UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERIA ELECTRICA

DISEÑO Y CONFIGURACIÓN DE UNA RED RT-ETHERNET ENRUTADA, ENFOQUE PRÁCTICO

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN REDES DE COMUNICACIONES

DANILO ALEJANDRO AEDO COFRÉ

PROFESOR GUIA:

JORGE SANDOVAL ARENAS

MIEMBROS DE LA COMISIÓN:
CÉSAR AZURDIA MEZA
NICOLAS AUGER SOUZA

SANTIAGO, CHILE

2019

RESUMEN DE LA TESIS PARA OPTAR AL TÍTULO DE MAGÍSTER EN INGENIERÍA DE REDES DE COMUNICACIONES.
POR: DANILO AEDO COFRÉ
FECHA: 2019
PROFESOR GUÍA: JORGE SANDOVAL ARENAS

DISEÑO Y CONFIGURACIÓN DE UNA RED RT-ETHERNET ENRUTADA, ENFOQUE PRACTICO

Hasta hace unos años atrás el retardo en las comunicaciones en el entorno de los 150ms – 200ms, incluso para transmisión de VoIP o Streaming, era suficiente para la mayoría de las aplicaciones que utilizan la pila de protocolos TCP/IP, además en caso de fallas los tiempos de reconfiguración a nivel de segundos eran adecuados para gran parte de las de las infraestructuras de red. Dado el desarrollo de nuevas aplicaciones en base a estos protocolos que necesitan respuestas mucho más exigentes como la telemedicina, el mercado financiero, la gestión de tráfico de vehículos en tiempo real, realidad virtual, etc. han abierto la necesidad de bajar estos valores de retardo al entorno de los 10ms e idealmente tiempos de convergencia por debajo de un segundo.

En el ambiente industrial la masificación de aplicaciones basadas en TCP/IP ha sido lenta pero constante, las utilities, plantas automatizadas o comunicaciones de misión crítica, han producido que se realicen múltiples esfuerzos para poder desarrollar mecanismos de software y hardware que logren el anhelado comportamiento determinista de las comunicaciones que necesitan muchas de las aplicaciones del mundo industrial. La evolución de las redes industriales ha llevado al protocolo ethernet prácticamente al dispositivo final, se puede ver cada vez más tarjetas remotas de entradas y salidas, sensores y actuadores compatibles con la pila TCP/IP y a lo menos en comunicaciones a nivel de capa 2 de modelo OSI, siendo menos comunes los equipos que soportan comunicaciones a través de dispositivos que realizan enrutamiento donde se hace relevante un buen diseño de red y la elección protocolos e implementaciones adecuadas para lograr un alto desempeño.

En este trabajo se realiza un diseño y propuesta de configuración en base a un caso real que permita obtener bajos niveles de latencia (retardo), jitter y tiempo de reconfiguración o convergencia de red ante fallas.

En primer término, se realizará una revisión de protocolos de comunicaciones industriales y de redes IP para obtener la orientación necesaria para el planteamiento de las pruebas y la propuesta de configuración final. En segundo lugar, se realizarán una serie de experimentos en búsqueda de datos reales del hardware presente en el caso práctico, lo que además permitirá obtener la base empírica de la propuesta de configuración. Posteriormente se realizará un diseño y una propuesta de configuración para la red planteada en el caso práctico, en base a los pasos antes descritos. Finalmente, a modo orientativo se plantearán recomendaciones para la mejora de la Ciberseguridad de la red en el caso práctico que se presentará.

Agradecimientos

Mis sinceros agradecimientos a los profesores Jorge Sandoval y Cesar Azurdia por su disposición, a la empresa COMSA Industrial por darme la posibilidad de ejecutar las pruebas en una infraestructura real, a mi colega y amigo Helbert Silva por su ayuda y consejos , a la empresa MyF Sistemas de Control por facilitarme sin ningún interés los equipos de control automático, a la Universidad de Chile por los conocimientos entregados, a mi familia, amigos y en especial a Andrea y Guadalupe por siempre brindarme el cariño y apoyo cuando más lo necesite.

Dedicatoria

A Andrea y Guadalupe que están conmigo día a día, A mis Padres Mónica y Rene por su cariño y mostrarme el camino, a mis abuelas María y Eliana por ser la mejores del mundo y a mis tatas Rene y Pedro que ya no están en este mundo.

También quiero dedicar este trabajo a todas las personas que me han soportado y me brindan alegría cada vez que nos reunimos, mis hermanos María, Rodrigo, mis primos casi hermanos, Felipe, Camila, Claudio, Paula, Pablo, Francisco, Carola, Leo y Pamela, a los mejores tíos Isabel y Osvaldo y a mis grandes amigos de la vida Enrique, Francisco, Sebastián, Felipe, José y Víctor.

Tabla de Contenido

Capítulo 1 Introducción 1
1.1 Motivación: 2
1.2 Objetivos: 2
1.2.1 Objetivos generales 2
1.2.2 Objetivos Específicos 2
1.3 Metodología: 3
Capítulo 2 Antecedentes Previos 4
2.1 Conceptos y protocolos básicos para Redes IP 4
2.1.1 Modelo OSI y TCP/IP 4
2.1.2 ARP 5
2.1.3 ICMP 5
2.1.4 TCP 5
2.1.5 UDP 7
2.1.6 DHCP 7
2.1.7 HTTP y HTTPS 8
2.1.8 DNS 8
2.1.9 Parámetros de Desempeño 9
2.2 Protocolos para las aplicaciones del ICS planteado en el caso práctico 10
2.2.1 SNMP 10
2.2.2 RTP 13
2.2.3 RTCP 14
2.2.4 VoIP 14
2.2.4.1 CODECs 15
2.2.4.2 Protocolos para el establecimiento de llamadas VoIP 15
2.2.4.2.1 H.323 15
2.2.4.2.2 SIP 16
2.2.5 CCTV Circuito cerrado de televisión 17
2.2.5.1 H.264/AVC (Advanced Video Coding) o MPEG-4 Part 10: 18
2.2.6 Modbus TCP 19

2.3 Redes de comunicación para ICS y protocolos RT-Ethernet 23
2.3.1 Diferencias entre sistemas IT tradicionales e ICS 24
2.3.2 Estado del arte de los protocolos RT-Ethernet para ICS 26
2.3.2.1 Clasificación de protocolos ethernet industriales según rendimiento 26
2.3.2.2 IEEE 1588 Precision Time Protocol PTP 27
2.3.2.3 Profinet 29
2.3.2.4 Ethernet/IP 31
2.3.2.5 Ethernet Powerlink 33
2.3.2.6 SERCOS III 35
2.3.2.7 EtherCAT y EAP 36
2.3.2.7.1 EtherCAT 36
2.3.2.7.2 EAP 39
2.4 Revisión de Protocolos de control de Redes IP 43
2.4.1 Capa de Acceso 43
2.4.1.1 Familia de protocolos Spannig Tree 44
2.4.1.1.1 STP 44
2.4.1.1.2 RSTP 47
2.4.1.1.3 MSTP 49
2.4.1.2 SEP 50
2.4.1.2.1 Conceptos básicos 50
2.4.1.2.2 Roles de interfaces en SEP: 50
2.4.1.2.3 Estado de interfaces: 51
2.4.1.2.4 Tramas SEP 51
2.4.1.2.5 SEP load balancing 53
2.4.1.2.6 Convergencia en SEP 53
2.4.2 Capa de agregación 54
2.4.2.1 VRRP 54
2.4.2.1.1 Timers 55
2.4.2.1.2 Paquete VRRP 57
2.4.2.1.3 VRRP load balancing 57
2.4.2.1.4 Convergencia 59
2.4.2.2 Enrutamiento 59

2.4.2.2.1 Conceptos Básicos 59
2.4.2.2.2 OSPF 60
2.4.2.2.3 BGP 65
2.4.3 Protocolos Auxiliares 70
2.4.3.1 Eth-Trunk: 70
2.4.3.1.1 Modo manual 71
2.4.3.1.2 Modo LACP 71
2.4.3.2 CSS 71
2.4.3.3 BFD 74
2.4.3.4 IP FRR LFA 75
2.5 QoS en Redes IP 77
2.5.1 Arquitectura de QoS 77
2.5.2 Manejo de QoS 77
2.5.2.1 Clasificación y marcado 77
2.5.2.1.1 Clasificación 77
2.5.2.1.2 Marcado 78
2.5.2.2 Gestión del tráfico: 79
2.5.2.2.1 Traffic Policing 79
2.5.2.2.2 Traffic Shapping 79
2.5.2.2.3 Gestión colas 80
2.5.2.3 MQC 81
2.6 Ciberseguridad en redes pata ICS 82
2.6.1 Conceptos básicos: 82
2.6.1.1 Triada de seguridad: 82
2.6.1.2 Protocolos AAA 83
2.6.1.2.1 RADIUS: 83
2.6.1.3 Cifrado 83
2.6.1.3.1 Algoritmos de cifrado 84
2.6.1.3.2 Funciones de HASH 84
2.6.1.4 Transmisión sobre un canal seguro 85
2.6.1.4.1 Seguridad en la capa de red 86
2.6.1.4.2 Seguridad en la capa de transporte 87

2.6.1.4.3 Seguridad en la capa de aplicación 88
2.6.1.5 Malware 88
2.6.1.6 Tipos y formas Ataques 90
2.6.1.6.1 Tipos básicos de ataques 90
2.6.1.6.2 Ataques ARP 90
2.6.1.6.3 Ataques ICMP 90
2.6.1.6.4 Ataques TCP 90
2.6.1.6.5 Ataques a DHCP 91
2.6.1.6.6 Otros Ataques 91
2.6.2 Políticas de Seguridad 92
2.6.3 Seguridad Perimetral 92
2.6.3.1 ACL 93
2.6.3.2 Firewalls 93
2.6.3.3 IDS/IPS 94
2.6.3.4 DMZ 94
2.6.4 Normativa de Seguridad y Organismos competentes: 94
2.6.4.1.1 CERT/CSIRT 95
2.6.4.1.1 ICS-CERT 95
2.6.4.1.2 ISA99 / IEC-62443 95
2.6.4.1.3 NIST SP 800-82 97
Capítulo 3 Planteamiento de caso práctico 101
3.1 Subsistema Red de Comunicaciones 101
3.1.1 Capa de acceso 102
3.1.2 Capa de Agregación 103
3.1.3 Capa de Core 103
3.2 Subsistemas del ITS 104
3.2.1 Consideraciones generales 104
3.2.2 Subsistema de Gestión de Red SGDR 105
3.2.2.1 Cálculo de ancho de banda: 105
3.2.3 Sistema de Control y Ventilación SCCV 106
3.2.3.1 Cálculo de ancho de banda: 106
3.2.4 Subsistema de Circuito Cerrado de Televisión SCTV 108

3.2.5 Subsistema de Detección Automática de Incidentes SDAI 110
3.2.6 Subsistema de telefonía STEL 110
3.2.6.1 Cálculo de Ancho de banda: 111
3.2.7 Subsistema Detección de Incendios SDTI 111
3.2.7.1 Cálculo de ancho de banda 111
3.2.8 Subsistema de Radiocomunicaciones SRAD 112
3.2.8.1 Cálculo de ancho de banda 113
3.2.9 Subsistema de Control iluminación SILU 113
3.2.9.1 Cálculo de ancho de banda 113
3.2.10 Subsistema de control energía de baja tensión SCBT 114
3.2.10.1 Cálculo de Ancho de Banda: 114
3.2.11 Subsistema de Postes SOS SSOS 114
3.2.11.1 Cálculo de ancho de banda 115
3.2.12 Subsistema de Megafonía SMEG 116
3.2.13 Subsistema de Señalización de tráfico SGTR 116
3.2.13.1 Cálculo de ancho de banda 117
Capítulo 4 Pruebas 118
4.1 Test de herramienta 119
4.1.1 Procedimiento 120
4.1.2 Pruebas 121
4.1.2.1 Prueba 1: Estabilidad de envío de paquetes y variación de jitter 64 bytes 121
4.1.2.2 Prueba 2: Estabilidad de envío de paquetes y variación jitter 768 bytes 123
4.1.2.3 Prueba 3: Estabilidad de envío de paquetes y variación jitter 1280 bytes 124
4.1.2.4 Prueba 4: jitter a partir de paquetes capturados con Wireshark para 1280 bytes. 126
4.1.3 Análisis de resultados: 128
4.2 Capa de Acceso 129
4.2.1 Procedimiento 130
4.2.2 Pruebas 130
4.2.2.1 Pruebas MSTP 131
4.2.2.2 Pruebas SEP 132
4.2.2.3 Pruebas SEP aumentando equipos 134
4.2.3 Análisis de Resultados 136

4.3 Capa de Agregación 137
4.3.1 VRRP 137
4.3.1.1 Procedimiento 138
4.3.1.2 Pruebas 138
4.3.1.3 Análisis de resultados 141
4.3.2 Protocolos de enrutamiento BGP y OSPF 141
4.3.2.1 Procedimiento 141
4.3.2.2 OSPF 142
4.3.2.2.1 Pruebas de convergencia 143
4.3.2.2.2 Pruebas de latencia 145
4.3.2.3 BGP 147
4.3.2.3.1 Pruebas de convergencia 148
4.3.2.3.2 Pruebas de latencia 150
4.3.2.4 Análisis de Resultados 152
4.4 Pruebas de comunicación entre PLCs 152
4.4.1 Procedimiento 152
4.4.2 Pruebas 154
4.4.2.1 Pruebas de tiempo de reacción 156
4.4.2.2 Pruebas de jitter y ancho de banda: 157
4.4.3 Análisis de resultados 158
Capítulo 5 Propuesta de Configuración 160
5.1 Nomenclatura de Switches 161
5.2 Cálculo de tráfico Agregado 164
5.3 Propuesta capa de Acceso 166
5.3.1 Direccionamiento IP para equipos terminales 166
5.3.2 Configuración Básica de switches 166
5.3.2.1 VLANs 166
5.3.2.2 Interfaces: 167
5.3.2.2.1 Switches de Acceso: 167
5.3.2.2.2 Switches de Agregación: 167
5.3.2.3 Protocolo para prevención de loops 167
5.3.2.3.1 Criterios de diseño: 167

5.3.2.3.2 Configuración básica de los switches de cada anillo de acceso: 168
5.3.2.3.3 Configuración de los switches de Agregación de los anillos: 168
5.3.2.4 QoS 169
5.3.2.4.1 Criterios de diseño 169
5.3.2.4.2 Configuración 170
5.4 Propuesta capa de Agregación 170
5.4.1 Configuración básica de switches 170
5.4.1.1 Conexiones entre switches de agregación y hacia el Core 170
5.4.1.2 Interfaces de VLAN 170
5.4.2 VRRP 171
5.4.2.1 Criterios de diseño: 171
5.4.2.2 Configuración a VRRP: 171
5.4.3 Enrutamiento 172
5.4.3.1 Criterios de diseño: 173
5.4.3.2 Configuración a BGP 173
5.4.4 QoS 174
5.4.4.1 Criterios de diseño 174
5.4.4.2 Configuración: 174
5.5 Propuesta capa de Core 175
5.5.1 Interfaces: 175
5.5.2 Configuración hacia equipos terminales 175
5.5.3 Configuración hacia la capa de agregación 175
5.5.4 Configuración Capa de Core 175
5.5.4.1 Configuración Eth-trunk 175
5.5.4.2 Configuración CSS 176
5.5.5 QoS 176
5.6 Propuesta de cambios para el subsistema de control centralizado y ventilación 176
Conclusiones 177
Glosario 179
Bibliografía 183
Anexo A Recomendaciones de Ciberseguridad para el caso práctico 187
Anexo B Distribución de equipos en switches de acceso. 199

Anexo C Scripts de Configuración para pruebas. 204
Anexo D Detalle de Hardware de pruebas. 249

Índice de tablas

Tabla 2-1 Detalles de los campos en mensaje SNMPv2 12
Tabla 2-2 Detalles de los campos en mensaje SNMPv3 13
Tabla 2-3 Codec para VoIP ITU 15
Tabla 2-4 Detalle de Cabecera ModbusTCP 20
Tabla 2-5 Tipos de registros Modbus / Modbus TCP 21
Tabla 2-6 Function Code más utilizados 22
Tabla 2-7 diferencias entre sistemas IT e ICS 25
Tabla 2-8 Evolución de estados de interfaces de STP a RSTP 47
Tabla 2-9 Evolución de roeles de interfaces o puertos de STP a RSTP 48
Tabla 2-10 Flags de BPDU RSTP 48
Tabla 3-1 Ancho de banda para los diferentes tipos de cámara 110
Tabla 3-2 Ancho de banda ocupado por el subsistema de telefonía 111
Tabla 3-3 Ancho de banda de audio para Subisistema SSOS 115
Tabla 4-1 Características del laptop del Cliente Iperf 118
Tabla 4-2 Características del laptop del Servidor Iperf 118
Tabla 4-3 Características del laptop para capturar tráfico 119
Tabla 4-4 Jitter por rango capturas Wireshark de generación de paquetes 127
Tabla 4-5 Jitter por rango capturas Wireshark de generación de paquetes 127
Tabla 4-6 Análisis de rango de jitter mayor a 3ms 128
Tabla 4-7 Comparativa SEP MSTP 129
Tabla 4-8 Resultados pruebas de convergencia MSTP 132
Tabla 4-9 Resultados pruebas de convergencia SEP 134
Tabla 4-10 Resultados pruebas de convergencia SEP con aumento de switches 135
Tabla 4-11 Resultados pruebas VRRP 141
Tabla 4-12 Resultados pruebas de convergencia OSPF 144
Tabla 4-13 Resultados de pruebas de latencia OSPF 147
Tabla 4-14 resultados de pruebas de latencia BGP 151
Tabla 4-15 Resultados pruebas de tiempo de reacción PLCs por EAP 156
Tabla 4-16 Resultados pruebas de jitter y ancho de banda de PLCs por EAP 157
Tabla 5-1 Base de propuesta de configuración. 163

Índice de figuras

Figura 2-1 Modelo OSI y TCP/IP. 5
Figura 2-2 Segmento TCP 6
Figura 2-3 Tree-handshake 6
Figura 2-4 Segmento UDP 7
Figura 2-5 Negociación DHCP con 2 servidores. 7
Figura 2-6 Pila de protocolos ocupados por HTTP y HTTPS 8
Figura 2-7 Detalle de funcionamiento por capas SNMP 10
Figura 2-8 Arquitectura de OID. 11
Figura 2-9 Mensaje SNMPv2. 12
Figura 2-10 Mensaje SNMPv3 13
Figura 2-11 Detalle mensaje RTP 14
Figura 2-12 Flujo de llamada SIP. 17
Figura 2-13 GOP con sus diferentes tipos de frames. 19
Figura 2-14 Pila de protocolos Modbus tradicional y ModbusTCP. 20
Figura 2-15 Mensaje ModbusTCP y relación con Modbus tradicional 21
Figura 2-16 Niveles de organización de los sistemas en un ICS. 23
Figura 2-17 Tendencias de mercado de los estándares en comunicaciones industriales. 24
Figura 2-18 Cuotas de mercado de protocolos de comunicaciones industriales. 24
Figura 2-19 Latencias para los diferentes tipos de controles industriales. 27
Figura 2-20 Proceso general de sincronización de relojes PTP 27
Figura 2-21 Ejemplo de proceso de sincronización PTP 28
Figura 2-22 Ejemplo de configuración Profinet IO 30
Figura 2-23 Ejemplo de configuración Profinet Cba 30
Figura 2-24 Detalle de Trama Profinet. 31
Figura 2-25 Ciclo de comunicación Profinet IRT. 31
Figura 2-26 Arquitectura Ethernet/IP, DeviceNet, ControlNet, DeviceNet - CIP 32
Figura 2-27 Flujo de mensajes explícitos e implícitos y de tiempo real Ethernet/IP 33
Figura 2-28 Ciclos de envío de datos en Powerlink 34
Figura 2-29 Trama ethernet Powerlink. 34

Figura 2-30 Trama SERCOS III. 35
Figura 2-31 Ciclo de comunicación SERCOS III. 36
Figura 2-32 Funcionamiento de comunicaciones SERCOS III. 36
Figura 2-33 Trama EtherCAT. 38
Figura 2-34 flujo de ingreso de datos en Subtelegramas. 39
Figura 2-35 Relación del campo de datos de EtherCAT con EAP. 40
Figura 2-36 Trama EAP. 41
Figura 2-37 Funcionamiento ADS, ... 42
Figura 2-38 ejemplo de problema de loop en capa 2 43
Figura 2-39 BPDU STP 45
Figura 2-40 Dinámica de estados de puertos en STP 46
Figura 2-41 Flags BPDU STP y RSTP 48
Figura 2-42 Roles de interfaces en SEP 50
Figura 2-43 Formato de trama SEP 52
Figura 2-44 SEP con balanceo de carga 54
Figura 2-45 Principio de funcionamiento de VRRP 55
Figura 2-46 Lógica de funcionamiento de VRRP 56
Figura 2-47 Paquete VRRP 57
Figura 2-48 Balanceo de carga en VRRP en el mismo segmento de red 58
Figura 2-49 Balanceo de carga en VRRP en segmentos de red distintos. 58
Figura 2-50 Protocolos de enrutamiento dinámico. 60
Figura 2-51 Roles de equipos dentro de dominio OSPF según su ubicación y función. 61
Figura 2-52 Establecimiento de adyacencias OSPF. 63
Figura 2-53 Estados para establecimiento de adyacencias BGP [78] 68
Figura 2-54 Ejemplo enlace Eth-Trunk. [79] 71
Figura 2-55 Ejemplo configuración CSS. [18] 72
Figura 2-56 Prioridades para tomar el rol de Master CSS. [18] 73
Figura 2-57 Ejemplo de falla de conexión CSS. [18] 73
Figura 2-58 CSS MAD en modo Relay. [18] 74
Figura 2-59 Paquete BFD 75
Figura 2-60 Campo de prioridad de VLAN 78
Figura 2-61 Marcado de prioridad en capa 3. 78

Figura 2-62 Recomendación de QoS 79
Figura 2-63 Gestión de tráfico por Traffic Shapping y Traffic Policing. 80
Figura 2-64 Triada de seguridad. 82
Figura 2-65 Alternativas por capas para implementar un canal seguro. 85
Figura 2-66 Implementación de AH en IPSec. 86
Figura 2-67 Implementación de ESP en IPSec. 87
Figura 2-68 Directivas básicas de Malware. 89
Figura 2-69 Diagrama de plan de Ciberseguridad en una compañía. 92
Figura 2-70 Funcionamiento de ACLs. 93
Figura 2-71 Evolución del estándar ISA99/IEC 62443. 96
Figura 2-72 Normativa ISA99/IEC 62443. 96
Figura 2-73 Proceso de manejo del riesgo NIST SP 800-82. 99
Figura 3-1 Arquitectura Red IP del sistema ITS 102
Figura 4-1 Montaje para test de herramienta 120
Figura 4-2 Grafico de test de generación de paquetes Iperf 64 bytes 121
Figura 4-3 Grafico de test de jitter Iperf 64 bytes 122
Figura 4-4 Grafico de test de generación de paquetes Iperf 768 bytes 123
Figura 4-5 Grafico de test de jitter Iperf 768 bytes 124
Figura 4-6 Grafico de test de generación de paquetes Iperf 1280 bytes 125
Figura 4-7 Grafico de test de jitter Iperf 1280 bytes 126
Figura 4-8 Topología pruebas capa de acceso 130
Figura 4-9 Grafico pruebas de convergencia MSTP 132
Figura 4-10 Grafico pruebas de convergencia SEP 133
Figura 4-11 Grafico pruebas de convergencia SEP con aumento de switches 135
Figura 4-12 Topología pruebas SEP con aumento de switches 136
Figura 4-13 Ejemplo de desconexión que no detecta VRRP 138
Figura 4-14 Topología de pruebas VRRP 140
Figura 4-15 Grafico de resultados de pruebas de convergencia VRRP 140
Figura 4-16 Topología pruebas protocolos de enrutamiento 142
Figura 4-17 Distribución de áreas pruebas OSPF 143
Figura 4-18 Grafico de resultados de pruebas de convergencia 145
Figura 4-19 Grafico de resultados de pruebas de latencia OSPF 146

Figura 4-20 Distribución de sistemas Autónomos para pruebas de convergencia BGP. .. 149
Figura 4-21 Resultados de convergencia VRRP + BGP 149
Figura 4-22 Grafico de resultados de pruebas de convergencia VRRP + BGP 150
Figura 4-23 Grafico de resultados de pruebas de latencia BGP 151
Figura 4-24 Topología para pruebas PLC con EAP 153
Figura 4-25 Configuración System Manager PLC01 155
Figura 4-26 Capturas de publicación de variables EAP. 155
Figura 4-27 Tiempo de ejecución de tarea en un ciclo CPU PLC01 156
Figura 4-28 Captura problemas de medición de jitter 157
Figura 4-29 Grafico de jitter recepción y transmisión por problema en medida 158
Figura 5-1 Distribución de anillos de la topología de la red de los túneles. 164
Figura 5-2 Trafico agregado por anillo 165
Figura 5-3 Configuración y sentido de tráfico con configuración SEP 169
Figura 5-4 Configuración VRRP propuesta 172

Capítulo 1 Introducción

Para nadie es un misterio que la pila de protocolos TCP/IP están cada vez más presentes en todas las comunicaciones que nos rodean, el crecimiento exponencial de los dispositivos conectados a internet, teniendo estimaciones para el 2023 de cuarenta mil millones de dispositivos conectado solo confirman esta alza.

Donde la penetración ha sido muchísimo más paulatina (52% al 2018), es en las redes privadas que dan servicios a los Sistemas de Control Industrial ICS (*Industrial Control System*), no pensemos necesariamente en una gran línea de producción ensamblando coches, sino en los miles de redes que existen a nivel mundial en las industrias, como las utilities, autopistas, hospitales, distribuidoras eléctricas, despliegues de misión crítica para fuerzas armadas, o plantas de automatización. La resistencia al cambio, además de, lógicamente, querer ocupar sus equipos con *Backbone* PDH/SDH y *Fieldbuses* clásicos hasta que cumplan su vida útil, es básicamente la falta de niveles de sincronismo y resiliencia que exigen este tipo de rubros y que no están de manera nativa en el mundo IP, sin embargo, la entrada de TCP/IP, y esencialmente de ethernet a la industria, ha hecho posible los deseos de las empresas que hacen uso de este tipo de redes, una excelente relación precio/performance, integración sencilla entre el área de operación y administración, posibilidad de realizar inteligencia distribuida, facilidad de soporte y una convergencia tecnológica que les permite tener una mucho mayor independencia a la hora de adquisición de equipos o escoger a sus proveedores.

Las nuevas TSN (*Time sensitive networks*) plantean un marco teórico y práctico que las lleven a latencias por debajo de 1ms y jitter menor al 1% para servicios de tiempo crítico de manera estandarizada, siendo ya una realidad de la mano de protocolos de RT-Ethernet (real time ethernet) como EtherCAT, Profinet IRT, Powerlink, etc.

En este trabajo se realiza un diseño y propuesta de configuración para una red multiservicio de un ICS que tenga un rendimiento *Soft Real Time Ethernet* (descrito en 2.3.2.1) en comunicaciones enrutadas. Para lo que se ocupará un proyecto real actualmente en desarrollo por la empresa COMSA Industrial, el cual tiene requerimientos particulares que se sumarán para la propuesta de configuración. Además, si bien, no es un requerimiento del proyecto, se plantearán recomendaciones que permitan mejorar la ciberseguridad de la red para el ICS.

1.1 Motivación:

La penetración de la pila de protocolos TCP/IP al mundo Industrial, la búsqueda de comunicaciones con un alto nivel de sincronismo y baja latencia para procesos de tiempo real, las altas exigencias de tiempos de reconfiguración bajo un segundo que permitan tener un nivel de resiliencia adecuado para prácticamente nunca parar ICSs en producción, trae como necesidad una profundización de los conocimientos de networking orientados a este tipo de redes.

Aprovechando un proyecto en curso de la empresa COMSA Industrial, el cual tiene la necesidad de presentar una propuesta de configuración, se pretende realizar un ejercicio práctico para conocer las características y protocolos del ICS que permitan llevar sus comunicaciones de la mano de protocolos abiertos o propietarios de Huawei, a obtener niveles de latencia, jitter adecuados transportar servicios RT-Ethernet a nivel de enrutamiento, rendimientos que su vez posibilitan la integración de servicios de Smart Cities o Industria 4.0.

1.2 Objetivos:

1.2.1 Objetivos generales

Realizar un diseño y propuesta de configuración para una red multiservicio para un ICS que sea capaz de transportar servicios RT-Ethernet de sistemas de control, con un alto nivel de resiliencia compartiendo tráfico con diversos Subisistemas en una red industrial.

Presentar recomendaciones de configuración de seguridad que debiese implementarse en la red industrial, utilizando como ejemplo el caso práctico.

1.2.2 Objetivos Específicos

- Profundizar conocimientos de networking orientado a los ICSs.
- Conocer aspectos relevantes de la Ciberseguridad para ICSs.
- Cumplir con los requerimientos del proyecto indicados en la presentación del caso práctico.
- Obtener en la red comunicaciones entre equipos distanciados a 4 satos de enrutamiento latencias menores a 10ms, y jitter menores al 15% para lograr un rendimiento Soft RT-Ethernet.
- Obtener convergencia a nivel de acceso por debajo de los 200ms, por debajo de los 300ms a nivel Gateway y por debajo de los 500ms a nivel de enrutamiento.
- Revisar el comportamiento a nivel de aplicación de comunicaciones RT-Ethernet entre *PLCs* (*Programmable Logic Controller*), obteniendo tiempos de respuesta y valores de jitter reales que permitan comprobar el rendimiento de la red.
- Programar una aplicación que permita ver la factibilidad de inteligencia distribuida con comunicación RT-Ethernet.
- Realizar una propuesta de configuración para la red del caso práctico.
- Realizar recomendaciones de Ciberseguridad para la red del caso práctico.

1.3 Metodología:

i. Revisar de protocolos de comunicación de las aplicaciones de la red Industrial multiservicio con el fin de obtener características, perfiles de tráfico y vulnerabilidades de seguridad.
ii. Estudiar los protocolos de comunicación de redes industriales más usados en el mercado para determinar cuál implementar en el caso práctico, tener un mejor conocimiento de las aplicaciones que los usan y obtener una base para perfilar sus tráficos de red para este y otros proyectos.
iii. Estudiar protocolos de control de redes IP a nivel de capa 2 y capa 3 del Modelo OSI, para poder tomar la decisión de cuales se podrían implementar para lograr los tiempos de latencia y de convergencia planteados en los objetivos.
iv. Revisar los aspectos más importantes de la ciberseguridad para redes industriales con el objetivo de plantear recomendaciones.
v. Revisar de generadores y capturadores de tráfico.
vi. Realizar pruebas del generador de tráfico.
vii. Realizar pruebas de convergencia a nivel de capa 2.
viii. Realizar pruebas de latencia y convergencia a nivel de capa 3.
ix. Realizar pruebas de comunicación entre PLCs, para revisar si se pudo alcanzar el rendimiento esperado de Soft RT-Ethernet
x. Presentar recomendaciones de mejoras de Ciberseguridad del caso práctico.

Capítulo 2 Antecedentes Previos

En el presente capítulo se revisan todos los aspectos relevantes para una red ICS. La profundidad en la que se aborda cada tema dependerá de la relevancia que tenga el mismo para el diseño de la red, la propuesta de configuración y la Ciberseguridad.

En las secciones 2.1 y 2.2 se define el marco teórico para el entendimiento y caracterización de los diferentes subsistemas que forman el ICS, orientando el estudio a los protocolos que forman que dan funcionamiento al Sistema Inteligente de Transporte ITS (*Intelligent Transportation Systems*) presentado en el caso práctico.

En la sección 2.3 se revisa el estado del arte de los protocolos con rendimiento RT- Ethernet con mayor participación en el mercado, lo que permitirá poder plantear posibles mejoras a la arquitectura del ITS presentado en el caso práctico.

En la sección 2.4 se define el marco Teórico para la elección de los protocolos de control en redes IP para lograr, tanto, obtener un rendimiento RT-Ethernet en comunicaciones a nivel de enrutamiento, como cumplir los tiempos de reconfiguración o convergencia exigidos en el proyecto del caso práctico, por lo que esta sección será la base fundamental para el planteamiento de las pruebas.

En la sección 2.5 se plantea los principales conceptos de Ciberseguridad y herramientas para su implementación en los ICS, lo que permitirá en conjunto con las secciones anteriores de este capítulo plantear directrices y recomendaciones de Ciberseguridad en el caso práctico.

2.1 Conceptos y protocolos básicos para Redes IP

2.1.1 Modelo OSI y TCP/IP

El modelo o arquitectura *Open Systems Interconnect* OSI desarrollado por la *International Standards Organization* ISO es un estándar desde 1980 y ha permitido el desarrollo de los diferentes fabricantes de equipamiento y software, poder converger en un funcionamiento en base a un modelo común, donde cada una de las 7 capas funciona como un servicio independiente.

La arquitectura o pila de protocolos TCP/IP reduce el modelo OSI a 4 capas, simplificando su descripción y análisis, orientándolo al punto de vista de los protocolos.

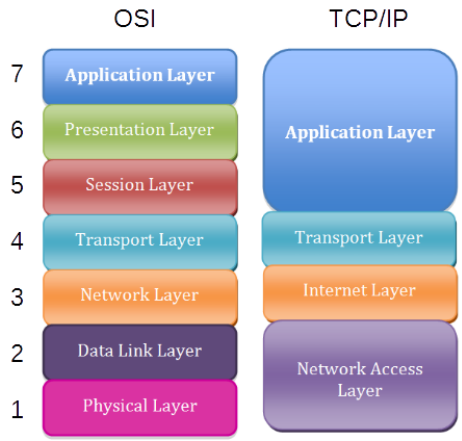


Figura 2-1 Modelo OSI y TCP/IP. [3]

2.1.2 ARP

Address Resolution protocol ARP está definido en el RFC 826, trabaja sobre las capas 2 y 3 del modelo OSI y se utiliza para encontrar la dirección física MAC (*Media Access Control*) de otro equipo de la red.

El equipo que quiere obtener la dirección envía un paquete de broadcast que incluye la dirección física e IP propia y la dirección IP del destino, el equipo que detecte que la IP de destino le pertenece, envía por unicast dirección MAC al equipo que realizo la solicitud, y con esto ya se puede entablar la comunicación.

2.1.3 ICMP

Internet Control Message Protocol ICMP está definido en el RFC 792, trabaja sobre la capa 3 del modelo OSI y se encarga de enviar reportes de error e información operativa. Algunos mensajes típicos son, host o red inalcanzable, problemas de congestión, Echo reply (ping), actualización de tablas de rutas, tiempo excedido de mensaje, etc.

2.1.4 TCP

Transmisión Control Protocol TCP definido en el RFC 793, es un protocolo de transporte orientado a la conexión.

Es el protocolo de transporte más utilizado en las redes en la actualidad, su orientación a la conexión lo hace muy útil en redes no controladas como internet. Su mecanismo se basa en que los nodos intercambian mensajes de control para confirmar recepción de mensajes, controlar errores, adaptar su flujo de comunicación ante condiciones adversas, todo con el objetivo de garantizar la entrega de los paquetes. En la figura 2-2 se puede ver el detalle de la cabecera del segmento TCP que puede tener un tamaño entre 20 y 60 bytes.

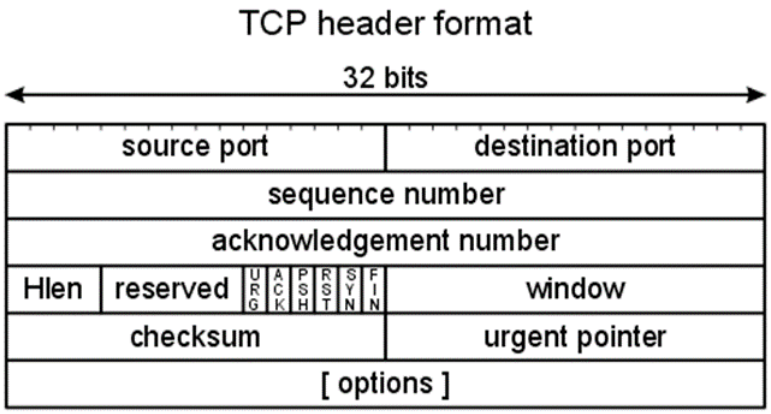


Figura 2-2 Segmento TCP. [52]

Para establecer la conexión s realiza una negociación de 3 vías o 3-handshake, done el servidor abre sus puertos de manera pasiva esperando conexiones.

i. El Cliente envía un mensaje con el flag *SYN* activo, un número de secuencia, tamaño de ventana de recepción y el mayor tamaño segmento con el que puede trabajar.
ii. El servidor responde con otro *SYN*, su propio número de secuencia, tamaño de ventana y límite de tamaño de segmento y el *ACK* del segmento recibido previamente.
iii. El Cliente recibe el *SYN ACK* y envía un *ACK* con la que la conexión queda establecida.

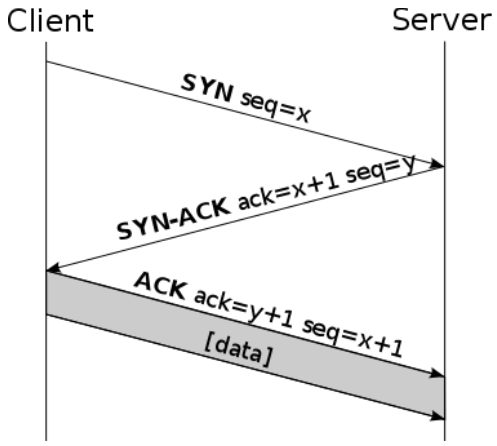


Figura 2-3 Tree-handshake. [53]

Las conexiones se cierran con el intercambio de mensajes con los flags *FIN* y *ACK* ya sea en una negociación de 3 o 4 vías o por la activación del flag de reset *RST* en alguno de los segmentos intercambiados.

2.1.5 UDP

User Datagram Protocol UDP está definido en el RFC 768, es un protocolo de transporte no orientado a la conexión. Realiza él envió de paquetes sin control alguno sin necesitar una conexión previa como TCP. Su cabecera es más pequeña que la de TCP con un largo de 8 bytes y se suele utilizar en aplicaciones de tiempo real, como videoconferencia, VoIP o RT-ethernet.

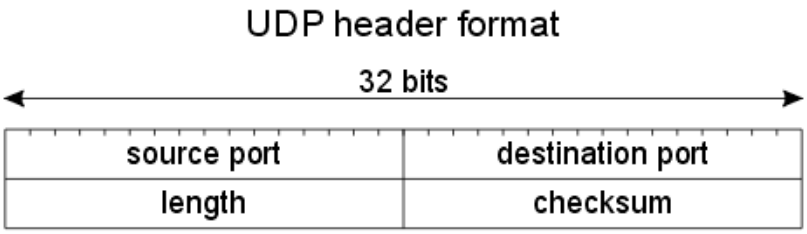


Figura 2-4 Segmento UDP [54]

2.1.6 DHCP

Dynamic Host Configuration Protocol DHCP está definido en el RFC 2131 y funciona sobre la capa de aplicación del modelo TCP/IP.

Tiene una arquitectura cliente servidor, donde el servidor se encarga de asignar las direcciones IP de manera dinámica a los clientes que la soliciten. La asignación pude ser automática asignando una IP a un cliente de manera permanente o dinámica por tiempo limitado.

Utiliza UDP en su capada de transporte, haciendo uso de los puertos 67 para el servidor y 68 para el cliente.

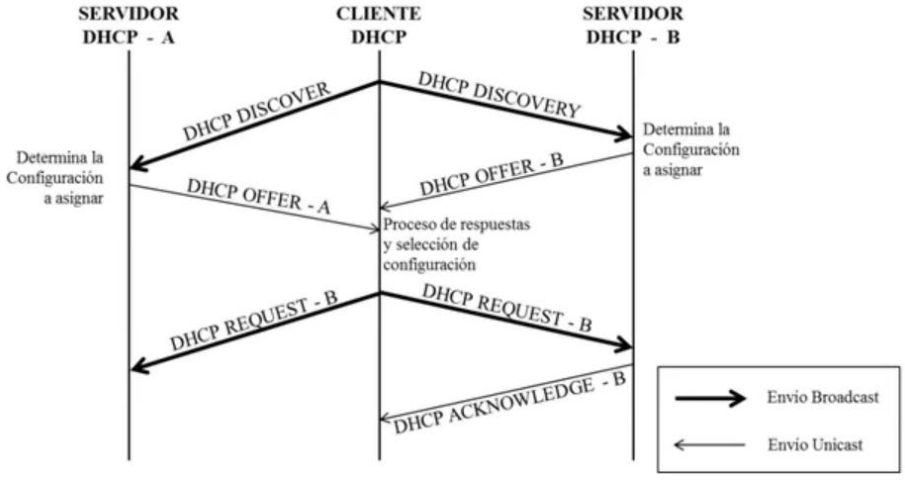


Figura 2-5 Negociación DHCP con 2 servidores. [55]

El Cliente inicia la comunicación enviando mensaje de broadcast *DISCOVER* para que algún servidor DHCP de su red o de otras redes le ofrezca una configuración. Los servidores responden con un mensaje de *OFFER* proponiendo configuraciones, el cliente elige una de las ofertas y comunica su elección con un mensaje de broadcast *REQUEST* a todos los servidores.

2.1.7 HTTP y HTTPS

Hyper Text Transfer Protocol HTTP está definido en el RFC 2616 en su versión HTTP/1.0 y el 2015 se publicó en el RFC 7540 su versión HTTP/2.0 y se encuentra disponible en la mayoría de los navegadores. Trabaja sobre la capa de aplicación del modelo TCP/IP y ocupa TCP en su capa de transporte, habitualmente utilizando el puerto 80.

HTTP se basa en una arquitectura cliente - servidor y solicitud - respuesta. Son varios los tipos de solicitudes o "verbos" que permiten al cliente realizar acciones sobre los recursos del servidor, algunos de los más populares son *GET* para obtener un recurso, *HEAD* para obtener la metadata de página web, *POST* para el ingreso de datos. Dentro de la metadata más más habitual se encuentra el lenguaje que se utilizara, detalle del navegador web, tipo de meta data (html es el más común), estado de la conexión, etc.

La versión segura de HTTP es *Hyper Text Transfer Protocol Secure* HTTPS que está definido en el RFC 2818. Básicamente incorpora seguridad entre las capas de transporte y aplicación usando *SSL* o *TLS* (descritos en 2.6.1.4.2.1) para cifrar los datos.

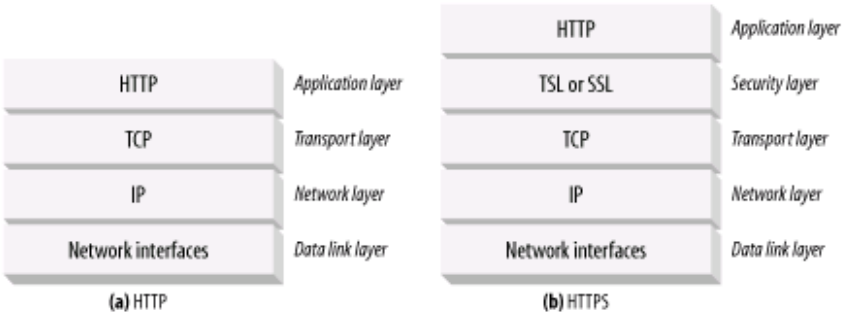


Figura 2-6 Pila de protocolos ocupados por HTTP y HTTPS [56]

2.1.8 DNS

Domain Name Service DNS, se refiere tanto al servicio de Nombres de Dominio como al servidor que ejecuta dicha función. Trabaja sobre la capa de aplicación de la pila de protocolos TCP/IP utilizando principalmente UDP en su capa de transporte.

Es un fundamental para el funcionamiento de Internet y precursor de su desarrollo. Su función principal es la de traductor nombre de dominio a direcciones IP, pudiendo acceder a los recursos sin la necesidad de memorización o almacenamiento de cada dirección en cada host que quiere acceder a internet.

2.1.9 Parámetros de Desempeño

Existen 3 formas básicas de medir rendimiento de una red, Perdida de paquetes, latencia y jitter. Además, se agrega el tiempo de restablecimiento o convergencia de la red, debido a los requerimientos planteados en el caso práctico.

i. **Latencia:** La latencia está definida en el RFC 1242. Es la suma de los retardos producidos dentro de la red que afectan a un paquete desde un nodo origen hasta un destino. Dentro de los retardos está el procesamiento de cada equipo intermedio y el tiempo de propagación por el medio físico.

ii. **Jitter:** Es la variación del tiempo de llegada de paquetes en una red, la cual puede ser producida por congestión, por diferentes rutas que tomen los paquetes o debido a que el envío no se realiza de manera cíclica. Es habitual que este valor se represente a traves de un porcentaje de variación.

iii. **Perdida de paquetes:** Es la cantidad de paquetes enviados por el emisor que no fueron recibidos por el receptor, habitualmente este valor se indica en base a porcentaje de paquetes perdidos sobre el total de paquetes enviados

iv. **Tiempo de convergencia:** La convergencia en redes es el tiempo que le toma a la red poder redirigir el tráfico al producirse una falla. Dentro de este tiempo está la detección de la falla, la propagación de esta al resto de equipos de la red, la decisión de que acción tomar para el redireccionamiento del tráfico y finalmente implementar dicha acción.

2.2 Protocolos para las aplicaciones del ICS planteado en el caso práctico

2.2.1 SNMP

Simple Network Management Protocol SNMP es un protocolo para la gestión de redes que trabaja por encima de la capa de transporte, es compatible con la mayoría de los equipos de networking existentes en el mercado, además en la actualidad diversos dispositivos como enlaces de microondas, estaciones base, servidores, cámaras, rectificadores, UPSs, PLCs, etc. También son compatibles con él protocolo.

Las comunicaciones SNMP se darán siempre entre una unidad administración *Network Management System NMS* y un equipo administrado que tendrá en funcionamiento un agente encargado de gestionar las solicitudes del NMS y enviar mensajes hacia este.

Como se puede observar en la figura 2-7 El NMS tendrá 2 tipos de solicitudes básicas hacia el agente, *Get* para solicitar lectura de cierta variable u objeto y *Set* para escribir en la misma si es que lo permite (no puede editarse la temperatura de un equipo).

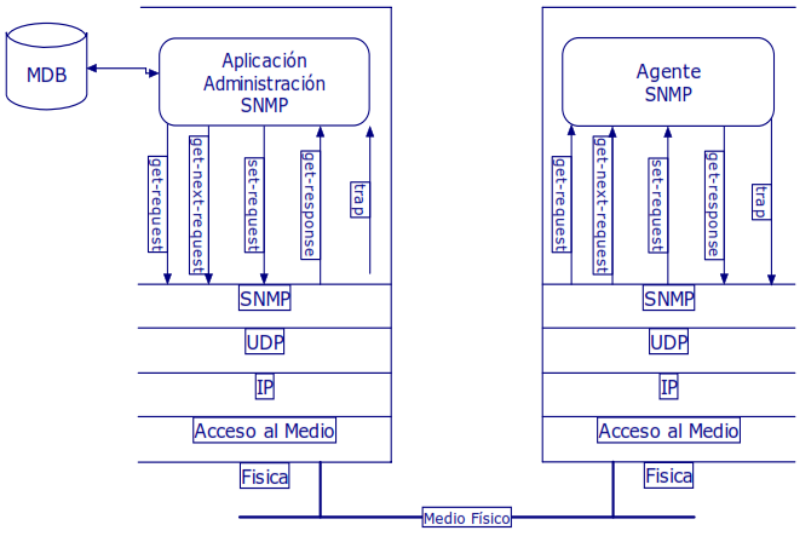


Figura 2-7 Detalle de funcionamiento por capas SNMP [57]

SNMP también permite configurar en los equipos gestionados el envío de mensajes desde el agente SNMP hacia el NMS sin ser solicitados, con el objetivo de informar inmediatamente alarmas, ya sea por posibles anomalías o debido a que variables crucen cierto umbral, por ejemplo, temperatura, uso excesivo de memoria, caída de una interfaz o adyacencia, etc. A estos mensajes se les denomina TRAPS.

Cada variable dentro del equipo administrado estará identificada por una cadena de tamaño fluctuante de números que forman su identificador *OID (Object IDentifier)* que a se agrupan en la base de datos de información de gestión *MIB (Management Information Base).*

Los OIDs se organizan en una jerarquía tipo árbol dentro de la MIB, donde los 4 primeros números 1.3.6.1 estarán presentes en todos los OIDs de las MIBs. Existen MIBS estandarizadas definidas por *IETF (Internet Engineering Task Force)* que pueden encontrarse en el RFC 1213, RFC 2790 y comienzan con la ramificación 1.3.6.1.**2**.1 y también las hay privadas, definidas por cada fabricante, que comienzan con la ramificación 1.3.6.1.**4**.1.

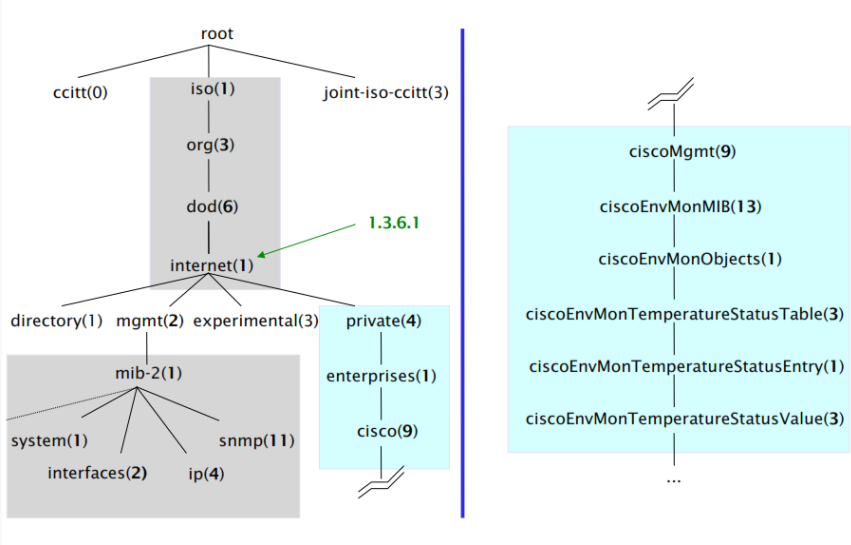


Figura 2-8 Arquitectura de OID. [58]

SNMP puede implementarse tanto usando TCP como UDP en su capa de transporte, siendo este último mucho más común, principalmente dado su menor tamaño de cabecera. En la actualidad existen 3 versiones de SNMP y todas utilizan el puerto UDP 161 para las solicitudes y el puerto 162 para los TRAPs.

La versión 1 (SNMPv1) está definida en los RFCs RFC1155, RFC1156, RFC1157 y la versión 2 (SNMPv2 y SNMPv2c) en los RFCs RFC1901, RFC1908, RFC2578, siendo su principal diferencia de su versión anterior la incorporación de nuevos tipos de solicitudes que optimizan la comunicación, como el comando *GetBulk* que permite solicitar o enviar varios OIDs con un solo mensaje. Ambas versiones incorporan el concepto *Community* (comunidad), que básicamente es una contraseña en texto plano presente en la cabecera del paquete SNMP, que utilizan el agente SNMP y el NMS para autenticar el envío de información.

En la figura 2-9 puede verse el detalle de los diferentes campos que tienen los mensajes el SNMP v1 y SNMP V2 más comunes.

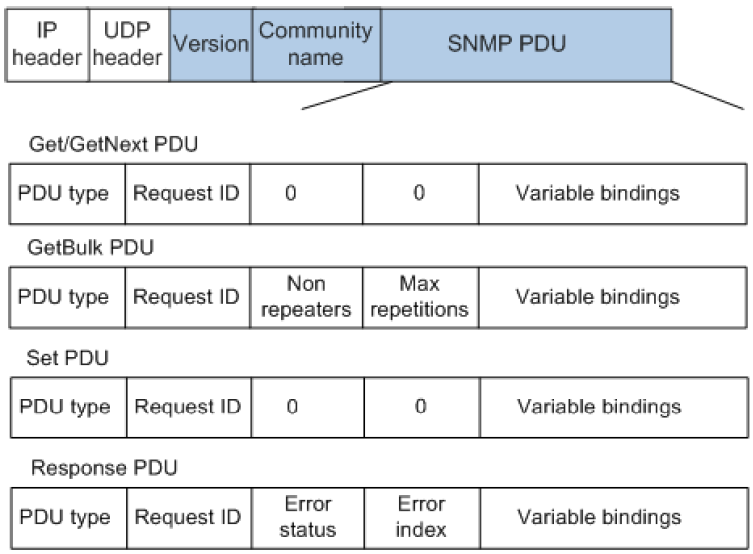


Figura 2-9 Mensaje SNMPv2. [60]

En la tabla 2-1 se indica una pequeña descripción y tamaño de cada campo de los mensajes el SNMP v1 y SNMP V2.

Campo	**Descripción**	**Tamaño**
Versión	Versión de SNMP que se está ocupando	4 bytes
Community Name	Nombre de comunidad para autenticación	Variable
PDU Type	Tipo de PDU, Set, Get, Trap, etc	4 bytes
Request ID	Identificador de la solicitud	4 bytes
Non repeater / Max Repetitions	Cantidad de objetos o variables a leer	8 bytes
Error Status	Reporte de errores, un valor de 0 indica que no hay errores	4 bytes
Error Index	Indica el objeto/ variable que se encuentra en error	4 bytes
Variable Bindings	Campo donde están los valores de cada OID	Variable

Tabla 2-1 Detalles de los campos en mensaje SNMPv2

Es importante indicar que los Traps en SNMPv2 tienen el mismo formato que el comando SET

La versión 3 (SNMPv3) está definido en los RFCs RFC3410 - RFC3418 y busca mejorar los problemas de seguridad de las versiones anteriores, incorpora dentro de sus mejoras, funciones de hash *MD5* y *SHA* (descritos en 2.6.1.3.2) para las contraseñas y cifrado tipo *AES*, *DES* y *3 DES* (descrito 2.6.1.3.1) para las comunicaciones, pudiendo funcionar de 3 modos:

- *NOAuth NoPriv*: Sin autenticación, sin cifrado
- *Auth NoPriv:* Autenticación, sin cifrado

- *AuthPriv:* Autenticación y cifrado.

Los mensajes de SNMPv3 incluyen varios cambios en la estructura de su cabecera en comparación a sus versiones anteriores, ampliándola con el fin de incrementar la seguridad. La estructura del mensaje puede verse en la figura 2-10.

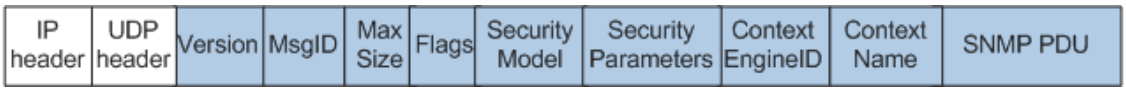


Figura 2-10 Mensaje SNMPv3 [60]

En la tabla 2-2 se indica una pequeña descripción y tamaños aproximados de cada campo de los mensajes el SNMPv3.

Campo	Descripción	Tamaño
Versión	Versión de SNMP que se está ocupando	4 bytes
MsgID	Número de secuencia de la solicitud	4 bytes
Max Size	Tamaño máximo que soporta el emisor	4 bytes
Flags	Bits de control	1 byte
Security Model	Debe ser el mismo en el NMS y el agente	4 bytes
Security Parameters	Parametros de seguridad, parámetros de autenticación, cifrado, etc.	Variable ~ 70 bytes
Context Engine ID / Context Name	Contexto de datos de la PDU	Variable ~ 30 bytes
PDU	Variables	Variable

Tabla 2-2 Detalles de los campos en mensaje SNMPv3

2.2.2 RTP

Real-time Transport Protocol RTP está definido en el RFC1889 y en su segunda versión en el RFC 3550. Se creó con el objetivo de transportar flujos multimedia como VoIP, Streaming, CCTV, etc., sobre redes sin *QoS (Quality of Service)* como internet.

Utiliza UDP para su transporte, ocupando siempre un número de puerto par. No realiza recuperación de errores y tampoco garantiza la entrega de los mensajes, dejando esta tarea de ser necesaria, a las capas superiores y *RTCP* (descrito en 2.2.3).

En la figura 2-9 se muestra el detalle del datagrama RTP, donde pueden verse los siguientes campos en su cabecera.

- *Sequence Number:* El número de secuencia de los datagramas, le permite al receptor identificar el flujo, reconstruir el datagrama, descartar duplicados, etc.

- *Time stamp:* La marca de tiempo permite la sincronización de los flujos de datos.
- *Source Identifier:* El Identificador le permite al receptor distinguir entre flujos de origen distinto.

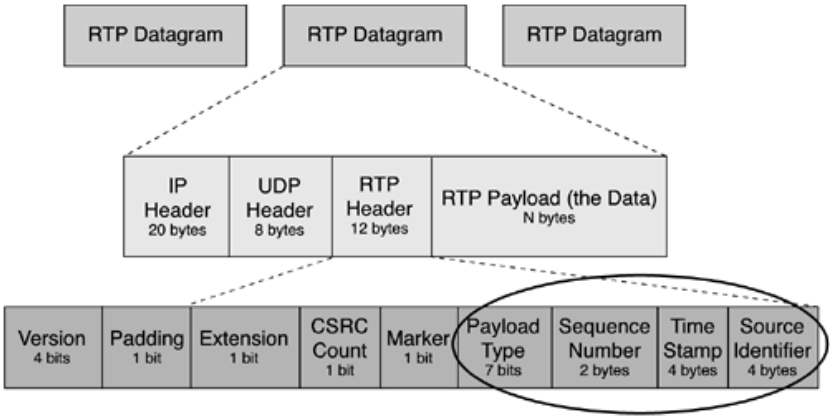


Figura 2-11 Detalle mensaje RTP

- *Payload Type:* Es un número que identifica el tipo de Codec (descrito en 2.2.4.1).) que está transportando RTP, ya sea audio video. En el RFC 3551 se define el número para los diferentes códecs, entre los más conocidos se encuentran H.261, *G.722, G.711*(detalle en 2.2.4.1). También existen otra sería de RFCs que singularizan los formatos del área de datos del datagrama RTP como los son para video el RFC 6184 para *H.264* (descrito en 2.2.5.1) y RFC 6416 para MPEG-4.

2.2.3 RTCP

Real-Time Control Protocol RTCP se ocupa en el plano de control de las sesiones multimedia que utilizan RTP, por cada sesión RTP existente se abrirá una sesión RTCP paralela y bidireccional utilizando UDP en la capa de transporte ocupando un número de puerto impar siguiente, al puerto par ocupado por RTP.

En RTCP se realizan transmisiones periódicas sobre aspectos relevantes de la comunicación, como el monitoreo las entregas, estadísticas de latencia, jitter y perdida de paquetes y también información relevante de los participantes de la sesión como lo son sus identificadores, que permite en una sesión multimedia con varios usuarios participantes detectar cuando algún usuario entra o sale de la sesión.

2.2.4 VoIP

Voz sobre IP, como su nombre lo indica es una tecnología que permite transmitir la voz utilizando la pila de protocolos TCP/IP, lo que permite entre otras cosas hacer más de una llamada por la misma línea, ampliar la cantidad de usuarios telefónicos dentro de una empresa, incorporar servicios como llamada en espera o identificación de manera gratuita, etc.

La transmisión de VoIP tiene 3 partes fundamentales, los protocolos de establecimiento de llamadas como *SIP y H323* (descritos en 2.2.4.2.1), los protocolos RTP y RTCP para cursar las llamadas luego que la sesión se ha establecido y los códecs que permiten la codificación y compresión del audio.

2.2.4.1 **CODECs**

La voz o cualquier otro tipo de señal proveniente del mundo físico debe codificarse en bits para poder ser transmitida por medios digitales. Codecs se denomina a las técnicas de **cod**ificación / **dec**odificación utilizadas para la transmisión de la voz o video que además se encargan de realizar una compresión de los datos con el objetivo de un menor uso de ancho de banda y/o carga computacional. En la tabla 2-3 se observan los Codecs de la ITU () para la transmisión y recepción de audio.

Codec & Bit Rate	Codec Sample Size	Codec Sample Interval	MOS	Voice Payload Size	Voice Payload Size	Packets Per Second (PPS)	Bandwidth Ethernet
G.711 (64 Kbps)	80 Bytes	10 ms	4.1	160 Bytes	20 ms	50	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	20.8 Kbps
G.726 (32 Kbps)	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	55.2 Kbps
G.726 (24 Kbps)	15 Bytes	5 ms			20 ms	50	47.2 Kbps
G.728 (16 Kbps)	10 Bytes	5 ms	3.61	60 Bytes	30 ms	33.3	31.5 Kbps
G722_64k (64 Kbps)	80 Bytes	10 ms	4.13	160 Bytes	20 ms	50	87.2 Kbps

Tabla 2-3 Codec para VoIP ITU [61].

Dentro de la tabla se indica el *MOS* (*Mean Opinion Score*) que indica la calidad de la comunicación que logra cada Codec.

2.2.4.2 **Protocolos para el establecimiento de llamadas VoIP**

Los 2 estándares más usados para el establecimiento de llamadas VoIP son H.323 y SIP, siendo este último más popular en la actualidad dada su facilidad de implementación.

2.2.4.2.1 H.323

El estándar H.323, es un conjunto de protocolos propuestos por la *ITU (International Telecommunication Union)* para comunicaciones multimedia sobre redes IP. Su creación se basó

en estándares predecesores que incluyen H.320 y Q.931. Es más antiguo y complejo que su principal competidor SIP.

Hace uso de los procedimientos de señalización contenidos en el protocolo H.245 para el establecimiento y finalización de llamada y el protocolo H.225 para la señalización y control de la misma.

Se sirve del protocolo RTP y puede utilizar SSL para seguridad en la capa de transporte, codifica los mensajes en formato binario compacto, adecuado para redes de gran ancho de banda.

2.2.4.2.2 SIP

Session Initiation Protocol SIP fue desarrollado por la IETF y en noviembre del año 2000 fue aceptado como protocolo de señalización por la *3GPP (3rd Generation Partnership Project*). Es mucho más simple que H.323 y puede trabajar con cualquier Codec registrado en la *IANA (Internet Assigned Numbers Authority)* o los Codecs de mutuo acuerdo *ASN.1(Abstract Syntax Notation One)*.

Es un protocolo de señalización que tiene la capacidad de iniciar, modificar o finalizar sesiones multimedia con uno o más usuarios utilizando una red basada en protocolos TCP/IP, funciona sobre la capa de aplicación y puede trabajar tanto con TCP como UDP en su capa de transporte

Utiliza en texto codificado en ASCII, incorpora elementos de HTTP como las cabeceras, códigos de error y forma de operar, basa su funcionamiento en dos entidades generales, los agentes y los servidores.

Los Agentes Usuario Cliente (*UAC User Agent Clients)* son quienes envían las peticiones SIP a los Agentes Usuario Servidores (*UAS User Agent Servers*) quienes reciben las peticiones y envía las respuestas. Todos los usuarios son identificados por direcciones SIP con la forma usuario@host.

Hay 3 tipos básicos de servidores en SIP, los servidores Proxys actúan como dispositivos intermedios pudiendo actuar como UAC o UAS pudiendo hacer peticiones a nombre de otros clientes, redirigir peticiones a otro servidor además pueden realizar funciones autenticación, control de acceso a la red, etc. Los servidores de Redirección entregan información de direcciones para el siguiente salto a los clientes y los servidores de Registro que procesan peticiones y almacenan información de localización de los UAC.

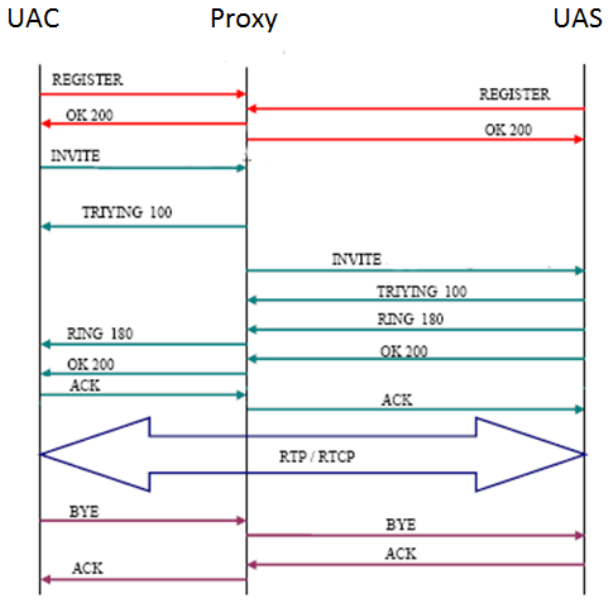


Figura 2-12 Flujo de llamada SIP. [64]

Una sesión exitosa se forma luego del envío de los mensajes *INVITE* y *ACK*, si el receptor acepta la llamada contesta con un *OK* y *BYE* si la rechaza. Si la respuesta es *OK* se inicia una sesión entre los dos puntos y comienza el flujo de información sobre RTP. En la figura 2-12 puede verse en detalle el flujo de una llamada con servidor proxy.

Por defecto el protocolo SIP ocupa los puertos TCP/UDP 5060, 5061.

2.2.5 CCTV Circuito cerrado de televisión

Los circuitos cerrados de televisión son sistemas de videovigilancia para supervisar la actividad de una zona determinada. Actualmente la gran mayoría de las cámaras de los sistemas CCTV cuentan con el hardware y software necesario para poder transmitir sus datos utilizando la pila de protocolos TCP/IP.

Tradicionalmente la transmisión de video en tiempo real consume gran cantidad de recursos en comparación con la transmisión de otros tipos de datos, los aspectos más influyentes tanto en el almacenamiento como en el ancho de banda de los datos de video son:

- Codec de compresión
- Complejidad de la escena
- Resolución
- FPS

Complejidad de la escena: Entre más variaciones de movimiento y texturas existan, mayor será este, valor, arboles, flores, animales, arbustos, rejas, personas caminando o vehículos en movimientos incrementaran tanto el ancho de banda como el espacio de almacenamiento requerido.

Resolución: la resolución indica la cantidad de "puntos" que tiene la imagen o el video, se suele expresar ya sea como la cantidad de pixeles totales como 2MP (2 Mega Pixeles) o en función de la cantidad de pixeles verticales y horizontales como 1920 x 1080. Entre mayor sea este valor, mayor será el ancho de banda consumido para la transmisión y mayor el espacio de almacenamiento que se necesitará

FPS: Fotogramas por segundo, son la cantidad de imágenes por segundo que procesa una cámara, entre mayor sea este valor, mayor será la calidad del video y por consiguiente ocupara más ancho de banda al ser transmitido y mayor espacio de almacenamiento.

Espacio de color: Los colores de una imagen pueden representarse de manera monocromática, en colores RGB (Red Gree Blue) donde se forman el color de cada pixel en función de proporciones de estos de estos 3 colores y YCbCr (luminancia o luma) y las diferencias de color Cb y Cr. La cantidad de bits que se usen para definir cada uno de los componentes de las 3 representaciones entrega una mejor imagen.

Compresión: Un video sin comprimir consumiría una enorme cantidad de datos, por ejemplo, una imagen en alta definición HD de 1280 x 720 pixeles, usando 8 bits por componente RGB, a 30 fps arrojaría un flujo de datos de más de 660 Mbps, haciendo inviable económicamente tanto su almacenamiento como su transmisión por la red, por lo que la compresión del video es un aspecto mandatorio en cualquier implementación.

$$1280x720\left(\frac{pixel}{frame}\right)x\ 30\left(\frac{frame}{s}\right)x3\left(\frac{color}{pixel}\right)x\ 8\left(\frac{bits}{pixel}\right) = 663{,}55M\left(\frac{bits}{s}\right) = 663{,}55Mbps$$

En las cámaras de los sistemas CCTV será habitual encontrarse con 2 tipos de configuración para la transmisión de los datos que son:

CBR: Constant Bitrate, Es habitual encontrar en las cámaras de los sistemas CCTV la posibilidad de una salida a una tasa constante de bits, lo que podría traer como consecuencia una disminución en la calidad de imagen producto de que muchos cambios en la escena que se esté transmitiendo producirán un incremento en el ancho de banda que se necesita, pero trae como ventaja que no habrán peaks de tráfico, por lo que su uso es habitual en redes con ancho de banda limitado

VBR Variable Bitrate, La cámara enviará una tasa de tráfico que variará según la complejidad de la escena y la calidad que se le configure.

2.2.5.1 **H.264/AVC (Advanced Video Coding) o MPEG-4 Part 10:**

H.264/AVC es un Codec desarrollado por la ITU, que entrega un gran nivel compresión del video con baja perdida, siendo actualmente es el estándar más utilizado en la industria. Define un formato y sintaxis para video comprimido y como este se decodifica para reproducirlo, pero no define como codificar dejando está tarea a cada fabricante.

Si bien el proceso del Codec es bastante complejo y posee más de una etapa, a grandes rasgos se puede indicar que basa su compresión en la construcción de un *GOP* (*Group Of Pictures*) compuesto por tres tipos de *frames* (imagenes):

- I-Frame o *Intra-Frame*, es un frame codificado sin ninguna referencia y podría considerarse un frame sin comprimir, como es lógico cada GOP comienza con un I-Frame.

- P-Frame - *Predictive Frame*, usa información previa para ser codificada, no teniendo que incluir datos nuevos si es que parte de la escena ha permanecido estática, por ejemplo, en una cámara de vigilancia fija que tenga una escena más menos constante, existirían muchos P-frames, logrando un nivel mucho mayor de compresión.

- B-Frame o *Bi predictive inter frame*, utiliza información tanto de las I-Frames y las P-Frames, tanto pasadas como futuras. Generalmente no se usan en la transmisión de video sobre TCP/IP debido a la latencia adicional que genera debido a el uso de tramas futuras que deben estar almacenadas en algún buffer.

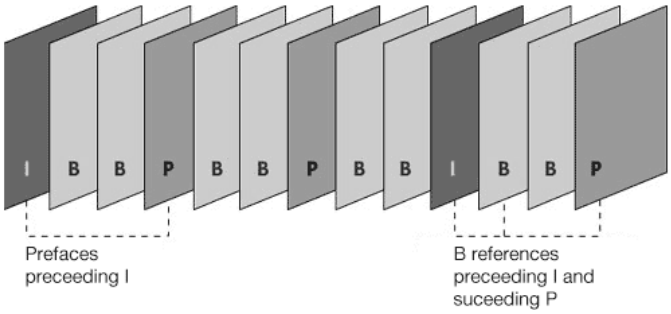


Figura 2-13 GOP con sus diferentes tipos de frames. [68]

En el caso de tener una cámara en continuo movimiento o un fondo cambiante el proceso anterior no lograría un alto nivel de compresión debido al continuo cambio de las características de los frames. Para compensar lo anterior se utiliza un proceso de compensación de movimiento basado en que la mayoría de los pixeles del frame se pueden encontrar en el frame anterior inclusive si ha existido movimiento en este, por lo que si un bloque de pixeles es encontrado en otra posición simplemente se mueve a la nueva ubicación sin la necesidad de volver a transmitir todo el frame nuevamente.

La transmisión de los datos comprimidos será por RTP, el detalle de la implementación está descrito en el RFC 6184.

2.2.6 Modbus TCP

Modbus TCP (Modicon Bus TCP) es un protocolo desarrollado por Schneider Electric, que adapta el tradicional Modbus RTU o ASCII montado sobre RS-485 para su funcionamiento en redes basadas en TCP/IP.

Es completamente compatible con la pila de protocolos TCP/IP sin modificaciones, funcionando sobre la capa de aplicación del modelo OSI, ocupa TCP en su capa de transporte y soporta conexiones con cualquier tipo de topología. Ocupa una filosofía Cliente-Servidor, en el mismo sentido que el Maestro-Esclavo del Modbus tradicional, carece de sincronismo por lo que no tiene un enfoque ni capacidades de establecer determinismo en sus comunicaciones para trabajar en tiempo real a menos que se logre por parte de las características propias de la red, por lo que es más adecuado para visualización y adquisición de datos desde sistemas de orden superior como *HMI*s (*Human Machine Interface*) o *SCADA*s (*Supervisory Control And Data Acquisition*) o para comunicación entre controladores y PLCs que no necesiten un rendimiento de tiempo real.

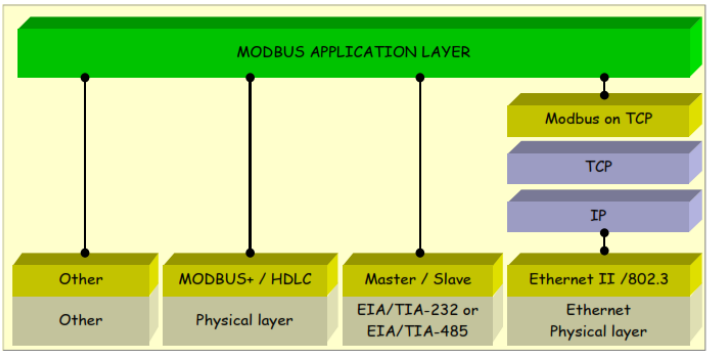


Figura 2-14 Pila de protocolos Modbus tradicional y ModbusTCP. [32]

Debido a la facilidad en su implementación y bajo coste, cuenta con una gran cantidad de productos estandarizados para su uso y es uno de los protocolos preferidos en los ICSs por su gran nivel de compatibilidad.

Como ocupa TCP en su capa de transporte, el protocolo es orientado a la conexión, en caso de que un mensaje desde el servidor no sea recibido correctamente por el Cliente, este lo vuelve a solicitar, todos los servidores (esclavos) estarán escuchando en el puerto TCP 502 las solicitudes del cliente (maestro).

El mensaje Modbus TCP tiene 6 campos importantes, cuatro de ellos incluidos en la cabecera Modbus *Application Protocol Header* (*MBPA*) de 7 bytes que no está presente en los mensajes Modbus RTU o ASCII.

Campo	Descripción	Tamaño
Transaction Identifier	Identificador para la transacción de datos entre el cliente y el servidor, se utiliza para que el cliente pueda identificar entre las diferentes conexiones que tenga, como se da entre un HMI o PLC con diferentes controladores subordinados.	2 bytes
Protocolo Identifier	Se establece como 0 para Modbus.	2 bytes
Length	Largo total en bytes de los campos Unit ID, Function Code y Data	2 bytes
Unit ID	Es el identificador o dirección del servidor (esclavo)	1 byte

Tabla 2-4 Detalle de Cabecera ModbusTCP

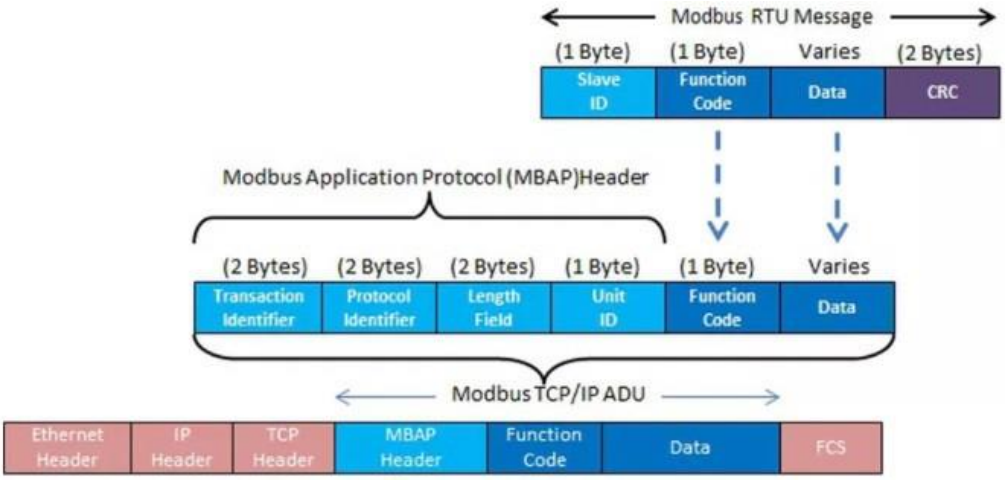


Figura 2-15 Mensaje ModbusTCP y relación con Modbus tradicional

Al igual que en el Modbus tradicional ModbusTCP mapea la memoria interna del equipo que tiene en funcionamiento el protocolo en 4 áreas de registros distintas indicadas en la tabla 2-4, *Función Code* indicará el tipo de registro y la acción a realizar sobre este, pudiendo leer o escribir uno o varios registros.

Registro	**Bits del registro**	**Tipo de acceso**
Discrete input	1 bit	Lectura
Coil (digital output)	1 bit	Lectura /escritura
Input register	16 bits	Escritura
Holding register	16 bits	Lectura /escritura

Tabla 2-5 Tipos de registros Modbus / Modbus TCP

El campo Data difiere levemente si es una trama de solicitud del cliente o de respuesta desde el servidor.

- El cliente divide en 2 subcampos el primero para indicar la dirección de inicio de la acción a realizar indicada por el *Fuction Code* y el segundo es el número de registros que serán afectados a partir de la dirección de inicio
- El Servidor también divide en 2 subcampos, el primero indica el número de bytes para responder al cliente y el segundo los datos en sí, estados discretos de entradas o salidas, valores internos de memoria, variables análogas, etc.

Existen muchos *Function Code* distintos que permiten efectuar diferentes formas de efectuar la escritura y lectura de registros, lo que hará variar la eficiencia de la comunicación y variará el tamaño del mensaje de solicitud. En la tabla 2-6 se indican los más importantes, donde ***N*** será igual al número de registros que se escribirán/leerán.

Function Code		Tamaño de campo Function Code de solicitud
Read Coils	01	5 bytes
Read Discrete Inputs	02	5 bytes
Read Holding Registers	03	5 bytes
Read Input Register	04	5 bytes
Write Single Coil	05	5 bytes
Write Single Register	06	5 bytes
Write Multiple Coils	15	6 bytes + N x 1 byte
Read/Write Multiple Registers	23	10 bytes + N x 2 bytes

Tabla 2-6 Function Code más utilizados

En [32] se puede encontrar el detalle de la implementación del protocolo y de cada *Function Code*.

2.3 Redes de comunicación para ICS y protocolos RT-Ethernet

Cada año que pasa la pila de protocolos TCP/IP ha ido tomando una mayor preponderancia en el mercado de las comunicaciones para ICS, su estandarización de facto, protocolos abiertos y lo económico de su hardware, han ido llevando el mundo de las redes industriales poco a poco hacia el. En la actualidad todos los fabricantes de equipos de automatización cuentan con ethernet como protocolo en la capa de enlace, variando su implementación según el requerimiento.

La implementación de ethernet permite la integración completa de la industria en un solo protocolo de base, pudiendo realizar una interconexión en todos los niveles de la empresa con mucha facilidad y flexibilidad, desde el nivel de sensores y actuadores, pasando por el *SCADA*, hasta los niveles administrativos y de planificación MES (*Manufacturing Execution Systems*) y ERP (*enterprise resource planning*).

Figura 2-16 Niveles de organización de los sistemas en un ICS. [71]

La penetración de ethernet en el mundo industrial ha sido lenta pero sostenida, vislumbrándose que la tendencia solo va al alza. el 2018 según el estudio de mercado de la empresa HMS [39] (Principal proveedor independiente de productos para la comunicación industrial) los protocolos basados en ethernet desplazaron a los fieldbuses clásicos como modbus o profbus, siendo los protocolos Ethernet/IP y Profinet lo que cuentan con las mayores cuotas de mercado, protocolos impulsados por Rockwell y Siemens respectivamente, que son dos de los fabricantes con mayor tradición y tamaño en el mercado.

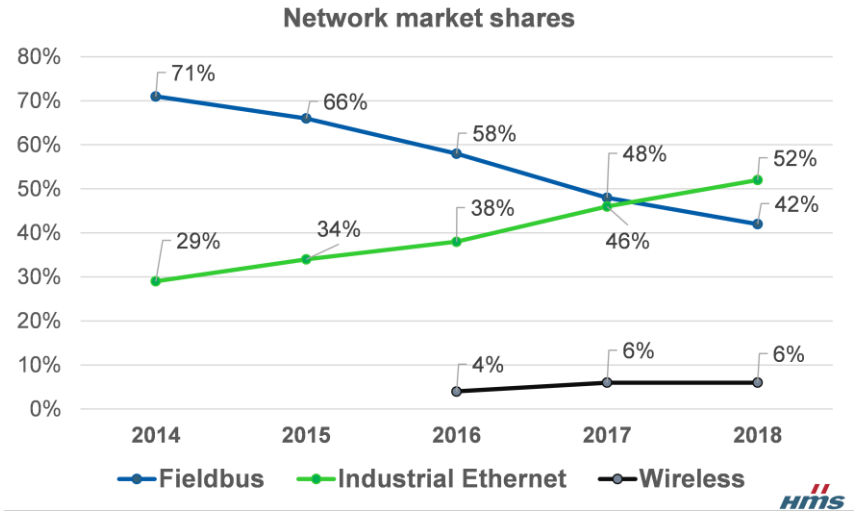


Figura 2-17 Tendencias de mercado de los estándares en comunicaciones industriales.[39]

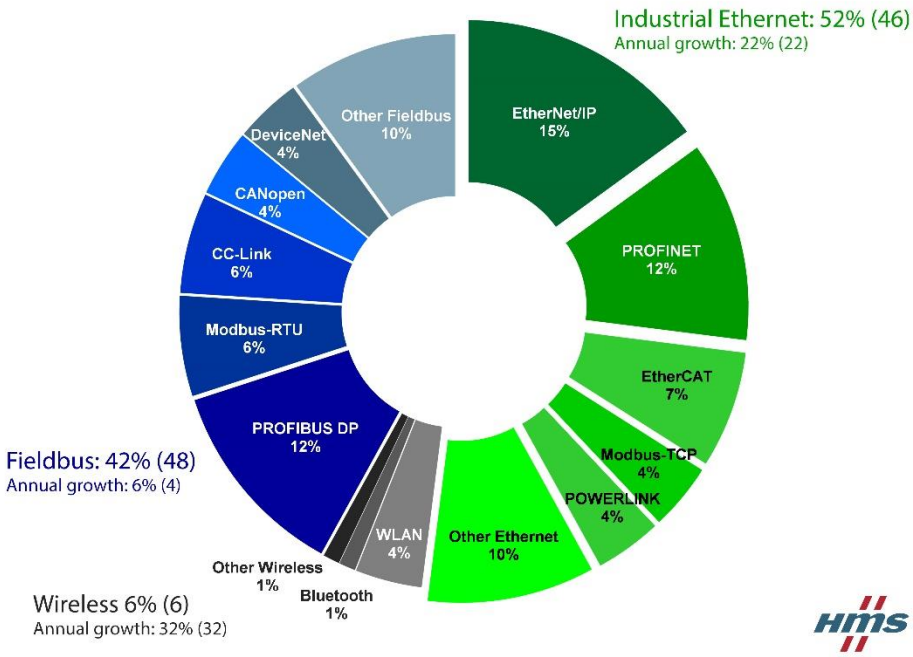


Figura 2-18 Cuotas de mercado de protocolos de comunicaciones industriales. [39]

2.3.1 Diferencias entre sistemas IT tradicionales e ICS

La penetración de la pila de protocolos TCP/IP en los ICS no ha estado exenta de problemas, la gran cantidad de protocolos propietarios y la diferencia en la naturaleza los sistemas ICS con los TI tradicionales, han contribuido la lentitud de la implementación, algunas de las diferencias más relevantes que deben tomarse en cuenta se indican en la tabla 2-7.

Campo	Sistemas IT	Sistemas ICS
Comunicaciones	• No es necesario tiempo real, tolera alto jitter y latencia • En general Necesita alto throughput • Utiliza protocolos estándar de la pila TCP/IP • Volúmenes de tráfico variables en horas del día	• Habitualmente necesita tiempo real con baja latencia y jitter. • En general necesita poco throughput • Existen gran cantidad de protocolos propietarios o que no son tradicionales en las redes TI • Pueden ocuparse otros tipos de acceso al medio como radio frecuencia o satelital. • Poca variación en volumen de tráfico dentro del día.
Disponibilidad	• En general Pueden reiniciarse los equipos. • La redundancia es opcional • Instalación de parches, actualizaciones o upgrades de software no es crítica y depende de los especialistas TI. • En general tolera reconfiguraciones por falla entre 1-60 segundos • Acceso sencillo a los equipos. • Tiempos de reparación pueden llevar días	• Reinicios de equipos no son tolerados y en caso de necesitarse debe planificarse con el tiempo necesario. • La redundancia es mandataria. • La instalación de parches, actualizaciones o upgrades de sofwares debe ser planificada con tiempo revisando la implicancia sobre otros sistemas y con diversos especialistas. • Las reconfiguraciones por falla deben estar por debajo de 1 segundo. • Puede ser dificultoso el acceso a los equipos debido a que pueden estar instalados en campo compartiendo gabinetes con otros equipos. • Los tiempos de reparación deben ser breves (horas) y pueden tener alto impacto económico. • Deben soportar altas temperaturas, presencia de polvo y humedad. • Alta tolerancia la interferencia electromagnética
Otros	• Ciclo de vida de la red de 3-5 años. • Gran cantidad de proveedores	• Ciclo de vida de la red de 10-15 años. • Algunos componentes pueden ser suministrados por pocos o solo un proveedor • Actúan sobre el mundo físico por lo que su falla puede implicar daños a personas o procesos.

Tabla 2-7 diferencias entre sistemas IT e ICS

2.3.2 Estado del arte de los protocolos RT-Ethernet para ICS

A continuación, se realizará una revisión de los protocolos para la comunicación de dispositivos en tiempo real que es esencialmente ocupado por PLCs de diferentes gamas y tarjetas remotas de entradas y salidas.

2.3.2.1 Clasificación de protocolos ethernet industriales según rendimiento

Según el rendimiento es habitual clasificar las comunicaciones Industriales en 3 grupos *No Real Time, Soft Real-Time* y *Hard Real Time* ethernet, en base los valores de jitter y latencia que logran. Según el fabricante los valores para cada clasificación varían levemente, en este documento se tomarán de base los valores de latencia y jitter indicado por Siemens que se describen en el punto 2.3.3.2.

i. **Estándar o no Real Time:** Se utiliza en comunicaciones no deterministas donde el tiempo no es crítico, por ejemplo, envío de datos a sistemas de orden superior como HMIs, transferencia a plataformas TI (IT Information Technology), automoción sencilla como líneas de llenado de peso, procesos no cíclicos o lentos, como el control de climatización o presión.
   Las latencias de este grupo se enmarcan entre los 10ms - 100ms con variacions jitter que puede llegar al 100%.

ii. **Soft Real Time:** comunicaciones donde el tiempo de respuesta es crítico, como procesos cíclicos o alarmas que provoquen interrupciones ya sea por seguridad o para evitar problemas en él proceso, se enmarca en comunicaciones que necesiten latencias entre 1-10ms y jitter por debajo del 15%. Este rendimiento es suficiente para la mayoría de las aplicaciones de automatización industrial como líneas de ensamblaje, procesos de señalización de emergencia, alarmas críticas, llenado de precisión, líneas de empaquetado, etc.

iii. **Hard Real Time:** Se considera que la comunicación es prácticamente determinista, tiempos de ciclo bajo 1ms con variación o jitter de 1µs, orientados principalmente a automoción, control de movimiento, posición de ejes, etc. en general los protocolos que se enmarcan en este grupo se apoyan en el protocolo *PTP Precision Time Protocol* IEEE 1588 para su sincronización. No es implementable en redes enrutadas y dependiendo del fabricante necesita hardware dedicado. Las aplicaciones que necesitan este tipo de rendimiento son por lo general de control preciso de movimiento como en la fabricación de tarjetas electrónicas, control de ejes, servomotores, robótica general, comunicación interna de máquinas como etiquetadoras, impresoras, inyección, etc.

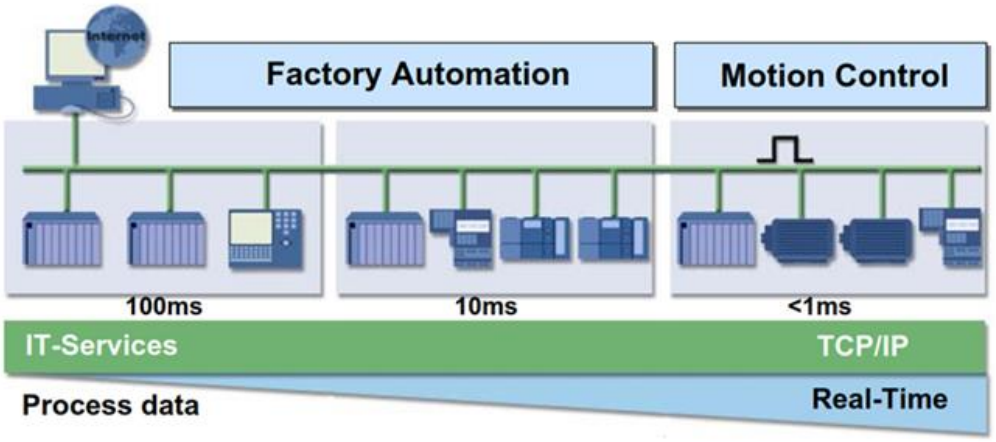


Figura 2-19 Latencias para los diferentes tipos de controles industriales. [38]

2.3.2.2 IEEE 1588 Precision Time Protocol PTP

PTP es un protocolo auxiliar que utilizan varios de los protocolos Real-Time para sincronizar sus relojes distribuidos que tendrán los diferentes controladores.

Los protocolos de tiempo de red *NTP* (*Network Time Protocol*) y el protocolo simple de tiempo de red *SNTP* (*Simple Network Time Protocol*) son métodos utilizados para la sincronización de equipos a fin de dar diferentes funcionalidades a la red, como son servidores, estaciones de trabajo, ERPs, etc. Estos protocolos son precisos en el entorno de los milisegundos alcanzando bajo condiciones óptimas en una red local los 200 microsegundos de precisión, valor más que suficiente para redes tradicionales, sin embargo, para las redes industriales de tiempo real, especialmente en las que necesitan rendimiento Hard-Real Time, la sincronización requiere una mayor precisión.

El estándar PTP IEEE 1588, proporciona un método para sincronizar el reloj con una precisión incluso menor a 1 microseundo.

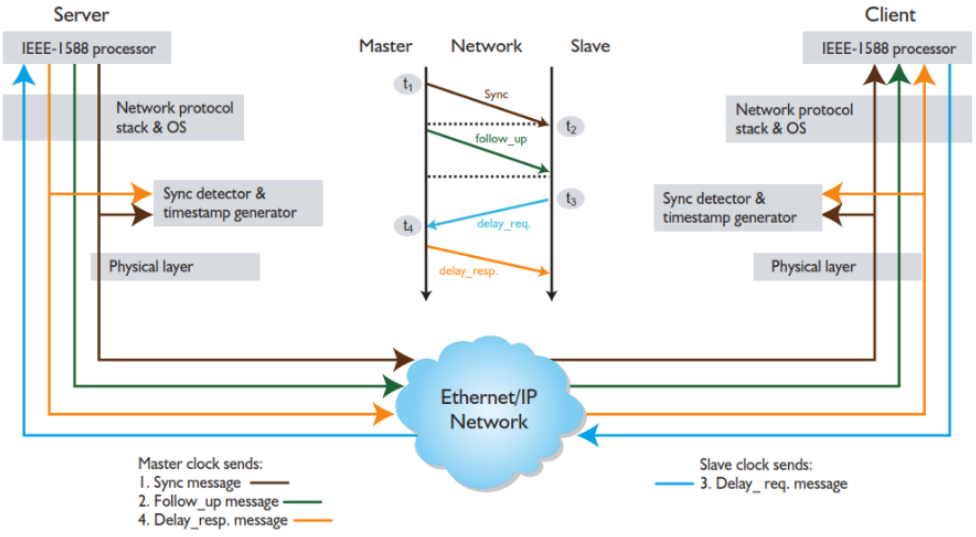


Figura 2-20 Proceso general de sincronización de relojes PTP [36]

El modo de comunicación de PTP es Maestro- Esclavo, donde podrán existir varios esclavos según las capacidades del maestro, a través del algoritmo *BCM* (*Best Master Cock*) PTP escoge el mejor reloj dentro de la topología, denominado *GrandMaster*, basandose en la calidad y estabilidad de los relojes de cada dispositivo, en caso de que exista un cambio en las características del reloj o que deje de funcionar, BCM calcula automáticamente un nuevo *GrandMaster*.

La sincronización de los equipos que sean parte de la topología PTP se lleva a partir del *GrandMaster* en una comunicación Multicast bidireccional con los esclavos al cabo de 2 etapas descritas en la figura 2-21.

En la etapa uno se busca el valor de offset, el *GrandMaster* ocupando UDP o directamente en ethernet, envía en TM1 un mensajes *SYNC* de sincronización al esclavo, que contienen la información del reloj local del *GrandMaster* y opcionalmente puede enviar un segundo mensaje *FOLLOW-UP* que contiene una marca de tiempo *timestamp* de cuando el mensaje *SYNC* fue efectivamente enviado, lo que permite diferenciar cuando el *GrandMaster* pretendía enviar el mensaje y cuando realmente lo hizo, lo que permite identificar posibles retrasos dentro del *GrandMaster*. El esclavo recibe el paquete *SYNC* en TS1 y el tiempo preciso de cuando este fue despachado. El proceso se realiza de manera repetitiva enviando los mensajes *SYNC* cada 2 segundos. En caso de que se utilice hardware dedicado el mensaje *FOLLOW-UP* no es necesario.

En la etapa 2 se revisa el retardo en la propagación, con el propósito que el esclavo pueda compensarlo. El esclavo transmite un paquete de solicitud *DELAY_REQUEST* en TS2 que contiene el tiempo preciso del envío desde el esclavo, el *GrandMaster* recibe el mensaje en TM2 y responde con el tiempo exacto TM2 que recibió el paquete enviado por el esclavo.

Puertos ocupados por protocolo PTP sobre UDP:

- Puerto UDP 319: Event port para los mensajes *SYNC* y *DELAY_REQUEST*.
- Puerto UDP 320: Para los mensajes *FOLLOW-UP* y *DELAY_RESP*.

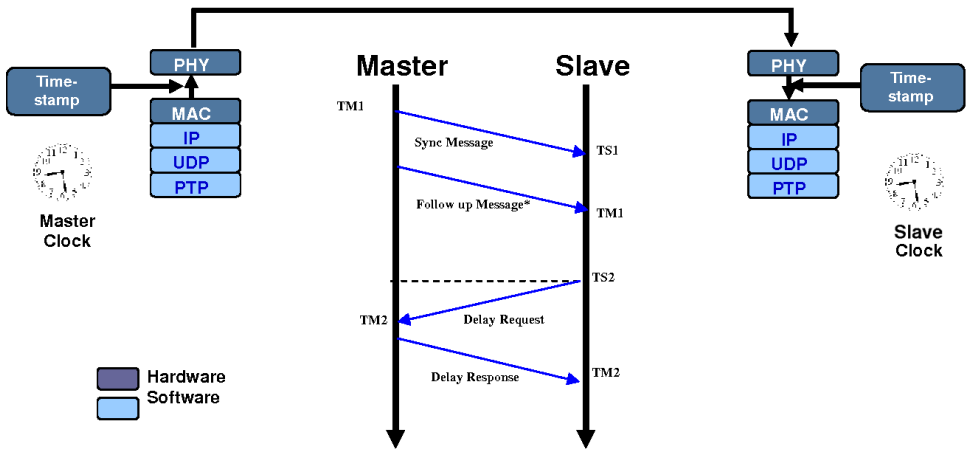


Figura 2-21 Ejemplo de proceso de sincronización PTP [36]

Para hacer sus cálculos PTP asume que la demora en la propagación entre el *GrandMaster* y el esclavo es simétrica, con lo que se obtienen los valores de retardo y Offset (formulas 2-1 y 2-2) que permite realizar la las sincronización de los relojes y conocer el retraso para la compensación.

$$Retardo = \frac{(TS1-TM1)+(TS2-TM2)}{2} \qquad (2\text{-}1)$$

$$Offset = \frac{TS1-TM1-(TS2-TM2)}{2} \qquad (2\text{-}2)$$

2.3.2.3 **Profinet**

Process Field Network Profinet, desarrollado por Siemens, es un protocolo de redes industriales abierto basado en ethernet que está estandarizado en IEC 61158 (*International Electrotechnical Commission*), es el sucesor natural de del Fieldbus también desarrollado por Siemens Profibus.

Tiene 2 clasificaciones generales Profinet IO y Profinet CBA:

i. Profinet IO Se utiliza para comunicar dispositivos de manera descentralizada. Los dispositivos de campo transmiten sus datos de manera cíclica a un dispositivo de orden superior, por ejemplo, de Módulos de entradas/salidas hacia un controlador o de un controlador hacia un HMI.

ii. Profinet CBA *Component Based Automation*: Se utiliza para plataformas de automatización distribuida. Construido sobre el estándar DCOM (*Distributed Component Object Model*) permite modularizar de manera sencilla fases o áreas del proceso de automatización, especialmente útil para aquellos procesos que poseen varias etapas, como son las líneas de llenado o ensamblado, ya que toda la funcionalidad de una etapa se puede encapsular en un "Módulo tecnológico" teniendo la información del módulo disponible en la red para realizar alguna acción en otra etapa o área del proceso. Una de sus ventajas es que la comunicación entre "Módulos Tecnológicos" no se programa, sino que se configura, lo que le quita procesamiento al programa y evita llamadas cíclicas dentro del código. Los ciclos de comunicación para para de este tipo de implementación se enmarcan entre los 10ms - 100ms con variacions jitter que puede llegar al 100%.

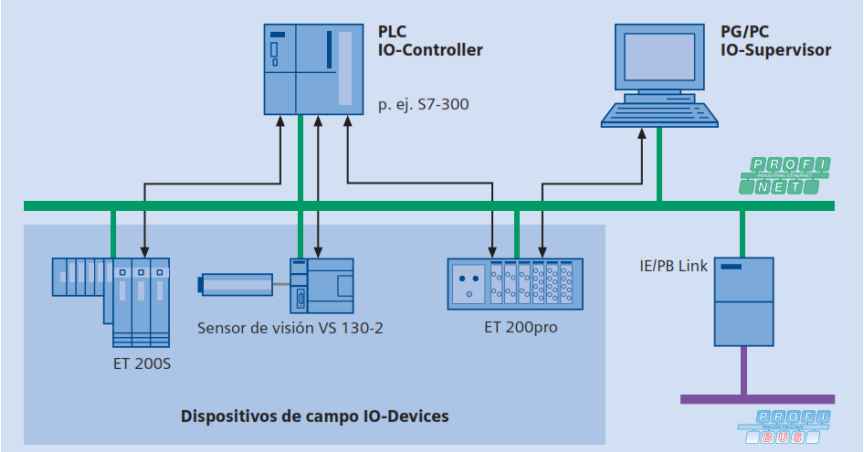


Figura 2-22 Ejemplo de configuración Profinet IO [39]

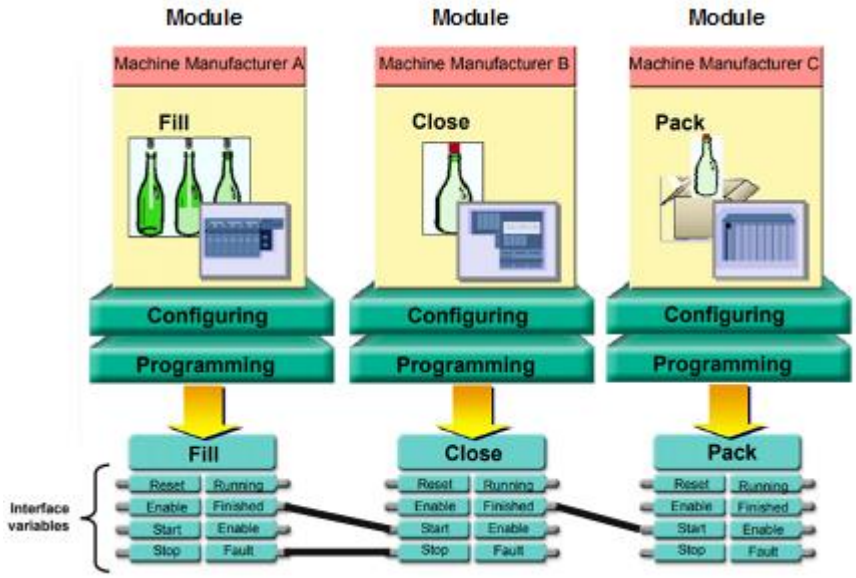


Figura 2-23 Ejemplo de configuración Profinet Cba.[38]

Dentro de las comunicaciones en tiempo real Profinet ocupa la siguiente terminología:

Real Time RT: Puede trabajar sobre equipos de red estándar. Envía mensajescíclicosbasados solo en su reloj local sin sincronizarse con el resto de los equipos de la topología. El campo ethertype de la trama ethernet se marca para RT-Ethernet con número 8892, registrado para Profinet. Además, se recomienda para tener un mejor rendimiento que el tráfico viaje priorizado marcando el campo prioridad de VLAN de las tramas ethernet. Se usa en procesos con tiempos de ciclo entre 1-10ms y pueden trabajar jitter por debajo del 15%.

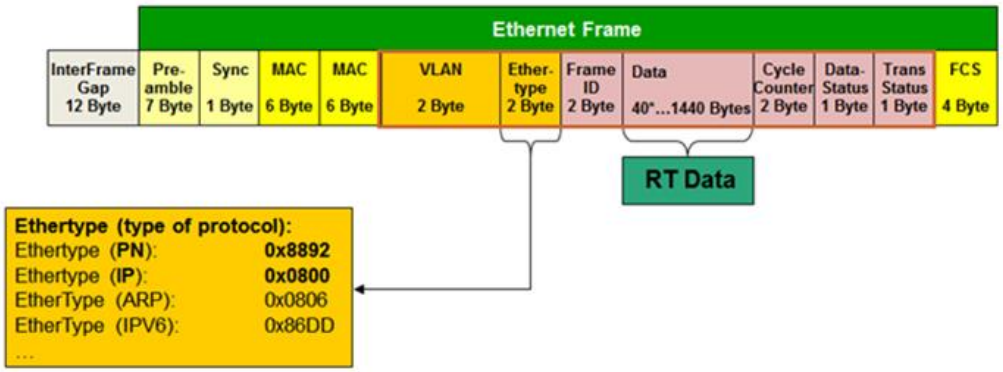


Figura 2-24 Detalle de Trama Profinet. [44]

Real Time Isócrono IRT: Está dentro del grupo Hard Real Time, divide el ciclo de comunicación en una parte determinista y una abierta, lo que permite compartir sin problema las comunicaciones entre IRT, RT y estándar, facilitando la integración y mantenimiento del equipamiento. Se usa en procesos con tiempos de ciclo menores a 1ms y con jitter incluso por debajo del 1µs.

Este tipo de implementaciones requiere hardware dedicado. Es habitual que los equipos de control vengan con switches o hubs integrados con el objetivo de poder conectar más de un equipo a la vez y poder realizar configuraciones tipo anillo sin equipamiento adicional, además son válidas topologías de anillo, bus o ramificadas.

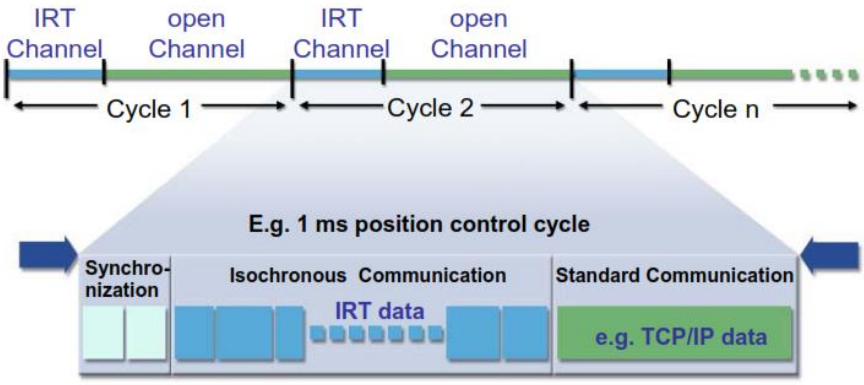


Figura 2-25 Ciclo de comunicación Profinet IRT. [38]

2.3.2.4 **Ethernet/IP**

Desarrollado por Rockwell y la *Open DeviceNet Vendors Association*™ ODVA, es una solución de redes industriales abierta que está estandarizada en IEC 61158 y IEC 6178, se clasifica dentro del grupo Soft Real Time y puede ser conectado bajo cualquier topología.

Utiliza el protocolo *CIP* (*Common Industrial Protocol*) para la transmisión de mensajes e información entre dispositivos similares, protocolo que también utilizan otras soluciones como DeviceNet y ControlNet que no ocupan ethernet en su capa de enlace. CIP es un protocolo que trabaja en las tres capas superiores del modelo OSI, por lo que es completamente compatible con tada la pila de protocolos TCP/IP sin ninguna modificación, siendo básicamente la implementación de CIP en ethernet.

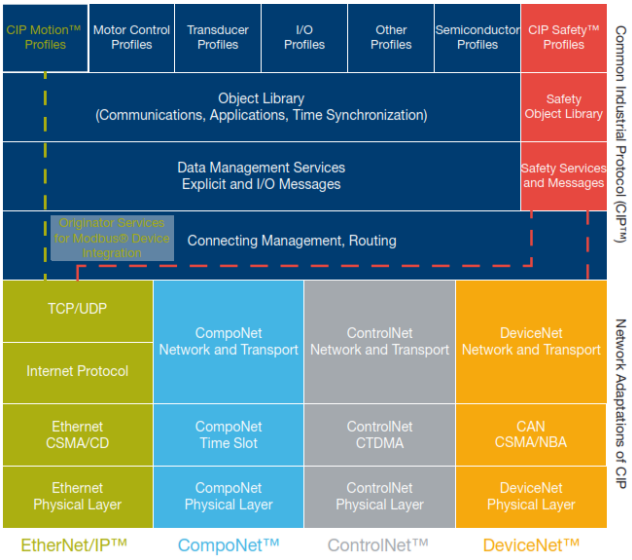


Figura 2-26 Arquitectura Ethernet/IP, DeviceNet, ControlNet, DeviceNet - CIP. [45]

CIP es un protocolo orientado a objetos, por lo que posee atributos (datos), servicios (comandos) y comportamientos (reacciones a eventos o alarmas), utiliza un modelo de comunicación denominado *producer-consumer* que permite un mejor aprovechamiento de los recursos de la red que una comunicación normal Maestro-Esclavo, gracias a que un *producer* puede enviar sus datos a uno o varios *consumers*, cada mensaje es identificado con un *Connection-ID* y a través de un grupo multicast se envía a los diferentes *consumers*, basta con que estos estén en el mismo grupo. Los *consumers* podrán identificar quien origina el mensaje gracias al *Connection-ID*.

Ethernet/IP maneja dos tipos de mensajes, explícitos e implícitos, los mensajes explícitos utilizan TCP para su transporte y son principalmente mensajes de configuración, carga de código y diagnóstico, tienen un rendimiento que se enmarca en el grupo de comunicaciones estándar. Los mensajes implícitos son principalmente para comunicación de tiempo real, usan UDP como protocolo de transporte y sirven para el intercambio de mensajes que contienen variables como son lecturas de entradas, activación de salidas o posiciones de memoria.

Ethernet/IP utiliza PTP IEEE 1588 para en conjunto con el servicio *CIP Sync* de CIP lograr el sincronismo necesario para comunicaciones en tiempo real, cabe indicar que no ocupa mensajes cíclicos, lo que sumado a que CIP es un protocolo que trabaja por encima de la capa de transporte necesita ayuda de funcionalidades de priorización en sus tramas para asegurar rendimiento de tiempo real. Ethenet/IP no es adecuado para aplicaciones que necesiten Hard Real Time.

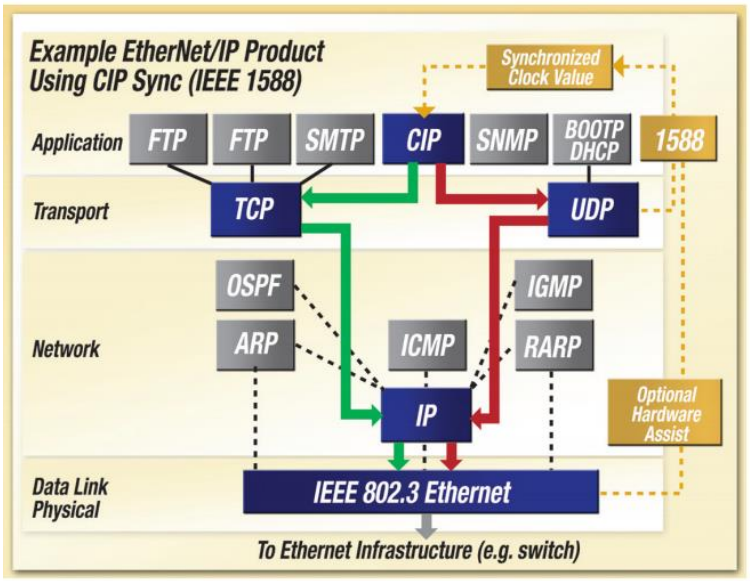


Figura 2-27 Flujo de mensajes explícitos e implícitos y de tiempo real Ethernet/IP

2.3.2.5 **Ethernet Powerlink**

Powerlink es un mantenido y desarrollado por el Ethernet *POWERLINK Standardization Group (EPSG)* y tiene su versión libre desde el 2008 para ser implementada por cualquier fabricante.

Puede ser montado sobre hardware estándar ethernet en su versión Soft Real Time. Para Hard Real Time necesita hardware adicional y equipos de red que soporten PTP.

En Powerlink la comunicación está gestionada por un dispositivo denominado el *Manager Node MN* que sincroniza uno o varios dispositivos denominados *Control Node CN*.

Las comunicaciones funcionan usando una mixtura entre *timeslot* y *polling*. El MN sincroniza a través de una señal de reloj, que también es el tiempo de ciclo de tarea en todos los CNs, en el transcurso de un ciclo el MN envía un mensaje de solicitud de datos *poll request* a cada CN de manera secuencial, donde cada CN responde inmediatamente con un mensaje broadcast *Poll Response*, por lo que todo el resto de CNs y el MN pueden tener acceso a los datos de la respuesta.

El Ciclo de comunicación de PowerLink se denomina *SCNM* (*Slot Communication Network Manement*) y se divide 3 etapas.

1) *Start Period*: El MN envía un mensaje *Start of Cycle* (*SoC*) a todos los CNs para sincronizarlos.
2) *Cyclic Period:* Sirve para el intercambio de datos en tiempo real entre los nodos de la red.
3) *Acyclic Period*: Es el último periodo y está reservado para la transmisión de datos asíncronos que no son críticos, como parámetros de configuración, carga de código, datos, etc.

El protocolo también permite realizar priorización de nodos o ahorro de ancho de banda a través de multiplexación, nodos con una mayor prioridad se transmitirán en cada ciclo mientras otros compartirán su slot con otros. En la figura 2-28 se puede ver que los nodos 1,2,3 transmiten en cada ciclo, mientras los nodos del 4 al 11 comparten los slots.

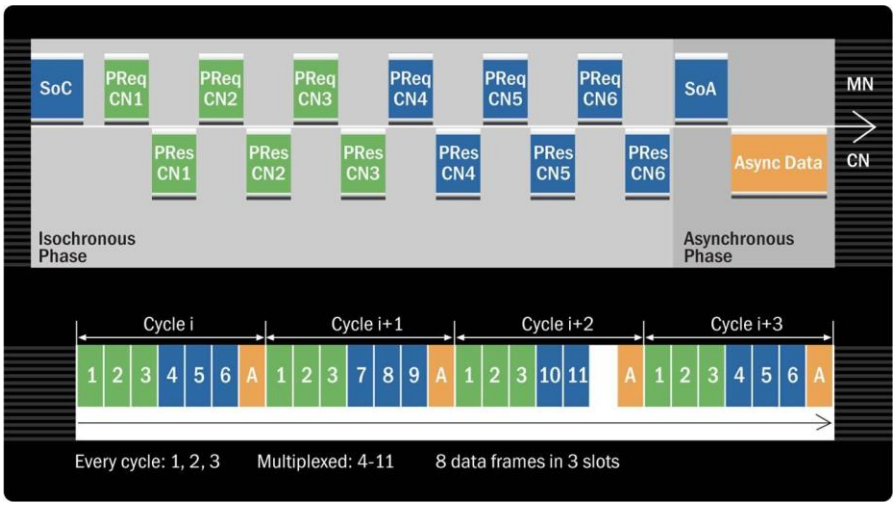


Figura 2-28 Ciclos de envío de datos en Powerlink [23]

PowerLink encapsula sus mensajes agregando 3 campos dentro del payload de la trama ethernet, los cuales son:

- *Message type:* El tipo de mensaje, *SoC*, P*ollRequest*, *PollResponse*, *Start of Asynchronous* y otros de uso menos común.
- *PowerLink Destination y Source*; Que son las direcciones de los nodos, el campo es de 8 bits el MN siempre tendrá la dirección 240, los nodos pueden tener direcciones entre la 1-239 y la 255 está reservada para broadcast.

Figura 2-29 Trama ethernet Powerlink. [23]

El Protocolo puede ser conectado mediante cualquier topología, estrella, ramificada, anillo o bus.

2.3.2.6 **SERCOS III**

Serial Real-Time Communication System III SERCOS III, estandarizado en IEC 61158/61784, fue creado por el conjunto de empresas Rockwell, Bosch Rexroth, ABB y Siemens, es la tercera generación del Fieldbus SERCOS.

SERCOS III tiene rendimiento de Hard Real Time, utiliza una filosofía de comunicación Maestro-Esclavo, intercambiando, en *timeslots*, datos de manera cíclica entre los nodos distribuidos, todos los mensajes empiezan y terminan en el Maestro.

El protocolo no ocupa las capas superiores a la capa de enlace, por lo que las direcciones IP no son interpretadas y su sincronismo se pierde en comunicaciones enrutadas. Las tramas son enviadas a la dirección de broadcast, por lo que todos los equipos de la topología podrán tener acceso a los datos; Dentro de la trama ethernet se marca el campo *Ethertype* con el numero 0x88CD, registrado para SERCOS III. La cabecera del mensaje contiene información de estados y control propias del protocolo y el área de datos se divide asignando una posición específica dentro de la trama a cada esclavo.

SERCOS III Maneja 2 tipos de mensajes, *Master Data Telegrama MDT* y *Acknowledge Telegram AT*, ambos enviados por el Master.

- MDT: Es la información generada por el maestro que es leída por los esclavos, ordenes o accionamientos.

- AT: También es generado por el maestro y pasa de esclavo en esclavo hasta volver al maestro, el primer esclavo en recibirlo edita el área de datos que le corresponde con estados discretos, variables análogas, etc y pasa la trama editada al siguiente esclavo que realizar el mismo proceso.

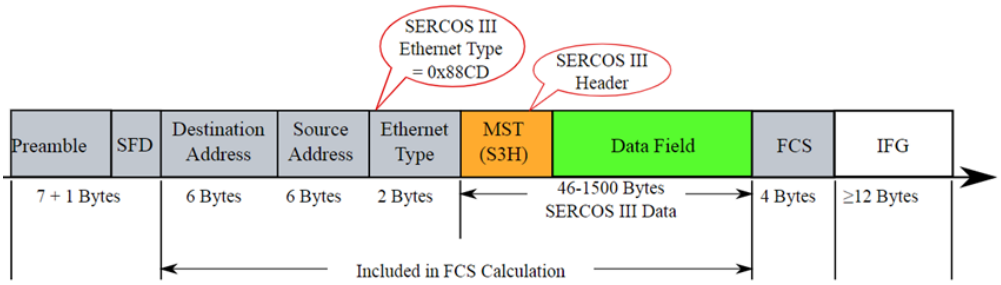


Figura 2-30 Trama SERCOS III. [73]

Para Sincronizarse el protocolo incluye un mensaje de sincronización *MASTER SYNC TELEGRAM* en el primer MDT transmitido por ciclo, los retrasos producido por cada salto entre los nodos de la red son interpretados por el protocolo y compensados para mantener el sincronismo.

SERCOS III permite en un ciclo compartir información de tiempo real con información no determinista, No Real Time NRT, en el espacio de tiempo sobrante del ciclo no ocupado por los mensajes MDT y AT.

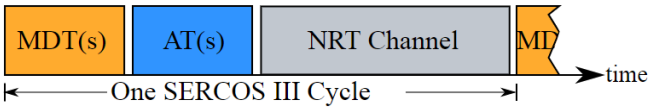


Figura 2-31 Ciclo de comunicación SERCOS III. [73]

Las topologías de Red que admite SERCOS III son de bus o de anillo y están orientadas a no ocupar equipamiento adicional, como switches o hubs. Se establece ocupando los 2 canales full duplex disponibles en los cables 100 Base-TX o 100Base-FX, quedando uno como primario y el otro como secundario. La configuración de anillo aporta un nivel de redundancia mucho mayor, el Maestro continuamente envía las tramas por ambos canales de la interfaz, que son recibidas por el mismo, al detectar algún cambio en la topología inmediatamente realiza el cambio, logrando tiempos de 25 µs.

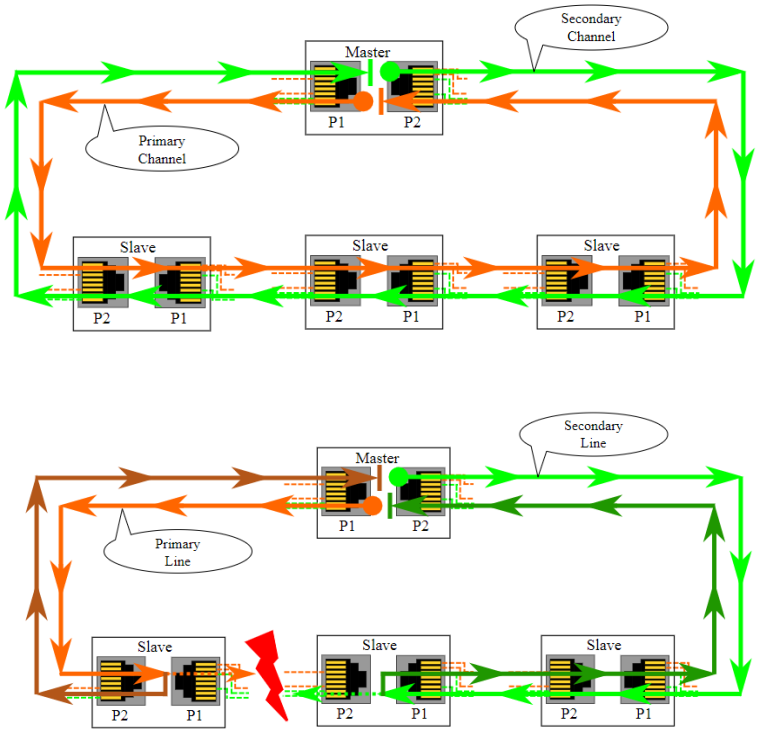


Figura 2-32 Funcionamiento de comunicaciones SERCOS III y proceso de convergencia. [73]

2.3.2.7 **EtherCAT y EAP**

2.3.2.7.1 EtherCAT

Ethernet for Control of Automation Technology EtherCAT, es una tecnología de Ethernet industrial abierta, de alto rendimiento estandarizada en la norma IEC 61158 desarrollada y mantenida por El

EtherCAT Technology Group (ETG). Puede tener un rendimiento de Hard Real Time y soporta cualquier tipo de topología.

EtherCAT Tiene gran versatilidad, si bien su mejor rendimiento lo alcanza en comunicaciones Maestro-Esclavo, también soporta modos Maestro-Maestro y Esclavo- Esclavo, pudiendo tener una jerarquía descentralizada,

El principio funcional clave de EtherCAT está en cómo sus dispositivos procesan las tramas Ethernet, el Maestro envía un telegrama que pasa por cada nodo. Cada dispositivo de la topología lee los datos direccionados a él, edita los datos en el área que le corresponde de la trama y la reenvía al siguiente dispositivo, con lo que el retardo de la trama se debe prácticamente a los tiempos de retardo de propagación del hardware.

EtherCAT funciona principalmente sobre comunicaciones ethernet sin equipamiento adicional, pero también es compatible su funcionamiento con equipos de red tradicionales e incluso es implementable sobre capas superiores con TCP o UDP, limitando su rendimiento a las características de la red.

El campo *ethertype* de la trama ethernet se identifica con en número 0x88A4 en el campo, registrado para EtherCAT.

Dentro del campo datos ya sea de la trama ethernet o utilizando algún protocolo de la capa de transporte, están los datagramas o subtelegramas EtherCAT, cada trama tiene una cabecera global que contiene 3 campos, *Length* largo de la trama, *Res*. Reservado para uso futuro y *type* que para las tramas EtherCAT tendrá un valor de 1. A su vez cada subtelegrama tiene su propia cabecera principalmente usada para envío de comandos y un campo *Working Counter WKC* utilizado para comprobar que los comandos indicados en la cabecera se ejecutaron correctamente.

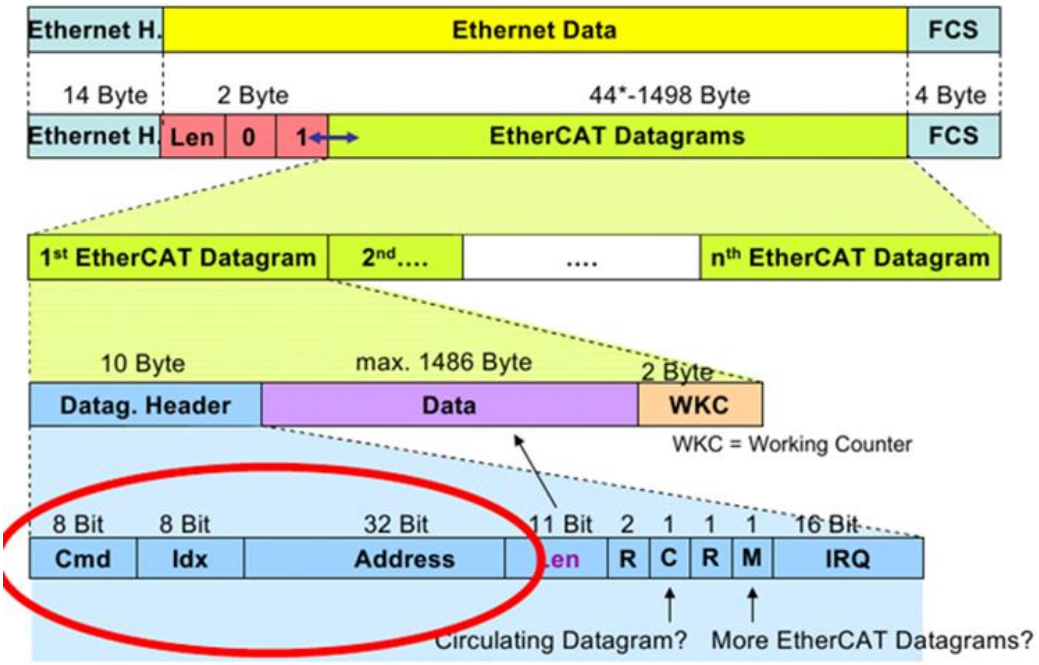


Figura 2-33 Trama EtherCAT. [10]

El protocolo construye una imagen global del proceso, dividida en áreas donde estarán todos los datos de variables/parámetros de los esclavos, cada subtelegrama direcciona una parte específica de la imagen de proceso, para la cual están disponibles 4 GBytes de espacio de direcciones. Durante el arranque de la red a cada dispositivo esclavo se le asignan una o más direcciones en este espacio global. Si a varios dispositivos esclavos se les asignan direcciones en la misma área, todos pueden ser direccionados con un único datagrama.

El Maestro utiliza hardware ethernet estándar, lo que permite implementar un Maestro en cualquier plataforma de hardware con un puerto ethernet disponible, independientemente de si el sistema operativo es en tiempo real o del software de aplicaciones que se utilice.

Los Esclavos EtherCAT necesitan un controlador en hardware *ESC (EtherCAT Slave Controller)* para procesar tramas y lograr rendimiento de Hard Real Time.

El protocolo tiene un gran rendimiento de convergencia al utilizar conexiones redundantes, comúnmente en anillo, en caso de una falla de conexión en un nodo, el vecino lo detecta y cierra la interfaz automáticamente para que el resto de la red pueda seguir funcionando, con tiempos de detección menores a 15 µs.

EtherCAT (P = potencia) es una adición al estándar de protocolo, permite la transmisión de tensión a través del cable ethernet de cobre estándar de cuatro hilos, modificando exclusivamente a la capa física.

Para su Sincronismo ocupa una filosofía de relojes distribuidos *DC (Distributed clocks),* a diferencia de la comunicación completamente síncrona, cuya calidad sufre inmediatamente de errores de comunicación, los relojes distribuidos sincronizados tienen un alto grado de tolerancia al jitter.

La calibración de los relojes en los nodos está completamente basada en hardware. Por defecto el primer dispositivo esclavo de la topología será el reloj de referencia o *MasterClock*, La hora de referencia se distribuye cíclicamente a todos los demás dispositivos de la topología para ajustarse con precisión al reloj de referencia logrando un jitter menor a 1 µs. opcionalmente el *MasterClock* puede ser externo, típicamente el *GrandMaster* que de PTP descrito en este capítulo en el punto 2.3.2.3.

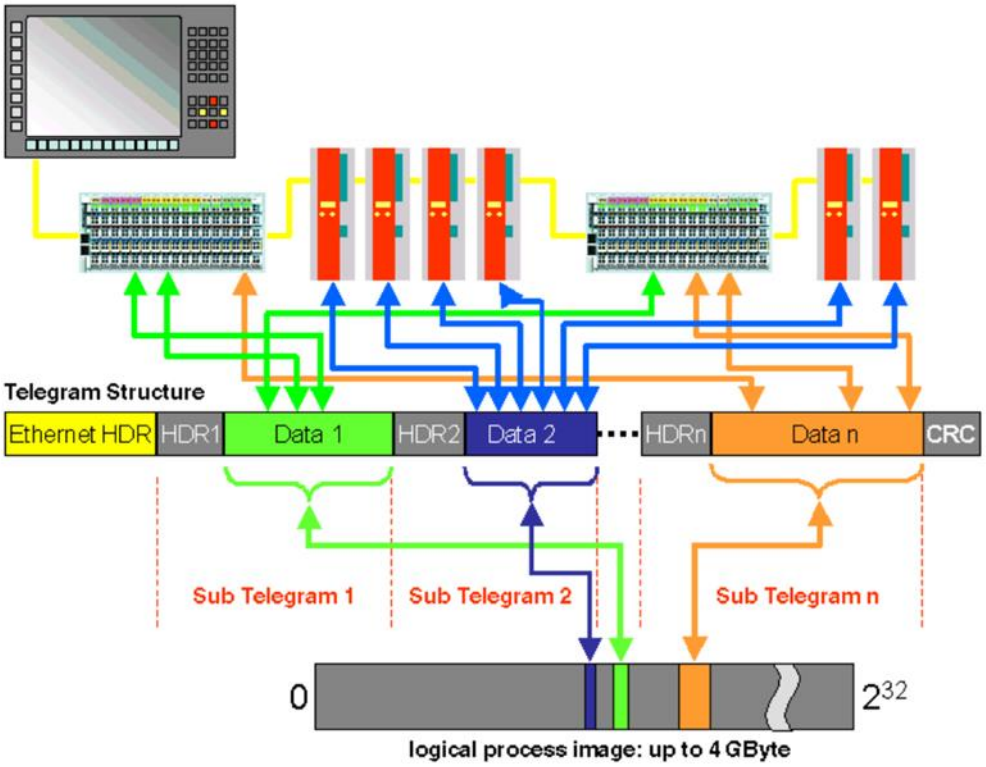


Figura 2-34 flujo de ingreso de datos en Subtelegramas. [51]

El proceso de sincronización de relojes tiene 3 acciones principales, similares a las que efectúa el protocolo PTP

i. Retardo de propagación: Se calcula al inicio y opcionalmente cada cierto intervalo, el Maestro calcula el retardo en función de los *timestamps* de envío y recepción hacia y desde los esclavos.
ii. Compensación de Offset: El Maestro escribe en un registro especifico de los esclavos para compensar la diferencia de su reloj y el propio de cada esclavo.
iii. Compensación derivada por variaciones: Luego de realizados los procedimientos 1 y 2 el desplazamiento natural del reloj por la diferencia en los osciladores se revisa periódicamente a través del algoritmo *TCL (Time Control Loop)* para reajustar el reloj local.

2.3.2.7.2 EAP

EtherCAT Automation Protocol EAP es un protocolo pensado para la comunicación entre Maestros EtherCAT o dispositivos de orden superior como HMIs o SCADAs, pero es perfectamente implementable para comunicación entre controladores de campo. EAP se configura, no se programa lo que permite simplificar el código y evita llamadas cíclicas. EAP en su implementación se sirve del protocolo ADS de Beckhoff (descrito en el punto 2.3.2.7.2.1) en su sistema Twincat.

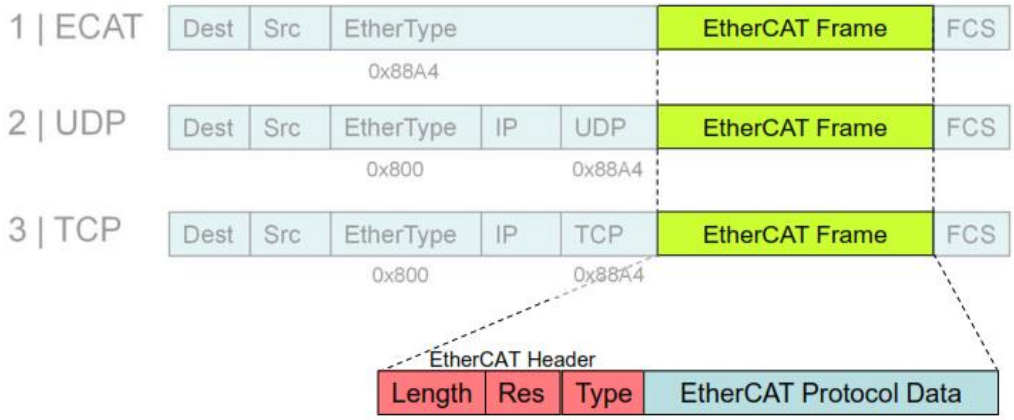


Figura 2-35 Relación del campo de datos de EtherCAT con EAP. [10]

EAP en el sistema Twincat soporta 2 métodos de envío de información, cíclico y acíclico; El cíclico es generalmente ocupado para la publicación de variables a través de tramas de datos de proceso *Process Data* (EtherCAT *header type* = 4) y el acíclico para tramas *Mailbox* (EtherCAT *header type* = 5) utilizadas principalmente para configuración y diagnóstico.

EAP *Process Data* es usado para el envío/recepción de variables, el envío puede realizarse por una solicitud que realiza un cliente EAP a un servidor EAP, o de manera cíclica ocupando el método de comunicaciones *Publisher/Subscriber*, cualquier dispositivo dentro de la topología puede publicar una o varias variables en la red, los equipos interesados en escuchar los datos se suscriben a las variables y pueden tener acceso a ellas. EAP soporta el envío de variables ya sea por unicast, multicast o broadcast.

Las tramas no pueden superar el tamaño máximo de 1514 bytes a fin de que no sea dividida fraccionada, la estructura de la trama se observa en la figura 2-36, dentro del campo de datos está la trama general EAP que a su vez se divide en diferentes *Process Data Objetcts PDOs*, similar a lo que realiza EtherCAT con los subtelegramas.

- *Process Data Frame*: Contiene la cabecera de la trama y uno más PDOs.

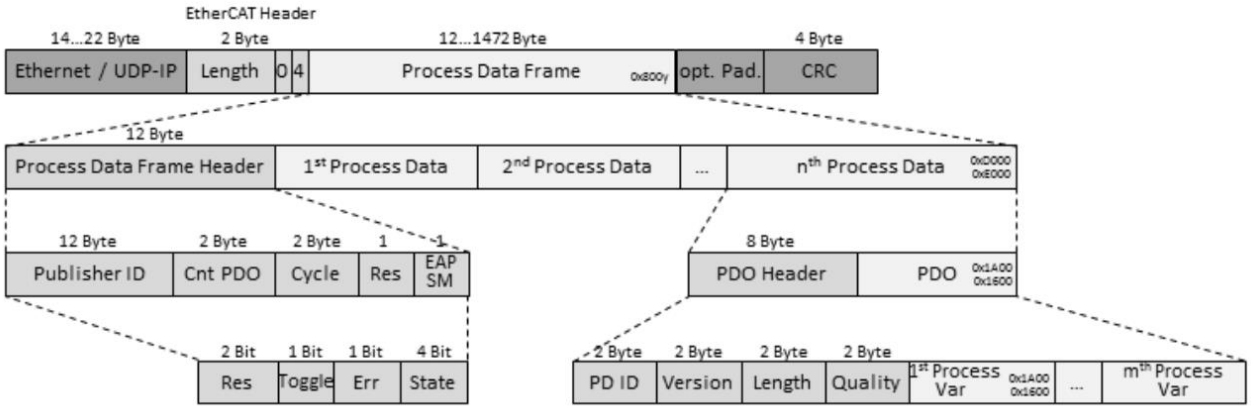


Figura 2-36 Trama EAP. [4]

- *Process Data Frame Header*: La cabecera se divide en 5 subcampos, siendo los más importantes:
    - *Publisher ID*= Dirección del dispositivo que publica los PDOs, se utiliza la dirección *AdsAmsNetId* de ADS, en EAP el receptor no tiene interés en quien publica las variables en la Red, por lo que el Publisher ID puede ser ocupado como filtro en la recepción.
    - *Cnt PDO*: Cantidad de PDOs
    - *Cycle*: Se incrementa en cada publicación/envío de variables, sirve para dar un sincronismo suave y detectar en el receptor cuando alguna trama se pierde.
    - *Res*: Reservado
    - EAP SM: Se usa para diagnóstico, identifica el estado operacional del dispositivo EAP y posibles errores.

- PDOs: son los contenedores de variables, puede tener solo una o varias variables, dentro de su cabecera se encuentran los siguientes campos
    - *PD ID:* Identificador de la variable, que será único en toda la topología.
    - *Version*: Versión de EAP
    - *Length*: Largo total en bytes del PDO sin incluir la cabecera.
    - *Quality*: Estado de operatividad de la variable.
    - *Variable ID*: Está en la cabecera de cada Process Data e identifica con un ID la variable en particular.
    - *Process Var*: Valor actual de la variable.

El intervalo de publicación de variables por EAP se puede definir de varias formas lo que permite variar la frecuencia de publicación de manera muy flexible.:

- *Poll Request Rx PD*: Cuando un dispositivo solicita una o varias variables.
- *Divider/Modulo*: Múltiplo del ciclo de tarea del controlador, por ejemplo, cada 2 o 4 ciclos de tarea se publican las variables.
- *Cycle Time*: Intervalo fijo.
- *Change of State*: Cuando las variables configuradas para publicar tienen un cambio en su valor, puede agregarse un Timeout que además asegure la publicación cada cierto intervalo de tiempo.

2.3.2.7.2.1 ADS

Automation Device Specification ADS, es un protocolo desarrollado por Beckhoff dentro de su sistema Twincat, es un método de envío de datos Cliente-Servidor que puede funcionar tanto sobre TCP/IP como directamente en ethernet. Cada dispositivo que se comunica por ADS tiene un software denominado *message router* que ocupa el Rol de interfaz entre los dispositivos. Cada dispositivo funcionara sobre un número de puerto *AdsPortNr* (no confundir con un puerto tcp/udp) y una dirección *AdsAmsNetId* que debe ser única dentro de la topología.

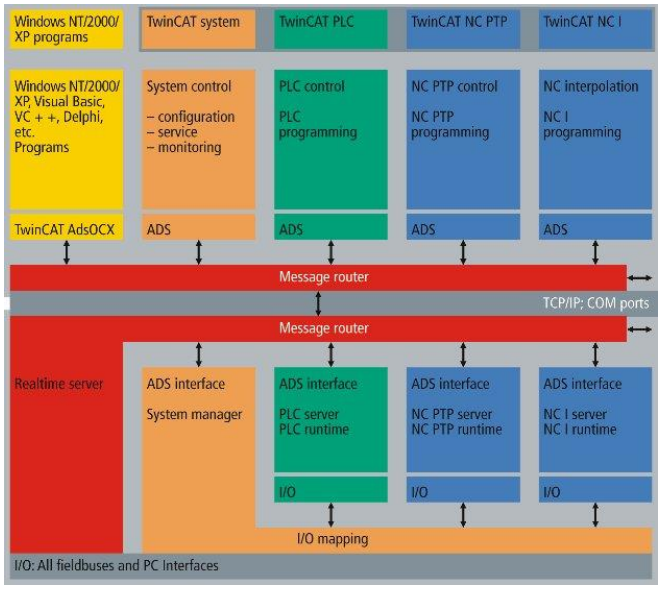


Figura 2-37 Funcionamiento ADS, [75]

2.4 Revisión de Protocolos de control de Redes IP

En esta sección se revisarán diferentes protocolos de redes IP, disponibles en el hardware del caso práctico, con el fin de poder elegir los protocolos más adecuados para plantear las pruebas que determinaran los protocolos a utilizar en la propuesta de configuración, que permitan cumplir con un rendimiento Soft Real Time Ethernet para comunicaciones enrutadas, por un lado, y por otro, obtener los tiempos de convergencia o reconfiguración exigidos en el caso práctico.

La revisión de esta sección se realizará con mayor profundidad dada la criticad de los protocolos dentro de la red, ya que una mala configuración de redundancia en capa 2 como los de la familia *Spanning tree*, de redundancia de Router o de enrutamiento, pueden causar la caída de parte o la totalidad de la red afectando las comunicaciones de los diferentes subsistemas.

2.4.1 Capa de Acceso

En cualquier red que conformemos y en especial en redes industriales y de utilities la resiliencia es un tema de importancia mayúscula, por lo que siempre se tendrá que tener al menos un camino alternativo, lo que trae un inconveniente para la capa inmediatamente superior a la capa física, la formación de *loop*, lo que hace obligatorio el uso de algún protocolo que lógicamente solucione el problema.

¿Por qué los loops producen estas fallas?

Los loops producen fallas debido a que las tramas se van replicando entre los dispositivos de manera descontrolada, provocando las temidas tormentas de broadcast.

Supongamos que conectamos 3 switches como se indica en la figura 2-38.

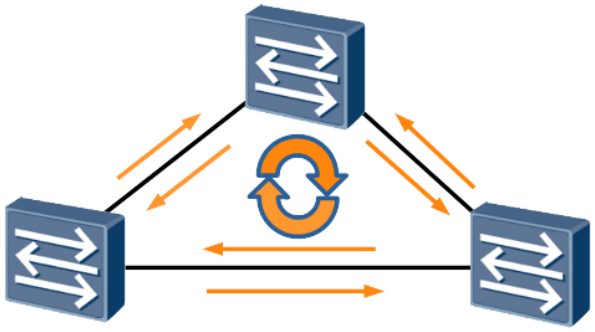


Figura 2-38 ejemplo de problema de loop en capa 2

Los switches al iniciar su trabajo necesita llenar su tabla de *MACs (Media Access Control)* para poder reenviar el tráfico a algún destino, para realizarlo envían una trama de broadcast hacia los otros switches por todas las interfaces, menos por la que recibieron previamente la trama de broadcast proveniente de otro switch o equipo terminal, los switches que reciban dichas tramas realizaran el mismo proceso, con lo que las tramas se irán multiplicando de manera exponencial sin parar ya que las tramas siquiera cuentan con un campo TTL como los paquetes IP, provocando

la tormenta de broadcast que copara la utilización de los enlaces y capacidades de las CPUs, haciendo caer la red.

Un segundo problema será la inestabilidad en la propia tabla MACs ya que tendrá dos o más interfaces para llegar a la misma MAC de destino, provocando un cambio continuo de la tabla.

Para el manejo de loops existen protocolos estandarizados por la IEEE y propietarios de los fabricantes de equipos networking, entre los estándares encontramos la familia de los protocolos Spaning Tree STP, RSTP, MSTP, protocolos ring protection de rápida convergencia ERPS, RRPS y dentro de los propietarios SEP, VBST de Huawei, PVST de Cisco, etc.

Dentro de los protocolos implementables dentro del hardware de la red de acceso descrita en el capítulo 3 se tiene la familia Spaning tree y SEP, por lo cual serán revisados.

2.4.1.1 Familia de protocolos Spannig Tree

La idea básica detrás de la familia de protocolos Spaning tree es formar un árbol de equipos, con raíz en uno de ellos, denominado *Root Bridge* y bloquear lógicamente una interfaz de red para la apertura en él loop. Cada switch dentro de la topología Spaning Tree tendrá un identificador *BID* (*Bridge ID*) formado por su MAC y valor de prioridad, el menor valor de BID dentro de la instancia Spaning tree, se convertirá en el *Root Bridge*, el valor de prioridad por defecto es 32.768.

2.4.1.1.1 STP

Spannig Tree Protocol STP está estandarizado por la IEEE 802.1D, es la versión más simple de la familia de protocolos Spaning Tree y su base de funcionamiento es aplicable a toda la familia de protocolos.

Las *BPDUs (Bridged Protocol Data Unit)*, son las tramas que permiten la configuración y actualizaciones de topología de Spaning tree, estas son enviadas por los switches a la dirección Multicast 01-80-C2-00-00-00. Existen 2 tipos de BPDUs:

- *Configuration*: Que contienen costo para alcanzar el *Root Bridge*, el *Root bridge*, etc
- *Toplogy change Notification*: Cambios de Topología

Los 2 tipos de BPDU tienen la misma estructura básica y se diferencian en el uso de flags que proporcionaran las notificaciones de los cambios de topología y su acuse de recibo.

La BPDU tiene varios campos, dentro de los más importantes:

- *Message Type*: Indica si es una BPDU de configuración o de cambio de topología.
- *Root ID*: ID del *Root Bridge*.
- *Root path Cost*: Se refiere a la suma de los costos que existe desde una interfaz de red del equipo para alcanzar *Root bridge*. El costo de cada interfaz puede indicarse manualmente o será determinado automáticamente según el ancho de banda de la interfaz.
- *Bridge ID*: ID de cada uno de los switches que no son *Root*, está formado por la prioridad del switch y su MAC interna.

- *Port ID:* ID interfaz por la que se envían las BPDUs.
- *Message Age*: Cantidad de saltos para llegar al *Root Bridge*.
- *Max Time*: Tiempo máximo donde la copia de la BPDU que almacenan los switches se considera valida. En el caso de que no se reciba una nueva BPDU en un tiempo dado por la resta del *Max Time* y *Message Age*, el switch entenderá que existe un problema en la red y volverá realizarse el cálculo de STP.
- *Hello Time*: Intervalo de tiempo del envío de BPDUs, el valor estándar es de dos segundos.

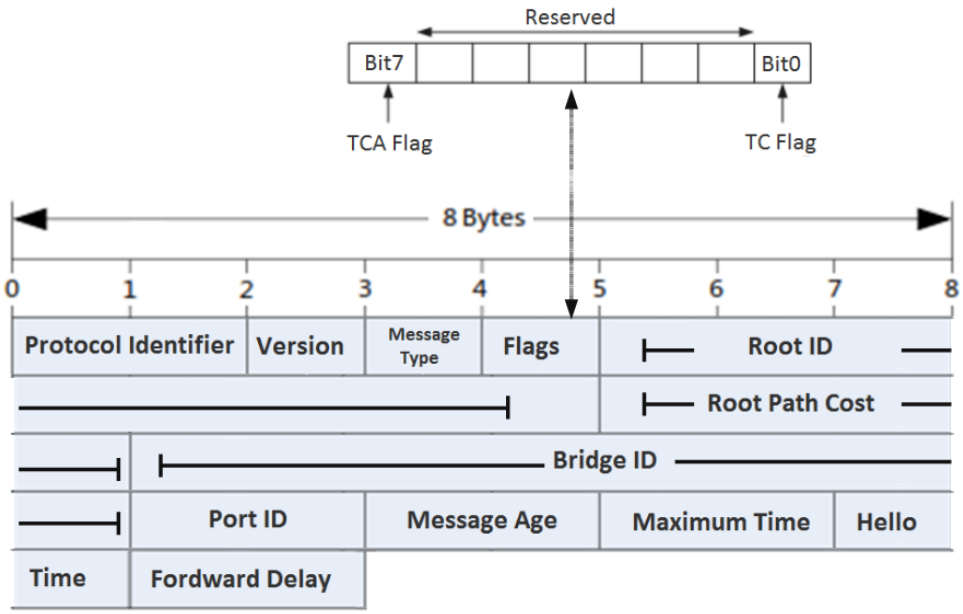


Figura 2-39 BPDU STP

- Fordward Delay: Tiempo de transición entre los estados de STP, el valor estándar es de 15 segundos.
- Los Timers *Hello Time, Max Time, Fordward Delay* y *Message Age* pueden ser cambiados a otros valores dependiendo de las capacidades particulares de cada equipo donde se configure STP.

2.4.1.1.1.1 Roles de interfaces dentro de STP:

Las interfaces del switch que pertenezcan al árbol STP tendrán diferentes roles para dar funcionamiento al protocolo

- *Root Port*: es la interfaz que tiene el menor costo para llegar al Root Bridge.
- Designated port: interfaz en estado "*no Bloqueado*" pero con un costo mayor que la interfaz root port para llegar al *Root Bridge.*
- *No Designated*: Interfaz bloqueada o no designada, es el puerto que no realizara forwarding (reenvío) de tráfico de datos y es el punto donde se abre la topología.

2.4.1.1.1.2 Estado de interfaces dentro de STP:

Las interfaces tendrán diferentes estados según la dinámica de la topología.

- *Blooking*: Puede ser el estado inicial o final de la interfaz, podrá recibir BPDUs, pero no realiza *fordwarding* del tráfico de datos.
- *Listening*: Estado de transición, puede recibir o transmitir BPDUs, revisando si existe una mejor ruta hacia el *Root Bridge*, pero no realiza *fordwarding* del tráfico de datos.
- *Learning*: Estado de transición, puede recibir o transmitir BPDUs, en este estado ya estará aprendiendo direcciones MAC, pero no realiza *fordwarding* del tráfico de datos.
- Fordward*ing*: Estado final de una interfaz, puede recibir o transmitir BPDUs, se aprenden direcciones MAC y se realiza reenvío de tráfico de datos
- *Disabled*: Interfaz apagada o en falla.

De cualquiera de los estados de las interfaces se puede pasar directamente a los estados de *Blocking* y *Disabled.*

El proceso completo desde que la interfaz se encuentra en *blooking* hasta el *fordwarding* será por defecto de 30s dado el valor de *Fordward Delay*:

blooking (0s) → listening (15s) → learning (15s) → fordwarding

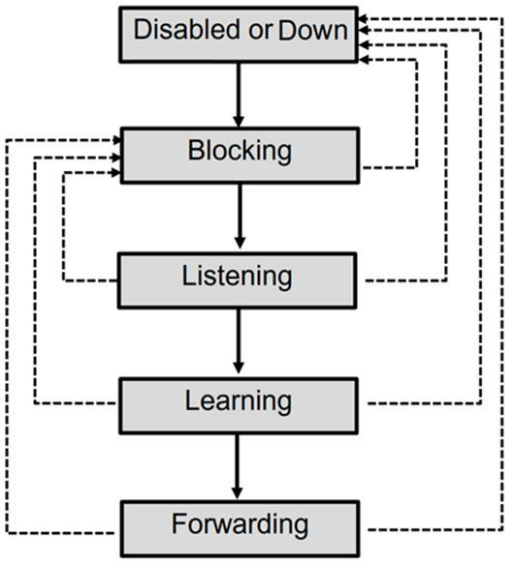


Figura 2-40 Dinámica de estados de puertos en STP

2.4.1.1.1.3 Convergencia en STP

Un puerto que está en estado *fordwarding* saldrá de dicho estado siempre que no reciba BPDUs por un tiempo de 20 segundos (por defecto), como se dijo anteriormente los timers serán modificables a valores menores en función de las capacidades de la marca/modelo del equipo en particular, pero por defecto la convergencia se dará en no menos de 50s.

fordwarding (20s) → listening (15s) → learning (15s) → blooking

La notificación de cambio de topología la informa el equipo que detecta el cambio, levantando el flag TC de la BPDU.

2.4.1.1.2 RSTP

Rapid Spannig Tree Protocol RSTP está estandarizado por la IEEE 802.1w, el funcionamiento es igual que el de STP, pero con menores tiempos de convergencia. La mejora se basa en acortar los timers, se introduce el concepto de tipo de puerto, se simplifican los estados y se crean nuevos roles que ahora serán variables incluidas en la BPDU.

2.4.1.1.2.1 Tipos de puertos

- *Puertos tipo Edge:* interfaces directamente conectadas a los equipos terminales que entran en estado de *fordwarding* de inmediato.
- *Puerto tipo p2p*: permite negociar entre dos switches conectados directamente cual interfaz quedara como *designated* o *root port*.

2.4.1.1.2.2 Estado de interfaces dentro de RSTP

Los estados *disabled*, *blocking* y *listening* son fusionados en el estado *discarding*, simplificando la operación.

Estado	STP	RSTP
Discarding	No	Si
Disabled	Si	No
Blocking	Si	No
Listening	Si	No
Learning	Si	Si
Fordwrding	Si	Si

Tabla 2-8 Evolución de estados de interfaces de STP a RSTP

- *Discarding*: Estado de transición, puede recibir o transmitir BPDUs y revisa si existe una mejor ruta hacia el *Root Bridge*, agrupa los estados *disabled*, *blooking* y *listening* de STP.

2.4.1.1.2.3 Roles de interfaces dentro de RSTP

Los roles dentro de RSTP pasan a ser variables que se integran a la BPDU, se crean nuevos roles a fin de mejorar los tiempos de convergencia, en la tabla 2-9 se indican los roles para STP y RSTP

- *Alternate Port*: Puerto alternativo al *root port*, en caso de que el *root port* deje de recibir las BPDUs inmediatamente este puerto tomara el rol de *root port*, solo existirá un *Alternate port* en la topología.

- *Backup Port*: Puerto alternativo para el *designated port*, en caso de que el *designated port* deje de recibir las BPDUs inmediatamente este puerto tomara el rol de *designated port*, no tiene necesariamente que estar en el mismo switch.

Rol	STP	RSTP
Root Port	Si	Si
Designated Port	Si	Si
No Designated Port	Si	No
Alternate Port	No	Si
Backup Port	No	Si

Tabla 2-9 Evolución de roeles de interfaces o puertos de STP a RSTP

Como se puede ver en la figura 2-41 y en la tabla 2-11, existe una importante diferencia en los flags de lo BPDU de STP a RSTP. Además, que ahora se incluyen los roles como variables en la BPDU, se agregan el bit 1 *Agreement* y el bit 6 *Proposal*, usados para la negociación de las conexiones p2p, un extremo enviará una propuesta de roles activando el bit 6 del byte de flags de la BPDU y en caso que el equipo que recibe la propuesta este de acuerdo enviará activo el flag de *Agreement*.

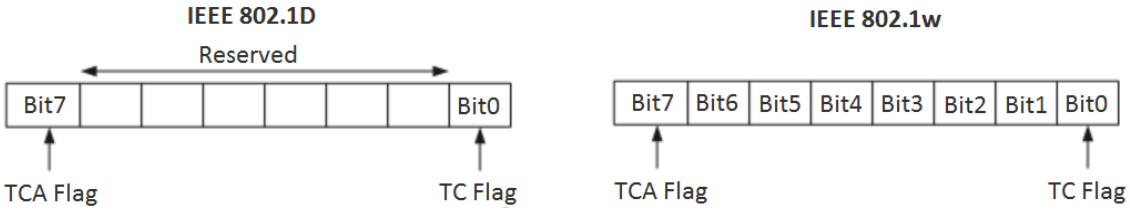


Figura 2-41 Flags BPDU STP y RSTP

Bit	Function
7	TC Topology Change
6	Proposal
5 -4	Port Role: 01: Alternate Port 10: Root Port 11: Designated Port
3	Learning
2	Fordwarding
1	Agreement
0	TCA Topology Change Ack

Tabla 2-10 Flags de BPDU RSTP

2.4.1.1.2.4 Convergencia en RSTP

La notificación de cambio de topología solo se realiza cuando el *root port* o el *designated port* del equipo deja de recibir BPDUs, pasando a *fodwarding* ya sea el *alternate port* o el *backup port* según sea el caso. El equipo que detecta el cambio, activa el bit TC en la BPDU, la transmite hacia los otros equipos de la topología y limpia su tabla MACs.

El tiempo de convergencia por defecto de RSTP estará alrededor de los 6 segundos basado en la no recepción de 3 BPDUs, pero al igual que en el caso de STP los timers serán modificables a valores menores en función de las capacidades de la marca/modelo del equipo en particular.

2.4.1.1.3 MSTP

Multiple Spanning-tree Protocol MSTP está estandarizado por la IEEE 802.1s.

Una de las desventajas tanto de RSTP como STP es que solo permiten una instancia Spanning Tree dentro de su topología, teniendo siempre enlaces principales y otros de backup, no siendo posible el balanceo de carga desaprovechando ancho de banda disponible. Para solucionarlo es que nace MSTP permitiendo lanzar diferentes instancias que podrán tener *root bridges* e interfaces bloqueadas distintas por cada instancia, obteniendo balanceo de carga.

Cada instancia MSTP ocupara RSTP para su funcionamiento, por lo que se tendrán los mismos roles, estados y tipos de interfaces.

Cada instancia de *Multiple Spanning Tree (MSTI)* tendrá un grupo de VLANs asociadas y todas estas instancias se englobarán en una región, todos los switches que compartan las instancias deben ser configurados en la misma región y sus instancias tener asociadas las mismas VLANs.

Se introducen 2 nuevos conceptos

- *CST: Common Spannig tree*, es la representación global el estado Spannig tree de una red, donde pueden coexistir tanto STP, RSTP como MSTP.
- *IST: Internal Spannig tree* es la interfaz entre la CST y lo que se encuentre dentro de la región MSTP, está interfaz permite que toda la región MSTP se vea como un solo switch virtual.

2.4.1.1.3.1 Convergencia en MSTP

Como se indicó en los párrafos anteriores la MSTP maneja instancias RSTP por lo que los tiempos de convergencia de cada instancia son iguales a los RSTP.

2.4.1.2 **SEP**

Smart Ethernet Protection SEP es un protocolo desarrollado por Huawei especialmente diseñado para anillos, pudiendo alcanzar tiempos de convergencia por debajo de los 50ms.

Al igual que la familia de protocolos Spanning Tree, SEP evita los loop en capa 2 bloqueando el reenvío de tráfico en algún punto de la topología.

2.4.1.2.1 Conceptos básicos

- *SEP Segment*: Un segmento SEP es bastante similar a una instancia MSTP, todas las interfaces que sean parte de dicho segmento deberán manejar la misma VLAN de control.

- *Control VLAN*: La VLAN de control será la encargada de manejar las tramas de configuración de SEP, teniendo un comportamiento similar a la BPDU de los protocolos Spanning tree. Al añadir cualquier interfaz al segmento, esta automáticamente dejara pasar la VLAN de control.
- *Node*: Cada equipo dentro del segmento SEP será un nodo en la topología.

2.4.1.2.2 Roles de interfaces en SEP:

SEP podrá utilizarse tanto en anillos abiertos como cerrados, cambiando los roles de los puertos en función de la configuración.

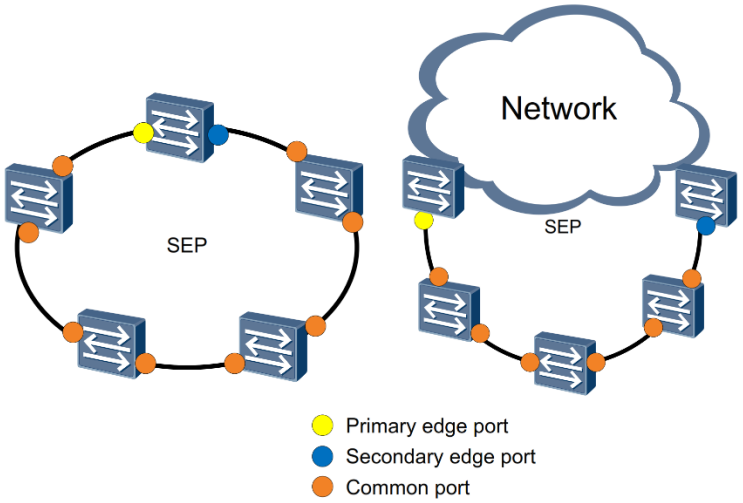


Figura 2-42 Roles de interfaces en SEP [21]

- *Primary edge port*: Solo existirá un *Primary edge port* por segmento dentro de la topología, el equipo que tenga dicho puerto será el principal dentro del segmento cumpliendo funciones similares al *Root Bridge* de los protocolos Spanning tree, en este equipo será donde se definan el método de decisión para el bloqueo de interfaces, los timers y como actuara el modo *preemption* (preferente).

- *Secondary edge port*: Solo existirá un *Secondary edge port* por segmento dentro de la topología, la mayoría de las tramas enviadas desde el *Primary edge port* por la VLAN de control terminaran en este puerto, que además cumplirá la misión de notificar a otras redes los cambios de topología en caso de utilizar anillos abiertos.
- *Common port*: Son todas las interfaces dentro de la topología que no son *Edge ports*.

Adicional a estos 2 roles existen *No-neighbor primary edge port* y *No-neighbor secondary edge port* que se utilizan para topologías que mezclan SEP con Spanning tree, pero no son relevantes parte del presente trabajo.

2.4.1.2.3 Estado de interfaces:

- *Fordwarding*: Envía y recibe tramas SEP y reenvía tramas de datos.
- *Discarding*: Es el puerto bloqueado para evitar los loops, envía y recibe tramas SEP y no reenvía tramas de datos.

2.4.1.2.4 Tramas SEP

Dentro de los campos más importantes de la trama se encuentran:

- *Dst MAC*: La MAC de destino puede ser 0025-9EFB-3D6F o 0025-9EFB-3D70, para 0025-9EFB-3D6F indicara que la trama termina en el *next hop (siguiente salto)*, estarán dentro de estas tramas *hellos, LSAs (link-state adevertisement)* y *graceful restart (GR).* Las tramas con destino 0025-9EFB-3D70 serán tramas que terminan en un *Edge port*, estarán dentro de estas tramas los *Edge port advertisement (EPA), Bloqued port Advertisement (BPA*) y *Topology change (TC).*
- Src. MAC: MAC de origen del equipo que envía la trama.
- *VLAN Tag:* Tag de la VLAN de Control.
- Type: A través de sus 2 bytes indicara que tipo de trama SEP se envía, pudiendo ser *hello, LSA, LSA Ack, preemption, GR_START, GR_END, EPA.*
- *Port Pri*. El byte más significativo es definido internamente por el protocolo, el byte menos significativo permite configurar la prioridad de bloqueo del puerto, un número mayor indicará mayor probabilidad de que el puerto quede bloqueado, por defecto su valor es de 64.
- *Flag*: un valor de 1 indicará que la trama lleva información de cambio de topología TC.

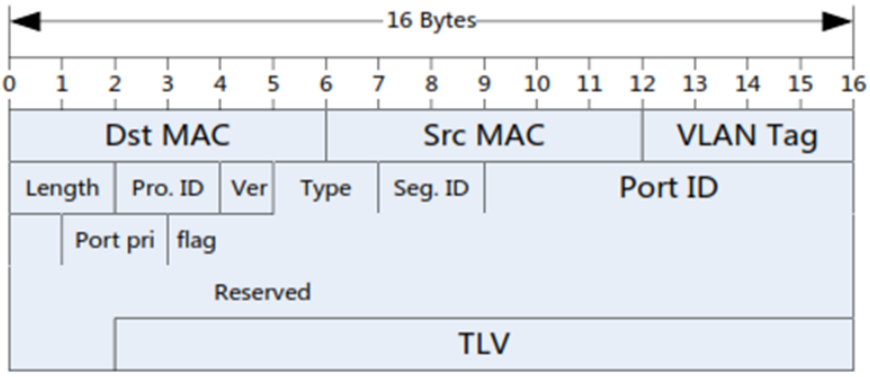


Figura 2-43 Formato de trama SEP

2.4.1.2.4.1 Tipos de tramas

- *Hello*: Mensaje periódico enviado/recibido desde un equipo conectado físicamente para conocer el estado del enlace.
- *LSA: Link-state adevertisement*, el mensaje actualiza periódicamente cada 20s la base de datos de la topología (LSDB), en caso de un cambio de topología por la caída de un enlace la actualización se realiza inmediatamente. Dentro de este tipo de mensajes encontramos:
    - BPA: Es enviado por el equipo que contiene el puerto bloqueado hacia los *Edge ports.*
    - TC: Es enviado por el equipo que detecta el cambio de topología hacia los *Edge ports*.
- Preemption: la trama se usa para indicar la interfaz que se bloqueara.
- *GR graceful restart* Tipo de trama que actúa en el proceso de switchover de algún dispositivo de la topología, *GR_START* se envía cuando comienza el switchover y *GR_END* cuando finaliza, básicamente les indica a dispositivos vecinos que continúen el envío de LSAs durante el periodo de switchover.
- *EPA Edge port advertisement:* La trama contiene los roles de las interfaces y la base de datos completa de la topología, se envían desde el *Primary edge port* hacia el *Secondary edge port* y desde el *Secondary edge port* hacia el *Primary edge port* cada 1 segundo.

2.4.1.2.4.2 Bloqueo de interfaz:

SEP tiene cuatro modos de bloqueo de interfaz, el modo que se ocupará se define en el equipo donde reside el *Primary edge port*:

- Bloquea el puerto con mayor prioridad.
- Bloquea el puerto en el medio del segmento.
- Bloque el puerto en base a la cantidad de saltos desde el Primary edge port.
- Bloquea un puerto especifico según el nombre del equipo.

2.4.1.2.4.3 Modo *Preemption* (Preferente)

El modo preferente toma importancia en el momento que luego de la caída de alguna conexión dentro del segmento SEP y por consiguiente un cambio en la topología. Cuando la conexión vuelve a estar activo, la topología puede o no volver a su estado inicial. Dependiendo de la necesidad se puede configurar de 3 formas distintas:

- *No preemption*: Luego que la topología vuelve a su estado primario no realiza el cambio.
- *Preemption*:
    - *Delayed*: Se configura un tiempo en segundos para que la topología vuelva a su estado original.
    - *Manual*: El cambio de topología se realizará de manera manual con un comando desde el dispositivo que tiene el *Primary edge port*.

2.4.1.2.5 SEP load balancing

SEP permite realizar balanceo de carga de una manera bastante similar a como lo hace MSTP, el balanceo se basa en la creación de segmentos que se asocian a instancias que estarán compuestas por un determinado número de VLANs, ya que SEP es un protocolo desarrollado para anillos, no tiene sentido tener más de 2 instancias.

2.4.1.2.6 Convergencia en SEP

El tiempo total de convergencia de SEP está por debajo de los 50ms.

Al detectarse un enlace caído o en falla, los dos equipos que tengan dicho enlace cambian la prioridad de bloqueo de las interfaces que conectan el enlace a una prioridad superior a la de la interfaz que se encuentra bloqueado antes de la falla y envían una trama BPA hacia los Edge ports para informar del cambio. Posteriormente ambos equipos envían una trama TC a todos los nodos para informar el cambio de topología.

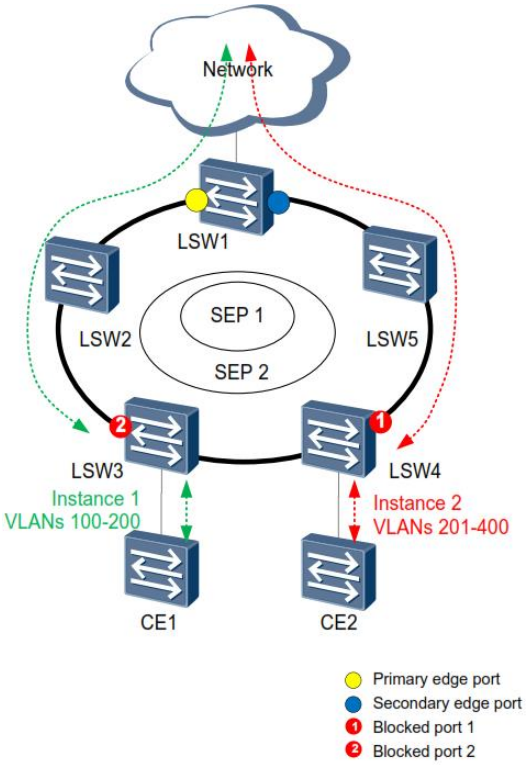


Figura 2-44 SEP con balanceo de carga [21]

2.4.2 Capa de agregación

2.4.2.1 **VRRP**

Virtual Router Redundancy Protocol VRRP es un protocolo que permite implementar redundancia de router o default gateway dentro de una topología de red, está definido primeramente en el RFC 2338, posteriormente en el RFC 3768 y en su versión 3 en el RFC 5798.

Existirá un grupo VRRP por cada segmento de red en la topología, es decir si tenemos diferentes segmentos de red asociados a una misma red física, como al usar VLANs, existirán tantos grupos VRRPs como VLANs.

Cada grupo VRRP debe tener un equipo que ocupe el rol de Master de la topología y uno o varios que ocupen el rol de Backup, el rol será definido por la prioridad del equipo en el grupo, a mayor prioridad mayor probabilidad de ser el Master. VRRP funciona en modo preemptivo lo que se traduce en que al ingresar un nuevo equipo al grupo VRRP con una mayor prioridad a los que estén funcionando, pasa a ser el Master.

Cada equipo tendrá su dirección IP y MAC propia y el grupo contará con una IP y MAC virtual, que es básicamente lo que permite la redundancia, las direcciones virtuales estarán asociadas directamente con el equipo que actúe como Master según la dinámica de la red, la IP se configura de la forma común y la dirección MAC es asignada automáticamente siendo 00-00-5E-00-01-XX donde XX es el ID del grupo en formato hexadecimal, siendo su máximo valor 255 o 0xFF.

Elección del Master será a partir de los criterios indicados a continuación, en caso de no cumplirse uno se pasa al siguiente:

i. El equipo que tenga asociada su dirección IP propia como virtual, con lo que obtendrá una prioridad de 255.

ii. El equipo que tenga el mayor valor de prioridad configurado, siendo esta la configuración más común, la prioridad por defecto es 100.

iii. El equipo que cuente con la dirección IP más alta.

iv. Una prioridad de 0 se traduce en que el equipo dejara de tener en funcionamiento VRRP.

El equipo Master será el único que enviará mensajes periódicamente a los Backups en función de la configuración de los timers y lo hará directamente sobre el protocolo IP, enviando los paquetes a la dirección multicast 224.0.0.18.

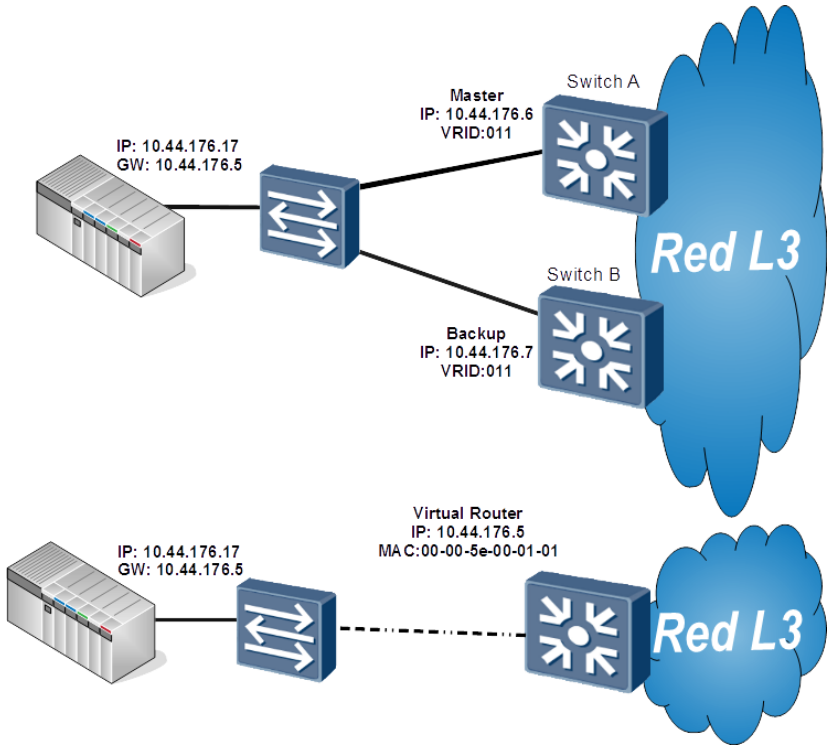


Figura 2-45 Principio de funcionamiento de VRRP

2.4.2.1.1 Timers

Los timers se utilizan principalmente para realizar el proceso de convergencia de VRRP, los equipos Backups estarán escuchando los mensajes desde Master y si se dejan de recepcionar por un tiempo determinado intentaran ocupar su lugar.

- *Advertisement Interval*: Intervalo de envío de mensajes desde el Master.

- *Master Adver Interval*: Intervalo de recepción de los mensajes en los equipos de Backup, por lo general será igual al *Advertisement Interval*, que es su valor inicial.
- *Skew Time:* Tiempo de desplazamiento ocupado para que el Backup de mayor prioridad pase a ser el Master, su valor es:

$$Skew\ time = \frac{(256 - priority) * Master\ Adver\ Interval}{256} \quad (2\text{-}3)$$

Lo que implica que, a mayor prioridad, el *Skew* time tendrá un menor valor.

- *Master Down Interval*: Tiempo para que el Backup declare al Master caído, su valor se calcula a partir de:

$$\text{Master Down Interval} = 3 * Master\ Adver\ Interval - Skew\ time \quad (2\text{-}4)$$

Un menor *skew time*, debido a una mayor prioridad se traducirá en un menor valor de *Master Down Interval* lo que hará que el Backup con mayor prioridad sea el primero en declarar al Master como caído y tomara su rol.

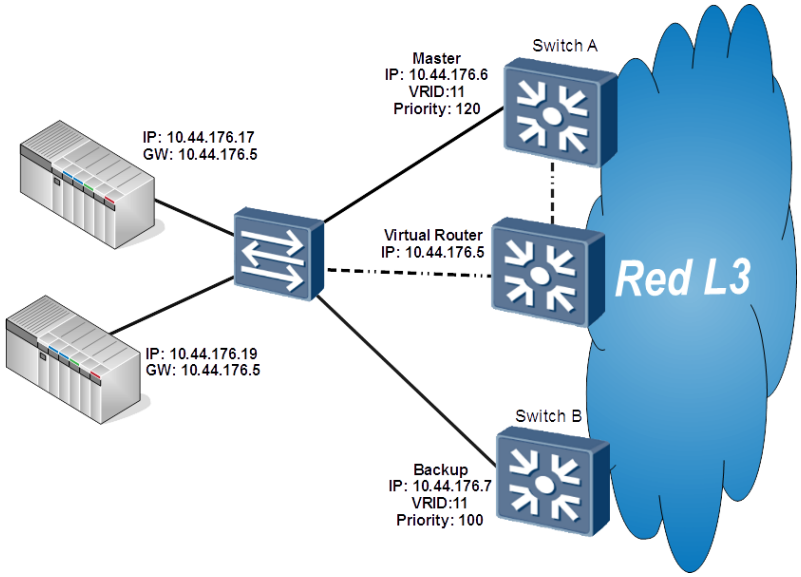


Figura 2-46 Lógica de funcionamiento de VRRP

2.4.2.1.2 Paquete VRRP

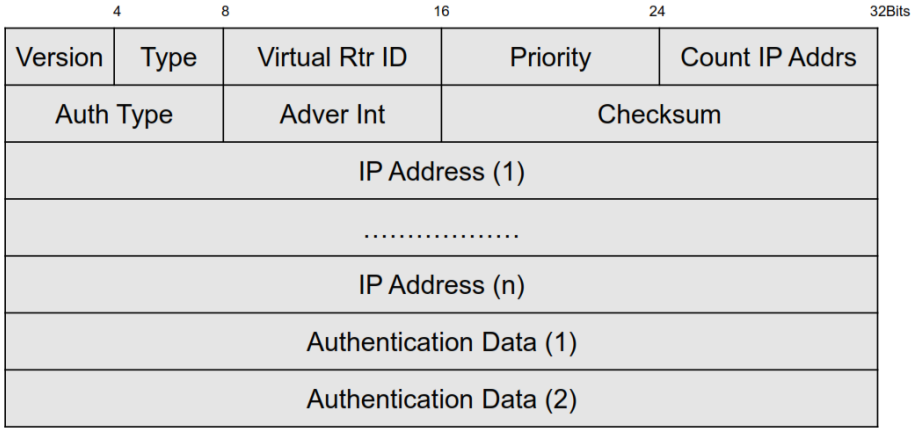


Figura 2-47 Paquete VRRP

Dentro del paquete VRRP los campos más importantes son:

- *Virtual Rtr ID*: identificador del equipo Master que envía los mensajes.
- *Type*: Solo podrá ser tipo *advertisement* que es el único tipo de paquete definido por VRRP, su inclusión es para aplicaciones futuras.
- *Priority*: La prioridad del equipo que actualmente es el Master.
- *Adver Int*: Intervalo de tiempo entre mensajes *advertisement* en centésimas de segundos, por defecto será 100 lo que se traduce en 1 segundo.

2.4.2.1.3 VRRP load balancing

El balanceo de carga en VRRP se puede realizar dentro del mismo segmento de red, configurando dos grupos VRID en el mismo segmento y asignando los defaults gateway en los equipos terminales hacia uno u otro Gateway, o en el caso de que el equipo maneje varias VLANs y/o segmentos de red, cada equipo puede ser el Master de determinadas subredes y Backup de otras, siempre teniendo en cuenta que solo puede existir un Master por grupo VRRP.

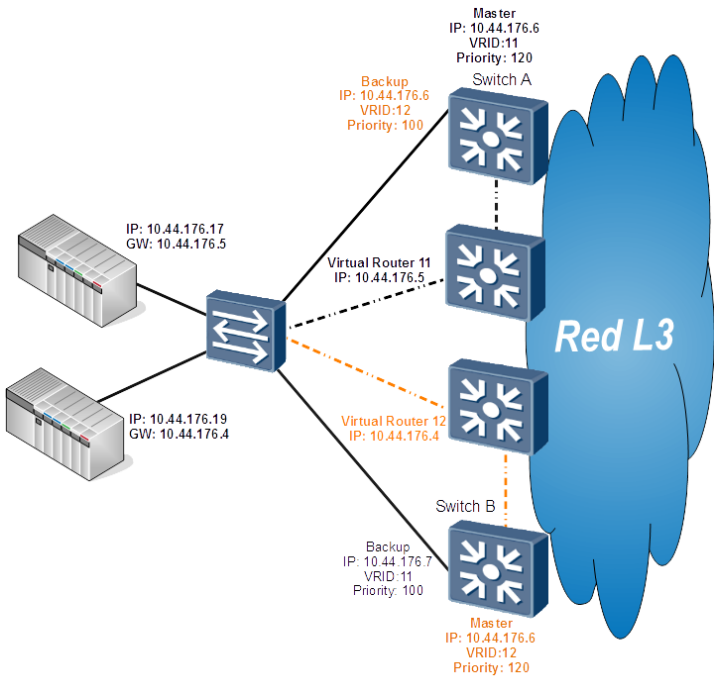


Figura 2-48 Balanceo de carga en VRRP en el mismo segmento de red

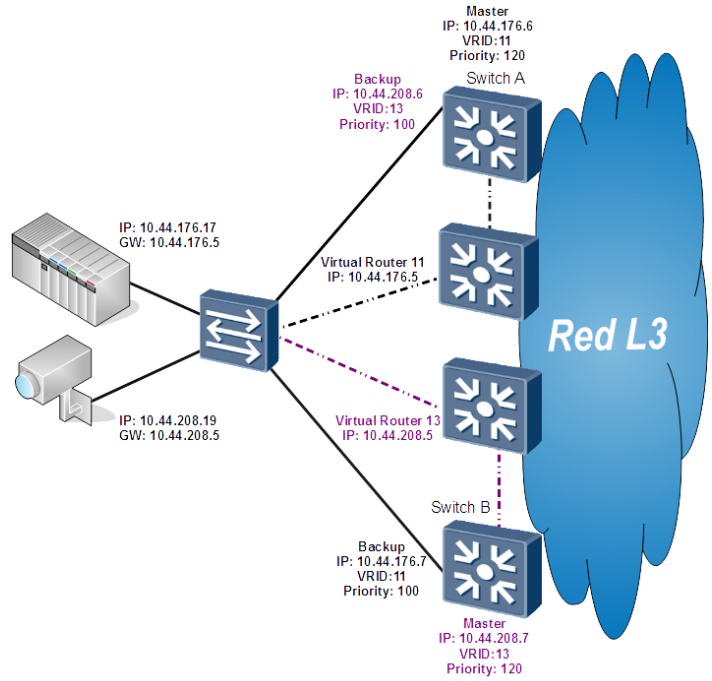


Figura 2-49 Balanceo de carga en VRRP en segmentos de red distintos.

2.4.2.1.4 Convergencia

La convergencia de VRRP estará dado por el Master Down Interval según la fórmula 2-4.

2.4.2.2 Enrutamiento

2.4.2.2.1 Conceptos Básicos

2.4.2.2.1.1 Autonomous Systems (AS)

Un Sistema Autónomo se define como un conjunto de redes IP que poseen una política de rutas independiente y común, utilizando por lo general un único protocolo de enrutamiento interno.

La IANA define un grupo de numeración para ASs de uso privado que van desde 65412 al 65535.

2.4.2.2.1.2 Clasificación de protocolos de enrutamiento

El enrutamiento se puede efectuar de manera estática declarando cada ruta en cada equipo o de manera dinámica intercambiándose las rutas entre los diferentes enrutadores con algún protocolo que lo permita, dentro de este grupo encontramos protocolos estandarizados como OSPF, RIP, IS-IS, BGP, y propietarios como EIGRP.

Los protocolos de enrutamiento dinámico se clasifican de dos formas distintas:

- Por su área de funcionamiento
  - *IGP* (*Internal Gateway Protocol*) para comunicación dentro del mismo Sistema Autónomo.
  - *EGP* (*Exterior gateway protocol*) para comunicaciones entre diferentes Sistemas Autónomos.
- Según su forma de conocimiento de las rutas:
  - *Distance Vector* (Vector-distancia), entrega visión sencilla de la red, se conoce el siguiente salto y la métrica para llegar a la ruta o prefijo de destino.
  - *Link-State* (Estado de enlace), se conoce la topología completa de la red o dentro de un área determinada si es que existen subdivisiones, todos los equipos manejan la misma base de datos.
  - *Path-Vector* (Vector-camino), tiene un funcionamiento similar al de vector distancia, pero además de conocer el siguiente salto conoce el camino para llegar al destino.

El detalle de donde se posiciona cada protocolo según su forma de funcionamiento se puede observar en la figura 2-50.

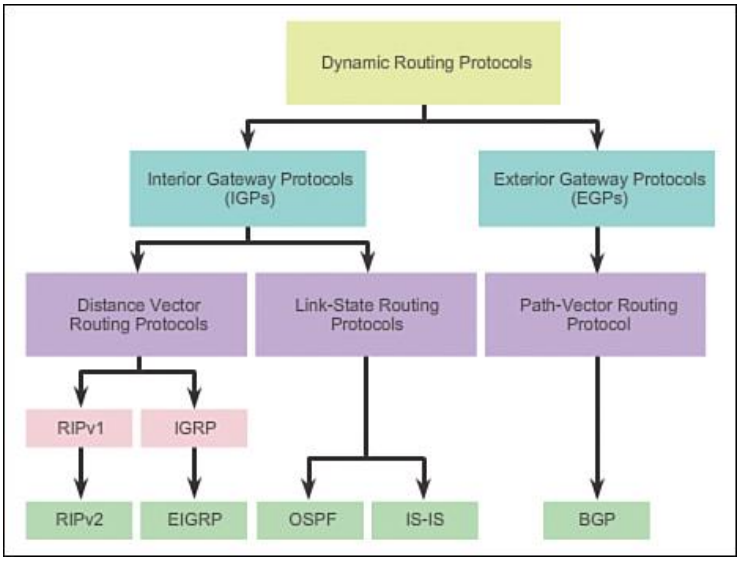


Figura 2-50 Protocolos de enrutamiento dinámico. [76]

Dentro de los diferentes protocolos existentes de libre implementación se estudiarán OSPF y BGP si bien este último no es de su uso común en redes privadas es perfectamente implementable.

2.4.2.2.2 OSPF

Open short path first OSPF, es un protocolo de enrutamiento dinámico especificado en su versión 2 en el RFC 2328. Tiene una filosofía *link-state*, ante cualquier falla en uno de sus enlaces inunda la red con actualizaciones a fin de que se realice el recalculo de rutas. Funciona directamente sobre IP utilizando el protocolo 89.

OSPF construye un árbol de la ruta más corta desde un equipo hasta su destino denominado *SPT* (*Shortest-Path- Tree*) a través del algoritmo *SPF(Shortest-Path-First)*. SPF usa el algoritmo Dijkstra para hacer su cálculo.

En OSPF se maneja el concepto área, pudiendo dividir el dominio OSPF en diferentes áreas, siempre teniendo en cuenta que todas las áreas deben estar unidas al área 0 que se considera el área de backbone, la división se lleva a cabo además de por razones administrativas, para que los cálculos del algoritmo SPF sean más sencillos ya que solo calcula a partir de los equipos que están en su misma área.

2.4.2.2.2.1 Elección de la mejor ruta

La métrica de OSPF es el costo del salto, si es que no se especifica el costo, se calcula como (10^8 / *ancho de banda)* de la conexión física, lo que implica que un enlace FE de 100 Mbps obtendrá un costo de 1, por lo tanto, en caso de ocupar enlaces de mayor capacidad, se debe especificar el costo de cada enlace o cambiar la base para el cálculo ya que el valor del costo no puede ser menor a 1.

2.4.2.2.2.2 Clasificación

Según el funcionamiento que tengan dentro del dominio OSPF los equipos se pueden clasificar de la siguiente manera:

- *Internal Router*: Tiene todas sus interfaces de red conectadas con equipos de su misma área, por lo que solo lleva cálculos SPF en su área.
- *Backbone router*: Tiene todas sus interfaces de red conectadas con equipos del área de backbone, por lo que solo lleva cálculos SPF en dicha área.
- *ABR Area Border Router*: Están conectados a dos o más áreas, realizan los cálculos SPF de manera independiente para cada área y principalmente se utilizan para unir áreas con el área de backbone.
- *ASBR Autonomous System Boundary Routers*: Intercambian información con otros Sistemas Autónomos o redes externas que pueden funcionar con otros protocolos de ruteo dinámico o estático. Los cálculos SPF los hacen en el área a la que pertenecen y pueden estar ubicados en cualquier punto de cualquier área.

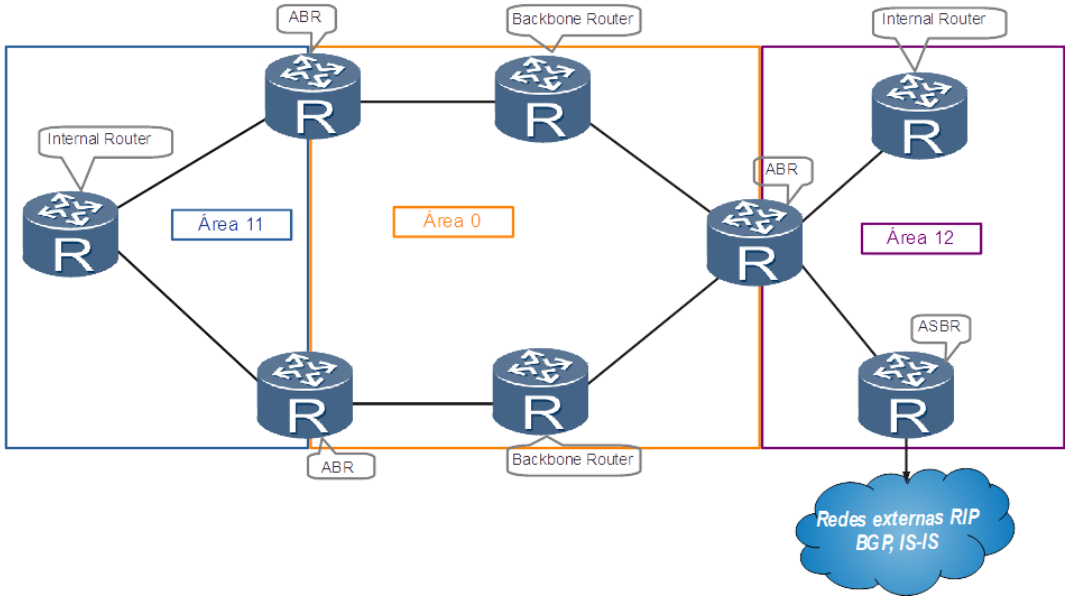


Figura 2-51 Roles de equipos dentro de dominio OSPF según su ubicación y función.

2.4.2.2.2.3 Tipos de mensajes

Para su funcionamiento el protocolo utiliza los siguientes mensajes:

- *Hello*: Realiza descubrimiento de vecinos y mantiene la relación con este, construye las adyacencias para el intercambio de información. Dentro de los parámetros que envía el mensaje se encuentra el *Router-ID* (identificador único del equipo) que debe ser único para

el dominio, el *dead Interval* para declarar el enlace como caído y el tipo y clave de autenticación en caso que se ocupe.

- *DBD* (*Data base description*): Controla la sincronización de las bases de datos de los equipos y entrega información sumarizada de la base de datos, los routers de la misma área tendrán bases de datos del área idénticas.
- *LSR Link State Request* Solicita registros específicos de estados a los equipos.
- *LSU Link State Update* Envía los estados de enlace específicamente solicitados por un LSR o se envía al detectarse algún cambio de la topología, un mensaje LSU contiene uno o más *LSAs* (*Link State Advertisement*).
- *Link State Acknowledgment*: acuse de recibo de los tipos de paquetes antes de descritos.

2.4.2.2.2.4 Caso de redes de acceso Múltiple

Para el caso de redes de acceso múltiple ya sean redes broadcast o no, puede existir un excesivo envío de LSUs ya que por cada envío de LSU debe existir una confirmación de recepción, para solucionar el problema se jerarquiza la topología eligiendo un router como designado DR y un router designado de backup BDR, quedando los demás equipos de la topología con la denominación de *Drothers*.

Los *Drothers* envían LSUs por la dirección a la 224.0.0.6 al DR y BDR y el DR reenvía dichos LSUs a todo el resto de equipos de la topología a través de la dirección 224.0.0.5, que es la dirección que multicast que todos los equipos que pertenezcan al dominio OSPF deben estar escuchando.

2.4.2.2.2.5 Establecimiento de adyacencias:

Lo primero a tener en cuenta es que se deben cumplir una serie de requisitos para establecer la adyacencia OSPF, dentro de las más importantes tenemos:

- El *Router ID* debe ser distinto para los 2 equipos que establecen la relación.
- Las interfaces de conexión deben estar en la misma área.
- Los intervalos de *Hello* y *dead interval* deben ser iguales.
- En caso de autenticación, deben coincidir los tipos y claves.

Las adyacencias para redes Multiacceso Broadcast y *NBMA (No Broadcast Multi Acces)* difieren levemente, pero se tomará como ejemplo la redes broadcast que son las que se ocuparan para las pruebas que se realizaran. En base en la figura 2-52 el establecimiento sigue el siguiente proceso:

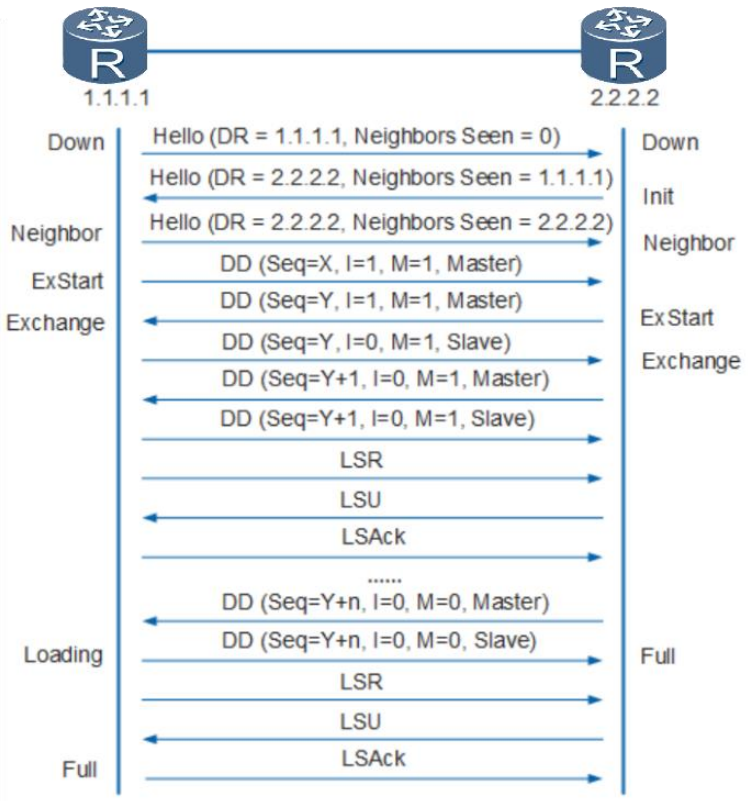


Figura 2-52 Establecimiento de adyacencias OSPF [77].

i. El router 2.2.2.2 recibe un mensaje de *Hello* de 1.1.1.1, como la relación aún no se establece el parámetro de *router ID* del vecino será 0.
ii. Se llega a la etapa de Neighboor o 2-way, tanto 1.1.1.1 como 2.2.2.2 incluyen ambos routers IDs en los mensajes de *Hello*, con lo que ya se determina que hay comunicación bidireccional.
iii. Se pasa *Exstart*, donde uno de los dos equipos se elige como Master y el otro como Slave, esta elección del Master-Slave es solamente para seleccionar el número de secuencia para compartir el DBD.
iv. El siguiente paso *Exchange*, se envían los mensajes DBD con el número de secuencia definido en la etapa anterior
v. En la etapa de *Loading* se solicita información detallada al vecino en función de lo recibido en el mensaje DBD con una solicitud LSR.
vi. Luego que las bases de datos estén sincronizadas y sean iguales se llega al estado Full y la adyacencia queda establecida.

2.4.2.2.2.6 LSAs

Los *Link State Advertisement LSAs* son fundamentales para el funcionamiento de OSPF, a partir de estos se construye la base de datos *LSDB (Link State Database)* que permite hacer los cálculos de SPT y SPF, existen 11 tipos definidos, pero nos centraremos en los 6 más comunes

i. LSA tipo 1 – *Router-LSA*:

Es el LSA más básico de OSPF y sin su existencia el protocolo no funcionaria, indica las conexiones de cada nodo del área y su costo para alcanzarlo. Puede describir 3 tipos de conexiones, Stub, conexiones con un o ningún vecino (loopback, redes directas, etc), Transito, donde existe más de un vecino y Punto a punto.

Este tipo de LSAs son reenviados solo en el área en la que fueron generados.

ii. LSA Tipo 2 – *Network-LSA*:

Detalla los segmentos de red/mascara que existen en el área y que equipos tienen acceso a cada segmento. En el caso de las redes multiacceso son generados por los DR.

Este tipo de LSAs son reenviados solo en el área en la que fueron generados.

iii. LSA Tipo 3 – *Summary-LSA*:

Son LSAs generados por los ABRs desde un área a otra distinta, sumarizan la información entregada los LSAs tipo 1 y tipo 2 y realizan un anuncio sencillo con la red/mascara más el costo desde el punto de vista del ABR hasta la red a alcanzar. Dentro de la información sumarizada no se encuentra la topología.

iv. LSA Tipo 5 – *External-LSA*:

Son LSAs generados por los ASBRs que detallan redes externas al dominio OSPF, básicamente pública la red externa con su máscara, el *Router ID* del ASBR y la métrica.

Los LSAs tipo 5 viajan intactos por todas las áreas.

v. LSA Tipo 4 – *ASBR Summary-LSA*:

Son generados por los ABRs, no por los ASBRs, sumarizan la información de los LSAs tipo 5 e indican como llegar al equipo ASBR que publica las rutas externas.

vi. LSA Tipo 7 - *NSSA External-LSA*:

Son muy similares a los LSA tipo 5 pero se usan en las áreas tipo *NSSA* (*Not-So-Stubby Area*), implementan un mecanismo llamado *fordward address* para indicar a la topología del área como se debe enrutar hacia el ASBR.

2.4.2.2.2.7 Tipos de Áreas

Como se indicó en los párrafos anteriores la división por áreas ayuda a la administración de la red, disminuye y simplifica los cálculos de SPF y evita el tránsito de LSAs tipo 1 y 2 a otras áreas, OSPF distingue 4 tipos de áreas distintas.

i. *Backbone*: Área 0 a la que debiesen tener conexiones todas áreas a través de un o más ABRs.

ii. *Standard*: Área común que permite el ingreso de LSAs tipo 4 y 5.

iii. *Stub*: Si no es suficiente con la limitación hecha con la separación por áreas se puede crear un área tipo Stub que limita además la entrada de LSAs tipo 4 y 5, por lo que los equipos dentro de esta área no sabrán como llegar a los ASBRs. Para llegar a las rutas externas existirá una ruta por defecto hacia el ABR quien se encargará de encaminar los paquetes hacia los ASBRs.

iv. *Not-So-Stubby Area (NSSA)*: Similares a las rutas Stub, ya que no aceptan LSAs tipo 4 y 5 dentro de su área ni el ingreso de estos LSAs desde áreas externas. Este tipo de áreas además no inyectan una ruta por defecto, pero si permite enrutar a los equipos de su área a redes externas a traves del ASBR utilizando los LSAs tipo 7. Estos LSAs serán transformados a LSAs tipo 5 para ser enviados a otras áreas, por el ABR con el *Router ID* más alto.

2.4.2.2.2.8 Convergencia:

OSPF dará un enlace como caído cuando se cumpla su *Dead Interval* sin recibir mensajes de *hello*. Por defecto los mensajes *Hello* son enviados cada 10s y el *dead Interval* es de 40s, por lo tanto la convergencia de OSPF no se dará antes de 40 segundos. Tanto el intervalo de Hello como *Dead Interval* son modificable según las capacidades del equipo.

2.4.2.2.3 BGP

Boder Gateway Protocol BGP está definido en el RFC 4271 y es comúnmente usado como EGP (Exterior Gatweway Protocol).

Se basa en el intercambio de paquetes a través de Sistemas Autónomos y necesita algún protocolo IGP para converger, aunque en caso de tener pocos equipos puede ser suficiente con rutas estáticas o directas. BGP solo publica la mejor ruta.

2.4.2.2.3.1 Sesiones y publicación de prefijos

Para realizar la publicación o anuncio de prefijos entre equipos, BGP establece adyacencias con pares *peers*, para lo que establece conexiones TCP en el puerto 179 (del peer) dejando la gestión

de la conexión a la capa de transporte. Si el peer está dentro del mismo AS será una sesión interna *IBGP (Internal BGP)* y en caso de que la sesión sea con un peer de otro AS será una sesión externa *EBGP (External BGP)*.

El intercambio de prefijos de BGP difiere según el tipo de sesión que se establezca, para el caso de los prefijos aprendidos por EBGP desde un vecino, estos pueden ser publicados a otros vecinos EBGP o IBGP, al mismo tiempo los prefijos aprendidos por IBGP pueden ser publicadas por EBGP , pero los prefijos aprendidos desde un vecino mediante IBGP no pueden publicarse a otro vecino IBGP, esto se realiza para evitar la reinyección de prefijos en el AS, ya que IBGP no tiene ningún mecanismo para evitar los loops de enrutamiento, que si tiene EBGP a través del atributo *As-Path* que se explicará en breve.

Para solucionar este problema existen 3 alternativas:

i. Realizar un *full-mesh* entre todos los equipos IBGP:

Esto se puede realizar ya que no tiene que existir necesariamente una conexión física entre 2 vecinos IBGP, en este caso como cada equipo tendrá una sesión independiente con los demás equipos dentro del AS los equipos podrán publicar sus prefijos propios y los que aprenda por EBGP, pudiendo todos los equipos aprender todos los prefijos sin riesgo de reinyección.

La principal desventaja que tiene este método es la poca escalabilidad ya que por cada equipo adicional que se integre al AS tendrá que existir una nueva sesión de este hacia todos los equipos del AS, haciendo que con muchos equipos la red sea administrativamente difícil de manejar. La razón de crecimiento será según la fórmula 2-5 donde n es el número de equipos:

$$\frac{n*(n-1)}{2} \qquad (2\text{-}5)$$

Como ventaja se tiene un buen nivel de resiliencia ya que si un equipo deja de funcionar solo se pierden los prefijos que este pública.

ii. Route Reflector:

Son uno o más routers que realizaran el reenvío de las rutas que le sean publicadas por IBGP al resto de equipos dentro del AS, complejiza un poco la configuración para evitar los bucles ya que agrega 2 atributos nuevos a las sesiones IBGP que son el *Cluster-ID*, que le servirá el o los equipos que actúen como Route reflector para saber si ya ha reflejado previamente él prefijo y el *Originator-ID* que les entregara a los Route reflector la información de quien público el prefijo para no reenviárselo nuevamente.

Su ventaja principal es la escalabilidad ya que solo se necesita que existan sesiones IBGP de los routers de la red hacía el Route reflector.

Como desventaja tenemos que disminuye la resiliencia ya que necesitamos que siempre esté en funcionamiento el Route reflector, una caída de este se traduce en que el resto de los routers de la red ya no podrían reenviar prefijos dentro del AS.

iii. Confederaciones:

Dividimos la topología en AS más pequeños y agregaremos atributos para saber si las rutas publicadas ya pasaron por el sistema autónomo de recepción. Esta alternativa es la menos utilizada.

2.4.2.2.3.2 Tipos de mensajes

Dentro de BGP existen 4 tipos de mensajes

i. *Open*, mensaje tipo 1

Se usa para establecer una sesión BGP sobre la conexión TCP previamente lograda. Envía los parámetros básicos para establecer la adyacencia como versión de BGP, AS, *holddown* (tiempo máximo antes de declarar la sesión caída), *router-id* (identificador único del equipo) y la *capabilities* (capacidades) que tiene el equipo, como protocolos que maneja, solicitud de refresco de prefijos, etc.

Existirá un mensaje open en cada sentido para establecer la adyacencia.

ii. *Keep alive*, mensaje tipo 4

Es el mensaje más sencillo de BGP y se usa básicamente para mantener la sesión BGP entre los peers, aunque en el inicio de la conexión también se utiliza para confirmar la recepción del mensaje de Open.

Habitualmente se envía cada 30 segundos de manera bidireccional entre ambos peer, es un mensaje pequeño y dada su periodicidad de envío ocupa muy poco ancho de banda.

iii. *Notifications*, mensaje tipo 3

Se utiliza para la notificación de errores que causan el cierre de la conexión, algunos ejemplos son errores en el mensaje Open, cumplimiento del tiempo de *holdown*, errores en los mensajes *update*, etc.

iv. *Updates*, mensaje tipo 2

Es el más extenso de los mensajes BGP y es a través de este que se realiza el envío de actualizaciones de prefijos, ya sea porque son nuevos dentro de la topología o porque deben eliminarse, además incluye en sus anuncios los atributos de los prefijos, haciéndolo de manera bastante eficiente ya que ordena los atributos comunes que puedan existir y luego indica a que prefijos aplican.

2.4.2.2.3.3 Establecimiento de adyacencias

Para establecer sesiones o adyacencias BGP pasa por diferentes estados que se describen a continuación:

i. En el estado Idle no se aceptan conexiones, ya sea porque no está configurada la interfaz, no esté funcionando BGP en el equipo, etc.

ii. El primer estado para establecer la sesión BGP es *Connect*, donde se intenta establecer la conexión TCP, si esta se logra se envía un mensaje de Open al peer y se pasa al estado *Open Sent*.

iii. En el estado *Open Sent* espera a que el peer envíe su mensaje de Open. Al recibirlo se revisa que las características propuestas por el peer, *capabilities*, timers, etc. sean correctas y compatibles con el equipo que inicio la conexión. En caso de que el *holdown* sea distinto al del peer se conserva el menor, si todo está correcto se le envía un *Keep alive* al peer y se pasa al estado *Open Confirm*.

iv. En el Estado *Open Confirm* el equipo espera a que el peer realice su propia revisión del mensaje *Open* y si esta es correcta enviara al equipo un *Keep alive* pasando la sesión a estado *Established* quedando formada la adyacencia.

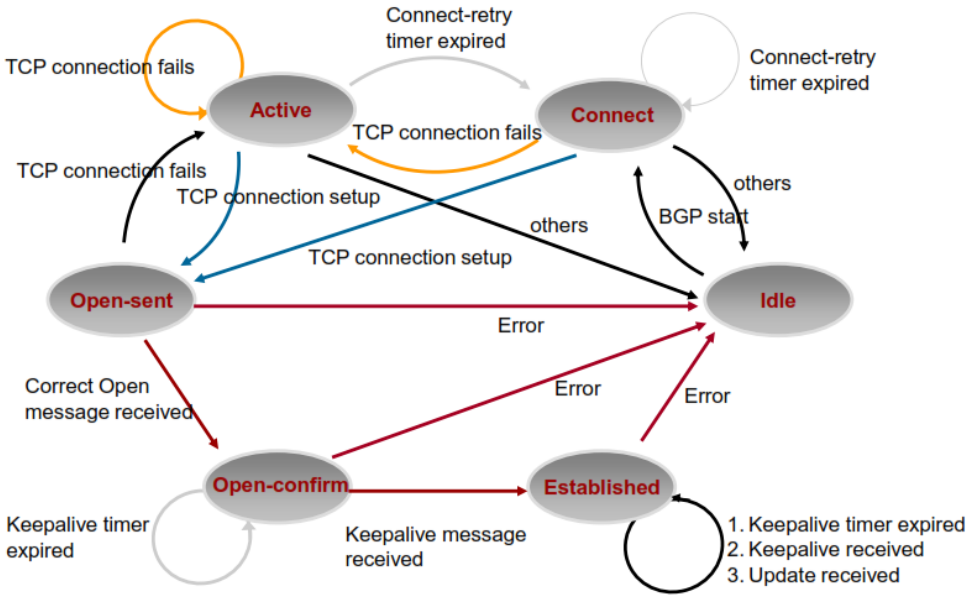


Figura 2-53 Estados para establecimiento de adyacencias BGP [78]

En caso de que exista algún error en cualquiera de los pasos anteriores, por ejemplo, por alguna incompatibilidad de *capabilitites*, errores en los numero de AS, etc. se pasa al estado Active donde espera que se corrija el error para volver establecer la sesión.

2.4.2.2.3.4 Atributos

Los atributos describen los caminos para alcanzar las rutas y se usan para el cálculo del algoritmo de decisión de BGP, existen 4 tipos de atributos:

i. *Well-known Mandatory*: Deben ser reconocidos por todos equipos que tengan sesiones BGP. Estarán en todos los mensajes *Update*.

ii. *Well-known Discretionary*: Deben ser reconocidos por todos los equipos que tengan sesiones BGP. Pueden o no encontrarse en los *Update*.

iii. *Optional Transitive*: Estos atributos pueden o no ser reconocidos por los peers BGP. Se deben preservar y publicar a otros vecinos inclusive si no son reconocidos.

iv. *Optional Non-Transitive*: Estos atributos pueden o no ser reconocidos por los peers BGP. Si se recibe un anuncio con este atributo, no debe ser enviado a otros vecinos si no se reconoce localmente.

Dentro de los atributos más importantes para la realización de las pruebas que se detallaran en el capítulo 4 encontramos:

- *Origin*: Atributo Well-known Mandatory, Indica como el equipo aprendió el prefijo, la letra *i* indicara que fue aprendida de forma interna ya sea declarando el prefijo en el equipo o por un IGP, la letra *e* indicará si fue aprendido por EGP, el signo de interrogación *?* indica que el prefijo no se aprendió ni por IGP ni por EGP, es el caso por ejemplo cuando se importan las rutas desde otros protocolos, o son rutas directas o estáticas.

- *AS-Path*: Atributo Well-known Mandatory, este atributo solo se modifica entre sesiones EBGP, añadiendo su número de AS al mensaje, con lo que el equipo sabrá porque sistemas autónomos ha pasado el paquete. El atributo sirve tanto para la detección de loops, ya que los equipos no aceptaran prefijos que ya hayan pasado por su AS, como para políticas de enrutamiento ya que se podrá saber a cuantos sistemas autónomos de distancia está el prefijo que se quiera alcanzar.

- *Next-Hop*: Atributo Well-known Mandatory, este atributo solo se modifica entre sesiones EBGP, Indica el salto siguiente para alcanzar el prefijo de destino, es especialmente útil cuando el siguiente salto no utiliza BGP.

- *Local-Preference*: Atributo Well-known Discretionary, solo es válido dentro del sistema autónomo en conexiones IBGP, indica cual es la salida que tienen mayor preferencia para salir del AS, un número mayor indica mayor preferencia.

- *MED (Multi-Exit-Discrimin)*: Atributo, Optional Non-Transitive, el atributo se utiliza cuando se tiene más de una conexión entre ASs, les indica a los equipos fuera del AS que ruta tomar para ingresar el tráfico al AS. Un número menor indica mayor preferencia.

- *PrefVal*: Atributo propietario de Huawei y es válido solo en el equipo donde es configurado, se asigna un valor numérico directamente al peer, a mayor número mayor preferencia.

2.4.2.2.3.5 Elección de la mejor ruta

BGP presenta muchos atributos que influyen en la decisión, por lo que existe una jerarquía para esta, el protocolo solo publica a sus vecinos el mejor prefijo según el resultado de su algoritmo, el orden que tienen los equipos para tomar su decisión es el siguiente:

i. Descarta las rutas que no se pueda alcanzar el *Next-Hop*
ii. El valor del atributo propietario de Huawei *PrefVal* más alto, lo que hace que no sea necesario revisar los atributos estándar de BGP, en caso de que este valor en 2 prefijos sea igual se pasa al siguiente atributo.
iii. Mayor *Local-Preference*
iv. Preferencia de rutas sumarizadas sobre las no sumarizadas, al contrario que la tabla de rutas general.
v. Ruta con el menor número de *AS-Path*.
vi. Rutas aprendidas por IGP, luego por EGP y finalmente origen desconocido (generalmente rutas importadas).
vii. Menor valor de MED.
viii. Rutas aprendidas por EBGP sobre las aprendidas por IBGP.

2.4.2.2.3.6 Convergencia

Una adyacencia se dará por caída ya sea por un mensaje de *Update* que reciba desde un vecino o porque el tiempo de *holdown* dado por la no respuesta de 3 *Keepalives* se cumpla, al igual que en otros protocolos esos parámetros son modificables según la marca/modelo del equipo.

2.4.3 Protocolos Auxiliares

Para las pruebas a realizar y la propuesta de configuración se estudiará una serie de protocolos adicionales necesarios para el funcionamiento de la red.

2.4.3.1 **Eth-Trunk:**

Es la versión de Huawei para la construcción de *LAGs* (*Link agregation Groups*). Un LAG es una suma de enlaces físicos que permiten formar un solo enlace lógico, lo que trae como ventaja un aumento del ancho de banda disponible y mayor nivel de redundancia sin tener que configurar protocolos anti-loops en capa 2 (RSTP, MSTP, SEP).

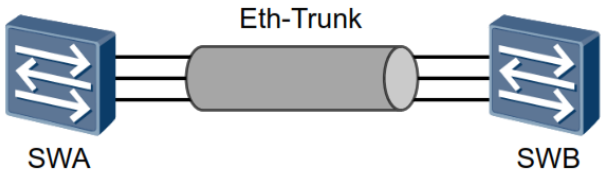


Figura 2-54 Ejemplo enlace Eth-Trunk. [79]

Eth- trunk tiene 2 modos de configuración, manual o utilizando el protocolo *LACP (Link Aggregate Control Protocol)*, especificado en IEEE 802.3ad.

2.4.3.1.1 Modo manual

En el modo manual se agregan los enlaces físicos al LAG Eth-Trunk y todos los enlaces participan en el envío de tráfico, en caso de que uno de los enlaces del grupo falle, la carga es asumida por los enlaces restantes. La desventaja del modo manual es que solo se pueden detectar fallas por desconexión del link, pero no puede detectar fallas por una mala conexión, por ejemplo, que uno de los enlaces miembros se conecte a un equipo incorrecto.

2.4.3.1.2 Modo LACP

Se puede configurar una mayor granularidad de parámetros y detectar cualquier tipo de falla en los links que forman el LAG.

Cada equipo que participe en la conexión LACP tendrá un *System-ID* formado por su prioridad y MAC, el equipo con mayor prioridad (menor valor numérico) tomara la función de Master LACP denominado *Actor*.

Cada equipo que forme el LAG intercambia periódicamente tramas de control *Link Aggregation Control Protocol Data Units (LACPDU)* con su extremo que contienen el *System-ID* el número de grupo LAG, las interfaces asignadas a este y una prioridad para cada interfaz. Con estos parámetros se realiza la negociación entre los equipos y se determina que interfaces y su prioridad en el LAG.

El modo LACP permite tener un grupo de interfaces activas y un grupo como backup, en caso de fallar la conexión entre cualquiera de las interfaces activas la de Backup toma su lugar.

2.4.3.2 **CSS**

Cluster Switch System CSS es un protocolo propietario de Huawei para la redundancia de equipos, dos equipos distintos pueden formar lógicamente un solo equipo, simplificando la configuración de la topología, no siendo necesario la configuración de protocolos como VRRP, MSTP o SEP.

El protocolo está definido para equipos de alta gama, generalmente utilizados como Core, la conexión se puede realizar mediante la tarjeta controladora de los equipos o mediante cualquier

interface presente en las tarjetas de servicio, por lo que CSS puede configurarse a larga distancia a través de interfaces de fibra óptica solo limitado por las pérdidas propias del enlace. Este tipo de equipos cuenta al menos con una tarjeta de procesamiento principal *MPU* (*Main Processing Unit*), aunque como son equipos de Core lo normal es que cuente almenos con una MPU de respaldo.

Dentro de la configuración de CSS existirá un equipo Master y uno Backup que forman el Cluster, lo que será transparente para los equipos aguas abajo, cada equipo del cluster tendrá un identificador CSS ID y una prioridad CSS *Priority*, el equipo con mayor prioridad se convertirá en el Master de la topología y será su MPU la que controle el funcionamiento del Cluster, en caso de no tener prioridad asignada el equipo con menor valor de MAC será el Master. Al iniciarse el Clúster La IP y MAC del Master será la del switch lógico, la que después puede ser modificada.

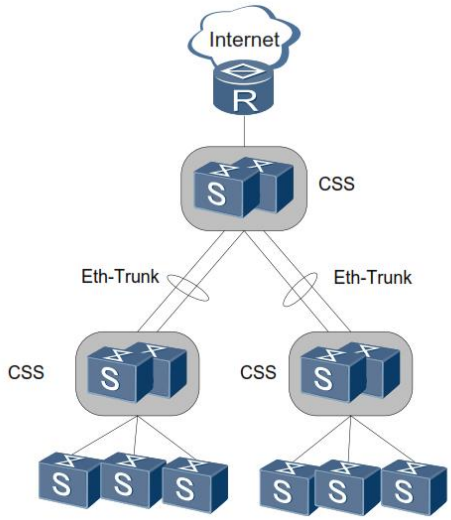


Figura 2-55 Ejemplo configuración CSS. [18]

En caso de falla de la MPU principal del Master, toma su lugar la MPU local en *Standby* y solo ante la falla de ambas, el control del Cluster pasa al equipo en Backup.

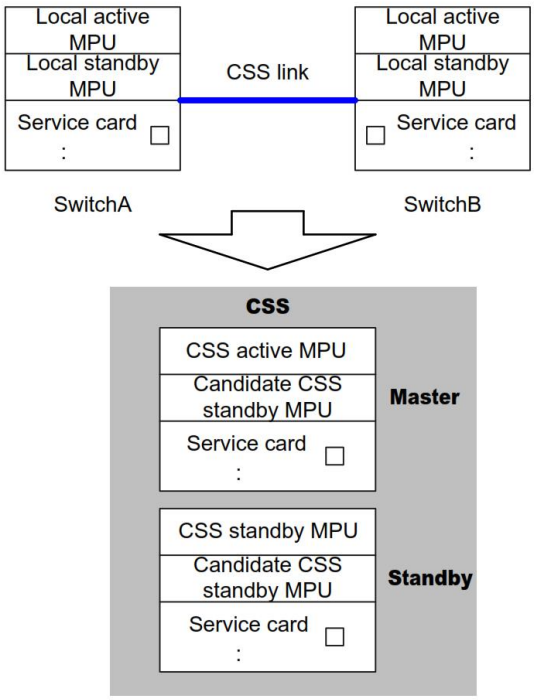


Figura 2-56 Prioridades para tomar el rol de Master CSS. [18]

Para el establecimiento de la topología en un inicio CSS detecta un paquete denominado *link detection* que indica que hay una conexión CSS, luego se envían una serie de paquetes denominados *Competition packets* usados para la negociación entre los equipos del Cluster y determinar qué equipo será el Master. Una vez establecido el Cluster los equipos se envían periódicamente paquetes *hello* denominados *Heartbeat packet* para revisar continuamente el estado del enlace.

En caso de producirse algún cambio y/o anomalía en cualquiera de los equipos que son parte del cluster, CSS genera inmediatamente paquetes de notificación *Event notification packets*, para que se realicen las acciones correspondientes.

En el cluster CSS ambos equipos tendrán la misma dirección IP y MAC, al producirse un fallo en el link que forma el Cluster, la MPUs del equipo de Backup también tomará el papel de Master, como habitualmente CSS se ocupa en la capa de Core, se provocará un conflicto de IP y MAC que puede provocar la falla completa de la red. Para evitar este problema CSS utiliza el protocolo *Multi-active detection (MAD)*, que puede funcionar de dos maneras:

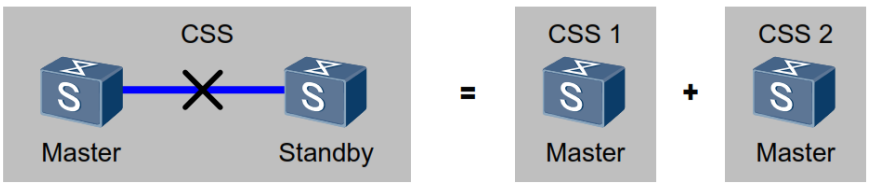


Figura 2-57 Ejemplo de falla de conexión CSS. [18]

i. *Direct Mode*:

Se configura un link físico directo entre ambos equipos del Cluster, distinto al link CSS. Al producirse la falla los paquetes MAD se envían cada 1s por ambos equipos, donde se incluye el CSS ID, MPU ID, prioridad y la MAC física del equipo, una vez recibidos los paquetes MAD el equipo que tiene la menor prioridad apaga sus interfaces de servicio a excepción de las que se le haya indicado previamente en la configuración.

ii. *Relay Mode*:

En el equipo denominado Relay se configura un enlace Eth-Trunk hacia ambos equipos pertenecientes al cluster CSS.

En condiciones normales los equipos pertenecientes al Cluster se envían cada 30s paquetes MAD a través del equipo Relay, que son descartados por el equipo de destino.

Una vez detectada la falla los equipos comienzan a enviar los paquetes MAD inmediatamente cada 1s y estos ahora son procesados, al igual que en el caso anterior el equipo que detecta que su prioridad es menor apaga sus interfaces de servicio a excepción de las que se le haya indicado previamente en la configuración.

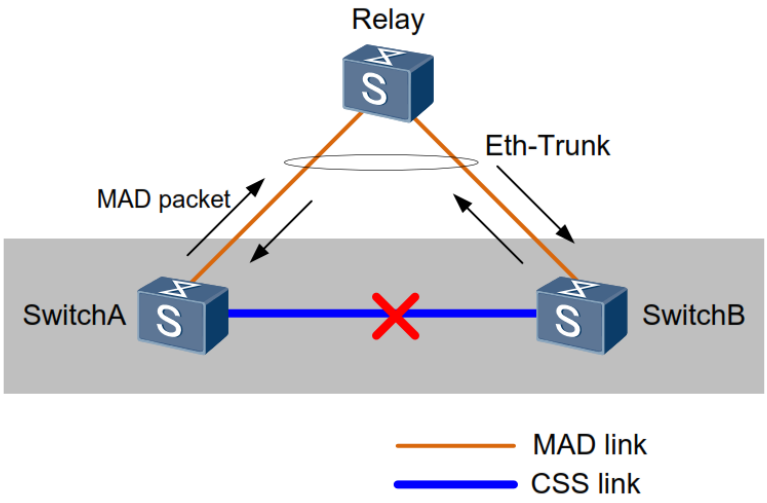


Figura 2-58 CSS MAD en modo Relay. [18]

2.4.3.3 **BFD**

BFD (*Bidirectional Forwarding Detection*) está definido en el RFC 5880, es un protocolo principalmente utilizado para detectar fallos en conexiones entre equipos. BFD solo detecta fallos, no realiza ninguna acción a partir de ello, por lo que su uso es de apoyo a otros protocolos con el fin de mejorar sus tiempos de convergencia, algunos de estos protocolos son VRRP, OSPF, BGP, IS-IS, etc.

BFD establece una sesión entre 2 equipos pares peers que pueden estar a uno o múltiples saltos, ambos peers envían periódicamente paquetes de control a su extremo que son recepcionados por este, en caso de no recibir paquetes por un intervalo de tiempo determinado la sesión se declara como caída e informa al protocolo que estaba realizando el seguimiento a la sesión, para que este puede tomar alguna acción. BFD puede funcionar con autenticación en caso que se requiera.

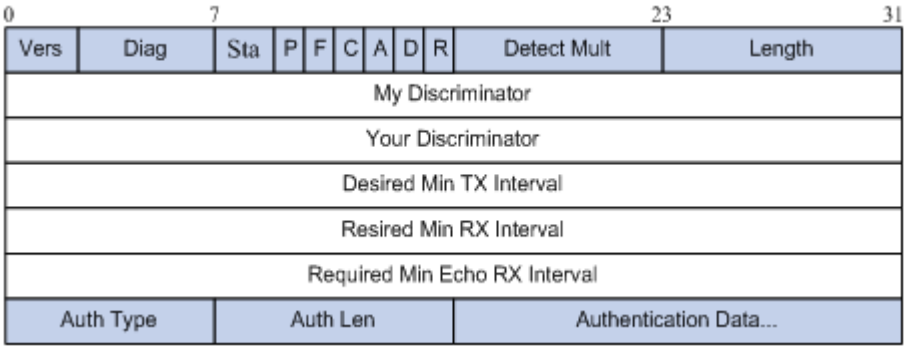


Figura 2-59 Paquete BFD

Para establecer la sesión y determinar los intervalos de envío, recepción y en qué momento declarar la sesión como caída BFD tiene los siguientes parámetros de configuración:

- *Local/My Discrimantor*: En cada Peer se pueden establecer múltiples sesiones BFD, el *Discriminator* local se asocia a la sesión especifica dentro del equipo, este valor debe ser igual al valor *Your Discrimnator* o *Remote Discriminator* del otro extremo de la sesión.
- *Remote/Your Discriminator*: Número asociado al discriminador remoto, que es el local del otro extremo de la sesión.
- *Min Rx Interval*: Intervalo de recepción de los paquetes de control enviados por el peer con el que se establece la sesión. Debe ser igual al valor de transmisión de dicho peer.
- *Min Tx Interval*: Intervalo de transmisión de los paquetes de control enviados hacia el peer con el que se establece la sesión. Debe ser igual al valor de recepción de dicho peer.
- *Detect Multiplier*: cantidad de periodos sin recepción del paquete de control con los que se declarará la sesión caída.

Es importantes señalar que los intervalos de envío de los peer que establecen la sesión no tienen que ser iguales y que el valor de *Detect Multiplier* presenta una forma sencilla de ajustar posibles problemas de *flapping* de la sesión.

2.4.3.4 **IP FRR LFA**

IP FRR LFA (*Fast Reroute Loop-Free Alternates*) tiene su especificación básica en el RFC 5286, Es un protocolo que permite alcanzar tiempos de convergencia de milisegundos.

IP FRR realiza un cálculo previo de un camino alternativo en caso de detectarse una falla en alguna ruta establecida, por ejemplo, en el caso de OSPF al detectar la caída de una ruta deberá volver a calcularse el SPT lo que tomara más o menos tiempo dependiendo del tamaño y cantidad de equipos

del área, esto es simplificado por IP FRR ya que tiene precalculado el camino alternativo en caso de falla y no tiene que esperar a que el protocolo realice el cálculo, una vez que SPT termine su cálculo se volverá a la ruta que este determine, que puede ser o no por el mismo camino . Este camino alternativo es lo que se conoce como Loop-Free Alternate LFA.

Cuando se activa IP FRR en un equipo, este puede calcular más de un LFA si es que está disponible, los caminos alternativos LFA puede ser determinado por prefijo o por link.

IP FRR es un protocolo que puede utilizarse con muchos protocolos de ruteo distintos como son OSPF, BGP, IS-IS además en combinación con la tecnología MPLS. Es importante señalar que el protocolo solo se encarga de tener precalculado el camino alternativo, pero no influye en el método de detección de la falla, si se quiere tener una convergencia veloz y el cuello de botella está en la detección se debe tener un método adicional para la detección, como BFD o ajustar los timers del protocolo de ruteo.

2.5 QoS en Redes IP

Si bien la red a evaluar en el caso práctico está sobredimensionada, es importante, a lo menos, dejar a ciertos aspectos de la calidad de servicio QoS (Quality Of Service) para asegurar un buen comportamiento de la red para posibles crecimientos futuros. La Orientación de la revisión será servicios diferenciados que es lo que se puede implementar en la red.

2.5.1 Arquitectura de QoS

Dentro de la arquitectura de Qos podemos encontrar:

Mejor esfuerzo *Best effort*: No existe priorización, todo el tráfico se trata de la misma manera

Servicios Integraddos *IntServ*: Su funcionamiento se basa en reserva de recursos en cada equipo de red, por lo que la garantía de QoS es casi completa, su desventaja es que requiere una señalización para que se reserven recursos en el camino del tráfico, por lo que es difícil de escalar.

Servicios Diferenciado *DiffServ*: El tráfico viaja etiquetado con una prioridad por los equipos que lo priorizan según las marcas, no existe reserva de recursos ni se comparte información del estado de los equipos de red. Es mucho más sencillo de escalar y es suficiente para muchas aplicaciones.

2.5.2 Manejo de QoS

El proceso del manejo de QoS tiene 3 pasos:

i. Clasificación y marcado
ii. Gestión del trafico
iii. Gestión de colas

2.5.2.1 Clasificación y marcado

2.5.2.1.1 Clasificación

La clasificación se puede hacer de muchas maneras, por ejemplo, a nivel de capa 2 podemos clasificar por

- MAC de origen o destino
- VLAN
- prioridad de VLAN
- mediante ACLs

Y en capa 3 tenemos

- DSCP
- IP de origen o destino
- Mediante ACLs

- protocolo

Cabe indicar que si los equipos no disponen de clasificadores especiales la QoS se manejara en capa 2 mediante la prioridad de VLAN y en capa 3 por el DSCP.

2.5.2.1.2 Marcado

Una vez clasificado se procede a realizar el marcado esto se realiza remarcando ya sea en la trama ethernet o en el paquete IP.

Si se realiza el marcado en capa 2 se sobrescribe los 3 bits del campo prioridad de la trama ethernet 802.p con un valor del 1 al 7 donde 7 es la mayor prioridad. Las prioridades 6 y 7 están reservados para el tráfico de control de la red.

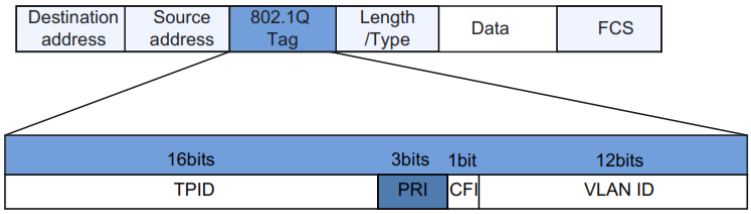


Figura 2-60 Campo de prioridad de VLAN [81]

Si se realiza el marcado en capa 3 se sobrescribe el campo de 6 bits DSCP del paquete IP.

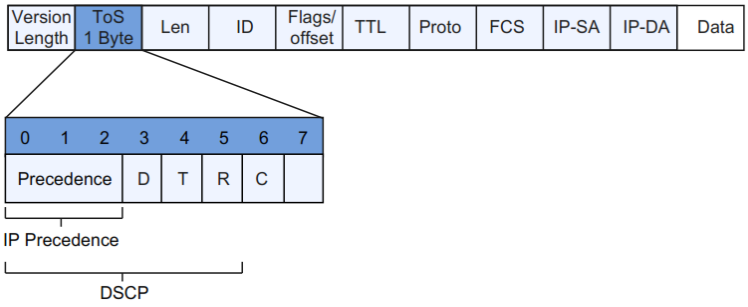


Figura 2-61 Marcado de prioridad en capa 3. [80]

Si bien con 6 bits pudiese obtenerse hasta 64 valores distintos, actualmente se definen hasta el número 48, los primeros 3 bits indican la prioridad de reenvió del paquete al igual que en capa 2 y los bits 3 y 4 la probabilidad de descarte, entre mayor sea el valor que formen estos 2 bits mayor probabilidad de que en caso de congestión el paquete sea desechado.

PHB Per-Hop Behaviors es la visión global por salto del marcado de los DSCPs. Define 3 clases de servicio *Expedited fordwarding* (*EF*), *Assured Fordwarding* (*AF*) y *Best effort*.

- Expedited fordwarding reenvío está definido en el RFC 3246 y es la clase con mayor nivel de prioridad, baja latencia, bajo jitter y ancho de banda garantizado.

- Assured Fordwarding o reenvío asegurado está definido en el RFC 2597, está dividido en 4 clases de reserva de ancho de banda y a su vez 4 subdivisiones según la probabilidad de descarte de paquetes.

Application	L3 Classification			L2
	IPP	PHB	DSCP	CoS
Routing	6	CS6	48	6
Voice	5	EF	46	5
Video Conferencing	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31*	26	3
Call Signaling	3	CS3*	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Best Effort	0	0	0	0
Scavenger	1	CS1	8	1

Figura 2-62 Recomendación de QoS [83]

2.5.2.2 **Gestión del tráfico:**

Existen básicamente dos formas de realizar la gestión del tráfico *Traffic Policing* y *Traffic Shapping*.

2.5.2.2.1 Traffic Policing

Consiste básicamente en estar revisando el tráfico cumple con los parámetros permitidos según su clasificación, generalmente relacionado al throughput, en caso de sobrepasarlo se realiza un descarte selectivo.

2.5.2.2.2 Traffic Shapping

Este método básicamente consiste en introducir demoras o limitaciones de throughput para evitar peaks de tráfico en la red antes de descartarlo, se implementa a través del algoritmo *Token bucket* o *leaky bucket*.

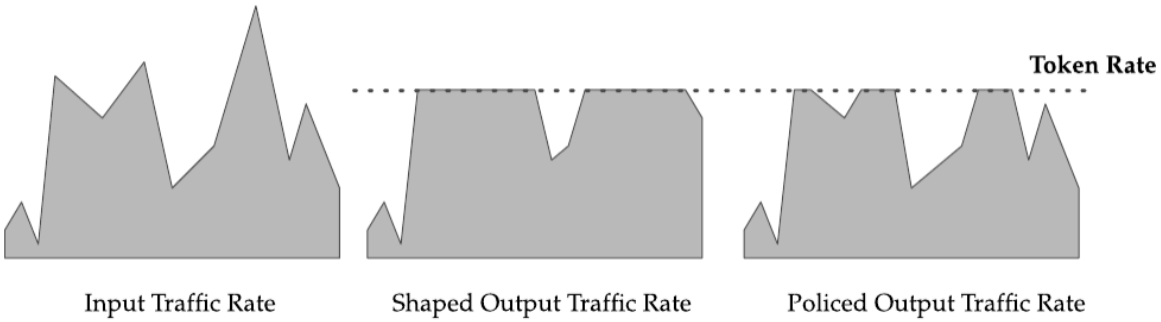


Figura 2-63 Gestión de tráfico por Traffic Shapping y Traffic Policing. [19]

Leaky Bucket: Regula thorugput según una tasa de tráfico limite, si el thorugput es mayor al límite, lo disminuye hasta el valor máximo y almacena el exceso de paquetes en un buffer, si el buffer se llena, el tráfico es descartado.

Token Bucket: Es un algoritmo para el descarte selectivo de tráfico, acepta paquetes que no excedan el throughput limite, pero además acepta pequeñas ráfagas que lo excedan si tiene disponibilidad de Tokens.

Se tiene un balde de tokens que se van almacenando, si la tasa de tráfico es menor a la de generación de tokens el tráfico siempre será renviado y además quedan tokens en el balde de reserva, en caso de que posteriormente existan ráfagas a una tasa mayor a la de generación de tokens, se procesara el tráfico hasta agotar los tokens del balde, en ese momento se pasara a un segundo balde que efectuara un proceso bajo el mismo razonamiento o se descartara el tráfico.

Dentro de la gestión ya sea con uno o dos baldes de la QoS se manejan los siguientes conceptos:

- *CAR* (*Committed Access Rate*): Se utiliza para limitar el tráfico que puede entrar o salir de una interfaz.
- *CIR* (*Committed Information Rate*): Throughput mínimo garantizado
- *CBS* (*Committed Burst Size*): Tamaño promedio de volumen de tráfico en un tiempo determinado
- *PIR* (*Peak Information Rate*): Es el throughput máximo o limite
- *PBS* (*Peak Burst Size*): Tamaño máximo de volumen de tráfico en una unidad de tiempo

2.5.2.2.3 Gestión colas

Existen diferentes algoritmos para el manejo de las colas que pueden ser ocupados individualmente o en conjunto, dentro de los más importantes encontramos:

***PQ* (*Priority Queuing*):** Se gestionan las colas de tráfico según su prioridad, una vez que la cola con mayor prioridad este vacía se pasa a la siguiente, su principal problema es que puede existir tráfico que nunca se reenvíe.

***WRR*(*Weighted Round Robin*):** Se gestionan las colas de manera circular, pero reenviados a una velocidad proporcional a su peso, por ejemplo se tienen 3 colas, la cola A tiene asignado el

un peso de 3, las colas B un peso de 2 y C un peso de 1, cuando se produce congestión y cada cola tiene 4 paquetes, en el primer ciclo de Round Robin se envía un paquete de cada cola, en el segundo Round Robin se envía un paquete de las colas A,B, pero no de C, finalmente en el tercer Round Robin se envía solo un paquete de A, en este punto la cola A tendrá un paquete la cola B dos paquetes y la Cola C tres.

***DRR* (*Deficit Round Robin*):** Funciona de manera similar a WRR, su diferencia radica en que maneja la congestión en función del largo de los paquetes y no por el número de paquetes.

***WFQ* (*Weighted Fair Queuing*):** Similar a WRR, pero trabaja directamente con ancho de banda, permite asignar un ancho de banda según porcentaje o una capacidad máxima de bps a cada cola para que sea gestionada.

2.5.2.3 **MQC**

Modular QoS Command-Line Interface o interfaz de línea de comando de QoS modular, es un método de configuración de QoS modular que simplifica la configuración y administración de la QoS y le aporta flexibilidad.

Se basa en la creación de clasificadores “clasifiers” y comportamientos “behaviors” que se unen en una política que luego se puede aplicar a una interfaz tanto para el tráfico de entrada como de salida.

2.6 Ciberseguridad en redes pata ICS

Si bien la integración de la pila de protocolos TCP/IP ha traído como ventaja una integración entre las diferentes áreas de la empresa, lo que es muy útil, especialmente para las áreas administrativas y de mantención, tiene como desventaja que integra las vulnerabilidades presentes en las redes basadas en TCP/IP a los ICS, lo que se acentúa debido a la imposibilidad de una rápida aplicación de parches, que muchos sistemas ICS debido a que están constantemente en producción, que tienen tecnología obsoleta para el mundo TI, que los profesionales de las áreas de Automatización no ven con buenos ojos la instalación de nuevos equipos para salvaguardar la seguridad basado en que se provoca un nuevo posible punto de falla y que los ICS dada su relevancia económica o su importancia debido a que suelen manejar infraestructura crítica, son un blanco tentador para los cibercriminales.

En esta sección se revisarán los conceptos más importantes de seguridad, orientando la búsqueda de información a poder realizar una directriz orientativa a como salvaguarda la seguridad de la red ITS presentada en el caso práctico.

2.6.1 Conceptos básicos:

2.6.1.1 **Triada de seguridad:**

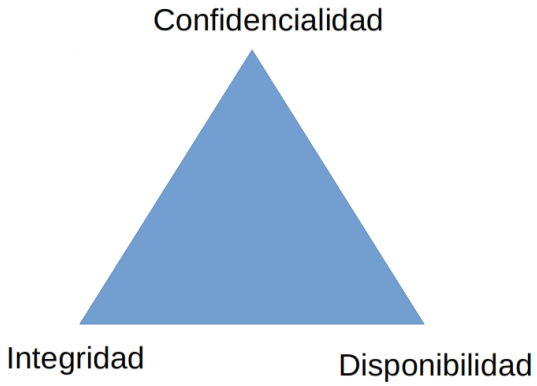


Figura 2-64 Triada de seguridad. [85]

Confidencialidad: Que la información o datos sean solo visibles para el receptor autorizado.

Integridad: Que la información no sea cambiada o destruida ya sea por un error o de forma intencional.

Disponibilidad: Que determinado recurso sea accesible según el diseño general del sistema.

2.6.1.2 Protocolos AAA

Authentication, Authorization and Accounting (Autenticación Autorización Contabilidad) son una serie de protocolos que garantizan la seguridad a través de la aplicación de estos 3 conceptos:

Autenticación: intercambio de credenciales o claves para comprobar que los usuarios o dispositivos se encuentran autorizados.

Autorización: En función de los privilegios, roles de usuarios o dispositivos especializados, se logra la asignación de recursos, servicios, funciones, etc.

Contabilización: Monitoreo de recursos y acciones realizadas por los dispositivos y/o usuarios.

2.6.1.2.1 RADIUS:

Remote Authentication Dial-In User Service es un protocolo que pertenece a la familia AAA. Tiene arquitectura cliente servidor y permite la gestión de usuarios de manera centralizada, el servidor RADIUS recibe las solicitudes desde el cliente, quién envía sus datos y responde con la información de conexión, recursos asignados.

2.6.1.3 Cifrado

El objetivo fundamental de cifrar la información es que esta sea indescifrable para cualquier receptor no autorizado, existen 2 tipos de cifrado denominados simétrico y asimétrico.

Criptografía: "Es la ciencia que hace uso de métodos y herramientas matemáticas con el objetivo principal de cifrar, y por tanto proteger un mensaje o archivo por medio de un algoritmo, usando para ello dos o más claves, con lo que logra en algunos casos la confidencialidad, en otra autenticidad, o bien ambas simultáneamente." [X]

. **Cifrado Simétrico:** Ambas partes presentes en la comunicación tienen una clave secreta previamente intercambiada y es utilizada para cifrar y descifrar los datos. Dentro de los algoritmos se encuentran A5, RC4, DES, 3DES, IDEA, AES, Serpent, TwoFish.

Destaca por su rapidez en el cifrado y descifrado, pero tiene las desventajas que las claves deben ser distintas para cada pareja que quiera realizar comunicación y el problema práctico que estas claves deben ser conocidas previamente.

Cifrado Asimétrico: Los participantes de la comunicación tiene 2 claves, una pública conocida y una privada secreta que es inversa a la pública. Al enviar un mensaje a un receptor conocido, el emisor cifra con la clave pública del receptor, quien podrá descifrar el mensaje con su clave privada, lo que le permite establecer un secreto en un canal inseguro. Dentro de los algoritmos se encuentran Diffie y Helman, RSA, El Gamal, Mochilas y curvas Elípticas.

Si bien tiene como ventaja que solo se requiere confiar en la clave pública, es mucho más lento que el cifrado simétrico y sus claves son más largas.

Cifrado Hibrido: Se usa el cifrado asimétrico para el intercambio de las claves simétricas y luego se usa está clave simétrica para el cifrado de los mensajes, logrando obtener lo mejor de ambos tipos de cifrado.

2.6.1.3.1 Algoritmos de cifrado

DES y 3DES: *Data Encryption Standard* DES, es un algoritmo de cifrado simétrico con un tamaño de clave de 56 bits, donde el emisor y receptor comparten una clave que les permite cifrar y descifrar los datos.

Fue adoptado como estándar para comunicaciones seguras en 1975, y en la actualidad se considera un cifrado débil ya que fue descifrado en 1997.

3-DES Triple DES es un cifrado simétrico que posee un tamaño de clave de 168 bits, fue adoptado en 1998 y se considera un cifrado fuerte.

AES: *Advanced Encription Standard* AES es un algoritmo de cifrado simétrico avanzado, estandarizado desde el año 2000 y puede trabajar con un tamaño de clave de 128, 192 y 256 bits. Entre más extensa es la clave el cifrado será más seguro, pero el proceso de cifrado y descifrado será más lento.

Diffie y Hellman: Fue desarrollado en 1976 por Whitfield Diffie y Martin Hellman para el intercambio seguro de claves y se basa en el esquema del logaritmo discreto utilizando una función matemática unidireccional.

RSA: Fue desarrollado por 3 investigadores del MIT Rivest, Shamir, Adleman y publicado en 1977, tiene su fortaleza en la factorización de números compuestos muy grandes resultado del producto de 2 primos grandes.

2.6.1.3.2 Funciones de HASH

Permiten formar una “huella digital” única de determinado texto, entregando siempre un resultado con un tamaño de bits fijo, sin importar el tamaño de la entrada a la función.

Son funciones unidireccionales, si se tiene un hash *h(m)* debe ser imposible computacionalmente encontrar el valor de *m* a partir solamente de *h(m)* y ser sencillo el proceso de la obtención de *h(m)* conociendo *m.*

Son útiles para el almacenado de contraseñas o para firmas digitales, ya que ante cualquier cambio en el texto el resultado de la función de hash cambiará.

Las funciones de Hash deben garantizar que una colisión, ósea que 2 textos obtengan el mismo hash, sea muy difícil.

MD5: *Message Digest* 5 MD5, desarrollado en 1991, es un algoritmo de función de hash que entrega una salida de 128 bits, si bien destaca por su alta velocidad de procesamiento, desde sus inicios se detectaron problemas de seguridad debido a colisiones, que a lo largo de los años

fueron siendo cada vez más comunes y peligrosas, principalmente debido a la posibilidad de duplicar certificados digitales, por lo que finalmente 2008 fue declarado como vulnerable por el US-CERT.

SHA-1: *Secure Hash Algorithm* 1 SHA-1, desarrollado en 1995, fue el sucesor de del SHA o SHA-0 desaconsejado ese año debido a sus vulnerabilidades. Entrega una salida de 160 bits por lo que se considera más seguro que MD5. El 2017 fue desaconsejado luego de que en un trabajo conjunto entre la CWI Institute de Amsterdam y Google se consiguiera un método para generar colisiones.

SHA-2 y SHA-3: Luego de que fuera desaconsejado SHA-1 el año 2017, y a la espera de que se estandarice SHA-3, se sugiere como alternativa un protocolo desarrollado el 2001 por la NCA de estados unidos llamado SHA-2.

SHA-2 Es considerado seguro y su mejora respecto a SHA-1 es el tamaño de sus hashes de salida pudiendo ser 224 bits, 256 bits, 384 bits y 512 bits.

SHA-3 Publicado el 2015 por el NIST, SHA-3 es un algoritmo mucho más complejo que sus antecesores y puede entregar salida de cualquier tamaño de bits.

2.6.1.4 **Transmisión sobre un canal seguro**

Para establecer un canal seguro para el flujo de información entre 2 puntos, generalmente deben realizarse 3 pasos:

i. Establecimiento de autenticación de ambas partes
ii. Las claves de cifrado *MAC* (*Message Authentication Code)* son derivadas de un secreto compartido
iii. Se cifra y descifra el tráfico a partir de estas claves

La seguridad puede implementarse en las diferentes capas con diferentes ventajas y desventajas.

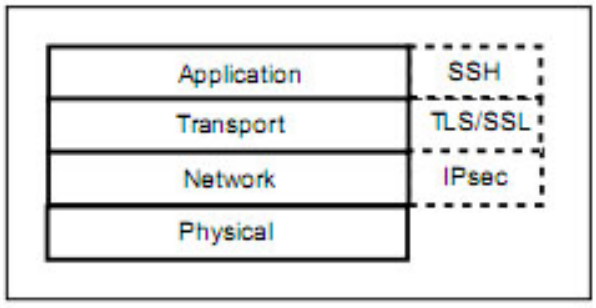


Figura 2-65 Alternativas por capas para implementar un canal seguro. [87]

2.6.1.4.1 Seguridad en la capa de red

Tiene como ventaja que no permite la visualización de todo el tráfico *End to End* E2E, es transparente para las aplicaciones e independiente de la capa de transporte, lo que trae la desventaja de que el poco control sobre las aplicaciones que están siendo comunicadas por la red.

2.6.1.4.1.1 IPSec

Internet Portocol Secure IPSec fue definido en los RFCs 2401–2412 en 1998, es compatible tanto con IPv4 como con IPv6, otorga seguridad a nivel de la capa de red cubriendo todos los paquetes IP a este nivel, no siendo visible en capas superiores.

Tiene dos modos básicos de uso, modo *transporte*, donde no se cifran las cabeceras IP y un modo *tunel* donde todo el paquete IP es cifrado y se agrega una nueva cabecera ocultando por completo el paquete original.

Está formado por 2 protocolos de seguridad AH y ESP y se sirve del protocolo de gestión de claves IKE.

AH: *Autentication Header* está definido en el RFC 2402, garantiza la integridad y autenticación de los paquetes.

Se ubica entre la cabecera IP y su campo de datos, tiene un largo de 24 bytes, usa MAC y clave secreta compartida entre los puntos finales. Realiza un cálculo de *HMAC* (*Hash Message Authentication Code*) usando una función de hash sobre el campo de datos del paquete y parte de la cabecera, a excepción de los campos que van cambiando salto a salto como TTL, TOS, flags, etc. y proporciona estados a las conexiones que no están presentes naturalmente en la capa de red.

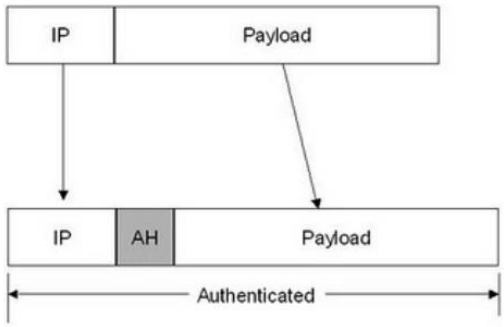


Figura 2-66 Implementación de AH en IPSec. [87]

ESP: *Encapsulating Security Payload* ESP está definido en el RFC 2406, garantiza la integridad, autenticación y confidencialidad de los paquetes.

Tiene un formato más complejo que AH, ya que introduce tanto una cabecera como una cola que encapsulan los datos. Utiliza cifrado simétrico y MAC en base a claves secretas compartidas entre los puntos finales.

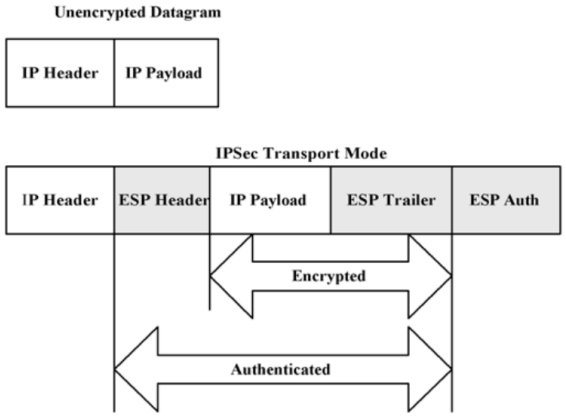


Figura 2-67 Implementación de ESP en IPSec. [87]

IKE: *Internet Key Exchange* IKE utiliza un intercambio de claves simétricas del tipo Diffie Hellman para establecer el secreto compartido de la sesión IPSec

2.6.1.4.2 Seguridad en la capa de transporte

Tiene como ventaja que no permite la visualización de todo el tráfico E2E, las aplicaciones tienen mayor visibilidad de esta capa por lo que pueden gestionar su uso y de manera natura tiene estados en las conexiones, como es el caso de TCP y tiene como desventaja que en esta capa las aplicaciones deben ser modificadas para la protección.

2.6.1.4.2.1 SSL y TLS

Trabaja con una arquitectura cliente-servidor y su objetivo proporcionar Autenticación, Integridad y Confidencialidad de la información que se está compartiendo a través de la red.

SSL: *Secure Socket Layer* fue desarrollado por la empresa Netscape comunications en 1995 y su versión 3.0 fue lanzada en 1996, quedando obsoleta en junio del 2015.

TSL: *Transport Layer Security* es una evolución del SSL por lo que es bastante similar a su predecesor, teniendo algunas mejoras como la protección ante nuevos ataques, evitar que se fuerce la comunicación a utilizar versiones más antiguas y vulnerables, incluye nuevos algoritmos de cifrado, su versión TLS 1.2, también conocida como SSL 3.3 fue publicada el 2008 y se especifica en el RFC 5246. Actualmente se trabaja en la versión TLS 1.3.

SSL/TLS Handshake protocol

Es la parte más compleja del protocolo y sirve para negociar los algoritmos que se utilizaran para:

- Negociar entre el cliente y el servidor los algoritmos que se utilizaran para cifrar, intercambio de claves y firmas, estos pueden ser 3DES, IDEA, AES, RSA, etc.
- Realizar el intercambio de claves y autenticación en base a certificados digitales.
- Cifrado del tráfico en base a criptografía simétrica a través de la clave de la sesión.

El cliente es quién propone los algoritmos y la versión más alta de SSL/TLS que tenga disponible, además de algoritmos de cifrado, MAC, autenticación, compresión y un número aleatorio. El servidor responde con lo que escoja, además de un certificado digital y un número aleatorio. El cliente verifica al servidor, ambos se envían una clave temporal *PreMasterSecret* y que, sumado, a los números aleatorios previamente intercambiados y a la llave privada en el caso del servidor, logran generar una clave común *MasterSecret*. En este punto el cliente le indica al servidor que el envío de tráfico será autenticado y cifrado, en caso que el servidor lo soporte y envía un mensaje *Finished* firmado y cifrado conteniendo un hash y MAC que el servidor debe descifrar y verificar, para luego informar al cliente que desde este punto todo el tráfico será firmado y cifrado en caso que la negociación así lo haya determinado y envía un mensaje *Finished* para que el cliente valide con el hash y MAC, con lo que finaliza el handshake y se inicia la comunicación en el canal seguro.

SSL/TLS Record protocol: Especifica la forma de encapsular los datos transmitidos y recibidos.

2.6.1.4.3 Seguridad en la capa de aplicación

La seguridad implementada en esta capa es para requerimientos muy exigente y permite tener un control sobre las aplicaciones.

2.6.1.4.3.1 SSH

Secure Shell SSH, está definido en los RFCs 4250-4256 y se utiliza principalmente para realizar conexiones remotas a un equipo a través de una red insegura, creando un canal cifrado entre ambos puntos. Reemplaza a protocolos inseguros como telnet o rsh, además, se utiliza para ejecución segura de comando, transmisiones de archivos y reenvío de puertos.

Garantiza confidencialidad, integridad a través de MAC y autenticación a lo menos del lado del servidor con métodos de llave pública como RSA o certificados, realiza una negociación similar a la del handshake de SSL donde se definen los tipos de cifrado, forma de intercambio de claves, forma de autenticación, firmas, etc. Funciona sobre el protocolo TCP utilizando el puerto 22.

2.6.1.5 Malware

Malicious software Malware es un software malicioso o molesto que contiene un código que está diseñado para ejecutar acciones con el fin de realizar daño o violar la seguridad de dispositivos computacionales. Dentro de los malwares encontramos virus, troyanos, rootkits, gusanos, botnets, etc.

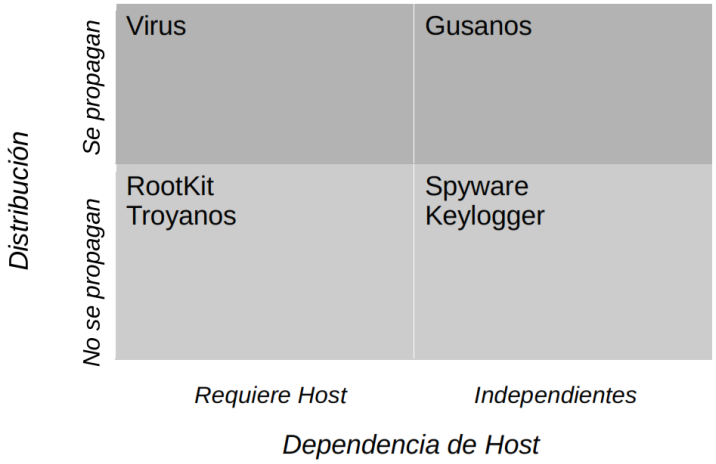


Figura 2-68 Directivas básicas de Malware. [88]

Virus: Son softwares maliciosos con la capacidad de incrustarse o auto-adjuntarse en otro software y se propagan a través de las aplicaciones. Pueden infectar directamente los archivos inmediatamente al ser ejecutados o el software malicioso puede estar residente en memoria, incluso en el sector de booteo (*boot sector*) evitando la acción de antivirus o el formateo del equipo. Siempre necesitan de un dispositivo para alojarse.

Gusanos: Los gusanos (*worms*) son tipos de malware que no necesitan una máquina para alojarse, ya que tienen la capacidad propagándose así mismo de dispositivo en dispositivo a través de la red, por algún puerto que este abierto o mediante auto envío por e-mail, por lo que funciona de manera activa. Al encontrar una vulnerabilidad intentan infectar todos los dispositivos que la presenten.

Troyanos: Este tipo de software malicioso que no puede ni replicarse ni propagarse y como su nombre hace suponer, intenta pasar desapercibido, presentándose como un software legítimo a fin de que el usuario lo acepte y lo ejecute, comúnmente toman un nombre muy similar a un software o librería propia del sistema operativo. Dentro de sus objetivos está crear acceso remotos maliciosos (backdoors) y el espionaje de datos como claves de softwares, datos bancarios, cuenta de e-mail, etc.

Spyware: Este malware se dedica a robar información de el o los usuarios y enviarlos al atacante.

Rootkits: Son un conjunto de herramientas que permite la explotación de diversas vulnerabilidades, además permite esconderse a sí mismo, comúnmente usadas para mantener acceso a sistema infectados.

Keylogger: El malware se dedica a monitorear la actividad del usuario en la máquina, pudiendo guardar la información de lo que teclea o incluso obtener capturas de pantalla para posteriormente enviar al atacante.

2.6.1.6 Tipos y formas Ataques

2.6.1.6.1 Tipos básicos de ataques

Ataque Man-in the-middle: Hombre en el medio, el atacante logra capturar el tráfico de red entre dos puntos, pudiendo modificarlo, eliminarlo provocando una *DoS (Denegate of service)* o simplemente almacenarlos para ver el comportamiento de la red y realizar un ataque más elaborado.

Ataques 0-day: Son ataques nunca antes realizados que explotan vulnerabilidades que no son conocidas por los administradores de redes ni fabricantes por lo que aún no hay antivirus o parches para su combate.

Ataques DoS: Ataques que no permiten el uso de recursos solicitados por el usuario.

2.6.1.6.2 Ataques ARP

ARP Spoofing: Es el ataque más común sobre ARP, también es llamada envenenamiento de ARP. El ataque consiste en que el atacante envía mensajes ARP con su IP y una dirección física falseada para que los paquetes sean enviados a él en vez de al host de destino con lo que logra capturar el tráfico. Es comúnmente realizado falseando la MAC del router con lo que todo el tráfico de salida de la LAN pasaría por el atacante pudiendo inspeccionar y/o modificar el tráfico, además de poder realizar una DoS descartando los paquetes.

2.6.1.6.3 Ataques ICMP

Ping of death: Funciona con equipos antiguos, se envía un paquete ping modificando el tamaño máximo de paquete puede soportar la máquina, colapsándola.

Ping flood: Es un ataque de DoS que consiste en enviar un gran número de pings a un host desde una máquina otra.

Smurf Attack: Es un ataque de DoS que consiste en enviar un ping hacia muchas máquinas falseando la dirección de origen que será la de la víctima, por lo que las máquinas que reciban el ping contestaran hacia esta dirección, colapsándola.

2.6.1.6.4 Ataques TCP

Ataque RST: El ataque de DoS que se basa en la activación del flag *RST* de la cabecera TCP, enviando un paquete falseado con los datos de dirección IP, puerto y número de secuencia correcto, pero levantando dicho flag, lo que provoca que la sesión termine o que nunca se establezca.

SYN Flooding: Es un ataque DoS muy popular en la actualidad, se trata del envío de muchos paquetes con el flag *SYN* activado con dirección IP de origen falseadas, con lo que la víctima empezará a enviar mensajes *SYN Ack* a estas direcciones agotando los recursos de la víctima.

TCP/IP Hijacking: Es un ataque que tiene el objetivo de adueñarse de una conexión entre un host o servidor y una víctima, enviando paquetes falseados con los números de secuencia, puertos e IP de la víctima correctos reemplazando al PC de la víctima por el del atacante en la sesión , pudiendo seguir interactuando con el host o servidor al que estaba conectada la víctima.

2.6.1.6.5 Ataques a DHCP

DHCP spoofing: El servidor de DHCP posee información valiosa como son el pool de direcciones IP, logs, en algunos casos características del sistema operativo, etc. por lo que para un cibercriminal es un objetivo muy apreciado.

El ataque se realiza suplantando al servidor DHCP real, pudiendo lograrlo al ofrecerse como servidor DHCP cuando un cliente envíe un mensaje de broadcast como solicitud de configuración DHCP y el servidor DHCP del atacante sea elegido, con lo que el atacante puede tanto capturar información como proponer una configuración a su conveniencia

DHCP DoS: Se genera una gran cantidad de solicitud de configuración por parte de atacantes que se hacen pasar por clientes, con el objetivo de acabar con las direcciones IP disponibles para que los clientes reales no puedan obtener conexión.

2.6.1.6.6 Otros Ataques

Desbordamiento de Buffer: ataque que se basa en que el atacante desborda el buffer enviando más datos que los que puede procesar la víctima, provocando que datos se sobrescriban en otras áreas de memoria, lo que pudiese permitir al atacante ejecutar códigos maliciosos.

SQL Injection: Aprovecha las vulnerabilidades de los formularios web para tener acceso a la base de datos del sitio web. También puede producirse ataques a plataformas SCADA aprovechando sus vulnerabilidades que presentan en estos sistemas, principalmente debido a su obsolencia.

Pharming: Aprovecha la vulnerabilidad existente en softwares de servidores DNS, cambiando la dirección IP real a la que se quiere acceder por la dirección IP que el atacante indica, lo que provoca que el usuario al acceder mediante su explorador se dirigirá a la página falsa.

Phishing: El atacante intenta adueñarse de datos como usuarios y contraseñas de las víctimas a partir de mensajes que enviados a estás desde un emisor de confianza u oficial. Existen diversos tipos de phishing como llamadas telefónicas, SMS, mensajería por internet, siendo el más habitual el phishing por correo electrónico.

Drive-by-Download: Se refiere a la descarga sin intención de softwares o códigos maliciosos en la red. Puede darse cuando el usuario autoriza la descarga desconociendo las consecuencias o en ataques más sofisticados basta con visitar un sitio web para infectarse.

Drive-by-pharming: El atacante aloja un código malicioso una alguna página web el cual es ejecutado por el browser del usuario.

2.6.2 Políticas de Seguridad

Definen el camino a seguir por la organización para implementar la seguridad. Deben reflejar el compromiso al más alto nivel dentro de la compañía. Las políticas son la base del programa de ciberseguridad de la organización.

Dentro de la creación de las políticas se debe tener en cuenta al menos aspectos como:

- Las políticas deben tener una vida útil al menos de 2 o 3 años, si bien se estarán revisando constantemente debido a la aparición de nuevos problemas de seguridad a nivel mundial, deben ser elaboradas para que su evolución sea sencilla.
- Utilizar notación con mandato evitando utilizar condicionales, por ejemplo, es mucho mejor usar "debe" que "debería".
- Evitar detalles técnicos de cómo se implementará, ya que la política debe cruzar por toda la jerarquía de la compañía y debe ser entendida por todos los empelados
- No realizar un documento excesivamente largo (más de 3 páginas) a fin de que se implementable de manera sencilla
- Definir tanto sanciones como incentivos al comportamiento de los usuarios que utilicen los recursos del sistema.
- Debiese incorporar políticas de uso ético

Figura 2-69 Diagrama de plan de Ciberseguridad en una compañía. [84]

2.6.3 Seguridad Perimetral

La seguridad perimetral se utiliza para la defensa de la red de incidentes externos, permitiendo la entrada y salida de tráfico de la red de forma segura. Por lo general se basa en al menos Firewalls e IDS.

2.6.3.1 **ACL**

Acces Control List (Lista de Control de Acceso) son una lista de instrucciones que permiten o deniegan el acceso del tráfico y pueden configurarse en la mayoría de los equipos networking que permiten administración.

La operación se realiza de manera secuencial hasta que se produce algún calce previamente configurado, ya sea por IP, MAC, VLAN o incluso protocolos específicos en dispositivos de mayor capacidad. Existe una denegación *Deny* implícita al final de cada ACL.

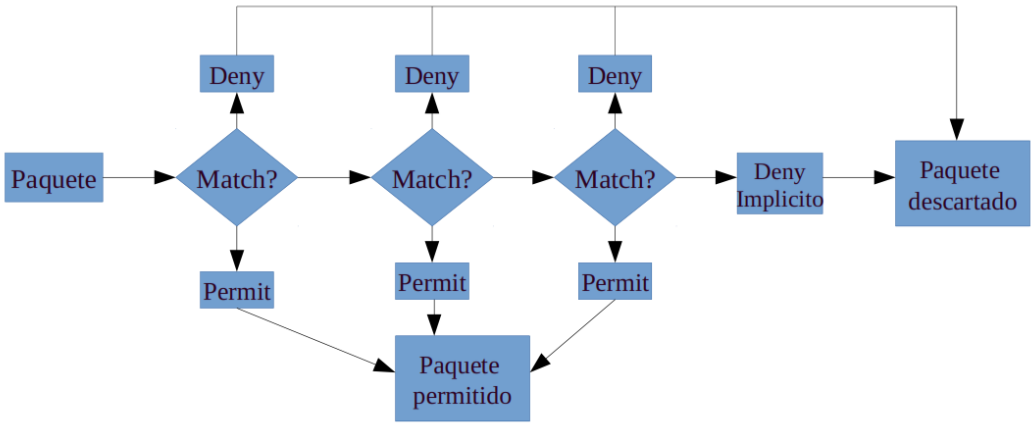


Figura 2-70 Funcionamiento de ACLs. [86]

2.6.3.2 **Firewalls**

Los cortafuegos o Firewalls se pueden clasificar en 3 tipos en base a su nivel de inspección del tráfico de Red:

Packet Filtering Firewalls: En general realizan la auditoria de tráfico en las capas 2 y 3 del modelo OSI, debido a su bajo nivel de inspección tienen un alto throughput.

Stateful Inspection Firewalls: Permiten inspeccionar hasta capa 4 y revisar el estado de las sesiones TCP, debido a su mayor capacidad de inspección es algo más complejo de administrar. Logra un buen throughput, siendo menor al del tipo Packet Filtering.

Application-Proxy Gateway Firewalls: Permiten revisar el tráfico hasta la capa de aplicación pudiendo auditar protocolos como FTP, SNMP, http y aplicaciones tipo browsers. Si bien soy muy seguros su alto nivel de inspección disminuye su throughput.

2.6.3.3 **IDS/IPS**

Los *Intrusion Detection/Protection Systems* actúan por detrás del firewall dentro de la red a defender, aunque es común que los equipos Firewall actuales incluyan dentro de su software el IDS/IP.

Su arquitectura se basa en Sensor + Recolector + Almacenamiento + Motor de Análisis, pueden realizar tareas complejas como el reconocimiento de patrones anómalos en el tráfico, reconstruir sesiones TCP, detección de firmas, detección de ataques con fecha/hora y reconstrucción de ataques, etc.

2.6.3.4 **DMZ**

Dentro de las empresas es común tener una serie de servidores que dan servicio tanto a conexiones internas como externas, como son los servidores DHCP, DNS, correo, web, etc. por lo que serán objetivos valiosos para un atacante, además de ser más vulnerables por la gran cantidad de conexiones que manejan, por lo cual se recomiendan que estos servidores sean instalados en una zona desmilitariza *DeMilitarized Zone* que siempre estará protegida por al menos un Firewall. Según las necesidades pudiese existir más de una DMZ.

2.6.4 Normativa de Seguridad y Organismos competentes:

En la actualidad existen diversos organismos realizando esfuerzos para dar un marco teórico para la implementación de la de ciberseguridad en los ICSs. Los esfuerzos mancomunados se realizan ya sea por sectores específicos, distribuciones geográficas, criticidad de infraestructura, etc.

Estados Unidos es el país que entrega mayor documentación de Ciberseguridad de manera gratuita y proactiva, dentro de los esfuerzos más importantes encontramos *Cryptographic Protection of SCADA Communications* (Protección Criptográfica para comunicaciones de SCADA) de la Asociación Americana de Gas AGA, *Pipeline SCADA Security* (Seguridad para SCADA de tuberías) del Instituto Americano de Petróleo (API), en el sector eléctrico se tiene la serie de recomendaciones NESCOR *National Electric Sector Cybersecurity Organization Resource* (Recursos de la Organización Nacional de Ciberseguridad del Sector Eléctrico) del Instituto de Investigación de Energía Eléctrica (EPRI) y el estándar NERC CIP de la Corporación de Fiabilidad Eléctrica Norteamericana (NERC). La serie de guías 800 para ciberseguridad ICSs del Instituto Nacional de Estandarización y Tecnología NIST, las recomendaciones del Equipos Comunitarios de Respuesta ante Emergencias para ICSs ICS-CERT.

En el resto del mundo, esencialmente en Europa existen una serie de organismo y comités para la Ciberseguridad. En Europa de La Agencia Europea de Seguridad de las Redes y de la Información ENISA ha desarrollado varios documentos donde destaca *Protegiendo los sistemas de control industrial – Recomendaciones para Europa y sus Estados Miembro* , El estándar ISO 27002, las recomendaciones del Consejo Internacional de Grandes Sistemas Eléctricos (CIGRE) con base en Francia, la serie de documentos ISA99 / IEC-62443 que actualmente sigue en evolución por la Comisión Electrotécnica Internacional IEC y para sector eléctrico los estándares IEEE 1686-2007 e IEEE P1711 de la IEEE.

A continuación, se revisarán con mayor profundidad algunos de estos esfuerzos poniendo el énfasis en la serie 800 del NIST la cual se utilizará de guía base para las directrices de seguridad que se plantearan.

2.6.4.1.1 CERT/CSIRT

Un *Computer Security Incident Response Team CSIRT* (Equipo de Respuestas a Incidentes de Seguridad Computacional CSIRT) o también llamado *Computer Emergency Response Team CERT* es una organización responsable de recibir, revisar y responder ante reportes de incidentes y actividades no autorizadas en los sistemas computacionales.

Existen CERT de ámbito privado de empresas, militares, organizados internacionalmente, nacionales, regionales como el CLCERT de Chile, Incibe-CERT de España, US-CERT de Estados Unidos, TF-CSIRT Europa, APCCERT en Asia-Pacifico y el FIRST que tiene alcance global y también orientado a las redes Industriales como el ICS-CERT de estados unidos.

Los CERT está continuamente investigando y analizando incidentes de manera proactiva, informando lecciones aprendidas respecto a los incidentes, entregando información relevante y estrategias de mitigación que aportan una excelente fuente información para que el administrador de los sistemas informáticos de como establecer sus estrategias de seguridad.

Una buena práctica dentro de las políticas de seguridad es tener contacto directo con su CERT/CSIRT correspondiente.

2.6.4.1.1 ICS-CERT

El *Industrial Control Systems - Computer Emergency Response Team ICS-CERT* es un CERT con base en Estados Unidos tiene como objetivo la reducción y monitoreo de incidentes riesgosos en ICS y/o infraestructura critica, trabajando en conjunto con diversos organismos gubernamentales, proveedores de equipos, operadores de ICSs, y otros ICS-CERT como lo es el KL ICS-CERT de Kaspersky, líder mundial en seguridad informática.

Busca de manera proactiva nuevas vulnerabilidades en los ICSs, realizando continuamente recomendaciones a la industria, para aplacar estas vulnerabilidades y educar a todo el personal que interviene en los ICSs.

2.6.4.1.2 ISA99 / IEC-62443

La International Society of Automation ISA en respuesta ante la evolución de los sistemas industriales y su integración con el mundo IT ha desarrollado una serie de normas con el objetivo de entregar información especializada para la mejora de la ciberseguridad.

Desde el año 2007 la ISA fue publicando las diferentes normas para la mejora en la seguridad, hasta el año 2010, donde International Electrotechnical Commission IEC continuo los desarrollos cambiando la nomenclatura de las publicaciones a IEC-62443

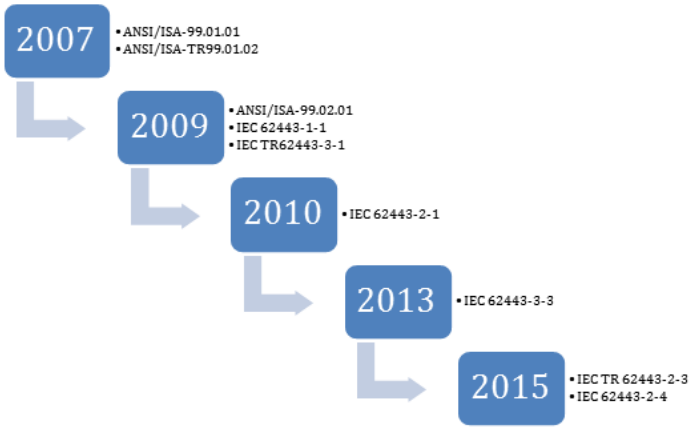


Figura 2-71 Evolución del estándar ISA99/IEC 62443. [89]

La norma se divide en 4 grandes grupos con 13 documentos que pueden verse en la figura 2-72, los cuales detallan conceptos específicos de la norma.

A diferencia de otras normativas o guías este conjunto de normas es vendidas por la ISA y cada documento tiene un precio distinto y pueden ser adquiridas en el sitipo web de la ISA. Como se

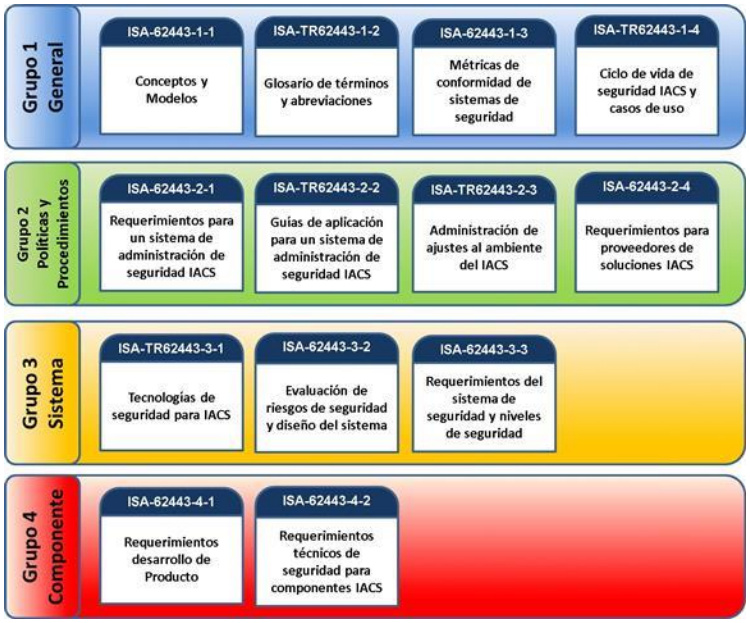


Figura 2-72 Normativa ISA99/IEC 62443.

La serie de normas permiten definir dominios de seguridad bajo los conceptos de la zonas y ductos de diferentes "Sistemas bajo consideración" *SuC* (*System under Consideration*).

Zonas: agrupación lógica o física de activos industriales (dichos activos puedes ser físicos, aplicaciones o información) los cuales comparten los mismos requisitos de seguridad.

Ductos: Un ducto to es un camino de comunicación entre dos zonas de seguridad. Proporciona las funciones de seguridad que permiten a dos zonas comunicarse de forma segura. Toda comunicación entre diferentes zonas ha de realizarse a través de un conducto.

2.6.4.1.3 NIST SP 800-82

El *National Institute of Standards and Technology* (Instituto Nacional de Estandarización y Tecnología) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

Según lo que indica en NIST la creación e implementación de un programa de seguridad debe realizarse de manera metódica para lo que ha publicado de manera gratuita una serie de guías que usan como documento central el documento 800-82, algunas guiás a destacar para un diseño de red son NIST SP 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy, NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)* y NIST SP 800-77, Guide to IPsec VPNs.

Debido a su claridad y gratuidad en la entrega de la información, las directrices de seguridad se realizarán mayoritariamente en base a la documentación de este organismo por lo cual se profundizará en mayor medida que los organismos anteriores.

2.6.4.1.3.1 Realizar un caso de negocio para la seguridad

El caso de negocio sirve para justificar el financiamiento de la compañía al crear el programa de seguridad. El equipo que lo construya debe ser multidisciplinario con almenos personal IT y en Sistemas de control y especialistas de sistemas dentro del ICS que no se enmarquen en las 2 especialidades anteriores.

En el caso de negocio debiesen incluirse aspectos como:

- Beneficios que trae la mejora de la seguridad en disponibilidad y confiabilidad de la red y los subsistemas que forman el ICS.
- Analizar consecuencias potenciales de afectación a la compañía, físicas, sociales, económicas, imagen, etc.
- Costos y recursos necesarios para el desarrollo, implementación y mantención del programa de seguridad.
- Presentar el caso de negocio al líder de la compañía y que sea aprobado y auspiciado por este, a fin de e la penetración en todas las estructuras de la compañía

Analizar Consecuencias potenciales: Un incidente de ciberseguridad puede afectar varias aristas en la compañía, una muy buena fuente de información son los casos de negocio de compañías similares y la información de seguridad propia de cada subsistema, dentro de las 3 consecuencias más importantes para los sistemas ICS se tiene:

- Impactos físicos: Si bien la afectación física más importante es la del riesgo de la vida de las personas, existen otros daños como destrucción a la propiedad, afectación en equipo de

almacenamiento de datos, fallas en los diferentes equipos que forman el ICS e incluso el medio ambiente.

- Económicos: Perdidas o daño en la producción, inhabilitación de infraestructura crítica como la transporte, energía o agua.
- Sociales: Especialmente importantes sobre infraestructura critica o con residuos contaminantes, algún ataque que provoque la falla en estos ICSs puede causar graves daños a la sociedad que además se traducirá en severas consecuencias económicas y de imagen.

Dentro de los análisis de las consecuencias potenciales no se deben perder de vista las reacciones en cadena producto de la interdependencia de los subsistemas que forman un ICS que puedan causar fallas en ciertas capas, zonas o la caída completa del sistema.

2.6.4.1.3.2 Crear un equipo Multidisciplinario

Dada la variabilidad en los tipos de ICS tanto en su función como distribución, para un correcto manejo de los riesgos, debiese existir un equipo con almenos un especialista de las tecnologías de la información, un Ingeniero de Control, operador de control, expertos en seguridad, personal del equipo de riesgo de riesgo de la empresa. En ICS con varios subsistemas como lo son los trenes, autopistas, Hospitales, etc. debe existir personal con conocimiento suficiente en todos los subisistemas para el análisis del riesgo.

Este equipo debiese reportar directamente al CEO de la empresa o a un delegado directo.

2.6.4.1.3.3 Definir carta y alcance

El equipo multidisciplinario debe establecer las políticas que defina como será estructurada la organización con respecto al ICS, interdependencia entre los sistemas, flujo de datos, responsables de áreas y sistemas. En caso de interdependencia de sistemas debe existir el detalle de la interoperabilidad y quienes, y a qué nivel pueden afectarse, etc.

2.6.4.1.3.4 Implementar el marco teórico para la gestión del riesgo.

Existe mucha documentación que puede servir de guía para implementar la gestión del riesgo, algunos ejemplos son:

- NIST 800-39, Managing Information Security Risk–Organization, Mission, and Information System View
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
- ISA-62443-2-1 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program,

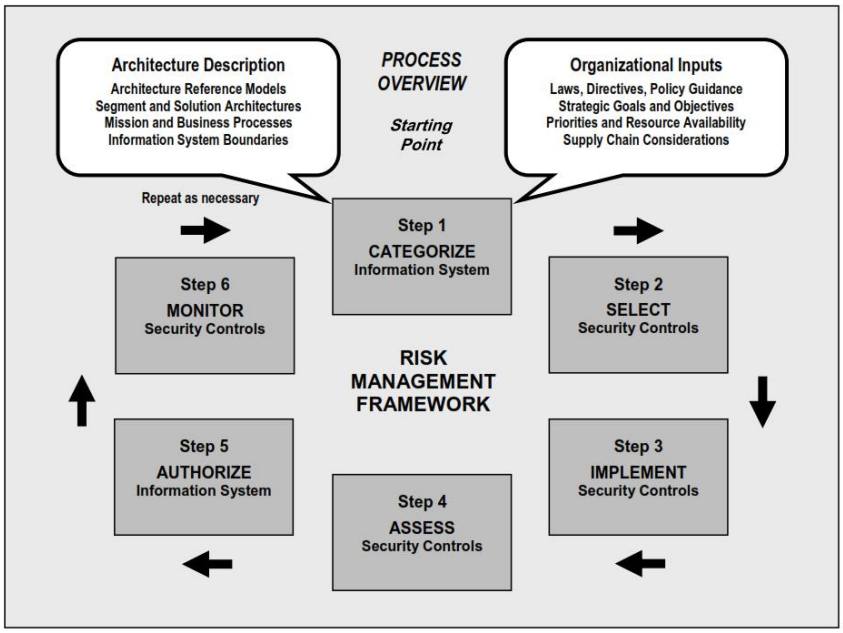


Figura 2-73 Proceso de manejo del riesgo NIST SP 800-82. [95]

Como se observa en la figura 2-73, el marco teórico se basa en 6 pasos en constante realimentación

i. Paso 1 Categorizar Sistemas de ICS:
Categorizar los equipos, sus características de hardware, software, comportamiento de comunicaciones e interacción con el mundo físico. Cada sistema dentro del ICS debe quedar documentado tanto el mismo como su interacción con otros subsistemas.

ii. Paso 2 Seleccionar controles de Seguridad:
Los controles de seguridad se elaboran a partir de la caracterización desarrollada en el paso uno y entre mayor sea el riesgo mayor debe ser en nivel de control.
Existen guías especialmente orientadas en este punto como la publicación del NIST 800-18 *Guide for Developing Security Plans for Federal Information Systems* , NIST Recommended Security Controls for Federal Information Systems and Organizations.

iii. Paso 3 Implementar controles de seguridad:
Se deben implementar los controles de seguridad previamente seleccionados ya sea incorporándolos ya sea en el plan de seguridad que actualmente rige en la organización o en el nuevo plan en caso de que sea una nueva organización. Luego de la incorporación los controles deben ser socializados.

iv. Paso 4 Evaluar controles de Seguridad
Se deben evaluar constantemente los controles de seguridad y corregir a causa de la detección de actividades sospechosas, nuevos riesgos detectados o cambios en la legislación, nuevos firmwares, softwares en los equipos, etc.

v. Paso 5 Autorización de sistemas de información

Decisión de la compañía de autorizar la incorporación de nuevos sistemas o servicios agregados al sistema actual en función de los análisis y evaluaciones hechas en los pasos anteriores.

vi. Monitoreo de los controles de seguridad
Monitorear constantemente los controles de seguridad, el documento del NIST SP800-37 provee una guía de como implementar el monitoreo constante.

2.6.4.1.3.5 Arquitectura de Seguridad:

La arquitectura de Red debiese tener separada la red ICS de la red corporativa. Su tráfico de red y objetivos son distintos, además la necesidad del acceso de la red corporativa a internet, acentúa esta necesidad.

Segmentación: La segmentación debe realizarse según cada caso particular, por ejemplo, podría segmentarse la red ICS en varias sub redes ICSs en función de las características del tráfico y función, también podría segmentarse en base a autorizaciones, políticas uniformes o niveles de confianza.

La segmentación siempre le agrega un problema al ciber atacante y además de tener un efecto positivo en caso de errores accidentales ya que estos solo afectarían a una parte acotada de la red

Algunas técnicas son:

- **Separación Logica:**
  - VLANs
  - VPNs con Cifrado (IPSec u otro).
  - Gateway unidireccionales

Separación física: No conectar en ningún punto las redes, lo que produce la máxima seguridad posible, pero es poco práctico en las redes de hoy.

- **Filtrado de tráfico:**
  - En base a enrutamiento
  - En base a red
  - En base a puerto-protocolo
  - Filtros a nivel de aplicación. (por ejemplo, no permitir el telnet)

- **Protección perimetral**
  - La protección perimetral estará formada por los equipos indicados en el punto 2.6.3, además de routers, gateways unidireccionales, tuneles cifrados, etc.
  - Transferencia de datos entre sistemas con politicas distintas de seguridad introduce un riesgo, ya que violara alguna política al realizar la comunicación.

Capítulo 3 Planteamiento de caso práctico

Actualmente existe un servicio que debe prestar la empresa COMSA Industrial enmarcado en un proyecto de una autopista formada por una serie de túneles. La autopista está ubicada en una zona rural que permite conectar por tierra 2 importantes zonas urbanas de un país Latinoamericano.

Se debe configurar una red de comunicaciones que pueda transportar el tráfico IP de todos los subsistemas que forman el ITS de la autopista, que permitirá mejorar la operación y la seguridad en el servicio prestado a los usuarios.

La información aportada por los diferentes subsistemas servirá para tomar decisiones en tiempo real para evitar o aplacar emergencias, mejorar la gestión del tráfico, realizar tarificación automática, etc.

Actualmente el proyecto está en construcción, el cliente que tiene una especificación técnica ET de requisitos y/o exigencias que deben tomarse en cuenta al momento de realizar una propuesta de configuración de la red y además está abierto a escuchar propuesta de mejoras.

En la autopista existirán dos centros de control donde estarán los servidores de todos los subisistemas del sistema ITS, uno funcionara como el centro de control principal y el segundo como respaldo, solo teniendo los servicios necesarios encendidos dentro de los que estarán un switch de Core y un PLC.

3.1 Subsistema Red de Comunicaciones

El proyecto está en construcción, ya tiene hardware instalado y/o definido el cuál no es modificable, con una distribución de red jerárquica en 3 capas, acceso, agregación y Core.

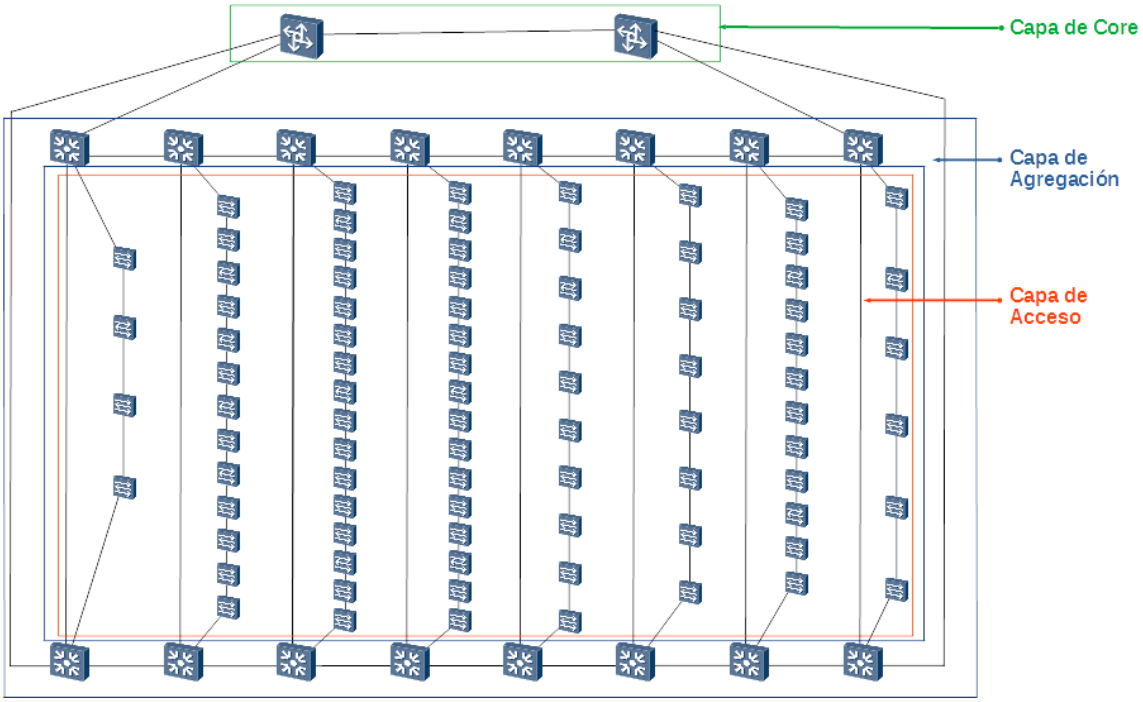


Figura 3-1 Arquitectura Red IP del sistema ITS

3.1.1 Capa de acceso

La red de acceso será la capa que se conectará a los diferentes equipos terminales en campo de los subsistemas que forman el ITS. Como se observa en la figura 3-1 la capa de acceso estará formada por 8 anillos y cada uno cerrará en 2 switches de agregación.

La cantidad de switches de acceso por cada anillo variará entre 4 -16 y estará dada por la densidad de equipos dentro de los tramos de la autopista, en zonas abiertas la densidad de equipos será mucho menor que en tramos de túnel.

Los switches de acceso estarán instalados principalmente dentro de gabinetes de los postes SOS y en salas eléctricas.

Especificaciones:

- Conexiones en base a fibra monomodo de 1 GE
- Los switches de acceso son marca Huawei de la serie IoT modelo AR550 con 8 o 24 puertos FE y 4 puertos GE combo (cobre y fibra óptica).

Requerimientos del cliente:

- Se basará en capa 2 del módelo OSI
- Cada subsistema debe funcionar en una VLAN distinta.

- El tiempo de convergencia de los switches a nivel de acceso debe ser de menos de 200ms y se deben ocupar protocolos que estén disponibles en el hadware, ya sea la familia Spannig-tree STP, RSTP, MSTP o el protocolo de Huawei SEP.

Mejoras a proponer:

- Balanceo de carga
- Configuración de QoS

3.1.2 Capa de Agregación

La capa de agregación será la encargada de conectar la capa de acceso con la capa de core y estará formada por 16 switches conectados en topología de anillo, que cerrará dicho anillo en los switches de Core. Los Switches estarán instalados en salas eléctricas y Centros de control.

Especificaciones

- Conexiones en base a fibra monomodo de 1 GE
- Los switches de agregación son marca Huawei de la serie IoT modelo AR2500 con 2 puerto 10GE y 4 puertos GE en fibra óptica y 4 puertos GE combo.

Requerimientos del cliente:

- Se basará en capa 3 del modelo OSI
- En estos switches deberán permitir comunicación InterVLAN
- Se debe ocupar un protocolo de enrutamiento dinámico, idealmente BGP
- El tiempo de convergencia de los switches a nivel de agregación debe ser de menos de 500ms

Mejoras a proponer:

- Configuración de QoS

3.1.3 Capa de Core

Especificaciones

- se utilizará un enlace redundante de 40GE sobre fibra monomodo
- Los switches de agregación son marca Huawei modelo S7706 con 48 puertos FE, 16 puertos 10GE y 4 puertos 40GE.
- Los switches tendrán conexiones GE sobre cable de cobre para conectar con los servidores de los diferentes subsistemas.

Requerimientos del cliente:

- Se debe ocupar algún protocolo tipo VSS (Virtual switching system) para que los equipos de Core trabajen en forma de Cluster.

3.2 Subsistemas del ITS

A continuación, se presentan las características más relevantes de los subsistemas que forman el ITS en búsqueda poder conocer el comportamiento de sus comunicaciones con el objetivo plantear la propuesta de configuración.

En un caso real en una red ICS, ya sea debido a la variabilidad en los subsistemas que lo forman, a que la pila de protocolos TCP/IP es relativamente nueva en este tipo de redes o que los especialistas son principalmente Ingenieros del área control Automático, no es sencillo obtener datos exactos de trafico de red para los subsistemas, por lo que la base información de las características del tráfico de red como ancho de banda ocupado, flujo de comunicaciones y protocolos ocupados, se construirá a partir de los datos entregados por el cliente del proyecto, la revisión de los protocolos y aplicaciones que usan los subsistemas y los antecedentes previos.

3.2.1 Consideraciones generales

Se revisarán en mayor profundidad

- Subsistema de Gestión de Red, dado que tiene directa implicancia en el funcionamiento de la red.
- Subsistema Control y ventilación, debido a que el subsistema más crítico de la red.
- Subsistema de Circuito cerrado de televisión, por ser el que típicamente ocupa mayor ancho de banda de los subsistemas.

Base de cálculo de ancho de banda

- Para el cálculo de ancho de banda de los diferentes subsistemas se considerará:

Capa 2: $14 \text{ bytes (Cabecera Ethernet)} + 4 \text{ bytes (VLAN)} + 4 \text{ bytes (FCS Ethernet)} = 22 \text{ bytes}$

Capa 3: $\text{Cabecera IP (mínima)} = 20 \text{ bytes}$

Capa 4: $\text{Cabecera TCP (mínima)} = 20 \text{ bytes}$

Capa 4: $\text{Cabecera UDP (mínima)} = 8 \text{ bytes}$

- Cada subsistema tendrá un pequeño tráfico de control de sus protocolos el cual se considerará despreciable.

3.2.2 Subsistema de Gestión de Red SGDR

El subsistema de gestión de red estará compuesto por 2 NMSs redundantes ubicados en los Centros de control y los agentes SNMP de los switches de Acceso, Agregación y Core que estarán distribuidos por diversas instalaciones de la autopista. Si bien pudiese integrarse otros equipos como UPSs, servidores o cámaras al subsistema, esto no se contempla en el proyecto ya que estos equipos serán atendidos por las plataformas de sus propios subsistemas.

SNMP funciona con 2 directivas básicas, solicitud de OIDs desde el NMS a los switches en forma de polling (solicitud del NMS a todos los switches de la red) y el envío de TRAPS desde los switches hacia el NMS en caso de la activación de alguna alarma.

Dentro de los requerimientos está que se ocupará SNMPv2, se supondrá una comunicación SNMP eficiente ocupando Getbulk para las solicitudes desde el NMS a los agentes de los switches.

El tráfico de red del subsistema será mayoritariamente ascendente debido a que serán los switches los que reportarán sus OIDs hacia NMS cuando este ejecute el polling, no tendrá una hora cargada, aunque podrá producirse un aumento considerable de tráfico de red debido a alguna anomalía o emergencia que cause que muchos agentes comiencen a enviar TRAPS hacia él NMS, como podría ser el caso de una caída de los switches de agregación que haga perder el balanceo de carga y aumente los consumos de CPUs, un incendio que cause subidas de temperatura en los equipos, cortes de fibra óptica, etc.

3.2.2.1 Cálculo de ancho de banda:

El ancho de banda que consumirá el subsistema de gestión será inversamente proporcional al intervalo de polling que se le configure en él NMS, en este caso se asumirá un funcionamiento con un intervalo de polling de 2 minutos y que las alarmas locales de los switches serán notificadas al NMS mediante TRAPS.

Capas 2, 3 y 4 (UDP)= 50 bytes

Mensaje SNMPv2 GetBulk solicitud:

$$\begin{aligned} 50\ bytes\ &+\ 4\ bytes\ (Versión)\ +\ \sim 10\ bytes\ (comunidad)\ +\ 4\ bytes\ (tipo\ de\ PDU) \\ &+\ 4\ bytes\ (Ident\ de\ sol.)\ +\ 8\ bytes\ (Ctd.\ A\ leer)\ +\ \sim 100\ bytes\ (OIDs) \\ &=\ \sim 130\ bytes \end{aligned}$$

$$130x8\ bits\ x\frac{1}{120}s\ = 8.7\ bps$$

Mensaje SNMPv2 GetBulk respuesta:

$$50\ bytes\ +\ 4\ bytes\ (Versión)\ +\ \sim 10\ bytes\ (comunidad)\ +\ 4\ bytes\ (tipo\ de\ PDU)\ +\ 4\ bytes\ (Ident\ de\ sol.)\ +\ 8\ bytes\ (Ctd.\ A\ leer)\ +\ \sim 600\ bytes\ (objetos)\ =\ \sim 630\ bytes$$

$$630x8\ bits\ x\frac{1}{120s}\ =42\ bps$$

Ahora si consideráramos una situación de emergencia mayor donde 50 equipos realicen él envió de TRAPS cada 1segundo, con un tamaño de trama igual de 630 bytes, igual que en el mesnaje GetBulk de respuesta, tendríamos:

Mensaje SNMPv2 Trap:

$$630x8\ bits\ x50/1s\ =252\ kbps$$

Como se pude observar el tráfico de red en un funcionamiento normal del subsistema es despreciable con un peak en una emergencia grave bajo los 300 kbps.

3.2.3 Sistema de Control y Ventilación SCCV

Estará formado por 2 PLCs redundantes ubicados en los centros de control y una serie de cabeceras de entradas y salidas remotas ubicadas en las salas eléctricas y postes SOS a lo largo de la autopista, siendo mucho más densa su cantidad en zonas de túnel. La comunicación entre las cabeceras y los PLCs será mediante ModbusTCP.

La función principal del subisistema será la de controlar y monitorear las condiciones de ventilación y gases dentro del túnel monitoreando, anemómetros, opacímetros, Sensores NO2, Sensores de CO, alarmas de ventiladores, controles de Galibo, etc. Además, monitoreará diversas variables de otros subsistemas, como los sensores de puertas de acceso a salas eléctricas o postes SOS, sensor de extintores, barreras, y estado de alimentación y/o emergencia a través de contactos libres de potencia que tienen la mayoría de los equipos que forman el ITS.

3.2.3.1 **Cálculo de ancho de banda:**

El flujo del tráfico de red del subsistema y ancho de banda ocupado estará principalmente dado por:

- Cantidad de entradas/salidas y registros internos que se necesite leer / escribir
- De cómo el programador de los PLCs y cabeceras defina la interacción entre los dispositivos, en función de la arquitectura Cliente-Servidor.
- Tipo de instrucción (Function Code) que se utilice.

Un error importante que puede afectar en el desempeño de la red es configurar PLCs y cabeceras, es la solicitud de lectura de registro de manera individual, provocando una trama por cada solicitud.

Por ejemplo, si tenemos que leer 100 registros cada 10 ms tendríamos:

Capas 2, 3 y 4 (TCP)= 62 bytes

Solicitud individual de lectura de registros internos ModbusTCP:

$$62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) + 2\ bytes\ (Dirección\ de\ Inicio) +\ 2\ bytes\ (Cantidad\ de\ Registros) = 74\ bytes$$

$$74\ x8\ bits\ x100x\ \frac{1}{0.01s} = 5.92\ Mbps$$

Respuesta a solicitud individual de lectura de registros internos ModbusTCP:

$$62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP)\ +\ 1\ byte\ (instrucción\ modbus) + 1\ (Contador)\ +\ 2\ bytes\ (Estado)\ +\ 2\ bytes\ (Cantidad\ de\ Registros) = 73\ bytes$$

$$73\ x8\ bits\ x100x\ \frac{1}{0.01s} = 5.84\ Mbps$$

Ahora si realizamos la misma implementación de manera eficiente con una solicitud de lectura múltiple de registros internos ModbusTCP, donde el tamaño de la trama será el mismo que en el caso de solicitud individual:

$$74\ x8\ bits\ x1x\ \frac{1}{0.01}s = 57.6\ kbps$$

Respuesta de lectura múltiple de registros internos ModbusTCP:

$$62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP)\ +\ 1\ byte\ (instrucción\ modbus) + 1\ (Contador)\ +100\ x\ 2\ bytes\ (Estado) + 2\ bytes\ (Cantidad\ de\ Registros)\ =\ 271\ bytes$$

$$271\ x8\ bits\ x\ \frac{1}{0.01s} = 216.8\ Kbps$$

Ya que no se tiene el detalle exacto de la cantidad de entradas, salidas , variables y forma en que se implementaran los PLCs se asumirá una arquitectura con los PLCs como clientes y cada cabecera como servidor, donde de cada cabecera se necesita leer 100 registros y escribir 30 registros, con un refresco de variables cada 10 ms lo que permitiría por ejemplo, monitorear 90 variables análogas y 160 estados digitales (1bit por entrada) desde registros internos, además de controlar 26 variables análogas y 64 digitales, también desde registros internos.

Se plantea las lecturas en registros internos ya que es común que la conversión desde el valor análogo a una unidad de ingeniería se realice en equipo terminal, Además, dentro de las instrucciones Function Code existentes en ModbusTCP, indicados en la tabla 2-6, se encuentra el 23 Read/Write Multiple registers, que permite leer/escribir múltiples registros con una sola instrucción, lo cual hace aún más eficiente la comunicación.

Desde el PLC hacia las cabeceras en campo de datos se tendrá:

$$\begin{aligned} 62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) \\ +\ 2\ bytes\ (Dirección\ de\ Inicio\ a\ leer) \\ +\ 2\ bytes\ (Cantidad\ de\ Registros\ a\ leer) \\ +\ 2\ bytes\ (Dirección\ de\ Inicio\ a\ escribir) \\ +\ 2\ bytes\ (Cantidad\ de\ Registros\ a\ escribir) \\ +\ 1\ byte\ (Contador\ de\ escritura) \\ +\ (22+8)x\ 2\ bytes\ (valores\ a\ escribir)\ =\ 139\ bytes \end{aligned}$$

$$139\ x8\ bits\ x\ \frac{1}{0.01s} = 111.2\ Kbps$$

De las cabeceras hacia el PLC:

$$\begin{aligned} 62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) \\ +\ 1\ byte\ (Contador\ ) +\ (90+10)x\ 2\ bytes\ (valores\ leidos)\ =\ 202\ bytes \end{aligned}$$

$$202\ x8\ bits\ x\ \frac{1}{0.01s} = 161.6\ Kbps$$

Como puede verse el tráfico puede perfilarse como bidireccional, el ancho de banda se mantendrá constante durante el día y no tendrá una hora cargada.

3.2.4 Subsistema de Circuito Cerrado de Televisión SCTV

El subsistema de CCTV ser compone de todas las cámaras distribuidas por las diferentes locaciones de los túneles y zonas abiertas y el servidor del subsistema ubicado en los Centros de Control.

Las cámaras serán en su mayoría fijas y en casos particulares móviles. Debido a que las imágenes serán grabadas en todo momento el flujo de tráfico hacia Centro de control Principal será más menos constante durante el día y principalmente ascendente, solo existiendo un pequeño tráfico de control o de comandos de forma descendente.

El Codec H.264/AVC será el ocupado para la compresión del video y ocupará RTP para su transmisión.

Cada cámara cuenta con un servidor Web que permite configuración local de las cámaras y también es posible configurar el envío de correo por eventos o alarmas.

Como se indicó en el punto 2.2.5 el ancho de banda que generan las diferentes cámaras del sistema depende fundamentalmente de 5 factores, resolución, complejidad y actividad en la escena, FPS y algoritmo de compresión.

Para obtener los valores de tráfico de manera lo más fiable posible se utilizará el calculador de tráfico de Arxys, especialista en análisis de datos, que se encuentra en [96] y permite elegir entre los diferentes parámetros de la cámara para determinar su ancho de banda. Como algoritmo de compresión se utilizará H.264-HQ (High Quality) que ofrece la mejor calidad dentro de la herramienta, además permite modificar:

Resolución: La herramienta permite elegir 22 niveles de resolución. Para obtener una resolución alta se trabajará con Full HD 2.1MP.

Complejidad: La herramienta tiene 4 niveles de complejidad de escena. Se asignará el nivel bajo (33%) para las escenas dentro del túnel y medio-alto (75%) para las escenas de exterior.

Actividad: La actividad corresponden al porcentaje de pixeles que cambian en la escena que principalmente dependerá del flujo de vehículos y del movimiento de la cámara.

La herramienta ofrece 5 niveles distintos. La mayoría de las cámaras serán fijas y estarán visualizando zonas con flujos de vehículos donde se elegirá un nivel muy bajo (15%) para un flujo bajo o nulo de vehículos, bajo (30%) para un flujo medio de vehículos y medio (50%) para un alto flujo de vehículos.

Para el caso de las cámaras con barrido o movimiento constante los valores de actividad serán medio (50%) para el flujo bajo de vehículos, medio-alto (60%) para un flujo medio de vehículos y alto (100%) para alto flujo de vehículos.

Existirán cámaras que estén enfocando controles de acceso a salas eléctricas, postes SOS u oficinas, donde se considerara un nivel medio (50%) para horario laboral en temporada de vacaciones y medio- bajo (30%) para horario laboral en temporada normal y bajo (15%).

FPS: La herramienta permite asignar cualquier valor, se utilizarán 20 y 30 FPS.

Existen 5 tipos de cámaras diferentes repartidas a lo largo de la autopista, fijas indoor, fijas outdoor móviles internos, móviles externas y térmicas. Las cámaras móviles en su mayoría solo serán movidas por el operador en casos esporádicos y solo en 2 casos en zonas abiertas tendrán una rotación constante haciendo un barrido de 180° en zonas.

En la tabla 3-1 se pueden ver los valores arrojados por la herramienta. Es importante indicar que los valores son aproximados y cuando la red esté en explotación pudiendo obtener estadísticas se podrá calibrar mejor el perfil.

Cámaras	Mínimo	Medio	Máximo
Indoor (20 FPS)	0.93 Mbps	1.74 Mbps	3.14 Mbps
Outdoor (20 FPS)	1.34 Mbps	2.51 Mbps	4.52 Mbps
Outdoor movimiento (20 FPS)	4.52 Mbps	9.22 Mbps	10.51 Mbps
Accesos (20 FPS)	0.93 Mbps	1.74 Mbps	3.14 Mbps
Indoor (30 FPS)	1.39 Mbps	2.61 Mbps	4.71 Mbps
Outdoor (30 FPS)	2.01 Mbps	3.76 Mbps	6.78 Mbps
Outdoor movimiento (30FPS)	6.78 Mbps	13.83 Mbps	15.77 Mbps
Accesos (30 FPS)	1.39 Mbps	2.61 Mbps	4.71 Mbps

Tabla 3-1 Ancho de banda para los diferentes tipos de cámara

3.2.5 Subsistema de Detección Automática de Incidentes SDAI

El Subsistema de Detección Automática de Incidentes es una ayuda para la gestión de tráfico dentro del túnel. Este sistema automatiza los procesos de búsqueda de vehículos detenidos, humo, marcha en sentido contrario, caída de objetos u obstrucción de la vía.

Combina la tecnología del procesamiento de imágenes y la conformación de filtros para determinar el tipo de evento a informar. Al ser un sistema integrable con el software de gestión de la autopista permite visualizar en tiempo real el estado de funcionamiento y visualización de alarmas como el resto de equipos de campo.

Si bien las cámaras del subsistema DAI tienen particularidades, ocuparán el mismo Codec que el subsistema CCTV H.264, por lo que los perfiles de tráfico serán igual que este subsistema con la salvedad que existirá un tráfico despreciable enviado por la cámara al detectar una incidencia.

3.2.6 Subsistema de telefonía STEL

El subsistema de telefonía es basado en SIP para el establecimiento de las sesiones y luego RTP para el tráfico de voz. El subsistema estará formado por 2 centrales PBX (Private Branch Exchange) ubicadas en cada centro de control para la interconexión y gestión de las llamadas, 2 centrales Gateway Telefónicos ubicadas en cada centro de control para llamadas hacia el exterior y una serie de teléfonos VoIP de diferentes características, los que en su gran mayoría ubicados en los centros de control y 10 repartidos en salas eléctricas y locales técnicos.

No se conoce el Codec que se utilizará por lo que se asumirá G.711 o G.722 que permite un alto nivel de MOS (More Score Opinion).

3.2.6.1 Cálculo de Ancho de banda:

A diferencia de los subsistemas SCTV o de comunicaciones M2M (machine to machine) como los subsistemas SDTI, SCCV, SILU, etc. el sistema de telefonía tendrá un aumento en su tráfico en horas de mayor trabajo dentro de la administración de la autopista o en algún caso de emergencia.

Para las horas fuera del horario laboral normal, por la noche, se considerará un factor de utilización de 10%, en el horario laboral de 30% y ante una emergencia de un 80%, lo que ocupando los valores de ancho de banda por Codec indicados en la tabla 2-3 se obtiene:

Llamada	Mínimo	Medio	Máximo
G.711	9 kbps	44 kbps	70 kbps
G.722	9 kbps	44 kbps	70 kbps

Tabla 3-2 Ancho de banda ocupado por el subsistema de telefonía

El flujo de tráfico será en su mayoría será dentro del centro de control debido a que es aquí donde se ubicarán la mayoría de los teléfonos y que las llamadas en general estarán dirigidas hacia el exterior a través de los Gateway. Para el tráfico de los teléfonos repartidos a lo largo de la autopista se considerará que el tráfico es bidireccional.

3.2.7 Subsistema Detección de Incendios SDTI

El subsistema de detección de incendios está compuesto por las centrales de detección puntual y línea más una serie de periféricos que realizaran el sensado e informaran a dichas centrales a través de señales análogas y digitales.

En el caso de las centrales puntuales su detección se basa en periféricos como pulsadores manuales, detectores de humo, temperatura, etc. además de una serie de relés para la conexión de actuadores para el cierre de puertas, alarmas sonoras, paro de ventiladores etc.

Las centrales de detección lineal se basan en un cable detector que se instala a lo largo de los túneles que se conecta a la central, estas centrales por lo general no están preparadas para la conexión de actuadores.

Ambos tipos de centrales envían sus datos a un servidor dedicado utilizando ModbusTCP, que en un funcionamiento normal será el ubicado en el Centro de Control.

3.2.7.1 Cálculo de ancho de banda

Como no se tiene el detalle de implementación del protocolo ModbusTCP en el subsistema, se asumirá una arquitectura donde el cliente será el servidor principal y cada central puntual y lineal los servidores.

Para las centrales puntuales las solicitudes de lectura y escritura enviadas por el servidor dedicado hacia la central serán de manera eficiente, ocupando la Function Code 23 que permite leer y escribir registros en la misma instrucción y el intervalo de solicitud será de 10 ms.

Se considerará la lectura de 20 registros internos que se traduce en la lectura de 18 variables análogas y 32 digitales.

Las centrales solo tienen salidas digitales por lo que se considerará la escritura de 2 registros lo que implican 32 salidas.

Capas 2, 3 y 4 (TCP)= 62 bytes

Desde el servidor del Centro de control hacia las centrales:

$$\begin{aligned} 62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) \\ +\ 2\ bytes\ (Dirección\ de\ Inicio\ a\ leer) \\ +\ 2\ bytes\ (Cantidad\ de\ Registros\ a\ leer) \\ +\ 2\ bytes\ (Dirección\ de\ Inicio\ a\ escribir) \\ +\ 2\ bytes\ (Cantidad\ de\ Registros\ a\ escribir) \\ +\ 1\ byte\ (Contador\ de\ escritura) +\ 2\ x\ 2\ bytes\ (valores\ a\ escribir) \\ =\ 83\ bytes \end{aligned}$$

$$83\ x8\ bits\ x\ \frac{1}{0.01s} = 66.4\ Kbps$$

Desde el servidor del Centro de control hacia las centrales:

$$\begin{aligned} 62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) \\ +\ 1\ byte\ (Contador\ ) +\ (20)x\ 2\ bytes\ (valores\ leidos)\ =\ 111\ bytes \end{aligned}$$

$$111x8\ bits\ x\ \frac{1}{0.01s} = 88.8\ Kbps$$

El tráfico se considera bidireccional, el ancho de banda se mantendrá constante durante el día y no tendrá una hora cargada.

3.2.8 Subsistema de Radiocomunicaciones SRAD

El sistema de Radiocomunicaciones será principalmente para las labores en campo del personal que estará en la explotación, brindar de cobertura FM de radios comerciales y conectar con sistemas de Policía y ambulancias.

Será un sistema digital de Radio DMR (Digital Mobile Radio) estandarizado por la de la ETSI (European Telecommunications Standards Institute), enmarcado en los sistemas de comunicaciones de emergencia.

El Subsistema estará formado por 2 estaciones maestras redundantes y 6 esclavos instalados cada aproximadamente 2 km de distancia.

Las estaciones maestras estarán recepcionando la cobertura radial de los sistemas de emergencia, radios FM y comunicaciones internas, les asignará diferentes canales en el sistema DMR y lo enviará a los esclavos que ya sea mediante cable radiante para zonas de túnel o de antenas en zonas abiertas brindaran la cobertura a los equipos radiales.

La comunicación entre las estaciones maestras esclavas se hará mediante fibra óptica monomodo y protocolos propietarios, además estos equipos estarán conectados a la red de comunicaciones para su gestión mediante SNMP.

3.2.8.1 Cálculo de ancho de banda

Al utilizar SNMP se considerarán los mismos parámetros que para el subsistema de gestión de la Red SDGR, con consultas SNMP cada 2 min y configurando los TRAPs en los equipos para el envío de alarmas por lo que su tráfico será despreciable

3.2.9 Subsistema de Control iluminación SILU

La iluminación de una autopista es fundamental para brindar mayor seguridad a los usuarios, estará formado 2 unidades controladoras ubicadas en los centros de control y 16 unidades remotas que controlaran la electrónica para el cambio en los niveles de luminosidad. Estas unidades estarán ubicadas en las diferentes zonas de la autopista, principalmente dentro de los túneles instalado en los gabinetes de los postes SOS.

Las comunicaciones entre las unidades remotas y las unidades controladoras serán mediante ModbusTCP.

3.2.9.1 Cálculo de ancho de banda

Como no se tiene el detalle de implementación del protocolo ModbusTCP en el subsistema, se asumirá una arquitectura donde el cliente será las unidades controladoras y los servidores las unidades remotas.

Debido a su similitud desde el punto de vista de la red, se ocuparán los datos de ancho de banda y comportamiento del subsistema de Detección de incendios SDTI.

3.2.10 Subsistema de control energía de baja tensión SCBT

El subsistema tendrá una arquitectura distribuida tipo DCS (Distributed Control System). estará formado por un PLC, UPSs, equipos de transferencia eléctrica de potencia, generadores y analizadores de red eléctrica. Las comunicaciones dentro del DCS se harán mediante buses seriales sobre RS-485 utilizando Profibus y serán centralizadas en el PLC que a su vez se comunicará con sistema SCADA principal ocupando PROFINET-IO.

3.2.10.1 Cálculo de Ancho de Banda:

Como no se tiene el detalle de implementación del protocolo Profinet IO en el subsistema, se asumirá una el uso de UDP en la capa de transporte y se considerará el envío desde el PLC hacia el SCADA sin que este realice solicitud con un intervalo de 5ms.

Se considerará el envío de 300 registros internos, que se traduce en de 280 variables análogas y 320 digitales, suficiente para todas las variables del DCS

Capas 2, 3 y 4 (UDP)= 50 bytes

$$50\ bytes\ +\ 2\ Bytes\ (\ Ident.de\ trama) +\ 2\ byte\ (contador\ ciclico) + 1byte\ (Estado\ de\ datos) +\ 1\ byte\ (Estado\ de\ transferencia) + 2\ x\ 300\ bytes\ (valores\ )\ =\ 656\ bytes$$

$$656\ x8\ bits\ x\ \frac{1}{0.005s}\ = 1.05\ Mbps$$

El tráfico se considera principalmente ascendente, el ancho de banda se mantendrá constante durante el día y no tendrá una hora cargada.

3.2.11 Subsistema de Postes SOS SSOS

El Subsistema de postes SOS está formado por 50 postes ubicados a lo largo de la autopista y servidores de control redundados ubicados en los centros de control.

habrá Postes tanto de interior para tramos de túnel y exteriores para tramos abiertos. En los postes se deja espacio en el gabienete para la conexión de otros equipos y la instalación de los switches de acceso.

Cada poste SOS tendrá diversos periféricos como altavoz, micrófono, pulsador de llamada de emergencia, etc. que se conectará a una tarjeta que concentra la información y se la comunicará al servidor.

3.2.11.1 **Cálculo de ancho de banda**

Las comunicaciones de voz desde los postes con el centro de control ocuparán los Codecs G.711 y G.722 con RTP. Las comunicaciones serán sumamente esporádicas ya que se dará en casos de emergencia, por lo que se asigna un porcentaje de utilización de 1% para un funcionamiento normal, 20% para una emergencia baja y 90% para una emergencia grave donde muchos usuarios en los Postes quieren hablar hacia el centro de emergencia.

En base a la tabla 2-3 el ancho de banda que el audio del subsistema será:

Llamada	**Mínimo (1%)**	**Medio (20%)**	**Máximo (90%)**
G.711	1 kbps	17 kbps	78 kbps
G.722	1 kbps	17 kbps	78 kbps

Tabla 3-3 Ancho de banda de audio para Subisistema SSOS

Las comunicaciones de control de pulsadores, detectores etc. se harán mediante un protocolo propietario del cuál no existe información accesible, por lo que se supondrá el uso de Modbus TCP, donde el servidor SOS será el cliente y cada unidad remota en el poste el servidor

Las solicitudes de lectura enviadas por el servidor hacia la central se supondrán ocupando la Función Code de lectura y el intervalo de solicitud de 10 ms.

Se considerará la lectura de 5 registros internos que se traduce en la lectura de 4 variables análogas y 16 digitales.

Capas 2, 3 y 4 (TCP)= 62 bytes

Desde el servidor del Centro de control hacia los postes:

$$62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ de\ lectura) + 2\ bytes\ (Dirección\ de\ Inicio) +\ 2\ bytes\ (Cantidad\ de\ Registros) = 74\ bytes$$

$$83\ x8\ bits\ x\ \frac{1}{0.01s} = 66.4\ Kbps$$

Desde los postes hacia el servidor del Centro de Control:

$$62\ bytes\ +\ 7\ Bytes\ (Cabecera\ MBAP) +\ 1\ byte\ (instrucción\ modbus) + 1\ byte\ (Contador\ ) +\ 5\ x\ 2\ bytes\ (valores\ leidos)\ =\ 81\ bytes$$

$$81x8\ bits\ x\ \frac{1}{0.01s} = 64.8\ Kbps$$

Se considerará que el flujo de tráfico es bidireccional, el ancho de banda se mantendrá más menos constante constante durante el día, donde pueden producirse peaks debido a alguna emergencia.

3.2.12 Subsistema de Megafonía SMEG

El Sistema de Megafonía se compone de un conjunto de altavoces instalados dentro de los túneles de la autopista, equipos de amplificación y control distribuidos para la alimentación y gestión de los altavoces y los servidores de gestión más la estación de micrófono ubicados en los centros de control.

El software de gestión será capaz de modificar y monitorear parámetros de las unidades como amplificación, estados internos, uso de potencia, etc y también permite la activación salidas digitales.

Cálculo de ancho de banda:

El sistema de megafonía ocupará los codec G.711 y G.722 para la codificación de audio además de RTP para su transporte. Su factor de utilización se comportará de manera muy similar al subsistema de postes SOS, por lo que los valores indicados en el punto 3.2.11.1 desde el servidor del Centro de control hacia las centrales serán válidos.

El software de gestión se comunicará los equipos de control y amplificación mediante un protocolo propietario del cuál no existe información accesible, por lo que se supondrá el uso de Modbus TCP, donde el servidor megafonía será el cliente y cada unidad de control y amplificación el servidor.

Los valores de ancho de banda indicados en el subsistema de detección de incendios SDTI serán valido para megafonía dado su similitud en la cantidad de variables a monitorear/controlar.

3.2.13 Subsistema de Señalización de tráfico SGTR

El subsistema se compone de una serie de dispositivos que le entregaran al usuario de la autopista la señalización que cambiará dinámicamente en función de tráfico y/o emergencias. Estará compuesto por paneles de mensajería variable, señales de aspa flecha, límite de velocidad, control de carril y servidores de gestión redundadnos ubicados en los centros de control.

3.2.13.1 Cálculo de ancho de banda

El subsistema utilizará ModbusTCP para la comunicación entre los diferentes equipos de campo con el servidor.

Por seguridad, la implementación del protocolo en este subsistema hace que el tráfico sea sumamente bajo ya que el mensaje ModbusTCP solo será enviado producto de algún cambio que deba cargarse en el dispositivo de señalización, por lo que se considerará despreciable, lo que produce que el tráfico de red sea principalmente ascendente con las pocas variables de estado que puede tener un dispositivo de señalización.

Debido al bajo número de variables y a que tráfico descendente es despreciables se utilizarán los valores de ancho de banda ascendente ModbusTCP indicados para el subsistema SOS.

El ancho de banda se mantendrá constante durante el día y no tendrá una hora cargada.

Capítulo 4 Pruebas

Con el propósito de determinar la configuración final y obtener valores de convergencia, latencia y jitter del equipamiento en particular se efectuaron una serie de pruebas.

Las pruebas se realizaron en el transcurso de 17 días en las oficinas del cliente quien facilito los equipos, estos serán los mismos indicados en el capítulo 3 donde se planteó el caso práctico.

Todas las conexiones entre switches se realizaron con módulos de fibra óptica marca Huawei 1310nm sobre patch cords de fibra mono modo de 4m.

Para todas las pruebas se ocuparon 2 o 3 laptops dependiendo de la prueba, estos tienen las siguientes características:

Rol	**Cliente Iperf**
Modelo	HP 14-cf0051 od
Almacenamiento	256 GB M.2 SSD
Procesador	Intel Core i5-8250U CPU 1.6GHz 1.8GHz
Memoria	8 GB DDR4-2400 SDRAM (1 x 8 GB)
NIC	Realtek PCIe GBE Family Controller
S.O	Windows 10 home 64 bits

Tabla 4-1 Características del laptop del Cliente Iperf

Rol	**Servidor Iperf**
Modelo	Hp 17-w202la
Almacenamiento	SATA de 1 TB y 7200 rpm
Procesador	Intel Core i7-7700HQ 2,8 GHz, 3,8 GHz
Memoria	12 GB DDR3-1600 SDRAM (1 x 4 GB, 1 x 8 GB)
NIC	Realtek PCIe GBE Family Controller
S.O	Windows 10 home 64 bits

Tabla 4-2 Características del laptop del Servidor Iperf

Rol	Capturador de tráfico
Modelo	Hp 15-k050la
Almacenamiento	SATA de 1 TB y 7200 rpm / 256 GB SSD
Procesador	Intel Core i7-4510U CPU 2GHz 3.1GHz
Memoria	8 GB DDR3-1600 SDRAM (1 x 8 GB)
NIC	Realtek PCIe GBE Family Controller
S.O	Windows 8.1 profesional

Tabla 4-3 Características del laptop para capturar tráfico

Para obtener la medición de convergencia se realizará el envío de paquetes a una tasa constante, luego se simula una desconexión y se mide la cantidad de paquetes perdidos para obtener el tiempo aproximado.

La herramienta elegida para este propósito es Iperf 3, software ampliamente utilizado en la academia, que entrega un informe de la cantidad de paquetes perdidos por un periodo configurable que por defectos es de 1 segundo y será el que se ocupará para simplificar el cálculo. Si bien en algunos trabajos [50] se ha revisado el determinismo que presenta Iperf, el software no es una herramienta profesional y estará limitada al comportamiento que presenten las tarjetas de red de los equipos donde se ejecutará el software, por lo se evaluará la estabilidad de la herramienta elegida con el propósito de determinar la fiabilidad de la medida.

Para la medición y comparación de jitter se realiza de dos formas, la primera también se utilizará Iperf 3, que entrega un informe de jitter por un periodo determinado configurable, que por defecto es de 1 segundo y será el que se ocupará para las pruebas. La segunda forma será utilizada en la prueba de comunicación entre PLCs, configurando una interfaz mirroring que reenvié los paquetes el switch donde estará conectado uno de los 2 PLCs al laptop capturador con el software wireshark, revisando la diferencia de recepción de los paquetes.

Para ver la dispersión y tendencia de los datos se determinará de cada medida el máximo, mínimo, y los estadísticos, promedio, mediana y coeficiente de variación (CV).

4.1 Test de herramienta

Para medir el tiempo de convergencia y obtener la medida con la mayor resolución lograble, lo lógico sería enviar la mayor cantidad de paquetes posibles al mayor throughput con el interpacket Gap (IPG) mínimo que permiten las tarjetas de red del cliente y servidor Iperf (96ns para FE). Lo ideal es que el tiempo entre el envío de cada paquete sea constante con lo que podría determinarse el tiempo de convergencia prácticamente sin errores, ahora, debido a que tanto Iperf 3 como los laptops que se utilizarán para las pruebas no son herramientas profesionales para medir tiempos de convergencia, latencia y jitter, se realizaran 4 pruebas para revisar la estabilidad de frecuencia de envío de paquetes de la herramienta.

Las pruebas 1,2 y 3 buscan determinar la variación de la frecuencia de envío de paquetes y variación de jitter de un segundo a otro, las cuales, si es que el envío de paquetes se realiza a

una tasa constante, debiese ser cercana a 0, y la prueba 4 busca ver la variación del jitter dentro de cada segundo.

Objetivos:

- Determinar el tamaño de paquete más adecuado para realizar las pruebas de convergencia, el tamaño de paquete que presente la mayor estabilidad (menor CV) en la frecuencia de envío de paquetes por segundo será el que se utilice para las pruebas siguientes.
- Determinar si la herramienta es adecuada para realizar las posteriores mediciones de variación de jitter (1%-15%) para un rendimiento Soft Real Time Ethernet.

4.1.1 Procedimiento

Para realizar la evaluación se tomarán 3 largos distintos de paquetes 64 bytes, 768 bytes y 1280 bytes sin incluir los 4 bytes de FCS en el tamaño y se generará tráfico por 60 segundos al mayor throughput posible que permita el software utilizando UDP en la capa de transporte.

i. Se ocupará el reporte de paquetes por segundos enviados que entrega el Cliente Iperf y se revisará su estabilidad en el envío en base a 20 medidas.
ii. Se ocupará el reporte de jitter por segundo que entrega el servidor Iperf y revisará su estabilidad en base a 20 medidas.
iii. Para poder tener un análisis más fino, se configura un puerto mirroring en el switch donde se conecta el cliente Iperf y se capturan los paquetes de las pruebas con wireshark, debido a la gran cantidad de datos que se generan solo se analizaran luego de tomar la decisión de que tamaño de paquete se ocupara en base a las pruebas 1 y 2 utilizando 30 segundos de 10 de las pruebas antes realizadas. No se ocupa wireshark en el mismo computador que Iperf a fin de no afectar la medida.

El montaje se realizará sobre la menor arquitectura posible dentro de la red propuesta en el capítulo de presentación del caso práctico, con 2 switches de acceso.

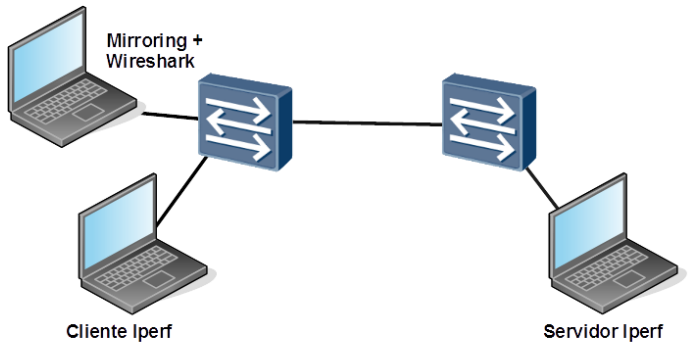


Figura 4-1 Montaje para test de herramienta

Configuración Switches

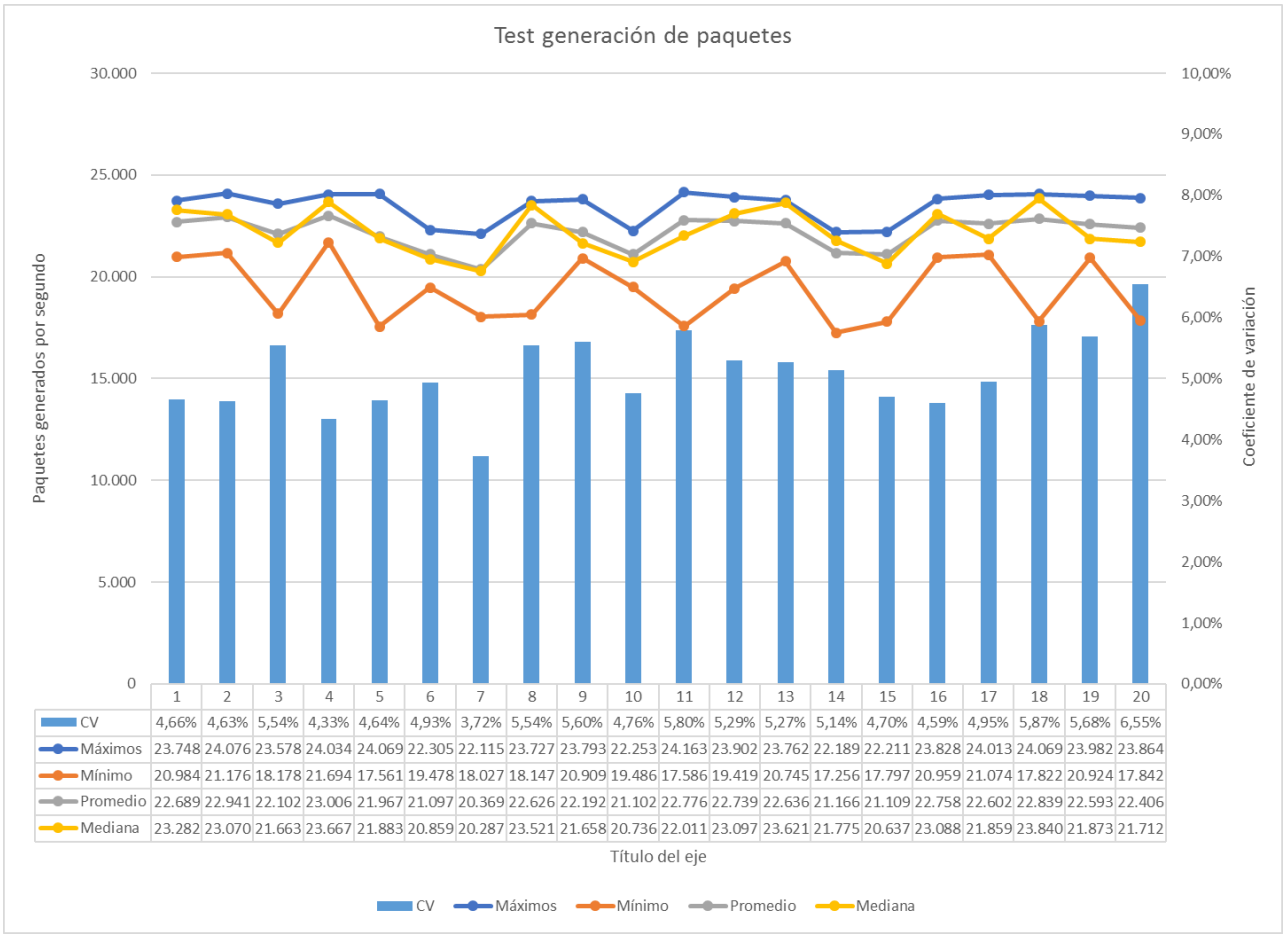
- Se configuran 2 Interfaces GE como troncales e Interfaces FE como accesos para permitir la conexión.
- Se configura una interfaz mirroring donde se conecta el cliente Iperf y se reenvían los paquetes a esta interfaz.

4.1.2 Pruebas

4.1.2.1 Prueba 1: Estabilidad de envío de paquetes y variación de jitter 64 bytes

Se configura Iperf para que envíe tramas por 60 segundos con un tamaño de 64 bytes y un ancho de banda de 100Mbps, lo que Iperf reduce a algo más de 5Mbps para no perder paquetes, con estos parámetros Iperf genera alrededor de 22.000 paquetes por segundo. Los resultados luego de 20 repeticiones se observan en el gráfico de la figura 4-2.

Resultados paquetes generados:



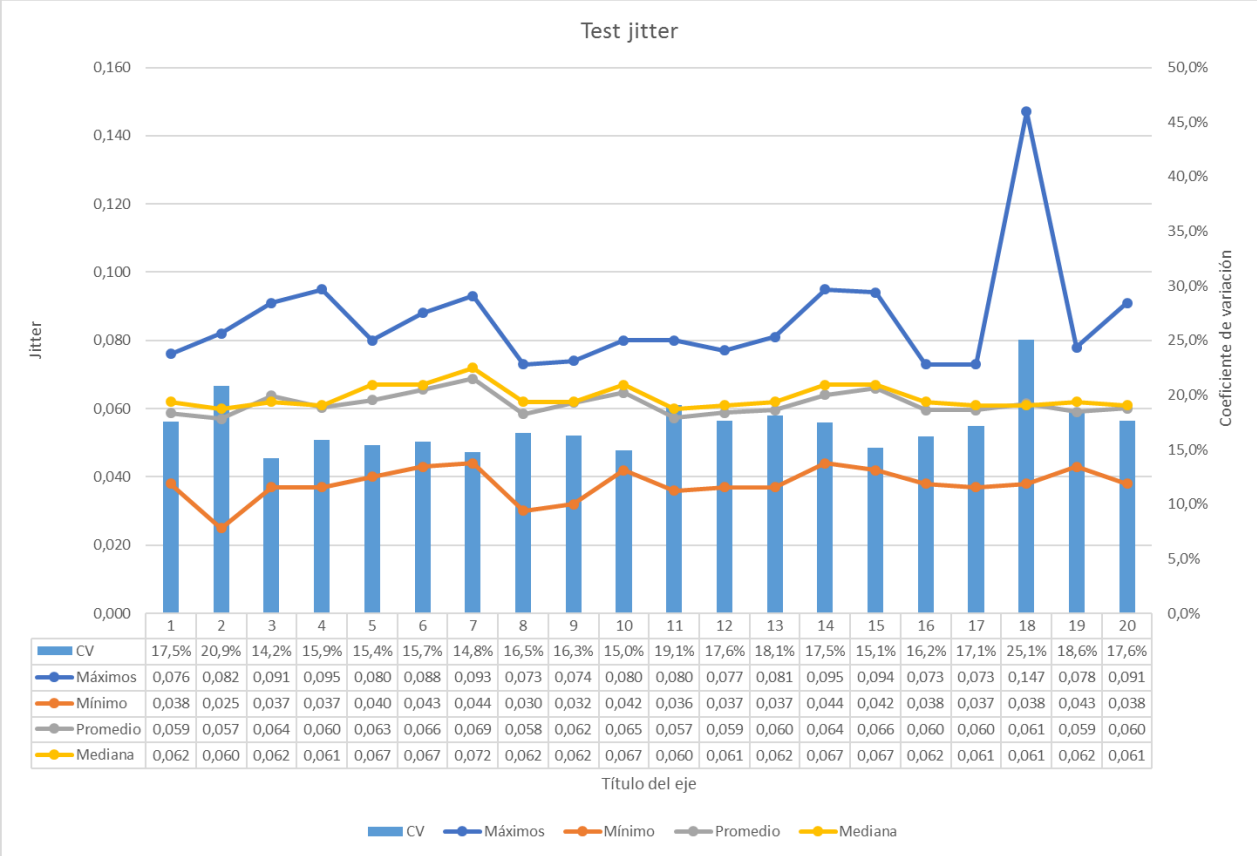
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	4,66%	4,63%	5,54%	4,33%	4,64%	4,93%	3,72%	5,54%	5,60%	4,76%	5,80%	5,29%	5,27%	5,14%	4,70%	4,59%	4,95%	5,87%	5,68%	6,55%
Máximos	23.748	24.076	23.578	24.034	24.069	22.305	22.115	23.727	23.793	22.253	24.163	23.902	23.762	22.189	22.211	23.828	24.013	24.069	23.982	23.864
Mínimo	20.984	21.176	18.178	21.694	17.561	19.478	18.027	18.147	20.909	19.486	17.586	19.419	20.745	17.256	17.797	20.959	21.074	17.822	20.924	17.842
Promedio	22.689	22.941	22.102	23.006	21.967	21.097	20.369	22.626	22.192	21.102	22.776	22.739	22.636	21.166	21.109	22.758	22.602	22.839	22.593	22.406
Mediana	23.282	23.070	21.663	23.667	21.883	20.859	20.287	23.521	21.658	20.736	22.011	23.097	23.621	21.775	20.637	23.088	21.859	23.840	21.873	21.712

Figura 4-2 Grafico de test de generación de paquetes Iperf 64 bytes

Observaciones de resultados:

- Para todas las muestras el coeficiente de variación es muy elevado lo que indica mucha variabilidad en la tasa de envío de paquetes de un segundo a otro.
- Existe una considerable variación entre muestras en todos los valores, máximos, mínimos, promedios y medianas.

Resultados jitter:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	17,5%	20,9%	14,2%	15,9%	15,4%	15,7%	14,8%	16,5%	16,3%	15,0%	19,1%	17,6%	18,1%	17,5%	15,1%	16,2%	17,1%	25,1%	18,6%	17,6%
Máximos	0,076	0,082	0,091	0,095	0,080	0,088	0,093	0,073	0,074	0,080	0,080	0,077	0,081	0,095	0,094	0,073	0,073	0,147	0,078	0,091
Mínimo	0,038	0,025	0,037	0,037	0,040	0,043	0,044	0,030	0,032	0,042	0,036	0,037	0,037	0,044	0,042	0,038	0,037	0,038	0,043	0,038
Promedio	0,059	0,057	0,064	0,060	0,063	0,066	0,069	0,058	0,062	0,065	0,057	0,059	0,060	0,064	0,066	0,060	0,060	0,061	0,059	0,060
Mediana	0,062	0,060	0,062	0,061	0,067	0,067	0,072	0,062	0,062	0,067	0,060	0,061	0,062	0,067	0,067	0,062	0,061	0,061	0,062	0,061

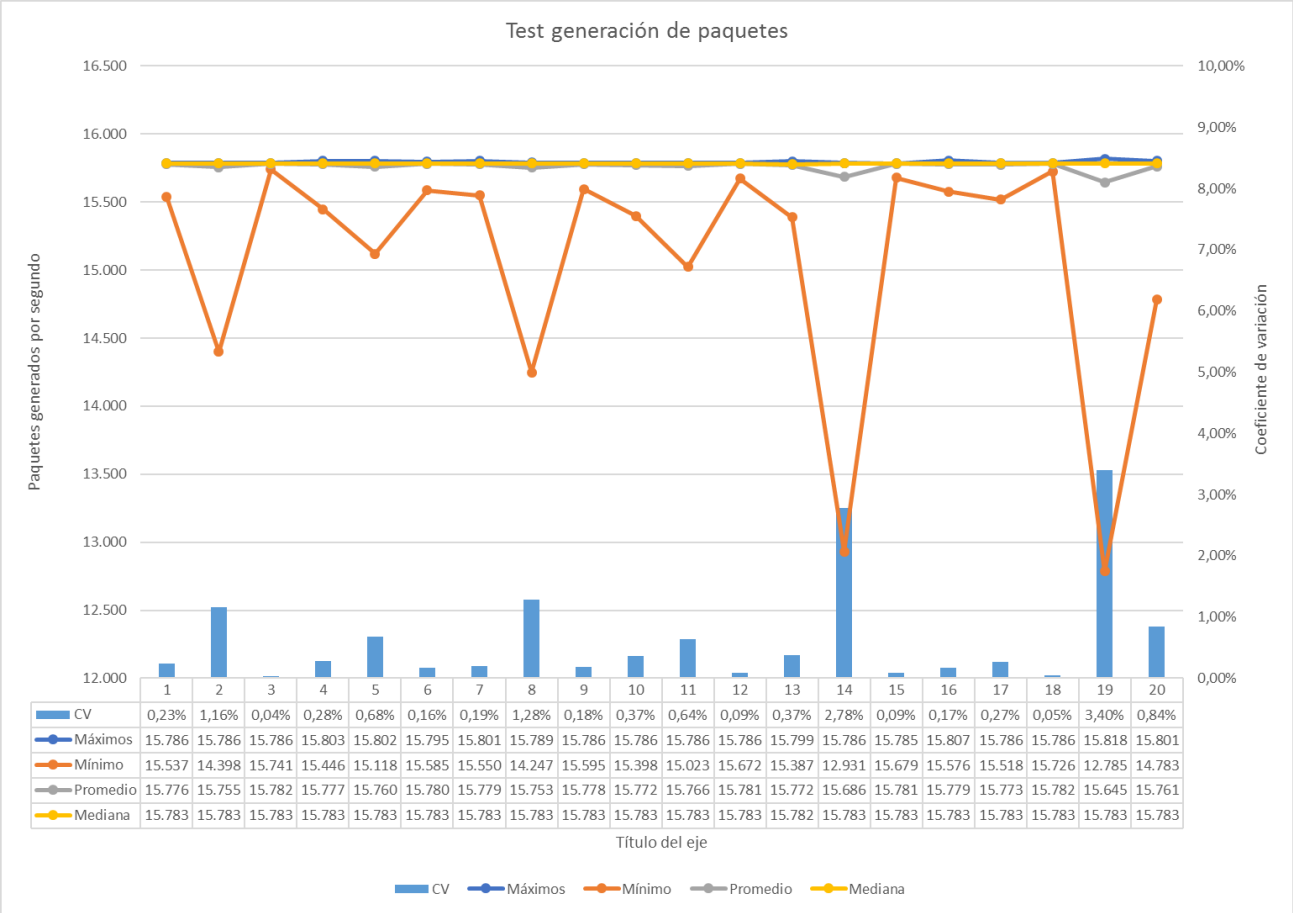
Figura 4-3 Grafico de test de jitter Iperf 64 bytes

Observaciones de resultados:

- El coeficiente de variación se dispara en la prueba debido a un jitter máximo muy elevado en la muestra 18 respecto a las otras muestras de la prueba.
- Todas las pruebas presentan un coeficiente de variación sobre el 15%, que es el valor máximo de jitter que se busca tener para un rendimiento Soft RT-Ethernet.

4.1.2.2 Prueba 2: Estabilidad de envío de paquetes y variación jitter 768 bytes

Se configura Iperf para que envíe tramas por 60 segundos con un tamaño de 768 bytes y un ancho de banda de 100Mbps, lo que Iperf reduce a algo más de 91.7 Mbps para no perder paquetes. con estos parámetros Iperf genera alrededor de 15.780 paquetes por segundo.



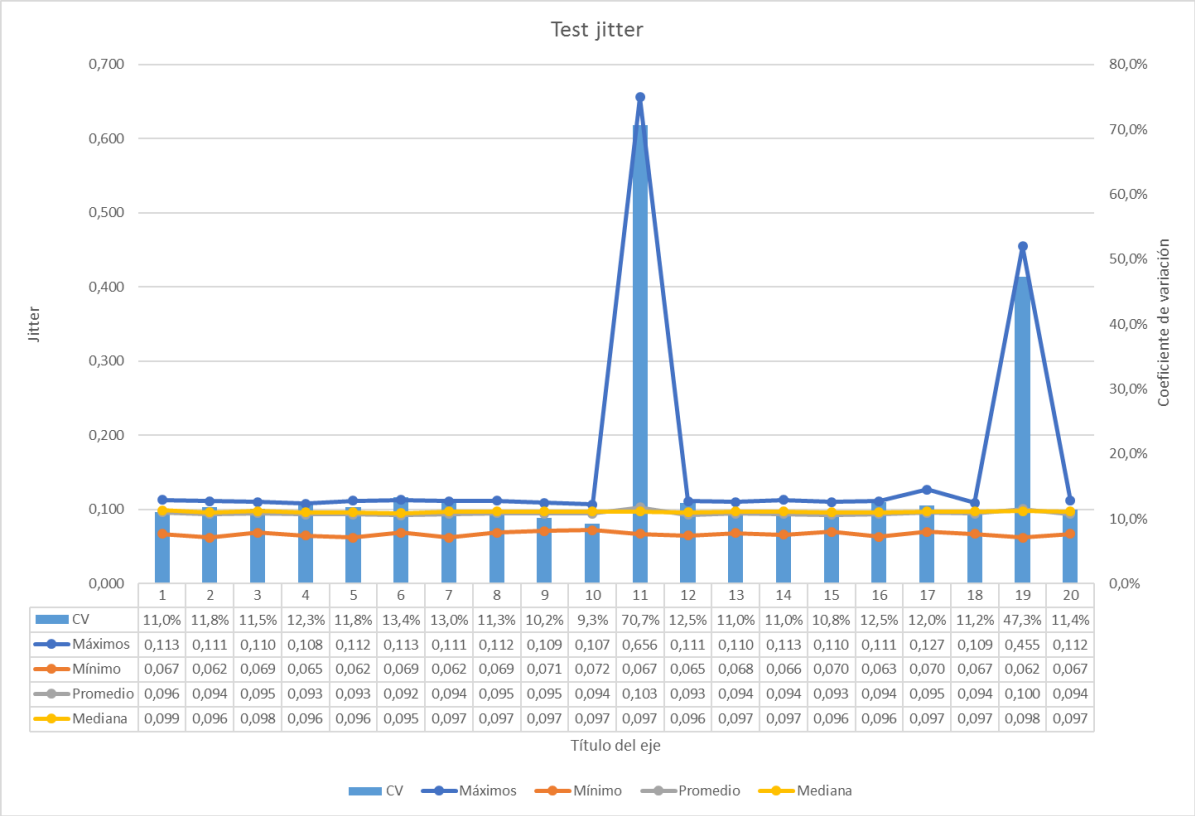
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	0,23%	1,16%	0,04%	0,28%	0,68%	0,16%	0,19%	1,28%	0,18%	0,37%	0,64%	0,09%	0,37%	2,78%	0,09%	0,17%	0,27%	0,05%	3,40%	0,84%
Máximos	15.786	15.786	15.786	15.803	15.802	15.795	15.801	15.789	15.786	15.786	15.786	15.786	15.799	15.786	15.785	15.807	15.786	15.786	15.818	15.801
Mínimo	15.537	14.398	15.741	15.446	15.118	15.585	15.550	14.247	15.595	15.398	15.023	15.672	15.387	12.931	15.679	15.576	15.518	15.726	12.785	14.783
Promedio	15.776	15.755	15.782	15.777	15.760	15.780	15.779	15.753	15.778	15.772	15.766	15.781	15.772	15.686	15.781	15.779	15.773	15.782	15.645	15.761
Mediana	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.783	15.782	15.783	15.783	15.783	15.783	15.783	15.783	15.783

Figura 4-4 Grafico de test de generación de paquetes Iperf 768 bytes

Observaciones de resultados:

- La generación de paquetes por segundo presenta, mucho mejor estabilidad que la prueba 1, con un peak de 3,4%. La variación recae en la presencia de mínimos muy pronunciados en alguno de los intervalos de generación.
- Los valores promedio y mediana presentan valores muy estables lo que indica que la presencia de mínimos muy pronunciados no es relevante dentro del total de las muestras y se deben a un evento en particular.

Resultados jitter:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	11,0%	11,8%	11,5%	12,3%	11,8%	13,4%	13,0%	11,3%	10,2%	9,3%	70,7%	12,5%	11,0%	11,0%	10,8%	12,5%	12,0%	11,2%	47,3%	11,4%
Máximos	0,113	0,111	0,110	0,108	0,112	0,113	0,111	0,112	0,109	0,107	0,656	0,111	0,110	0,113	0,110	0,111	0,127	0,109	0,455	0,112
Mínimo	0,067	0,062	0,069	0,065	0,062	0,069	0,062	0,069	0,071	0,072	0,067	0,065	0,068	0,066	0,070	0,063	0,070	0,067	0,062	0,067
Promedio	0,096	0,094	0,095	0,093	0,093	0,092	0,094	0,095	0,095	0,094	0,103	0,093	0,094	0,094	0,093	0,094	0,095	0,094	0,100	0,094
Mediana	0,099	0,096	0,098	0,096	0,096	0,095	0,097	0,097	0,097	0,097	0,097	0,096	0,097	0,097	0,096	0,096	0,097	0,097	0,098	0,097

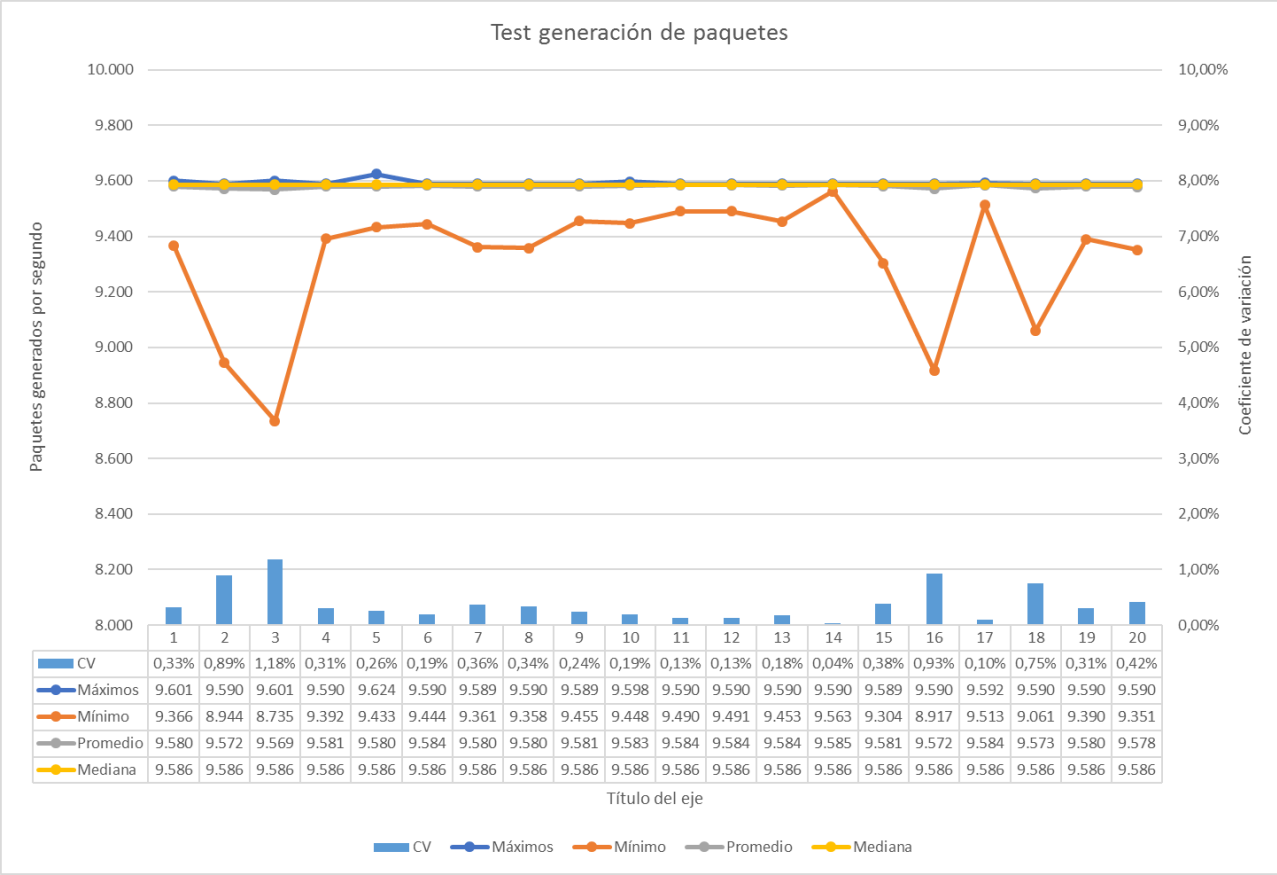
Figura 4-5 Grafico de test de jitter Iperf 768 bytes

Observaciones de resultados:

- El coeficiente de variación se dispara en la muestra 11 debido a un segundo de la muestra con un jitter promedio muy elevado respecto a las otros, lo cual provoca que el CV sea del 70%.
- Todas las pruebas presentan un coeficiente de variación alrededor del 11%, con 2 peaks en las pruebas 11 y 19, lo que indica inestabilidad para poder realizar medidas comparativas de jitter.

4.1.2.3 Prueba 3: Estabilidad de envío de paquetes y variación jitter 1280 bytes

Se configura Iperf para que envíe tramas por 60 segundos con un tamaño de 1280 bytes y un ancho de banda de 100Mbps, lo que Iperf reduce a alrededor de 95 Mbps para no perder paquetes. con estos parámetros Iperf genera alrededor de 9580 paquetes por segundo.



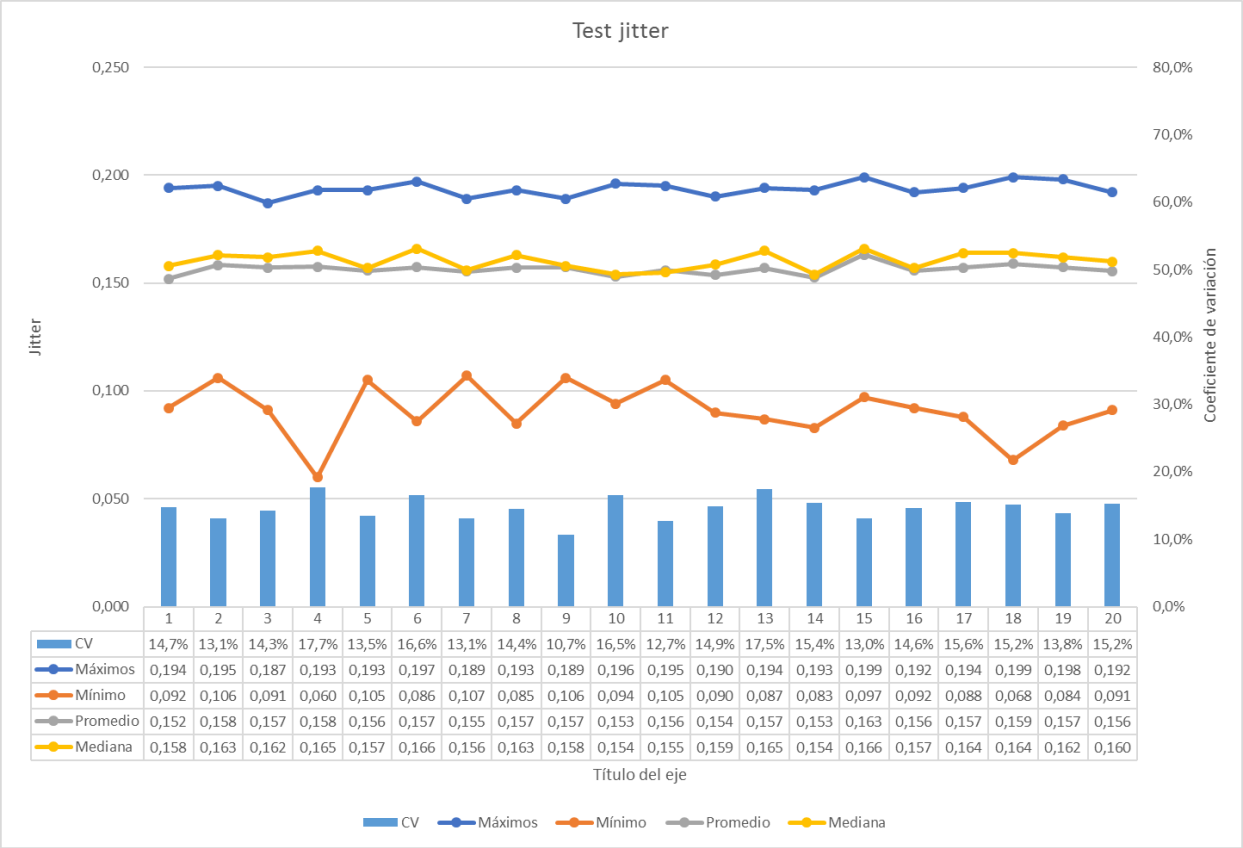
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	0,33%	0,89%	1,18%	0,31%	0,26%	0,19%	0,36%	0,34%	0,24%	0,19%	0,13%	0,13%	0,18%	0,04%	0,38%	0,93%	0,10%	0,75%	0,31%	0,42%
Máximos	9.601	9.590	9.601	9.590	9.624	9.590	9.589	9.590	9.589	9.598	9.590	9.590	9.590	9.590	9.589	9.590	9.592	9.590	9.590	9.590
Mínimo	9.366	8.944	8.735	9.392	9.433	9.444	9.361	9.358	9.455	9.448	9.490	9.491	9.453	9.563	9.304	8.917	9.513	9.061	9.390	9.351
Promedio	9.580	9.572	9.569	9.581	9.580	9.584	9.580	9.580	9.581	9.583	9.584	9.584	9.584	9.585	9.581	9.572	9.584	9.573	9.580	9.578
Mediana	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586	9.586

Figura 4-6 Grafico de test de generación de paquetes Iperf 1280 bytes

Observaciones de resultados:

- Si bien existen 2 peaks de valores mínimos que disparan el coeficiente de variación, en base a la mediana y al promedio y que no existe un máximo de una magnitud importante, se puede inferir que es un evento aislado, lo que se corrobora al observar el detalle de la prueba.

Resultados jitter:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CV	14,7%	13,1%	14,3%	17,7%	13,5%	16,6%	13,1%	14,4%	10,7%	16,5%	12,7%	14,9%	17,5%	15,4%	13,0%	14,6%	15,6%	15,2%	13,8%	15,2%
Máximos	0,194	0,195	0,187	0,193	0,193	0,197	0,189	0,193	0,189	0,196	0,195	0,190	0,194	0,193	0,199	0,192	0,194	0,199	0,198	0,192
Mínimo	0,092	0,106	0,091	0,060	0,105	0,086	0,107	0,085	0,106	0,094	0,105	0,090	0,087	0,083	0,097	0,092	0,088	0,068	0,084	0,091
Promedio	0,152	0,158	0,157	0,158	0,156	0,157	0,155	0,157	0,157	0,153	0,156	0,154	0,157	0,153	0,163	0,156	0,157	0,159	0,157	0,156
Mediana	0,158	0,163	0,162	0,165	0,157	0,166	0,156	0,163	0,158	0,154	0,155	0,159	0,165	0,154	0,166	0,157	0,164	0,164	0,162	0,160

Figura 4-7 Grafico de test de jitter Iperf 1280 bytes

- No se presentan peaks del coeficiente de variación importantes en comparación a las pruebas anteriores.
- Todas las pruebas presentan un coeficiente de variación alrededor del 15%, que es el jitter objetivo.

4.1.2.4 Prueba 4: jitter a partir de paquetes capturados con Wireshark para 1280 bytes.

Al observar las tramas capturadas por wireshark se detecta un comportamiento de ráfagas en la recepción, se observa una serie de paquetes con diferencias de recepción entre ns,1µs y 2µs y luego 3 o 4 paquetes el valor se incrementa alrededor de 300µs, que hace suponer que es el arribo de la siguiente ráfaga, el comportamiento se repite para diferentes rangos de datos, variando el aumento proporcionalmente al aumento del jitter, por ejemplo al detectar un jitter de 1ms los paquete siguientes serán alrededor de 20 con un jitter ns,1µs y 2µs.

Para la medida de tiempo de convergencia que se quiere obtener esto no afecta mayormente ya que se buscan valores en el entorno de los 200ms, si en el transcurso de 1 ms el jitter varía

el error estaría en el entorno de 1ms, además el problema puede radicar tanto en la tarjeta de red emisora como receptora, como en el software.

Para poder obtener un error aproximado se revisa el porcentaje de paquetes que tienen menos de 1ms de jitter y los que se encuentran en tramos superiores, los valores obtenidos sobre 10 muestras de 30 segundo cada una son los siguientes:

	0-1ms	**1-2ms**	**2-3ms**	**3-5ms**	**5-8ms**	**8-10ms**
1	99,84%	0,13%	0,01%	0,00%	0,00%	0,00%
2	99,88%	0,09%	0,02%	0,01%	0,00%	0,00%
3	99,87%	0,08%	0,02%	0,02%	0,00%	0,00%
4	99,87%	0,11%	0,01%	0,00%	0,00%	0,00%
5	99,75%	0,18%	0,04%	0,04%	0,00%	0,00%
6	98,45%	0,52%	0,46%	0,53%	0,03%	0,00%
7	99,90%	0,07%	0,02%	0,01%	0,00%	0,00%
8	97,52%	0,92%	0,62%	0,76%	0,17%	0,01%
9	99,87%	0,11%	0,01%	0,00%	0,00%	0,00%
10	99,86%	0,09%	0,03%	0,02%	0,00%	0,00%

Tabla 4-4 Jitter por rango capturas Wireshark de generación de paquetes

Si bien la cantidad de paquetes que presentan un alto jitter parece despreciable esto puede traer problemas en la medida según la distribución temporal que tenga estos retardos, ya que el tiempo de convergencia se medirá en función de los paquetes perdidos.

Por lo que se toma el peor caso de los mostrados en la tabla 4-4 y se disgrega en la tabla 4-5.

	CTD Paquetes	**% sobre el total**
0-1ms	276024	97,52%
1-2ms	2591	0,92%
2-3ms	1757	0,62%
3-5ms	2154	0,76%
6-8ms	481	0,17%
8-10ms	15	0,01%

Tabla 4-5 Jitter por rango capturas Wireshark de generación de paquetes

Se observa una importante cantidad de paquetes en el rango sobre los 3ms por lo que se revisa la distribución temporal de los eventos y no su probabilidad de suceso, por ejemplo, que entrega la función de distribución acumulada, ya que la probabilidad de suceso será baja, pero afectará más o menos dependiendo de su temporalidad.

	Diferencia
Máximo (ms)	1.282,9
Mínimo (ms)	3,1
Promedio (ms)	10,1
Mediana (ms)	4,4

Tabla 4-6 Análisis de rango de jitter mayor a 3ms

4.1.3 Análisis de resultados:

- Las pruebas 1,2 y 3 muestran que el tamaño del paquete además de influir en la cantidad de paquetes enviados por segundo tiene directa relación con la variación de la tasa de envío de paquetes, siendo el tamaño de **1280 bytes con ancho de banda de 95 Mbps** el que tiene la tasa de envío de paquetes de un segundo a otro con menores Coeficiente de Variación, promediando 0.38% en las 20 muestras, versus 0.66% para paquetes de 768 bytes y 5.11% para 64 bytes.

- En las pruebas 1, 2 y 3 se observan mínimos muy pronunciados. Al mirar el detalle de las pruebas queda de manifiesto que esto se debe a algún segundo dentro de la muestra en el que se genera una cantidad de paquetes muy por debajo del promedio, lo que se debe probablemente a que el hardware/software de las pruebas no es profesional y se pudo haber producido alguna recarga en los buffers. Se descarta una sobrecarga de CPU ya que se monitorearon las durante las pruebas y los consumos no llegaron al 50%

- Dentro de las pruebas 1, 2 y 3 se observa que las variaciones de jitter están muy cercanas o sobre el 15%, que es el valor máximo de jitter para un rendimiento RT-Ethernet, lo que sumado a que la prueba se realizó solo con 2 switches y en comunicaciones sin enrutamiento hace concluir que la herramienta Iperf 3 en el hardware ocupado no permitirá medir posibles mejoras en la red para reducir el jitter ya que el jitter base está demasiado cercano al jitter objetivo.

- En la prueba 4, tomando el peor caso de los mostrados en la tabla 4-4, la posibilidad del suceso de un evento con un jitter elevado dentro de un segundo puede entregar una medida errónea y dado que la mediana de los jitter sobre 1ms está en 4,4ms se tomará un valor de 5ms como un error aproximado en la medida de convergencia, y valores obtenidos bajo los 10ms se calificaran como menores a 10ms, no asegurando su valor por las razones antes expuestas.

4.2 Capa de Acceso

En la revisión de protocolos para evitar los loops se pasó por la familia de protocolos Spaning tree STP, RSTP y MSTP, además del protocolo propietario de Huawei SEP.

STP cuenta con tiempos de convergencia demasiado altos y RSTP que mejora este aspecto no tiene la capacidad de realizar balanceo de carga, si bien es una red sobredimensionada, el balanceo es un deseable del diseño preliminar, además de permitir una fácil mejora en caso de crecimiento futuro.

Los dos protocolos que pueden cumplir con esta tarea son SEP y MSTP, en la tabla se indican las principales ventajas y desventajas de cada protocolo.

En una evaluación primaria SEP presenta mejores características que MSTP para la red planteada, especialmente dada su facilidad de administración, que toma preponderancia en este tipo de redes para la industria, que tiene como objetivo nunca tener caídas.

SEP	**MSTP**
Permite balanceo de carga	Permite balanceo de carga
Protocolo para anillos	Protocolo para anillos o configuraciones malladas
Sencillo de configurar y administrar, se puede revisar la topología de cualquier equipo dentro del segmento.	Laborioso de configurar, la revisión de los roles y estados de puerto debe hacerse equipo a equipo
Flexibilidad y facilidad para la configuración de puerto bloqueado	Bloqueo de puerto en base a costo
Protocolo propietario de Huawei no configurable con otras marcas.	Protocolo estándar
Fácil determinación y configuración del tiempo de preemptive	
Puede combinarse con otras tecnologías Spannig-tree en anillos vecinos	Puede combinarse con otras tecnologías Spannig-tree en anillos vecinos
Convergencia entorno a 50ms	Convergencia depende de la configuración

Tabla 4-7 Comparativa SEP MSTP

Objetivos:

- Lograr tiempos de convergencia con MSTP o SEP por debajo de los 200ms, tiempo de convergencia exigido por los requerimientos del proyecto.
- Determinar entre SEP y MSTP cual es el protocolo que se implementará en la propuesta de configuración, siendo elegido el que presente menores tiempos de convergencia.

4.2.1 Procedimiento

Se utilizará una topología como la que se muestra en la figura 4-8, que es el tipo de anillo más pequeño que se tendrá en la red, con 2 switches de agregación y 4 de acceso

Configuración previa en todos los switches:

- VLAN e IP de Gestión
- Acceso Telnet
- 10 VLANs correspondientes a los subsistemas
- Se configuran 2 Interfaces GE como troncales e Interfaces FE como accesos, a las interfaces troncales se les indica que puedan pasar las 10 VLANs .

4.2.2 Pruebas

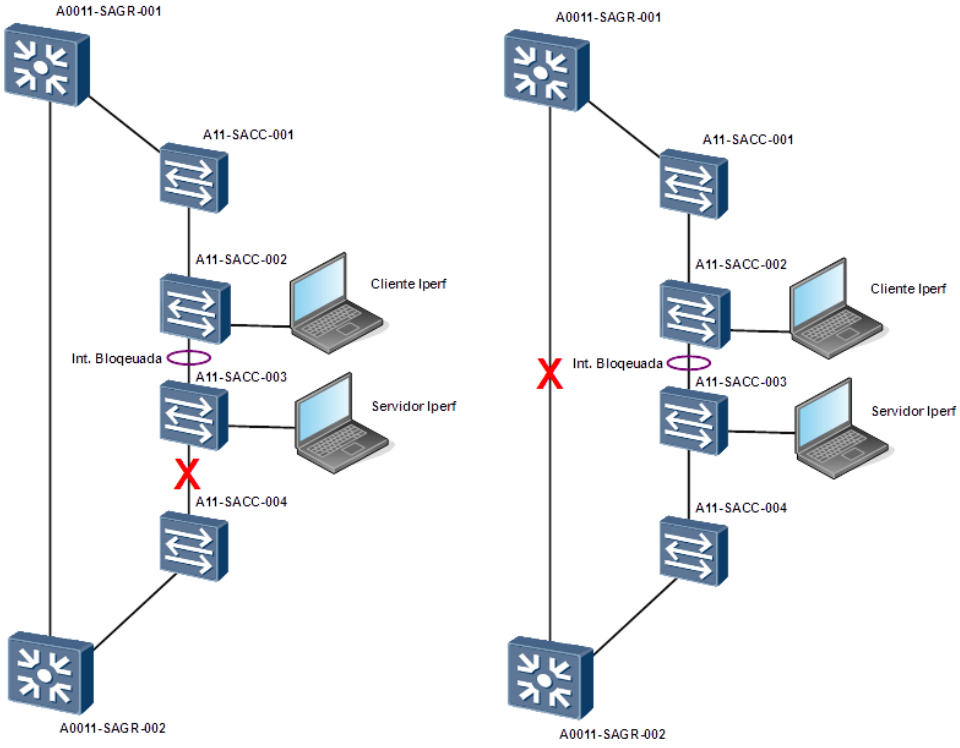


Figura 4-8 Topología pruebas capa de acceso

Se realizarán 2 pruebas, simulando la caída de un enlace pasando la interfaz a apagado (shutdown). El puerto bloqueado o discarding para ambas topologías será el que conecta A11-SACC-002 y A11-SACC-003 que son los switches donde se conectaran los equipos terminales.

i. Se simulará el corte en la interfaz que une los switches A11-SACC-003 y A11-SACC-004, como A11-SACC-003 es quien tiene una de sus interfaces en discarding o bloqueo el cambio de topología debiese producirse de manera casi instantánea lo que nos entregará el mejor rendimiento del protocolo para realizar la comparación.

ii. Se simulará el corte en la interfaz que une los switches A0011-SAGR-001 y A0011-SAGR-001, que físicamente será el enlace más largo de la topología y por lo mismo el que cuenta con la mayor probabilidad de falla ante un desastre.

Según el análisis de resultados del Test de la herramienta se utilizará un tamaño de trama de 1280 bytes con un ancho de banda cercano a 95Mbps para realizar las pruebas.

4.2.2.1 **Pruebas MSTP**

MSTP puede mejorar su convergencia básicamente de dos formas, disminuyendo el Timer de Hello a valores menores de 2 segundos o declarando el enlace caído antes de recibir 3 BPDU, ahora, un caso real, en este tipo de redes que tienen un gran ancho de banda disponibles y que es virtualmente imposible que existe congestión o un exceso de trabajo de las CPUs, la falla más común en el caso de la topología a evaluar es el corte o falla del enlace, con lo que la interfaz Root pasa inmediatamente a discarding, haciendo que el algoritmo vuelva a calcularse sin espera.

Configuración MSTP en todos los switches:

- Se activa el modo Spanning tree MSTP fast.
- Se configura la región con las instancias 1 y 2
- Se asignan las 5 VLANs por instancia.
- Se activa MSTP en todas las interfaces troncales que son parte del anillo.

Configuración MSTP en los Root Bridge:

- Se asigna el Switch de A0011-SAGR-001 como Root Bridge de la instancia 1 y A0011-SAGR-002 de la instancia 2.

Configuración MSTP en el equipo con puerto discarding:

En el switch A11-SACC-003 Se le asigna un costo de 20.000 para ambas instancias a la interfaz que lo conecta con el switch A11-SACC-003 para que el puerto quede en Discarding.

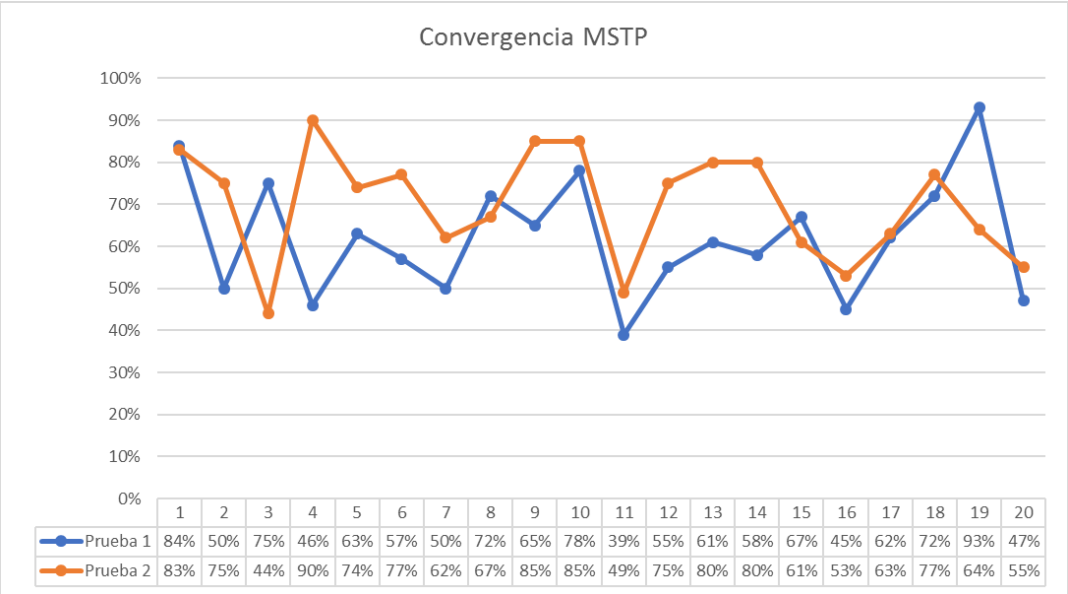


Figura 4-9 Grafico pruebas de convergencia MSTP

	Prueba 1	**Prueba 2**
Máximo	93%	90%
Mínimo	39%	44%
Promedio	62%	70%
Mediana	62%	75%
Desv. Estandar	14,11%	13,08%

Tabla 4-8 Resultados pruebas de convergencia MSTP

Observaciones de resultados:

- El tiempo mínimo aproximado de convergencia alcanzado por el protocolo está en el entorno de los 400ms (39%), lo que ya no satisface las necesidades planteadas en los objetivos.
- No existe diferencia relevante en la convergencia entre ambas pruebas, aunque el equipo que debe cambiar estado de los puertos A11-SACC-003 tenga conexión directa al punto de falla.

4.2.2.2 **Pruebas SEP**

Configuración SEP en todos los switches

- Se crean 2 segmentos, segmento SEP 11 y segmento SEP 12, control VLAN 11 para ambos segmentos.

- Se configuran las instancias instancias 1 y 2 utilizando spannig tree.
- Se asignan las 5 VLANs por instancia.
- Se asigna la instancia 1 al segmento SEP 11 y la instancia 2 al segmento SEP 12.
- Se desactiva STP en las interfaces troncales que serán parte del anillo y se les asignan los segmentos SEP 11 y 12.

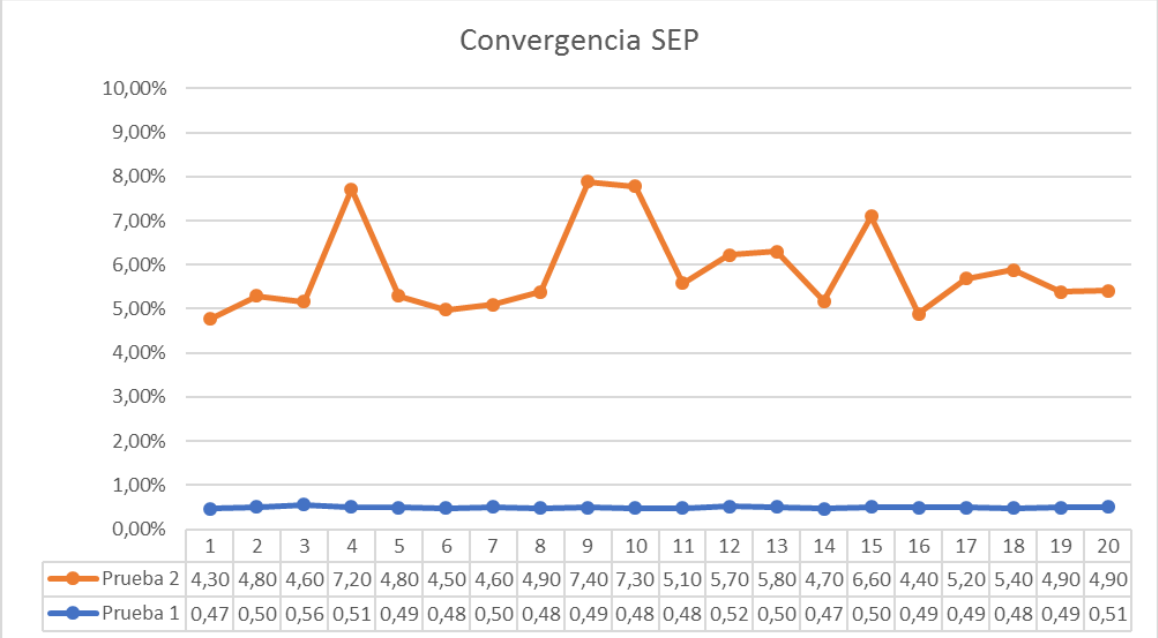
Configuración SEP en los Primary Edge port

- Se asigna en el Switch A0011-SAGR-001 la interfaz que conecta con el switch A11-SACC-001 como Primary Edge port del segmento 11 y la interfaz que conecta con el switch A0011-SAGR-002 como Sencondary Edge port del segmento 12.
- Se indica en el Switch A0011-SAGR-001 que el modo de bloqueo de interfaz del segmento 11 será por prioridad.
- Se asigna en el Switch A0011-SAGR-002 la interfaz que conecta con el switch A11-SACC-004 como Primary Edge port del segmento 12 y la interfaz que conecta con el switch A0011-SAGR-001 como Secondary Edge port del segmento 11.
- Se indica en el Switch A0011-SAGR-002 que el modo de bloqueo de interfaz del segmento 12 será por prioridad.

Configuración SEP en el equipo con puerto bloqueado:

1. En el switch A11-SACC-003 se asigna una prioridad de 100 en ambas instancias en la interfaz que lo conecta con A11-SACC-002 para que sea la interfaz bloqueada.

Resultados:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prueba 2	4,30	4,80	4,60	7,20	4,80	4,50	4,60	4,90	7,40	7,30	5,10	5,70	5,80	4,70	6,60	4,40	5,20	5,40	4,90	4,90
Prueba 1	0,47	0,50	0,56	0,51	0,49	0,48	0,50	0,48	0,49	0,48	0,48	0,52	0,50	0,47	0,50	0,49	0,49	0,48	0,49	0,51

Figura 4-10 Grafico pruebas de convergencia SEP

	Prueba 1	Prueba 2
Máximo	0,56%	7,40%
Mínimo	0,47%	4,30%
Promedio	0,49%	5,36%
Mediana	0,49%	4,90%
Desv. Estándar	0,02%	1,00%

Tabla 4-9 Resultados pruebas de convergencia SEP

Observaciones de resultados:

- En la prueba 1 se observa que la conexión directa del switch A11-SACC-003 que envía la notificación de cambio de topología provoca una convergencia que logra obtener una pérdida de paquetes menor al 1%, obteniendo el tiempo mínimo reportable por Iperf según el Test de la herramienta por debajo de los 10ms.

- En la prueba 2 se observa que los tiempos de convergencia aumentan con respecto a la prueba uno y están en el entorno de los 50ms (5%) como se indica en la descripción del protocolo.

4.2.2.3 **Pruebas SEP aumentando equipos**

Como se observó en la prueba SEP anterior, al existir una distancia mayor a un salto entre el switch que tiene su interfaz bloqueada y el switch donde se produce la falla produce una diferencia importante en el tiempo de convergencia, por lo cual se aumentará el tamaño de la topología a fin de comprobar si al aumentar el número de saltos existe un cambio relevante en el tiempo de convergencia.

Las configuraciones serán prácticamente iguales que en el caso de las pruebas MSTP, la diferencia estará que los switches donde se conectarán los equipos serán los switches A11-SACC-004 y A11-SACC-005 según la topología indicada en la figura 4-12 y es en la interfaz que une ambos switches donde se configura la interfaz bloqueada. Además, se deben realizar las configuraciones previas y las configuraciones indicadas en las pruebas SEP del punto 4.2.2.2 en todos los switches.

Resultados:

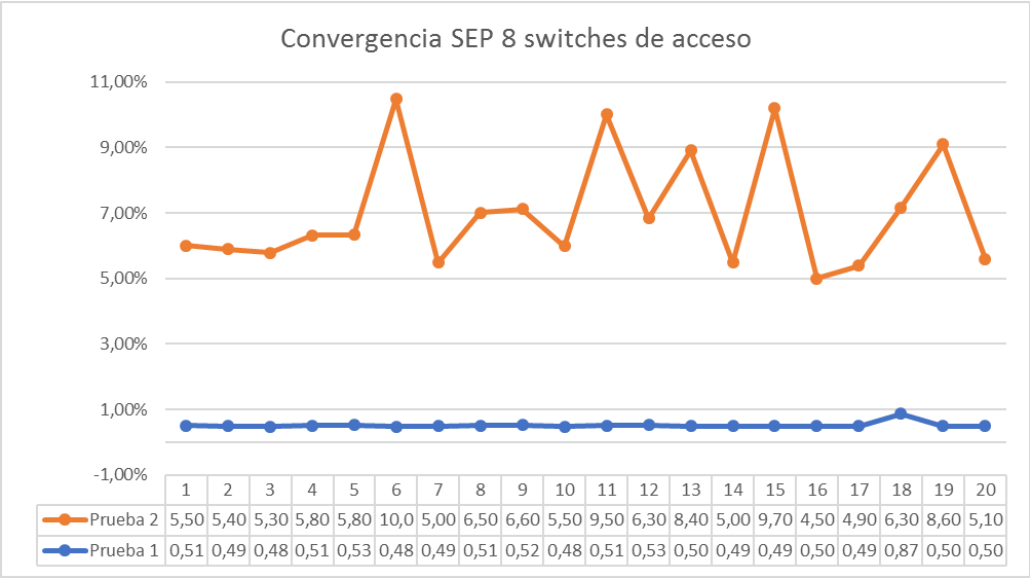


Figura 4-11 Grafico pruebas de convergencia SEP con aumento de switches

	Prueba 1	**Prueba 2**
Máximo	0,87%	10,00%
Mínimo	0,48%	4,50%
Promedio	0,52%	6,49%
Mediana	0,50%	5,80%
Desv. Estándar	0,08%	1,75%

Tabla 4-10 Resultados pruebas de convergencia SEP con aumento de switches

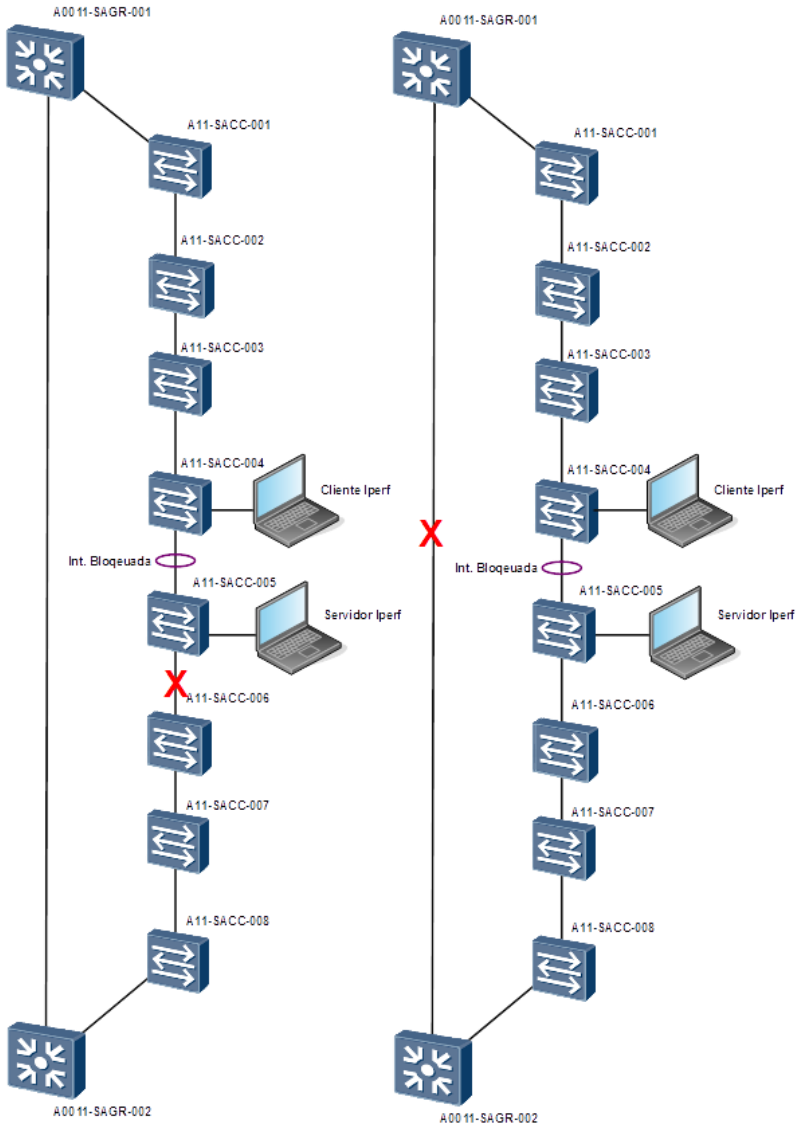


Figura 4-12 Topología pruebas SEP con aumento de switches

Observaciones de resultados:

- Los tiempos de convergencia se ven levemente aumentados, pero están dentro del error establecido en el Test de la herramienta, por lo que no se puede concluir que exista un aumento en los tiempos, pero sí que el orden de magnitud del cambio es menor.

4.2.3 Análisis de Resultados

- Tal como se indica en los antecedentes previos SEP proporciona tiempos de convergencia entorno a los 50ms.

- Luego de revisar el comportamiento de ambos protocolos, SEP muestra ser la mejor alternativa desde el punto de vista del tiempo de convergencia, lo que sumado a su facilidad de configuración y administración será el protocolo que se propondrá a utilizar en la configuración de la Red.

- Como se pudo observar en las pruebas SEP si en el mismo switch que se tiene configurada la interfaz bloqueada es el que debe notificar la falla, la convergencia se produce en menos de 10ms. Por lo que una buena medida sería bloquear la interfaz para un segmento SEP en el switch que tenga el enlace más largo del anillo y por lo tanto con mayor riesgo de corte

4.3 Capa de Agregación

4.3.1 VRRP

Como se indicó en el capítulo 2 el tiempo de convergencia de VRRP viene dado por la formula (2-4), que se dará en el caso que se pierda la conexión entre el Master y el Backup del grupo VRRP, en la red en la que se realizará la propuesta de configuración, las conexiones entre ambos equipos estarán redundadas por lo que es muy improbable que se pierda la conexión, además las comunicaciones por lo general irán en dirección a la capa de Core, lo que se traduce en que la relevancia de VRRP será determinar el mejor camino de salida del anillo de Acceso para llegar al Core.

Dada la configuración, si es que existe alguna desconexión fuera del anillo por donde fluye la comunicación entre los equipos del grupo VRRP, no existirá ningún cambio en la topología. Para solucionar este problema VRRP permite realizar un seguimiento (track) a algún parámetro externo que detone el cambio de prioridades, se puede utilizar seguimiento a rutas, interfaces físicas, sesiones BFD, monitoreo NQA (Similar a IPSLA de Cisco), etc.

Por ejemplo en la figura 4-13, la HMI está recibiendo variables desde el PLC, el Switch A0011-SAGR-001 es el Master del grupo VRRP, si cae el enlace entre A0011-SAGR-001 y A0010-SAGR-001, dentro del grupo VRRP no se produce ningún cambio ya que la conexión entre A0011-SAGR-001 y A0011-SAGR-002 sigue igual, sin embargo la comunicación el HMI y el PLC se perderá.

Objetivos:

- Determinar el tiempo de convergencia de VRRP realizando un seguimiento a una interfaz física, lo que proporcionará le mejor desempeño del protocolo.
- Determinar el tiempo de convergencia VRRP en base a una sesión BFD.
- Obtener tiempos de convergencia por debajo de los 300ms. A fin de cumplir con el requerimiento del proyecto.

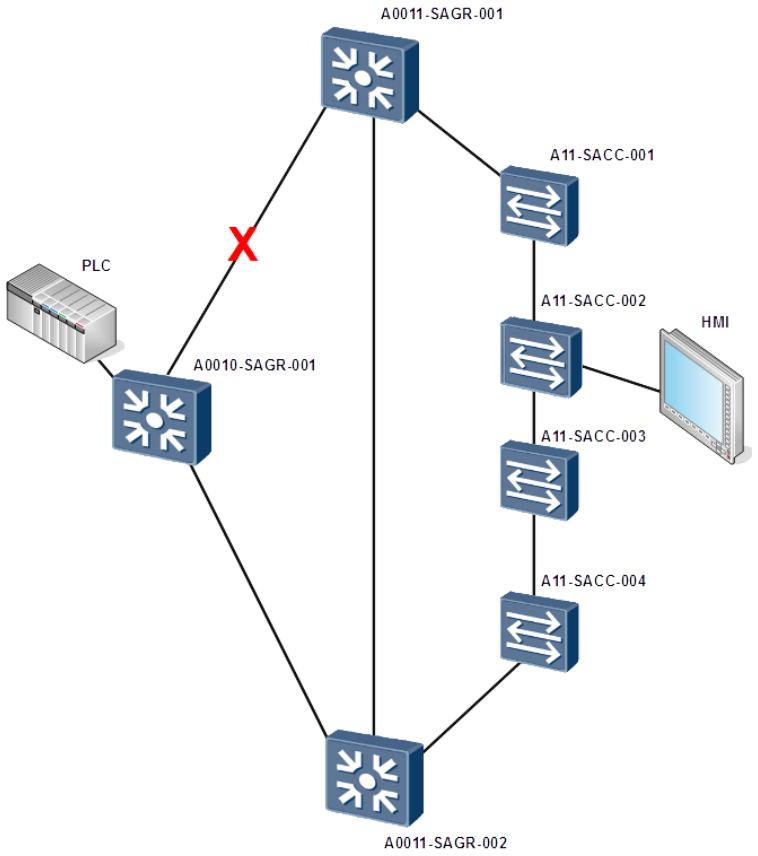


Figura 4-13 Ejemplo de desconexión que no detecta VRRP

4.3.1.1 **Procedimiento**

Se utilizará una topología como la que se muestra en la figura 4-14, que es el tipo de anillo más pequeño que se tendrá en la red, con 2 switches de agregación y 4 de acceso, el switch Master del grupo VRRP del cliente Iperf será el Switch A0011-SAGR-001.

Según lo indicado por el Test de la herramienta se utilizará un tamaño de trama de 1280 bytes con un ancho de banda cercano a 95Mbps.

4.3.1.2 **Pruebas**

Se realizarán 2 pruebas, ambas simulando la caída del enlace que A0011-SAGR-001 y A10-SACC-001.

i. El switch Master del grupo VRRP que servirá de Gateway al cliente Iperf, realizará un seguimiento (track) a la interfaz que tiene conexión con el Switch A10-SAGR-001, al detectarse la caída el Master disminuirá su prioridad quedando como Backup.

ii. El switch Master del grupo VRRP que servirá de Gateway al cliente Iperf, tendrá una sesión BFD con el switch A10-SAGR-001, al detectarse la caída de la sesión el Master disminuirá su prioridad quedando como Backup.

Configuración previa:

- Tanto en los switches de acceso como de agregación se tendrá la misma configuración descrita en el punto 4.2.2.2 de las pruebas SEP.

Configuración en los Switches común para pruebas 1 y 2.

- En los switches A0011-SAGR-001 y A0011-SAGR-002 se configuran 10 grupos VRRP, 11-20, para las subredes de las 10 VLANs y los enlaces capa 3 con rutas estáticas hacia el switch A0010-SAGR-001.
- En el switch de agregación A0011-SAGR-001 se configura como Master para las subredes de las 5 primeras VLAN, se le asigna una prioridad de 120 (100 por defecto).
- En el switch de agregación A0011-SAGR-002 se configura como Master para las subredes de las 5 VLANs restantes, se le asigna una prioridad de 120 (100 por defecto).
- En el Switch A0010-SAGR-001 se configura las rutas estáticas hacia A0011-SAGR-001 y A0011-SAGR-002 y se habilita un puerto de acceso para conectar el servidor Iperf.

Configuración particular en los Switches prueba 1

- En el A0011-SAGR-001 se configura un track a una interfaz que disminuya en 40 la prioridad del Master del grupo 11 en caso de detectarse la caída.

Configuración particular en los Switches prueba 2

- En los switches A0011-SAGR-001 y A0010-SAGR-001 se configura una sesión BFD con las direcciones IPs de la conexión en capa 3 entre ambos switches, el intervalo de envío y recepción será de 50ms igual para ambos extremos, y el detector "Detect Multiplier" se configurará con un valor de 3.
- A0011-SAGR-001 se configurará en el grupo VRRP 11 un track a la sesión BFD que disminuya en 40 la prioridad del Master del grupo 11 en caso de detectarse la caída de la sesión.

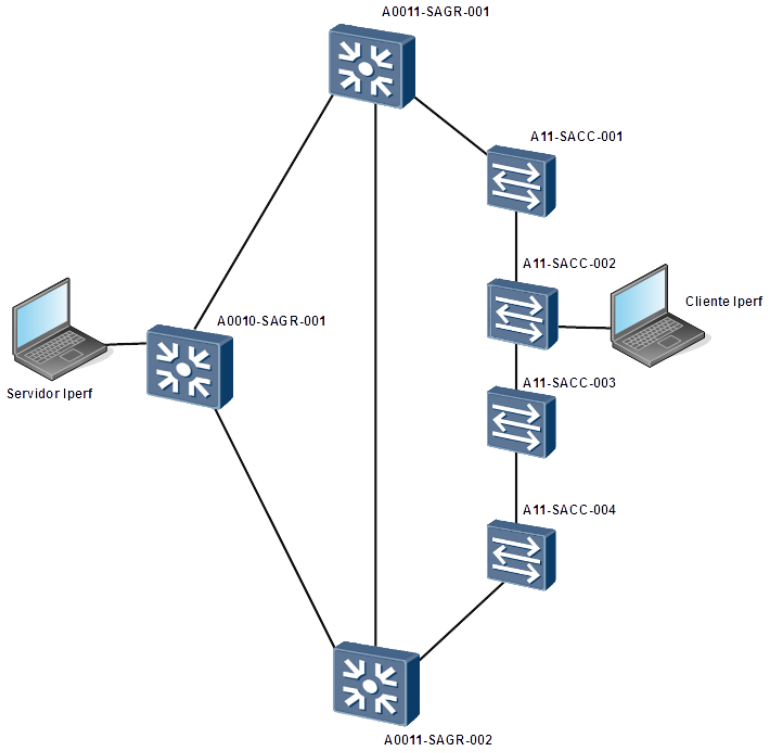
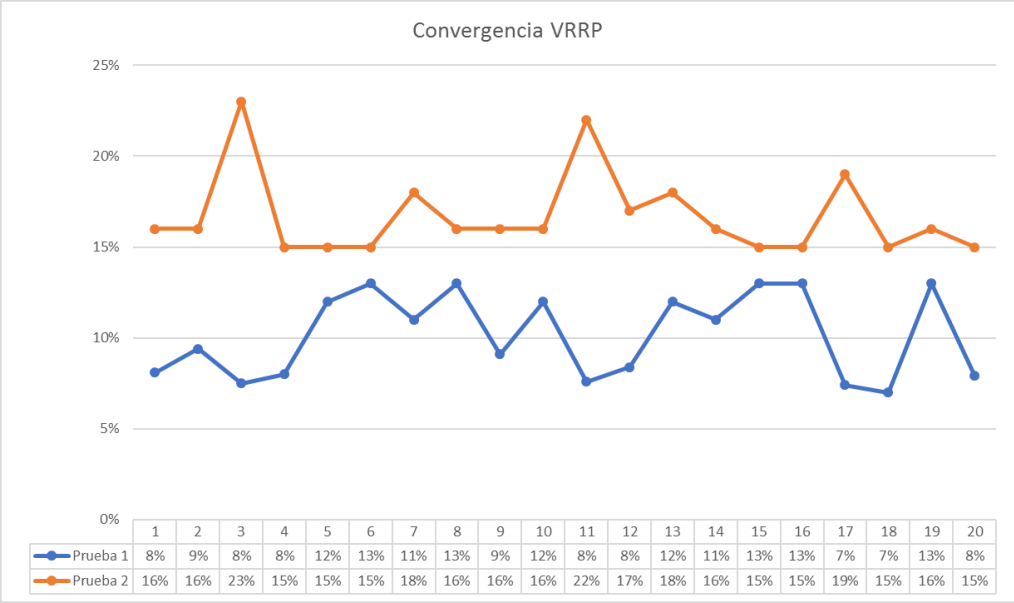


Figura 4-14 Topología de pruebas VRRP

Resultados:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prueba 1	8%	9%	8%	8%	12%	13%	11%	13%	9%	12%	8%	8%	12%	11%	13%	13%	7%	7%	13%	8%
Prueba 2	16%	16%	23%	15%	15%	15%	18%	16%	16%	16%	22%	17%	18%	16%	15%	15%	19%	15%	16%	15%

Figura 4-15 Grafico de resultados de pruebas de convergencia VRRP

	Prueba 1	Prueba 2
Máximo	23,0%	13,0%
Mínimo	15,0%	7,0%
Promedio	16,7%	10,2%
Mediana	16,0%	10,2%
Desv. Estandar	2,3%	2,3%

Tabla 4-11 Resultados pruebas VRRP

4.3.1.3 **Análisis de resultados**

- Como es lógico, la respuesta de convergencia ante la desconexión física obtiene un mejor rendimiento que la sesión BFD, la intención del seguimiento a la interfaz fue solo revisar el mejor rendimiento posible ya que en la realidad una implementación de este tipo podría causar flapping en los grupos VRRP.

- La convergencia a la sesión BFD arrojo resultados con un tiempo máximo de convergencia en el entorno de los 230ms y la mediana de las pruebas fue de 16%, lo que implica que VRRP con BFD ofrece una convergencia en el entorno de los 160ms.

- La configuración cumple con el requerimiento de convergencia a nivel de Gateway por debajo de los 300ms.

4.3.2 Protocolos de enrutamiento BGP y OSPF

Se realizarán pruebas con los protocolos BGP y OSPF, el escenario común de pruebas se muestra en la figura 4-16, Como se mostró en el capítulo 3 la topología a implementar presenta 8 anillos con 16 switches en su capa de agregación, debido al problema que trae manejar tantos equipos para la realización de las pruebas se montara una topología representativa.

4.3.2.1 **Procedimiento**

Se montara la topología con 4 anillos y un total de 10 switches esto en base a que el sentido del tráfico será principalmente ascendente hacia la capa de Core, el número de saltos máximo que debiese viajar el tráfico es de 4, ya que siempre tendrá 2 caminos disponibles hacia el Core, además las pruebas se hacen simulando que la capa de Core ha perdido su conexión de Cluster a fin de lograr almenos 4 saltos en el tráfico y que la convergencia no se dé por dicho camino.

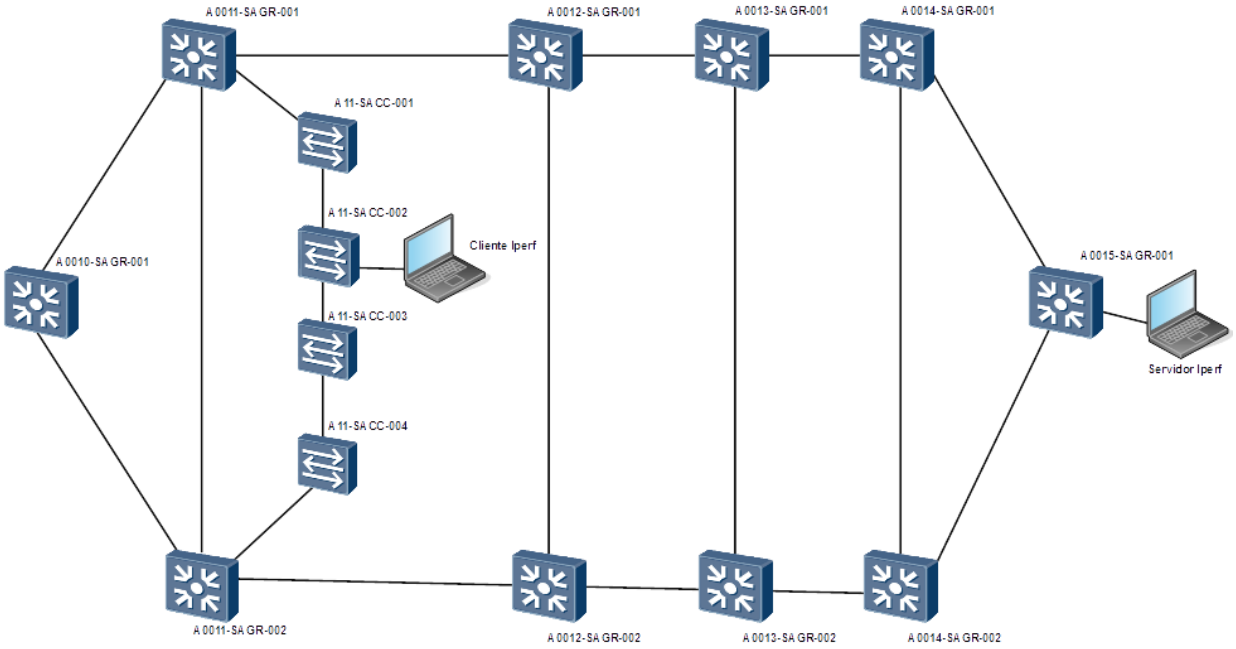


Figura 4-16 Topología pruebas protocolos de enrutamiento

Las conexiones entre los switches de agregación se harán en las interfaces GE mediante fibra óptica monomodo y no en las interfaces de 10GE que serán las que finalmente se implementaran para esta capa, esto debido a la falta de atenuadores y a que no afecta en la medida dado que la pruebas se realizan sin carga de tráfico.

Tanto las pruebas a realizar en OSPF como en BGP tendrán las siguientes configuraciones comunes:

- Los switches de Agregación A0011-SAGR-001 y A0011-SAGR-002 heredan las configuraciones indicadas en las pruebas de VRRP, con la salvedad de que se eliminan los tracks.
- En todos los switches restantes de la topología a los indicados en el punto anterior se crean 10 VLANs y 10 subredes, los switches de agregación que estén en el mismo anillo tendrán las mismas subredes.
- Las interfaces que conectan los switches de agregación del mismo anillo se asignan como troncales para todas las VLAN creadas y puedan levantar las rutas. Lo mismo se realizar con los switches A0010-SAGR-001 y A0015-SAGR-001, con la diferencia que el puerto se conectará a un switch de acceso con el único objetivo de levantar las rutas.
- Se crean conexiones capa 3 mascara 30 entre todos los switches vecinos que no pertenezcan al mismo anillo para levantar las adyacencias.

4.3.2.2 **OSPF**

Si bien el protocolo sugerido por parte del cliente es BGP, se realizará una configuración práctica para ver los tiempos de convergencia que ofrece el protocolo OSPF y si en este

aspecto es una mejor alternativa que la propuesta de BGP, dentro de su funcionamiento OSPF es un protocolo basado en el estado de los enlaces por lo que debiese presentar una mejor funcionalidad respecto a la convergencia.

Como se muestra en la figura 4-17 cada anillo se configurará con un área distinta y todos los switches de agregación se conectarán al área de backbone, por lo tanto, todos estos switches funcionarán como ABRs, esta configuración se realiza para evitar el flujo de LSAs y poder implementar sumarización en la entrega de rutas.

Las conexiones entre los switches de agregación fuera del área/anillo 11 se realizan para poder levantar las rutas y se llenen las tablas de enrutamiento, por lo que en los switches de las áreas 10 y 15 se activará un puerto trunk y se conectará a cualquier puerto de red para que reciba energía y levante las rutas.

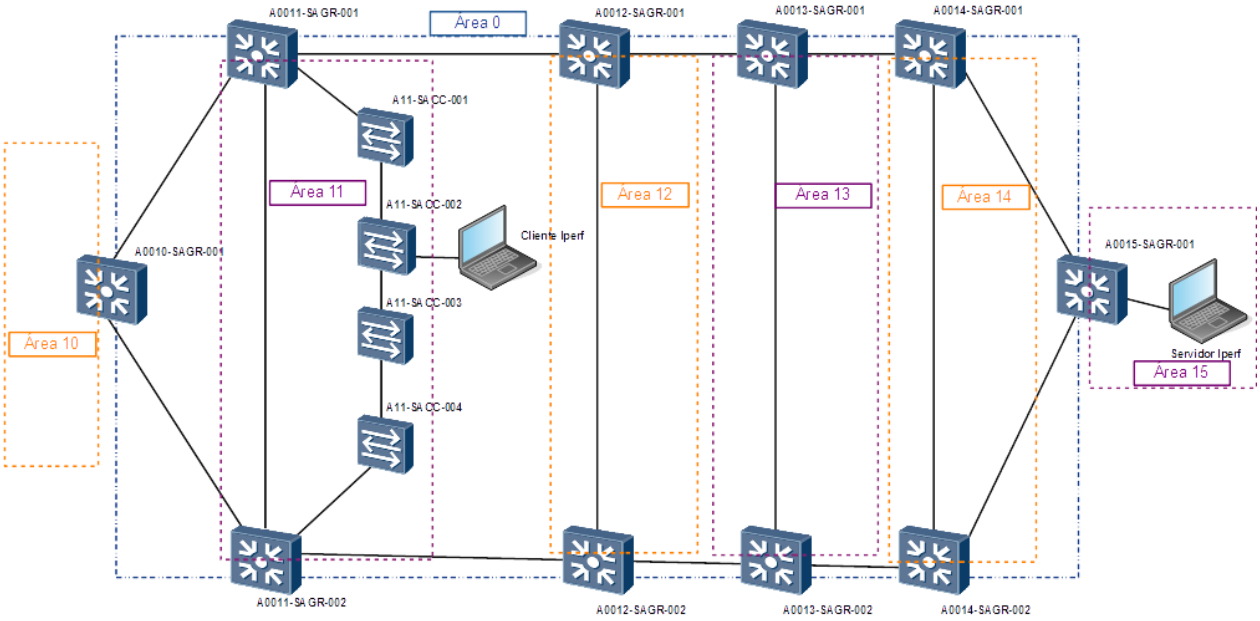


Figura 4-17 Distribución de áreas pruebas OSPF

4.3.2.2.1 Pruebas de convergencia

Objetivos:

- Determinar tiempos de convergencia de OSPF sin modificaciones de implementación y que permitan compararlos con los de BGP.
- Determinar tiempos de convergencia de IP FRR LFA y que permitan compararlos con los de BGP.
- Obtener tiempos de convergencia por debajo de 500ms a nivel de enrutamiento a fin de cumplir los requerimientos del proyecto.

Si bien en OSPF la convergencia se produce luego que el enlace se declara como caído ante la no recepción de 3 hellos, en el caso de fallas físicas los LSAs se generan de manera casi automática para que los switches de la topología vuelvan a calcular el SPT.

Configuraciones para pruebas

i. En todos los switches de agregación se activa el área 0 y se declaran las rutas de sus vecinos con el wildcard 0.0.0.3.
ii. En todos los switches de agregación se crea el área correspondiente según el anillo al que pertenezcan como se muestra en la figura 4-17.
iii. Se declaran todas las rutas internas del anillo, si bien podrían importarse debido a que las subredes ya están creadas dentro de los switches, en el proceso de configuraciones previas, estas se importan al área 0 no permitiendo realizar la sumarización.
iv. Las conexiones internas en las áreas distintas al área de backbone se configuran con un costo de 100 a fin de no tener que configurar listas de acceso para evitar que tráfico del área 0 pueda ingresar al anillo.

Se realizarán 2 pruebas, ambas simulando la caída del enlace que A0013-SAGR-001 y A0014-SAGR-001, esto con el fin que el switch no tenga conexión física directa con la falla.

Se conectará el cliente y servidor Iperf como se muestra en la figura 4-17, como no se asignan costos a los enlaces y el Master del grupo VRRP de la subred del cliente Iperf es A0011-SAGR-001, el tráfico fluirá por la parte superior de la topología ya que es el camino con menor costo para llegar a A0015-SAGR-001. Un error que podría aparecer en las pruebas es que A0013-SAGR-001 redirija el tráfico por su conexión interna, lo que no pasara por los costos indicados en la configuración para OSPF.

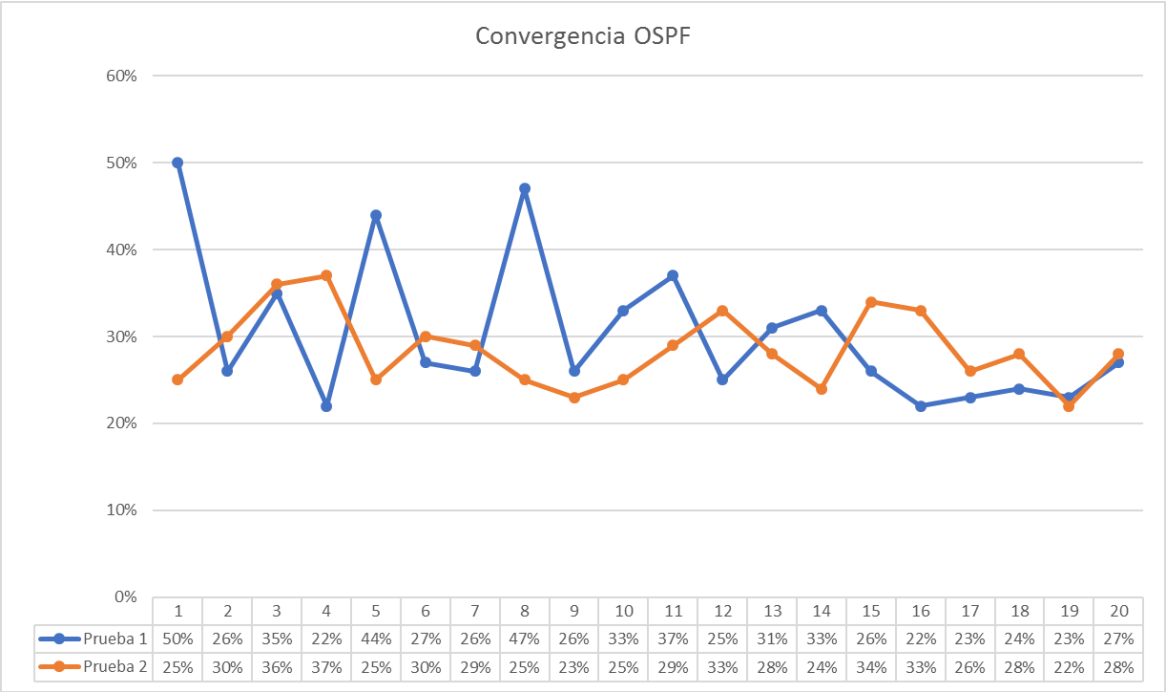
i. Prueba 1 se realizará con la configuración estándar de OSPF, no se realizan modificaciones en los parámetros de hello o de holdtime, ya que como se indicó la falla será física.

ii. La Prueba 2 se configurar IP FRR LFA, en el switch simplemente se activa su uso para que la funcionalidad compute la mejor ruta, debido a la baja carga de trabajo que tendrán los switches y que el número de rutas de las pruebas estará en el entorno de las 100, el algoritmo SPF no debiese tener demoras mayores en el cálculo.

Resultados:

	Prueba 1	**Prueba 2**
Máximo	50,0%	37,0%
Mínimo	22,0%	22,0%
Promedio	30,4%	28,5%
Mediana	26,5%	28,0%
Desv. Estandar	8,4%	4,3%

Tabla 4-12 Resultados pruebas de convergencia OSPF



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prueba 1	50%	26%	35%	22%	44%	27%	26%	47%	26%	33%	37%	25%	31%	33%	26%	22%	23%	24%	23%	27%
Prueba 2	25%	30%	36%	37%	25%	30%	29%	25%	23%	25%	29%	33%	28%	24%	34%	33%	26%	28%	22%	28%

Figura 4-18 Grafico de resultados de pruebas de convergencia

Observaciones de resultados pruebas de convergencia:

- Los tiempos de convergencia de OSPF reportan excelentes resultados, solo en una de las pruebas se llegó al valor máximo indicado en los objetivos de 500ms, pero la mediana de las pruebas de 26, 5% lo que significa un valor aproximado de 270ms está muy por debajo de lo planteado en los objetivos.
- La inclusión del protocolo IP FRR LFA como era de esperarse no tiene mayor relevancia debido a que el algoritmo SPF no tiene una exigencia mayor, pero de todas formas reporta una menor variación en los resultados

4.3.2.2.2 Pruebas de latencia

Objetivos:

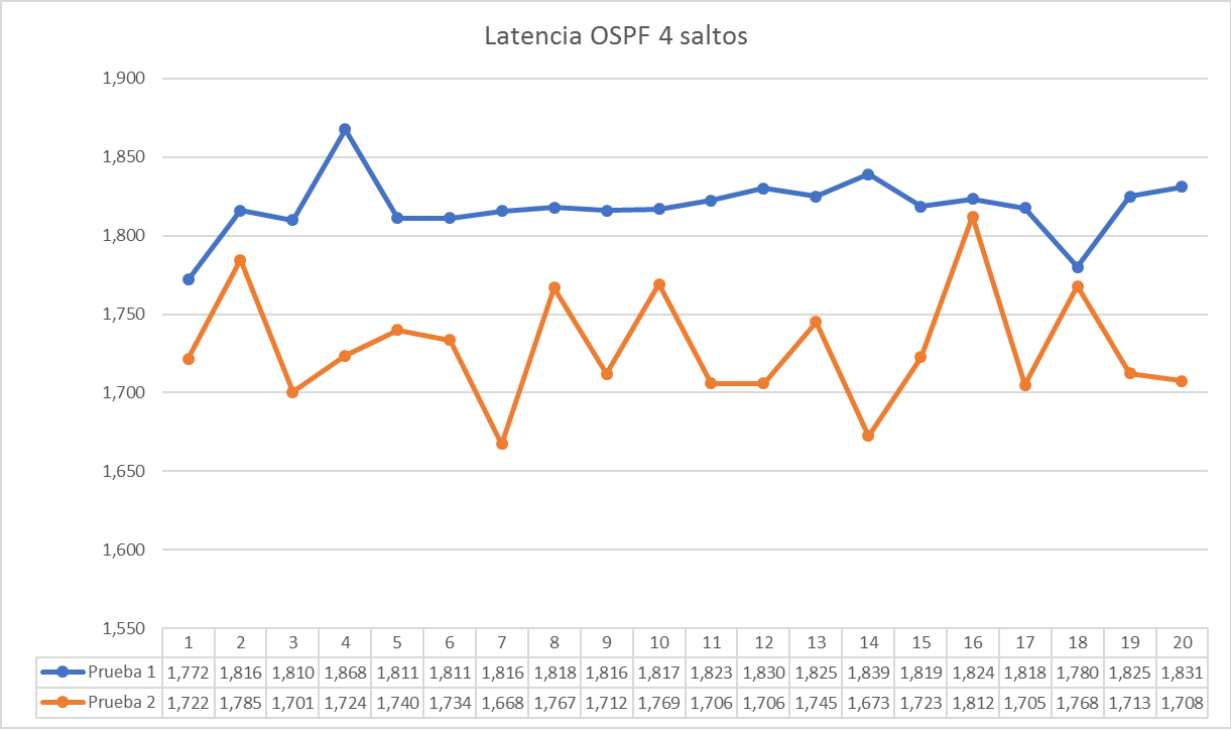
- Determinar la latencia que presentan las comunicaciones a 4 saltos de enrutamiento de distancia con la configuración de OSPF sin modificaciones.
- Determinar la latencia que presentan las comunicaciones a 4 saltos de enrutamiento de distancia con la configuración de OSPF sumarizando las rutas.
- Comparar las latencias que se producen en ambas configuraciones y si se produce alguna diferencia relevante con la sumarización

Las pruebas de latencia se realizarán ocupando la aproximación del RTT/2, si bien está aproximación produce un error debido a que el valor se ve incrementado por el procesamiento de los equipos es una técnica ampliamente usada y se considera suficiente.

Las pruebas se realizarán con el software HRping, la única razón para ocupar el software y no ocupar el comando normal presente en Windows es que la herramienta reporta una resolución de microsegundos.

Ocupando la configuración antes señalada se realizan 2 pruebas, ambas enviando paquetes de 1280 bytes con un intervalo de 500ms, cada prueba tendrá una duración de 100 segundo y se enviaran 200 paquetes.

i. Prueba 1: Se probará la latencia con exactamente la misma configuración indicada en las pruebas de convergencia y con la misma ubicación de los laptops.
ii. Prueba 2: Se sumarizaran las rutas para ver si se produce alguna disminución en la latencia, si bien la cantidad de rutas presentes en los equipos (alrededor de 100) no representa un número elevado para el switch, la intención es comprobar la premisa. La sumarización se realizan los ABRs al publicar sus rutas, basta con activar la configuración en cada ABR de la topología. Las sumarización se hace cambiando la máscara /20 por un mascara /14.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prueba 1	1,772	1,816	1,810	1,868	1,811	1,811	1,816	1,818	1,816	1,817	1,823	1,830	1,825	1,839	1,819	1,824	1,818	1,780	1,825	1,831
Prueba 2	1,722	1,785	1,701	1,724	1,740	1,734	1,668	1,767	1,712	1,769	1,706	1,706	1,745	1,673	1,723	1,812	1,705	1,768	1,713	1,708

Figura 4-19 Grafico de resultados de pruebas de latencia OSPF

	Prueba 1	Prueba 2
Máximo (ms)	1,868	1,812
Mínimo (ms)	1,772	1,668
Promedio (ms)	1,818	1,729
Mediana (ms)	1,818	1,722
Desv. Estandar	0,019	0,037

Tabla 4-13 Resultados de pruebas de latencia OSPF

4.3.2.3 **BGP**

Como se indicó en el capítulo 3 la intención primaria es ocupar BGP como protocolo de enrutamiento, por las ventajas que tiene desde el punto de vista de la administración, pero con respecto a la convergencia no destaca por su velocidad, BGP declara un vecino caído luego de la no recepción de 3 keepAlives o por alguna actualización, con respecto a la red sobre la que se realizará una propuesta de configuración presenta una desventaja con respecto a OSPF debido a que tiene algunos problemas prácticos en las configuraciones.

Si observamos la figura 3-1 donde se plantea la configuración física de la red a que se propondrá la configuración y tomamos en cuenta la asignación de switches indicada en la figura 4-20, en caso de que algún equipo necesite comunicación desde el anillo 12 AS 65112 al 14 AS 65114 y por la dinámica de la red el tráfico esté fluyendo por la parte superior de la topología, el tráfico abandona el anillo por el switch A0012-SAGR-001 pasa por el switch A0013-SAGR-001 para finalmente llegar A0014-SAGR-001 e ingresar al anillo, en caso de que ocurra una falla en el enlace que une A0013-SAGR-001 y A0014-SAGR-001 y quiebre la adyacencia EBGP, se generara un Update que dará la ruta como caída, por lo tanto el switch A0012-SAGR-001 debiese redirigir el tráfico hacia A0011-SAGR-001 y luego este al Core para que lo redirija por esta capa hacia el switch A0014-SAGR-001. Ahora el enlace de Core será uno de los más largos de la topología y por lo mismo las pruebas OSPF se ha realizado sin este enlace, en caso de un desastre y perder la conexión entre Cores existe la alternativa que el Core, ya sin la configuración de Cluster, redirigiera el tráfico hacia A0011-SAGR-002 para ingresar por la parte inferior hacia el anillo 14 lo que no ocurrirá debido a que A0011-SAGR-002 no podría recibir prefijos que publique A0014-SAGR-001, ya que estos tendrían que pasar previamente por A0014-SAGR-002 que al ver que las prefijos publicados vienen de su mismo AS aplicaría el mecanismo anti-loop y no reenviaría el prefijo. Si bien es un escenario donde tiene que darse la desconexión de 2 enlaces y que el flujo del tráfico comúnmente no se dará entre anillos sino en dirección al Core, se debe tener en cuenta. Las alternativas para mejorar este aspecto sería configurar un solo sistema autónomo y dentro de este un Full Mesh u ocupar los Cores como Route reflector, además de configurar algún IGP que haga converger la red, lo que complejiza la configuración y quita la principal ventaja de BGP que es su facilidad de administración.

4.3.2.3.1 Pruebas de convergencia

Objetivos:

- Determinar el tiempo de convergencia de BGP ocupando VRRP como protocolo auxiliar
- Determinar el tiempo de convergencia VRRP/BGP y poder compáralo con los de OSPF en base a una sesión BFD.

Por la razón descrita en el párrafo anterior las pruebas de BGP para el escenario planteado se realizarán trabajando este en conjunto con VRRP, al detectar la falla VRRP se encargará de hacer salir el tráfico del anillo por una ruta alternativa y BGP de redirigirlo.

Configuraciones para pruebas:

i. Se activará BGP en todos los switches de agregación con el sistema autónomo correspondiente al valor 651XX, donde XX será el número de anillo.
ii. Se importan las rutas directas que están dentro del switch configuradas en las pruebas VRRP
iii. Se configuran los peer EBGP con los switches de agregación vecinos, la IP del peer será la de los enlaces capa 3 mascará 30 previamente configurados, además se les asigna una preferencia PrefVal de 150 para evitar que el tráfico pueda ingresar a los anillos cuando no corresponda.
iv. Se crea una VLAN adicional y una interfaz virtual VLANIF correspondiente, además se agrega dicha VLAN a las permitidas por los puertos troncales de todos los switches del anillo.
v. Se configuran los Peers IBGP con las direcciones IP configuradas en el punto anterior.
vi. Se crea una sesión BFD entre el switch A0011-SAGR-002 y la IP de A0014-SAGR-001 que tiene su conexión con A0013-SAGR-001, el intervalo de envío y recepción será de 50ms igual para ambos extremos, y el detector “Detect Multiplier” se configurará con un valor de 3.

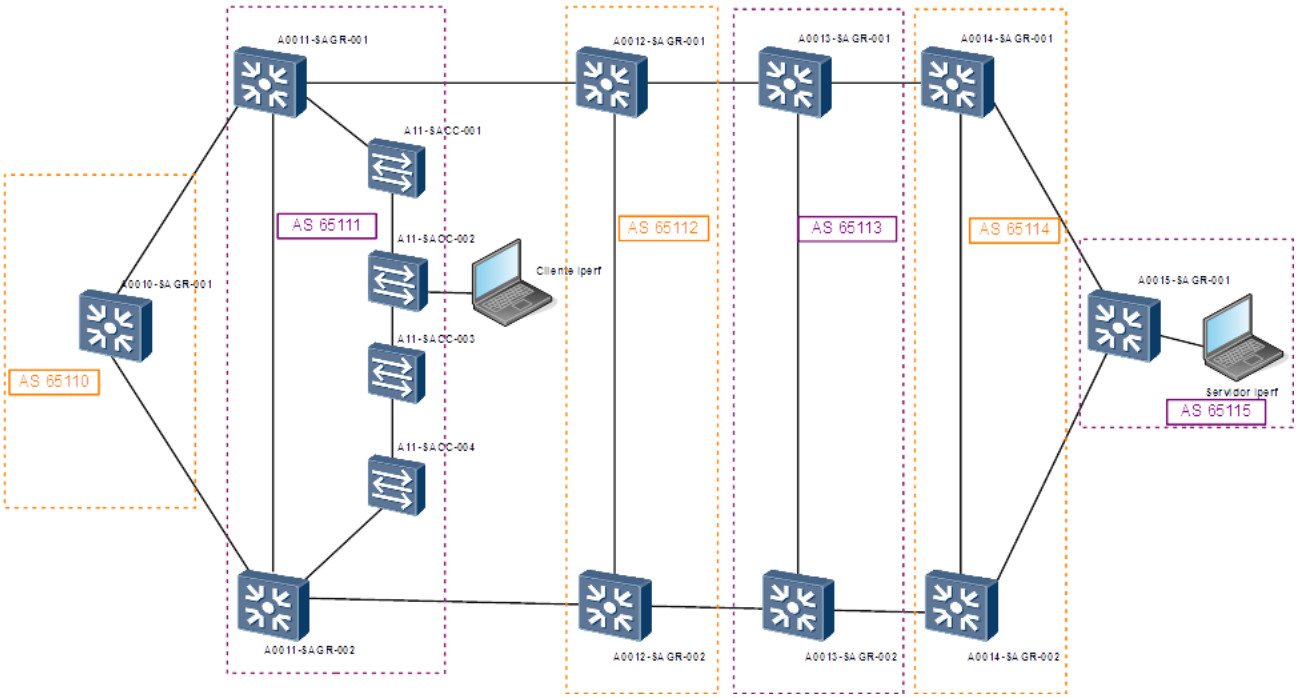


Figura 4-20 Distribución de sistemas Autónomos para pruebas de convergencia BGP.

Resultados:

	Prueba 1
Máximo	26,0%
Mínimo	15,0%
Promedio	19,2%
Mediana	18,5%
Desv. Estandar	2,9%

Figura 4-21 Resultados de convergencia VRRP + BGP

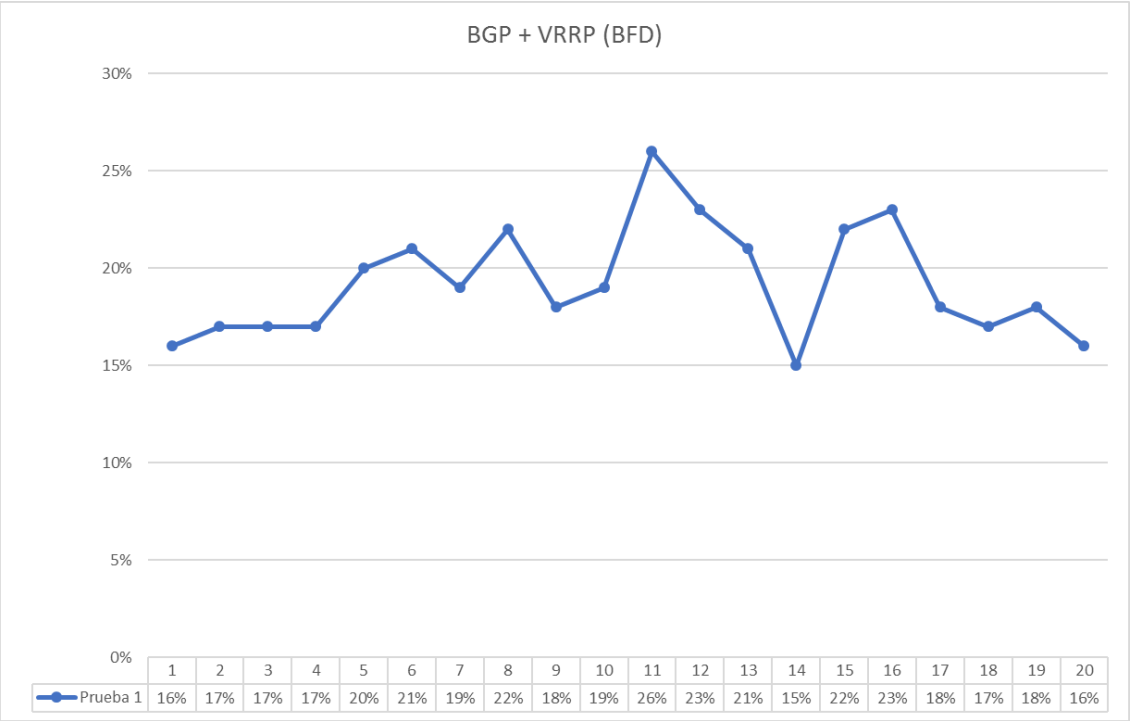


Figura 4-22 Grafico de resultados de pruebas de convergencia VRRP + BGP

Observaciones de resultados:

- Básicamente los tiempos son los correspondientes a la convergencia de VRRP alrededor de un 20% superiores a las pruebas VRRP BFD realizadas previamente
- Los tiempos de convergencia son cercanos a los 190ms.

4.3.2.3.2 Pruebas de latencia

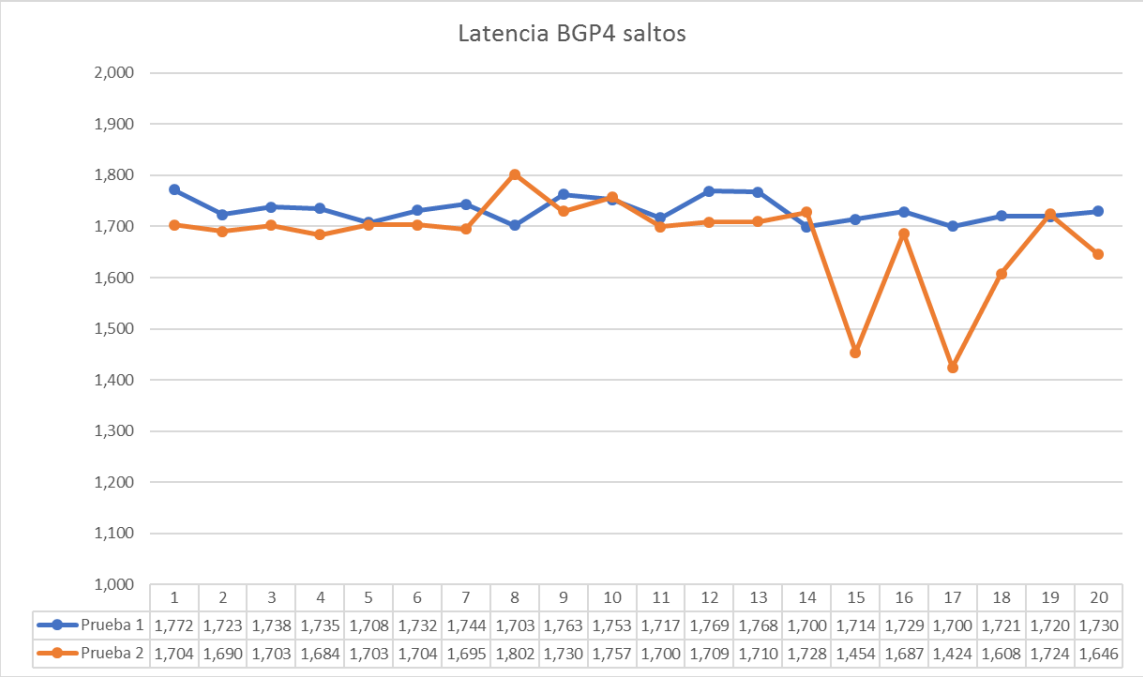
Objetivos:

- Determinar la latencia que presentan las comunicaciones a 4 saltos de enrutamiento de distancia con la configuración de BGP sin modificaciones.
- Determinar la latencia que presentan las comunicaciones a 4 saltos de enrutamiento de distancia con la configuración de BGP sumarizando las rutas.
- Comparar las latencias que se producen en ambas configuraciones y si se produce alguna diferencia relevante con la sumarización.

Se realizarán 2 pruebas ambas enviando tramas de 1280 bytes cada 500ms, cada prueba tendrá una duración de 100 segundo y se enviaran 200 paquetes.

i. Se probará la latencia con exactamente la misma configuración indicada en las pruebas de convergencia y con la misma ubicación de los las sondas.
ii. Se sumarizaran las rutas para ver si se produce alguna disminución en la latencia, si bien la cantidad de rutas presentes en los equipos (alrededor de 100) no representa un número elevado para el switch, la intención es comprobar la premisa. La sumarización se logra indicándole a las conexiones EBGP que publiquen los prefijos de manera sumarizada.

Resultados:



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prueba 1	1,772	1,723	1,738	1,735	1,708	1,732	1,744	1,703	1,763	1,753	1,717	1,769	1,768	1,700	1,714	1,729	1,700	1,721	1,720	1,730
Prueba 2	1,704	1,690	1,703	1,684	1,703	1,704	1,695	1,802	1,730	1,757	1,700	1,709	1,710	1,728	1,454	1,687	1,424	1,608	1,724	1,646

Figura 4-23 Grafico de resultados de pruebas de latencia BGP

	Prueba 1	**Prueba 2**
Máximo	1,772	1,802
Mínimo	1,700	1,424
Promedio	1,732	1,678
Mediana	1,729	1,703
Desv. Estandar	0,023	0,090

Tabla 4-14 resultados de pruebas de latencia BGP

Observaciones de resultados:

- La sumarización representa una leve mejora en el entorno de los 25 microsegundos lo se considera irrelevante

4.3.2.4 **Análisis de Resultados**

- Las pruebas de convergencia indican que la configuración VRRP + BGP tiene mejores tiempos que OSPF, pero esto es en base a lo que realiza VRRP, por lo que se concluye que OSPF presenta mejores resultados en convergencia.
- Tanto la configuración VRRP + BGP como OSPF tienen tiempos de convergencia por debajo de los del tiempo requerido por el proyecto de 500ms.
- Si bien BGP presenta menores niveles de latencia que OSPF, esta diferencia es de alrededor de 100µs por lo cual no es relevante.
- La sumarización de rutas no se traduce en una disminución relevante de la latencia, esto puede ser debido a la baja cantidad de rutas o prefijos que se sumarizan, sin embargo, la disminución de latencia si bién es baja es sostenida en todas las pruebas.

4.4 Pruebas de comunicación entre PLCs

Luego de haber obtenido los tiempos de latencia y los tiempos aproximados de convergencia se procede a realizar un ejercicio práctico para revisar los tiempos de respuesta a nivel de PLC en la red enrutada.

4.4.1 Procedimiento

Utilizando la configuración de las pruebas realizadas con el protocolo BGP en el punto 4.3.2.3.1, se conectan 2 PLCS Beckhoff modelo CX8090 a la red, como se indica en la figura 4-24 con el fin de establecer una comunicación por el protocolo EAP (descrito en 2.3.2.7.2) entre ellos.

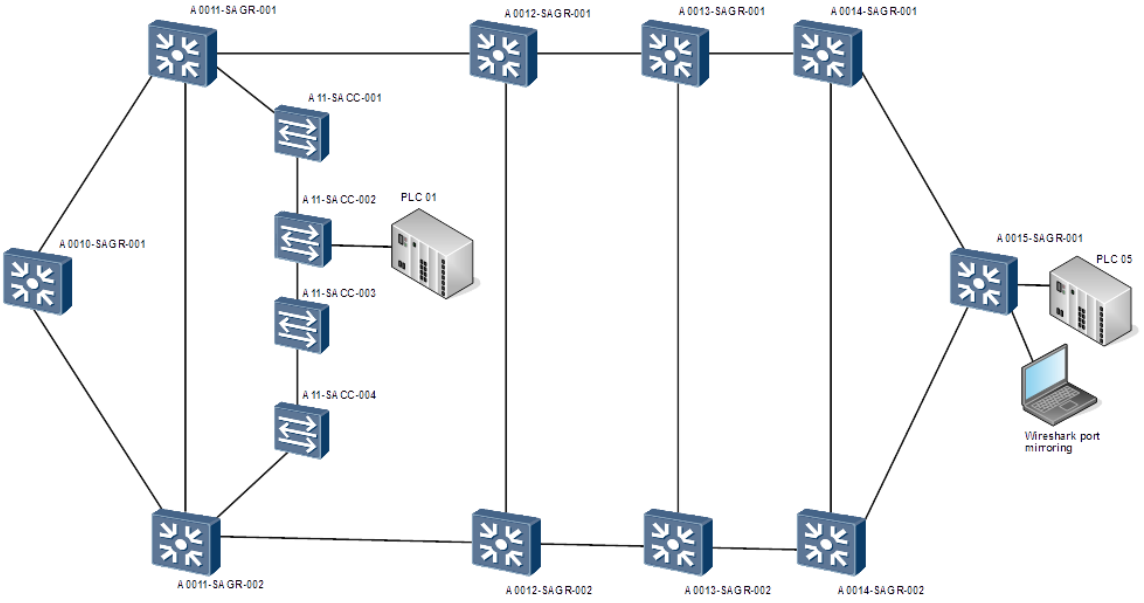


Figura 4-24 Topología para pruebas PLC con EAP

Según el manual del fabricante Beckhoff [4] de los PLCs el protocolo EAP presenta un rendimiento de 10ms en comunicaciones a nivel de capa 2 y de 100ms en comunicaciones enrutadas lo que dado los ciclos de tarea ofrecido por el PLC que se ocupara pueden ser menores a 1ms parecen tiempos tentativamente elevados.

Como se indicó en la descripción del protocolo EAP, este no se programa, sino que se configura para lo que se usara el software de configuración de Beckhoff Twincat System Manager de suite Twincat 2.

Los tiempos de Ciclo de tarea de ambos PLCs se configuran en 1ms y la velocidad de publicación se configura sin división de tiempo estableciendo el parámetro de configuración Divider/Modulo en 1, por lo tanto, la publicación de variables debiese ocurrir en cada ciclo de tarea, el PLC01 se configura en el anillo 11 con la dirección IP 10.44.176.12/20 y dirección ADS 10.44.176.12.1.1, el PLC05 en el anillo 15 con la dirección 10.60.176.14/20 y dirección ADS 10.60.176.12.1.1.

La programación de las rutinas para las pruebas se hizo con el software Twincat PLC Control de la Suite Twincat 2, donde se realizaron dos programas sencillos en ambos PLCs, en el PLC01 se genera de manera cíclica un pulso en una de sus salidas que tendrá 5 segundo de duración y luego estará 3 segundo en reposo, la salida será conectada una entrada digital del mismo PLC01. Al detectar el cambio en su entrada el PLC01 iniciará un temporizador T01, además el estado de esta entrada se estará publicando constantemente por EAP hacia el PLC05.

El PLC05 se suscribe a la variable publicada por el PLC01, al detectar el cambio de estado de la entrada en el PLC01, cambiará de estado una variable y la publicará hacia el PLC01, el PLC01 se suscribirá a la variable publicada por PLC05 y al detectar el cambio de estado de la variable iniciará un segundo temporizador T02, cabe destacar que los temporizadores entregan resolución a nivel de milisegundos. La diferencia de tiempo entre ambos temporizadores entregará el tiempo de demora de accionamiento desde que el PLC01 detecto el cambio hasta que el PLC05 actuó sobre el PLC01 por dicho cambio, el resultado se almacenará en arreglo dentro del programa.

4.4.2 Pruebas

Objetivos:

- Determinar el tiempo aproximado en una comunicación EAP que tarda un PLC en leer un estado de otro PLC a una distancia de 4 saltos de enrutamiento y actuar sobre el mismo, con el fin de evaluar si es posible implementar inteligencia distribuida.
- Revisar si existen diferencias en los tiempos de comunicación entre PLCs al aumentar el tamaño de las tramas.
- Determinar el jitter de la comunicación EAP a una distancia de 4 saltos de enrutamiento.

Se realizarán 3 pruebas con la misma programación, la diferencia estará en la cantidad de variables que los PLCs publicaran, primero se probara solo con una variable, luego con 6 variables de diferentes tamaños para obtener un tamaño de trama de 768 bytes y finalmente se aumenta a 8 variables para generar un tamaño de trama de 1280 bytes, estas variables solo se configuran y no son parte del programa principal.

Se realizarán 200 repeticiones de cada prueba para observar la variación de los tiempos de reacción para cada tamaño de paquete y a través de una interfaz mirroring que se configurará en el switch del que se conecta PLC05 se intentará determinar el jitter de los paquetes recibidos a partir de capturas de paquetes, tomando un rango de tiempo para el análisis de 60 segundos y se registrará el ancho de banda aproximado con el porcentaje de utilización del enlace.

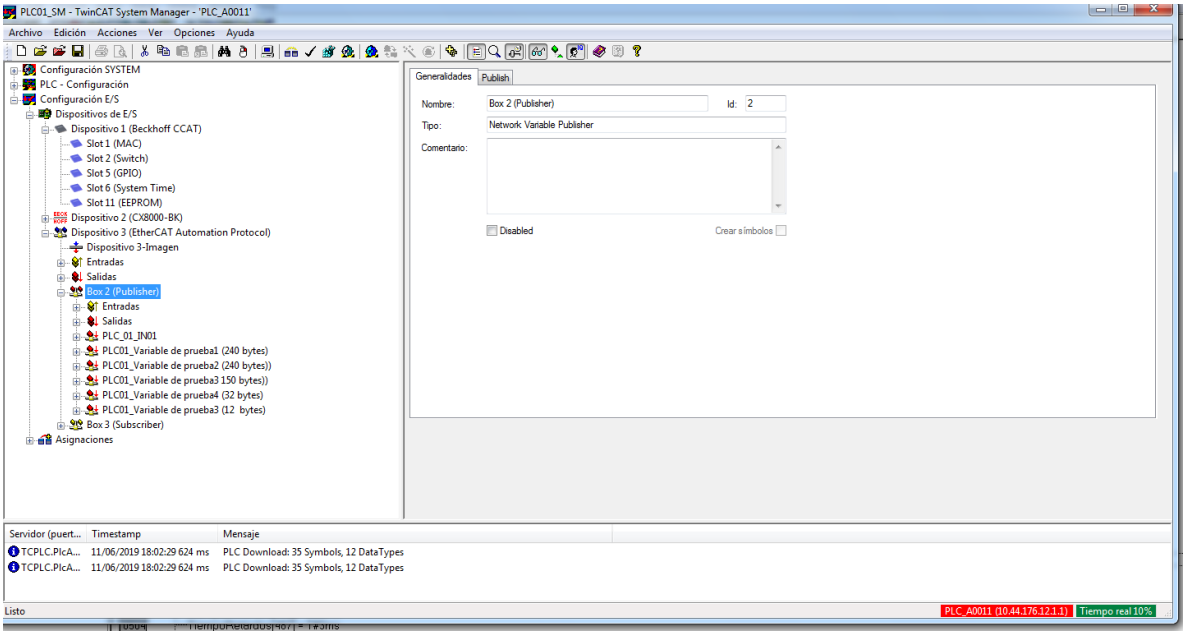


Figura 4-25 Configuración System Manager PLC01

	Time	Source	Destination	Protocol	Length	Info
2210	1.088897	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2211	1.088899	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2212	1.089791	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2213	1.090558	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2214	1.090560	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2215	1.091298	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2216	1.092145	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2217	1.092146	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2218	1.093019	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2219	1.093020	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2220	1.093896	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)
2221	1.094758	10.44.176.12	10.60.176.14	TC-NV	66	Network Vars from 10.44.176.12.1.1 - 1 Var(s)
2222	1.094760	10.60.176.14	10.44.176.12	TC-NV	66	Network Vars from 10.60.176.14.1.1 - 1 Var(s)

```
▷ Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
◢ Ethernet II, Src: Beckhoff_16:be:03 (00:01:05:16:be:03), Dst: IETF-VRRP-VRID_0b (
   ▷ Destination: IETF-VRRP-VRID_0b (00:00:5e:00:01:0b)
   ▷ Source: Beckhoff_16:be:03 (00:01:05:16:be:03)
     Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 10.44.176.12, Dst: 10.60.176.14
▷ User Datagram Protocol, Src Port: 34980, Dst Port: 34980
◢ EtherCAT frame header
     .... .000 0001 0110 = Length: 0x016
     .... 0... .... .... = Reserved: Valid (0x0)
     0100 .... .... .... = Type: NV (0x4)
◢ TwinCAT NV: Network Vars from 10.44.176.12.1.1 - 1 Var(s)
   ◢ Header
        Publisher 10.44.176.12.1.1
        Count: 0x0001
        CycleIndex: 0x4152
   ◢ Variable - Id = 1, Length = 2
      ◢ VarHeader
           Id: 0x0001
           Hash: 0x0000
           Length: 0x0002
           Quality: 0x0000
```

Figura 4-26 Capturas de publicación de variables EAP.

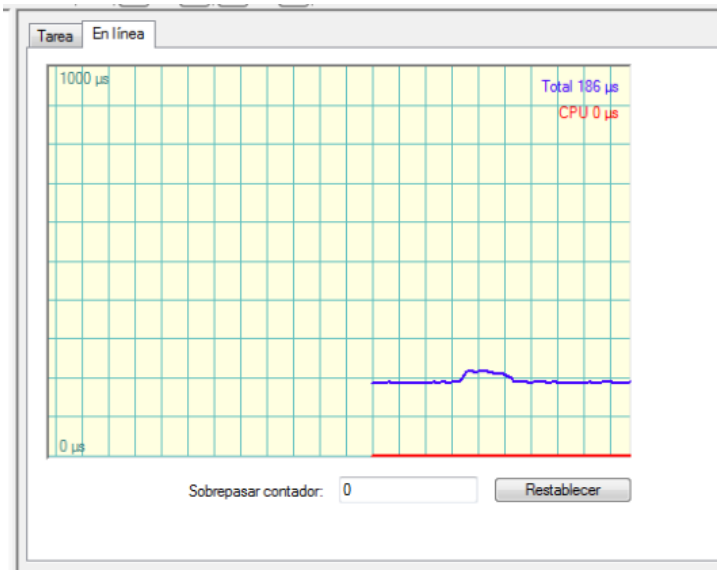


Figura 4-27 Tiempo de ejecución de tarea en un ciclo CPU PLC01

4.4.2.1 **Pruebas de tiempo de reacción**

Resultados:

CTD Variables	**1**	**6**	**8**
Tam. Trama	64 bytes	768 bytes	1280 bytes
Máximo (ms)	3,0	4,0	4,0
Mínimo(ms)	1,0	1,0	2,0
Promedio(ms)	1,6	2,7	3,0
Mediana(ms)	2,0	3,0	3,0
Desv. Estandar	0,5	0,6	0,6

Tabla 4-15 Resultados pruebas de tiempo de reacción PLCs por EAP

Observaciones de resultados:

- El tiempo de reacción de los PLCs varia levemente en función de la cantidad de variables y tamaño de paquete.
- Los tiempos de reacción están muy por debajo de los 100ms indicados por el fabricante.
- A pesar de la continua publicación de variables la CPU realiza las tareas sin inconvenientes ni retardos en un ciclo de 180µs aproximadamente.

4.4.2.2 **Pruebas de jitter y ancho de banda:**

CTD Variables	**1**	**6**	**8**
Tam. Trama	66 bytes	768 bytes	1280 bytes
% ocupación de enlace	0,56	4,7	10
Máximo (µs)	40.531	2.462	64.599
Mínimo(µs)	0	0	0
Promedio(µs)	1051	1051	1051
Mediana(µs)	886	1.297	1.070
Desv. Estandar (µs)	737	661	947

Tabla 4-16 Resultados pruebas de jitter y ancho de banda de PLCs por EAP

Observaciones de resultados:

Al revisar las medidas de jitter se encuentran variaciones indeseables y de magnitudes muy elevadas como las indicadas en los máximos de la tabla 4-16, especialmente para el caso de 1 y 8 variables, que se explican por la herramienta de medición y no con la comunicación de los PLCs.

Ambos PLCs estarán publicando sus variables de manera independiente por lo que si tuviesen problemas en sus buffers o en sus capacidades de procesamiento esto no debiese porque ocurrir al mismo instante. El puerto mirroring se configuro para observar tráfico bidireccional hacia el PLC05, y teniendo en cuenta que los buffers de transmisión y recepción son independientes no debise porque variar en el mismo momento, pero al realizar una observación general los tráficos entre los PLCs tanto del PLC05 al PLC01 como del PLC01 al PLC05 se encuentra que los eventos ocurren al mismo tiempo, como se puede ver en la figura 4-28.

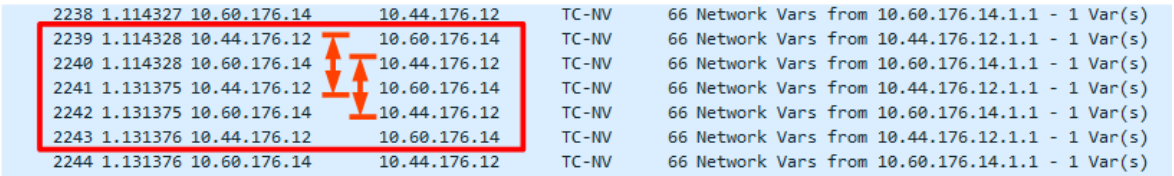


Figura 4-28 Captura problemas de medición de jitter

El comportamiento registrado en wireshark es que en determinado momento las tramas tienen un salto de jitter desde alrededor de 1ms que sería el valor ideal a valores que alcanzan 10ms - 20ms llegando a los peaks indicados en los máximos de la tabla 4.16, para luego de ese peak tener una serie de tramas con jitter por debajo de 1us, por lo que se registra un promedio ideal luego de pasado el peak.

En el grafico a continuación se muestran ambos jitter en un largo de 5 segundos, se aplica un desplazamiento de 200 paquetes para una mejor visión de los resultados, donde claramente se observa una correspondencia temporal en los saltos de jitter de recepción y transmisión en

PLC05, tanto en tiempo como en magnitud, por lo tanto, la herramienta no permite determinar con exactitud el jitter instantáneo, sólo el jitter promedio el cual es igual para todas las pruebas.

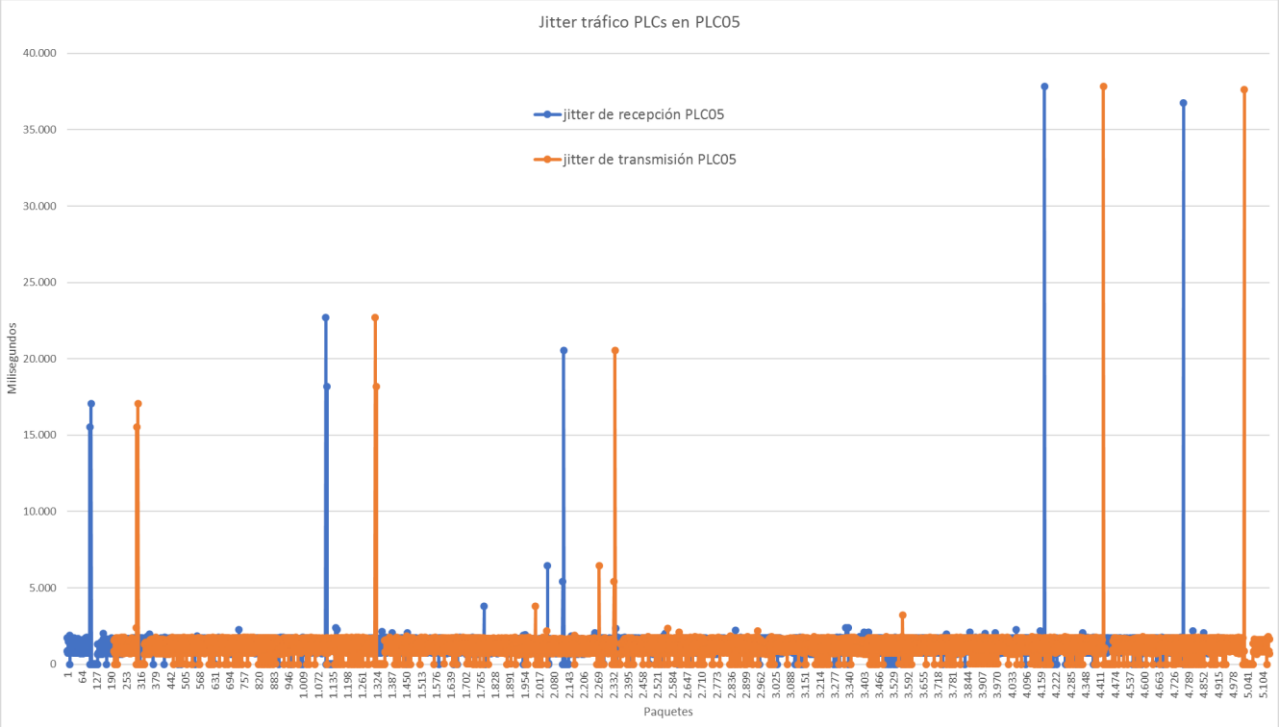


Figura 4-29 Grafico de jitter recepción y transmisión por problema en medida

4.4.3 Análisis de resultados

- El protocolo EAP demostró ser una excelente alternativa, la mayoría de los protocolos de comunicaciones industriales para lograr bajos niveles de latencia funcionan solamente a nivel de capa 2 y EAP se adapta perfectamente a las necesidades obtener una red para manejar Real-Time en redes enrutadas.
- Dado el bajo tiempo de reacción de EAP incluso para el mayor tamaño de trama con una mediana de 4ms lo hacen perfectamente viable para implementar inteligencia distribuida en redes enrutadas.
- Todos los tamaños de trama generados por los PLCs se enmarcaron dentro de la comunicación de RT-Ethernet que tiene un límite de 10ms, estando muy por debajo de este valor.
- Las pruebas de EAP se realizaron con un ciclo de tarea de 1ms que es el menor tiempo que se permite para la publicación de variables en los PLCs CX8090 ocupados en las pruebas, presentando muy buenos resultados, este ciclo de publicación es fácilmente modificable con la división por ciclo de tarea indicada en la descripción del protocolo

para implementar soluciones que consuman un menor ancho de banda o que se prefiera bajar la carga de las CPU de los PLCs.

- Al igual que en el Test de la herramienta no se consigue medir el jitter de manera correcta, presumiblemente debido al sistema operativo o a las tarjetas de red.

Capítulo 5 Propuesta de Configuración

En el presente capítulo se presenta una propuesta de configuración con los objetivos, tanto cumplir con los requerimientos y mejoras al Proyecto planteado en el caso práctico, que la red tenga un rendimiento RT-Ethernet y plantear posibles mejoras en el Subsistema de Control y ventilación.

En el capítulo 3 se llevó a cabo una descripción general de todos los Subsistemas que compondrán el ITS, en la tabla 5-1 se muestra el detalle de sus flujos de tráfico, ancho de banda, cantidades de equipos y protocolos que compondrán el ITS. Se singulariza el detalle de los equipos para SDAI y SCTV debido a que presentan diferentes anchos de banda en función de su ubicación. Es importante señalar que las cantidades se han modificado leve y proporcionalmente por motivos de seguridad.

La propuesta de configuración se realiza en base a tabla 5-1 que se construye a partir de los antecedentes previos, la descripción de los subsistemas y las pruebas realizadas.

Con respecto a la QoS y el balanceo de carga, si bien a simple vista la red está sobredimensionada, de todas formas, se plantea una propuesta de su configuración, en primer punto para evitar problemas de disponibilidad de la red por peaks de tráfico inesperados que puedan producirse en caso de alguna falla o problemas seguridad y, en segundo lugar, para dejar planteada la configuración y sea sencillo la ampliación a nuevos subsistemas.

Los parámetros de QoS se asignaron bajo 2 criterios, el primero, la prioridad del subsistema indicada por él cliente y el segundo, la recomendación del RFC 4594 “Configuration Guidelines for DiffServ Service Classes”, por ejemplo para el caso de telefonía, si bien no están en la escala de mayor prioridad para el cliente, es un tráfico sensibles a demoras y consume muy poco ancho de banda, por lo que se le asigna una alta prioridad, en el caso del sistema de detección de incendios tiene una alta prioridad pero viaja sobre TCP por lo que puede tolerar mejor alguna demora y perdida de paquetes. Es importante recordar que de las 7 prioridades que se pueden otorgar a nivel de VLAN lo recomendable es solo trabajar con las 5 más bajas ya que las prioridades altas son ocupadas por los protocolos de control de la red, en este caso la prioridad 7 es para SEP y 6 para VRRP y son asignadas automáticamente por el protocolo, mismo caso a nivel de enrutamiento con los DSCP, la mayor prioridad 48 (CS6) es asignada para BGP u OSPF.

El balanceo de carga se implementa a nivel de capa 2 configurando 2 segmentos SEP en cada anillo, el segmento SEP 1 tomara las instancias de las VLAN de los 4 subsistemas más prioritarios, uno de ellos el subsistema de detección automática de incidentes SDAI el cual es uno de los que consume más ancho de banda en conjunto con SCTV, con esto la carga de tráfico quedara repartida en los 2 sentidos del anillo.

5.1 Nomenclatura de Switches

Cada Switch dentro de la topología tendrá una nomenclatura en función de su anillo de trabajo y su función, para el caso de los switches de agregación se ocupará la sigla SAGR, además, ya que en casos futuros pudiesen trabajar con más de un anillo, se dejan 2 dígitos libres. Los switches de acceso tendrán la sigla SACC y un número según el orden dentro del anillo y los switches de Core ocuparán SCOR como sigla inicial. En resumen, cada switch será nombrado de la forma Axxyy-Tipo-número de switch, por ejemplo, el segundo switch de agregación en el anillo 20 será A0020-SAGR-002, en caso que también se conecte al anillo 19 sería A1920-SAGR-002.

N° subs	Subsistema	Sigla	CTD	Protocolos Principales	Flujo de tráfico	Ancho de banda			Pri.	802.p	DSCP (PHB)
						min	avg	máx			
10	Subsistema de Control y Ventilación	SCCV	96	TCP / ModbusTCP	Bidireccional	162 kbps	162 kbps	162 kbps	1	5	46 (EF)
11	Subsistema de Gestión de Red	SGDR	103	UDP/ SNMPv2/ HTTP /SSH	Ascendente	1 kbps	1 kbps	5 kbps	5	3	16 (CS2)
12	Subsistema de Telefonía	STEL	38	UDP/RTP, RTCP/SIP	Bidireccional	9 kbps	44 kbps	70 kbps	9	5	46 (EF)
13	Subsistema Detección de Incendios	SDTI	35	TCP / ModbusTCP/ HTTP	Bidireccional	89 kbps	89 kbps	89 kbps	3	5	36 (AF42)
14	Subsistema de Radiocomunicaciones	SRAD	10	UDP/SNMPv2/HTTP	Ascendente	1 kbps	1 kbps	5 kbps	7	0	0 (BE)
15	Subsistema de Control iluminación	SILU	39	UDP/SNMPv2/HTTP	Bidireccional	89 kbps	89 kbps	89 kbps	11	1	18 (AF21)
16	Subsistema de control energía de baja tensión	SCBT	10	UDP/Profinet/HTTP	Ascendente	1.1 Mbps	1.1 Mbps	1.1 Mbps	10	0	0 (BE)
17	Subsistema de Postes SOS	SSOS	86	UDP/TCP/RTP, RTCP/SIP /ModbusTCP / HTTP	Bidireccional	66 kbps	82 kbps	143 kbps	2	5	46 (EF)
18	Subsistema de Megafonía	SMEG	25	UDP/RTP, RTCP/SIP /HTTP	Descendente	90 kbps	106 kbps	167 kbps	6	4	26 (AF31)
19	Subsistema de Señalización de tráfico	SGTR	68	TCP / ModbusTCP/ HTTP	Bidireccional	65 kbps	65 kbps	65 kbps	8	1	20 (AF22)
20	Subsistema de Circuito Cerrado de Televisión	SCTV	105	UDP/ RTP, RTCP / HTTP	Ascendente				12	0	0 (BE)
	Cámara Indoor (30 FPS)	CTVI	79			1.4 Mbps	2.6 Mbps	4.7 Mbps			

	Cámara Outdoor (30 FPS)	CTVO	21			2 Mbps	3.8 Mbps	6.8 Mbps			
	Cámara Outdoor movimiento (30FPS)	CTVM	5			6.8 Mbps	13.8 Mbps	15.8Mbps			
21	Subsistema de Detección Automática de Incidentes	SDAI	84	UDP/ RTP, RTCP / HTTP	Ascendente				4	2	34 (AF41)
	Cámara Indoor (30 FPS)	DAII	68			1.4 Mbps	2.6 Mbps	4.7 Mbps			
	Cámara Outdoor (30 FPS)	DAIO	16			2 Mbps	3.8 Mbps	6.8 Mbps			

Tabla 5-1 Base de propuesta de configuración.

A cada anillo de la topología más el cluster formado por los 2 Cores, se le asignara un número de anillo, el anillo de Core será el 1 y luego de izquierda a derecha se iniciará del 10 en adelante, no se ocupan del 2-9 por posibles crecimientos futuros, la distribución puede verse en la figura 5-1.

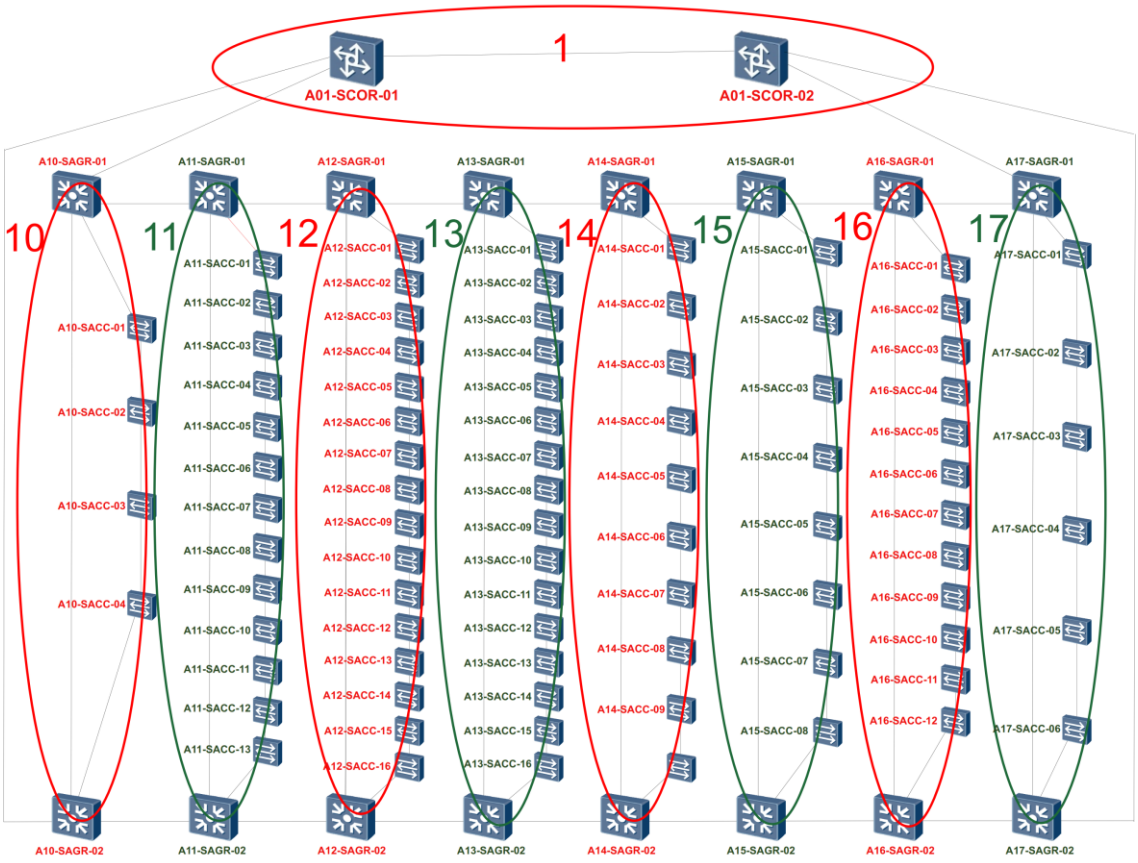


Figura 5-1 Distribución de anillos de la topología de la red de los túneles.

5.2 Cálculo de tráfico Agregado

Dentro de las características de tráfico de red de los Subsistemas se puede indicar que los que ocupan ModbusTCP su flujo será bidireccional siendo el flujo ascendente levemente superior, los Subsistemas con tráfico de voz como SSOS, STEL o SMEG el ancho banda consumido tendrá su peak en situaciones de emergencia y los 2 Subsistemas que tienen mayor consumo de ancho serán SCTV y SDAI, los cuales tienen un flujo primordialmente ascendente. Además, en los análisis de resultados de las pruebas detalladas en el capítulo 4 se determinó que el protocolo a ocupar para los loops en capa 2 será SEP y en el Análisis de Resultado de las pruebas VRRP el uso de BFD lo que conlleva a que existirá una carga de tráfico adicional por estos 3 protocolos las cuales, en base a las capturas de tráfico realizadas en las pruebas, será de menos de 1kbps por lo cual se considerará despreciable. El tráfico de control generado por el protocolo BGP o OSPF es aún menor que el de los protocolos que trabajan en los anillos de acceso por lo que también se considera despreciable.

Para hacer el cálculo de tráfico se tomará el flujo ascendente que será el que tenga la mayor carga y se asumirá un escenario de falla en que se pierde el balanceo de carga, fluyendo todo el tráfico por los switches de agregación AXX-SAGR-0001.

Desde la capa de agregación se asumirá también el peor escenario donde todo el tráfico sube desde la capa de agregación al Core A01-SCOR-01

En la Tabla II-2 del Anexo II puede verse en detalle la distribución de equipos de los diferentes subisistemas en cada switch y el ancho de banda consumido por cada uno, siendo la base para el cálculo del tráfico agregado. Ninguno de los switches superan los 25Mbps lo que es un 2.5% de la capacidad de 1Gbps teórica del switch.

Luego al sumar los tráficos agregados por anillos se obtiene:

Switch	**Min**	**Avg**	**Max**
A10-SAGR-0001	17 mbps	31 mbps	45 mbps
A11-SAGR-0001	64 mbps	114 mbps	180 mbps
A12-SAGR-0001	70 mbps	118 mbps	202 mbps
A13-SAGR-0001	71 mbps	125 mbps	218 mbps
A14-SAGR-0001	41 mbps	73 mbps	129 mbps
A15-SAGR-0001	28 mbps	49 mbps	86 mbps
A16-SAGR-0001	50 mbps	90 mbps	158 mbps
A17-SAGR-0001	30 mbps	56 mbps	81 mbps
Agregado	372 mbps	656 mbps	1.098 mbps

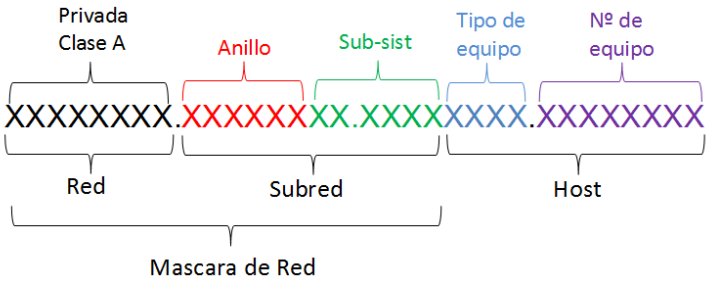
Figura 5-2 Trafico agregado por anillo.

Como puede observarse en la tabla 5-2 el Anillo 13 es el que presenta la mayor carga de tráfico y corresponde a un 22% de la capacidad nominal de los switches de Acceso, además en el switch A10-SAGR-0001 en el peor escenario existirá un tráfico agregado de aproximadamente 1Gbps que corresponde a un 10% de su capacidad nominal por lo que tal como se indicó al inicio de este capítulo la red está sobredimensionada.

5.3 Propuesta capa de Acceso

5.3.1 Direccionamiento IP para equipos terminales

Se ocuparán direcciones válidas para Clase A mascara 20, en función de 4 criterios, anillo, subsistema, tipo de equipo y n° consecutivo del tipo de equipo dentro del anillo más 10. Se utilizarán 6 bits para el anillo, 6 bits para el subsistema, 4 bits para el tipo de equipo y 8 bits para el n°de equipo



Según la cantidad de bits ocupados se podrá tener hasta 64 anillos, pero con la nomenclatura de VLAN que se explicará a continuación quedara limitado a 40, 64 subsistemas, 16 tipos de equipos distintos y hasta 245 equipos de un tipo en el mismo anillo (ya que las primeras 10 direcciones se reservan).

Si bien la nomenclatura propuesta limita en un grado de magnitud del crecimiento de la red, tiene un margen muy amplio y se obtiene un direccionamiento orientativo de la ubicación de los equipos para facilitar la administración y troubleshooting.

Es importante indicar que las direcciones IP de los equipos de la red ITS se configurarán manualmente, por lo tanto no se utilizará DHCP y además no se utilizara DNS.

5.3.2 Configuración Básica de switches

5.3.2.1 **VLANs**

Cada subsistema trabajara en una VLAN distinta, si bien no debiese existir comunicación entre subsistemas, es una exigencia por parte del cliente y solo se realizará en los switches de agregación de cada anillo, las VLAN pudiesen ocupar simplemente el número de Subistema en cada anillo, pero esto puede llevar a confusiones desde el punto de vista administrativo. Para evitar este problema las VLAN de cada subsistema se formarán con los primeros 2 dígitos correspondientes al anillo y los segundos 2 dígitos al subsistema.

Por ejemplo, una cámara del Subsistema de SCTV que esté conectada dentro del anillo 14, tendrá asignada la VLAN 1420.

Debido a que el número máximo de VLAN que se permite en el equipamiento es de 4096, la nomenclatura permite tener hasta 40 anillos y 96 subsistemas.

Definido el formato se deberán crear en cada switch del anillo, las VLANs correspondientes a cada Subisistema.

5.3.2.2 **Interfaces:**

5.3.2.2.1 Switches de Acceso:

Los switches de acceso tienen interfaces GE y FE.

- Las interfaces GE son del tipo combo (fibra y cobre) y serán interconectadas mediante fibra óptica monomodo, las conexiones serán configuradas como enlaces de capa 2 tipo Trunk, limitando el acceso solo a las VLANs creadas en cada switch.
- Las interfaces FE se configurarán como acceso y asignarán una VLAN al tráfico que ingrese por ellas en función de la interfaz ocupada.

5.3.2.2.2 Switches de Agregación:

Los switches de agregación tienen interfaces de 1GE y 10GE, 4 de las interfaces GE son del tipo combo.

- Se utilizarán 2 interfaces GE para conectar con los switches de acceso, por lo que estas interfaces deben configurarse como capa 2 en modo trunk, limitando el acceso solo a las VLANs creadas en cada Switch

5.3.2.3 **Protocolo para prevención de loops**

SEP será el protocolo que se ocupará en los anillos

5.3.2.3.1 Criterios de diseño:

- Balanceo de carga, si bien la red está sobredimensionada el dejar el balanceo de carga configurado hará mucho más simple su uso en caso de crecimientos futuros.
- El balanceo se realiza según la prioridad del subsistema.
- El enlace que une los switches de agregación del mismo anillo se establecerá como respaldo para los segmentos SEP, no debiese circular tráfico de usuario en condiciones normales.
- Nomenclatura que permite identificar el anillo.
- Tiempo de preempt de 60 segundos.

5.3.2.3.2 Configuración básica de los switches de cada anillo de acceso:

i. Se configurarán dos segmentos SEP 1 y 2.
ii. La VLAN de control de los segmentos tendrán el mismo número del anillo, por ejemplo, los segmentos 1 y 2 del anillo 11, tendrá la VLAN de control 11.
iii. Se desactiva STP en las interfaces de que serán parte de la topología SEP y se les asignan los segmentos SEP 1 y 2.
iv. Se crean las instancias 1 y 2 utilizando de spannig tree.
v. Se asignan las VLANs de los subsistemas 4 subsistemas más prioritarios a la instancia 1, ya que tienen un mayor nivel de prioridad.
vi. Se asignan las VLAN de los subsistemas restantes a la instancia 2, que será menos prioritarias y estarán en el sentido de mayor carga, aunque no debiese jamás producirse congestión.
vii. Se asigna la instancia 1 al segmento SEP 1 y la instancia 2 al segmento SEP 2

5.3.2.3.3 Configuración de los switches de Agregación de los anillos:

En el Switch A00XX-SAGR-001 (XX número de anillo)

i. la interfaz que conecta con su switch de acceso más próximo será configurada como Primary edge port del segmento SEP 1 y se le asignara una prioridad de bloqueo de 100 (64 por defecto) para el segmento SEP 2, lo que provocará que el puerto sea bloqueado para dicho segmento.
ii. La interfaz que conecta con el switch A00XX-SAGR-002 como Sencondary edge port del segmento SEP 2.
iii. Se activará la configuración de bloqueo de puerto según prioridad.
iv. Se configura el tiempo de preempt en 60 segundos.

En el Switch A00XX-SAGR-002:

i. la interfaz que conecta con su switch de acceso vecino será configurada como Primary Edge port del segmento SEP 2 y se le asignara una prioridad de bloqueo de 100 para el segmento SEP 1, lo que provocará que el puerto sea bloqueado para dicho segmento.
ii. La interfaz que conecta con el switch A00XX-SAGR-001 se configurara como Secondary edge port del segmento SEP 1.
iii. Se activará la configuración de bloqueo de puerto según prioridad.
iv. Se configura el tiempo de preempt en 60 segundos.

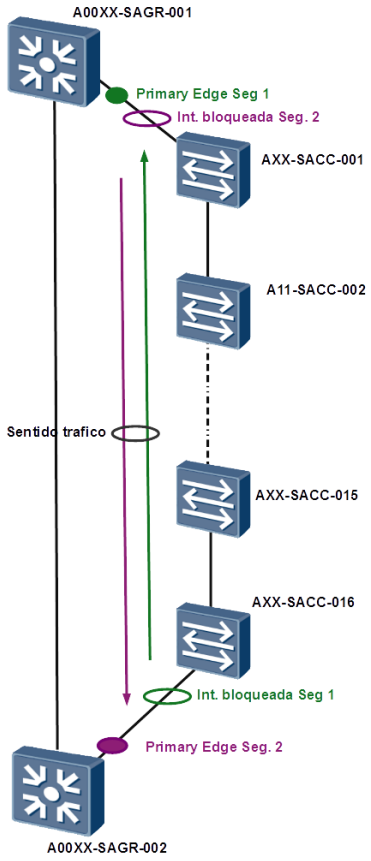


Figura 5-3 Configuración y sentido de tráfico con configuración SEP

5.3.2.4 **QoS**

La calidad de servicio solo cobra relevancia cuando la red esta congestionada, la configuración que se propone es pensando en crecimientos futuros.

5.3.2.4.1 Criterios de diseño

- El tráfico en la interfaz no puede exceder el límite indicado para el equipo terminal del subsistema, a fin de evitar la congestión en el ingreso y no en la interfaz troncal ya que estas tendrán tráfico acumulado de los diferentes switches y la granularidad de la configuración lo hace complejo de administrar.
- Se marcarán los paquetes en el campo prioridad de VLAN de la trama ethernet según lo indicado en la tabla 5-1, cabe señalar que la prioridad de VLAN, solo funcionará en el anillo de acceso ya que al subir de capa a la de agregación se realizará una clasificación distinta.
- SCTV funcionara con servicio mejor esfuerzo debido a que es el subsistema que consume mayor ancho de banda.

5.3.2.4.2 Configuración

i. Se asigna directamente en la interfaz el marcado de paquetes en el campo de prioridad de VLAN en concordancia con el subsistema que se conecte a dicha interfaz según la tabla 5-1.
ii. Se realiza una limitación del tráfico de entrada configurando el CAR PIR según el ancho de banda máximo indicado en la tabla 5-1 más un 10%.

5.4 Propuesta capa de Agregación

5.4.1 Configuración básica de switches

5.4.1.1 Conexiones entre switches de agregación y hacia el Core

Como se indicó en la descripción inicial de la red las conexiones entre los switches de agregación son 10GE, éstas serán configurada como enlaces capa 3 mascara 30, por lo que en primer punto se debe aplicar un comando que deje la interfaz en esta capa.

Para el direccionamiento IP de las conexiones entre switches de agregación se tendrá la siguiente nomenclatura:

192.168.X.Y /30

X= número de anillo menor del enlace.

Y podrá ser:

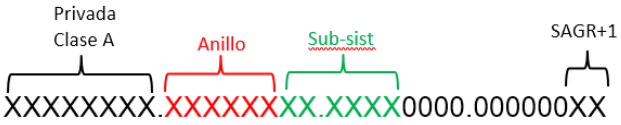
- 5 si es la interfaz del switch de agregación 1 del anillo menor del enlace.
- 6 si es la interfaz del switch de agregación 1 del anillo mayor del enlace.
- 9 si es la interfaz del switch de agregación 2 del anillo menor del enlace.
- 10 si es la interfaz del switch de agregación 2 del anillo menor del enlace.

Por ejemplo, las conexiones entre los switches A0013-SAGR-001 y A0014-SAGR-001

En su interfaz XG0 el switch A0013-SAGR-001 tendrá la dirección 192.168.13.5/30 y A0014-SAGR-001 tendrá 192.168.13.6/30.

5.4.1.2 Interfaces de VLAN

En cada switch de agregación se crearán interfaces virtuales VLANIF, para las VLANs que tengan configuradas, las direcciones de la subred de cada interfaz se asignaran en los mismos términos de lo que se indicó para los equipos terminales. Los switches de agregación A00XX-SAGR-001 tendrán direcciones .2 y los switches de A00XX-SAGR-002 .3.



5.4.2 VRRP

5.4.2.1 **Criterios de diseño:**

- Balanceo de carga, los Master de los grupos VRRPs tienen que corresponder con el sentido del tráfico que se configurará en SEP.
- El balanceo se realiza según la prioridad de cada subsistema
- Nomenclatura que permita identificar el subsistema del grupo VRRP.
- El Master deberá cambiar su prioridad en función de los 2 enlaces capa 3 que tiene con los switches de agregación de los anillos vecinos, para lo que se utilizaran sesiones BFD.
- Tiempo de preempt de 60 segundo.

5.4.2.2 **Configuración a VRRP:**

i. Se creará un grupo VRRP para cada subsistema con las interfaces VLANIF previamente creadas.
ii. Se asignarán las direcciones virtuales de subred del subsistema IP .1 a cada grupo VRRP
iii. Se crearán sesiones BFD con las 2 las interfaces capa 3 de los switches de agregación vecinos a fin de detectar rápidamente la caída.
iv. La nomenclatura de las sesiones BFD serán AXXntoAYYr, donde XX será el anillo propio *n* el número de switch de agregación del anillo YY el anillo del switch del peer y *r* el número de switch de agregación del peer, por ejemplo, una sesión entre los switches de agregación A0011-SAGR-002 y A0012-SAGR-002, en A0011-SAGR-002 se llamará A112toA122.
v. El *Discriminator* local de las sesiones será XXY, donde XX será el número de anillo e Y el número de sesión, la sesión conformada hacia un switch de un anillo mayor será la 1 y la sesión hacia un switch de un anillo menor la 2.
vi. Los parámetros de configuración de la sesión BFD serán, intervalo de envío y recepción de 50ms, igual para ambos extremos, y el detector *Detect Multiplier* con un valor de 3.
vii. Los switches A00XX-SAGR-001 serán los Masters para los 4 subsistemas con mayor prioridad y tendrán una prioridad de 120 y los switches A00XX-SAGR-002 los Masters para los subsistemas de restantes, con una prioridad de 120.
viii. Los switches A00XX-SAGR-001 y A00XX-SAGR-002 serán los Backups de los grupos VRRP de los que no son Master, su prioridad será la por defecto del protocolo que es de 100.

ix. Todos los Masters de los grupos VRRP tendrán tracks a las sesiones BFD establecidas con sus switches de agregación vecinos con decrementadores de 15, en caso de detectar una caída, la prioridad disminuirá en 15, quedando con una prioridad de 105 con lo que continuara siendo el Master ya que aún tendrá una ruta alternativa, en caso de caer la segunda sesión la prioridad bajara a 90 y se producirá el cambio.
x. Se configurará un tiempo de preempt de 60 segundos.

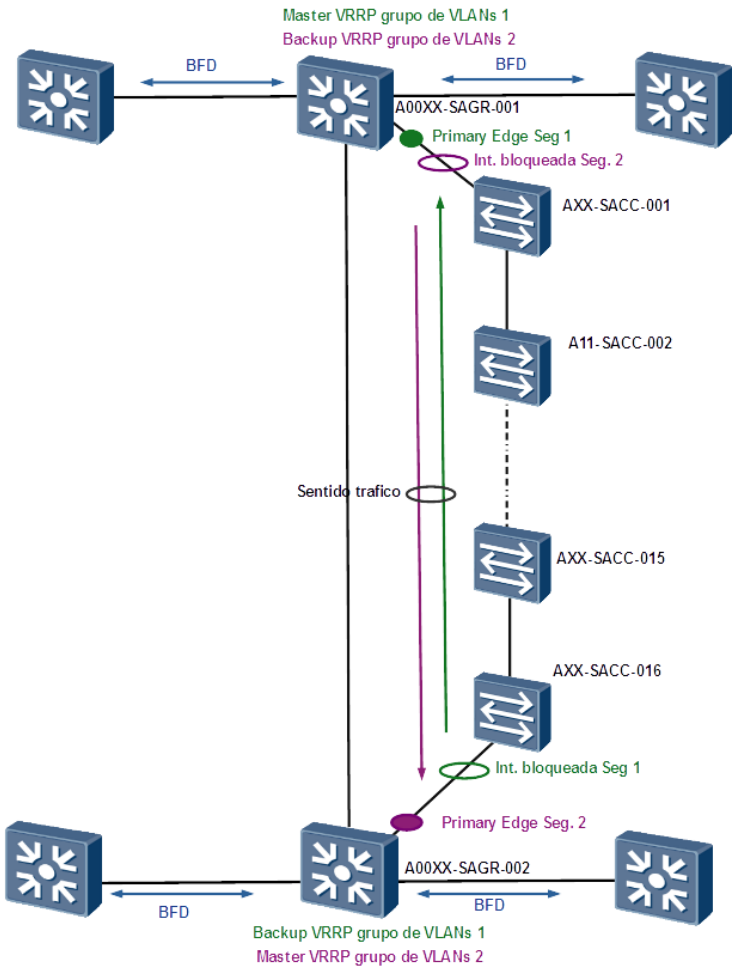


Figura 5-4 Configuración VRRP propuesta

5.4.3 Enrutamiento

Si bien OSPF presento excelentes resultados con respecto a la convergencia y aunque BGP presenta un grado de convergencia menor para topologías de tipo anillo, se ocupara este como protocolo de ruteo básicamente por su facilidad y flexibilidad de administración en base a políticas, además OSPF cuenta con la desventaja que al ser capa 2 la red de acceso la

comunicación intra-area se realizaría entre todas las interfaces VLANIF del anillo que tendrían ambos switches de agregación, habría intercambio constante de hellos y LSAs entre cada subred del anillo, lo que no ocurre con BGP ya que la sesión IBGP solo se realiza entre una dirección especifica. Dado además que su latencia fue prácticamente igual que la obtenida con OSPF y que se puede ocupar en conjunto con BFD directamente en los peers para dar caídas las adyacencias, BGP será el protocolo que se implementará.

5.4.3.1 **Criterios de diseño:**

- Conexiones de vecinos EBGP mediante interfaces capa 3
- Conexiones IBGP con interfaces virtuales VLANIF.
- Se crearán grupos para las conexiones EBGP e IBGP.
- Preferencias de rutas EBGP con valor de 150 utilizando el atributo *PrefVal*, para evitar que tráfico externo utilice el anillo como camino.
- No se utilizará la preferencia para el tráfico de salida del anillo con *Local preference*, ya que la dirección de salida la manejaran los protocolos VRRP y SEP.
- La ruta EBGP hacia el Core tendrá un *PrefVal* de 20 a fin de evitar que tráfico entre Switches de Agregación suba innecesariamente al Core.

5.4.3.2 **Configuración a BGP**

i. Se activará el protocolo BGP en todos los switches de agregación, el número de sistema autónomo estará dado por 651XX, donde XX será el número de anillo.
ii. Se le asignará un router Id al equipo de la forma 1.0.XX.Y, donde XX será el número de anillo e Y el número de Switch de agregación del anillo.
iii. Se crean 2 grupos para los peers BGP, com_EBGP se definirá como un grupo external y com_IBP como un grupo internal.
iv. Se crean los peers EBGP, con la dirección IP de la interfaz capa 3 y sistema autónomo de destino.
v. En cada peer EBGP se activará BFD con intervalos de transmisión y recepción de 100ms y un *Detect Multiplier* de 4.
vi. A los peers EBGP se les asignara una preferencia *PrefVal* de 150 y se agregarán al grupo com_EBGP.
vii. Se creará una VLAN con nomenclatura XX70 para la comunicación IBGP, donde XX es el número de anillo, ésta VLAN además se creará en todos los switches del anillo de acceso y se agregará a las VLANs permitidas por las interfaces troncales del anillo.
viii. Se configurará una interfaz de virtual VLANIF en los 2 switches de agregación de los anillos con la dirección 192.168.1XX.5/30 para los switches de agregación A00XX-SAGR-001 y 192.168.1XX.6/ para los switches de agregación A00XX-SAGR-002, donde XX será el número de anillo.
ix. Se creará el peer IBGP en cada switch a través de las interfaces VLANIF previamente configuradas y se agregaran al grupo com_IBGP. No se asignará ningún tipo de preferencia.

x. Se importarán los prefijos directos que ya estarán dentro del switch debido a que fueron creados en la etapa de establecimiento de interfaces VLANIF en VRRP por lo que no es necesario declarar las rutas.
xi. Por defecto la sincronización viene desactivada en los equipos, pero se comprobará para no tener problemas con la publicación de prefijos.

5.4.4 QoS

5.4.4.1 Criterios de diseño

- Se crearán políticas en base a clasificadores *classifier* y un comportamiento *behaviors*, utilizando MQC que podrán ser replicable en todos los anillos, esto permitirá en el futuro ampliar fácilmente las políticas de QoS.
- Se creará un *classifier* en función de las VLAN de cada subsistema y no de la marca 802p que serán configuradas en las interfaces de los switches de acceso a fin de obtener una mayor granularidad y flexibilidad en la configuración.
- Se configurará un *behavior* para el marcado de los paquetes en función de la VLAN del subsistema con un DSCP según la tabla 5-1.
- La política de descarte de paquetes se realizará en función de los DSCPs, por lo que no se asignaran perfiles especiales.
- El tráfico del sistema de control es el más importante de la red por lo que debe tener un ancho de banda garantizado.

5.4.4.2 Configuración:

1. Se creará un *classifier* para cada subsistema que tendrán el nombre cla_SSSS_1 donde SSSS será la sigla del subsistema.
2. El *classifier* se configurará para realizar un match a la VLAN del subsistema.
3. Se creará un *behavior* para cada subsistema que tendrá nombre beh_SSSS_1 donde SSSS será la sigla del Subsistema.
4. El *behavior* remarcara los paquetes en que hagan match con su classifier respectivo marcándolo con un DSCP según lo indicado en la tabla 5-1.
5. Se creará una política para cada subsistema que tendrán el nombre pol_SSSS donde SSSS será la sigla del subsistema.
6. Se asignará a la política el *classifier* y *behavior* creados previamente para el Subsistema. La política posteriormente puede ser editada agregando nuevos elementos en función del crecimiento de la red.
7. Se le aplicara la política en el ingreso de tráfico (inbound) a las interfaces GE de los switches de agregación que cierran los anillos en capa 2. Esto debido a que la mayoría del tráfico fluirá de la capa de acceso a la de agregación y luego a la de CORE.
8. Para el tráfico de bajada de agregación al anillo de acceso, será mucho menor que el de subida, por lo que se realizará un mapeo simple, según el DSCP se asignará una prioridad a la VLAN, esto se realiza "confiando" en el mapeo con un *trust*, básicamente ocupará los 3 bits del IP *precedence* para asignárselos a la prioridad de la VLAN.

9. Se configura el *behavior* de control beh_SCCV con un CAR CIR de 100Mbps para garantizar su ancho de banda.

5.5 Propuesta capa de Core

La capa de Cores será la que conectará la capa de agregación con los servidores de todos los Subsistemas que forman el ITS del proyecto, se considerará como otro anillo más con el número 1.

Estará formada por dos equipos conectados a distancia formando un Cluster, si bien no es parte de esta propuesta de configuración la seguridad de la red, el acceso debe ser sumamente restringido a estos equipos ya que cualquier cambio involuntario podría causar el colapso completo de la red

5.5.1 Interfaces:

Los switches de Core tendrán 3 tipos de interfaces:

- 48 interfaces de 1GE de cobre para conectar los servidores de los diferentes Subsistemas.
- 16 interfaces de 10GE para conectar a los switches de agregación, cerrar los anillos de esta capa y también se ocuparán para formar un Eth-trunk disponible para la conexión MAD.
- 2 interfaces de 40GE para conectar con el switch de Core del Centro de Control de Respaldo.

5.5.2 Configuración hacia equipos terminales

Para las VLAN se ocuparán la misma política de asignación indicadas para los switches de acceso en 5.3.2.1 y la de interfaces VLANIF para dichas indicadas en 5.4.1.2.

5.5.3 Configuración hacia la capa de agregación

- Se ocupará la misma política de enlaces capa 3 mascará 30 indicas en el punto 5.4.1.1 para los enlaces hacia la agregación.
- Se ocupará el mismo procedimiento para establecer BGP indicado en los switches de agregación en 5.4.3.2.

5.5.4 Configuración Capa de Core

5.5.4.1 Configuración Eth-trunk

- Se crea el trunkport Eth-Trunk 3 y se le asignan las interfaces 10GE 5 y 6

- Se le asigna funcionamiento de balanceo de carga.

5.5.4.2 Configuración CSS

1. Se activa CSS en los switchs modo LPU para ocupar las interfaces de servicio de 40 GE en ambos switches que formaran el cluster
2. Al switch de Core del centro principal se le asigna el id 1 y la prioridad 50
3. Al switch de Core del centro de respaldo se le asigna el id 2 y la prioridad 10
4. Se le asigna al trunkport Eth-Trunk 2 MAD en modo directo para el caso de la duplicidad de Masters CSS.

5.5.5 QoS

Se aplicará la misma política descrita en el punto 5.4.4.2 para la capa de agregación con la diferencia que la política se aplicará al tráfico de salida (outbound) de la interfaz que conecte con los switches de agregación.

5.6 Propuesta de cambios para el subsistema de control centralizado y ventilación

La arquitectura propuesta actualmente en el proyecto es la de tener 2 PLCs en los centros de control que sean los Masters de las cabeceras distribuidas en los diferentes anillos de la red. Esta configuración trae el inconveniente de que ante la falla de una conexión ya sea a nivel de acceso de agregación o de Core provoca que las cabeceras dejen de actuar debido a que pierden la comunicación con el maestro. En segundo lugar, el protocolo que se pretende implementar ModbusTCP según los antecedentes previos revisado no puede asegurar determinismo alguno en base que simplemente es una encapsulación del antiguo Modbus.

En base a lo anterior se propone en primer término realizar un cambio en la arquitectura teniendo PLCs más sencillos y económicos que estén redundados en cada anillo y que estos sean los Maestros que se encarguen de reportar al sistema de orden superior SCADA y controlar el las cabeceras distribuidas que tengan dentro de su anillo, lo que aporta aún más robustez al sistema y garantiza que las fallas que se produzcan solo afectan a un área controlada. Además, con el cambio y en base a que todas las marcas tienen protocolos con alto nivel de determinismo a nivel de enlaces capa 2 almenos para comunicaciones Soft Real Time, se podrían implementar PLCs de cualquier marca, dejando solo las comunicaciones hacia SCADA con Modbus TCP.

En segundo punto, en caso de estar disponible en los PLCs adquiridos, se propone EAP como protocolo de comunicación, debido a sus excelentes resultados tanto en determinismo y en tiempo de reacción en comunicaciones a nivel de capa 3 lo que en conjunto con su filosofía de Publisher/Suscriber usando o no multicast permite tener aún más redundancia a nivel de PLCs ya que en caso de falla podría perfectamente el PLC de otra ubicación de la red tomar el control del anillo, además la filosofía permitiría implementar inteligencia distribuida en caso de requerirse bastaría con tener algún flag que reporte de un PLC a otro la necesidad de apoyo.

Conclusiones

i. Uno de los objetivos más importantes de esta Tesis era lograr diseñar y proponer una configuración para un caso real a partir del estudio previo de los protocolos de las aplicaciones e información empírica a través de pruebas, ambos items entregarían la base de la configuración para obtener un rendimiento Soft RT-Ethernet en sus comunicaciones. Para lo anterior debían medirse valores de latencia y jitter, pero debido a la falta de una herramienta confiable, no se pudo obtener la medición de jitter ni con la herramienta Iperf ni con la medición realizada con wireshark por lo cual no pudo cumplirse por completo el objetivo de obtener una base empírica y tuvo que omitirse el jitter como métrica a considerar en la elección de protocolos.

ii. Cada día existen más dispositivos como sensores, actuadores, microcontroladores, etc. que tienen integrados alguna tarjeta de red TCP/IP, además las tendencias a sistemas distribuidos en la automatización y la masificación de IoT, presentan un escenario en las que son más adecuadas las comunicaciones enrutadas que las switcheadas, ya que permiten mayores controles de seguridad, hacen más pequeños los dominios de broadcast optimizando el ancho de banda y previenen las tormentas de broadcast que se pudiesen producirse por malas configuraciones.

iii. El protocolo SEP propietario de Huawei demostró excelentes prestaciones logrando convergencias por debajo de los 10ms cuando la falla se produce en el mismo equipo que debe realizar la convergencia, además estuvo siempre en niveles entorno de los 50ms incluso duplicando la cantidad de equipos, también su flexibilidad en la configuración, facilidad en el balanceo de tráfico lo hacen una alternativa en implementaciones futuras.

iv. La inclusión del protocolo BFD para mejorar la velocidad de convergencia, demostrada con VRRP y su fácil calibración con sus parámetros de trasmisión, recepción y detect multiplier en caso de encontrar problemas de flapping lo convierten en una excelente alternativa para la implementación de redes que necesiten los niveles de tiempo de convergencia como la presentada en el ejemplo práctico.

v. La entrada del 5G y las extensiones de las comunicaciones fibra Optica, trabajando en conjunto en una red local enrutada con rendimiento RT-Ethernet, pudiesen hacer posibles servicios tipo *Control-as-a-service* [35]. En los sistemas ICS, si bien se abre un gran agujero en la Ciberseguridad, ya que se debiese conectar una Red de ICS a Internet, pudiese funcionar bajo estrictas medidas de filtrado de tráfico solo para casos de mantención o fallas de PLCs Implementando un PLC en la nube por periodos acotados de tiempo, también pudiese aplicar para empresas con ICSs similares que cuentan con PLCs iguales en distintas áreas o zonas geográficas de las empresas.

vi. A pesar de ocupar laptops de alta capacidad para el desarrollo de las pruebas se detectó poco determinismo en la generación de tráfico, una de las causas posibles fue

la utilización de Windows como S.O por lo que en trabajos futuros se plantea repetir las pruebas con S.O Linux.

vii. Las configuraciones de QoS con MQC le aportan buen grado de flexibilidad al manejo de la de la calidad de servicios ya que luego de realizar una política general se pueden fácilmente incorporar nuevos requerimientos.

viii. Durante el estudio y las pruebas de generadores de tráfico no se pudo obtener uno que contara con la suficiente estabilidad para poder realizar pruebas confiables con carga como se indica en el RFC-2544 y en la recomendación ITU Y-1564 por lo que la pruebas tuvieron que realizarse en base al comando ping.

Trabajos Futuros

i. Si bien en teoría las comunicaciones cifradas no son adecuadas para comunicaciones RT-Ethernet debido al necesario proceso de cifrado y descifrado se plantea como trabajo futuro una comparación de rendimientos entre comunicaciones cifradas y sin cifrar para obtener un basé empírica real del hardware y plantear la posibilidad de implementación con lo que se lograrán evitar alguna consecuencia con los ataques main-in the middle por completo.

ii. Realizar pruebas de convergencia de Gateway VRRP y enrutamiento BGP y OSPF con autenticación para determinar su influencia en los tiempos de convergencia.

iii. Medir tiempo de convergencia de una aplicación real a través de la perdida de paquetes en la comunicación unicast enrutada entre 2 PLCs, ya sea por EAP o Ethernet/IP. Se consideran estos 2 protocolos ya que incluyen número de secuencia o paquete por encima de la capa 2.

iv. Realizar ejercicio práctico para comprobar el uso de inteligencia distribuida en comunicaciones enrutadas a través de 2 o más PLCs y una serie de tarjetas remotas de entradas y salida, todos comunicados ya sea por EAP o Ethernet/IP usando multicast lo que permitirá que las variables de todos los dispositivos sean publicadas en la red. Luego en los códigos de programación de los PLCs se deben tener flags que se activen y desactiven en función de las variables de vida tipo “keep Alive” o procentaje de CPU usado. Los flags permitirán activar o deactivar partes del código y compartir la carga parcial o total del trabajo de los PLCs.

Glosario

3GPP	3rd Generation Partnership Project
ABR	Area Border Router
ARP	Address Resolution Protocol
AS	Autonomous Systems
ASBR	Autonomous System Boundary Routers
ASN.1	Abstract Syntax Notation One
AT	Acknowledge Telegram
BDR	Backup Designated Router
BFD	Bidirectional Forwarding Detection
BGP	Boder Gateway Protocol
BPA	Block port advertisement
BPDU	Bridged Protocol Data Unit
CBA	Component Based Automation
CCTV	closed circuit television
CIP	Common Industrial Protocol
CSS	Cluster switch System
DBD	Data base description
DCOM	Distributed Component Object Model
DNS	Domain Name Service
DR	Designated Router
EAP	EtherCAT Automation Protocol EAP
EGP	Exterior gateway protocol
EPA	Edge port advertisement
EPSG	Ethernet POWERLINK Standardization Group
ERP	enterprise resource planning
ERPS	Ethernet Ring Protection Switching
EtherCAT	Ethernet for Control of Automation Technology
FE	Fast Ethernet
FRR LFA	Fast Reroute Loop-Free Alternates
GE	Gigabit Ethernet

GOP	Group Of Pictures
HMI	Human Machine Interface
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IEC	International Electrotechnical Commission),
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IGP	Internal Gateway Protocol
IP	Internet Protocol
IPG	Interpacket GAP
ISO	International Standards Organization
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
LACP	Link Aggregate Control Protocol
LACPDU	Link Aggregation Control Protocol Data Units
LAG	Link agregation Groups
LSA	Link State Advertisement
LSDB	Link-state adevertisement,
LSU	Link State Update
MAC	Media Access Control
MAD	Multi-active detection
MBPA	Modbus Application Protocol Header
MDT	Master Data Telegrama
MED	Multi-Exit-Discrimin
MES	Manufacturing Execution Systems
MIB	Management Information Base
Modbus	Modicon Bus
MPU	Main Processing Unit
MQC	Modular QoS Command-Line
MSTI	Multiple Spanning Tree Instance
MSTP	Multi Spanning tree protocol

NSSA	Not-So-Stubby Area
NTP	Network Time Protocol
ODVA	Open DeviceNet Vendors Association™
OID	Object Identifier
OSI	Open Systems Interconnect
OSPF	Open short path first,
PDH	Plesiochronous Digital Hierarchy
PLC	Programmable Logic Controller
PQ	Priority Queuing
PTP	Precisión Time Protocol
QoS	Quality of Service
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid spanning tree protocol
RTCP	Real-Time Control Protocol
RTP	Real-time Transport Protocol
SCADA	Supervisory Control And Data Acquisition
SCNM	Slot Communication Network Management
SDH	Synchronous Digital Hierarchy
SEP	Smart ethernet protection
SERCOS	Serial Real-Time Communication System
SIP	
SNTP	Simple Network Time Protocol
SPF	Shortest Path First
SPT	Shortest Path Tree
STP	Spanning tree protocol
TC	Topology change
TCP	Transmission Control Protocol
TSN	Time sensitive networking
UDP	User Datagram Protocol
UAC	User Agent Clients
UAS	User Agent Servers
VLAN	Virtual LAN

VRRP	Virtual Router Redundancy Protocol
WFQ	Weighted Fair Queuing
WRR	Weighted Round Robin

Bibliografía

[1] A. Atlas, Ed, *Basic Specification for IP Fast Reroute: Loop-Free Alternates RFC 5286*, 2008

[2] ANDREW S. TANENBAUM, *Redes de computadoras*,2003

[3] M. Herrero, A. López, *Protocols and network security in ICS infrastructures*, INCIBE, 2015.

[4] Beckhoff, *Manual EAP Twincat* 3, 2018

[5] Beckoff, *CX8090 Embedded PC for Ethernet*, 2018

[6] Cisco, *Deploying IP Fast Reroute for ISIS, OSPF, and BGP*, 2010

[7] Cisco, *Guía de diseño de OSPF*, 2005

[8] David Romero, *Evaluación de alternativas en la aplicación de Spanning Tree Protocol*, 2008

[9] EtherCAT Technology Group, *EtherCAT and TSN – Best Practices for Industrial Ethernet System Architectures*, 2018

[10] EtherCAT Technology Group, *EtherCAT forFactory Networking, EtherCAT Automation Protocol (EAP)*, 2010.

[11] EtherCAT Technology Group, *Industrial Ethernet Technologies*, 2014

[12] Gunnar Prytz, ABB AS Corporate Research Center, *A performance analysis of EtherCAT and PROFINET IRT*, 1-4244-1506-3/08 2008 IEEE

[13] György Kálmán, *Quality of Service in Ethernet Networks*, 2013

[14] Beckoff, *EtherCAT Communication*, 2007.

[15] Huawei, *AR550 V200R005C70 Configuration Guide - Reliability*, 2019

[16] Huawei, *AR550 V200R008 CLI-based Configuration Guide - IP Unicast Routing*, 2019

[17] Huawei, *AR550 V200R010 CLI-based Configuration Guide - Ethernet Switching*, 2019

[18] Huawei, *CSS Technology White Paper*, 2013

[19] Laboratorio de Redes, *Calidad de servicio*, Universidad Nacional de Lujan.

[20] Huawei, *QoS Technology White Paper*, 2013

[21] Huawei, *SEP Technology White Paper*, 2013

[22] Huawei, *Virtual Router Redundancy Protocol (VRRP) White Paper*, 2012

[23] Industrial Ethernet Facts, *System Comparison, the 5 Major Technologies*, 2015.

[24] IXIA, *Measuring Network Convergence Time*, 2014

[25] J. Babiarz, *Configuration Guidelines for DiffServ Service Classes*, RFC 4594, 2006

[26] J. Moy, *OSPF Version2*, 1998

[27] James T, *Yu Measuring Failover time for High Avaibility Network*,2018

[28] Jorge Sandoval, *Implementación de QoS*, Catedra MIRC U. de Chile, 2016

[29] Kingstar, *White Paper 5 Real-Time*, Ethernet-BasedFieldbuses Compared

[30] Ledisi G. Kabari, Onwuka C. Ugochukwu , *Comparative Analysis of OSPF, Rip And EIGRP Convergence Time Using Riverbed Modeler*, University of Education, Port Harcourt

[31] Mark Hantel, Günter Steind, Jordon Woods, *New Ethernet Applications – Industrial Networking Requirements*, 2018

[32] Modbus-IDA, *MODBUS Messaging on TCP/IP Implementation Guide V1.0b*, 2006

[33] Mukul Goyal, Mohd Soperi, Improving Convergence Speed and Scalability in OSPF: A Survey, 2012 IEEE

[34] network faculty, www.networkfaculty.com.

[35] Omid Givehchi, Jahanzaib Imtiaz, Henning Trsek and Juergen Jasperneit, *Control-as-a-Service from the Cloud: A Case Study for using Virtualized PLCs*, University of Applied Sciences, D-32657 Lemgo, Germany

[36] Palláres, Aplicación *de Técnicas de Sincronismo para Sistemas de Medida Distribuidos y Desarrollo de un Medidor Fasorial basado en el protocolo IEEE1588*, 2012.

[37] Prado, Ethernet Industrial: *Modelos y conectividad en el ámbito de procesos industriales*, 2010

[38] PROFIBUS, International *Profinet Real-Time Communication*

[39] https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-bigger-than-fieldbuses, accedido el 04 de junio de 2019

[40] Reinhard Langmann, Leandro F. Rojas-Peña, *A PLC as an Industry 4.0 component* , 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV)

[41] Ricardo Prado, *Convergencia en Protocolos de Ruteo IGP*, Webcast, 2014

[42] Richard Zurawski, *Industrial Communication Technology Handbook*,2015

[43] Rockwell, Cisco, *Deploying a Resilient Converged Plantwide Ethernet Architecture*, 2018

[44] https://us.profinet.com/profinet-network-geeks-want/ , accedió el 05 de mayo de 2019.

[45] ODVA, *Common Industrial Protocol (CIP) And The Family Of Cip Networks*, 2016.

[46] Wayne Qiu, *Future Industrial Network Requirement Discussion for TSN*, St. John's NL 2017

[47] Wikipedia, *SERCOS III*, https://es.wikipedia.org/wiki/SERCOS_III

[48] Yonas Tsegaye , *Tewodros Geberehana, OSPF Convergence Times*, UNIVERSITY OF TECHNOLOGY Göteborg, Sweden, 2012

[49] v. Manral, *Benchmarking Basic OSPF Single Router Control Plane Convergence*, RFC 4061, 2005.

[50] Vasileios Papadopoulos, *Experimental Assessment of Benchmark-oriented Network Traffic Generators*, Universidad Carlos III de Madrid.

[51] Beckhoff, EtherCAT System Documentation, 2018.

[52] http://telescript.denayer.wenk.be/~hcr/cn/idoceo/tcp_header.html, accedido el 8 de octubre de 2019.

[53] https://es.wikipedia.org/wiki/Protocolo_de_control_de_transmisi%C3%B3n, accedido el 8 de octubre de 2019.

[54] http://telescript.denayer.wenk.be/~hcr/cn/idoceo/udp_header.html, accedido el 8 de octubre de 2019.

[55] https://www.youtube.com/watch?v=4QRJZQYpdGU, accedido el 9 de octubre de 2019.

[56] https://www.oreilly.com/library/view/http-the-definitive/1565925092/ch04s01.html., accedido el 9 de octubre de 2019.

[57] S. Castro, *Administración de redes y SNMP*, Universidad de Chile, 2006

[58] NSRC, *Gestión de Redes, Introducción a SNMP*.

[59] Adrián García, *Implementación de un agente extensible SNMP sobre la plataforma Raspberry Pi para la simulación de MIB propietarias, Universidad de Cantabria*, 2015.

[60] https://support.huawei.com/enterprise/en/doc/EDOC1100086963, accedido el 10 de septiembre de 2019.

[61] https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html , accedió el 11 de septiembre de 2019.

[62] B. Rojas, *Análisis del Impacto de la Telefonía IP Sobre Operadores de Telefonía Móvil*, Universidad de Chile, 2007.

[63] José Joskowicz, *Voz Video y Telefonía sobre IP, Universidad de la República*, Uruguay, 2012

[64] *https://serverfault.com/questions/819450/call-flow-explanation*, accedido el 13 de septiembre del 2019

[65] J. Michell, G. Ruiz, *Compresión de Víde*, Universidad de Cantabria.

[66] Polycom, *H.264 de perfil alto (High Profile)*, 2010.

[67] AXIS Communications, *Guía técnica de vídeo IP*, 2008.

[68] https://www.networkwebcams.co.uk/blog/2009/04/03/h264-video-compression-in-ip-video-surveillance-systems/ , accedió el 14 de septiembre de 2019.

[69] https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-bigger-than-fieldbuses, accedió el 25 de septiembre de 2019.

[70] R. Hinden, *Virtual Router Redundancy Protocol (VRRP)*, 2004

[71] http://bibing.us.es/proyectos/ abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf, accedido el 23 de mayo de 2019.

[72] Wang Zejia, *Measurement of Spanning Tree performance between different protocols*, 2014

[73] https://es.wikipedia.org/wiki/SERCOS_III, Accedo el 05 de junio de 2019.

[74] Huawei, *AR500, AR510, AR531, AR550, AR1500, and AR2500 V200R010 Product Documentation*, 2019.

[75] https://infosys.beckhoff.com/english.php?content=../content/1033/tcadscommon/html/tcadscommon_intro.htm&id=, accedido el 06 de junio de 2019.

[76] http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=8, accedido el 10 de julio de 2019.

[77] https://support.huawei.com/enterprise/my/doc/EDOC1000141879/32a400ec/fundamentals-of-ospf, accedido el 8 de julio de 2019.

[78] Huawei, *BGP Feature and Configuration*, 2012

[79] Huawei, Ethernet Link Aggregation, 2012

[80] https://support.huawei.com/enterprise/en/doc/EDOC1100065681/3e33f422/understanding-priority-mapping, accedido en 12 de julio de 2019.

[81] https://forum.huawei.com/enterprise/es/qos-problemas-problema-3-implementaci%C3%B3n-qos-clasificaci%C3%B3n-de-tr%C3%A1fico-simple-y-re-marcado/thread/487225-100237, accedido el 11 de julio de 2019.

[82] Huawei, *MSTP Technology White Paper* , 2012

[83] https://slideplayer.com/slide/6203781/, accedido el 20 de julio de 2019.

[84] Sergio Miranda, *Introducción*, Catedra Seguridad en Redes MIRC U. de Chile, 2016.

[85] Sergio Miranda, *Criptografía*, Catedra Seguridad en Redes MIRC U. de Chile, 2016.

[86] Sergio Miranda, *Filtros de paquetes y Firewalls*, Catedra Seguridad en Redes MIRC U. de Chile, 2016.

[87] Sergio Miranda, *IPSec, SSL, SSH, VPN*, Catedra Seguridad en Redes MIRC U. de Chile, 2016.

[88] Sergio Miranda, *Malware*, Catedra Seguridad en Redes MIRC U. de Chile, 2016.

[89] https://www.incibe-cert.es/en/blog/iec62443-evolution-of-isa99, accedido el 25 de septiembre de 2019.

[90] INCIBE, *Protocols and network security in ICS infrastructures,*

[91] J. Castillo, *Estableciendo zonas y Conductos, Según estándar ISA99/IEC6443*, 2018

[92] J. Garcia, *Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con énfasis en el sector energético*, Universidad Oberta de Catalunya, 2017

[93] K. Astudillo, Hacking Ético 101, 2013.

[94] Huawei, *Agile Campus Network Solution Design Guide and Best Practices*, 2018

[95] NIST, *Special Publication (SP) 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security*, 2015.

[96] https://www.arxys.com/bandwidth-storage-calculator/, accedido el 05 de octubre de 2019.

[97] http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion2.html, accedido el 19 de octubre de 2019.

Anexo A Recomendaciones de Ciberseguridad para el caso práctico.

Como se indicó en el caso práctico se debe realizar un diseño y propuesta de configuración para que los diferentes subsistemas logren comunicarse cumpliendo los requerimientos establecidos, dentro de los cuales no se considera la seguridad, dejando esta tarea a la red administrativa.

En esta directriz no se pretende abordar todos los aspectos de la Ciberseguridad para un ICS ya que para esto habría que elaborar el plan de seguridad, elegir las políticas, y guiar la implementación de todos los Subisistemas, lo que puede implicar una Tesis completa. Solo se quiere dar una orientación a como implementar la seguridad en la Red ITS y en los equipos networking que la componen, además de agregar algunas recomendaciones generales para los diferente ssubisistemas.

Como se indicó en el punto 2.6.4 existen varios organismos estandarizares y guías de diseño para implementar la seguridad en una red que comunique los subsistemas de un ICS, en el presente caso se tomará como guías principales el documento 800-82 del NIST y las recomendaciones del ICS-CERT, básicamente por su facilidad de acceso a información y la gratuidad en la misma.

Al no tener el detalle de la implementación de los diferentes Subsistemas, se realiza un ejemplo acotado de modo orientativo en base a la información que se tiene del proyecto más la revisión de los antecedentes previos.

Una puesta en servicio del ICS que garantice la seguridad debe tener la implementación de cada subsistema debidamente documentadas, con aspectos como los protocolos de comunicación que usan, interacción con otros subsistemas, detalle de puertos, flujo de comunicaciones entre los diferentes dispositivos, necesidad de comunicaciones a nivel de enrutamiento y sobre todo si existen conexiones externas.

En primer punto se realiza una caracterización de los diferentes Subisistemas desde el punto de vista de la seguridad en base a la tabla 5-1 y de la recomendación del NIST, además para la tabla se tomaron en cuenta aspectos como:

- El sistema de detección de incendios funciona conectado a extinción de incendios de manera independiente de la red de comunicaciones, por lo que su desconexión si bien causa un daño de que los operadores en el Centro de Control no verán la alarma los sistemas locales de sonorización y cámaras ayudarán a la detección, por lo que su dependencia no genera un riesgo alto.
- La administración de la red es sumamente importante debido a que podría poner en peligro cualquier subsistema que se comunique por la red.

- Un ataque de DoS sobre el sistema de telefonía, tiene como alternativas la red celular siempre y cuando exista cobertura, si su confidencialidad o integridad son vulnerados y por ejemplo se intenta dar indicaciones falsas a un operador siempre estará la comprobación por la voz del propio operador.
- Una falta de disponibilidad de cámaras en los accesos y del sistema DAI es muy relevante para la seguridad.
- El subsistema de Control y ventilación es fundamental su funcionamiento ya que tiene conexiones por entrada libre de potencia y monitoreo de las variables análogas de los sistemas.

N° subs	Subsistema	Sigla	Protocolos Principales	Flujo de tráfico principal	Pri.	Confidencialidad	integridad	disponibilidad
10	Subsistema de Control y Ventilación	SCCV	TCP / ModbusTCP	Bidireccional	1	ALTA	ALTA	ALTA
11	Subsistema de Gestión de Red	SGDR	UDP/ SNMPv2/ HTTP /SSH	Ascendente	5	BAJO	MODERADO	ALTA
12	Subsistema de Telefonía	STEL	UDP/RTP, RTCP/SIP	Bidireccional	9	BAJO	MODERADO	MODERADO
13	Subsistema Detección de Incendios	SDTI	TCP / ModbusTCP/ HTTP	Bidireccional	3	BAJO	MODERADO	BAJO
14	Subsistema de Radiocomunicaciones	SRAD	UDP/SNMPv2/HTTP	Ascendente	7	BAJO	MODERADO	MODERADO
15	Subsistema de Control iluminación	SILU	UDP/SNMPv2/HTTP	Bidireccional	11	BAJA	BAJO	MODERADO
16	Subsistema de control energía de baja tensión	SCBT	UDP/Profinet/HTTP	Ascendente	10	BAJO	BAJO	MODERADO
17	Subsistema de Postes SOS	SSOS	UDP/TCP/RTP, RTCP/SIP /ModbusTCP / HTTP	Bidireccional	2	ALTA	MODERADO	MODERADO
18	Subsistema de Megafonía	SMEG	UDP/RTP, RTCP/SIP /HTTP	Descendente	6	BAJO	MODERADO	MODERADO
19	Subsistema de Señalización de tráfico	SGTR	TCP / ModbusTCP/ HTTP	Bidireccional	8	BAJO	BAJO	BAJO
20	Subsistema de Circuito Cerrado de Televisión	SCTV	UDP/ RTP, RTCP / HTTP	Ascendente	12	BAJO	BAJO	BAJO
21	Subsistema de Detección Automática de Incidentes	SDAI	UDP/ RTP, RTCP / HTTP	Ascendente	4	BAJO	MODERADO	BAJO
	Tráfico de Control		BGP/SEP/VRRP		1	MODERADO	ALTO	MODERADO

II. Identificación de Vulnerabilidades:

A. Vulnerabilidades detectadas en los subisistemas

- Ninguno de los subsistemas utiliza protocolos seguros.
- ModbusTCP y Profinet no cuentan con mecanismos de autenticación.
- El subsistema de gestión de la red está solicitado con protocolo SNMPv2 el cuál no tiene cifrado.
- Varios de los equipos en los Subsistemas tienen acceso vía http para configuración.
- Existirá interconexión entre los sistemas de Megafonía, Radiocomunicaciones, SOS y telefonía.
- El sistema de radiocomunicaciones tiene una interfaz inalámbrica, si bien su tráfico no es ethernet sino de DMR es un posible acceso al equipo.
- El sistema de Radiocomunicaciones tendrá conexión tanto a la red corporativa como a la red propia de radiocomunicaciones.
- Se piensa en la integración de postes SOS a la red e internet móvil lo cual es un punto de acceso muy riesgosos
- Todos los subsistemas son especialidades distintas, por lo tanto, especialistas y computadoras distintas estarán conectados a la red, al menos en la puesta en marcha.
- Los protocolos de control de Red VRRP y BGP no están implementados de manera segura.

B. Vulnerabilidades en Arquitectura de Red:

La red actual tiene una arquitectura como la indicada en la figura A-1.

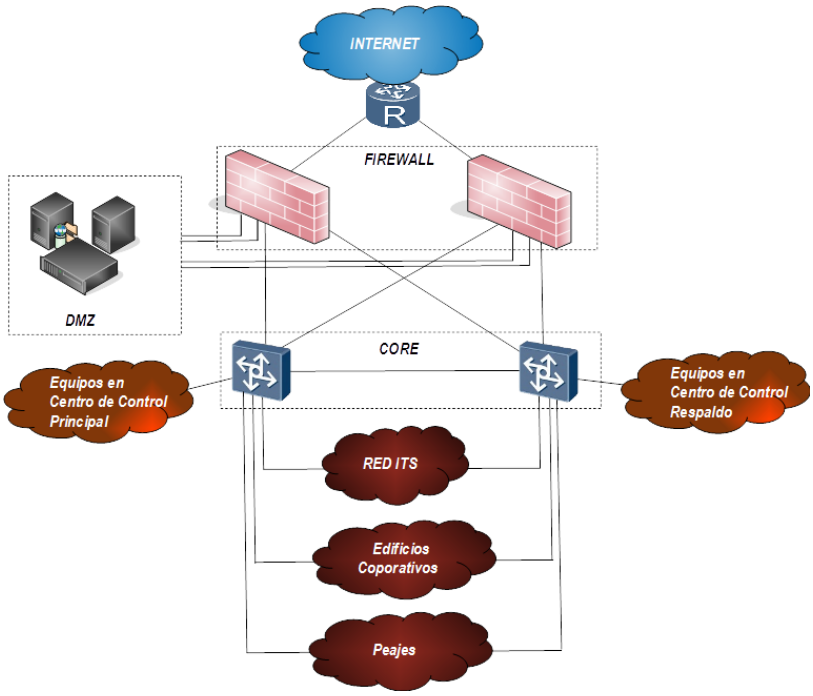


Figura A- 1 Arquitectura actual red ICS

- Los equipos del Centro de Control se conectan directamente al switch de Core.
- Existen otras redes dentro del sistema fuera de los equipos que hacen funcionar el ITS, por lo que la red ITS no se encuentra aislada.
- Los edificios corporativos y la red de los peajes manuales se conectarán directamente al Core mediante una conexión capa 3, interconectando todas las redes.
- Los servidores de los subsistemas ITS y los de servicios corporativos están dentro de la misma DMZ.

III. Mejoras en Seguridad

Un ataque a la red ITS se puede realizar desde dentro de la red o desde afuera, la seguridad perimetral se encargará de evitar los ataques desde el exterior, pero ataques internos no son una anormalidad, ya sea contaminando con virus máquinas que se conecten a la red como los computadores de soporte de las diferentes especialidades, virus que residan en los mismos equipos en el software de los PLCs y/o en servidores web o mediante la conexión física directa a la red que se dificulta al ser una red cableada, todas las formas antes indicadas son ataques muy elaborados, pero al ser un ITS un ICS atractivo para un ciberataque estos aspectos, sumados a ataques 0-day deben ser contemplados, por lo cual el primer punto de mejora es tener un plan de recuperación de desastres debidamente documentado, elaborado por un equipo multidisciplinario, ya que aunque se intente mejorar la seguridad constantemente el riesgo siempre existirá.

Recomendaciones generales a la compañía:

- Que la información del sitio web de la autopista se mantenga secreta y que no sea publicada en páginas web como Who-Is que entregan información valiosa para un atacante, es común que los NIC locales ofrezcan el servicio de mantener dicha información privada.
- Educar constantemente al personal en el uso de las herramientas informáticas dentro de la compañía, respetar las políticas impuestas en el plan de seguridad, especialmente a los ataques de Ingeniería social como Phishing.
- Que el plan de seguridad que se implemente tenga el auspicio del máximo representante de la compañía.
- Tener contactos identificados de CERT local y deseablemente con algún CERT especializado.
- Ocupar todos los subsistemas para implementar la seguridad, por ejemplo, una alarma de desconexión de un cable de un equipo de red puede ser complementada con la cámara que apunte al sector.

A. Mejoras de seguridad en Arquitectura y equipos de Red:

Lo primero que se propone es el cambio de algunos aspectos en la arquitectura de la red que implica el aumento de equipos en algunos puntos, pero es mandatorio para poder mejorar la seguridad actual.

1. Cambios en la arquitectura:

i. Los switches de Core son sumamente importante en la configuración de la red, por lo que una falla en estos podría traer graves consecuencias para el funcionamiento de las comunicaciones por lo que en cada Centro de control se deben incluir switches concentradores para la conexión de los equipos terminales y dicho switch se conectará en con el Core capa 3, restringiendo el acceso primero en el switch.
ii. Las redes de peajes y edificios corporativos deben conectarse a los Firewalls actuales antes de conectarse al Core.
iii. Se deben agregar 2 Firewalls con servicios de IDS para la conexión de la red ITS hacia al Core evitando el ingreso de tráfico a la red ITS desde otras redes. Está implementación le quitará throughput a la comunicación.

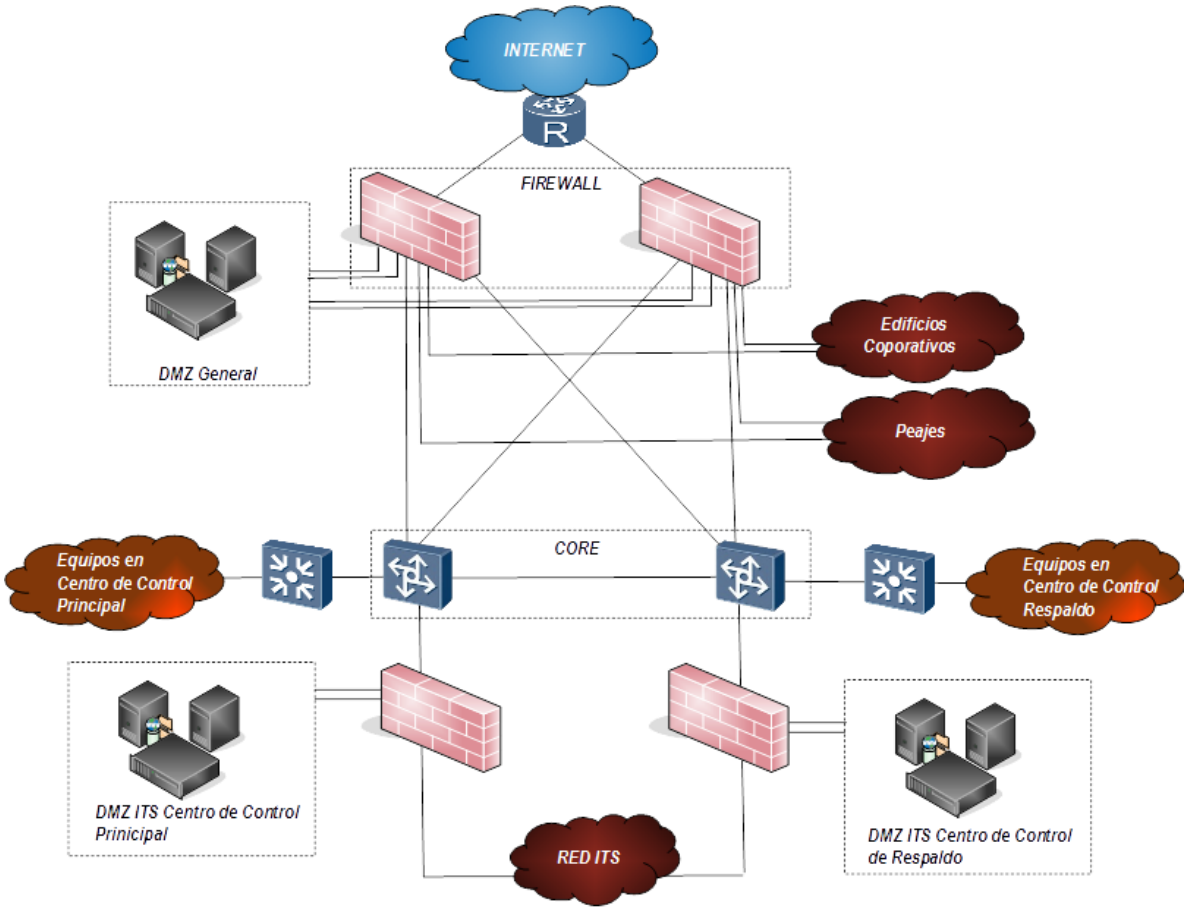


Figura I- 2 Arquitectura Propuesta

B. **Mejoras de seguridad en la implementación de los diferentes subsistemas:**

Como se indicó anteriormente se desconoce la implementación exacta de cada subsistema, por lo que a continuación se señalan una serie de recomendaciones a tener en cuenta a la hora de su puesta en servicio y elaboración del plan de seguridad:

- Debe documentarse todas las interacciones y características de cada subsistema.
- Cada servidor debe tener al menos 3 Roles para los diferentes usuarios con permisos acotados y específicos para cada perfil. Idealmente utilizar los mismos Roles presentes en el sistema operativo a fin de mantener una jerarquía ordenada y manejable.
- Cada subsistema debe contar con un modo degradado de funcionamiento en caso de perder conexión con su servidor principal o Maestro.
- Los servidores de cada subsistema deben tener un registro de gestión de cambios y debe tener copias de seguridad de su configuración en el último estado autorizado.

- Disponer de las últimas actualizaciones oficiales de los sistemas operativos de todos los hosts de la red.
- Deshabilitar actualizaciones automáticas, para testear dichas actualizaciones antes de implementarlas y empezar la explotación
- Habilitar los Firewall de los sistemas operativos, solo permitiendo el tráfico entrante y saliente que sea expresamente necesario
- Desinstalar aplicaciones, servicios de sistema y protocolos de sistema no operativos o no utilizados.
- Contar con antivirus en todos los servidores.
- Definir e imponer restricciones para evitar la instalación no autorizada de software.
- Debe existir un inventario de todos los equipos con su número de parte y MAC.
- Se recomienda autenticación mutua entre dispositivos a fin de evitar que producto de ataques Man-in-the- Middle se puedan realizar cambio de estado de ciertas alarmas, variables o datos trayendo como consecuencia acciones indeseables del operador.
- Evitar el acceso remoto y de ser indispensable debe hacerse mediante SSH o algún otro protocolo remoto que funcione sobre SSL o TLS
- Evitar acceso a la configuración de los diferentes equipos de la red mediante HTTP.
- En el caso de usar autenticación centralizada tipo RADIUS o similar, las contraseñas deben almacenarse en forma de hash.
- No se permitirá la notificación de alarmas mediante correo desde los equipos terminales, está tarea solo se les permitirá a los servidores de manera particular.
- La implementación de equipos presentes en la red ITS a la red de telefonía móvil, debe estar prohibida y solo se hacerse en casos estrictamente necesarios para resguardar la vida de las personas y siempre mediante un firewall administrado centralizadamente.
- Evitar implementaciones tipo OPC DCOM debido a su aleatoriedad en la asignación de puertos, si se permite el servidor OPC debiese estar dentro de la red ITS por detrás del firewall.
- En caso de tener que utilizar transferencia de archivos tipo FTP, se preferirá protocolos como *Secure FTP (SFTP)* o *Secure Copy (SCP).* si no son soportados el tráfico FTP solo se permitirá dentro de la red ITS, no se permitirá el ingreso y la salida solo será mediante un túnel cifrado.
- En caso de que la red corporativa necesita tener acceso a los datos en los servidores de los subsistemas, los servidores se ubicarán en la DMZ y no dentro de la red ITS para evitar el ingreso a la red ITS de protocolos como http y SQL que pueden ser ocupados por los atacantes desde una red externa a la del ITS.
- Los equipos networking de red ITS no realizaran cifrado dentro de la red ITS ya que es perjudicial para su rendimiento, en caso de necesitarse y que las aplicaciones no soporten SSL o TLS se debe implementar caso a caso.
- No se permitirán conexiones inalámbricas a los equipos en cualquiera de los Subsisitemas.

1. Mejoras de configuración para todos los Switches:

- Se debe activar AAA para la autenticación en cada equipo, se recomienda el cambio mensual de las contraseñas, especialmente en el Core.
- Se proponen en 3 tipos de roles operador, mantenimiento, administración, sobre los que se crearán los diferentes usuarios. Los usuarios con rol de administrador deben ser sumamente limitados y con los conocimientos necesarios y debe ser el único que podrá realizar cambios en la configuración de los equipos.
- Se debe mantener apagadas todas las interfaces que no estén en uso y solo se habilitarse a través de una solicitud formal según las políticas que se platee la compañía.
- Permitir el acceso remoto por SSH a todos los equipos de red, permitiendo las conexiones remotas solamente desde la IP del NMS de gestión a fin de asegurar que ninguna otra plataforma pueda realizar algún cambio en los equipos.
- No permitir el uso de DNS dentro de la red ITS.
- Se recomienda configuración estática de direcciones, si en algún periodo de la explotación de la red esto sufre cambios y se debe hacer dinámicamente mediante DHCP, se debe activar en los equipos de Red la protección DHCP *Snooping* que permite configurar interfaces de confianza por las cuales se recibirán las propuestas enviadas por el servidor DHCP, denegando el acceso (cancelando el *ACK DHCP*) a los servidores que envíen su propuesta por interfaces que no sean de confianza.
- Para evitar DoS por ataques DHCP/ARP se recomienda configurar perfiles de tráfico máximo para estos protocolos usando ACLs y perfiles, por ejemplo, regular el tráfico de salida a ARP o DHCP, al hacer *match* con la ACL se asignan valores máximos para uno o varios de parámetros como CIR, PIR, CBS o PBS.
- No se recomienda el uso de http, si es necesario solo podrá funcionar dentro de la red ITS en caso de que conexiones necesiten ingresar a la red ITS se deben aplicar controles de origen y destino.
- Los servidores de los subsistemas del ITS se ubicarán en DMZ y se debiesen conectarse directamente al Firewall, en caso de que este no cuente con las interfaces suficientes se utiliz un switch de agregación como concentrador.
- En general cualquier tipo de ataque de la red ITS se basará en que previamente el atacante pueda capturar tráfico de la red, como no exisitrá una red inalámbrica para hacerlo deberá conectarse a algún switch de la red por lo que los controles de acceso a estas ubicaciones deben ser restringidos y complementados por cámaras.

2. Mejoras para Switches de Acceso

Seguridad Física: Los switches de acceso estarán principalmente instalados en los gabinetes de los postes SOS al igual que otros equipos de los diferentes Subisistemas, lo que implica que ante falla de cualquiera de los equipos dentro del gabinete, él personal interno o externo que realice la reparación tendrá acceso directo al switch, además estos gabinetes estarán repartidos a lo largo de la autopista en ubicaciones geográficas separadas por lo cual serán más vulnerables al acceso de un tercero. Si bien ambos problemas antes descritos se pueden aplacar si se respetan las políticas de seguridad, los ataques a un ICS suelen ser

elaborados y en ocasiones cuentan con cooperación interna de las compañías, por lo cual los diferentes métodos de seguridad como cámaras que apunten a los postes SOS, alerta de apertura de puertas o alertas en el NMS por alguna desconexión de cable son útiles para evitar este tipo de ataques.

- Realizar filtros por MAC mediante ACL para evitar ataques man in the middle por ARP spoofing. Además de mejorar la seguridad permitirá manejar la red con mayor orden.
- Activar chequeo de los paquetes ARP para que se envíe una alarma al recibir solicitudes ARP que no se encuentren en su tabla.
- Configurar supresión de las tormentas de broadcast para evitar la caída de la red por algún error producido por un cambio de configuración mal realizado.

3. Mejoras para Switches de Agregación

Seguridad Física: Los switches de agregación estarán principalmente instalados en las salas eléctricas y centros de control, por lo cual solo personal autorizado que tenga la llave del rack y autorización de ingreso a estas zonas debe tener acceso a los equipos.

- Realizar filtros por MAC mediante ACL en las conexiones capa 2 del switch con el fin de evitar ataques man-in-the-middle por ARP spoofing. Además de mejorar la seguridad permitirá manejar la red con mayor orden.
- Se sugiere utilizar autenticación de VRRP con clave cifrada para que si algún atacante logre realizara capturas de tráfico no pueda realizar cambios en la configuración del protocolo.
- Se propone la implementación de MD5 para la autenticación para el protocolo de enrutamiento BGP.
- Activar la protección de CPU para que en caso de que un atacante logre burlar la seguridad no pueda realizar un ataque de denegación de servicio DoS por saturación, como por ejemplo los ataques de *Ping Flooding*, *Smurf* o *SYN flooding*.

4. Mejoras para Switches de Core

Seguridad Física: Los switches de Cores estarán en los centros de control por lo que el acceso a estos será en función del acceso al centro de control.

- Activar la protección de CPU para que en caso de que un atacante logre burlar la seguridad no pueda realizar un ataque de denegación de servicio DoS por saturación, como por ejemplo los ataques de *Ping Flooding*, *Smurf* o *SYN flooding*.
- Se propone la implementación de MD5 para la autenticación para el protocolo de enrutamiento BGP.

5. Recomendaciones para Firewalls fuera de la red ITS.

- Se recomienda una política restrictiva, ósea se negará todo el tráfico a menos que se configure directamente.
- Se recomeinda deshabilitará cualquier tipo de acceso remoto
- La conexión a la DMZ se configurará primariamente por número de puerto de la capa de transporte.
- Se habilitará la opción de IPS en el firewall la cual disminuirá el rendimiento per mejorará la seguridad.
- Se activará la protección de antivirus, siendo muy importante mantener actualizada la base de datos debido a la creación de nuevos malwares.

6. Recomendaciones para Firewalls red ITS

- Se aplicará una política restrictiva, ósea se negará todo el tráfico a menos que se configure directamente.
- Los filtros se harán por direcciones IP y/o números de protocolo IP y/o puertos TCP/UDP, en el orden antes indicado.
- Se prohibirá le tráfico ICMP de entrada a la red ITS, solo permitiéndose en casos particulares a través de ACLs, evitando que un atacante pueda obtener información relevante y evite ataques como ping flood y smurf attack. Incluso Ping of death dado que algún subisistema pueda manejar equipos con sistemas operativos obsoletos.
- Se bloqueará el tráfico HTTP de ingreso, solo se permitirá en casos específicos luego de solicitudes formales y docmuentadas.
- Se habilitará la opción de IPS/IDS en el firewall la cual disminuirá el rendimiento per mejorará la seguridad.
- Solo se permitirá la salida de tráfico desde la Red ITS desde IPs especificas a través de ACLs.
- Si personal de los niveles ERP o MES necesitan hacer acceso a la DMZ del ITS se hará mediante un proceso documentado y caso a caso.
- El soporte vía remota de los equipos solo se permitirá con conexiones por un canal cifrado que pasen primariamente por el firewall que aísla de DMZ general y luego por el Firewall ITS siempre por un c. solo se permitirá en casos específicos luego de solicitudes formales y documentadas.

7. Recomendaciones para NMS

- Se sugiere para las comunicaciones desde y hacia el NMS SNMP v3c que otorga un mayor grado de seguridad que sus versiones anteriores, utilizando comunicaciones cifradas.
- El acceso al NMS vía browser será limitado por IP y MAC, mediante ACLs.
- Se utilizará primeramente el tipo autenticación local del NMS, pero podrá ser habilitada la autenticación remota por Radius o LDAP si se requiere y se habilita en el subsistema del Centro de Control.

- Se realizará el cambio de password por defecto de todos los niveles de la aplicación, desde el acceso a BIOS, base de datos y los referentes a los roles.

Anexo B Distribución de equipos en switches de acceso.

Equipo		Subsisitema
CTVI	Cámara Indoor estática	SCTV
CTVO	Cámara Outdoor estática	SCTV
CTVOM	Cámara Otdoor Movimiento	SCTV
DAII	Cámara DAI Indoor estática	SDAI
DAIO	Cámara DAI Outdoor estática	SDAI
SCCV	Cabecera de entradas y salidas	SCCV
STEL	Teléfono en campo	STEL
SDTI	Centrales detectoras	SDTI
SRAD	Maestros y Esclavos de Radiocomunicaciones	SRAD
SILU	Equipos Remotos de Control de Iluminación	SILU
SCBT	PLCs del subsistema	SCBT
SSOS	Postes SOS	SSOS
SMEG	Equipos concentradores de Megafonía	SMEG
SGTR	Equipos de señalización dinámica.	SGTR

Tabla B-1 Nomenclatura en Tabla II-2 de equipos conectados a switches

	Min mbps	Avg mbps	Máx mbps	1	2	3	4	5	6	7	8	9	10	11	12
A10-SACC-01	4.4	7.9	14.0	CTVO-01	DAIO -01	SCCV-01	SILU-01	SSSOS-01							
A10-SACC-02	3.1	4.9	7.9	CTVO-02	SCBT-01	SILU-02	SSSOS-02	SSTEL-01							
A10-SACC-03	7.3	14.3	16.3	CTVOM-03	SCCV-02	SILU-03	SSOS-03	SRAD-01							
A10-SACC-04	2.2	3.9	7.0	CTVO-04	SILU-04	SSOS-04									
A11-SACC-01	4.5	8.0	14.1	CTVO-05	DAIO -02	SCCV-03	SILU-05	SSOS-05							
A11-SACC-02	6.9	14.0	16.0	CTVOM-06	SILU-06	SSOS-06									
A11-SACC-03	8.4	15.5	17.5	CTVOM-07	SCCV-04	SGTRR-01	SCBT-02	SILU-07	SDTI-01	SSOS-07	STEL-02	SMEG-01			
A11-SACC-04	4.5	8.2	14.5	CTVI-08	DAII -03	DAII -77	SGTR-02	SILU-08	SDTI-02	SSOS-08					
A11-SACC-05	5.0	8.6	15.1	CTVI-09	CTVI-86	DAII -04	DAII -78	SCCV-05	SGTR-03	SGTR-43	SILU-09	SDTI-03	SSOS-09	SMEG-02	
A11-SACC-06	3.5	5.9	10.2	CTVI-10	DAII -05	SCCV-06	SGTR-04	SGTR-44	SILU-10	SDTI-04	SSOS-10	SRAD-02			
A11-SACC-07	3.2	5.7	10.0	CTVI-11	CTVI-87	DAII -06	SGTR-05	SILU-11	SDTI-05	SSOS-11	SMEG-03				
A11-SACC-08	5.0	8.7	15.1	CTVI-12	DAII -07	DAII -79	SCCV-07	SCCV-80	SGTR-06	SILU-12	SDTI-06	SSOS-12	SSOS-85		
A11-SACC-09	6.0	9.7	16.1	CTVI-13	DAII -08	DAII -80	SCCV-08	SGTR-07	SCBT-03	SILU-13	SDTI-07	SSOS-13	STEL-03	SMEG-04	
A11-SACC-10	4.8	8.5	14.8	CTVI-14	CTVI-88	DAII -09	DAII -81	SCCV-09	SGTR-08	SILU-14	SDTI-08	SSOS-14			
A11-SACC-11	5.2	8.9	15.4	CTVI-15	DAII -10	DAII -82	SCCV-10	SCCV-81	SGTR-09	SGTR-45	SILU-15	SDTI-09	SSOS-15	SSOS-86	SMEG-05
A11-SACC-12	3.6	6.1	10.4	CTVI-16	DAII -11	SCCV-11	SCCV-82	SGTR-10	SGTR-46	SILU-16	SDTI-10	SSOS-16			
A11-SACC-13	3.6	6.0	10.4	CTVI-17	DAII -12	SCCV-12	SGTR-11	SGTR-47	SILU-17	SDTI-11	SSOS-17	SMEG-06			
A12-SACC-01	3.7	6.2	10.5	CTVI-18	DAII -13	SCCV-13	SCCV-83	SGTR-12	SGTR-48	SILU-18	SDTI-12	SSOS-18	SMEG-07		
A12-SACC-02	5.0	8.7	15.1	CTVI-19	CTVI-89	DAII -14	DAII -83	SCCV-14	SCCV-84	SGTR-13	SGTR-49	SILU-19	SDTI-13	SSOS-19	STEL-04
A12-SACC-03	3.5	6.0	10.3	CTVI-20	DAII -15	SCCV-15	SGTR-14	SGTR-50	SILU-20	SSOS-20	SMEG-08				
A12-SACC-04	4.4	6.9	11.2	CTVI-21	DAII -16	SCCV-16	SGTR-15	SGTR-51	SCBT-04	SILU-21	SSOS-21	SRAD-03	STEL-05		
A12-SACC-05	3.5	6.0	10.3	CTVI-22	DAII -17	SCCV-17	SGTR-16	SGTR-52	SILU-22	SSOS-22	SMEG-09				
A12-SACC-06	4.8	8.5	14.8	CTVI-23	CTVI-90	DAII -18	DAII -84	SCCV-18	SGTR-17	SGTR-53	SILU-23	SSOS-23			
A12-SACC-07	3.5	6.0	10.3	CTVI-24	DAII -19	SCCV-19	SGTR-18	SGTR-54	SILU-24	SSOS-24	SMEG-10				
A12-SACC-08	5.1	8.8	15.2	CTVI-25	CTVI-91	DAII -20	SCCV-20	SCCV-85	SGTR-19	SGTR-55	SILU-25	SDTI-14	SSOS-25	SMEG-11	

A12-SACC-09	4.7	7.2	11.5	CTVI-26	DAII -21	SCCV-21	SCCV-86	SGTR-20	SGTR-56	SCBT-05	SILU-26	SDTI-15	SSOS-26	STEL-06	
A12-SACC-10	5.1	8.8	15.2	CTVI-27	DAII -22	SCCV-22	SCCV-87	SGTR-21	SGTR-57	SILU-27	SDTI-16	SSOS-27	SMEG-12		
A12-SACC-11	5.0	8.7	15.1	CTVI-28	DAII -23	DAII -85	SCCV-23	SCCV-88	SGTR-22	SGTR-58	SILU-28	SDTI-17	SSOS-28		
A12-SACC-12	3.6	6.1	10.4	CTVI-29	CTVI-92	DAII -24	SCCV-24	SCCV-89	SGTR-23	SGTR-59	SILU-29	SDTI-18	SSOS-29		
A12-SACC-13	6.0	9.7	16.2	CTVI-30	DAII -25	SCCV-25	SGTR-24	SGTR-60	SCBT-06	SILU-30	SDTI-19	SSOS-30	STEL-07	SMEG-13	
A12-SACC-14	3.5	5.9	10.2	CTVI-31	DAII -26	SCCV-26	SGTR-25	SGTR-61	SILU-31	SDTI-20	SSOS-31	SRAD-04			
A12-SACC-15	3.5	5.9	10.2	CTVI-32	CTVI-93	DAII -27	SCCV-27	SGTR-26	SGTR-62	SILU-32	SDTI-21	SSOS-32			
A12-SACC-16	5.1	8.8	15.2	CTVI-33	DAII -28	DAII -86	SCCV-28	SCCV-90	SGTR-27	SGTR-63	SILU-33	SDTI-22	SSOS-33	SMEG-14	
A13-SACC-01	3.7	6.1	10.5	CTVI-34	DAII -29	SCCV-29	SCCV-91	SGTR-28	SILU-34	SDTI-23	SSOS-34	SMEG-15			
A13-SACC-02	6.3	11.2	19.7	CTVI-35	CTVI-94	DAII -30	DAII -87	SCCV-30	SGTR-29	SILU-35	SDTI-24	SSOS-35	SMEG-16		
A13-SACC-03	5.9	9.6	16.1	CTVI-36	DAII -31	DAII -88	SCCV-31	SCBT-07	SILU-36	SDTI-25	SSOS-36	STEL-08	SMEG-17		
A13-SACC-04	3.5	6.0	10.2	CTVI-37	DAII -32	SCCV-32	SCCV-92	SILU-37	SDTI-26	SSOS-37					
A13-SACC-05	4.7	8.4	14.8	CTVI-38	DAII -33	DAII -89	SCCV-33	SCCV-93	SSOS-38						
A13-SACC-06	6.1	11.0	19.5	CTVI-39	CTVI-95	DAII -34	DAII -90	SCCV-34	SCCV-94	SSOS-39					
A13-SACC-07	3.8	6.8	12.0	CTVO-40	DAII -35	SCCV-35	SSOS-40								
A13-SACC-08	4.4	7.9	14.0	CTVO-41	DAIO -36	SCCV-36	SSOS-41								
A13-SACC-09	4.4	7.9	14.0	CTVO-42	DAIO -37	SCCV-37	SSOS-42	SRAD-05							
A13-SACC-10	5.8	10.6	18.8	CTVO-43	DAIO -38	DAII -91	SCCV-38	SSOS-43	STEL-09						
A13-SACC-11	5.2	9.4	16.7	CTVI-44	DAIO -39	SCCV-39	SSOS-44								
A13-SACC-12	3.2	5.7	10.0	CTVI-45	CTVI-96	DAII -40	SCCV-40	SGTR-30	SSOS-45						
A13-SACC-13	1.9	3.2	5.4	CTVI-46	DAII-41	SCCV-41	SGTR-31	SSOS-46	SMEG-18						
A13-SACC-14	3.3	5.7	10.1	CTVI-47	DAII -42	SCCV-42	SSOS-47	SMEG-19							
A13-SACC-15	4.7	8.4	14.8	CTVI-48	DAII -43	SCCV-43	SGTR-64	SDTI-27	SSOS-48						
A13-SACC-16	4.5	7.0	11.4	CTVI-49	CTVI-97	DAII -44	SCCV-44	SGTR-32	SGTR-65	SCBT-08	SDTI-28	SSOS-49	STEL-10	SMEG-20	
A14-SACC-01	3.4	5.8	10.1	CTVI-50	DAII -45	SCCV-45	SGTR-33	SGTR-66	SDTI-29	SSOS-50					
A14-SACC-02	4.6	8.3	14.7	CTVI-51	DAII -46	SCCV-46	SDTI-30	SSOS-51							
A14-SACC-03	3.3	5.8	10.1	CTVI-52	DAII -47	SCCV-47	SDTI-31	SSOS-52	SMEG-21						
A14-SACC-04	3.3	5.7	10.0	CTVI-53	CTVI-98	DAII -48	SCCV-48	SDTI-32	SSOS-53						

A14-SACC-05	4.8	8.5	14.8	CTVI-54	DAII -49	SCCV-49	SGTR-34	SGTR-67	SDTI-33	SSOS-54	SRAD-06	
A14-SACC-06	4.9	8.6	15.0	CTVI-55	CTVI-99	DAII -50	SCCV-50	SGTR-35	SGTR-68	SDTI-34	SSOS-55	SMEG-22
A14-SACC-07	4.7	8.4	14.8	CTVI-56	CTVI-100	DAII -51	SCCV-51	SGTR-36	SDTI-35	SSOS-56		
A14-SACC-08	3.2	5.7	10.0	CTVI-57	DAII -52	SCCV-52	SSOS-57	STEL-11				
A14-SACC-09	4.6	8.3	14.8	CTVI-58	CTVI-101	DAII -53	SCCV-53	SSOS-58	SMEG-23			
A14-SACC-10	4.6	8.3	14.7	CTVI-59	CTVI-102	DAII -54	SCCV-54	SGTR-37	SSOS-59			
A15-SACC-01	3.3	5.7	10.1	CTVI-60	DAII -55	SCCV-55	SSOS-60	SMEG-24				
A15-SACC-02	3.2	5.7	10.0	CTVI-61	DAII -56	SCCV-56	SGTR-38	SSOS-61				
A15-SACC-03	5.7	9.4	15.8	CTVI-62	CTVI-103	DAII -57	SCCV-57	SGTR-39	SCBT-09	SSOS-62	STEL-12	
A15-SACC-04	3.2	5.6	9.9	CTVI-63	DAII -58	SCCV-58	SSOS-63					
A15-SACC-05	3.3	5.8	10.1	CTVI-64	DAII -59	SCCV-59	SGTR-40	SSOS-64	SRAD-07	SMEG-25		
A15-SACC-06	3.2	5.6	9.9	CTVI-65	DAII -60	SCCV-60	SSOS-65					
A15-SACC-07	3.2	5.7	10.0	CTVI-66	DAII -61	SCCV-61	SSOS-66	STEL-14				
A15-SACC-08	3.2	5.7	10.0	CTVI-67	DAII -62	SCCV-62	SGTR-41	SSOS-67				
A16-SACC-01	3.2	5.6	9.9	CTVI-68	DAII -63	SCCV-63	SSOS-68					
A16-SACC-02	3.2	5.6	9.9	CTVI-69	DAII -64	SCCV-64	SSOS-69					
A16-SACC-03	4.6	8.3	14.7	CTVI-70	CTVI-104	DAII -65	SCCV-65	SGTR-42	SSOS-70			
A16-SACC-04	3.2	5.7	10.0	CTVI-71	DAII -66	SCCV-66	SSOS-71	STEL-15				
A16-SACC-05	4.4	7.9	14.0	CTVO-72	DAIO -67	SCCV-67	SSOS-72					
A16-SACC-06	4.4	7.9	14.0	CTVO-73	DAIO -68	SCCV-68	SSOS-73					
A16-SACC-07	5.5	9.0	15.2	CTVO-74	DAIO -69	SCCV-69	SCBT-10	SSOS-74	SRAD-08	STEL-16		
A16-SACC-08	4.4	7.9	14.0	CTVO-75	DAIO -70	SCCV-70	SSOS-75					
A16-SACC-09	4.4	7.9	14.0	CTVO-76	DAIO -71	SCCV-71	SSOS-76					
A16-SACC-10	6.4	11.7	20.8	CTVO-77	CTVO-105	DAIO -72	SCCV-72	SSOS-77				
A16-SACC-11	4.4	7.9	14.0	CTVO-78	DAIO -73	SCCV-73	SSOS-78					
A16-SACC-12	2.4	4.2	7.3	CTVO-79	SCCV-74	SSOS-79	SRAD-09					
A16-SACC-01	4.4	7.9	14.0	CTVO-80	DAIO -74	SCCV-75	SSOS-80					

A16-SACC-02	2.4	4.2	7.2	CTVO-81	SCCV-76	SSOS-81			
A16-SACC-03	7.2	14.2	16.2	CTVOM-82	SCCV-77	SSOS-82			
A16-SACC-04	4.4	7.9	14.0	CTVO-83	DAIO -75	SCCV-78	SSOS-83		
A16-SACC-05	9.2	18.0	23.0	CTVOM-84	DAIO -76	SCCV-79	SSOS-84	SRAD-10	
A16-SACC-06	2.0	3.8	6.8	CTVO-85					

Tabla B-2 Detalle de distribución switches de Acceso

Anexo C Scripts de Configuración para pruebas.

Configuración de Switches

Prueba 4.1 Test de la Herramienta:

Iperf:

Cliente Iperf : iperf-3.1.3-win32\iperf3.exe -c 10.44.176.11 -u -l22 -b100Mb -t60

Cliente Iperf : iperf-3.1.3-win32\iperf3.exe -c 10.44.176.11 -u -l726 -b100Mb -t60

Cliente Iperf : iperf-3.1.3-win32\iperf3.exe -c 10.44.176.11 -u -l1238 -b100Mb -t60

Servidor Iperf: iperf-3.1.3-win32\iperf3.exe -s

Switch 1:

```
sysname A0011-SACC-001

vlan 1111
observe-port interface Ethernet0/0/4

interface Ethernet0/0/2
 port link-type access
 port default vlan 1111
 mirror to observe-port inbound

interface GigabitEthernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 1111
 combo-port fiber
```

Switch2

```
sysname A0011-SACC-002

vlan 1111
interface Ethernet0/0/2
port link-type access
```

port default vlan 1111

interface GigabitEthernet0/0/0

port link-type trunk

port trunk allow-pass vlan 1111

combo-port fiber

Prueba 4.2 Capa de Acceso

Configuración previa en todos los switches:

user-interface con 0

 authentication-mode password

 set authentication password cipher %@%@-b7bWcec)1@^o")5GGq),LDuGUqZ(xEO7.9d~yC%M-cDLDx,%@%@

user-interface vty 0

authentication-mode aaa

 user privilege level 15

 protocol inbound telnet

user-interface vty 1 4

 authentication-mode aaa

 protocol inbound telnet

telnet server enable

Pruebas MSTP

Configuración en todos los switches:

vlan batch 1111 to 1120 1150

stp converge fast

region-name A11

 instance 1 vlan 1111 to 1115

 instance 2 vlan 1116 to 1120

 active region-configuration

Configuracion en los switches de acceso:

interface GigabitEthernet0/0/0

 port link-type trunk

port trunk allow-pass vlan 1111 to 1120 1150
combo-port fiber

Interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 1111 to 1120 1150
combo-port fiber

Configuraciones particulares:
sysname A0011-SAGR-001
stp instance 1 root primary
interface GigabitEthernet0/0/6
port link-type trunk
port trunk allow-pass vlan 1111 to 1120 1150
interface GigabitEthernet0/0/7
port link-type trunk
port trunk allow-pass vlan 1111 to 1130 1150

Configuracion: A0011-SAGR-002
sysname A0011-SAGR-002
stp instance 2 root primary
interface GigabitEthernet0/0/6
port link-type trunk
port trunk allow-pass vlan 1111 to 1120 1150
interface GigabitEthernet0/0/7
port link-type trunk
port trunk allow-pass vlan 1111 to 1130 1150

sysname A0011-SACC-003
interface GigabitEthernet0/0/0
stp instance 1 cost 20000
stp instance 2 cost 20000

Pruebas SEP

Se heredan configuraciones de VLANs, instancias, configuración de puertos.

Configuración en todos los switches:

```
sep segment 11
control-vlan 11
protected-instance 1

sep segment 12
control-vlan 11
protected-instance 2
```

Configuración en los switches de acceso:

```
interface GigabitEthernet0/0/0
stp disable
sep segment 12
sep segment 11

interface GigabitEthernet0/0/1
stp disable
sep segment 12
sep segment 11
```

Configuraciones particulares:

```
sysname A0011-SAGR-001
control-vlan 11
 block port optimal
 protected-instance 1

interface GigabitEthernet0/0/6
stp disable
sep segment 11
sep segment 12
sep segment 12  edge secondary

interface GigabitEthernet0/0/7
stp disable
```

```
sep segment 11
sep segment 12
sep segment 11  edge primary


sysname A0011-SAGR-002
control-vlan 11
 block port optimal
 protected-instance 2

interface GigabitEthernet0/0/6
stp disable
sep segment 12
sep segment 11
sep segment 12  edge primary

interface GigabitEthernet0/0/7
stp disable
sep segment 12
sep segment 11
sep segment 11  edge primary


sysname A0011-SACC-003
interface GigabitEthernet0/0/0
sep segment 11 priority 100
sep segment 12 priority 100
```

Pruebas 4.3 Capa de Agregación

Pruebas VRRP

```
sysname A0011-SAGR-001
```

Configuración común para pruebas 1 y 2:

```
interface Vlanif1111
 ip address 10.44.176.6 255.255.240.0
 vrrp vrid 11 virtual-ip 10.44.176.5
 vrrp vrid 11 priority 120
 vrrp vrid 11 preempt-mode timer delay 20
```

```
 vrrp vrid 11 track interface g0/0/1 reduced 40

interface Vlanif1112
 ip address 10.44.192.6 255.255.240.0
 vrrp vrid 12 virtual-ip 10.44.192.5
 vrrp vrid 12 priority 120
 vrrp vrid 12 preempt-mode timer delay 20

interface Vlanif1113
 ip address 10.44.208.6 255.255.240.0
 vrrp vrid 13 virtual-ip 10.44.208.5
 vrrp vrid 13 priority 120
 vrrp vrid 13 preempt-mode timer delay 20

interface Vlanif1114
 ip address 10.44.224.6 255.255.240.0
 vrrp vrid 14 virtual-ip 10.44.224.5
 vrrp vrid 14 priority 120
 vrrp vrid 14 preempt-mode timer delay 20

interface Vlanif1115
 ip address 10.45.0.6 255.255.240.0
 vrrp vrid 15 virtual-ip 10.45.0.5

interface Vlanif1116
 ip address 10.45.16.6 255.255.240.0
 vrrp vrid 16 virtual-ip 10.45.16.5

interface Vlanif1117
 ip address 10.45.32.6 255.255.240.0
 vrrp vrid 17 virtual-ip 10.45.32.5

interface Vlanif1118
 ip address 10.45.48.6 255.255.240.0
 vrrp vrid 18 virtual-ip 10.45.48.5
```

interface Vlanif1119
 ip address 10.45.64.6 255.255.240.0
 vrrp vrid 19 virtual-ip 10.45.64.5

interface Vlanif1120
 ip address 10.45.80.6 255.255.240.0
 vrrp vrid 20 virtual-ip 10.45.80.5

interface GigabitEthernet0/0/4
undo portswitch
 ip address 192.168.71.10 255.255.255.252

 ip route-static 10.40.176.0 255.255.240.0 192.168.71.9

sysname A0011-SAGR-002
Configuración común para pruebas 1 y 2:
interface Vlanif1111
 ip address 10.44.176.7 255.255.240.0
 vrrp vrid 11 virtual-ip 10.44.176.5
interface Vlanif1112
 ip address 10.44.192.7 255.255.240.0
 vrrp vrid 12 virtual-ip 10.44.192.5

interface Vlanif1113
 ip address 10.44.208.7 255.255.240.0
 vrrp vrid 13 virtual-ip 10.44.208.5

interface Vlanif1114
 ip address 10.44.224.7 255.255.240.0
 vrrp vrid 14 virtual-ip 10.44.224.5

interface Vlanif1115
 ip address 10.45.0.7 255.255.240.0
 vrrp vrid 15 virtual-ip 10.45.0.5

interface Vlanif1116

```
 ip address 10.45.16.7 255.255.240.0
 ip address 10.45.16.5 255.255.240.0
 vrrp vrid 16 priority 120
 vrrp vrid 16 preempt-mode timer delay 20

interface Vlanif1117
 ip address 10.45.32.7 255.255.240.0
 ip address 10.45.32.5 255.255.240.0
 vrrp vrid 17 priority 120
 vrrp vrid 17 preempt-mode timer delay 20

interface Vlanif1118
 ip address 10.45.48.7 255.255.240.0
 ip address 10.45.48.5 255.255.240.0
 vrrp vrid 18 priority 120
 vrrp vrid 18 preempt-mode timer delay 20

interface Vlanif1119
 ip address 10.45.64.7 255.255.240.0
 ip address 10.45.64.5 255.255.240.0
 vrrp vrid 19 priority 120
 vrrp vrid 19 preempt-mode timer delay 20

interface Vlanif1120
 ip address 10.45.80.7 255.255.240.0
 ip address 10.45.80.5 255.255.240.0
 vrrp vrid 20 priority 120
 vrrp vrid 20 preempt-mode timer delay 20

interface GigabitEthernet0/0/4
undo portswitch
 ip address 192.168.71.10 255.255.255.252

  ip route-static 10.40.176.0 255.255.240.0 192.168.82.9


sysname A0010-SAGR-001
```

interface GigabitEthernet0/0/5
undo portswitch
ip address 192.168.82.10 255.255.255.252

interface GigabitEthernet0/0/4
undo portswitch
ip address 192.168.71.9 255.255.255.252

ip route-static 10.44.176.0 255.255.240.0 192.168.71.10
ip route-static 10.44.176.0 255.255.240.0 192.168.82.9

Prueba 1

sysname A0011-SAGR-001
interface Vlanif1111
vrrp vrid 11 track interface g0/0/1 reduced 40

Prueba 2

sysname A0011-SAGR-001
 bfd a11toa10 bind peer-ip 192.168.71.9
 discriminator local 11
 discriminator remote 10
 min-tx-interval 50
 min-rx-interval 50
 commit

sysname A0011-SAGR-001
interface Vlanif1111
vrrp vrid 1 track bfd-session 11 reduced 40

sysname A0010-SAGR-001

 bfd a10toa11 bind peer-ip 192.168.71.10
 discriminator local 10

```
 discriminator remote 11
 min-tx-interval 50
 min-rx-interval 50
 commit
```

Pruebas de protocolos de enrutamiento BGP y OSPF

OSPF Configuración común pruebas de convergencia y latencia

```
sysname A0010-SAGR-001
router id 10.0.0.1
vlan batch 1011 to 1020
interface Vlanif1011
 ip address 10.40.176.6 255.255.240.0

interface Vlanif1012
 ip address 10.40.192.6 255.255.240.0

interface Vlanif1013
 ip address 10.40.208.6 255.255.240.0

interface Vlanif1014
 ip address 10.40.224.6 255.255.240.0

interface Vlanif1015
 ip address 10.41.0.6 255.255.240.0

interface Vlanif1016
 ip address 10.41.16.6 255.255.240.0

interface Vlanif1017
 ip address 10.41.32.6 255.255.240.0

interface Vlanif1018
 ip address 10.41.48.6 255.255.240.0

interface Vlanif1019
```

```
 ip address 10.41.64.6 255.255.240.0

interface Vlanif1020
 ip address 10.41.80.6 255.255.240.0

interface GigabitEthernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 1010 to 1030
 stp disable
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.80.10 255.255.255.252
 combo-port fiber

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.71.9 255.255.255.252
 combo-port fiber

ospf 1
area 0.0.0.0
  network 192.168.71.8 0.0.0.3
  network 192.168.80.8 0.0.0.3
 area 0.0.0.10
  network 10.40.176.0 0.0.15.255
  network 10.40.192.0 0.0.15.255
  network 10.40.208.0 0.0.15.255
  network 10.40.224.0 0.0.15.255
  network 10.41.0.0 0.0.15.255
  network 10.41.16.0 0.0.15.255
  network 10.41.32.0 0.0.15.255
  network 10.41.48.0 0.0.15.255
  network 10.41.64.0 0.0.15.255
  network 10.41.80.0 0.0.15.255
  network 192.168.110.8 0.0.0.3

 sysname A0011-SAGR-001
```

```
interface Vlanif1111
 ip address 10.44.176.6 255.255.240.0
 vrrp vrid 11 virtual-ip 10.44.176.5
 vrrp vrid 11 priority 120
 vrrp vrid 11 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1112
 ip address 10.44.192.6 255.255.240.0
 vrrp vrid 12 virtual-ip 10.44.192.5
 vrrp vrid 12 priority 120
 vrrp vrid 12 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1113
 ip address 10.44.208.6 255.255.240.0
 vrrp vrid 13 virtual-ip 10.44.208.5
 vrrp vrid 13 priority 120
 vrrp vrid 13 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1114
 ip address 10.44.224.6 255.255.240.0
 vrrp vrid 14 virtual-ip 10.44.224.5
 vrrp vrid 14 priority 120
  ospf cost 100

interface Vlanif1115
 ip address 10.45.0.6 255.255.240.0
 vrrp vrid 15 virtual-ip 10. 45.0.5
 vrrp vrid 15 priority 120
 ospf cost 100

interface Vlanif1116
 ip address 10.45.16.6 255.255.240.0
 vrrp vrid 16 virtual-ip 10.45.16.5
 ospf cost 100
```

```
interface Vlanif1117
 ip address 10.45.32.6 255.255.240.0
 vrrp vrid 17 virtual-ip 10.45.32.5
 ospf cost 100

interface Vlanif1118
 ip address 10.45.48.6 255.255.240.0
 vrrp vrid 18 virtual-ip 10.45.48.5
 ospf cost 100

interface Vlanif1119
 ip address 10.45.64.6 255.255.240.0
 vrrp vrid 19 virtual-ip 10.45.64.5
 ospf cost 100

interface Vlanif1120
 ip address 10.45.80.6 255.255.240.0
 vrrp vrid 20 virtual-ip 10.45.80.5
 ospf cost 100


 sysname A0012-SAGR-001
router id 12.0.0.1

vlan batch  1211 to 1220
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.72.10 255.255.255.252
interface Vlanif1211
 ip address 10.48.176.6 255.255.240.0
 ospf cost 100
interface Vlanif1212
 ip address 10.48.192.6 255.255.240.0
 ospf cost 100

interface Vlanif1213
```

```
 ip address 10.48.208.6 255.255.240.0
 ospf cost 100

interface Vlanif1214
 ip address 10.48.224.6 255.255.240.0
 ospf cost 100

interface Vlanif1215
 ip address 10.49.0.6 255.255.240.0
 ospf cost 100

interface Vlanif1216
 ip address 10.49.16.6 255.255.240.0
 ospf cost 100

interface Vlanif1217
 ip address 10.49.32.6 255.255.240.0
 ospf cost 100

interface Vlanif1218
 ip address 10.49.48.6 255.255.240.0
 ospf cost 100

interface Vlanif1219
 ip address 10.49.64.6 255.255.240.0
 ospf cost 100

interface Vlanif1220
 ip address 10.49.80.6 255.255.240.0
 ospf cost 100

interface GigabitEthernet0/0/0
port link-type trunk
 port trunk allow-pass vlan 1210 to 1230
 stp disable
 interface GigabitEthernet0/0/4
 undo portswitch
```

```
 ip address 192.168.72.10 255.255.255.252

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.73.9 255.255.255.252

ospf 1
 import-route static
area 0.0.0.0
  network 192.168.72.8 0.0.0.3
  network 192.168.73.8 0.0.0.3
 area 0.0.0.12
  network 10.48.176.0 0.0.15.255
  network 10.48.192.0 0.0.15.255
  network 10.48.208.0 0.0.15.255
  network 10.48.224.0 0.0.15.255
  network 10.49.0.0 0.0.15.255
  network 10.49.16.0 0.0.15.255
  network 10.49.32.0 0.0.15.255
  network 10.49.48.0 0.0.15.255
  network 10.49.64.0 0.0.15.255
  network 10.49.80.0 0.0.15.255
  network 10.49.96.0 0.0.15.255
  network 10.49.112.0 0.0.15.255
  network 192.168.112.8 0.0.0.3

sysname A0013-SAGR-001
router id 13.0.0.1
vlan batch 1311 to 1320
interface Vlanif1311
 ip address 10.52.176.6 255.255.240.0
 ospf cost 100

interface Vlanif1312
 ip address 10.52.192.6 255.255.240.0
 ospf cost 100
```

```
interface Vlanif1313
 ip address 10.52.208.6 255.255.240.0
 ospf cost 100

interface Vlanif1314
 ip address 10.52.224.6 255.255.240.0
 ospf cost 100

interface Vlanif1315
 ip address 10.53.0.6 255.255.240.0
 ospf cost 100

interface Vlanif1316
 ip address 10.53.16.6 255.255.240.0
 ospf cost 100

interface Vlanif1317
 ip address 10.53.32.6 255.255.240.0
 ospf cost 100

interface Vlanif1318
 ip address 10.53.48.6 255.255.240.0
 ospf cost 100

interface Vlanif1319
 ip address 10.53.64.6 255.255.240.0
 ospf cost 100

interface Vlanif1320
 ip address 10.53.80.6 255.255.240.0
 ospf cost 100
interface GigabitEthernet0/0/0
 bandwidth 100
 port link-type trunk
 port trunk allow-pass vlan 1310 to 1330 1371
 stp disable
```

```
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.73.10 255.255.255.252

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.74.9 255.255.255.252
ospf 1
area 0.0.0.0
  network 192.168.73.8 0.0.0.3
  network 192.168.74.8 0.0.0.3
 area 0.0.0.13
  network 10.52.176.0 0.0.15.255
  network 10.52.192.0 0.0.15.255
  network 10.52.208.0 0.0.15.255
  network 10.52.224.0 0.0.15.255
  network 10.53.0.0 0.0.15.255
  network 10.53.16.0 0.0.15.255
  network 10.53.32.0 0.0.15.255
  network 10.53.48.0 0.0.15.255
  network 10.53.64.0 0.0.15.255
  network 10.53.80.0 0.0.15.255
  network 10.53.96.0 0.0.15.255


sysname A0014-SAGR-001
router id 14.0.0.1
vlan batch 1411 to 1420
interface Vlanif1411
 ip address 10.56.176.6 255.255.240.0
 ospf cost 100

interface Vlanif1412
 ip address 10.56.192.6 255.255.240.0
 ospf cost 100

interface Vlanif1413
```

```
 ip address 10.56.208.6 255.255.240.0
 ospf cost 100

interface Vlanif1414
 ip address 10.56.224.6 255.255.240.0
 ospf cost 100

interface Vlanif1415
 ip address 10.57.0.6 255.255.240.0
 ospf cost 100

interface Vlanif1416
 ip address 10.57.16.6 255.255.240.0
 ospf cost 100

interface Vlanif1417
 ip address 10.57.32.6 255.255.240.0
 ospf cost 100

interface Vlanif1418
 ip address 10.57.48.6 255.255.240.0
 ospf cost 100

interface Vlanif1419
 ip address 10.57.64.6 255.255.240.0
 ospf cost 100

interface Vlanif1420
 ip address 10.57.80.6 255.255.240.0
 ospf cost 100
interface GigabitEthernet0/0/0
port link-type trunk
 port trunk allow-pass vlan 1410 to 1420
 stp disable
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.74.10 255.255.255.252
```

```
interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.75.9 255.255.255.252

ospf 1
 area 0.0.0.0
  network 192.168.74.8 0.0.0.3
  network 192.168.75.8 0.0.0.3
 area 0.0.0.14
  network 10.56.176.0 0.0.15.255
  network 10.56.192.0 0.0.15.255
  network 10.56.208.0 0.0.15.255
  network 10.56.224.0 0.0.15.255
  network 10.57.0.0 0.0.15.255
  network 10.57.16.0 0.0.15.255
  network 10.57.32.0 0.0.15.255
  network 10.57.48.0 0.0.15.255
  network 10.57.64.0 0.0.15.255
  network 10.57.80.0 0.0.15.255
  network 192.168.114.8 0.0.0.3

sysname A0015-SAGR-001
router id 15.0.0.1

vlan batch 1511 to 1520
interface Vlanif1511
 ip address 10.60.176.6 255.255.240.0

interface Vlanif1512
 ip address 10.60.192.6 255.255.240.0

interface Vlanif1513
 ip address 10.64.208.6 255.255.240.0

interface Vlanif1514
 ip address 10.60.224.6 255.255.240.0
```

```
interface Vlanif1515
 ip address 10.60.240.6 255.255.240.0

interface Vlanif1516
 ip address 10.61.0.6 255.255.240.0

interface Vlanif1517
 ip address 10.61.16.6 255.255.240.0

interface Vlanif1518
 ip address 10.61.32.6 255.255.240.0

interface Vlanif1519
 ip address 10.61.48.6 255.255.240.0

interface Vlanif1520
 ip address 10.61.80.6 255.255.240.0
interface GigabitEthernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 1511 to 1520
 stp disable
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.75.10 255.255.255.252

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.76.9 255.255.255.252

ospf 1
area 0.0.0.0
  network 192.168.75.8 0.0.0.3
  network 192.168.76.8 0.0.0.3
 area 0.0.0.15
  network 10.60.176.0 0.0.15.255
  network 10.60.192.0 0.0.15.255
```

```
  network 10.60.208.0 0.0.15.255
  network 10.60.224.0 0.0.15.255
  network 10.61.0.0 0.0.15.255
  network 10.61.16.0 0.0.15.255
  network 10.61.32.0 0.0.15.255
  network 10.61.48.0 0.0.15.255
  network 10.61.64.0 0.0.15.255
  network 10.61.80.0 0.0.15.255
  network 192.168.115.8 0.0.0.3

sysname A0014-SAGR-002

router id 14.0.0.2

vlan batch 1411 to 1420

interface Vlanif1411
 ip address 10.56.176.7 255.255.240.0
 ospf cost 100

interface Vlanif1412
 ip address 10.56.192.7 255.255.240.0
 ospf cost 100

interface Vlanif1413
 ip address 10.56.208.7 255.255.240.0
 ospf cost 100

interface Vlanif1414
 ip address 10.56.224.7 255.255.240.0
 ospf cost 100

interface Vlanif1415
 ip address 10.57.0.7 255.255.240.0
 ospf cost 100

interface Vlanif1416
```

```
 ip address 10.57.16.7 255.255.240.0
 ospf cost 100

interface Vlanif1417
 ip address 10.57.32.7 255.255.240.0
 ospf cost 100

interface Vlanif1418
 ip address 10.57.48.7 255.255.240.0
 ospf cost 100

interface Vlanif1419
 ip address 10.57.74.7 255.255.240.0
 ospf cost 100

interface Vlanif1420
 ip address 10.57.80.7 255.255.240.0
 ospf cost 100
interface GigabitEthernet0/0/0
 bandwidth 100
 port link-type trunk
 port trunk allow-pass vlan 1410 to 1420
 stp disable

interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.76.10 255.255.255.252

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.77.9 255.255.255.252

ospf 1
 import-route direct
area 0.0.0.0
  network 192.168.76.8 0.0.0.3
  network 192.168.77.8 0.0.0.3
```

```
 area 0.0.0.1
 area 0.0.0.14
  network 10.56.176.0 0.0.15.255
  network 10.56.192.0 0.0.15.255
  network 10.56.208.0 0.0.15.255
  network 10.56.224.0 0.0.15.255
  network 10.57.0.0 0.0.15.255
  network 10.57.16.0 0.0.15.255
  network 10.57.32.0 0.0.15.255
  network 10.57.48.0 0.0.15.255
  network 10.57.64.0 0.0.15.255
  network 10.57.80.0 0.0.15.255
  network 192.168.114.8 0.0.0.3

<A0013-SAGR-002>
router id 13.0.0.2
vlan batch 1311 to 1320
interface Vlanif1311
 ip address 10.52.176.7 255.255.240.0
 ospf cost 100

interface Vlanif1312
 ip address 10.52.192.7 255.255.240.0
 ospf cost 100

interface Vlanif1313
 ip address 10.52.208.7 255.255.240.0
 ospf cost 100

interface Vlanif1314
 ip address 10.52.224.7 255.255.240.0
 ospf cost 100

interface Vlanif1315
 ip address 10.53.0.7 255.255.240.0
 ospf cost 100
```

```
interface Vlanif1316
 ip address 10.53.16.7 255.255.240.0
 ospf cost 100

interface Vlanif1317
 ip address 10.53.32.7 255.255.240.0
 ospf cost 100

interface Vlanif1318
 ip address 10.53.48.7 255.255.240.0
 ospf cost 100

interface Vlanif1319
 ip address 10.53.74.7 255.255.240.0
 ospf cost 100

interface Vlanif1320
 ip address 10.53.80.7 255.255.240.0
 ospf cost 100
interface GigabitEthernet0/0/0
 bandwidth 100
 port link-type trunk
 port trunk allow-pass vlan 1310 to 1320
 stp disable
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.77.10 255.255.255.252

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.78.9 255.255.255.252
ospf 1
area 0.0.0.0
  network 192.168.77.8 0.0.0.3
  network 192.168.78.8 0.0.0.3
 area 0.0.0.13
  network 10.52.176.0 0.0.15.255
```

```
 network 10.52.192.0 0.0.15.255
 network 10.52.208.0 0.0.15.255
 network 10.52.224.0 0.0.15.255
 network 10.53.0.0 0.0.15.255
 network 10.53.16.0 0.0.15.255
 network 10.53.32.0 0.0.15.255
 network 10.53.48.0 0.0.15.255
 network 10.53.64.0 0.0.15.255
 network 10.53.80.0 0.0.15.255
 network 192.168.113.8 0.0.0.3

<A0012-SAGR-002>
router id 12.0.0.2
vlan batch 1211 to 1220
interface Vlanif1211
 ip address 10.48.176.7 255.255.240.0
 ospf cost 100

interface Vlanif1212
 ip address 10.48.192.7 255.255.240.0
 ospf cost 100

interface Vlanif1213
 ip address 10.48.208.7 255.255.240.0
 ospf cost 100

interface Vlanif1214
 ip address 10.48.224.7 255.255.240.0
 ospf cost 100

interface Vlanif1215
 ip address 10.49.0.7 255.255.240.0
 ospf cost 100

interface Vlanif1216
 ip address 10.49.16.7 255.255.240.0
 ospf cost 100
```

```
interface Vlanif1217
 ip address 10.49.32.7 255.255.240.0
 ospf cost 100

interface Vlanif1218
 ip address 10.49.48.7 255.255.240.0
 ospf cost 100

interface Vlanif1219
 ip address 10.49.64.7 255.255.240.0
 ospf cost 100

interface Vlanif1220
 ip address 10.49.80.7 255.255.240.0
 ospf cost 100
interface GigabitEthernet0/0/0
port link-type trunk
 port trunk allow-pass vlan 1211 to 1220
 stp disable
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 192.168.78.10 255.255.255.252
 mirror to observe-port inbound

interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.79.9 255.255.255.252

ospf 1

 area 0.0.0.0
  network 192.168.78.8 0.0.0.3
  network 192.168.79.8 0.0.0.3
 area 0.0.0.12
  network 10.48.176.0 0.0.15.255
  network 10.48.192.0 0.0.15.255
```

```
  network 10.48.208.0 0.0.15.255
  network 10.48.224.0 0.0.15.255
  network 10.49.0.0 0.0.15.255
  network 10.49.16.0 0.0.15.255
  network 10.49.32.0 0.0.15.255
  network 10.49.48.0 0.0.15.255
  network 10.49.64.0 0.0.15.255
  network 10.49.80.0 0.0.15.255
  network 192.168.112.8 0.0.0.3

sysname A0011-SAGR-002
router id 11.0.0.2
interface Vlanif1111
 ip address 10.44.176.7 255.255.240.0
 vrrp vrid 11 virtual-ip 10.44.176.5
ospf cost 100

interface Vlanif1112
 ip address 10.44.192.7 255.255.240.0
 vrrp vrid 12 virtual-ip 10.44.192.5
ospf cost 100

interface Vlanif1113
 ip address 10.44.208.7 255.255.240.0
 vrrp vrid 13 virtual-ip 10.44.208.5
ospf cost 100

interface Vlanif1114
 ip address 10.44.224.7 255.255.240.0
 vrrp vrid 14 virtual-ip 10.44.224.5
 ospf cost 100

interface Vlanif1115
 ip address 10.45.0.7 255.255.240.0
 vrrp vrid 15 virtual-ip 10.45.0.5
ospf cost 100
```

```
interface Vlanif1116
 ip address 10.45.16.7 255.255.240.0
 vrrp vrid 16 priority 120
 vrrp vrid 16 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1117
 ip address 10.45.32.7 255.255.240.0
ip address 10.45.32.5 255.255.240.0
 vrrp vrid 17 priority 120
 vrrp vrid 17 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1118
 ip address 10.45.48.7 255.255.240.0
 ip address 10.45.48.5 255.255.240.0
 vrrp vrid 18 priority 120
 vrrp vrid 18 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1119
 ip address 10.45.64.7 255.255.240.0
 ip address 10.45.64.5 255.255.240.0
 vrrp vrid 19 priority 120
 vrrp vrid 19 preempt-mode timer delay 20
 ospf cost 100

interface Vlanif1120
 ip address 10.45.80.7 255.255.240.0
 ip address 10.45.80.5 255.255.240.0
 vrrp vrid 20 priority 120
 vrrp vrid 20 preempt-mode timer delay 20
 ospf cost 100
```

Pruebas

Prueba 1 convergencia

Misma configuración ya realizada

Prueba 2 Convergencia

En todos los switches de agregación se realizó lo siguiente:

```
ospf 1
 frr
  loop-free-alternate
```

Configuraciones pruebas de latencia

Prueba 1

Misma configuración de las pruebas anteriores

Prueba 2

Sumarización de rutas

```
sysname A0010-SAGR-001

ospf 1
  asbr-summary 10.40.0.0 255.252.0.0

sysname A0011-SAGR-001

ospf 1
  asbr-summary 10.44.0.0 255.252.0.0

sysname A0012-SAGR-001

ospf 1
  asbr-summary 10.48.0.0 255.252.0.0
```

```
sysname A0013-SAGR-001

ospf 1
 asbr-summary 10.52.0.0 255.252.0.0

sysname A0014-SAGR-001

ospf 1
 asbr-summary 10.56.0.0 255.252.0.0

sysname A0015-SAGR-001

ospf 1
 asbr-summary 10.60.0.0 255.252.0.0

sysname A0014-SAGR-002

ospf 1
 asbr-summary 10.56.0.0 255.252.0.0

sysname A0013-SAGR-002

ospf 1
 asbr-summary 10.52.0.0 255.252.0.0

sysname A0012-SAGR-002

ospf 1
 asbr-summary 10.48.0.0 255.252.0.0

sysname A0011-SAGR-002

ospf 1
 asbr-summary 10.44.0.0 255.252.0.0
```

5.3.2.3 BGP

```
sysname A0010-SAGR-001

bgp 65110
 router-id 1.0.10.01
 group rutasExternas external
 peer 192.168.71.10 as-number 65111
 peer 192.168.71.10 group rutasExternas
 peer 192.168.80.09 as-number 65111
 peer 192.168.80.09 group rutasExternas

ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.71.10 enable
  peer 192.168.71.10 group rutasExternas
  peer 192.168.71.10 preferred-value 150
  peer 192.168.80.09 enable
  peer 192.168.80.09 group rutasExternas
  peer 192.168.80.09 preferred-value 150


sysname A0011-SAGR-001

vlan 1171

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1171

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1171

interface Vlanif1171
 ip address 192.168.111.9 255.255.255.252
```

```
bgp 65111
 router-id 1.0.11.1
 group rutasExternas external
 peer 192.168.71.9 as-number 65110
 peer 192.168.71.9 group rutasExternas
 peer 192.168.72.10 as-number 65112
 peer 192.168.72.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.111.10 as-number 65111
 peer 192.168.111.10 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.71.9 enable
  peer 192.168.71.9 group rutasExternas
  peer 192.168.71.9 preferred-value 150
  peer 192.168.72.10 enable
  peer 192.168.72.10 group rutasExternas
  peer 192.168.72.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.111.10 enable
  peer 192.168.111.10 group rutasInternas


sysname A0012-SAGR-001

vlan 1271

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1271

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1271
```

```
interface Vlanif1271
 ip address 192.168.112.9 255.255.255.252


bgp 65112
 router-id 1.0.12.1
 group rutasExternas external
 peer 192.168.72.9 as-number 65111
 peer 192.168.72.9 group rutasExternas
 peer 192.168.73.10 as-number 65113
 peer 192.168.73.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.112.10 as-number 65112
 peer 192.168.112.10 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.72.9 enable
  peer 192.168.72.9 group rutasExternas
  peer 192.168.72.9 preferred-value 150
  peer 192.168.73.10 enable
  peer 192.168.73.10 group rutasExternas
  peer 192.168.73.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.112.10 enable
  peer 192.168.112.10 group rutasInternas


sysname A0013-SAGR-001

vlan 1371

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1371
```

```
interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1371

interface Vlanif1371
 ip address 192.168.113.9 255.255.255.252


bgp 65113
 router-id 1.0.13.1
 group rutasExternas external
 peer 192.168.73.9 as-number 65112
 peer 192.168.73.9 group rutasExternas
 peer 192.168.74.10 as-number 65114
 peer 192.168.74.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.113.10 as-number 65113
 peer 192.168.113.10 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.73.9 enable
  peer 192.168.73.9 group rutasExternas
  peer 192.168.73.9 preferred-value 150
  peer 192.168.74.10 enable
  peer 192.168.74.10 group rutasExternas
  peer 192.168.74.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.113.10 enable
  peer 192.168.113.10 group rutasInternas


sysname A0014-SAGR-001

vlan 1471
```

```
interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1471

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1471

interface Vlanif1471
 ip address 192.168.114.9 255.255.255.252

bgp 65114
 router-id 1.0.14.1
 group rutasExternas external
 peer 192.168.74.9 as-number 65113
 peer 192.168.74.9 group rutasExternas
 peer 192.168.75.10 as-number 65115
 peer 192.168.75.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.114.10 as-number 65114
 peer 192.168.114.10 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.74.9 enable
  peer 192.168.74.9 group rutasExternas
  peer 192.168.74.9 preferred-value 150
  peer 192.168.75.10 enable
  peer 192.168.75.10 group rutasExternas
  peer 192.168.75.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.114.10 enable
  peer 192.168.114.10 group rutasInternas
```

```
sysname A0015-SAGR-001

bgp 65115
 router-id 1.0.15.1
 group rutasExternas external
 peer 192.168.75.9 as-number 65114
 peer 192.168.75.9 group rutasExternas
 peer 192.168.76.10 as-number 65114
 peer 192.168.76.10 group rutasExternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.75.9 enable
  peer 192.168.75.9 group rutasExternas
  peer 192.168.75.9 preferred-value 150
  peer 192.168.76.10 enable
  peer 192.168.76.10 group rutasExternas
  peer 192.168.76.10 preferred-value 150
sysname A0014-SAGR-002

vlan 1471

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1471

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1471

interface Vlanif1471
 ip address 192.168.114.10 255.255.255.252


bgp 65114
 router-id 1.0.14.2
 group rutasExternas external
```

```
 peer 192.168.76.9 as-number 65115
 peer 192.168.76.9 group rutasExternas
 peer 192.168.77.10 as-number 65113
 peer 192.168.77.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.114.9 as-number 65114
 peer 192.168.114.9 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.76.9 enable
  peer 192.168.76.9 group rutasExternas
  peer 192.168.76.9 preferred-value 150
  peer 192.168.77.10 enable
  peer 192.168.77.10 group rutasExternas
  peer 192.168.77.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.114.9 enable
  peer 192.168.114.9 group rutasInternas


sysname A0013-SAGR-002


vlan 1371

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1371

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1371

interface Vlanif1371
 ip address 192.168.113.10 255.255.255.252
```

```
bgp 65113
 router-id 1.0.13.2
 group rutasExternas external
 peer 192.168.77.9 as-number 65114
 peer 192.168.77.9 group rutasExternas
 peer 192.168.78.10 as-number 65112
 peer 192.168.78.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.113.9 as-number 65113
 peer 192.168.113.9 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.77.9 enable
  peer 192.168.77.9 group rutasExternas
  peer 192.168.77.9 preferred-value 150
  peer 192.168.78.10 enable
  peer 192.168.78.10 group rutasExternas
  peer 192.168.78.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.113.9 enable
  peer 192.168.113.9 group rutasInternas

sysname A0012-SAGR-002

vlan 1271

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1271

interface GigabitEthernet0/0/7
 port trunk allow-pass vlan 1271

interface Vlanif1271
```

```
 ip address 192.168.112.10 255.255.255.252


bgp 65112
 router-id 1.0.12.2
 group rutasExternas external
 peer 192.168.78.9 as-number 65114
 peer 192.168.78.9 group rutasExternas
 peer 192.168.79.10 as-number 65112
 peer 192.168.79.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.112.9 as-number 65112
 peer 192.168.112.9 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.78.9 enable
  peer 192.168.78.9 group rutasExternas
  peer 192.168.78.9 preferred-value 150
  peer 192.168.79.10 enable
  peer 192.168.79.10 group rutasExternas
  peer 192.168.79.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.112.9 enable
  peer 192.168.112.9 group rutasInternas


sysname A0011-SAGR-002

vlan 1171

interface GigabitEthernet0/0/6
 port trunk allow-pass vlan 1171

interface GigabitEthernet0/0/7
```

```
 port trunk allow-pass vlan 1171

interface Vlanif1171
 ip address 192.168.111.10 255.255.255.252


bgp 65111
 router-id 1.0.11.2
 group rutasExternas external
 peer 192.168.79.9 as-number 65112
 peer 192.168.79.9 group rutasExternas
 peer 192.168.80.10 as-number 65110
 peer 192.168.80.10 group rutasExternas
 group rutasInternas internal
 peer 192.168.111.9 as-number 65111
 peer 192.168.111.9 group rutasInternas

 ipv4-family unicast
  undo synchronization
  import-route direct
  peer rutasExternas enable
  peer 192.168.79.9 enable
  peer 192.168.79.9 group rutasExternas
  peer 192.168.79.9 preferred-value 150
  peer 192.168.80.10 enable
  peer 192.168.80.10 group rutasExternas
  peer 192.168.80.10 preferred-value 150
  peer rutasInternas enable
  peer 192.168.111.9 enable
  peer 192.168.111.9 group rutasInternas
```

Configuración pruebas de convergencia

```
sysname A0011-SAGR-001

 bfd a11toa14 bind peer-ip 192.168.74.10
 discriminator local 11
```

discriminator remote 14
min-tx-interval 50
min-rx-interval 50
commit

sysname A0011-SAGR-001
interface Vlanif1111
vrrp vrid 1 track bfd-session 11 reduced 40

sysname A0014-SAGR-001
bfd a11toa14 bind peer-ip 192.168.72.9
discriminator local 14
discriminator remote 14
min-tx-interval 50
min-rx-interval 50
commit

Configuración pruebas de latencia

Prueba 1

Se utiliza la configuración ya realizada

Prueba 2

Se configura la sumarizacion de rutas

sysname A0010-SAGR-001

bgp 65110
aggregate10.40.0.0 255.252.0.0 detail-suppressed

sysname A0011-SAGR-001

bgp 65111
aggregate10.44.0.0 255.252.0.0 detail-suppressed

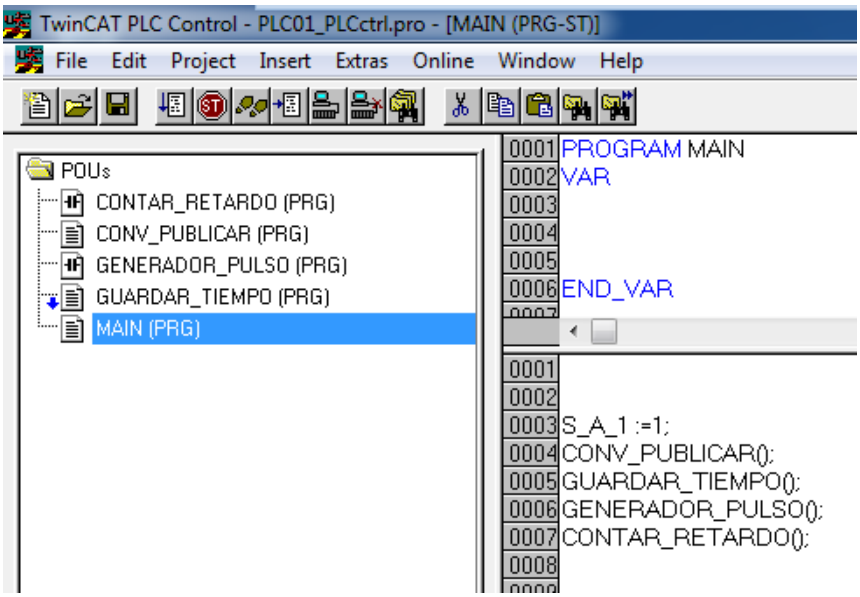
```
sysname A0011-SAGR-001

bgp 65111
 aggregate10.44.0.0 255.252.0.0  detail-suppressed

sysname A0012-SAGR-001

bgp 65112
 aggregate10.48.0.0 255.252.0.0  detail-suppressed

sysname A0012-SAGR-002

bgp 65112
 aggregate10.48.0.0 255.252.0.0  detail-suppressed

sysname A0013-SAGR-001

bgp 65113
 aggregate10.52.0.0 255.252.0.0  detail-suppressed

sysname A0013-SAGR-002

bgp 65113
 aggregate10.52.0.0 255.252.0.0  detail-suppressed


sysname A0014-SAGR-001

bgp 65114
 aggregate10.56.0.0 255.252.0.0  detail-suppressed

sysname A0014-SAGR-002

bgp 65114
 aggregate10.56.0.0 255.252.0.0  detail-suppressed

sysname A0015-SAGR-001
```

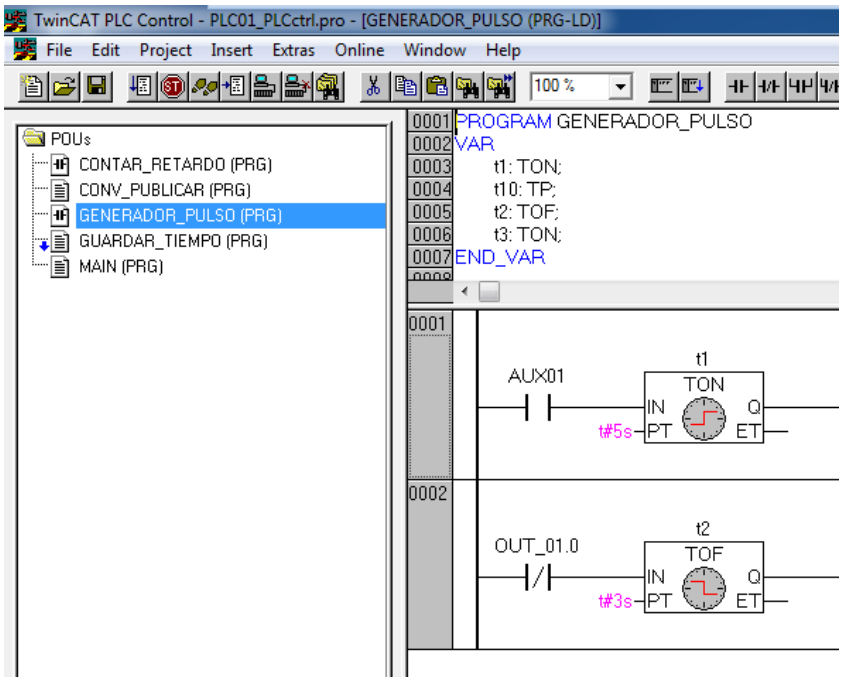
bgp 65115

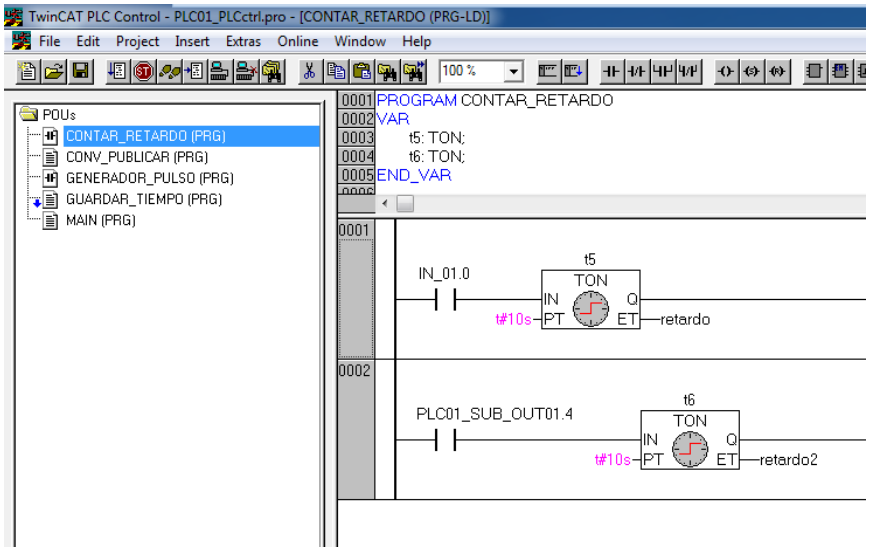
aggregate10.60.0.0 255.252.0.0 detail-suppressed

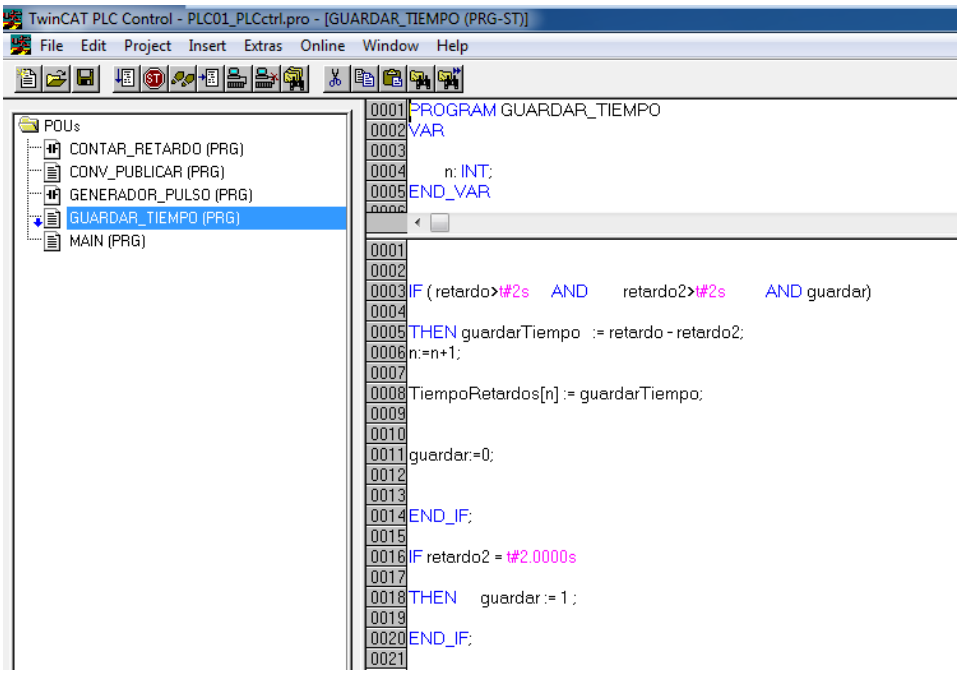
Prueba 4.4 Comunicación entre PLCs

Programa PLC01

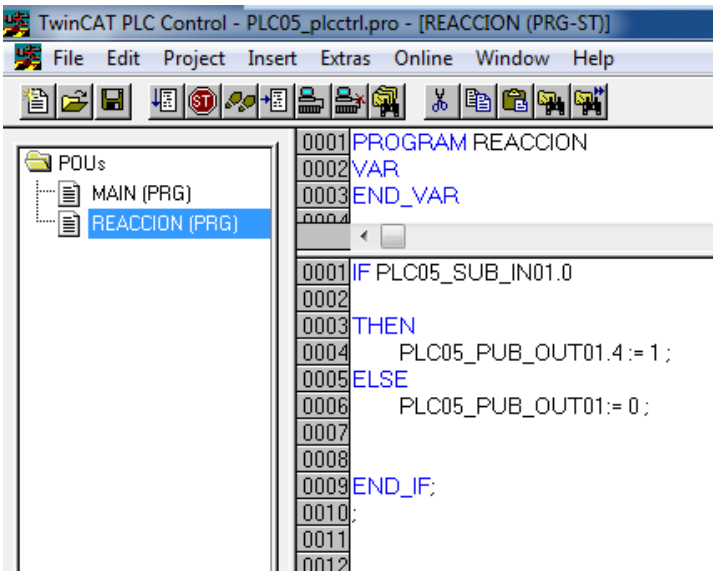



TwinCAT PLC Control - PLC01_PLCctrl.pro - [GENERADOR_PULSO (PRG-LD)]
File Edit Project Insert Extras Online Window Help
100 %
POUs
CONTAR_RETARDO (PRG)
CONV_PUBLICAR (PRG)
GENERADOR_PULSO (PRG)
GUARDAR_TIEMPO (PRG)
MAIN (PRG)
0001 PROGRAM GENERADOR_PULSO
0002 VAR
0003 t1: TON;
0004 t10: TP;
0005 t2: TOF;
0006 t3: TON;
0007 END_VAR
0001
AUX01
t1
TON
IN
PT
Q
ET
t#5s
0002
OUT_01.0
t2
TOF
IN
PT
Q
ET
t#3s


TwinCAT PLC Control - PLC01_PLCctrl.pro - [CONTAR_RETARDO (PRG-LD)]
File Edit Project Insert Extras Online Window Help
100 %
POUs
CONTAR_RETARDO (PRG)
CONV_PUBLICAR (PRG)
GENERADOR_PULSO (PRG)
GUARDAR_TIEMPO (PRG)
MAIN (PRG)
0001 PROGRAM CONTAR_RETARDO
0002 VAR
0003 t5: TON;
0004 t6: TON;
0005 END_VAR
0001
IN_01.0
t5
TON
IN
PT
Q
ET
t#10s
retardo
0002
PLC01_SUB_OUT01.4
t6
TON
IN
PT
Q
ET
t#10s
retardo2



Programa PLC05



Anexo D Detalle de Hardware de pruebas.

Switch de Agregación

Modelo AR2504E-H de la línea IoT Gateway de Huawei. Están fabricado para un ambiente industrial, pero no inhóspito.

figura 1 Switch Huawei AR2504E-H, sin tarjetas de expansión

Sus principales características son:

a) Performance:

- Capacidad de conmutación:144 Gbit/s
- Rendimiento: 66 Mpps

b) Hardware

- Procesador Dual-core, 533 MHz
- Memoria 2 GB
- Flash 512 MB
- Temperatura de operación -40°C to +65°C
- Humedad de operación 5% a 95%
- Nivel de protección IP: IP30
- Alimentación
    - Módulos de alimentación redundante
    - CA: 100 V a 240 V, 50 Hz/60 Hz (90V a 264V, 47 Hz a 63 Hz)
    - CC: 110 V a 250 V (88 V a 300 V)
    - Protección contra sobretensión y baja tensión de entrada
    - Protección contra cortocircuitos
    - Protección contra el sobrecalentamiento
    - Protección contra conexión inversa
- Consumo (normal / máximo): 20W / 25W
- Compatibilidad EMC
- Certificaciones
    - América del Norte: UL
    - Alemania: GS
    - Global: CB
    - Unión Europea: CE (2004/108/EC, EN 55022, EN 55024, and EN 300386)

- Estados Unidos: FCC (47CFR parte 15)
- Canadá: IC (ICES-003)
- Australia: RCM (original C-Tick: AS/NZS CIPSR22)
- Energía eléctrica: IEC61850-3/IEEE1613 (para subestaciones de transformadores)
- State Grid: Clase A

c) Software

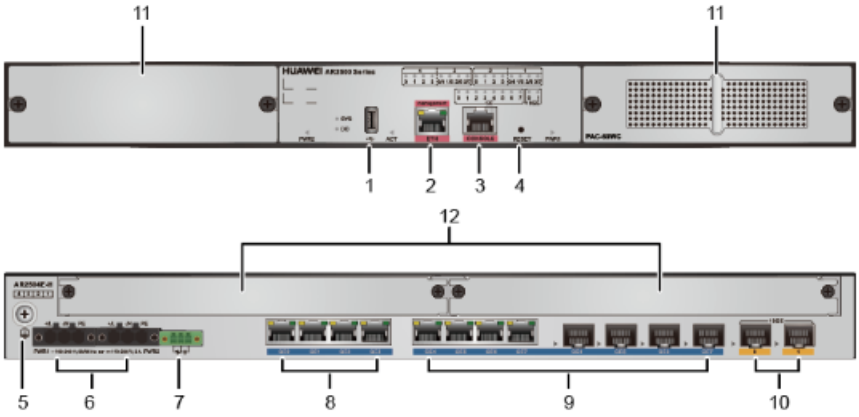
- Gestión de anillos en capa 2 STP, RSTP y MSTP
- IPv4/IPv6
  - IPv4 Unicast:
    - Ruteo estatico
    - RIP, OSPF, ISIS, and BGP
    - RIPng, OSPFv3, ISISv6, and BGP4IPv6 unicast
    - RIPng, OSPFv3, IS-Isv6 y BGP4+, VRRP6
  - Multicast:
    - IGMPv1/v2/v3
    - PIM-DM, PIM-SM, and PIM-SSM
    - MSDP and MBGP
    - Multiple routing policies
- Confiabilidad
  - VRRP
  - BFD
- Ethernet OAM
- QoS
  - DiffServ (Servicios diferenciados)
  - Traffic shaping
  - HQoS Modular QoS (traffic class, traffic behavior, and traffic policy)
- Seguridad
  - Zone-based stateful firewall
  - Access Control List (ACL)
  - Autenticación 802.1X, MAC y web por AAA y RADIUS
  - Seguridad en ARP y defensa para ataques ICMP
  - Control para broadcast storm
  - Black list

d) Chasis

Las dimensiones del chasis de switch son 442 mm x 420 mm x 44.4 mm (Ancho x profundidad x Alto), 1U.
La configuración basica del chasis se muestra en la figura.

1. Interfaz USB
2. ETH (administración)
3. Consola
4. Reset

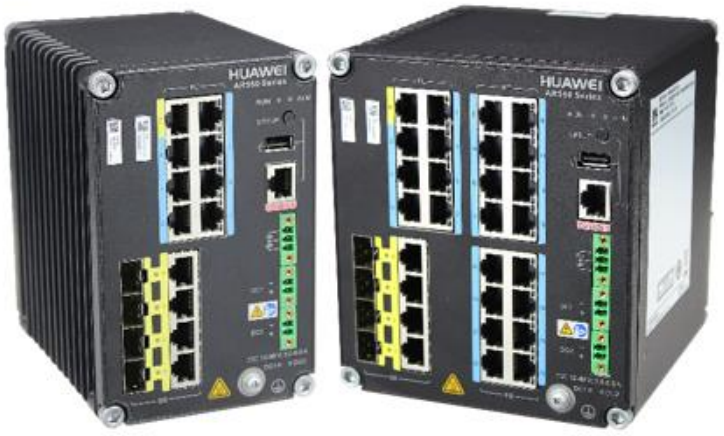
5. Tierra



Detalle de Chasis Switch Huawei AR2504E-H

Switch de acceso

Los equipos switches de acceso son modelo AR550-8FE-D-H y AR550-24FE-D-H de la línea IoT Gateway de Huawei.



Switches Huawei AR550-8FE-D-H y AR550-24FE-D-H

Las principales características de estos switches son:

a) Performance:

- Capacidad de conmutación: 24.8 Gbit/s
- Rendimiento AR550-8FE: 7,2 Mpps
- Rendimiento AR550-24FE: 9,6 Mpps

b) Hardware

- Procesador Dual-core, 533 MHz
- Memoria 512 MB

- Flash 128 MB
- Consumo AR550-8FE: 21W
- Consumo AR550-24FE: 28W
- Dimensiones AR550-8FE: 97 mm x 133 mm x 150 mm (Ancho x profundidad x Alto), 3U.
- Dimensiones AR550-24FE: 133 mm x 133 mm x 150 mm (Ancho x profundidad x Alto), 3U.
- Peso AR550-8FE: 1.6 kg
- Peso AR550-24FE: 2.1 kg
- Temperatura de operación -40°C a +70°C
- Humedad de operación 5% a 95%
- Nivel de protección IP: IP40

- Instalación en Riel DIN
- Alimentación

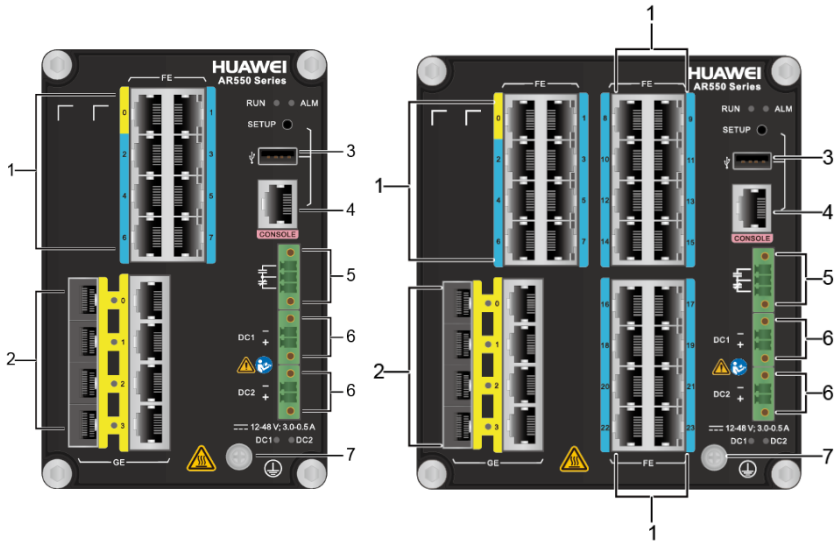
    - Módulos de alimentación redundante
    - 12 Vdc a 48 Vdc
- Compatibilidad EMC
    - FCC 47 CFR PART15, CLASS A
    - EN55022, CLASS A
    - VCCI, CLASS A
    - AS/NZS CISPAR 22 CLASS A, AN/NZS CISPR 24
    - ICES 003 CLASS A
    - CE
    - C-TICK (Australia)
    - ETSI EN 300386
    - IEC61000-4-2 (ESD): ±8 kV contact discharge, ±15 kV air discharge
    - IEC61000-4-3 (RS): 20 V/m, 80 MHz-2700 MHz
    - IEC61000-4-4 (EFT): Power cable: ±4 kV; data cable: ±4 kV
    - IEC61000-4-5 (Surge): Power cable: ±4 kV (CM)/±2 kV (DM); data cable: ±4 kV
    - IEC61000-4-6 (Conducted Disturbances Immunity)
    - IEC61000-4-8 (Power Frequency Magnetic Field Immunity)
    - IEC61000-4-9 (Pulse Magnetic Field Immunity)
    - IEC61000-4-10 (Damped Oscillatory Magnetic Field Immunity)
- Certificaciones
    - CB (IEC 60950)
    - NRTL (UL60950-1)
    - EU CE (EN 55022, EN 55024 y EN 300386)
    - USA FCC (47CFR Part 15)
    - Canadá IC (ICES-003)
    - Australia C-Tick (AS/NZS CIPSR22)

- Energía eléctrica IEC61850-3/IEEE1613 (subestación)
- EN50155 (ferrocarril)

c) Software

- Gestión de anillos en capa 2 STP, RSTP y MSTP, SEP
- IPv4/IPv6
  - IPv4 Unicast:
    - Ruteo estatico
    - RIP
    - RIPng
  - Multicast:
    - PIM-DM, PIM-SM, PIM-SSM
    - MSDP
    - IGMP, IGMP Snooping
    - MLD, MLD Snooping
- QoS
  - DiffServ (Servicios diferenciados)
  - Traffic shaping
  - HQoS Modular QoS (traffic class, traffic behavior, and traffic policy)
- Seguridad
  - Zone-based stateful firewall
  - Access Control List (ACL)
  - Autenticación 802.1X, MAC y web por AAA y RADIUS
  - Seguridad en ARP y defensa para ataques ICMP
  - Control para broadcast storm
  - Black list

Detalle del equipo:



Detalle switches Huawei AR550-8FE-D-H y AR550-24FE-D-H

1. 8 o 24 Interfaces FE RJ-45
2. 4 interfaces GE combo (RJ-45 / FO)
3. Interfaz USB
4. Consola
5. Contacto seco NO / NC
6. 2 conexiones de alimentación
7. Tierra

Los switches cuentan con varios Leds indicadores, dos de los más útiles son:

- Run / trabajando, color verde
    - Off: La tarjeta está alimentada pero su software interno no se ha iniciado
    - Slow blinking (Parpadeo lento): La tarjeta está alimentada y el software funciona normalmente
    - Fast blinking (Parpadeo rápido): El software se está iniciando
- ALM/ Alarma, color rojo

Módulos de Fibra óptica 1GE

SFP-GE-LX-SM310

Transceiver form factor	eSFP
Transmission speed	GE
Center wavelength (nm)	1310

Standards compliance	1000BASE-LX10
Connector type	LC
Applicable cable and maximum transmission distance	• Multimode fiber (OM1) (with diameter of 62.5 μm): 550 m • Multimode fiber (with diameter of 50 μm): 550 m • Multimode fiber (OM2) (with diameter of 50 μm): 550 m • Single-mode fiber (G.652) (with diameter of 9 μm): 10 km
Modal bandwidth	• Multimode fiber (OM1): 200/500 MHz*km • Multimode fiber: 400/400 MHz*km • Multimode fiber (OM2): 500/500 MHz*km • Single-mode fiber (G.652): -
Transmit power (dBm)	-9 to -3
Maximum receiver sensitivity (dBm)	-20
Overload power (dBm)	-3
Extinction ratio (dB)	≥ 9
Operating temperature	0°C to 70°C