ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD POLITÉCNICA DE CARTAGENA

**Trabajo Final de Grado.**

# ARQUITECTURA DE RED TELEMÁTICA PARA LA GESTIÓN DE TRES PUERTOS Y TERMINAL MARITIMA

AUTOR: Jose Afelio Salmerón Saura
DIRECTOR: Alejandro Santos Martínez Sala

Enero / 2016



| | |
|---|---|
| **Autor** | José Afelio Salmerón Saura |
| **E-mail del autor** | jasalmerons@gmail.com |
| **Director** | Alejandro Santos Martínez Sala |
| **E-mail del director** | alejandros.martinez@upct.es |



| | |
|---|---|
| **Titulo del TFG** | ARQUITECTURA DE RED TELEMÁTICA PARA LA GESTIÓN DE TRES PUERTOS Y TERMINAL MARITIMA |


**Resumen**

**1.-Planteamiento inicial del Proyecto**

Se ha preparado este documento con el objeto de dar servicio a través de Arquitectura de Red de transmisión para recepción y entrega de datos de los equipos de campo, de seguridad, proceso y comunicaciones de los frentes de atraque a un Terminal Marítimo.

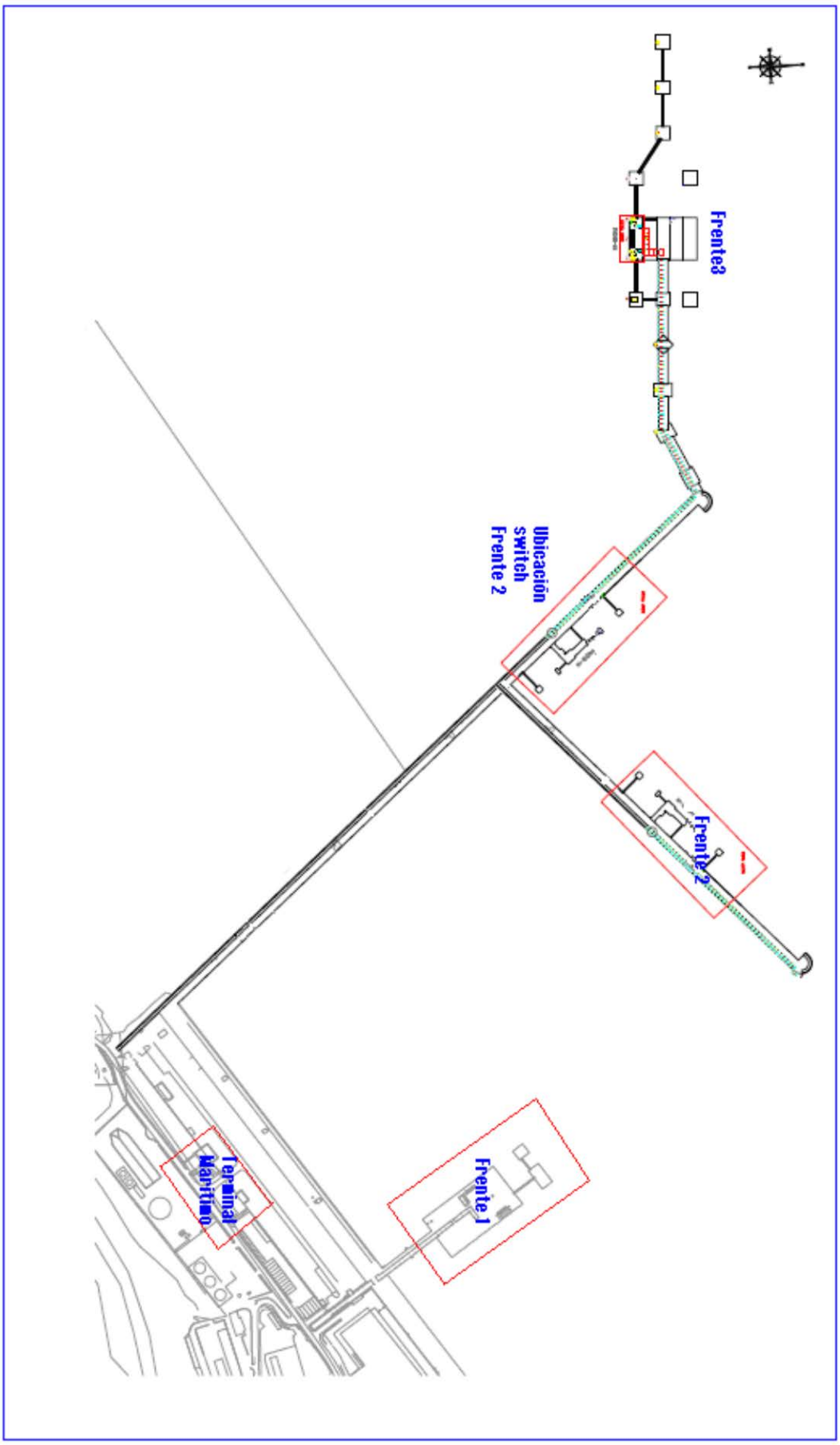
**2.- Objetivos del Proyecto**

Implantar una Red de comunicaciones segura y que permita la transmisión de datos de forma bidireccional, desde los distintos componentes de campo de los tres Frentes(Puertos) hasta los servidores y estaciones del terminal marítimo, y por otra, la selección, suministro e instalación de estos elementos de campo.
Por último, el sistema proyectado suministrará y entregará en el terminal marítimo el interface adecuado para la conexión de los equipos a Sistema de Control Distribuido con el fin de que a través de su software integre todas estas señales en su Sistema.

Auditoría y análisis de la red existente y de los requisitos funcionales y de seguridad. - Rediseño de la arquitectura de red, plan de direccionamiento IP y diseño de VLANs IEEE 802.1Q.

Diseño del cableado estructurado. - Política de seguridad y gestión de la red. - Pruebas de montaje y validación. - Documentación.


| | |
|---|---|
| **Titulación** | Grado en Ingeniería Telemática |
| **Departamento** | Tecnologías de la información y las comunicaciones |
| **Fecha de Presentación** | Enero – 2016 |


Frente3
Ubicación switch Frente 2
Frente 2
Terminal Marítimo
Frente 1

# Índice

# Figuras

# Capítulo 1: Análisis, Auditoria y Captura de requisitos de Cliente.

## 1.1 Introducción.

La Autoridad Portuaria, plantea la instalación de una red de comunicaciones para dar servicio remoto desde la Terminal Marítima, ya que actualmente se lleva el servicio localmente desde cada pantalán y algunos recursos con su propia red como el atraque laser.

Se ha preparado este documento con el objeto de dar la mejor opción para la implementación de la Red estructurada según necesidades del cliente. Con este sistema planteado, se optimiza el servicio para una red estructurada, ya que se ha optado por un sistema redundante ante fallos de dispositivos comunes y acceso a dispositivos de servicios diversos.

Se plantean 3 protocolos distintos de red desde cada pantalán hasta la Terminal Marítima, el protocolo principal desde cada Pantalán hasta la Terminal Marítima será Ethernet, pero desde cada pantalán hasta los elementos de medida y mando a nivel remoto, utilizaremos protocolos como Modbus/TCP, Red serie y Red Serie con protocolo Hart.

## 1.2 Protocolo de Comunicaciones del Terminal a los Pantalanes.

Ethernet: Sistema de detección de Incendios (Moec), Sistema de monitorización de válvulas Eléctricas(Rotork), Sistema de megafonía(Optymus), Telefonía IP y CCTV (cámaras Pelco, y Servidor de video Axis).Sistema de Aproximación y Amarre(Marimatex).

## 1.3 Protocolo de Comunicación de los Pantalanes a los Instrumentos.

Modbus/TCP: Red industrial conectada a Switch Sneider, PLC modicon cuantum.

Red Serie: Red serie que comunica la pack-scan con todas las válvulas Rotork para apertura/cierre remoto, Red serie para los equipos de campo como transmisores(presión, temperatura,caudal, etc) y detectores con protocolo de comunicación Hart.

El objeto de este proyecto es doble, por una parte implantar un canal de comunicaciones seguro y que permita la transmisión de datos de forma bidireccional, desde los distintos componentes de campo de los tres Frentes(Puertos) hasta los servidores y estaciones del Terminal Marítimo, y por otra, la selección, suministro e instalación de estos elementos campo.

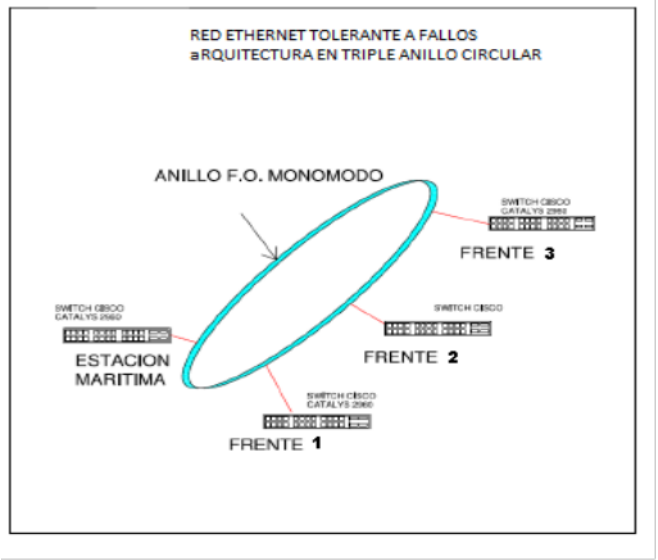



Figura-1

El sistema proyectado suministrará e instala en el Terminal Marítimo el interface adecuado para la conexión de los equipos a Sistema de Control Distribuido Scada (Honeywell) con el fin de que a través de su software integre todas estas señales en su sistema.

Uno de los objetivos del proyecto es garantizar la fiabilidad y seguridad de las comunicaciones. Quizás este sea el objetivo principal puesto que se trata de implantar la infraestructura soporte del sistema de comunicaciones y de las ampliaciones previsibles durante la vida útil de los pantalanes.

La forma física del pantalán ha sido vital para la decisión de la arquitectura e implementación final. Recordemos que el mismo es una estructura de hormigón estrecha y alargada por donde pasan los cables tanto de datos como de alimentación y en el cual el espacio tiene una gran importancia. Por ello, para reducir al mínimo los problemas de interferencias y de atenuación existentes en los cables de cobre, se decidió el empleo de fibra óptica para la transmisión de las señales hasta el terminal marítimo.

Se propone al cliente formar redes Ethernet tolerantes a fallos. La topología de Triple anillo realizada mediante cable de fibra óptica monomodo para fallos de switch o enlaces en algún pantalan. Esta red se encarga de la transmisión vía TCP/IP de las señales de megafonía, CCTV, Detección de Incendios, Sistema de Control Distribuido, de la Central PackScan, del Sistema de Control de Monitores Contra Incendios, Sistema de Aproximación Marimatex, Telefonía, Datos Ofimáticos y para cualquier otro equipo que se prevea conectar en el futuro.

La topología planteada presenta las siguientes ventajas respecto de otras basadas en cobre y con otros protocolos de comunicaciones, las soluciones las he basado en lo siguiente:

-He adoptado una solución al inconveniente de comunicaciones de carácter industrial que se basan en protocolos cerrados como pueden ser fieldbus, CAN, Hart, etc.

-La solución de comunicaciones propuesta, es la del protocolo TCP/IP sobre Ethernet, que es un estándar de comunicaciones abierto y ampliamente usado en la actualidad

-Precisamente al utilizar un estándar como Ethernet, el sistema es fácilmente expandible,

permitiendo integrar nuevos sistemas o elementos con tan solo conectarlos a un punto de red.

-La red planteada es tolerante a fallo al haber previsto la comunicación por Ethernet en Triple anillo, que de producirse la interrupción en un enlace, se habilitaría automáticamente la de otro enlace controlado por Spanning Tree Protocol (STP), garantizando la continuidad de las comunicaciones.

-El medio físico previsto para la comunicación es la fibra óptica, con lo que se eliminan las perturbaciones e interferencias creadas por campos magnéticos de cables de potencia, motores eléctricos, etc.

Tanto es así que en ciertas aplicaciones como las grúas de los terminales marítimos de contenedores, la fibra óptica va en el interior de los cables de alimentación cuya tensión es 20000 V lo que permite en este caso utilizar las mismas bandejas de los cables de baja tensión.

## 1.4 Los criterios para la elección de la tecnología.

-Funcionalidad, operatividad y facilidad de manejo de cada equipo, tanto de forma aislada, como integrado en el conjunto de medios de seguridad.

-Máximo aprovechamiento posible de los sistemas existentes en la instalación.

-Fiabilidad de los equipos, y posibilidad de integración de nuevos elementos y sistemas, sin más problemas que conectarlos a la red de fibra óptica.

-Facilidad de mantenimiento del sistema y cada uno de sus componentes.

# Capítulo 2: Diseño VLAN`s y Plan Direccionamiento Ipv4

## 2.1 Tabla membership Vlan`s de los switches.

Tabla membership de los switches

| VLAN ID membership | U (untagged) | T (tagged) |
|---|---|---|
| 1 | X | |
| 10 | | X |
| 20 | | X |
| 30 | | X |

VLAND10:

- Servidor de vídeo Axis Q7900
- PC-Camaras
- Pupitre de megafonia y Amplificadores

VLAND20:

- Servidor PackScan Rotork
- Servidor Sistema de Aprox.Amarre
- Servidor Extincion de Incendios
- Servidor Scada Honeywell

1.

VLAND30:

- Datos
  - Teléfonos IP
  - Impresoras

Se configuran los Switch de Terminal Marítimo y Pantalanes, de la forma siguiente, relacionado con su puerto.

### 2.1.1 Switch Terminal Maritima.

Definición y tablas de configuración PVID

**Tabla PVID**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PVID | 10 | 10 | 10 | 20 | 20 | 20 | 20 | 20 | 20 | 30 | 30 | 30 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

| 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|
| 1 | 1 | 1 | -- | -- |

**Tabla enlaces trunking**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trunking | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|
| NO | NO | NO | NO | NO | NO | NO | NO | SI |

SWITCH TERMINAL MARITIMO : Enlaces F.O.

| | | | |
|---|---|---|---|
| Enlace: Router-Switch Terminal Maritimo | Port 24 | Trunk | F.O. |

### 2.1.2 Switch Troncal.

**Tabla enlaces trunking**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trunking | SI | SI | SI | SI | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|
| NO | NO | NO | NO | NO | NO | NO | NO | NO |

Enlaces F.O.

| | | | |
|---|---|---|---|
| Enlace: Router-Switch Troncal | Port 01 | Trunk | F.O. |
| Enlace: Switch Troncal – Switch Pantalan 01 | Port 02 | Trunk | F.O. |
| Enlace: Switch Troncal – Switch Pantalan 02 | Port 03 | Trunk | F.O. |
| Enlace: Switch Troncal – Switch Pantalan 03 | Port 04 | Trunk | F.O. |

### 2.1.3 Switch Pantalan 01.

Definición y tablas de configuración PVID

**Tabla PVID**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PVID | 10 | 10 | 10 | 20 | 20 | 20 | 20 | 30 | 30 | 30 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

| 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|
| 1 | 1 | -- | -- | -- |

**Tabla enlaces trunking**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trunking | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|
| NO | NO | NO | NO | NO | NO | SI | SI | SI |

Enlaces F.O.

| | | | |
|---|---|---|---|
| Enlace: Switch Pantalan 01 – Switch Troncal | Port 22 | Trunk | F.O. |
| Enlace: Switch Pantalan 01 – Switch Pantalan 02 | Port 23 | Trunk | F.O. |
| Enlace: Switch Pantalan 01 – Switch Pantalan 03 | Port 24 | Trunk | F.O. |

### 2.1.4 Switch Pantalan 02.

Definición y tablas de configuración PVID

**Tabla PVID**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PVID | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 20 | 20 | 20 | 20 | 30 | 30 | 30 | 1 | 1 | 1 | 1 |

| 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|
| 1 | 1 | -- | -- | -- |

**Tabla enlaces trunking**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trunking | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|
| NO | NO | NO | NO | NO | NO | SI | SI | SI |

Enlaces F.O.

| | | | |
|---|---|---|---|
| Enlace: Switch Pantalan 02 – Switch Troncal | Port 22 | Trunk | F.O. |
| Enlace: Switch Pantalan 02 – Switch Pantalan 01 | Port 23 | Trunk | F.O. |
| Enlace: Switch Pantalan 02 – Switch Pantalan 03 | Port 24 | Trunk | F.O. |

### 2.1.5 Switch Pantalan 03.

**Definición y tablas de configuración PVID**

**Tabla PVID**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PVID | 10 | 10 | 10 | 10 | 10 | 10 | 20 | 20 | 20 | 20 | 30 | 30 | 30 | 1 | 1 | 1 | 1 | 1 | 1 |

| 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|
| 1 | 1 | -- | -- | -- |

**Tabla enlaces trunking**

| Puerto | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Trunking | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|
| NO | NO | NO | NO | NO | NO | SI | SI | SI |

**Enlaces F.O.**

| | | | |
|---|---|---|---|
| Enlace: Switch Pantalan 03 – Switch Troncal | Port 22 | Trunk | F.O. |
| Enlace: Switch Pantalan 03 – Switch Pantalan 01 | Port 23 | Trunk | F.O. |
| Enlace: Switch Pantalan 03 – Switch Pantalan 02 | Port 24 | Trunk | F.O |

## 2.2 Plan de direccionamiento Ipv4.

Usamos IPs privadas de clase C sin subredes, podemos asignar las siguientes redes:

192.168.1.0/24 -- CCTV, Megafonía
192.168.2.0/24 -- Sistema de Aproximación y Amarre, PLC´s, PakScan Rotork, Extinción de Incendios Moec, Honeywell
192.168.3.0/24 -- Telefonía y datos

### 2.2.1 Switch Terminal Maritima.

| | | | | | |
|---|---|---|---|---|---|
| Servidor de vídeo Axis Q7900- | 192.168.1.1 | 255.255.255.0 | Vlan 10 | Port 01 | F.O. |
| PC-Camaras | 192.168.1.2 | 255.255.255.0 | Vlan 10 | Port 02 | UTP |
| Pupitre de megafonia- | 192.168.1.3 | 255.255.255.0 | Vlan 10 | Port 03 | UTP |
| Servidor PackScan Rotork- | 192.168.2.1 | 255.255.255.0 | Vlan 20 | Port 04 | F.O. |
| Servidor Sistema de Aprox.Amarre - | 192.168.2.2 | 255.255.255.0 | Vlan 20 | Port 05 | F.O |
| Servidor Extincion de Incendios- | 192.168.2.3 | 255.255.255.0 | Vlan 20 | Port 06 | F.O. |
| Servidor Scada Honeywell - | 192.168.2.4 | 255.255.255.0 | Vlan 20 | Port 07 | F.O. |
| PC1-Operador- | 192.168.2.5 | 255.255.255.0 | Vlan 20 | Port 08 | UTP |
| PC2-Operador- | 192.168.2.6 | 255.255.255.0 | Vlan 20 | Port 09 | UTP |
| PC-oficina | 192.168.3.1 | 255.255.255.0 | Vlan 30 | Port 10 | UTP |
| Impresora- | 192.168.3.2 | 255.255.255.0 | Vlan 30 | Port 11 | UTP |
| Telefono-TM1 | 192.168.3.3 El call-manager de configuración router asigna IP con DHCP | 255.255.255.0 | Vlan 30 | Port 12 | UTP |

### 2.2.2 Switch Pantalan 01.

| | | | | | |
|---|---|---|---|---|---|
| CTV01 - PO1 | 192.168.1.4 | 255.255.255.0 | Vlan 10 | Port 01 | F.O. |
| CCTV – CTV02 - PO1 | 192.168.1.5 | 255.255.255.0 | Vlan 10 | Port 02 | F.O. |
| Amplificador Megafonia P01 | 192.168.1.6 | 255.255.255.0 | Vlan 10 | Port 03 | UTP |
| Moec Ext. De Incendios | 192.168.2.7 | 255.255.255.0 | Vlan 20 | Port 04 | F.O. |
| PackScan Rotork | 192.168.2.8 | 255.255.255.0 | Vlan 20 | Port 05 | F.O. |

| | | | | |
|---|---|---|---|---|
| Sistema de Aprox.Amarre | 192.168.2.9 255.255.255.0 | Vlan 20 | Port 06 | F.O. |
| Switch sneider -PLC | 192.168.2.10 255.255.255.0 | Vlan 20 | Port 07 | F.O. |
| PC-Pantalan 01 | 192.168.3.4 255.255.255.0 | Vlan 30 | Port 08 | UTP |
| Impresora- | 192.168.3.5 255.255.255.0 | Vlan 30 | Port 09 | UTP |
| Telefono-P01 | 192.168.3.6 255.255.255.0 El call-manager de configuración router asigna IP con DHCP | Vlan 30 | Port 10 | UTP |

### 2.2.3 Switch Pantalan 02.

| | | | | |
|---|---|---|---|---|
| CCTV – CTV01 - PO2 | 192.168.1.7 255.255.255.0 | Vlan 10 | Port 01 | F.O. |
| CCTV – CTV02 - PO2 | 192.168.1.8 255.255.255.0 | Vlan 10 | Port 02 | F.O. |
| CCTV – CTV03 - PO2 | 192.168.1.9 255.255.255.0 | Vlan 10 | Port 03 | F.O. |
| CCTV – CTV04 - PO2 | 192.168.1.10 255.255.255.0 | Vlan 10 | Port 04 | F.O. |
| CCTV – CTV05 - PO2 | 192.168.1.11 255.255.255.0 | Vlan 10 | Port 05 | F.O. |
| CCTV – CTV06 - PO2 | 192.168.1.12 255.255.255.0 | Vlan 10 | Port 06 | F.O. |
| CCTV – CTV07 - PO2 | 192.168.1.13 255.255.255.0 | Vlan 10 | Port 07 | F.O. |
| Amplificador Megafonia P02 | 192.168.1.14 255.255.255.0 | Vlan 10 | Port 08 | UTP |
| Moec Ext. De Incendios P02 | 192.168.2.11 255.255.255.0 | Vlan 20 | Port 09 | F.O. |
| PackScan Rotork P02 | 192.168.2.12 255.255.255.0 | Vlan 20 | Port 10 | F.O. |
| Sistema de Aprox.Amarre P02 | 192.168.2.13 255.255.255.0 | Vlan 20 | Port 11 | F.O. |
| Switch sneider -PLC P02 | 192.168.2.14 255.255.255.0 | Vlan 20 | Port 12 | F.O. |
| PC-Pantalan 02 | 192.168.3.7 255.255.255.0 | Vlan 30 | Port 13 | UTP |
| Impresora- P02 | 192.168.3.8 255.255.255.0 | Vlan 30 | Port 14 | UTP |
| Telefono-P02 | 192.168.3.9 255.255.255.0 El call-manager de configuración router asigna IP con DHCP | Vlan 30 | Port 15 | UTP |

### 2.2.4 Switch Pantalan 03.

| | | | | |
|---|---|---|---|---|
| CCTV – CTV01 - PO3 | 192.168.1.15 255.255.255.0 | Vlan 10 | Port 01 | F.O. |
| CCTV – CTV02 - PO3 | 192.168.1.16 255.255.255.0 | Vlan 10 | Port 02 | F.O. |
| CCTV – CTV03 - PO3 | 192.168.1.17 255.255.255.0 | Vlan 10 | Port 03 | F.O. |

| | | | | |
|---|---|---|---|---|
| CCTV – CTV04 - PO3 | 192.168.1.18 255.255.255.0 | Vlan 10 | Port 04 | F.O. |
| CCTV – CTV05 - PO3 | 192.168.1.19 255.255.255.0 | Vlan 10 | Port 05 | F.O. |
| Amplificador Megafonia P03 | 192.168.1.20 255.255.255.0 | Vlan 10 | Port 06 | UTP |
| Moec Ext. De Incendios P03 | 192.168.2.15 255.255.255.0 | Vlan 20 | Port 07 | F.O. |
| PackScan Rotork P03 | 192.168.2.16 255.255.255.0 | Vlan 20 | Port 08 | F.O. |
| Sistema de Aprox.Amarre P03 | 192.168.2.17 255.255.255.0 | Vlan 20 | Port 09 | F.O. |
| Switch sneider -PLC P03 | 192.168.2.18 255.255.255.0 | Vlan 20 | Port 10 | F.O. |
| PC-Pantalan 03 | 192.168.3.10 255.255.255.0 | Vlan 30 | Port 11 | UTP |
| Impresora- P03 | 192.168.3.11 255.255.255.0 | Vlan 30 | Port 12 | UTP |
| Telefono-P03 | 192.168.3.12 255.255.255.0 El call-manager de configuración router asigna IP con DHCP | Vlan 30 | Port 13 | UTP |

# Capítulo 3: Diseño de la Arquitectura de Red.

## 3.1 Descripción, Selecciónde Equipos y Electronica de Red.

Dentro de la Sala de Rack del Terminal Marítimo estarán situados en un armario Rack los distintos servidores.

Figura-2

### 3.1.1 Distribución de Equipos e Instrumentos en Pantalan 01.

Servidor de proceso:

ModBus/TCP: Red industrial conectada a Switch Sneider, PLC modicon cuantum.

-Cuatro (4) transmisores de presión

-Uno (1) contadores másicos, uno de fuel-oil y otro de gas-oil.

-Tres (3) señales digitales DI

-Una (1) señal digital DO

-Dos (2) detectores de H2S

Servidor de Seguridad:

Sistema de detección de Incendios (Moec), CCTV (cámaras Pelco, y Servidor de vídeo Axis) y Sistema de megafonía (Optymus)

-Dos cámaras de CCTV

-Tres Altavoces de megafonía y 1 Amplificador

-Tres detectores de incendios

Comunicaciones Red y datos:

-Un Teléfono IP

- Un punto para Datos

Servidores para sistemas de Operación:

Red serie que comunica la pack-scan con todas las válvulas Rotork

-Las 10 válvulas motorizadas de la plataforma

-Sistema de aproximación de Marimatech

-Sistema Scada Honeywell.

### 3.1.2 Distribución de Equipos e Instrumentos en Pantalan 02.

Servidor de proceso:

ModBus/TCP: Red industrial conectada a Switch Sneider, PLC modicon cuantum.

-Diez transmisores de presión

-Tres contadores másicos, uno de fuel-oil y otro de gas-oil.

-Ocho señales digitales DI

-Dos señales digitales DO

-Nueve detectores de H2S

Servidor de Seguridad:

Sistema de detección de Incendios (Moec), CCTV (cámaras Pelco, y Servidor de vídeo Axis) y Sistema de megafonía (Optymus)

-Siete cámaras de CCTV

-Nueve Altavoces de megafonía y 1 Amplificador

- Nueve detectores de incendios

Comunicaciones Red y datos:

- Un Teléfono IP

- Un punto para Datos

Servidores para sistemas de Operación:

Red serie que comunica la pack-scan con todas las válvulas Rotork

-Las 18 válvulas motorizadas de la plataforma

-Sistema de aproximación de Marimatech

-Sistema Scada Honeywell.

### 3.1.3 Distribución de Equipos e Instrumentos en Pantalan 03.

Servidor del proceso:

ModBus/TCP: Red industrial conectada a Switch Sneider, PLC modicon cuantum.

-Seis transmisores de presión

-Dos contadores másicos, uno de fuel-oil y otro de gas-oil.

-Cuatro señales digitales DI

-Una señal digital DO

-Cinco detectores de H2S

Servidor de Seguridad:

Sistema de detección de Incendios (Moec), CCTV (cámaras Pelco, y Servidor de vídeo Axis) y Sistema de megafonía (Optymus)

- Cinco Cámaras de CCTV
- Cinco Altavoces de megafonía y 1 Amplificador
- Cinco detectores de incendios

Comunicaciones Red y datos:

- Un Teléfono IP
- Un punto para Datos

Servidores para sistemas de Operación:

Red serie que comunica la pack-scan con todas las válvulas Rotork

-Las 15 válvulas motorizadas de la plataforma

-Sistema de aproximación de Marimatech

-Sistema Scada Honeywell.

## 3.2 Equipos, Instrumentos y soporte telemático de Red.

### 3.2.1 Switch`s.

En cada nodo existe un switch marca Cisco modelo Catalys 2960 con 24 puertos de cobre de 10/100/1000 Además 4 puertos adaptados en F.O., es decir, también basados en SFP(son de acoplamiento activo de E/S) los cuales acomodan un amplio rango de transceivers.

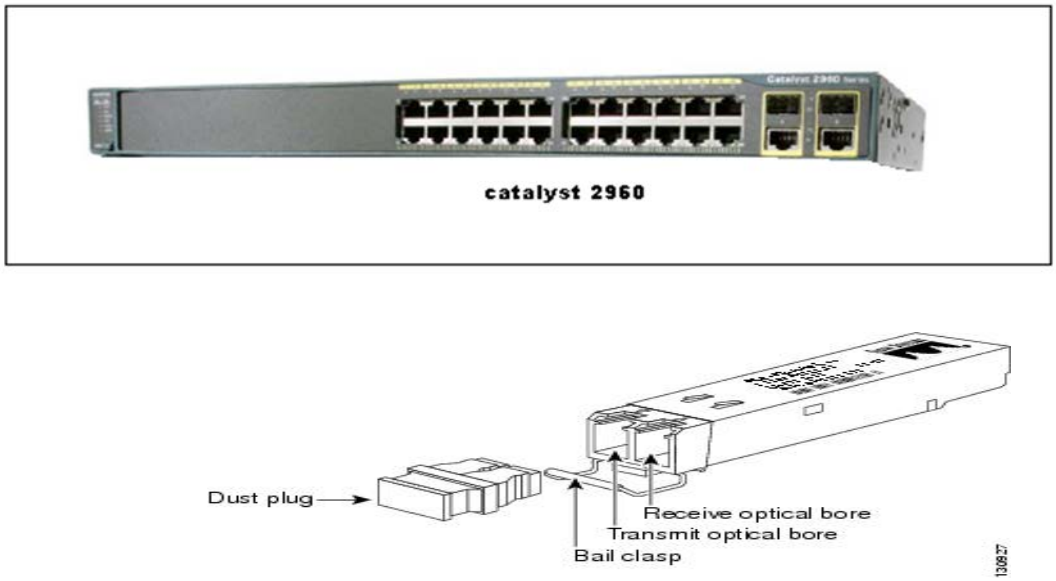



Figura-3

Los 4 switches se encuentran unidos mediante un anillo troncal de 6 fibras ópticas monomodo. Un esquema de la red puede observarse en la figura.

Los switches van montados en los armarios existentes en cada Frente y su alimentación se toma a partir de SAI que existe en cada emplazamiento.

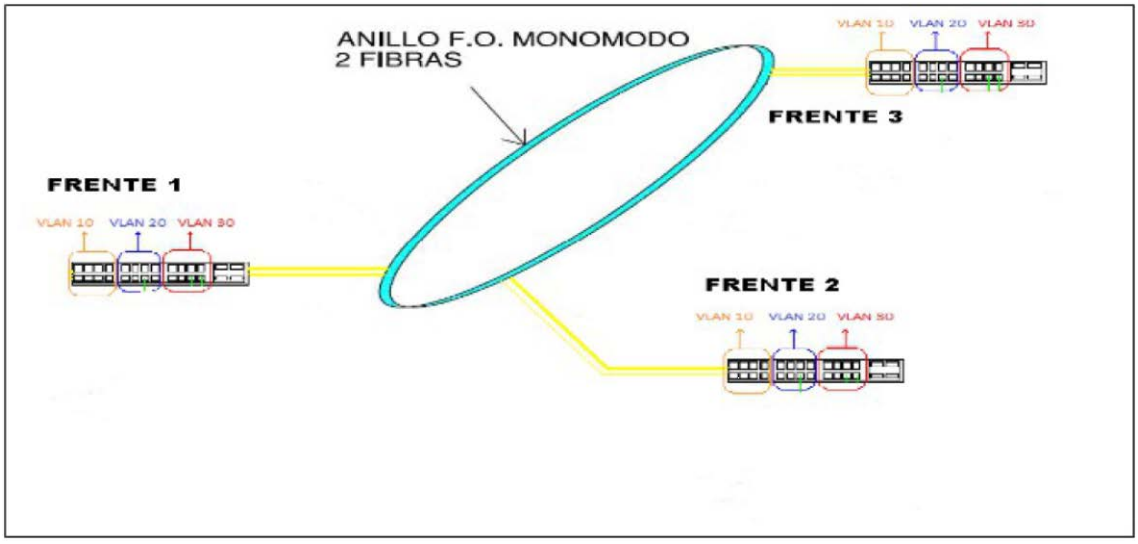



Figura-4

### 3.2.2 Router.

En la terminal Marítima, también tenemos ubicado el único Router que soporta todas las comunicaciones entre los Pantalanes, Internet y la Terminal Marítima. El modelo elegido es un Cisco modelo LINKSYS E2500.

Facilita, este modelo, la configuración de nuestro sistema de monitorización NetFlow.

Figura-5

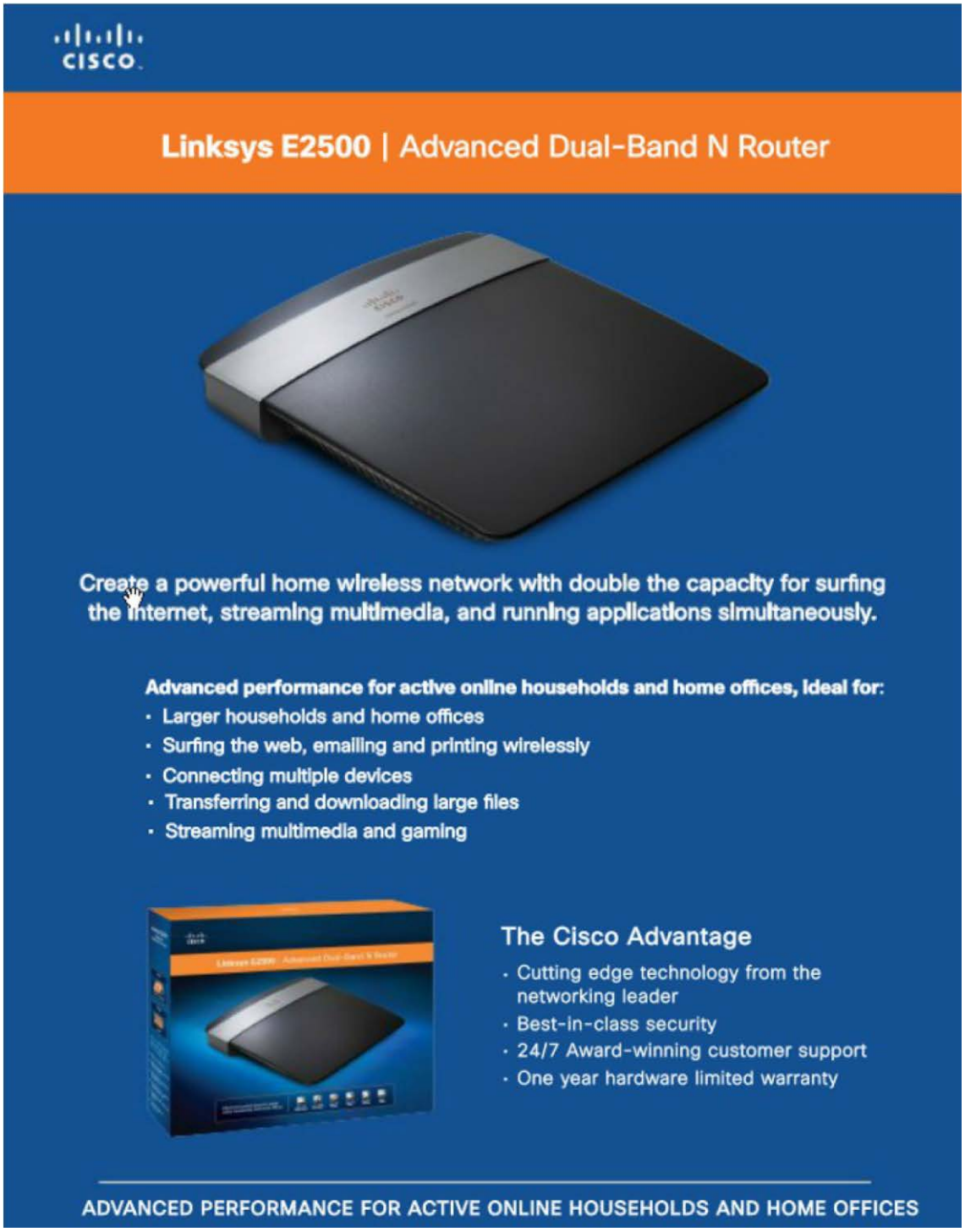
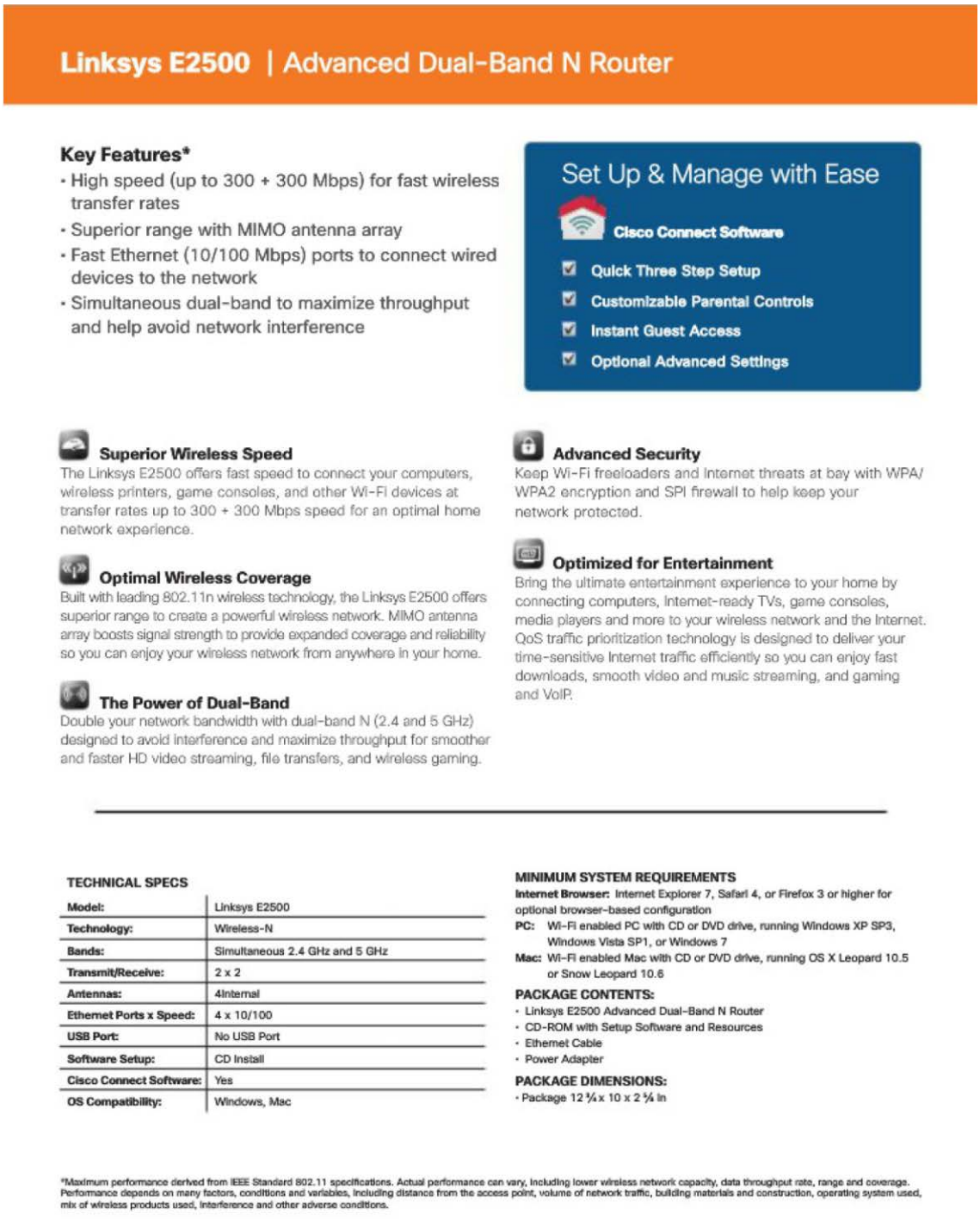

cisco
Linksys E2500 | Advanced Dual-Band N Router
Create a powerful home wireless network with double the capacity for surfing the internet, streaming multimedia, and running applications simultaneously.
Advanced performance for active online households and home offices, ideal for:
· Larger households and home offices
· Surfing the web, emailing and printing wirelessly
· Connecting multiple devices
· Transferring and downloading large files
· Streaming multimedia and gaming
The Cisco Advantage
· Cutting edge technology from the networking leader
· Best-in-class security
· 24/7 Award-winning customer support
· One year hardware limited warranty
ADVANCED PERFORMANCE FOR ACTIVE ONLINE HOUSEHOLDS AND HOME OFFICES

Figura-6



## Linksys E2500 | Advanced Dual-Band N Router

### Key Features*

- High speed (up to 300 + 300 Mbps) for fast wireless transfer rates
- Superior range with MIMO antenna array
- Fast Ethernet (10/100 Mbps) ports to connect wired devices to the network
- Simultaneous dual-band to maximize throughput and help avoid network interference

### Set Up & Manage with Ease

**Cisco Connect Software**

- Quick Three Step Setup
- Customizable Parental Controls
- Instant Guest Access
- Optional Advanced Settings

### Superior Wireless Speed

The Linksys E2500 offers fast speed to connect your computers, wireless printers, game consoles, and other Wi-Fi devices at transfer rates up to 300 + 300 Mbps speed for an optimal home network experience.

### Optimal Wireless Coverage

Built with leading 802.11n wireless technology, the Linksys E2500 offers superior range to create a powerful wireless network. MIMO antenna array boosts signal strength to provide expanded coverage and reliability so you can enjoy your wireless network from anywhere in your home.

### The Power of Dual-Band

Double your network bandwidth with dual-band N (2.4 and 5 GHz) designed to avoid interference and maximize throughput for smoother and faster HD video streaming, file transfers, and wireless gaming.

### Advanced Security

Keep Wi-Fi freeloaders and Internet threats at bay with WPA/WPA2 encryption and SPI firewall to help keep your network protected.

### Optimized for Entertainment

Bring the ultimate entertainment experience to your home by connecting computers, Internet-ready TVs, game consoles, media players and more to your wireless network and the Internet. QoS traffic prioritization technology is designed to deliver your time-sensitive Internet traffic efficiently so you can enjoy fast downloads, smooth video and music streaming, and gaming and VoIP.

**TECHNICAL SPECS**

| | |
|---|---|
| **Model:** | Linksys E2500 |
| **Technology:** | Wireless-N |
| **Bands:** | Simultaneous 2.4 GHz and 5 GHz |
| **Transmit/Receive:** | 2 x 2 |
| **Antennas:** | 4Internal |
| **Ethernet Ports x Speed:** | 4 x 10/100 |
| **USB Port:** | No USB Port |
| **Software Setup:** | CD Install |
| **Cisco Connect Software:** | Yes |
| **OS Compatibility:** | Windows, Mac |

**MINIMUM SYSTEM REQUIREMENTS**

**Internet Browser:** Internet Explorer 7, Safari 4, or Firefox 3 or higher for optional browser-based configuration

**PC:** Wi-Fi enabled PC with CD or DVD drive, running Windows XP SP3, Windows Vista SP1, or Windows 7

**Mac:** Wi-Fi enabled Mac with CD or DVD drive, running OS X Leopard 10.5 or Snow Leopard 10.6

**PACKAGE CONTENTS:**

- Linksys E2500 Advanced Dual-Band N Router
- CD-ROM with Setup Software and Resources
- Ethernet Cable
- Power Adapter

**PACKAGE DIMENSIONS:**

- Package 12 ¾ x 10 x 2 ¾ in

*Maximum performance derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Figura-7

### 3.2.3 Balanceo de Carga.

En nuestra Arquitectura de red para dar soporte a nuestros servidores, siendo una de las características más importantes, aparte de la seguridad, flexibilidad y la tolerancia a fallos es la escalabilidad.
Esta escalabilidad es la capacidad de nuestra estructura a dar más servicios a los usuarios de la Empresa al acceso a los servidores, sin que requiera cambios importantes.
El balanceador de carga que utilizaremos debido al diseño de nuestra arquitectura, es **Zen Load Balancer** ofrece las funciones básicas, y en nuestro sistema es suficiente, debido a que el incremento de usuarios de la empresa no va a ser notable ya que es de acceso restringido.


Figura-8

### 3.2.4 Firewall.

Dentro de la selección de equipos, tenemos el Firewall, aunque es imprescindible para la seguridad de nuestra red en este apartado de arquitectura pondremos el modelo y las características del mismo.


Figura-9

| | |
|---|---|
| Rendimiento del firewall | • 940 Mbps |
| Rendimiento del firewall de aplicaciones | • 940 Mbps |
| Rendimiento del antivirus | • 110 Mbps |
| Rendimiento de IPS | • 620 Mbps |
| Rendimiento de UTM (tráfico HTTP) | • 82 Mbps |
| Rendimiento de UTM (tráfico distinto a HTTP, como P2P, DNS, SSH) | • 620 Mbps |
| Máximo rendimiento en VPN | • 586 Mbps |
| Número máximo de conexiones simultáneas | • 80 000 |
| Conexiones VLAN 802.1q | • 255 |
| SEGURIDAD DE CONTENIDOS | |
| Protocolos web y de correo electrónico analizados | • HTTP, HTTPS, FTP, SMTP, IMAP, POP3 |
| Stream Scanning | • Sí |
| Inspección de entrada y salida | • Sí |
| Protección de hora cero sin firma | • Sí |
| Firmas de malware | • 45 millones |
| Filtros de contenido web | • Filtros por: bloqueo inteligente de HTTPS, palabras clave en el cuerpo de HTML, extensión del archivo |
| Filtros de objetos web | • ActiveX, Java™, Flash, JavaScript™, proxy, cookies |
| Filtros de contenidos de correo electrónico | • Filtros por: palabras clave en el asunto, archivos adjuntos protegidos por contraseña, extensión del archivo, nombre del archivo |
| Análisis de spam distribuido | • Sí |
| Protocolos compatibles de análisis de spam distribuido | • SMTP, POP3 |
| Lista negra en tiempo real antispam (RBL) | • Sí |
| Listas de permiso/bloqueo de spam definidas por el usuario | • Sin límite |
| CARACTERÍSTICAS DEL FIREWALL | |
| Inspección dinámica de paquetes (SPI) | • Bloqueo de servicios/puertos, prevención de la denegación de servicio (DoS), modo de incógnito, bloqueo de ataques de desbordamiento de TCP, bloqueo de ataques de desbordamiento de UDP, control de la respuesta de ping de WAN/LAN |
| Firewall de aplicaciones | • Modo global, modo de políticas, descifrado SSL, políticas de aplicación pormenorizada, supervisión de sesiones de aplicaciones, panel de control de aplicaciones |
| Aplicaciones con protección | • 1212 |
| Detección y prevención de intrusos (IPS) | • Sí |
| Firmas IPS | • 2114 |
| Modos WAN | • NAT, enrutamiento clásico |
| Asignación de direcciones ISP | • DHCP, asignación de IP estática, PPPoE, PPTP |

| | |
|---|---|
| Direcciones IP de la red WAN secundaria | • 64 |
| Modos NAT | • NAT 1:1, PAT |
| Enrutamiento | • Estático, dinámico, RIPv1 y RIPv2 |
| VoIP | • SIP ALG |
| DDNS | • DynDNS.org, TZO.com, Oray.net, 3322 DDNS |
| Funciones del firewall | • Reenvío del intervalo de puertos, activación de puertos, proxy DNS, simulación/clonación de direcciones MAC, compatibilidad con el protocolo de tiempo de red (NTP), herramientas de diagnóstico (ping, búsqueda DNS, rastreo de rutas, etc.), Auto Uplink en los puertos del switch, calidad de servicio (QoS) de capa 3, LAN a WAN y WAN a LAN (tipo de servicio, ToS) |
| DHCP | • Servidor DHCP, relé DHCP |
| Autenticación de usuario para VPN | • Active Directory, LDAP, Radius, base de datos de usuarios local |
| Políticas de seguridad basadas en Active Directory con Single Sign-On (SSO) | • Sí |
| Compatibilidad con autenticación de dos factores de conformidad con PCI | • Sí |
| VPN | |
| Túneles VPN de sitio a sitio | • 150 |
| Túneles VPN SSL | • 75 |
| L2TP, PPTP, túneles VPN | • 5 |
| Algoritmo de cifrado IPsec | • DES, 3DES, AES (128,192, 256 bits)/SHA-1, MD5 |
| Intercambio de claves | • IKE, clave manual, clave precompartida, PKI, X.500 |
| NAT Traversal de IPsec | • Sí |
| Compatibilidad con cliente VPN nativo de iPhone | • Sí |
| Incluye licencias de ProSafe VPN Client Lite | • 3 |
| Compatibilidad con la versión SSL | • SSLv3, TLS1.0 |
| Compatibilidad con cifrado SSL | • DES, 3DES, ARC4, AES (128, 256 bits) |
| Integridad de mensajes SSL | • MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1 |
| Compatibilidad con certificados SSL | • RSA, Diffie-Hellman, propio (longitud de clave de 512 bits, 1024 bits, 2048 bits) |
| Plataformas VPN SSL compatibles | • Windows 2000 / XP / Vista® (32 bits), Windows 7 (32 y 64 bits), Mac OS® x 10.4.x/10.6. |
| IMPLEMENTACIÓN | |
| Compatibilidad con VLAN | • Sí |
| Fallo multi-WAN | • Sí |
| Balanceo de carga de tráfico inteligente en función del recuento de bytes de tráfico | • Sí |
| Compatibilidad con llave USB para conexiones WAN 3G/4G | • n/c |
| Asistentes de configuración | • Configuración, VPN sobre IPsec, VPN SSL |
| Licencia electrónica | • Sí |

| REGISTRO E INFORMES | |
|---|---|
| Gestión | • HTTP/HTTPS, SNMP v2c |
| Informes | • Resúmenes estadísticos, informes gráficos, alertas de expansión automáticas, notificaciones de malware automáticas, notificaciones del sistema |
| Registro | • Tráfico, malware, spam, filtrado de contenidos, filtrado de correo electrónico, sistema, servicio, IPS, aplicaciones, búsqueda de puertos, IM, P2P, VPN sobre IPsec, VPN SSL |
| Entrega de registros | • Consulta de la interfaz gráfica de usuario de gestión, entrega de correos electrónicos, Syslog |
| HARDWARE | |
| Puertos WAN/LAN Gigabit RJ454 | • 4/4 |
| Interfaces DMZ (configurable) | • 1 |
| Memoria Flash/RAM | • 2 GB/1 GB |
| Puertos USB | • 1 |
| Certificados | • ICSA: antivirus VPNC: interoperabilidad AES, interoperabilidad básica Checkmark: antimalware, antispam, firewall empresarial, VPN, IPS, filtrado de URL |
| Cumplimiento de las normativas principales | • FCC parte 15 clase A, marca comercial CE, VCCI, C-Tick clase A, CE/LVD, cUL, RoHS, RoHS China |
| Temperatura de almacenamiento y funcionamiento | • Temperatura de funcionamiento de 0 a 45 °C (32 a 113 °F), temperatura de almacenamiento de -20 a 70 °C (-4 a 158 °F) |
| Humedad | • Funcionamiento: 90 % máxima relativa, Almacenamiento: 95 % máxima relativa |
| Tensión de entrada de potencia | • 100-240 V CA/50-60 Hz, entrada universal, 1,2 A máx. |
| Dimensiones (ancho x alto x profundidad) en cm | • 44 x 4,3 x 25,3 |
| Dimensiones (ancho x alto x profundidad) en pulg. | • 17,3 x 1,7 x 9,96 |
| Peso kg/lb | • 2,9/6,4 |
| Contenido de la caja | • Dispositivo UTM ProSecure, cable de alimentación, patas de goma, CD de recursos, kit de montaje en bastidor, tarjeta de garantía, guía de instalación rápida, licencia electrónica (solo para paquetes) |
| Garantía | • Vida útil |

## 3.2.5 Equipos y Sistemas CCTV.

Tipo de cámaras PELCO: Características del modelo

SE MUESTRA CON EL SOPORTE DE PARED WXM100

- Fabricación en acero inoxidable 316L con pulido eléctrico
- Funcionamiento en vertical o invertido
- Receptor, unidad de giro horizontal/vertical y carcasa con Paquete Óptico Integrado (IOP)
- Dos paquetes ópticos integrados de alta resolución con enfoque automático
  - Día/noche de 23X, rango dinámico amplio de 80X y detección de movimiento
  - Color 22X EXview HAD™
- Menús multilingües en pantalla
- Protección por contraseña
- Configuraciones de cámara programables
- Visualización de compás, giro vertical y zoom en pantalla
- Giro horizontal de velocidad variable: 0,1° a 40°/segundo con giro horizontal proporcional
- 360° de rotación horizontal continua
- Intervalo de giro vertical de +90° a -90° desde la horizontal
- Posicionamiento preprogramado, patrones, modos de exploración múltiples
- Diseñado para mantenimiento mínimo
- Memoria del sistema incorporada
- Configuración y actualización de software mediante puerto de datos remoto (IPS-RDPE-2)
- Conector integrado para
  - Convertidor de video VC-UTP de Pelco
  - Tarjetas traductoras de la Serie TXB de Pelco para usar con Hernis y otros protocolos
  - El FS85011A de Pelco y transmisores de fibra óptica de otros fabricantes

Figura-10

### 3.2.6 Equipos y Sistema de Megafonia.

CCTV en frente 1

En el Frente 1 existen actualmente 2 cámaras domo motorizadas que deberán integrarse en el sistema de CCTV.Las cámaras seleccionadas son resistentes a la corrosión y tres de ellas clasificadas ATEX ya que serán ubicadas en zonas con riesgo de explosión.
Esta integración consiste en adaptar el sistema actual al lazo de comunicaciones por Ethernet. Para ello, se seguirá la misma arquitectura que en el frente 3.

CCTV en frente 2

Se ha determinado la instalación y montaje de 7 cámaras domos para cubrir todas las áreas más importantes del frente 2. Las cámaras seleccionadas son resistentes a la corrosión y tres de ellas clasificadas ATEX ya que serán ubicadas en zonas con riesgo de explosión.

La distribución de las cámaras y función de cada una, queda de la siguiente manera.

Cámaras 1 y 2: Son antideflagrantes y se situarán en la zona más cercana al atraque del buque, permitiendo monitorizar todo aquello que ocurra tanto en la zona de la plataforma como en el propio buque. No existen zonas oscuras significativas para estas cámaras. Va colocada en soporte en posición invertida.

Cámara 3 y 4: También es antideflagrante y con zoom por 36. Se situará en la parte superior de la plataforma siendo su objetivo vigilar la zona de instalaciones y zona de evacuación. No existen zonas oscuras significativas para estas cámaras. Va colocada en soporte en posición invertida.

Cámara 5: Se situará en la parte más alejada de la zona de atraque y en la parte baja de la plataforma. Se colocará de pié sobre un mástil de 11 metros que permita captar imágenes incluso hasta de la zona superior de la plataforma.

El objetivo de esta cámara es visualizar imágenes correspondientes a la zona de acceso al frente 3, la zona donde se encuentran los equipos de control y parte de la zona de purgas y equipos S.C.I. Por su ubicación, existirían algunas zonas oscuras en el área de S.C.I y purgas por lo que se aconsejó el montaje e instalación de la cámara_5.

Cámara 6 y 7: Ubicada en zona de S.C.I y purgas. Su objetivo es el de visualizar las imágenes de esta zona de la plataformas, así como la visualización de las purgas.
Va colocada en soporte en posición invertida. No existen zonas oscuras significativas para estas cámaras.

Todas las cámaras trabajan con el protocolo Pelco P para la telemetría.

CCTV en frente 3

Se ha determinado la instalación y montaje de 5 cámaras domos para cubrir todas las áreas más importantes del frente 3. Las cámaras seleccionadas son resistentes a la corrosión y tres de ellas clasificadas ATEX ya que serán ubicadas en zonas con riesgo de explosión.

La distribución de las cámaras y función de cada una, queda de la siguiente manera.

Cámaras 1 y 2: Son antideflagrantes y se situarán en la zona más cercana al atraque del buque, permitiendo monitorizar todo aquello que ocurra tanto en la zona de la plataforma como en el propio buque. No existen zonas oscuras significativas para estas cámaras. Va colocada en soporte en posición invertida.

Cámara 3 : También es antideflagrante y con zoom por 36. Se situará en la parte superior de la plataforma siendo su objetivo vigilar la zona de instalaciones y zona de evacuación. No existen zonas oscuras significativas para esta cámara. Va colocada en soporte en posición invertida.

Cámara 4: Se situará en la parte más alejada de la zona de atraque y en la parte baja de la plataforma. Se colocará de pié sobre un mástil de 11 metros que permita captar imágenes incluso hasta de la zona superior de la plataforma.

El objetivo de esta cámara es visualizar imágenes correspondientes a la zona de acceso al frente 3, la zona donde se encuentran los equipos de control y parte de la zona de purgas y equipos S.C.I. Por su ubicación, existirían algunas zonas oscuras en el área de S.C.I y purgas por lo que se aconsejó el montaje e instalación de la cámara_5.

Cámara 5 : Ubicada en zona de S.C.I y purgas. Su objetivo es el de visualizar las imágenes de esta zona de la plataforma, así como la visualización de las purgas.
Va colocada en soporte en posición invertida. No existen zonas oscuras significativas para esta cámara.

Todas las cámaras trabajan con el protocolo Pelco P para la telemetría.

Arquitectura del sistema CCTV

Como ejemplo, en la figura siguiente se muestra la arquitectura del sistema de CCTV. En el frente 3, la integración de las dos cámaras se realizará de la misma forma.

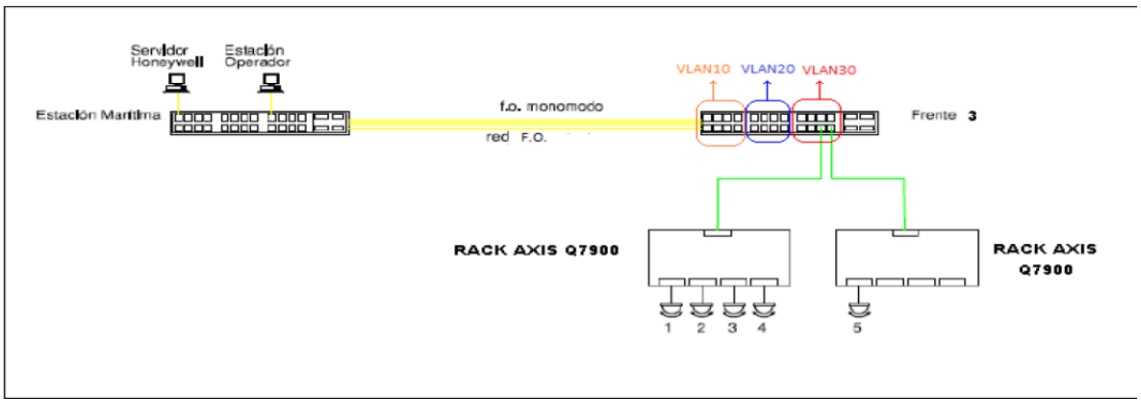



Figura-11

Streamers de vídeo Axis Q7900.

Estos servidores tienen cuatro canales por lo que permiten codificar hasta 4 cámaras domo y presentan una dirección IP para cada cámara de forma independiente.

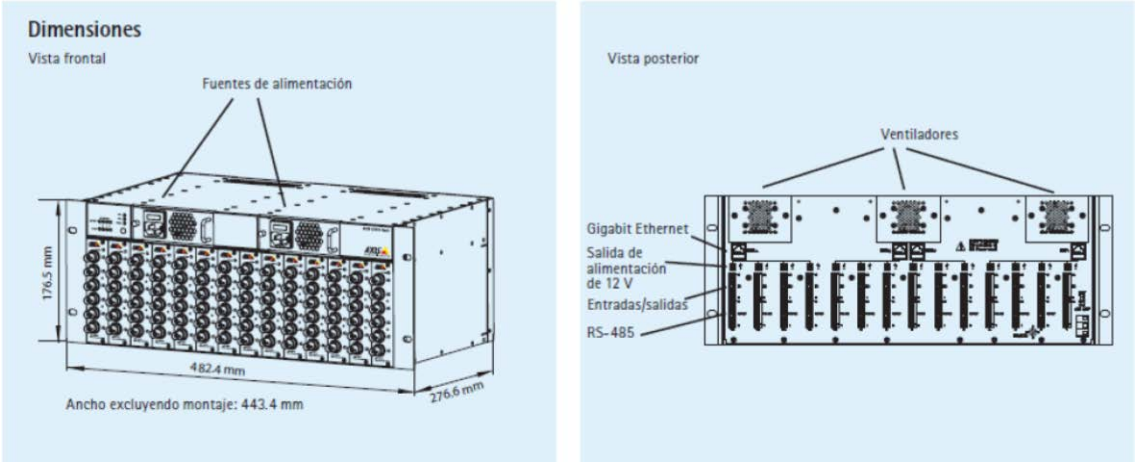



Figura-12

Entre sus ventajas principales tenemos:

a) Detección de movimiento en vídeo y memoria previa y posterior a la alarma

b) Velocidad de fotogramas completa en MPEG-4 o motion J-PEG en todos los canales

c) Solución en rack que puede utilizar cualquier combinación de tarjetas transferibles e intercambiables en caliente.

d) Para la configuración del servidor de vídeo, se utilizará el driver para Pelco-P y cargándolo en los cuatro canales de vídeo, ya que este protocolo resulta el más estandarizado hasta el momento.



e) La alimentación de los decoficadores se realiza a través del SAI general existente en cada caseta. Los decodificadores van montados en el rack de 19 pulgadas de los armarios.

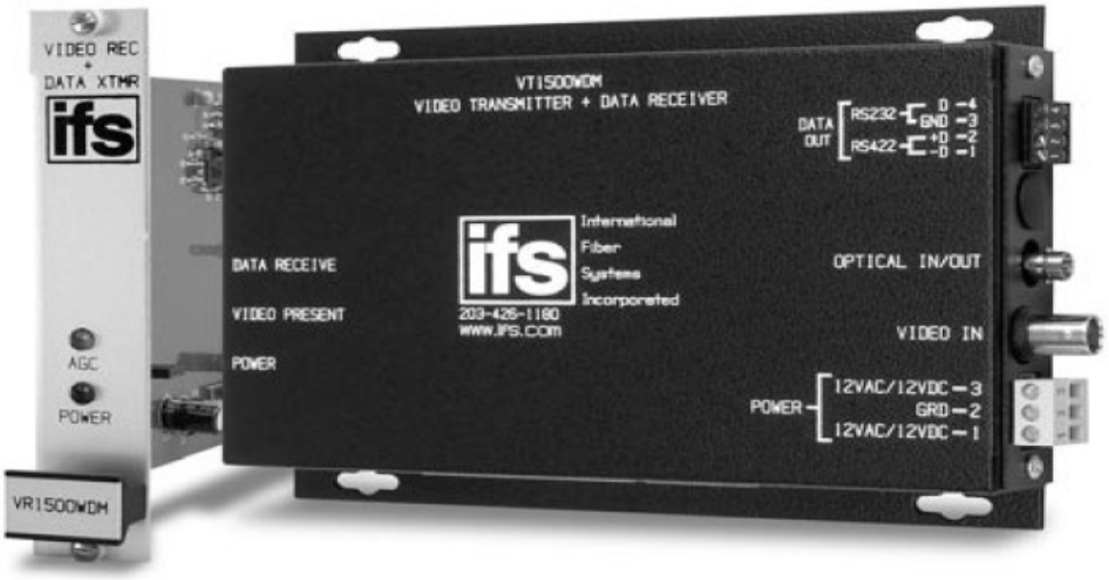



Figura-13

**Cableado a cada Cámara.**

Tanto la señal de video como la telemetría y la alimentación llegan a cada cámara mediante un cable compuesto que agrupa en una sola manguera todos los cables necesarios. Este cable tiene una longitud máxima de 10 m conectándose el otro extremo a un dispositivo que suministra la tensión de alimentación y las señales de video y telemetría.
Este equipo al poder estar en zona clasificada deberá estar ubicado en una caja de aparellaje antideflagrante de medidas tales que permitan la colocación de dicha fuente de alimentación. La sujeción de esta caja se definirá de acuerdo a las características de cada emplazamiento. Cada caja de aparellaje llevará su propio certificado ATEX y a ellas llegará tres cables diferentes:

-Un RG59 armado desde el servidor de video para la señal de video analógico

-Un UTP Cat-6 armado desde un distribuidor de bus de RS485 para la señal de telemetría.

-Una manguera de 3 x 2,5 mm para la alimentación de las cámaras.

El esquema de conexionado es el que se muestra en la siguiente figura-14.

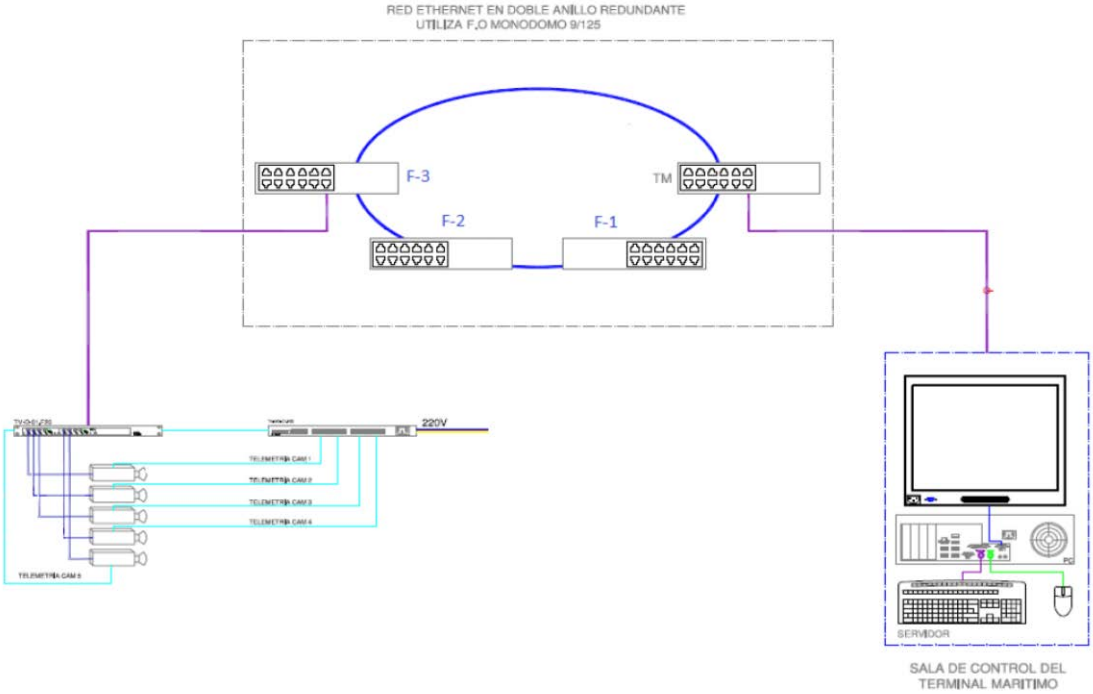



Figura-14

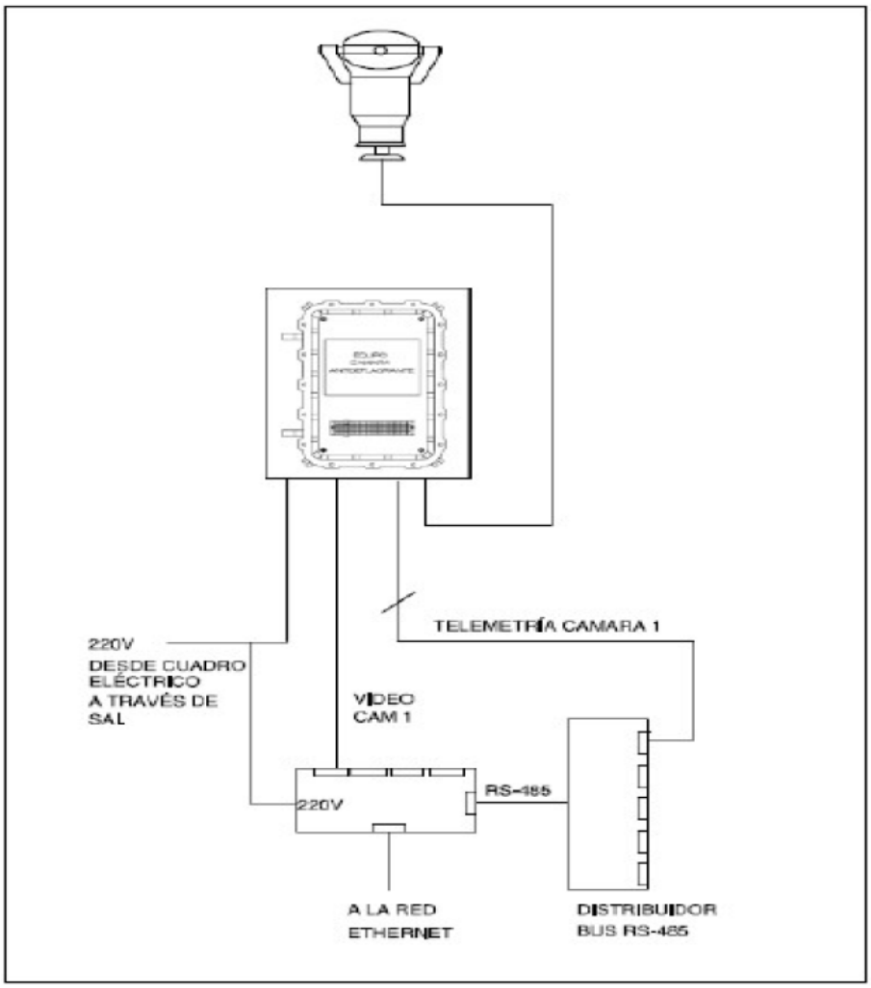



Figura-15

### 3.2.6 Equipos y Sistema de Megafonia.

Arquitectura del sistema

El sistema de megafonía prevé la transmisión de voz sobre IP utilizando equipos de la marca **Optimus** cuya información se acompaña al final de este apartado. La arquitectura del sistema es la que se muestra en el siguiente esquema:


Figura-16

El pupitre con micrófono se ubicará en la estación marítima y el mismo se alimenta a 24 V a través de un alimentador que se conecta directamente a la red de 220 V. Este pupitre tiene una conexión mediante RJ45 a un puerto del switch permitiendo de esta forma la transmisión de los datos a través de la red creada.


Figura-17

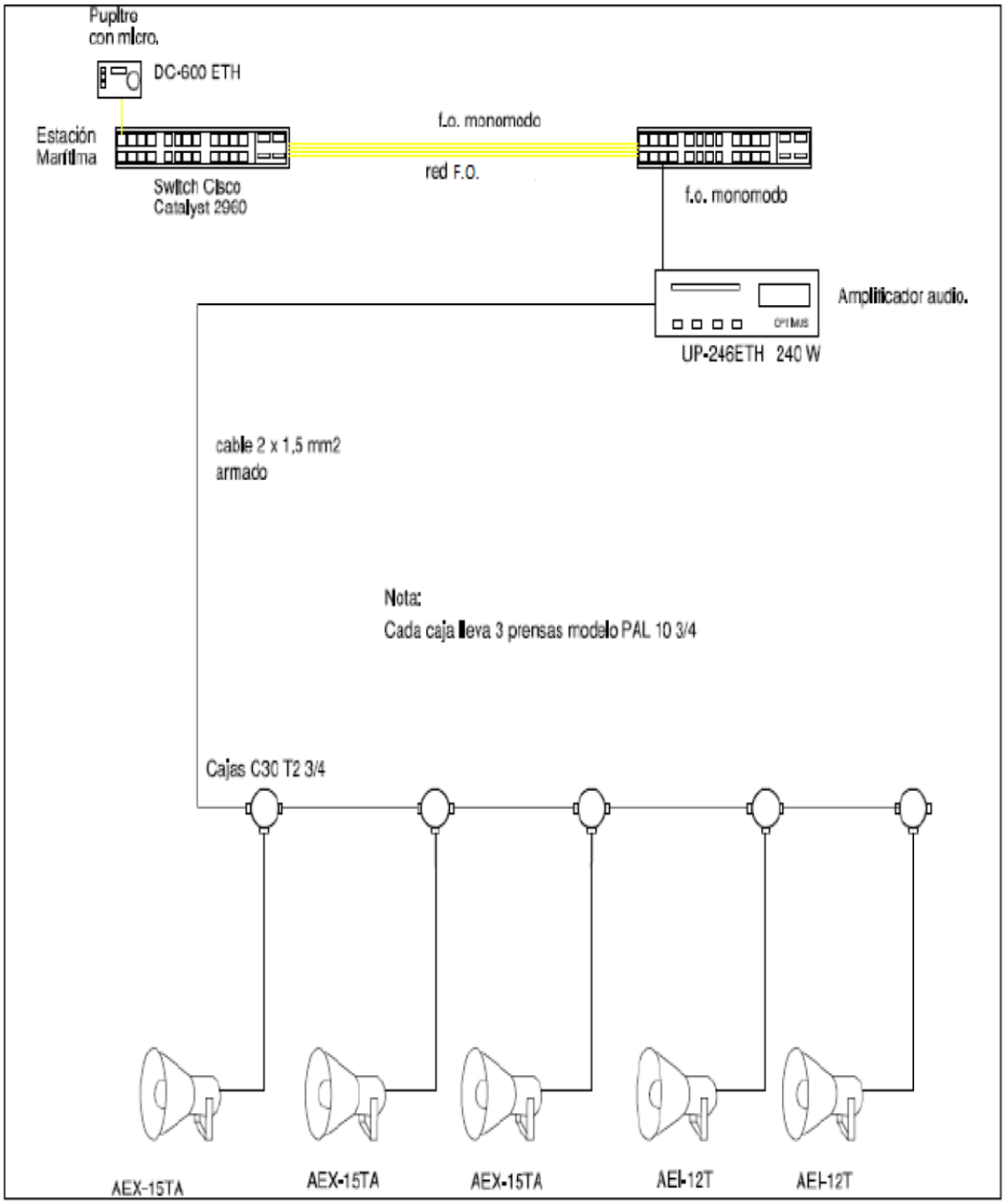



Figura-18

Por su parte, en los frentes 1, 2 y 3, se colocará en el armario de datos, el equipo amplificador que recibe a través de un puerto Ethernet los datos enviados a su dirección IP. Este amplificador, recibe los datos, los amplifica y los lleva hasta los altavoces en forma de tensión.

La instalación de los altavoces se realiza de forma serie para lo cual se utiliza una manguera de 2 hilos armada que lleva la señal de audio a cada uno de los altavoces.

Debido a la ubicación de los altavoces, se han determinado que sean ATEX (se encuentran en zona clasificada). Cada uno de ellos nunca supera la potencia de 25 W pudiéndose colocar hasta 26 de ellos sin llegar a superar la potencia del amplificador.

Zonas de influencia

Frente 1:

La ubicación y tipo de cada altavoz propuesto se resume en el párrafo siguiente:

Altavoz 1: Se ubicará en el exterior de la caseta del vigilante en la parte superior de la plataforma, en zona clasificada. Intentará cubrir toda la parte superior de la plataforma incluso la cubierta del buque. Se colocará un altavoz ATEX

Altavoz 2: Se colocará en la zona próxima a SCI y cercano a la escalera de acceso a la planta superior. Intenta cubrir toda esta zona. Se colocará un altavoz ATEX.

Altavoz 3: Se colocará en la torre de evacuación y dada la importancia de esta zona se ha decidido colocar este altavoz ATEX.

Teniendo en cuenta el nivel sonoro que existe en la zona y la potencia de los altavoces, en principio, no existen zonas muertas donde no llegue la señal de audio. En caso de que se quiera aumentar el nivel sonoro en algunas de las zonas, se pueden colocar más altavoces hasta lograr un nivel de sonido deseado, SIEMPRE SIN AUMENTAR LA POTENCIA DE LOS MISMOS, ya que en zonas ATEX la potencia de los altavoces no debe superar nunca los 25 W..

Frente 2:

La ubicación y tipo de cada altavoz propuesto se resume en el párrafo siguiente:

Altavoz 1 y 2: Se ubicará en la parte más alejada del atraque del buque, en zona no clasificada y muy cerca de la caseta de control y otro en la zona contraria y también alejado. Intentará cubrir toda la zonas de las plataformas y el acceso al frente 2. Se colocarán dos altavoces ATEX.

Altavoz 3: Se ubicará en el exterior de la caseta del vigilante en la parte superior de la plataforma, en zona clasificada. Intentará cubrir toda la parte superior de la plataforma incluso la cubierta del buque. Se colocará un altavoz ATEX

Altavoz 4 y 5: Se colocará en las zonas próxima a SCI y cercano a las escaleras de acceso a las plantas superiores. Intenta cubrir todas estas zonas. Se colocará dos altavoz ATEX.

Altavoz 6 y 7: Se colocará en la torre de evacuación y dada la importancia de esta zona se ha decidido colocar 2 altavoces ATEX.

Teniendo en cuenta el nivel sonoro que existe en la zona y la potencia de los altavoces, en principio, no existen zonas muertas donde no llegue la señal de audio. En caso de que se quiera aumentar el nivel sonoro en algunas de las zonas, se pueden colocar más altavoces hasta lograr un nivel de sonido deseado, SIEMPRE SIN AUMENTAR LA POTENCIA DE LOS MISMOS,

ya que en zonas ATEX la potencia de los altavoces no debe superar nunca los 25 W..

Frente 3:

La ubicación y tipo de cada altavoz propuesto se resume en el párrafo siguiente:

Altavoz 1: Se ubicará en la parte más alejada del atraque del buque, en zona no clasificada y muy cerca de la caseta de control. Intentará cubrir toda la zonas de la plataforma y el acceso al frente 3. Se colocará Un altavoz ATEX.

Altavoz 2: Se ubicará en el exterior de la caseta del vigilante en la parte superior de la plataforma, en zona clasificada. Intentará cubrir toda la parte superior de la plataforma incluso la cubierta del buque. Se colocará un altavoz ATEX

Altavoz 3 : Se colocará en las zonas próxima a SCI y cercano a la escalera de acceso a las planta superior. Intenta cubrir toda esta zona. Se colocará un altavoz ATEX.

Altavoz 4 y 5: Se colocará en la torre de evacuación y dada la importancia de esta zona se ha decidido colocar 2 altavoces ATEX.

Teniendo en cuenta el nivel sonoro que existe en la zona y la potencia de los altavoces, en principio, no existen zonas muertas donde no llegue la señal de audio. En caso de que se quiera aumentar el nivel sonoro en algunas de las zonas, se pueden colocar más altavoces hasta lograr un nivel de sonido deseado, SIEMPRE SIN AUMENTAR LA POTENCIA DE LOS MISMOS, ya que en zonas ATEX la potencia de los altavoces no debe superar nunca los 25 W.

### 3.2.7 Equipos y Sistema de Teléfonia.

Especificaciones del Sistema

1. Según las especificaciones del proyecto, se plantea la instalación de 4 terminales telefónicos IP para la TM y las casetas de Operadores en los Frentes 1, 2 y 3

Arquitectura del sistema

Se implementa el servicio de telefonía CALL-MANAGER para disponer del servicio de telefonía en la red interna de la Empresa, así como la salida a la red nacional de este servicio contratando dos líneas telefónicas al proveedor de telecomunicaciones que elija la empresa.

Conexionado del Teléfono

El cableado es bastante sencillo pues para la comunicación entre la estación marítima y los frentes se utiliza la fibra óptica a través de los switch ubicados en cada frente, de ahí con latiguillos de cable UTP cat6 con el teléfono IP, También facilita la comunicación con el exterior de la red interna de la Empresa

| | | | |
|---|---|---|---|
| 1 | Puerto de red (10/100 SW) | 4 | Fuente de alimentación CA-CC |
| 2 | Puerto del auricular | 5 | Cable de alimentación de CA |
| 3 | Puerto del adaptador de CC (DC48V) | | |

Figura-19

Caracteristicas:


| | Elemento | Descripción | Para obtener más información, consulte... |
|---|---|---|---|
| 1 | Pantalla del teléfono | Muestra los menús del teléfono y la actividad de las llamadas, incluida la identificación de la persona que llama, duración de la llamada y estado de la llamada. | "Menús de aplicaciones" en la página 11 e "Iconos de línea e iconos de llamada" en la página 12. |
| 2 | Serie del teléfono IP de Cisco Unified | Indica las series del modelo de su teléfono IP de Cisco Unified. | — |
| 3 | Teclas programadas | Cada una activa una opción de tecla programada en la pantalla del teléfono. | "Definición de las teclas programadas" en la página 3. |
| 4 | Botón de navegación | Permite desplazarse por los elementos de menú y seleccionar elementos. Cuando el teléfono está colgado, muestra la Marcación rápida. | "Menús de aplicaciones" en la página 11 y "Marcación rápida" en la página 25. |
| 5 | Botón del menú de aplicaciones | Muestra el menú de aplicaciones que permite acceder al sistema de mensajes de voz, registros y directorios del teléfono, configuración, servicios y ayuda. | "Menús de aplicaciones" en la página 11. |
| 6 | Botón de espera | Pone la llamada activa en espera, reanuda una llamada en espera y permite cambiar de una llamada activa a una llamada en espera. | "Utilización de la llamada en espera y reanudación" en la página 17. |
| 7 | Teclado | Permite marcar números, introducir letras y elegir elementos de menú. | "Gestión de llamadas básica" en la página 13. |
| 8 | Botón de volumen | Controla el auricular, los auriculares, el altavoz y el volumen del timbre. | "Utilización del auricular, los auriculares y el altavoz" en la página 35. |
| 9 | Auricular con banda luminosa | La banda luminosa del auricular indica una llamada entrante o un nuevo mensaje de voz. | "Acceso a los mensajes de voz" en la página 43. |
| 10 | Soporte | Permite colocar el teléfono con el ángulo adecuado en un escritorio o mesa. | — |

Figura-20

Arquitectura de telefonia IP

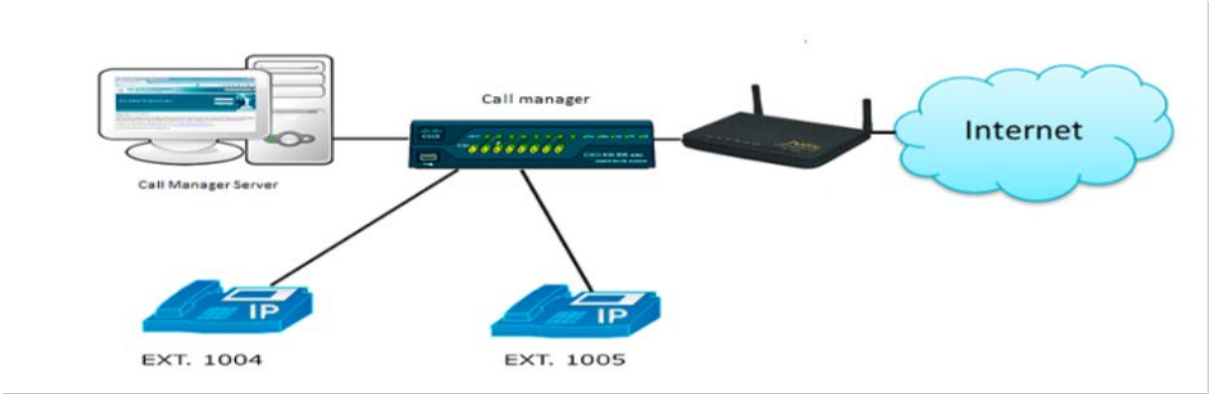



Figura-21

### 3.2.8 Equipos y Sistema de Control Distribuido.

El sistema de control distribuido, luego de varias etapas de diseño, se ha implementado teniendo como núcleo los Autómatas Programables de Schneider Modelo Modicom Quantum con alimentación y CPU redundantes.

La comunicación del PLC con el Servidor Honeywell se realiza mediante la red Ethernet tolerante a fallos en anillo simple, mediante el protocolo ModBus TCP soportado por el Modicom Quantum y ampliamente utilizado por Honeywell en sus sistemas SCADA.

Por su parte, la comunicación del PLC con los elementos de campo, se realiza también con el protocolo ModBus TCP y se implenta mediante islas Advantis ubicadas cerca de los elementos de control.

En la figura siguiente se muestra un esquema general de la arquitectura del sistema de control distribuido a instalar en los frentes 1, 2 y 3.

La estructura parte del anillo de red Ethernet de donde se conectan los PLC para la comunicación de los mismos con los SCADAs que se encuentran en la estación marítima. La comunicación de los
PLCs Modicom Quantum con los elementos de campo se realiza mediante islas Advantis unidas también por medio de un anillo redundante en fibra óptica multimodo, y ubicadas convenientemente en campo, cerca de los elementos de control, y colocadas en cajas antideflagrantes por la naturaleza de la zona donde se encuentran dichos
Equipos.

La arquitectura presenta redundancia en la CPU y en la alimentación, existiendo dos PLCs en

cada emplazamiento, de forma que ante la caída de uno de ellos, se habilita inmediatamente el segundo con un tiempo de respuesta inferior a 50 µseg. La alimentación redundante se garantiza con fuentes de alimentación independientes para cada CPU y evidentemente con protecciones independientes de forma que ante la ausencia de suministro en una de las fuentes, la otra se encuentre operativa.

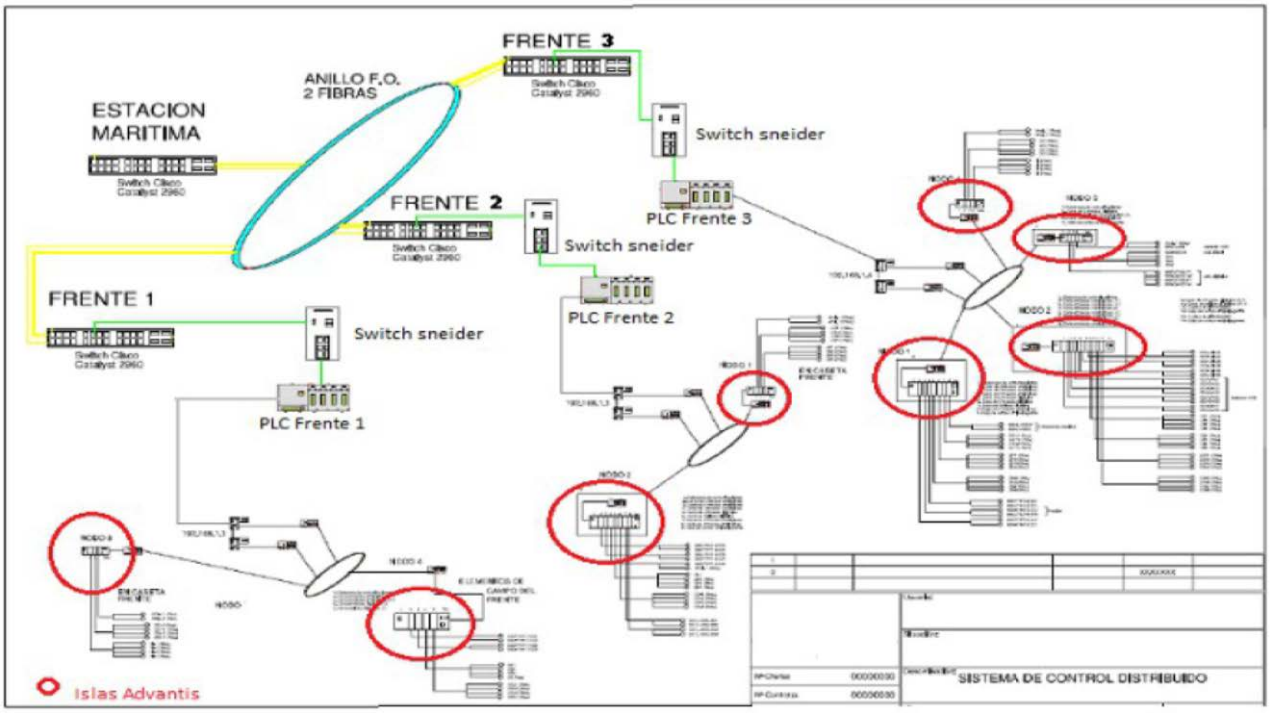



Figura-22

La selección del emplazamiento de las islas advantis se ha realizado teniendo en cuenta la proximidad con los elementos de control, la agrupación de funciones similares de dichos elementos así como facilidad del cableado.

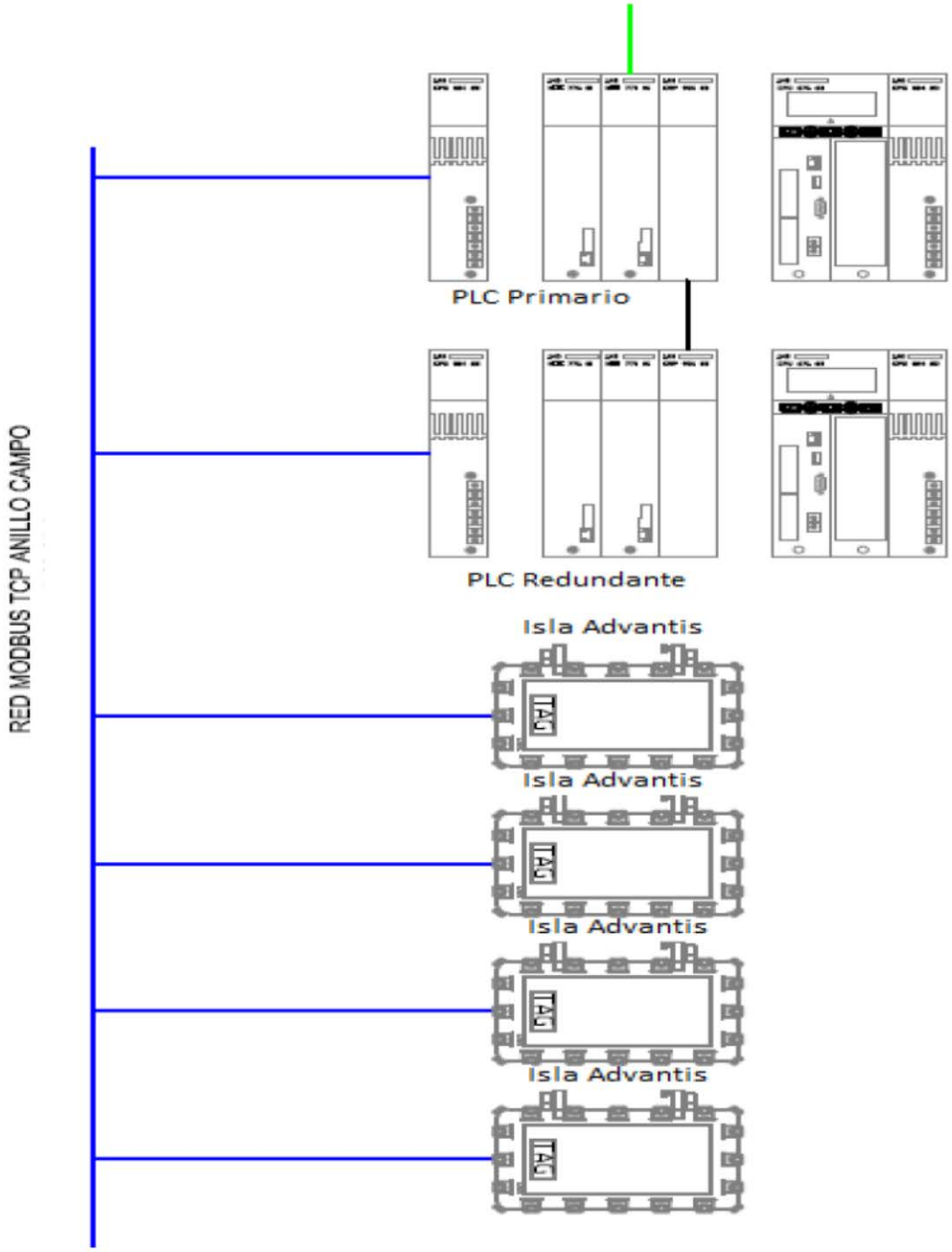



Figura-23

La ubicación definitiva de las islas o nodos es la siguiente:

Frente 1:

Posee 2 nodos o islas Advantis

Isla Advantis 1: Ubicado en el Rack del frente 1. Su objetivo es permitir el control inteligente del Rack que alberga toda la electrónica como puede ser: iluminación, temperatura, vvvv humedad, encendido de equipos, suministro eléctrico, etc. Aunque el número de entradas y

salidas digitales y analógicas puede ser ampliado, en principio dispone de 4 entradas digitales, 4 salidas digitales y 2 entradas analógicas con resolución de 16 bits.

Isla Advantis 2: Se ubicará en campo del frente 1 en su correspondiente caja antidefragante con los prensas respectivos. Posee el número de entradas necesarias para controlar 5

Transmisores de presión existentes en la zona y 4 detectores de H2S, así como algunas señales DI/DO. La ubicación física de la caja de aparellaje conteniendo la Isla Advantis es aquella que permita un cableado más eficiente desde la caja hasta cada elemento de control así como una sujeción adecuada de la misma.

Frente 2:

Posee 2 nodos o islas Advantis

Isla Advantis 1: Posee el número de entradas necesarias para controlar 5 transmisores de presión existentes en la zona y 4 detectores de H2S, así como algunas señales DI/DO. La ubicación física de la caja de aparellaje conteniendo la Isla Advantis es quella que permita un cableado más eficiente desde la caja hasta cada elemento de control.

Islas Advantis 2: Ubicado en campo, permite efectuar el control de 4 transmisores de presión existentes en el frente así como de un detector de sulfhídrico y también de una señal digital necesaria de controlar.

Frente 3:

Posee 4 nodos o islas Advantis

Isla Advantis 1: Se ubicará en campo, cercano a la zona donde se encuentran los sensores de presión y los contadores másicos. La isla se colocará en el interior de una caja ATEX desde la que sale el cableado a cada uno de los elementos de control. El objetivo de esta isla es garantizar el control del PLC sobre los 6 sensores de presión y los 2 contadores másicos. Se dejan entradas y salidas digitales auxiliares que pueden ser utilizadas para el control de los contadores másicos.

Isla Advantis 2: Se ubicará en campo, cercano a la zona de SCI y purgas. Con esta isla podemos controlar los detectores de gas ubicados por la zona así como los detectores de llama. Suministra además entradas y salidas digitales que pueden ser usadas en el control de dichos sensores.

Isla Advantis 3: Se ubicará en Rack, situado en la caseta del vigilante situada en la parte superior. Contiene de la plataforma las tarjetas necesarias para el control de las señales DI/DO. Al ser zona clasificada, se ubicará en caja de aparellaje antideflagrante en el interior de la caseta.

Isla Advantis 4: Ubicado en el armario existente en el frente 3.

Tiene la misma función que los nodos 1 y 2 del frente 2.

La comunicación del PLC con sus islas respectivas se realiza mediante el protocolo ModBus TCP soportado por los PLC Modicom Quantum de Schneider. En cada isla existe una cabecera de comunicaciones que es la encargada de la comunicación con su PLC la cual soporta el protocolo ModBus TCP. El medio físico utilizado para la comunicación de las islas con el PLC es fibra óptica ajustada multimodo cuyas características se detallan más adelante.

Estructura de las islas

La estructura general de una isla Advantis es la siguiente:

a) Módulo comunicador modelo STB NIP 2212 : Se encarga de la comunicación mediante ModBus TCP con el PLC a través de f.o. multimodo.

b) Módulo de alimentación interna modelo STB PDT 3100K: Suministra la alimentación interna de todos los módulos que integran la isla.

c) Módulo de entradas digitales modelo STB DDI 3425K que permite la entrada de hasta 4 señales digitales entre 0 y 24 V proveniente de dispositivos externos.

d) Módulo de salidas digitales modelo STB DDO 3410 el cual suministra 4 salidas digitales entre 0 y 24 V entre cuyos terminales de salida se coloca un relé de 24 V para el envío de señales de 0 o 24 V a dispositivos externos.

e) Módulo de entradas analógicas modelo STB ACI 1225K el cual suministra 2 canales de entrada para señales de 0 a 20 mA con una resolución de 16 bits por canal.

f) Switch gestionable de 4 puertos (2 RJ45 y 2 FO multi) para la creación del anillo interior tolerante a fallos

Distribución de Tarjetas en Rack de Islas Advantis:

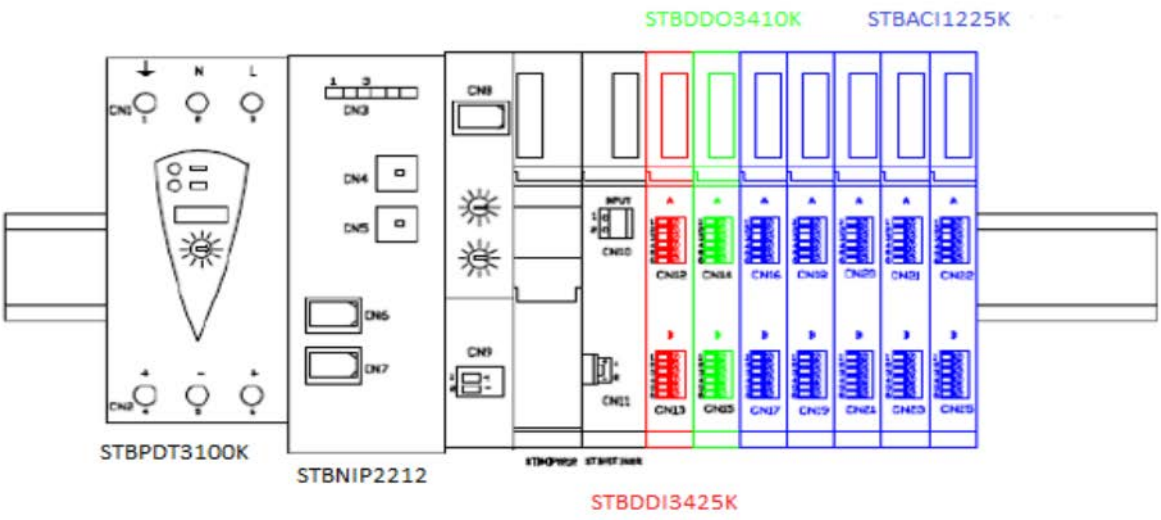



Figura-24

### 3.2.9 Equipos y Sistema Central PackScan de Rotork.

El alcance de este proyecto, consiste en realizar el cableado de las válvulas motorizadas y la colocación en el armario rack de la central PakScan así como suministrar las tensiones de alimentación y el medio físico para el transporte de las diferentes señales comunicadas.

El equipo a instalar en el frente 3 y 2 es el Modelo PakScan 3 Estación Maestra la cual introduce una nueva tecnología en el tratamiento de datos y en las facilidades de acceso
remoto sobre Internet.

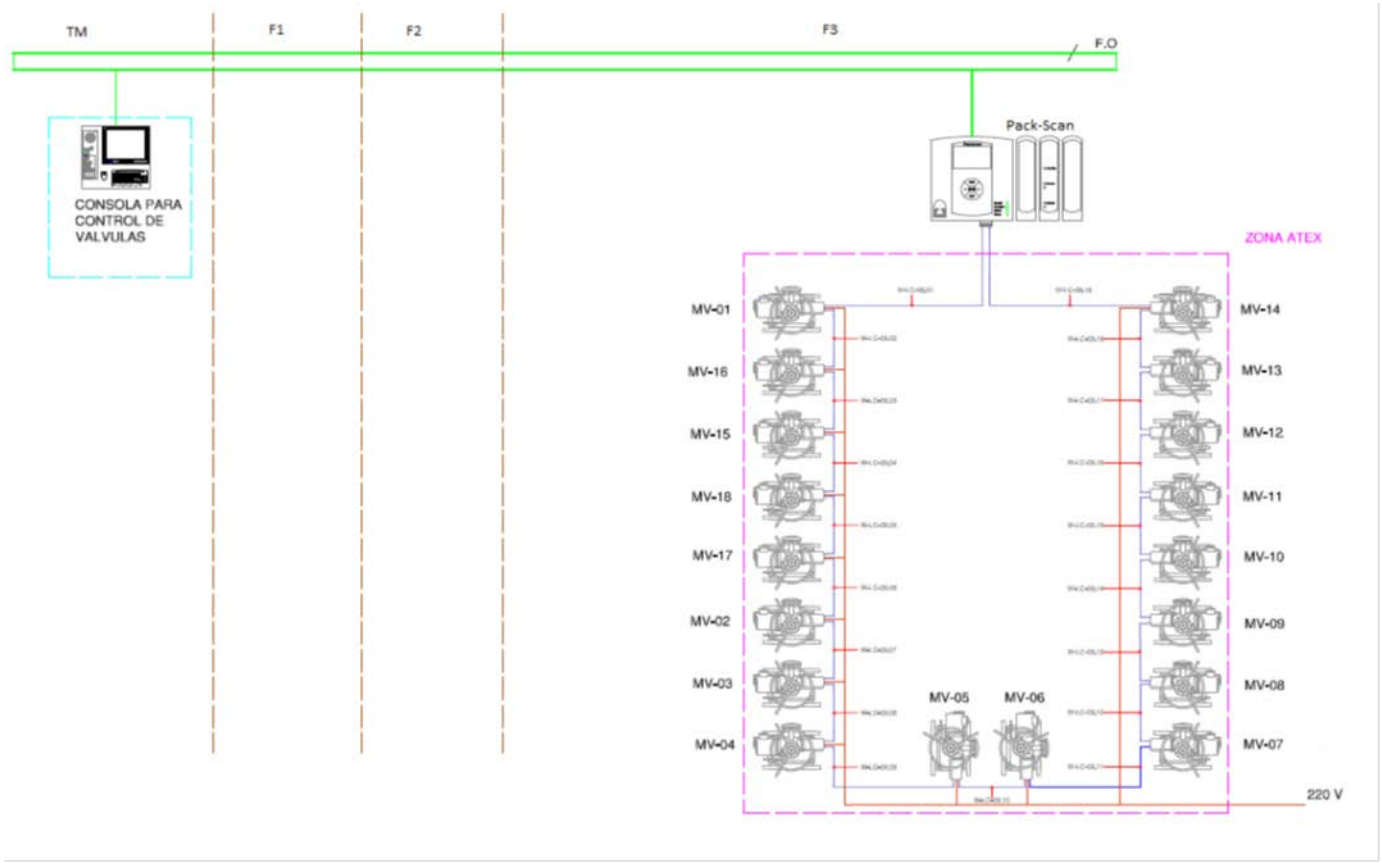



Figura-25

En la siguiente figura se muestra el esquema de la Central PakScan y una vista frontal e inferior de la misma en la que destacan todos los conectores de que dispone la misma.

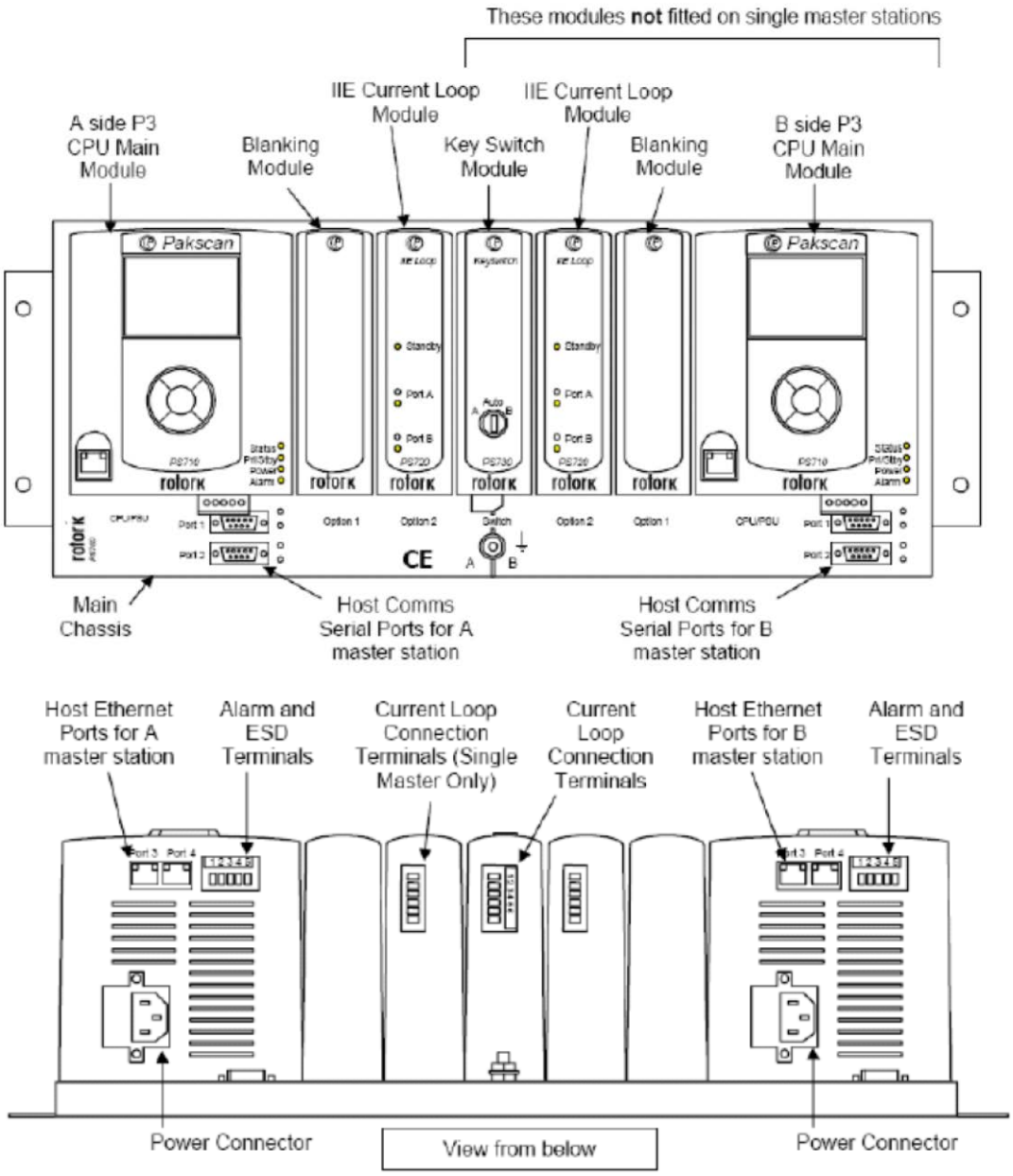



Figura-26

La central PakScan puede tener dos configuraciones diferentes:

a) P3 Hot Standby Estación Maestra que es la que se representa en esta figura

b) P3 Single Estación Maestra que es la configuración utilizada en este proyecto y es la formada por el módulo CPU y el módulo de Lazo de corriente.

La central PakScan va montada en el rack de 19 pulgadas que se encuentra en cada frente y su ubicación dentro del rack tiene que ser tal que permita una fácil visualización del panel de display de la que ella dispone.

Puertos de comunicaciones Ethernet

El módulo CPU (módulo de estación maestra), el PS710, posee por la parte inferior, dos conectores RJ45 para la comunicación con el host vía Ethernet identificados como Puerto 3 y Puerto 4.
Otro conector RJ45 se encuentra ubicado en la parte frontal del módulo y el mismo se utiliza para el diagnóstico y la programación del sistema al permitir la conexión de un portátil a este puerto.

2. Para este tipo de conexiones se pueden utilizar los cables de parcheo estándar de Ethernet.
3. Conexiones del lazo de corriente
4. En la parte inferior del módulo de Lazo de corriente existe un conector con 6 terminales, en los cuales se conecta el lazo de corriente que va hasta los actuadores
5. En el lazo de corriente se pueden conectar hasta 240 actuadores, abarcando un área de 20 Km. Por ejemplo en el frente 3 tenemos 15 actuadores y el área no supera los 300 m.

La resistencia y capacitancia del lazo no debe exceder de los valores permitidos para cada una de las velocidades de transmisión de datos. Así pues para una velocidad de 2400 Baudios, la Resistencia de los dos núcleos del cable no deben superar los 500 Ohmios y la capacitancia debe ser como máximo de 0,3 microfaradios.

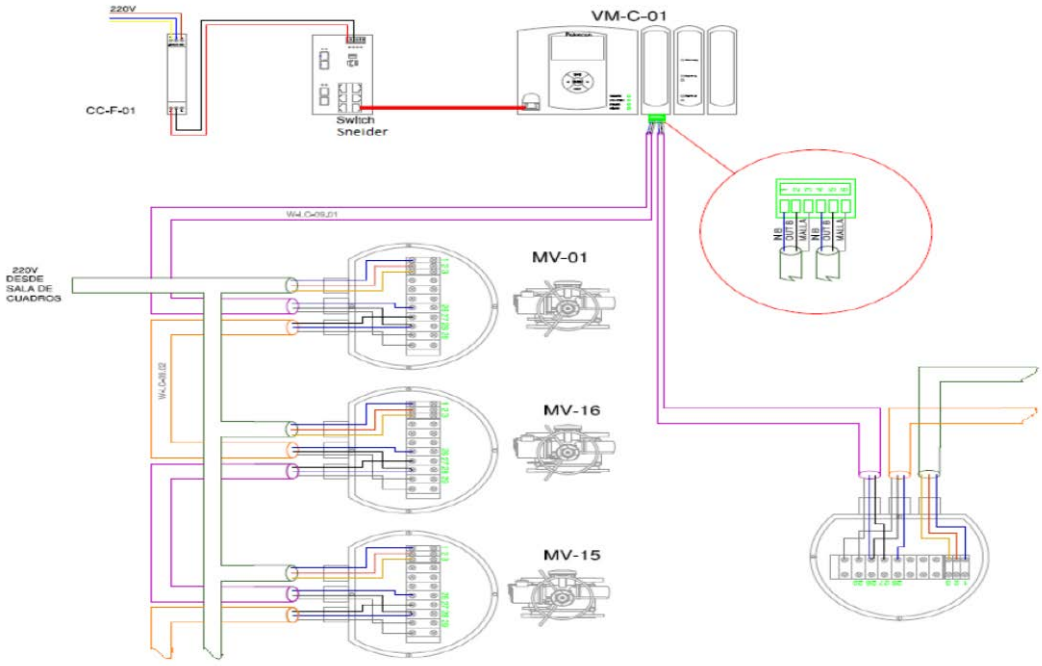



Figura-27

Los pines relacionados en cada actuador son los siguientes:
Observando la figura anterior podemos indicar que:

1.- El cable a utilizar para realizar el cableado del lazo de corriente es un cable trenzado, apantallado y armado de 2 conductores de 1,5 mm2

2.- El lazo se establece entre los terminales del 1 al 6 del conector existente en el Módulo de Lazo de Corriente.

3.- La pantalla o screen del cable deberá conectarse a tierra en un solo punto del lazo.

Los actuadores IQ e IQT de RotorK

Los actuadores existentes en los frentes a ser controlados por la PakScan son del modelo IQ de Rotork.
Estos actuadores necesitan tensión de alimentación de 220V a suministrar por otros y la señal del lazo de corriente proveniente de la central PakScan.

Los pines de la caja de conexiones del actuador entre los que se conectan el cable del lazo de corriente son los siguientes:

Pin 26 . Entrada al actuador
Pin 27 . Salida del actuador
Pin 28 . Común del actuador
Pin 29 . Malla

Todos los actuadores se conectan en un lazo de corriente, de forma serie, y la comunicación de ellos con la central se realiza mediante un protocolo propietario de RotorK en el que por defecto, la velocidad de comunicación es de 1200 Baudios y la misma depende de la resistencia y capacitancia del lazo que a su vez dependen de la longitud del lazo y de la cantidad de elementos conectados al mismo.

### 3.2.10 Equipos y Sistema de Extinción de Incendio Moec.

Los monitores de extinción de incendio son comandados a partir de unas consolas construidas por MOEC que suministra los interfaces necesarios para el control de dichos monitores.

La actuación sobre los monitores puede realizarse desde 4 puntos diferentes dentro del muelle, los cuales son: desde la estación marítima, desde los propios frentes. Por ello en cada una de estas ubicaciones existe una consola desde la cual podemos dar las órdenes a los monitores. Esta consola se comunica vía Ethernet con la controladora de los monitores ubicada en cada frente y que es la encargada de actuar directamente con los monitores.

Como puede observarse en el esquema general de conexionado, las consolas existentes en los diferentes puntos del muelle se conectan al anillo Ethernet de Seguridad por donde viajan los comandos hasta el interface de control de los monitores. En el caso del frente 2, la ubicación de la consola es en el morro del muelle y por tanto hay que llevar la señal Ethernet hasta el switch que se encuentra en el rack ubicado en la caseta del frente 2. Como la distancia entre ambos puntos es de unos 300 m aproximadamente se decidió el empleo de fibra óptica de 4 conductores del tipo multimodo para realizar esta conexión. Para la conversión de medio Ethernet a fibra óptica se emplean los convertidores de IFS modelo D7120, uno ubicado en la consola del morro y otro en el rack del frente 2. Se necesitan también pequeñas cajas de empalme de fibra para 4 conductores en cada emplazamiento.

Ubicación de los componentes y descripción de latiguillos

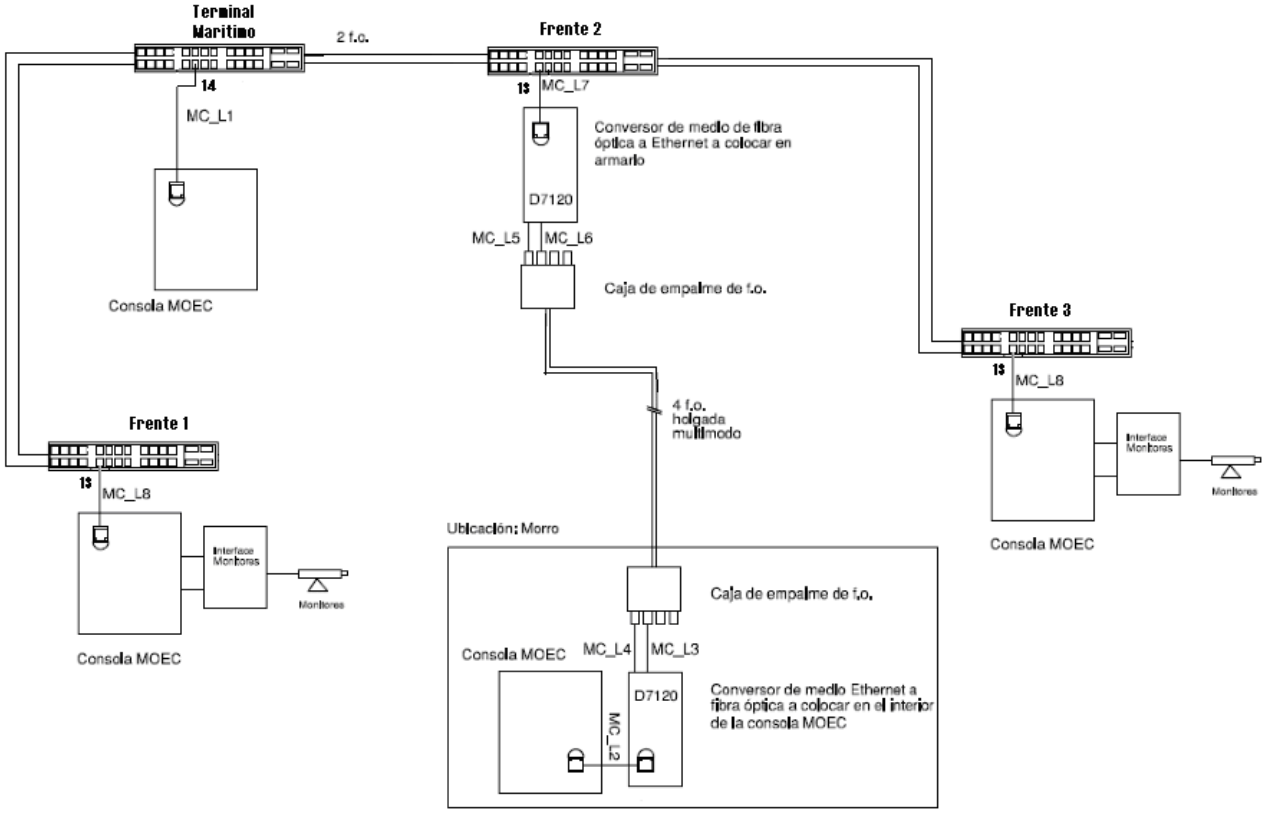



Figura-28

En el frente 1 y 3:

En esta ubicación se encuentra la consola de control de los monitores ubicados en este frente la cual puede recibir comando de forma local remota a través de la red Ethernet de Seguridad. Por tanto, es necesario la conexión de la consola a la Red lo cual consiste en conectar con un latiguillo de parcheo con conector RJ45, el interface Ethernet ubicado en la consola y al puerto correspondiente de la VLAN20 del Switch-Cisco ubicado en el rack de datos.

La longitud de este latiguillo no debe superar los 5 m lo que condiciona que la consola de control de los monitores se sitúe a menos de 5 metros del rack de datos.

El cable a utilizar para este latiguillo deberá ser UTP Cat5 armado y en el extremo irá conectado en la consola MOEC, y deberá llevar prensaestopas.

En el frente 2:

La consola de Moec se coloca en el Morro del muelle a unos 300m aproximadamente del rack de comunicaciones.

El interface que suministra la consola Moec es Ethernet debiéndose conectar ésta con el puerto correspondiente de la VLAND20 del Switch-Cisco el cual forma el anillo de comunicaciones que se encuentra en el rack. Debido a la distancia a que se encuentra el switch y a las condiciones de la instalación, se decidió unir ambos puntos mediante fibra óptica para lo que se necesitan los conversores de medio y las cajas de empalme descritas en el esquema de conexionado.

En la consola MOEC se colocarán un conversor de medio D7120 referenciado como CMC_02 y caja de empalme de fibra para cuatro conductores referenciada como CEFO_4C_02. Por su parte en el rack de comunicaciones se colocará el otro conversor de medio referenciado como CMC_01 y la caja de empalme referenciada como CEFO_4C_01.

La fibra óptica utilizada es una fibra multimodo de 62,5 con 4 conductores libre de halógenos y resistente a hidrocarburos.

Cada caja de empalme necesita 4 pasamuros SC-SC para fibra de 62,5 y 4 pigtails SC para fibra de 62,5.

La unión de las cajas de empalme con los conversores de medio se realiza mediante los latiguillos MC_L3, MC_L4, MC_L5 y MC_L6 los cuales son latiguillos de parcheo SC-SC para fibra de 62,5.

También se necesita llevar la alimentación de 220V hasta la consola ubicada en el morro para lo que se utiliza cable de 3 x 2,5 mm2 que se toma de la zona de alimentación segura en el rack del frente 2. Este cable se referencia como CRED_01

En la estación marítima:

Aquí también existe una consola MOEC desde la que podemos maniobrar los monitores contra incendio. La comunicación de esta consola, como en los casos anteriores, se realiza sobre la red Ethernet en anillo y la misma posee un conector RJ45 como interface de conexión a dicha red.

Por tanto, se hace necesario unir mediante latiguillo el interface Ethernet de la consola con el puerto 14 de la VLAND2 de Switch-Cisco del rack de comunicaciones. Este latiguillo será de 5 m con lo que la distancia entre la consola y el switch no deberá superar esta distancia.

## 3.3 Instrumentos de Medición

Los instrumentos de medición existentes en el proyecto y sobre los que se efectúa el control distribuido son los siguientes:

1. Transmisores de Presión
2. Detectores de H2S (sulfhídrico)
3. Contadores másicos de fuel oil y gas oil
4. Señales digitales de entrada
5. Señales digitales de salida.

En este capítulo se indicarán las características principales de los sensores e instrumentos de medida que serán necesarios controlar mediante el sistema de control distribuido.

### 3.3.1 Transmisores de Presión

Características del sensor:

El modelo de transmisor de presión es el STG94l-E1G-00000DE,SM,TC,MB,3D+XXXX.

La serie ST3000 de transmisores de presión pueden sustituir cualquier transmisor que se esté utilizando actualmente cuya salida sea en el formato de 4 a 20 mA y trabaja sobre el estándar de dos conductores. El sistema de medida se basa en un sensor piezorresistivo que contiene 3 sensores en uno solo: Contiene un sensor de presión diferencial, un sensor de temperatura y un sensor de presión estática.

Su tecnología microprocesada garantiza una gran fiabilidad en la medida y una mejora en la compensación de la temperatura y la presión.

El cuerpo metálico donde se aloja la electrónica y los sensores, lo hace resistente a las vibraciones, impactos y a la corrosión y también garantiza su uso en zonas clasificadas.

Las características principales del modelo seleccionado son:

-Presión de trabajo máxima permisible: 35 bares -Exactitud en modo digital de 0.0625% y en modo analógico

de 0.075%. -Estabilidad de 0.015% de URL al año. -Salida: Dos hilos: Señal analógica de 4 a 20 mA -Acepta cable de 1,5 mm de diámetro -Uso en zona clasificada ATEX -Posee adaptador para tubería NPT ½ “

### 3.3.2 Detectores de H2S.

Características del sensor:

El sensor de gas seleccionado para la aplicación es el modelo Sieger APEX de Honeywell Analitics el cual se usa típicamente en las distribuciones de gas y crudo y en las industrias químicas y de extracción de petróleo.

Este sensor funciona con un amplio rango de gases tóxicos e inflamables y su envolvente en acero inoxidable lo hace idóneo para ser colocado en sitios con condiciones climatológicas adversas o en lugares corrosivos.

Entre sus características más importantes tenemos:

-Tensión de alimentación: 24 VDC -Salidas: 4-20 mA y salidas de relé -Sistema con un menú de operación muy intuitivo -Salidas de relé para activación de alarmas sonoras -Fácil de mantener y de usar.

Las hojas de características del sensor se anexan en este documento.

### 3.3.3 Transmisores Másicos de fuel-Oil y Gas-Oil

Características del sensor:

Existen dos contadores de flujo másico en el frente 20. Uno de ellos es el encargado de medir la cantidad de fuel-oil y el otro la cantidad de gas-oil.

El sensor utilizado es el modelo RHK 100 basado en el efecto coriolis cuyas principales características son las siguientes:

-Exactitud: 0,20% -Se acopla a unidad remota modelo RHE07 (transmisor) -El transmisor RHE07 ofrece el interface de comunicación con el sistema de control distribuido.

-Rango típico de medida: 240 a 12000 kg/min

Las características más importantes del transmisor RHE 07 son las siguientes:

-Se programa en local mediante 3 botoneras

-Posee dos salidas analógicas de 0/4-20 mA para indicar flujo, densidad, temperatura o volumen galvánicamente aisladas con una carga máxima menor de 500 Ohmios.

-Salidas Digitales: 1 Salida de pulso y 3 salidas de estado (límite, error/ alarma, dirección de flujo, etc).

-Entradas Digitales: Posee dos entradas de estado: zero remoto, mantener totalizador, reset total, salir de error/alarma.

A continuación se incluyen las características del transmisor Rheonik.

RHEONIK

# RHE 07 / RHE 08 - The advanced Rheonik transmitters

Thousands of units worldwide in use. Suitable for all Rheonik mass flowmeters, with multiple functions and outputs.

## The RHE 07


## FEATURES RHE 07

- Rack mounting version
- Allows to operate flow sensor in hazardous area, optional: ATEX Approval Ex II (1) G [EEx ia] IIC or CSA 220705 - Class 1, Div 2
- 2 analog outputs (0/4 - 20/22 mA)
- 1 pulse/frequency output - 2 inputs
- Available in all common supply voltages
- Multifunctions (density, brix, concentration...)
- Version available with RS 422/485/232
- Protection class: IP 20 / Nema 1
- Power consumption: < 15 W
- Temperature range: -40 to +60°C
- NMI custody transfer approved version available (TC 3382) with double pulse output
- Batch control

## The RHE 08


## FEATURES RHE 08

- Wall mounting version
- Allows to operate flow sensor in hazardous area, optional: ATEX Approval Ex II (1) G [EEx ia] IIC or CSA 220705 - Class 1, Div 2
- 2 analog outputs (0/4 - 20/22 mA)
- 1 pulse/frequency output - 2 inputs
- Available in all common supply voltages
- Multifunctions (density, brix, concentration...)
- Version available with RS 422/485/232 HART interface
- Protection class: IP 65 / Nema 4X
- Power consumption: < 15 W
- Temperature range: -40 to +60°C
- Batch Control
- NTEP (US Weight & Measures) Approval

Figura-29

## 3.4 Configuración de Equipos y Electrónica de Red.

Configuration switches:

### 3.4.1 Switch Terminal Maritima.

```
Switch>en
Switch#conf ter
Switch(config)#vlan 10
Switch(config-vlan)#name tv_mega
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name operacion
Switch(config-vlan)#exit
Switch(config)#interface range fa0/4-9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name miscelanea
Switch(config-vlan)#exit
Switch(config)#interface range fa0/10-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range fa0/12-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

### 3.4.2 Switch Troncal.

```
Switch>en
Switch#conf ter
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit

Switch(config)#interface fa0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/3
```

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

### 3.4.3 Switch Pantalan 01.

```
Switch>en
Switch#conf ter
Switch(config)#vlan 10
Switch(config-vlan)#name tv_mega
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name operacion
Switch(config-vlan)#exit
Switch(config)#interface range fa0/4-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name miscelanea
Switch(config-vlan)#exit
Switch(config)#interface range fa0/8-9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#interface fa0/22
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range fa0/10-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

### 3.4.4 Switch Pantalan 02.

```
Switch>en
Switch#conf ter
Switch(config)#vlan 10
Switch(config-vlan)#name tv_mega
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name operacion
Switch(config-vlan)#exit
Switch(config)#interface range fa0/9-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name miscelanea
Switch(config-vlan)#exit
Switch(config)#interface range fa0/13-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#interface fa0/22
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range fa0/15-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

### 3.4.5 Switch Pantalan 03.

```
Switch>en
Switch#conf ter
Switch(config)#vlan 10
Switch(config-vlan)#name tv_mega
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-6
```

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name operacion
Switch(config-vlan)#exit
Switch(config)#interface range fa0/7-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name miscelanea
Switch(config-vlan)#exit
Switch(config)#interface range fa0/11-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#interface fa0/22
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface range fa0/13-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport voice vlan 30
Switch(config-if-range)#exit
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

### 3.4.6 Router Troncal.

```
// Levantamos la interfaz 0/0
Router>ena
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa 0/0
Router(config-if)#no shut down

//Levantamos la interfaz 0/1

Router>ena
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa 0/1
Router(config-if)#no shut down
```

```
//Configuramos los enlaces virtuales en un mismo enlace(como si hubiera 3 router`s) en el interfaz 0/0

Router(config-if)#exit
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.254 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
Router#

//Configuramos los enlaces virtuales en un mismo enlace(como si hubiera 3 routers) en el interfaz 0/1

Router(config-if)#exit
Router(config)#interface fa0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.1.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/1.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/1.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.254 255.255.255.0
Router(config-subif)#exit
Router(config)#exit
Router#

//Levantamos la interface 0/2  Salida a internet

Router(config)#interface fa0/2
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```

```
//Configuramos teléfonos IP

Router>ena
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool voice
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.254
Router(dhcp-config)#option 150 ip 192.168.3.254
Router(dhcp-config)#exit
Router(config)#telephony-service
Router(config-telephony)#max-dn 16
Router(config-telephony)#max-ephones 16
Router(config-telephony)#ip source-address 192.168.3.254 port 2000
Router(config-telephony)#auto assign 1 to 16
Router(config-telephony)#exit
Router(config)#exit

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

Router#conf ter
Router(config)#ephone-dn 1
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state
to up
Router(config-ephone-dn)#number 83001
Router(config-ephone-dn)#ephone-dn 2
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state
to up
Router(config-ephone-dn)#number 83002
Router(config-ephone-dn)#ephone-dn 3
Router(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state
to up
Router(config-ephone-dn)#number 83003
```

### 3.4.7 Configuración de listas ACL.

Las ACLs tienen como objetivo la configuración de los permisos de acceso a determinados recursos dentro de la red interna de la empresa. Hemos realizado una configuración de los permisos de acceso en función de la red especificada, por lo que la configuración de dichas ACLs es crítica para poder asegurar que dichas demandas se cumplen a la vez que reforzamos el nivel de seguridad de la red contra accesos no autorizados y ataques desde el interior y exterior.

Entre los recursos a los que restringiremos el acceso mediante ACLs, tenemos los distintos servidores que posee la red interna de la empresa.

También se bloqueará por completo el tráfico ICMP y FTP que proceda del exterior de la red privada de la empresa, ya que el permitir que este tipo de tráfico del exterior acceda a la red puede conllevar fácilmente hackeos, o robo de información crítica por parte de usuarios malintencionados para eso se le ha dotado para acceso a la red interna a través de wifi con 192.168.4.0/24.

Todos estos permisos serán configurados en el router (Troncal) que posee la red, y permitirán o denegarán el acceso a los recursos expuestos anteriormente en función de los departamentos y VLANs de donde proceda el host que realiza la petición.

La configuración es la siguiente:

CONFIGURACIÓN DE LISTAS ACL  ROUTERS TRONCAL Y DISCO DURO

```
Router>enable
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.4.0 0.0.0.255
Router(config)#access-list 10 perm
Router(config)#access-list 10 permit any
Router(config)#interface fa 0/0.10
Router(config-subif)#ip access-group 10 out
Router(config-subif)#exit
Router(config)#access-list 20 deny 192.168.4.0 0.0.0.255
Router(config)#access-list 20 permit any
Router(config)#interface fa 0/0.20
Router(config-subif)#ip access-group 20 out
Router(config-subif)#exit
Router(config)#access-list 30 deny 192.168.4.0 0.0.0.255
Router(config)#access-list 30 permit any
Router(config)#interface fa 0/0.30
Router(config-subif)#ip access-group 30 out
Router(config-subif)#exit
Router(config)#
```

### 3.4.8 Diseño Red Wifi.

La configuración de los puntos de acceso Wi-Fi (APs). Debemos tener en cuenta, que a pesar de que utilizamos un punto de acceso (necesitaremos un SSID para los visitantes y para los empleados.

**AP para Visitantes y Empleados**

El AP se ubicará en la TM, con una cobertura suficiente para toda la planta y las dirección IP será asignada de manera estática por el responsable de comunicaciones, por lo que no necesitaremos servidores DHCP. Esta IP pertenecerán a la VLAN default (192.168.4.0/24), creada especialmente para los visitantes y los empleados que quieran utilizar sus dispositivos particulares y quieran conectarse a internet y tener cobertura de datos en sus dispositivos.(sólo se permitirá el acceso a Internet).

Los datos utilizados para el acceso serán los siguientes:

SSID: TM
Cifrado: WEP
Contraseña: 1234567890

### 3.4.9 Diseño Spanning Tree Protocol.

Para garantizar una conexión constante e ininterrumpida entre los equipos, la red de empresa, se establece una serie de Switch y enlaces redundantes, de manera que ante la posible caída de un enlace siempre exista un enlace alternativo, proporcionando una alta fiabilidad.

Estos enlaces redundantes producirán bucles en nuestra red, por el motivo que dentro de todos los switch de la red de Empresa la mac más pequeña puede ser uno de ellos y no el que nos interesa para utilizarlo como **root**. Lo que necesitaremos un protocolo que sea capaz de habilitar a los switches para que estos bucles no se produzcan. Este protocolo es el Spanning Tree Protocol (STP), el cual en función de unos valores de prioridad para cada switch y para cada VLAN, desactivará ciertos enlaces de la red impidiendo la formación de los bucles antes mencionados.

El protocolo STP elegirá a un switch para cada VLAN (no tiene por qué ser el mismo para todas las VLANs) como Root Bridge, del cual colgarán el resto de switches del dominio broadcast y un switch alternativo el cuál tomará el rol de Root Bridge si el primero cae. Este switch será el

que tenga una prioridad con valor más bajo.

La configuración de las prioridades de switch Troncal para cada VLAN de manera que los Root Bridge para cada VLAN sea el siguiente:

SWITCH TRONCAL

```
Switch#conf ter
Switch(config)#spanning-tree vlan 10 root primary
Switch(config)#spanning-tree vlan 20 root primary
Switch(config)#spanning-tree vlan 30 root secondary
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch
```

# Capítulo 4: Política de Seguridad y Filtrado de Trafico.

## 4.1 Seguridad de la Red Corporativa.

Hay que considerar que la seguridad de la información no es un problema de tecnología, si no de buenas prácticas y de ética de los empleados, además del apoyo de la administración de la red de la Empresa, para la implantación del programa de seguridad.
Es recomendable que la Empresa defina un comité de Seguridad formado por un equipo multidisciplinario que sean los responsables de la creación y aprobación de todas las normas de seguridad que se barajen.
Se deben de tener en cuenta los equipos involucrados en toda la red de la Empresa. Debido que la salida a internet solamente está autorizada para empleados dentro del perfil de usuario. La red está diseñada para la utilización del personal de la empresa exclusivamente, es una red privada.
La política de seguridad de la misma excluye cualquier comunicación con la red de Empresa, a partir del Terminal Marítimo, hacia los pantalanes desde el exterior(Internet). Esta directrices estratégicas, en este contexto, son todos los valores que deben ser seguidos para que la información, que es parte muy importante para la Empresa, tenga el nivel de seguridad exigido para garantizar su privacidad con el exterior.
Muy importante para los empleados, estos estarán basados en claves de usuario, en los equipos informáticos, que no sean equipos de control de elementos relacionados con la operatividad de los pantalanes y servidores para la video vigilancia, megafonía y sistemas de control distribuidos, ya que estos están operativos las 24 horas del día 365 días al año.

Seguridad de la red corporativa:

Configuración de los sistemas operativos, acceso lógico y remoto, autenticación, internet, disciplina operativa, desarrollo de aplicaciones.
Medidas de Protección.
– Protección contra virus
– Implementación de firewalls
– Control de acceso a los recursos de la red
– Control de acceso físico.(Portátiles)
– Sistemas de vigilancia
– Detección y control de invasiones(Herramientas que analice el tránsito de red y detecte y reduzca el ataque en tiempo real)
– Políticas específicas de seguridad(ACL`s)
– Protocolo de Administración de Red Simple(SNMP)
– Clasificación de la información
– Moritoneo y gestión de la seguridad

La meta final de una respuesta rápida a una violación de seguridad, es la restauración de la operación normal de red

Para la monitorización y gestión de la red, hay en el mercado herramientas especializadas en hacer diagnosis o en analizar el rendimiento o la disponibilidad de un sistema. Además de desarrollos de protocolos específicos para determinados tipos de análisis o monitoreo.
La herramientas de diagnóstico son aquellas que nos dicen en qué estado está el dispositivo, además de decirnos si esta encendido o apagado nos puede decir si están los puertos abiertos o

cerrados, servicios activos, versión del software del S.O. Y que aplicaciones de red se están usando.
Podemos distinguir las siguientes herramientas:

**Ping**- Informa de la conectividad de un dispositivo remoto y la calidad de la conexión.
**Traceroute**- Informa lo mismo que el ping, pero da una información adicional de por cuantos routers está pasando la información.
**Netstat**- se usa de forma local, dice cuántos conexiones se tienen en este momento.
**Nmap**- Sirve para testear los puertos que tiene abiertos un equipo remoto, informando sobre servicios asociados.(Versión grafica llamada Zenmap)
**Analizadores de Protocolo**- Popular mente llamados “sniffers” Permiten analizar el tráfico en el segmento local que se encuentre.(Wireshark).
**Analizadores de vulnerabilidades**- realiza un tés remoto del sistema y averigua vulnerabilidades en ese momento. (Nessus, OpenVas)
**Monitorización activa mediante SNMP**- se analiza de forma activa los dispositivos, se obtienen mediante un sondeo repetitivo cada cierto tiempo, el mejor proceso que hace esto es el SNMP.

En nuestro sistema de monitorización utilizaremos **NetFlow**. Se trata de un protocolo patentado por Cisco y diseñado para recolección de datos del estado de la red. Se convierte en un estándar de la IETF(Internet Engieering Task Force) conocido como IPFIX (Internet Protocol Flow Información eXport) que puede consultarse en la RFC 3954.
Suele instalarse en los Routers y Switches para generar informes y puedan ser enviados a un equipo centralizado.
Su funcionamiento es el siguiente; se activa el protocolo de las interfaces de los router o Switch (tarjetas de red), pudiendo discriminas trafico entrante o saliente. Puede generar información de IP, Puertos de origen y destino, así como tipo de tráfico.
La aplicación NetFlow le permite ver representaciones visuales de los datos recopilados por la aplicación de recopilación de datos y le proporcionan un visualizador de tráfico de flujo interactivo con diagramas y tablas de uso detallado en las conversaciones y hosts que consumen el mayor nivel de ancho de banda de la red. Como GoToAssist se ofrece a petición, proporciona una visión de valor en el uso de ancho de banda en la empresa sin la complejidad y los gastos relacionados con sondeos de software y hardware de implementación. Para comenzar, simplemente instale esta aplicación y seleccione un sondeo de NetFlow en el enrutador para el Crawler, el cual actuará como selector de NetFlow (NetFlow es un protocolo de red desarrollado por Cisco Systems para recopilar información de tráfico de IPs).

## 4.2 Configurar NetFlow.

Primero debe configurar la herramienta de NetFlow para enviar datos a GoToAssist Crawler para ver los datos de NetFlow de GoToAssist. Si aún no lo ha hecho, verá el siguiente mensaje cuando abra la aplicación de NetFlow: "No se ha recopilado ningún dato de NetFlow. Si dispone de datos de NetFlow podrá visualizarlos como en la captura de pantalla siguiente".

Cómo configurar el enrutador de Cisco para exportar datos de NetFlow a GoToAssist Crawler.

1. Ejecute el siguiente comando con la dirección IP del dispositivo en la que GoToAssist Crawler se está ejecutando para exportar las entradas de caché de NetFlow a una dirección IP especificada. El Crawler escucha a NetFlow en el puerto 9996:

```
ip flow-export destination <ip address of crawler> 9996
```

2. GoToAssist Crawler comprende la versión 5 de de los paquetes de NetFlow:

```
ip flow-export version 5
```

3. De forma predeterminada, el enrutador envía información de NetFlow a GoToAssist Crawler durante flujos de larga duración cada 30 minutos. Sin embargo, puede obtener más información inmediata acerca del flujo en tiempo real mediante la división de flujos de larga duración en fragmentos de 1 minuto.

Puede elegir cualquier número de minutos entre 1 y 60. Si lo deja en el valor predeterminado de 30 minutos, los informes de tráfico tendrán picos.

Es importante establecer este valor en 1 minuto para generar alertas y ver datos detallados para solucionar posibles problemas.

```
ip flow-cache timeout active 1
```

4. Para asegurarse de que los flujos finalizados se exportan periódicamente, ejecute el siguiente comando. El valor predeterminado es de 15 segundos. Puede elegir cualquier número de segundos entre 10 y 600. Sin embargo, si selecciona un valor superior a 250 segundos, el analizador de NetFlow puede registrar niveles de tráfico niveles demasiado bajos:

```
ip flow-cache timeout inactive 15
```

5. Para establecer la persistencia de ifIndex (nombres de interfaz) de forma global, ejecute el siguiente comando. De esta forma se garantiza que los valores de ifIndex son valores que permanecen durante reinicios del dispositivo. De lo contrario, el flujo de datos puede ser incoherente después de reiniciar o invertido en comparación con valores anteriores:

```
snmp-server ifindex persist
```

6. Ejemplo de la configuración de un enrutador para enviar NetFlow a un Crawler:

```
router>enable

Password: <enable password goes here>

router#configure terminal

router(config)#interface FastEthernet 0/1
```

```
router(config-if)#ip route-cache flow

router(config-if)#exit

router(config)#ip flow-export destination
<crawler ip goes here> 9996

router(config)#ip flow-export source
FastEthernet 0/1

router(config)#ip flow-export version 5

router(config)#ip flow-cache timeout active 1

router(config)#ip flow-cache timeout inactive
15

router(config)#snmp-server ifindex persist

router(config)#^Z

router#write
```

7. NOTA: seleccione la interfaz que de la que desea realmente recopilar datos de NetFlow. Es posible que se deba a la interfaz WAN si tiene un solo enrutador entre su empresa e Internet.

8. Para ver las configuraciones, ejecute los siguientes comandos:

```
show ip flow export  y  show ip cache flow
```

## 4.3 Configurar el Crawler.

GoToAssist Crawler recopila datos de NetFlow automáticamente para dispositivos de cualquier subred que el Crawler esté supervisando. Normalmente, no se requiere ninguna configuración adicional del Crawler. Si el enrutador de NetFlow está fuera de un firewall NAT, debe añadir la subred externa del firewall a las redes que analizará el Crawler para recopilar datos de NetFlow de esa fuente. También es posible que desee añadir redes al Crawler para recopilar datos de NetFlow de otras fuentes.

Pestaña Visualizador

Puede usar la aplicación de NetFlow para ver los datos en una representación gráfica.

Cómo ver una representación gráfica de datos

1. Haga clic en la pestaña Visualizador, en la aplicación de NetFlow.

2. Realice las acciones siguientes para obtener acceso a otras opciones:

- *Desplazar el mouse*– Cuando desplaza el mouse sobre los dispositivos, verá más direcciones IP disponibles para utilizar como fuente.

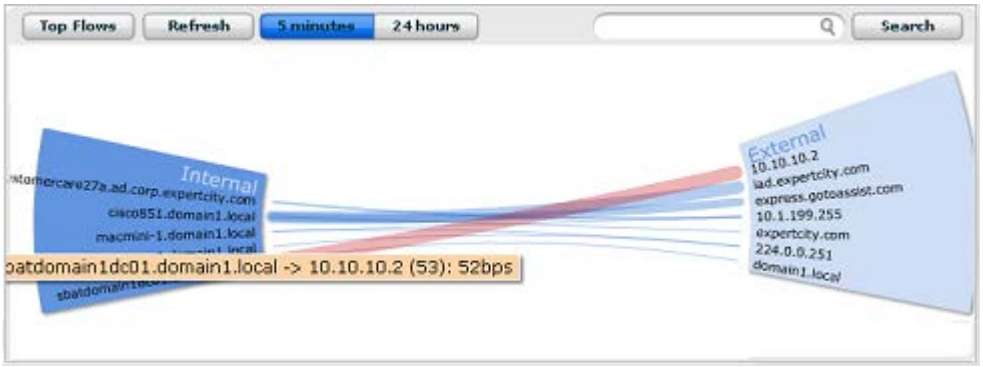



Figura-30

- *Un clic del mouse*– Al hacer clic en un dispositivo o flujo aparece un diagrama/gráfico de la historia de ese dispositivo específico.

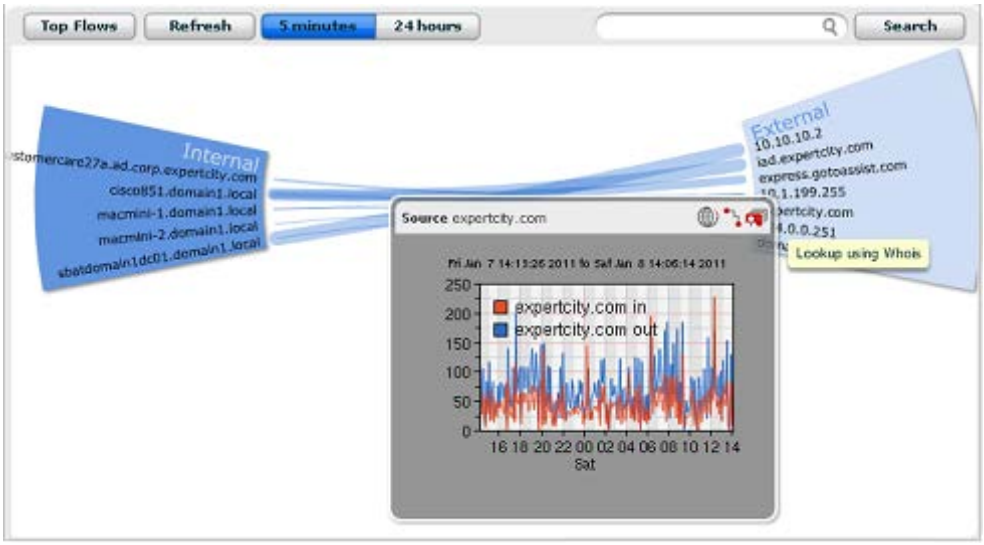



Figura-31

- *Doble clic del mouse*– Hacer doble clic en un flujo cambia la vista.

Pestaña Detalles

También se puede ver y administrar los datos de NetFlow en diagramas y en gráficos.

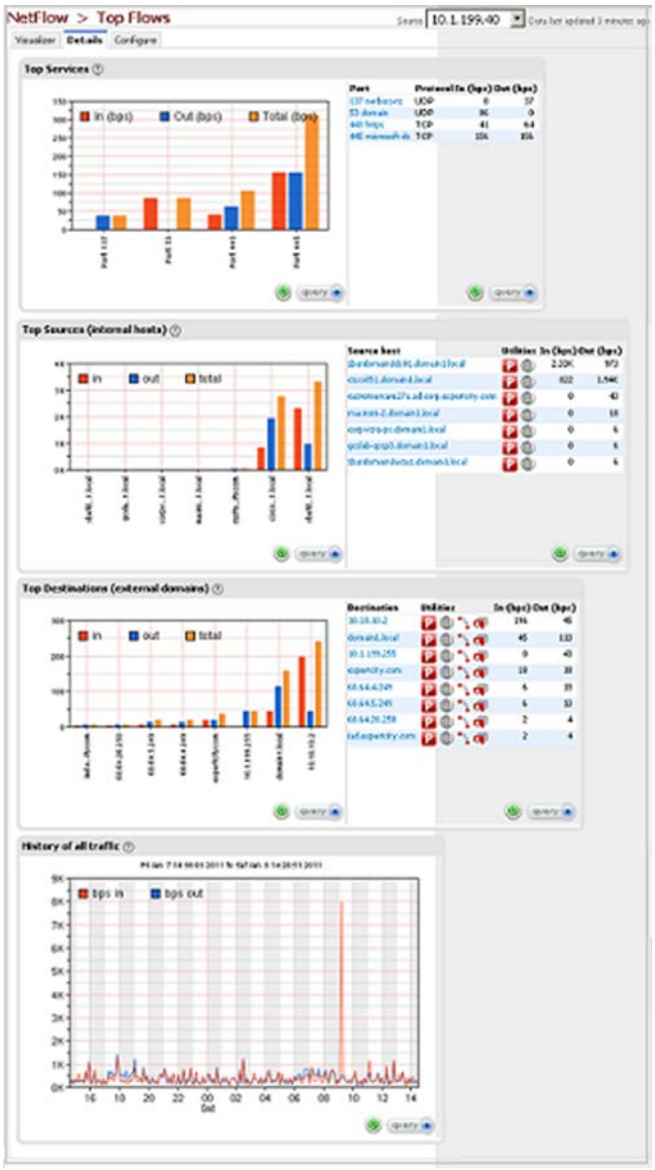



Figura-32

## Cómo administrar los datos de NetFlow en diagramas y en gráficos

1. Se hace clic en la pestaña Detalles de NetFlow.

2. Usar las siguientes opciones para manipular la vista de datos:

- *IP de origen* – Cambie la dirección IP de origen del menú desplegable para mostrar nuevos datos en el diagrama o gráfico.


- *Actualizar* – Haga clic en el botón verde Actualizar para actualizar la vista según los nuevos datos.
- *Consulta* – Haga clic en el icono de consulta para ver y modificar la consulta de los datos que se muestran o para modificar el formato de los diagramas y de los gráficos.

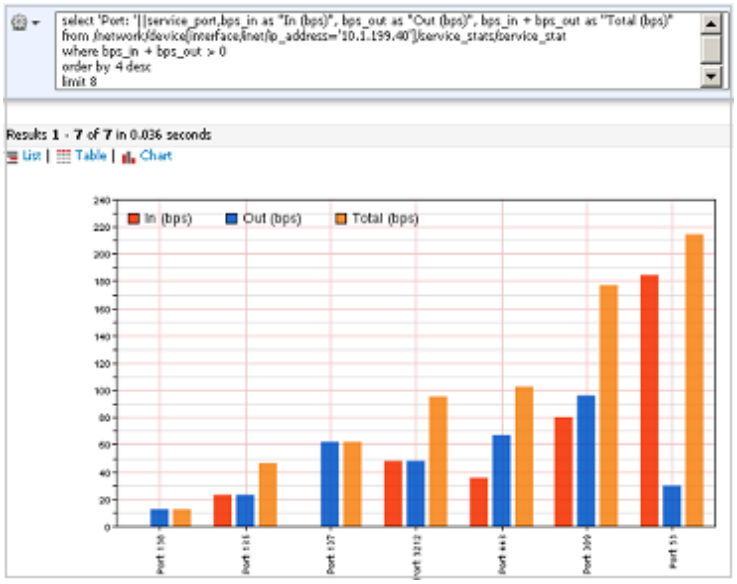
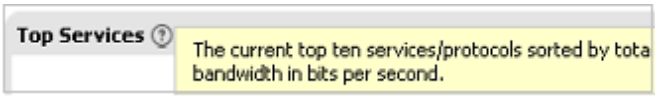



Figura-33

- *Lista* – Haga clic en el icono de una lista, tabla o diagrama para mostrar los mismos datos en un formato diferente.


- *Comunidad* – Haga clic en el icono de la comunidad para formular preguntas a la comunidad de GoToAssist.


- *Pregunta* – Desplace el mouse sobre el signo de interrogación gris para mostrar una etiqueta que describe lo que muestra el diagrama.




- *Diagrama en directo* – Haga clic en un puerto en directo o en un host de origen de los propios diagramas para obtener más detalles.

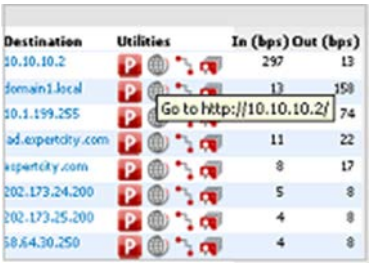



Figura-34

- *Red P* – Haga clic en una red P para abrir los resultados de búsqueda de activos, en los que puede ver detalles de datos de huellas digitales.

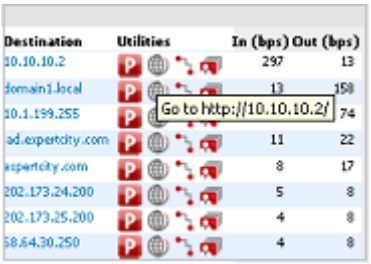



Figura-35

- *Globo*– Haga clic en el icono del globo para ver información externa.

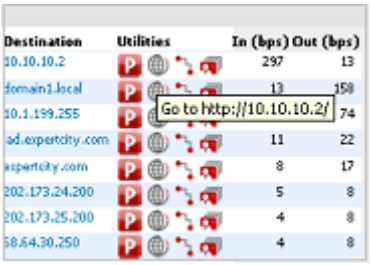



Figura-36

- *Traceroute*– Haga clic en el icono de traceroute para ejecutar un comando traceroute a la dirección IP.
- *Whois*– Haga clic en el icono de whois para realizar una búsqueda 'whois' en la dirección IP.

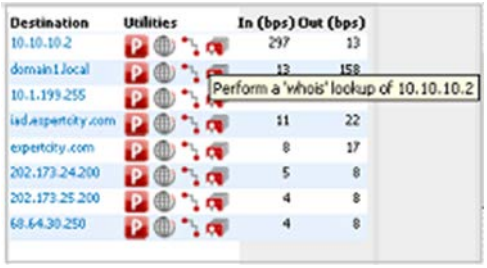



Figura-37

## Pestaña Configurar

Puede ver la cantidad de ancho de banda total de entrada/salida que están utilizando flujos específicos mediante la configuración del ancho de banda de entrada y de salida de una fuente, que a continuación muestra los porcentajes en la pestaña Detalles.

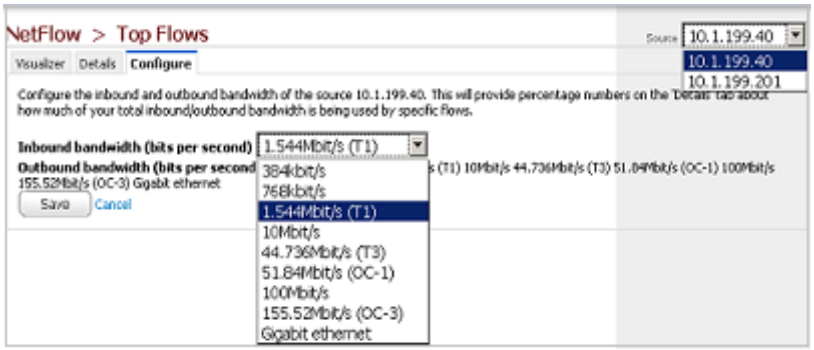



Figura-38

**Cómo configurar el ancho de banda de entrada y salida**

1. Haga clic en la pestaña Configurar de NetFlow.

2. En la casilla de verificación Fuente del margen superior derecho, elija una fuente en el menú emergente.

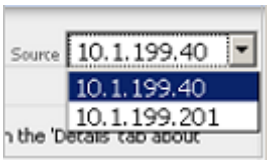



Figura-39

3. En la casilla de verificación Ancho de banda entrante, elija un ancho de banda en el menú emergente.

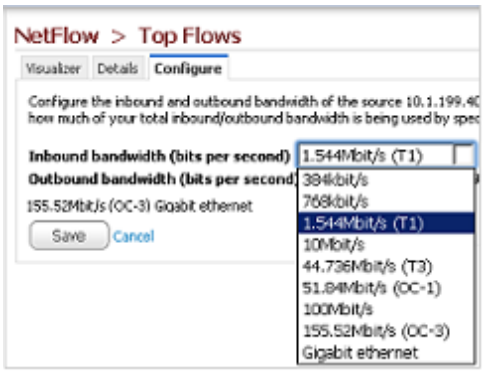



Figura-40

4. Haga clic en **Guardar** cuando haya terminado

# Capítulo 5: Diseño del Cable Estructurado de la Instalación.

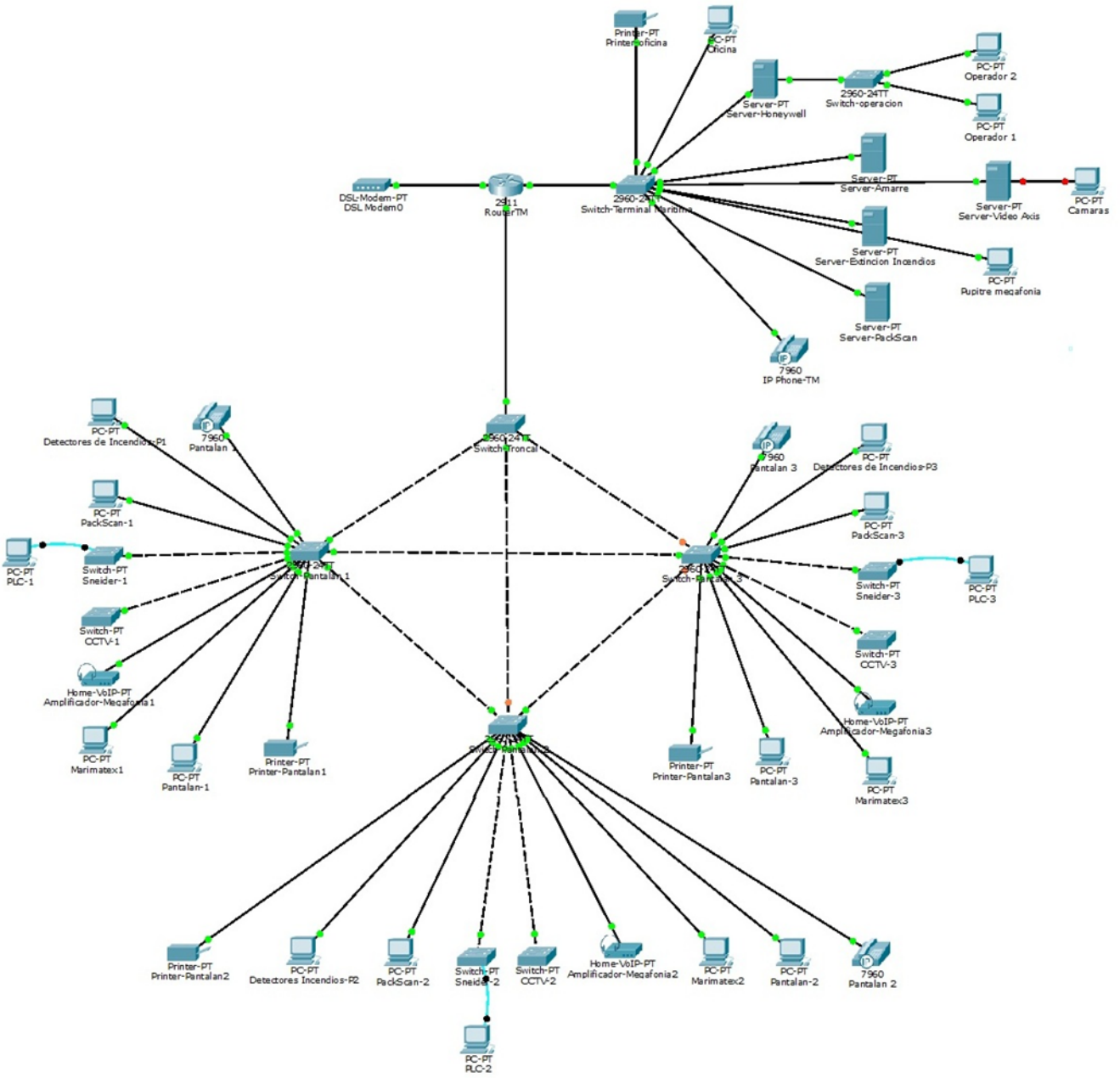



Figura-41

Todo el cableado de red desde la terminal marítima hasta el frente 3 y vuelta, pasando por cada uno de los Switch mencionados anteriormente, se realiza con una manguera de fibra óptica con 48 conductores de los cuales 32 corresponden a fibra óptica monomodo de 9 /125 micras. El resto corresponde a fibra multimodo de 62,5 /125 micras.

La manguera de fibra está formada por 6 tubos de 8 conductores cada uno. Los tubos que contienen las fibras monomodo son: Tubo Rojo, Tubo Verde, Tubo Azul y Tubo Amarillo. Los tubos gris y violeta corresponden a la fibra multimodo.

La manguera de fibra parte desde la terminal marítima hacia cada uno de los frentes hasta llegar al frente 3 y este hasta la terminal marítima en donde se cierra el lazo de red. Tanto en la Terminal Marítima como en cada Frente, la manguera de fibra llega al armario o rack de datos y mediante una caja de empalme de fibra para 48 conductores, se separa cada conductor y se brinda un punto de conexión a la misma.

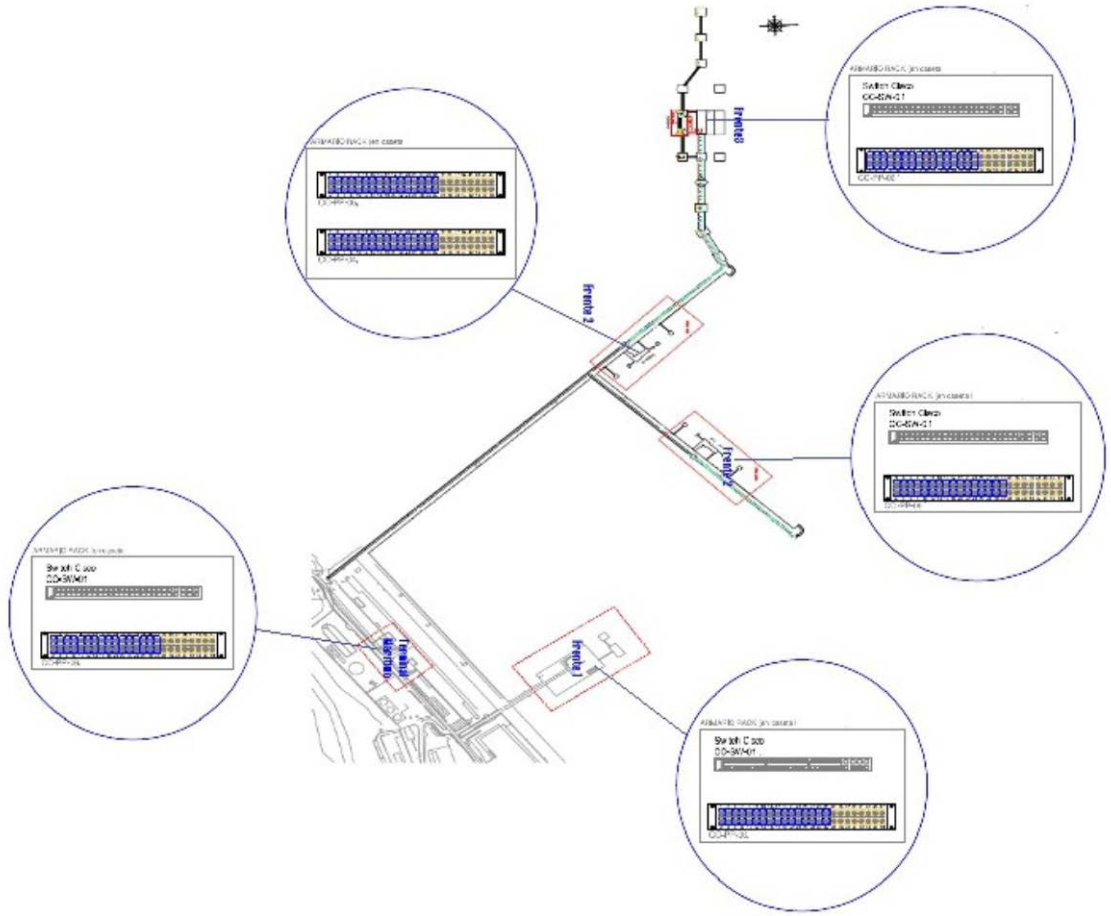



Figura-42

## 5.1 Esquema conexionado de Fibra.

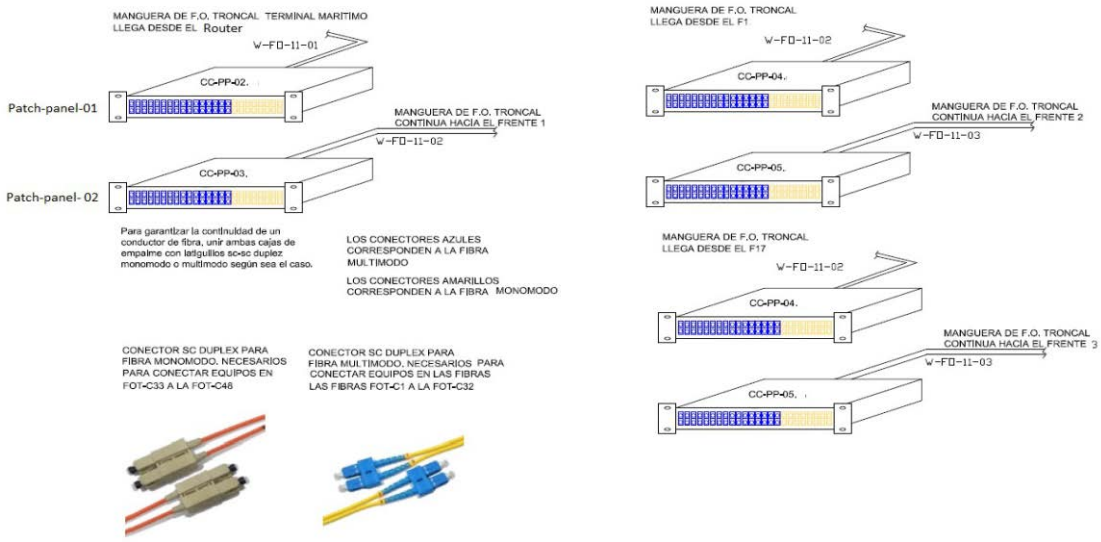



Figura-43

A continuación se muestra el esquema de conexionado de la fibra y la codificación de los conductores.

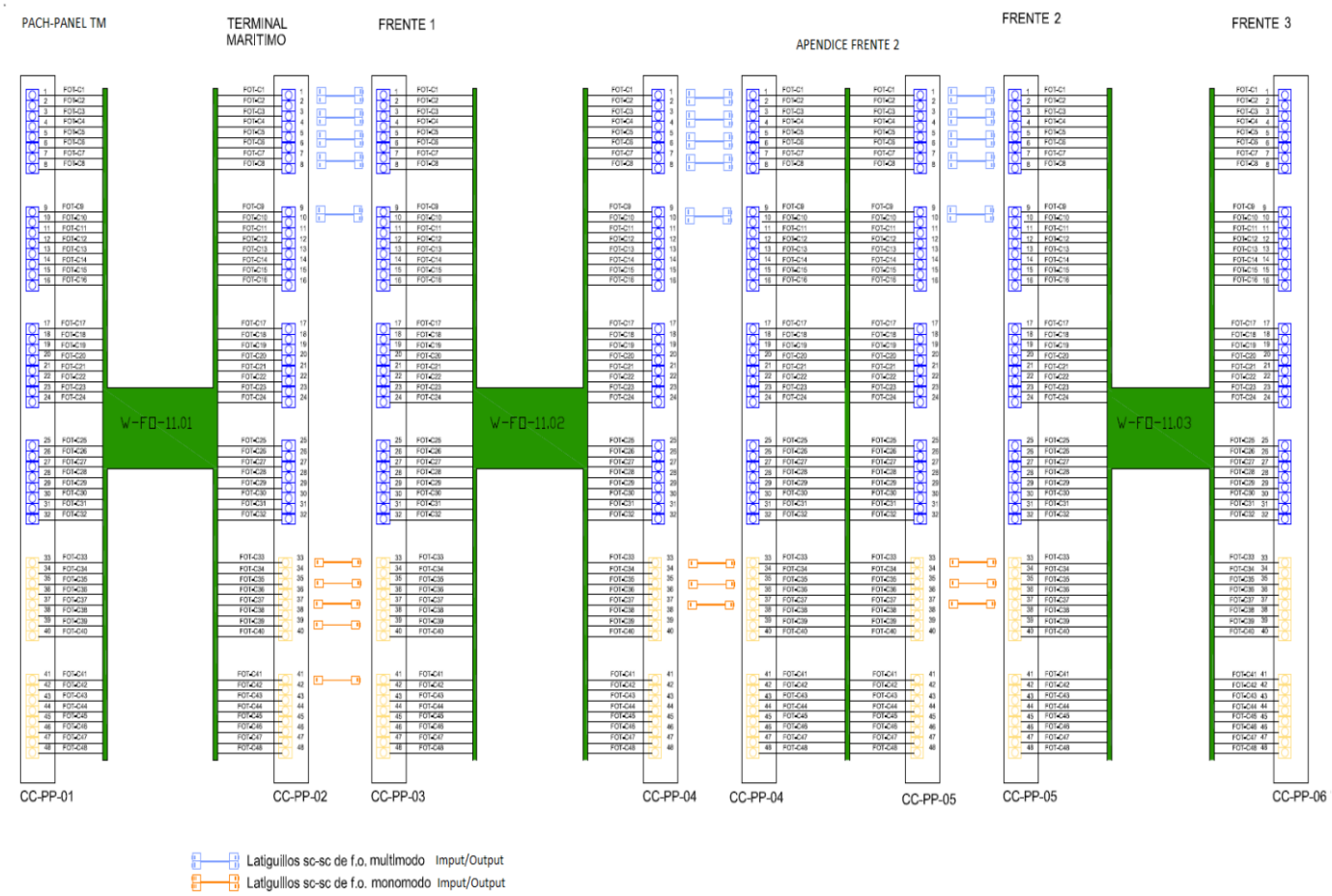



Figura-44

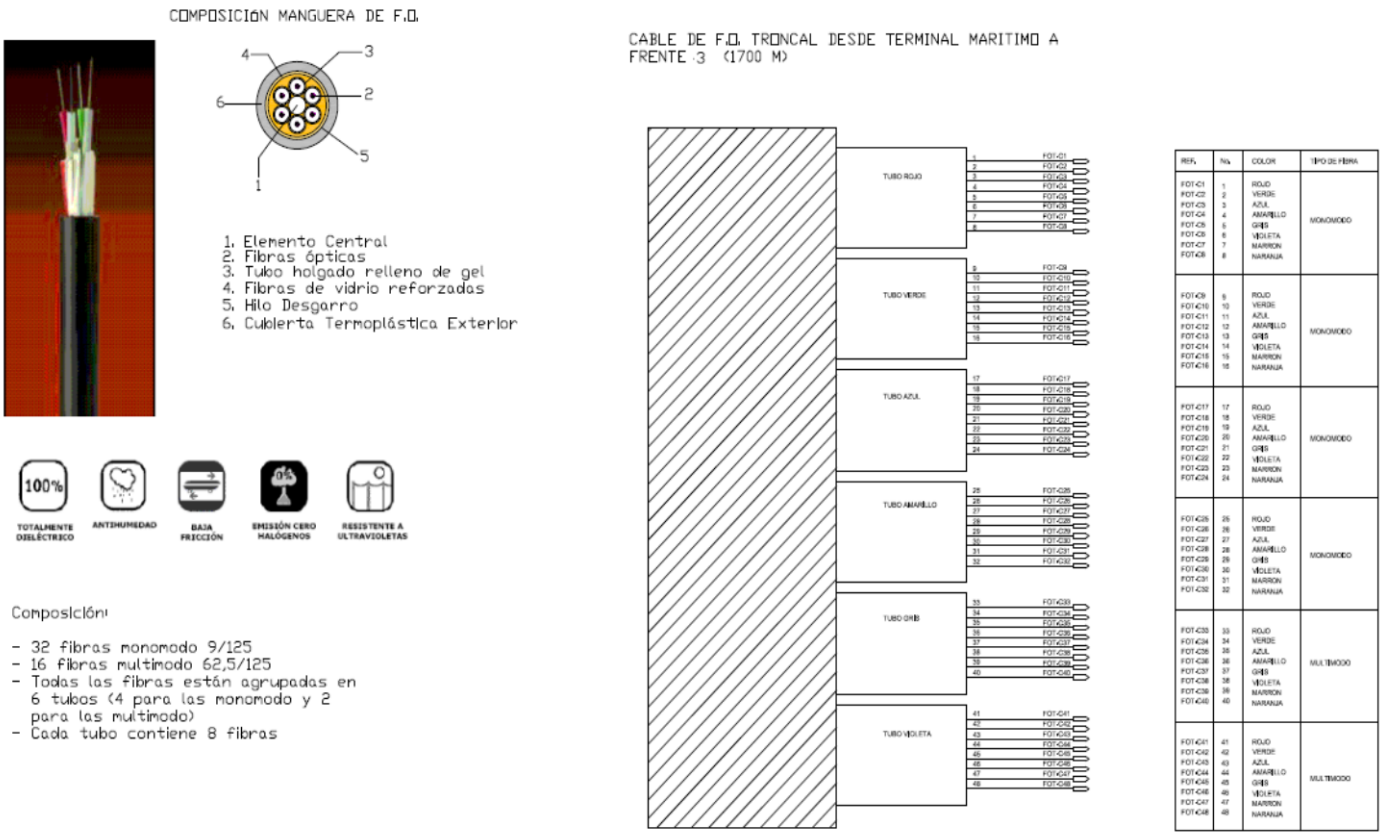



Figura-45

## 5.2 Conexionado de Patch-Panel.


Figura-46

## 5.3 Cableado de Red Industrial para Sistema de Control.

En este proyecto se implementa una red de instrumentación industrial con conectividad TCP/IP, donde es capaz de supervisar y controlar remotamente a través del protocolo

Modbus/TCP usando el sistema embebido TINI (Tiny InterNet Interface) permite a dispositivos como sensores y actuadores ser monitoreados, controlados y manejados remotamente. Estos sistemas embebidos son Fieldbus Foundation, Profibus y HART, siendo sistemas comunes en comunicaciones para instrumentación de control de procesos.

En una red de control distribuido, el protocolo Modbus/TCP puede ser usado para comunicarse con una serie de controladores o PLCs distribuidos alrededor de la planta. Esto permite a una sola persona supervisar remotamente diversos procesos simultáneamente desde una posición única.

Modbus/TCP básicamente embebe un marco MODBUS dentro de un marco TCP en una manera simple como es mostrado en la Figura siguiente.

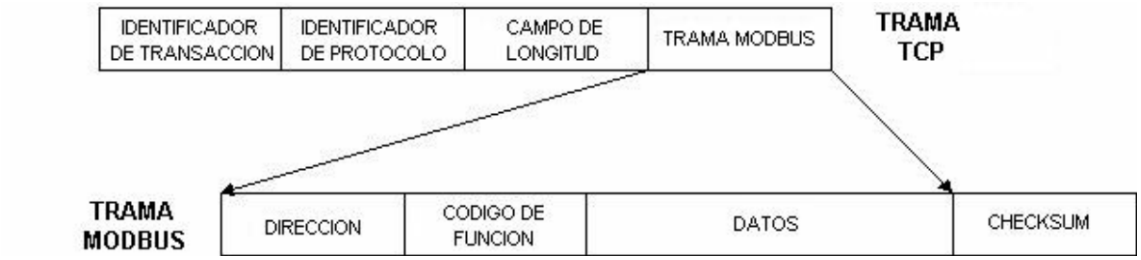



Figura-47

Pero además se podrian haber utilizado existen otros tres protocolos para el Ethernet industrial que existen en el mercado como por ejemplo lo siguiente:

EtherNet/IP (esencialmente objetos ControlNet y DeviceNet sobre TCP/IP y UDP)

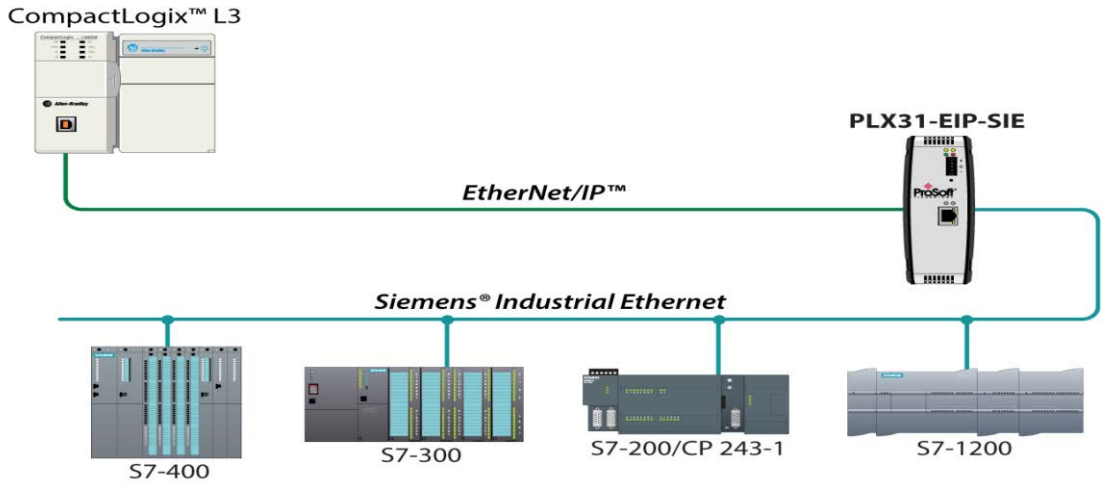


Figura-48

ProfiNet (combina el protocolo Profibus, OLE paracontrol de procesos OPC y TCP/IP).

Fieldbus Foundation high-speed Ethernet HSE (coloca el protocolo H1 de Foundation
Fieldbus sobre TCP/IP y añade OPC y el lenguaje XML).


Figura-49

Como se ha planteado para esta red la transmisión de los paquetes de datos correspondientes a las señales del Sistema de Control Distribuido, a las de la Central PakScan y al Sistema de Monitores de Extinción de Incendios de Moec, a través de la VLAN 20 del switch de cada frente.

En cada VLAN´S y conectado al switch de cada frente. Disponemos de un switch Modbus/TCP gestionable marca Schneider con dos puertos para fibra óptica monomodo 100BASE-FX que son los encargados de conformar el anillo Inferior y poseen también 6 puertos 10/100 BASE-TX con conector RJ45 para la conexión de los diferentes elementos de red. Estos switches van ubicados dentro de los armarios de datos existentes en cada emplazamiento, en carril DIN y se alimentan mediante una fuente de alimentación que toma el suministro del cuadro general mediante el SAI.

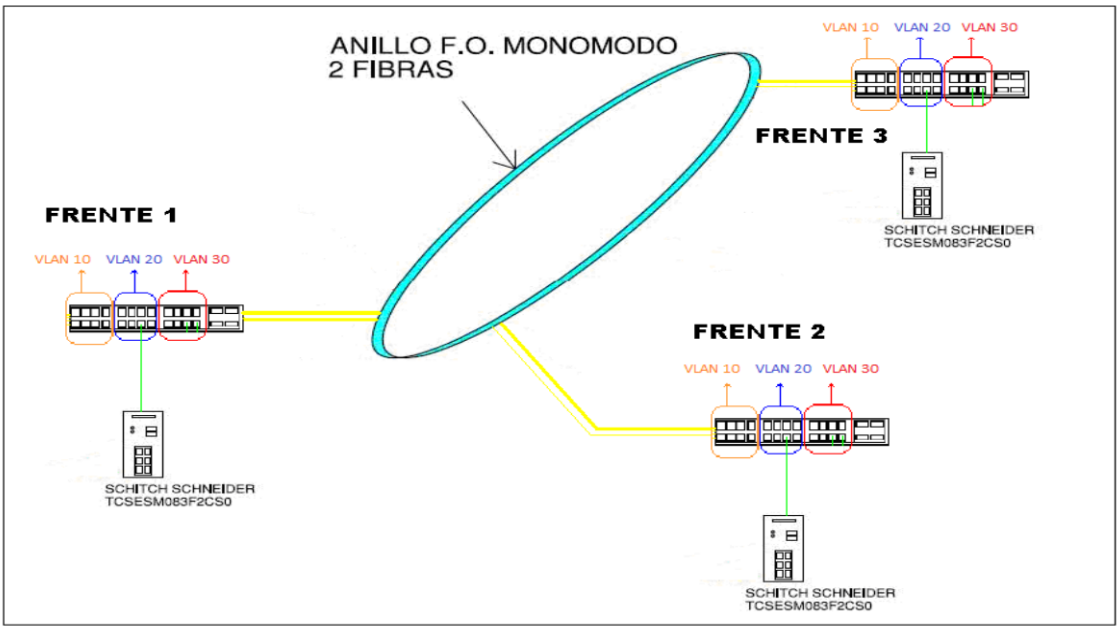



Figura-50

Cableado del anillo exterior

El anillo exterior se forma utilizando la manguera de fibra óptica de 48 conductores, de los cuales se utilizan dos fibras monomodo de 9/125 µm. Este anillo enlaza los 4 switches gestionables que forman la red Ethernet para control industrial

Cableado del anillo interior

El anillo interior se forma enlazando los puertos de fibra óptica de los switches gestionables que se encuentran en cada una de las islas Advantis. Para realizar este anillo se utiliza fibra óptica multimodo ajustada de 4 conductores.

Las uniones de los switches con los dispositivos de red (PLCs, cabeceras, etc), se realiza con latiguillos de red de longitud adecuada. Se ha decidido utilizar dos fibras multimodo de 62,5 /125 µm para unir los nodos.

Cableado de los elementos de campo

Los elementos de campo existentes (Sensores de presión, contadores másicos, detectores de sulfhídrico y detectores de llama) utilizan señales de 0 a 20 mA para indicar el nivel de medida en cada momento. Estas señales tienen que llegar a los módulos de entradas analógicas de las islas advantis y se hace mediante un cable de dos hilos de 1,5 mm2 de sección debidamente apantallado. Este cable entra a las cajas de aparellaje mediante los prensa correspondientes.

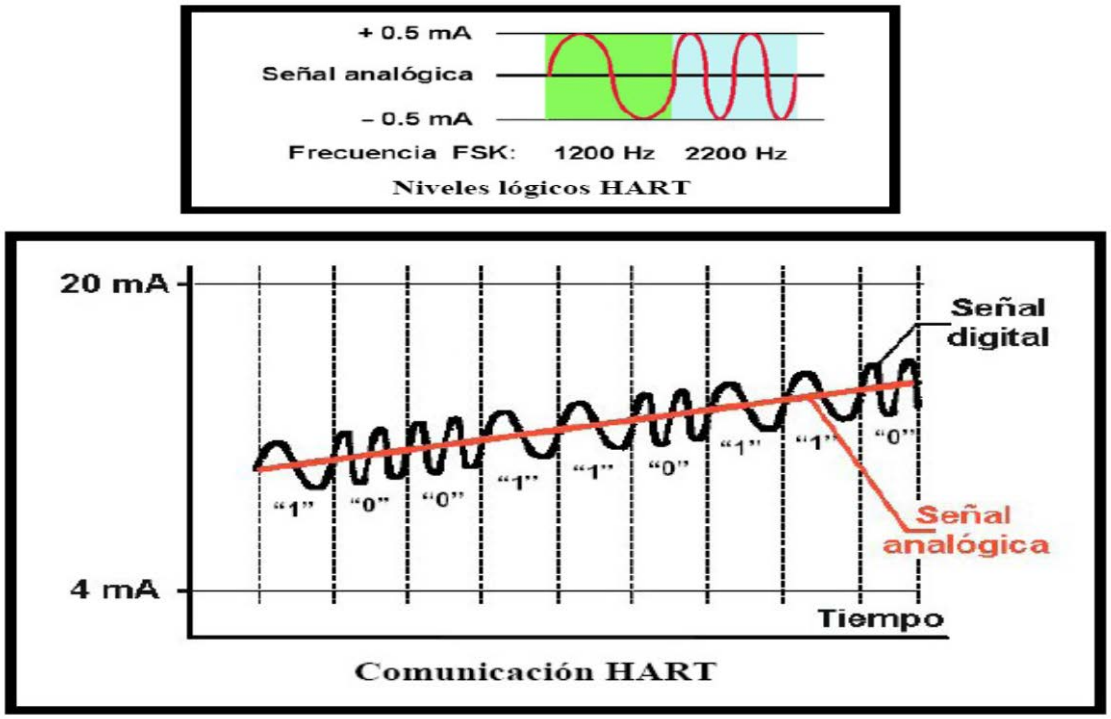



Figura-51

## 5.4 Cableado de CCTV.

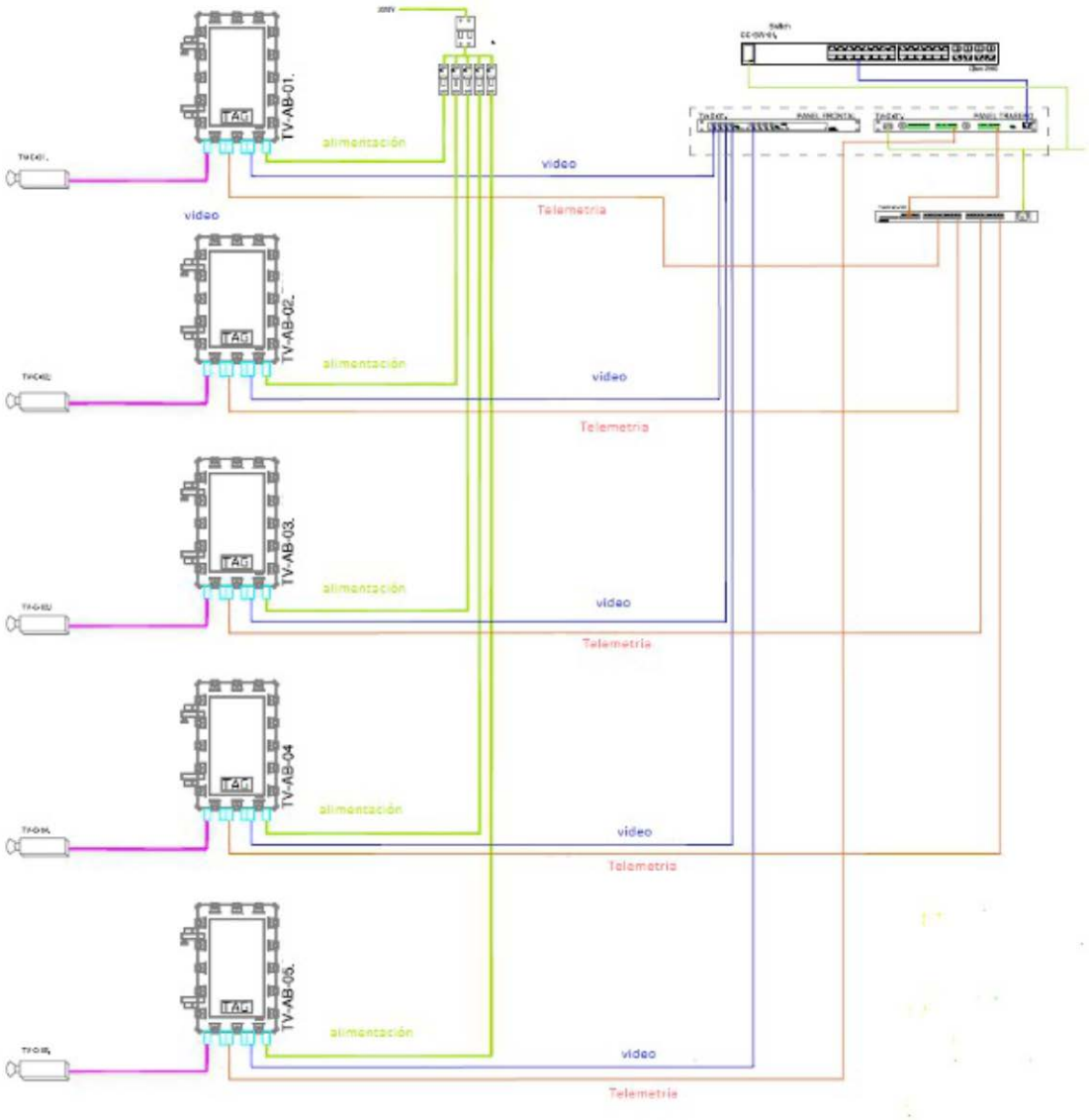



Figura-52

## 5.5 Cableado de Megafonia.

La conexión del pupitre con micrófono en la terminal marítima a la red Ethernet se realiza por medio de un latiguillo de red. Es simplemente conectar el puerto Ethernet del pupitre a un puerto del Switch existente en el rack de datos.

Por su parte en los frentes 1, 2 y 3, de igual manera se conectaran al amplificador de audio a la red y la alimentación de 220 V la toma a partir de la alimentación general del armario que se suministra a través de un SAI.

La conexión del amplificador de audio a cada uno de los altavoces se realiza mediante una línea de 2 hilos en una manguera de 2 x 1,5 mm2 libre de halógenos y con buen comportamiento frente a hidrocarburos.

Para realizar las conexiones se utilizan cajas de empalme antideflagrantes y resistentes a la corrosión modelo Aplei 3002-B EEx e, con sus prensas correspondientes

Figura-53

# Capítulo 6: Pruebas de Validación de Red.

Una vez finalizada la instalación del cableado total mente etiquetado (cables, tomas, equipos, armarios y paneles de parcheo), y configuración de los equipos (host, routers, switches, etc…), se procederá a realizar los CHECK-LIST según formato facilitado por el proyecto, esta auditoria será aceptada por el cliente y subsanadas aquellas partidas que no cumplen con los requisitos del proyecto.

## 6.1 Comisionado De Telemática Nodal Fibra-Cabinas.

| | | | | |
|---|---|---|---|---|
| | **Comisionado de Telemática NODAL FIBRA - Cabinas (Check-list)** | | | |
| **Proyecto:** | | | | |
| **Ubicación:** | | **Fecha:** | | **Rev:** 0 |
| **Cabina:** | | | **Sala:** | |
| **Realiza precomisionado:** | | | **Observaciones:** | |
| Fdo. | **Realiza comisionado:** | **Otros participantes:** | **Aprobación:** | **Empresa:** |
| **Comentarios:** | Fdo. | Fdo. | Fdo. | Fdo. |

**Check-list Telemática NODAL FIBRA – CABINAS / RACK**

| TAREA | | FASE | TAGS | | | |
|---|---|---|---|---|---|---|
| | | | SI | NO | N-APL | OBSERVACIONES |
| 1.Documentación | Disponible documentación del sistema según índice del vendedor | C/P | | | | |
| | Disponible informe pruebas FAT del sistema | C/P | | | | |
| 2. Inspección mecánica cabina | Faltas de pruebas FAT subsanadas | C/P | | | | |
| | Orientación e Implantación según plano | C/P | | | | |
| | Ausencia de abolladuras y desperfectos | C/P | | | | |
| | Apertura/Cierre correcto y espacio libre | C/P | | | | |
| | Fijación, nivelación y apriete de tornillería correctos | C/P | | | | |
| | Etiquetado según planos (Incluido componentes y cableado entre componentes) | C/P | | | | |
| | Cables bien peinados y organizados | C/P | | | | |
| | Ausencia de material de desecho dentro de cabina | C/P | | | | |
| | Dimensiones de cabinas según plano | C/P | | | | |
| | Disponibilidad de 25% de reserva | C/P | | | | |
| 3. Inspección Hardware | Verificar accesibilidad de conexión a los puertos de fibra | C | | | | |
| | Verificar Tag de mangueras de fibras | C | | | | |
| | Identificación de puertos de fibra | | | | | |
| | Verificar Tag de paneles de distribución de fibra SM | C | | | | |
| | Verificar conexionado de la totalidad de las fibras de la manguera | C | | | | |
| | Empleo de radios de curvatura según fabricante en el de acceso de manguera a rack | C | | | | |
| | Verificar etiquetado de latiguillos de asignación de fibra óptica | C | | | | |
| | Comprobación de conexionado de fibras | C/P | | | | |
| | Verificar enlace con electrónica de red Ethernet. | C | | | | |

NOTAS:

C/P - Fase Construcción/Precomisionado: equipo instalado en sala sin alimentación
C / PL - Fase Construcción/Precomisionado: Pruebas Provisional a modo local
C - Fase de comisionado: equipo alimentado
C1 - Fase de comisionado: equipo comunicado con nodo de control y multicables/fibras tendidos

Figura-54

## 6.2 Comisionado De Telemática Voz y Datos.

| | Comisionado de Telemática VOZ Y DATOS – Cableado y tomas / (Check-list) | | | |
|---|---|---|---|---|
| Proyecto: | | Fecha: | | Rev: 0 |
| Ubicación: | | | Sala: | |
| Cabina: | | | Observaciones: | |
| Realiza precomisionado: | Realiza comisionado: | Otros participantes: | Aprobación: | Empresa: |
| Fdo. | Fdo. | Fdo. | Fdo. | Fdo. |
| Comentarios: | | | | |

**Check-list Telemática VOZ Y DATOS – CABLEADO Y TOMAS.**

**Hoja _1_ de _1_**

| TAREA | | FASE | TAGS | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | OBSERVACIONES |
| | | | S | N | N/A | S | N | N/A | S | N | N/A | S | N | N/A | |
| 1. Documentación | Disponible documentación de los elementos según indice del vendedor | C/P | | | | | | | | | | | | | |
| 2. Inspección mecánica | Implantación según plano | C/P | | | | | | | | | | | | | |
| | Ausencia de abolladuras y desperfectos | C/P | | | | | | | | | | | | | |
| | Fijación, nivelación y accesibilidad correcta (cajas, placas y perslanillas) | C/P | | | | | | | | | | | | | |
| | Etiquetado de tomas RJ45 y cables UTP según planos | C/P | | | | | | | | | | | | | |
| | Cables bien peinados y no amontonados | C/P | | | | | | | | | | | | | |
| | Ausencia de destrenzado final en el conexionado | C/P | | | | | | | | | | | | | |
| | Conexión y desconexión de tomas sin deterioro. | C/P | | | | | | | | | | | | | |
| | Ausencia en el cableado de cortes, y aplastamientos | C/P | | | | | | | | | | | | | |
| | Se respeta el radio de curvatura en el cableado | C/P | | | | | | | | | | | | | |
| | Separación de líneas de alimentación según normativa. | C/P | | | | | | | | | | | | | |
| 3. Prueba final | Reflectometria Cat.6A 100% instalados . disponible. | C/PL | | | | | | | | | | | | | |

**NOTAS:**

C / P - Fase Construcción/Precomisionado: equipo instalado en sala sin alimentación
C / PL - Fase Construcción/Precomisionado: Pruebas Provisional a modo local
C - Fase de comisionado: equipo alimentado
C1 - Fase de comisionado: equipo comunicado con nodo de control.

Figura-55

Una vez aceptado por parte del cliente se debe proceder a la implementación de la solución adoptada, según listas de tareas a realizar. Durante la ejecución de los trabajos cualquier modificación del proyecto inicial ha de ser aprobado por el cliente, además de los inconvenientes físicos que puedan surgir durante la instalación, además de ser comunicados al cliente donde después de plantearle dichos cambios ha de ser aprobado por el cliente.

El proceso de ejecución del proyecto, incluye los siguientes puntos:

1.- Replanteo, soportación, rozas para tubos conduit o PVC y cajas. Bancadas de armarios.

2.- Instalación de cajas y tubos con guias.

3.- Tirada de cableado UTP y F.O. Con instalación en las cajas.

4.- Conexionado de terminales en cables UTP y fusionado de la fibra Optica.

5.- Montaje de armarios en la salas de Rack.

6.- Instalación de los equipos en los armarios

7.- Parcheo delcable UTP y F.O. En los armarios.

8.- Configuración de los equipos (Vlan`s, IP´s, Router, etc...).

9.- Pruebas SAT de la red y Equipos.

10.-Ingenieria de detalle de planos building.

# Capítulo 7: Conclusiones, Riesgos y Trabajos Futuros.

## 7.1 Introducción.

Como conclusión a este proyecto, es imprescindible llevar a cabo los siguientes puntos y con ellos asegurar el ajuste de recursos y la optimización de la ejecución:

| |
|---|
| Análisis de los objetivos de negocio y empresarial |
| Auditoria de la red actual: Análisis de la topología |
| Análisis del tráfico que se genera y patrones del tráfico |
| Análisis y recomendaciones sobre servicios de Red |
| Análisis de las previsiones de crecimiento y requisitos de escalabilidad de la red |
| Recomendaciones sobre la política de seguridad, tolerancia a fallos QoS y fiabilidad |
| Diseño lógico de la arquitectura de la red |
| Capa de distribución |
| Capa de acceso |
| Esquema lógico de la red y esquema físico de la red |
| Conexionado y alimentación de armarios |
| Cableado estructurado |
| Arquitectura de red |
| Documentación equipos |
| Configuración equipos |

RIESGOS

Entendemos como riesgos a analizar los propios de las tareas especificadas anteriormente (redacción del proyecto, aceptación, implementación, check-list.), sin incluir en estos los riesgos de seguridad inherentes a la seguridad informática de la red que serán tratados en el punto *"Politica de Seguridad"*.
Desglosados los siguientes puntos:

1. Estudio

   Los riesgos pueden venir de un mal análisis del punto de partida por el nulo conocimiento o escasa información remitida por parte del cliente, estos se solventaran en la fase de desarrollo y las necesidades (actuales y futuras) del cliente.

2. Redacción del proyecto

Los riesgos en la fase de redacción del proyecto vienen determinados por la experiencia y conocimientos del equipo redactor del mismo, así como de las herramientas a su alcance, un apartado de especial atención es el intercambio de información entre el cliente/auditor y el equipo de redacción, el riesgo más común es el retraso en la finalización del proyecto, por ello se recomiendan el disponer un jefe de proyecto experimentado.

3. Implementación.

Uno de los mayores riesgos en este tipo de instalaciones es la recepción del material que será convenientemente negociada con los proveedores mediante contrato.

Se tendrán en cuenta los riesgos laborales según la legislación vigente, el personal deberá estar formado adecuadamente con dispondrá de sus EPI correspondientes, deberá existir un responsable de seguridad que llevará a cabo del plan de seguridad y salud de la obra, así como el control del cumplimiento del plan de autoprotección de la empresa implementadora, y la empresa donde se realiza la instalación.

4. Check-list.

El mayor riesgo que se puede producir en el apartado del chequeo es no testear la instalación o hacerlo de manera inadecuada, para ello el personal que prueba la instalación deberá tener elaborado su protocolo escrito, el material correctamente calibrado y verificado, así como el conocimiento y manejo para el correcto análisis de la instalación, su posible certificación en caso de ser necesario.

En prevención de las necesidades futuras, se ha previsto la reserva de más del 20% en capacidad de nuevos enlaces, así cubrimos el punto de escalabilidad del sistema y con ello la instalación de nuevos dispositivos para el servicio de operaciones industriales en los pantalanes, por si la empresa se plantea aumentar su área de negocio.