Sistema de Comunicaciones y Telefonía del Metro de Granada. Descripción de la Instalación

Este documento ha sido generado electrónicamente y no necesita firma. No puede tener modificaciones manuales.				
	Nombre	**Empresa**	**Fecha**	**Firma**
Puesta en Vigor	A.M. López Raya	SIEMENS / I MO		
Revisado	A. d'Andrea	SIEMENS / I MO		
Autor	F. J. Choza	ACT Sistemas		

Índice de actualizaciones			
ED	Fecha	Motivo del cambio	Autor
A0	20/02/2017	Edición preliminar	F. J. Choza
B0	15/09/2017	Actualización as-built	F. J. Choza

INDICE

1. Introducción 5
2. Descripción general de la arquitectura 5
2.1. Red de Señalización 6
2.2. Red de Telemando de Energía 8
2.3. Red Multiservicio 10
2.4. Red WLAN de Talleres y Cocheras 13
2.5. Arquitectura lógica 13
2.6. Seguridad de Red 14
2.7. Telefonía IP 14
2.8. Gestión Centralizada: Cisco Prime 15
3. Instalación de cableado 16
3.1. Cableado de fibra óptica monomodo de la Red de Transmisión 16
3.2. Cableado de la Red Local de Acceso 23
3.2.1. Red local de parada en superficie, sin enclavamiento de señalización asociado 24
3.2.2. Red local de parada en superficie, con enclavamiento de señalización asociado 24
3.2.3. Red local de subestación eléctrica 25
3.2.4. Red local de estación subterránea, sin enclavamiento asociado 26
3.2.5. Red local de estación subterránea, con enclavamiento asociado 27
4. Equipamiento físico 27
4.1. Cisco 4506-E 27
4.2. Cisco IE3000 e IE4000 29
4.3. Switches de la serie 2960 29
4.3.1. Cisco 2960X 29
4.3.2. Cisco 2960 Series 31
4.4. Firewall Fortigate 32
4.5. FortiAnalyzer 33
4.6. IPS/IDS 33
4.7. Telefonía 34
4.8. Puntos de Acceso Wifi 34
4.9. Servidor Multiproposito Cisco UCS C220 M3 35
5. Configuración Lógica 35
5.1. Virtual Routing and Forwarding (VRF) 36
5.1.1. Configuración de VRF 37

5.2. Configuraciones VLANES e Interfaces 37
5.2.1. Configuración de vlanes 39
5.2.2. Configuración de interfaces vlanes 39
5.2.3. Interfaces Agregadas 40
5.2.4. Configuración entre los 4500 40
5.3. Configuraciones de macros 44
5.4. Configuración de QoS 45
5.5. Resilient Ethernet Protocol (REP) 49
5.5.1. Configuración de REP 49
5.6. Configuración de routing 51
5.7. Configuración global 52
5.7.1. Licencia. 52
5.7.2. IOS 52
5.7.3. Usuarios 52
5.7.4. Hora y fecha 53
5.7.5. Archive 53
5.7.6. Spanning-tree Protocol 53
5.7.7. VPT 54
5.7.8. SNMP 54
5.7.9. Line y VTY 54
5.8. Configuración Multicast 55
5.9. Configuración Lógica General IE3000 e IE4000 57
5.10. Configuración Lógica General c2960 58
6. Configuración Wifi 59
7. Seguridad 61
7.1. Seguridad interna. 61
7.1.1. El Enrutamiento Virtual y Reenvío (VRF) 61
7.1.2. VLANES 61
7.1.3. Port Security 62
7.1.4. Storm Control 62
7.1.5. Spaning-Tree 62
7.2. Seguridad Perimetral 62
7.2.1. Configuracion en HA 63
7.2.2. Interfaces 63
7.2.3. Routing 64
7.2.4. Firewall Objects 64
7.2.5. Políticas 65
7.2.6. Usuarios 66
8. Configuraciones especiales 67

8.1. Red Avanza y Logista 67
8.2. SCADA Local túnel 69
8.3. Control de tráfico Armilla 70
8.4. Conexión equipos Tetra 71
8.5. Conexión equipos AOPJA 72
8.6. CCAA MONDRAGONES 72
8.7. Enclavamientos Señalización 73
8.8. Punto de atención al cliente de Avanza (provisional) 73
9. Servidor Multipropósito 73
10. Telefonía 75
10.1. Centralita IP 76
10.2. Plan de numeración (rangos de extensiones) 76
10.3. Plan de enrutamiento de llamadas 78
10.4. Permiso de llamadas (CSS – Calling Search Space) 89
10.5. Grupos de Salto 90
10.6. Grupos de captura 90
10.7. Desvíos 91
10.8. DHCP 91
10.9. Servidor de grabación: CrossRecorder 92
10.9.1. Filtros 96
10.9.2. Detalles en grabaciones 96
11. Topología física 98
12. Topología lógica 100

1. Introducción

El presente documento describe la solución empleada para el Sistema de Comunicaciones y Telefonía IP del Metropolitano de Granada, dentro del PROYECTO DE CONSTRUCCIÓN DE SEÑALIZACIÓN, SEGURIDAD Y COMUNICACIONES DEL METRO LIGERO DE GRANADA.

El objetivo fundamental del proyecto es dotar al Metropolitano de Granada de un sistema robusto de comunicaciones que permita el correcto funcionamiento de sus diferentes servicios reduciendo al mínimo la posibilidad de una parada no controlada en alguno de ellos.

2. Descripción general de la arquitectura

En el presente apartado se describe la arquitectura general del equipamiento de comunicaciones IP objeto del Proyecto.
Se contempla un esquema de red jerárquico en el que un Nodo Central, compuesto por dos equipos en configuración redundante, instalados en la sala técnica de Talleres y Cocheras, que gestionan el tráfico de la red del corporativa del Metropolitano a través de los distintos nodos de acceso, que proporcionan conectividad IP, en cada una de las estaciones, paradas y subestaciones eléctricas, a los distintos subsistemas existentes:

- Señalización
- Telemando de Energía
- Gestión
- Semaforización
- Sistema de Información al viajero (SIV)
- Sistema de Ayuda a la Explotación (SAE)
- Telemando de Instalaciones/SCADA
- Sistema de Billetaje
- Telemetría Audio y de Megafonía de las estaciones/paradas
- Cronometría
- Interfonía IP
- Telefonía IP
- Video vigilancia IP
- Control de accesos

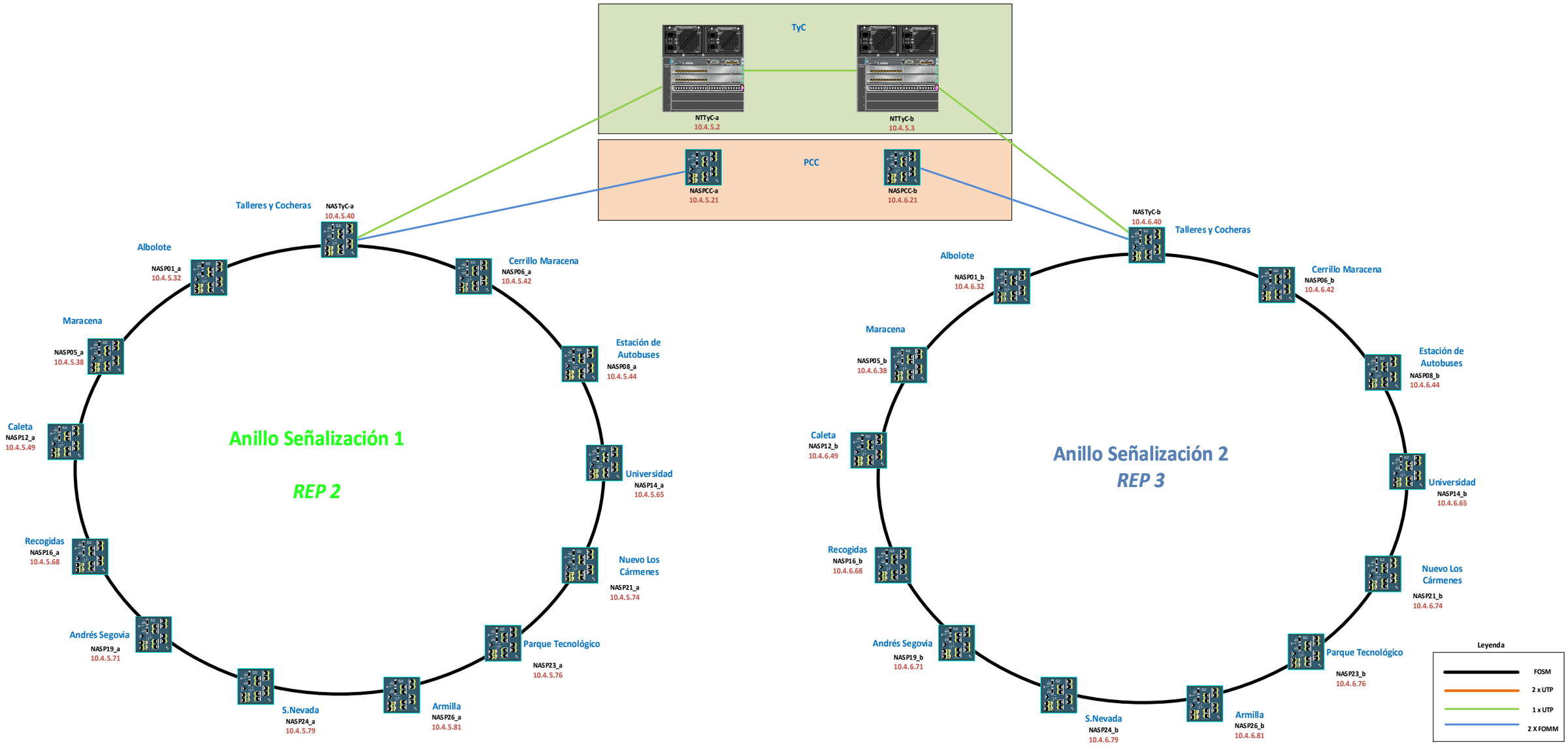
Cada nodo de acceso queda conectado de manera redundante al Nodo Central, mediante un anillo GbE de fibra óptica monomodo.
Dentro de la red corporativa del Metropolitano, se distingue entre 5 subredes, totalmente independientes entre sí:

- Red de Señalización A: cuenta con un nodo de acceso propio en cada una de las paradas/estaciones en las que existe un enclavamiento, así como otro nodo de acceso en el PCC, para conexión con los puestos de operador del sistema de señalización. Es una red exclusiva del sistema de Señalización. La única conexión física con el resto de las redes se realiza a través de los nodos de Core (Cisco 4500) exclusivamente para la gestión de la electrónica de red de la red de señalización.
- Red de Señalización B: cuenta con un nodo de acceso propio en cada una de las paradas/estaciones en las que existe un enclavamiento, así como otro nodo de acceso en el PCC, para conexión con los puestos de operador del sistema de señalización. Es una red exclusiva del sistema de Señalización. La única conexión física con el resto de las redes se realiza a través de los nodos de Core (Cisco 4500) exclusivamente para la gestión de la electrónica de red de la red de señalización.

- Red de Telemando de Energía: cuenta con un nodo de acceso propio en cada una de las subestaciones de tracción, así como en las subestaciones de acometida eléctrica y los centros de transformación de las paradas subterráneas. Es una red exclusiva del sistema de Telemando de Energía. Los nodos centrales de la red son los nodos de Core (Cisco 4500) ubicados en la sala técnica de TyC.
- Red Multiservicio: cuenta con un nodo de acceso en cada una de las paradas/estaciones y en cada una de las subestaciones de tracción y de acometida eléctrica. Adicionalmente cuenta con un switch aguas abajo del nodo de acceso de la parada/estación dedicado en exclusiva al servicio de Video vigilancia. La Red Multiservicio, da soporte al resto de subsistemas del Metropolitano, es decir: Semaforización, SIV, SAE, Telemando de Instalaciones, Billetaje, Audio/Megafonía, Interfonía, Telefonía, Video vigilancia y Control de accesos. Por último, se han instalado nodos de acceso en la sala técnica del PCC para conexión de los puestos de operador multiservicio y los KVM de los mismos, nodos de acceso en distintas ubicaciones de TyC y un nodo de acceso para para conexiones con la Red Corporativa de la Junta de Andalucía y el Operador.
- Red WLAN de Talleres y Cocheras: red inalámbrica que da cobertura a la zona de la playa de vías para la transmisión de datos entre los trenes y los equipos de Talleres.

2.1. Red de Señalización

Al tratarse de un sistema crítico, la red de comunicaciones del sistema de señalización tranviaria está totalmente redundada, distinguiéndose dos redes totalmente independientes.
En cada parada que lleva asociada un enclavamiento se han instalado sendos nodos de acceso, cada uno de ellos conectados físicamente a anillos de fibras independientes, que se gestionan desde el Nodo Central redundante de Talleres y Cocheras.
Las paradas que llevan asociadas un enclavamiento son: Albolote, Maracena, Cerrillo Maracena, Estación de Autobuses, Caleta, Universidad, Recogidas, Andrés Segovia, Nuevo Los Cármenes, Parque Tecnológico, Sierra Nevada y Armilla.
Así mismo se han instalado sendos nodos de acceso en la sala técnica de Talleres y cocheras, que dan servicio al enclavamiento previsto en la playa de vías. Igualmente, se han instalado dos nodos de acceso a la red de señalización en la sala PCC, para conexión de los puestos de operador con el Nodo Central, mediante fibra óptica multimodo.
A continuación, podemos ver un esquema de la arquitectura de los anillos de señalización donde se muestra a su vez la IP de gestión de cada nodo:


TyC
NTTyC-a
10.4.5.2
NTTyC-b
10.4.5.3
PCC
NASPCC-a
10.4.5.21
NASPCC-b
10.4.6.21
Talleres y Cocheras
NASTyC-a
10.4.5.40
Albolote
NASP01_a
10.4.5.32
Cerrillo Maracena
NASP06_a
10.4.5.42
Maracena
NASP05_a
10.4.5.38
Estación de Autobuses
NASP08_a
10.4.5.44
Caleta
NASP12_a
10.4.5.49
Anillo Señalización 1
REP 2
Universidad
NASP14_a
10.4.5.65
Recogidas
NASP16_a
10.4.5.68
Nuevo Los Cármenes
NASP21_a
10.4.5.74
Andrés Segovia
NASP19_a
10.4.5.71
Parque Tecnológico
NASP23_a
10.4.5.76
S.Nevada
NASP24_a
10.4.5.79
Armilla
NASP26_a
10.4.5.81
NASTyC-b
10.4.6.40
Talleres y Cocheras
Albolote
NASP01_b
10.4.6.32
Cerrillo Maracena
NASP06_b
10.4.6.42
Maracena
NASP05_b
10.4.6.38
Estación de Autobuses
NASP08_b
10.4.6.44
Caleta
NASP12_b
10.4.6.49
Anillo Señalización 2
REP 3
Universidad
NASP14_b
10.4.6.65
Recogidas
NASP16_b
10.4.6.68
Nuevo Los Cármenes
NASP21_b
10.4.6.74
Andrés Segovia
NASP19_b
10.4.6.71
Parque Tecnológico
NASP23_b
10.4.6.76
S.Nevada
NASP24_b
10.4.6.79
Armilla
NASP26_b
10.4.6.81
Leyenda
FOSM
2 x UTP
1 x UTP
2 X FOMM

El documento anexo “switches” muestra la configuración de los puertos de cada uno de estos switches (VLAN) y el dispositivo final que conecta con cada uno de estos.

El esquema general y detallado de la red de señalización se muestra en el documento anexo “diagrama_red”.

Como nodos de accesos a la red de comunicaciones del sistema de señalización, se han instalado switches industriales Cisco IE3000 con 8 puertos 100Base-Tx y dos puertos 1000Base-LX. Las especificaciones técnicas de estos equipos se detallan más adelante.

En el documento anexo “Equipamiento de red” se detallan los equipos instalados en cada ubicación.

A pesar de ser una red independiente de los nodos de core Cisco 4500, ya que estos no forman parte del anillo de señalización, es desde dichos nodos desde donde se realiza la gestión de todos los nodos correspondientes a los anillos de señalización.

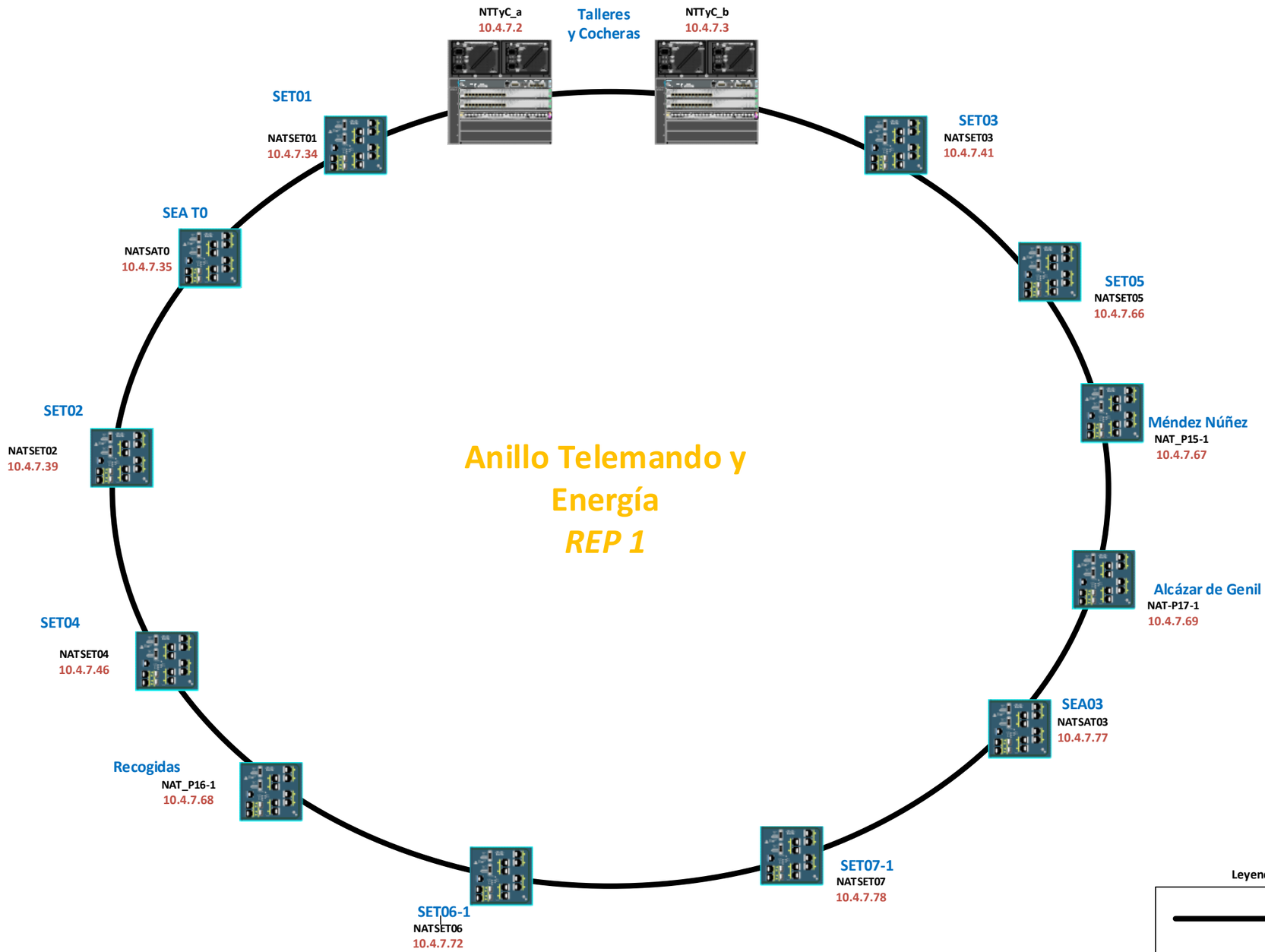
2.2. Red de Telemando de Energía

En cada una de las subestaciones de tracción instaladas a lo largo de la línea, así como en las subestaciones de acometida eléctrica, se ha instalado un nodo de acceso que conecta con el Nodo Central mediante un anillo de fibra óptica monomodo dedicado. Además, para la conexión de los centros de transformación de las estaciones subterráneas, se ha instalado en las mismas otro nodo de acceso.

El listado de subestaciones en las que se han instalado los nodos de acceso a la red de telemando de energía es el siguiente:

- Subestación de tracción de Juncaril
- Subestación de acometida de Juncaril
- Subestación de tracción de Talleres y Cocheras
- Subestación de tracción de Cerrillo Maracena
- Subestación de tracción de Argentinita
- Subestación de tracción de Universidad
- Centro de transformación de Méndez Núñez
- Centro de transformación de Recogidas
- Centro de transformación de Alcázar de Genil
- Subestación de tracción de Palacio de Deportes
- Subestación de acometida de Nevada
- Subestación de tracción de Sierra Nevada

En la sala PCC, para la conexión de los puestos de operador de Telemando de Energía con el Nodo Central, mediante fibra óptica multimodo, se utilizan los nodos de acceso previstos para Multiservicio, dado que el puesto de operación de SCADA y Telemando de Energía es compartido para ambos servicios. A continuación, podemos ver un esquema de la arquitectura del anillo de Telemando de Energía donde se muestra a su vez la IP de gestión de cada nodo:


NTTyC_a
10.4.7.2
Talleres
y Cocheras
NTTyC_b
10.4.7.3
SET01
NATSET01
10.4.7.34
SET03
NATSET03
10.4.7.41
SEA T0
NATSAT0
10.4.7.35
SET05
NATSET05
10.4.7.66
SET02
NATSET02
10.4.7.39
Méndez Núñez
NAT_P15-1
10.4.7.67
Anillo Telemando y
Energía
REP 1
Alcázar de Genil
NAT-P17-1
10.4.7.69
SET04
NATSET04
10.4.7.46
SEA03
NATSAT03
10.4.7.77
Recogidas
NAT_P16-1
10.4.7.68
SET07-1
NATSET07
10.4.7.78
SET06-1
NATSET06
10.4.7.72
Leyenda
FOSM
FOMM

El esquema general y detallado de la red de telemando de energía se muestra en el documento anexo “diagrama_red”.

Como nodos de accesos a la red de comunicaciones del sistema de telemando de energía, se han instalado switches industriales, de las mismas características que los de la red de señalización, es decir, con 8 puertos 100Base-Tx y dos puertos 1000Base-LX. Las especificaciones técnicas de estos equipos se detallan más adelante.

En el documento anexo “Equipamiento de red” se detallan los equipos instalados en cada ubicación.

La gestión de todos los nodos de la red de Telemando y Energía se realiza a través de los nodos de Core Cisco 4500, los cuales pertenecen al anillo de Telemando de Energía.

2.3. Red Multiservicio

En todas las paradas, estaciones subterráneas y subestaciones eléctricas, se ha instalado un nodo de acceso a la red de comunicaciones Multiservicio, que proporciona conectividad IP al resto de subsistemas del Metropolitano, que se han configurado como redes virtuales independientes (VLANs): Semaforización, SIV, SAE, Telemando de Instalaciones, Billetaje, Audio/Megafonía, Cronometría, Interfonía/Telefonía, Video vigilancia, radio TETRA y Control de accesos. Cada nodo de acceso de la red Multiservicio enlaza de forma redundante con el Nodo Central de Talleres y Cocheras mediante un anillo de fibra óptica monomodo. Como caso especial, el servicio de Videovigilancia, cuenta con un switch aguas abajo del nodo de acceso de parada/estación, dedicado en exclusiva a proporcionar conectividad IP a las videocámaras IP.
Igualmente, se han instalado nodos de acceso a la red multiservicio en las siguientes ubicaciones:

- En Sala Técnica de Talleres y Cocheras, un nodo de acceso para dar servicio los equipos terminales de este emplazamiento.
- En la garita de control de acceso a Talleres y Cocheras, un nodo de acceso para el equipamiento cercano a la misma.

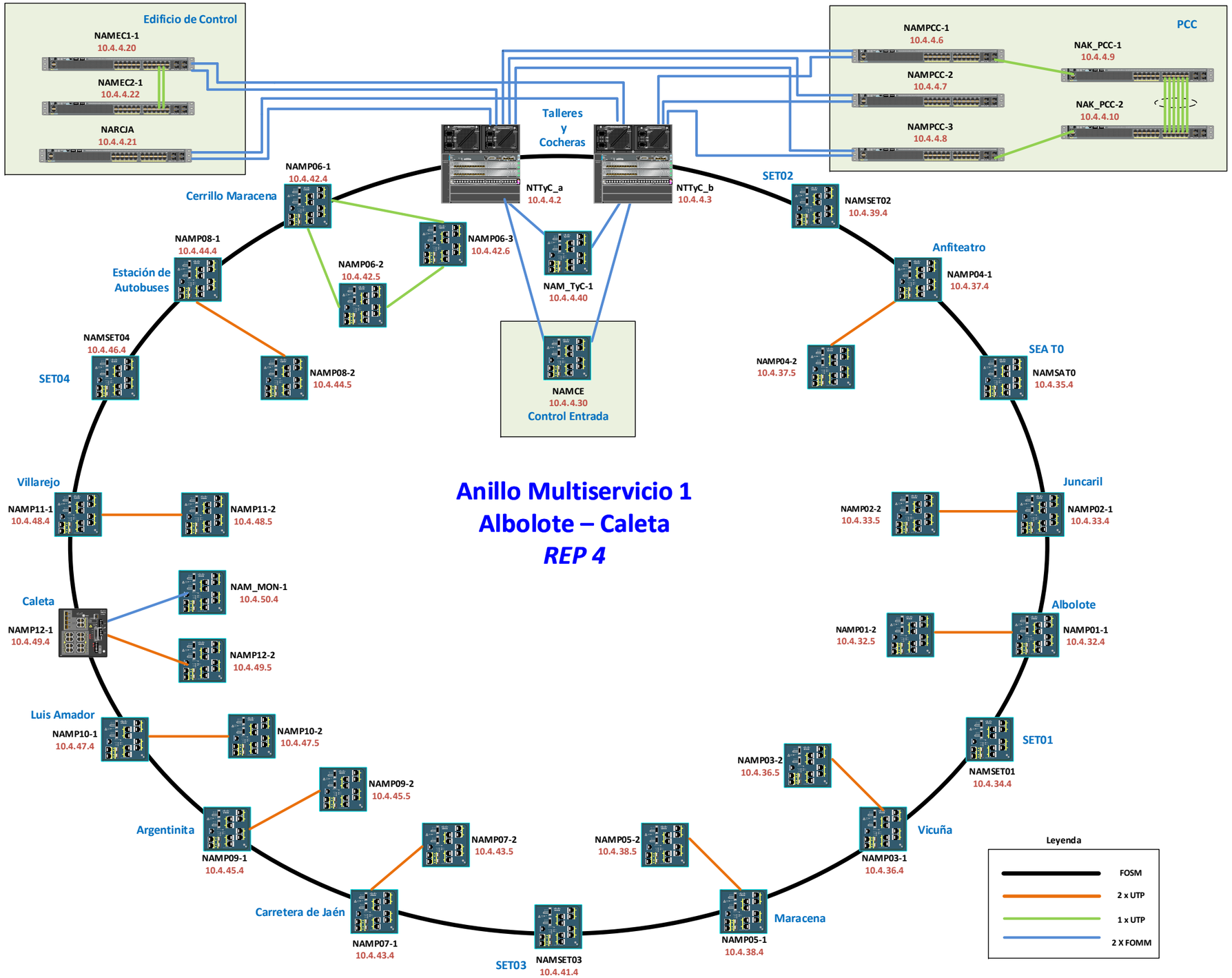
- En Sala Técnica del PCC, tres nodos de acceso (NAMPCC-1, NAMPCC-2, NAMPCC-3) para conexión de los puestos de operador con el Nodo Central, mediante fibra óptica multimodo, estando conectado cada uno de los tres nodos de acceso del PCC con los 3 principales operadores respectivamente, y un nodo para conexiones con las redes de la Red Corporativa de la Junta de Andalucía.

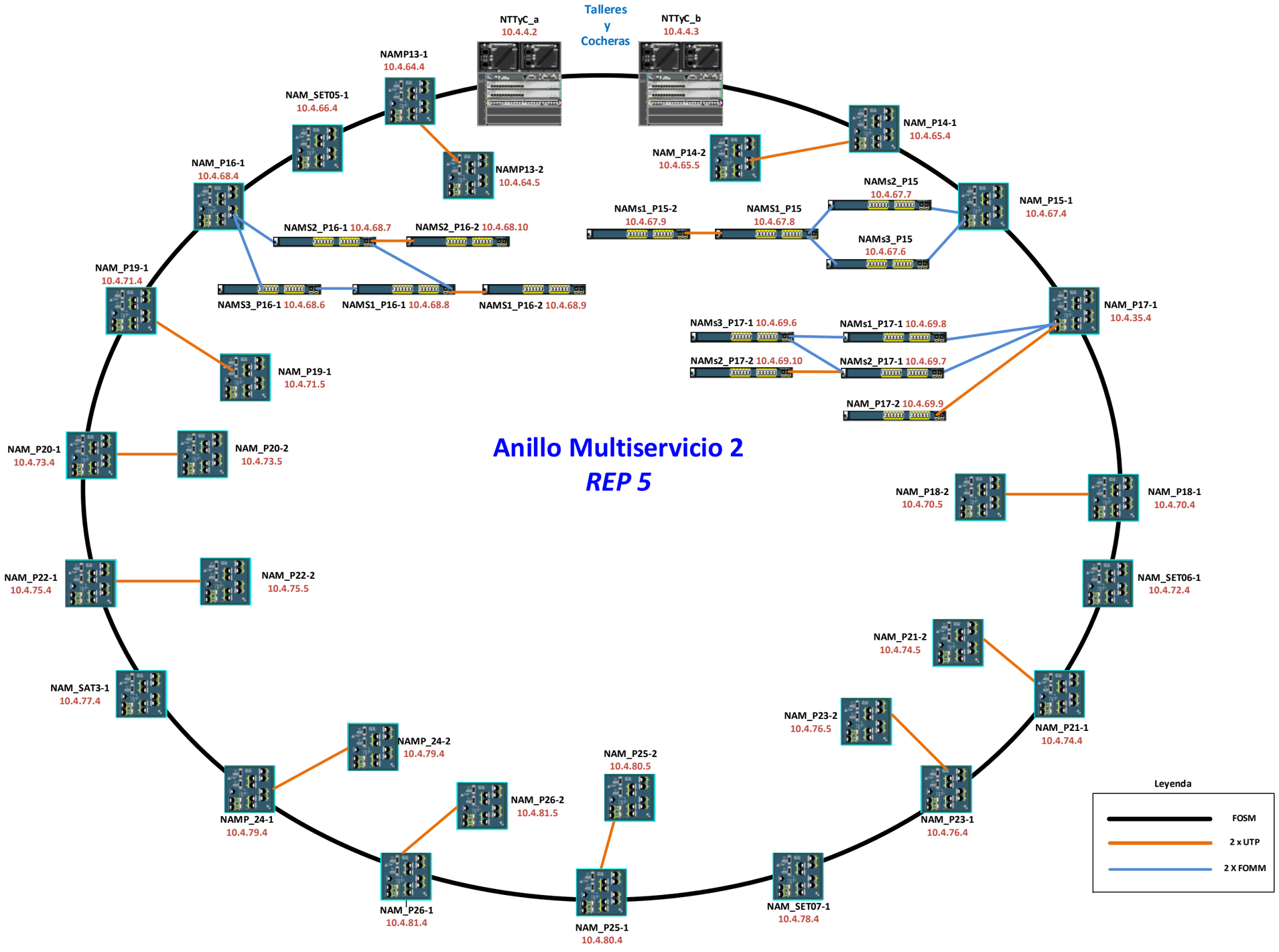
- En la Sala Técnica del PCC, dos nodos de acceso (NAK-1 y NAK-2) para visualización en las pantallas de operadores de la información de cada una de las distintas técnicas a través del sistema KVM. Dado el gran ancho de banda que atraviesa la conexión entre estos dos nodos, se encuentran interconectados entre sí mediante un PortChannel compuesto por 6 enlaces, así como conectados contra los nodos del punto anterior (NAMPCC-X) formando un semianillo. (Ver esquema general anexo “diagrama_red”). El método de balanceo de carga elegido para la configuración del port-channel y que reporta la mejor performance de red ha sido **src-ip** (source ip).

- En la Sala Técnica del PCC, un nodo de acceso para para conexiones con las redes de la Red Corporativa de la Junta de Andalucía.

- En el Edificio de Control de Talleres y Cocheras, se ha instalado un nodo de acceso de 48 puertos en la sala auxiliar de la planta primera y otro en la de la planta segunda para dar servicio a las oficinas de trabajo del explotador de la línea y a las oficinas destinadas a personal administrativo de la Agencia de Obra Pública de la Junta de Andalucía y del operador.

A continuación, podemos ver varios esquemas con la arquitectura de la red de multiservicio donde se muestra a su vez la IP de gestión de cada nodo.


Edificio de Control
NAMEC1-1
10.4.4.20
NAMEC2-1
10.4.4.22
NARCJA
10.4.4.21
PCC
NAMPCC-1
10.4.4.6
NAMPCC-2
10.4.4.7
NAMPCC-3
10.4.4.8
NAK_PCC-1
10.4.4.9
NAK_PCC-2
10.4.4.10
Talleres y Cocheras
NTTyC_a
10.4.4.2
NTTyC_b
10.4.4.3
SET02
NAMSET02
10.4.39.4
Cerrillo Maracena
NAMP06-1
10.4.42.4
NAMP06-2
10.4.42.5
NAMP06-3
10.4.42.6
NAM_TyC-1
10.4.4.40
Anfiteatro
NAMP04-1
10.4.37.4
NAMP04-2
10.4.37.5
SEA T0
NAMSAT0
10.4.35.4
Estación de Autobuses
NAMP08-1
10.4.44.4
NAMP08-2
10.4.44.5
SET04
NAMSET04
10.4.46.4
NAMCE
10.4.4.30
Control Entrada
Anillo Multiservicio 1
Albolote – Caleta
REP 4
Villarejo
NAMP11-1
10.4.48.4
NAMP11-2
10.4.48.5
Juncaril
NAMP02-2
10.4.33.5
NAMP02-1
10.4.33.4
Caleta
NAMP12-1
10.4.49.4
NAM_MON-1
10.4.50.4
NAMP12-2
10.4.49.5
Albolote
NAMP01-2
10.4.32.5
NAMP01-1
10.4.32.4
Luis Amador
NAMP10-1
10.4.47.4
NAMP10-2
10.4.47.5
SET01
NAMSET01
10.4.34.4
NAMP03-2
10.4.36.5
NAMP09-2
10.4.45.5
Argentinita
NAMP09-1
10.4.45.4
NAMP07-2
10.4.43.5
Vicuña
NAMP03-1
10.4.36.4
NAMP05-2
10.4.38.5
Carretera de Jaén
NAMP07-1
10.4.43.4
SET03
NAMSET03
10.4.41.4
Maracena
NAMP05-1
10.4.38.4
Leyenda
FOSM
2 x UTP
1 x UTP
2 X FOMM


Talleres y Cocheras
NTTyC_a
10.4.4.2
NTTyC_b
10.4.4.3
NAMP13-1
10.4.64.4
NAM_SET05-1
10.4.66.4
NAMP13-2
10.4.64.5
NAM_P14-1
10.4.65.4
NAM_P14-2
10.4.65.5
NAM_P16-1
10.4.68.4
NAMS2_P16-1 10.4.68.7
NAMS2_P16-2 10.4.68.10
NAMs1_P15-2
10.4.67.9
NAMS1_P15
10.4.67.8
NAMs2_P15
10.4.67.7
NAMs3_P15
10.4.67.6
NAM_P15-1
10.4.67.4
NAM_P19-1
10.4.71.4
NAMS3_P16-1 10.4.68.6
NAMS1_P16-1 10.4.68.8
NAMS1_P16-2 10.4.68.9
NAM_P19-1
10.4.71.5
NAMs3_P17-1 10.4.69.6
NAMs1_P17-1 10.4.69.8
NAMs2_P17-2 10.4.69.10
NAMs2_P17-1 10.4.69.7
NAM_P17-1
10.4.35.4
NAM_P17-2 10.4.69.9
NAM_P20-1
10.4.73.4
NAM_P20-2
10.4.73.5
Anillo Multiservicio 2
REP 5
NAM_P18-2
10.4.70.5
NAM_P18-1
10.4.70.4
NAM_SET06-1
10.4.72.4
NAM_P22-1
10.4.75.4
NAM_P22-2
10.4.75.5
NAM_P21-2
10.4.74.5
NAM_SAT3-1
10.4.77.4
NAM_P23-2
10.4.76.5
NAM_P21-1
10.4.74.4
NAMP_24-2
10.4.79.4
NAM_P25-2
10.4.80.5
NAM_P26-2
10.4.81.5
NAMP_24-1
10.4.79.4
NAM_P23-1
10.4.76.4
NAM_P26-1
10.4.81.4
NAM_P25-1
10.4.80.4
NAM_SET07-1
10.4.78.4
Leyenda
FOSM
2 x UTP
2 X FOMM

El documento Anexo “Switches” muestra configuración de los puertos de cada uno de estos switches (VLAN) y el dispositivo final que conecta con cada uno de estos.
Dado el alto número de nodos de acceso a la red multiservicio, se ha dividido la misma en dos anillos independientes, con el objetivo de reducir los tiempos de acceso a la red. El primer anillo parte de la parada de Albolote y, pasando por el Nodo Central del PCC de Talleres y Cocheras, llega hasta la parada de Caleta. El segundo anillo parte de la parada de Estación de Ferrocarril y pasa por todas las paradas desde ésta hasta el final de la línea llegando a la parada de Universidad donde vuelve otra vez a Estación de Ferrocarril, pasando entre ambas por el Nodo Central del PCC de Talleres y Cocheras.

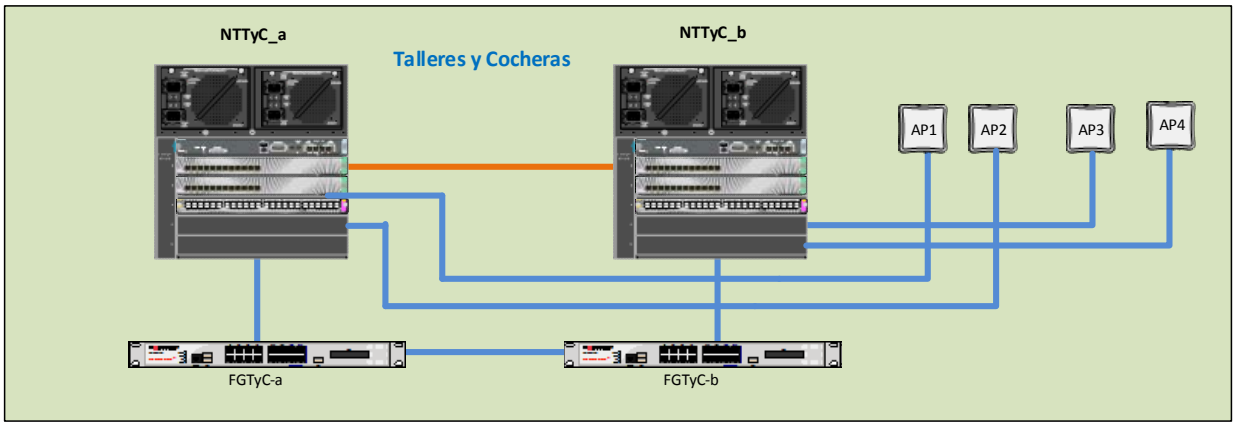
El esquema general y detallado de la red multiservicio se muestra en el siguiente documento anexo “diagrama_red”.

Como nodos de accesos a la red de comunicaciones multiservicio, se han instalado switches industriales, con al menos 24 puertos 100Base-Tx y dos puertos 1000Base-LX. Para el servicio de Video vigilancia, se han instalado igualmente switches industriales con hasta 10 puertos disponibles 100Base-Tx. En las estaciones subterráneas y en Talleres y Cocheras se han instalado switches no industriales de 24 y 48 puertos.

En el documento anexo “Equipamiento de red” se detallan los equipos instalados en cada ubicación.

2.4. Red WLAN de Talleres y Cocheras

Se ha instalado una red inalámbrica WLAN en la zona de la playa de vías de Talleres y Cocheras. El objetivo de esta red es la de posibilitar el intercambio rápido de información entre los equipos embarcados de los sistemas SAE y Billetaje con los servidores centrales de Talleres y Cocheras.
Para ello, se han suministrado e instalado cuatro puntos de acceso en armarios de intemperie, sobre postes de catenaria en la zona de la playa de vías. Cada punto de acceso queda conectado mediante fibra óptica multimodo al Nodo Central.
El esquema de la red WLAN de Talleres y Cocheras, se muestra en la siguiente imagen:



2.5. Arquitectura lógica

La arquitectura lógica propuesta plantea que, para cada servicio de la red multiservicio, se establecen al menos 4 VLANs distintas:
1. Una primera VLAN en la que se ubican los equipos, asociados al servicio en cuestión, distribuidos por el anillo 1 (anillo que recoge emplazamientos desde Albolote a Caleta).
2. Una segunda VLAN en la que se ubican los equipos, asociados al servicio en cuestión, distribuidos por el anillo 2 (anillo que recoge emplazamientos desde Caleta hasta Armilla).
3. Una tercera VLAN en la que se ubican los servidores del servicio en cuestión ubicados en la "Sala Técnica" de Talleres y Cocheras.
4. Una cuarta VLAN cortafuegos del servicio considerado.

5. Una quinta VLAN donde se ubican los equipos de ofimática de los administradores y operadores de ese servicio en cuestión, en el PCC.

2.6. Seguridad de Red

Para dotar de seguridad a la red de comunicaciones IP del metropolitano, se ha llevado a cabo la instalación y configuración de un sistema completo de seguridad de red, así como un sistema de gestión y generación de informes que refuerza la integridad y seguridad de los datos transmitidos a través de la red corporativa.
Se ha optado por un planteamiento mixto:
Por una parte, se ha instalado un sistema de seguridad perimetral hacia el exterior, con la inclusión de dos firewalls en alta disponibilidad (HA), así como un generador de informes y agregador de logs para gestionar el conjunto.
Por otra parte, la seguridad interna se ha reforzado con la inclusión de un sistema mixto de prevención y detección de intrusos (IPS/IDS) que monitorice el tráfico interno de la red, alertando y previniendo posibles ataques.
El objetivo es el de proteger las distintas redes que conforman la red de comunicaciones del Metropolitano de injerencias que puedan provenir tanto del exterior como del interior. Especial mención tiene la red de señalización, ya que, al tratarse de una red crítica, ha de garantizarse su blindaje frente a posibles usos indeseados.
Se ha configurado la seguridad a nivel de red de forma que se posibilite una comunicación segura con el exterior, dadas las necesidades existentes de interacción de varios de los sistemas del metropolitano, con entidades externas como, por ejemplo:

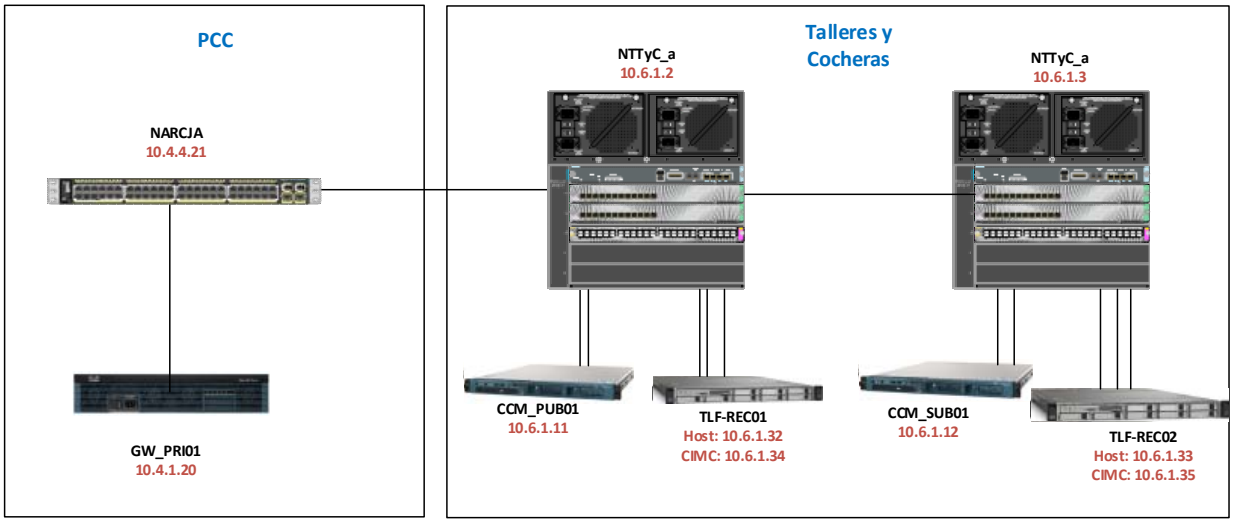
- Comunicaciones entre el sistema de billética y entidades bancarias.
- Visualización de las imágenes de videovigilancia en entidades externas tales como ayuntamientos o policía.
- Comunicaciones vocales entre la red telefónica privada del metropolitano y la red telefónica pública.
- Puestos de trabajo remotos del personal de explotación del metropolitano.

2.7. Telefonía IP

El sistema de telefonía del Metropolitano de Granada está basado en tecnología IP y se compone de los siguientes elementos:

- Cluster Servidor de llamadas: Es el elemento central, el cerebro de la red de telefonía IP. Se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, traducción de direcciones, administración de zonas, autorización y administración de llamadas, etc. Sus principales características se detallan más adelante.
- Gateway de voz (Pasarela): Es el dispositivo encargado de proporcionar el acceso hacia las redes exteriores a los terminales de la red IP conectados a él.
- Grabador de voz: Se han instalado equipos especiales de grabación digital compatibles con la centralita IP a instalar, para cumplir con los requisitos legales de seguridad. Las grabaciones son accesibles y se pueden almacenar mensajes para recuperarlos posteriormente.
- Teléfonos IP: Como terminal de usuario de telefonía se han utilizado terminales telefónicos IP estándar, homologados para su utilización en la red telefónica pública europea. Se distinguen tres tipos de terminales: de funcionalidad básica, de funcionalidad media y de funcionalidad avanzada.

A continuación, se incluye un esquema con la electrónica de red del sistema de telefonía:



Como podemos observar, en la sala del PCC se encuentra el Gateway Primario (cisco 2601) conectado al switch NARCJA (cisco 2960), localizado también en el PCC. Este switch se conecta a su vez al core de la red (c4500). Esta arquitectura se debe al hecho de que el acceso primario a la red de telefonía pública se encuentra en la sala del PCC, y a que la conexión entre dicho acceso y gateway de telefonía IP debe ser mediante un cable dicrecto, no permitiendo la existencia de electrónica de red entre ambos.

Los servidores de Call Manager (COM_PUB01 y COM_SUB01) han sido instalados en la sala técnica de Talleres y Cocheras, directamente conectados a sendos cores de la red (NTTyC_a y NTTyC_b) respectivamente.
Así mismo, los servidores de grabación (TLF-REC01 y TLF-REC02) están en la sala técnica de Talleres y Cocheras, conectados a los switches de core de la red.

2.8. Gestión Centralizada: Cisco Prime

La gestión centralizada de todo el equipamiento de red se realiza a través del software de monitorización Cisco Prime Infrastructure 1.2 instalado sobre el servidor de comunicaciones instalado en la sala técnica de Talleres y Cocheras e identificado mediante la IP 10.4.1.11.

Esta plataforma es accesible a través de la siguiente URL:

https://10.4.1.11/CSCOnm/servlet/login/login.jsp

El usuario y contraseña ha sido suministrado en el documento de contraseñas

Mediante los diferentes interfaces que ofrece Cisco Prime se realizan las siguientes funcionalidades principales:

- **Monitorización y Troubleshooting:**

Todos los equipos reportan las alarmas y traps configurados. Cisco Prime muestra una lista con todos los eventos o fallas de cada uno de los equipos (Enlace con alto consumo, utilización de CPU, desconexión de equipo, desconexión de enlace…).

- **Gestión de la Configuración**

Mediante Cisco Prime podemos acceder a la configuración de cada equipo y realizar cambios en sus parámetros de forma centralizada.

- **Reportes:**

Cisco Prime permite generar una serie de informes con el estado de todos los equipos incluyendo el detalle de las funcionalidades que interesen en cada momento.

- **Mantenimiento:**

La gestión centralizada de todos los equipos permite una fácil administración de versiones de firmware de los mismos.

Se anexa una Guía Básica de utilización de Cisco Prime en la que se detallan las principales funcionalidades.

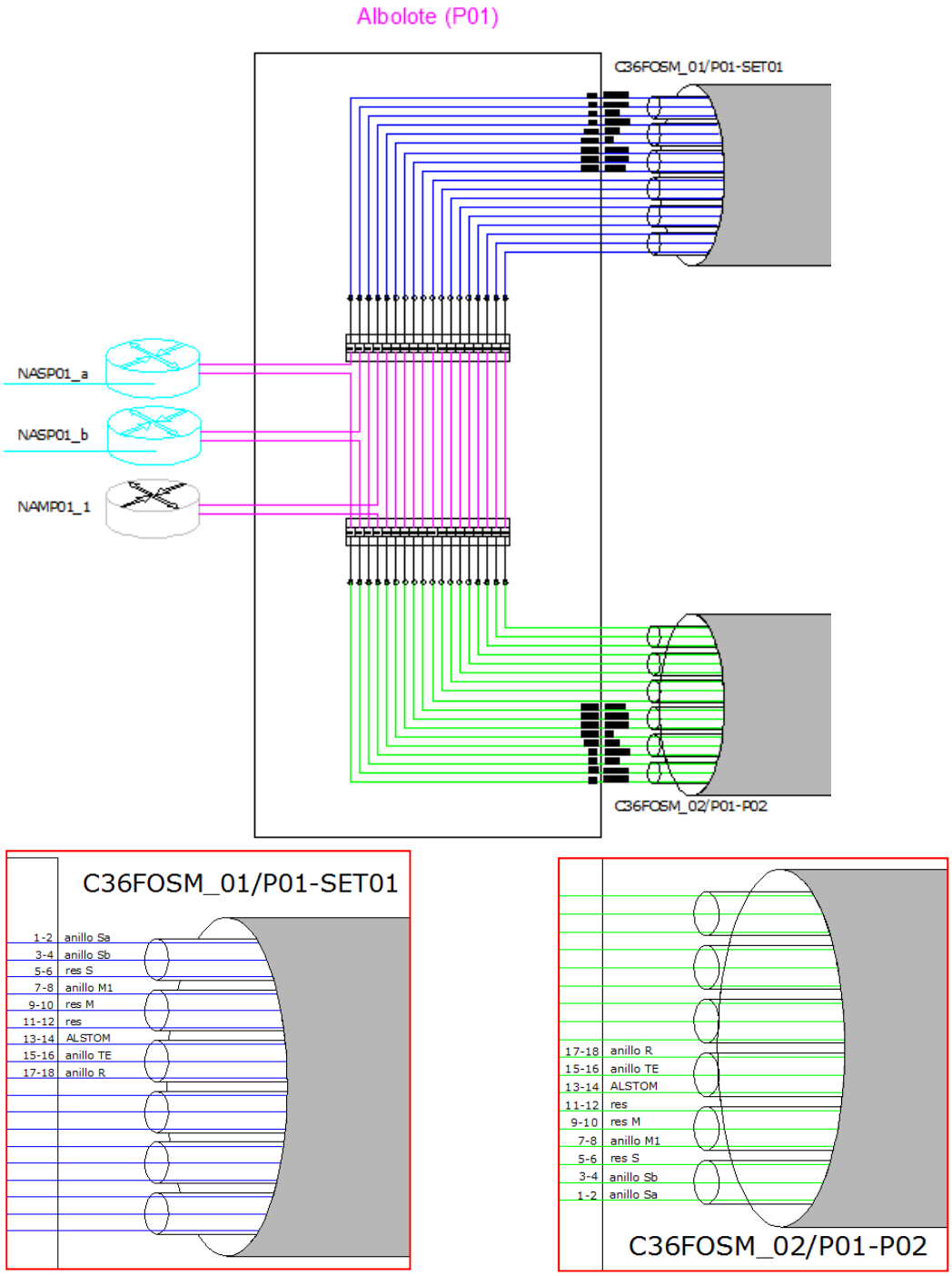
3. Instalación de cableado

3.1. Cableado de fibra óptica monomodo de la Red de Transmisión

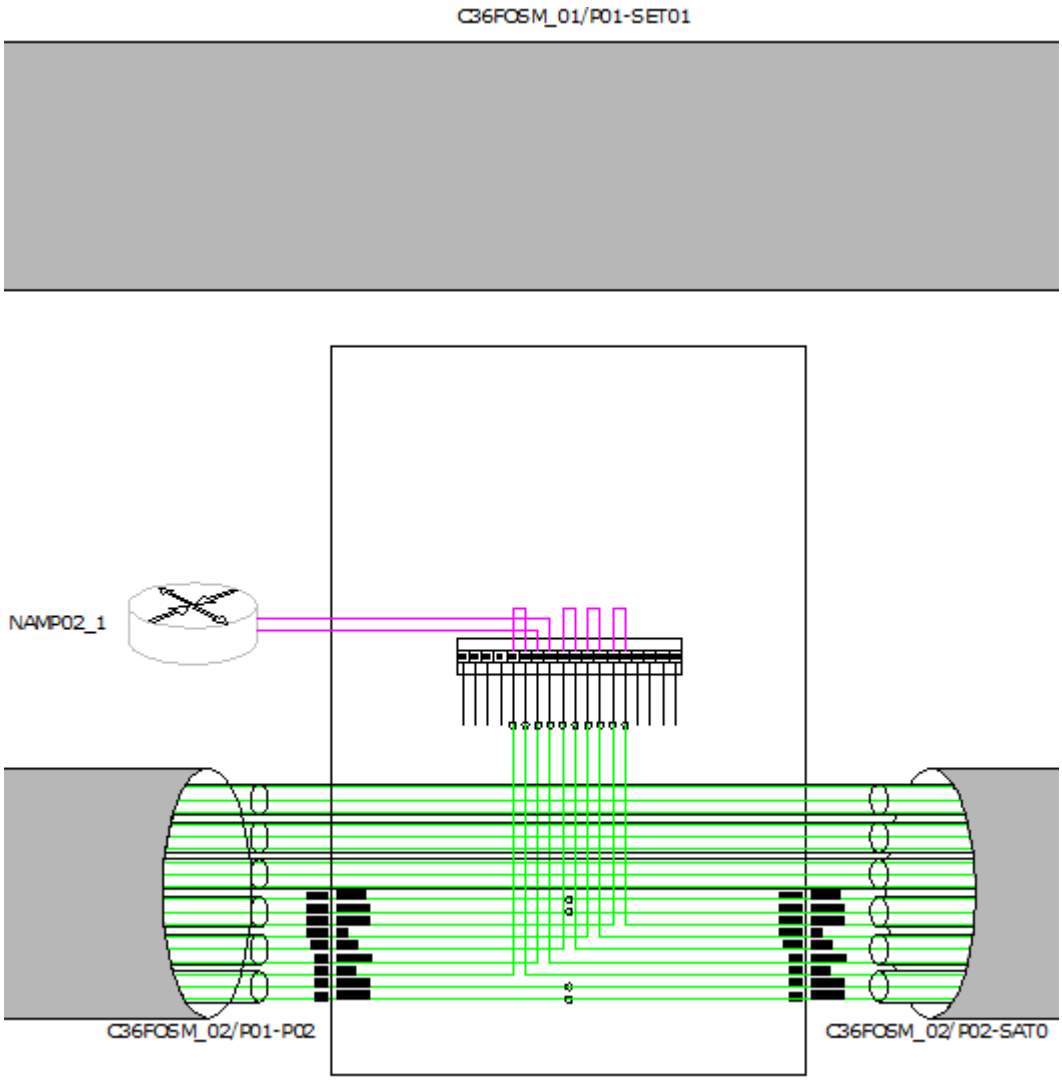
Como medio físico de transmisión se han empleado sendos cables de 36 fibras ópticas monomodo, instalados a ambos lados de la vía por las canalizaciones existentes previstas a tal efecto.
El cable está compuesto por 6 tubos de 6 fibras ópticas OS1 cada uno y es apto para instalaciones tanto en exteriores como en exteriores, contando con una armadura de protección.
Sólo se terminan los 2 cables al completo en las siguientes ubicaciones:

- Parada de Albolote (inicio de la línea)
- Sala técnica de Talleres y Cocheras
- Parada de Caleta (fin del primer tramo de la línea)
- Parada de Armilla (fin de la línea)

En el resto de ubicaciones (paradas, y subestaciones eléctricas), únicamente se acomete con uno de los dos cables de fibras (según planos constructivos) excepto en las estaciones subterráneas, a las que se acomete con sendos cables.
Los tubos cuyas fibras no se utilizan en la parada a la que acometen (tubos de reserva), no son cortados si no que se han dejado en paso dentro del repartidor de fibras. Así, los paneles repartidores cuentan con bandejas que permiten la correcta organización de fibras, de tal forma que es posible tanto terminar la fibra óptica mediante fusiones a pigtails preconectorizados, como alojar empalmes de paso. Los paneles repartidores de fibras monomodo se han instalado en bastidores de 19'' en las marquesinas de paradas y en armarios racks en las subestaciones eléctricas, estaciones subterráneas y salas técnicas de talleres y cocheras.
A continuación se muestran algunas imágenes de los distintos tipos de conectorización de los cables de fibra óptica monomodo a lo largo de la traza (para más información, consultar los planos constructivos adjuntos).

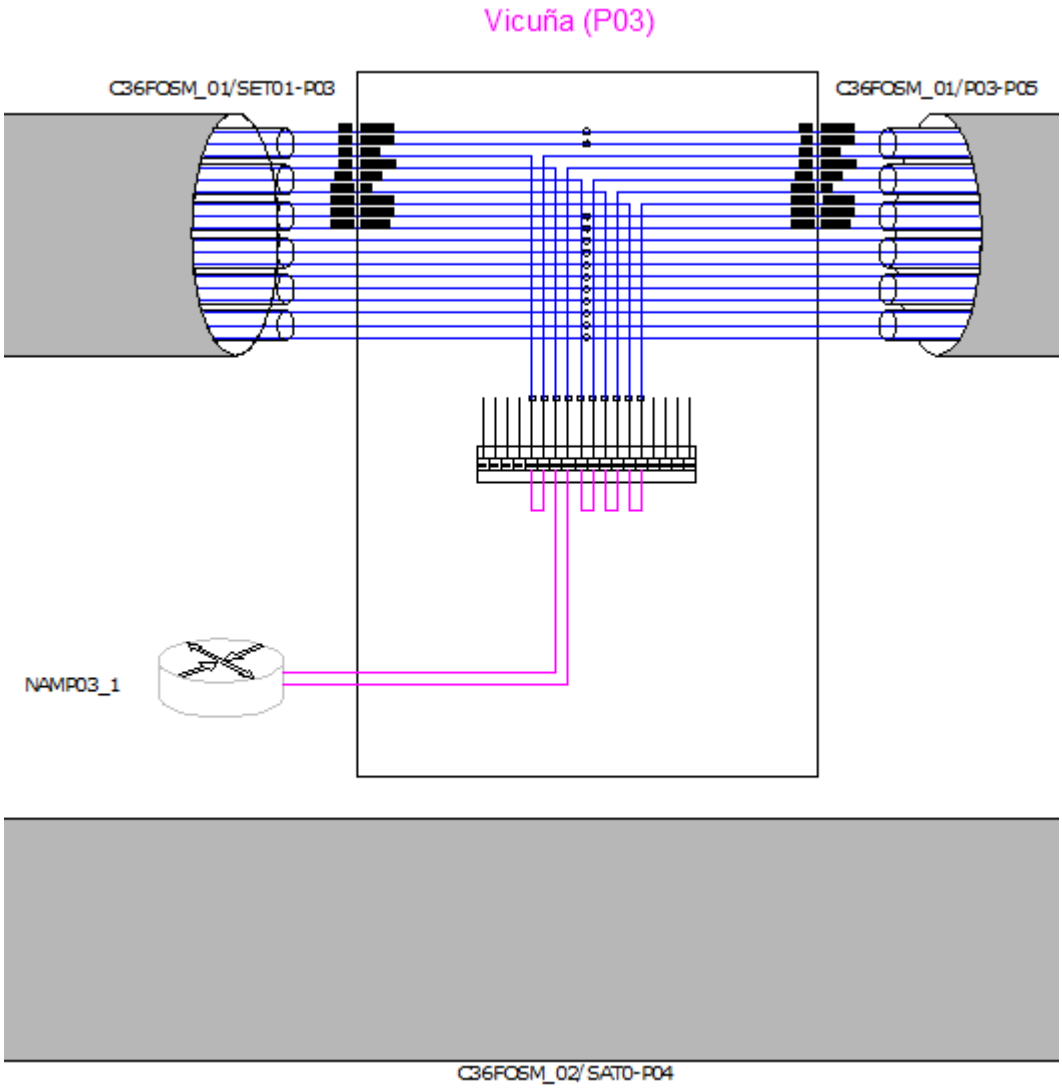


Esquema de Conexionado parada de inicio (Albolote). Se fusionan los dos cables completos.

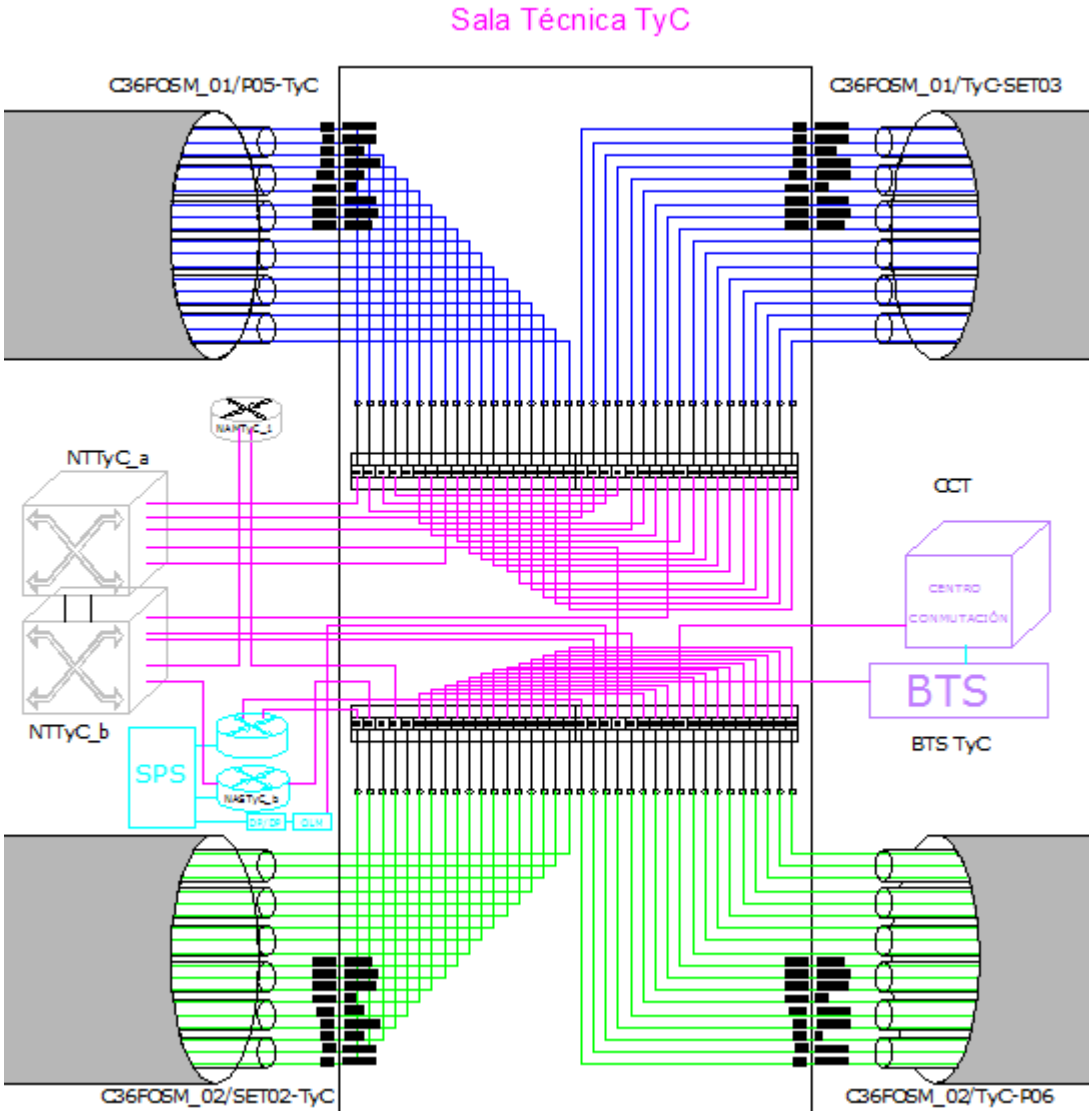


Juncaril (P02)

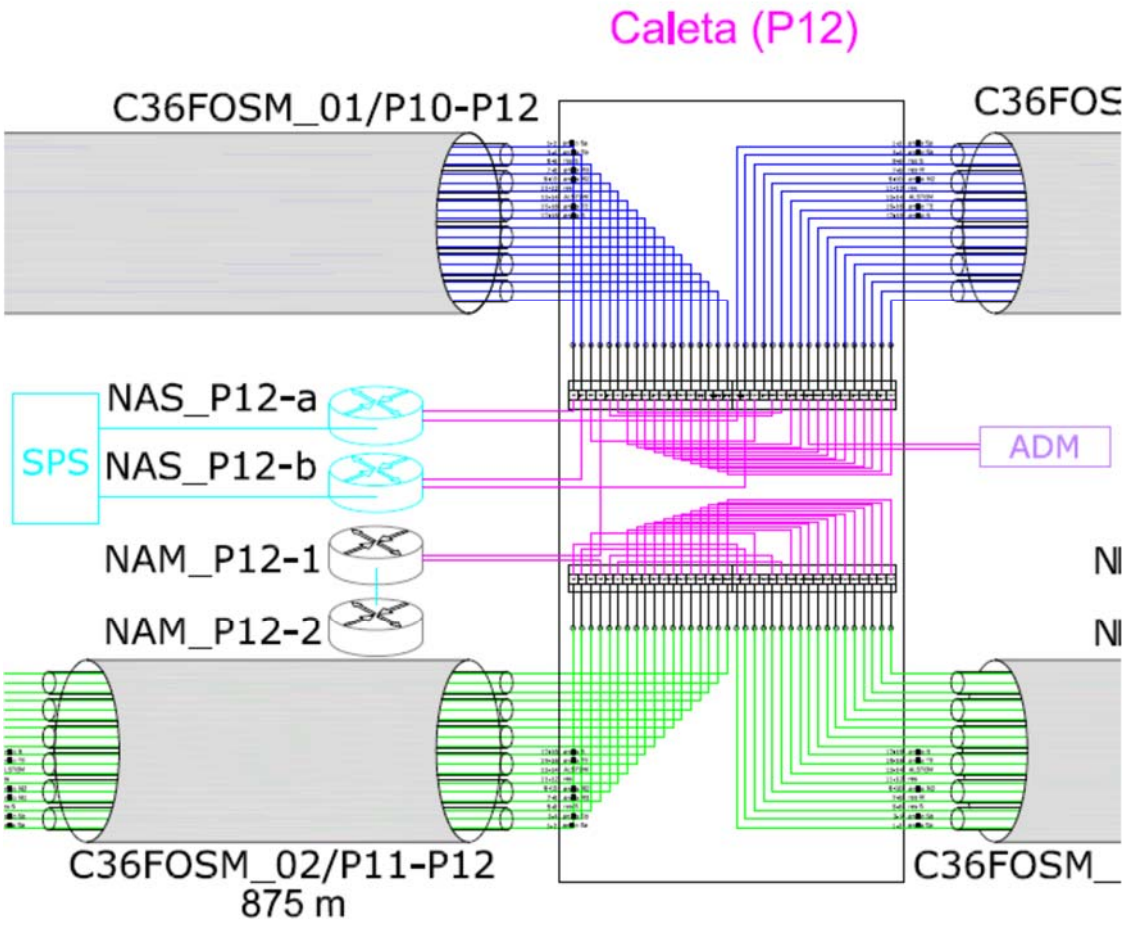
Esquema de Conexionado parada Juncaril. El cable 1 pasa de largo (se deja una coca de reserva en el foso de parada), mientras que para el cable 2, se segregan los 3 primeros tubos
Se fusionan en paso las fibras 1-2 y 3-4 del cable de entrada con el cable de salida.
Se fusionan a pigtail las fibras 5-6, 7-8, 9-10, 11-12 y 13-14 del cable de entrada y el de salida.
Se fusionan en paso las fibras 15-16 y 17-18 del cable de entrada con el cable de salida.
No se han de cortar los 3 tubos que contienen las fibras de la 19 a la 36 (tubos de reserva).



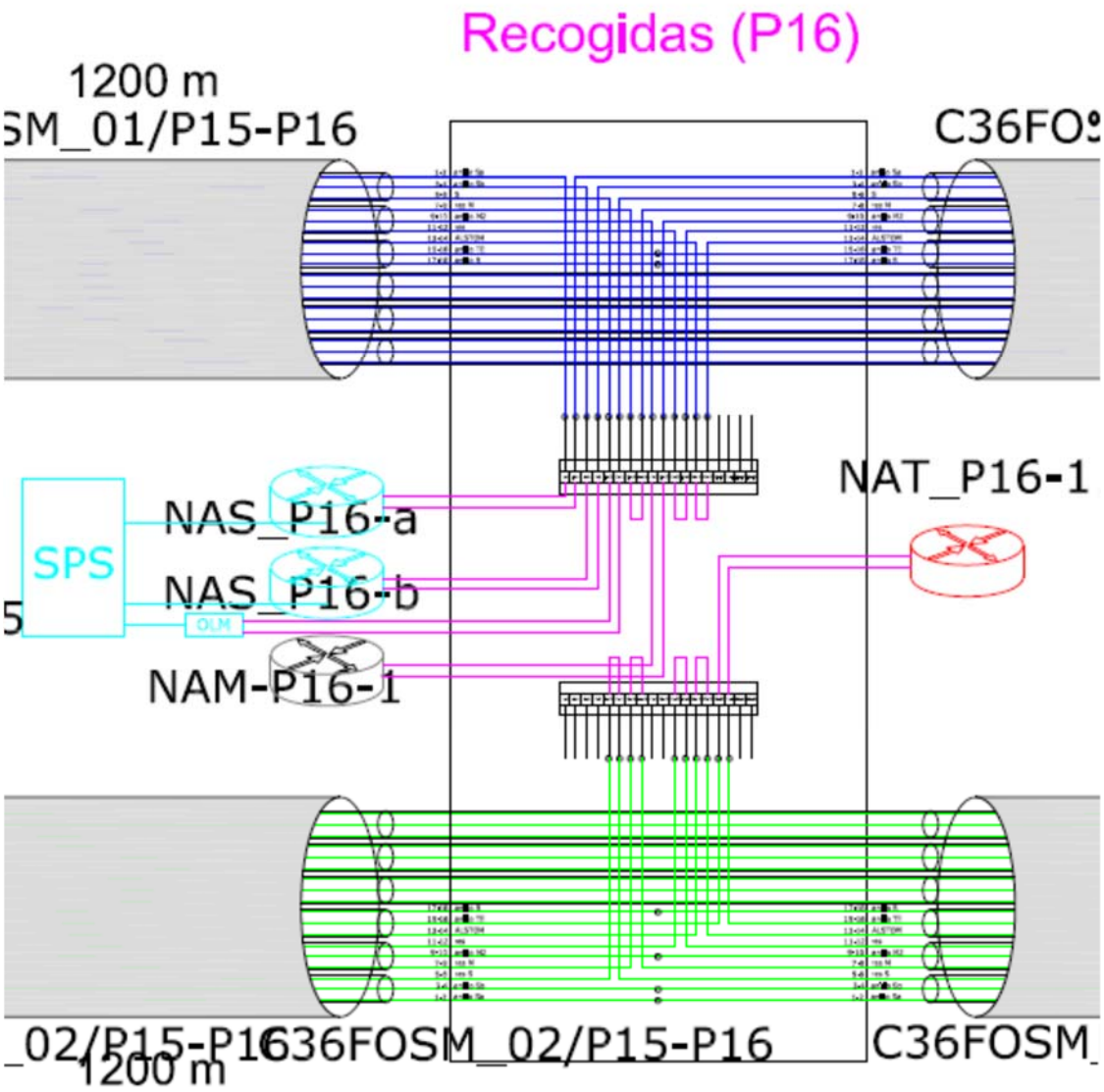
Esquema de Conexionado parada Vicuña. En este caso es el cable 2 el que pasa de largo, mientras que para el cable 1, se segregan los 6 tubos (fin de bobina):
Se fusionan en paso las fibras 1-2 y 3-4 del cable de entrada con el cable de salida.
Se fusionan a pigtail las fibras 5-6, 7-8, 9-10, 11-12 y 13-14 del cable de entrada y el de salida.
Se fusionan en paso las fibras 15-16 y 17-18 del cable de entrada con el cable de salida.
Se fusionan en paso los 3 tubos que contienen las fibras de la 19 a la 36 (fin de bobina).



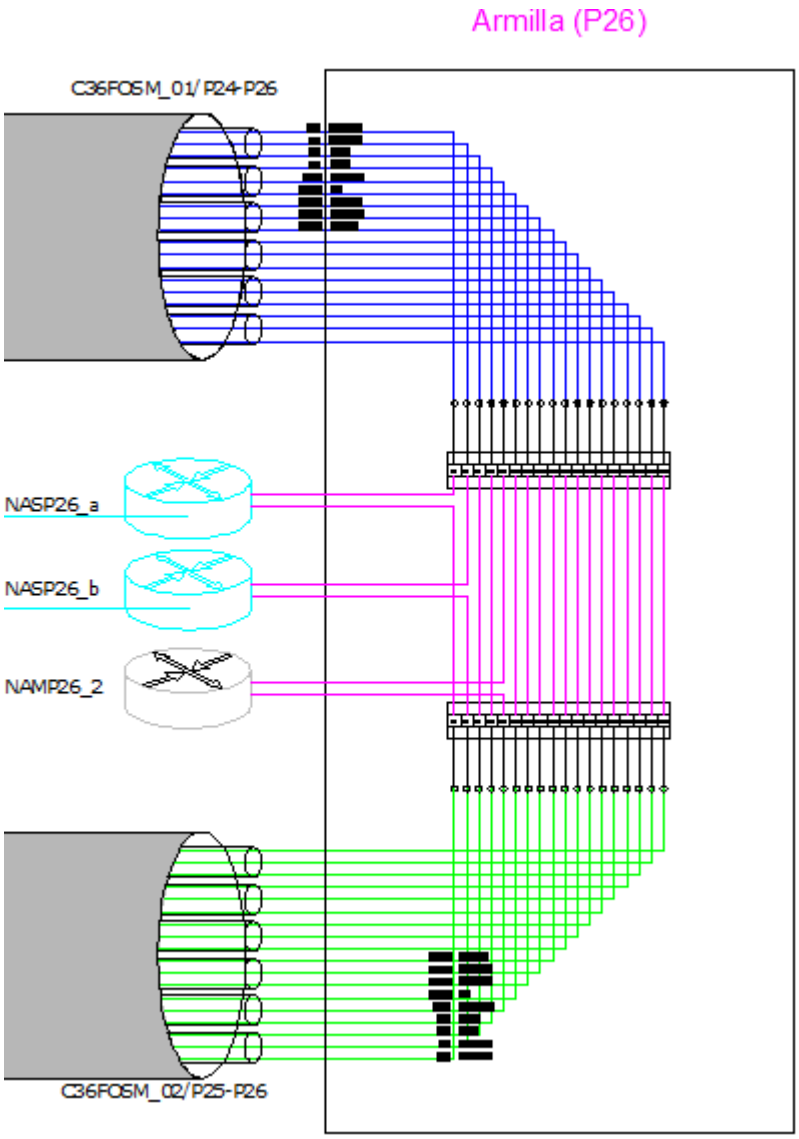
Esquema de Conexionado Sala Técnica de Talleres y Cocheras. En este caso se fusionan a pigtail todas las fibras de entra y salida de cada uno de los dos cables.



Esquema de Conexionado parada Caleta (fin del primer tramo de la línea). En este caso se fusionan a pigtail todas las fibras de entra y salida de cada uno de los dos cables.



Esquema de Conexionado estación Recogidas. En este caso, se acomete al rack principal de estación con los dos cables de fibras ópticas. Se fusionan a pigtail y en paso, las fibras necesarias de los tres primeros tubos de cada cable. Los 3 últimos tubos (fibras de la 19 a la 36), de cada uno de los dos cables, deben continuar su paso sin ser cortados y fusionados.



Esquema de Conexionado parada de fin de línea final (Armilla). Se fusionan los dos cables completos.

3.2. Cableado de la Red Local de Acceso

Por cada una de las paradas, estaciones y subestaciones eléctrica de las Línea del metropolitano se ha instalado una LAN ETHERNET TCP/IP constituida por switches (nodos de acceso) como elementos de estructura de red a los que se conectan los equipos terminales de los distintos sistemas de control de la parada, estación o subestación eléctrica. Cuando un determinado equipo terminal se encuentra a una distancia superior a los 100m del nodo de acceso o switch, se ha empleado conversores de medios de fibra óptica a cobre para poder establecer la conexión.
Se han instalado todos los elementos necesarios para la correcta comunicación entre los equipos terminales y los nodos de acceso de cada ubicación:

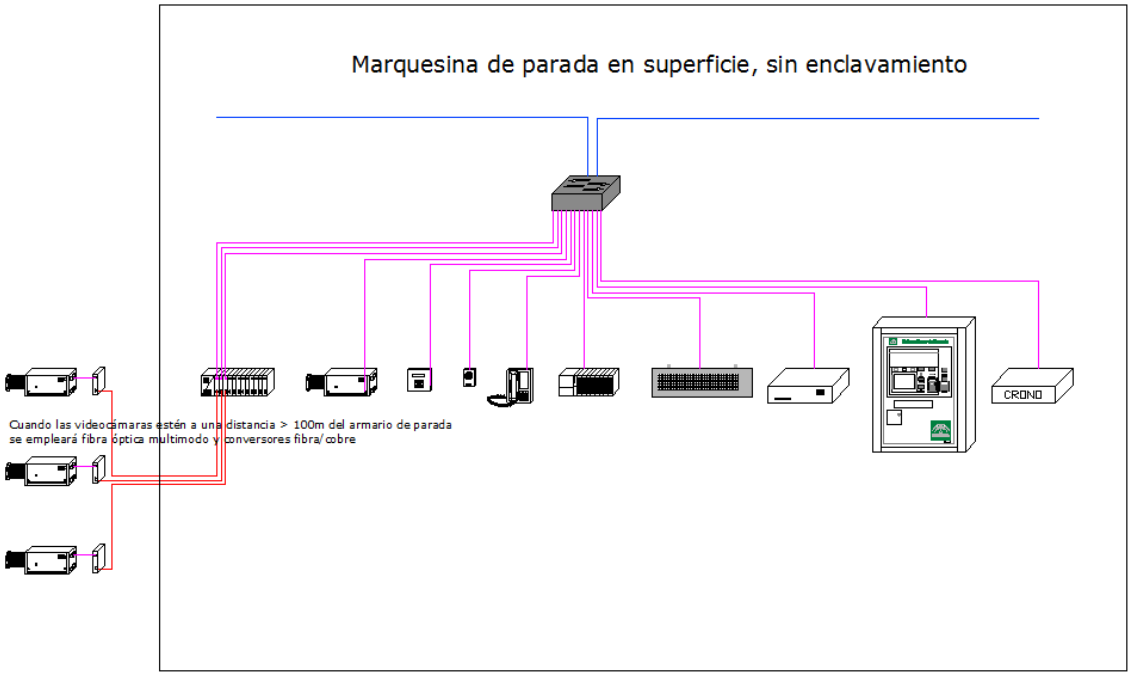
- Tomas de datos RJ45 categoría 6
- Cabledo de datos UTP categoría 6
- Panel repartidor de 24 tomas RJ45 categoría 6
- Panel pasahilos
- Cable de 8 fibras ópticas multimodo OM3
- Panel repartidor de hasta 24 fibras ópticas multimodo, con adaptadores FC
- Conversores de medios de 100BaseTX a 100BaseFX

Además, se ha instalado el panel repartidor de fibras ópticas monomodo, que da acceso a la red GbE, así como los latiguillos y todos los elementos de conectorización necesarios para el correcto funcionamiento de la instalación.

A continuación se presentan los distintos casos en función de la ubicación y de los sistemas a los que se da servicio, incluyendo un esquema de los mismos. El detalle de la instalación realizada en cada una de las ubicaciones puede verse en los planos constructivos adjuntos.

3.2.1. Red local de parada en superficie, sin enclavamiento de señalización asociado

En este caso, solo se ha instalado un nodo de acceso a la red multiservicio al que quedan conectados todos los equipos terminales de los sistemas no críticos de la parada.
El esquema de la red local de una parada en superficie, sin enclavamiento de señalización asociado, se muestra en la siguiente figura:

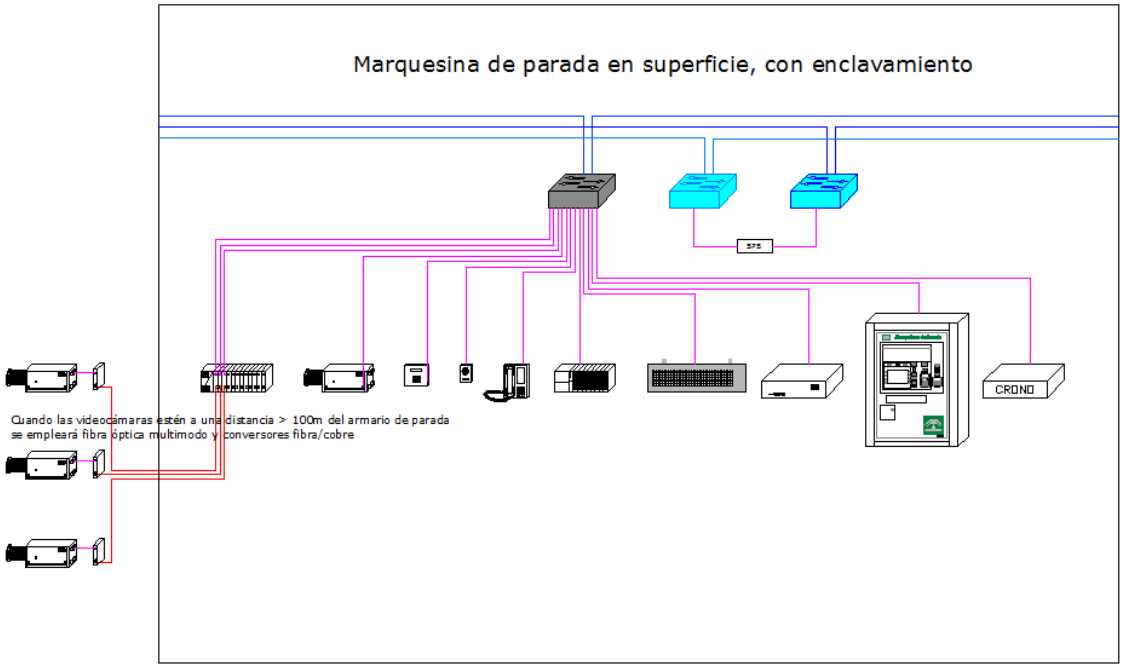


Esquema red local parada sin enclavamiento

En las paradas de superficie, el equipamiento de la red local se ha instalado directamente en un bastidor de 19'' existente en el interior de la marquesina de la parada:
Se ha instalado un nodo de acceso a la red multiservicio, conectado mediante panel repartidor, latiguillos y cable de categoría 6 a los equipos terminales de los distintos sistemas integrados en la marquesina (interfono, teléfono, videocámara, panel teleindicador, máquina expendedora de billetes de metro, amplificador de megafonía, etc…)
Igualmente se ha instalado en el bastidor de 19'' un panel repartidor de Fibra óptica multimodo, precargado con hasta 24 adaptadores y pigtails FC, para la conectorización de elementos terminales, tales como cámaras de videovigilancia, que disten más de 100m de la parada. También se han instalado convertidores de medios 100BaseTX a 100BaseFX.

3.2.2. Red local de parada en superficie, con enclavamiento de señalización asociado

En este caso, además del nodo de acceso a la red multiservicio, se han instalado dos nodos de acceso a la red segura de señalización a los que se ha conectado, de manera redundante, el módulo de comunicaciones del enclavamiento de señalización (SPS). El esquema de la red local de una parada en superficie, con enclavamiento de señalización asociado, se muestra en la siguiente figura:

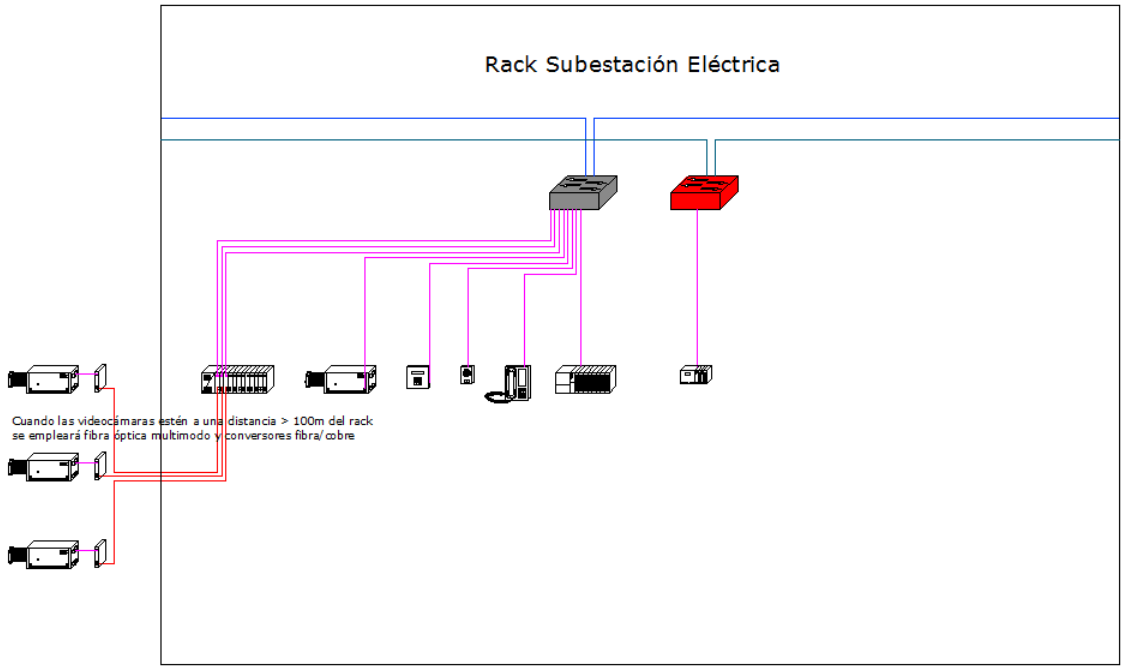


Esquema red local parada con enclavamiento

Se han ejecutado todos los trabajos comentados en el apartado anterior además de la instalación, conectorización, configuración y puesta en marcha de los dos nodos de acceso a la red de señalización.

3.2.3. Red local de subestación eléctrica

En este caso, además del nodo de acceso a la red multiservicio, se ha instalado un nodo de acceso a la red segura de telemando de energía.
El esquema de la red local de una subestación eléctrica, se muestra en la siguiente figura:

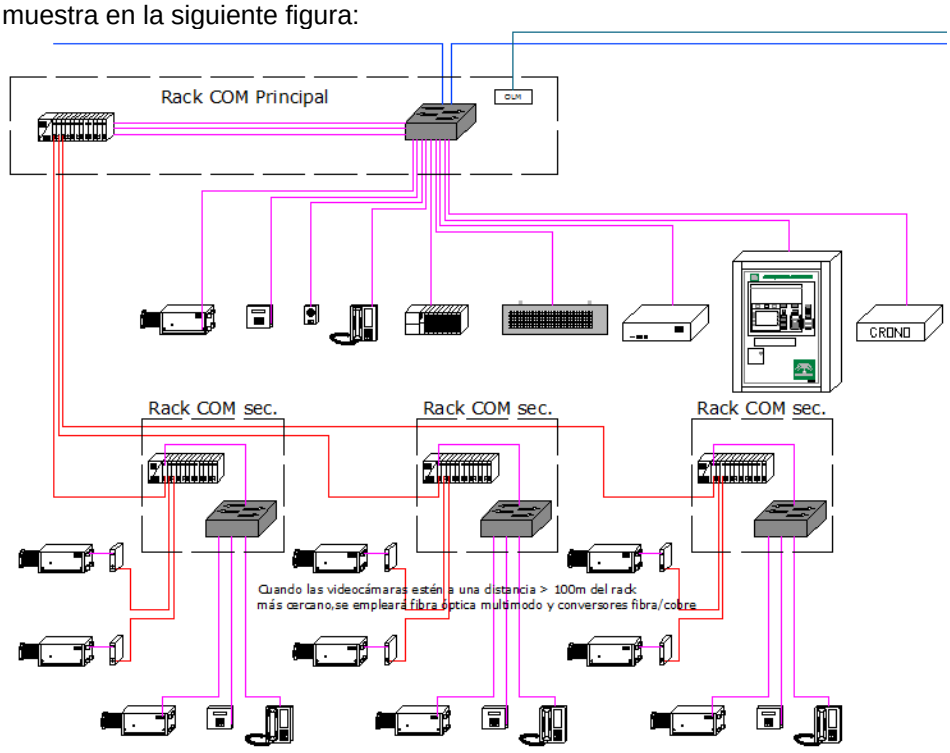


Esquema red local subestación eléctrica
En este caso, se ha instalado un armario rack en el que se ha instalado el siguiente equipamiento:

Un nodo de acceso a la red multiservicio y un nodo de acceso a la red segura de telemando de energía, conectados mediante panel repartidor, latiguillos y cable de categoría 6 a los equipos terminales de los distintos sistemas existentes en la subestación eléctrica. El nodo de acceso a la red multiservicio proporciona conectividad IP a los equipos terminales de sistemas no críticos (videovigilancia, telefonía, control de accesos…) y el nodo de acceso a la red de telemando de energía permite la conectividad IP de la pasarela de comunicaciones del autómata de la red de telemando de energía.
Igualmente se ha instalado en el bastidor de 19'' un panel repartidor de Fibra óptica multimodo, precargado con hasta 24 adaptadores y pigtails FC, para la conectorización de elementos terminales, tales como cámaras de videovigilancia, que disten más de 100m de la subestación. También se han instalado convertidores de medios 100BaseTX a 100BaseFX.

3.2.4. Red local de estación subterránea, sin enclavamiento asociado

En las estaciones soterradas, se han instalado hasta seis switches de la red multiservicio distribuidos en cuatro racks de comunicaciones, funcionando uno de ellos como nodo de acceso a la red GbE y quedando los tres racks restantes conectados en anillo mediante fibra óptica multimodo.
El esquema general de una estación subterránea, sin enclavamiento de señalización asociado, se muestra en la siguiente figura:



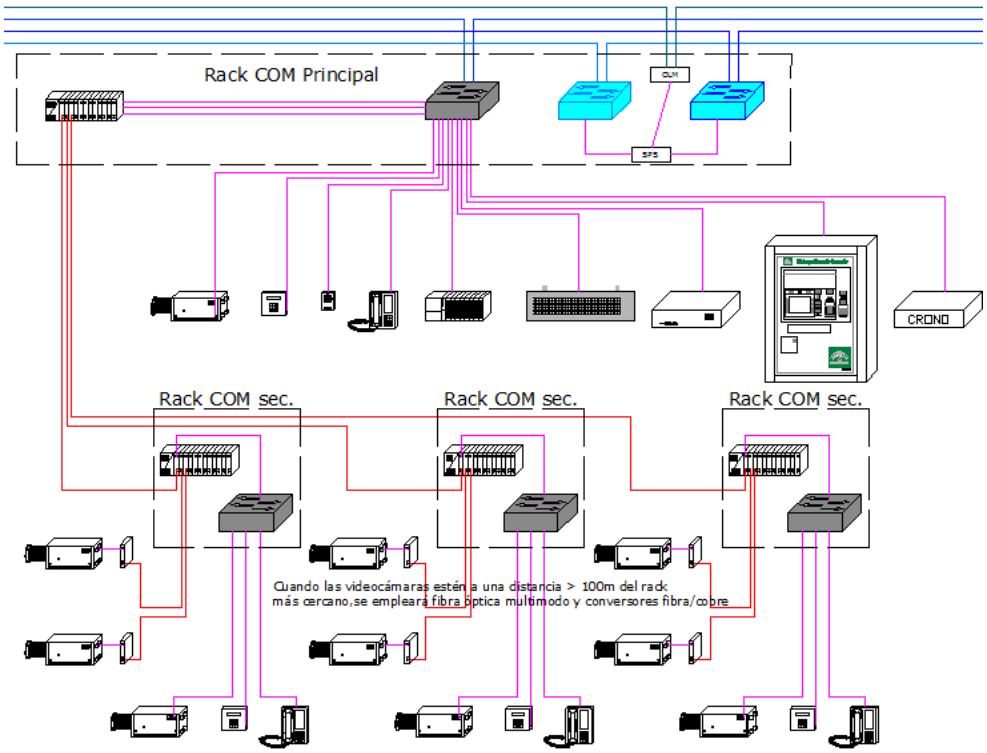
Esquema red local estación subterránea sin enclavamiento

En este caso, se ha instalado en la estación cuatro armarios rack en los que se instalará, para cada uno, el siguiente equipamiento:
Uno o dos switches de la red multiservicio al que se ha conectado mediante panel repartidor, latiguillos, cable de categoría 6 y tomas de datos RJ45, los equipos terminales de los distintos sistemas existentes en estación: interfonos, teléfonos, videocámaras, paneles teleindicadores, máquinas expendedoras de billetes de metro, tornos de paso, amplificador de megafonía, etc.
Igualmente, se ha instalado en cada rack un panel repartidor de Fibra óptica multimodo, precargado con hasta 24 adaptadores y pigtails FC, para la conexión entre los distintos racks de estación, así como la conectorización de elementos terminales, que disten más de 100m del rack más cercano.
También se ha instalado en cada rack varios convertidores de medios 100BaseTX a 100BaseFX para poder realizar dichas conexiones.

En el rack de estación designado como principal, se ha instalado además el repartidor de fibras ópticas monomodo para la conexión del nodo de acceso a la red GbE.

3.2.5. Red local de estación subterránea, con enclavamiento asociado

En este caso, además de todo el equipamiento comentado en el apartado anterior, se ha instalado en el rack principal dos nodos de acceso a la red segura de señalización, a los que se ha conectado, de manera redundante, el módulo de comunicaciones del enclavamiento de señalización (SPS).
El esquema general de una estación subterránea, con enclavamiento de señalización asociado, se muestra en la siguiente figura:



Esquema red local estación subterránea con enclavamiento

4. Equipamiento físico

Cómo equipos centrales de la infraestructura de red (core) se han instalado equipos Cisco 4500E. Estos equipos tienen las siguientes características:

4.1. Cisco 4506-E

Como core de la red se instala un chasis Cisco modelo 4506. A grandes rasgos, las principales características diferenciadoras de la serie de switches Catalyst 4500 de Cisco son las siguientes:

- Plataforma modular de gama media diseñada para organizaciones y proveedores de servicios de todos los tamaños.
- Servicios de red inteligentes de capa 2 a 4 con PoE integrada para comunicaciones unificadas.
- Funciones innovadoras de alta disponibilidad que incluyen actualizaciones de software en servicio (ISSU) a fin de maximizar el tiempo de disponibilidad de la red.
- Amplias funciones de seguridad, incluida la norma 802.1x, control de admisión de la red (NAC), Netflow, vigilancia de plano de control.

- Alta densidad de puertos con conectividad Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet.
- Gestión simplificada para una mayor facilidad de uso.
- El modelo se corresponde con la referencia WS-4506-E, un switch de 6 slots para la gestión del cual se propone la Supervisora 7-L. Las características y capacidades ofrecidas con este equipamiento propuesto son las siguientes:
  - Número de slots dedicado a supervisoras: 1.
  - Número de slots dedicados al resto de módulos: 5.
  - Alta densidad de puertos:
    - 240 puertos Fast Ethernet/Gigabit Ethernet.
    - 244 puertos 1000Base-X.
    - 50 puertos 10 Gigabit Ethernet.
  - Ancho de banda de hasta 48 Gbps por slot.
  - Capacidad centralizada de switching de hasta 520 Gbps ofrecido por la supervisora 7L
  - Capacidad de throughput:
    - 225 Mpps para IPv4.
    - 110 Mpps para IPv6.
  - Capacidad de entrada de rutas:
    - 64000 rutas para IPv4.
    - 32000 rutas para IPv6.
  - Capacidad de 32000 rutas multicast.
  - Capacidad para 55000 direcciones MAC.
  - Capacidad VLANs activas: 4094.
  - Hardware preparado para futura implementación de VSS (Virtual Switching System).

Catalyst 4500-E

En concreto se ha equipado con las siguientes tarjetas:
- 1 supervisora modelo 7-L
- 2 módulos de 12 puertos SFP.
- 1 módulos de 48 puertos 10/100/1000 Mbps sin PoE.

El equipo cuenta con fuente de alimentación redundante para ofrecer mayor fiabilidad al sistema.

4.2. Cisco IE3000 e IE4000

Los switches de la serie Cisco IE3000-4000 son equipos preparados para entornos industriales que ofrecen las siguientes ventajas:

- Rugerizados: Son switches diseñados específicamente para las duras condiciones ambientales. Exceden las especificaciones de la mayoría de productos de switching comercial. Incluyen las normas IEEE 1613 y IEC 61850.
- Sencillos de usar: Los switches son sencillos de administrar. Para ellos se puede hacer uso de la herramienta de interfaz gráfica que viene integrada o el asistente basado en la red.
- Altamente seguros: Estos switches ayudan a garantizar que sólo los usuarios autorizados pueden acceder al tráfico y atravesar la red.
- Basada en las Normas: Esta serie de equipamiento ayuda a asegurar que el sistema funcionará con otros dispositivos habilitados para Ethernet y aplicaciones IP. También facilita la integración entre aplicaciones de oficina y equipos industriales.
- 

Cisco IE3000

Cisco IE4000

4.3. Switches de la serie 2960

Se han implementado dos tipos de switches de la serie 2960. Veamos algunas de sus características.

4.3.1. Cisco 2960X

Se han incorporado varios switches de la serie 2960X que incorporan las siguientes características:

- Posibilidad es stack: Estos equipos permiten la opción de estacamiento de forma que puedan ser gestionados y utilizados como si se tratase de un único dispositivo.

- Posibilidad de estacar hasta 8 switches a través de un módulo adicional (el cual se ha incluido en la propuesta) con capacidad de 80Gbps de throughput.
- Puertos 10/100/1000 Mbps.
- Capacidad de PoE en determinados modelos.
- Uplinks a través de puertos SFP+ que permiten conectividad de hasta 10Gb.
- Funciones de gestión de consumo energético.
- Integra Netflow-Lite
- Garantía limitada de por vida que permitirá el reemplazo de equipos en un tiempo de NBD (Next Business Day).

Cisco 2960X

A continuación, se muestran unas tablas con otras de las características de los equipos:

Hardware Specifications	
Flash memory	128 MB for LAN Base & IP Lite SKUs, 64 MB for LAN Lite SKUs
DRAM	512 MB
CPU	APM86392 600MHz dual core
Console Ports	USB (Type-B), Ethernet (RJ-45)
Storage Interface	USB (Type-A) for external flash storage
Network Management Interface	10/100 Mbps Ethernet (RJ-45)

Performance and Scalability			
	2960-X LAN Lite	2960-X LAN Base	2960-XR IP Lite
Forwarding bandwidth	50 Gbps	108 Gbps	108 Gbps
Switching bandwidth*	100 Gbps	216 Gbps	216 Gbps
Maximum active VLANs	64	1023	1023
VLAN IDs available	4096	4096	4096
Maximum transmission unit (MTU) - L3 packet	9198 bytes	9198 bytes	9198 bytes
Jumbo frame - Ethernet frame	9216 bytes	9216 bytes	9216 bytes

* Switching bandwidth is full-duplex capacity.

Características switch 2960X

4.3.2. Cisco 2960 Series

Las principales características de los switches de Catalyst 2960 Series son:

- Comunicaciones integrales: Obtenga soporte de datos, tecnología inalámbrica y voz de forma que cuando esté listo para implementar estos servicios disponga de una red que admita todas sus necesidades empresariales.
- Inteligencia: Dé prioridad al tráfico de voz o al intercambio de datos para ajustar la entrega de información a sus requisitos empresariales.
- Seguridad mejorada: Proteja la información importante, mantenga a los usuarios no autorizados alejados de la red y consiga un funcionamiento ininterrumpido.
- Confiabilidad: Aprovéchese de las ventajas de los métodos basados en normas para conseguir una mayor confiabilidad y una rápida recuperación de errores. También puede agregar un suministro de energía redundante para obtener una confiabilidad adicional.
- Fácil configuración: Utilice Cisco Network Assistant para simplificar la configuración, las actualizaciones y la solución de problemas.

- Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.
- Función Power over Ethernet que le permite implementar fácilmente nuevas funciones como comunicaciones por voz e inalámbricas sin necesidad de realizar nuevas conexiones.
- Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de 1000 megabits por segundo), en función del precio y sus necesidades de rendimiento.
- Varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
- Capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
- Seguridad integrada
- Funciones de supervisión de red y solución de problemas de conectividad mejoradas.
- Actualizaciones de software sin gastos adicionales.
- Garantía limitada de hardware por vida

Switch 2960S

4.4. Firewall Fortigate

HA o High Availability (Alta Disponibilidad ó Redundancia) se define como el conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.
Se ha optado por una configuración HA Pasivo-Activo para el clúster de Firewalls.
Se trata de disponer de un nodo funcionando, contando con todos los servicios que componen el sistema de información al que denominaremos Activo, y el otro nodo que se denominará Pasivo en el que se encuentran duplicados todos estos servicios, pero detenidos a espera de que se produzca un fallo.
Así nos aseguramos una redundancia del servicio completo. Si una máquina fallase, la otra entraría en funcionamiento al instante, siendo además una copia idéntica de la máquina que ha caído.
Para la implantación de la infraestructura de seguridad perimetral se ha optado por el fabricante Fortinet. En concreto la serie 200.

Fortigate 200B

Cómo características más destacadas podemos destacar:

- Procesamiento de las comunicaciones en modo hardware gracias a las placas ASIC dedicada.
- Escalabilidad.

- Rendimiento.
- Seguridad de despliegue.
- Unica plataforma de Gestión unificada de Amenazas UTM (UTM, Unified Threat Management)
- VPN.
- QoS.
- IPS/IDS.
- Antivirus.
- AntiSpam.
- Filtrado URL.
- Dominios Virtuales
- Sistema de Gestión basado en WEB e interfaz de comandos.

4.5. FortiAnalyzer

Los dispositivos FortiAnalyzer minimizan el esfuerzo requerido para monitorear y mantener un uso aceptable de políticas, para identificar patrones de ataques y para cumplir con regulaciones gubernamentales referentes a la privacidad y señalamientos de brechas de seguridad. Aceptan y procesan un amplio rango de registros proveídos por los sistemas FortiGate, incluyendo tráfico, eventos, virus, ataques, filtrado de contenidos y datos de filtrado de correo electrónico.
El dispositivo elegido para ser implementado en el Metro de Granada es el Fortianalyzer 200D

Fortianalyzer 200D

4.6. IPS/IDS

Una solución de seguridad IPS, proporciona las siguientes funcionalidades:

- Detección de vulnerabilidades a través de firmas
- Detección de anomalías de tráfico y protocolos
- Protección frente a ataques de día cero
- Detección de ataques mediante mecanismos heurísticos basado en algoritmos estadísticos
- Selección de políticas basadas en el nivel de riesgo de un ataque
- Correlación de eventos de seguridad
- Software y Hardware Bypass

Para este proyecto se ha elegido el equipo Fortigate 100D

Fortigate 100D

4.7. Telefonía

Para poder ofrecer servicio de telefonía a las diferentes estaciones del Metropolitano de Granada, se ha optado por una solución de telefonía IP basado en un Call Manager de Cisco.
La voz sobre IP proporciona a su empresa una base para ofrecer aplicaciones de comunicaciones unificadas más avanzadas, incluyendo videoconferencias y conferencias en línea, que pueden transformar su forma de hacer negocios.

Ventajas de la voz sobre IP:

- La voz sobre IP y las comunicaciones unificadas le permiten:
- Reducir los gastos de desplazamiento y formación, mediante el uso de videoconferencias y conferencias en línea.
- Actualizar su sistema telefónico de acuerdo a sus necesidades.
- Tener un número de teléfono que suena a la vez en varios dispositivos, para ayudar a sus empleados a estar conectados entre sí y con sus clientes.
- Reducir sus gastos telefónicos.
- Utilizar una sola red para voz y datos, simplificando la gestión y reduciendo costes.
- Acceder a las funciones de su sistema telefónico en casa o bien en las oficinas de sus clientes, en aeropuertos, hoteles o en cualquier parte donde haya una conexión de banda ancha.

4.8. Puntos de Acceso Wifi

Los dispositivos elegidos como puntos de acceso son los Hirschmann BAT54

Las principales características de estos puntos de acceso son las siguientes:

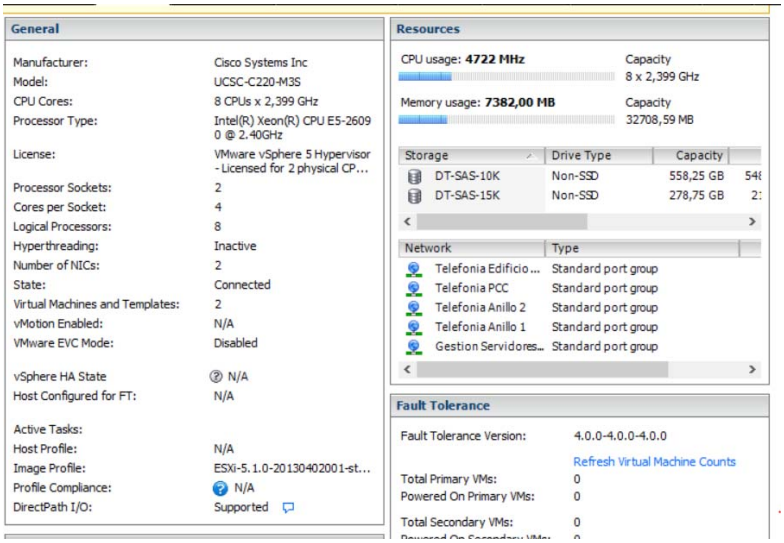
- Dispositivo de doble banda industrial con dos módulos radio independientes IEEE 802.11ª/b/g/h/i

- Ancho de banda de 54Mbps de acuerdo a IEEE802.11g
- Operan tanto en 2.4Ghz como en 5GHz
- Modos de funcionamiento: WLAN Acess Pint, Bridge, Router, Point-toPoint, Client, Client-Bridge Mode.
- Amplio rango de condiciones ambientales soportadas

4.9. Servidor Multiproposito Cisco UCS C220 M3

Para ofrecer varios servicios en la red se utiliza un servidor multipropósito donde se crean distintas máquinas virtuales

El servidor es equipado con un procesador Intel Xeon E5-2609 y 32 GB de memoria RAM:



5. Configuración Lógica

La configuración lógica aplicada en la solución se aplica a la totalidad de los dispositivos de red. Vamos a centralizar la documentación de esta configuración en lo switches 4500, que además de ser el core de la red son los que más configuración tienen.
La configuración de cada uno de los puertos de cada equipo instalado ha sido incluida como anexo en el documento “Switches”.
La versión de firmware de cada equipo se ha incluido como anexo en el documento “Equipamiento de red”.

5.1. Virtual Routing and Forwarding (VRF)

Para la separación lógica de los diferentes servicios se ha optado por configurar VRF (Virtual Routing and Forwarding). Este protocolo de Cisco convierte el router físico en tantos routers virtuales como servicios queramos separar. La principal ventaja es que permite utilizar un único hardware. En este caso, cada instancia de enrutamiento es totalmente independiente, con su propia tabla de enrutamiento, sin interacción con el enrutamiento de otras instancias, lo que permite incluso que haya superposición de redes IP en una misma infraestructura sin que haya conflictos de direccionamiento.
Para este proyecto se han definido una serie de servicios que por su comportamiento necesitaban incorporarse a una instancia diferente de VRF. Hasta el momento las instancias configuradas son 15 y corresponden a los siguientes servicios:

Descripción VRF	Descripción del servicio
VRF_BILLET	Billetaje
VRF_CAA	Control de Accesos
VRF_CCTV	CCTV
VRF_CRONO	Cronometría
VRF_GESTION	Gestión
VRF_INTERF	Interfonía
VRF_MEGAF	Megafonía
VRF_SAE	SAE
VRF_SEMAF	Semaforización
VRF_SIV	SIV
VRF_TELEF	Telefonía
VRF_TETRA	Radio TETRA
VRF_TIF	Telemando Instalaciones Fijas
VRF_TYC_EXPL	Explotador
VRF_TYC_WIFI	Servicios Especiales de Talleres y Cocheras

Cada una de estas VRF está compuesta por diferentes redes (vlanes). Vamos a ver su composición en la siguiente tabla:

Nombre	Direccionamiento	Vlanes que pertenecen a esa VRF
VRF_BILLET	10.11.0.0/16	Vl460, Vl461, Vl472, Vl473, Vl474
VRF_CAA	10.8.0.0/16	Vl340, Vl341, Vl352, Vl353
VRF_CCTV	10.5.0.0/16	Vl220, Vl221, Vl232, Vl233
VRF_CRONO	10.16.0.0/16	Vl660, Vl661, Vl672, Vl673
VRF_GESTION	10.4.0.0/16	Vl180, Vl181, Vl192, Vl193, Vl197, Vl198, Vl199, Vl196
VRF_INTERF	10.7.0.0/16	Vl300, Vl301, Vl312, Vl313
VRF_MEGAF	10.9.0.0/16	Vl380, Vl381, Vl392, Vl393, Vl394
VRF_SAE	10.13.0.0/16	Vl540, Vl541, Vl552, Vl553
VRF_SEMAF	10.15.0.0/16	Vl620, Vl621, Vl632, Vl633
VRF_SIV	10.10.0.0/16	Vl420, Vl421, Vl432, Vl433
VRF_TELEF	10.6.0.0/16	Vl260, Vl261, Vl272, Vl273, Vl274, Vl275
VRF_TETRA	10.14.0.0/16	Vl580, Vl581, Vl592, Vl593
VRF_TIF	10.12.0.0/16	Vl500, Vl501, Vl512, Vl513
VRF_TYC_EXPL	10.0.81.0/24	Vl27, Vl47
VRF_TYC_WIFI	10.0.80.0/24	Vl10, Vl46

5.1.1. Configuración de VRF

Para ver la configuración que se ha aplicado en VRF vamos a coger como ejemplo la VRF_GESTION: En primer lugar definimos la lista de acceso que va a permitir la red completa que va a pertenecer a la red de Gestión. En este caso la red 10.4.0.0/16

```
access-list 104 permit ip 10.4.0.0 0.0.255.255 any
```

Ahora creamos un mapa de rutas con prioridad 1 donde vamos a asociar la acl recién creada.

```
!
route-map ROUTEMAP_GESTION permit 1
 match ip address 104
!
```

Ahora ya podemos definir el VRF_GESTION con la red que va a manejar y el mapa de rutas que hemos creado previamente.

```
!
ip vrf VRF_GESTION
 rd 10.4.0.0:1
 import map ROUTEMAP_GESTION
!
```

Una vez creada la instancia para el servicio de Gestión, procedemos a crear las vlanes correspondientes a gestión.

5.2. Configuraciones VLANES e Interfaces

Cada una de las redes definidas para los servicios que hemos visto anteriormente, se dividen en otra serie de servicios. Vamos a ver los que se han configurado y el direccionamiento que poseen:

Vlan	Descripción	IP HSRP	IP NTTyC_a	IP NTTYC_b
Vlan10	WIFI_PLAYA_VIAS	10.0.0.246	10.0.0.247	10.0.0.248
Vlan27	TyC_EXPL_ED_CONTROL	10.0.32.1	10.0.32.2	10.0.32.3
Vlan46	TyC_WIFI_FIREW	10.0.80.1	10.0.80.2	10.0.80.3
Vlan47	TyC_EXPL_FIREW	10.0.81.1	10.0.81.2	10.0.81.3
Vlan180	GESTION_ANILLO1	10.4.32.1	10.4.32.2	10.4.32.3
Vlan181	GESTION_ANILLO2	10.4.64.1	10.4.64.2	10.4.64.3
Vlan192	GESTION_FIREW	10.4.0.1	10.4.0.2	10.4.0.3
Vlan193	GESTION_SERV1	10.4.1.1	10.4.1.2	10.4.1.3
Vlan196	GESTION_PCC_TYC	10.4.4.1	10.4.4.2	10.4.4.3
Vlan197	GESTION_SE1	10.4.5.1	10.4.5.2	10.4.5.3
Vlan198	GESTION_SE2	10.4.6.1	10.4.6.2	10.4.6.3
Vlan199	GESTION_TE1	10.4.7.1	10.4.7.2	10.4.7.3
Vlan220	CCTV_ANILLO1	10.5.32.1	10.5.32.2	10.5.32.3
Vlan221	CCTV_ANILLO2	10.5.64.1	10.5.64.2	10.5.64.3

Vlan232	CCTV_FIREW	10.5.0.1	10.5.0.2	10.5.0.3
Vlan233	CCTV_SERV1	10.5.1.1	10.5.1.2	10.5.1.3
Vlan260	TELEF_ANILLO1	10.6.32.1	10.6.32.2	10.6.32.3
Vlan261	TELEF_ANILLO2	10.6.64.1	10.6.64.2	10.6.64.3
Vlan272	TELEF_FIREW	10.6.0.1	10.6.0.2	10.6.0.3
Vlan273	TELEF_SERV1	10.6.1.1	10.6.1.2	10.6.1.3
Vlan274	TELEF_PCC	10.6.2.1	10.6.2.2	10.6.2.3
Vlan275	TELEF_EDIF_CONTROL	10.6.3.1	10.6.3.2	10.6.3.3
Vlan300	INTERF_ANILLO1	10.7.32.1	10.7.32.2	10.7.32.3
Vlan301	INTERF_ANILLO2	10.7.64.1	10.7.64.2	10.7.64.3
Vlan312	INTERF_FIREW	10.7.0.1	10.7.0.2	10.7.0.3
Vlan313	INTERF_SERV1	10.7.1.1	10.7.1.2	10.7.1.3
Vlan340	CAA_ANILLO1	10.8.32.1	10.8.32.2	10.8.32.3
Vlan341	CAA_ANILLO2	10.8.64.1	10.8.64.2	10.8.64.3
Vlan352	CAA_FIREW	10.8.0.1	10.8.0.2	10.8.0.3
Vlan353	CAA_SERV1	10.8.1.1	10.8.1.2	10.8.1.3
Vlan380	MEGAF_ANILLO1	10.9.32.1	10.9.32.2	10.9.32.3
Vlan381	MEGAF_ANILLO2	10.9.64.1	10.9.64.2	10.9.64.3
Vlan392	MEGAF_FIREW	10.9.0.1	10.9.0.2	10.9.0.3
Vlan393	MEGAF_SERV1	10.9.1.1	10.9.1.2	10.9.1.3
Vlan394	MEGAF_MICROFONOS_PCC	10.9.2.1	10.9.2.2	10.9.2.3
Vlan420	SIV_ANILLO1	10.10.32.1	10.10.32.2	10.10.32.3
Vlan421	SIV_ANILLO2	10.10.64.1	10.10.64.2	10.10.64.3
Vlan432	SIV_FIREW	10.10.0.1	10.10.0.2	10.10.0.3
Vlan433	SIV_SERV1	10.10.1.1	10.10.1.2	10.10.1.3
Vlan460	BILLET_ANILLO1	10.11.32.1	10.11.32.2	10.11.32.3
Vlan461	BILLET_ANILLO2	10.11.64.1	10.11.64.2	10.11.64.3
Vlan472	BILLET_FIREW	10.11.0.1	10.11.0.2	10.11.0.3
Vlan473	BILLET_SERV1	10.11.1.1	10.11.1.2	10.11.1.3
Vlan474	BILLET_PCC	10.11.2.1	10.11.2.2	10.11.2.3
Vlan500	TIF_ANILLO1	10.12.32.1	10.12.32.2	10.12.32.3
Vlan501	TIF_ANILLO2	10.12.64.1	10.12.64.2	10.12.64.3
Vlan512	TIF_FIREW	10.12.0.1	10.12.0.2	10.12.0.3
Vlan513	TIF_SERV1	10.12.1.1	10.12.1.2	10.12.1.3
Vlan540	SAE_ANILLO1	10.13.32.1	10.13.32.2	10.13.32.3
Vlan541	SAE_ANILLO2	10.13.64.1	10.13.64.2	10.13.64.3
Vlan552	SAE_FIREW	10.13.0.1	10.13.0.2	10.13.0.3
Vlan553	SAE_SERV1	10.13.1.1	10.13.1.2	10.13.1.3
Vlan580	TETRA_ANILLO1	10.14.32.1	10.14.32.2	10.14.32.3
Vlan581	TETRA_ANILLO2	10.14.64.1	10.14.64.2	10.14.64.3
Vlan592	TETRA_FIREW	10.14.0.1	10.14.0.2	10.14.0.3

Vlan593	TETRA_SERV1	10.14.1.1	10.14.1.2	10.14.1.3
Vlan620	SEMAF_ANILLO1	10.15.32.1	10.15.32.2	10.15.32.3
Vlan621	SEMAF_ANILLO2	10.15.64.1	10.15.64.2	10.15.64.3
Vlan632	SEMAF_FIREW	10.15.0.1	10.15.0.2	10.15.0.3
Vlan633	SEMAF_SERV1	10.15.1.1	10.15.1.2	10.15.1.3
Vlan660	CRONO_ANILLO1	10.16.32.1	10.16.32.2	10.16.32.3
Vlan661	CRONO_ANILLO2	10.16.64.1	10.16.64.2	10.16.64.3
Vlan672	CRONO_FIREW	10.16.0.1	10.16.0.2	10.16.0.3
Vlan673	CRONO_SERV1	10.16.1.1	10.16.1.2	10.16.1.3

5.2.1. Configuración de vlanes

Al igual que se ha comentado con el VRF, para la configuración de las vlanes vamos a coger como ejemplo las vlanes correspondientes al VRF_GESTION.

En primer lugar, vamos a crear las vlanes correspondientes y vamos a asignarles un nombre que identifique su función:

```
!
vlan 180
 name GESTION_ANILLO1
!
vlan 181
 name GESTION_ANILLO2
!
vlan 192
 name GESTION_FIREW
!
vlan 193
 name GESTION_SERV1
!
vlan 196
 name GESTION_PCC_TYC
!
vlan 197
 name GESTION_SN1
!
vlan 198
 name GESTION_SN2
!
```

5.2.2. Configuración de interfaces vlanes

Una vez creadas las vlanes procedemos a crear sus interfaces correspondientes. Como ambos 4500 funcionan de forma independiente, es decir no están configurados como un único equipo virtual (VSS), al tener que utilizar el protocolo REP, se ha tenido que hacer uso del protocolo HSRP para que ambos equipos respondan a una IP virtual.
Vamos a ver como ejemplo de configuración de interfaz vlan a la VLAN 180 que se utiliza para la gestión del anillo 1 en ambos 4500.

NTTyC_a

```
!
interface Vlan180
 description GESTION_ANILLO1
 ip vrf forwarding VRF_GESTION
 ip address 10.4.32.2 255.255.224.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 180 ip 10.4.32.1
 standby 180 priority 120
 standby 180 preempt
 standby 180 authentication md5 key-string 7 040A5B485B6F1F1C4748
 standby 180 name GESTION_ANILLO1
 standby 180 track 1 decrement 20
!
```

NTTyC_b

```
interface Vlan180
 description GESTION_ANILLO1
 ip vrf forwarding VRF_GESTION
 ip address 10.4.32.3 255.255.224.0
 standby delay minimum 30 reload 60
 standby version 2
 standby 180 ip 10.4.32.1
 standby 180 priority 110
 standby 180 preempt
 standby 180 authentication md5 key-string 7 025754155F485C73021E
 standby 180 name GESTION_ANILLO1
 standby 180 track 1 decrement 20
```

Dentro de la configuración podemos distinguir la parte de HSRP señalada en rojo. Cómo se puede observar la configuración en ambos equipos es muy parecida, tan solo varía la ip física de cada vlan en cada 4500 y la prioridad de HSRP. En este caso el equipo que respondería a la IP virtual es el NTTyC_a ya que tiene la prioridad más alta.

5.2.3. Interfaces Agregadas

Para determinadas comunicaciones como la que se realiza entre ambos 4500 (NTTyC_a y NTTyC_b) o la comunicación entre estos y los firewalls perimetrales, se hace necesaria una configuración diferente que ofrezca redundancia en la comunicación. Para estos casos se han implementado otros protocolos como LACP o el protocolo PAGP propietario de Cisco.

5.2.4. Configuración entre los 4500

En las siguientes imágenes podemos ver la configuración de los puertos que comunican ambos 4500. En primer lugar, definimos una interfaz virtual (port-channel) que agrupara a varias interfaces físicas.

NTTyC_a

```
!
interface Port-channel1
 description Conexion entre NTTyC_X Cisco 4500
 switchport
 switchport mode trunk
end
```

Una vez creada vamos a las interfaces que deseemos que se incorporen a la interfaz virtual y las añadimos de la siguiente forma. En la configuración de las interfaces se puede ver como no especificamos las vlanes que queremos que pasen a través de la interfaz, de este modo todas las vlanes tienen la posibilidad de pasar entre ambos 4500 (azul).

```
!
interface TenGigabitEthernet1/1
 description Etherchannel 1 entre Cisco 4500 - PAgP
 switchport mode trunk
 macro description PUERTO_ETHERCHANNEL_1 | PUERTO_ETHERCHANNEL_1
 channel-group 1 mode desirable
!
interface TenGigabitEthernet1/2
 description Etherchannel 1 entre Cisco 4500 - PAgP
 switchport mode trunk
 macro description PUERTO_ETHERCHANNEL_1 | PUERTO_ETHERCHANNEL_1
 channel-group 1 mode desirable
!
```

Los comandos señalados en rojo incorporan los puertos físicos al puerto virtual en el modo desirable (protocolo PAGP)
Esta es la macro que añadimos a ambos puertos. Las macros se verán más adelante.

```
!
macro name PUERTO_ETHERCHANNEL_1
 description Etherchannel 1 entre Cisco 4500 - PAgP
 channel-group 1 mode desirable
 no shutdown
@
```

La configuración del segundo 4500 es igual a la del primero, no obstante, se añaden las imágenes para que quede constancia en la documentación.

NTTyC_b

```
!
interface Port-channel1
 description Conexion entre NTTyC_X Cisco 4500
 switchport
 switchport mode trunk
end
```

```
!
interface TenGigabitEthernet1/1
 description Etherchannel 1 entre Cisco 4500 - PAgP
 switchport mode trunk
 macro description PUERTO_ETHERCHANNEL_1 | PUERTO_ETHERCHANNEL_1
 channel-group 1 mode desirable
!
interface TenGigabitEthernet1/2
 description Etherchannel 1 entre Cisco 4500 - PAgP
 switchport mode trunk
 macro description PUERTO_ETHERCHANNEL_1 | PUERTO_ETHERCHANNEL_1
 channel-group 1 mode desirable
!
```

```
!
macro name PUERTO_ETHERCHANNEL_1
 description Etherchannel 1 entre Cisco 4500 - PAgP
 channel-group 1 mode desirable
 no shutdown
@
```

5.2.4.1. Configuración contra los firewalls.

En la siguiente imagen podemos ver la configuración del puerto que comunican ambos 4500 contra los firewalls. En este caso la comunicación se va a realizar entre equipos de diferente fabricante. En este caso en lugar de utilizar el protocolo propietario de Cisco (Pagp), se ha utilizado el estándar LACP. Podemos observar como en la configuración de esta interfaz virtual solo permitimos determinadas vlanes. Aquellas vlanes que no estén no podrán pasar a través del puerto.

NTTyC_a

```
!
interface Port-channel2
 description Conexion a los Fortigate
 switchport
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
end
```

También podemos ver como el portchannel en este caso es el 2 y los puertos físicos tienen que estar asociados a este nuevo interfaz virtual (azul).

```
!
interface GigabitEthernet4/1
 description Etherchannel 2 contra Fortinet 200B - LACP
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet4/2
 description Etherchannel 2 contra Fortinet 200B - LACP
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
 channel-group 2 mode active
!
```

En esta configuración podemos ver como la macro que se aplica a los puertos tiene mucho más contenido. Este contenido lo describiremos más delante cuando veamos las interfaces físicas.

```
macro name PUERTO_TE_FIREW
 description Puerto TE_FIREW
 no shutdown
 switchport mode access
 switchport access vlan 112
 ! storm-control multicast level 25.00
 storm-control broadcast level 25.00
 storm-control action shutdown
 no cdp enable
 no shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
@
```

Al igual que sucede con el Port-channel 1, la configuración del segundo 4500 es idéntica al del primer 4500, no obstante la añado a la documentación.

NTTyC_b

```
!
interface Port-channel2
 description Conexion a los Fortigate
 switchport
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
end
```

```
!
interface GigabitEthernet4/1
 description Etherchannel 2 contra Fortinet 200B - LACP
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
 channel-group 2 mode active
!
interface GigabitEthernet4/2
 description Etherchannel 2 contra Fortinet 200B - LACP
 switchport trunk allowed vlan 30-35,44,46,47,100,112,152,192,232,272,312,352
 switchport trunk allowed vlan add 392,432,472,512,552,592,632,672
 switchport mode trunk
 channel-group 2 mode active
!
```

```
macro name PUERTO_TE_FIREW
 description Puerto TE_FIREW
 no shutdown
 switchport mode access
 switchport access vlan 112
 ! storm-control multicast level 25.00
 storm-control broadcast level 25.00
 storm-control action shutdown
 no cdp enable
 no shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
@
```

5.3. Configuraciones de macros

Las macros son configuraciones predefinidas en el equipo y listas para ser usadas. Debido al número de puertos a configurar, se ha optado por la opción de crear diferentes macros a fin de que sea mucho más ágil configurar los diferentes puertos. Para aplicar una macro habrá que entrar dentro de la interfaz que se desee configurar y ejecutar la macro de la siguiente forma:

```
NTTyC_a#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
NTTyC_a(config)#int g2/4
NTTyC_a(config-if)#macro apply PUERTO_ROUTER3G
NTTyC_a(config-if)#
```

Para eliminar la configuración de un puerto completamente y dejarlo por defecto, introducir el siguiente comando desde el modo de configuración global:

```
NTTyC_a(config)#default interface g2/4
Interface GigabitEthernet2/4 set to default configuration
```

Veamos unos ejemplos de macros configurados en los equipos.

```
macro name PUERTO_GESTION_FIREW
 description Puerto GESTION_FIREW
 no shutdown
 switchport mode access
 switchport access vlan 192
 ! storm-control multicast level 25.00
 storm-control broadcast level 25.00
 storm-control action shutdown
 no cdp enable
 no shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree bpdufilter enable
@
```

En este ejemplo podemos ver estos diferentes comandos. Vamos a comentarlos:

- Nombre de la macro (PUERTO_GESTION_FIREW)
- Descripción (Puerto GESTION_FIREW)
- El puerto está encendido administrativamente (no shutdown)
- Puerto en modo acceso en la vlan 192 (rojo)
- Control para las tormentas de broadcast y multicast para que no sobrepasen un 25% de peticiones. En caso afirmativo, apagaría el puerto. En este caso el tráfico multicast no lo controla.
- Tiene deshabilitado el protocolo CDP (Cisco Discovery Protocol) en ese puerto.
- La configuración relativa al protocolo de spanning-tree en la que se establece que el puerto no va a considerar las notificaciones de spanning-tree para el recalculo del árbol que forma el protocolo a la hora de impedir bucles en la red.
- Las macros predefinidas por el usuario se pueden ver con el comando show run. Para ver las macros predefinidas por el sistema usamos el comando show macro auto device.

Los comandos aplicados a todos los puertos de acceso son los siguientes:

switchport mode access
switchport access vlan X
switchport port-security maximum 1
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
storm-control multicast level 25.00
storm-control broadcast level 25.00
storm-control action shutdown
no cdp enable
no shutdown
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree bpdufilter enable

5.4. Configuración de QoS

En el caso de macros para puertos de telefonía aparecerán también las siguientes líneas:

```
 auto qos voip cisco-phone
 qos trust device cisco-phone
 service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

Esta es la configuración sobre calidad de servicio que se aplica en una interfaz de telefonía. Esta QoS viene predefinida en los equipos Catalyst y tiene el siguiente formato.

```
class-map match-all AutoQos-4.0-Scavenger-Classify
  match access-group name AutoQos-4.0-ACL-Scavenger
class-map match-all AutoQos-4.0-Signaling-Classify
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-any AutoQos-4.0-Priority-Queue
  match cos  5
  match  dscp ef
  match  dscp cs5
  match  dscp cs4
class-map match-all AutoQos-4.0-VoIP-Data-Cos
  match cos  5
class-map match-any AutoQos-4.0-Multimedia-Stream-Queue
  match  dscp af31
  match  dscp af32
  match  dscp af33
class-map match-all AutoQos-4.0-Network-Mgmt
  match  dscp cs2
class-map match-all AutoQos-4.0-VoIP-Signal-Cos
  match cos  3
class-map match-any AutoQos-4.0-Multimedia-Conf-Queue
  match cos  4
  match  dscp af41
  match  dscp af42
  match  dscp af43
  match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-any AutoQos-4.0-Transaction-Data
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-all AutoQos-4.0-Network-Ctrl
  match  dscp cs7
class-map match-all AutoQos-4.0-Scavenger
  match  dscp cs1
class-map match-all AutoQos-4.0-Default-Classify
  match access-group name AutoQos-4.0-ACL-Default
class-map match-any AutoQos-4.0-Signaling
  match  dscp cs3
  match cos  3
```

```
class-map match-any AutoQos-4.0-Bulk-Data-Queue
  match cos  1
  match  dscp af11
  match  dscp af12
  match  dscp af13
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Transaction-Classify
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-all AutoQos-4.0-Broadcast-Vid
  match  dscp cs5
class-map match-any AutoQos-4.0-Bulk-Data
  match  dscp af11
  match  dscp af12
  match  dscp af13
class-map match-any AutoQos-4.0-Scavenger-Queue
  match  dscp cs1
  match cos  1
  match access-group name AutoQos-4.0-ACL-Scavenger
class-map match-any AutoQos-4.0-VoIP
  match  dscp ef
  match cos  5
```

```
class-map match-any AutoQos-4.0-Multimedia-Conf
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any AutoQos-4.0-Control-Mgmt-Queue
  match cos  3
  match  dscp cs7
  match  dscp cs6
  match  dscp cs3
  match  dscp cs2
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Bulk-Data-Classify
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-any AutoQos-4.0-Trans-Data-Queue
  match cos  2
  match  dscp af21
  match  dscp af22
  match  dscp af23
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-any AutoQos-4.0-Multimedia-Stream
  match  dscp af31
  match  dscp af32
  match  dscp af33
class-map match-any AutoQos-4.0-VoIP-Data
  match  dscp ef
  match cos  5
class-map match-all AutoQos-4.0-Internetwork-Ctrl
  match  dscp cs6
class-map match-all AutoQos-4.0-Realtime-Interact
  match  dscp cs4
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
  match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-any AutoQos-4.0-VoIP-Signal
  match  dscp cs3
  match cos  3
```

Con respecto a las políticas a aplicar tanto en entrada como en salida de la interfaz, se configura también por defecto y tienen el siguiente formato:

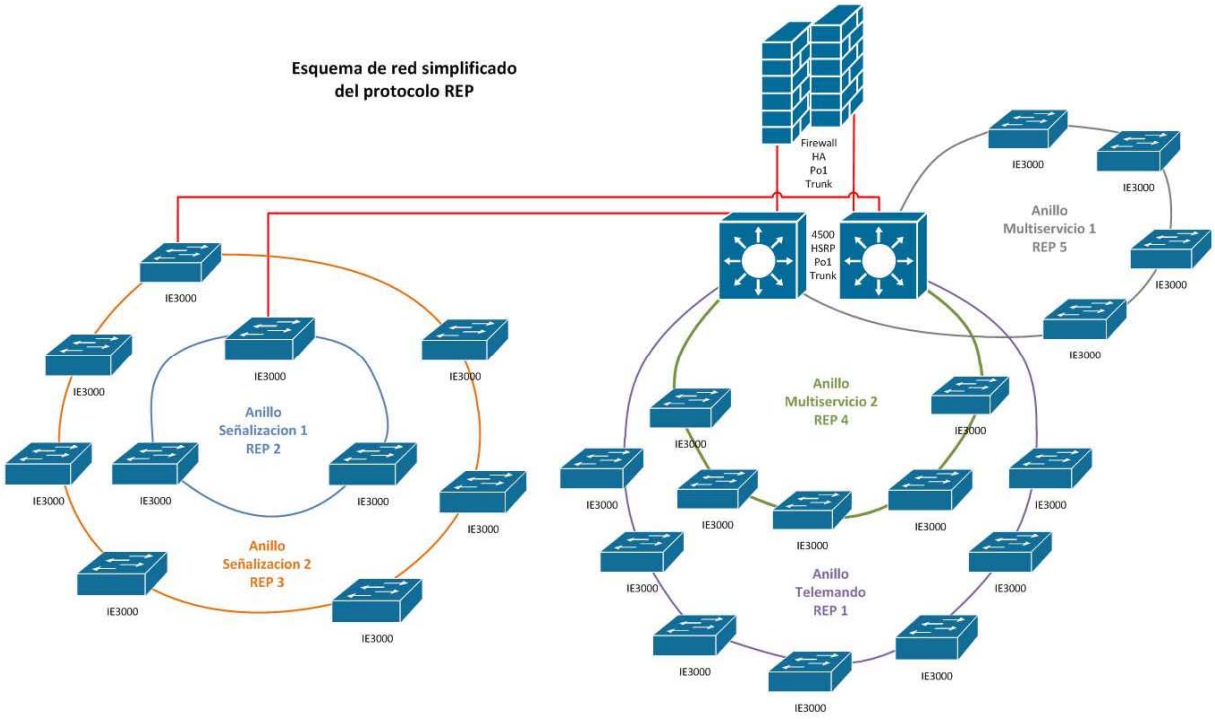
```
policy-map AutoQos-4.0-Input-Policy
 class AutoQos-4.0-VoIP
 class AutoQos-4.0-Broadcast-Vid
 class AutoQos-4.0-Realtime-Interact
 class AutoQos-4.0-Network-Ctrl
 class AutoQos-4.0-Internetwork-Ctrl
 class AutoQos-4.0-Signaling
 class AutoQos-4.0-Network-Mgmt
 class AutoQos-4.0-Multimedia-Conf
 class AutoQos-4.0-Multimedia-Stream
 class AutoQos-4.0-Transaction-Data
 class AutoQos-4.0-Bulk-Data
 class AutoQos-4.0-Scavenger
```

```
policy-map AutoQos-4.0-Cisco-Phone-Input-Policy
 class AutoQos-4.0-VoIP-Data-Cos
   set dscp ef
    police cir 128000 bc 8000
      exceed-action set-dscp-transmit cs1
      exceed-action set-cos-transmit 1
 class AutoQos-4.0-VoIP-Signal-Cos
   set dscp cs3
    police cir 32000 bc 8000
      exceed-action set-dscp-transmit cs1
      exceed-action set-cos-transmit 1
 class class-default
   set dscp default
   set cos 0
policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
    bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
    priority
    police cir percent 30 bc 33 ms
 class AutoQos-4.0-Control-Mgmt-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
    bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
    bandwidth remaining percent 10
    dbl
 class AutoQos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
    dbl
 class class-default
    bandwidth remaining percent 25
    dbl
```

5.5. Resilient Ethernet Protocol (REP)

La opción elegida para controlar la redundancia en los anillos y evitar bucles en la red del Metropolitano de Granada es el protocolo REP (Resilient Ethernet Protocol). REP es un protocolo propiedad de Cisco que proporciona una alternativa al Spanning Tree Protocol (STP), ofreciendo control sobre caminos redundantes impidiendo bucles en la red con una importante mejora a la hora de converger en caso de fallo en alguno de los caminos.
Este protocolo se habilita en las interfaces que van a formar parte del anillo. Cómo hemos comentado anteriormente, se pretenden desplegar cinco anillos multiservicio.

El esquema simplificado sería el siguiente:



En los 4500 están configurado el protocolo REP para dar servicio a tres redes: red de telemando, red multiservicio 1 y red multiservicio 2. Los dos anillos configurados en la red: Señalización 1 y señalización 2 están configurados en los equipos IE3000 situados en Talleres y Cocheras.

5.5.1. Configuración de REP

Vamos a ver las configuraciones aplicadas de REP en los 4500:

```
!
interface GigabitEthernet2/1
 description Conexion al anillo Telemando 1
 switchport trunk allowed vlan 100,199
 switchport mode trunk
 rep segment 1 edge primary
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 macro description PUERTO_ANILLO_TE_1
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
```

Señalamos (en rojo) la parte de configuración que aplica a REP en este puerto.

```
!
interface GigabitEthernet2/2
 description Conexion al anillo Multiservicio 1
 switchport trunk allowed vlan 180,220,260,300,340,380,420,460,500,540,580,620
 switchport trunk allowed vlan add 660
 switchport mode trunk
 rep segment 4 edge primary
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 auto qos trust
 macro description PUERTO_ANILLO_MS_1
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
interface GigabitEthernet2/3
 description Conexion al anillo Multiservicio 2
 switchport trunk allowed vlan 181,221,261,301,341,381,421,461,501,541,581,621
 switchport trunk allowed vlan add 661
 switchport mode trunk
 rep segment 5 edge primary
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 auto qos trust
 macro description PUERTO_ANILLO_MS_2
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
```

Cómo se puede ver en estas configuraciones de estos puertos también se aplica unas macros previamente configuradas.
Al igual que sucede con el resto de configuraciones la parte de REP que aplica al segundo 4500 es muy parecida al del primer equipo.

Veámosla a continuación:

```
!
interface GigabitEthernet2/1
 description Conexion al anillo Telemando 1
 switchport trunk allowed vlan 100,199
 switchport mode trunk
 rep segment 1 edge
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 macro description PUERTO_ANILLO_TE_1
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
```

```
!
interface GigabitEthernet2/2
 description Conexion al anillo Multiservicio 1
 switchport trunk allowed vlan 180,220,260,300,340,380,420,460,500,540,580,620
 switchport trunk allowed vlan add 660
 switchport mode trunk
 rep segment 4 edge
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 auto qos trust
 macro description PUERTO_ANILLO_MS_1
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

```
!
interface GigabitEthernet2/3
 description Conexion al anillo Multiservicio 2
 switchport trunk allowed vlan 181,221,261,301,341,381,421,461,501,541,581,621
 switchport trunk allowed vlan add 661
 switchport mode trunk
 rep segment 5 edge
 rep stcn stp
 rep stcn segment 1-5
 rep stcn interface Port-channel1
 rep preempt delay 30
 rep block port preferred vlan 1-4094
 auto qos trust
 macro description PUERTO_ANILLO_MS_2
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

Cómo se puede ver la única diferencia es que en la parte de configuración de REP en este segundo equipo se omite la opción primary lo que indica que este segundo equipo no es el principal a la hora de aplicar el protocolo.

5.6. Configuración de routing

Cómo ya hemos comentado al utilizar el protocolo VRF, vamos a simular diferentes routers virtuales con sus tablas de enrutamiento independientes. Vamos a ver las configuradas en los equipos.

```
!
ip route 0.0.0.0 0.0.0.0 10.4.0.4
ip route 10.0.67.0 255.255.255.0 10.1.0.1
ip route 10.4.0.0 255.255.255.0 10.1.0.1
ip route 10.4.1.0 255.255.255.0 Vlan193
ip route vrf VRF_BILLET 0.0.0.0 0.0.0.0 10.11.0.4
ip route vrf VRF_CAA 0.0.0.0 0.0.0.0 10.8.0.4
ip route vrf VRF_CCTV 0.0.0.0 0.0.0.0 10.5.0.4
ip route vrf VRF_CRONO 0.0.0.0 0.0.0.0 10.16.0.4
ip route vrf VRF_GESTION 0.0.0.0 0.0.0.0 10.4.0.4
ip route vrf VRF_INTERF 0.0.0.0 0.0.0.0 10.7.0.4
ip route vrf VRF_MEGAF 0.0.0.0 0.0.0.0 10.9.0.4
ip route vrf VRF_SAE 0.0.0.0 0.0.0.0 10.13.0.4
ip route vrf VRF_SEMAF 0.0.0.0 0.0.0.0 10.15.0.4
ip route vrf VRF_SIV 0.0.0.0 0.0.0.0 10.10.0.4
ip route vrf VRF_TELEF 0.0.0.0 0.0.0.0 10.6.0.4
ip route vrf VRF_TETRA 0.0.0.0 0.0.0.0 10.14.0.4
ip route vrf VRF_TIF 0.0.0.0 0.0.0.0 10.12.0.4
ip route vrf VRF_TYC_EXPL 0.0.0.0 0.0.0.0 10.0.81.4
ip route vrf VRF_TYC_WIFI 0.0.0.0 0.0.0.0 10.0.80.4
!
```

La ruta por defecto para el equipo son los firewalls perimetrales, mientras que para cada vrf configurado su Gateway será el configurado en el propio VRF.

5.7. Configuración global

Vamos a ver la configuración que se ha aplicado al equipo de forma global. Esta configuración se aplica al resto de electrónica desplegada en la red.

5.7.1. Licencia.

El equipo dispone de una licencia Enterprise Services de carácter permanente. Se puede ver con el siguiente comando:
show license feature

```
NTTyC_a#sh license feature
Feature name        Enforcement  Evaluation  Clear Allowed  Enabled   Right...
-------------------------------------------------------------------------------
entservices         true         true        true           true      true
ipbase              true         true        true           false     true
lanbase             false        false       true           false     false
internal_service    true         false       true           false     false
```

5.7.2. IOS

Antes de realizar ninguna configuración, se actualizaron los equipos a la última versión disponible en el momento liberada por el fabricante. Actualmente ambos cores tienen la versión:

cat4500e-universalk9.SPA.03.04.03.SG.151-2.SG3.bin

```
boot system flash bootflash:cat4500e-universalk9.SPA.03.04.03.SG.151-2.SG3.bin
```

5.7.3. Usuarios

Se han creado dos usuarios para gestionar los 4500. Ambos disponen del máximo nivel de prioridad. Los usuarios son Wtelecom y admin como podemos ver a continuación:

```
username Wtelecom privilege 15 password 7 072925741C5E2F3A0F0325380B0F2360
username admin privilege 15 password 7 01170F495112240B377F61
```

5.7.4. Hora y fecha

Todos los equipos de la electrónica de la Red de Comunicaciones de Metro de Granada han de estar sincronizados.
El protocolo utilizado para la sincronización ha sido el Network Time Protocolo (NTP). Todos los equipos se han configurado para realizar una consulta a un servidor Linux, localizado en la IP 10.4.1.20, mediante protocolo NTP teniendo en cuenta que éste se encuentra en la VRF de Gestión. Dicho servidor se encuentra en un servidor virtual dentro del servidor físico Gest_COM, que está ubicado en el armario de comunicaciones CORE-1 de la Sala Técnica de Talleres y Cocheras.

```
clock timezone CEST 1 0
clock summer-time CEST recurring
ntp server vrf VRF_GESTION 10.4.1.20
```

Adicionalmente, este servidor Linux se sincronizará a su vez con un servidor de cronometría localizado en la IP 10.16.1.250.

5.7.5. Archive

Se ha configurado el comando Archive para que se exporte la configuración del equipo a un servidor de backup. Dicho servidor se encuentra en un servidor virtual dentro del servidor físico Gest_COM, que está ubicado en el armario de comunicaciones CORE-1 de la Sala Técnica de Talleres y Cocheras.
La configuración permite que se realice una copia cada 7 días. De esta forma nos automatizamos el backup de los equipos y nos permite disponer de una copia de seguridad actualizada cada poco periodo de tiempo.

```
archive
 path scp://backup_config:OV9j-FWa4n@10.4.1.21/NTTyC_a.cfg
 write-memory
 time-period 10080
!
```

5.7.6. Spanning-tree Protocol

Para evitar bucles en la red en los caminos que no implican a protocolo REP se ha implementado spanning-tree. El modo elegido es rapid-pvst y en el 4500 principal se ha definido una prioridad para todas las vlanes de 4096.

NTTyC_a

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 4096
```

En el core secundario la prioridad es de 8192.

NTTyC_b

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 8192
```

Esta prioridad irá en aumento en los equipos según vayan alejándose de los Cores principales, creando un árbol de prioridades que permite tener el control del protocolo en toda la red.

5.7.7. VPT

El modo de VTP configurado es el modo trasparente, es decir los equipos no participan del protocolo VTP, por lo que las vlanes que se crearan en el futuro sería necesario propagarlas por la red de forma manual.

```
vtp mode transparent
```

5.7.8. SNMP

La configuración de SNMP apunta al servidor 10.4.1.11 y se han establecido dos comunidades, una de lectura y otro de escritura. La información que se envía al servidor podemos verla a continuación (rojo). El motivo de utilizar SNMP v2 en lugar de v3 es que la versión 2 ofrece además de una seguridad ya contrastada, ofrece mayor transferencia de información entre sistemas, debido a las mejoras en el protocolo SNM y de rendimiento que la versión 3 en el que el rendimiento se ve afectado en función de que aumenta la seguridad con funciones de autenticación y encriptamiento.

```
snmp-server community mlg-rw-comm RW
snmp-server community mlg-ro-comm RO
snmp-server host 10.4.1.11 version 2c mlg-ro-comm rep storm-control energywise hsrp vrfmib
snmp ifmib ifindex persist
```

5.7.9. Line y VTY

La configuración de line con 0 y line VTY para las sesiones remotas se han configurado bajo el protocolo SSH, como podemos ver en la imagen siguiente.

```
line con 0
 login local
 stopbits 1
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 no exec
 transport input none
 transport output none
```

Se ha elegido el protocolo SSH ya que disminuye amenazas a la seguridad notablemente. Esto es porque el cliente SSH y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una llave conocida sólo por el sistema local y el remoto.

5.8. Configuración Multicast

La red ha sido configurada para soportar la comunicación multicast de los sistemas CCTV y de Megafonía.
Dado que la comunicación entre diferentes equipos ha de pasar por routers y switches, el multicast ha de estar configurado tanto a nivel 2 como a nivel 3 del modelo OSI.

IGMP Snooping
Es el protocolo habilitado en cada uno de los switches (nivel 2) que permite a los dispositivos finales subscribirse a grupos multicast, así bien hará que sólo reciban el tráfico multicast los puertos que lo necesiten. Este protocolo está habilitado por defecto en todos los switches para cada una de las VLANs.

```
NAMP01-2#sh ip igmp snooping vlan 220
Global IGMP Snooping configuration:
---------------------------------------
IGMP snooping                 : Enabled
IGMPv3 snooping (minimal)     : Enabled
Report suppression            : Enabled
TCN solicit query             : Disabled
TCN flood query count         : 2
Robustness variable           : 2
Last member query count       : 2
Last member query interval    : 1000

Vlan 220:
--------
IGMP snooping                          : Enabled
CAPWAP enabled                         : Disabled
IGMPv2 immediate leave                 : Disabled
Multicast router learning mode         : pim-dvmrp
CGMP interoperability mode             : IGMP_ONLY
Robustness variable                    : 2
Last member query count                : 2
Last member query interval             : 1000
```

PIM-DM:
Es el protocolo de nivel 3 que permite el enrutamiento del tráfico multicast entre los elementos capa 3 de la red.
En primer lugar, se ha activado el enrutamiento a nivel global de tráfico multicast para las VRF de CCTV y Megafonía en los elementos capa 3 de la red.

```
ip multicast-routing vrf VRF_CCTV
ip multicast-routing vrf VRF_MEGAF
```

A continuación, para cada uno de los interfaces nivel 3 participantes en el tráfico multicast del Master HSRP del core de la red (NTTyC_a) se ha habilitado el protocolo PIM-DM de la siguiente forma:

```
interface Vlan220
 description CCTV_ANILLO1
 ip vrf forwarding VRF_CCTV
 ip address 10.5.32.2 255.255.224.0
 ip pim dr-priority 60
 ip pim dense-mode
 standby delay minimum 30 reload 60
 standby version 2
 standby 220 ip 10.5.32.1
 standby 220 priority 120
 standby 220 preempt
 standby 220 authentication md5 key-string 7 101F5957505941594255
 standby 220 name CCTV_ANILLO1
 standby 220 track 1 decrement 20
end
```

Los Interfaces configurados para CCTV son los siguientes:

- Vlan220
- Vlan221
- Vlan232
- Vlan233

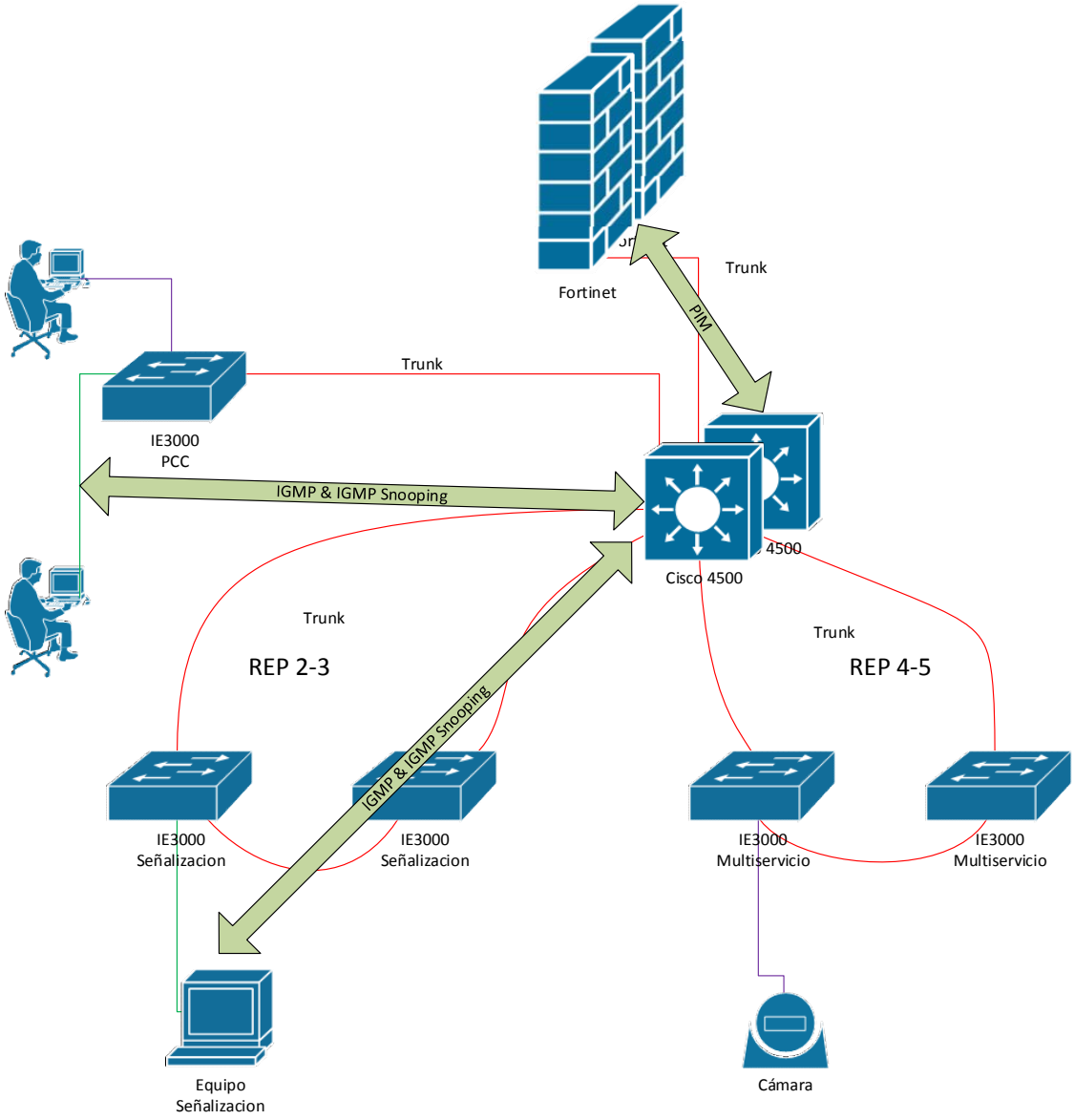
Los interfaces configurados para Megafonía son los siguientes:

- Vlan380
- Vlan381
- Vlan 392
- Vlan393
- Vlan394

En el nodo core Stand-by del HSRP (NTTyC_b) se ha configurado un Event Manager que detectará cuando el nodo Backup HSRP pase a ser el activo; en este momento, activará el protocolo PIM-DM Dense Mode en las mismas interfaces descritas anteriormente. Cuando detecte que el nodo Master ha levantado, dado que en HSRP se ha configurado el Preempt, éste repondrá su figura de Master y el Nodo Backup pasara de Activo a Stand-by de nuevo. Cuando el nodo backup detecte esta situación, descativará el protocolo PIM-DM previamente activado en las interfaces señaladas.

La configuración descrita anteriormente, se ha realizado para prevenir que el protocolo PIM-DM esté activo tanto en el NTTyC_a como en NTTyC-b a la vez formando un HSRP, lo que provocaría una duplicidad de paquetes y un comportamiento no controlado de las comunicaciones multicast.

A continuación, se representa visualmente la configuración de nivel 2 y 3 expuesta anteriormente.



5.9. Configuración Lógica General IE3000 e IE4000

Como ya se ha descrito anteriormente en otros apartados, los switches IE3000 e IE4000 han sido instalados a lo largo de toda la vía formando anillos de comunicaciones. Éstos anillos de comunicaciones se cierran mediante los dos routers de core c4500.

Las funciones principales de estos switches serán dos:

- Clasificar los paquetes en la VLAN que corresponda
- Gestionar la redundancia del anillo

Cada puerto de cada switch se ha configurado para etiquetar paquetes entrantes en una determinada VLAN (ver anexo “switches”) y los puertos libres han sido deshabilitados:

```
NAMP06-1#sh int status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/1     SEMAF_ANILLO_MS1   connected    620        a-full  a-100 10/100BaseTX
Fa1/2     SEMAF_ANILLO_MS1   connected    620        a-full  a-100 10/100BaseTX
Fa1/3     SEMAF_ANILLO_MS1   connected    620        a-full  a-100 10/100BaseTX
Fa1/4     SEMAF_ANILLO_MS1   disabled     620          auto   auto 10/100BaseTX
Fa1/5     SEMAF_ANILLO_MS1   disabled     620          auto   auto 10/100BaseTX
Fa1/6     SEMAF_ANILLO_MS1   disabled     620          auto   auto 10/100BaseTX
Fa1/7     Conexion a otro sw connected    trunk      a-full  a-100 10/100BaseTX
Fa1/8     Conexion a otro sw connected    trunk      a-full  a-100 10/100BaseTX
Fa2/1     TELEF_ANILLO_MS1   notconnect   260          auto   auto 10/100BaseTX
Fa2/2     MEGAF_ANILLO_MS1   notconnect   380          auto   auto 10/100BaseTX
Fa2/3     INTERF_ANILLO_MS1  notconnect   300          auto   auto 10/100BaseTX
Fa2/4     INTERF_ANILLO_MS1  notconnect   300          auto   auto 10/100BaseTX
Fa2/5     TIF_ANILLO_MS1     notconnect   500          auto   auto 10/100BaseTX
Fa2/6     TIF_ANILLO_MS1     notconnect   500          auto   auto 10/100BaseTX
Fa2/7     MANTEN_ANILLO_MS1  notconnect   700          auto   auto 10/100BaseTX
Fa2/8     MANTEN_ANILLO_MS1  notconnect   700          auto   auto 10/100BaseTX
Fa3/1     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/2     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/3     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/4     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/5     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/6     BILLET_ANILLO_MS1  notconnect   460          auto   auto 10/100BaseTX
Fa3/7     SIV_ANILLO_MS1     notconnect   420          auto   auto 10/100BaseTX
Fa3/8     SIV_ANILLO_MS1     notconnect   420          auto   auto 10/100BaseTX
Gi1/1     Conexion al anillo connected    trunk      a-full a-1000 1000BaseLX SFP
Gi1/2     Conexion al anillo connected    trunk      a-full a-1000 1000BaseLX SFP
NAMP06-1#
```

La configuración de seguridad y QoS, se corresponden a las macros aplicadas y descritas en la sección 5.3

Los interfaces que conectan con los demás switches pertenecientes al anillo han sido configurados para transportar todas las VLANs (modo trunk), como puede observarse en el ejemplo anterior en los puertos Gi1/1 y Gi1/2.

Cada uno de los switches pertenecientes al anillo se ha configurado de forma que pertenezca a un segmento REP tal y como se indica en la sección 5.5.

5.10. Configuración Lógica General c2960

Como ya se ha descrito anteriormente, los switches c2960 se han instalado en arquitectura de estrella contra los routers de core c4500. A diferencia de los IE3000, la redundancia de estos dispositivos se gestiona mediante una doble conexión contra los routers de core. En este caso, la lógica de la redundancia se configura en los c4500 a través de los grupos HSRP descritos en la sección 5.2 del presente documento.

Cada puerto de cada switch se ha configurado para etiquetar paquetes entrantes en una determinada VLAN (ver anexo “switches”) y los puertos libres han sido deshabilitados:

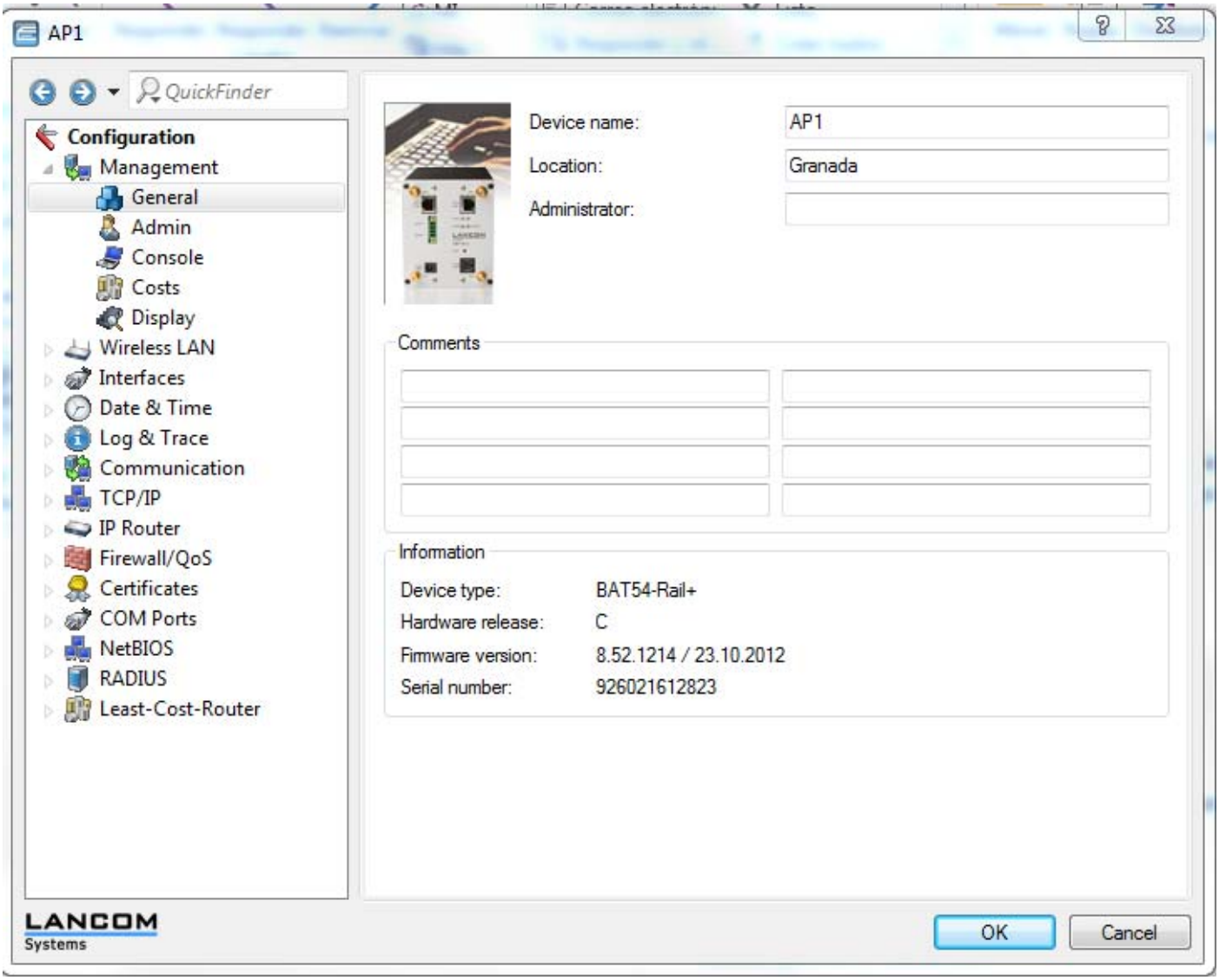
```
NAMCE#sh int status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa1/1     TELEF_ANILLO_MS1   notconnect   260          auto   auto 10/100BaseTX
Fa1/2     CAA_ANILLO_MS1     connected    340        a-full  a-100 10/100BaseTX
Fa1/3     CAA_ANILLO_MS1     connected    340        a-full  a-100 10/100BaseTX
Fa1/4     CAA_ANILLO_MS1     notconnect   340          auto   auto 10/100BaseTX
Fa1/5     CCTV_ANILLO_MS1    notconnect   220          auto   auto 10/100BaseTX
Fa1/6     CCTV_ANILLO_MS1    notconnect   220          auto   auto 10/100BaseTX
Fa1/7     CCTV_ANILLO_MS1    notconnect   220          auto   auto 10/100BaseTX
Fa1/8     CCTV_ANILLO_MS1    notconnect   220          auto   auto 10/100BaseTX
Fa2/1     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa2/2     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa2/3     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa2/4     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa2/5     SEMAF_ANILLO_MS1   notconnect   620          auto   auto 10/100BaseTX
Fa2/6     SEMAF_ANILLO_MS1   notconnect   620          auto   auto 10/100BaseTX
Fa2/7     MANTENIMIENTO      notconnect   700          auto   auto 10/100BaseTX
Fa2/8     MANTENIMIENTO      notconnect   700          auto   auto 10/100BaseTX
Fa3/1     Puerto OPER_CCTV_C connected    30         a-full  a-100 10/100BaseTX
Fa3/2     Puerto OPER_CCTV_C notconnect   30           auto   auto 10/100BaseTX
Fa3/3     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa3/4     Puerto deshabilita disabled     1            auto   auto 10/100BaseTX
Fa3/5     AOPJA              connected    595        a-full  a-100 10/100BaseTX
Fa3/6     AOPJA              notconnect   595          auto   auto 10/100BaseTX
Fa3/7     AOPJA              notconnect   595          auto   auto 10/100BaseTX
Fa3/8     AOPJA              notconnect   595          auto   auto 10/100BaseTX
Gi1/1     Conexion a otro sw connected    trunk      a-full  a-100 10/100/1000BaseTX
Gi1/2     Conexion a otro sw connected    trunk      a-full  a-100 10/100/1000BaseTX
NAMCE#
```

La configuración de seguridad y QoS, se corresponden a las macros aplicadas y descritas en la sección 5.3
Los interfaces que conectan con los routers de core, han sido configurados para transportar todas las VLANs (modo trunk), como puede observarse en el ejemplo anterior en los puertos Gi1/1 y Gi1/2.

6. Configuración Wifi

La configuración de los puntos de acceso se ha realizado mediante el software LANconfig.



A través de este software se descubre cada uno de los puntos de acceso y se accede a su configuración.

Los puntos de acceso han sido configurados en el rango de 5GHz en modo Access-Point y utilizando el interfaz WLAN 1 (de los dos disponibles).

La distribución de Canales/Frecuencias en los puntos de acceso han sido las siguientes:

	IP	CANAL	FRECUENCIA
AP1	10.0.0.249	Auto	5 GHz
AP2	10.0.0.250	Auto	5 GHz
AP3	10.0.0.251	Auto	5 GHz
AP4	10.0.0.252	Auto	5 GHz

Esta distribución asegura que no se produzcan interferencias entre los canales, lo que podría provocar la caída de las comunicaciones.

La única configuración de rutas, es la ruta por defecto. Todos los paquetes de clientes wifi, irán dirigidos a la puerta de enlace por defecto: 10.0.0.246

7. Seguridad

En este apartado vamos a tratar la configuración aplicada en la parte de seguridad en el proyecto. Inicialmente podemos distinguir dos tipos de seguridad: Seguridad interna y Seguridad perimetral.

7.1. Seguridad interna.

Sobre la seguridad interna ya hemos hablado en puntos anteriores, no obstante vamos a resumir las medidas de seguridad que se ha tomado en los equipos de switching en el metro de Granada.

7.1.1. El Enrutamiento Virtual y Reenvío (VRF)

Es una tecnología incluida en routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar al simultáneamente. Esto aumenta la funcionalidad al permitir que las rutas de red sean segmentadas sin usar varios dispositivos. Dado que el tráfico es automáticamente segregados, VRF también aumenta la seguridad de la red y puede eliminar la necesidad de cifrado y autenticación.

Proveedores de Servicios de Internet (ISP) a menudo toman ventaja del VRF para crear distintas redes privadas virtuales (VPNs) para los clientes, por lo que la tecnología es también conocida como VPN enrutamiento y reenvío. VRF actúa como un router lógico, pero mientras que un router lógico puede incluir muchas tablas de enrutamiento, una instancia VRF sólo utiliza una. Además, VRF requiere una tabla de reenvío que designa el siguiente salto para cada paquete de datos, una lista de dispositivos que pueden ser llamados al enviar el paquete, y un conjunto de normas y protocolos de enrutamiento que rigen la forma en que el paquete se reenvía.

Estas tablas evitan el tráfico dado que están siendo reenvía las fuera de la ruta de un VRF específico y también mantienen fuera el tráfico que podría permanecer fuera de la ruta del VRF.

7.1.2. VLANES

Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).
La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores
- Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
- Disminución en la transmisión de tráfico en la red.

7.1.3. Port Security

Es una característica de los switches Cisco que nos permite retener las direcciones MAC conectadas a un puerto y permitir solamente esas direcciones MAC registradas comunicarse a través de ese puerto del switch.

Nos permite restringir:

- Restringir el acceso a los puertos del switch según la MAC.
- Restringir el número de MACs por puerto en el switch.
- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
- Establecer la duración de las asociaciones MAC-Puerto.

Si un dispositivo con otra dirección MAC intenta comunicarse a través de un puerto de la LAN, port-security deshabilitará el puerto.

7.1.4. Storm Control

Una tormenta de paquetes ocurre cuando se reciben en un puerto gran número de paquetes broadcast, unicast o multicast Las respuestas a mensajes reenviados se acumulan en la red, lo que provoca una sobrecarga en los recursos de ésta o que se agote el tiempo de espera, los usuarios no pueden acceder a servidores o el acceso de correo electrónico u otros recursos de la red. Storm Control usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast. El control de tormentas se activa en cada puerto mediante la definición del tipo de paquete y la velocidad de transmisión de los paquetes. El sistema mide la velocidad de las tramas entrantes de broadcast, unicast o multicast, por separado en cada puerto y descarta las tramas cuando la velocidad supera un valor definido por el usuario, es como ponerles un límite de velocidad.

Usa un método basado en ancho de banda. Los umbrales se expresan como un porcentaje del total de ancho de banda que puede ser empleado para cada tipo de tráfico. El Broadcast Strom Control se lleva a cabo con umbrales altos y bajos. La aplicación umbral sigue un patrón porcentaje. Si el tráfico de difusión en cualquier puerto Ethernet supera el umbral alto porcentaje, de la velocidad del enlace, el conmutador descarta el tráfico de la emisión hasta que el tráfico devuelve al porcentaje bajo umbral o menos. Un umbral más alto permite que más paquetes de difusión para pasar a través.

7.1.5. Spaning-Tree

Fue desarrollado para enfrentar los inconvenientes de bucles en la red. STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al realizar un bloque de forma intencional a aquellas rutas redundantes que puedan ocasionar un bucle. Un puerto se considera bloqueado cuando el tráfico de la red no puede ingresar ni salir del puerto. Esto no incluye las tramas de unidad de datos del protocolo comúnmente llamadas (BPDU) utilizadas por STP para evitar bucles. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active. Como medida de seguridad se han habilitado en ciertos puertos la opción de ignorar tramas BDPU y así evitar errores a la hora de recalcular el protocolo.

7.2. Seguridad Perimetral

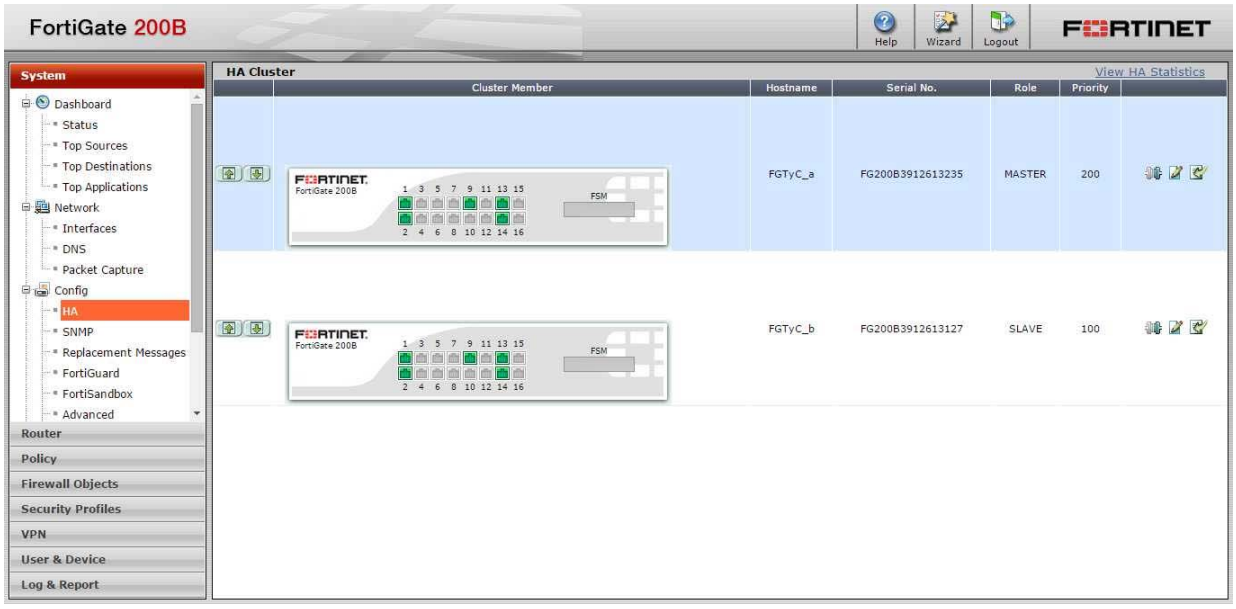
Para la seguridad perimetral se ha instalado una pareja de firewall Fortinet 200B que actualmente trabajan en activo-pasivo.

La gestión de los dispositivos de seguridad se realiza a través de la VLAN192 incluida en la VRF de Gestión.

A continuación se describe la configuración de la pareja de firewall.

7.2.1. Configuracion en HA

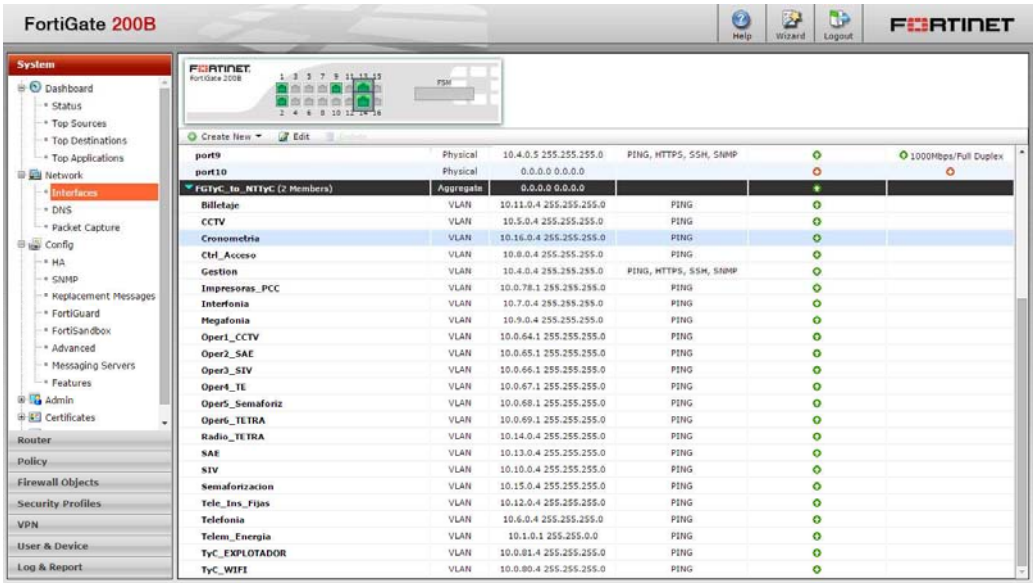
Los equipos se han configurado en activo pasivo como se puede ver en la siguiente imagen:



FGTyC_a es el equipo maestro y funciona como activo. En caso de fallo por parte del firewall maestro, FGTyC_b pasara a ser el activo y tomar el control de la seguridad.

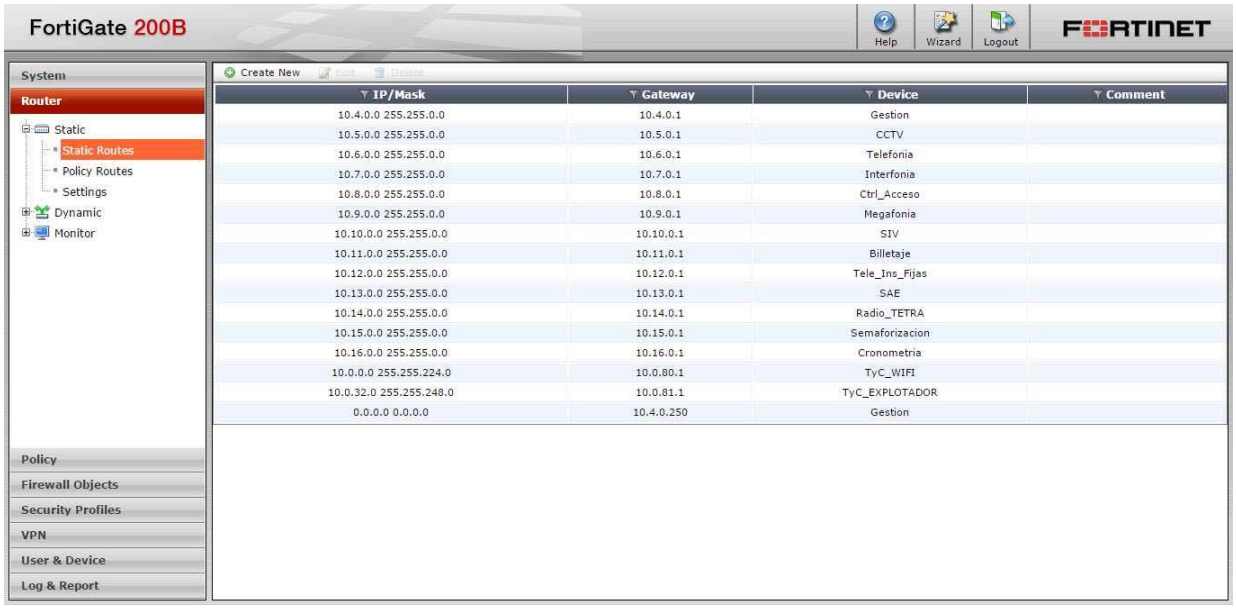
7.2.2. Interfaces

La interfaces configuradas en ambos firewalls corresponde a una interfaz virtual agregada compuesta por los puertos 13 y 14 de cada equipo. A través de estos puertos agregados están definidas las vlanes correspondientes a los gateways de cada una de la VRF configuradas en los 4500. Esto posibilita mayor seguridad ya que cualquier servicio que quisiera comunicarse con otro tendría que pasar por el firewall y obtener los permisos necesarios.



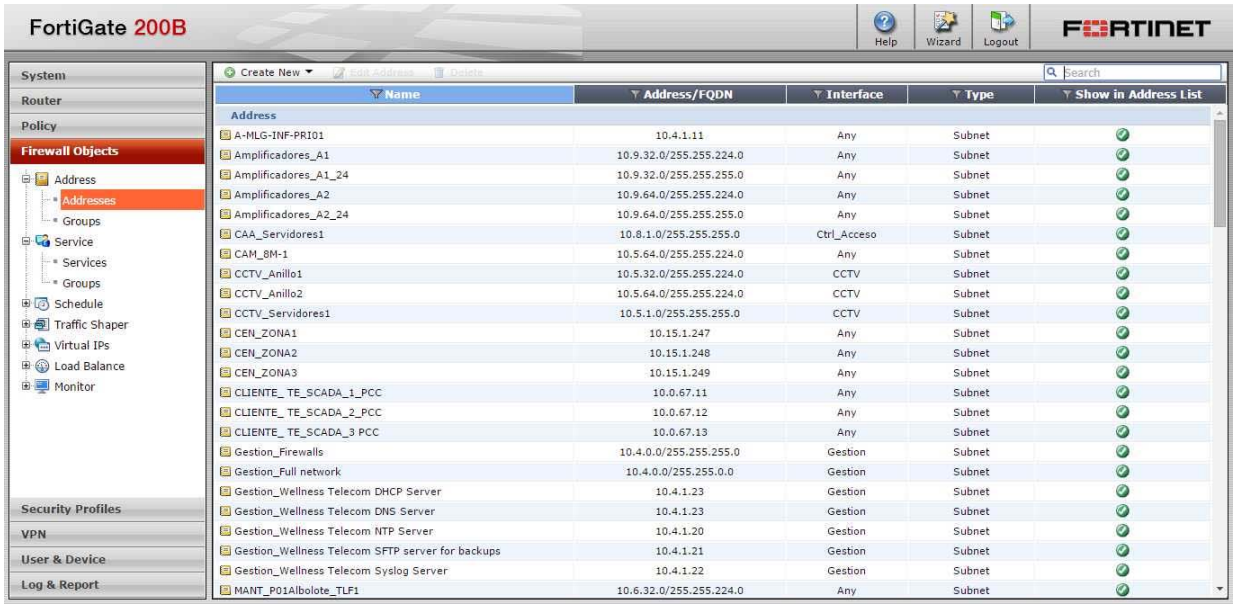
7.2.3. Routing

El equipo no tiene configurado un acceso exterior por lo que se ha definido la ruta por defecto hacia la red de Gestión. También se han definido las rutas estáticas correspondientes para acceder a las redes multiservicio, siempre que las políticas de seguridad lo permitan.

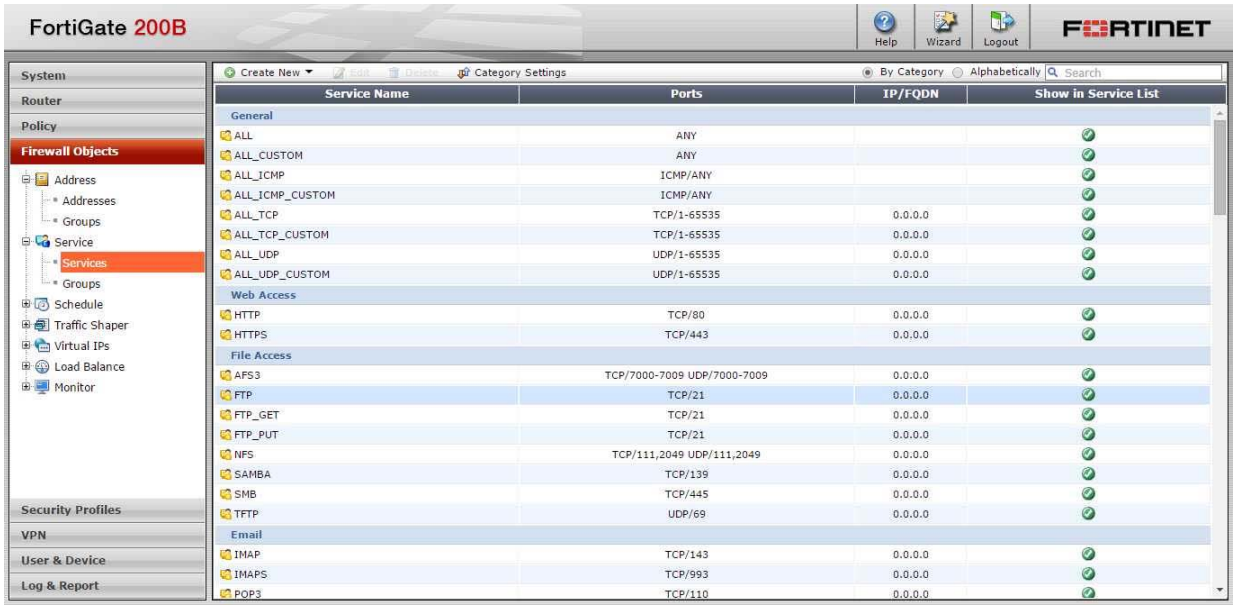


7.2.4. Firewall Objects

En esta parte del firewall es donde definimos los objetos o grupo de objetos que queremos representar para más tarde dar o quitar acceso sobre una o varias políticas.

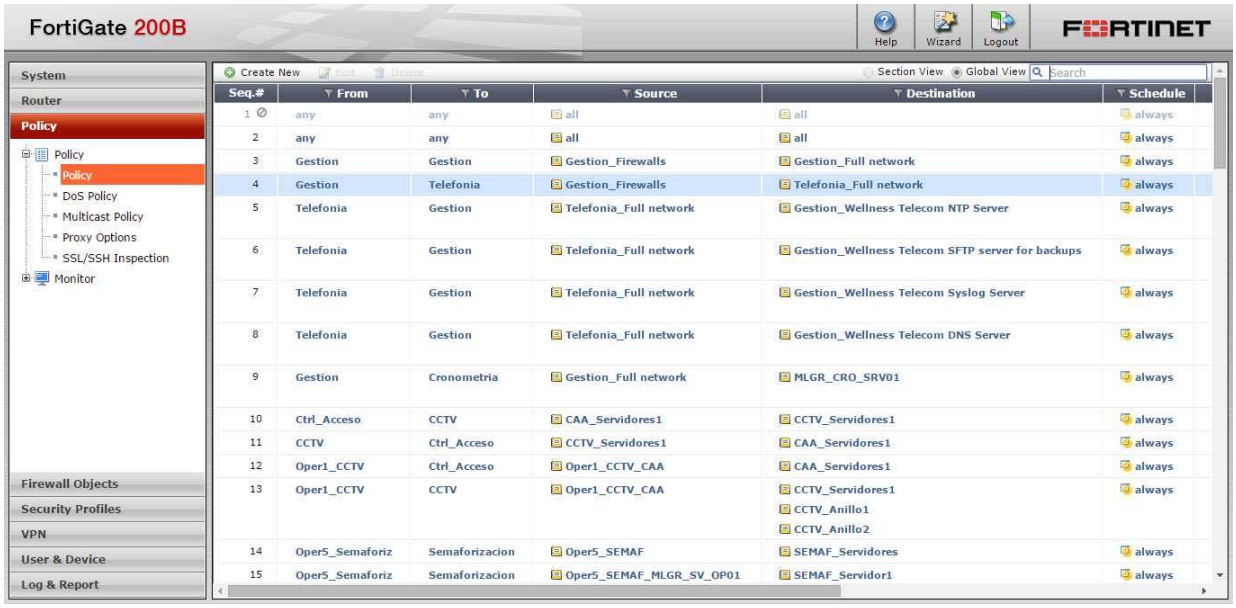


Al igual que los objetos también podemos crear servicios o aplicaciones que igualmente usaremos más tarde en dichas políticas ya sea para permitir o denegar.



7.2.5. Políticas

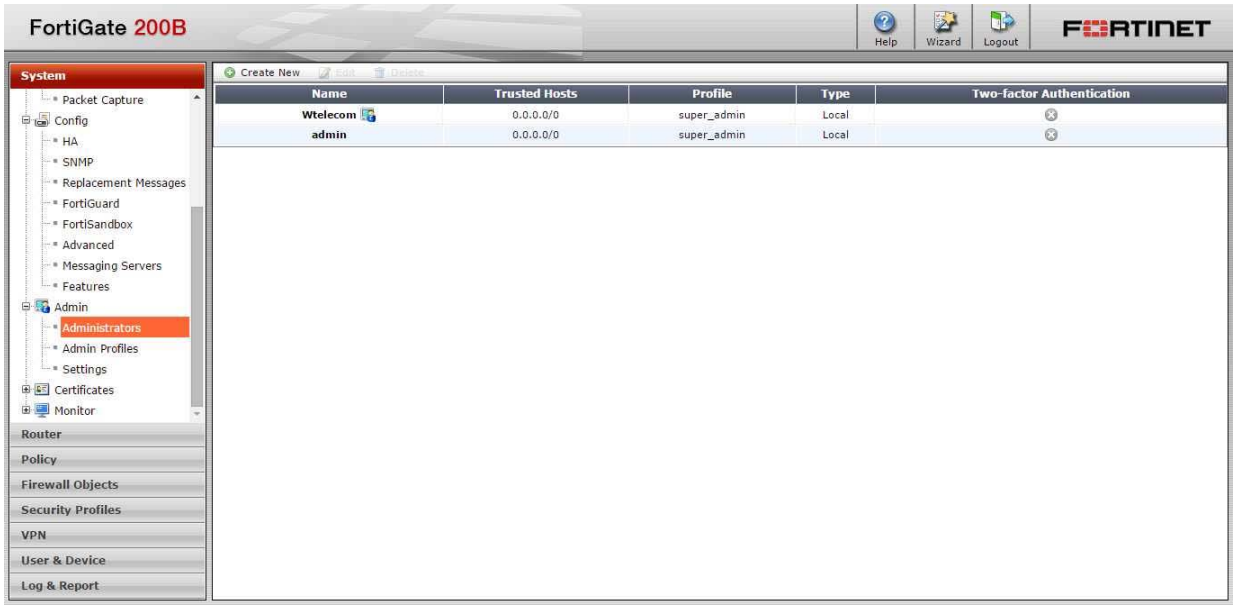
Las políticas que se han definido hasta el momento son las que vienen definidas por la dirección y se pueden ver en el apartado de Policy.



Todas las políticas, rutas, objetos e interfaces configurados se muestran en el archivo adjunto “Firewall Request”.

7.2.6. Usuarios

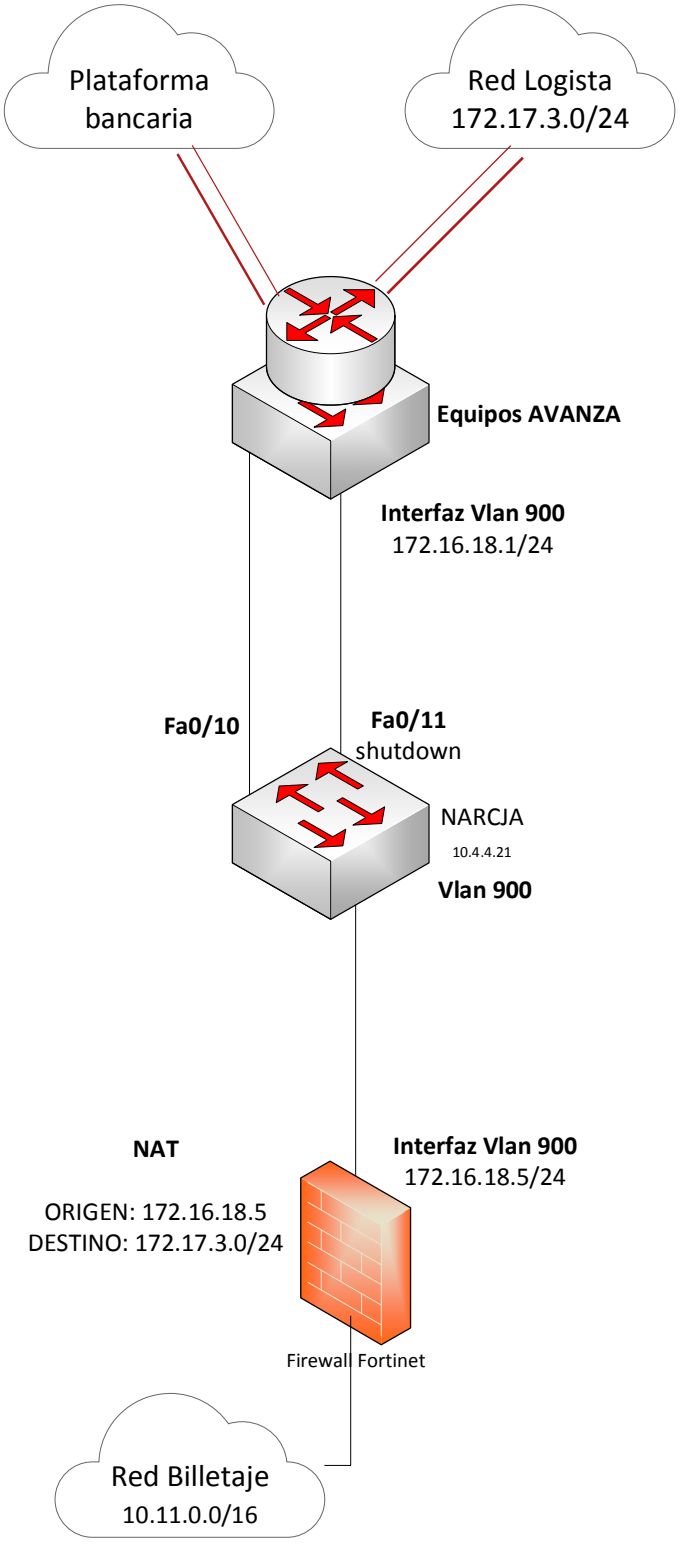
Los usuarios definidos para poder gestionar el firewall desde la red de gestión son los mostrados a continuación:



8. Configuraciones especiales

8.1. Red Avanza y Logista

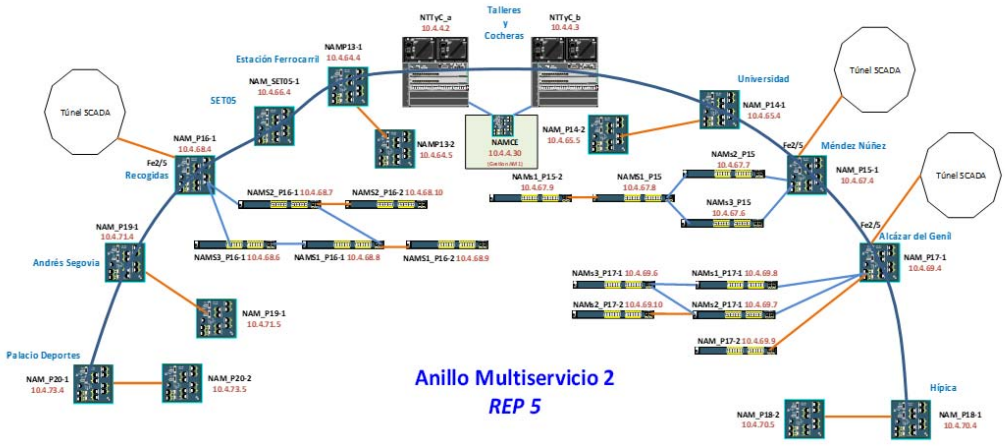
La conexión entre los equipos de la red de Billetaje de Metro y el servidor de la empresa externa Logista para la validación de las tarjetas del Consorcio de Transportes se ha realizado a través de la red del operador Avanza, al no disponer Metro de Granada de un acceso directo a Internet. La conexión física entre la red de Metro y la de Avanza se realiza en los puertos 10 y 11 del switch NARCJA.
Por la parte de Avanza se ha generado un túnel vpn con Logista a través de la salida a Internet y se han implementado las rutas para el encaminamiento entre la red de Avanza en Talleres y Cocheras y dicho túnel.
Por la parte de la red de metro de Granada, se ha configurado una Vlan (900) con un direccionamiento compartido (172.16.18.0/24), implementándose una ruta para la conexión a la red de Logista a través del firewall de Avanza y una política que permite la comunicación entre la red de Billetaje y la de Avanza para direcciones destino en la red de Logista. En la política de Firewall se ha configurado NAT para evitar overlap de IPs con las redes externas. De esta forma, todos los paquetes provenientes de la red de Billetaje salen hacia la red de Avanza con IP origen 172.16.18.5.



Tal como se muestra en la imagen, la comunicación con la pasarela bancaria está previsto realizarla igualmente a través de la conexión con la red de Avanza.

8.2. SCADA Local túnel

En cada una de las tres estaciones de túnel (P15, P16 y P17) existe una red de SCADA local externa a la red de Metro, que se conecta a esta última a través del puerto Fe2/5 del switch principal de dicha parada:

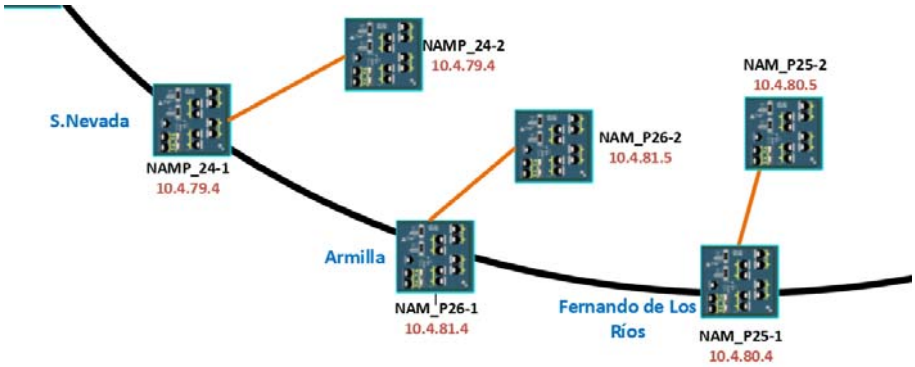


Debido a que al conectar la red de SCADA local a la red de Metro se producía un fallo de MAC-FLAP con la dirección f0:b4:e5:9f:f0:b4, se ha filtrado dicha MAC en el puerto del switch de Metro donde se conecta la red de SCADA local, respectivamente en cada una de las tres estaciones.
Además, para reforzar la seguridad frente a problemas de red que posibles modificaciones en la red de SCADA local puedan introducir en un futuro, se ha limitado el número de MAC máximas admitidas a 32. De esta forma, si en el futuro se añadiese a alguna de las redes de SCADA local algún equipo nuevo tendrían que comunicarlo a Metro para que se ampliase el número de MACs y así pueda tener conexión con la red de Metro.

```
interface FastEthernet2/5
 description TIF_ANILLO_MS2
 switchport access vlan 501
 switchport mode access
 switchport port-security maximum 34
 switchport port-security violation restrict
 switchport port-security mac-address 000c.f900.491f
 switchport port-security mac-address 001b.1bad.41a9
 switchport port-security mac-address 001b.1bb1.b605
 switchport port-security mac-address 001b.1bb2.5223
 switchport port-security mac-address 001b.1bb2.748f
 switchport port-security mac-address 001b.1bb2.74b2
 switchport port-security mac-address 001b.1bb3.01fb
 switchport port-security mac-address 001b.1bb3.02cd
 switchport port-security mac-address 001b.1bef.d9e9
 switchport port-security mac-address 0030.110c.2486
 switchport port-security mac-address 0030.110c.2489
 switchport port-security mac-address 0030.110c.2492
 switchport port-security mac-address 0030.110c.24a4
 switchport port-security mac-address 0030.110c.dfe9
 switchport port-security mac-address 0030.110c.e011
 switchport port-security mac-address 0090.c2f2.c22b
 switchport port-security mac-address 0800.271f.7bf4
 switchport port-security mac-address 20bb.c033.c2c2
 switchport port-security mac-address 2863.3680.bd60
 switchport port-security mac-address 2863.3680.bd66
 switchport port-security mac-address 2863.3680.bd84
 switchport port-security mac-address 2863.3685.824f
 switchport port-security mac-address 2863.3685.85a9
 switchport port-security mac-address 2863.3685.85fe
 switchport port-security mac-address 2863.3685.8647
 switchport port-security mac-address 2863.3685.8673
 switchport port-security mac-address 2863.3686.b79e
 switchport port-security mac-address 2863.3689.acc5
 switchport port-security mac-address 4216.7eb5.e6f0
 switchport port-security mac-address d8cb.8af2.8097
 switchport port-security mac-address e0dc.a000.6dc3
 switchport port-security mac-address e0dc.a000.6ea8
 switchport port-security mac-address e0dc.a000.8a71
 storm-control broadcast level 25.00
 storm-control multicast level 25.00
 storm-control action shutdown
 macro description PUERTO_TIF
 mac access-group MAC_FILTER_SCADA in
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
```

8.3. Control de tráfico Armilla

En los switches de las paradas 24, 25 y 26 (Anillo Multiservicio 2) se han configurado varios puertos en una misma VLAN, sin conectividad con el resto de la red, solo para interconexión entre los equipos del Control de tráfico de Armilla conectados a dichos puertos. La VLAN es la 800, llamada CTRAF_ARMILLA.



En la configuración de los puertos de esta VLAN se ha eliminado la limitación de una única MAC permitida por el puerto.

```
interface FastEthernet2/7
 description CTRAF_ARMILLA
 switchport access vlan 800
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 storm-control broadcast level 25.00
 storm-control multicast level 25.00
 storm-control action shutdown
 macro description PUERTO_TRAFARMILLA
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
end
```

8.4. Conexión equipos Tetra

Se configuran varios puertos en los 4500 y en los switches NAMPCC en una misma VLAN (Vlan 35), sin conectividad con el resto de la red, solo para interconexión entre equipos del Sistema Tetra conectados a dichos puertos.

```
NAMPCC-1#sh vlan | i TETRA
35   TYC_PCC_OPER_TETRA               active    Gi1/0/14
NAMPCC-1#
```

```
NAMPCC-1#sh run int gi 1/0/14
Building configuration...

Current configuration : 367 bytes
!
interface GigabitEthernet1/0/14
 description Operadores TETRA
 switchport access vlan 35
 switchport mode access
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 macro description cisco-desktop
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

Igualmente, se configuran varios puertos en los 4500 y en el switch NARCJA en una misma VLAN (Vlan 595,596 y 597), sin conectividad con el resto de la red, solo para interconexión entre equipos del Sistema Tetra conectados a dichos puertos:

```
NTTyC_a#sh vlan | i TETRA
35   TYC_PCC_OPER_TETRA               active    Gi4/41
580  TETRA_ANILLO1                    active
581  TETRA_ANILLO2                    active
592  TETRA_FIREW                      active
593  TETRA_SERV1                      active
595  TETRA-P23                        active
596  TETRA-P24                        active    Gi4/40
597  TETRA-P31                        active
NTTyC_a#
```

```
NARCJA#sh vlan | i TETRA
595  TETRA-P23                        active    Fa0/7
596  TETRA-P24                        active    Fa0/8
597  TETRA-P31                        active    Fa0/9
```

8.5. Conexión equipos AOPJA

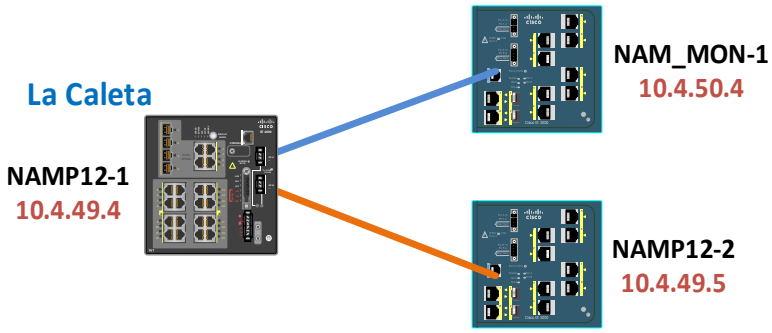
Se configuran varios puertos en el switch NAMCE y en el switch NARCJA en una misma VLAN (Vlan 28), sin conectividad con el resto de la red, solo para interconexión entre equipos de la AOPJA conectados a dichos puertos.

```
NAMCE#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa2/1, Fa2/2, Fa2/3, Fa2/4
                                                Fa2/7, Fa2/8, Fa3/3, Fa3/4
28   AOPJA                            active    Fa3/5, Fa3/6, Fa3/7, Fa3/8
```

8.6. CCAA MONDRAGONES

En la parada de Caleta (Anillo Multiservicio 1), como switch principal del nodo se ha instalado un IE-4000 que enlaza mediante FO multimodo con el IE-3000 instalado en el Complejo Administrativo Los Mondragones (NAM_MON-1), para conectividad de un PC de semaforización y un teléfono, según el siguiente esquema:



Se ha optado por un IE-4000, en lugar de un IE-3000 como en el resto de paradas, debido a la necesidad de disponer de un mayor número de puertos gigabit para poder conectar, además del anillo multiservicio y el switch de CCTV, el switch del CCAA Los Mondragones mediante dos enlaces de fibra óptica multimodo.

8.7. Enclavamientos Señalización

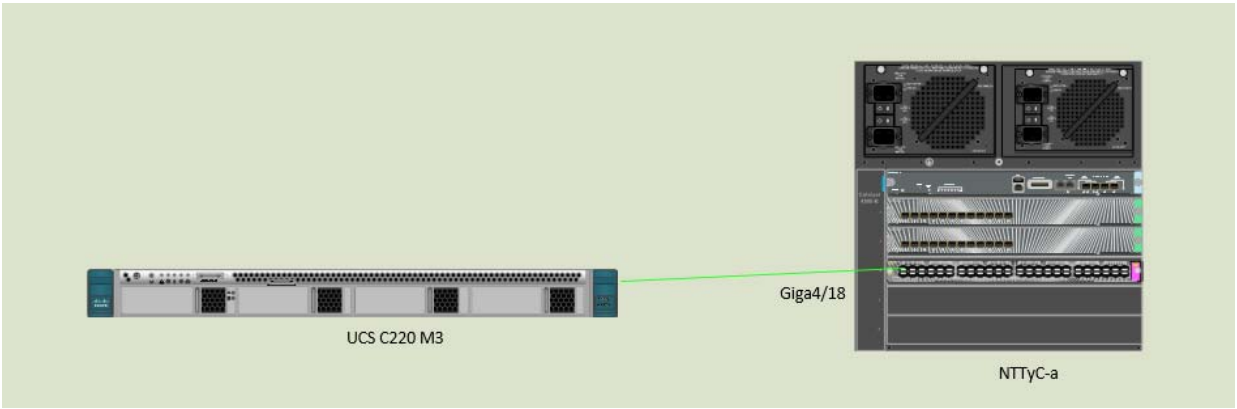
En los switches de la red de señalización se ha eliminado la limitación de una única MAC permitida por puerto en los puertos donde se conectan los emplazamientos.

8.8. Punto de atención al cliente de Avanza (provisional)

En la parada P16 Recogidas se han instalado dos PC´s en el puesto de atención al cliente, ubicado en las taquillas de dicha estación, que requieren conexión con la red de Avanza en TyC. De forma provisional, hasta que se genere una nueva VRF Avanza que se extienda por los anillos multiservicio 1 y 2, se le ha asignado a dichos PCs dos direcciones IP (10.7.68.120, 10.7.68.121) dentro del direccionamiento reservado para la red de interfonía en el anillo multiservicio 2 y se ha creado una política en el firewall para permitir la comunicación entre dichas IPs y la red de Avanza en Talleres y Cocheras.

9. Servidor Multipropósito

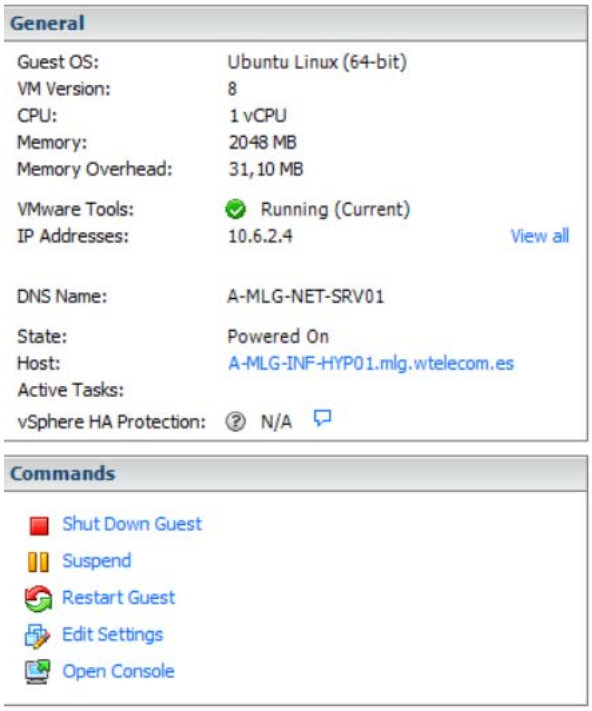
El Servidor multipropósito está conectado a los Cisco 4500 de Talleres y Cocheras según el siguiente esquema:

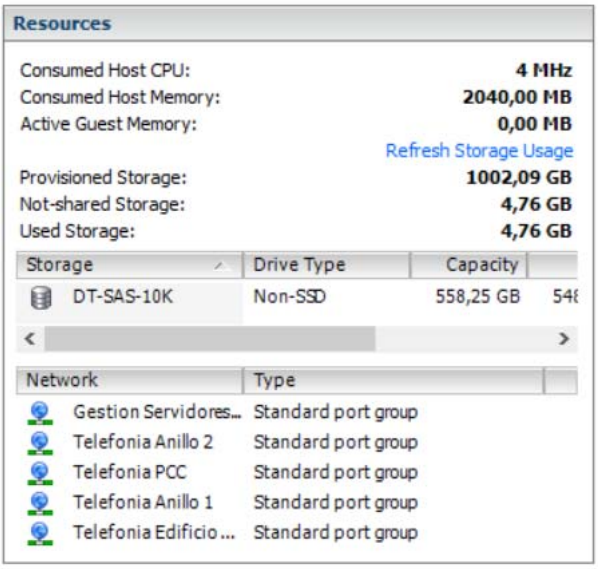


En este servidor se han creado dos máquinas virtuales:

a. **A-MLG-INF-SYS01**

Los recursos asignados a este servidor son los siguientes:





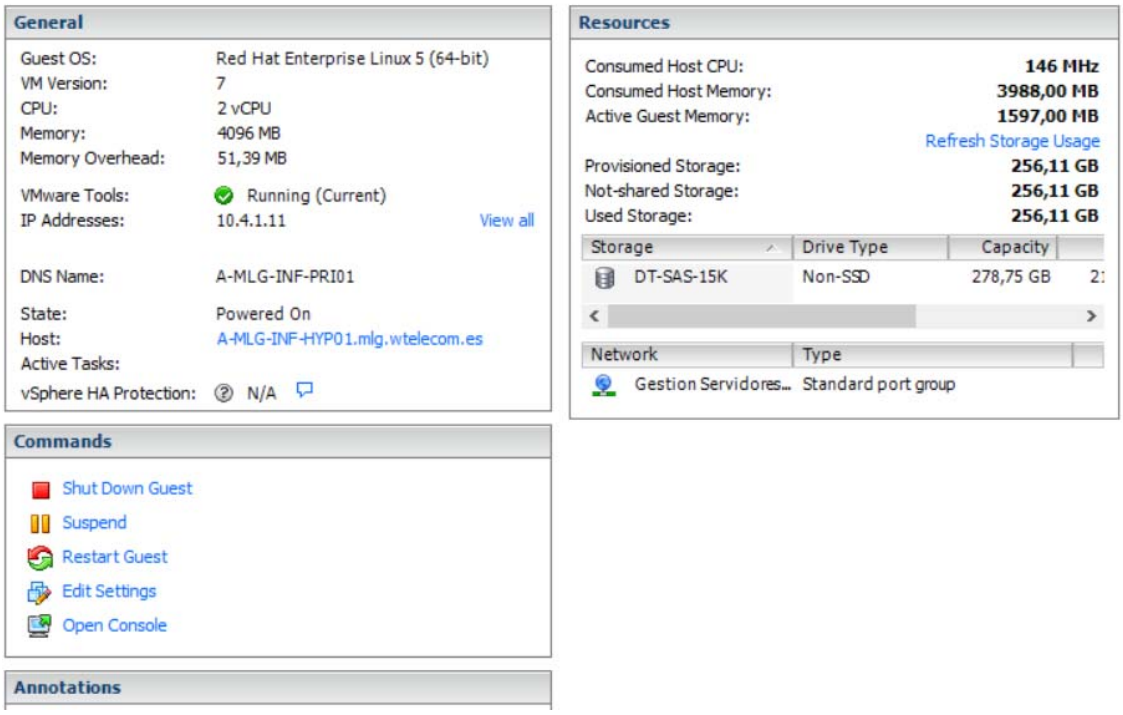
Esta máquina está dedicada a los siguientes servicios:

NTP, DHCP, DNS, SYSLOG, SFTP, DHCP

IP	Servicios
10.6.2.4	DHCP Telefonía
10.6.32.4	DHCP Telefonía
10.6.64.4	DHCP Telefonía
10.4.1.20	NTP Server
10.4.1.21	SFTP/SCP Server
10.4.1.22	Syslog Server
10.4.1.24	DNS Server

b. **Cisco Prime LAN Management Solution**

Los recursos asignados a este servidor son los siguientes:



Esta máquina está dedicada al servicio Cisco Prime Management:

IP	Servicios
10.4.1.11	SNMP Server

10. Telefonía

El sistema de telefonía del Metropolitano de Granada está basado en tecnología IP y se compone de los siguientes elementos:

- Cluster Servidor de llamadas (Call Manager): Es el elemento central, el cerebro de la red de telefonía IP. Se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, traducción de direcciones, administración de zonas, autorización y administración de llamadas, etc. Sus principales características se detallan más adelante.
- Gateway de voz (Pasarela): Es el dispositivo encargado de proporcionar el acceso hacia las redes exteriores a los terminales de la red IP conectados a él.
- Grabador de voz: Se han instalado equipos especiales de grabación digital compatibles con la centralita IP a instalar, para cumplir con los requisitos legales de seguridad. Las grabaciones son accesibles y se pueden almacenar mensajes para recuperarlos posteriormente.
- Teléfonos IP: Como terminal de usuario de telefonía se han utilizado terminales telefónicos IP estándar, homologados para su utilización en la red telefónica pública europea. Se distinguen tres tipos de terminales: de funcionalidad básica, de funcionalidad media y de funcionalidad avanzada

En la siguiente tabla se resume el equipamiento que compone la red de Telefonía:

Electrónica de Red IP Telefonía Metro de Granada					
Red	**Equipos**	**Cantidad**	**Marca/modelo**	**Descripción**	**Ubicación**
Telefonía	CCM_PUB01 CCM_SUB01	2	MCS7825I5-K9-CME1	Servidor para Call Manager	Sala Técnica TyC (2)
Telefonía	GW_PRI01	1	Cisco 2961	Router Gateway Telefonía	Sala Técnica PCC (1)
Telefonía	Grabadores	2	UCS-C220-M3	Servidor para aplicación de grabación	Sala Técnica TyC (2)
Telefonía	A-MLG-NET-SRV01	1	UCS-C220-M3 Ubuntu 12.04.2 LTS	Servidor DHCP	Sala Técnica TyC

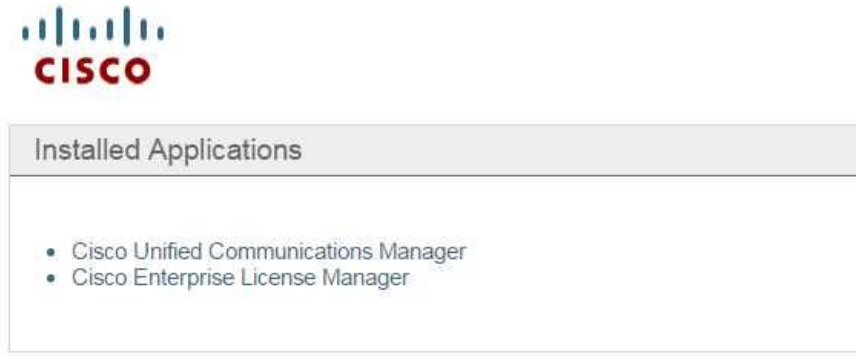
10.1. Centralita IP

El servidor central de telefonía está formado por un clúster de dos servidores MCS:

- CUCM Publisher: 10.6.1.11
- CUCM Subscriber: 10.6.1.12

Cisco Call Manager es el servicio principal de la plataforma de telefonía, y se encarga de gestionar las llamadas. Dicho servicio está activo en los servidores que forman el clúster (Publisher y Subscriber).

Para acceder a la administración de la centralita hay que hacerlo a través de la url: http://10.6.1.11/



La distribución de los terminales telefónicos en las diferentes ubicaciones se muestra en el archivo adjunto “MLGR_Datos para configuracion CM”.

10.2. Plan de numeración (rangos de extensiones)

Los Directory Number (DN) son las extensiones propias de los usuarios. Dentro de cada DN se definen multitud de parámetros, entre los que destacan los siguientes:

- **Particiones**: Las particiones nos permiten dividir el plan de numeración en grupos lógicos con similares características, y, mediante el uso de CSS, restringir el acceso a dichos recursos.

  La configuración de las particiones admite multitud de posibilidades, y va a depender de la granularidad que se quiera a la hora de hacer restricciones en las llamadas, ya que aumentar mucho el número de particiones supone un aumento de complejidad en el plan de numeración.

  Se han configurado las siguientes particiones:

PT_112	PT_112
PT_900	PT_900
PT_901	PT_901
PT_EXT_JUNTA	PT_EXT_JUNTA
PT_TETRA	PT_TETRA
PT_cortos	PT_cortos
PT_extensiones	PT_extensiones
PT_fijos	PT_fijos
PT_interfono	PT_interfono
PT_internacionales	PT_internacionales
PT_moviles	PT_moviles

- **CSS (Calling Search Space)**:
  En los *CSS* se lleva a cabo la agrupación de una serie de particiones a las cuales tendrá acceso el dispositivo al que se le aplique el CSS.

  Los *CSS* definidos son los siguientes:

CSS Name ▲	
CSS_L0	Llamadas a extensiones coporativas + 112
CSS_L1	Llamadas a L0 + fijos + cortos + mov
CSS_L2	Llamadas a L1 + especiales
CSS_L3	Llamadas a L2 + internacionales
CSS_interfono	Llamadas a centralita

  Se han considerado 4 niveles de permisos para cada sede. Conforme se aumenta el nivel del CSS aumentan los permisos para realizar llamadas a números públicos, teniendo el mismo comportamiento en cualquiera de las sedes.

- **Desvíos**: Se han configurado los desvíos según diversas condiciones (desvío incondicional, por no respuesta, ocupado…). Además, se asigna un permiso a cada tipo de desvío con un CSS. Este aspecto es importante tenerlo controlado, ya que existe un tipo de fraude que consiste en realizar desvíos hacia números personales. Por ejemplo, si un trabajador se va de vacaciones puede desviar su número del trabajo a un número extranjero o a su propio móvil, y decir a sus familiares que para localizarle le llamen al número del trabajo, de manera que la empresa pagará todas esas llamadas personales. Se recomienda que por defecto se tenga permiso para realizar desvíos a otras extensiones. En el caso de que sea necesario siempre se puede ampliar esa restricción.

- **External Phone Number Mask**: Define el número público que se usará para realizar llamadas.

- **Número Máximo de Llamadas**: Define el número máximo de llamadas simultáneas que puede procesar la línea.
- **Busy Trigger**: Define el número máximo de llamadas permitidas antes de que devuelva tono de ocupado.

Una línea se puede usar en más de un teléfono, denominándose una línea compartida. A la hora de recibir una llamada sonaría en los dos teléfonos de manera simultánea. También es posible que un teléfono tenga más de una línea (para ello necesita que tenga más de un botón, 794X en adelante), de manera que dos usuarios pudieran compartir terminal con la restricción que solo uno podría usarlo al mismo tiempo.

Para evitar el solape entre los diferentes rangos de numeración el plan de numeración propuesto es el siguiente:

- Rango de extensiones asociadas a terminales fijos corporativos: 3XXX
- Rango de extensiones asociadas a terminales móviles corporativos: 4XXX
- Rango de extensiones asociadas a terminales TETRA: 5XXX
- Rango de extensiones asociadas a los interfonos: 6XXX

Por otro lado, se ha llevado a cabo la integración de la telefonía de Metro con la telefonía de la Red Corporativa de la Junta de Andalucía (RCJA). Para ello, se ha reservado una serie de extensiones (rango no solapado en el sistema de telefonía de la RCJA):

Largo	Corto	Largo	Corto	Largo	Corto	Largo	Corto
958575830	170830	958575840	170840	958575850	170850	958575860	170860
958575831	170831	958575841	170841	958575851	170851	958575861	170861
958575832	170832	958575842	170842	958575852	170852	958575862	170862
958575833	170833	958575843	170843	958575853	170853	958575863	170863
958575834	170834	958575844	170844	958575854	170854	958575864	170864
958575835	170835	958575845	170845	958575855	170855	958575865	170865
958575836	170836	958575846	170846	958575856	170856	958575866	170866
958575837	170837	958575847	170847	958575857	170857		
958575838	170838	958575848	170848	958575858	170858		
958575839	170839	958575849	170849	958575859	170859		

Como se puede ver el rango reservado es el 1708[3-6]X.

La asignación de extensiones a usuarios se muestra en el archivo adjunto “MLGR_Datos para configuracion CM”.

10.3. Plan de enrutamiento de llamadas

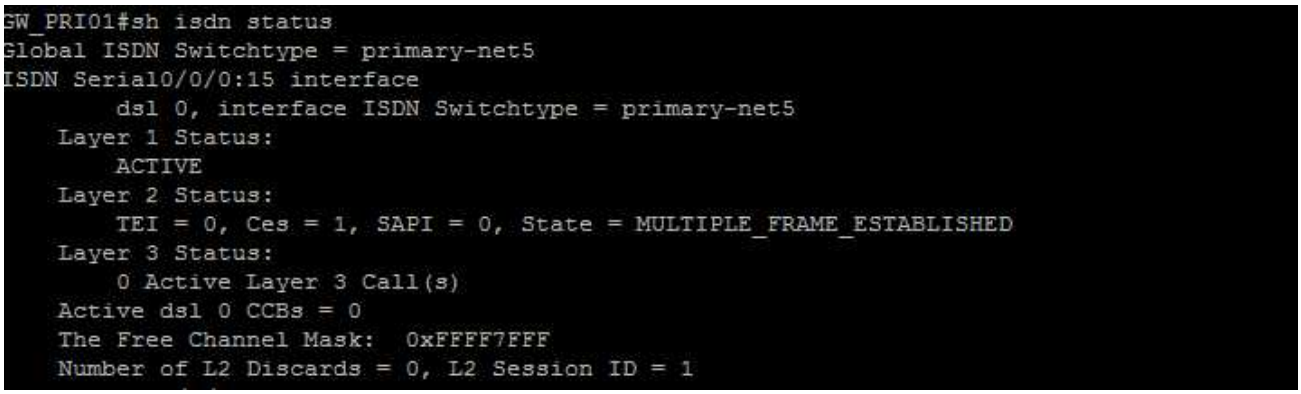
Para las llamadas al exterior se ha instalado un primario E1 de 30 canales instalado en el rack de la Agencia de Obra Pública de la Junta de Andalucía (AOPJA) ubicado en la sala técnica del PCC. Esto ha hecho necesario que el Gateway de voz (router 2901) se instale también en dicho rack, debido a la distancia con la sala técnica de TyC. De esta forma, la conexión entre el Gateway y los 4500 a los que se conecta el Call Manager se ha realizado mediante la conexión del primero al switch NARCJA, ubicado en el rack de la AOPJA, que está conectado a los nodos troncales 4500 mediante fibra óptica multimodo.

A dicho switch NARCJA se ha conectado también un router Macrolan de la AOPJA que proporciona una conexión con el SBC de la Red Corporativa de la Junta de Andalucía (RCJA), permitiendo la comunicación entre este último y el Call Manager (CM) de Metro. Así, se ha configurado el CM para que las llamadas entre las extensiones de Metro integradas en la RCJA citadas anteriormente y los

teléfonos de la RCJA (fijos y móviles corporativos) se realicen a través de dicho enlace, sin coste alguno para ambos.

Para establecer la comunicación entre el SBC y el CUCM es necesario llevar a cabo un NAT en el firewall Fortinet que conecta las diferentes redes.:

El primario está listo para recibir y realizar llamadas a través del mismo como se puede observar en la siguiente imagen:



La configuración realizada para llevar a cabo la puesta en marcha del primario es la siguiente:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GW_PRI01
!
boot-start-marker
boot-end-marker
!
!
card type e1 0 0
card type e1 0 1
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 warnings
!
no aaa new-model
clock timezone GMT+1 1 0
network-clock-participate wic 0
network-clock-participate wic 1
network-clock-select 1 E1 0/0/0
network-clock-select 2 E1 0/0/1
network-clock-select 3 E1 0/1/0
!
ip cef
!
!
!
!
!
!
ip domain name yourdomain.com
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-net5
!
!
trunk group PRIMARIO
 hunt-scheme longest-idle
!
!
crypto pki trustpoint TP-self-signed-2870714897
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2870714897
 revocation-check none
 rsakeypair TP-self-signed-2870714897
```

```
!
controller E1 0/0/0
 pri-group timeslots 1-31
!
controller E1 0/0/1
 pri-group timeslots 1-31
!
controller E1 0/1/0
 pri-group timeslots 1-31
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 10.6.1.20 255.255.255.0
 duplex auto
 speed auto
!
interface ISM0/0
 no ip address
 shutdown
 service-module fail-open
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ISM0/1
 description Internal switch interface connected to Internal Service Module
 no ip address
!
interface Serial0/0/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn bchan-number-order ascending
 isdn sending-complete
 trunk-group PRIMARIO 1
 no cdp enable
!
```

Como se puede ver, el Gateway dispone de dos tarjetas HWIC para la conexión de hasta tres primarios E1. Una tarjeta con dos puertos E1 y otra con uno.

```
!
interface Serial0/0/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn bchan-number-order ascending
 isdn sending-complete
 trunk-group PRIMARIO 1
 no cdp enable
!
interface Serial0/0/1:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn bchan-number-order ascending
 isdn sending-complete
 no cdp enable
!
interface Serial0/1/0:15
 no ip address
 encapsulation hdlc
 logging event link-status bchan
 isdn switch-type primary-qsig
 isdn timer T310 120000
 isdn overlap-receiving
 isdn protocol-emulate network
 isdn incoming-voice voice
 isdn sending-complete
 trunk-group TETRA
 no cdp enable
!
```

El primario está conectado al puerto E0 de la tarjeta instalada en el slot HWIC0 del Gateway de voz. Las llamadas salientes al exterior desde los teléfonos de Metro se realizarán a través de este primario. Para evitar solapamiento con los diferentes rangos de extensiones de la RCJA se debe de marcar el “0” delante del número a marcar.

Para las llamadas entre teléfonos y terminales Tetra de Metro, se ha conectado el Gateway del sistema Tetra (MTIG+EC), ubicado en el mismo rack de la AOPJA, al puerto E0 de la tarjeta instalada en el slot HWIC1 del Gateway de telefonía.

El estado de la conexión es el correcto:

```
ISDN Serial0/1/0:15 interface
        ******* Network side configuration *******
        dsl 2, interface ISDN Switchtype = primary-qsig
         **** Master side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask:  0xFFFF7FFF
    Number of L2 Discards = 0, L2 Session ID = 227
    Total Allocated ISDN CCBs = 0
```

Siendo la configuración de la interfaz la que sigue:

```
!
interface Serial0/1/0:15
 no ip address
 encapsulation hdlc
 logging event link-status bchan
 isdn switch-type primary-qsig
 isdn timer T310 120000
 isdn overlap-receiving
 isdn protocol-emulate network
 isdn incoming-voice voice
 isdn sending-complete
 trunk-group TETRA
 no cdp enable
end
```

Se han definido los siguientes *Route Patterns* en el Call Manager para poder enrutar las diferentes llamadas:

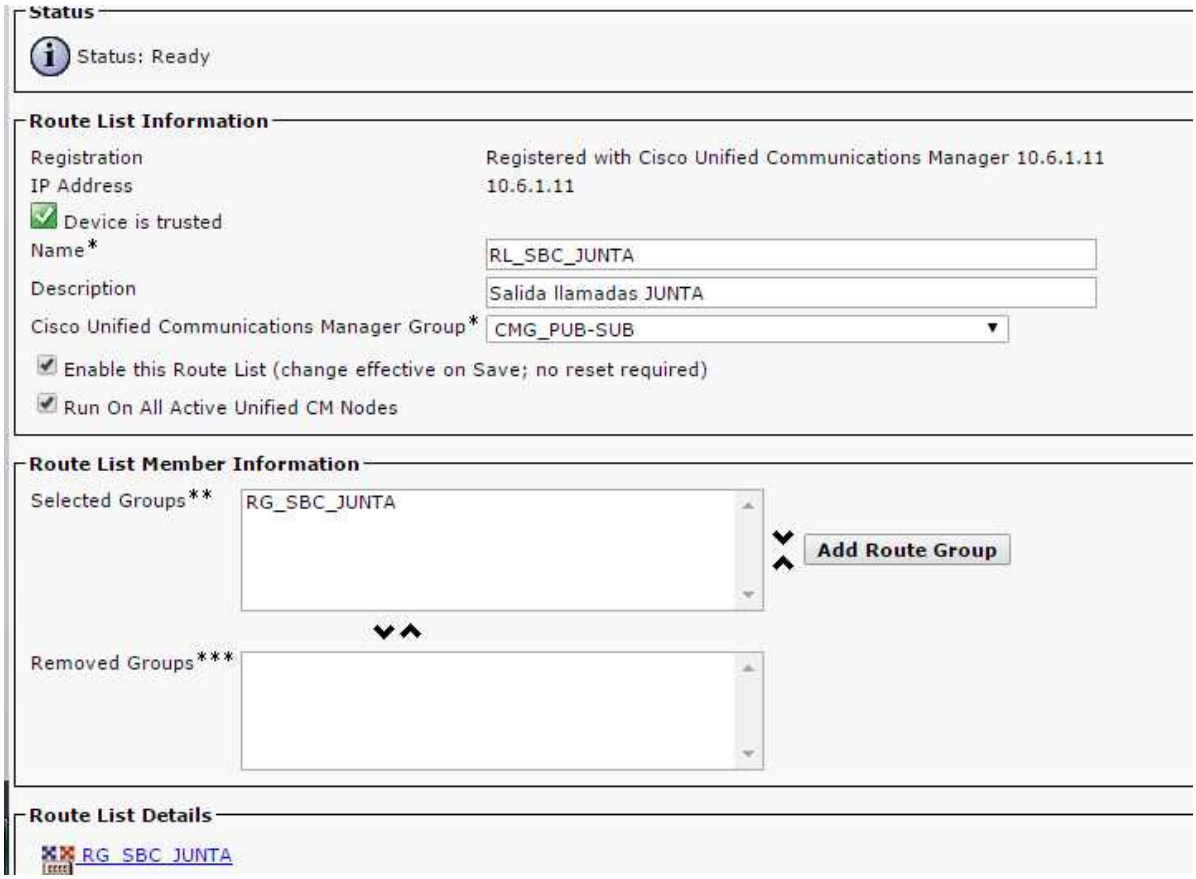
Pattern	Description	Partition	Route Filter	Associated Device
0.00!	Números Internacionales	PT_internacionales		RL_ES-Metro
0.0[1-9]x	Numeros Cortos 3 Cifras	PT_cortos		RL_ES-Metro
0.112	Emergencias con 0	PT_112		RL_ES-Metro
0.118XX	Numeros Cortos 5 Cifras	PT_cortos		RL_ES-Metro
0.1[02-9]XX	Numeros Cortos 4 Cifras	PT_cortos		RL_ES-Metro
0.900[1-9]XXXXX	Numeros Cobro Revertido	PT_900		RL_ES-Metro
0.90[1-2]XXXXXX	Numeros Pago Compartido/Llamante	PT_900		RL_ES-Metro
0.[67]XXXXXXXX	Números Móviles España	PT_moviles		RL_ES-Metro
0.[8-9][1-9]XXXXXXX	Numeros Geograficos España	PT_fijos		RL_ES-Metro
112	Emergencias	PT_112		RL_ES-Metro
1XXXXX	Llamadas a extensiones fijas JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
2XXXXX	Llamadas a extensiones fijas JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
3999	RP_CrossRecorder_1812	PT_extensiones		RL_CrossRecorder_1812
3XXXXX	Llamadas a extensiones fijas JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
5XXX	Llamadas a extensiones red TETRA	PT_TETRA		RL_ES-Metro
5XXXXX	Llamadas a extensiones fijas JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
6XXXXX	Llamadas a moviles JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
7[0-2]XXXX	Llamadas a fijas JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA
7[3-6]XXXX	Llamadas a moviles JUNTA Andalucia	PT_EXT_JUNTA		RL_SBC_JUNTA

Las llamadas internas entre las extensiones de Metro, interfonía y móviles corporativos, no requieren de prefijo para llamar, por lo que directamente se marcará la extensión del teléfono a marcar.

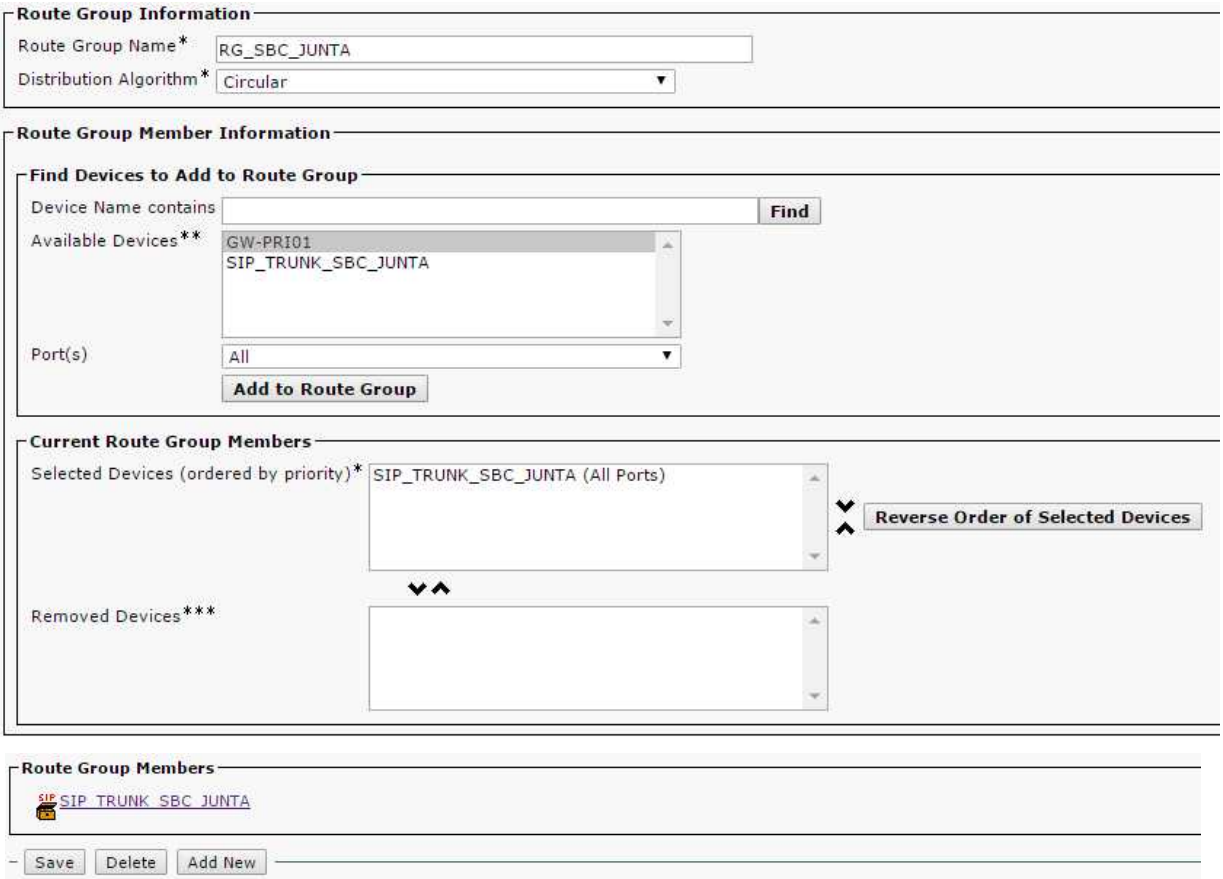
Tal como se ha indicado, las llamadas entre las extensiones de Metro integradas en la RCJA citadas anteriormente (170830- 170864) y los teléfonos de la RCJA (fijos y móviles corporativos) se realizan a través del enlace entre el CM de Metro y el SBC de la RCJA.

Para el enrutamiento de llamadas se han definido los siguientes **Route List**:

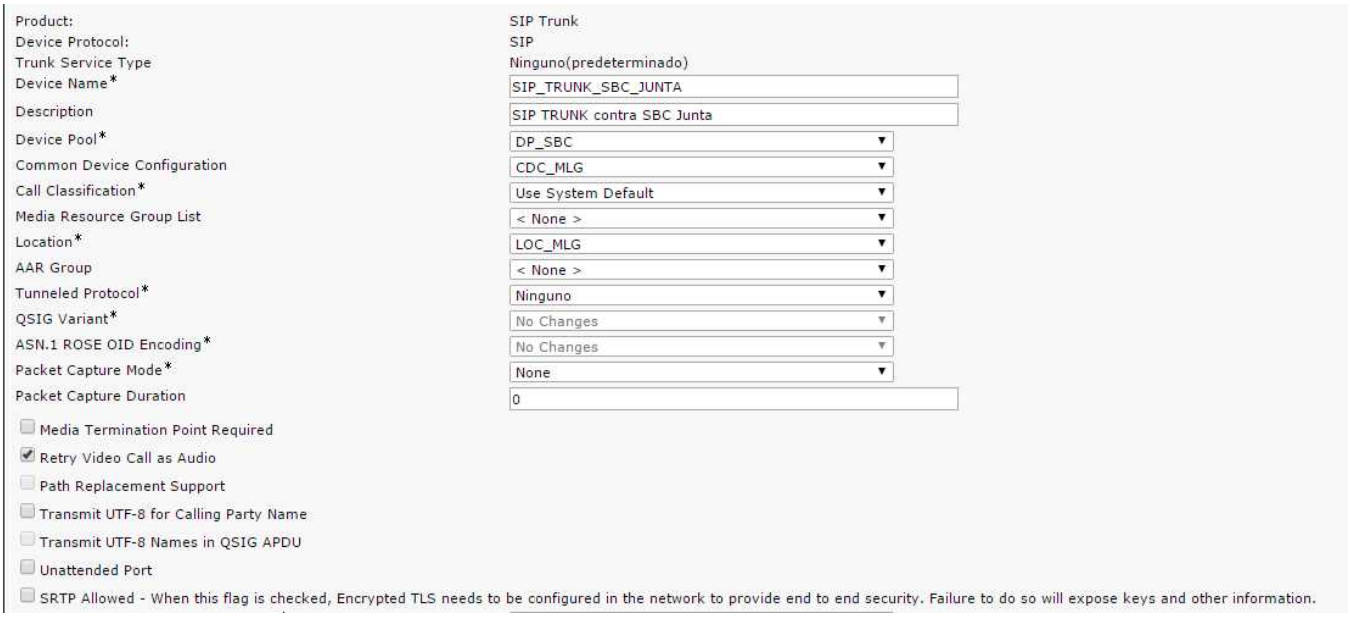
- Salida de llamadas por el SBC de la RCJA:

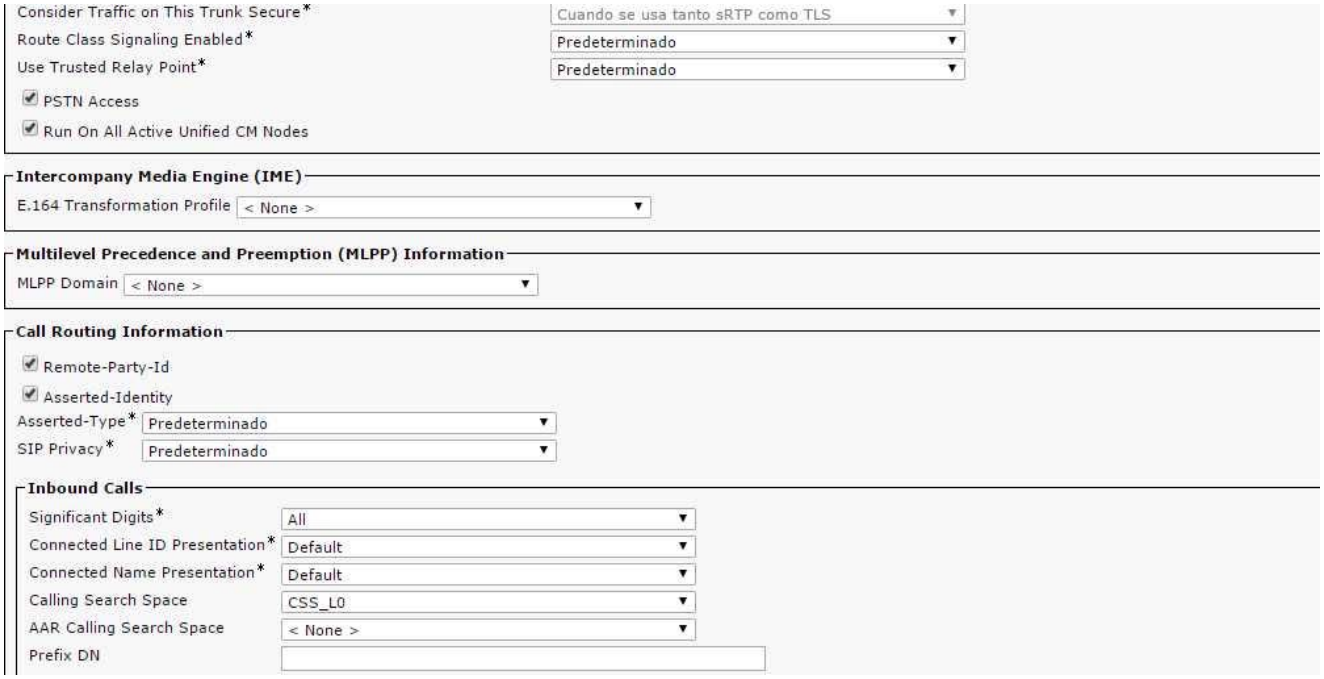


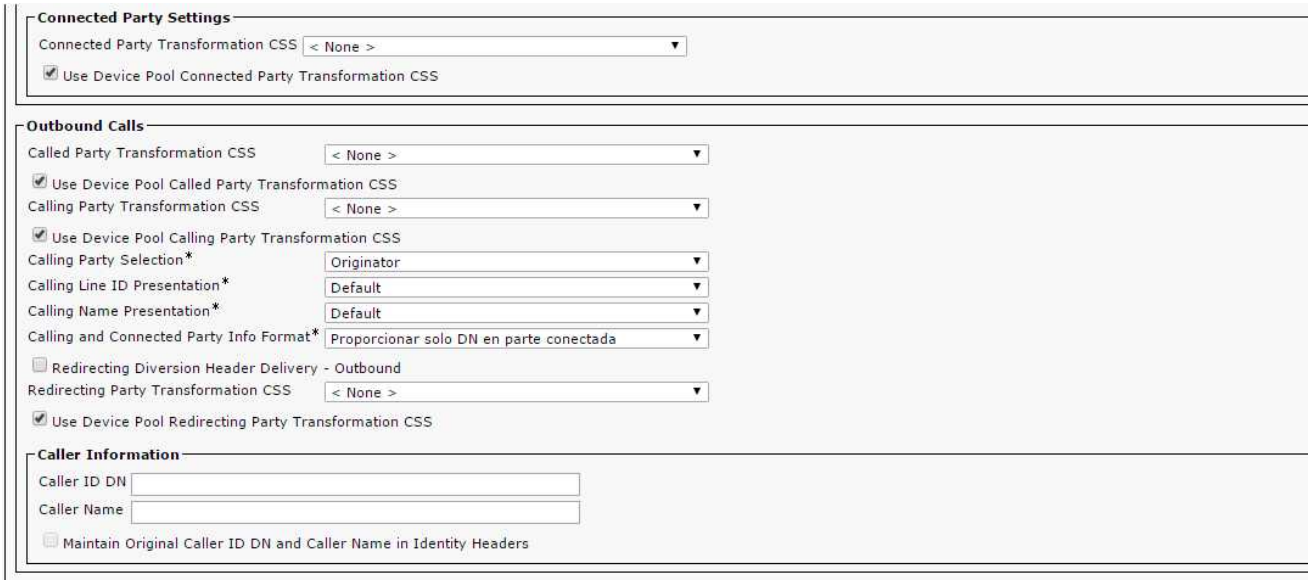
Que está formado por un Route Group donde se define la conexión mediante un SIP Trunk con el SBC de la RCJA:

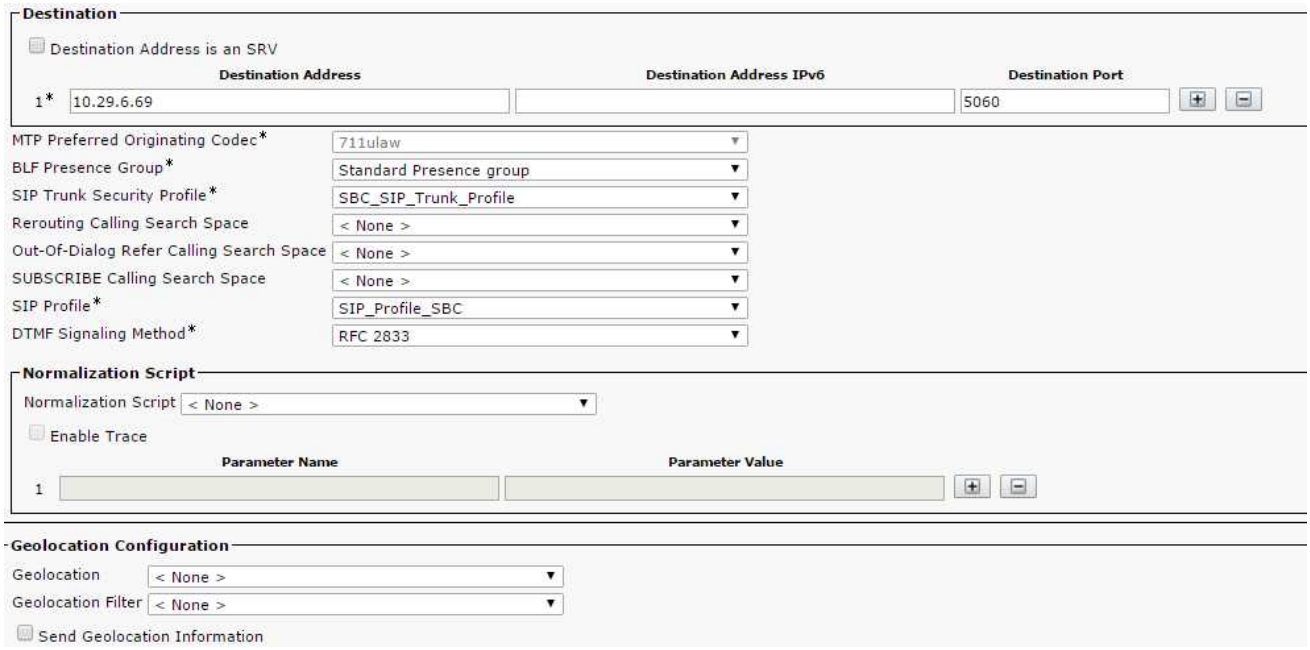


Dicho SIP Trunk está configurado como se detalla a continuación:




Consider Traffic on This Trunk Secure*
Cuando se usa tanto sRTP como TLS
Route Class Signaling Enabled*
Predeterminado
Use Trusted Relay Point*
Predeterminado
PSTN Access
Run On All Active Unified CM Nodes
Intercompany Media Engine (IME)
E.164 Transformation Profile
< None >
Multilevel Precedence and Preemption (MLPP) Information
MLPP Domain
< None >
Call Routing Information
Remote-Party-Id
Asserted-Identity
Asserted-Type*
Predeterminado
SIP Privacy*
Predeterminado
Inbound Calls
Significant Digits*
All
Connected Line ID Presentation*
Default
Connected Name Presentation*
Default
Calling Search Space
CSS_L0
AAR Calling Search Space
< None >
Prefix DN

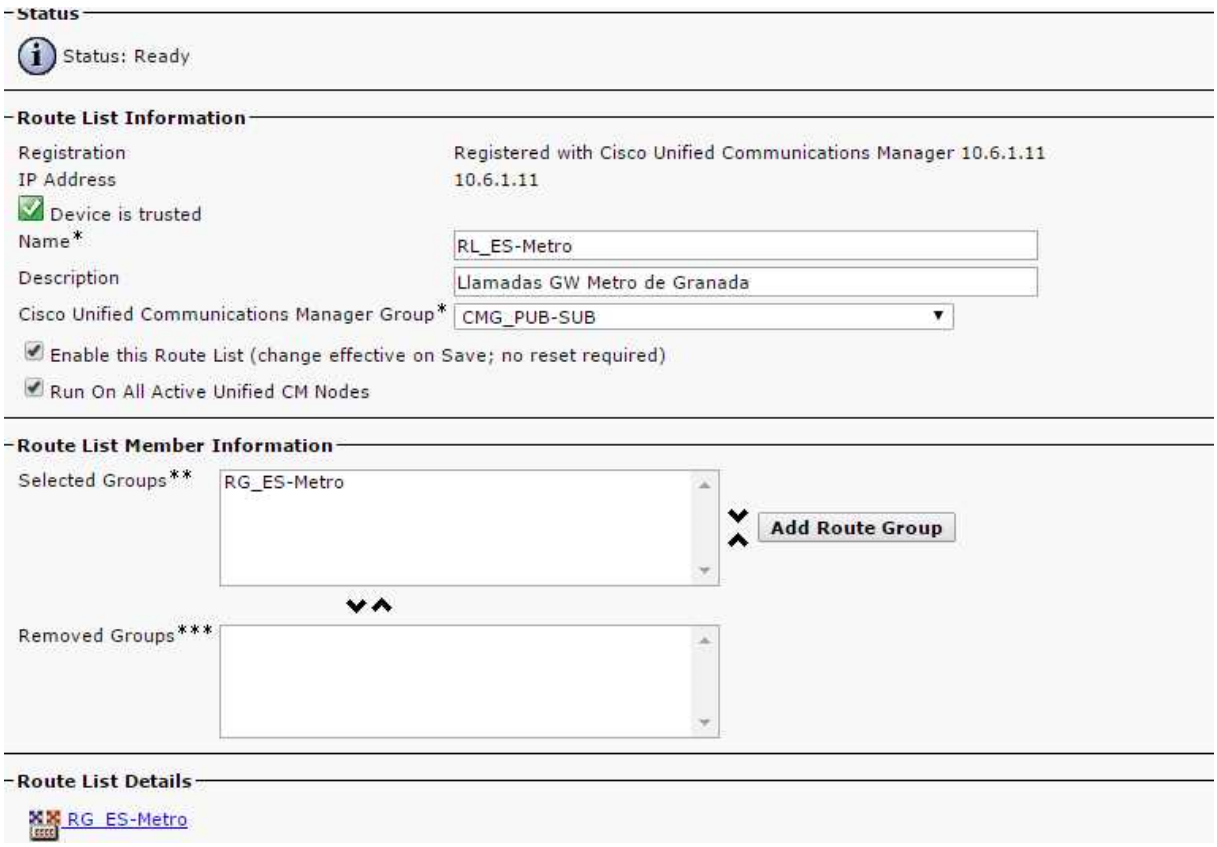

Connected Party Settings
Connected Party Transformation CSS
< None >
Use Device Pool Connected Party Transformation CSS
Outbound Calls
Called Party Transformation CSS
< None >
Use Device Pool Called Party Transformation CSS
Calling Party Transformation CSS
< None >
Use Device Pool Calling Party Transformation CSS
Calling Party Selection*
Originator
Calling Line ID Presentation*
Default
Calling Name Presentation*
Default
Calling and Connected Party Info Format*
Proporcionar solo DN en parte conectada
Redirecting Diversion Header Delivery - Outbound
Redirecting Party Transformation CSS
< None >
Use Device Pool Redirecting Party Transformation CSS
Caller Information
Caller ID DN
Caller Name
Maintain Original Caller ID DN and Caller Name in Identity Headers



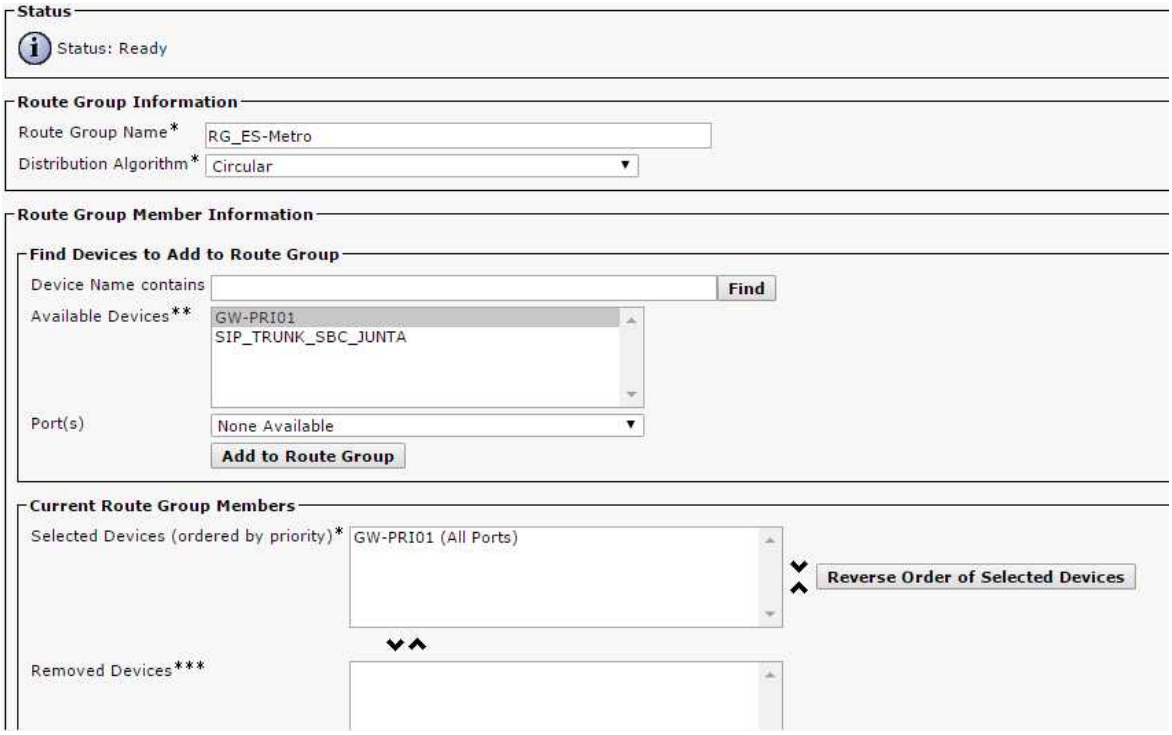
El direccionamiento asignado al CUCM y Gateway para establecer la comunicación con la infraestructura de la RCJA es el siguiente:

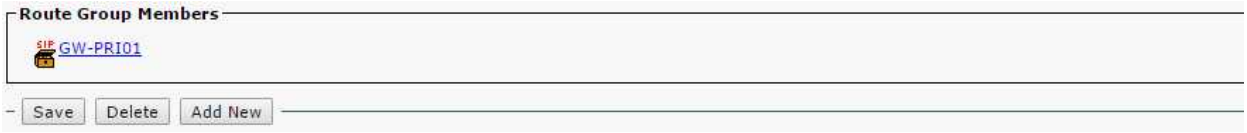
- CCM_PUB01 (Publisher): 10.92.86.11
- CCM_SUB01 (Subscriber): 10.92.86.12
- GW_PRI01 (Gateway primario): 10.92.86.20
- SBC:10.29.6.69:5060

Las llamadas hacia el PSTN/GSM se enrutan hacia el primario de Metro de Granada:



Donde se define el Route Group que está definido por el Gateway de voz donde está conectado el primario de telefonía:





Las llamadas externas entrantes hacia la numeración de Metro se cursarán a través del primario conectado al Gateway de voz.

Actualmente se dispone de la siguiente numeración:

- 958145990 (número de cabecera del primario)
- 958145991
- 958145992
- 958145993
- 958145994
- 958145995

El Gateway de voz y el Call Manager se han configurado para que todas las llamadas entrantes al número 958145990 se reciban en la extensión 170830 (extensión reservada para el teléfono de la Recepción de Metro). Igualmente, las llamadas entrantes al número 958145995 se recibirán en la extensión 170861 (extensión reservada para el teléfono de la Recepción de la AOPJA) y las llamadas entrantes al número 958145994 se recibirán en la extensión 3004 (extensión reservada para elgrupo de salto de Secretaría del Operador Avanza).

Respecto a las llamadas al exterior, siempre por el primario de Metro, las que salgan desde un teléfono de la AOPJA (170850-170863) lo harán mostrando el número 958145995, las que salgan desde un teléfono de Avanza (3450-3468, 3406, 3407) lo harán mostrando el número 958145994 y las salientes desde el resto de extensiones de Metro lo harán mostrando el número 958145990.

Por último, las extensiones de Metro integradas en la RCJA citadas anteriormente (170830- 170864) podrán recibir llamadas externas directamente mediante el número público asignado por la RCJA (958575830-958575864). Dichas llamadas serán cursadas a través del SIP Trunk establecido entre el SBC y el CM, no entrando por el primario de Metro.

10.4. Permiso de llamadas (CSS – Calling Search Space)

En los CSS agrupamos una serie de particiones a las cuales tendrá acceso el dispositivo al que se le aplique el CSS. A continuación se detallan los CSS configurados en el proyecto de Metro Ligero de Granada:

CSS Name	Description
CSS_L0	Llamadas a extensiones coporativas + 112
CSS_L1	Llamadas a L0 + fijos + cortos + mov
CSS_L2	Llamadas a L1 + especiales
CSS_L3	Llamadas a L2 + internacionales
CSS_interfono	Llamadas a centralita

Se han considerado 4 niveles de permisos para cada sede. Conforme se aumenta el nivel del CSS aumentan los permisos para realizar llamadas a números públicos, teniendo el mismo comportamiento en cualquiera de las sedes.

La asignación de permisos de llamada a usuarios se muestra en el archivo adjunto “MLGR_Datos para configuracion CM”.

10.5. Grupos de Salto

Los grupos de salto nos permiten definir un grupo de extensiones que responderán ante un solo número piloto común (Hunt Pilot), siguiendo un algoritmo de distribución definido. Los distintos algoritmos que podemos seleccionar son los siguientes:

1. **Top Down** (secuencial empezando siempre por el primero y siguiendo el orden de la definición del grupo)
2. **Circular** (empieza por la extensión siguiente a la última que atendió una llamada y sigue en el orden de la definición del grupo, pasando de la última a la primera en caso de alcanzar el final del grupo)
3. **Longest Idle Time** (la primera línea seleccionada será la que lleve más tiempo sin atender una llamada)
4. **Broadcast** (se seleccionan todas de manera simultánea). Además, es necesario definir dos timers, uno que indica el tiempo total del grupo de salto (Maximum Hunt Timer, por defecto 1800 segundos), y otro que indica la duración de la llamada en cada extensión (RNA Reversion Timeout).

El valor de los temporizadores está relacionado con el algoritmo usado y el número de líneas del grupo. Habrá que tener en cuenta que los grupos de salto son usados principalmente en la recepción de llamadas externas, por lo que habrá que mantenerla un tiempo relativamente largo antes de rechazarla, ya que en caso contrario se corre el riesgo de perder la llamada porque no da tiempo a coger el teléfono. Si se tiene en cuenta que un tono dura aproximadamente unos 4 segundos, se recomienda permitir la llamada, en general, del orden de 1 minuto si no se le da ningún mensaje de espera, y más tiempo si se le pone un mensaje en espera.

Se han configurado 5 grupos de salto:

- Grupo de salto **PCC**. Extensión del grupo: 3000. Formado por las extensiones 170831, 170832, 170833. La llamada suena en los 3 puestos de operador a la vez. Si pasan 16 segundos (4 tonos) y no es atendida, salta al Agente Comercial (170834), suena 4 tonos y termina.
- Grupo de salto **Destino Interfonos Murales**. Extensión del grupo: 3001. Formado por los teléfonos que recibirán las llamadas de todos los interfonos murales. La llamada suena en los puestos de Att. Cliente (actualmente la extensión 3161) a la vez. Si pasan 16 segundos (4 tonos) y no es atendida, salta al grupo 3000.
- Grupo de salto **Destino Interfonos DAT**. Extensión del grupo: 3002. Formado por los teléfonos que recibirán las llamadas de todos los interfonos de las máquinas DAT. La llamada suena en los puestos de Att. Cliente (actualmente la extensión 3161) a la vez. Si pasan 16 segundos (4 tonos) y no es atendida, salta al grupo 3000.
- Grupo de salto **Destino Interfonos Ascensores**. Extensión del grupo: 3003. Formado por los teléfonos que recibirán las llamadas de todos los interfonos de los ascensores. La llamada suena en los 3 puestos de operador a la vez. Si pasan 16 segundos (4 tonos) y no es atendida, salta al Agente Comercial (170834), suena 4 tonos y termina.
- Grupo de salto **Secretaría Operador**. Extensión del grupo: 3004. La llamada suena en el 3450 y tras 4 tonos pasa a sonar a la vez en los números 3451, 3465 y 3466 (broadcast). Tras 4 tonos vuelve al 3450, suena 4 tonos y termina.

10.6. Grupos de captura

Los grupos de captura permiten rescatar una llamada que está sonando en otra extensión que pertenece al mismo grupo. Habitualmente se configuran por grupos de trabajos comunes o ubicados físicamente en la misma estancia. Una vez definidos, en la configuración de las extensiones podremos indicar el grupo de captura al que pertenece.

Grupo de captura	Descripción	Identificador	Extensiones
GC001	Grupo de Captura 001	1	170831, 170832, 170833, 170834
GC002	Grupo de Captura 002	2	170850, 170851, 170852, 170853, 170854, 170855, 170856, 170857, 170858, 170859, 170860, 170861, 170862, 170863
GC003	Grupo de Captura 003	3	3450, 3464, 3465

10.7. Desvíos

Se pueden configurar desvíos por tiempo, o si el destinatario está ocupado, la llamada salta a otro terminal. Además, se pueden definir cuáles son los destinatarios válidos a la hora de activar el desvío, por ejemplo, solo extensiones internas) mediante los Calling Search Space.
Los desvíos que podrían activarse:

- Desvío incondicional
- Desvío si no contesta
- Desvío si el destinatario está ocupado

Además, se asigna un permiso a cada tipo de desvío con un CSS. Este aspecto es importante ya que existe un tipo de fraude que consiste en realizar desvíos hacia números personales. Por ejemplo, si un trabajador se va de vacaciones puede desviar su número del trabajo a un número extranjero o a su propio móvil, y decir a sus familiares que para localizarle le llamen al número del trabajo, de manera que la empresa pagará todas esas llamadas personales.

Para todas las extensiones, el permiso de desvío asignado es el L0, de forma que únicamente se pueden realizar desvíos a otras extensiones.

10.8. DHCP

Aunque todos los teléfonos se han configurado con IP estática, por si fuese necesario en el futuro se ha dejado configurado en el servidor multipropósito el servicio Dynamic Host Configuration Protocol (DHCP) para las VLAN correspondientes a las redes de telefonía (272, 273, 274, 275 y 276). Para ello, se ha configurado un servidor DHCP sobre el servidor Linux localizado en la VRF de Gestión en la IP 10.4.1.20.
Para que las direcciones IP se puedan servir, ya que el servidor de DHCP está en la VRF de gestión y las VLAN de telefonía están en la VRF de Telefonía, se ha incluido un helper-address en los interfaces VLAN de telefonía del 4500, que redirige las peticiones de DHCP hacia el servidor a través del firewall, que es el elemento encargado de enrutar entre VRFs.

```
interface Vlan274
 description TELEF_PCC
 ip vrf forwarding VRF_TELEF
 ip address 10.6.2.2 255.255.255.0
 ip helper-address 10.4.1.20
 standby delay minimum 30 reload 60
 standby version 2
 standby 274 ip 10.6.2.1
 standby 274 priority 120
 standby 274 preempt
 standby 274 authentication md5 key-string 7 08701C005F57575943
 standby 274 name TELEF_PCC
 standby 274 track 1 decrement 20
end
```

Si a un teléfono se le configura el direccionamiento por DHCP, el servidor DHCP servirá a dicho teléfono una IP del rango correspondiente configurado, así como la dirección del servidor TFTP del que deberá descargar el firmware necesario, extensión etc; Este servidor TFTP no es más que el Publisher del Call Manager, localizado en la IP 10.6.1.11.

10.9. Servidor de grabación: CrossRecorder

La aplicación se encuentra virtualizada en dos servidores UCS usando la plataforma vMware.
El direccionamiento de cada host es el siguiente:

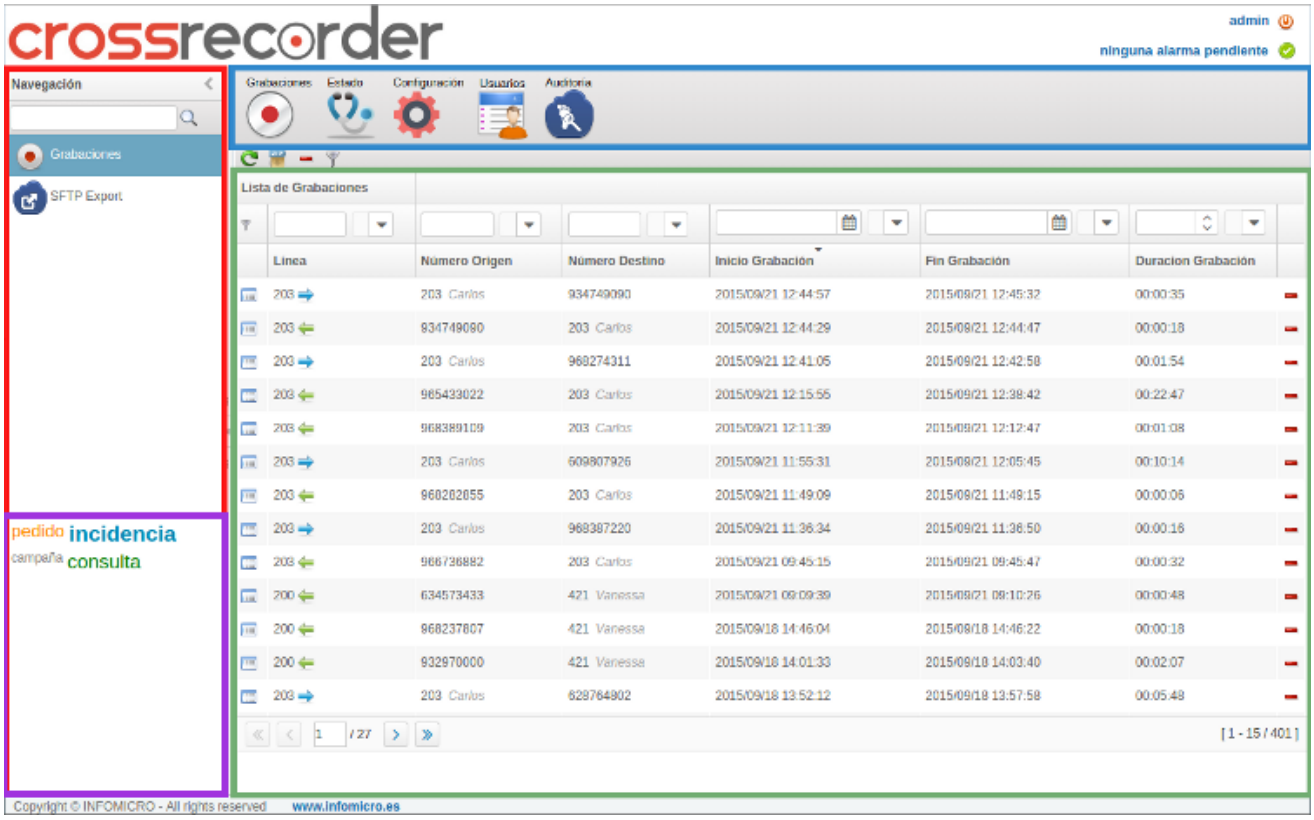
Host ESXi servidor1: 10.6.1.32
CIMC servidor1: 10.6.1.34

Host ESXi servidor2: 10.6.1.33
CIMC servidor1: 10.6.1.35

En cada uno de los nodos se ha implementado una máquina virtual en la que se ha instalado la aplicación CrossRecorder. Dicha aplicación se ha desplegado en alta disponibilidad, de modo que si uno de los nodos cae la aplicación seguirá funcionando correctamente.

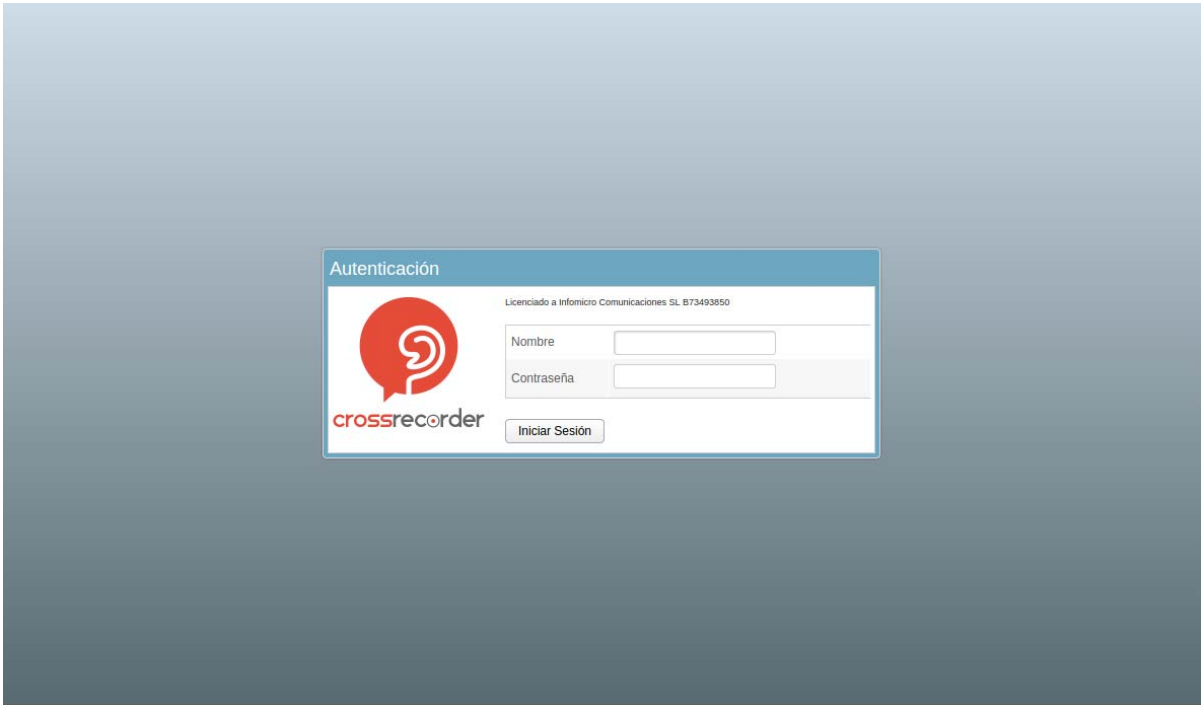
Nodo1 CrossRecorder: 10.6.1.36
Nodo2 CrossRecorder: 10.6.1.37
IP Virtual CrossRecorder (HA): 10.6.1.31

El sistema se basa en una interfaz puramente Web, donde encontramos una barra superior de opciones y otra en el lateral izquierdo, en la zona aparece la zona de visualización y acciones.



En la ilustración podemos ver apreciar la distribución de las zonas, identificado en azul el menú principal de opciones, en rojo el menú secundario de opciones, en lila la sección dedicada a la "nube de tags" y en verde la zona de visualización y de acción.

El acceso al sistema se realiza a través del navegador Mozilla mediante una petición HTTP a la URL específica del sistema en el IMI, que es: https://10.6.1.31/RecordBrowser



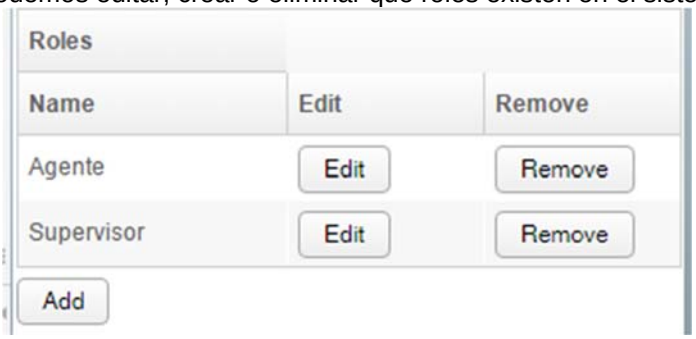
Este enlace nos lleva a la pantalla de *login* inicial, donde se nos pedirán las credenciales de usuario, nombre de usuario y contraseña.

En la pantalla de acceso aparecen los detalles de licencia del producto, identificando claramente el CIF del usuario final, así como su denominación comercial.

- **Gestión de usuarios**

Para la gestión y visualización de las grabaciones se ha diseñado un esquema de usuario/roles, donde se definen una serie de permisos a nivel general y se aplican a nivel funcional de usuario.

Roles: En apartado podemos editar, crear o eliminar qué roles existen en el sistema.

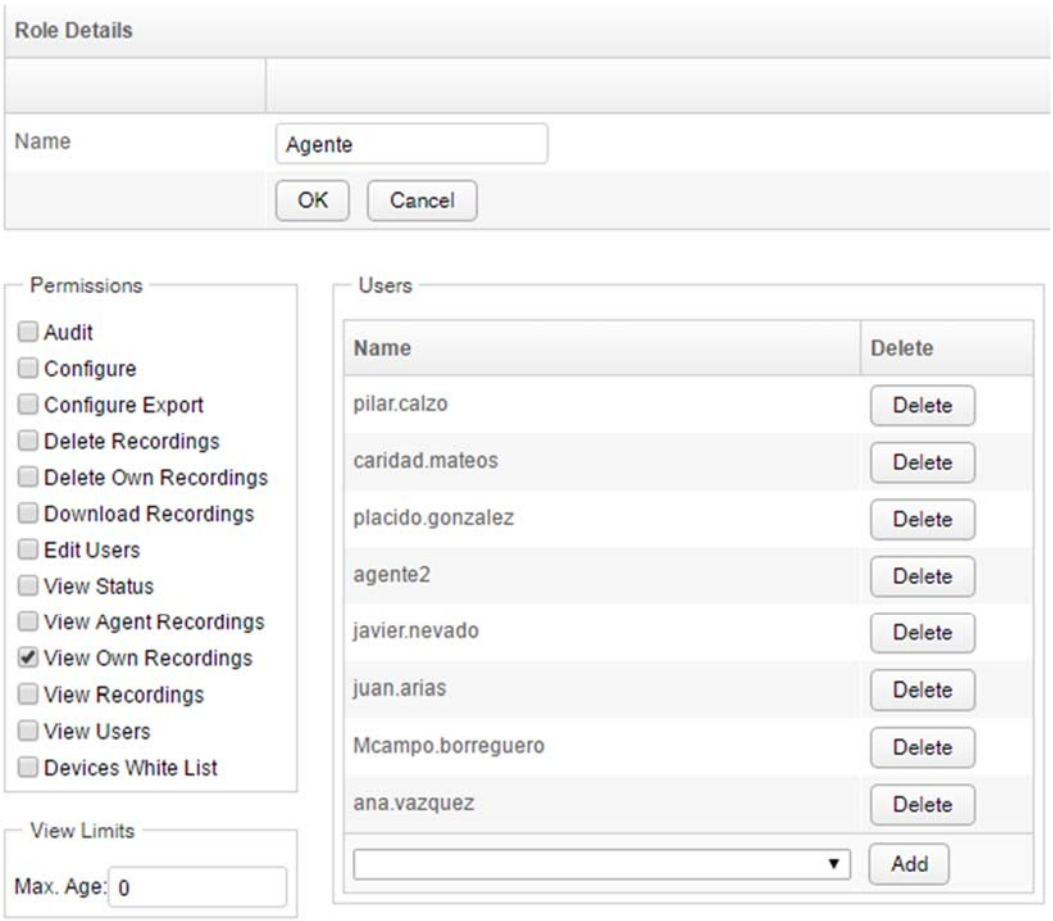


En la página de edición de roles podemos seleccionar de qué permisos dispondrán aquellos usuarios que tengan asociado dicho rol.

En concreto se pueden seleccionar los siguientes:

Rol	Descripción
Borrar grabaciones	Permite al usuario borrar todas las grabaciones del sistema.
Borrar grabaciones propias	Permite al usuario borrar sus grabaciones, es decir, aquellas que están asociadas a líneas pertenecientes al usuario.
Ver grabaciones	Permite al usuario ver todas las grabaciones del sistema.
Ver grabaciones propias	Permite al usuario ver sus grabaciones, es decir, aquellas que están asociadas a líneas pertenecientes al usuario, o a sus variables UCCX.
Ver reglas	Permite al usuario ver las reglas de grabación que se aplican sobre las líneas.
Editar reglas	Permite al usuario editar las reglas de grabación que se aplican sobre las líneas.
Ver usuarios	Permite al usuario ver los usuarios del sistema.
Editar usuarios	Permite al usuario editar los usuarios del sistema.
Configurar	Permite al usuario que ha realizado el login acceder a la parte perteneciente a configuración del sistema.
Ver estado	Permite al usuario que ha realizado el login acceder a la parte perteneciente a estado del sistema.

Además, se establece en el parámetro `Máxima Antigüedad` de `Limites Consulta` cuanto días de grabaciones desde la fecha actual es capaz de visualizar el usuario. Si este valor se deja a 0 indica que no hay límite de antigüedad.
Además, desde aquí es posible asociar usuarios al rol. Para ello debe seleccionar el usuario en el desplegable de `Usuarios` y asignar el rol que deseamos otorgarle al mismo, tras lo que pulsaremos el botón de `Añadir`.

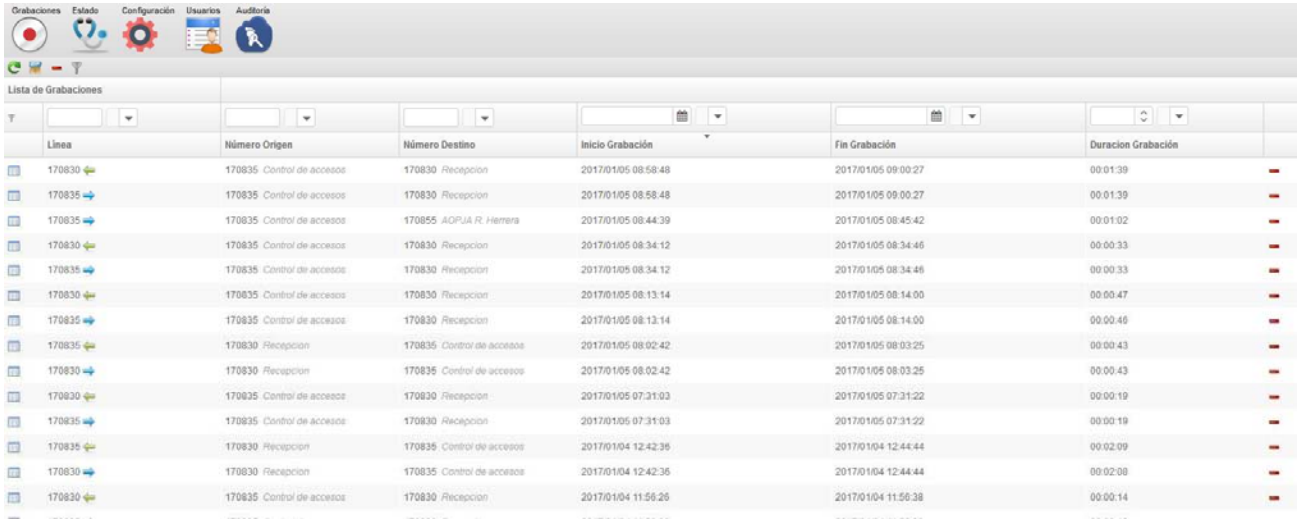


- **Grabaciones**

La pantalla donde se muestran las grabaciones se comporta como una aplicación de escritorio, permitiendo la multi-selección así como la selección vía doble click.

En la parte superior izquierda disponemos de tres iconos que nos permiten realizar las acciones de refrescar el listado de grabaciones, comprimir en zip y descargar las grabaciones seleccionadas y eliminar las grabaciones seleccionadas.

Para tener multi-selección podemos utilizar tanto la tecla de *Ctrl*, selección individual, como la de *Shift* para una selección seguida.



La última de las columnas, que es un signo de rojo horizontal, que puede identificarse con un signo de resta, sirve para eliminar únicamente la grabación que tiene implicada en su fila.
En la parte inferior izquierda podemos encontrar la paginación de las grabaciones, que nos permite ir navegando entre las distintas grabaciones, ya sea con filtro aplicado o sin filtro.

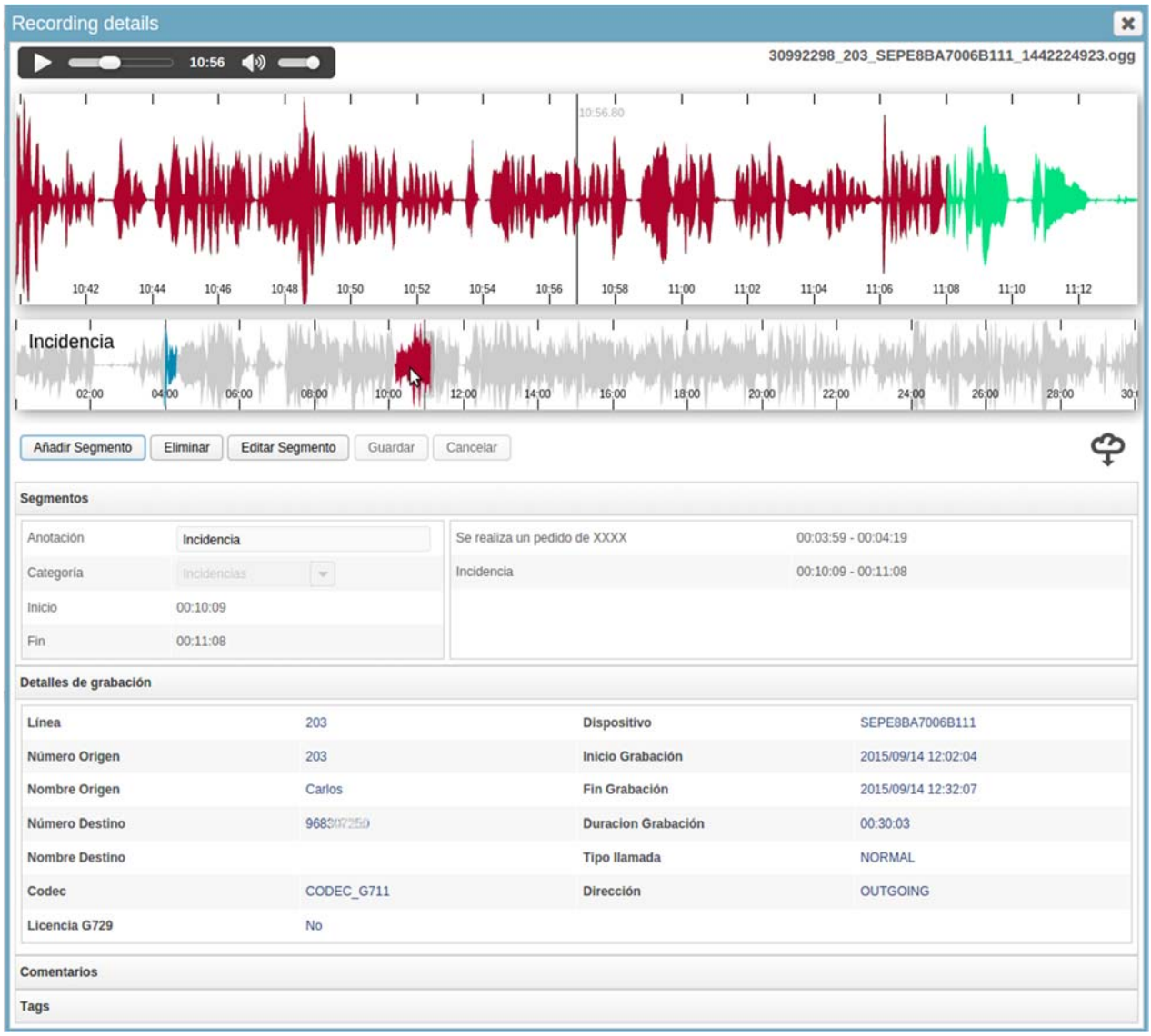
10.9.1. Filtros

Los filtros de búsqueda se aplican a las grabaciones, y permiten visualizar únicamente aquellas cuyos datos coinciden con los filtros aplicados sobre los campos deseados.
Los filtros pueden ser únicos por columna o conjuntarse con un filtro de otra columna, siendo los operadores que se pueden utilizar los siguientes:

- Igual
- Menor
- Menor o igual
- Mayor
- Mayor o igual
- Distinto
- Entre

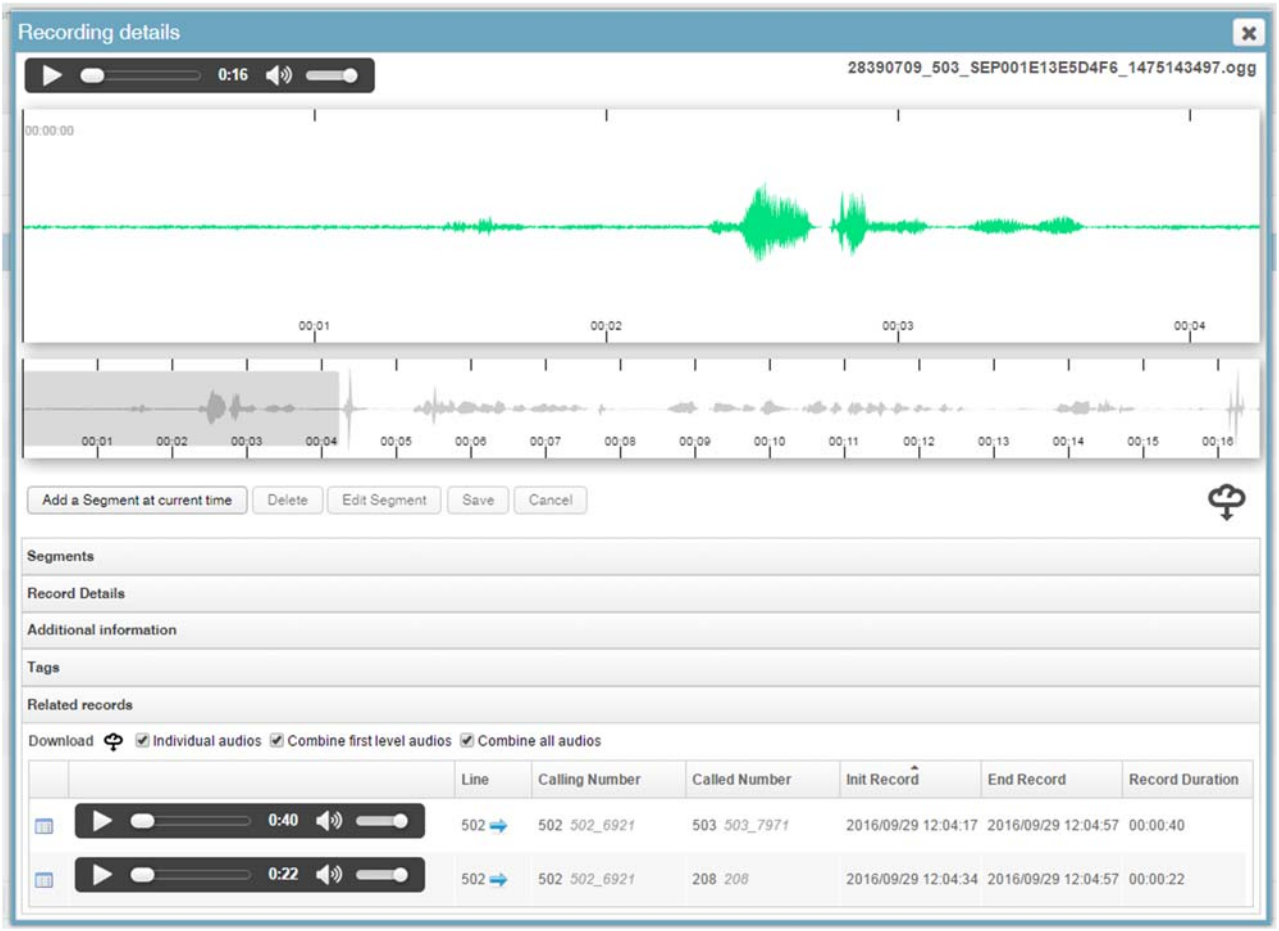
10.9.2. Detalles en grabaciones

Cuando hacemos un doble click sobre la grabación, o pulsamos para que nos muestre los detalles obtenemos una ventana emergente que nos permite, además de escuchar la grabación, descargar la misma y ver todos los datos obtenidos por el sistema, incluyendo los datos recibidos por el Contact Center, si los hubiese.



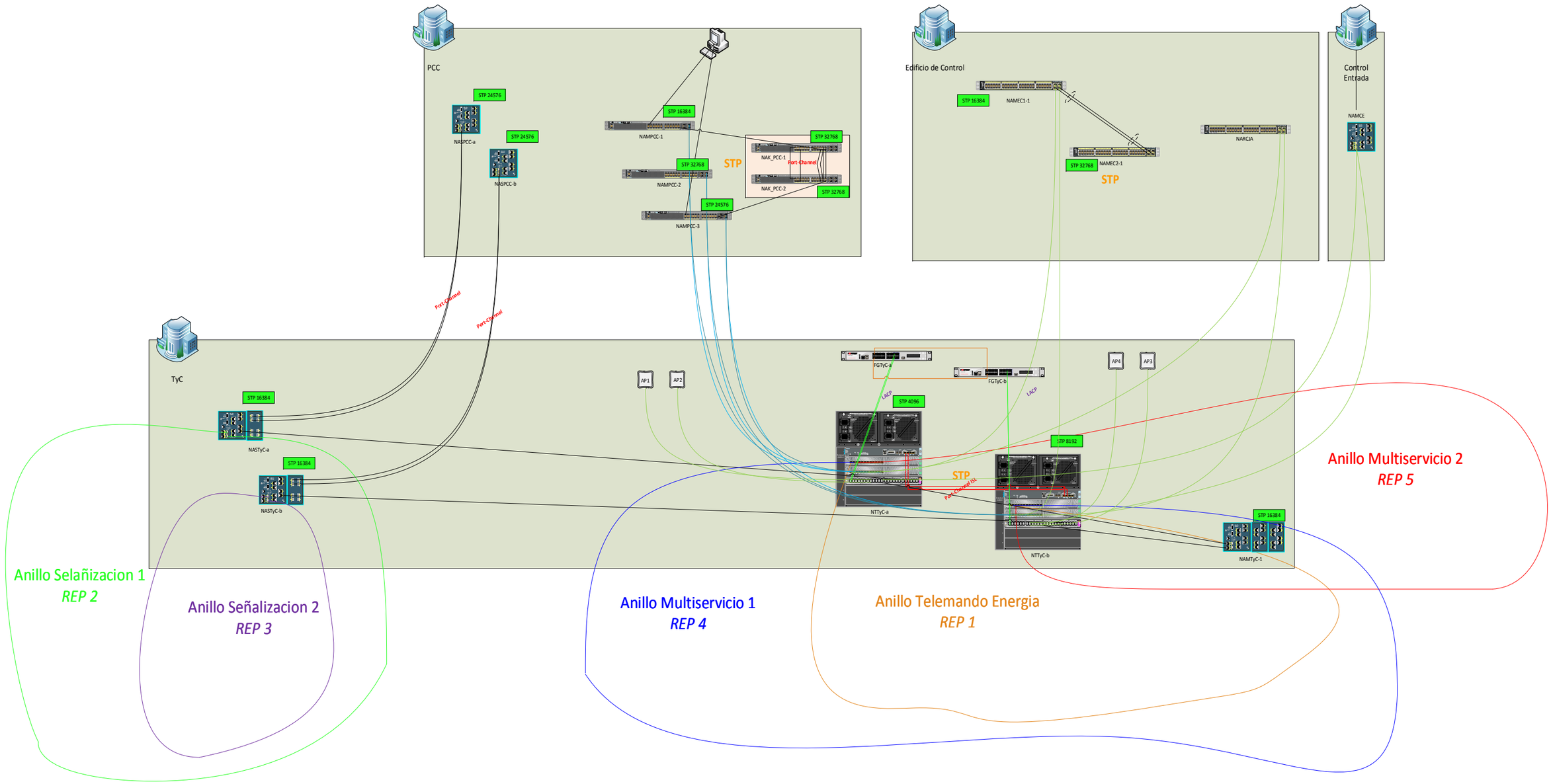
Podemos observar que el sistema dibuja un audiograma de la grabación en dos niveles. El primero está ampliado y muestra una sección acotada y el segundo muestra la totalidad de la grabación. Podemos hacer click en cualquiera de los dos niveles y reproducir a partir de dicho punto.

Por último, para cada grabación podremos ver sus grabaciones relacionadas. Si, por ejemplo, durante una llamada ha habido transferencias entre líneas, en el sistema se crearán varias grabaciones, pero todas ellas estarán relacionadas, pues formarán parte de la misma conversación.

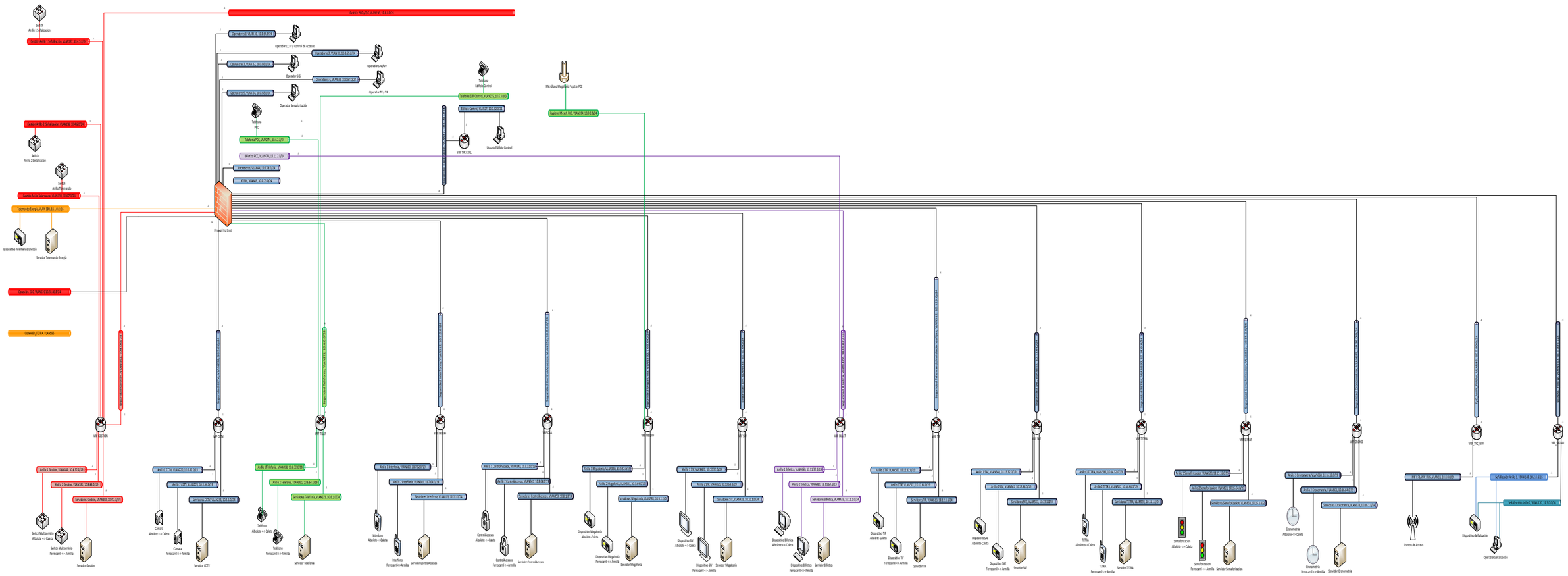


Tal y como se aprecia en la imagen, al ver los detalles de una grabación podremos ver sus grabaciones relacionadas, así como descargar un ZIP con todas ellas, e incluso un fichero único con el audio montado de manera que se reconstruya la totalidad de la llamada original utilizando estos fragmentos. Podremos escuchar las llamadas relacionadas con un pequeño reproductor embebido, así como navegar entre ellas.

11. Topología física


PCC
STP 24576
NASPCC-a
STP 24576
NASPCC-b
STP 16384
NAMPCC-1
STP 32768
NAMPCC-2
STP 24576
NAMPCC-3
STP 32768
NAK_PCC-1
Port-Channel
NAK_PCC-2
STP 32768
STP
Edificio de Control
STP 16384
NAMEC1-1
NARCJA
STP 32768
NAMEC2-1
STP
Control
Entrada
NAMCE
Port-Channel
Port-Channel
TyC
STP 16384
NASTyC-a
STP 16384
NASTyC-b
AP1
AP2
FGTyC-a
FGTyC-b
LACP
LACP
STP 4096
NTTyC-a
STP 8192
NTTyC-b
STP
Port-Channel
AP4
AP3
STP 16384
NAMTyC-1
Anillo Multiservicio 2
REP 5
Anillo Selañizacion 1
REP 2
Anillo Señalizacion 2
REP 3
Anillo Multiservicio 1
REP 4
Anillo Telemando Energia
REP 1

12. Topología lógica


Switch Anillo 1 Señalizacion
Switch Anillo 2 Señalizacion
Switch Anillo Telemando
Telemando Energia, VLAN 130, 10.1.0.0/24
Dispositivo Telemando Energia
Servidor Telemando Energia
Conexión_SIRC, VLAN 2179, 10.0.91.0/24
Conexión_SETRA , VLAN 695
Gestion PCC y TDC, VLAN 196, 10.4.0.0/24
Operadores 1, VLAN 50, 10.0.50.0/24
Operador CCTV y Control de Accesos
Operadores 2, VLAN 51, 10.0.51.0/24
Operadores 3, VLAN 52, 10.0.66.0/24
Operador SAE
Operadores 4, VLAN 53, 10.0.53.0/24
Operador SAE/SAV
Operadores 5, VLAN 54, 10.0.68.0/24
Operador Semaforizacion
Operador TF y TIP
Telefono Edificio Control
Telefono
PCC
Telefonia Edificio Control, VLAN 575, 10.4.3.0/24
Telefonia PCC, VLAN 574, 10.4.2.0/24
Radio y Cuarto, VLAN 577, 10.0.152.0/21
Usuario Edificio Control
VHF TVC ESPIL
Microfono Megafonia Puyetec PCC
Puyetec Micro PCC, VLAN 694, 10.0.2.0/24
Telefonia PCC, VLAN 574, 10.4.2.0/24
Biometrico PCC, VLAN 696, 10.12.2.0/24
Ingresscio, VLAN 64, 10.1.78.0/24
ATOS, VLAN 65, 10.0.70.0/24
Firewall Fortinet
VRF ESTACION
VRF CCTV
VRF TORNO
VRF TELEFONIA
VRF MEGAFONIA
VRF CONTROLACCESOS
VRF SAE
VRF TIP
VRF SAV
VRF TETRA
VRF SEMAFORIZACION
VRF CRONOMETRIA
VRF TVC_WIFI
VRF_RADIAL
Switch Multiservicio Albolote <> Caleta
Switch Multiservicio Ferrocarril <> Arenilla
Servidor Gestion
Anillo 1 CCTV, VLAN 210, 10.5.0.0/19
Anillo 2 CCTV, VLAN 211, 10.5.64.0/19
Servidores CCTV, VLAN 220, 10.5.0.0/24
Camara Albolote <> Caleta
Camara Ferrocarril <> Arenilla
Servidor CCTV
Anillo 1 Telefonia, VLAN 592, 10.4.32.0/19
Anillo 2 Telefonia, VLAN 593, 10.4.64.0/19
Servidores Telefonia, VLAN 573, 10.0.1.0/24
Telefono Albolote <> Caleta
Telefono Ferrocarril <> Arenilla
Servidor Telefonia
Anillo 1 Interfonia, VLAN 581, 10.7.0.0/19
Anillo 2 Interfonia, VLAN 582, 10.7.64.0/19
Servidores Interfonia, VLAN 572, 10.0.2.0/24
Interfono Albolote <> Caleta
Interfono Ferrocarril <> Arenilla
Servidor Controlaccesos
Anillo 1 ControlAccesos, VLAN 581, 10.8.0.0/19
Anillo 2 ControlAccesos, VLAN 582, 10.8.64.0/19
Servidores ControlAccesos, VLAN 571, 10.0.3.0/24
ControlAccesos Albolote <> Caleta
ControlAccesos Ferrocarril <> Arenilla
Servidor ControlAccesos
Anillo 1 Megafonia, VLAN 601, 10.9.0.0/19
Anillo 2 Megafonia, VLAN 602, 10.9.64.0/19
Servidores Megafonia, VLAN 570, 10.0.4.0/24
Dispositivo Megafonia Albolote-Caleta
Dispositivo Megafonia Ferrocarril <> Arenilla
Servidor Megafonia
Anillo 1 DIV, VLAN 621, 10.10.0.0/19
Anillo 2 DIV, VLAN 622, 10.10.64.0/19
Servidores DIV, VLAN 569, 10.0.5.0/24
Dispositivo DIV Albolote <> Caleta
Dispositivo DIV Ferrocarril <> Arenilla
Servidor Megafonia
Anillo 1 Biblioteca, VLAN 641, 10.11.0.0/19
Anillo 2 Biblioteca, VLAN 642, 10.11.64.0/19
Servidores Biblioteca, VLAN 675, 10.11.3.0/24
Dispositivo Biblioteca Albolote <> Caleta
Dispositivo Biblioteca Ferrocarril <> Arenilla
Servidor Biblioteca
Anillo 1 TIP, VLAN 585, 10.17.0.0/19
Anillo 2 TIP, VLAN 586, 10.17.64.0/19
Servidores TIP, VLAN 565, 10.17.3.0/24
Dispositivo TIP Albolote-Caleta
Dispositivo TIP Ferrocarril <> Arenilla
Servidor TIP
Anillo 1 SAE, VLAN 645, 10.13.0.0/19
Anillo 2 SAE, VLAN 646, 10.13.64.0/19
Servidores SAE, VLAN 659, 10.13.1.0/24
Dispositivo SAE Albolote-Caleta
Dispositivo SAE Ferrocarril <> Arenilla
Servidor SAE
Anillo 1 TETRA, VLAN 590, 10.19.0.0/19
Anillo 2 TETRA, VLAN 591, 10.19.64.0/19
Servidores TETRA, VLAN 595, 10.19.1.0/24
TETRA Albolote <> Caleta
TETRA Ferrocarril <> Arenilla
Servidor TETRA
Anillo 1 Semaforizacion, VLAN 627, 10.15.0.0/19
Anillo 2 Semaforizacion, VLAN 628, 10.15.64.0/19
Servidores Semaforizacion, VLAN 655, 10.15.2.0/24
Semaforizacion Albolote <> Caleta
Semaforizacion Ferrocarril <> Arenilla
Servidor Semaforizacion
Anillo 1 Cronometria, VLAN 660, 10.18.0.0/19
Anillo 2 Cronometria, VLAN 661, 10.18.64.0/19
Servidores Cronometria, VLAN 671, 10.18.3.0/24
Cronometria Albolote <> Caleta
Cronometria Ferrocarril <> Arenilla
Servidor Cronometria
NAT TUNEL VHF, VLAN 57, 10.0.0.0/24
Puntos de Acceso
Señalizacion Anillo 1, VLAN 240, 10.0.0.0/19
Señalizacion Anillo 2, VLAN 241, 10.0.32.0/19
Dispositivo Señalizacion
Operador Señalizacion