	28
	35	Servidores_CNOR	120.32.10.144	28
	36	Camaras_CNOR_1	120.32.10.160	28

2.5.13 OSPF8 CNOR | PB

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 8	CNOR_R_PB	120.32.70.0	G0/3/0	120.32.70.1	30
	CNOR_R_P1		G0/3/0	120.32.70.2	30

2.5.6 Centro de Neurología | Piso 1 – Conexión entre dispositivos



En esta ilustracion se muestra el centro de Neurologia (Piso 1) y todos los dispositivos que se encuentran en esta planta, se observa 1 router, 1 switch, 4, telefonos, 1 WLC, 4 AP, 4 pc's, 2 laptops, y 4 camaras.

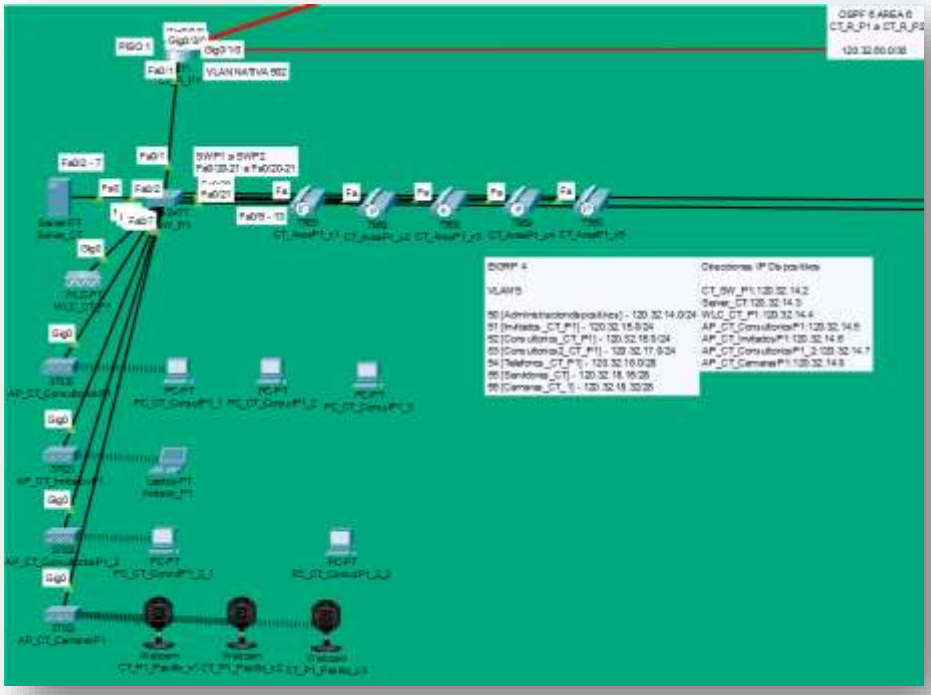
2.5.14 EIGRP7 CNOR | P1

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 7	37	Aulas_CNOR_P1	120.32.11.0	24
	38	Consultorios_CNOR_P1	120.32.12.0	24
	39	RezoJudip_CNOR_P1	120.32.13.0	25
	40	Telefonos_CNOR_2	120.32.13.128	28
	41	Camaras_CNOR_2	120.32.13.144	28

2.5.15 OSPF8 CNOR | P1

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 8	CNOR_R_PB	120.32.70.0	G0/3/0	120.32.70.1	30
	CNOR_R_P1		G0/3/0	120.32.70.2	30

2.5.7 Torre de Consultorios | Piso 1 – Conexión entre dispositivos



En esta ilustracion se muestra la torre de consultorios (Piso 1) y todos los dispositivos que se encuentran en esta planta, se observa 1 router, 1 servidor, 1 switch, 5 telefonos, 1 WLC, 4 AP, 5 pc's (consultorios planta baja 1 y 2), 2 laptops, y 3 camaras.

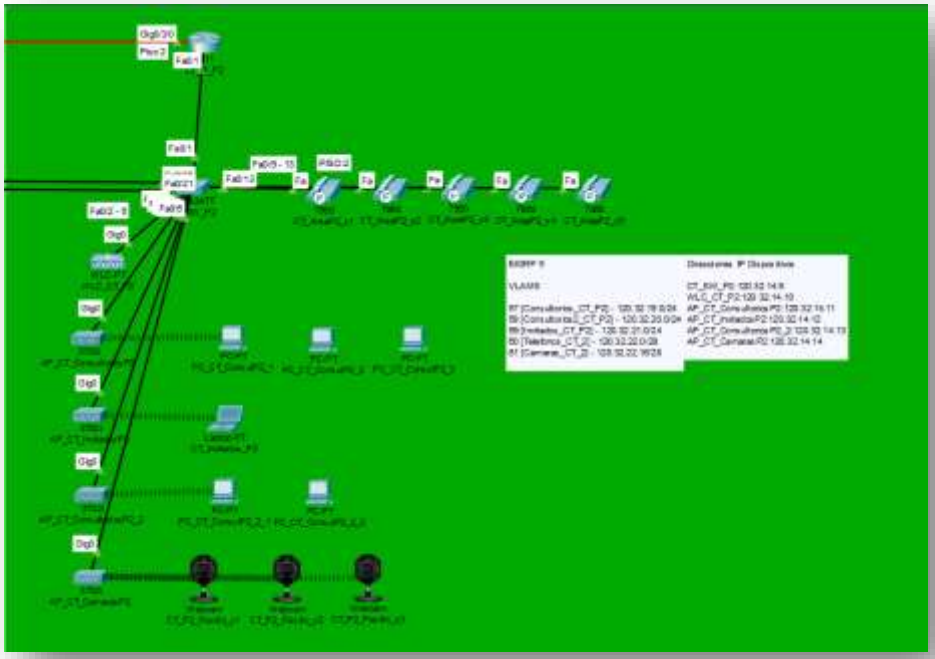
2.5.16 EIGRP4 CT | P1

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 4	50	Administraciondispositivos	120.32.14.0/24	24
	51	Invitados_CT_P1	120.32.15.0/24	24
	52	Consultorios_CT_P1	120.32.16.0/24	24
	53	Consultorios2_CT_P1	120.32.17.0/24	24
	54	Telefonos_CT_P1	120.32.18.0/28	28
	55	Servidores_CT	120.32.18.16/28	28
	56	Camaras_CT_1	120.32.18.32/28	28

2.5.17 OSPF6 CT | P1

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 6	CT_R_P1	120.32.60.0	G0/3/0	120.32.60.1	30
	CT_R_P2		G0/3/0	120.32.60.2	30

2.5.8 Torre de Consultorios | Piso 2 – Conexión entre dispositivos



En esta ilustracion se muestra la torre de consultorias (Piso 2) y todos los dispositivos que se encuentran en esta planta, se observa 1 router, 1 switch, 1 WLC, 4 AP, 5 telefonos, 5 pc's (consultorios), 1 laptop, y 3 camaras.

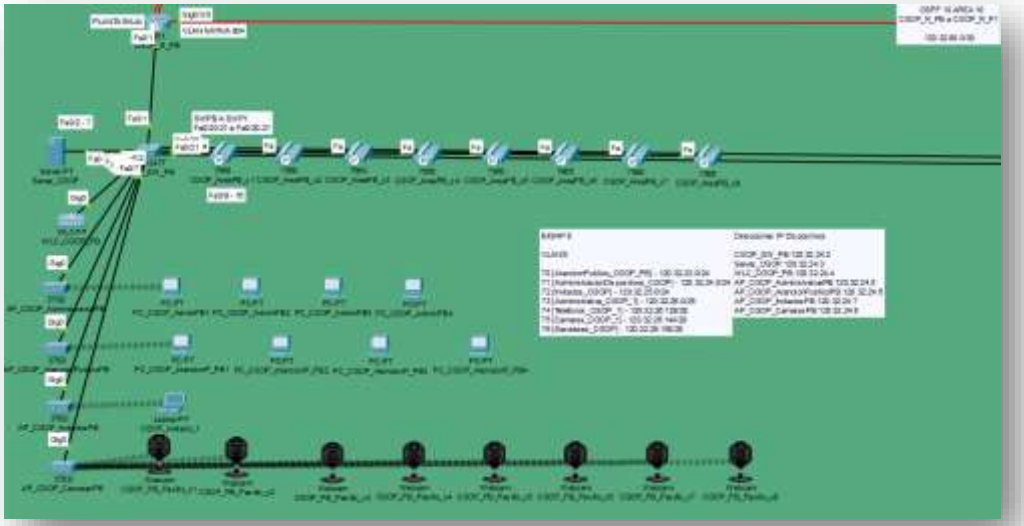
2.5.18 EIGRP5 CT | P2

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 5	57	Consultorios_CT_P2	120.32.19.0/24	24
	58	Consultorios2_CT_P2	120.32.20.0/24	24
	59	Invitados_CT_P2	120.32.21.0/24	24
	60	Telefonos_CT_2	120.32.22.0/28	28
	61	Camaras_CT_2	120.32.22.16/28	28

2.5.19 OSPF6 CT | P2

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 6	CT_R_P1	120.32.60.0	G0/3/0	120.32.60.1	30
	CT_R_P2		G0/3/0	120.32.60.2	30

2.5.9 Centro de Gineco | Planta Baja – Conexión entre dispositivos



En esta ilustracion se muestra el centro de Ginecologia (Planta baja) y todos los dispositivos que se encuentran en esta plan ta, se observa 1 router, 1 servidor, 1 switch, 1 WLC, 4 AP, 8 pc's, 8 telefonos, 1 laptop, y 8 camaras.

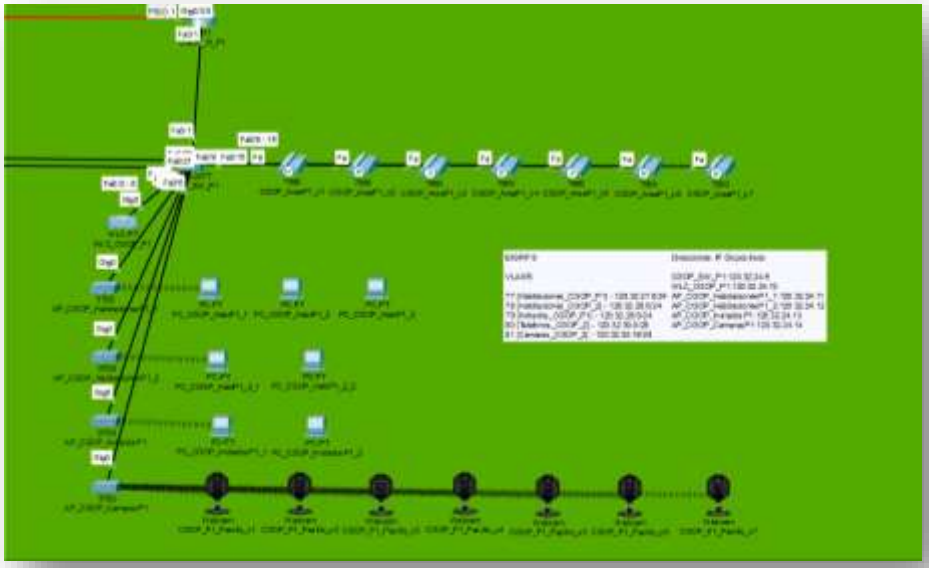
2.5.20 EIGRP8 CGOP | PB

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 8	70	AtencionPublico_CGOP_PB	120.32.23.0	24
	71	AdministracionDispositivos_CGOP	120.32.24.0	24
	72	Invitados_CGOP	120.32.25.0	24
	73	Administrativa_CGOP_1	120.32.26.0	25
	74	Telefonos_CGOP_1	120.32.26.128	28
	75	Camaras_CGOP_1	120.32.26.144	28
	76	Servidores_CGOP	120.32.26.160	28

2.5.21 OSPF10 CGOP | PB

	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 10	CGOP_R_PB	120.32.80.0	G0/3/0	120.32.80.1	30
	CGOP_R_P1		G0/3/0	120.32.80.2	30

2.5.10 Centro de Gineco | Piso 1 – Conexión entre dispositivos



En esta ilustracion se muestra el centro de Ginecologia (Piso 1) y todos los dispositivos que se encuentran en esta planta, se observa 1 router, 1 switch, 1 WLC, 4 AP, 7 telefonos, 7 pc's, y 7 camaras.

2.5.22 EIGRP9 CGOP | P1

	Num VLAN	Nombre de VLAN	Red	Mascara
EIGRP 9	77	Habitaciones_CGOP_P1	120.32.27.0	24
	78	Habitaciones_CGOP_2	120.32.28.0	24
	79	Invitados_CGOP_P1	120.32.29.0	24
	80	Telefonos_CGOP_2	120.32.30.0	28
	81	Camaras_CGOP_2	120.32.30.16	28

2.5.23 OSPF10 CGOP | P1

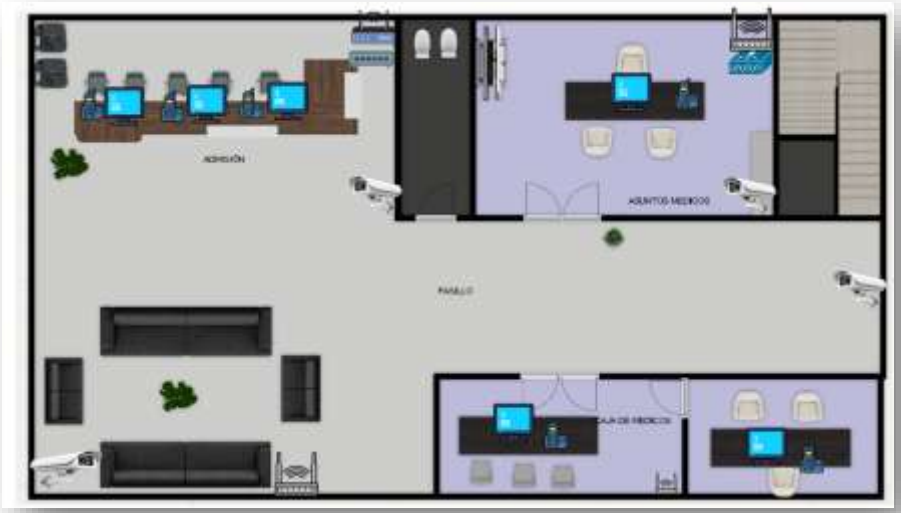
	Dispositivos	Red	Interfaz	Direccion IP	Mascara
OSPF 10	CGOP_R_PB	120.32.80.0	G0/3/0	120.32.80.1	30
	CGOP_R_P1		G0/3/0	120.32.80.2	30

2.6 Diagramas físicos (Ubicación de dispositivos)

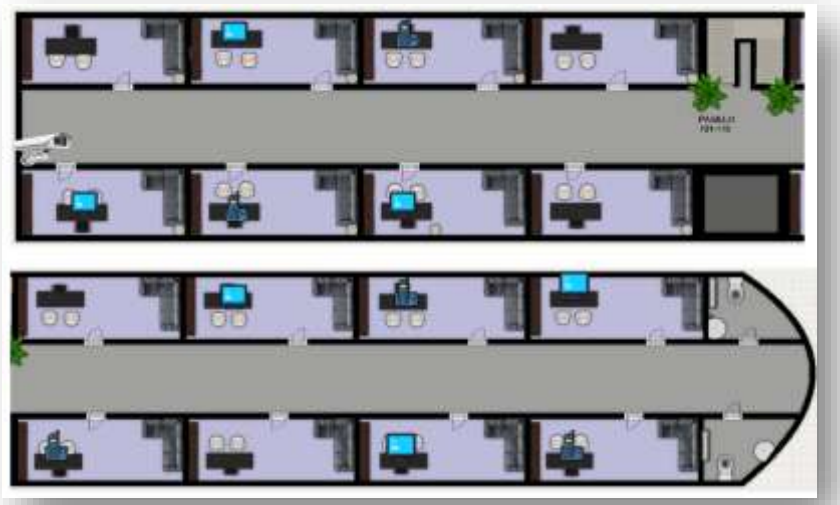
2.6.1 Diagrama físico TC | NP

2.6.2 Diagrama físico TC | PB

2.6.3 Diagrama físico TC | P1

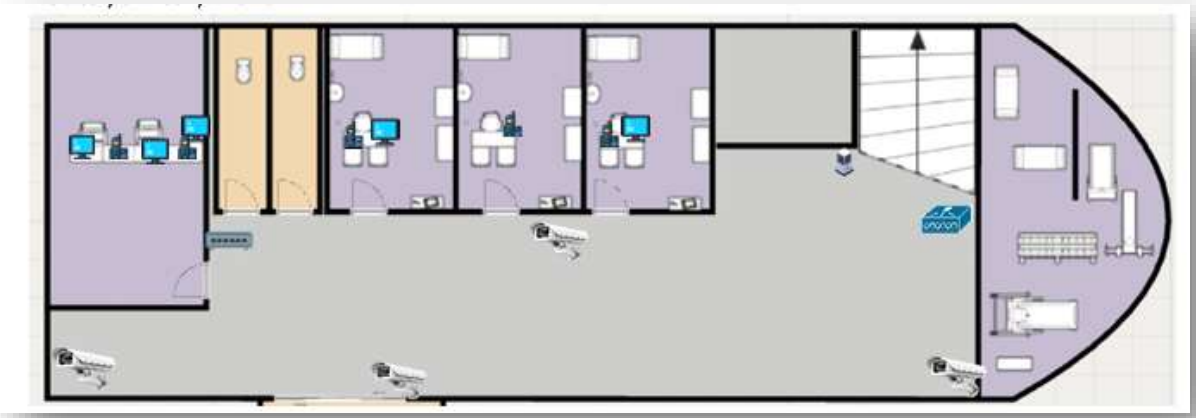


2.6.4 Diagrama físico CT | P1

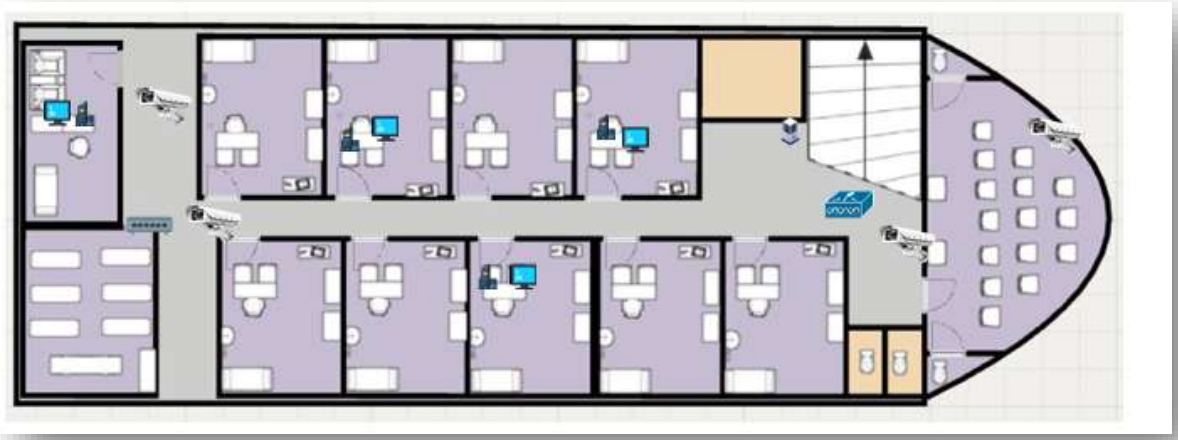


2.6.5 Diagrama físico CT | P2

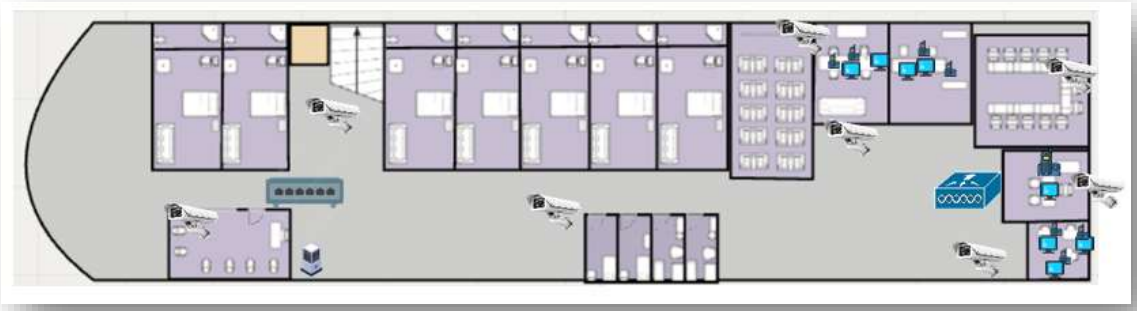
2.6.6 Diagrama físico CNOR | PB



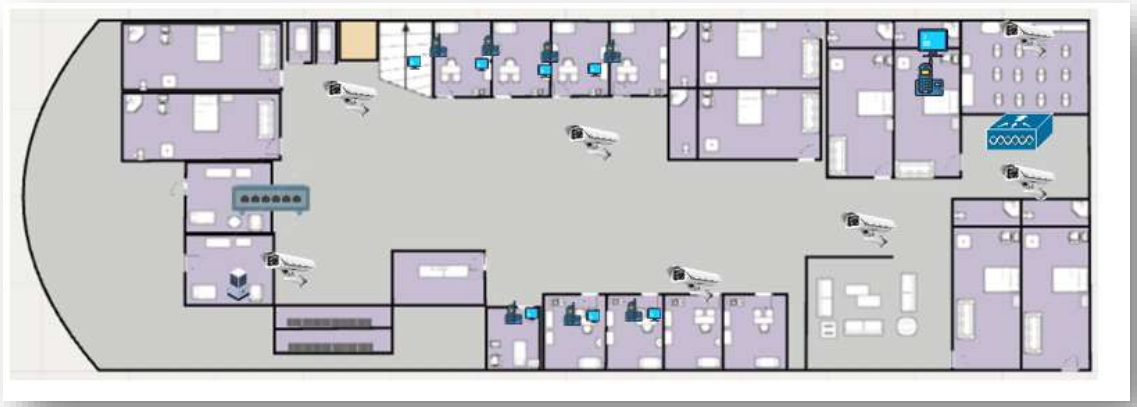
2.6.7 Diagrama físico CNOR | P1



2.6.8 Diagrama físico CGOP | PB



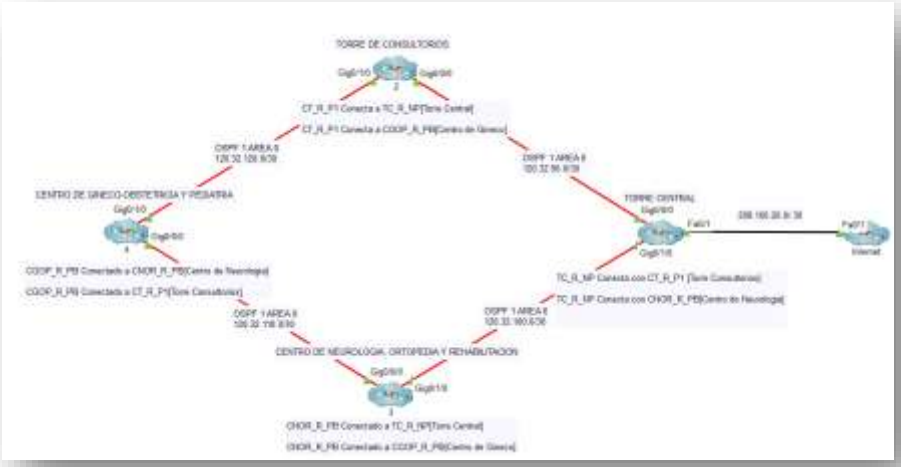
2.6.9 Diagrama físico CGOP | P1



Fase 3

3.1 Conexiones y Topología

3.1.1 Conexión entre routers centrales



En la ilustración se observa toda la topologia de la red de todos los ediciones, se observa 5 clousters, 4 para cada edicfio (torre central, gineco, torre de consultorios, y neurología) y otro representa el Internet

3.1.1 Conexiones de Router (1) | Torre Central

Dispositivos conectados	Interfaz	Interfaz
Routers TC_R_NP a CT_R_P1	G0/0/0	G0/0/0
Routers TC_R_NP a CNOR_R_PB	G0/1/0	G0/1/0

3.1.2 Conexiones de Router (2) | CNOR

Dispositivos conectados	Interfaz	Interfaz
Routers CT_R_P1 a TC_R_NP	G0/0/0	G0/0/0
Routers CT_R_P1 a CGOP_R_PB	G0/1/0	G0/1/0

3.1.3 Conexiones de Router (3) | CNOR

Dispositivos conectados	Interfaz	Interfaz
Routers CNOR_R_PB a TC_R_NP	G0/1/0	G0/1/0
Routers CNOR_R_PB a CGOP_R_PB	G0/0/0	G0/0/0

3.1.4 Conexiones de Router (4) | CGOP

Dispositivos conectados	Interfaz	Interfaz
Routers CGOP_R_PB a CT_R_P1	G0/1/0	G0/1/0
Routers CGOP_R_PB a CNOR_R_PB	G0/0/0	G0/0/0

3.1.5 Conexión de dispositivos | Torre central | Nivel Plaza

Dispositivos conectados	Interfaz	Interfaz
Routers TC_R_NP a TC_R_PB	G0/2/0	G0/2/0
Routers TC_R_NP a TC_R_P1	G0/3/0	G0/3/0
Routers TC_R_NP a Internet	Fa0/1	Fa0/1
Router TC_R_NP a TC_SW_NP	Fa0/0	Fa0/1
Switch TC_SW_NP a Server_TC	Fa0/2	Fa0/0
Switch TC_SW_NP a Server_Camaras_TC	Fa0/3	Fa0/0
Switch TC_SW_NP a WLC_TC_NP	G0/1	Gig0
Switch TC_SW_NP a AP_TC_InvitadosNP	Fa0/4	Gig0
Switch TC_SW_NP a AP_TC_AtencionPublicoNP	Fa0/5	Gig0
Switch TC_SW_NP a AP_TC_CamarasNP	Fa0/6	Gig0
Switch TC_SW_NP a AP_TC_AdministrativaNP	Fa0/7	Gig0
Switch TC_SW_NP a AP_TC_TINP	Fa0/8	Gig0
Switch TC_SW_NP a TC_Area_x1 [Telefono]	Fa0/9	Switch
Switch TC_SW_NP a TC_Area_x2 [Telefono]	Fa0/10	Switch
Switch TC_SW_NP a TC_Area_x3 [Telefono]	Fa0/11	Switch
Switch TC_SW_NP a TC_Area_x4 [Telefono]	Fa0/12	Switch
Switch TC_SW_NP a TC_Area_x5 [Telefono]	Fa0/13	Switch
Switch TC_SW_NP a TC_Area_x6 [Telefono]	Fa0/14	Switch
Switch TC_SW_NP a TC_Area_x7 [Telefono]	Fa0/15	Switch

3.1.6 Conexión de dispositivos | Torre central | PB

Dispositivos conectados	Interfaz	Interfaz
Routers TC_R_PB a TC_R_NP	G0/2/0	G0/2/0
Router TC_R_PB a TC_SW_PB	Fa0/1	Fa0/1
Switch TC_SW_PB a WLC_TC_PB	Fa0/2	Gig0
Switch TC_SW_PB a AP_TC_AdministrativaPB	Fa0/3	Gig0
Switch TC_SW_PB a AP_TC_AtencionPublicoPB	Fa0/4	Gig0
Switch TC_SW_PB a AP_TC_CamarasPB	Fa0/5	Gig0
Switch TC_SW_PB a AP_TC_CajaMedicosPB	Fa0/6	Gig0
Switch TC_SW_PB a TC_AreaPB_x1 [Telefono]	Fa0/9	Switch
Switch TC_SW_PB a TC_AreaPB_x2 [Telefono]	Fa0/10	Switch
Switch TC_SW_PB a TC_AreaPB_x3 [Telefono]	Fa0/11	Switch
Switch TC_SW_PB a TC_AreaPB_x4 [Telefono]	Fa0/12	Switch
Switch TC_SW_PB a TC_AreaPB_x5 [Telefono]	Fa0/13	Switch
Switch TC_SW_PB a TC_AreaPB_x6 [Telefono]	Fa0/14	Switch
Switch TC_SW_PB a TC_AreaPB_x7 [Telefono]	Fa0/15	Switch

3.1.7 Conexión de dispositivos | Torre central | Piso 1

Dispositivos conectados	Interfaz	Interfaz
Routers TC_R_P1 a TC_R_NP	G0/3/0	G0/3/0
Router TC_R_P1 a TC_SW_P1	Fa0/1	Fa0/1
Switch TC_SW_P1 a WLC_TC_P1	Fa0/2	Gig0
Switch TC_SW_P1 a AP_TC_AdministrativaP1	Fa0/3	Gig0
Switch TC_SW_P1 a AP_TC_MedicosP1	Fa0/4	Gig0
Switch TC_SW_P1 a AP_TC_CamarasP1	Fa0/5	Gig0
Switch TC_SW_P1 a TC_AreaP1_x1 [Telefono]	Fa0/9	Switch
Switch TC_SW_P1 a TC_AreaP1_x2 [Telefono]	Fa0/10	Switch
Switch TC_SW_P1 a TC_AreaP1_x3 [Telefono]	Fa0/11	Switch
Switch TC_SW_P1 a TC_AreaP1_x4 [Telefono]	Fa0/12	Switch
Switch TC_SW_P1 a TC_AreaP1_x5 [Telefono]	Fa0/13	Switch
Switch TC_SW_P1 a TC_AreaP1_x6 [Telefono]	Fa0/14	Switch

3.1.8 Conexión de dispositivos | Torre de Consultorios | Piso 1

Dispositivos conectados	Interfaz	Interfaz
Routers CT_R_P1 a CT_R_P2	G0/3/0	G0/3/0
Router CT_R_P1 a CT_SW_P1 [Switch]	Fa0/1	Fa0/1
Switch CT_SW_P1 a Server_CT	Fa0/2	Fa0/0
Switch CT_SW_P1 a WLC_CT_P1	Fa0/3	Gig0
Switch CT_SW_P1 a AP_CT_ConsultoriosP1	Fa0/4	Gig0
Switch CT_SW_P1 a AP_CT_InvitadosP1	Fa0/5	Gig0
Switch CT_SW_P1 a AP_CT_ConsultoriosP1_2	Fa0/6	Gig0
Switch CT_SW_P1 a AP_CT_CamarasP1	Fa0/7	Gig0
Switch CT_SW_P1 a CT_AreaP1_x1	Fa0/9	Switch
Switch CT_SW_P1 a CT_AreaP1_x2	Fa0/10	Switch
Switch CT_SW_P1 a CT_AreaP1_x3	Fa0/11	Switch
Switch CT_SW_P1 a CT_AreaP1_x4	Fa0/12	Switch
Switch CT_SW_P1 a CT_AreaP1_x5	Fa0/13	Switch

3.1.9 Conexión de dispositivos | Torre de Consultorios | Piso 2

Dispositivos conectados	Interfaz	Interfaz
Routers CT_R_P2 a CT_R_P1	G0/3/0	G0/3/0
Router CT_R_P2 a CT_SW_P2 [Switch]	Fa0/1	Fa0/1
Switch CT_SW_P2 a WLC_CT_P1	Fa0/2	Gig0
Switch CT_SW_P2 a AP_CT_ConsultoriosP2	Fa0/3	Gig0
Switch CT_SW_P2 a AP_CT_InvitadosP2	Fa0/4	Gig0
Switch CT_SW_P2 a AP_CT_ConsultoriosP2_2	Fa0/5	Gig0
Switch CT_SW_P2 a AP_CT_CamarasP2	Fa0/6	Gig0
Switch CT_SW_P2 a CT_AreaP2_x1	Fa0/9	Switch
Switch CT_SW_P2 a CT_AreaP2_x2	Fa0/10	Switch
Switch CT_SW_P2 a CT_AreaP2_x3	Fa0/11	Switch
Switch CT_SW_P2 a CT_AreaP2_x4	Fa0/12	Switch
Switch CT_SW_P2 a CT_AreaP2_x5	Fa0/13	Switch

3.1.10 Conexión de dispositivos | CNOR | Planta Baja

Dispositivos conectados	Interfaz	Interfaz
Routers CNOR_R_PB a CNOR_R_P1	G0/3/0	G0/3/0
Router CNOR_R_PB a CNOR_SW_PB [Switch]	Fa0/1	Fa0/1
Switch CNOR_SW_PB a Server_CNOR	Fa0/2	Fa0/0
Switch CNOR_SW_PB _P1 a WLC_CNOR_PB	Fa0/3	Gig0
Switch CNOR_SW_PB a AP_CNOR_MedicosPB	Fa0/4	Gig0
Switch CNOR_SW_PB a AP_CNOR_InvitadosPB	Fa0/5	Gig0
Switch CNOR_SW_PB a AP_CNOR_ConsultoriosPB	Fa0/6	Gig0
Switch CNOR_SW_PB a AP_CNOR_CamarasPB	Fa0/7	Gig0
Switch CNOR_SW_PB a CNOR_AreaPB_x1	Fa0/9	Switch
Switch CNOR_SW_PB a CNOR_AreaPB_x2	Fa0/10	Switch
Switch CNOR_SW_PB a CNOR_AreaPB_x3	Fa0/11	Switch
Switch CNOR_SW_PB a CNOR_AreaPB_x4	Fa0/12	Switch
Switch CNOR_SW_PB a CNOR_AreaPB_x5	Fa0/13	Switch

3.1.11 Conexión de dispositivos | CNOR | Piso 1

Dispositivos conectados	Interfaz	Interfaz
Routers CNOR_R_P1 a CNOR_R_PB	G0/3/0	G0/3/0
Router CNOR_R_PB a CNOR_SW_P1 [Switch]	Fa0/1	Fa0/1
Switch CNOR_SW_P1 _P1 a WLC_CNOR_P1	Fa0/2	Gig0
Switch CNOR_SW_P1 a AP_CNOR_ConsultoriosP1	Fa0/3	Gig0
Switch CNOR_SW_P1 a AP_CNOR_AulasP1	Fa0/4	Gig0
Switch CNOR_SW_P1 a AP_CNOR_RezosJudiosP1	Fa0/5	Gig0
Switch CNOR_SW_P1 a AP_CNOR_CamarasP1	Fa0/6	Gig0
Switch CNOR_SW_P1 a CNOR_AreaP1_x1	Fa0/9	Switch
Switch CNOR_SW_P1 a CNOR_AreaP1_x2	Fa0/10	Switch
Switch CNOR_SW_P1 a CNOR_AreaP1_x3	Fa0/11	Switch
Switch CNOR_SW_P1 a CNOR_AreaP1_x4	Fa0/12	Switch

3.1.12 Conexión de dispositivos | CGOP | Planta Baja

Dispositivos conectados	Interfaz	Interfaz
Routers CGOP_R_PB a CGOP_R_P1	G0/3/0	G0/3/0
Router CGOP_R_PB a CGOP_SW_PB	Fa0/1	Fa0/1
Switch CGOP_SW_PB a Server_CGOP	Fa0/2	Fa0/0
Switch CGOP_SW_PB a WLC_CGOP_PB	Fa0/3	Gig0
Switch CGOP_SW_PB a AP_CGOP_AdministrativaPB	Fa0/4	Gig0
Switch CGOP_SW_PB a AP_ CGOP _AtencionPublicoPB	Fa0/5	Gig0
Switch CGOP_SW_PB a AP_ CGOP _InvitadosPB	Fa0/6	Gig0
Switch CGOP_SW_PB a AP_ CGOP _CamarasPB	Fa0/7	Gig0
Switch CGOP_SW_PB a CGOP _AreaPB_x1 [Telefono]	Fa0/9	Switch
Switch CGOP_SW_PB a CGOP _AreaPB_x2 [Telefono]	Fa0/10	Switch
Switch CGOP_SW_PB a CGOP _AreaPB_x3 [Telefono]	Fa0/11	Switch
Switch CGOP_SW_PB a CGOP _AreaPB_x4 [Telefono]	Fa0/12	Switch
Switch CGOP_SW_PB a CGOP _AreaPB_x5 [Telefono]	Fa0/13	Switch
Switch CGOP_SW_PB a CGOP _AreaPB_x6 [Telefono]	Fa0/14	Switch
Switch CGOP _SW_PB a CGOP _AreaPB_x7 [Telefono]	Fa0/15	Switch
Switch CGOP _SW_PB a CGOP _AreaPB_x8 [Telefono]	Fa0/16	Switch

3.1.13 Conexión de dispositivos | CGOP | Piso 1

Dispositivos conectados	Interfaz	Interfaz
Routers CGOP_R_P1 a CGOP_R_PB	G0/3/0	G0/3/0
Router CGOP_R_P1 a CGOP_SW_P1	Fa0/1	Fa0/1
Switch CGOP_SW_P1 a WLC_CGOP_P1	Fa0/2	Gig0
Switch CGOP_SW_P1 a AP_CGOP_HabitacionesP1_1	Fa0/3	Gig0
Switch CGOP_SW_P1 a AP_ CGOP _ HabitacionesP1_2	Fa0/4	Gig0
Switch CGOP_SW_P1 a AP_ CGOP _InvitadosP1	Fa0/5	Gig0
Switch CGOP_SW_P1 a AP_ CGOP _CamarasP1	Fa0/6	Gig0
Switch CGOP_SW_P1 a CGOP _AreaP1_x1 [Telefono]	Fa0/9	Switch
Switch CGOP_SW_P1 a CGOP _AreaP2_x2 [Telefono]	Fa0/10	Switch
Switch CGOP_SW_P1 a CGOP _AreaP3_x3 [Telefono]	Fa0/11	Switch
Switch CGOP_SW_P1 a CGOP _AreaP4_x4 [Telefono]	Fa0/12	Switch
Switch CGOP_SW_P1 a CGOP _AreaP5_x5 [Telefono]	Fa0/13	Switch
Switch CGOP_SW_P1 a CGOP _AreaP6_x6 [Telefono]	Fa0/14	Switch
Switch CGOP _SW_P1 a CGOP _AreaP7_x7 [Telefono]	Fa0/15	Switch

3.2 Tablas de direcciones IP

3.2.1 Torre Central | Nivel Plaza

Dispositivos	Interfaz	Direccion IP	Mascara
TC_R_NP	G0/0/0	120.32.90.1	30
	G0/1/0	120.32100.1	30
	G0/2/0	120.32.40.1	30
	G0/3/0	120.32.50.1	30
	Fa0/0.10	120.32.0.1	24
	Fa0/0.11	120.32.1.1	24
	Fa0/0.12	120.32.2.1	25
	Fa0/0.13	120.32.2.129	26
	Fa0/0.14	120.32.2.193	26
	Fa0/0.15	120.32.3.1	28
	Fa0/0.16	120.32.3.17	28
	Fa0/0.17	120.32.3.33	28
	Fa0/1	208.100.20.1	30
TC_SW_NP	Vlan 12	120.32.2.2	25
Server_TC	Fa0	120.32.3.18	28
Server Camaras_TC	Fa0	120.32.3.19	28
WLC_TC_NP	Gig0	120.32.2.4	25
AP_TC_InvitadosNP	Gig0	120.32.2.5	25
AP_TC_AtencionPublicoNP	Gig0	120.32.2.6	25
AP_TC_CamarasNP	Gig0	120.32.2.7	25
AP_TC_AdministrativaNP	Gig0	120.32.2.8	25
AP_TC_TINP	Gig0	120.32.2.9	25
TC_Area_x1 [Teléfono]	Vlan 15	120.32.3.2	28
TC_Area_x2 [Teléfono]	Vlan 15	120.32.3.3	28
TC_Area_x3 [Teléfono]	Vlan 15	120.32.3.4	28
TC_Area_x4 [Teléfono]	Vlan 15	120.32.3.5	28
TC_Area_x5 [Teléfono]	Vlan 15	120.32.3.6	28
TC_Area_x6 [Teléfono]	Vlan 15	120.32.3.7	28
TC_Area_x7 [Teléfono]	Vlan 15	120.32.3.8	28
TC_NP_Pasillo_x1 [Cámara]	Wireless0	120.32.3.34	28
TC_NP_Pasillo_x2 [Cámara]	Wireless0	120.32.3.35	28
TC_NP_Pasillo_x3 [Cámara]	Wireless0	120.32.3.36	28
TC_NP_Pasillo_x4 [Cámara]	Wireless0	120.32.3.37	28
PC_TC_Admin1	Wireless0	120.32.2.194	26
PC_TC_Admin2	Wireless0	120.32.2.195	26
PC_TC_Admin3	Wireless0	120.32.2.196	26
PC_TC_Admin4	Wireless0	120.32.2.197	26
TI_1	Wireless0	120.32.2.130	26
TI_2	Wireless0	120.32.2.131	26
TI_3	Wireless0	120.32.2.132	26
TI_4	Wireless0	120.32.2.133	26

3.2.2 Torre Central | Planta Baja

Dispositivos	Interfaz	Direccion IP	Mascara
TC_R_PB	G0/2/0	120.32.40.2	30
	Fa0/1.18	120.32.4.1	24
	Fa0/1.19	120.32.5.1	26
	Fa0/1.20	120.32.5.65	26
	Fa0/1.21	120.32.5.129	28
	Fa0/1.22	120.32.5.145	28
TC_SW_NP	Vlan 12	120.32.2.10	25
WLC_TC_NP	Gig0	120.32.2.11	25
AP_TC_InvitadosNP	Gig0	120.32.2.12	25
AP_TC_AtencionPublicoNP	Gig0	120.32.2.13	25
AP_TC_CamarasNP	Gig0	120.32.2.14	25
AP_TC_AdministrativaNP	Gig0	120.32.2.15	25
TC_AreaPB_x1 [Teléfono]	Vlan 15	120.32.5.130	28
TC_AreaPB_x2 [Teléfono]	Vlan 15	120.32. 5.131	28
TC_AreaPB_x3 [Teléfono]	Vlan 15	120.32. 5.132	28
TC_AreaPB_x4 [Teléfono]	Vlan 15	120.32. 5.133	28
TC_AreaPB_x5 [Teléfono]	Vlan 15	120.32. 5.134	28
TC_AreaPB_x6 [Teléfono]	Vlan 15	120.32. 5.135	28
TC_AreaPB_x7 [Teléfono]	Vlan 15	120.32. 5.136	28
TC_PB_Pasillo_x1 [Cámara]	Wireless0	120.32.5.146	28
TC_PB_Pasillo_x2 [Cámara]	Wireless0	120.32.5.147	28
TC_PB_Pasillo_x3 [Cámara]	Wireless0	120.32.5.148	28
TC_PB_Pasillo_x4 [Cámara]	Wireless0	120.32.5.149	28
PC_TC_AdminPB1	Wireless0	120.32.5.2	26
PC_TC_AdminPB2	Wireless0	120.32. 5.3	26
PC_TC_AdminPB3	Wireless0	120.32. 5.4	26
PC_TC_AdminPB4	Wireless0	120.32. 5.5	26
PC_TC_AdminPB5	Wireless0	120.32.5.6	26
PC_TC_AdminPB6	Wireless0	120.32. 5.7	26

3.2.3 Torre Central | Piso 1

Dispositivos	Interfaz	Direccion IP	Mascara
TC_R_P1	G0/3/0	120.32.50.2	30
	Fa0/1.23	120.32.4.1	25
	Fa0/1.24	120.32.5.1	26
	Fa0/1.25	120.32.5.65	28
	Fa0/1.26	120.32.5.129	28
TC_SW_ P1	Vlan 12	120.32.2.16	25
WLC_TC_ P1	Gig0	120.32.2.17	25
AP_TC_Administrativa P1	Gig0	120.32.2.18	25
AP_TC_MedicosP1	Gig0	120.32.2.19	25
AP_TC_Camaras P1	Gig0	120.32.2.20	25
TC_Area P1_x1 [Teléfono]	Vlan 15	120.32.6.194	28
TC_Area P1_x2 [Teléfono]	Vlan 15	120.32.6.195	28
TC_Area P1_x3 [Teléfono]	Vlan 15	120.32.6.196	28
TC_Area P1_x4 [Teléfono]	Vlan 15	120.32.6.197	28
TC_Area P1_x5 [Teléfono]	Vlan 15	120.32.6.198	28
TC_Area P1_x6 [Teléfono]	Vlan 15	120.32.6.199	28
TC_ P1_Pasillo_x1 [Cámara]	Wireless0	120.32.6.210	28
TC_ P1_Pasillo_x2 [Cámara]	Wireless0	120.32.6.211	28
TC_ P1_Pasillo_x3 [Cámara]	Wireless0	120.32.6.212	28
TC_ P1_Pasillo_x4 [Cámara]	Wireless0	120.32.6.213	28
PC_TC_Admin P1_1	Wireless0	120.32.6.130	26
PC_TC_Admin P1_2	Wireless0	120.32.6.131	26
PC_TC_Admin P1_3	Wireless0	120.32.6.132	26
PC_TC_MedicosP1_1	Wireless0	120.32.6.2	25
PC_TC_ MedicosP1_2	Wireless0	120.32.6.3	25
PC_TC_ MedicosP1_3	Wireless0	120.32.6.4	25

3.2.4 Torre de Consultorios | Piso 1

Dispositivos	Interfaz	Direccion IP	Mascara
CT_R_P1	G0/0/0	120.32.90.2	30
	G0/1/0	120.32120.1	30
	G0/3/0	120.32.60.1	30
	Fa0/1.50	120.32.14.1	24
	Fa0/1.51	120.32.15.1	24
	Fa0/1.52	120.32.16.1	24
	Fa0/1.53	120.32.17.1	24
	Fa0/1.54	120.32.18.1	28
	Fa0/1.55	120.32.18.17	28
	Fa0/1.56	120.32. 18.33	28
CT_SW_P1	Vlan 50	120.32.14.2	24
Server_CT	Fa0	120.32.14.3	24
WLC_CT_P1	Gig0	120.32.14.4	24
AP_CT_ConsultoriosP1	Gig0	120.32.14.5	24
AP_CT_InvitadosP1	Gig0	120.32.14.6	24
AP_CT_ConsultoriosP1_2	Gig0	120.32.14.7	24
AP_CT_CamarasP1	Gig0	120.32.14.8	24
CT_Area P1_x1 [Teléfono]	Vlan 54	120.32.3.2	28
CT_Area P1_x2 [Teléfono]	Vlan 54	120.32.3.3	28
CT_Area P1_x3 [Teléfono]	Vlan 54	120.32.3.4	28
CT_Area P1_x4 [Teléfono]	Vlan 54	120.32.3.5	28
CT_Area P1_x5 [Teléfono]	Vlan 54	120.32.3.6	28
CT_ P1_Pasillo_x1 [Cámara]	Wireless0	120.32.3.34	28
CT_ P1_Pasillo_x2 [Cámara]	Wireless0	120.32.3.35	28
CT_ P1_Pasillo_x3 [Cámara]	Wireless0	120.32.3.36	28
PC_CT_ConsultoriosP1_1	Wireless0	120.32.2.194	24
PC_CT_ConsultoriosP1_2	Wireless0	120.32.2.195	24
PC_CT_ConsultoriosP1_3	Wireless0	120.32.2.196	24
PC_CT_ConsultoriosP1_2_1	Wireless0	120.32.2.197	24
PC_CT_ConsultoriosP1_2_2	Wireless0	120.32.2.130	24

3.2.5 Torre de Consultorios | Piso 2

Dispositivos	Interfaz	Direccion IP	Mascara
CT_R_P2	G0/3/0	120.32.60.2	30
	Fa0/1.57	120.32.14.1	24
	Fa0/1.58	120.32.15.1	24
	Fa0/1.59	120.32.16.1	24
	Fa0/1.60	120.32.17.1	28
	Fa0/1.61	120.32.18.1	28
CT_SW_P2	Vlan 50	120.32.14.9	24
WLC_CT_P2	Gig0	120.32.14.10	24
AP_CT_ConsultoriosP2	Gig0	120.32.14.11	24
AP_CT_InvitadosP2	Gig0	120.32.14.12	24
AP_CT_ConsultoriosP2_2	Gig0	120.32.14.13	24
AP_CT_CamarasP2	Gig0	120.32.14.14	24
CT_Area P2_x1 [Teléfono]	Vlan 60	120.32.22.2	28
CT_Area P2_x2 [Teléfono]	Vlan 60	120.32.22.3	28
CT_Area P2_x3 [Teléfono]	Vlan 60	120.32.22.4	28
CT_Area P2_x4 [Teléfono]	Vlan 60	120.32.22.5	28
CT_Area P2_x5 [Teléfono]	Vlan 15	120.32.22.6	28
CT_ P2_Pasillo_x1 [Cámara]	Wireless0	120.32.22.18	28
CT_ P2_Pasillo_x2 [Cámara]	Wireless0	120.32.22.19	28
CT_ P2_Pasillo_x3 [Cámara]	Wireless0	120.32.22.20	28
PC_CT_ConsultoriosP2_1	Wireless0	120.32.19.1	24
PC_CT_ConsultoriosP2_2	Wireless0	120.32.19.2	24
PC_CT_ConsultoriosP2_3	Wireless0	120.32.19.3	24
PC_CT_ConsultoriosP2_2_1	Wireless0	120.32.20.2	24
PC_CT_ConsultoriosP2_2_2	Wireless0	120.32.20.3	24

3.2.6 Centro de Neurología, Ortopedia y Rehabilitación | Planta Baja

Dispositivos	Interfaz	Direccion IP	Mascara
CNOR_R_PB	G0/0/0	120.32.110.1	30
	G0/1/0	120.32100.2	30
	G0/3/0	120.32.70.1	30
	Fa0/1.30	120.32.7.1	24
	Fa0/1.31	120.32.8.1	24
	Fa0/1.32	120.32.9.1	24
	Fa0/1.33	120.32.10.1	25
	Fa0/1.34	120.32.10.129	28
	Fa0/1.35	120.32.10.145	28
	Fa0/1.36	120.32.10.161	28
CNOR_SW_PB	Vlan 30	120.32.8.2	24
Server_CNOR	Fa0	120.32.8.3	24
WLC_CNOR_PB	Gig0	120.32.8.4	24
AP_ CNOR _MedicosPB	Gig0	120.32.8.5	24
AP_ CNOR _InvitadosPB	Gig0	120.32.8.6	24
AP_ CNOR _ConsultoriosPB	Gig0	120.32.8.7	24
AP_ CNOR _CamarasPB	Gig0	120.32.8.8	24
CNOR_Area PB_x1 [Teléfono]	Vlan 34	120.32.10.130	28
CNOR_Area PB_x2 [Teléfono]	Vlan 34	120.32.10.131	28
CNOR_Area PB_x3 [Teléfono]	Vlan 34	120.32.10.132	28
CNOR_Area PB_x4 [Teléfono]	Vlan 34	120.32.10.133	28
CNOR_Area PB_x5 [Teléfono]	Vlan 34	120.32.10.134	28
CNOR_PB_Pasillo_x1 [Cámara]	Wireless0	120.32.10.162	28
CNOR_PB_Pasillo_x2 [Cámara]	Wireless0	120.32. 10.163	28
CNOR_PB_Pasillo_x3 [Cámara]	Wireless0	120.32. 10.164	28
CNOR_PB_Pasillo_x4 [Cámara]	Wireless0	120.32. 10.165	28
PC_CNOR_MedicoPB1	Wireless0	120.32.10.2	24
PC_CNOR_MedicoPB2	Wireless0	120.32.10.3	24
PC_CNOR_ConsultoriosPB_1	Wireless0	120.32.9.2	24
PC_CNOR_ConsultoriosPB_2	Wireless0	120.32.9.3	24
PC_CNOR_ConsultoriosPB_3	Wireless0	120.32.9.4	24

3.2.7 Centro de Neurología, Ortopedia y Rehabilitación | Piso 1

Dispositivos	Interfaz	Direccion IP	Mascara
CNOR_R_P1	G0/3/0	120.32.70.2	30
	Fa0/1.37	120.32.11.1	24
	Fa0/1.38	120.32.12.1	24
	Fa0/1.39	120.32.13.1	25
	Fa0/1.40	120.32.13.129	28
	Fa0/1.41	120.32.13.145	28
CNOR_SW_P1	Vlan 30	120.32.8.9	24
WLC_CNOR_P1	Gig0	120.32.8.10	24
AP_ CNOR _ConsultoriosP1	Gig0	120.32.8.11	24
AP_ CNOR _AulasP1	Gig0	120.32.8.12	24
AP_ CNOR _RezoJudiosP1	Gig0	120.32.8.13	24
AP_ CNOR _CamarasP1	Gig0	120.32.8.14	24
CNOR_Area P1_x1 [Teléfono]	Vlan 40	120.32.13.130	28
CNOR_Area P1_x2 [Teléfono]	Vlan 40	120.32.13.131	28
CNOR_Area P1_x3 [Teléfono]	Vlan 40	120.32.13.132	28
CNOR_Area P1_x4 [Teléfono]	Vlan 40	120.32.13.133	28
CNOR_P1_Pasillo_x1 [Cámara]	Wireless0	120.32.13.146	28
CNOR_P1_Pasillo_x2 [Cámara]	Wireless0	120.32.13.147	28
CNOR_P1_Pasillo_x3 [Cámara]	Wireless0	120.32.13.148	28
CNOR_P1_Pasillo_x4 [Cámara]	Wireless0	120.32.13.149	28
PC_CNOR_ConsultoriosP1_1	Wireless0	120.32.12.2	24
PC_CNOR_ConsultoriosP1_2	Wireless0	120.32.12.3	24
PC_CNOR_ConsultoriosP1_3	Wireless0	120.32.12.4	24
PC_CNOR_ConsultoriosP1_4	Wireless0	120.32.12.5	24

3.2.8 Centro de Gineco-Obstetricia y Pediatría | Planta Baja

Dispositivos	Interfaz	Direccion IP	Mascara
CGOP_R_PB	G0/0/0	120.32.110.2	30
	G0/1/0	120.32120.2	30
	G0/3/0	120.32.80.1	30
	Fa0/1.70	120.32.23.1	24
	Fa0/1.71	120.32.24.1	24
	Fa0/1.72	120.32.25.1	24
	Fa0/1.73	120.32.26.1	25
	Fa0/1.74	120.32.26.129	28
	Fa0/1.75	120.32.26.145	28
	Fa0/1.76	120.32.26.161	28
CGOP_SW_PB	Vlan 71	120.32.24.2	24
Server_CGOP	Fa0	120.32.24.3	24
WLC_CGOP_PB	Gig0	120.32.24.4	24
AP_CGOP_MedicosPB	Gig0	120.32.24.5	24
AP_CGOP_InvitadosPB	Gig0	120.32.24.6	24
AP_CGOP_ConsultoriosPB	Gig0	120.32.24.7	24
AP_CGOP_CamarasPB	Gig0	120.32.24.8	24
CGOP_Area PB_x1 [Teléfono]	Vlan 34	120.32.26.130	28
CGOP_Area PB_x2 [Teléfono]	Vlan 34	120.32.26.131	28
CGOP_Area PB_x3 [Teléfono]	Vlan 34	120.32.26.132	28
CGOP_Area PB_x4 [Teléfono]	Vlan 34	120.32.26.133	28
CGOP_Area PB_x5 [Teléfono]	Vlan 34	120.32.26.134	28
CGOP_Area PB_x6 [Teléfono]	Vlan 34	120.32.26.135	28
CGOP_Area PB_x7 [Teléfono]	Vlan 34	120.32.26.136	28
CGOP_Area PB_x8 [Teléfono]	Vlan 34	120.32.26.137	28
CGOP_PB_Pasillo_x1 [Cámara]	Wireless0	120.32.26.146	28
CGOP_PB_Pasillo_x2 [Cámara]	Wireless0	120.32.26.147	28
CGOP_PB_Pasillo_x3 [Cámara]	Wireless0	120.32.26.148	28
CGOP_PB_Pasillo_x4 [Cámara]	Wireless0	120.32.26.149	28
CGOP_PB_Pasillo_x5 [Cámara]	Wireless0	120.32.26.150	28
CGOP_PB_Pasillo_x6 [Cámara]	Wireless0	120.32.26.151	28
CGOP_PB_Pasillo_x7 [Cámara]	Wireless0	120.32.26.152	28
CGOP_PB_Pasillo_x8 [Cámara]	Wireless0	120.32.26.153	28
PC_CGOP_AdministrativaPB1	Wireless0	120.32.26.2	24
PC_CGOP_AdministrativaPB2	Wireless0	120.32.26.3	24
PC_CGOP_AdministrativaPB3	Wireless0	120.32.26.4	24
PC_CGOP_AdministrativaPB4	Wireless0	120.32.26.5	24
PC_CGOP_AtencionPublicoPB1	Wireless0	120.32.23.2	24
PC_CGOP_AtencionPublicoPB2	Wireless0	120.32.23.3	24
PC_CGOP_AtencionPublicoPB3	Wireless0	120.32.23.4	24
PC_CGOP_AtencionPublicoPB4	Wireless0	120.32.23.5	24

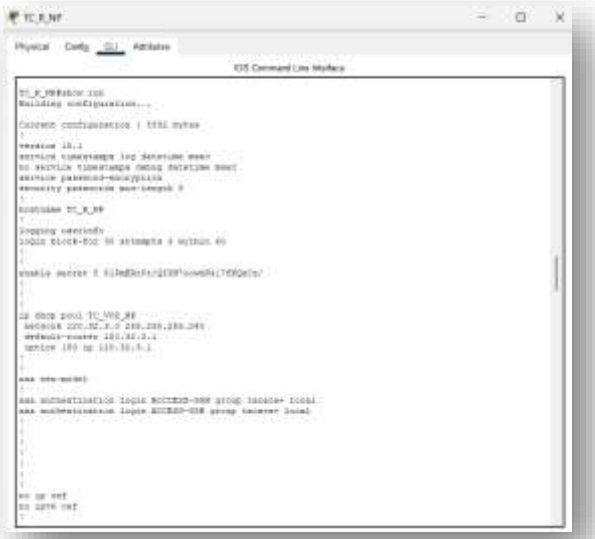
3.2.9 Centro de Gineco-Obstetricia y Pediatría | Planta Baja

Dispositivos	Interfaz	Direccion IP	Mascara
CGOP_R_P1	G0/3/0	120.32.80.2	30
	Fa0/1.77	120.32.23.1	24
	Fa0/1.78	120.32.24.1	24
	Fa0/1.79	120.32.25.1	24
	Fa0/1.80	120.32.26.1	28
	Fa0/1.81	120.32.26.129	28
CGOP_SW_P1	Vlan 71	120.32.24.9	24
WLC_CGOP_P1	Gig0	120.32.24.10	24
AP_CGOP_MedicosP1	Gig0	120.32.24.11	24
AP_CGOP_InvitadosP1	Gig0	120.32.24.12	24
AP_CGOP_ConsultoriosP1	Gig0	120.32.24.13	24
AP_CGOP_CamarasP1	Gig0	120.32.24.14	24
CGOP_Area P1_x1 [Teléfono]	Vlan 34	120.32.30.2	28
CGOP_Area P1_x2 [Teléfono]	Vlan 34	120.32.30.2	28
CGOP_Area P1_x3 [Teléfono]	Vlan 34	120.32.30.3	28
CGOP_Area P1_x4 [Teléfono]	Vlan 34	120.32.30.4	28
CGOP_Area P1_x5 [Teléfono]	Vlan 34	120.32.30.5	28
CGOP_Area P1_x6 [Teléfono]	Vlan 34	120.32.30.6	28
CGOP_Area P1_x7 [Teléfono]	Vlan 34	120.32.30.7	28
CGOP_P1_Pasillo_x1 [Cámara]	Wireless0	120.32.30.18	28
CGOP_P1_Pasillo_x2 [Cámara]	Wireless0	120.32.30.19	28
CGOP_P1_Pasillo_x3 [Cámara]	Wireless0	120.32.30.20	28
CGOP_P1_Pasillo_x4 [Cámara]	Wireless0	120.32.30.21	28
CGOP_P1_Pasillo_x5 [Cámara]	Wireless0	120.32.30.22	28
CGOP_P1_Pasillo_x6 [Cámara]	Wireless0	120.32.30.23	28
CGOP_P1_Pasillo_x7 [Cámara]	Wireless0	120.32.30.24	28
PC_CGOP_HabitacionesP1_1	Wireless0	120.32.27.2	24
PC_CGOP_HabitacionesP1_2	Wireless0	120.32.27.3	24
PC_CGOP_HabitacionesP1_3	Wireless0	120.32.27.4	24
PC_CGOP_HabitacionesP1_2_1	Wireless0	120.32.28.2	24
PC_CGOP_HabitacionesP1_2_2	Wireless0	120.32.28.3	24
PC_CGOP_InvitadosP1_1	Wireless0	120.32.29.2	24
PC_CGOP_InvitadosP1_2	Wireless0	120.32.29.3	24

Fase 4

4.1 Configuración de Dispositivos

4.1.1 Configuracion TC | TC_R_NP



La imagen muestra la configuración del router ubicado en el Nivel Plaza de la Torre Central (TC_R_NP). Se puede observar que hay un dhcp pool (TC_VOZ_NP) con la red 120.32.2.0.

La imagen muestra el username y password ftp (AdminTC), ssh version, el domain-name (abc.com) tambien la interfaz 0/0 con la ip add 120.32.3.50 /30, ip flow egress/ingress y el duplex y speed, se observ

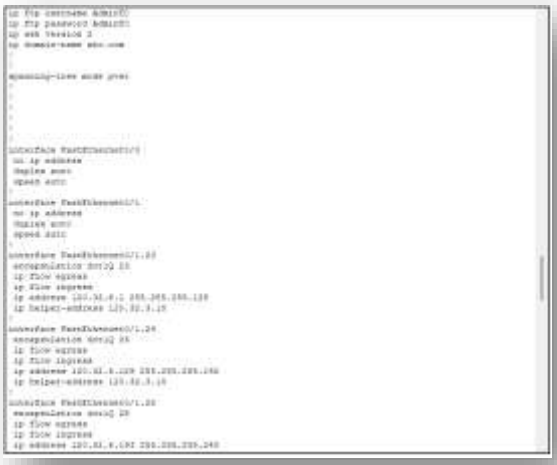
4.1.2 Configuracion TC | TC_R_PB

La imagen muestra la configuración del router ubicado en la Planta baja de la Torre Central (TC_R_NP). Se puede observar que hay un dhcp pool (TC_VOZ_NP) con la red 120.32.5.128/28

La imagen muestra el username y password ftp (AdminTC), ssh version, el domain-name (abc.com) , tambien la interfaz 0/0, la interfaz 0/1 y la interfaz 0/01.18 con la ip add 120.32.4.1 /24, que cuenta con ip flow egress/ingress, e ip helper-address.

4.1.3 Configuracion TC | TC_R_P1

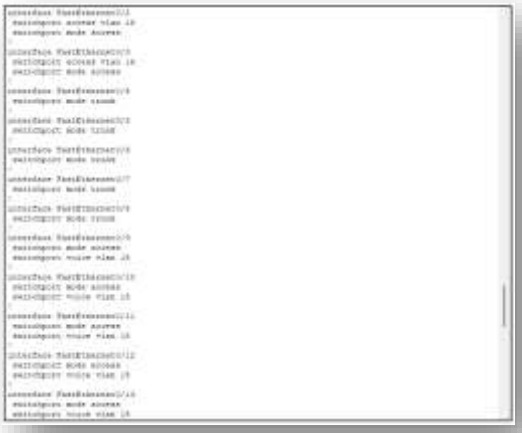
La imagen muestra la configuración de un dispositivo de red que establece políticas de seguridad, crea un servidor DHCP para asignar direcciones IP a los teléfonos IP, configura un usuario de acceso local y define una autenticación combinada con un servidor TACACS+ y una base de datos local.



La imagen muestra la configuración de un dispositivo de red que establece el nombre de dominio, configura SSHv1, habilita el protocolo Spanning Tree, y asigna direcciones IP a varias sub-interfaces VLAN, incluyendo la configuración para reenviar solicitudes de DHCP a un servidor.

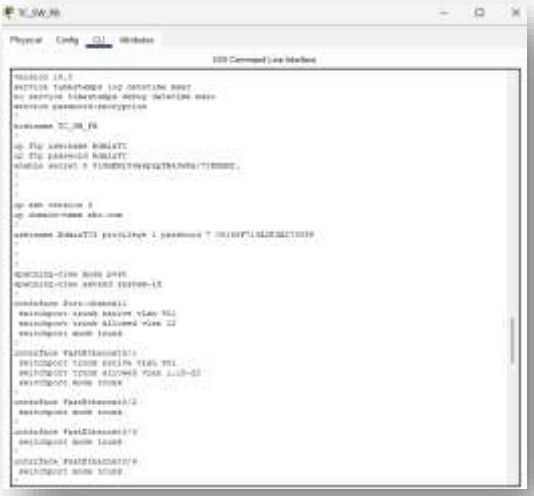
4.1.4 Configuracion TC | TC_SW_NP

La imagen muestra la configuración de un switch que establece el nombre del dispositivo, encripta contraseñas y configura SSH v2 para un acceso seguro. Además, habilita el protocolo Spanning Tree (PVST) y configura múltiples interfaces como puertos trunk (tanto físicos como EtherChannels), permitiendo el paso de las VLANs 1 y 2, y definiendo la VLAN 991 como nativa.

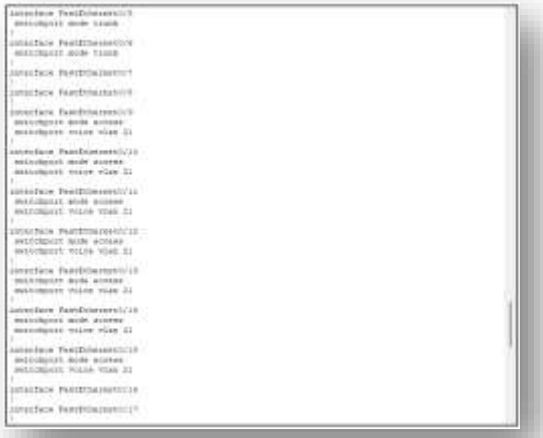


La imagen muestra la configuración de un switch que separa sus puertos en diferentes tipos:. Puertos de tronco (FastEthernet0/4 al /8) que permiten el paso de múltiples VLANs, típicamente para conectar a otros switches. Puertos de acceso (FastEthernet0/9 al /13) asignados a la VLAN 15.

4.1.5 Configuracion TC | TC_SW_PB

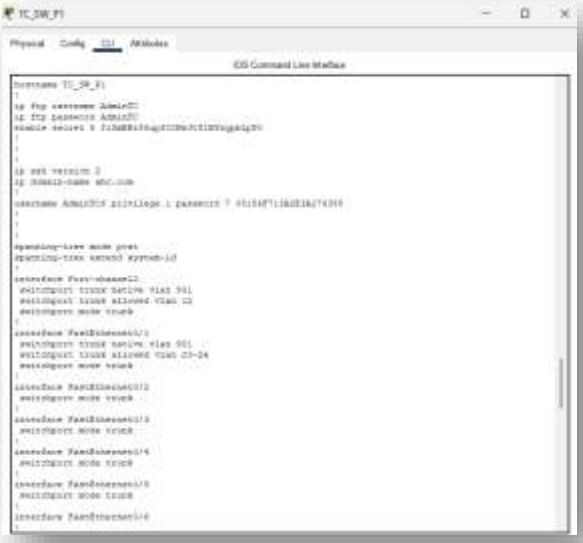


La imagen muestra la configuración de un switch que encripta contraseñas, habilita SSHv2, define un usuario administrador y un dominio. También configura el protocolo Spanning Tree (PVST) y establece interfaces como puertos troncales, permitiendo el paso de las VLANs 1, 10 y 20. Se configura el acceso remoto al dispositivo a través de SSH y sincroniza el reloj del sistema con un servidor NTP para mantener la hora exacta. Finalmente, la tercera imagen configura un teléfono IP (ephone) de modelo 7960, le asigna una dirección MAC y asocia el botón 1 con la línea 1.

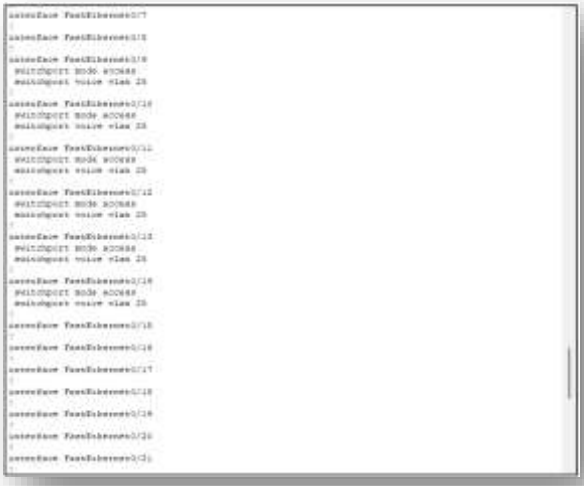


La imágenen muestran la configuración de teléfonos IP, un servidor DHCP para asignarles direcciones, un router con seguridad de acceso y sincronización de hora, y un switch configurado con puertos troncales y de acceso para diferentes VLANs de datos y voz.

4.1.6 Configuracion TC | TC_SW_P1



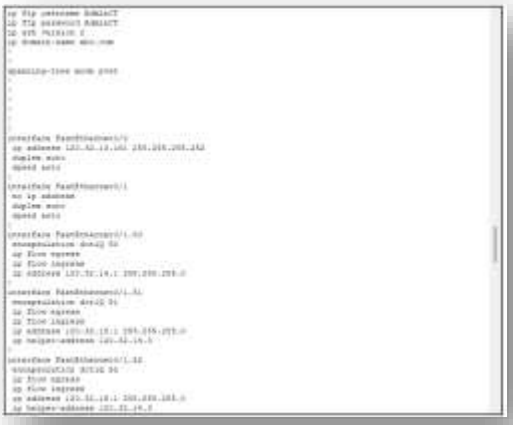
La imágen muestra la configuración de un sistema de red que integra telefonía IP, un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra la configuración de un sistema de red que integra telefonía IP, un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

4.1.7 Configuracion CT | CT_R_P1

La imágen muestra la configuración de un sistema de red que integra telefonía IP (con ephones y servidor DHCP), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.



La imágen muestra la configuración de un sistema de red que integra telefonía IP, con servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

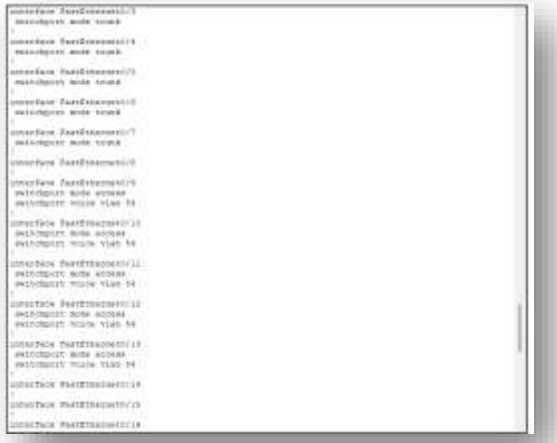
4.1.8 Configuracion CT | CT_R_P2

La imágen muestra la configuración de una red que integra telefonía IP (con ephones y servidor DHCP para su aprovisionamiento), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

4.1.9 Configuracion CT | CT_SW_P1

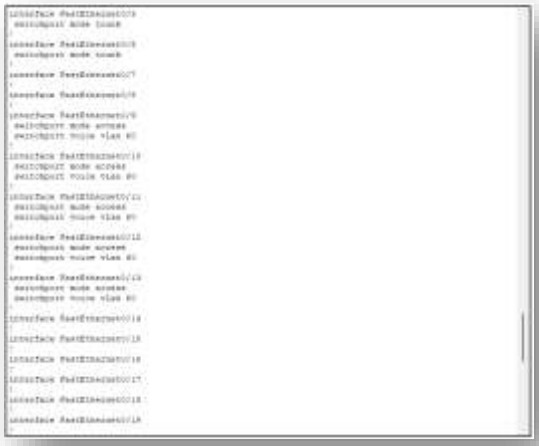
La imágen muestra la configuración de un sistema de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

4.1.10 Configuracion CT | CT_SW_P2

La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



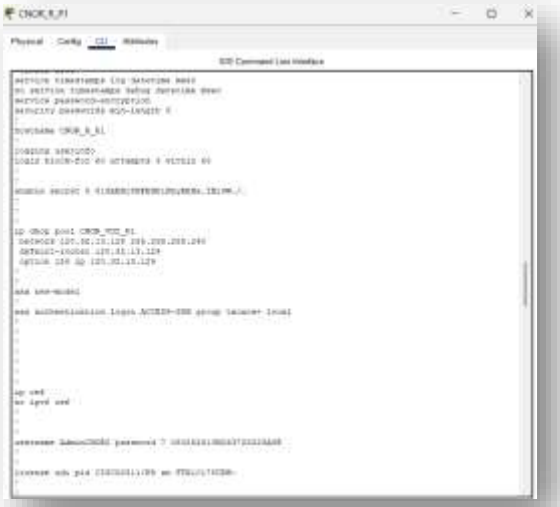
La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

4.1.11 Configuracion CNOR | CNOR_R_PB

Se utilizo la configuración de show interface para mostrar configuraciones iniciales del router, incluyendo nombre de host, autenticación y asignación de direcciones IP.

Muestra Configuración de interfaces de red con direcciones IP y parámetros de tráfico.

4.1.12 Configuracion CNOR | CNOR_R_P1

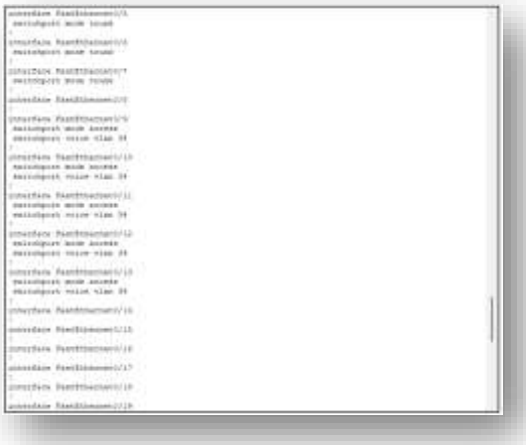


se configura la seguridad, el acceso, la asignación de direcciones IP y las características avanzadas del dispositivo.

En resumen, se realiza la configuración básica de acceso FTP, Spanning Tree y las interfaces de red con sus parámetros asociados.

4.1.13 Configuracion CNOR | CNOR_SW_PB

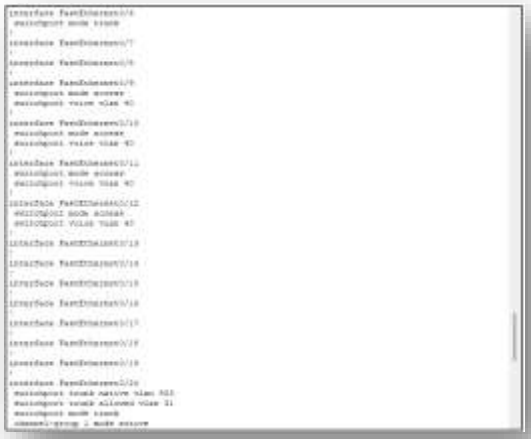
se configura el switch con autenticación segura, spanning tree, y puertos trunk para permitir la transmisión de tráfico de múltiples VLANs.



se configuran puertos trunk para transportar múltiples VLANs y puertos de acceso para asignarles una VLAN específica, con énfasis en la VLAN de voz para algunas interfaces.

4.1.14 Configuracion CNOR | CNOR_SW_P1

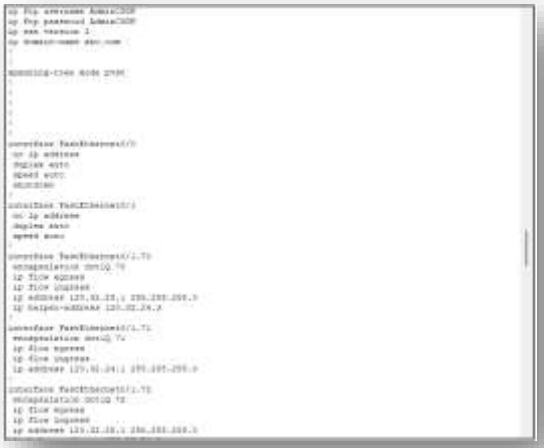
establece un dispositivo con seguridad mediante la encriptación de contraseñas y acceso FTP. Además, configura Spanning Tree para evitar bucles de red, habilita trunks para el transporte de múltiples VLANs a través de las interfaces y agrupa enlaces utilizando LACP para mejorar el rendimiento de la red.



La configuración establece que varias interfaces operen en modo trunk para permitir el paso de tráfico de múltiples VLANs. Además, algunas interfaces están configuradas en modo de acceso para una VLAN específica, con VLAN 40 asignada para el tráfico de voz. También se configura un agrupamiento de enlaces para mejorar el rendimiento.

4.1.15 Configuracion CGOP | CGOP_R_PB

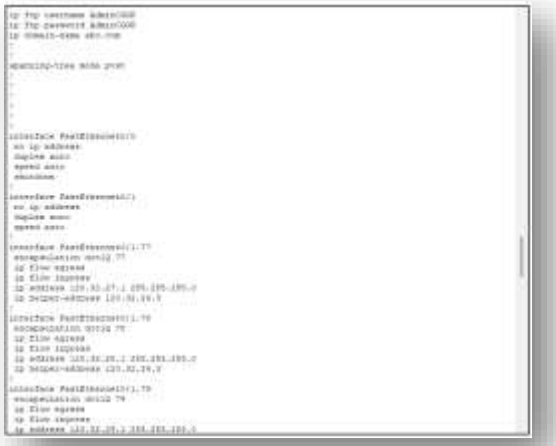
La configuración establece un nombre de host, configura un pool DHCP con direcciones IP, habilita autenticación AAA para el acceso remoto, y encripta las contraseñas. También configura un servidor DNS y TFTP para los clientes DHCP, y muestra información de licencia para el dispositivo.



La configuración establece un acceso FTP seguro y habilita SSH para la administración remota. Configura el spanning tree en modo PVST y define varias subinterfaces en las interfaces FastEthernet para manejar el tráfico de VLANs específicas, asignando direcciones IP a cada subinterfaz y habilitando el monitoreo de flujo de tráfico.

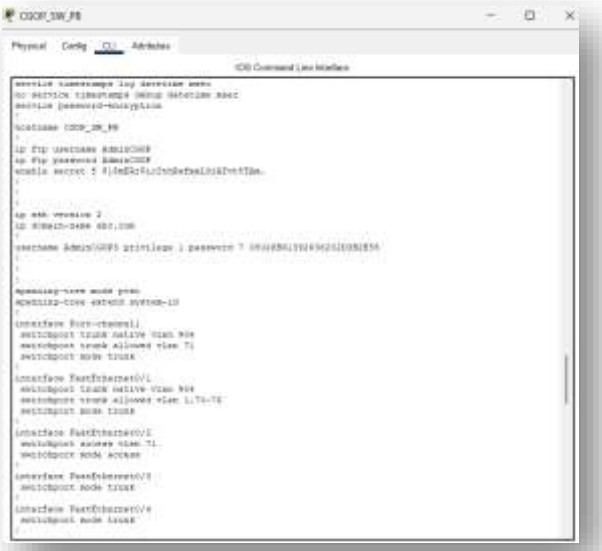
4.1.16 Configuracion CGOP | CGOP_R_P1

Esta configuración establece la seguridad de contraseñas, configura un pool DHCP para la asignación de direcciones IP y configura un servidor de autenticación AAA para controlar el acceso. Además, muestra detalles sobre la licencia del dispositivo y configura las marcas de tiempo en los logs del dispositivo.

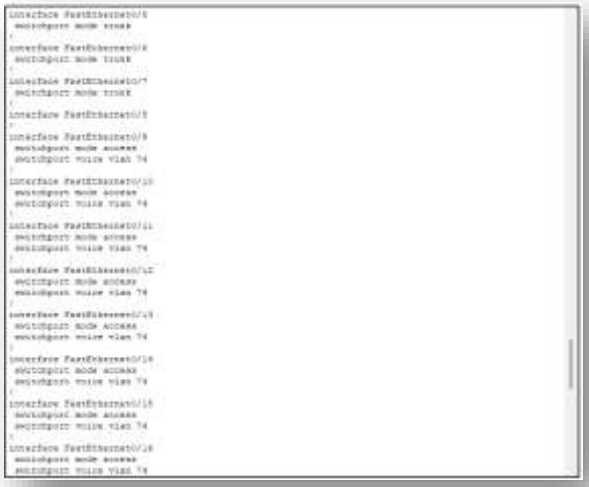


La configuración se centra en el acceso FTP, el Spanning Tree en modo PVST, y la configuración de varias interfaces FastEthernet, algunas de las cuales están configuradas con subinterfaces para el manejo de tráfico de VLANs específicas. Además, se asignan direcciones IP a algunas interfaces y se habilita el monitoreo de flujo de tráfico y la funcionalidad helper-address para redirigir solicitudes DHCP.

4.1.17 Configuracion CGOP | CGOP_SW_PB

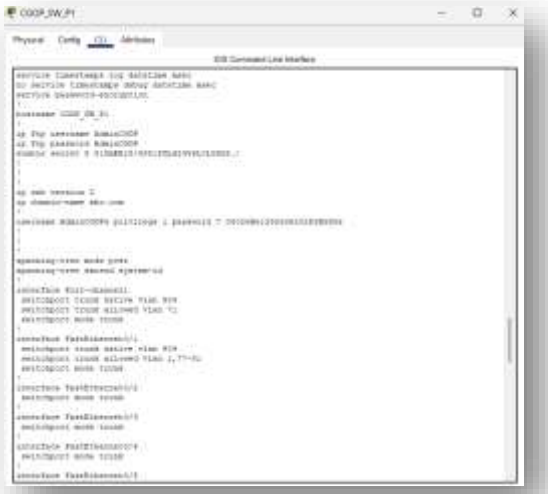


La configuración establece la seguridad con SSH para el acceso remoto, configura Spanning Tree en modo PVST y habilita la extensión del system-id. Además, se configuran puertos trunk para el transporte de múltiples VLANs y un puerto de acceso para una VLAN específica. También se establece un pool de direcciones IP para FTP y un nombre de dominio para el dispositivo.



Esta configuración gestiona una mezcla de puertos trunk (para transmitir tráfico de múltiples VLANs) y puertos de acceso específicos para la VLAN 74, configurada para el tráfico de voz. Se utiliza para asegurar que los puertos de voz en el switch estén correctamente asignados a la VLAN correspondiente para servicios como la telefonía IP.

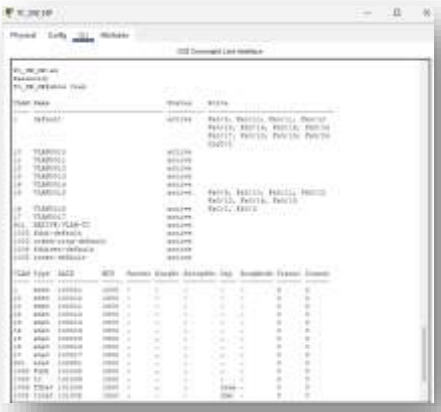
4.1.18 Configuracion CGOP | CGOP_SW_P1



La configuración abarca la configuración básica de seguridad y acceso, activando SSH para administración remota, configurando puertos trunk para transmitir el tráfico de la VLAN 71 y una VLAN nativa (VLAN 904). También se gestionan las configuraciones de Spanning Tree y de acceso FTP con credenciales configuradas.

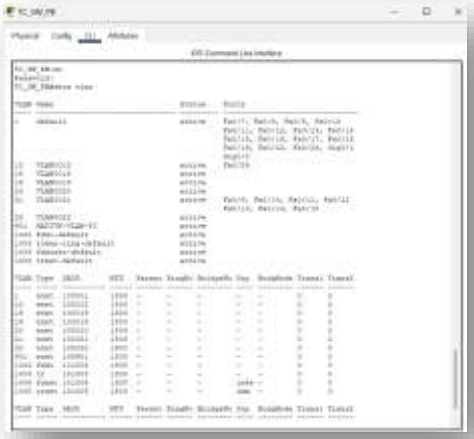
La configuración define varios puertos en modo trunk para el transporte de tráfico de varias VLANs, y puertos de acceso configurados específicamente para manejar el tráfico de voz en la VLAN 80. Esto asegura que los puertos para dispositivos de voz (como teléfonos IP) tengan el tráfico adecuado separado y etiquetado correctamente.

4.1.19 VLANS | Torre Central | TC_SW_NP



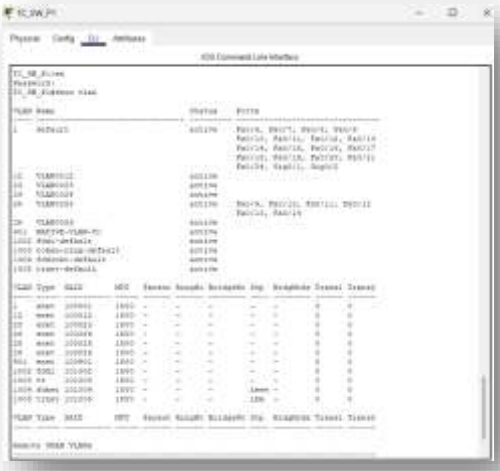
La salida del comando muestra un resumen de todas las VLANs configuradas en el dispositivo, sus puertos asignados, y su estado. Cada VLAN tiene una identificación única (SAID), un MTU de 1500 bytes y está activada para el uso en la red. Las VLANs están configuradas para diferentes puertos del dispositivo, lo que permite la segmentación del tráfico de red.

4.1.20 VLANS | Torre Central | TC_SW_PB



Esta salida muestra la configuración de múltiples VLANs en un switch, incluyendo la VLAN predeterminada y varias VLANs de usuario (como VLAN0012, VLAN0018, VLAN0021, etc.), cada una con puertos asignados. Además, se proporciona el SAID único de cada VLAN, junto con la configuración de MTU y otros detalles internos.

4.1.21 VLANS | Torre Central | TC_SW_P1

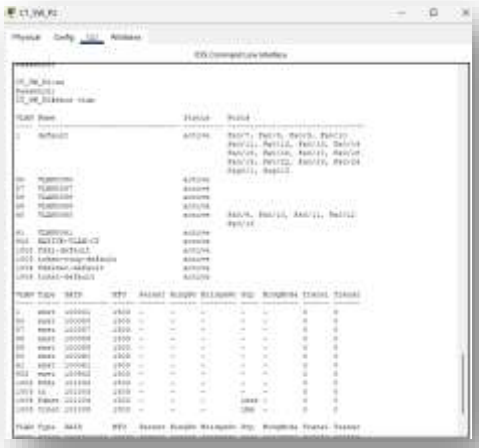


Esta salida proporciona una visión detallada de las VLANs activas en el switch Cisco, sus puertos asignados, y configuraciones de red avanzadas como SAID, MTU y configuraciones de puenteo. También muestra las configuraciones relacionadas con las tecnologías más antiguas como token-ring y FDDI.

4.1.22 VLANS | Torre de Consultorios | CT_SW_P1

Esta salida muestra una lista de VLANs activas en el switch, junto con los puertos asignados a cada una. Además, muestra los detalles de SAID, MTU y otras configuraciones relacionadas con el puenteo de VLANs. También se mencionan algunas configuraciones de tecnologías antiguas de redes como token-ring y FDDI.

4.1.23 VLANS | Torre de Consultorios | CT_SW_P2

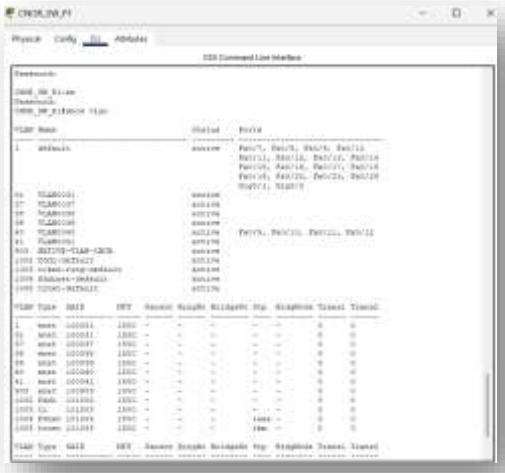


La salida muestra un resumen de todas las VLANs activas en el switch, con puertos asignados a cada VLAN y detalles de configuración relacionados con los identificadores SAID, MTU, y otras configuraciones de puenteo. También se observa que las VLANs están configuradas para una segmentación de tráfico eficiente en la red.

4.1.24 VLANS | CNOR | CNOR _SW_PB

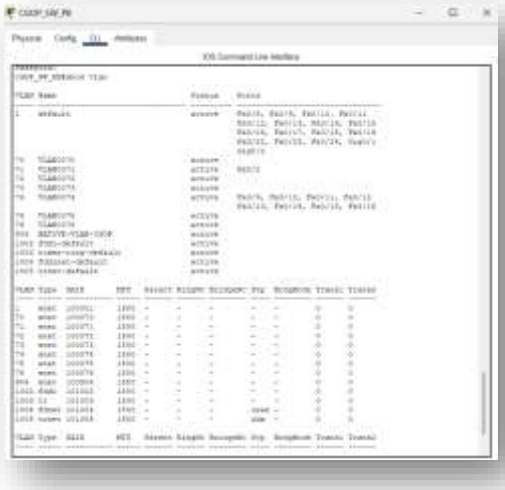
La salida muestra una lista de VLANs activas en el switch, con los puertos asignados a cada VLAN. También proporciona detalles técnicos como el SAID, MTU, y la configuración de los puertos. Además, se muestra la VLAN nativa para la gestión de tráfico no etiquetado, y se incluye información sobre tecnologías antiguas, aunque no se está utilizando ninguna de ellas en esta configuración.

4.1.25 VLANS | CNOR | CNOR _SW_P1



La salida muestra las VLANs activas en el switch, sus puertos asignados y otros detalles como SAID, MTU, y la configuración de puenteo. También se indica la VLAN nativa, que maneja el tráfico no etiquetado. Las VLANs están configuradas para permitir la segmentación del tráfico en la red de forma eficiente.

4.1.26 VLANS | CGOP | CGOP _SW_PB

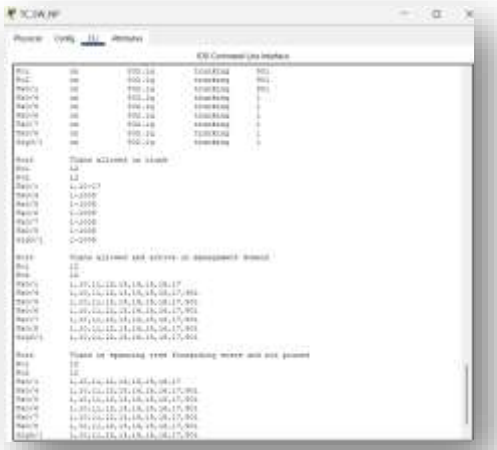


La salida muestra la configuración de varias VLANs activas en el switch Cisco, junto con los puertos asignados a cada una. También proporciona detalles técnicos como el SAID, MTU y configuraciones de puenteo para cada VLAN. Además, se observa la VLAN nativa que maneja el tráfico no etiquetado y la segmentación del tráfico dentro de la red.

4.1.27 VLANS | CGOP | CGOP _SW_P1

La salida muestra un resumen de las VLANs activas en el switch, los puertos asignados a cada VLAN y algunos detalles técnicos como SAID, MTU y las configuraciones de puenteo. Además, se observa la VLAN nativa que maneja el tráfico no etiquetado y una configuración adicional para VLAN edit-default que parece no tener puertos asignados en esta configuración.

4.1.28 Modo Troncal | Torre Central | TC_SW_NP

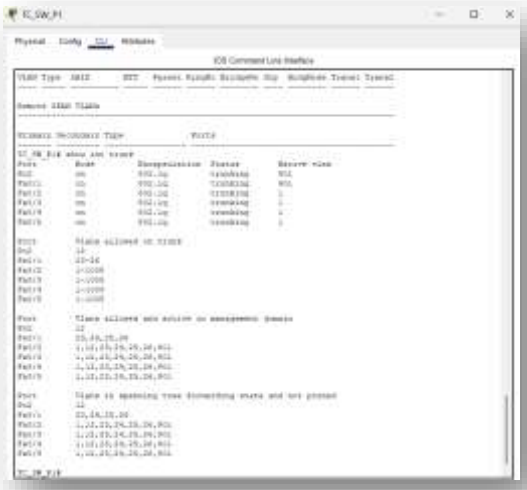


La configuración muestra que VLANs 1, 10-17 y 901 están habilitadas para el trunking en varios puertos de agregación (Po1 a Po4) y puertos de acceso. Además, se utiliza el protocolo 802.1Q para el trunking y se aseguran de que estas VLANs estén activas y participen en el Spanning Tree para evitar problemas de bucles en la red.

4.1.29 Modo Troncal | Torre Central | TC_SW_PB

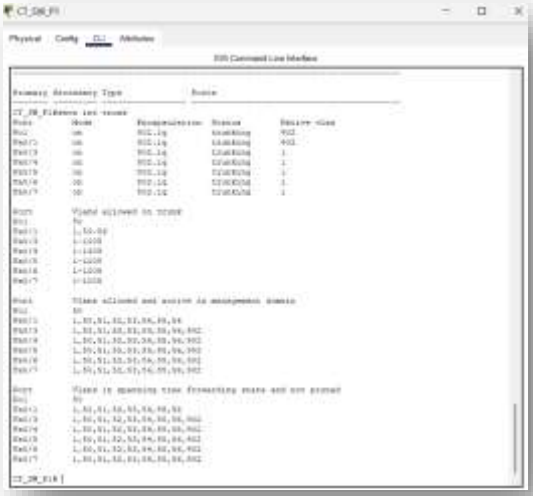
La configuración muestra una red que usa 802.1Q trunking para transportar varias VLANs a través de un enlace troncal entre varios puertos. El trunking está habilitado en varios puertos del switch, permitiendo las VLANs 1 a 1005 y configurando VLAN 901 como la nativa. Además, se asegura que las VLANs activas estén habilitadas en el Spanning Tree para evitar bucles en la red.

4.1.30 Modo Troncal | Torre Central | TC_SW_P1



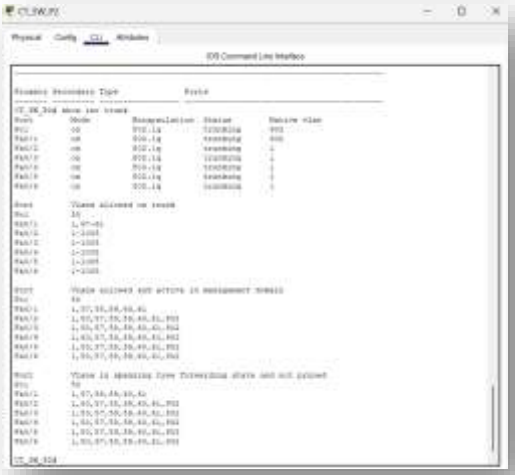
Los puertos Po1, Fa0/1 a Fa0/4 están configurados para 802.1Q trunking, permitiendo VLANs 1-1005 con VLAN 901 como nativa. Las VLANs 1, 12, 18-22, 901 están activas en Spanning Tree y no podadas, asegurando la segmentación y evitando bucles en la red.

4.1.31 Modo Troncal | Torre de Consultorios | CT_SW_P1



Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo VLANs 1-1005 y con VLAN 902 como nativa. Las VLANs 1, 50-56, 902 están activas en el Spanning Tree y no están podadas, asegurando que el tráfico fluya correctamente entre ellas.

4.1.32 Modo Troncal | Torre de Consultorios | CT_SW_P2



Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo VLANs 1-1005 y 50-61, con VLAN 902 como nativa. Las VLANs 1, 50-61, 902 están activas en Spanning Tree, asegurando tráfico fluido sin bloqueos.

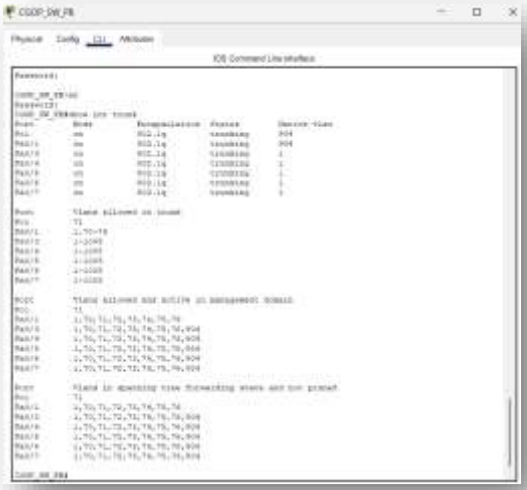
4.1.33 Modo Troncal | CNOR | CNOR _SW_PB

Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo VLANs 1-1005, 3, 30-36, y 903, con VLAN 903 como la VLAN nativa. Las VLANs 1, 3, 30-36, 903 están activas en Spanning Tree, permitiendo un tráfico fluido y sin bloqueos.

4.1.34 Modo Troncal | CNOR | CNOR _SW_P1

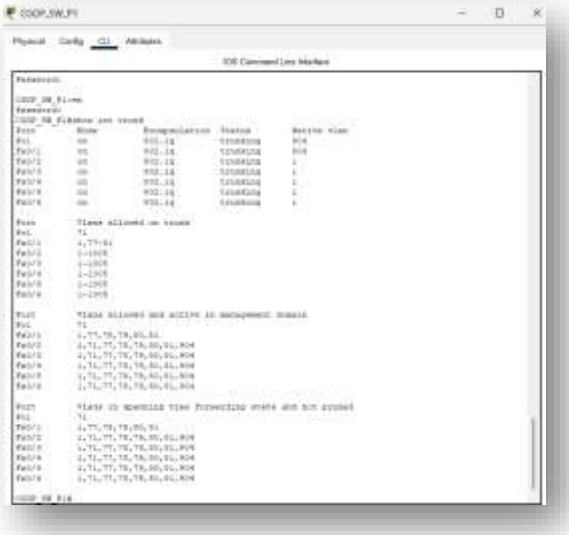
Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo las VLANs 1-1005 y VLANs 31, 37-41, 903, con VLAN 903 como la VLAN nativa. Las VLANs 1, 31, 37-41, 903 están activas en Spanning Tree, permitiendo el tráfico sin bloqueos.

4.1.35 Modo Troncal | CGOP | CGOP _SW_PB



Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo las VLANs 1-1005 y 70-76, con VLAN 904 como la VLAN nativa. Las VLANs 1, 70-76, 904 están activas en Spanning Tree, lo que permite el paso de tráfico sin bloqueos.

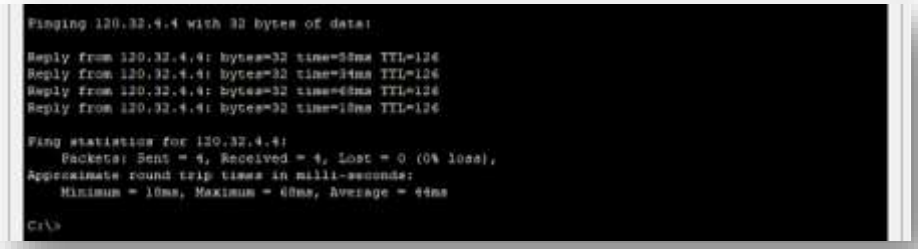
4.1.36 Modo Troncal | CGOP | CGOP _SW_P1



Los puertos Po1, Fa0/1 a Fa0/6 están configurados para 802.1Q trunking, permitiendo VLANs 1-1005, 71-81, y 904, con VLAN 904 como la VLAN nativa en algunos puertos. Las VLANs 1, 71-81, 904 están activas en Spanning Tree, lo que asegura el paso de tráfico sin bloqueos.

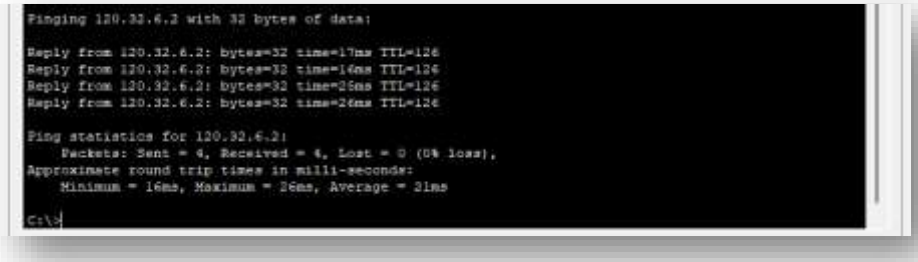
4.2 Pruebas de Conectividad (Ping)

4.2.1 Conectividad TC | Nivel Plaza a Planta Baja



Red 120.32.0.0 [AtencionPublico_TC_NP] a Red 120.32.4.0 [AtencionPublico_TC_PB]

4.2.2 Conectividad TC | Nivel Plaza a Piso 1



Red 120.32.1.0 [Invitados_TC_NP] a Red 120.32.6.0 [Medicos_TC_P1]

4.2.3 Conectividad TC | Nivel Plaza a Internet

Red 120.32.1.128 [TI_TC_NP] a Internet

4.2.4 Conectividad TC | Nivel Plaza a Torre de Consultorios

```
Pinging 120.32.15.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.15.2: bytes=32 time=40ms TTL=126
Reply from 120.32.15.2: bytes=32 time=8ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 40ms, Average = 19ms

C:\>
```

Red 120.32.1.128 [Invitados_TC_NP] a 120.32.15.0 [Invitados_CT_P1]

4.2.5 Conectividad TC | Nivel Plaza a CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

Red 120.32.1.128 [TI_TC_NP] a 120.32.7.0 [Invitados_CNOR]

4.2.6 Conectividad TC | Nivel Plaza a CGOP

```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

Red 120.32.2.192 [Administrativa_TC_NP] a 120.32.25.0 [Invitados_CGOP

4.2.7 Conectividad TC | Planta Baja Torre de Consultorios

```
Pinging 120.32.15.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.15.2: bytes=32 time=40ms TTL=126
Reply from 120.32.15.2: bytes=32 time=8ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 40ms, Average = 19ms

C:\>
```

Red 120.32.4.0 [AtencionPublico_TC_PB] a 120.32.15.0 [Invitados_CT_P1]

4.2.8 Conectividad TC | Planta Baja a CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

Red 120.32.5.0 [Administrativa_TC_2] a 120.32.7.0 [Invitados_CNOR]

4.2.9 Conectividad TC | Planta Baja a CGOP

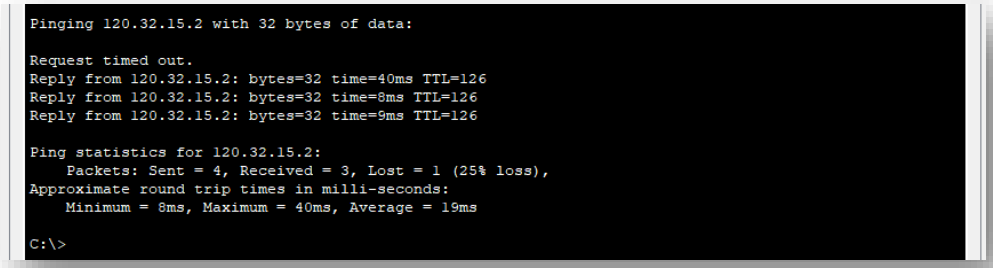
```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

Red 120.32.5.64 [CajaMedicos_TC_PB] a 120.32.25.0 [Invitados_CGOP]

4.2.10 Conectividad TC | Planta Baja a Internet

Red 120.32.4.0 [AtencionPublico_TC_PB] a Internet

4.2.11 Conectividad TC | Piso 1 Torre de Consultorios



Red 120.32.6.0 [Medicos_TC_P1] a 120.32.15.0 [Invitados_CT_P1]

4.2.12 Conectividad TC | Piso 1 a CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

Red 120.32.5.0 [Administrativa_TC_3] a 120.32.7.0 [Invitados_CNOR]

4.2.13 Conectividad TC | Piso 1 a CGOP

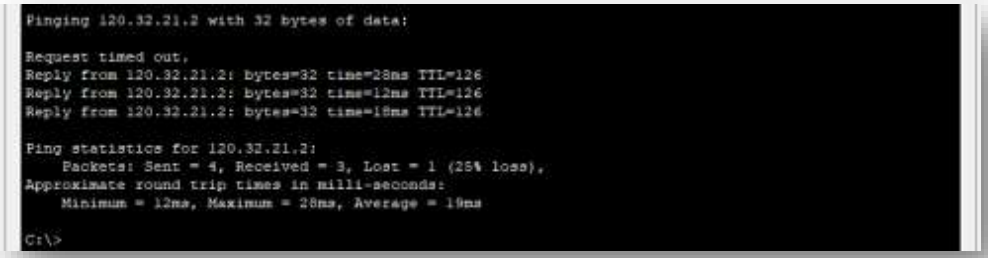
```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

Red 120.32.6.0 [Medicos_TC_P1] a 120.32.25.0 [Invitados_CGOP]

4.2.14 Conectividad TC | Piso 1 a Internet

Red 120.32.6.128 [Administrativa_TC_3] a Internet

4.2.15 Conectividad CT | Piso 1 a Piso 2



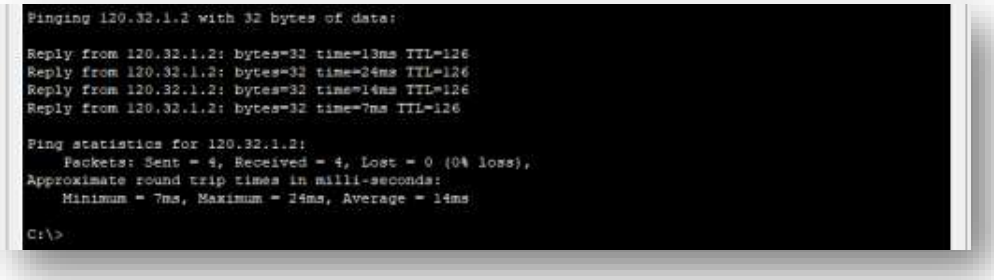
```
Pinging 120.32.21.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.21.2: bytes=32 time=28ms TTL=126
Reply from 120.32.21.2: bytes=32 time=12ms TTL=126
Reply from 120.32.21.2: bytes=32 time=18ms TTL=126

Ping statistics for 120.32.21.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 28ms, Average = 19ms

C:\>
```

Red 120.32.15.0 [Invitados_CT_P1] a Red 120.32.21.0 [Invitados_CT_P2]

4.2.16 Conectividad CT | Piso 1 a Internet

Red 120.32.16.0 [Consultorios_CT_P1] a [Internet]

4.2.17 Conectividad CT | Piso 1 a Torre Central



```
Pinging 120.32.1.2 with 32 bytes of data:

Reply from 120.32.1.2: bytes=32 time=13ms TTL=126
Reply from 120.32.1.2: bytes=32 time=24ms TTL=126
Reply from 120.32.1.2: bytes=32 time=14ms TTL=126
Reply from 120.32.1.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 24ms, Average = 14ms

C:\>
```

Red 120.32.1.128 [Invitados_CT_P1] a Red 120.32.1.0 [Invitados_TC_NP]

4.2.18 Conectividad CT | Piso 1 a CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=50ms TTL=125
Reply from 120.32.7.2: bytes=32 time=37ms TTL=125
Reply from 120.32.7.2: bytes=32 time=9ms TTL=125
Reply from 120.32.7.2: bytes=32 time=12ms TTL=125

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 50ms, Average = 27ms

C:\>
```

Red 120.32.16.0 [Consultorios_CT_P1] a Red 120.32.7.0 [Invitados_CNOR]

4.2.19 Conectividad CT | Piso 1 a CGOP

```
Pinging 120.32.23.2 with 32 bytes of data:

Reply from 120.32.23.2: bytes=32 time=15ms TTL=126
Reply from 120.32.23.2: bytes=32 time=23ms TTL=126
Reply from 120.32.23.2: bytes=32 time=19ms TTL=126
Reply from 120.32.23.2: bytes=32 time=15ms TTL=126

Ping statistics for 120.32.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 23ms, Average = 18ms

C:\>
```

Red 120.32.17.0 [Consultorios_CT_P1_2] a Red 120.32.23.0 [AtencionPublico_CGOP_PB]

4.2.20 Conectividad CT | Piso 2 a Piso 1

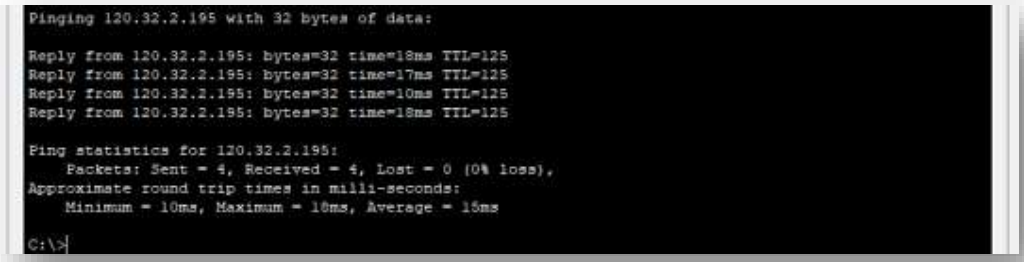
```
Pinging 120.32.15.2 with 32 bytes of data:

Reply from 120.32.15.2: bytes=32 time=37ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126
Reply from 120.32.15.2: bytes=32 time=32ms TTL=126
Reply from 120.32.15.2: bytes=32 time=38ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 38ms, Average = 29ms

C:\>
```

Red 120.32.21.0 [Invitados_CT_P2] a Red 120.32.15.0 [Invitados_CT_P1]

4.2.21 Conectividad CT | Piso 2 a Internet

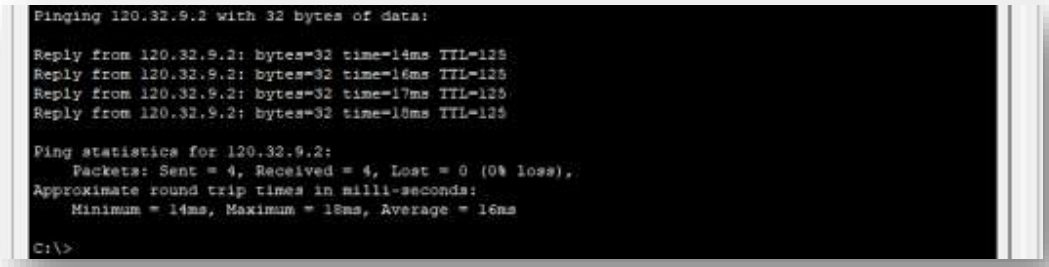
Red 120.32.19.0 [Consultorios_CT_P2] a [Internet]

4.2.22 Conectividad CT | Piso 2 a Torre Central



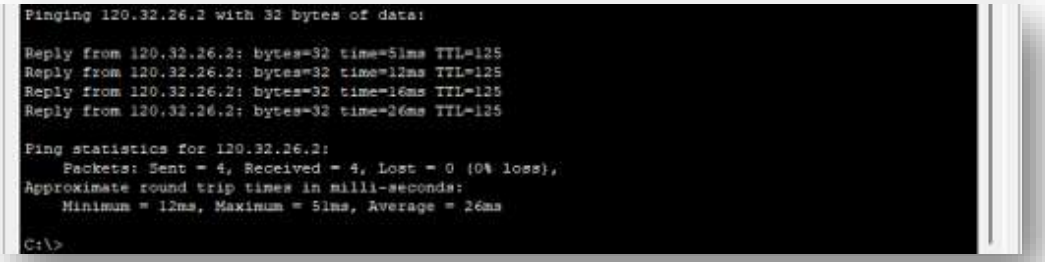
Red 120.32.21.0 [Invitados_CT_P2] a Red 120.32.2.192 [Administrativa_TC]

4.2.23 Conectividad CT | Piso 2 a CNOR



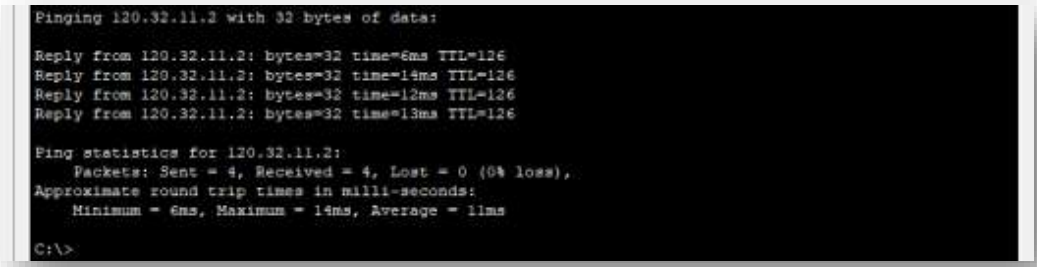
Red 120.32.20.0 [Consultorios_CT_P2_2] a Red 120.32.9.0 [Consultorios_CNOR_PB]

4.2.24 Conectividad CT | Piso 2 a CGOP



Red 120.32.21.0 [Invitados_CT_P2] a Red 120.32.26.0 [Administrativa_CGOP_1]

4.2.25 Conectividad CNOR | Planta Baja a Piso 1



Red 120.32.7.0 [Invitados_CNOR] a Red 120.32.11.0 [Aulas_CNOR_P1]

4.2.26 Conectividad CNOR | Planta Baja a Internet

Red 120.32.9.0 [Consultorios_CNOR_PB] a [Internet]

4.2.27 Conectividad CNOR | Planta Baja a Torre Central

```
Pinging 120.32.6.130 with 32 bytes of data:

Reply from 120.32.6.130: bytes=32 time=26ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=14ms TTL=125

Ping statistics for 120.32.6.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 26ms, Average = 20ms

C:\>
```

Red 120.32.10.0 [Medicos_CNOR_PB] a Red 120.32.6.128[Administrativa_TC_3]

4.2.28 Conectividad CNOR | Planta Baja a Torre de Consultorios

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=13ms TTL=124
Reply from 120.32.19.2: bytes=32 time=17ms TTL=124
Reply from 120.32.19.2: bytes=32 time=14ms TTL=124
Reply from 120.32.19.2: bytes=32 time=15ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 17ms, Average = 14ms

C:\>
```

Red 120.32.7.0 [Invitados_CNOR_PB] a Red 120.32.19.0 [Consultorios_CT_P2]

4.2.29 Conectividad CNOR | Planta Baja a CGOP

```
Pinging 120.32.29.2 with 32 bytes of data:

Reply from 120.32.29.2: bytes=32 time=6ms TTL=125
Reply from 120.32.29.2: bytes=32 time=28ms TTL=125
Reply from 120.32.29.2: bytes=32 time=14ms TTL=125
Reply from 120.32.29.2: bytes=32 time=29ms TTL=125

Ping statistics for 120.32.29.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 29ms, Average = 19ms

C:\>
```

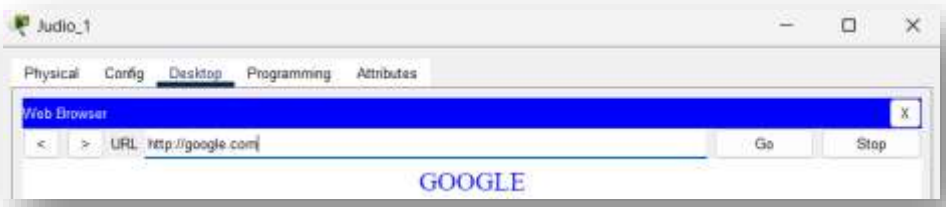
Red 120.32.10.0 [Medicos_CNOR_PB] a Red 120.32.29.0 [Invitados_CGOP_P1]

4.2.30 Conectividad CNOR | Piso 1 a Planta Baja

```
Pinging 120.32.10.3 with 32 bytes of data:

Reply from 120.32.10.3: bytes=32 time=25ms TTL=126
Reply from 120.32.10.3: bytes=32 time=20ms TTL=126
Reply from 120.32.10.3: bytes=32 time=19ms TTL=126
Reply from 120.32.10.3: bytes=32 time=15ms TTL=126

Ping statistics for 120.32.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 25ms, Average = 19ms

C:\>
```

Red 120.32.11.0 [Invitados_CGOP_P1] a Red 120.32.10.0 [Medicos_CGOP_PB]

4.2.31 Conectividad CNOR | Piso 1 a Planta Baja



Red 120.32.13.0 [RezosJudios_CGOP_P1] a [Internet]

4.2.32 Conectividad CNOR | Piso 1 a Torre Central

```
Pinging 120.32.6.130 with 32 bytes of data:

Reply from 120.32.6.130: bytes=32 time=26ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=14ms TTL=125

Ping statistics for 120.32.6.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 26ms, Average = 20ms

C:\>
```

Red 120.32.11.0 [Aulas_CNOR_P1] a Red 120.32.6.128 [Administrativa_TC_3]

4.2.33 Conectividad CNOR | Piso 1 a Torre de Consultorios

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=13ms TTL=124
Reply from 120.32.19.2: bytes=32 time=17ms TTL=124
Reply from 120.32.19.2: bytes=32 time=14ms TTL=124
Reply from 120.32.19.2: bytes=32 time=15ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 17ms, Average = 14ms

C:\>
```

Red 120.32.7.0 [Consultorios_CNOR_P1] a Red 120.32.19.0 [Consultorios_CT_P2]

4.2.34 Conectividad CNOR | Piso 1 a CGOP

```
Pinging 120.32.29.2 with 32 bytes of data:

Reply from 120.32.29.2: bytes=32 time=6ms TTL=125
Reply from 120.32.29.2: bytes=32 time=28ms TTL=125
Reply from 120.32.29.2: bytes=32 time=14ms TTL=125
Reply from 120.32.29.2: bytes=32 time=29ms TTL=125

Ping statistics for 120.32.29.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 29ms, Average = 19ms

C:\>
```

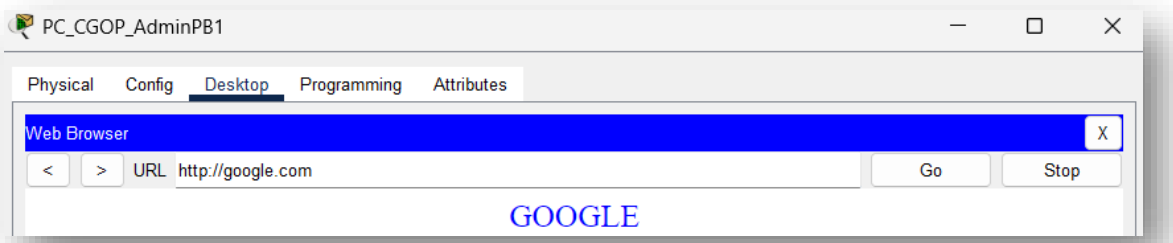
Red 120.32.10.0 [RezoJudio_CNOR_P1] a Red 120.32.29.0 [Invitados_CGOP_P1]

4.2.35 Conectividad CGOP | Planta Baja a Piso 1

```
Pinging 120.32.27.2 with 32 bytes of data:

Reply from 120.32.27.2: bytes=32 time=44ms TTL=126
Reply from 120.32.27.2: bytes=32 time=45ms TTL=126
Reply from 120.32.27.2: bytes=32 time=52ms TTL=126
Reply from 120.32.27.2: bytes=32 time=25ms TTL=126

Ping statistics for 120.32.27.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 52ms, Average = 41ms

C:\>
```

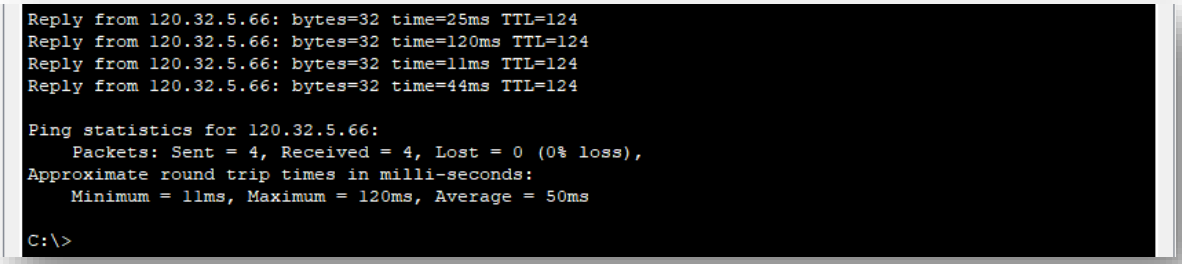
Red 120.32.23.0 [AtencionPublico_CGOP_PB] a Red 120.32.27.0 [Habitaciones_CGOP_P1]

4.2.36 Conectividad CGOP | Planta Baja a Internet



Red 120.32.26.0 [Administrativa_CGOP_1] a [Internet]

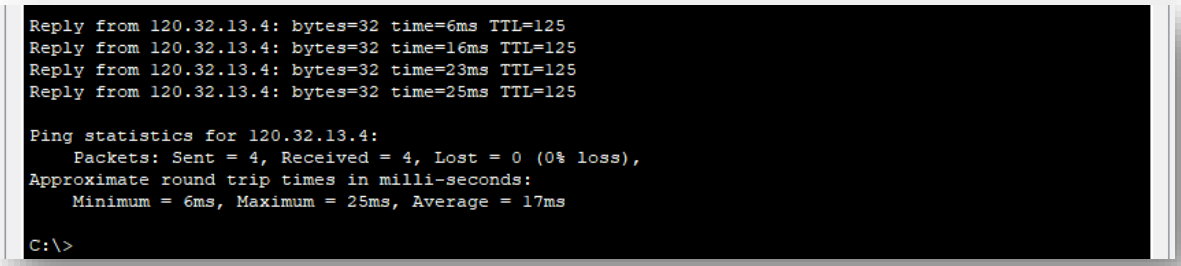
4.2.37 Conectividad CGOP | Planta Baja a Torre Central



```
Reply from 120.32.5.66: bytes=32 time=25ms TTL=124
Reply from 120.32.5.66: bytes=32 time=120ms TTL=124
Reply from 120.32.5.66: bytes=32 time=11ms TTL=124
Reply from 120.32.5.66: bytes=32 time=44ms TTL=124

Ping statistics for 120.32.5.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 120ms, Average = 50ms

C:\>
```

Red 120.32.25.0 [Invitados_CGOP] a Red 120.32.5.64 [CajaMedicos_TC_PB]

4.2.38 Conectividad CGOP | Planta Baja a CNOR



```
Reply from 120.32.13.4: bytes=32 time=6ms TTL=125
Reply from 120.32.13.4: bytes=32 time=16ms TTL=125
Reply from 120.32.13.4: bytes=32 time=23ms TTL=125
Reply from 120.32.13.4: bytes=32 time=25ms TTL=125

Ping statistics for 120.32.13.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 25ms, Average = 17ms

C:\>
```

Red 120.32.26.0 [Administrativa_CGOP_1] a Red 120.32.13.0 [RezosJudios_CNOR_P1]

4.2.39 Conectividad CGOP | Planta Baja a Torre de Consultorios

```
Reply from 120.32.21.3: bytes=32 time=26ms TTL=125
Reply from 120.32.21.3: bytes=32 time=25ms TTL=125
Reply from 120.32.21.3: bytes=32 time=17ms TTL=125
Reply from 120.32.21.3: bytes=32 time=33ms TTL=125

Ping statistics for 120.32.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 33ms, Average = 25ms

C:\>
```

Red 120.32.23.0 [AtencionPublico_CGOP_PB] a Red 120.32.21.0 [Invitados_CT_P2]

4.2.40 Conectividad CGOP | Piso 1 a Planta Baja

```
Pinging 120.32.26.2 with 32 bytes of data:

Reply from 120.32.26.2: bytes=32 time=64ms TTL=126
Reply from 120.32.26.2: bytes=32 time=36ms TTL=126
Reply from 120.32.26.2: bytes=32 time=44ms TTL=126
Reply from 120.32.26.2: bytes=32 time=6ms TTL=126

Ping statistics for 120.32.26.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 64ms, Average = 37ms

C:\>
```

Red 120.32.27.0 [Habitaciones_CGOP_P1] a Red 120.32.26.0 [Administrativa_CGOP_1]

4.2.41 Conectividad CGOP | Piso 1 a Internet

Red 120.32.28.0 [Habitaciones_CGOP_P1_2] a [Internet]

4.2.42 Conectividad CGOP | Piso 1 a Torre Central

```
Pinging 120.32.5.2 with 32 bytes of data:

Reply from 120.32.5.2: bytes=32 time=40ms TTL=123
Reply from 120.32.5.2: bytes=32 time=27ms TTL=123
Reply from 120.32.5.2: bytes=32 time=24ms TTL=123
Reply from 120.32.5.2: bytes=32 time=20ms TTL=123

Ping statistics for 120.32.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 40ms, Average = 27ms

C:\>
```

Red 120.32.29.0 [Invitados_CGOP_P1] a Red 120.32.5.0 [Administrativa_TC_2]

4.2.43 Conectividad CGOP | Piso 1 a CNOR

```
Reply from 120.32.11.2: bytes=32 time=12ms TTL=124
Reply from 120.32.11.2: bytes=32 time=21ms TTL=124
Reply from 120.32.11.2: bytes=32 time=20ms TTL=124
Reply from 120.32.11.2: bytes=32 time=39ms TTL=124

Ping statistics for 120.32.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 39ms, Average = 23ms

C:\>
```

Red 120.32.27.0 [Habitaciones_CGOP_P1] a Red 120.32.11.0 [Aulas_CNOR_P1]

4.2.44 Conectividad CGOP | Piso 1 a Torre de Consultorios

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=71ms TTL=124
Reply from 120.32.19.2: bytes=32 time=12ms TTL=124
Reply from 120.32.19.2: bytes=32 time=28ms TTL=124
Reply from 120.32.19.2: bytes=32 time=23ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 71ms, Average = 33ms

C:\>
```

Red 120.32.28.0 [Habitaciones_CGOP_P1_2] a Red 120.32.19.0 [Consultorios_CT_P2]

4.3 Verificación de Servicios

4.3.1 Servicio DNS | TC a Server_TC

Red 120.32.1.128 [TI_TC_NP] a Internet

4.3.2 Servicio DNS | CT a Server_TC

Red 120.32.16.0 [Consultorios_CT_P1] a [Internet]

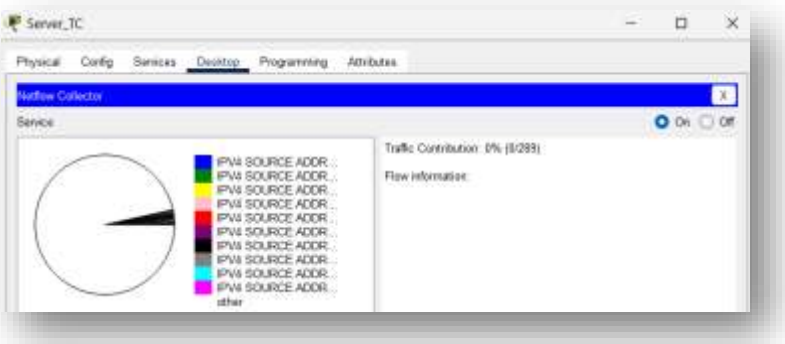
4.3.3 Servicio DNS | CNOR a Server_TC

Red 120.32.9.0 [Consultorios_CNOR_PB] a [Internet]

4.3.4 Servicio DNS | CGOP a Server_TC

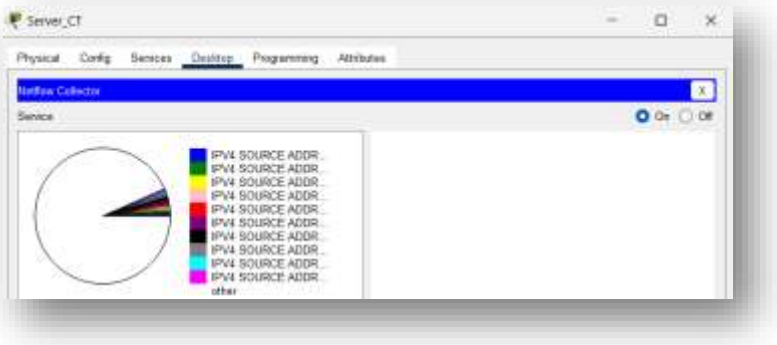
Red 120.32.28.0 [Habitaciones_CGOP_P1_2] a [Internet]

4.3.5 Servicio Netflow | Server_TC



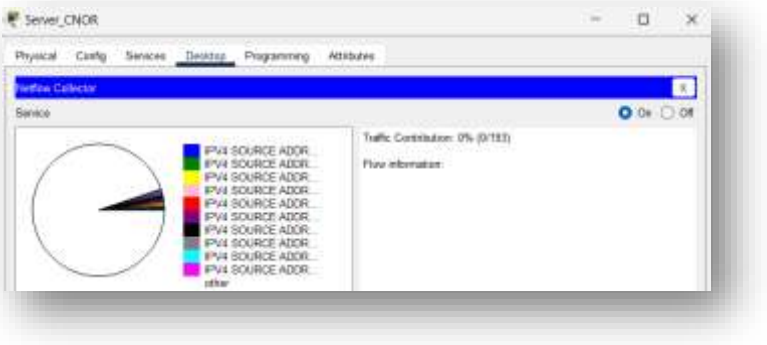
Netflow de servidor TC

4.3.6 Servicio Netflow | Server_CT



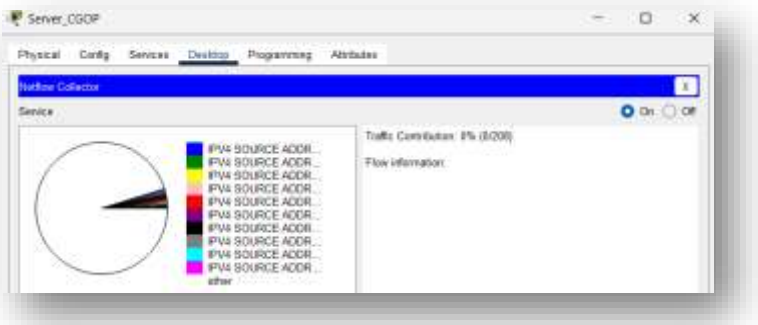
Netflow de servidor CT

4.3.7 Servicio Netflow | Server_CNOR



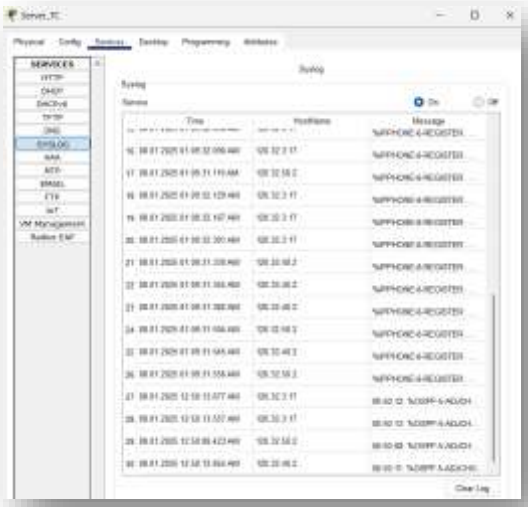
Netflow de servidor CNOR

4.3.8 Servicio Netflow | Server_CGOP



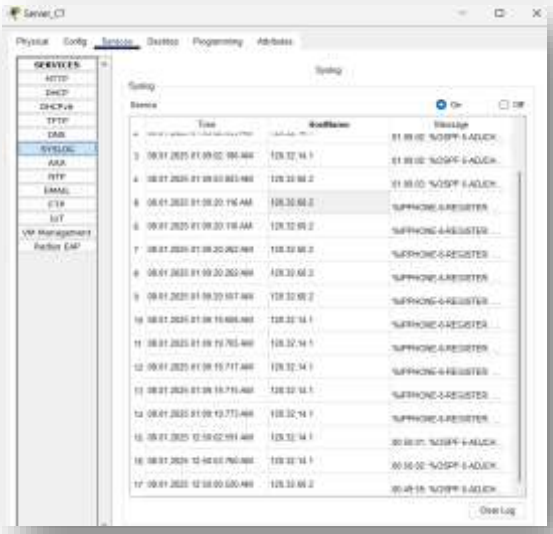
Netflow de servidor CGOP

4.3.9 Servicio Syslog | Server_TC



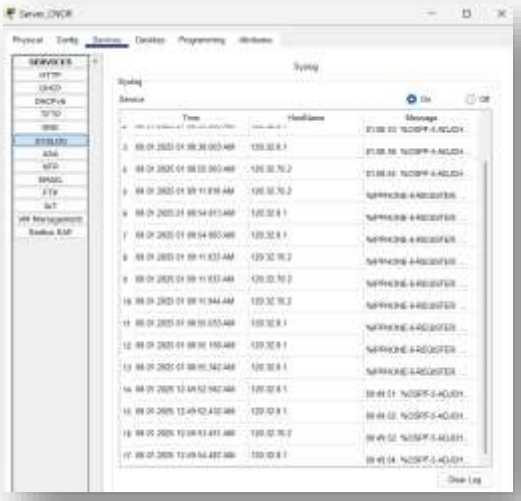
La imagen muestra la salida de un servidor Syslog. Los mensajes del registro indican que se han registrado varios teléfonos IP (IPPHONE-6-REGISTER) y que también se están estableciendo adyacencias de OSPF (OSPF-5-ADJCH).

4.3.10 Servicio Syslog | Server_CT



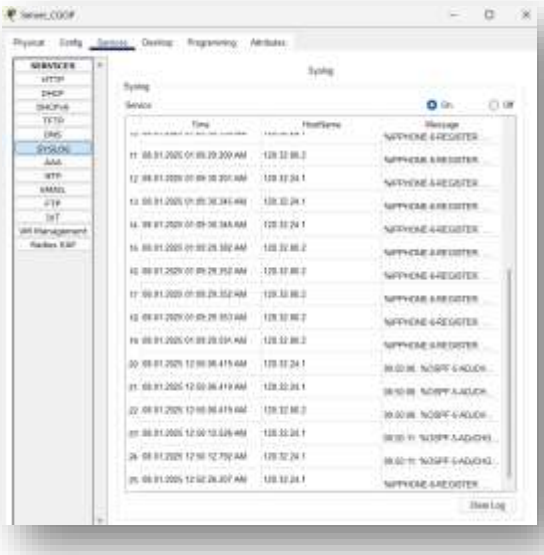
La imagen muestra la salida de un servidor Syslog. Los mensajes del registro indican que se han registrado varios teléfonos IP (IPPHONE-6-REGISTER) y que también se están estableciendo adyacencias de OSPF (OSPF-5-ADJCH).

4.3.11 Servicio Syslog | Server_CNOR



La imagen muestra la salida de un servidor Syslog. Los mensajes del registro indican que se han registrado varios teléfonos IP (IPPHONE-6-REGISTER) y que también se están estableciendo adyacencias de OSPF (OSPF-5-ADJCH).

4.3.12 Servicio Syslog | Server_CGOP



La imagen muestra la salida de un servidor Syslog. Los mensajes del registro indican que se han registrado varios teléfonos IP (IPPHONE-6-REGISTER) y que también se están estableciendo adyacencias de OSPF (OSPF-5-ADJCH).

4.3.13 Servicio DHCP | Server_TC

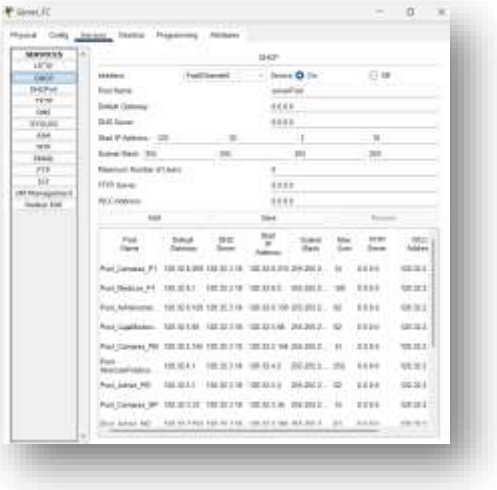
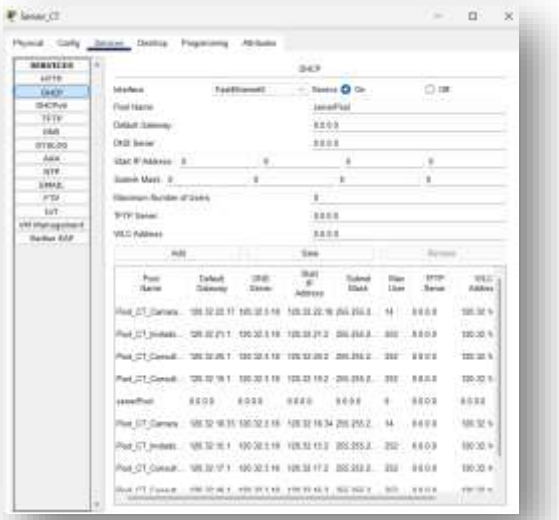


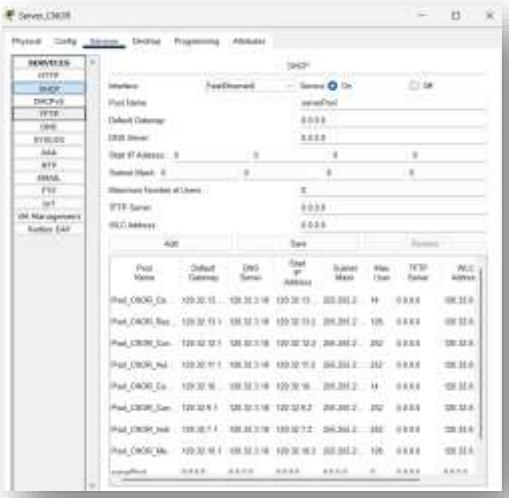
Ilustración 2 Se configura un servidor DHCP para asignar direcciones IP de forma automática a diferentes grupos de dispositivos, como cámaras, equipos médicos y administrativos, cada uno en su propio segmento de red. Esto se logra mediante pools de DHCP específicos, asegurando que cada tipo de dispositivo reciba las configuraciones de red adecuadas.

4.3.14 Servicio DHCP | Server_CT



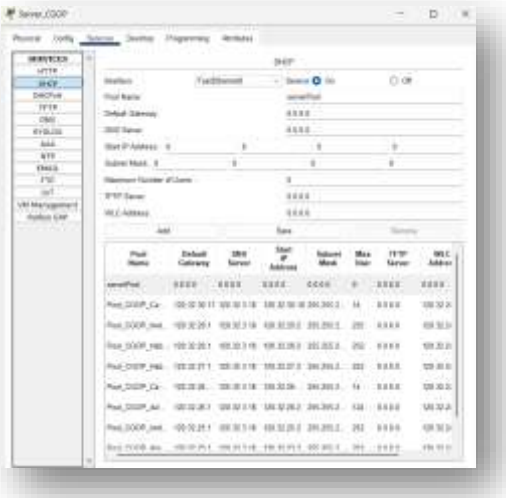
Se configura un servidor DHCP para asignar direcciones IP de forma automática a diferentes grupos de dispositivos, como cámaras, equipos médicos y administrativos, cada uno en su propio segmento de red. Esto se logra mediante pools de DHCP específicos, asegurando que cada tipo de dispositivo reciba las configuraciones de red adecuadas.

4.3.15 Servicio DHCP | Server_CNOR



Se configura un servidor DHCP para asignar direcciones IP de forma automática a diferentes grupos de dispositivos, como cámaras, equipos médicos, administrativos y de conserjería, cada uno en su propio segmento de red. Esto permite una gestión de direcciones organizada y eficiente.

4.3.16 Servicio DHCP | Server_CGOP



Se configura un servidor DHCP para asignar direcciones IP de forma automática a diferentes grupos de dispositivos, como cámaras, equipos médicos, administrativos y de conserjería, cada uno en su propio segmento de red. Esto permite una gestión de direcciones organizada y eficiente.

4.3.17 Servicio PAT | TC a Internet

Red [TecnologiaInformatica_TC] 120.32.2.128

```
Pro  Inside global      Inside local        Outside local       Outside global
icmp 208.100.20.1:5     120.32.2.130:5      192.168.0.3:5       192.168.0.3:5
icmp 208.100.20.1:6     120.32.2.130:6      192.168.0.3:6       192.168.0.3:6
icmp 208.100.20.1:7     120.32.2.130:7      192.168.0.3:7       192.168.0.3:7
icmp 208.100.20.1:8     120.32.2.130:8      192.168.0.3:8       192.168.0.3:8
```

Salida de TC a Internet

4.3.18 Servicio PAT | CT a Internet

Red [Invitados_CT_P1] 120.32.15.0

```
Pro  Inside global      Inside local        Outside local       Outside global
icmp 208.100.20.1:3     120.32.15.2:3       192.168.0.3:3       192.168.0.3:3
icmp 208.100.20.1:4     120.32.15.2:4       192.168.0.3:4       192.168.0.3:4
```

Salida de CT a Internet

4.3.19 Servicio PAT | CNOR a Internet

Red [Invitados_CNOR] 120.32.7.0

```
Pro  Inside global      Inside local        Outside local       Outside global
icmp 208.100.20.1:1     120.32.7.2:1        192.168.0.3:1       192.168.0.3:1
icmp 208.100.20.1:2     120.32.7.2:2        192.168.0.3:2       192.168.0.3:2
icmp 208.100.20.1:3     120.32.7.2:3        192.168.0.3:3       192.168.0.3:3
icmp 208.100.20.1:4     120.32.7.2:4        192.168.0.3:4       192.168.0.3:4
```

Salida de CNOR a Internet

4.3.20 Servicio PAT | CGOP a Internet

Red [AtencionPublico_CGOP_PB] 120.32.23.0

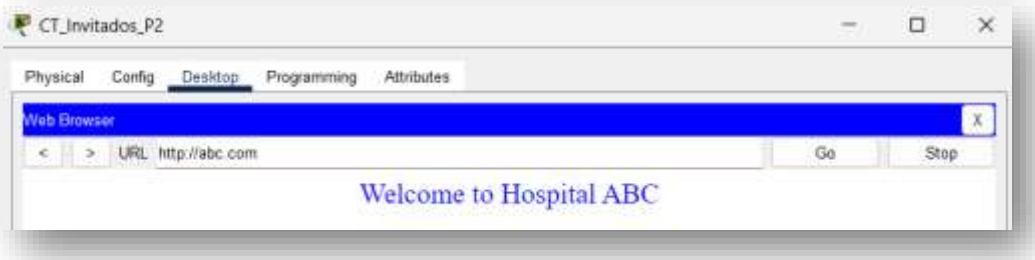
```
Pro  Inside global     Inside local       Outside local      Outside global
icmp 208.100.20.1:1024 120.32.23.2:1      192.168.0.3:1      192.168.0.3:1024
icmp 208.100.20.1:1025 120.32.23.2:2      192.168.0.3:2      192.168.0.3:1025
icmp 208.100.20.1:1026 120.32.23.2:3      192.168.0.3:3      192.168.0.3:1026
icmp 208.100.20.1:1027 120.32.23.2:4      192.168.0.3:4      192.168.0.3:1027
```

Salida de CGOP a Internet

4.3.21 Servicio HTTP | TC

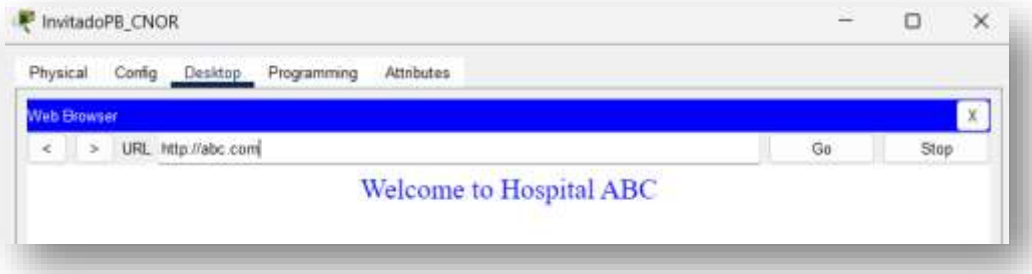
Pagina ABC por HTTP

4.3.22 Servicio HTTP | CT



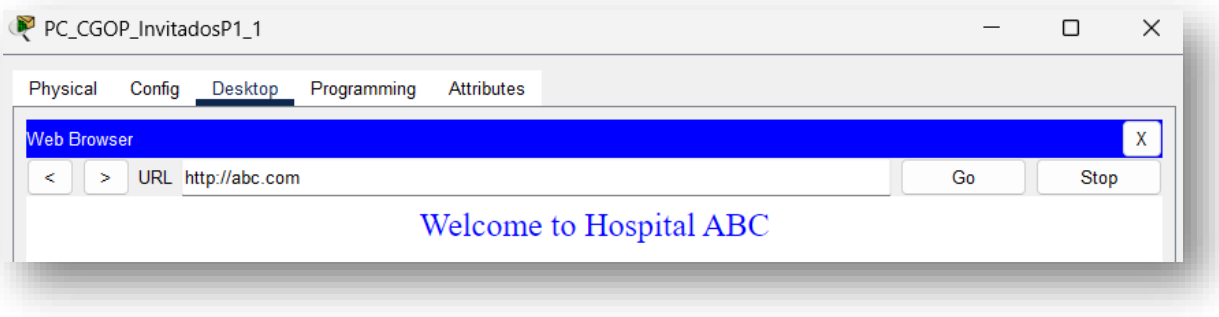
Pagina ABC por HTTP

4.3.23 Servicio HTTP | CNOR



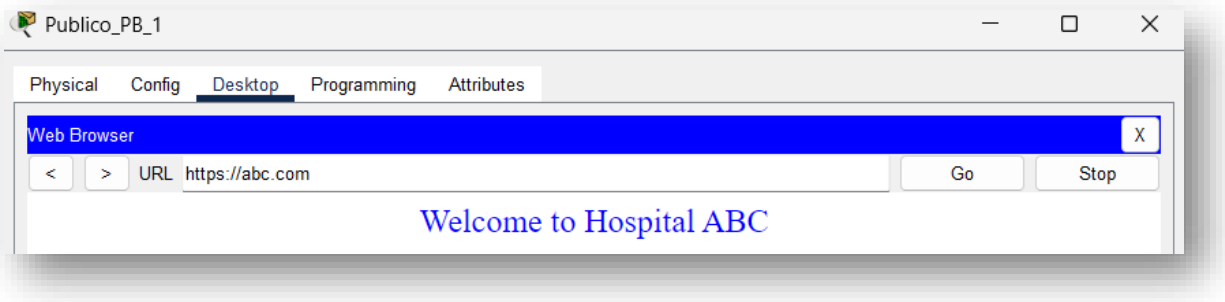
Pagina ABC por HTTP

4.3.24 Servicio HTTP | CGOP



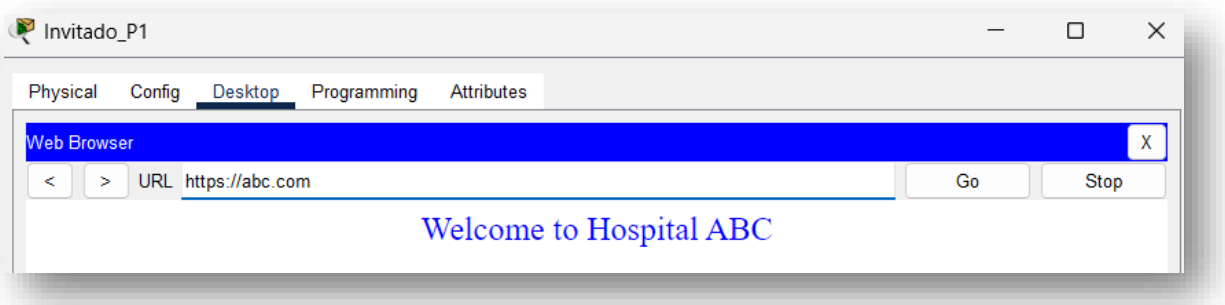
Pagina ABC por HTTP

4.3.25 Servicio HTTPS | TC



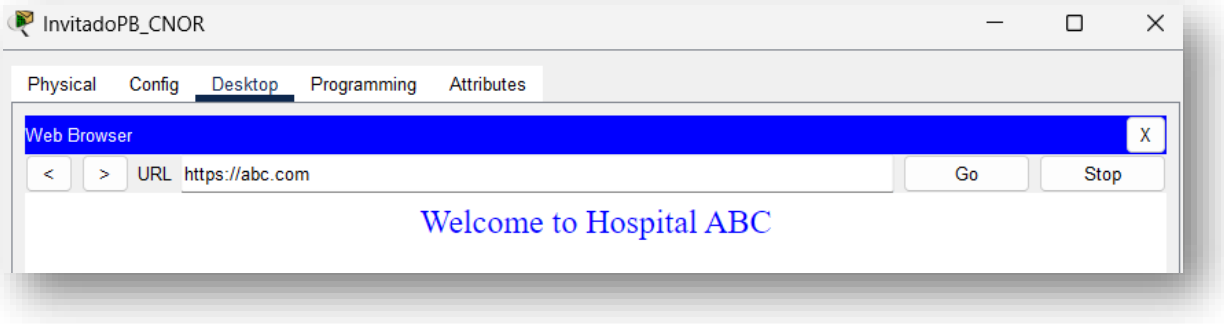
Este tipo de interfaz es utilizada en un entorno de red o sistema para acceder a sitios web, y en este caso, parece ser un portal institucional o informativo de un hospital.

4.3.26 Servicio HTTPS | CT



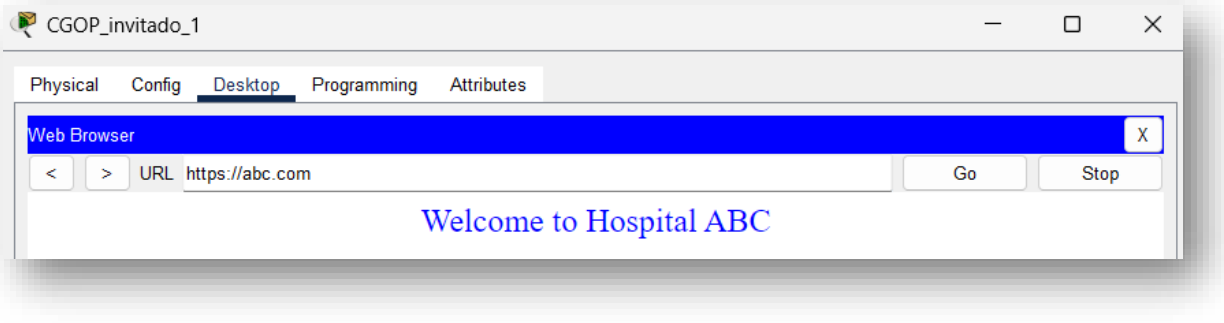
Este tipo de interfaz se utiliza comúnmente en redes o dispositivos para acceder a aplicaciones web o información en línea. En este caso, parece ser un acceso a una página de bienvenida o portal institucional.

4.3.27 Servicio HTTPS | CNOR



Este tipo de interfaz podría usarse dentro de un entorno corporativo o en una red para acceder a páginas web o aplicaciones internas, proporcionando información o recursos a los usuarios del sistema.

4.3.28 Servicio HTTPS | CGOP



Este tipo de interfaz podría ser utilizada en un dispositivo o red dentro de una infraestructura de una organización para acceder a recursos como páginas web internas o servicios de información.

4.3.29 Servicio NTP | TC

Server_TC

Este panel permite gestionar la configuración de NTP, lo que garantiza que el sistema esté sincronizado con la hora correcta.

4.3.30 Servicio TC_R_NP | TC_R_PB | TC_R_P1

```
TC_R_NP#show clock
23:54:13.31 UTC Thu Jul 31 2025
TC_R_NP#
```

Esto refleja la hora actual configurada en el dispositivo en UTC (Tiempo Universal Coordinado), mostrando que el reloj del sistema está correctamente sincronizado y actualizado.

```
TC_R_PB#show clock
23:54:33.92 UTC Thu Jul 31 2025
TC_R_PB#
```

Este comando refleja la hora actual del dispositivo en UTC (Tiempo Universal Coordinado), lo que confirma que el reloj está configurado correctamente y actualizado.

```
TC_R_P1#show clock
*23:54:54.340 UTC Thu Jul 31 2025
TC_R_P1#
```

Esto muestra la hora actual configurada en el dispositivo en UTC (Tiempo Universal Coordinado), reflejando que el reloj del sistema está correctamente configurado y sincronizado.

4.3.31 Servicio TC_SW_NP | TC_SW_PB | TC_SW_P1

```
TC_SW_NP#show clock
23:55:26.414 UTC Thu Jul 31 2025
TC_SW_NP#
```

Esto refleja la hora actual del dispositivo en UTC (Tiempo Universal Coordinado), confirmando que el reloj del sistema está configurado correctamente y sincronizado con la hora precisa.

```
TC_SW_PB#show clock
23:55:51.812 UTC Thu Jul 31 2025
TC_SW_PB#
```

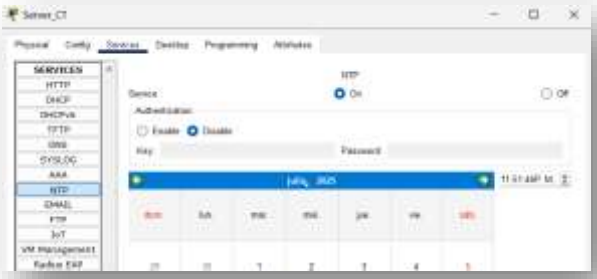
Este comando muestra la hora actual configurada en el dispositivo en UTC (Tiempo Universal Coordinado), indicando que el reloj está correctamente configurado y actualizado.

```
TC_SW_P1#show clock
23:56:11.363 UTC Thu Jul 31 2025
TC_SW_P1#
```

Este comando muestra la hora actual del dispositivo en UTC (Tiempo Universal Coordinado), confirmando que el reloj del sistema está configurado y sincronizado correctamente.

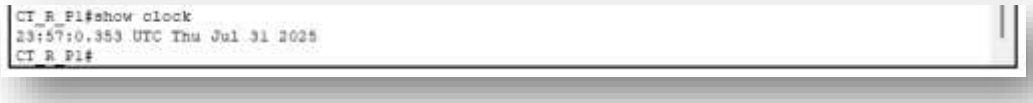
4.3.32 Servicio NTP | CT

Server_CT



Esto indica que el servidor NTP está configurado correctamente y sincronizado con la hora exacta, según la visualización en el calendario.

4.3.33 Servicio CT_R_P1 | CT_R_P2



```
CT_R_P1#show clock
23:57:0.353 UTC Thu Jul 31 2025
CT_R_P1#
```

Esto refleja la hora actual configurada en el dispositivo en UTC (Tiempo Universal Coordinado), lo que indica que el reloj del sistema está correctamente configurado y sincronizado.

```
CT_R_P2#show clock
23:57:19.111 UTC Thu Jul 31 2025
CT_R_P2#
```

Esto muestra la hora actual del dispositivo en UTC (Tiempo Universal Coordinado), reflejando la hora precisa y actualizada del sistema.

4.3.34 Servicio CT_SW_P1 | CT_SW_P2

```
CT_SW_P1#show clock
23:57:41.95 UTC Thu Jul 31 2025
CT_SW_P1#
```

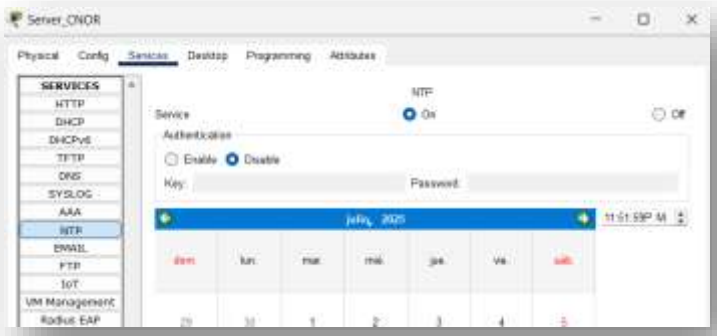
Esto refleja la hora actual del dispositivo en UTC (Tiempo Universal Coordinado), mostrando que el reloj está configurado correctamente y está sincronizado con la hora precisa.

```
CT_SW_P2#show clock
23:57:58.603 UTC Thu Jul 31 2025
CT_SW_P2#
```

Este comando muestra la hora actual configurada en el dispositivo, que está en UTC (Tiempo Universal Coordinado), reflejando la hora precisa y actualizada del sistema.

4.3.35 Servicio NTP | CNOR

Server_CNOR



Este panel de configuración permite gestionar cómo el servidor NTP sincroniza la hora del dispositivo con un servidor NTP externo.

4.3.36 Servicio CNOR_R_PB | CNOR_R_P1

```
CNOR_R_PB#show clock
23:58:41.947 UTC Thu Jul 31 2025
CNOR_R_PB#
```

Esto muestra la hora actual en UTC (Tiempo Universal Coordinado) en el dispositivo, confirmando que el reloj del sistema está correctamente configurado y actualizado.

```
CNOR_R_P1#show clock
23:59:0.618 UTC Thu Jul 31 2025
CNOR_R_P1#
```

Esto muestra la hora actual en UTC (Tiempo Universal Coordinado) en el dispositivo, confirmando que el reloj está correctamente configurado y sincronizado.

4.3.37 Servicio CNOR_SW_PB | CNOR_SW_P1

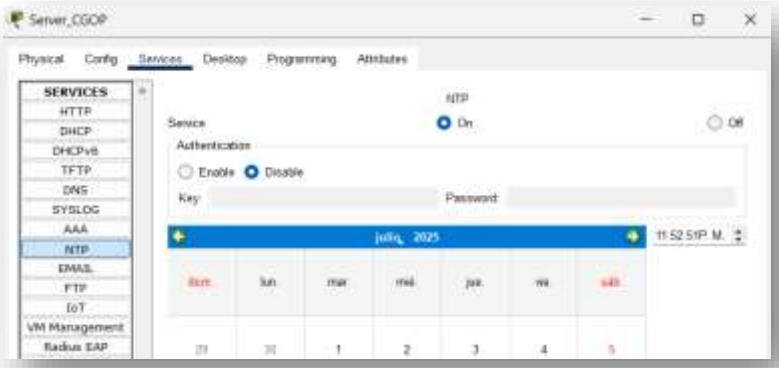
```
CNOR_SW_PB#show clock
23:59:26.882 UTC Thu Jul 31 2025
CNOR_SW_PB#
```

Este comando muestra la hora actual del dispositivo en formato UTC (Tiempo Universal Coordinado), lo que indica que el reloj del switch está configurado correctamente y refleja la hora precisa del sistema.

```
CNOR_SW_P1#show clock
23:59:43.439 UTC Thu Jul 31 2025
CNOR_SW_P1#
```

indica que el reloj del switch está configurado correctamente, mostrando la hora actual según el tiempo UTC.

4.3.38 Servicio NTP | CGOP



Este panel de configuración permite gestionar cómo el servidor NTP sincroniza la hora del dispositivo con un servidor NTP externo.

4.3.39 Servicio CGOP_R_PB | CNOR_R_P1

```
CGOP_R_PB#show clock
0:0:44.321 UTC Fri Aug 1 2025
CGOP_R_PB#
```

Esto muestra la hora actual en UTC (Tiempo Universal Coordinado) en el dispositivo, confirmando que el reloj del sistema está correctamente configurado y actualizado.

```
CGOP_R_P1#show clock
0:1:30.468 UTC Fri Aug 1 2025
CGOP_R_P1#
```

Esto muestra la hora actual en UTC (Tiempo Universal Coordinado) en el dispositivo, confirmando que el reloj está correctamente configurado y sincronizado.

4.3.40 Servicio CGOP_SW_PB | CNOR_SW_P1

```
CGOP_SW_PB#show clock
0:1:52.490 UTC Fri Aug 1 2025
CGOP_SW_PB#
```

Indica que el reloj del switch está configurado correctamente, mostrando la hora actual según el tiempo UTC.

```
CGOP_SW_P1#show clock
0:2:9.146 UTC Fri Aug 1 2025
CGOP_SW_P1#
```

Indica que el reloj del switch está configurado correctamente, mostrando la hora actual según el tiempo UTC.

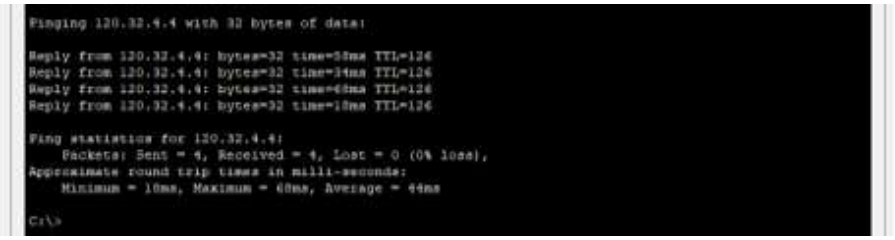
Fase 5

5.1 Validación del funcionamiento de todos los servicios de la red

Servicio	Torre Central	Torre de Consultorios	CNOR	CGOP
NTP	Funcionando	Funcionando	Funcionando	Funcionando
DHCP	Funcionando	Funcionando	Funcionando	Funcionando
NTP	Funcionando	Funcionando	Funcionando	Funcionando
PAT	Funcionando	Funcionando	Funcionando	Funcionando
FTP	Funcionando	Funcionando	Funcionando	Funcionando
TFTP	Funcionando	Funcionando	Funcionando	Funcionando
SSH	Funcionando	Funcionando	Funcionando	Funcionando
HTTP	Funcionando	Funcionando	Funcionando	Funcionando
HTTPS	Funcionando	Funcionando	Funcionando	Funcionando
AAA [Tacacs]	Funcionando	Funcionando	Funcionando	Funcionando
Gmail	Funcionando	Funcionando	Funcionando	Funcionando
Syslog	Funcionando	Funcionando	Funcionando	Funcionando
Netflow	Funcionando	Funcionando	Funcionando	Funcionando
loT	Funcionando	Funcionando	Funcionando	Funcionando
ACL	En proceso	En proceso	En proceso	En proceso
VPN	Funcionando	Funcionando	Funcionando	Funcionando

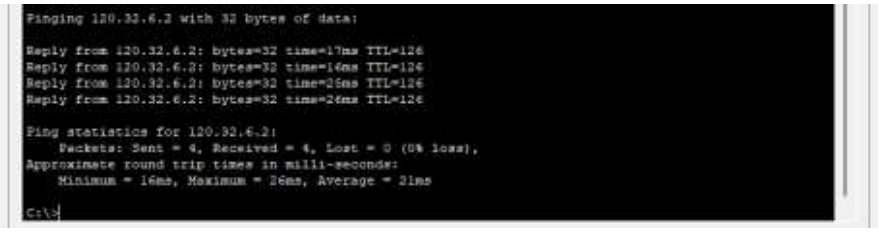
5.2 Pruebas de Conectividad entre áreas VLAN

5.2.1 Conectividad Entre VLAN de TC



VLAN [AtencionPublico_TC_NP | 120.32.0.0] a VLAN [AtencionPublico_TC_PB | Red 120.32.4.0]

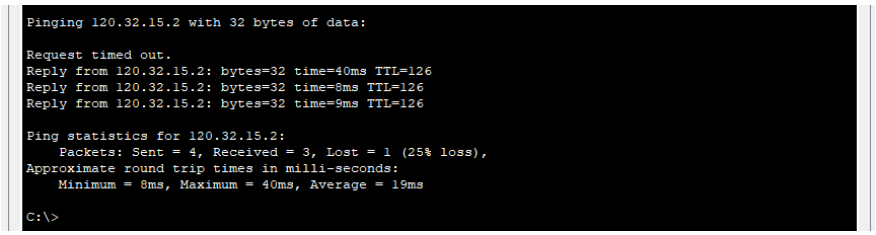
En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.4.4 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.



VLAN [Invitados_TC_NP | 120.32.1.0] a VLAN [Medicos_TC_P1 | Red 120.32.6.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.6.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.2 Conectividad VLAN TC a VLAN CT



VLAN [Invitados_TC_NP | 120.32.1.128] a VLAN [Invitados_CT_P1 | 120.32.15.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.15.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.3 Conectividad VLAN TC a VLAN CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

VLAN [TI_TC_NP | 120.32.1.128] a VLAN [Invitados_CNOR | 120.32.7.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.7.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.4 Conectividad VLAN TC a VLAN CGOP

```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

VLAN [Administrativa_TC_NP | 120.32.2.192] a VLAN [Invitados_CGOP | 120.32.25.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.25.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.5 Conectividad VLAN TC a VLAN CT

```
Pinging 120.32.15.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.15.2: bytes=32 time=40ms TTL=126
Reply from 120.32.15.2: bytes=32 time=8ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 40ms, Average = 19ms

C:\>
```

VLAN [AtencionPublico_TC_PB | 120.32.4.0] a VLAN [Invitados_CT_P1 | 120.32.15.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.15.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable

5.2.6 Conectividad VLAN TC a VLAN CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

VLAN [Administrativa_TC_2 | 120.32.5.0] a VLAN [Invitados_CNOR | 120.32.7.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.7.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.7 Conectividad VLAN TC a VLAN CGOP

```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

VLAN [CajaMedicos_TC_PB | 120.32.5.64] a VLAN [Invitados_CGOP | 120.32.25.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.25.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.8 Conectividad VLAN TC a VLAN CT

```
Pinging 120.32.15.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.15.2: bytes=32 time=40ms TTL=126
Reply from 120.32.15.2: bytes=32 time=8ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 40ms, Average = 19ms

C:\>
```

VLAN [Medicos_TC_P1 | 120.32.6.0] a VLAN [Invitados_CT_P1 | 120.32.15.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.15.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.9 Conectividad VLAN TC a VLAN CNOR

```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=10ms TTL=126
Reply from 120.32.7.2: bytes=32 time=29ms TTL=126
Reply from 120.32.7.2: bytes=32 time=15ms TTL=126
Reply from 120.32.7.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 29ms, Average = 15ms

C:\>
```

VLAN [Administrativa_TC_3 | 120.32.5.0] a VLAN [Invitados_CNOR | 120.32.7.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.7.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

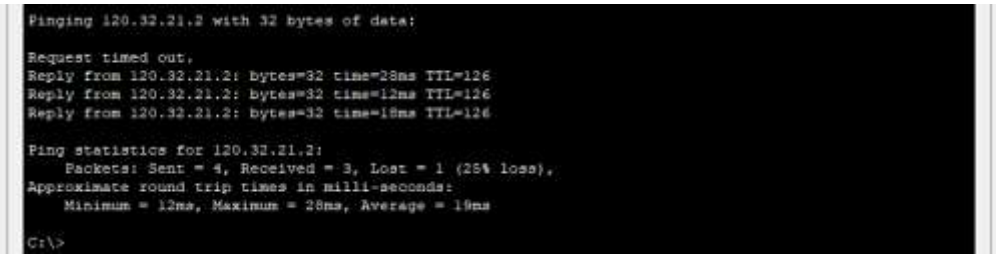
5.2.10 Conectividad VLAN TC a VLAN CGOP

```
Pinging 120.32.25.2 with 32 bytes of data:

Reply from 120.32.25.2: bytes=32 time=13ms TTL=125
Reply from 120.32.25.2: bytes=32 time=16ms TTL=125
Reply from 120.32.25.2: bytes=32 time=35ms TTL=125
Reply from 120.32.25.2: bytes=32 time=15ms TTL=125

Ping statistics for 120.32.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 35ms, Average = 19ms

C:\>
```

VLAN [Medicos_TC_P1 | 120.32.6.0] a VLAN [Invitados_CGOP | 120.32.25.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.25.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.11 Conectividad VLAN CT a VLAN CT

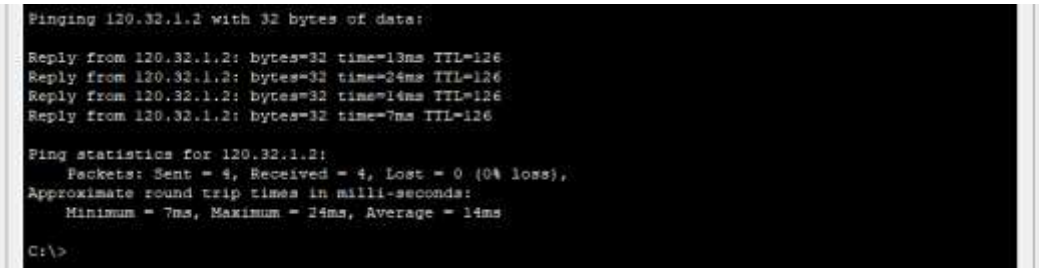


```
Pinging 120.32.21.2 with 32 bytes of data:

Request timed out.
Reply from 120.32.21.2: bytes=32 time=28ms TTL=126
Reply from 120.32.21.2: bytes=32 time=12ms TTL=126
Reply from 120.32.21.2: bytes=32 time=18ms TTL=126

Ping statistics for 120.32.21.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 28ms, Average = 19ms

C:\>
```

VLAN [Invitados_CT_P1 | 120.32.15.0] a VLAN [Invitados_CT_P2 | 120.32.21.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.21.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.12 Conectividad VLAN CT a VLAN TC

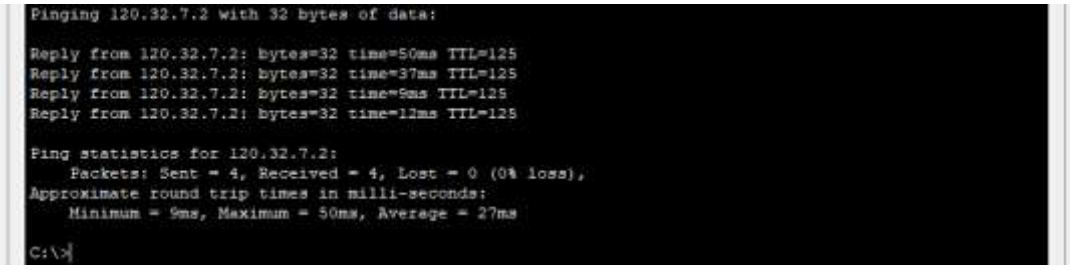


```
Pinging 120.32.1.2 with 32 bytes of data:

Reply from 120.32.1.2: bytes=32 time=13ms TTL=126
Reply from 120.32.1.2: bytes=32 time=24ms TTL=126
Reply from 120.32.1.2: bytes=32 time=14ms TTL=126
Reply from 120.32.1.2: bytes=32 time=7ms TTL=126

Ping statistics for 120.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 24ms, Average = 14ms

C:\>
```

VLAN [Invitados_CT_P1 | 120.32.1.128] a VLAN [Invitados_TC_NP | 120.32.1.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.1.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

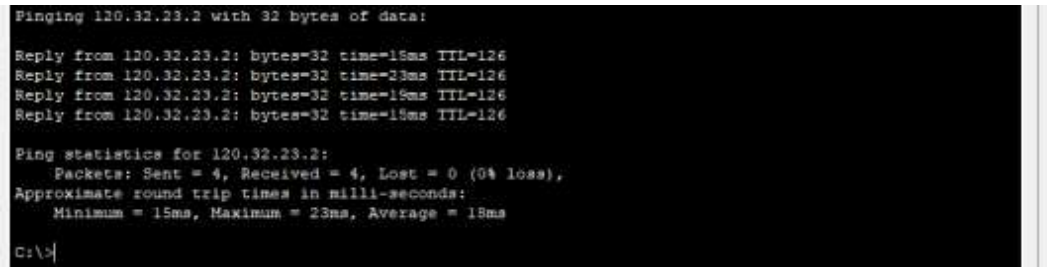
5.2.13 Conectividad VLAN CT a VLAN CNOR



```
Pinging 120.32.7.2 with 32 bytes of data:

Reply from 120.32.7.2: bytes=32 time=50ms TTL=125
Reply from 120.32.7.2: bytes=32 time=37ms TTL=125
Reply from 120.32.7.2: bytes=32 time=9ms TTL=125
Reply from 120.32.7.2: bytes=32 time=12ms TTL=125

Ping statistics for 120.32.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 50ms, Average = 27ms

C:\>
```

VLAN [Consultorios_CT_P1 | 120.32.16.0] a VLAN [Invitados_CNOR | 120.32.7.0]

5.2.14 Conectividad VLAN CT a VLAN CGOP

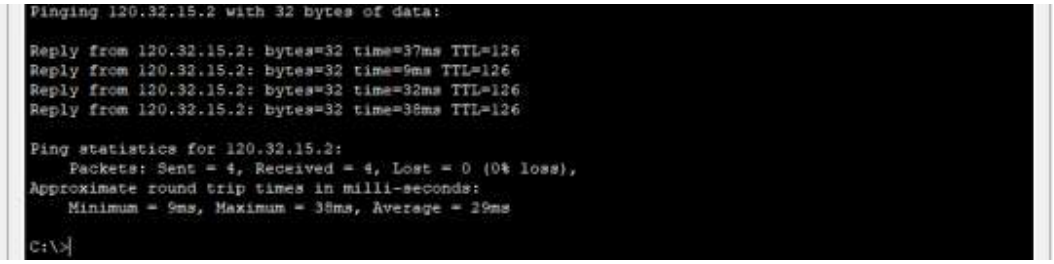


```
Pinging 120.32.23.2 with 32 bytes of data:

Reply from 120.32.23.2: bytes=32 time=15ms TTL=126
Reply from 120.32.23.2: bytes=32 time=23ms TTL=126
Reply from 120.32.23.2: bytes=32 time=19ms TTL=126
Reply from 120.32.23.2: bytes=32 time=15ms TTL=126

Ping statistics for 120.32.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 23ms, Average = 18ms

C:\>
```

VLAN [Consultorios_CT_P1_2 | 120.32.17.0] a VLAN [AtencionPublico_CGOP_PB | 120.32.23.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.23.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.15 Conectividad VLAN CT a VLAN CT

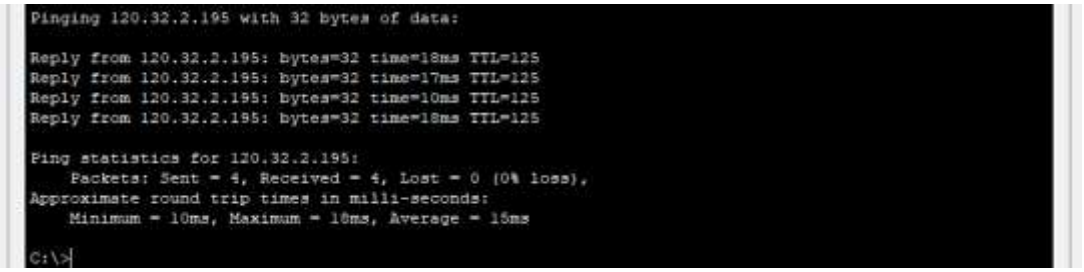


```
Pinging 120.32.15.2 with 32 bytes of data:

Reply from 120.32.15.2: bytes=32 time=37ms TTL=126
Reply from 120.32.15.2: bytes=32 time=9ms TTL=126
Reply from 120.32.15.2: bytes=32 time=32ms TTL=126
Reply from 120.32.15.2: bytes=32 time=38ms TTL=126

Ping statistics for 120.32.15.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 38ms, Average = 29ms

C:\>
```

VLAN [Invitados_CT_P2 | 120.32.21.0] a VLAN [Invitados_CT_P1 | 120.32.15.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.15.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.16 Conectividad VLAN CT a VLAN TC

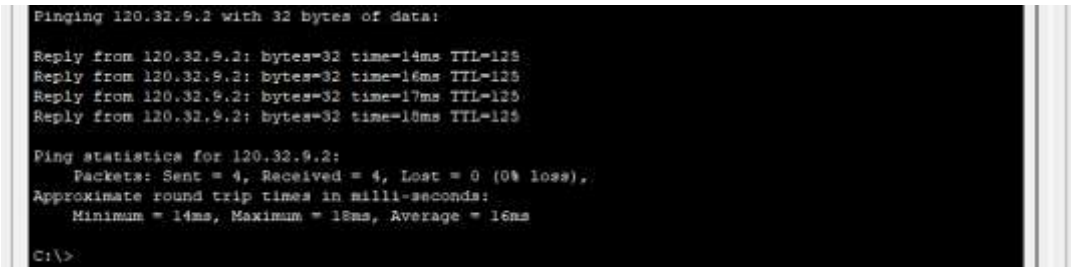


```
Pinging 120.32.2.195 with 32 bytes of data:

Reply from 120.32.2.195: bytes=32 time=18ms TTL=125
Reply from 120.32.2.195: bytes=32 time=17ms TTL=125
Reply from 120.32.2.195: bytes=32 time=10ms TTL=125
Reply from 120.32.2.195: bytes=32 time=18ms TTL=125

Ping statistics for 120.32.2.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 18ms, Average = 15ms

C:\>
```

VLAN [Invitados_CT_P2 | 120.32.21.0] a VLAN [Administrativa_TC | 120.32.2.192]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.2.195 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.17 Conectividad VLAN CT a VLAN CNOR

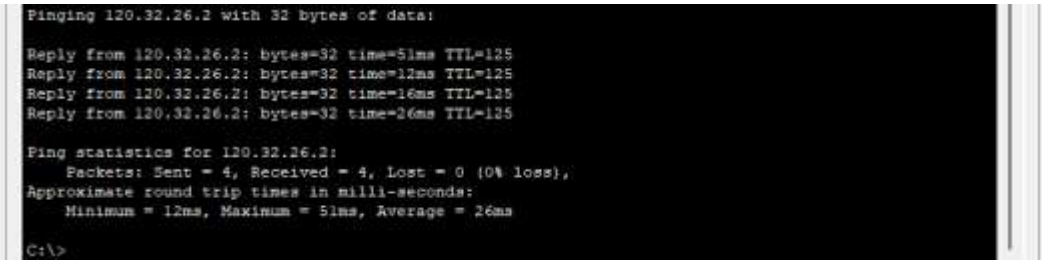


```
Pinging 120.32.9.2 with 32 bytes of data:

Reply from 120.32.9.2: bytes=32 time=14ms TTL=125
Reply from 120.32.9.2: bytes=32 time=16ms TTL=125
Reply from 120.32.9.2: bytes=32 time=17ms TTL=125
Reply from 120.32.9.2: bytes=32 time=18ms TTL=125

Ping statistics for 120.32.9.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 18ms, Average = 16ms

C:\>
```

VLAN [Consultorios_CT_P2_2 | 120.32.20.0] a VLAN [Consultorios_CNOR_PB | 120.32.9.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.9.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.18 Conectividad VLAN CT a VLAN CGOP



```
Pinging 120.32.26.2 with 32 bytes of data:

Reply from 120.32.26.2: bytes=32 time=51ms TTL=125
Reply from 120.32.26.2: bytes=32 time=12ms TTL=125
Reply from 120.32.26.2: bytes=32 time=16ms TTL=125
Reply from 120.32.26.2: bytes=32 time=26ms TTL=125

Ping statistics for 120.32.26.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 51ms, Average = 26ms

C:\>
```

VLAN [Invitados_CT_P2 | 120.32.21.0] a VLAN [Administrativa_CGOP_1 | 120.32.26.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.26.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.19 Conectividad VLAN CNOR a VLAN CNOR

```
Pinging 120.32.11.2 with 32 bytes of data:

Reply from 120.32.11.2: bytes=32 time=6ms TTL=126
Reply from 120.32.11.2: bytes=32 time=14ms TTL=126
Reply from 120.32.11.2: bytes=32 time=12ms TTL=126
Reply from 120.32.11.2: bytes=32 time=13ms TTL=126

Ping statistics for 120.32.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 14ms, Average = 11ms

C:\>
```

VLAN [Invitados_CNOR | 120.32.7.0] a VLAN [Aulas_CNOR_P1 | 120.32.11.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.11.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.20 Conectividad VLAN CNOR a VLAN TC

```
Pinging 120.32.6.130 with 32 bytes of data:

Reply from 120.32.6.130: bytes=32 time=26ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=14ms TTL=125

Ping statistics for 120.32.6.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 26ms, Average = 20ms

C:\>
```

VLAN [Medicos_CNOR_PB | 120.32.10.0] a VLAN [Administrativa_TC_3 | 120.32.6.128]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.6.130 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.21 Conectividad VLAN CNOR a VLAN CT

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=13ms TTL=124
Reply from 120.32.19.2: bytes=32 time=17ms TTL=124
Reply from 120.32.19.2: bytes=32 time=14ms TTL=124
Reply from 120.32.19.2: bytes=32 time=15ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 17ms, Average = 14ms

C:\>
```

VLAN [Invitados_CNOR_PB | 120.32.7.0] a VLAN [Consultorios_CT_P2 | 120.32.19.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.19.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.22 Conectividad VLAN CNOR a VLAN CGOP

```
Pinging 120.32.29.2 with 32 bytes of data:

Reply from 120.32.29.2: bytes=32 time=6ms TTL=125
Reply from 120.32.29.2: bytes=32 time=28ms TTL=125
Reply from 120.32.29.2: bytes=32 time=14ms TTL=125
Reply from 120.32.29.2: bytes=32 time=29ms TTL=125

Ping statistics for 120.32.29.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 29ms, Average = 19ms

C:\>
```

VLAN [Medicos_CNOR_PB | 120.32.10.0] a VLAN [Invitados_CGOP_P1 | 120.32.29.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.29.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.23 Conectividad VLAN CNOR a VLAN CNOR

```
Pinging 120.32.10.3 with 32 bytes of data:

Reply from 120.32.10.3: bytes=32 time=25ms TTL=126
Reply from 120.32.10.3: bytes=32 time=20ms TTL=126
Reply from 120.32.10.3: bytes=32 time=19ms TTL=126
Reply from 120.32.10.3: bytes=32 time=15ms TTL=126

Ping statistics for 120.32.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 25ms, Average = 19ms

C:\>
```

VLAN [Invitados_CGOP_P1 | 120.32.11.0] a VLAN [Medicos_CGOP_PB | 120.32.10.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.10.3 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.24 Conectividad VLAN CNOR a VLAN TC

```
Pinging 120.32.6.130 with 32 bytes of data:

Reply from 120.32.6.130: bytes=32 time=26ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=20ms TTL=125
Reply from 120.32.6.130: bytes=32 time=14ms TTL=125

Ping statistics for 120.32.6.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 26ms, Average = 20ms

C:\>
```

VLAN [Aulas_CNOR_P1 | 120.32.11.0] a VLAN [Administrativa_TC_3 | 120.32.6.128]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.6.130 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.25 Conectividad VLAN CNOR a VLAN CT

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=13ms TTL=124
Reply from 120.32.19.2: bytes=32 time=17ms TTL=124
Reply from 120.32.19.2: bytes=32 time=14ms TTL=124
Reply from 120.32.19.2: bytes=32 time=15ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 17ms, Average = 14ms

C:\>
```

VLAN [Consultorios_CNOR_P1 | 120.32.7.0] a VLAN [Consultorios_CT_P2 | 120.32.19.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.19.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.26 Conectividad VLAN CNOR a VLAN CGOP

```
Pinging 120.32.29.2 with 32 bytes of data:

Reply from 120.32.29.2: bytes=32 time=6ms TTL=125
Reply from 120.32.29.2: bytes=32 time=28ms TTL=125
Reply from 120.32.29.2: bytes=32 time=14ms TTL=125
Reply from 120.32.29.2: bytes=32 time=29ms TTL=125

Ping statistics for 120.32.29.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 29ms, Average = 19ms

C:\>
```

VLAN [RezoJudio_CNOR_P1 | 120.32.10.0] a VLAN [Invitados_CGOP_P1 | 120.32.29.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.29.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.27 Conectividad VLAN CGOP a VLAN CGOP

```
Pinging 120.32.27.2 with 32 bytes of data:

Reply from 120.32.27.2: bytes=32 time=44ms TTL=126
Reply from 120.32.27.2: bytes=32 time=45ms TTL=126
Reply from 120.32.27.2: bytes=32 time=52ms TTL=126
Reply from 120.32.27.2: bytes=32 time=25ms TTL=126

Ping statistics for 120.32.27.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 52ms, Average = 41ms

C:\>
```

VLAN [AtencionPublico_CGOP_PB | 120.32.23.0] a VLAN [Habitaciones_CGOP_P1 | 120.32.27.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.27.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.28 Conectividad VLAN CGOP a VLAN TC

```
Reply from 120.32.5.66: bytes=32 time=25ms TTL=124
Reply from 120.32.5.66: bytes=32 time=120ms TTL=124
Reply from 120.32.5.66: bytes=32 time=11ms TTL=124
Reply from 120.32.5.66: bytes=32 time=44ms TTL=124

Ping statistics for 120.32.5.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 120ms, Average = 50ms

C:\>
```

VLAN [Invitados_CGOP | 120.32.25.0] a VLAN [CajaMedicos_TC_PB | 120.32.5.64]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.5.66 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.29 Conectividad VLAN CGOP a VLAN CNOR

```
Reply from 120.32.13.4: bytes=32 time=6ms TTL=125
Reply from 120.32.13.4: bytes=32 time=16ms TTL=125
Reply from 120.32.13.4: bytes=32 time=23ms TTL=125
Reply from 120.32.13.4: bytes=32 time=25ms TTL=125

Ping statistics for 120.32.13.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 25ms, Average = 17ms

C:\>
```

VLAN [Administrativa_CGOP_1 | 120.32.26.0] a VLAN [RezosJudios_CNOR_P1 | 120.32.13.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.13.4 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.30 Conectividad VLAN CGOP a VLAN CT

```
Reply from 120.32.21.3: bytes=32 time=26ms TTL=125
Reply from 120.32.21.3: bytes=32 time=25ms TTL=125
Reply from 120.32.21.3: bytes=32 time=17ms TTL=125
Reply from 120.32.21.3: bytes=32 time=33ms TTL=125

Ping statistics for 120.32.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 33ms, Average = 25ms

C:\>
```

VLAN [AtencionPublico_CGOP_PB | 120.32.23.0] a VLAN [Invitados_CT_P2 | 120.32.21.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.21.3 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.31 Conectividad VLAN CGOP a VLAN CGOP

```
Pinging 120.32.26.2 with 32 bytes of data:

Reply from 120.32.26.2: bytes=32 time=64ms TTL=126
Reply from 120.32.26.2: bytes=32 time=36ms TTL=126
Reply from 120.32.26.2: bytes=32 time=44ms TTL=126
Reply from 120.32.26.2: bytes=32 time=6ms TTL=126

Ping statistics for 120.32.26.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 64ms, Average = 37ms

C:\>
```

VLAN [Habitaciones_CGOP_P1 | 120.32.27.0] a VLAN [Administrativa_CGOP_1 | 120.32.26.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.26.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.32 Conectividad VLAN CGOP a VLAN TC

```
Pinging 120.32.5.2 with 32 bytes of data:

Reply from 120.32.5.2: bytes=32 time=40ms TTL=123
Reply from 120.32.5.2: bytes=32 time=27ms TTL=123
Reply from 120.32.5.2: bytes=32 time=24ms TTL=123
Reply from 120.32.5.2: bytes=32 time=20ms TTL=123

Ping statistics for 120.32.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 40ms, Average = 27ms

C:\>
```

VLAN [Invitados_CGOP_P1 | 120.32.29.0] a VLAN [Administrativa_TC_2 | 120.32.5.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.5.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.33 Conectividad VLAN CGOP a VLAN CNOR

```
Reply from 120.32.11.2: bytes=32 time=12ms TTL=124
Reply from 120.32.11.2: bytes=32 time=21ms TTL=124
Reply from 120.32.11.2: bytes=32 time=20ms TTL=124
Reply from 120.32.11.2: bytes=32 time=39ms TTL=124

Ping statistics for 120.32.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 39ms, Average = 23ms

C:\>
```

VLAN [Habitaciones_CGOP_P1 | 120.32.27.0] a VLAN [Aulas_CNOR_P1 | 120.32.11.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.11.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

5.2.34 Conectividad VLAN CGOP a VLAN CT

```
Pinging 120.32.19.2 with 32 bytes of data:

Reply from 120.32.19.2: bytes=32 time=71ms TTL=124
Reply from 120.32.19.2: bytes=32 time=12ms TTL=124
Reply from 120.32.19.2: bytes=32 time=28ms TTL=124
Reply from 120.32.19.2: bytes=32 time=23ms TTL=124

Ping statistics for 120.32.19.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 71ms, Average = 33ms

C:\>
```

VLAN [Habitaciones_CGOP_P1_2 | 120.32.28.0] a VLAN [Consultorios_CT_P2 | 120.32.19.0]

En la imagen se muestra la conectivadad exitosa a la dirección IP 120.32.19.2 con una conexión estable y tiempos de respuesta variables pero dentro de un rango aceptable.

Recomendaciones de seguridad

Anexo A

6.1.1 Políticas de acceso para mitigar las vulnerabilidades

Vulnerabilidad	***Politica recomendada***	***Justificacion***
Uso de protocolos inseguros (como Telnet) para acceso remoto	Deshabilitar Telnet y forzar el uso de SSH o VPN para administración remota	Telnet transmite credenciales en texto plano, lo que expone la red a intercepciones y ataques de intermediarios. SSH y VPN cifran la comunicación.
Ausencia de listas de control de acceso (ACLs)	Implementar ACLs extendidas para controlar el acceso entre VLANs	Las ACLs permiten limitar el tráfico entre zonas sensibles, como servidores o cámaras, evitando accesos no autorizados.
Falta de segmentación de tráfico de invitados	Crear VLAN específica para invitados y aplicar ACLs que restrinjan su acceso a la red interna	Los invitados podrían comprometer recursos internos si comparten red con usuarios autorizados. Una VLAN separada reduce este riesgo.
Conexión directa de dispositivos sin autenticación (ej. IoT, cámaras)	Usar VLANs específicas para dispositivos IoT, segmentadas del resto de la red, y aplicar control de puertos con 802.1X si es posible	Los dispositivos IoT suelen tener menos protección, lo que los convierte en vectores de ataque. Segmentar y controlar su conexión reduce el riesgo.
Configuración por defecto en routers y switches	Cambiar credenciales por defecto y deshabilitar servicios innecesarios (CDP, HTTP, etc.)	Los dispositivos con configuraciones por defecto son fácilmente explotables. Minimizar servicios expuestos reduce la superficie de ataque.

Anexo B

6.1.2 Sistemas de control de seguridad

	Preventive	***Detective***	***Corrective***
Physical Controls	-Acceso restringido con tarjetas RFID en áreas críticas (Data Center, salas de servidores) - Cámaras en pasillos clave - Puertas blindadas en cuartos de equipos - Control de acceso biométrico para personal autorizado - Señalización de seguridad en áreas restringidas	- Monitoreo continuo con CCTV y grabación 24/7 - Sensores de movimiento y apertura en puertas críticas - Alarmas de intrusión en salas técnicas - Registro de accesos físicos	- Reparación inmediata de cerraduras o puertas dañadas - Sustitución de cámaras defectuosas - Reemisión de credenciales de acceso - Mantenimiento correctivo de sistemas de control de acceso
Technical Constrols	- Firewalls configurados para segmentar la red por VLAN - Configuración de ACLs extendidas para limitar acceso a datos confidenciales - Actualizaciones periódicas de firmware en switches y routers - Redundancia en enlaces críticos (FHRP)	- Monitoreo en tiempo real de la red con herramientas como SNMP y Syslog - Escaneos de vulnerabilidades periódicos - Alertas automáticas por intentos de acceso no autorizados	- Aplicación de parches de seguridad ante vulnerabilidades detectadas - Reconfiguración de ACLs ante incidentes - Sustitución de hardware comprometido - Restauración de configuración desde backups
Administrative Controls	- Políticas de acceso basadas en roles (RBAC) - Capacitación de personal en ciberseguridad y manejo de información sensible - Procedimientos documentados para la gestión de incidentes - Plan de continuidad operativa y recuperación ante desastres	- Auditorías internas y externas periódicas - Revisión de logs de seguridad y accesos - Evaluaciones de cumplimiento de políticas	- Actualización de políticas de seguridad tras incidentes - Capacitación correctiva al personal que incumpla protocolos - Ajustes en el plan de continuidad operativa

Anexo C

6.1.3 Medidas de recuperación ante desastres naturales, etc

Tipo de daño	***Identificar los riesgos potenciales***	***Recomendar un plan de recuperación ante desastres***
Desastre Natural	- Terremotos o incendios que afecten el Data Center - Cortes de energía prolongados - Daños estructurales en las instalaciones	- Implementar un sitio alterno (DR Site) fuera de la zona de riesgo - Contar con UPS y generadores de respaldo para suministro eléctrico - Respaldar periódicamente datos críticos en almacenamiento externo y en la nube - Realizar simulacros periódicos de evacuación y continuidad de operaciones
Fallas de equipos en el centro de datos	- Avería de servidores, switches, routers o almacenamiento - Sobrecalentamiento por falla del sistema de climatización - Pérdida de conectividad interna	- Mantener inventario de repuestos críticos - Contratar soporte técnico 24/7 con proveedores - Implementar redundancia en hardware clave (servidores, switches, enlaces de red) - Restaurar configuraciones desde copias de seguridad actualizadas
Ataque DDoS o peridida de datos	- Interrupción de servicios en línea por saturación de tráfico - Acceso no autorizado y borrado o robo de información sensible - Corrupción de bases de datos	- Implementar protección anti-DDoS en el firewall y en el ISP - Configurar ACLs y segmentación de red para limitar el impacto - Realizar respaldos automáticos y cifrados de datos críticos - Definir y aplicar un plan de respuesta a incidentes con roles y tiempos claros

Plan de mantenimiento preventivo y correctivo

El mantenimiento de la infraestructura es esencial para garantizar la disponibilidad, seguridad y rendimiento de la red hospitalaria.

Mantenimiento preventivo

- **Revisión mensual** de logs de routers, switches y servidores.
- **Verificación trimestral** de las configuraciones de ACLs y políticas de seguridad.
- **Actualización semestral** de firmware en switches, routers y APs.
- **Pruebas de conectividad** periódicas (ping, traceroute) para validar enlaces troncales y enlaces entre routers.
- **Inspección física** de cableado, ventilación y alimentación (UPS) cada 6 meses.
- **Backups programados** de configuraciones críticas y almacenados fuera del dispositivo.
-

Mantenimiento correctivo

- **Respaldo inmediato** de configuraciones ante fallos.
- **Reemplazo de hardware** dañado en menos de 24h, especialmente switches troncales.
- **Reconfiguración rápida** de dispositivos comprometidos o desconfigurados.
- **Revisión post-incidente** para documentar la causa raíz y actualizar el plan preventivo.
- **Aplicación de parches** o actualizaciones ante descubrimiento de vulnerabilidades.

Referencias

Cisco Systems. (s.f.). *Design methodology: PPDIOO*. Cisco. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Architecture/ENTBPG_3.html

Cisco Networking Academy. (2022). *CCNA: Switching, Routing, and Wireless Essentials (SRWE)*. Cisco Press.

Cisco Networking Academy. (2021). *CCNA: Enterprise Networking, Security, and Automation (ENSA)*. Cisco Press.

Rouse, M. (2018). *Access Control List (ACL)*. TechTarget. https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL

N-able. (s.f.). *Computer security vulnerabilities*. https://www.n-able.com/features/computer-security-vulnerabilities

Palo Alto Networks. (s.f.). *What is Network Segmentation?* https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Protecting Network Infrastructure Devices*. Recuperado de https://www.cisa.gov/news-events/news/protecting-network-infrastructure-devices

Fortinet. (s.f.). *What Is VLAN (Virtual Local Area Network)?* https://www.fortinet.com/resources/cyberglossary/vlan

Cisco Systems. (s.f.). *Redundant network design*. Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-redundancy.html

TechTarget. (2022). *Power over Ethernet (PoE)*. https://www.techtarget.com/searchnetworking/definition/Power-over-Ethernet-PoE

Ubiquiti. (s.f.). *Best Practices for Access Point Placement*. https://help.ui.com/hc/en-us/articles/360012282453-UniFi-Design-Center-Access-Point-Placement

D-Link. (s.f.). *Switches PoE para videovigilancia IP*. https://eu.dlink.com/es/es/soporte/faq/switches/seguridad/que-es-un-switch-poe-y-para-que-se-utiliza

Cisco. (s.f.). *Cisco Catalyst 9200 Series Switches Data Sheet*. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

Cisco. (s.f.). *Cisco CBS220-48P-4G-NA Smart Switch*. https://www.cisco.com/c/en/us/products/switches/business-220-series-smart-switches/index.html

Cisco. (s.f.). *Cisco 2811 Integrated Services Router*. https://www.cisco.com/c/en/us/products/collateral/routers/2800-series-integrated-services-routers/product_data_sheet0900aecd8016fa68.html

Grandstream. (s.f.). *Teléfono IP Grandstream GXP1625*. https://www.grandstream.com/products/ip-voice-telephony/ip-phones/gxp1600-series-small-medium-business-ip-phones/product/gxp1625

Hikvision. (s.f.). *DS-2CD1023G0E-I cámara IP de videovigilancia*. https://www.hikvision.com/es-la/products/IP-Products/Network-Cameras/EasyIP-2.0-plus/ds-2cd1023g0e-i/

TP-Link. (s.f.). *Omada EAP245 Access Point WiFi AC1750*. https://www.tp-link.com/mx/business-networking/omada-sdn-access-point/eap245/

Amazon México. (2025). *Cotización de dispositivos de red para hospital*. https://www.amazon.com.mx

Anexos

7.1.1 Cronograma de actividades

Fase PPDIOO	*Actividad*	*Responsable*	*Fecha de inicio*	*Fecha de fin*
Preparar	1.1 Recorrido virtual o físico por el hospital	Diego, Diana, Paola	09/06/2025	10/06/2025
	1.2 Identificación de departamentos clave(Urgencias, Consultorios,		10/06/2025	11/06/2025
	1.3 Detección de necesidades tecnológicas en cada área.		11/06/2025	12/06/2025
	1.4 Registro de dispositivos y servicios requeridos por area		12/06/2025	12/06/2025
	1.-5 Documentacion	Diego	13/06/2025	14/06/2025
Planear	2.1 Investigación de precios de los dispositivos	Paola	16/06/2025	18/06/2025
	2.2 Definición de políticas de red	Diego	19/06/2025	20/06/2025
	2.3 Segmentación de red por subredes VLSM	Diego	21/06/2025	22/06/2025
	2.4 Diseño lógico de la red	Diego	23/06/2025	24/06/2025
	2.5 Documentacion	Diego	25/06/2025	26/06/2025
Designar	3.1 Elaboración del diagrama físico (ubicación de equipos en plano)	Diana, Paola	30/06/2025	01/07/2025
	3.2 Creación del diagrama lógico (conexiones y topología)	Diego	02/07/2025	03/07/2025
	3.3 Definición y asignación de VLANs por área o función	Diego	04/07/2025	05/07/2025
	3.4 Diseño y configuración de listas de control de acceso (ACLs) para control de tráfico	Diego	06/07/2025	08/07/2025
	3.5 Construcción de la tabla IP con direcciones asignadas por subred/VLAN	Diego	09/07/2025	10/07/2025
	3.6 Documentacion	Diego	11/07/2025	12/07/2025
Implementar	4.1 Creación del entorno de red en Cisco Packet Tracer.	Diego	14/07/2025	16/07/2025
	4.2 Configuración de dispositivos de red		17/07/2025	18/07/2025

	(switches, routers, PCs, servidores)			
	4.3 Asignación de direcciones IP y VLANs en los dispositivos		18/07/2025	19/07/2025
	4.4 Implementación de ACLs y pruebas de filtrado de tráfico		19/07/2025	20/07/2025
	4.5 Pruebas de conectividad (ping, traceroute)		21/07/2025	22/07/2025
	4.6 Verificación de servicios como DHCP, DNS, NAT, HTTP/HTTPS, etc		23/07/2025	24/07/2025
	4.7 Documentacion		24/07/2025	26/07/2025
Funcionar	5.1 Validación del funcionamiento de todos los servicios de red	Diego	28/07/2025	28/07/2025
	5.2 Pruebas de conectividad entre áreas/VLANs		28/07/2025	28/07/2025
	5.3 Revisión de accesos permitidos y denegados por ACLs		29/07/2025	29/07/2025
	5.4 Monitoreo básico del tráfico en Packet Tracer		28/07/2025	28/07/2025
	5.5 Detección de posibles errores o mejoras en el diseño/configuración		30/07/2025	30/07/2025
	5.6 Documentacion		31/07/2025	01/08/2025
Optimizar	6.1.-Redacción del informe final del proyecto	Diego	09/06/2025	07/08/2025
	6.2.-Inclusión de capturas de pantalla de Packet Tracer, diagramas, tablas y configuraciones			
	6.3.-Justificación de decisiones técnicas tomadas			
	6.4.-Conclusiones generales del proyecto (retos, soluciones, aprendizajes)			
	6.5.-Organización de anexos técnicos (cotizaciones, planos, scripts, etc)			

Glosario de términos

1. **PPDIOO** (*Prepare, Plan, Design, Implement, Operate, Optimize*): Metodología de Cisco para el ciclo de vida de redes, que abarca desde la preparación hasta la optimización del sistema.
2. **VLAN** (*Virtual Local Area Network*): Red lógica que segmenta un switch en múltiples redes independientes, mejorando seguridad y eficiencia.
3. **ACL** (*Access Control List*): Lista de control de acceso que define reglas para permitir o denegar tráfico en una red según direcciones IP, puertos o protocolos.
4. **NAT** (*Network Address Translation*): Traducción de direcciones IP privadas a públicas para permitir comunicación con redes externas como Internet.
5. **PAT** (*Port Address Translation*): Variante de NAT que usa diferentes puertos para que múltiples dispositivos compartan una sola dirección IP pública.
6. **PoE** (*Power over Ethernet*): Tecnología que permite suministrar energía eléctrica y datos a través de un mismo cable de red.
7. **EtherChannel**: Técnica para agrupar varios enlaces físicos entre switches o routers y combinarlos como un solo enlace lógico para aumentar capacidad y redundancia.
8. **FHRP** (*First Hop Redundancy Protocol*): Protocolos como HSRP o VRRP que garantizan continuidad del servicio de gateway en caso de falla de un router.
9. **Servidor NTP** (*Network Time Protocol*): Servidor que sincroniza la hora de todos los dispositivos de red.
10. **Router**: Dispositivo que interconecta redes diferentes y dirige el tráfico de datos según su destino.
11. **Switch**: Dispositivo que conecta múltiples dispositivos en una red local y envía datos solo al destinatario correspondiente.
12. **Access Point (AP)**: Punto de acceso inalámbrico que conecta dispositivos Wi-Fi a la red cableada.
13. **Topología Lógica**: Representación de cómo fluye la información en una red, independiente de la disposición física de los equipos.
14. **Subred / VLSM** (*Variable Length Subnet Masking*): Técnica para dividir una red en subredes de distintos tamaños según las necesidades de cada segmento.
15. **IoT** (*Internet of Things*): Conjunto de dispositivos conectados a Internet que pueden recopilar y compartir datos.
16. **Ataque DDoS** (*Distributed Denial of Service*): Ataque que busca saturar un servicio o red con tráfico excesivo proveniente de múltiples fuentes.

Caracteristicas de dispositivos

Router Cisco con firewall integrado de la serie 100, con **8 puertos RJ-45 y 4 puertos SFP**

Router Cisco de la serie 100 que conecta redes, protege con firewall integrado y permite conexiones rápidas con 8 puertos RJ-45 para cableado Ethernet y 4 puertos SFP para enlaces de fibra óptica. Ideal para pequeñas empresas.

7.1.2 Tabla de características | Router

Característica	Evaluación
Firewall Integrado	Excelente para controlar tráfico entre VLANs, oficinas o sitios remotos.
8 puertos RJ-45 LAN	Ideal para conexiones directas a switches, servidores o PC clave.
4 puertos SFP	Te permite conexiones **de fibra óptica** hacia otros edificios o switches troncales.
Administrable y seguro	Soporta ACLs, VPN, NAT/PAT, QoS, etc. Perfecto para entornos hospitalarios.
Serie ISR 1000 (posiblemente 1100)	Soporta IOS XE (versión moderna), más rendimiento que routers pequeños.

7.1.3 Tabla de Ventajas | Router

Ventaja	Explicación
Mayor seguridad	Tiene un **firewall empresarial integrado**, no necesitas un equipo externo para proteger tu red.
Mejor rendimiento	Esta serie soporta más throughput que los routers básicos. Puede manejar tráfico más intenso y muchas VLANs.
Soporte de VPN	Puedes configurar **VPNs site-to-site o cliente-servidor** si el hospital requiere conexiones externas seguras.
Escalabilidad	Al tener puertos SFP puedes hacer **uplinks de fibra** entre switches de distribución o hacia otros edificios.

Medidas de Cisco 8x rj-45, 4x sfp

- Altura: 1U – 4.445cm
- Profundidad: 33.2cm
- Ancho: Estandar 19
- Peso: 4.2kg – 4.3kg

Switch Cisco CBS220-48P-4G-NA - Gigabit Ethernet - 48 Puertos PoE - 4 Puertos SFP

Switch Cisco de 48 puertos PoE para conectar y alimentar dispositivos, con 4 puertos SFP para enlaces de fibra.

7.1.4 Tabla de Caracteristicas | Switch

Característica	Detalle
Puertos PoE+ (Power over Ethernet)	Perfecto para alimentar cámaras IP, Access Points, teléfonos IP sin adaptadores externos.
PoE Budget	Hasta 370W de potencia total PoE disponible (repartida entre los 48 puertos).
4 Puertos uplink SFP (1G)	Para conexión de fibra óptica a otros switches o al router.
Administrable (L2+)	Soporta VLANs, QoS, Link Aggregation, Spanning Tree, SNMP, ACLs.
Interfaz Web amigable	Muy fácil de configurar si aún estás aprendiendo, pero con opciones avanzadas.
Seguridad	Compatible con 802.1X, ACLs, DHCP snooping, etc.

Medidas de Cisco CBS220-48P-4G-NA

- Altura: 1U
- Profundidad: 32.8cm
- Ancho: Estandar 19
- Peso: 5.1kg

Access Points Ubiquiti U6-Lite

Access Point permite conectar dispositivos inalámbricos a la red WiFi con alta velocidad y cobertura. Ideal para oficinas y negocios.

Razón de elección:

- Buena relación costo/rendimiento.
- Soporte Wi-Fi 6, ideal para entornos de alta densidad como hospitales.
- Compatibles con el controlador Ubiquiti Cloud Key G2+.

Características técnicas:

- Wi-Fi 6 (802.11ax), doble banda (2.4GHz y 5GHz).
- Hasta 300 usuarios simultáneos por unidad.
- Montaje en techo o pared.

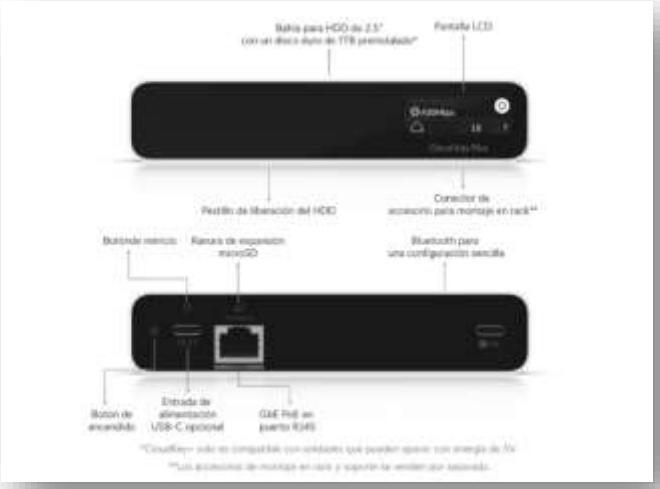
Funciones clave:

- Brinda conectividad inalámbrica estable y rápida.
- Múltiples SSID para segmentar usuarios (médicos, pacientes, administrativos).

Utilidad en hospital:

- Asegura cobertura Wi-Fi en salas de espera, consultorios y áreas comunes.
- Soporta gran cantidad de dispositivos conectados sin saturación.

Controladores Wi-Fi – Ubiquiti Cloud Key G2+



Controlador Ubiquiti Cloud Key G2+ gestiona y monitorea redes Wi-Fi Ubiquiti desde la nube, con almacenamiento local para grabaciones. Ideal para redes empresariales.

Razón de elección:

- Permiten administrar múltiples APs desde una única interfaz por edificio.
- Incluyen almacenamiento interno para registros y monitoreo.
- Ideal tener **uno por edificio** para no depender de un solo punto de control.

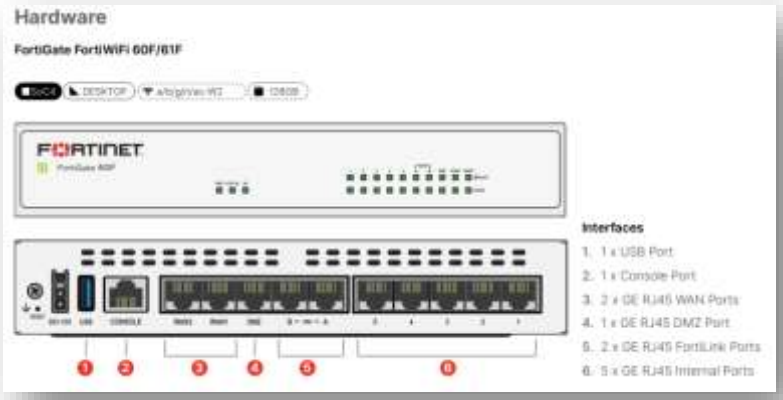
Funciones clave:

- Centraliza la configuración y monitoreo de la red inalámbrica.
- Genera estadísticas, alertas y reportes en tiempo real.

Utilidad en hospital:

- Permite mantener estable la red Wi-Fi del hospital incluso con muchas zonas.
- Gestiona accesos y ancho de banda por perfil.

Firewall Fortigate 60F



Firewall FortiGate 60F protege la red contra amenazas con seguridad avanzada, VPN y control de tráfico. Ideal para pequeñas y medianas empresas.

Razón de elección:

- Control total del tráfico saliente y entrante desde la red principal.
- Permite configurar reglas, segmentación y VPNs de forma segura.
- Será instalado en el cuarto de comunicaciones principal, en conjunto con los servidores.

PCs HP ProDesk 400 G7

PC HP ProDesk 400 G7 computadora de escritorio confiable y potente para oficinas, ideal para tareas administrativas y de productividad diaria.

Razón de elección:

- Estaciones confiables para áreas administrativas, laboratorios y personal médico.
- Distribuidas en:
    - Consultorios
    - Administración
    - Recepciones
    - Centros de diagnóstico

Cámaras Hikvision DS-2CD2046G2-I

Cámara Hikvision DS-2CD2046G2-I: cámara de seguridad IP con alta resolución y visión nocturna, ideal para vigilancia en interiores o exteriores.

Características técnicas:

- Resolucion 4MP (2560x1440)
- Tecnologia AcuSense
- Soporte ONVIF y RTSP (Compatible con la mayoría de softwares de videovigilancia para el servidor Dell PowerEdge R250)
- PoE (Power over Ethernet)
- Resistencia IP67
- Almacenamiento en servidor/NVR o microSD

Servidores Dell PowerEdge T40

Servidor Dell PowerEdge T40 servidor básico y confiable para pequeñas empresas, ideal para centralizar archivos, aplicaciones y respaldo de datos.

Razón de elección:

- Soporta servicios múltiples como DHCP, VMS (para cámaras), DNS, o backup.
- Tiene buena capacidad de almacenamiento y procesamiento.
- Es fiable, escalable y con soporte de Dell, una marca reconocida en servidores.
- Su tamaño 1U permite alojarlo cómodamente en un gabinete de red.

7.1.5 Tabla de Caracteristicas | Servidor

Característica	Detalle
Factor de forma	Rack 1U (ocupa 1 unidad en gabinete)
Procesador	Intel Xeon E-2300 series (hasta 8 núcleos)
Memoria RAM	Hasta 128 GB DDR4 ECC UDIMM
Almacenamiento	Hasta 2 discos SATA/SAS de 3.5" o 4 discos de 2.5" (RAID opcional)
Red	2 puertos Ethernet integrados 1GbE
Alimentación	Fuente redundante (opcional) de 350W/600W
Puertos	USB 3.0, VGA, iDRAC9 (gestión remota)
Administración	iDRAC9 Enterprise (acceso remoto, monitoreo, actualizaciones)

Funciones clave:

- Almacena y procesa datos clínicos, registros médicos, sistema de hospital.
- Permite crear máquinas virtuales para separar servicios (por ejemplo, DHCP, DNS, backup, almacenamiento de video cámara).

UPS APC SMT1500C

UPS APC SMT1500C respaldo de energía que protege equipos ante cortes de luz y picos de voltaje, ideal para servidores y equipos críticos.

Razón de elección:

- Proteger dispositivos clave (switches, routers, servidores) ante cortes eléctricos.
- 4 unidades para cubrir gabinetes críticos por edificio.

Utilidad en hospital:

- Mantiene servidores y equipos críticos encendidos ante cortes.
- Evita fallas en bases de datos médicas o sistema de cámaras.

Gabinetes de red Tripp Lite SR18UB SmartRack

Gabinete de red Tripp Lite SR18UB SmartRack estructura para organizar y proteger equipos de red en un solo lugar, facilitando su instalación y mantenimiento.

Razón de elección:

- Este gabinete es ideal para centros de datos pequeños o medianos, como los cuartos de comunicaciones en hospitales.
- Ofrece suficiente espacio (18U) para alojar dispositivos clave como servidores, switches, routers, UPS, e incluso dejar espacio adicional para crecimiento.
- Es cerrado, seguro y ventilado, perfecto para ambientes donde la protección física y la organización de los equipos es esencial.
- Compatible con estándares de 19 pulgadas, lo que lo hace apto para prácticamente cualquier equipo de red o servidor rackeable, incluido el Dell PowerEdge R250.

Características Técnicas

- **Altura útil:** 18U (espacios para equipos de 1U a 4U)
- **Dimensiones externas (alto x ancho x profundidad):**
  94.0 cm x 60.0 cm x 83.8 cm (37 x 23.63 x 33 pulgadas aproximadamente)
- **Peso máximo soportado:** 454 kg (1000 lb) con instalación fija
- **Compatibilidad:** Estándar EIA-310-E para racks de 19"

- **Construcción:** Acero robusto, con puertas delantera y trasera ventiladas (optimiza flujo de aire)
- **Accesibilidad:** Paneles laterales removibles y puertas con cerradura (seguridad y fácil mantenimiento)
- **Gestión de cables:** Pasa-cables superior e inferior, soporte interno para organización

Funciones Claves

- **Aloja de forma segura equipos críticos:** como el servidor Dell PowerEdge R250 (1U), un router Cisco de 1U, y el switch Cisco CBS220-48P-4G-NA (1U), quedando aún 15U libres para UPS, bandejas, organizadores o crecimiento futuro.
- **Facilita ventilación adecuada:** gracias a su estructura con ventilación frontal y trasera, lo que previene el sobrecalentamiento del servidor y los switches PoE.
- **Soporta un UPS interno:** puedes agregar una unidad UPS de respaldo para mantener operativa la red hospitalaria en caso de corte de energía.

Cableado Cat6

Cableado Cat6 cable de red que permite conexiones rápidas y estables, ideal para transmitir datos a alta velocidad en redes modernas.

Razón de elección:

- Es el estándar actual para redes Gigabit Ethernet, ideal para hospitales que requieren alta velocidad y confiabilidad en conexiones LAN.
- Excelente para conectar PCs, switches, cámaras PoE + loT, Puntos de acceso WiFi, Wirreless Controller.
- Las canaletas permiten una instalación limpia, segura y protegida del cableado estructurado, especialmente en pasillos y oficinas médicas.

Características Técnicas

- **Categoría:** Cat6 UTP (Unshielded Twisted Pair)
- **Velocidad soportada:** Hasta 1 Gbps (Gigabit Ethernet)
- **Frecuencia:** Hasta 250 MHz
- **Longitud por bobina:** 305 metros
- **Compatibilidad:** Con conectores RJ-45 Cat6 y Cat6A

Funciones Clave

- Distribuye red a todos los nodos **en oficinas, salas médicas, etc.**
- **La canaleta facilita el** orden, mantenimiento y seguridad física del cableado**.**

Cable de Fibra Óptica Monomodo OS2

Cable de Fibra Óptica Monomodo OS2 transmite datos a largas distancias con alta velocidad y baja pérdida, ideal para conexiones de red críticas.

Razón de elección

- Ideal para interconexión entre edificios o racks distantes dentro del hospital, garantizando transmisión a alta velocidad y sin interferencia electromagnética.
- OS2 es la opción estándar para enlaces de larga distancia, hasta 10 km o más con módulos adecuados.

Características Técnicas

- Tipo: Monomodo (Singlemode)
- Estándar: OS2
- Diámetro del núcleo: 9/125 μm
- Cubierta: LSZH (baja emisión de humo y cero halógenos, segura para ambientes hospitalarios)

Funciones clave

- Une edificios del hospital con conexiones de alta velocidad y sin pérdidas.
- Evita interferencias, ideal cerca de equipos médicos o zonas con alta electromagnética.
- Requiere menos mantenimiento y soporta futuras actualizaciones de velocidad (10G, 40G, etc.).

Módulo SFP GLC-LH-SMD (Compatible con Cisco)

Módulo SFP GLC-LH-SMD adapta puertos para conectar fibra óptica a larga distancia en equipos Cisco, facilitando enlaces rápidos y estables.

Razón de elección

- Adaptador de red óptica, indispensable para conectar switches o routers a la fibra OS2.
- Totalmente compatible con switches Cisco como los CBS220 o Catalyst.
- Soporta Gigabit Ethernet sobre fibra monomodo, ideal para enlaces troncales en hospitales.

Características técnicas

- **Modelo:** GLC-LH-SMD (Cisco compatible)
- **Tipo de conexión:** LC dúplex
- **Tipo de fibra:** Monomodo
- **Distancia soportada:** Hasta 10 km (OS2)
- **Velocidad:** 1 Gbps
- **Formato:** Hot-swappable (se pueden instalar en caliente)

Funciones Clave

- Permite usar fibra óptica con Routers y Switches compatibles
- Ideal para crear **backbones entre edificios o pisos distantes**
- Evita tener que usar cobre en distancias largas o donde hay interferencia

Conector LC-LC UPC Duplex Monomodo (OP-ACLCUD)

Conector LC-LC UPC Duplex Monomodo: conecta cables de fibra óptica monomodo con alta precisión para enlaces de datos estables y eficientes.

Razón de elección

- Esencial para interconectar tramos de fibra óptica monomodo, o conectar módulos SFP a paneles de parcheo.
- Estilo duplex para transmitir y recibir simultáneamente.
- Tipo UPC (Ultra Physical Contact) que ofrece menor pérdida de señal.

Características Técnicas

- Tipo de conector: LC-LC dúplex
- Pulido: UPC (Ultra Physical Contact)
- Modo de fibra: Monomodo OS2

Funciones clave

- Conecta equipos activos (SFPs) con paneles o enlaces de fibra.
- Ideal para mantener baja atenuación en enlaces ópticos del hospital.
- Fácil instalación y reemplazo sin herramientas especializadas.

Conector RJ-45 Panduit CJ6X88TGIW-Cat6A

Conector RJ-45 Panduit CJ6X88TGIW-Cat6A conecta cables Cat6A para redes Ethernet de alta velocidad, asegurando una conexión estable y eficiente.

Razón de elección

- Es uno de los mejores conectores modulares keystone del mercado.
- Alta calidad, compatibilidad garantizada con Cat6A y hacia abajo (Cat6, Cat5e).
- Utilizado en hospitales, oficinas gubernamentales y data centers por su construcción robusta y precisión.

Características técnicas

- Modelo: CJ6X88TGIW
- Categoría: Cat6A
- Tipo: Keystone Jack

Funciones clave

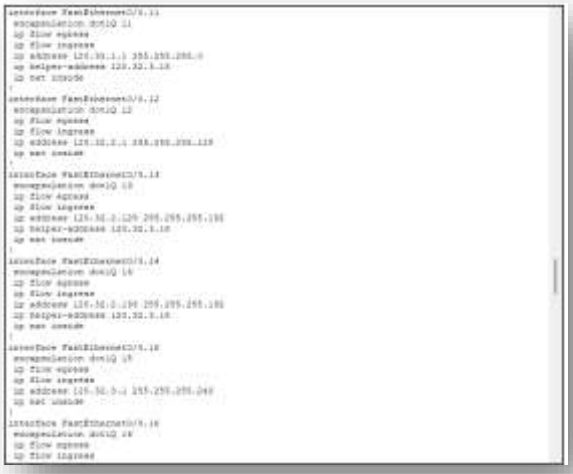
- Finaliza el cableado estructurado en salidas de pared o patch panels
- Garantiza conexión estable y libre de ruido para datos críticos.
- Soporta hasta 10 Gbps, lo que lo hace ideal para futuras expansiones.

Configuracion de dispositivos

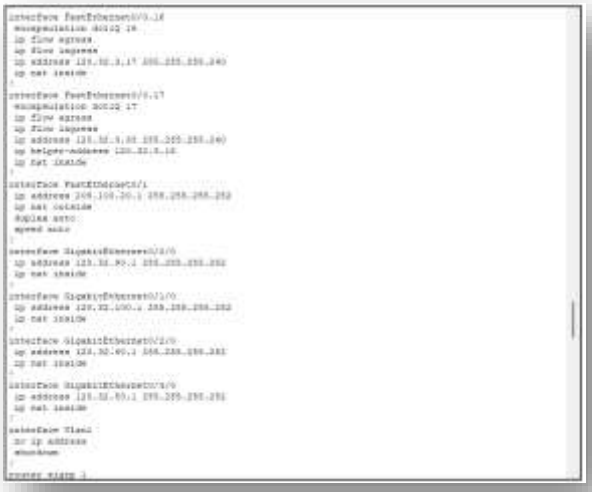
Torre Central | TC_R_NP

La imagen muestra la configuración del router ubicado en el Nivel Plaza de la Torre Central (TC_R_NP). Se puede observar que hay un dhcp pool (TC_VOZ_NP) con la red 120.32.2.0.

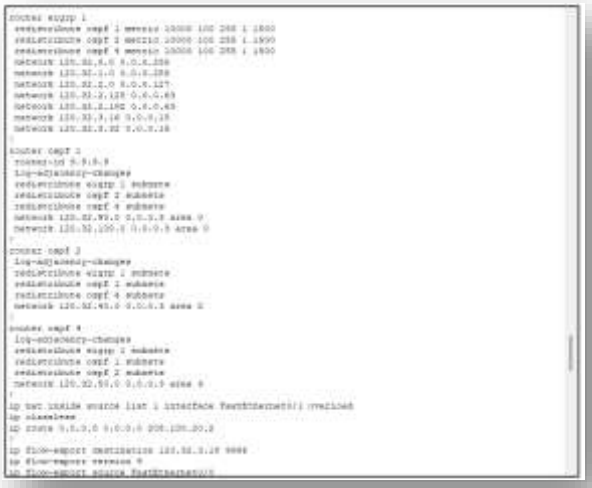
La imagen muestra el username y password ftp (AdminTC), ssh version, el domain-name (abc.com) tambien la interfaz 0/0 con la ip add 120.32.3.50 /30, ip flow egress/ingress y el duplex y speed, se observa la interfaz 0/0.10 con la ip 120.32.0.1/24 que cuenta con ip flow egress/ingress, ip helper-address e ip nat inside.



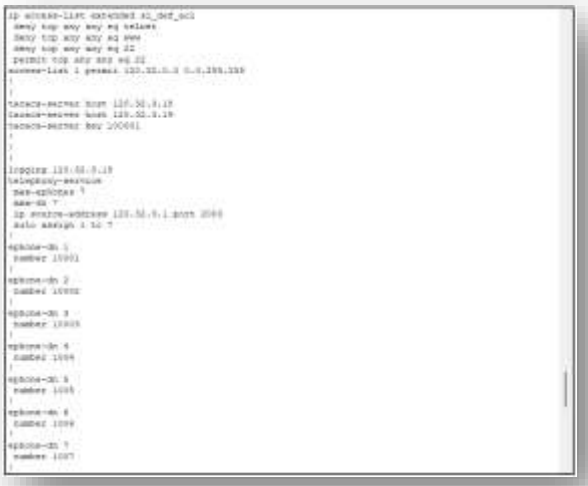
En esta imagen se pueden observar las configuraciones de algunas subinterfaces, Interface FastEthernet 0/0.11, 0.12, 0.13, 0.14, 0.15, 0.16, se puede observar las encapsulaciones con (encapsulation dot1q 11), ip flow egress-ingress, su direccion ip, el ip helper-address 120.32.3.18 para asignar su ip y el ip nat inside en cada subinterfaz.



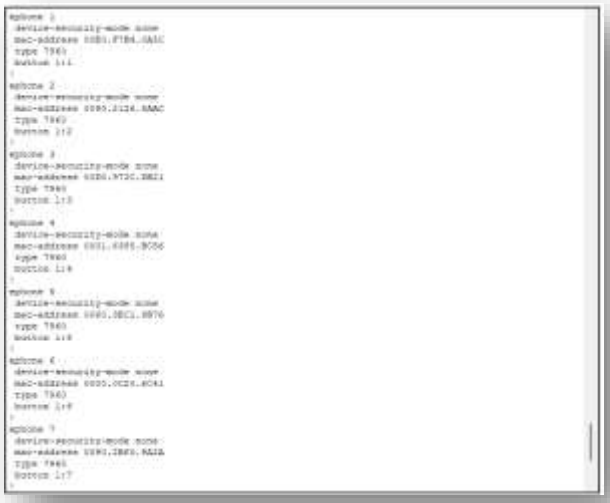
En esta imagen se puede observar algunas interfaces con las siguientes caracteristicas se puede observar las encapsulaciones con (encapsulation dot1q 11), ip flow egress-ingress, su direccion ip, el ip helper-address 120.32.3.18 para asignar su ip y el ip nat inside en cada subinterfaz, tambien se muestra la configuracion de los Gibabits s e pueden observar las ip's de cada interfaz.



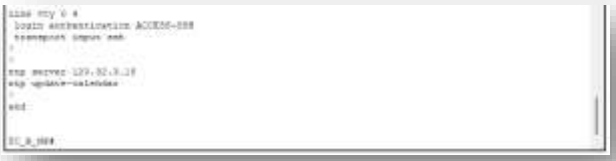
En esta imagen se muestra la configuracion de eigrp 1 se puede observar todas las redes, y el (redistribute ospf 1-2-4 metric 10000 100 255 1 1500) que sirve para redistribuir cada red a ospf, tambien se muestra el ip nat inside que sirve para traducir las direcciones.



*En esta imagen se observa una l*ista de control de acceso (ACL) extendida en un dispositivo de red, se observa la direcion del servidor tacas, tambein se muestra telephony-services se pueden observar 7 telefonos.



En esta imagen se puede observar las configuraciones de los teléfonos IP número 1, desactiva su seguridad, le asigna una dirección MAC, especifica su modelo (Cisco 7960) y configura su botón principal para la línea telefónica. Esto es típico de la configuración de sistemas de telefonía IP en un entorno de red.

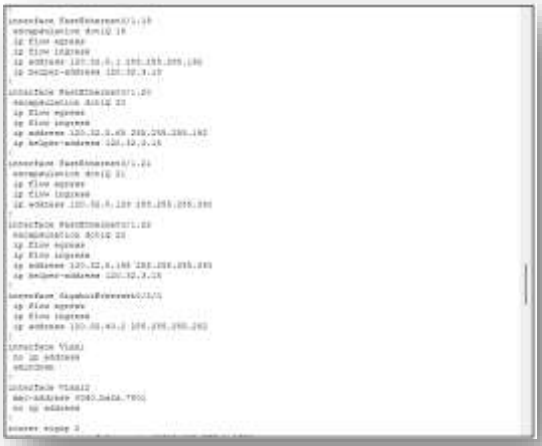


En esta imagen se puede la configuración mostrada establece un acceso remoto seguro al dispositivo a través de SSH y lo sincroniza con un servidor de tiempo para mantener la hora exacta.

Torre Central | TC_R_PB

La imagen muestra la configuración del router ubicado en la Planta baja de la Torre Central (TC_R_NP). Se puede observar que hay un dhcp pool (TC_VOZ_NP) con la red 120.32.5.128/28

La imagen muestra el username y password ftp (AdminTC), ssh version, el domain-name (abc.com) , tambien la interfaz 0/0, la interfaz 0/1 y la interfaz 0/01.18 con la ip add 120.32.4.1 /24, que cuenta con ip flow egress/ingress, e ip helper-address.



En esta imagen se pueden observar las configuraciones de algunas subinterfaces, Interface FastEthernet 0/1.19, 1.20, 1.21, 1.22, int g0/2/0, se puede observar las encapsulaciones con (encapsulation dot1q 21), ip flow egress-ingress, su direccion ip, el ip helper-address 120.32.3.18 para asignar su ip y el ip nat inside en cada subinterfaz.

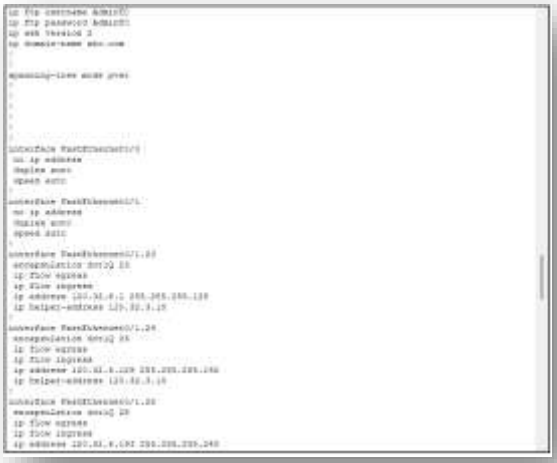
En esta imagen se muestra la configuracion de eigrp 2 se puede observar todas las redes, y el (redistribute ospf 2 metric 100 00 100 255 1 1500) que sirve para redistribuir cada red a ospf, tambien ospf 2 con su router-id, sus redes en el area 2, tambien se muestra una lista de access-list, la direccion de el servidor tacas y el servicio de telefonia.

En esta imagen se puede observar las configuraciones de los teléfonos IP número 1, desactiva su seguridad, le asigna una dirección MAC, especifica su modelo (Cisco 7960) y configura su botón principal para la línea telefónica. Esto es típico de la configuración de sistemas de telefonía IP en un entorno de red.

En esta imagen se puede observar las configuraciones de los teléfonos IP número 1, desactiva su seguridad, le asigna una dirección MAC, especifica su modelo (Cisco 7960) y configura su botón principal para la línea telefónica. Esto es típico de la configuración de sistemas de telefonía IP en un entorno de red.

Torre Central | TC_R_P1

La imagen muestra la configuración de un dispositivo de red que establece políticas de seguridad, crea un servidor DHCP para asignar direcciones IP a los teléfonos IP, configura un usuario de acceso local y define una autenticación combinada con un servidor TACACS+ y una base de datos local.



La imagen muestra la configuración de un dispositivo de red que establece el nombre de dominio, configura SSHv1, habilita el protocolo Spanning Tree, y asigna direcciones IP a varias sub-interfaces VLAN, incluyendo la configuración para reenviar solicitudes de DHCP a un servidor.

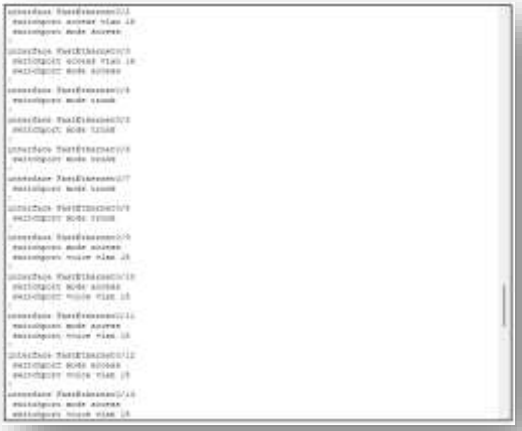
La imagen muestra una configuración de red que establece enrutamiento OSPF (router ospf 3 y router ospf 4), reenvía solicitudes DHCP (ip helper-address), configura el monitoreo de flujo de tráfico (ip flow-export) y, finalmente, usa una lista de acceso (access-list) para denegar el tráfico de Telnet y otros servicios a ciertas interfaces, permitiendo todo lo demás.

La imagen muestra la configuración establece la conexión con un servidor TACACS+ para la seguridad, define los parámetros de un sistema telefónico (cantidad de teléfonos, líneas, etc.) y configura los teléfonos IP (ephones) individualmente, asignándoles una dirección MAC, un modelo y un número de línea.

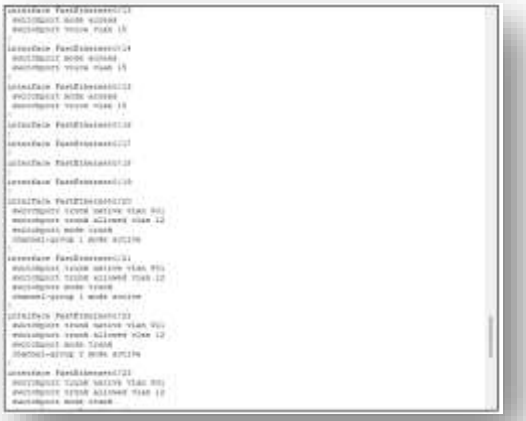
La imagen muestra una configuración de un dispositivo de red que establece parámetros para cuatro teléfonos IP (ephones), asignándoles direcciones MAC y números de línea. Además, configura el acceso remoto seguro a través de SSH, una contraseña para la consola (line con 0) y la sincronización de la hora con un servidor NTP.

Torre Central | TC_SW_NP

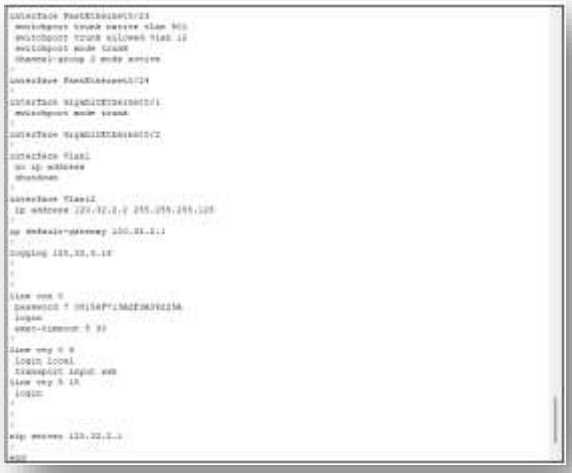
La imagen muestra la configuración de un switch que establece el nombre del dispositivo, encripta contraseñas y configura SSHv2 para un acceso seguro. Además, habilita el protocolo Spanning Tree (PVST) y configura múltiples interfaces como puertos trunk (tanto físicos como EtherChannels), permitiendo el paso de las VLANs 1 y 2, y definiendo la VLAN 991 como nativa.



La imagen muestra la configuración de un switch que separa sus puertos en diferentes tipos:. Puertos de tronco (FastEthernet0/4 al /8) que permiten el paso de múltiples VLANs, típicamente para conectar a otros switches. Puertos de acceso (FastEthernet0/9 al /13) asignados a la VLAN 15.



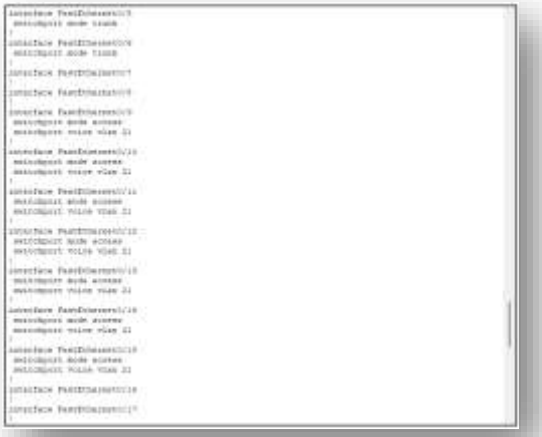
La imagen muestra la configuración de un switch que establece puertos para datos y voz en distintas VLANs, como la VLAN 20 para datos y la 25 para voz. Además, agrupa varias interfaces en dos EtherChannels (channel-group 1 y channel-group 2) para crear enlaces troncales que permiten el paso de la VLAN 12, con la VLAN 99 como nativa.



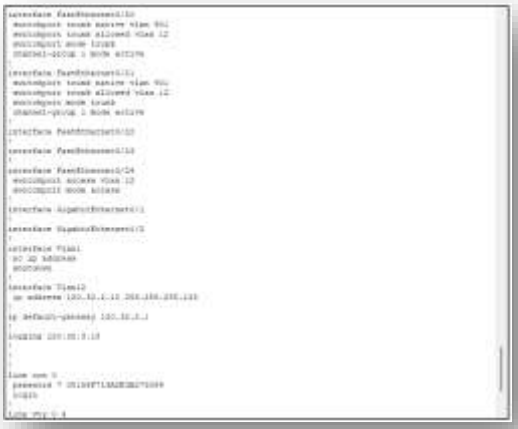
La imagen muestra la configuración de un switch que establece una interfaz troncal (FastEthernet0/23) para formar parte de un EtherChannel y permitir el paso de la VLAN 12. Define una interfaz virtual VLAN 12 con una dirección IP y su puerta de enlace. Establece la seguridad para el acceso remoto, permitiendo solo SSH y configurando una contraseña encriptada para la consola. Finalmente, sincroniza el reloj del dispositivo con un servidor NTP (120.32.2.1).

Torre Central | TC_SW_PB

La imagen muestra la configuración de un switch que encripta contraseñas, habilita SSHv2, define un usuario administrador y un dominio. También configura el protocolo Spanning Tree (PVST) y establece interfaces como puertos troncales, permitiendo el paso de las VLANs 1, 10 y 20. Se configura el acceso remoto al dispositivo a través de SSH y sincroniza el reloj del sistema con un servidor NTP para mantener la hora exacta. Finalmente, la tercera imagen configura un teléfono IP (ephone) de modelo 7960, le asigna una dirección MAC y asocia el botón 1 con la línea 1.

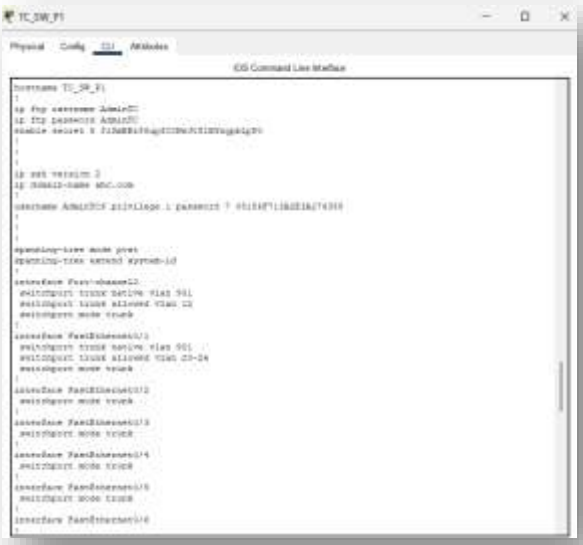


La imágenen muestran la configuración de teléfonos IP, un servidor DHCP para asignarles direcciones, un router con seguridad de acceso y sincronización de hora, y un switch configurado con puertos troncales y de acceso para diferentes VLANs de datos y voz.

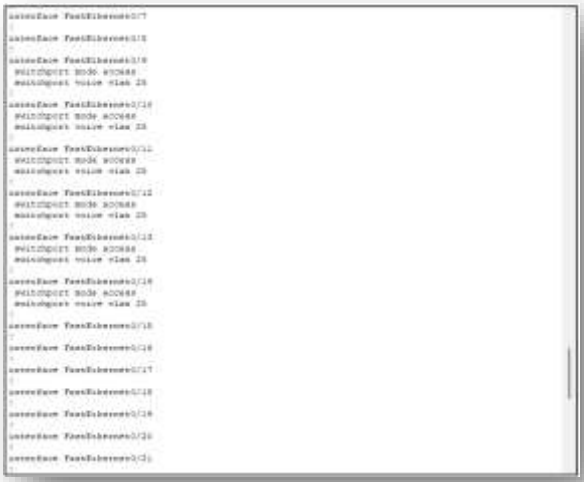


La imágen muestra la configuración de una red que incluye telefonía IP, con servidor DHCP para su aprovisionamiento, y la gestión de la seguridad de acceso remoto mediante SSH y AAA. Además, se configuran switches con VLANs para separar el tráfico y se establecen servicios de red como NTP y enrutamiento OSPF.

Torre Central | TC_SW_P1



La imágen muestra la configuración de un sistema de red que integra telefonía IP, un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



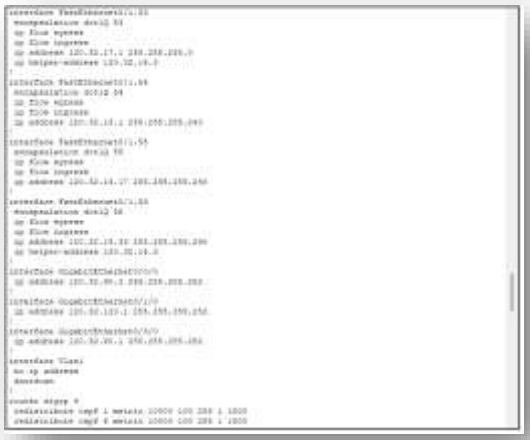
La imágen muestra la configuración de un sistema de red que integra telefonía IP, un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

La imágen muestra una serie de configuraciones de red que, en conjunto, establecen un sistema completo. Se configuran teléfonos IP con sus extensiones, se crea un servidor DHCP para asignarles servicios, y se establece un sistema de seguridad de acceso remoto con SSH y AAA. Además, se configuran switches con VLANs para separar el tráfico y se implementan servicios de red como NTP y enrutamiento OSPF.

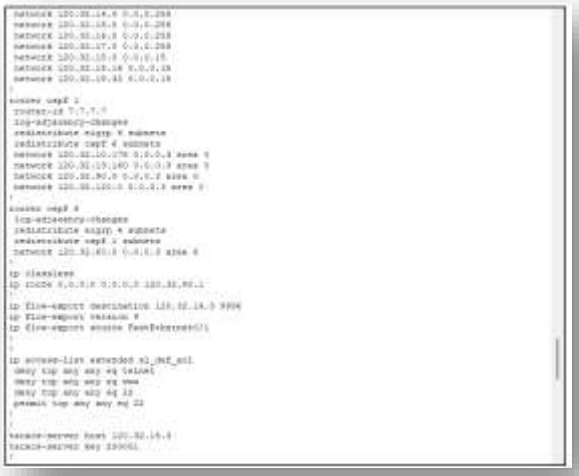
Torre de Consultorios | CT_R_P1

La imágen muestra la configuración de un sistema de red que integra telefonía IP (con ephones y servidor DHCP), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

La imágen muestra la configuración de un sistema de red que integra telefonía IP, con servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

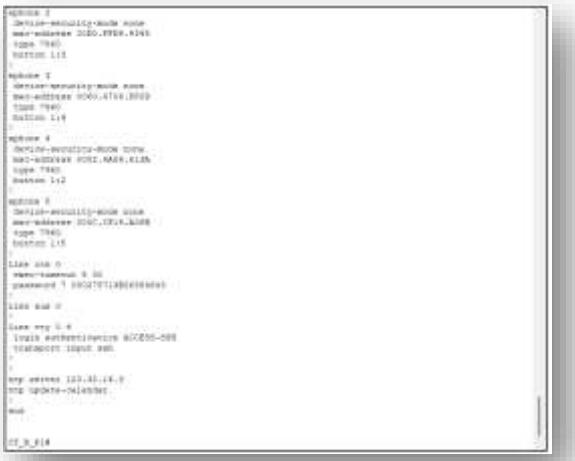


La imagen muestra la configuración de un sistema de red integral que incluye telefonía IP con el uso de teléfonos ephones, un servidor DHCP para su aprovisionamiento automático y seguridad de acceso remoto mediante SSH y autenticación AAA. Además, se configuran switches con VLANs para la segmentación del tráfico de voz y datos, puertos troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra la configuración de un sistema de red integral que incluye telefonía IP (con ephones y servidor DHCP para su aprovisionamiento), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

La imágen muestra la configuración de un sistema de red integral que incluye telefonía IP con el uso de teléfonos ephones y servidor DHCP para su aprovisionamiento, y la seguridad de acceso remoto mediante SSH y autenticación AAA. Además, se configuran switches con VLANs para la segmentación del tráfico de voz y datos, puertos troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

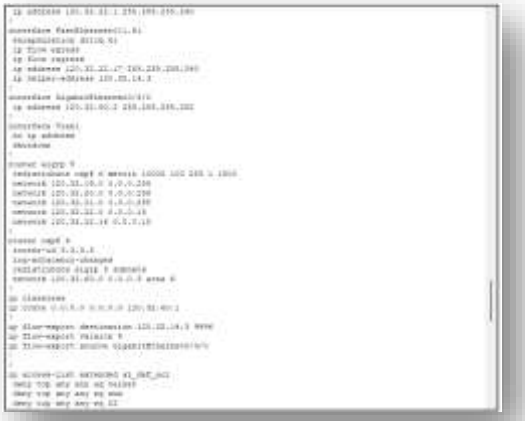


La imágen muestra la configuración de un sistema de red integral que incluye telefonía IP (con ephones y servidor DHCP para su aprovisionamiento), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

Torre de Consultorios | CT_R_P2

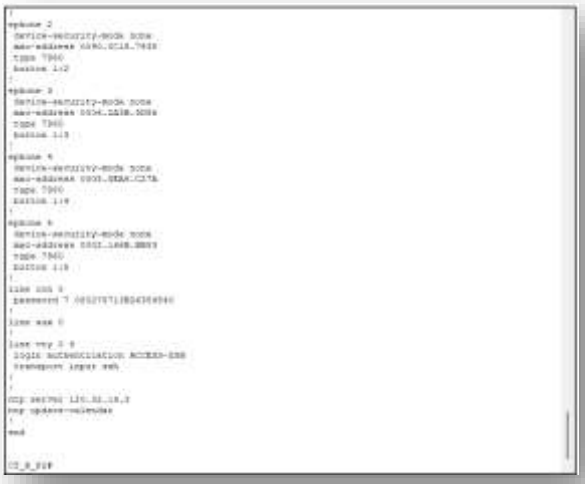
La imágen muestra la configuración de una red que integra telefonía IP (con ephones y servidor DHCP para su aprovisionamiento), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. Se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.

La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra la configuración de una red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

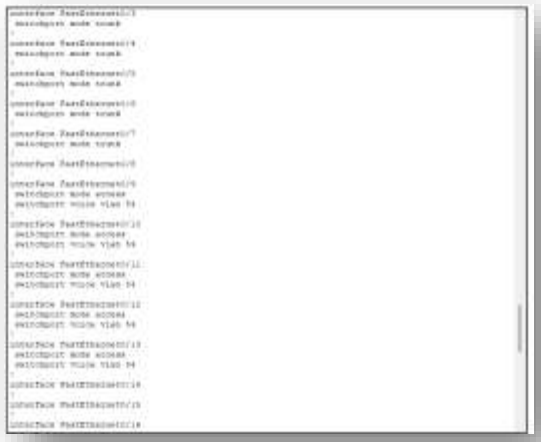
Las imágen muestra la configuración de un sistema de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra la configuración de una red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

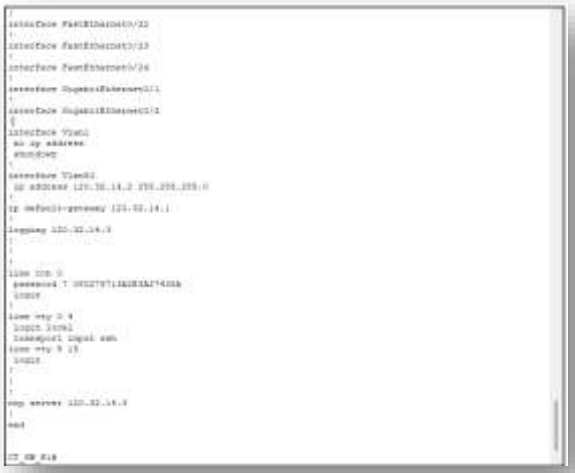
Torre de Consultorios | CT_SW_P1

La imágen muestra la configuración de un sistema de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

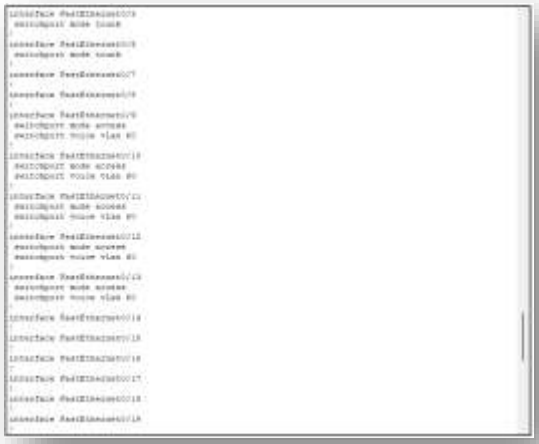
La imágen muestra una configuración de red que integra telefonía IP (con ephones y servidor DHCP para su aprovisionamiento), seguridad de acceso remoto con SSH y AAA, y la gestión del tráfico mediante VLANs y puertos troncales en switches. También se establecen servicios de red como NTP y enrutamiento OSPF, además de políticas de seguridad para el inicio de sesión.



La imágen muestra la configuración de un sistema de red integral que incluye telefonía IP con el uso de teléfonos ephones y servidor DHCP para su aprovisionamiento. También se configura la seguridad de acceso remoto mediante SSH y autenticación AAA. Se gestiona el tráfico mediante VLANs y puertos troncales en switches. Además, se establecen servicios de red como NTP y enrutamiento OSPF, y se aplican políticas de seguridad para el inicio de sesión.

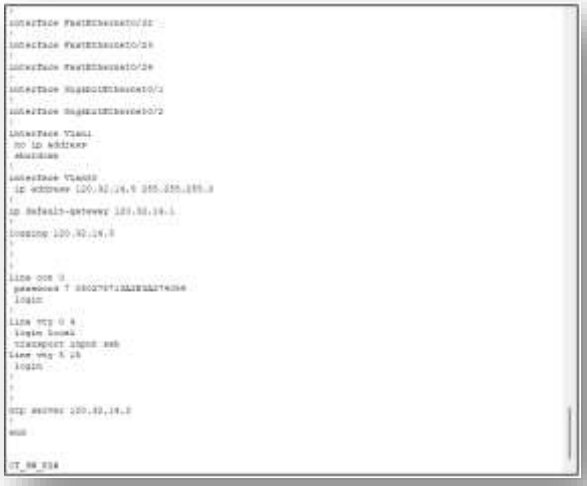
Torre de Consultorios | CT_SW_P2

La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



La imágen muestra una configuración de red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.

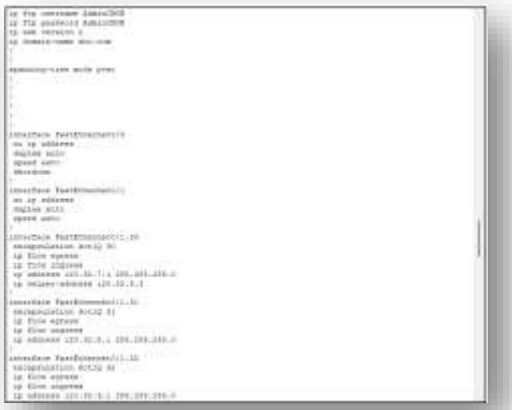
La imágen muestra la configuración de una red que integra telefonía IP, con un servidor DHCP para su aprovisionamiento y seguridad de acceso remoto con SSH y AAA. Se utilizan VLANs para la segmentación del tráfico de voz y datos, con puertos de switch configurados como troncales y de acceso, y se implementan servicios de red como NTP y enrutamiento OSPF.



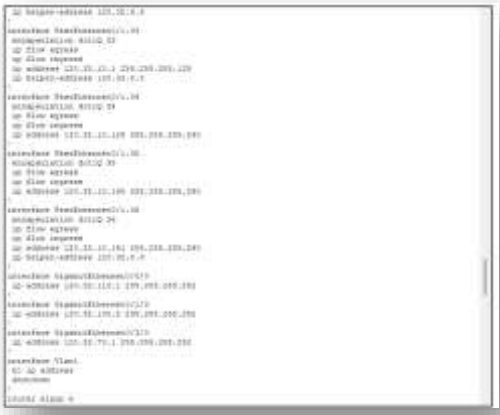
La imágen muestra la configuración de un sistema de red integral que incluye telefonía IP con el uso de teléfonos ephones y servidor DHCP para su aprovisionamiento. La seguridad de acceso remoto está configurada con SSH y autenticación AAA. Se utiliza la gestión del tráfico mediante VLANs y puertos troncales en switches. Además, se establecen servicios de red como NTP y se aplican políticas de seguridad para el inicio de sesión.

Centro de Neurología, Ortopedia y Rehabilitación | CNOR_R_PB

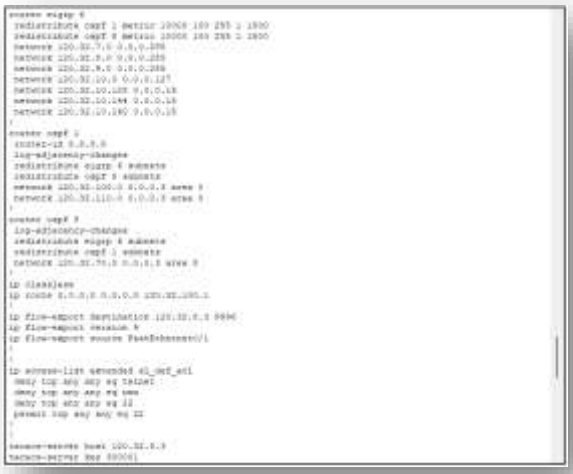
Se utilizo la configuración de show interface para mostrar configuraciones iniciales del router, incluyendo nombre de host, autenticación y asignación de direcciones IP.



Muestra Configuración de interfaces de red con direcciones IP y parámetros de tráfico.

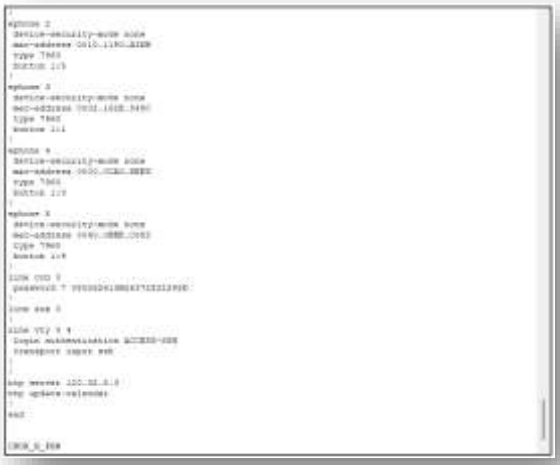


Se puede observar más configuraciones de interfaces y asignación de direcciones IP.



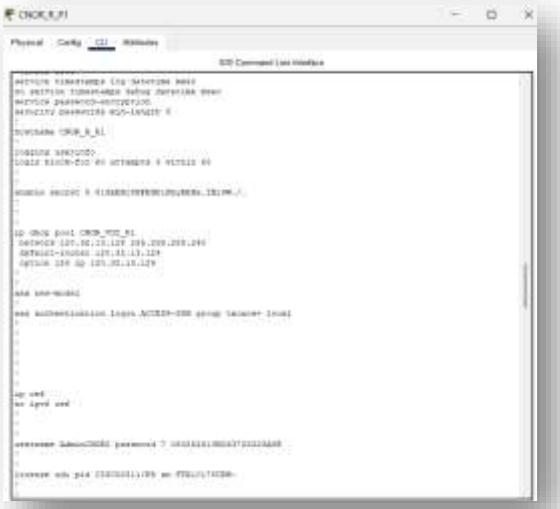
Se observa la configuración de enrutamiento con OSPF y EIGRP, incluyendo acceso y control de tráfico.

Aquí se puede ver la configuración de servidores TACACS y teléfonos IP (números y dispositivos asociados).



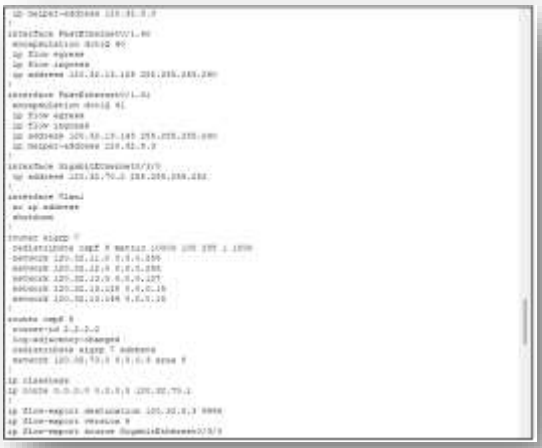
Se percibe a continuación la configuración de teléfonos IP con parámetros de seguridad y número.

Centro de Neurología, Ortopedia y Rehabilitación | CNOR_R_P1



se configura la seguridad, el acceso, la asignación de direcciones IP y las características avanzadas del dispositivo.

En resumen, se realiza la configuración básica de acceso FTP, Spanning Tree y las interfaces de red con sus parámetros asociados.



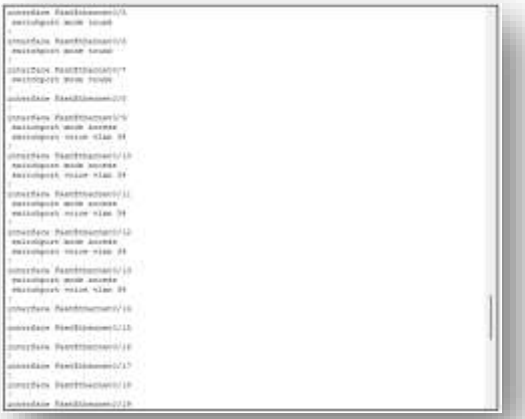
Configuración de interfaces con direcciones IP y control de flujo de tráfico.

se configura una lista de control de acceso (ACL), un servidor TACACS+ para autenticación, teléfonos IP con direcciones asignadas y configuraciones de seguridad para dispositivos.

se configura la seguridad de los teléfonos IP, las líneas de acceso remoto y el servidor NTP para la sincronización del tiempo.

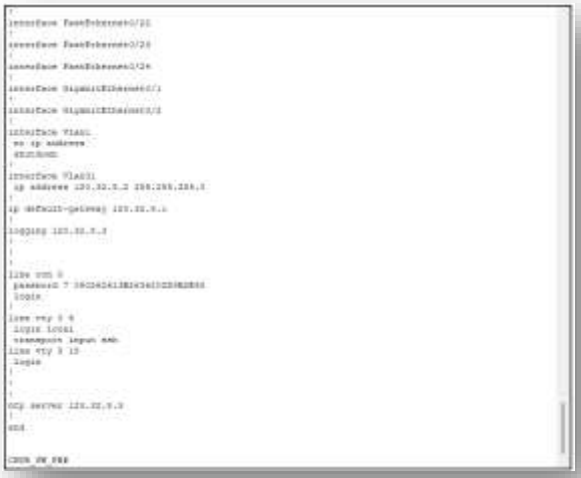
Centro de Neurología, Ortopedia y Rehabilitación | CNOR_SW_PB

se configura el switch con autenticación segura, spanning tree, y puertos trunk para permitir la transmisión de tráfico de múltiples VLANs.



se configuran puertos trunk para transportar múltiples VLANs y puertos de acceso para asignarles una VLAN específica, con énfasis en la VLAN de voz para algunas interfaces.

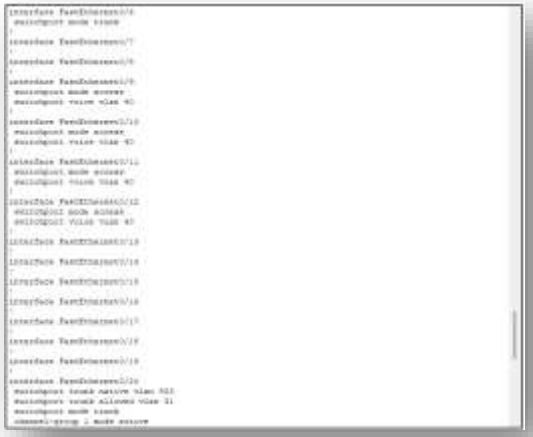
la configuración establece interfaces trunk con VLANs permitidas y nativas, agrega un grupo de enlaces (LACP), asigna una dirección IP a la VLAN 1, configura la puerta de enlace predeterminada y establece contraseñas para el acceso local y remoto.



establece interfaces Ethernet y GigabitEthernet, configura una dirección IP en la VLAN 1, asigna una puerta de enlace predeterminada, establece contraseñas para el acceso local y remoto (por SSH), y configura un servidor NTP para la sincronización de tiempo.

Centro de Neurología, Ortopedia y Rehabilitación | CNOR_SW_P1

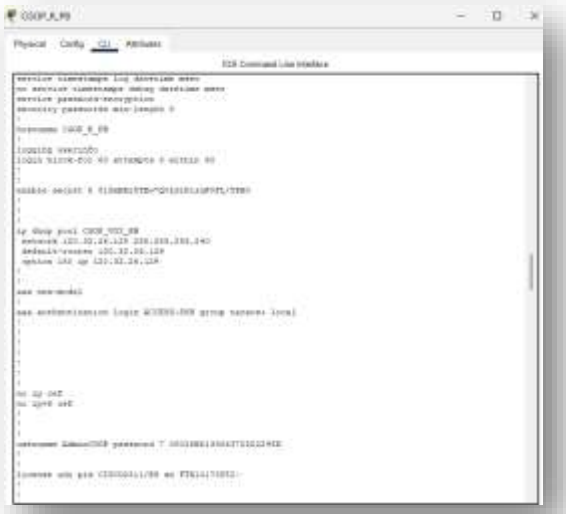
establece un dispositivo con seguridad mediante la encriptación de contraseñas y acceso FTP. Además, configura Spanning Tree para evitar bucles de red, habilita trunks para el transporte de múltiples VLANs a través de las interfaces y agrupa enlaces utilizando LACP para mejorar el rendimiento de la red.



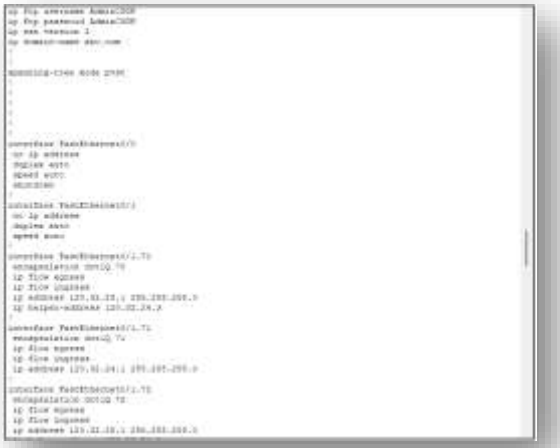
La configuración establece que varias interfaces operen en modo trunk para permitir el paso de tráfico de múltiples VLANs. Además, algunas interfaces están configuradas en modo de acceso para una VLAN específica, con VLAN 40 asignada para el tráfico de voz. También se configura un agrupamiento de enlaces para mejorar el rendimiento.

La configuración establece puertos trunk para permitir el paso de tráfico de la VLAN 31, crea un agrupamiento de enlaces con LACP, configura la VLAN 1 con una dirección IP, establece contraseñas para acceso local y remoto (SSH), y define un servidor NTP para sincronización horaria.

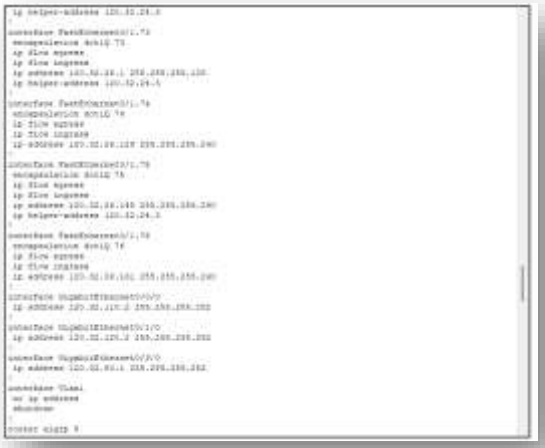
Centro de Gineco-Obstetricia y Pediatría | CGOP_R_PB



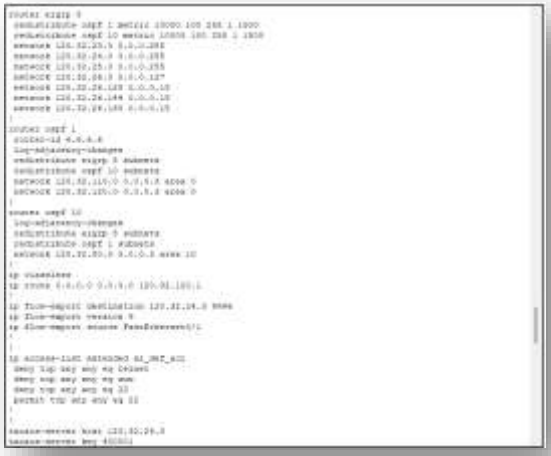
La configuración establece un nombre de host, configura un pool DHCP con direcciones IP, habilita autenticación AAA para el acceso remoto, y encripta las contraseñas. También configura un servidor DNS y TFTP para los clientes DHCP, y muestra información de licencia para el dispositivo.



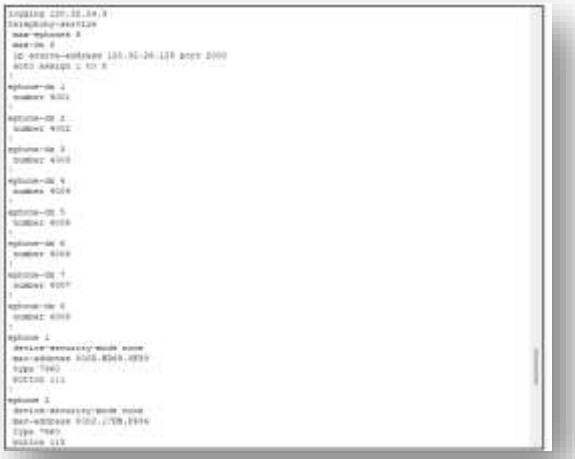
La configuración establece un acceso FTP seguro y habilita SSH para la administración remota. Configura el spanning tree en modo PVST y define varias subinterfaces en las interfaces FastEthernet para manejar el tráfico de VLANs específicas, asignando direcciones IP a cada subinterfaz y habilitando el monitoreo de flujo de tráfico.



La configuración define varias interfaces y subinterfaces con encapsulación dot1Q para el tráfico de VLANs, asigna direcciones IP y habilita el monitoreo de tráfico. También se configuran direcciones helper para redirigir solicitudes DHCP. Además, se habilita EIGRP para el enrutamiento dinámico y se configuran interfaces GigabitEthernet con sus respectivas direcciones IP.



La configuración incluye EIGRP y OSPF para enrutamiento, con redistribución entre los dos. También se configura la exportación de flujos NetFlow y una lista de control de acceso (ACL) para bloquear tráfico Telnet y permitir SSH. Además, se configuran servidores TACACS+ para la autenticación.



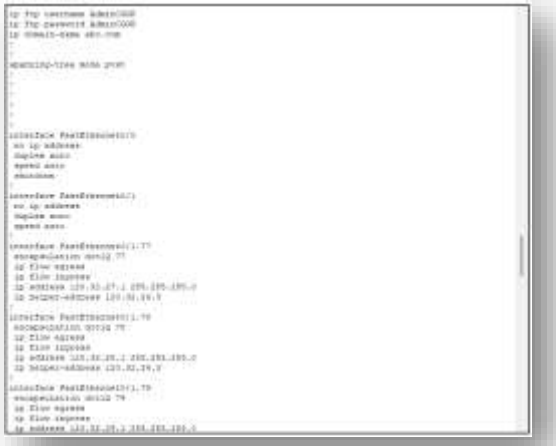
La configuración se centra en la gestión de teléfonos IP Cisco, asignando números de extensión (DN) y configurando teléfonos específicos con direcciones MAC y modelos, además de establecer parámetros como el número máximo de teléfonos y el servidor de telefonía para registro. Se establece el puerto y la dirección IP para la comunicación con los teléfonos y se configuran las funciones básicas de seguridad y botones en los teléfonos.

La configuración establece varios teléfonos IP Cisco 7960, asignando direcciones MAC y configurando botones específicos en cada uno para facilitar el acceso a las líneas de teléfono. También se configura una línea auxiliar con un tiempo de espera y contraseña para su acceso remoto o local.

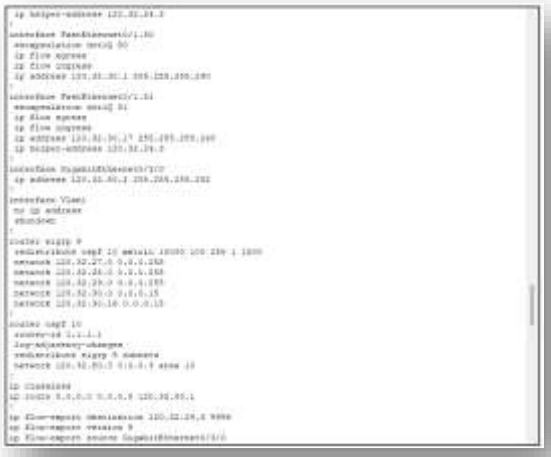
La configuración establece varios teléfonos IP Cisco 7960 con direcciones MAC únicas y asignaciones de botones específicas para cada teléfono. También se configuran líneas de acceso para SSH y consola, con un tiempo de espera configurado y contraseñas encriptadas. Además, se configura un servidor NTP para sincronización horaria.

Centro de Gineco-Obstetricia y Pediatría | CGOP_R_P1

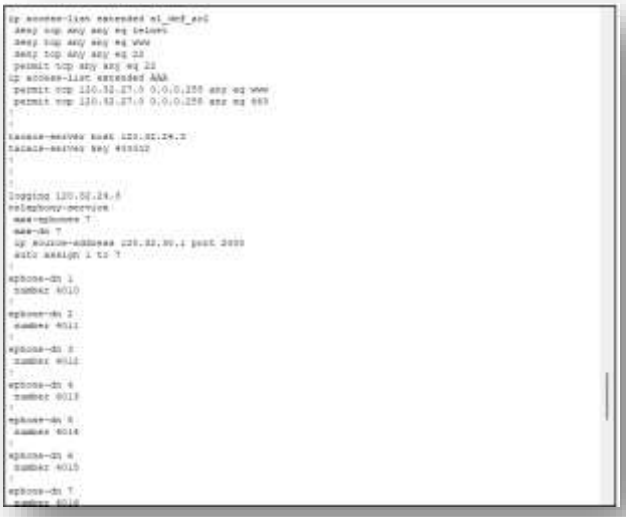
Esta configuración establece la seguridad de contraseñas, configura un pool DHCP para la asignación de direcciones IP y configura un servidor de autenticación AAA para controlar el acceso. Además, muestra detalles sobre la licencia del dispositivo y configura las marcas de tiempo en los logs del dispositivo.



La configuración se centra en el acceso FTP, el Spanning Tree en modo PVST, y la configuración de varias interfaces FastEthernet, algunas de las cuales están configuradas con subinterfaces para el manejo de tráfico de VLANs específicas. Además, se asignan direcciones IP a algunas interfaces y se habilita el monitoreo de flujo de tráfico y la funcionalidad helper-address para redirigir solicitudes DHCP.



La configuración incluye la gestión de tráfico y flujos de red (NetFlow), enrutamiento dinámico utilizando EIGRP y OSPF, la configuración de interfaces de red con VLANs y direcciones IP, así como el uso de helper-addresses para redirigir solicitudes DHCP. También se configura la exportación de flujos NetFlow hacia un servidor específico para el monitoreo y análisis del tráfico.



La configuración establece una ACL extendida para controlar el acceso a puertos Telnet, HTTP y HTTPS, configura un servidor TACACS+ para la autenticación, y habilita el servicio de telefonía para permitir el registro de hasta 7 teléfonos IP. Además, se asignan números de teléfono (DN) a cada uno de los ephones configurados para la telefonía IP.

```
ephone-dn 7
 number 6018
!
ephone 1
 device-security-mode none
 mac-address 0060.8248.8187
 type 7960
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 0002.1686.E88A
 type 7960
 button 1:8
!
ephone 4
 device-security-mode none
 mac-address 0080.8943.379C
 type 7960
 button 1:7
!
ephone 5
 device-security-mode none
 mac-address 0080.8908.E7E9
 type 7960
 button 1:4
!
ephone 3
 device-security-mode none
 mac-address 00E0.8FEB.3B8A
 type 7960
 button 1:2
!
ephone 6
 device-security-mode none
 mac-address 0040.0861.9B97
 type 7960
 button 1:3
!
ephone 7
 device-security-mode none
 mac-address 0080.8A83.C94E
 type 7960
```

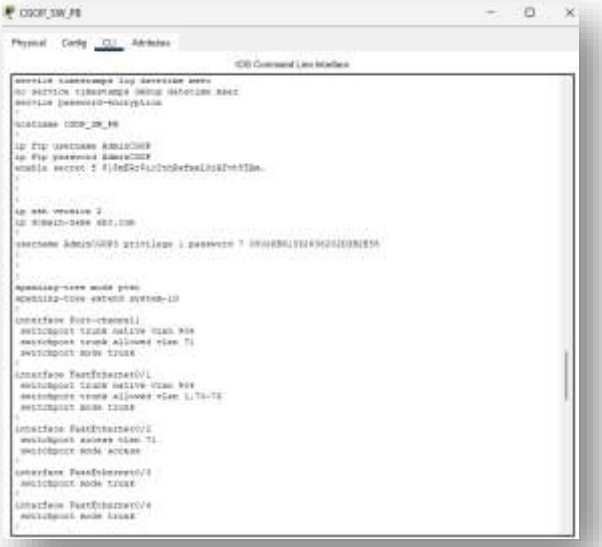
La configuración muestra la asignación de números de línea directa (DN) a cada teléfono IP Cisco 7960, asignando direcciones MAC únicas a cada dispositivo y configurando botones para cada uno de los teléfonos. La seguridad adicional para los dispositivos está desactivada, lo que implica que no se aplican restricciones de seguridad adicionales.

```
ephone 4
 device-security-mode none
 mac-address 0080.8908.E7E9
 type 7960
 button 1:4
!
ephone 5
 device-security-mode none
 mac-address 00E0.8FEB.3B8A
 type 7960
 button 1:2
!
ephone 6
 device-security-mode none
 mac-address 0040.0861.9B97
 type 7960
 button 1:3
!
ephone 7
 device-security-mode none
 mac-address 0080.8A83.C94E
 type 7960
 button 1:5
!
line vty 0
 exec-timeout 5 30
 password 7 [illegible]
!
line aux 0
!
line vty 0 4
 login authentication ACCESS-SSH
 transport input ssh
!
!
ntp server 129.35.24.9
ntp update-calendar
!
end

CISCO_R_R1#
```

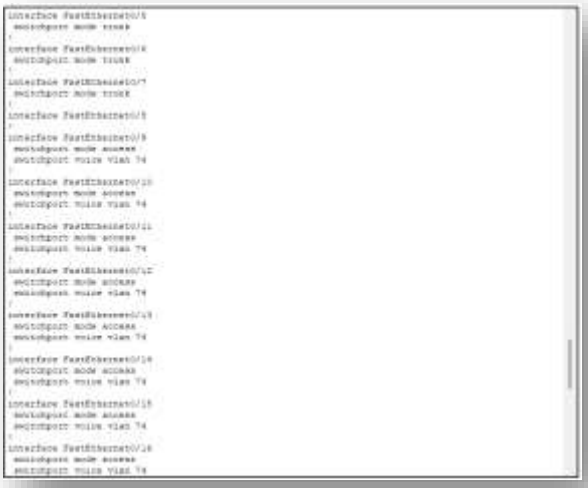
La configuración establece varios teléfonos IP Cisco 7960 con asignaciones de direcciones MAC y configuraciones de botones para las líneas de teléfono. También se configura el acceso remoto SSH y se

define una contraseña para la consola y las líneas VTY. Además, se configura un servidor NTP para la sincronización del tiempo.

Centro de Gineco-Obstetricia y Pediatría | CGOP_SW_PB

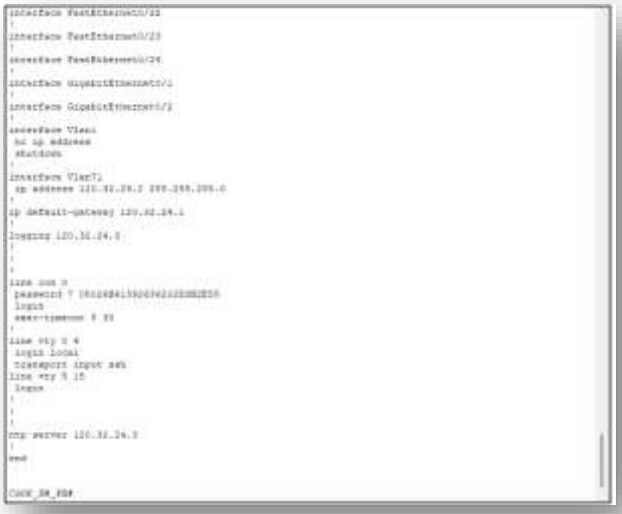


La configuración establece la seguridad con SSH para el acceso remoto, configura Spanning Tree en modo PVST y habilita la extensión del system-id. Además, se configuran puertos trunk para el transporte de múltiples VLANs y un puerto de acceso para una VLAN específica. También se establece un pool de direcciones IP para FTP y un nombre de dominio para el dispositivo.



Esta configuración gestiona una mezcla de puertos trunk (para transmitir tráfico de múltiples VLANs) y puertos de acceso específicos para la VLAN 74, configurada para el tráfico de voz. Se utiliza para asegurar que los puertos de voz en el switch estén correctamente asignados a la VLAN correspondiente para servicios como la telefonía IP.

La configuración establece varios puertos trunk para transmitir tráfico de VLAN 71 y una VLAN nativa de VLAN 904. También se agrupan puertos mediante LACP para una mayor eficiencia. Además, se configura la VLAN 71 con una dirección IP y se establece una puerta de enlace predeterminada. La configuración de la línea de consola también incluye una contraseña para el acceso local.



La configuración gestiona varias interfaces de red (FastEthernet y GigabitEthernet), asignando direcciones IP y desactivando ciertas interfaces. Se configura la VLAN 71 con su dirección IP y se establece una

puerta de enlace predeterminada. También se configura la seguridad para el acceso local y remoto, usando contraseñas encriptadas y acceso SSH. Además, se configura un servidor NTP para la sincronización del reloj del dispositivo.

Centro de Gineco-Obstetricia y Pediatría | CGOP_SW_P1

La configuración abarca la configuración básica de seguridad y acceso, activando SSH para administración remota, configurando puertos trunk para transmitir el tráfico de la VLAN 71 y una VLAN nativa (VLAN 904). También se gestionan las configuraciones de Spanning Tree y de acceso FTP con credenciales configuradas.

La configuración define varios puertos en modo trunk para el transporte de tráfico de varias VLANs, y puertos de acceso configurados específicamente para manejar el tráfico de voz en la VLAN 80. Esto asegura que los puertos para dispositivos de voz (como teléfonos IP) tengan el tráfico adecuado separado y etiquetado correctamente.

La configuración establece puertos trunk para el paso de tráfico de las VLANs 71 y 904, y usa LACP para agregar enlaces. Además, se configura la VLAN 71 con una dirección IP y puerta de enlace predeterminada, y se habilitan las líneas de acceso local para la consola y el acceso remoto por SSH. También se configura un servidor para registrar los logs del dispositivo.

La configuración establece interfaces FastEthernet y GigabitEthernet sin direcciones IP asignadas. Configura la VLAN 71 con una dirección IP y una puerta de enlace predeterminada, aunque la interfaz VLAN 71 está desactivada. Además, se configura la seguridad de acceso tanto para la consola como para el acceso remoto SSH, y se sincroniza el tiempo mediante un servidor NTP

Conclusiones del proyecto

Joseph Diego Moysen Ramirez: El desarrollo de este proyecto para el Hospital ABC Santa Fe representó una oportunidad significativa para aplicar y consolidar mis conocimientos en redes y telecomunicaciones. Más allá del aspecto técnico, este trabajo me permitió entender la importancia de planificar soluciones reales para entornos de alta demanda.

Diana Laura Miualteclatl Rodriguez: En conclusión, desarrollar este proyecto para el Hospital ABC me permitió adquirir una experiencia integral que integró el análisis, el diseño y la implementación de una infraestructura de red robusta y confiable, que puso a prueba mis conocimientos técnicos en la configuración de servicios esenciales, y también reforzó la importancia de implementar soluciones de redundancia, seguridad y monitoreo continuo.

Paola Xiqui Garcia: Este proyecto representó una experiencia integral en el diseño y planificación de una red de alto rendimiento, y pudimos poner en práctica conocimientos sobre segmentación de red, VLANs, ACLs, servicios esenciales, y resaltar la importancia de entender el entorno, priorizar servicios críticos y anticipar el futuro crecimiento de una infraestructura.