

**DRAFT**

Provisión Escenarios Híbridos – Red Virtualizada – Red Física: POC

Versión 0.1

*Versión: 1.1*

Tabla de contenido

[1 Cláusula de confidencialidad 4](#_Toc22298650)

[2 Situación actual 5](#_Toc22298651)

[2.1 Estado 5](#_Toc22298652)

[2.2 Objetivo 5](#_Toc22298653)

[3 Descripción del escenario para desplegar los Casos de Uso 6](#_Toc22298654)

[3.1 Productos 6](#_Toc22298655)

[4 Caso de Uso 1: Fulfillment del producto 9](#_Toc22298656)

[4.1 Escenario Inicial – Conectividad VPN Sede Central, Fábrica y Almacén 9](#_Toc22298657)

[4.1.1 Journey 11](#_Toc22298658)

[4.1.2 Actividades 11](#_Toc22298659)

[4.1.2.1 DISEÑO DATOS ESCENARIO 12](#_Toc22298660)

[4.2 Escenario 2: Provisión Servicio SD-Wan 15](#_Toc22298661)

[4.2.1 Journey 15](#_Toc22298662)

[4.3 Escenario 3: Modificar el ancho de banda de sede 3 16](#_Toc22298663)

[4.3.1 Journey 16](#_Toc22298664)

[4.4 Escenario 4: Dar de baja la sede 3 16](#_Toc22298665)

[4.4.1 Journey 16](#_Toc22298666)

[5 Caso de Uso 2: Assurance 17](#_Toc22298667)

[6 SOM 18](#_Toc22298668)

[6.1 Definición Estructura CFS-RFS 18](#_Toc22298669)

[7 Anexo 1: MPLS Service Details 20](#_Toc22298670)

[8 Anexo 2: Información a progresar por UNICA al inventario 21](#_Toc22298671)

Información del documento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proyecto** | **-** | | | |
| **Preparado por:** | **Convergent Telco Architecture** | **Versión de documento** | **1.0** |
| **Título** | **Provisión Escenarios Híbridos – Red Virtualizada – Red Física: POC** | **Fecha de documento** | **11.10.19** |
| **Revisado por** |  | **Fecha de revisión** |  |

Lista de distribución

Equipos de Arquitectura de las OBs.

Vendors a colaborar en la POC.

| **De** | **Fecha** | **email** |
| --- | --- | --- |
| **Convergent Telco Architecture** | **11.10.19** | **marta.besteiromartinez@telefonica.com** |
| **Destinatarios** | | |
|  | | |

Histórico de versiones

| **Versión** | **Fecha** | **Revisado por** | **Descripción** | **Fichero** |
| --- | --- | --- | --- | --- |
| **1.0** | **11.10.19** |  | **Primera versión del documento** | **TEF\_GCTIO\_POC\_Integración\_BSS\_OSS\_UNICA\_Escenarios Híbridos\_v1.0.docx** |

# Cláusula de confidencialidad

Toda la información contenida en este documento y derivada del proceso de licitación y del proyecto que se va a licitar es CONFIDENCIAL, estando el suministrador obligado a no compartir ni divulgar su contenido ya sea total o parcialmente sin permiso de Telefónica.

Esta obligación no aplica a posible información pública contenida en este documento y obtenida durante el proceso y el proyecto objeto de licitación.

Si el suministrador no está de acuerdo con lo anteriormente mencionado, deberá destruir inmediatamente todas las copias del documento que tuviera.

La presente cláusula de confidencialidad se considerará automáticamente aceptada, salvo que el suministrador exprese lo contrario.

Una vez aceptada la presente cláusula, el suministrador estará obligado a:

* Toda la información de este documento, la derivada del presente proceso y del proyecto objeto de licitación será tratada como CONFIDENCIAL y no deberá ser divulgada por ningún medio sin permiso explícito de Telefónica.
* La presente cláusula tendrá validez incluso ante la cancelación, finalización o interrupción de la relación entre ambas partes.
* No se considerará como información CONFIDENCIAL:
  + Aquellas partes del documento que sean de dominio público.
  + Si el receptor dispone con anterioridad a que le sea remitida de derechos legales sobre la misma.
* El suministrador no divulgará esta información a terceras compañías que pudieran estar involucradas en el proceso sin el consentimiento explícito de Telefónica.

1. Situación actual

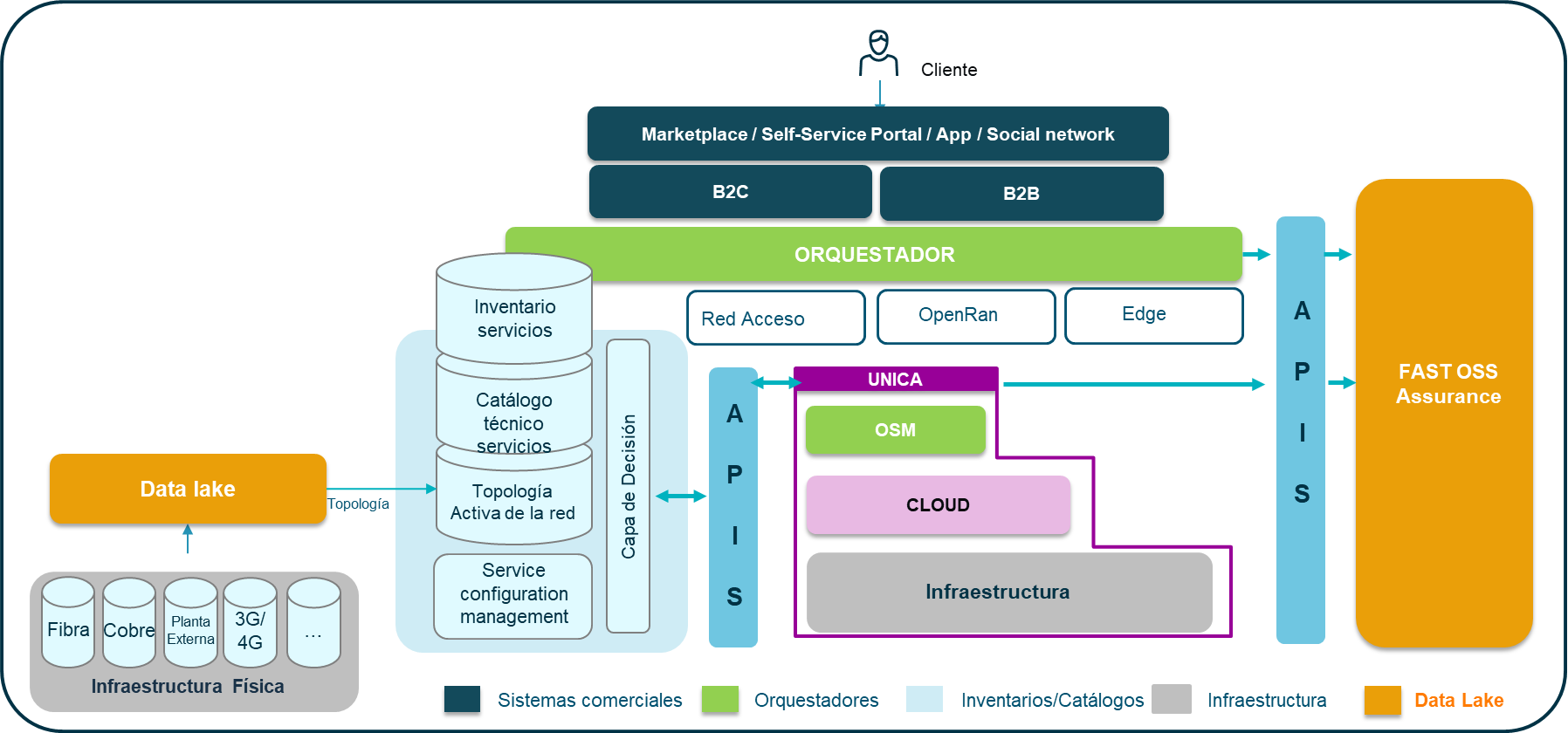
## Estado

TO-DO

## Objetivo

El objetivo de esta PoC es presentar un caso real que sea lo suficientemente amplio como para poder demostrar la necesidad de una arquitectura que permita aunar la provisión de servicios sobre redes híbridas (física-virtualizada), así como probar los diferentes elementos necesarios, tanto para la provisión como el assurance de servicios complejos B2B.

Para esto, se propone la siguiente arquitectura a alto nivel:



En este se tiene los siguientes elementos:

* Red virtual. Compuesta por dos datacenters donde está desplegado UNICA.
* Red física. Compuesta por cuatro datacenters conectados a través de conexión física con una serie de elementos de red y routers físicos y cuya topología de red irá modificándose de manera dinámica durante la POC.
* Sistemas de Assurance. Siguiendo la arquitectura FAST OSS de Telefonica.
* Sistemas de fulfillment.
* ------ [COMPLETAR]

# Descripción del escenario para desplegar los Casos de Uso

El caso de uso para el estudio de dominios de integración de los sistemas BSS/OSS con UNICA se basa en un producto B2B completo, cuyo diseño se irá desgranando durante las versiones del presente documento.

El detalle del caso es el que se presenta a continuación.

Telefónica debe desplegar un producto a una empresa de fabricación y venta de moda que tiene tres sedes principales en Madrid, Málaga y Pamplona, y piensa desplegar 200 tiendas durante los próximos años durante toda España.

Las características de la VPN que Telefónica está vendiendo están especificadas en el apartado: Anexo 1: MPLS Service Details

## Productos

Se ha cerrado un acuerdo con un cliente dedicado a la fabricación que posee una extensa cadena de tiendas.

El acuerdo consiste en una solución completa de telecomunicaciones, dando soporte tanto a los datos como a la voz y parte de IT.

Producto VPN Corporativa

Red de Datos MPLS para las tres sedes:

Sede Central:

* Circuito con un caudal de 500 Mb:
  + 100 Mb Calidad Oro – Latencia máximo de 20 ms
  + 150 Mb Calidad Plata – Latencia máximo de 20 ms
  + 100 Mb Calidad Bronce
  + 150 Mb de salida a Internet

Sede Fábrica:

* Circuito con Caudal de 300 Mb
  + 40 Mb Calidad Oro – Latencia máximo de 20 ms
  + 60 Mb Calidad Plata – Latencia máximo de 20 ms
  + 150 Mb Calidad Bronce
  + 50 Mb de salida a Internet

Sede Almacén:

* Circuito con Caudal de 150 Mb
  + 20 Mb Calidad Oro – Latencia máximo de 20 ms
  + 30 Mb Calidad Plata – Latencia máximo de 20 ms
  + 75 Mb Calidad Bronce
  + 25 Mb de salida a Internet

Producto VPN tiendas

Las tiendas se dividen en tres grandes grupos en función del tamaño de las mismas. Las tiendas se conectarán a través de una VPN definida por software todas ellas con acceso a internet. Y con conexión a la vez a la red corporativa. El acuerdo es el siguiente:

* **Tienda Tipo L**

VPN IP 100 Mb con Caudal de 50 Mb

2 Línea Individual

1 Línea Móvil

1 Software Gestión de tiendas

Seguridad Periférica con 4 Cámaras

* **Tienda Tipo M**

VPN IP 50 Mb con Caudal de 30 MB

1 Línea Individual

1 Línea Móvil

1 Software Gestión de tiendas

Seguridad Periférica de 3 Cámaras

* **Tienda Tipo S**

VPN IP 20 Mb con Caudal de 10 Mb

1 Línea Individual

1 Línea Móvil

1 Software Gestión de Restaurantes

Seguridad Periférica de 3 Cámaras

Producto Telefonía Fija

La telefonía fija se desplegará sobre Telefonía IP desplegada con nodo central de la sede central.

El plan de telefonía contendrá las siguientes Bolsas:

* Bolsa de Tráfico Fijo nacional 1.000.000 de Minutos (Las bolsas están en la Central porque las gestionan de forma centralizada)
* Bolsa de Tráfico Fijo internacional 50.000 de Minutos (Las bolsas están en la Central porque las gestionan de forma centralizada)

Existirán como máximo 2500 puestos de Telefonía y éstos se podrán definir en dos perfiles:

* Categoría Manager
  + Acceso a Telefonía Fija Nacional e Internacional ilimitada
* Categoría Empleado
  + Acceso a 300 minutos de tráfico nacional mensual.

Producto Telefonía Móvil

La telefonía móvil se desplegará con un nodo corporativo móvil que gestione las comunicaciones al exterior e intracompañía.

El plan de telefonía móvil contendrá la siguiente bolsa:

* Bolsa de Tráfico Móvil 2.000.000 de Minutos
* Bolsa de Tráfico Móvil internacional 10.000 de Minutos

Se desplegarán 2000 móviles con las mismas categorías que en la telefonía fija.

# Caso de Uso 1: Fulfillment del producto

## Escenario Inicial – Conectividad VPN Sede Central, Fábrica y Almacén

En el escenario inicial empezamos por provisionar la VPN entre las tres sedes. La topología de red disponible no nos permite conectar las tres sedes con la latencia requerida.

En el escenario t0 se tienen los siguientes componentes y topología de red:

Sede 1 (sede central):

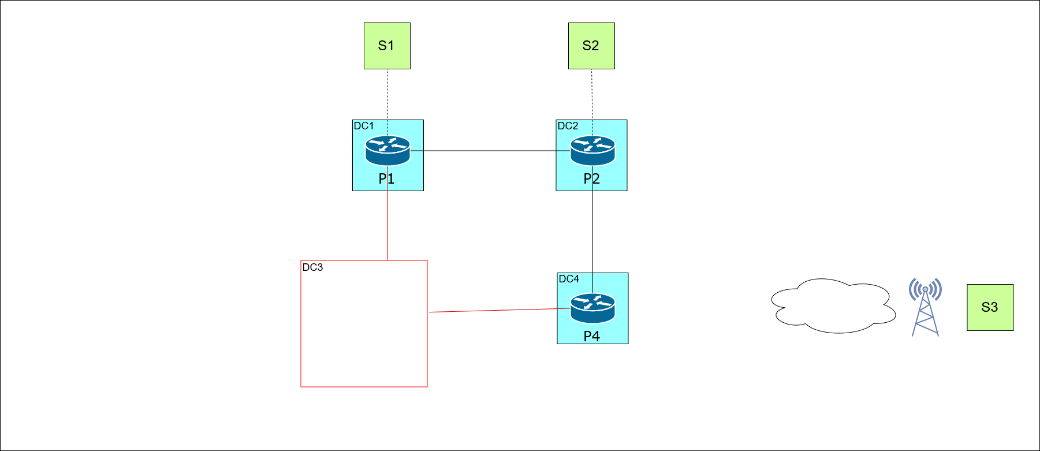
* Datacenter más cercano, DC1. Existe conexión física entre DC1 y la localización de la sede a través de fibra con los requisitos de BW y latencia requeridos. Existe un router PE1 en DC1 que se puede configurar para dar la conexión VPN.

Sede 2 (fábrica):

* Datacenter más cercano, DC2. Existe conexión física entre DC2 y la localización de la sede a través de fibra con los requisitos de BW y latencia requeridos. Existe un router PE2 en DC2 que se puede configurar para dar la conexión VPN.

Sede 3 (almacén):

* Datacenter más cercano, DC4. No existe conexión física entre DC4 y la localización de la sede a través de fibra con los requisitos de BW y latencia requeridos. Existe una antena cercana a la localización de DC3 a través de la cual se puede llegar por conexión móvil al almacén con los requisitos de latencia y BW requeridos. Existe capacidad en DC3 para provisionar un Network Service para crear el network slice entre DC4 y la fábrica a través de la red móvil.
* La conexión entre DC2 y DC4 (física) no permite cumplir los requisitos de latencia. Existe otro DC3 conectado a DC1 y DC4. Existen capacidades en DC3 para provisionar un router virtual que permita conectar la red VPN entre las 3 sedes con los requisitos de latencia.



El servicio de Serviceability arrojará el siguiente resultado:

* Sede Central: El servicio de disponibilidad en función de la dirección nos ofrece una última milla de Fibra de 1 Gb para poder asegurar el caudal de 500 Mb
* Sede Fábrica: El servicio de disponibilidad en función de la dirección nos ofrece una última milla de Fibra de 500 Mb para poder ofrecer 300 Mb
* Sede Almacén: El servicio de disponibilidad en función de la dirección no nos ofrece disponibilidad de acceso fijo.
  + Se chequea la disponibilidad de la red móvil para ello y se obtiene la posibilidad de realizarlo a través de red móvil.

Por tanto, será necesario también provisionar una slice de red virtualizada para dar conectividad a la sede almacén (Site 3).

Parámetros Físicos de los elementos de red relevantes para la POC

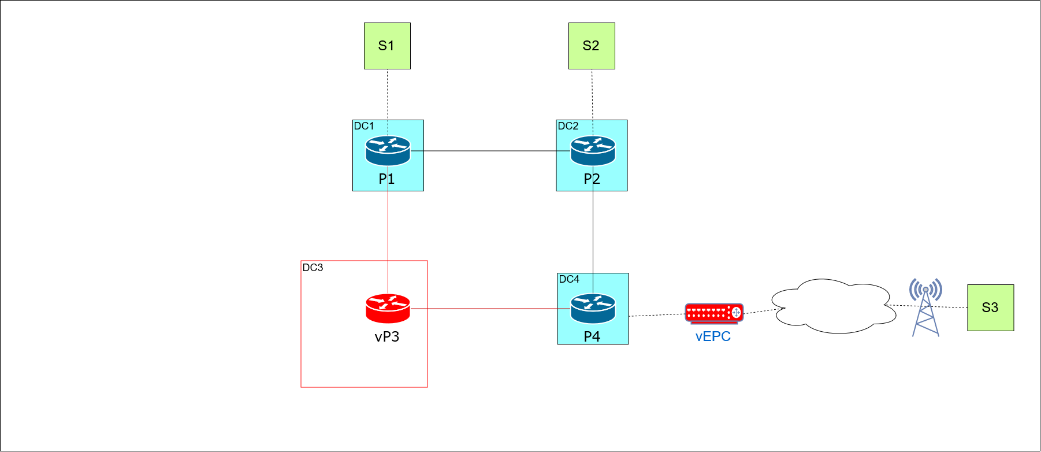
* Antenas: ratio de degradación, esquema de modulación, dúplex
* VLAN Antena – PE4: Caudal, Latencia
* Recursos Físicos CPDs: CPU, Memoria, Storage, Network
* Nodos y conexiones red de transporte y acceso: caudal, latencia, número de conexiones.

Red Virtualizada:

* Compuesta por dos Datacenters.

### Journey

* Desde la fase de negociación de la oferta, se lanzará una solicitud de serviceability, considerando los datos de la propuesta
  + El serviceability es correcto para las dos primeras sedes.
  + El serviceability va a dar error al no cumplir la latencia requerida en la ruta PE1-PE2- PE4.
  + El decisor confirma al Gestor Comercial, la posibilidad de crear un router virtual en DC3 para proporcionar la latencia requerida entre PE1-PE4.
  + El proceso sigue revalidando el serviceability. En este serviceability se asigna que vayamos por un slice de red.
* A partir de la respuesta, se crea una orden de producto con las sedes,
* SOM descompone en ordenes de servicio, y se lanza el proceso de D/A, y configuración/activación, tanto para las sedes físicas como para la sede virtual dar de alta el slice de red. SOM lanza este requerimiento a la capa de decisión, que responde tanto los NS que se requieren instanciar en OSM, como los recursos necesarios desde la red e inventarios físicos.
* Como el vRouter vPE3 es público porque así se ha definido en la oferta, se tiene que crear una orden específica de creación de red para este router, para que si en algún momento se tramita la baja alguna sede, no sé incluya la baja el vRouter público.
* SOM solicita actualizar los inventarios de servicios, de topología activa, y físicos, y zenoss.



### Actividades

1.- Insertar en la topología activa la topología móvil más la topología fija correspondientes al escenario t0, teniendo en cuenta que las características de esa topología no cumplen las condiciones de conectividad requeridas (latencia PE1-PE2-PE4 mayor que la requerida). Y el DataCenter en el punto 3. Y los DC tienen que estar conectados entre ellos.

2.- Simular orden de VPN S1, S2, S3. Simular Servicio Creación Orden en SOM

- Estructura Orden de Producto

- Estructura CFS, RFS

3.- Serviceability.

- Hay que invocar al serviceability actual, y ver cómo completar para poder dar el caso completo.

- Serviceability S3 KO por dos razones:

- Latencia

- Acceso

4.- Decisor.

- Tiene que ir al Inventario Activo, ver que hay una antena en S3 y determinar que se puede dar cobertura móvil para los requisitos. Para esto tendrá que tener en cuenta la información del Inventario activo, catálogo técnico de servicios, y gestor configuración.

- Tiene que ir al IA para ver que hay un DC3 conectado a los DCs 1, 2, y 4, con recursos físicos suficientes para levantar un vRouter vPE3 que permita la latencia requerida entre PE1, PE4, y vPE3.

5.- SOM. Ejecuta.

- Definir CFS y RFS.

- D&A: Definir cómo hacer la transformación de la respuesta al orquestador a estructura de Inventario Activo.

- Lanza las distintas ordenes de configuración / activación

- Actualizar inventarios, assurance, zenoss, con cada creación.

- Definir integración inventario de servicios - inventario Activo

#### DISEÑO DATOS ESCENARIO

* El serviceability es correcto para las dos primeras sedes. La orden se provisiona para crear la VPN entre dos sedes.
  + Datos para simular el servicio (RCEC / AI)

**Acceso Sede 1.**

|  |  |  |
| --- | --- | --- |
| CE1-PE1 | Caudal Disponible X | Inventario Activo |
|  | Latencia Disponible Y | Inventario Activo |
|  | #Conexiones Máximas Z | Inventario Activo |
|  | #Conexiones Actual W | Inventario Activo |

**Acceso Sede 2.**

|  |  |  |
| --- | --- | --- |
| CE2-PE2 | Caudal Disponible X | Inventario Activo |
|  | Latencia Disponible Y | Inventario Activo |
|  | #Conexiones Máximas Z | Inventario Activo |
|  | #Conexiones Actual W | Inventario Activo |

**Transporte.**

|  |  |  |
| --- | --- | --- |
| PE1-PE2 | Caudal Disponible X | Inventario Activo |
|  | Latencia Disponible Y | Inventario Activo |
|  | #Conexiones Máximas Z | Inventario Activo |
|  | #Conexiones Actual W | Inventario Activo |

* El serviceability va a dar error al no tener BW o Latencia en la ruta PE1-PE2- PE4
  + Datos para simular el servicio (RCEC / AI)

**Acceso Sede 3.**

|  |  |  |
| --- | --- | --- |
| CE2-PE2 | Caudal Disponible: no hay red física disponible | Inventario Activo |
|  | Latencia Disponible: idem | Inventario Activo |
|  | #Conexiones Máximas: idem | Inventario Activo |
|  | #Conexiones Actual: idem | Inventario Activo |

**Transporte.**

|  |  |  |
| --- | --- | --- |
| PE1-PE2-PE4 | Caudal Disponible: X | Inventario Activo |
|  | Latencia Disponible: Y | Inventario Activo |
|  | #Conexiones Máximas: Z | Inventario Activo |
|  | #Conexiones Actual: W | Inventario Activo |

**Transporte.**

|  |  |  |
| --- | --- | --- |
| PE1-PE4 | Caudal Disponible: X | Inventario Activo |
|  | Latencia Disponible: Y | Inventario Activo |
|  | #Conexiones Máximas: Z | Inventario Activo |

* + Datos para comprobar disponibilidad recursos para instanciar NS

**Acceso Sede 4.**

|  |  |  |  |
| --- | --- | --- | --- |
| Parámetros Antena eNodeB | Propagación G | Inventario Activo | Con esta info más la localización de la antena y de la sede el decisor sabrá si existe ancho de banda/caudal/latencia suficiente en la red móvil para provisionar el slice de red con la calidad de servicio requerida |
| Atenuación H | Inventario Activo |
| VLAN entre eNodeB y PE4 | Caudal X | Inventario Activo |  |
| Latencia Y | Inventario Activo |  |
| Recursos Físicos CPD | CPU A | Inventario Activo/Gestor Configuración |  |
| Memoria B | Inventario Activo/Gestor Configuración |  |
| Storage C | Inventario Activo/Gestor Configuración |  |
| Network D | Inventario Activo/Gestor Configuración |  |

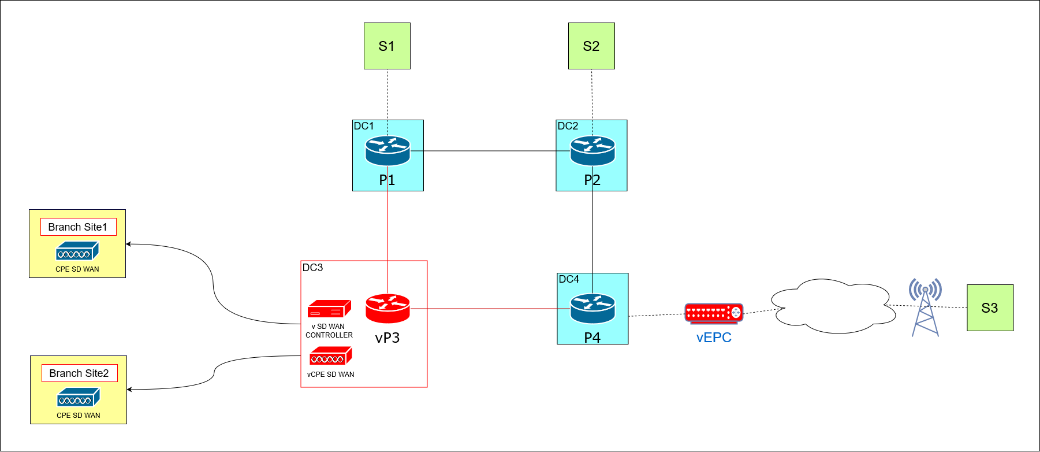
* Una vez instanciado el Network Service para el vEPC, el OSM actualizará el repositorio común indicando que se ha completado esa instancia en el Data Center correspondiente, y el Data center actualizará el repositorio indicando:
  + los valores actualizados de CPU, memoria, storage y network disponible para poder instanciar nuevos servicios virtualizados  gestor de la configuración.
  + la información específica de la VNF, latencia que soporta y caudal máximo que soporta  gestión de la configuración e Inventario Activo.

## Escenario 2: Provisión Servicio SD-Wan

El cliente contrata el servicio SD-Wan para conectar sus 2 tiendas desplegadas en dos ubicaciones del territorio nacional.

### Journey

* Se hace una orden de producto con las tiendas SD-Wan
* El serviceability da OK para los accesos de las 2 tiendas
* Se provisionan los accesos de las 2 tiendas
  + Un CPE físico en cada tienda
  + Un CPE virtual en la central más cercana a cada tienda, en este caso, el DC3
* El serviceability da OK para los VNFs a instanciar para la gestión y el control de la SDWan (en DC3)
* Se provisionan las VNFs
* Se actualizan todos los inventarios



## Escenario 3: Modificar el ancho de banda de sede 3

El cliente solicita aumentar el ancho de banda para la conectividad de la S3

### Journey

* Se crea la orden de producto solicitando la modificación.
  + El serviceability da Ok en el Slice de Red, para la conectividad, y nOK en la capacidad del vRouter en DC3.
  + El Decisor decide escalar la capacidad del vRouter en DC3.
  + Subcaso: posibilidad de escalar sobre la instancia del NS que está corriendo.
  + Subcaso: no existe la posibilidad de escalar sobre la misma instancia y se instancia un nuevo NS.
* Se actualiza la configuración de las VNFs.
* Se actualizan todos los inventarios.

## Escenario 4: Dar de baja la sede 3

El cliente solicita dar la baja de la S3

### Journey

* Se crea la orden de producto solicitando la modificación.
* SOM crear la orden de servicio, para dar la baja.
* Tener en cuenta que el vPE3 se dio de alta para esta sede, y es público. Por tanto, al dar de baja la sede, no se puede dar de baja este vrouter.
* En la orden de alta del vPE3 tiene que haber una orden específica de creación de red que lo identifique, porque es público. Es decir, la creación del vPE3 tiene que ir en otra orden, no asociada al alta de la sede 3. Porque si no al dar de baja la sede 3, va a comparar lo que hay con lo que había, borrar todo lo que sea distinto y daría de baja el vPE3.
* Se actualizan todos los inventarios.

# Caso de Uso 2: Assurance

Pendiente de definir, incluyendo la integración con Zenoss, y el monitoreo a implementar.

## Baja Latencia en ruta PE1-PE2

Zenoss, o el monitor que corresponda, monitoriza y levanta una alarma por baja latencia en la ruta física PE1-PE2

Assurance lee la alarma de ahí.

Reconfiguro VIM en PE3 y cambio ruta PE1-PE3-PE4-PE2.

[Definir qué va a resolver Assurance y qué va a llamar a SOM. Pool de reglas.]

### Journey

* El VIM del DataCenter actualiza periódicamente la información sobre los parámetros relevantes necesarios para monitorización de la infraestructura, tales como los valores actualizados de consumo de CPU, temperatura, heartbeat, …
* En un momento dado hay un fallo de infraestructura de transporte (pérdida de un enlace entre routers PE que garantizaba el datarate y la latencia necesarios entre sedes 1 y 2)
* El OSM publica este evento en su bus de mensajería.
* Zenoss levanta alarma y el sistema de Assurance lee la alarma
* Assurance llama al decisor que, a partir de la topología de red física y virtual registrada en AI, decide que es posible reconfigurar VIM en PE3 y cambiar la ruta PE1-PE2 por PE1-vPE3-PE4-PE2
* Se provisionan los cambios y se actualizan los inventarios

## Fallo en VNF EPC

Zenoss monitoriza y levanta una alarma por fallo en el VNF EPC en la sede Almacén.

Assurance lee la alarma de ahí.

El decisor confirma disponibilidad para instanciar otro vEPC

Definir qué va a resolver Assurance y qué va a llamar a SOM. Pool de reglas.

### Journey

* El VIM del DataCenter actualiza periódicamente la información sobre los parámetros relevantes necesarios para monitorización de la infraestructura, tales como los valores actualizados de consumo de CPU, temperatura, heartbeat, …
* En un momento dado hay un fallo del vRouter (por ejemplo, pérdida de dataRate en el puerto de llegada al datacenter en que se ha virtualizado el vRouter)
* El vRouter comunica su fallo al OSM, quien a su vez lo publica en su bus de mensajería.
* Zenoss levanta alarma y el sistema de Assurance lee la alarma
* Assurance llama al decisor que indentifica el Servicio Virtual y el Datacenter afectado (consultando la información de configuración del repositorio común) y confirma hay capacidad disponible en el Data Center para levantar otro vRouter.
* El sistema decisor/Assurance solicita al OSM en el Data Center correspondiente que instancie un nuevo vRouter en otra máquina del mismo DataCenter o de otro (si no hay recursos en el momento, y los requerimientos de conectividad y capacidad se satisfacen en el DC alternativo) para garantizar el servicio.
* Se provisionan los cambios y se actualizan los inventarios.

## Fallo en conexión física en red de acceso de Sede 1 y reemplazo con slice de red virtual

Zenoss monitoriza y levanta una alarma por fallo en la fibra que une la Sede 1 con el PE1.

Assurance lee la alarma de ahí.

El decisor confirma disponibilidad para instanciar un vEPC en PE1.

Definir qué va a resolver Assurance y qué va a llamar a SOM. Pool de reglas.

Se provisiona el vEPC y se actualizan inventario activo y gestor de la configuración.

* Fallo en un VNF dentro del NS vEPC (MME o HSS por ejemplo). Zenoss está monitorizando y se debería poder configurar las reglas para disparar alarmas. En función de unos umbrales y ver si también la variable temporal (a partir de cuántas veces mala medida se levanta una alarma), si no se tendría que poner en Fast OSS. Una vez esa alarma es tratada por Fast OSS, se reconfigura esa VNF (el objetivo del caso es demostrar que se puede llegar directamente a una VNF sin tener que reconfigurar todo el NS).

# SOM

## Definición Estructura CFS-RFS

* CFS VPN\_G  crear la VPN a nivel global.
* CFS VPN\_SITE\_FO (Sede VPN – Fibra)
  + CFS S.Site (Conectividad VPN)  meter el PE en la VPN
  + CFS Acceso Main  obtener fibra para esta sede
    - VPN  alta de esa conexión en el PE1.
    - VoIP
    - Internet
    - Last Mile
    - Acceso BackUp  Apunta al Sede VPN-Fibra (VPN\_SITE\_FO) que sea back up de éste. El Acceso BackUp se configurará dentro del Acceso Main del VPN\_SITE\_FO de Back Up. Habrá un atributo a nivel de VPN\_SITE\_FO que te dirá si es un site de back up o no.
  + CFS CPE  Configurar el CE
* CFS VPN\_SITE\_M (Sede VPN – Móvil)
  + CFS Conectividad VPN  meter el PE en la VPN
  + CFS Acceso eNodeB  VLANS + IP (El SOM tendrá que coger cierta info de aquí y llevarla al CFS NS).
    - eNode – MPLS
    - datacenter – MPLS
    - Pseudowire
  + CFS NS (Network Service) + Configuración (con la configuración que le hayas vendido al cliente)  para acceder a Unica
  + CFS S.Site (Conectividad VPN)
  + CFS CPE
  + CFS Servicio Móvil (Configurar el HLR)
* CFS VPN\_SDWAN
  + SDWAN (Infraestructura)
  + S.Site (Conectividad VPN)  Conectar con el PE3
  + Acceso SDWan (Virtual entre SDWAN y S.Site)
* CFS VPN\_Branch (Sin BroadBand)
  + Branch
  + Virtual CPE
    - Network Service
  + Physical CPE
* CFS ROUTER
  + PE
    - Conectividad
  + vPE
    - Conectividad

# Anexo 1: MPLS Service Details

Tipos de servicio que se proporcionan son:

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **Type of Traffic** | **TOS** | **Comments** |
| Control | Internal Routing and Management | 7 |  |
| Management | Internal Routing and Management | 6 |  |
| Voice | Voice | 5 | Highest priority for performance-sensitive traffic. |
| Video | Video | 4 | Video. |
| Data | Platinum | 3 | Mission critical data traffic. For example SNA, SAP, citrix… |
| Data | Gold | 2 | Mission critical data traffic . For example SNA, SAP, citrix… |
| Data | Silver | 1 | Routing traffic and Management traffic (precedence 6/7) |
| Data | Bronze | 0 | No mission critical data traffic. For example FTP, http, Intranet. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type** | **Characteristics** | **TOS** | **Traffic Processing** | **EXP** | **Characteristics** |
| Voice | Voice. Performance Sensitive | 5 | High Priority | 5 | Performance Sensitive |
| Video | Video | 4 | Guaranteed | 3 | Low latency and Packet Loss |
| Data-Platinum | Mission Critical Data | 3 | Guaranteed | 3 | Low latency and Packet Loss |
| Data-Gold | Mission Critical | 2 | Guaranteed | 3 | Low latency and Packet Loss |
| Management | Management Traffic precedence and routing | 6/7 | 16K Guaranteed | 3 | Low latency and Packet Loss |
| Data-Silver | NO Mission critical. Intranet | 1 | Guaranteed | 2 | Low packet Loss |
| Data-Bronze | NO Mission critical. Internet | 0 | Guaranteed | 2 | Internet |

# Anexo 2: Información a progresar por UNICA al inventario

La información que se precisará de UNICA para la siguiente PoC será la siguiente:

* Información estática

Es aquella información referida a la configuración que tenemos en los distintos elementos que conforman el servicio de un cliente.

En este caso, los siguientes elementos deberán volcar su información correspondiente:

* + CE1,
  + PE1, PE2, PE3 y PE4
  + SDWAN
  + 5G Network slice

UNICA tendrá que proporcionar la siguiente información:

Repositorio de NS:

Recursos necesarios

* CPU
* MEM
* Storage
* Network

Recursos disponibles (estos serán específicos del NS). En el caso del PE:

* Ratio Trafico Slice red 5G Umbrales bajos
* Latencia