UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UNA ARQUITECTURA PARA UN DATA CENTER

TESIS

PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

CHARNICHART LÓPEZ ARLET GUADALUPE

OROZCO CRUZ RUBÍ

ROSALES MARROQUÍN EDUARDO

ASESORA:

M. EN I. NORMA ELVA CHÁVEZ RODRÍGUEZ

MÉXICO D.F. FEBRERO DEL 2016

Tabla de contenido

Capítulo 1: Descripción general de la arquitectura de referencia

1.1 Introducción

La red de un Data Center proporciona cualidades inherentes, tales como capacidad de penetración, transparencia, escalabilidad y orientación hacia estándares que la hacen ideal como plataforma para la consolidación de los servicios de infraestructura (tales como firewalls, balanceo de carga, protección de intrusos, replicación de datos, servidores y virtualización de almacenamiento). Al mismo tiempo permite el despliegue y la expansión gradual para cumplir con la participación de los requerimientos del negocio.

La arquitectura de red de un Data Center permite a la Empresa construir una infraestructura más dinámica, ágil y con servicios virtualizados. El objetivo se alcanzará de manera gradual y con bajo riesgo. La arquitectura se basa en los más importantes principios de las prácticas, directrices y modelos que se han probado en los laboratorios de Cisco y las implementaciones en el mundo real.

Con la implementación,de éste proyecto, se pretenden reducir las siguientes limitaciones a las que se ha enfrentado la Empresa dentro de su red:

- ➔ Limitaciones de potencia y refrigeración
- ➔ Utilización de servidores y almacenamiento
- ➔ Refuerzo de la seguridad de extremo a extremo
- ➔ Cumplimiento de normativas
- ➔ Continuidad del negocio
- ➔ Eficiencia y gestión energética

El alcance del proyecto es cubrir aspectos de diseño de bajo nivel para unacloud privada de un Data Center. La Empresa se ha centrado en servicios de infraestructura de un Data Center como área de crecimiento estratégico y ha puesto en marcha la construcción de cinco Data Center. Los cuales se encontrarán en:

- ➔ Reynosa
- ➔ Villahermosa
- ➔ Veracruz
- ➔ Poza Rica

➔ Ciudad del Carmen

La arquitectura define a continuación, un conjunto de principios de diseño que aseguran que el diseño se adhiere a la arquitectura y cumple con los requisitos generales.

Los requisitos arquitectónicos claves definidos por el cliente son los siguientes:

➔ La arquitectura de red del Data Center tiene que ser altamente disponible, escalable y segura.

➔ Se deben proporcionar servicios de red consistentes a través de los Data Center y ayudar a asegurar la continuidad del negocio sin fisuras.

➔ Debe ser capaz de proporcionar una plataforma de red para albergar Citrix Cloud y aplicaciones empresariales Legacy.

Se propone una arquitecturade cloud de un Data Center modular y altamente flexible, construida a partir de las normas basadas en componentes modulares escalables.

Dicha arquitectura permite que los elementos activos sean tratados como grupos lógicos de recursos. Estos grupos de recursos pueden ser asignados dinámicamente y ayudan a lograr tiempos de respuesta más cortos para apoyar la expansión del negocio. La virtualización y la segmentación también proporcionan la flexibilidad para abrir un nuevo servicio.

En la figura 1.1 se muestra una propuesta de una arquitectura cloud modular para un Data Center

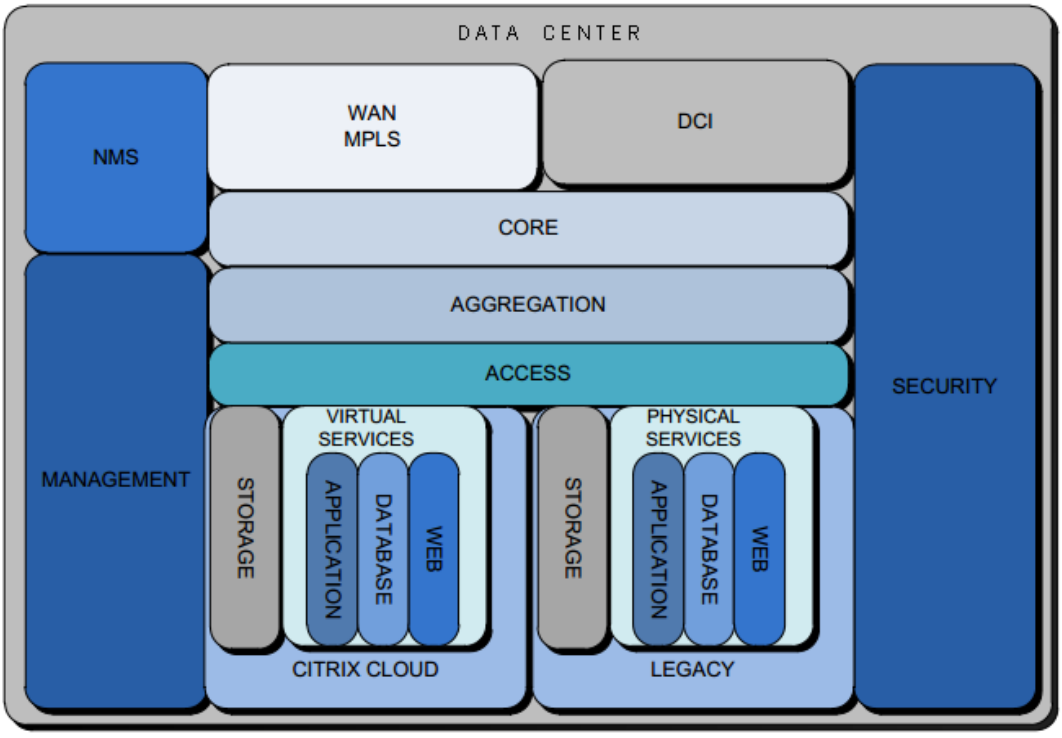


Figura 1.1 Propuesta de arquitectura cloud modular para un Data Center

Cada módulo representa un elemento clave de la capacidad en el Data Center. El enfoque de bloques de construcción da flexibilidad en soluciones personalizadas de selección o tecnología para un bloque dado, mientras que el mantenimiento de la arquitectura general es más flexible.

A continuación se ofrece una breve descripción de las capacidades y la funcionalidad que proporciona cada bloque.

1.2Bloque centro de interconexión de datos (DCI)

El bloque de interconexión de Data Center proporciona la capacidad de una red de comunicación entre los Data Centers. Este bloque vincula la actividad de los Data Centers para la continuidad del negocio, su recuperación ante desastres, su migración e integración.

La alta velocidad, alto rendimiento y baja latencia de servicio de red proporciona gran ancho de banda agregada entre los Data Centers. El servicio es compatible con operaciones de alto rendimiento y alta confiabilidad. El mecanismo de transporte subyacente soporta la capa 2, la capa 3 del modelo OSI, y el canal de conectividad entre fibras.

La figura 1.2 muestra el diagrama OVT (OverlayTransport Virtual), de la interconexión del Data Center para el bloque DCI.

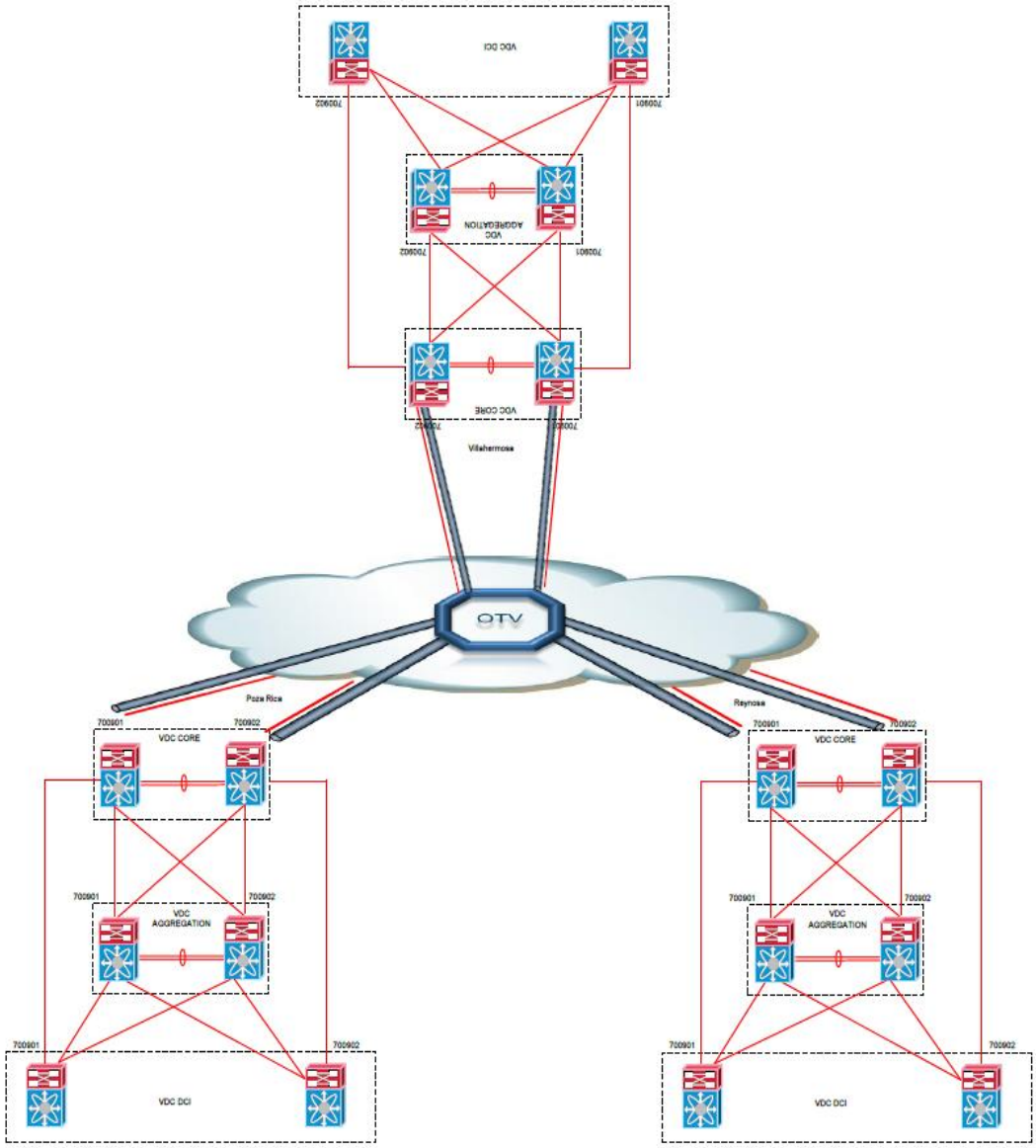


Figura 1.2 Diagrama OTV donde se involucrará el bloque DCI

1.3 Bloque de sistema de administración de red (NMS)

Un bloque de la administración se conecta a todos los elementos de la red. Proporciona servicios esenciales a la red, como servidoresproxy de autenticación, colecciones de syslog, protocolo simple de administración de redes (SNMP), capturas de traps y estaciones de gestión centralizada de varios elementos de la red.

Las herramientas de gestión de red están obligadas a proporcionar la visibilidad y el control de la arquitectura subyacente. Es indispensable tener por lo menos un mínimo de las siguientes funcionalidades:

- ➔ Gestión de fallas
- ➔ Gestión de la configuración

- ➔ Gestión de Contabilidad
- ➔ La gestión del rendimiento
- ➔ Gestión de Seguridad

Todos los componentes de la red soportan el acceso CLI y SNMP. Comunicaciones cifradas utilizando protocolos como SSH y SNMP V3 entre los diferentes componentes administrados y de la estación de gestión de red, se requieren para cumplir con los requisitos de seguridad. Estaciones de consola de administración de red se alojarán en las instalaciones de Reynosa.

Los recursos de red enviarán varios logs del sistema y traps SNMP que pueden ser utilizados para la notificación de las condiciones de alarma. Estos eventos se procesan para determinar qué eventos pueden hacer que la infraestructura y el impacto de negocios.

El rendimiento, la capacidad y el poder de los datos de utilización del tiempo histórico y / o reales de todos los elementos de la red deben ser encuestados y recolectados. Estos datos pueden ser exportados a otras herramientas para generar informes y crear alarmas basadas en umbrales.

En la figura 1.3 sepodrá observar la topología de los equipos administrativos que monitorearan los Data Centers de cada región

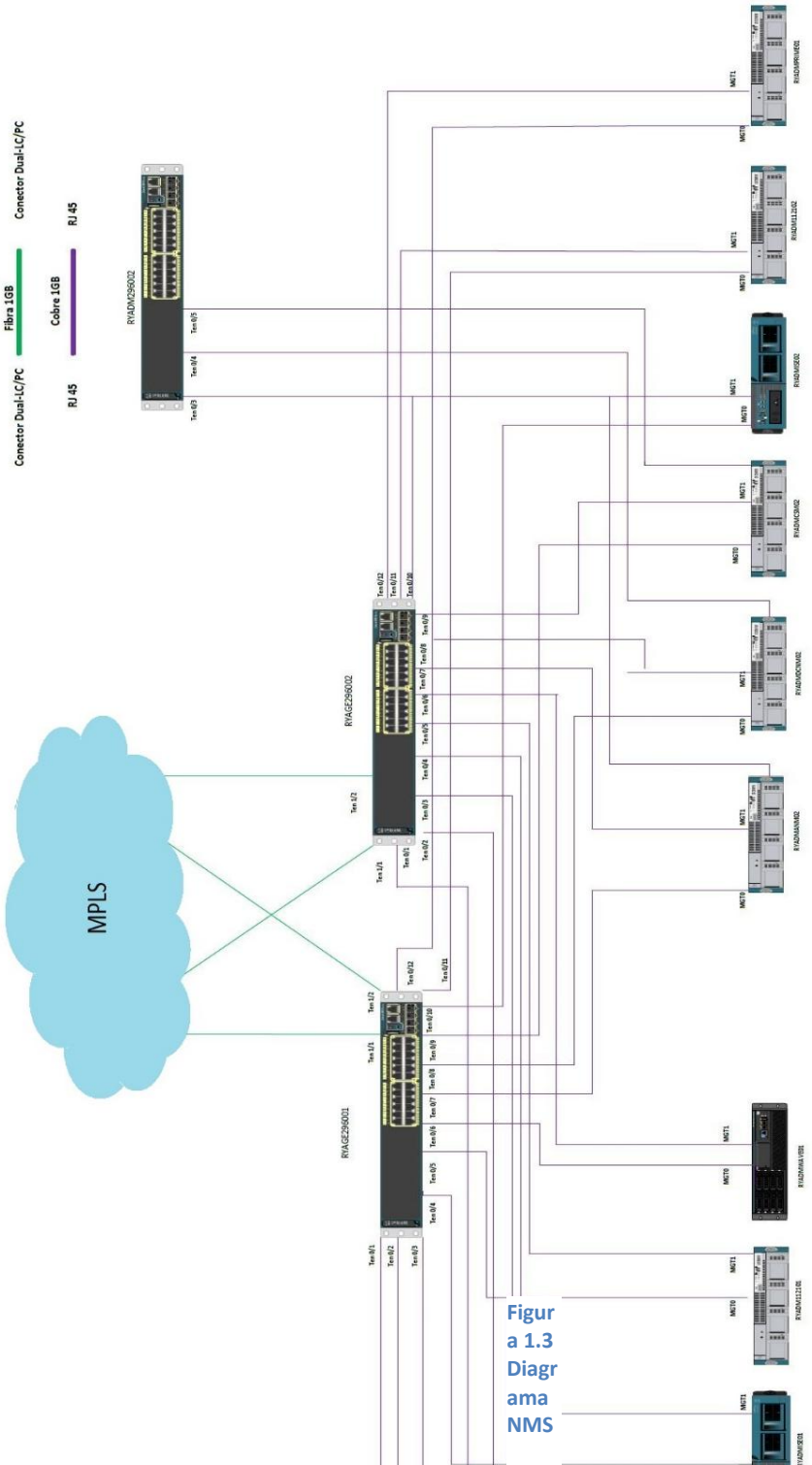


Figura 1.3 Diagrama NMS

1.4 Bloque de seguridad

El bloque de seguridad proporciona las capacidades que permiten de extremo a extremo la seguridad de la red en el Data Center.

Los aspectos de seguridad deben ser incluidos de manera integral para comprobar que no hay vulnerabilidades u otras puertas traseras que se pasan por alto en el proceso de asegurar el Data Center. La seguridad no está garantizada mediante la instalación de firewalls y sólo las sondas de detección de intrusos, sino que es fundamental contar con una política de seguridad que se alinee con los objetivos de negocio y haya sido aprobada por todas las partes involucradas.

En el contexto de la arquitectura de referencia de un Data Center, la atención se centra principalmente en los aspectos de seguridad que se tocan en LAN, SAN y la granja de servidores. En el sistema operativo (OS) el nivel de protección de los servidores no está incluido.

La seguridad de la granja de servidores está predominantemente con un enfoque por capas en servidores con una política de seguridad común y se agrupan detrás de uno o más contextos de firewalls. Aunque la detección y prevención de intrusiones (IDS / IPS) funciona mejor en las proximidades de los servidores físicos para asegurar una detección precisa de anomalías y una solución IPS basado en host deben estar en su lugar.

Los servidores de correlación trabajan entre los distintos niveles de los actuales productos y soluciones de seguridad y proporcionan el monitoreo correspondiente de las anomalías sin la carga de ser abrumados con los falsos positivos.

La figura 1.4muestra el diagrama de seguridad para un Data Center.

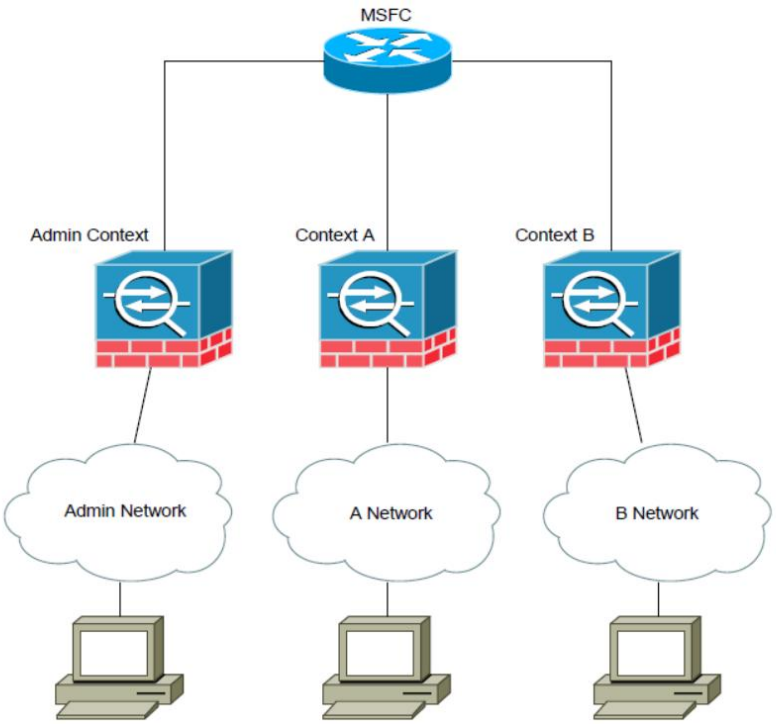


Figura 1.4 Diagrama de seguridad

1.5 Bloque de servicios de red

Este es un bloque lógico que proporciona la entrega de aplicaciones basadas en la red y servicios de optimización a los residentes de los Data Centers. Los servicios que se ofrecerán por este bloque son el balanceo de carga del servidor, firewall, prevención de intrusiones y la descarga de SSL, todos estos servicios se implementarán con una configuración redundante en sus bloques físicos. Estos servicios de red estarán basados para mejorar la escalabilidad de las aplicaciones y su disponibilidad. Mejorarán la entrega de aplicaciones a los usuarios finales, ampliarán y mejorarán la comunicación entre los niveles de la aplicación.

La capa de agregación será una localidad común para la integración de estos servicios, ya que normalmente proporciona el límite entre el nivel 2 y nivel 3 en el Data Center, y permitirá que los dispositivos de servicio puedan ser compartidos a través de múltiples switches de la capa de acceso.

La capa de servicios servirá también en 3 niveles: Web, bases de datos y aplicaciones. Estos niveles serán los que alojarán el front-end para todas las aplicaciones que serán visibles en el MPLS de la Empresa, al igual será la sede del middleware y servidores de aplicaciones, junto con el sistema de base de datos para las aplicaciones.

En la figura 1.5 se muestra el diagrama lógico del bloque de servicios.

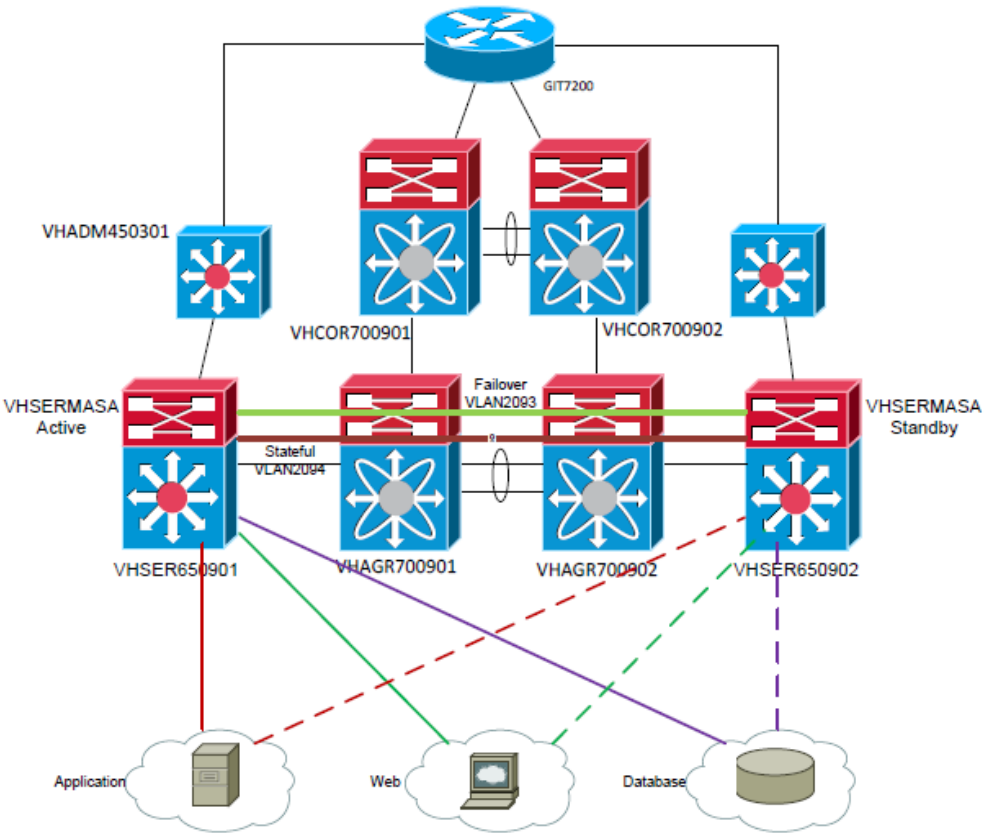


Figura 1.5 Diagrama lógico – bloque de servicios

1.6 Bloque de plataforma Citrix Cloud

Citrix CloudPlatform™ es una plataforma de software de código abierto que reúne los recursos del Data Center para construir infraestructuras públicas, privadas e híbridas como servicio (IaaS) en las diferentes clouds. Con este bloque se representarála capacidad de virtualización de los elementos de la infraestructura de red subyacente los cuales se podrán aprovechar para ofrecer múltiples end to end pools (procesos de monitoreo) lógicamente asegurados y aislados de los recursos. La virtualización ayudaráa lograr una mejor utilización de los recursos y proporcionará un mejor retorno de la inversión a través de la consolidación y estandarización de los servicios. Estos servicios basados en la red centralizada proporcionarán un rendimiento mejorado.

La siguiente figura 1.6 muestra el diagrama lógico-CITRIX Cloud

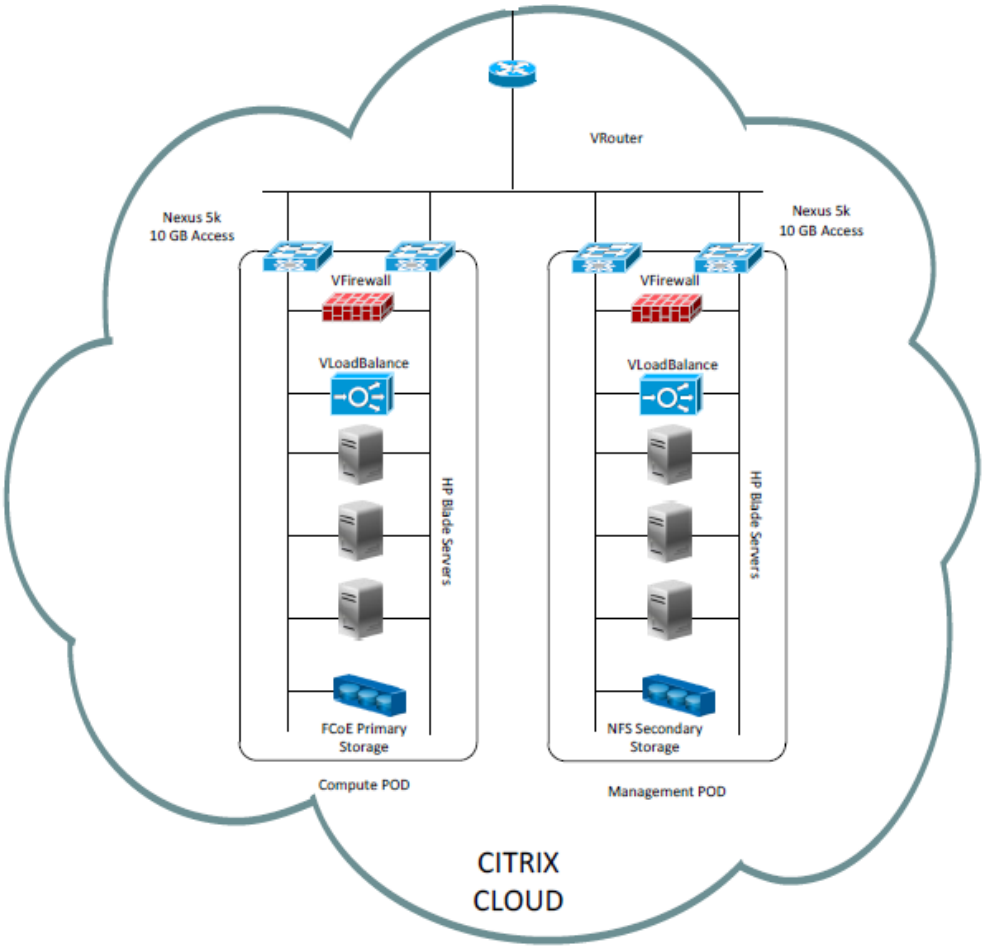


Figura 1.6 Diagrama lógico CITRIX Cloud

1.7 Bloque de core

El Bloque de Core se requerirá para mantener un alto grado de modularidad en la arquitectura general. El Bloque de Core será visto como el eje de alta velocidad que interconecta todos los otros bloques de la arquitectura, por ejemplo de la WAN, la agregación y el bloque de interconexión de Data Center. En teoría, un diseño sin infraestructura básica es posible, pero derivaría límites entre funcionalidad y rapidez y esto se convertiría en un impedimento para la expansión controlada del Data Center. Sin un bloque de Core en la solución ésta no sería una arquitectura escalable. (Véase Figura 1.7)

1.8 Bloque de agregación

El Bloque de agregación, se encontrará conectado hacia la capa de Acceso de la arquitectura, tendrá la responsabilidad principal de la distribución de miles de sesiones que entran y salen del Data Center. Los switches que se encontrarán en el Bloque de agregación son capaces de soportar múltiples interconexiones Ethernet a velocidades de 10 Gigabit y 1 Gigabit. El bloque de agregación o conocido también como distribución también proporcionará conectividad a la capa de servicios de red, que proporciona seguridad y optimización de aplicaciones. (Véase Figura 1.7)

1.9 Bloque de acceso

La capa de acceso del Data Center proporciona el nivel de apego físico a los recursos del servidor, y opera en la capa 2. La capa de acceso juega un papel fundamental en el cumplimiento de determinados requisitos del servidor, tales como la agrupación de NIC como también de la agrupación y contención de broadcast. (Véase Figura 1.7)

El bloque de acceso provee lo siguiente:

- ➔ Arquitectura de nivel de acceso flexible la cual respalda la ubicación lógica de los servidores a través de la Infraestructura de un Data Center.
- ➔ Es el primer punto de sobresuscripción en los Data Centers ya que agrega el tráfico en los enlaces ascendentes de 10 Gigabit ethernet
- ➔ Opera en capa 2.
- ➔ Opción estandarizada para la ubicación de dispositivos de acceso a nivel de red.
- ➔ Facilidad de administración con un número reducido de puntos de administración.

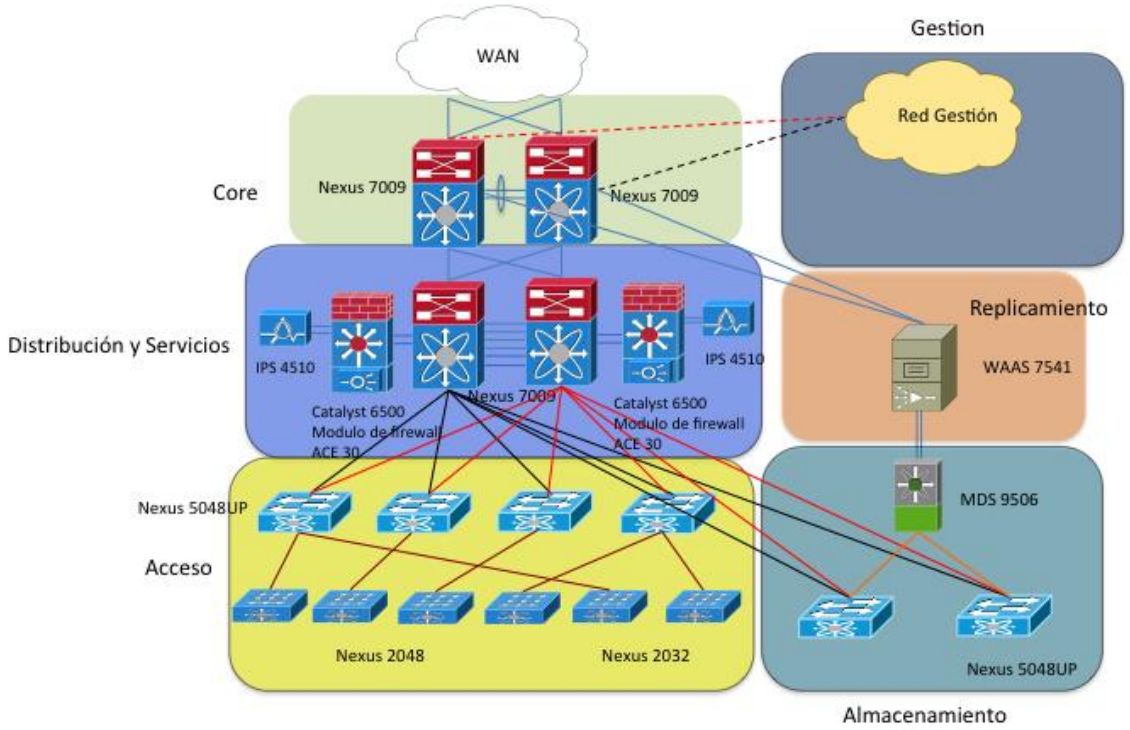


Figura 1.7 Diagrama lógico de bloques

1.10 Bloque de área de almacenamiento

El bloque de almacenamiento (SAN-Storage Area Network) proporciona la capacidad de conectar el almacenamiento relacionado con los servicios de almacenamiento.

Los servicios típicos y componentes de almacenamiento son:

- ➔ Matrices de almacenamiento
- ➔ Servidores de copia de seguridad
- ➔ Las bibliotecas de cintas o bibliotecas de cintas virtuales
- ➔ Almacenamiento de datos
- ➔ Replicación de datos de almacenamiento
- ➔ Copia de seguridad de SAN / LAN

Hoy en día, se utilizan adaptadores de bus de host (HBA´s) en los servidores para proporcionar conectividad del canal de fibra de los equipos existentes a la SAN.

En la figura 1.8 se muestra el diagrama lógico para la capa de SAN

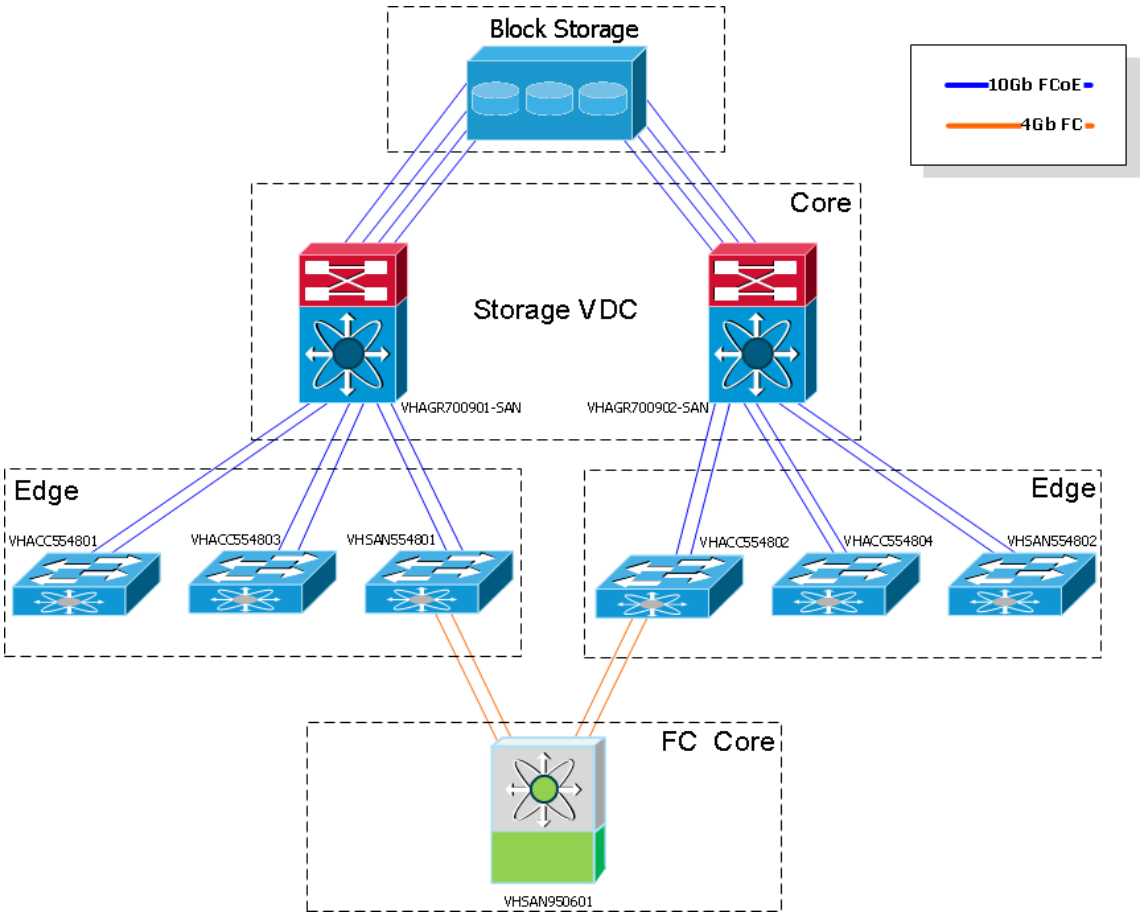


Figura 1.8 Diagrama lógico Almacenamiento

1.11 Bloque de administración

El bloque de administración proporciona la capacidad de acceder a los componentes en todos los bloques independientemente del estado de funcionamiento de estos. El Bloque de Administración nos permiteadministrar remotamente los servidores, elementos de red y cualquier otro sistema en todo momento.Existe una condición para el bloque de administración el cual consiste en que se proporcione un camino separado para la gestión del tráfico a cada dispositivo del Data Center(de red o sistemas) ya sea a través de Ethernet o comunicaciones en serie. Una red dedicada físicamente separada se utiliza para la gestión de la infraestructura de red y una red lógica separada se utiliza para los sistemas. La seguridad se implementa en este bloque para garantizar que ninguna solicitud no autorizada y no autenticada sea permitida en este bloque.

En la figura 1.9 se muestra el diagrama lógico del bloque de Administración de la red

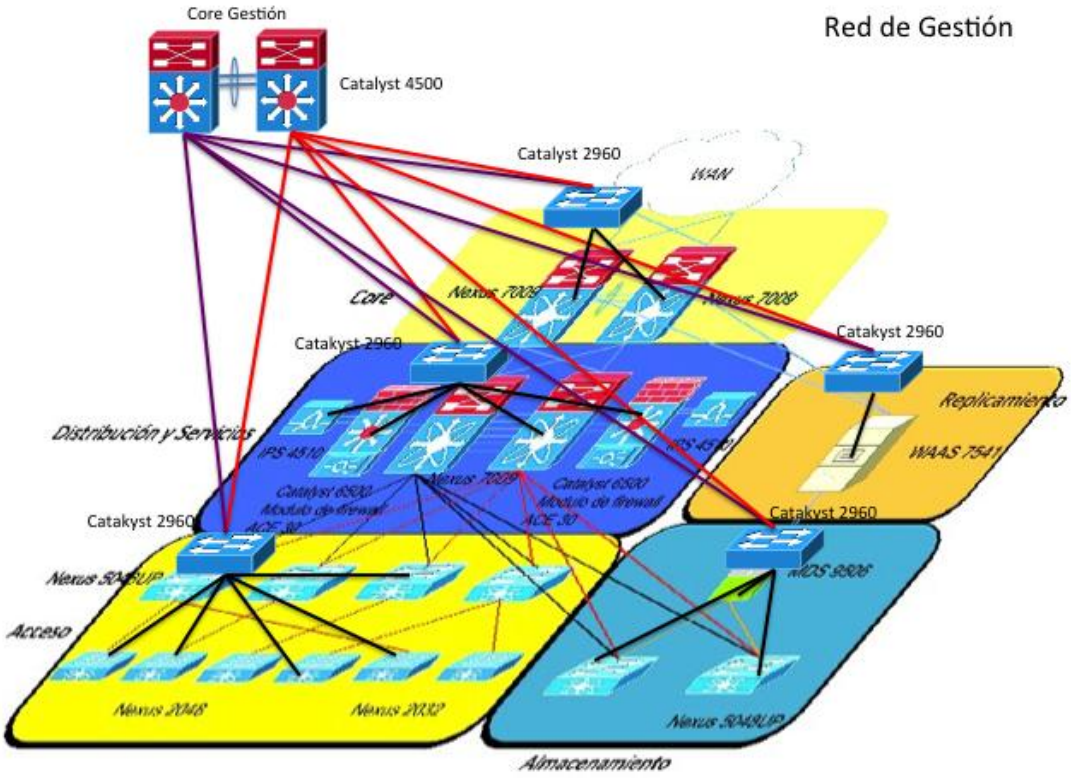


Figura 1.9 Diagrama lógico Administración

1.12 Asignación de una arquitectura para Data Center de diseño de red física

La arquitectura actúa como un marcador de posición para capturar todos los requisitos sin ahondar en detalles sobre el hardware y el software. Al asignar la arquitectura al diseño, los siguientes principios de diseño se cumplen:

- **Alta disponibilidad:** El objetivo del diseño es evitar cualquier punto único de fallo y lograr rápidas y predecibles convergencias. Los elementos elegidos y el diseño integra conceptos de N +1 de alta disponibilidad en el enlace, nodo, protocolo y nivel de sitio. Los protocolos de enrutamiento, puerto de conexión virtual, NSF / SSO, características de replicación del estado, HSRP, balanceo de carga IGP y la selección del sitio global son aprovechados para lograr estos objetivos.

- **Escalabilidad:** La arquitectura permite la expansión e incremento de elementos en cada nivel principal de la red. El diseño permite la adición de switches y otros servicios sin interrumpir los existentes. La escalabilidad se logra por múltiples maneras, por la puesta en común de los recursos para proporcionar una sola entidad agregada y/o el uso de particiones lógicas de los recursos físicos o añadiendo más dispositivos horizontalmente para apoyar el crecimiento.

- **Simplicidad:** El diseño se mantiene lo más simple posible para asegurarse de que es fácil de administrar, mantener y permitir la facilidad de expansión futura. El diseño permite rutas de tráfico fiables y trazables proporcionan determinismo en estado estacionario y conmutación por error para mejorar y apoyar las operaciones y resolución de problemas. El aislamiento de errores se consigue mediante la restricción de dominios de fallo a un tamaño manejable y rutas de datos óptimos de ingeniería usando contextos lógicos en diversos elementos de la infraestructura de manera que un problema en una parte de la red no afecta otra parte.

- **La modularidad y flexibilidad:** El diseño se hace flexible, de modo que cualquier combinación de módulos se puede implementar para los nuevos bloques de servicio existentes. El diseño es modular para permitir la fácil integración de nuevos servicios para satisfacer las crecientes necesidades de la empresa.

- **Normalización y Virtualización:** El diseño se basa en estándares y cuidando reducir el número y tipo de elementos propuestos. Los elementos elegidos para este diseño pueden proporcionar la capacidad de la virtualización y segmentación.

1.13 Consideraciones de diseño

Las consideraciones clave que se han tomado en cuenta para la formulación del diseño de bajo nivel son:

- La capacidad de cómputo soporta hasta 900 solicitudes de asignación de alrededor de 400 servicios.

- Seguridad multiempresa que permite más de una organización para compartir recursos informáticos.

- Cada usuario puede tener varios ambientes como Base de Datos, Web y aplicaciones.

- Lapresentación final al usuario del portal y un portal de auto-servicio interno donde la infraestructura como servicio (IaaS) se puede consumir de un catálogo de aplicaciones predefinidas (plantillas virtuales) proporcionadas por CITRIX.

Un mecanismo de devolución de cargo, por lo que los recursos se pueden asignar metódicamente, su consumo medido, y el costo asociado al usuario final adecuado proporcionado por Citrix.

- Firewall Virtual, Balanceo de carga virtual y Virtual Router proporcionado por CITRIX

- Firewall físico, Balanceo de carga física y Router físico para las aplicaciones Legacy.

- Conectividad de la cloud de la red externa MPLS.

- Reducir los costos y mejorar la eficiencia.

- ➔ Soporte de provisión en línea de la máquina virtual en el entorno de la Citrix cloud en términos de disponibilidad de infraestructura y conectividad.
- ➔ Permitir a los usuarios de "Legacy" un acceso seguro o servicios desarrollados en las instalaciones.
- ➔ Infraestructura escalable, flexible y confiable para satisfacer las necesidades y los servicios empresariales dinámicos.
- ➔ Reducir la complejidad y permitir la separación lógica de los niveles del Data Center
- ➔ Permitir una implementación más rápida conforme a las iniciativas empresariales.
- ➔ La infraestructura de red ágil podrá asimilar rápidamente aplicaciones actuales, como Legacy o servicios desarrollados en instalaciones e integrar nuevos sistemas o aplicaciones, como los que viven en Citrix Cloud.
- ➔ Pasar a un modelo de servicios virtualizados actuales con centralización y distribución de servicios en la cloud.
- ➔ La arquitectura debe permitir la extensión de los servicios a otro Data Center a través de Interconexión Data Center (DCI)
- ➔ Soporte de una red con alto número de servidores.
- ➔ La implementación de los Data Centers se puede replicar en sus implementaciones de Data Center
- ➔ No hay necesidad de proporcionar firewalls, IPS y servicios de balanceo de carga de las aplicaciones que residen en la Citrix Cloud. Citrix proporcionará estos servicios en su router virtual, actuando también como la puerta de enlace predeterminada para este entorno.
- ➔ La Capa de Agregación Cisco proveerá de firewall, IPS o servicios de balanceo de carga para aplicaciones que no se ejecutan en Citrix Cloud de acuerdo a las necesidades de cada aplicación.
- ➔ Si el entorno de Citrix Cloud puede requerir de balanceo de carga de servicios externos, estos requisitos no serán provistos, en cambio, Citrix puede hacer uso de Netscalers.
- ➔ El balanceo de carga para aplicaciones que no viven en Citrix Cloud estará a cargo de los servicios del ACE.
- ➔ No hay necesidad de ejecutar un firewall que actúe como una frontera o firewall perimetral.
- ➔ El entorno de Citrix Cloud utilizará VNX como el almacenamiento primario con FCoE, mientras Isilon proporcionará almacenamiento secundario.
- ➔ Todos los servidores físicos que pertenecen al entorno de Citrix Cloud usarán tarjetas CNA para la conectividad FCoE.
- ➔ Todos los servidores físicos fuera del entorno de la Citrix Cloud usarán tarjetas HBA conectadas directamente al switch MDS.

- El entorno de Citrix Cloud utilizará su propia VLAN y direcciones IP.

- El Data Center de Villahermosa debe actuar como el Data Center principal para Citrix Cloud.

- HP y EMC ofrecerán esquema WWN para la zonificación aplicación en la solución de Cisco.
- El Core apoyará capa 3 con conectividad pura a todos los otros bloques funcionales. Las interfaces entre la base y agregación de ancho de banda a utilizar los puertos dedicados 10GE.

- Los firewalls, balanceadores de carga y otros elementos de servicios de optimización de aplicaciones se pueden implementar en el modo de capa 2.

- La gestión de acceso a los recursos del Data Center se facilitará a través de la zona de administración. La zona de administración tendrá acceso a todos los otros bloques funcionales que se aplicará mediante el uso conjunto físicamente discreta de firewalls y de infraestructura de conmutación.

- En el caso del G10 BladeSystems HP, en entornos de servidores virtualizados, se utilizará un módulo de paso a través de un dispositivo externo TdR. Este método se puede usar para habilitar 10 G / 10 G capacidad FCoE a los sistemas blade HP.

- La solución de copia de seguridad de red, utiliza la red de producción como de transporte. El tráfico de backup de red utilizará los mismos enlaces, switches y servidores de seguridad como el tráfico del servidor estándar.

- La solución SAN se llevará a cabo mediante el uso de un diseño de borde de Core.

- Los administradores de los elementos de red se pueden implementar en Data Center Reynosa para ayudar a facilitar la gestión de la infraestructura de red y proporcionar una mayor visibilidad en la red.

Capítulo 2: Diseño de infraestructura

2.1 Descripción de hardware y software

La tabla 2.1muestra el hardware y software que será configurado durante la etapa de implementación de la solución:

Tabla 2.1 Componentes de Hardware y Software

Numero de Parte	Cantidad	Descripción	Nivel
N7K-C7009-B2S2-R	2	Nexus 7009 Bundle (Chassis 2xSUP2 5xFAB2) No Power Supplies	Core
N7K-C7009-B2S2-R	2	Nexus 7009 Bundle (Chassis 2xSUP2 5xFAB2) No Power Supplies	Agregación
IPS-4510-K9	2	IPS 4510 with SW 4x SFP/SFP+ 6 GE Cu 2xGe Mgmt.	Servicios
WS-C6509-E	2	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray	Servicios
ACE30-MOD-K9	4	Application Control Engine 30 Hardware	Servicios
WS-SVC-ASA-SM1-K7	2	ASA Services Module for Catalyst 6500-E NPE	Servicios
N5K-C5548UP-FA	6	Nexus 5548 UP Chassis 32 10GbE Ports 2 PS 2 Fans	Acceso
DS-C9506	1	MDS 9506 Chassis	Almacenamiento
WS-C4503-E	2	Cat4500 E-Series 3-Slot Chassis fan no ps	Administración
WS-C2960S-24TS-L	8	Catalyst 2960S 24 GigE 4 x SFP LAN Base	Administración
WAVE-7541-K9	1	Wide Area Virtualization Engine 7541	DCI

Nota:

Sólo cinco (5) de los ocho switches (8) Cat2960 se utilizan en el Data Center. Los switches restantes serán utilizados en un futuro.

2.2 Sistemas operativos

Las versiones de los sistema operativos que se cargarán en los dispositivos de red se muestran en la tabla 2.2, estos sistemas operativos fueron escogidos originalmente en base a las características, los requisitos y la validación de hardware para los componentes que se van a utilizar. Algunas de estas versiones se pueden cambiar durante la fase de ejecución si se produce un error desconocido.

En la tabla 2.2 se muestra las versiones del SO para cada dispositivo del Data Center

Tabla 2.2 IOS-Versiones para los componentes de hardware

Dispositivo	Versión del SO
N7K-C7009-B2S2-R	NxOS EPLD 6.1(2a), NxOS Kick Start 6.1.2, NxOS System Software 6.1.2
N7K-C7009-B2S2-R	IPS 7.1.6E4
WS-C6509-E	12.2(33)SXJ1
ACE30-MOD-K9	A5(2.1)
WS-SVC-ASA-SM1-K7	ASA-SM 9.1(1)/ ASDM 7.1(2)
N5K-C5548UP-FA	NxOS Kick Start 6.0(2)N1(1), NxOS System Software 6.0(2)N1(1)
DS-C9506	5.2.1
WS-C4503-E	12.2(54)SG1
WS-C2960S-24TS-L	12.2(58)SE2
WAVE-7541-K9	5.0.3c
DCNM	6.1.2
ANM	5.2
CSM	4.4
ACS	5.3
Prime LMS	4.2

2.3 Convenciones de nomenclatura

La estrategia general para la convención de nombres es el de identificar fácilmente los dispositivos o funciones dentro de la red. La convención de nomenclatura generalmente incluye la ubicación del equipo, bloque funcional, tipo de dispositivo y por último un identificador de número consecutivo. Todos los nombres de host se representan en mayúsculas.

Una convención de nomenclatura típica que Cisco Advanced Services recomienda a las empresas es la siguiente:

Sintaxis de Dispositivo: Ubicación + Bloque Funcional + Número y nombre del dispositivo + Número ID

Ejemplo:

VHDCI700901

La tabla 2.3 muestra la convención de nomenclatura para cada ubicación funcional.

Tabla 2.3 Ubicación funcional-Convención de Nomeclatura

Abreviación	Ubicación
VH	Villa Hermosa
RY	Reynosa
VZ	Veracruz
CC	Ciudad del Carmen
PR	Poza Rica

La tabla 2.4 muestra la convención de nomenclatura para cada bloque o módulo funcional.

Tabla 2.4 Bloque funcional. Convención de nomenclatura

Abreviación	Tipo
DCI	Data Center Interconnect (Interconexión de Data Centers)
COR	Core Module (Módulo de Core)
AGR	Aggregation Module (Módulo almacenamiento de agregación)
ADM	Management Module (Módulo de administración)
SAN	Storage Area Network Module (Módulo de almacenamiento)
REP	Storage Replication Module (Módulo de replicación)
ACC	Access (Acceso)
SER	Services (Servicios)

La tabla 2.5 muestra la convención de nomenclatura para cada dispositivo.

Tabla 2.5 Dispositivo – Convención de nomenclatura

Dispositivo	Capa	Nombre
Nexus 7009-1	Admin VCD	VHCOR700901
	Core VDC	VHCOR700901-CORE
	Replication VDC	VHCOR700901-REPLICATION
Nexus 7009-2	Admin VDC	VHCOR700902
	Core VDC	VHCOR700902-CORE

	Replication VDC	VHCOR700902-REPLICATION
Nexus 7009-1	Admin VDC	VHAGG700901
	Aggregation VDC	VHAGR700901-AGGREGATION
	DCI VDC	VHAGR700901-DCI
	Storage VDC	VHAGR700901-SAN
Nexus 7009-2	Admin VDC	VHAGR700902
	Aggregation VDC	VHAGR700902-AGGREGATION
	DCI VDC	VHAGR700902-DCI
	Storage VDC	VHAGR700902-SAN
Catalyst 6509-1	Services	VHSER650901
Catalyst 6509-2	Services	VHSER650902
IPS 4510-1	Services	VHSER451001
FW Module-1	Services	VHSERMASA01
FW Module-2	Services	VHSERMASA02
ACE Module-1	Services	VHSERMACE01
ACE Module-2	Services	VHSERMACE02
Nexus 5548-1	Access/SAN	VHSAN554801
Nexus 5548-2	Access/SAN	VHSAN554802
Nexus 5548-3	Access	VHACC554801
Nexus 5548-4	Access	VHACC554802
Nexus 5548-5	Access	VHACC554803
Nexus 5548-6	Access	VHACC554804
MDS 9506	SAN	VHSAN950601
WAE 7541	Replication	VHREP754101
Catalyst 4503-1	Management	VHADM450301
Catalyst 4503-2	Management	VHADM450302
Catalyst 2960-S-1	Management	VHADM296001
Catalyst 2960-S-2	Management	VHADM296002
Catalyst 2960-S-3	Management	VHADM296003
Catalyst 2960-S-4	Management	VHADM296004
Catalyst 2960-S-5	Management	VHADM296005
Catalyst 2960-S-6	Management	VHADM296006
Catalyst 2960-S-7	Management	VHADM296007
Catalyst 2960-S-8	Management	VHADM296008

2.4 Mapeo de puertos

La infraestructura de interconexiones son interfaces de punto a punto que se asignan para proporcionar interconexión entre los distintos elementos de la red en el Data Center. Las siguientes tablas de esta sección muestran la conectividad de la asignación de puertos para cada módulo.

Nota:

Tenga en cuenta que no se muestran los puertos reservados o no utilizados.

En la tabla 2.6 se muestra el mapeo de puertos del módulo de Administración

Tabla 2.6 Mapeo de puertos – Módulo de administración

Equipo A	Tipo	Puerto A	Conector	Equipo B	Tipo	Puerto B	Conector
VHADM296001	Gig	0/1	RJ-45	VHCOR700901	Gig	MGT0	RJ-45
VHADM296001	Gig	0/2	RJ-45	VHCOR700902	Gig	MGT0	RJ-45
VHADM296001	Gig	0/3		Free			
VHADM296001	Gig	0/4		Free			
VHADM296001	Gig	0/5		Free			
VHADM296001	Gig	0/6		Free			
VHADM296001	Gig	0/7		Free			
VHADM296001	Gig	0/8		Free			
VHADM296001	Gig	0/9		Free			
VHADM296001	Gig	0/10		Free			
VHADM296001	Gig	0/11		Free			
VHADM296001	Gig	0/12		Free			
VHADM296001	Gig	0/13		Free			
VHADM296001	Gig	0/14		Free			
VHADM296001	Gig	0/15		Free			
VHADM296001	Gig	0/16		Free			
VHADM296001	Gig	0/17		Free			
VHADM296001	Gig	0/18		Free			
VHADM296001	Gig	0/19		Free			
VHADM296001	Gig	0/20		Free			
VHADM296001	Gig	0/21		Free			
VHADM296001	Gig	0/22		Free			
VHADM296001	Gig	0/23		Free			
VHADM296001	Gig	0/24		Reserved for Administrators			
VHADM296001	Gig	1/1	Dual LC/PC	VHADM450301	Gig	3/1	GLC-SX-MMD

VHADM296001	Gig	1/2	Dual LC/PC	VHADM450302	Gig	3/1	GLC-SX-MMD
VHADM296001	Gig	1/3		Free			
VHADM296001	Gig	1/4		Free			
VHADM296002	Gig	0/1	RJ-45	VHCOR700901		MGT1	RJ-45
VHADM296002	Gig	0/2	RJ-45	VHCOR700902		MGT1	RJ-45
VHADM296002	Gig	0/3		Free			
VHADM296002	Gig	0/4		Free			
VHADM296002	Gig	0/5		Free			
VHADM296002	Gig	0/6		Free			
VHADM296002	Gig	0/7		Free			
VHADM296002	Gig	0/8		Free			
VHADM296002	Gig	0/9		Free			
VHADM296002	Gig	0/10		Free			
VHADM296002	Gig	0/11		Free			
VHADM296002	Gig	0/12		Free			
VHADM296002	Gig	0/13		Free			
VHADM296002	Gig	0/14		Free			
VHADM296002	Gig	0/15		Free			
VHADM296002	Gig	0/16		Free			
VHADM296002	Gig	0/17		Free			
VHADM296002	Gig	0/18		Free			
VHADM296002	Gig	0/19		Free			
VHADM296002	Gig	0/20		Free			
VHADM296002	Gig	0/21		Free			
VHADM296002	Gig	0/22		Free			
VHADM296002	Gig	0/23		Free			
VHADM296002	Gig	0/24		Reserved for Administrators			
VHADM296002	Gig	1/1	Dual LC/PC	VHADM450301	Gig	3/2	GLC-SX-MMD
VHADM296002	Gig	1/2	Dual LC/PC	VHADM450302	Gig	3/2	GLC-SX-MMD
VHADM296002	Gig	1/3		Free			
VHADM296002	Gig	1/4		Free			
VHADM296003	Gig	0/1	RJ-45	VHAGR700901	Gig	MGT0	RJ-45
VHADM296003	Gig	0/2	RJ-45	VHSER650901	Gig	5/3	RJ-45
VHADM296003	Gig	0/3	RJ-45	VHSER650902	Gig	5/3	RJ-45
VHADM296003	Gig	0/4	RJ-45	VHSEC451001	Gig	MGT	RJ-45
VHADM296003	Gig	0/5	RJ-45	VHAGR700902	Gig	MGT1	RJ-45
VHADM296003	Gig	0/6		Free			
VHADM296003	Gig	0/7		Free			
VHADM296003	Gig	0/8		Free			
VHADM296003	Gig	0/9		Free			
VHADM296003	Gig	0/10	RJ-45	MGMT_EMC	Gig		RJ-45

VHADM296003	Gig	0/11	RJ-45	MGMT_EMC	Gig		RJ-45
VHADM296003	Gig	0/12	RJ-45	MGMT_EMC	Gig		RJ-45
VHADM296003	Gig	0/13		Free			
VHADM296003	Gig	0/14		Free			
VHADM296003	Gig	0/15		Free			
VHADM296003	Gig	0/16		Free			
VHADM296003	Gig	0/17		Free			
VHADM296003	Gig	0/18		Free			
VHADM296003	Gig	0/19		Free			
VHADM296003	Gig	0/20		Free			
VHADM296003	Gig	0/21		Free			
VHADM296003	Gig	0/22		Free			
VHADM296003	Gig	0/23		Free			
VHADM296003	Gig	0/24		Reserved for Administrators			
VHADM296003	Gig	1/1	Dual LC/PC	VHADM450301		3/3	GLC-SX-MMD
VHADM296003	Gig	1/2	Dual LC/PC	VHADM450302	Gig	3/3	GLC-SX-MMD
VHADM296003	Gig	1/3		Free			
VHADM296003	Gig	1/4		Free			
VHADM296004	Gig	0/1	RJ-45	VHAGR700902		MGT0	RJ-45
VHADM296004	Gig	0/2	RJ-45	VHSER650901	Gig	6/3	RJ-45
VHADM296004	Gig	0/3	RJ-45	VHSER650902	Gig	6/3	RJ-45
VHADM296004	Gig	0/4	RJ-45	VHSEC451002	Gig	MGT	RJ-45
VHADM296004	Gig	0/5	RJ-45	VHSAN950601	Gig	MGT0	RJ-45
VHADM296004	Gig	0/6	RJ-45	VHACC554801	Gig	MGT	RJ-45
VHADM296004	Gig	0/7	RJ-45	VHACC554802	Gig	MGT	RJ-45
VHADM296004	Gig	0/8	RJ-45	VHACC554803	Gig	MGT	RJ-45
VHADM296004	Gig	0/9	RJ-45	VHAGR700901	Gig	MGT1	RJ-45
VHADM296004	Gig	0/10	RJ-45	MGMT_EMC	Gig		RJ-45
VHADM296004	Gig	0/11	RJ-45	MGMT_EMC	Gig		RJ-45
VHADM296004	Gig	0/12	RJ-45	MGMT_EMC	Gig		RJ-45
VHADM296004	Gig	0/13		Free			
VHADM296004	Gig	0/14		Free			
VHADM296004	Gig	0/15		Free			
VHADM296004	Gig	0/16		Free			
VHADM296004	Gig	0/17		Free			
VHADM296004	Gig	0/18		Free			
VHADM296004	Gig	0/19		Free			
VHADM296004	Gig	0/20		Free			
VHADM296004	Gig	0/21		Free			
VHADM296004	Gig	0/22		Free			
VHADM296004	Gig	0/23		Free			

VHADM296004	Gig	0/24		Reserved for Administrators			
VHADM296004	Gig	1/1	Dual LC/PC	VHADM450301		3/4	GLC-SX-MMD
VHADM296004	Gig	1/2	Dual LC/PC	VHADM450302		3/4	GLC-SX-MMD
VHADM296004	Gig	1/3		Free			
VHADM296004	Gig	1/4		Free			
VHADM296005	Gig	0/1	RJ-45	VHSAN950601		MGT1	RJ-45
VHADM296005	Gig	0/2	RJ-45	VHACC554804		MGT	RJ-45
VHADM296005	Gig	0/3	RJ-45	VHSAN554801		MGT	RJ-45
VHADM296005	Gig	0/4	RJ-45	VHSAN554802		MGT	RJ-45
VHADM296005	Gig	0/5	RJ-45	VHREP754101		MGT	RJ-45
VHADM296005	Gig	0/6		Free			
VHADM296005	Gig	0/7		Free			
VHADM296005	Gig	0/8		Free			
VHADM296005	Gig	0/9		Free			
VHADM296005	Gig	0/10		Free			
VHADM296005	Gig	0/11		Free			
VHADM296005	Gig	0/12		Free			
VHADM296005	Gig	0/13		Free			
VHADM296005	Gig	0/14		Free			
VHADM296005	Gig	0/15		Free			
VHADM296005	Gig	0/16		Free			
VHADM296005	Gig	0/17		Free			
VHADM296005	Gig	0/18		Free			
VHADM296005	Gig	0/19		Free			
VHADM296005	Gig	0/20		Free			
VHADM296005	Gig	0/21		Free			
VHADM296005	Gig	0/22		Free			
VHADM296005	Gig	0/23		Free			
VHADM296005	Gig	0/24		Reserved for Administrators			
VHADM296005	Gig	1/1	Dual LC/PC	VHADM450301	Gig		GLC-SX-MMD
VHADM296005	Gig	1/2	Dual LC/PC	VHADM450302	Gig		GLC-SX-MMD
VHADM296005	Gig	1/3		Free			
VHADM296005	Gig	1/4		Free			
VHADM450301	Gig	1/1	Not available	Not available			
VHADM450301	Gig	1/2	Not available	Not available			
VHADM450301	Gig	1/3	Dual LC/PC	VHADM450302	Gig	1/3	
VHADM450301	Gig	1/4		Free			
VHADM450301	Gig	1/5	Dual LC/PC	VHADM450302	Gig	1/5	
VHADM450301	Gig	2/1		Free			
VHADM450301	Gig	2/2		Free			
VHADM450301	Gig	2/3		Free			

VHADM450301	Gig	2/4		Free			
VHADM450301	Gig	2/5		Free			
VHADM450301	Gig	2/6		Free			
VHADM450301	Gig	2/7		Free			
VHADM450301	Gig	2/8		Free			
VHADM450301	Gig	2/9		Free			
VHADM450301	Gig	2/10		Free			
VHADM450301	Gig	2/11		Free			
VHADM450301	Gig	2/12		Free			
VHADM450301	Gig	2/13		Free			
VHADM450301	Gig	2/14		Free			
VHADM450301	Gig	2/15		Free			
VHADM450301	Gig	2/16		Free			
VHADM450301	Gig	2/17		Free			
VHADM450301	Gig	2/18		Free			
VHADM450301	Gig	2/19		Free			
VHADM450301	Gig	2/20		Free			
VHADM450301	Gig	2/21		Free			
VHADM450301	Gig	2/22		Free			
VHADM450301	Gig	2/23		Free			
VHADM450301	Gig	2/24		Free			
VHADM450301	Gig	2/25		Free			
VHADM450301	Gig	2/26		Free			
VHADM450301	Gig	2/27		Free			
VHADM450301	Gig	2/28		Free			
VHADM450301	Gig	2/29		Free			
VHADM450301	Gig	2/30		Free			
VHADM450301	Gig	2/31		Free			
VHADM450301	Gig	2/32		Free			
VHADM450301	Gig	2/33		Free			
VHADM450301	Gig	2/34		Free			
VHADM450301	Gig	2/35		Free			
VHADM450301	Gig	2/36		Free			
VHADM450301	Gig	2/37		Free			
VHADM450301	Gig	2/38		Free			
VHADM450301	Gig	2/39		Free			
VHADM450301	Gig	2/40		Free			
VHADM450301	Gig	2/41		Free			
VHADM450301	Gig	2/42		Free			
VHADM450301	Gig	2/43		Free			
VHADM450301	Gig	2/44		Free			

VHADM450301	Gig	2/45		Free			
VHADM450301	Gig	2/46		Free			
VHADM450301	Gig	2/47		Free			
VHADM450301	Gig	2/48		Free			
VHADM450301	Gig	3/1	Dual LC/PC	VHADM296001		1/1	GLC-SX-MMD
VHADM450301	Gig	3/2	Dual LC/PC	VHADM296002	Gig	1/1	GLC-SX-MMD
VHADM450301	Gig	3/3	Dual LC/PC	VHADM296003	Gig	1/1	GLC-SX-MMD
VHADM450301	Gig	3/4	Dual LC/PC	VHADM296004	Gig	1/1	GLC-SX-MMD
VHADM450301	Gig	3/5	Dual LC/PC	VHADM296005	Gig	1/1	GLC-SX-MMD
VHADM450301	Gig	3/6	Dual LC/PC	Switch HP MGT			
VHADM450301	Gig	3/7		Free			
VHADM450301	Gig	3/8		Free			
VHADM450301	Gig	3/9	Dual LC/PC	VHSER650901	Gig	5/1	GLC-SX-MMD
VHADM450301	Gig	3/10	Dual LC/PC	Free	Gig		GLC-SX-MMD
VHADM450301	Gig	3/11	Dual LC/PC	Free	Gig		GLC-SX-MMD
VHADM450301	Gig	3/12	Dual LC/PC	7600 GIT	Gig	TBD	
VHADM450302	Gig	1/1	Not available	Not available	Gig	1/1	GLC-SX-MMD
VHADM450302	Gig	1/2	Not available	Not available	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	1/3	Dual LC/PC	VHADM450301	Gig		
VHADM450302	Gig	1/4	Free	Free			
VHADM450302	Gig	1/5	Dual LC/PC	VHADM450301	Gig		
VHADM450302	Gig	2/1		Free			
VHADM450302	Gig	2/2		Free			
VHADM450302	Gig	2/3		Free			
VHADM450302	Gig	2/4		Free			
VHADM450302	Gig	2/5		Free			
VHADM450302	Gig	2/6		Free			
VHADM450302	Gig	2/7		Free			
VHADM450302	Gig	2/8		Free			
VHADM450302	Gig	2/9		Free			
VHADM450302	Gig	2/10		Free			
VHADM450302	Gig	2/11		Free			
VHADM450302	Gig	2/12		Free			
VHADM450302	Gig	2/13		Free			
VHADM450302	Gig	2/14		Free			
VHADM450302	Gig	2/15		Free			
VHADM450302	Gig	2/16		Free			
VHADM450302	Gig	2/17		Free			
VHADM450302	Gig	2/18		Free			
VHADM450302	Gig	2/19		Free			
VHADM450302	Gig	2/20		Free			

VHADM450302	Gig	2/21		Free			
VHADM450302	Gig	2/22		Free			
VHADM450302	Gig	2/23		Free			
VHADM450302	Gig	2/24		Free			
VHADM450302	Gig	2/25		Free			
VHADM450302	Gig	2/26		Free			
VHADM450302	Gig	2/27		Free			
VHADM450302	Gig	2/28		Free			
VHADM450302	Gig	2/29		Free			
VHADM450302	Gig	2/30		Free			
VHADM450302	Gig	2/31		Free			
VHADM450302	Gig	2/32		Free			
VHADM450302	Gig	2/33		Free			
VHADM450302	Gig	2/34		Free			
VHADM450302	Gig	2/35		Free			
VHADM450302	Gig	2/36		Free			
VHADM450302	Gig	2/37		Free			
VHADM450302	Gig	2/38		Free			
VHADM450302	Gig	2/39		Free			
VHADM450302	Gig	2/40		Free			
VHADM450302	Gig	2/41		Free			
VHADM450302	Gig	2/42		Free			
VHADM450302	Gig	2/43		Free			
VHADM450302	Gig	2/44		Free			
VHADM450302	Gig	2/45		Free			
VHADM450302	Gig	2/46		Free			
VHADM450302	Gig	2/47		Free			
VHADM450302	Gig	2/48		Free			
VHADM450302	Gig	3/1	Dual LC/PC	VHADM296001	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	3/2	Dual LC/PC	VHADM296002	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	3/3	Dual LC/PC	VHADM296003	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	3/4	Dual LC/PC	VHADM296004	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	3/5	Dual LC/PC	VHADM296005	Gig	1/2	GLC-SX-MMD
VHADM450302	Gig	3/6	Dual LC/PC	Switch HP MGT			
VHADM450302	Gig	3/7		Free			
VHADM450302	Gig	3/8		Free			
VHADM450302	Gig	3/9	Dual LC/PC	VHSER650902	Gig	5/1	GLC-SX-MMD
VHADM450302	Gig	3/10	Dual LC/PC	Free	Gig		GLC-SX-MMD
VHADM450302	Gig	3/11	Dual LC/PC	Free	Gig		GLC-SX-MMD
VHADM450302	Gig	3/12	Dual LC/PC	7600 GIT	Gig	TBD	GLC-SX-MMD

En la tabla 2.7 se muestra el mapeo de puertos del módulo de Agregación.

Tabla 2.7 Mapeo de puertos- Módulo de Agregación

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHAGR700901	Mgt0	1/1	RJ-45	VHADM296003	Gig	0/1	RJ-45
VHAGR700901	Mgt1	2/1	RJ-45	VHADM296004	Gig	0/9	RJ-45
VHAGR700901	Ten	3/1	Dual SC/PC	VHAGR700902	Ten	3/1	X2-10GB-SR
VHAGR700901	Ten	3/2	Dual SC/PC	VHCOR700901	Ten	3/2	X2-10GB-SR
VHAGR700901	Ten	3/3	Dual SC/PC	VHAGR700902	Ten	3/3	X2-10GB-SR
VHAGR700901	Ten	3/4	Dual SC/PC	VHCOR700901	Ten	3/4	X2-10GB-SR
VHAGR700901	Ten	3/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	3/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	3/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	3/8	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	4/1	Dual SC/PC	VHAGR700902	Ten	4/1	X2-10GB-SR
VHAGR700901	Ten	4/2	Dual SC/PC	VHCOR700902	Ten	4/2	X2-10GB-SR
VHAGR700901	Ten	4/3	Dual SC/PC	VHAGR700902	Ten	4/3	X2-10GB-SR
VHAGR700901	Ten	4/4	Dual SC/PC	VHCOR700901	Ten	4/4	X2-10GB-SR
VHAGR700901	Ten	4/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	4/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	4/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	4/8	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	5/1	Dual SC/PC	DD	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	5/2	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	5/3	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	5/4	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	5/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	5/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	5/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	5/8	Dual SC/PC	VHAGR700902	Ten	5/8	X2-10GB-SR
VHAGR700901	Ten	6/1	Dual SC/PC	DD	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	6/2	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	6/3	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	6/4	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700901	Ten	6/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	6/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	6/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700901	Ten	6/8	Dual SC/PC	VHAGR700902	Ten	6/8	X2-10GB-SR
VHAGR700901	Ten	8/1	Dual LC/PC	VHAGR700902	Ten	8/1	SFP-10G-SR
VHAGR700901	Ten	8/2	Dual LC/PC	VHSER650901	Ten	4/1	SFP-10G-SR
VHAGR700901	Ten	8/3	Dual LC/PC	VHACC554801	Ten	1/27	SFP-10G-SR

VHAGR700901	Ten	8/4	Dual LC/PC	VHACC554801	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	8/5	Dual LC/PC	VHACC554803	Ten	1/27	SFP-10G-SR
VHAGR700901	Ten	8/6	Dual LC/PC	VHACC554803	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	8/7	Dual LC/PC	VHACC554804	Ten	1/27	SFP-10G-SR
VHAGR700901	Ten	8/8	Dual LC/PC	VHACC554804	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	8/9	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700901	Ten	8/10	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700901	Ten	8/11	Dual LC/PC	VHACC554801	Ten	1/25	SFP-10G-SR
VHAGR700901	Ten	8/12	Dual LC/PC	VHACC554803	Ten	1/25	SFP-10G-SR
VHAGR700901	Ten	8/13	Dual LC/PC	VHSAN554801	Ten	1/25	SFP-10G-SR
VHAGR700901	Ten	8/14	Dual LC/PC	Free	Ten		SFP-10G-SR
VHAGR700901	Ten	8/15	Dual LC/PC	ISILON	Gig	TBD	SFP-10G-SR
VHAGR700901	Ten	8/16	Dual LC/PC	Free	Gig	TBD	SFP-10G-SR
VHAGR700901	Ten	8/17	Dual LC/PC	VHSER650902	Ten	4/1	SFP-10G-SR
VHAGR700901	Ten	8/18	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700901	Ten	8/19	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700901	Ten	8/20	Dual LC/PC	ISILON	Ten		GLC-SX-MMD
VHAGR700901	Gig	8/21	RJ-45	Data_Mover_01	Gig	TBD	RJ-45
VHAGR700901	Gig	8/22	RJ-45	Data_Mover_02	Gig	TBD	RJ-45
VHAGR700901	Gig	8/23	RJ-45	Data_Mover_03	Gig	TBD	RJ-45
VHAGR700901	Gig	8/24	Dual LC/PC	Data_Mover_01	Gig	TBD	GLC-SX-MMD
VHAGR700901	Gig	8/25	Dual LC/PC	Data_Mover_02	Gig	TBD	GLC-SX-MMD
VHAGR700901	Gig	8/26	Dual LC/PC	Data_Mover_03	Gig	TBD	GLC-SX-MMD
VHAGR700901	Ten	8/27	Dual SC/PC	VHAGR700901	Ten	8/31	SFP-10G-SR
VHAGR700901	Ten	8/28	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700901	Ten	8/29	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700901	Ten	8/30	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700901	Ten	8/31	Dual SC/PC	VHAGR700901	Ten	8/27	SFP-10G-SR
VHAGR700901	Ten	8/32	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700901	Ten	9/1	Dual LC/PC	VHAGR700902	Ten	9/1	SFP-10G-SR
VHAGR700901	Ten	9/2	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700901	Ten	9/3	Dual LC/PC	VHACC554802	Ten	1/27	SFP-10G-SR
VHAGR700901	Ten	9/4	Dual LC/PC	VHACC554802	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	9/5	Dual LC/PC	VHSAN554801	Ten	1/27	SFP-10G-SR
VHAGR700901	Ten	9/6	Dual LC/PC	VHSAN554801	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	9/7	Dual LC/PC	VHSAN554802	Ten	1/27	SFP-10G-SR
VHAGR700901	Ten	9/8	Dual LC/PC	VHSAN554802	Ten	1/28	SFP-10G-SR
VHAGR700901	Ten	9/9	Dual LC/PC	VNX	Ten	9/9	SFP-10G-SR
VHAGR700901	Ten	9/10	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700901	Ten	9/11	Dual LC/PC	VHACC554801	Ten	1/26	SFP-10G-SR
VHAGR700901	Ten	9/12	Dual LC/PC	VHACC554803	Ten	1/26	SFP-10G-SR

VHAGR700901	Ten	9/13	Dual LC/PC	VHSAN554801	Ten	1/26	SFP-10G-SR
VHAGR700901	Gig	9/14	RJ-45	Free	Gig	TBD	RJ-45
VHAGR700901	Gig	9/15	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/16	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/17	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/18	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/19	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/20	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/21	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/22	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/23	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/24	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/25	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Gig	9/26	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Ten	9/27	Dual SC/PC	VHAGR700902	Ten	8/31	SFP-10G-SR
VHAGR700901	Gig	9/28	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Ten	9/29	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700901	Ten	9/30	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700901	Ten	9/31	Dual SC/PC	VHAGR700902	Ten	8/27	SFP-10G-SR
VHAGR700901	Ten	9/32	Dual LC/PC	Free	Ten		SFP-10G-SR
VHAGR700902	Mgt0	1/1	RJ-45	VHADM296004	Gig	0/1	RJ-45
VHAGR700902	Mgt1	2/1	RJ-45	VHADM296003	Gig	0/5	RJ-45
VHAGR700902	Ten	3/1	Dual SC/PC	VHAGR700901	Ten	3/1	X2-10GB-SR
VHAGR700902	Ten	3/2	Dual SC/PC	VHCOR700902	Ten	3/2	X2-10GB-SR
VHAGR700902	Ten	3/3	Dual SC/PC	VHAGR700901	Ten	3/3	X2-10GB-SR
VHAGR700902	Ten	3/4	Dual SC/PC	VHCOR700902	Ten	3/4	X2-10GB-SR
VHAGR700902	Ten	3/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	3/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	3/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	3/8	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	4/1	Dual SC/PC	VHAGR700901	Ten	4/1	X2-10GB-SR
VHAGR700902	Ten	4/2	Dual SC/PC	VHCOR700901	Ten	4/2	X2-10GB-SR
VHAGR700902	Ten	4/3	Dual SC/PC	VHAGR700901	Ten	4/3	X2-10GB-SR
VHAGR700902	Ten	4/4	Dual SC/PC	VHCOR700902	Ten	4/4	X2-10GB-SR
VHAGR700902	Ten	4/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	4/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	4/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	4/8	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	5/1	Dual SC/PC	DD	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/2	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/3	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR

VHAGR700902	Ten	5/4	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	5/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	5/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	5/8	Dual SC/PC	VHAGR700901	Ten	5/8	X2-10GB-SR
VHAGR700902	Ten	5/1	Dual SC/PC	DD	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/2	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/3	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	5/4	Dual SC/PC	ISILON	Ten	TBD	X2-10GB-SR
VHAGR700902	Ten	6/5	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	6/6	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	6/7	Dual SC/PC	Free	Ten		X2-10GB-SR
VHAGR700902	Ten	6/8	Dual SC/PC	VHAGR700901	Ten	6/8	X2-10GB-SR
VHAGR700902	Ten	8/1	Dual LC/PC	VHAGR700901	Ten	8/1	SFP-10G-SR
VHAGR700902	Ten	8/2	Dual LC/PC	VHSER650901	Ten	7/1	SFP-10G-SR
VHAGR700902	Ten	8/3	Dual LC/PC	VHACC554801	Ten	1/29	SFP-10G-SR
VHAGR700902	Ten	8/4	Dual LC/PC	VHACC554801	Ten	1/30	SFP-10G-SR
VHAGR700902	Ten	8/5	Dual LC/PC	VHACC554803	Ten	1/29	SFP-10G-SR
VHAGR700902	Ten	8/6	Dual LC/PC	VHACC554803	Ten	1/30	SFP-10G-SR
VHAGR700902	Ten	8/7	Dual LC/PC	VHACC554804	Ten	1/29	SFP-10G-SR
VHAGR700902	Ten	8/8	Dual LC/PC	VHACC554804	Ten	1/30	SFP-10G-SR
VHAGR700902	Ten	8/9	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700902	Ten	8/10	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700902	Ten	8/11	Dual LC/PC	VHACC554802	Ten	1/25	SFP-10G-SR
VHAGR700902	Ten	8/12	Dual LC/PC	VHACC554804	Ten	1/25	SFP-10G-SR
VHAGR700902	Ten	8/13	Dual LC/PC	VHSAN554802	Ten	1/25	SFP-10G-SR
VHAGR700902	Ten	8/14	Dual LC/PC	Free	Ten		SFP-10G-SR
VHAGR700902	Gig	8/15	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700902	Gig	8/16	Dual LC/PC	Free	Ten		SFP-10G-SR
VHAGR700902	Ten	8/17	Dual LC/PC	VHSER650902	Ten	7/1	SFP-10G-SR
VHAGR700902	Ten	8/18	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700902	Ten	8/19	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700902	Ten	8/20	Dual LC/PC	ISILON	Ten		GLC-SX-MMD
VHAGR700902	Gig	8/21	RJ-45	Data_Mover_01	Gig	TBD	RJ-45
VHAGR700902	Gig	8/22	RJ-45	Data_Mover_02	Gig	TBD	RJ-45
VHAGR700902	Gig	8/23	RJ-45	Data_Mover_03	Gig	9/31	RJ-45
VHAGR700902	Gig	8/24	Dual LC/PC	Data_Mover_01	Gig	TBD	GLC-SX-MMD
VHAGR700902	Gig	8/25	Dual LC/PC	Data_Mover_02	Gig	TBD	GLC-SX-MMD
VHAGR700902	Gig	8/26	Dual LC/PC	Data_Mover_03	Gig	TBD	GLC-SX-MMD
VHAGR700902	Ten	8/27	Dual SC/PC	VHAGR700901	Ten	9/31	SFP-10G-SR
VHAGR700902	Ten	8/28	Dual LC/PC	Free	Ten		GLC-SX-MMD

VHAGR700902	Ten	8/29	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700902	Ten	8/30	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700902	Ten	8/31	Dual SC/PC	VHAGR700901	Ten	9/27	SFP-10G-SR
VHAGR700902	Ten	8/32	Dual LC/PC	Free	Ten		GLC-SX-MMD
VHAGR700902	Ten	9/1	Dual LC/PC	VHAGR700901	Ten	9/1	SFP-10G-SR
VHAGR700902	Ten	9/2	Dual LC/PC	ISILON	Ten		GLC-SX-MMD
VHAGR700902	Ten	9/3	Dual LC/PC	VHACC554802	Ten	1/29	SFP-10G-SR
VHAGR700902	Ten	9/4	Dual LC/PC	VHACC554802	Ten	1/30	SFP-10G-SR
VHAGR700902	Ten	9/5	Dual LC/PC	VHSAN554801	Ten	1/3	SFP-10G-SR
VHAGR700902	Ten	9/6	Dual LC/PC	VHSAN554801	Ten	1/4	SFP-10G-SR
VHAGR700902	Ten	9/7	Dual LC/PC	VHSAN554802	Ten	1/3	SFP-10G-SR
VHAGR700902	Ten	9/8	Dual LC/PC	VHSAN554802	Ten	1/4	SFP-10G-SR
VHAGR700902	Ten	9/9	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700902	Ten	9/10	Dual LC/PC	VNX	Ten	TBD	SFP-10G-SR
VHAGR700902	Ten	9/11	Dual LC/PC	VHACC554802	Ten	1/26	SFP-10G-SR
VHAGR700902	Ten	9/12	Dual LC/PC	VHACC554804	Ten	1/26	SFP-10G-SR
VHAGR700902	Ten	9/13	Dual LC/PC	VHSAN554802	Ten	1/26	SFP-10G-SR
VHAGR700902	Gig	9/14	RJ-45	Free	Gig	TBD	RJ-45
VHAGR700902	Gig	9/15	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/16	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/17	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/18	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/19	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/20	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/21	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/22	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/23	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/24	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/25	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Gig	9/26	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Ten	9/27	Dual SC/PC	VHAGR700902	Ten	9/31	SFP-10G-SR
VHAGR700902	Gig	9/28	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Ten	9/29	RJ-45	ISILON	Gig	TBD	RJ-45
VHAGR700902	Ten	9/30	Dual LC/PC	ISILON	Ten		SFP-10G-SR
VHAGR700902	Ten	9/31	Dual SC/PC	VHAGR700902	Ten	9/27	SFP-10G-SR
VHAGR700902	Ten	9/32	Dual LC/PC	Free	Ten		SFP-10G-SR

En la tabla 2.8 se muestra el mapeo de puertos del módulo de Servicios.

Tabla 2.8 Mapeo de puertos-Módulo de Servicios

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHSER650901	Ten	4/1	Dual SC/PC	VHAGR700901		8/2	X2-10GB-SR
VHSER650901	Ten	4/2	Dual SC/PC	VHSEC451001		0/6	SFP-10G-SR
VHSER650901	Ten	4/3	Dual SC/PC	VHSEC451001		0/7	SFP-10G-SR
VHSER650901	Ten	4/4	Dual SC/PC	VHSER650902		4/4	XENPAK-10GB-SR
VHSER650901	Gig	5/1	Dual LC/PC	VHADM450301	Gig	3/9	Dual LC/PC
VHSER650901	Gig	5/2		Free			
VHSER650901	Gig	5/3	RJ-45	VHADM296003	Gig	0/2	RJ-45
VHSER650901	Ten	5/4	Dual SC/PC	Free			
VHSER650901	Ten	5/5		Free			
VHSER650901	Gig	6/1		Free			
VHSER650901	Gig	6/2		Free			
VHSER650901	Gig	6/3	RJ-45	VHADM296004	Gig	0/2	RJ-45
VHSER650901	Ten	6/4	Dual SC/PC	Free			
VHSER650901	Ten	6/5		Free			
VHSER650901	Ten	7/1	Dual SC/PC	VHAGR700902		8/2	X2-10GB-SR
VHSER650901	Ten	7/2	Dual SC/PC	VHSEC451001		0/8	SFP-10G-SR
VHSER650901	Ten	7/3	Dual SC/PC	VHSEC451001		0/9	SFP-10G-SR
VHSER650901	Ten	7/4	Dual SC/PC	VHSER650902		7/4	XENPAK-10GB-SR
VHSER650902	Ten	4/1	Dual SC/PC	VHAGR700901		8/17	X2-10GB-SR
VHSER650902	Ten	4/2	Dual SC/PC	VHSEC451002		0/6	SFP-10G-SR
VHSER650902	Ten	4/3	Dual SC/PC	VHSEC451002		0/7	SFP-10G-SR
VHSER650902	Ten	4/4	Dual SC/PC	VHSER650901		4/4	XENPAK-10GB-SR
VHSER650902	Gig	5/1	Dual LC/PC	VHADM450302	Gig	3/9	Dual LC/PC
VHSER650902	Gig	5/2		Free			
VHSER650902	Gig	5/3	RJ-45	VHADM296003	Gig	0/3	RJ-45
VHSER650902	Ten	5/4	Dual	Free			

			SC/PC				
VHSER650902	Ten	5/5		Free			
VHSER650902	Gig	6/1		Free			
VHSER650902	Gig	6/2		Free			
VHSER650902	Gig	6/3	RJ-45	VHADM296004	Gig		RJ-45
VHSER650902	Ten	6/4	Dual SC/PC	Free			
VHSER650902	Ten	6/5		Free			
VHSER650902	Ten	7/1	Dual SC/PC	VHAGR700902		8/17	X2-10GB-SR
VHSER650902	Ten	7/2	Dual SC/PC	VHSEC451002		0/8	SFP-10G-SR
VHSER650902	Ten	7/3	Dual SC/PC	VHSEC451002		0/9	SFP-10G-SR
VHSER650902	Ten	7/4	Dual SC/PC	VHSER650901	Ten	7/4	XENPAK-10GB-SR
VHSEC451001	Ten	0/6	Dual LC/PC	VHSER650901	Ten	4/2	XENPAK-10GB-SR
VHSEC451001	Ten	0/7	Dual LC/PC	VHSER650901	Ten	4/3	XENPAK-10GB-SR
VHSEC451001	Ten	0/8	Dual LC/PC	VHSER650901	Ten	7/2	XENPAK-10GB-SR
VHSEC451001	Ten	0/9	Dual LC/PC	VHSER650901	Ten	7/3	XENPAK-10GB-SR
VHSEC451002	Ten	O/6	Dual LC/PC	VHSER650902	Ten	4/2	XENPAK-10GB-SR
VHSEC451002	Ten	0/7	Dual LC/PC	VHSER650902	Ten	4/3	XENPAK-10GB-SR
VHSEC451002	Ten	0/8	Dual LC/PC	VHSER650902	Ten	7/2	XENPAK-10GB-SR
VHSEC451002	Ten	0/9	Dual LC/PC	VHSER650902	Ten	7/3	XENPAK-10GB-SR
VHSEC451001	MGT	1/1	RJ-45	VHADM296003	Gig	0/4	RJ-45
VHSEC451002	MGT	1/1	RJ-45	VHADM296004	Gig	0/4	RJ-45

En la tabla 2.9 se muestra el mapeo de puertos del módulo de Core.

Tabla 2.9 Mapeo de puertos-Módulo de Core

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHCOR700901	Mgt	MGT0		VHADM296001		0/1	
VHCOR700901	Mgt	MGT1		VHADM296002		0/1	
VHCOR700901	Ten	3/1	Dual SC/PC	VHCOR700902		3/1	X2-10GB-SR
VHCOR700901	Ten	3/2	Dual SC/PC	VHAGR700901	Ten	3/2	X2-10GB-SR
VHCOR700901	Ten	3/3	Dual SC/PC	VHCOR700902	Ten	3/3	X2-10GB-SR
VHCOR700901	Ten	3/4	Dual SC/PC	VHAGR700901	Ten	3/4	X2-10GB-SR

VHCOR700901	Ten	3/5	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	3/6	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	3/7	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	3/8	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	4/1	Dual SC/PC	VHCOR700902	Ten	4/1	X2-10GB-SR
VHCOR700901	Ten	4/2	Dual SC/PC	VHAGR700902	Ten	4/2	X2-10GB-SR
VHCOR700901	Ten	4/3	Dual SC/PC	VHCOR700902	Ten	4/3	X2-10GB-SR
VHCOR700901	Ten	4/4	Dual SC/PC	VHAGR700901	Ten	4/4	X2-10GB-SR
VHCOR700901	Ten	4/5	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	4/6	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	4/7	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Ten	4/8	Dual SC/PC	Free			X2-10GB-SR
VHCOR700901	Gig	9/1	Dual LC/PC	760001	Gig		GLC-SX-MMD
VHCOR700901	Gig	9/2		**Free**			
VHCOR700901	Gig	9/3	Dual LC/PC	Free			
VHCOR700901	Gig	9/4	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/5	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/6	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/7	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/8	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/9	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/10	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/11	RJ-45	Free			RJ-45
VHCOR700901	Gig	9/12	Free				
VHCOR700901	Gig	9/13	Dual LC/PC	760002	Gig	TBD	GLC-SX-MMD
VHCOR700901	Gig	9/14		Free			
VHCOR700901	Gig	9/15		Free			
VHCOR700901	Gig	9/16		Free			
VHCOR700901	Gig	9/17		Free			
VHCOR700901	Gig	9/18		Free			
VHCOR700901	Gig	9/19		Free			
VHCOR700901	Gig	9/20		Free			
VHCOR700901	Gig	9/21		Free			
VHCOR700901	Gig	9/22		Free			
VHCOR700901	Gig	9/23		Free			
VHCOR700901	Gig	9/24		Free			
VHCOR700901	Gig	9/25		Free			
VHCOR700901	Gig	9/26		Free			
VHCOR700901	Gig	9/27		Free			
VHCOR700901	Gig	9/28		Free			
VHCOR700901	Gig	9/29		Free			

VHCOR700901	Gig	9/30		Free			
VHCOR700901	Gig	9/31		Free			
VHCOR700901	Gig	9/32		Free			
VHCOR700901	Gig	9/33		Free			
VHCOR700901	Gig	9/34		Free			
VHCOR700901	Gig	9/35		Free			
VHCOR700901	Gig	9/36		Free			
VHCOR700901	Gig	9/37	Dual LC/PC	VHREP754101	Gig	1/0	GLC-SX-MMD
VHCOR700901	Gig	9/38	Dual LC/PC	760001	Gig	TBD	GLC-SX-MMD
VHCOR700901	Gig	9/39		Free			
VHCOR700901	Gig	9/40		Free			
VHCOR700901	Gig	9/41		Free			
VHCOR700901	Gig	9/42		Free			
VHCOR700901	Gig	9/43		Free			
VHCOR700901	Gig	9/44		Free			
VHCOR700901	Gig	9/45		Free			
VHCOR700901	Gig	9/46		Free			
VHCOR700901	Gig	9/47		Free			
VHCOR700901	Gig	9/48		Free			
VHCOR700902	Mgt	MGT0		VHADM296001		**0/2**	
VHCOR700902	Mgt	MGT1		VHADM296002		**0/2**	
VHCOR700902	Ten	3/1	Dual SC/PC	VHCOR700901	Ten	3/1	X2-10GB-SR
VHCOR700902	Ten	3/2	Dual SC/PC	VHAGR700902	Ten	3/2	X2-10GB-SR
VHCOR700902	Ten	3/3	Dual SC/PC	VHCOR700901	Ten	3/3	X2-10GB-SR
VHCOR700902	Ten	3/4	Dual SC/PC	VHAGR700902	Ten	3/4	X2-10GB-SR
VHCOR700902	Ten	3/5	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	3/6	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	3/7	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	3/8	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	4/1	Dual SC/PC	VHCOR700901	Ten	4/1	X2-10GB-SR
VHCOR700902	Ten	4/2	Dual SC/PC	VHAGR700901	Ten	4/2	X2-10GB-SR
VHCOR700902	Ten	4/3	Dual SC/PC	VHCOR700902	Ten	4/3	X2-10GB-SR
VHCOR700902	Ten	4/4	Dual SC/PC	VHAGR700902	Ten	4/4	X2-10GB-SR
VHCOR700902	Ten	4/5	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	4/6	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	4/7	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Ten	4/8	Dual SC/PC	Free			X2-10GB-SR
VHCOR700902	Gig	9/1	Dual LC/PC	760002	Gig	TBD	GLC-SX-MMD
VHCOR700902	Gig	9/2		**Free**			
VHCOR700902	Gig	9/3	Dual LC/PC	Free			
VHCOR700902	Gig	9/4	RJ-45	Free			RJ-45

VHCOR700902	Gig	9/5	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/6	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/7	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/8	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/9	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/10	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/11	RJ-45	Free			RJ-45
VHCOR700902	Gig	9/12		**Free**			
VHCOR700902	Gig	9/13	Dual LC/PC	760001	Gig	TBD	GLC-SX-MMD
VHCOR700902	Gig	9/14		**Free**			
VHCOR700902	Gig	9/15		Free			
VHCOR700902	Gig	9/16		Free			
VHCOR700902	Gig	9/17		Free			
VHCOR700902	Gig	9/18		Free			
VHCOR700902	Gig	9/19		Free			
VHCOR700902	Gig	9/20		Free			
VHCOR700902	Gig	9/21		Free			
VHCOR700902	Gig	9/22		Free			
VHCOR700902	Gig	9/23		Free			
VHCOR700902	Gig	9/24		Free			
VHCOR700902	Gig	9/25		Free			
VHCOR700902	Gig	9/26		Free			
VHCOR700902	Gig	9/27		Free			
VHCOR700902	Gig	9/28		Free			
VHCOR700902	Gig	9/29		Free			
VHCOR700902	Gig	9/30		Free			
VHCOR700902	Gig	9/31		Free			
VHCOR700902	Gig	9/32		Free			
VHCOR700902	Gig	9/33		Free			
VHCOR700902	Gig	9/34		Free			
VHCOR700902	Gig	9/35		Free			
VHCOR700902	Gig	9/36		Free			
VHCOR700902	Gig	9/37	Dual LC/PC	VHREP754101	Gig	1/3	GLC-SX-MMD
VHCOR700902	Gig	9/38	Dual LC/PC	760002	Gig	TBD	GLC-SX-MMD
VHCOR700902	Gig	9/39		Free			
VHCOR700902	Gig	9/40		Free			
VHCOR700902	Gig	9/41		Free			
VHCOR700902	Gig	9/42		Free			
VHCOR700902	Gig	9/43		Free			
VHCOR700902	Gig	9/44		Free			
VHCOR700902	Gig	9/45		Free			

VHCOR700902	Gig	9/46		Free			
VHCOR700902	Gig	9/47		Free			
VHCOR700902	Gig	9/48		Free			

En la tabla 2.10 se muestra el mapeo de puertos del módulo de Acceso.

Tabla 2.10 Mapeo de puertos – Módulo de Acceso

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHACC554801	MGT	1/0	RJ-45	VHADM296004	Gig	0/6	RJ-45
VHACC554801	Gig	1/1	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/2	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/3	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/4	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/5	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/6	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/7	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/8	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/9	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Gig	1/10	RJ-45	Server 1G	Gig		RJ-45
VHACC554801	Ten	1/11	Dual LC/PC	HP SERVERS 10G-PRIM-01	Ten		SFP-10G-SR
VHACC554801	Ten	1/12	Dual LC/PC	HP SERVERS 10G-PRIM-02	Ten		SFP-10G-SR
VHACC554801	Ten	1/13	Dual LC/PC	HP SERVERS 10G-PRIM-03	Ten		SFP-10G-SR
VHACC554801	Ten	1/14	Dual LC/PC	HP SERVERS 10G-PRIM-04	Ten		SFP-10G-SR
VHACC554801	Ten	1/15	Dual LC/PC	HP SERVERS 10G-PRIM-05	Ten		SFP-10G-SR
VHACC554801	Ten	1/16	Dual LC/PC	HP SERVERS 10G-PRIM-06	Ten		SFP-10G-SR
VHACC554801	Ten	1/17	Dual LC/PC	HP SERVERS 10G-PRIM-07	Ten		SFP-10G-SR
VHACC554801	Ten	1/18	Dual LC/PC	HP SERVERS 10G-PRIM-08	Ten		SFP-10G-SR
VHACC554801	Ten	1/19	Dual LC/PC	HP SERVERS 10G-PRIM-09	Ten		SFP-10G-SR
VHACC554801	Ten	1/20	Dual LC/PC	HP SERVERS 10G-PRIM-10	Ten		SFP-10G-SR
VHACC554801	Ten	1/21	Dual LC/PC	HP SERVERS 10G-PRIM-11	Ten		SFP-10G-SR
VHACC554801	Ten	1/22		Free			
VHACC554801	Ten	1/23		Free			
VHACC554801	Ten	1/24		Free			
VHACC554801	Ten	1/25	Dual LC/PC	VHAGR700901	Ten	8/11	SFP-10G-SR
VHACC554801	Ten	1/26	Dual LC/PC	VHAGR700901	Ten	9/11	SFP-10G-SR
VHACC554801	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	8/3	SFP-10G-SR
VHACC554801	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	8/4	SFP-10G-SR
VHACC554801	Ten	1/29	Dual LC/PC	VHAGR700902	Ten	8/3	SFP-10G-SR

VHACC554801	Ten	1/30	Dual LC/PC	VHAGR700902	Ten	8/4	SFP-10G-SR
VHACC554801	Ten	1/31	Dual LC/PC	VHACC554802	Ten	1/31	SFP-10G-SR
VHACC554801	Ten	1/32	Dual LC/PC	VHACC554802	Ten	1/32	SFP-10G-SR
VHACC554801	Ten	2/1	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/2	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/3	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/4	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/5	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/6	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/7	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/8	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554801	Ten	2/14		Free			
VHACC554801	Ten	2/15		Free			
VHACC554801	Ten	2/16		Free			
VHACC554802	MGT	1/0	RJ-45	VHADM296004	Gig	0/7	RJ-45
VHACC554802	Ten	1/1		**Free**			
VHACC554802	Gig	1/2	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/3	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/4	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/5	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/6	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/7	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/8	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/9	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/10	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Gig	1/11	RJ-45	Server 1G	Gig		RJ-45
VHACC554802	Ten	1/12	Dual LC/PC	HP SERVERS 10G-SEC-01	Ten		SFP-10G-SR
VHACC554802	Ten	1/13	Dual LC/PC	HP SERVERS 10G-SEC-02	Ten		SFP-10G-SR
VHACC554802	Ten	1/14	Dual LC/PC	HP SERVERS 10G-SEC-03	Ten		SFP-10G-SR
VHACC554802	Ten	1/15	Dual LC/PC	HP SERVERS 10G-SEC-04	Ten		SFP-10G-SR
VHACC554802	Ten	1/16	Dual LC/PC	HP SERVERS 10G-SEC-05	Ten		SFP-10G-SR
VHACC554802	Ten	1/17	Dual LC/PC	HP SERVERS 10G-SEC-06	Ten		SFP-10G-SR
VHACC554802	Ten	1/18	Dual LC/PC	HP SERVERS 10G-SEC-07	Ten		SFP-10G-SR
VHACC554802	Ten	1/19	Dual LC/PC	HP SERVERS 10G-SEC-08	Ten		SFP-10G-SR
VHACC554802	Ten	1/20	Dual LC/PC	HP SERVERS 10G-SEC-09	Ten		SFP-10G-SR
VHACC554802	Ten	1/21	Dual LC/PC	HP SERVERS 10G-SEC-10	Ten		SFP-10G-SR

VHACC554802	Ten	1/22		Free			
VHACC554802	Ten	1/23		Free			
VHACC554802	Ten	1/24		Free			
VHACC554802	Ten	1/25	Dual LC/PC	VHAGR700902	Ten	8/11	SFP-10G-SR
VHACC554802	Ten	1/26	Dual LC/PC	VHAGR700902	Ten	9/11	SFP-10G-SR
VHACC554802	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	9/3	SFP-10G-SR
VHACC554802	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	9/4	SFP-10G-SR
VHACC554802	Ten	1/29	Dual LC/PC	VHAGR700902	Ten	9/3	SFP-10G-SR
VHACC554802	Ten	1/30	Dual LC/PC	VHAGR700902	Ten	9/4	SFP-10G-SR
VHACC554802	Ten	1/31	Dual LC/PC	VHACC554801	Ten	1/31	SFP-10G-SR
VHACC554802	Ten	1/32	Dual LC/PC	VHACC554801	Ten	1/32	SFP-10G-SR
VHACC554802	Ten	2/1	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/2	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/3	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/4	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/5	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/6	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/7	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/8	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554802	Ten	2/14		Free			
VHACC554802	Ten	2/15		Free			
VHACC554802	Ten	2/16		Free			
VHACC554803	MGT	1/0	RJ-45	VHADM296004	Gig	0/8	RJ-45
VHACC554803	Gig	1/1	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/2	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/3	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/4	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/5	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/6	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/7	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/8	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/9	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Gig	1/10	RJ-45	Server 1G	Gig		RJ-45
VHACC554803	Ten	1/11	Dual LC/PC	HP SERVERS 10G-PRIM-01	Ten		SFP-10G-SR
VHACC554803	Ten	1/12	Dual LC/PC	HP SERVERS 10G-PRIM-02	Ten		SFP-10G-SR
VHACC554803	Ten	1/13	Dual LC/PC	HP SERVERS 10G-PRIM-03	Ten		SFP-10G-SR

VHACC554803	Ten	1/14	Dual LC/PC	HP SERVERS 10G-PRIM-04	Ten		SFP-10G-SR
VHACC554803	Ten	1/15	Dual LC/PC	HP SERVERS 10G-PRIM-05	Ten		SFP-10G-SR
VHACC554803	Ten	1/16	Dual LC/PC	HP SERVERS 10G-PRIM-06	Ten		SFP-10G-SR
VHACC554803	Ten	1/17	Dual LC/PC	HP SERVERS 10G-PRIM-07	Ten		SFP-10G-SR
VHACC554803	Ten	1/18	Dual LC/PC	HP SERVERS 10G-PRIM-08	Ten		SFP-10G-SR
VHACC554803	Ten	1/19	Dual LC/PC	HP SERVERS 10G-PRIM-09	Ten		SFP-10G-SR
VHACC554803	Ten	1/20	Dual LC/PC	HP SERVERS 10G-PRIM-10	Ten		SFP-10G-SR
VHACC554803	Ten	1/21	Dual LC/PC	HP SERVERS 10G-PRIM-11	Ten		SFP-10G-SR
VHACC554803	Ten	1/22		Free			
VHACC554803	Ten	1/23		Free			
VHACC554803	Ten	1/24		Free			
VHACC554803	Ten	1/25	Dual LC/PC	VHAGR700901	Ten	8/12	SFP-10G-SR
VHACC554803	Ten	1/26	Dual LC/PC	VHAGR700901	Ten	9/12	SFP-10G-SR
VHACC554803	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	8/5	SFP-10G-SR
VHACC554803	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	8/6	SFP-10G-SR
VHACC554803	Ten	1/29	Dual LC/PC	VHAGR700902	Ten	8/5	SFP-10G-SR
VHACC554803	Ten	1/30	Dual LC/PC	VHAGR700902	Ten	8/6	SFP-10G-SR
VHACC554803	Ten	1/31	Dual LC/PC	VHACC554804	Ten	1/31	SFP-10G-SR
VHACC554803	Ten	1/32	Dual LC/PC	VHACC554804	Ten	1/32	SFP-10G-SR
VHACC554803	Ten	2/1	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/2	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/3	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/4	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/5	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/6	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/7	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/8	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554803	Ten	2/14		Free			
VHACC554803	Ten	2/15		Free			
VHACC554803	Ten	2/16		**Free**			
VHACC554804	MGT	1/0	RJ-45	VHADM296005	Gig	0/2	RJ-45
VHACC554804	Gig	1/1	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/2	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/3	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/4	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/5	RJ-45	Server 1G	Gig		RJ-45

VHACC554804	Gig	1/6	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/7	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/8	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/9	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Gig	1/10	RJ-45	Server 1G	Gig		RJ-45
VHACC554804	Ten	1/11	Dual LC/PC	HP SERVERS 10G-SEC-01	Ten		SFP-10G-SR
VHACC554804	Ten	1/12	Dual LC/PC	HP SERVERS 10G-SEC-02	Ten		SFP-10G-SR
VHACC554804	Ten	1/13	Dual LC/PC	HP SERVERS 10G-SEC-03	Ten		SFP-10G-SR
VHACC554804	Ten	1/14	Dual LC/PC	HP SERVERS 10G-SEC-04	Ten		SFP-10G-SR
VHACC554804	Ten	1/15	Dual LC/PC	HP SERVERS 10G-SEC-05	Ten		SFP-10G-SR
VHACC554804	Ten	1/16	Dual LC/PC	HP SERVERS 10G-SEC-06	Ten		SFP-10G-SR
VHACC554804	Ten	1/17	Dual LC/PC	HP SERVERS 10G-SEC-07	Ten		SFP-10G-SR
VHACC554804	Ten	1/18	Dual LC/PC	HP SERVERS 10G-SEC-08	Ten		SFP-10G-SR
VHACC554804	Ten	1/19	Dual LC/PC	HP SERVERS 10G-SEC-09	Ten		SFP-10G-SR
VHACC554804	Ten	1/20	Dual LC/PC	HP SERVERS 10G-SEC-10	Ten		SFP-10G-SR
VHACC554804	Ten	1/21		Free			
VHACC554804	Ten	1/22		Free			
VHACC554804	Ten	1/23		Free			
VHACC554804	Ten	1/24		Free			
VHACC554804	Ten	1/25	Dual LC/PC	VHAGR700902	Ten	8/12	SFP-10G-SR
VHACC554804	Ten	1/26	Dual LC/PC	VHAGR700902	Ten	9/12	SFP-10G-SR
VHACC554804	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	8/7	SFP-10G-SR
VHACC554804	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	8/8	SFP-10G-SR
VHACC554804	Ten	1/29	Dual LC/PC	VHAGR700902	Ten	8/7	SFP-10G-SR
VHACC554804	Ten	1/30	Dual LC/PC	VHAGR700902	Ten	8/8	SFP-10G-SR
VHACC554804	Ten	1/31	Dual LC/PC	VHACC554803	Ten	1/31	SFP-10G-SR
VHACC554804	Ten	1/32	Dual LC/PC	VHACC554803	Ten	1/32	SFP-10G-SR
VHACC554804	Ten	2/1	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/2	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/3	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/4	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/5	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/6	Ten	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/7	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/8	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHACC554804	Ten	2/14		Free			

VHACC554804	Ten	2/15		Free			
VHACC554804	Ten	2/16		Free			
VHSAN554801	MGT	1/0	RJ-45	VHADM296005	Gig	0/3	RJ-45
VHSAN554801	Ten	1/1	Dual LC/PC	VHSAN554802	Ten	1/1	SFP-10G-SR
VHSAN554801	Ten	1/2	Dual LC/PC	VHSAN554802	Ten	1/2	SFP-10G-SR
VHSAN554801	Ten	1/3	Dual LC/PC	VHAGR700902	Ten	9/5	SFP-10G-SR
VHSAN554801	Ten	1/4	Dual LC/PC	VHAGR700902	Ten	9/6	SFP-10G-SR
VHSAN554801	8G	1/5	Dual LC	Free	8G		DS-SFP-FC8G-SW
VHSAN554801	8G	1/6	Dual LC	Free	8G		DS-SFP-FC8G-SW
VHSAN554801	Ten	1/7		Free			
VHSAN554801	Ten	1/8		Free			
VHSAN554801	Ten	1/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/14	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/15	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/16	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/17	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/18	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/19	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/20	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/21	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/22	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/23	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/24	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554801	Ten	1/25	Dual LC/PC	VHAGR700901	Ten	8/13	SFP-10G-SR
VHSAN554801	Ten	1/26	Dual LC/PC	VHAGR700901	Ten	9/13	SFP-10G-SR
VHSAN554801	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	9/5	SFP-10G-SR
VHSAN554801	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	9/6	SFP-10G-SR
VHSAN554801	Ten	1/29	Dual LC/PC	Free			SFP-10G-SR
VHSAN554801	Ten	1/30	Dual LC/PC	Free			SFP-10G-SR
VHSAN554801	8G	1/31	Dual LC	VHSAN950601	8G	4/5	DS-SFP-FC8G-SW
VHSAN554801	8G	1/32	Dual LC	VHSAN950601	8G	3/5	DS-SFP-FC8G-SW
VHSAN554802	MGT	1/0	RJ-45	VHADM296005	Gig	0/4	RJ-45
VHSAN554802	Ten	1/1	Dual LC/PC	VHSAN554801	Ten	1/1	SFP-10G-SR
VHSAN554802	Ten	1/2	Dual LC/PC	VHSAN554801	Ten	1/2	SFP-10G-SR
VHSAN554802	Ten	1/3	Dual LC/PC	VHAGR700902	Ten	9/7	SFP-10G-SR
VHSAN554802	Ten	1/4	Dual LC/PC	VHAGR700902	Ten	9/8	SFP-10G-SR
VHSAN554802	8G	1/5	Dual LC	Free	8G		DS-SFP-FC8G-SW

VHSAN554802	8G	1/6	Dual LC	Free	8G		DS-SFP-FC8G-SW
VHSAN554802	Ten	1/7		Free			
VHSAN554802	Ten	1/8		Free			
VHSAN554802	Ten	1/9	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/10	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/11	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/12	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/13	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/14	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/15	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/16	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/17	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/18	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/19	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/20	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/21	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/22	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/23	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/24	Dual LC/PC	Server 10G FCoE	Ten		SFP-10G-SR
VHSAN554802	Ten	1/25	Dual LC/PC	VHAGR700902	Ten	8/13	SFP-10G-SR
VHSAN554802	Ten	1/26	Dual LC/PC	VHAGR700902	Ten	9/13	SFP-10G-SR
VHSAN554802	Ten	1/27	Dual LC/PC	VHAGR700901	Ten	9/7	SFP-10G-SR
VHSAN554802	Ten	1/28	Dual LC/PC	VHAGR700901	Ten	9/8	SFP-10G-SR
VHSAN554802	Ten	1/29	Dual LC/PC	Free			SFP-10G-SR
VHSAN554802	Ten	1/30	Dual LC/PC	Free			SFP-10G-SR
VHSAN554802	8G	1/31	Dual LC	VHSAN950601	8G	4/6	DS-SFP-FC8G-SW
VHSAN554802	8G	1/32	Dual LC	VHSAN950601	8G	3/6	DS-SFP-FC8G-SW

Nota:

Lasiguiente asignación de puertos para el módulo de Acceso es una excepción que sólo se aplica a los sitios de Poza Rica y de Reynosa.

En la tabla 2.11 se muestra el mapeo de puertos del módulo de Acceso.

Tabla 2.11 Mapeo de puertos – Módulo de Acceso

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHACC554801	Ten	1/22	Dual LC/PC	ACC223201	Ten	1/1	SFP-10G-SR
VHACC554801	Ten	1/23	Dual LC/PC	ACC223202	Ten	1/1	SFP-10G-SR
VHACC554801	Ten	1/24	Dual LC/PC	ACC224801	Ten	1/2	SFP-10G-SR
VHACC554802	Ten	1/22	Dual LC/PC	ACC223201	Ten	1/2	SFP-10G-SR

VHACC554802	Ten	1/23	Dual LC/PC	ACC224801	Ten	1/1	SFP-10G-SR
VHACC554802	Ten	1/24	Dual LC/PC	ACC223202	Ten	1/2	SFP-10G-SR
VHACC554803	Ten	1/22	Dual LC/PC	ACC223203	Ten	1/1	SFP-10G-SR
VHACC554803	Ten	1/23	Dual LC/PC	ACC223204	Ten	1/1	SFP-10G-SR
VHACC554803	Ten	1/24	Dual LC/PC	ACC224802	Ten	1/2	SFP-10G-SR
VHACC554804	Ten	1/22	Dual LC/PC	ACC223203	Ten	1/2	SFP-10G-SR
VHACC554804	Ten	1/23	Dual LC/PC	ACC224802	Ten	1/1	SFP-10G-SR
VHACC554804	Ten	1/24	Dual LC/PC	ACC223204	Ten	1/2	SFP-10G-SR

En la tabla 2.12 se muestra el mapeo de puertos del módulo de Almacenamiento.

Tabla 2.12 Mapeo de puertos – Módulo de Almacenamiento

Device A	Type	Port A	Connector	Device B	Type	Port B	Connector
VHREP754101	MGT	0/1	RJ-45	VHADM296005	Gig	0/5	RJ-45
VHREP754101	Gig	1/0	GLC-SX-MMD	VHCOR700901	Gig	9/37	
VHREP754101	Gig	1/1	GLC-SX-MMD	VHCOR700902	Gig	9/37	
VHREP754101	Gig	1/0	GLC-SX-MMD	VHSAN950601	Gig	1/1	
VHREP754101	Gig	1/1	GLC-SX-MMD	VHSAN950601	Gig	1/2	
VHSAN950601	Gig	1/1	DS-SFP-FCGE-FW	VHREP754101	Gig	1/0	
VHSAN950601	Gig	1/2	DS-SFP-FCGE-FW	VHREP754101	Gig	1/1	
VHSAN950601	Gig	1/3	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/4	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/5	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/6	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/7	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/8	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/9	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/10	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/11	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/12	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/13	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/14	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/15	DS-SFP-FCGE-FW	Free			
VHSAN950601	Gig	1/16	DS-SFP-FCGE-	Free			
VHSAN950601	Fiber Channel 8Gbps	3/1	DS-SFP-FC8G-SW	VNX	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/2	DS-SFP-FC8G-SW	VNX	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/3	DS-SFP-FC8G-SW	DD	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel	3/4	DS-SFP-FC8G-SW	DD	Fiber Channel	TBD	DS-SFP-FC8G-

	8Gbps				8Gbps		SW
VHSAN950601	Fiber Channel 8Gbps	3/5	DS-SFP-FC8G-SW	VHSAN554801	Fiber Channel 8Gbps	1/32	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/6	DS-SFP-FC8G-SW	VHSAN554802	Fiber Channel 8Gbps	1/32	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/7	DS-SFP-FC8G-SW	TAPE_LB	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/8	DS-SFP-FC8G-SW	TAPE_LB	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/9	DS-SFP-FC8G-SW	TAPE_LB	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	3/10	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/11	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/12	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/13	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/14	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/15	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/16	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/17	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/18	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/19	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/20	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/21	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/22	DS-SFP-FC8G-SW	Free			

VHSAN950601	Fiber Channel 8Gbps	3/23	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/24	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/25	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/26	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/27	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/28	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/29	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/30	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/31	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	3/32	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/1	DS-SFP-FC8G-SW	VNX		TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/2	DS-SFP-FC8G-SW	VNX	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/3	DS-SFP-FC8G-SW	DD	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/4	DS-SFP-FC8G-SW	DD	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/5	DS-SFP-FC8G-SW	VHSAN554801	Fiber Channel 8Gbps	1/31	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/6	DS-SFP-FC8G-SW	VHSAN554802	Fiber Channel 8Gbps	1/31	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/7	DS-SFP-FC8G-SW	TAPE_LB	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel 8Gbps	4/8	DS-SFP-FC8G-SW	TAPE_LB	Fiber Channel 8Gbps	TBD	DS-SFP-FC8G-SW
VHSAN950601	Fiber Channel	4/9	DS-SFP-FC8G-SW	Free			

	8Gbps						
VHSAN950601	Fiber Channel 8Gbps	4/10	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/11	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/12	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/13	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/14	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/15	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/16	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/17	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/18	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/19	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/20	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/21	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/22	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/23	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/24	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/25	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/26	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/27	DS-SFP-FC8G-SW	Free			

VHSAN950601	Fiber Channel 8Gbps	4/28	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/29	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/30	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/31	DS-SFP-FC8G-SW	Free			
VHSAN950601	Fiber Channel 8Gbps	4/32	DS-SFP-FC8G-SW	Free			
VHSAN950601	Mgt	5/0	RJ-45	VHADM296004	Gig	0/5	RJ-45
VHSAN950601	Mgt0	6/0	RJ-45	VHADM296005	Gig	0/1	RJ-45

Nota:

La definición de TBD significa "Por ser definido", esta información será proporcionada por el cliente o socio del equipo antes de la implementación. Si no se proporciona en el momento de escribir este documento o en fase de ejecución, se espera que esta información sea recibida en la fase de operación, por lo que el equipo de operación debe aplicarla.

2.5 Esquema de direccionamiento de VLAN e IP

La empresa ha asignado redes privadas para el Data Center de Villahermosa, estas redes se pueden dividir en subredes más pequeñas para adaptarse a cada módulo o requisitos específicos de cada nivel.

La tabla 2.13 muestra la VLAN global y la asignación de direcciones IP que se utilizará en el sitio de Villahermosa.

Tabla 2.13 Esquema de Direccionamiento

DESCRIPCIÓN	RANGO DE VLAN	NETWORK (RED)	MASK 1
Base de Datos	1801-1900	172.28.A.0	255.255.255.0
Cliente-Servidor (1)	2701-2800	172.28.B.0	255.255.255.0
Cliente-Servidor (2)	2801-2900	172.28.C.0	255.255.255.0
FW Context	1950-1999	172.28.D.0	255.255.255.0
Gestión	2087-2094	172.28.E.0	255.255.255.0
Gestión en comunicaciones	2000-2086	172.28.F.0	255.255.255.0
Legacy	2901-3000	172.28.G.0	255.255.255.0
PI	2401-2500	172.28.H.0	255.255.255.0

Respaldos	2501-2600	172.28.I.0	255.255.255.0
WEB	2601-2700	172.28.J.0	255.255.255.0
NAS	3001-3100	172.28.K.0	255.255.255.0
HPC	3101-3200	172.28.L.0	255.255.255.0

Capítulo 3: Módulo de Core del Data Center

3.1 Descripción general

El Core proporciona conectividad entre todos los otros módulos del Data Center; se utiliza para mantener la modularidad de la arquitectura general. Debe proporcionar una alta disponibilidad y adaptarse a los cambios rápidamente así como escalabilidad y convergencia rápida.

Sus características son las siguientes:

- ➔ Complejidad Baja
- ➔ Alto rendimiento
- ➔ Alta disponibilidad
- ➔ Arquitectura modular

3.2 Componentes de hardware

En las tablas se muestranlos componentes a nivel hardware que se utilizarán para los Switches Nexus 7009.

En la tabla 3.1 se muestranlas tarjetas físicas y módulos del equipo Nexus 7009.

Tabla 3.1 Nexus 7009 – Ubicación de las tarjetas físicas y sus módulos

Slot	Módulo	Descripción
1	N7K-SUP2	Nexus 7000 – Supervisor 2 Includes External 8GB USB Flash
2	N7K-SUP2	Nexus 7000 – Supervisor 2 Includes External 8GB USB Flash
3	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
4	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
5	Vacío	Vacío
6	Vacío	Vacío
7	Vacío	Vacío

8	Vacío	Vacío
9	N7K-M148GS-11L	Nexus 7000 – 48 Port GE Module with XL Option (req. SPF)
FM1	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM2	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM3	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM4	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM5	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
PS1	N7K-AC-6.0KW	Nexus 7000 – 6.0KW AC Power Supply Module
PS2	N7K-AC-6.0KW	Nexus 7000 – 6.0KW AC Power Supply Module

En la tabla 3.2 se muestran los tipos de transceiver utilizados.

Tabla 3.2 Módulos Nexus 7009 SFP

Cantidad	Módulo	Descripción
32	X2-10GB-SR	10GBASE-SR X2 Module
8	GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM
16	GLC-T	1000BASE-T SFP

Nota:

Los Módulos X2 son 10GBBASE-SR, cada supervisor tiene 1 puerto de administración de Gigabit ethernet.

En la figura 3.1 se muestra el equipo Nexus 7009 en su vista frontal y trasera.

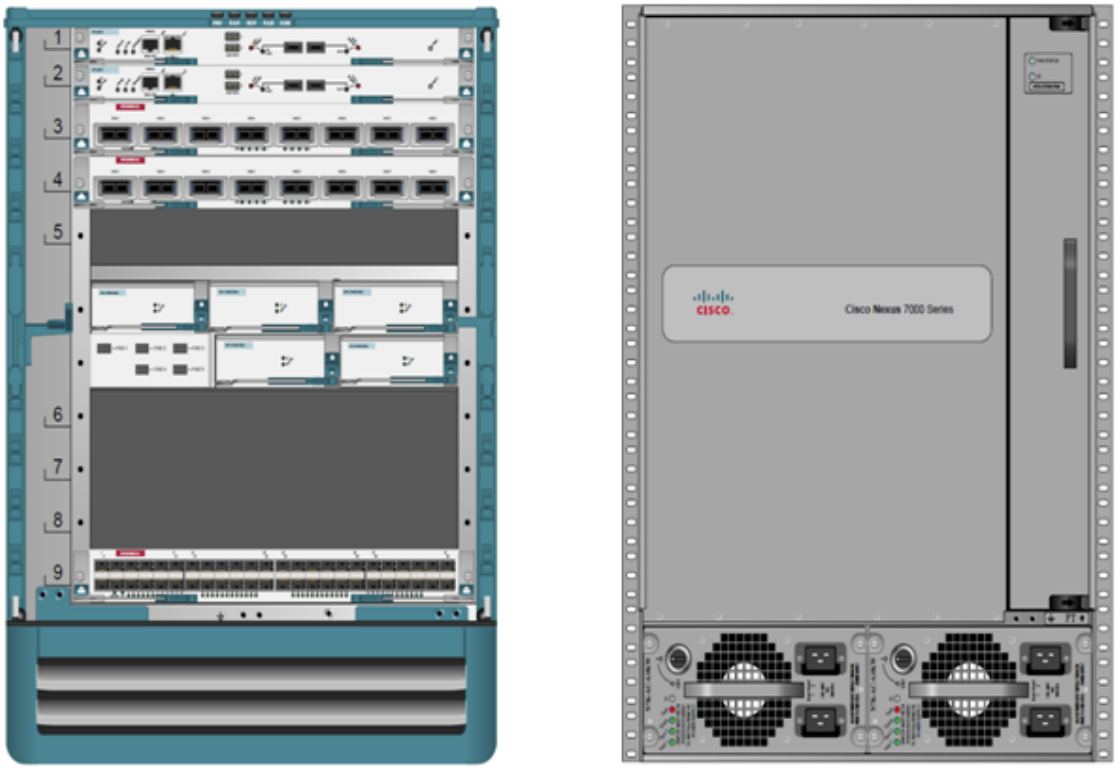


Figura 3.1 Vista frontal y trasera del equipo Nexus 7009

3.3 Sistema de nivel de alta disponibilidad

Los Switches Nexus 7009 de Cisco proveen varias características de redundancia a nivel de sistema que incluyen las siguientes capacidades:

- ➔ La redundancia de doble supervisor ofrece capacidades tales como stateful supervisor de conmutación y la actualización de software (ISSU).
- ➔ Los módulos de fabricación redundantes proporcionan protección contra los fallos de módulos individuales.
- ➔ Las fuentes de alimentación redundantes protegen el sistema contra cualquier falla en el suministro de energía o interrupción de la red cuando se configura adecuadamente.
- ➔ Posibilidad de instalar múltiples módulos de E/S de hardware, los cuales permiten construir redes con direccionamiento y diversos módulos de E/S para el PortChannel con igual costo (ECMP).

3.4 Especificaciones de software

El chasis del Nexus 7009 corre el NX-OS. Cisco NX-OS es un sistema operativo diseñado para el Data Center con modularidad, flexibilidad y capacidad de servicio desde su creación. La licencia "Enterprise"ofrece enrutamiento IP, el protocolo OSPF versión 2 sobre IPv4 y un conjunto de características. La virtualización en el protocolo Overlay Transport será apoyada con la licencia de servicios de transporte.

La tabla3.3 proporciona el software recomendado para switches Nexus.

Tabla 3.3 Sistema Operativo de los equipos Nexus 7009

Software	Descripción
NxOS EPDL 6.1(2a), NxOS Kick Start 6.1.2 NxOS System Software 6.1.2	Nexus 7000 Release 6.1.2
NxOS EPDL 6.1(2a), NxOS Kick Start 6.1.2 NxOS System Software 6.1.2	Nexus 7000 Release 6.1.2

La licencia de 'Enterprise LAN Advanced" proporciona capacidades de virtualización como los Contextos de Dispositivos Virtuales (VDC´s).

La tabla 3.4 muestra el licenciamiento para el funcionamiento del equipo Nexus 7009.

Tabla 3.4 Licenciatura de los equipos Nexus 7009

Cantidad	Licencia	Descripción
2	DCNM-PAK	DCNM Advanced License kit for Nexus and MDS witches
2	N7K-SBUN-P1	Includes LAN ADV TRS EL2 DCNM License – Promotion
2	DCNM-N7K-K9-SBUN	DCNM for LAN Enterprise License for one Nexus 7000
2	N7K-ADV1K9-SBUN	Nexus 7000 Advanced LAN Enterprise License (VDC CTS Only)
2	N7K-EL21K9-SBUN	Nexus 7000 Enhanced Layer 2 Licenses (FabricPath)
2	N7K-LAN1K9-SBUN	Nexus 7000 LAN Enterprise License (L3 protocols)
2	N7K-TRS1K9-SBUN	Nexus 7000 Transport Services License
2	N7K-SAN1K9	Nexus 7000 SAN Enterprise License

3.5 Diseño físico de la red

La figura 3.2 muestran la conectividad física del Bloque de Core

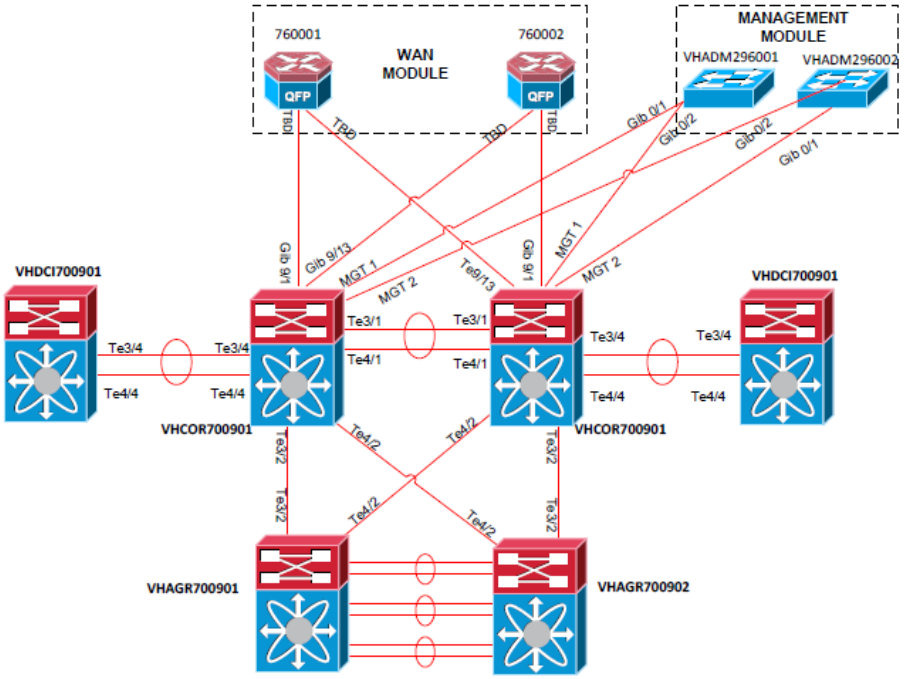


Figura 3.2 Core-conectividad Física

3.6 Virtualización

El Switch de Cisco Nexus 7009 tiene la capacidad de dividir un Switch físicoen cuatro switches virtualesmáximo. Estos switches virtuales llevan el nombre de contextos de dispositivo virtual (VDC s), donde cada VDC opera como un switch autónomo cada uno con un archivo de configuración, puertos físicos asignados y separa las instancias necesarias del protocolo de plano de control (CP), como los protocolos de enrutamiento y de spanning-tree. Los switches físicos Nexus 7009 en la Empresa se dividirán en entidades lógicas es decir VDC´s.

En el diseño propuesto para la Empresa los VDC´s se pueden aprovechar para proporcionar:

- ➔ Escalabilidad del hardware disponible para múltiples bloques lógicos del Data Center.
- ➔ Capa 2, Capa 3 y la zona de seguridad de la segmentación
- ➔ Una infraestructura de gestión independiente y controles de acceso dentro de los VDC´s.

Cada uno de los dos switches Nexus 7009 destinados para el bloque de Core se dividen en VDC´s lógicos, siguiendo el diseño se muestra el diagrama en la figura 3.3.

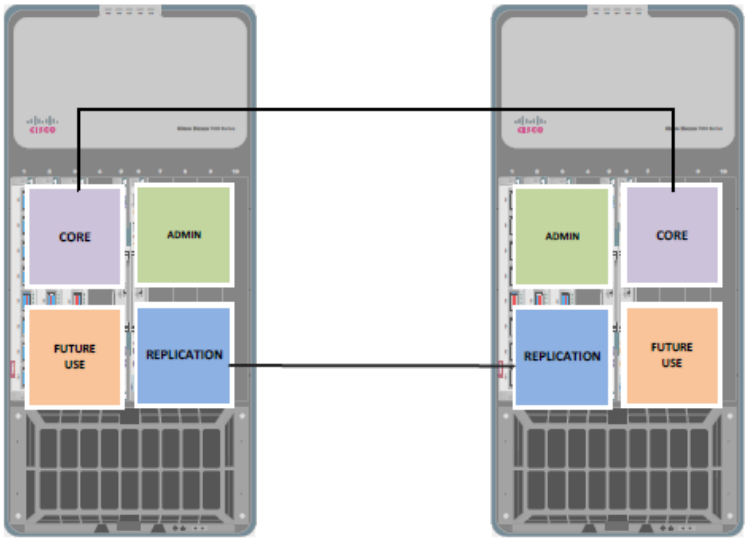


Figura 3.3 Core-VDC's Lógicos

Nota:

La versión 6.1 Cisco NX-OS introduce un nuevo tipo de VDC que proporciona un aislamiento aprueba de fallas para las funciones administrativas. El nuevo VDC es llamado VDC Admin, este se puede activar en el arranque inicial del sistema a través de un script de configuración. El administrador del VDC es compatible con los módulos Supervisor 2 y Supervisor 2E solamente. Cuando un VDC Admin está activado, sólo el puerto mgmt0 se asigna a esté. No es necesaria una licencia para la activación del VDC Admin.

Se crearán 2 VDC´s en la red de producción los cuales serán:

VDC Core

VDC Replicación

Los siguientes puntos son referentes a la topología física para el VDC Core:

- El VDC´s de Core, VHCOR700901-CORE y VHCOR700902-CORE a nivel físico habrá una interconexión entre ambos contextos virtuales por medio de 2 enlaces de 10 gigabitethernet, los cuales serán configurados en port-channel a nivel de L3 (capa 3) con protocolo LACP. Los puertos que compondrán este port-channel estarán en diferentes tarjetas físicas de los módulos del equipo de alta disponibilidad y redundancia máxima.

- Tendrá enlaces de 10 GE que se utilizaran para la conectividad del VDC Core con el Módulo de Agregación.

- Tendrá enlaces de 1 GE que se utilizaran para la conectividad del VDC Core con la WAN.

Los siguientes puntos son referentes a la topología física para el VDC de Replicación:

- Los VDC´s de Core, VHCOR700901-REP y VHCOR700902-REP, se conectaran entre sí por medio de 2 enlaces de 10 gigabitethernet, los cuales serán configurados en port-channel a nivel de L3 (capa 3) con protocolo LACP. Los puertos que compondrán este port-channel serán en diferentes tarjetas de línea de alta disponibilidad y redundancia máxima.

- Tendrá enlaces de 1 GE que se utilizaran para la conectividad del VDC Replicación con la WAN.

3.6.1 VDC Función asignación

Cada VDC proporcionará un conjunto único de funcionalidadespara la red, en la tabla 3.5 se describe el rol de cada VDC

Tabla 3.4 VDC Asignación de rol

Contexto de Dispositivo Virtual	Dispositivo Físico	Default	Redundante	Función
Admin	VHCOR700901 VHCOR700902	Yes	Yes	Switch Administrativo
Core	VHCOR700901 VHCOR700902	No	Yes	Data Center Core
Replicación	VHCOR700901 VHCOR700902	No	Yes	Storage IP Replication
Futuro Uso 1	VHCOR700901 VHCOR700902	No	Yes	Futuro Uso
Futuro Uso 2	VHCOR700901 VHCOR700902	No	Yes	Futuro Uso

Las siguientes consideraciones deben ser respetadas para el diseño de un VDC:

- El VDC Core es el contexto más crítico y el diseño debe soportar su disponibilidad.
- El VDC Admin que es el VDC default en el dispositivo tiene ciertas características especiales.
- Todos los parámetros en el sistema, tales como la vigilancia del plano de control (CoPP), asignación de recursos VDC, y el Protocolo de Tiempo de Red (NTP) se pueden configurar desde el VDC default que es el Admin.
- El licenciamiento del software del switch se controla desde el VDC default.
- Los algoritmos hash de los port-channel se configuran desde el VDC Default y se aplican a todo el sistema. Estos se pueden establecer específicamente por módulo.
- La instalación del software se debe realizar desde el VDC default: todos los VDC´s ejecutan la misma versión de software.
- Reinicios del sistema o recargas solamente se emiten desde el VDC default.

Nota:

La comunicación entre los VDC´s en una sola máquina física sólo puede ocurrir a través de un cable físico externo. Como medida de seguridad, los VDC´s no pueden comunicarse entre sí, salvo cuando se realice la conectividad física entre ellos.

3.6.2 NxOS - Compatibilidad de características en los VDC´s

Las características del soporte de VDC del software NX-OS de Cisco varían, dependiendo de la función. Sin embargo, las excepciones son los siguientes:

- **Control Plano Vigilancia (CoPP)** - Debido al soporte de hardware, se puede configurar las políticas CoPP solamente desde el VDC default. Las políticas CoPP se aplican a todos los VDC´s en el dispositivo físico.
- **Fabric-Extender** – Debe instalar la función Fabric Extender Nexus 2000 Series Cisco establecida en el VDC default antes de poder activar el Fabric Extender de cualquier VDC (incluido el VDC default).
- **Tasa de límites** - Debido al soporte de hardware, se pueden configurar límites de frecuencia sólo en el VDC default. Los límites de velocidad se aplican a todos los VDC´s en el dispositivo físico.

- **Túneles IP** – En versiones anteriores al Cisco NX-OS 4.2, se puede crear túneles sólo en el VDC default. Sin embargo, a partir de Cisco NX-OS versión 4.2 (1), se pueden poner interfaces de túnel en los VDC´s no default y VRFs.

- **FCoE** - A partir de Cisco NX-OS versión 5.2 (1) los dispositivos de la Serie Nexus 7000, tienen soporte FCoE para proporcionar a los usuarios de la red de área local (LAN) / red de área de almacenamiento (SAN) la separación de la administración de una interfaz física Ethernet. El Cisco NX-OS soporta Ethernet y FCoE solamente en los VDC´s no default que controlan partes Ethernet y almacenamiento de la red. Usted puede tener un solo VDC de almacenamiento configurado en el dispositivo.

Los VDC´s admin tienen las siguientes consideraciones y limitaciones para la configuración:

- No hay funciones o conjuntos de funciones que se puedan habilitar desde el VDC Admin.

- No se puede asignar ninguna interface física de los módulos al VDC Admin., Este VDC sólo puede tener asignado la interface mgmt0. Esto significa que para el admin VDC, sólo tiene su banda de gestióna través de la interfaz mgmt0.

- Cuando el VDC administrador está activado en el arranque, este sustituye el VDC default.

- Una vez creado el VDC de administración, no se puede eliminar y no se puede cambiar de nuevo al VDC default. Para cambiar al VDC default, se requiere un nuevo arranque.

3.6.3 VDC – Alta disponibilidad

En una implementación estándar para los VDC, los switches de la serie Nexus 7000 con supervisores duales utilizan un modelo de alta disponibilidad (HA) de conmutación, es decir, si hay un fallo a nivel de la tarjeta supervisora activa, todos los procesos se cambiarán a la tarjeta supervisora en espera. En caso de que se presentara una situación en donde no es posible, que la tarjeta supervisora en espera está listaporque está cargando, el sistema realizara en su lugar un reinicio dela tarjeta supervisora activa

.

Mientras que la política de HA no se puede cambiar para el VDC default, la política puede ser cambiada para los VDC´s no default en un sistema supervisor simple y doble. Las opciones para las políticas de HA para los VDC no default se encuentran en un entorno de supervisor dual:

- **Bringdown -** Pone el VDC en el estado fallido. Para recuperarse del estado fallido, debe volver a reiniciar el dispositivo físico.

- **Reiniciar –** Tira los procesos VDC e interfaces y lo reinicia con la configuración de inicio.

- **Conmutación (predeterminado para sistemas duales de supervisor) -** Inicia un módulo de conmutación de supervisor.

Esta opción en el diseño es para apoyar el funcionamiento del VDC Core y VDC Replicación ya que permite la conmutación con el supervisor VDC no crítico, mientras realiza el reinicio del VDC erróneo.

En la figura 3.4 se observa un ejemplo de la configuración de alta disponibilidad para los equipos Nexus 7009.

```
Nexus7k (config)#vdc xxxx
Nexus7k (config)#ha-policy dual-sup switchover
Nexus7k (config)# show vdc xxxx detail
```

Figura 3.5 VDC-Configuración de Alta Disponibilidad

3.7 Asignación de interfaces

El aspecto más importante de la asignación de recursos a los VDC´s, es la asignación de las interfaces a los contextos de dispositivos virtuales. Para permitir que un VDC pueda comunicarse con otros dispositivos en la red, el administrador debe asignar explícitamente interfaces para una VDC, excepto para el VDC por default que tendrá el control de todas las interfaces que no están ocupadas.

Los siguientes módulos Cisco Nexus 7009 Ethernet que pertenece a la capa de Core tienen el siguiente número de grupos de puertos e interfaces:

- N7K-M108X2-12L (1 interfaz x 8 grupos de puertos = 8 interfaces) - No hay restricciones en la asignación de interfaz entre los VDC´s.
- N7K-M148GS-11L, N7K-M148GT-11, N7K-M148GT-11L y N7K-M148GS-11 (12 x 4 grupos de interfaces de puerto = 48 interfaces) - No hay restricciones en la asignación de interfaz entre los VDC´s, pero recomiendan que las interfaces que pertenecen al mismo grupo de puertos estén en un sólo VDC.

En la tabla 3.6 observaremos la asignación de interfaces para cada VDC creado.

Tabla 3.6 Asignación de puertos VDC

Chasis	VDC	Puertos
Nexus 7009	VHCOR700901_CORE	Te3/1, Te3/2, Te3/4-8 Te4/1, Te4/2, Te4/4-8 Gig 9/1-9/36

Nexus 7009	VHCOR700902_CORE	Te3/1, Te3/2, Te3/4-8 Te4/1, Te4/2, Te4/4-8 Gig 9/1-9/36
Nexus 7009	VHCOR700901_REP	Te3/3 Te4/3 Gig 9/37-48
Nexus 7009	VHCOR700902_REP	Te3/3 Te4/3 Gig 9/37-48
Nexus 7009	VHCOR700901	Mgt1 Mgt2
Nexus 7009	VHCOR700902	Mgt1 Mgt2

3.8 Capa 3

El VDC Core proporciona la funcionalidad de ruteo en capa 3 a los módulos deAgregación, DCI y WAN. La funcionalidad de ruteo en la capa de Core será proporcionada por el protocolo de enrutamiento OSPF.

OSPF es el principal protocolo de enrutamiento IGP en el Data Center de la cloud de la Empresa. Las rutas redundantes de igual costo se proporcionan sobre la capa de agregación, algo por debajo de agregación esta en capa 2, y por lo tanto el protocolo de spanning-tree bloqueará los puertos redundantes. La autenticación MD5 se utiliza para minimizar la posibilidad de realizar enrutamiento con routers desconocidos.

Los puntos clave relativos a la implementación de la capa 3 de enrutamiento son los siguientes:

- ➔ La capa de VCD´s Core recibirá una ruta por default del VDC Agregación. Estos valores serán de igual costo, por lo que cada VDC de la capa de Core realizará el protocolo ECMP (CEF based) repartiendo la carga sobre ambos enlaces principales.

- ➔ La capa de Core dará comunicación L3 al VDC DCI, por medio deuna dirección IP para OTV y se anunciará en el protocolo OSPF a los MPLS.

- ➔ La autenticación MD5 se configurará en todos los enlaces en lo que OSPF se está ejecutando.

- ➔ El Ancho de Banda de referencia OSPF auto-cost se configurará a 100 MB para alinearse con el resto de la infraestructura del protocolo de OSPF (Nexus 7000 por default es 40 Gbps – un valor superior a IOS).

En la figura 3.5 se muestra el diseño de red a nivel de capa 3 del modelo OSI

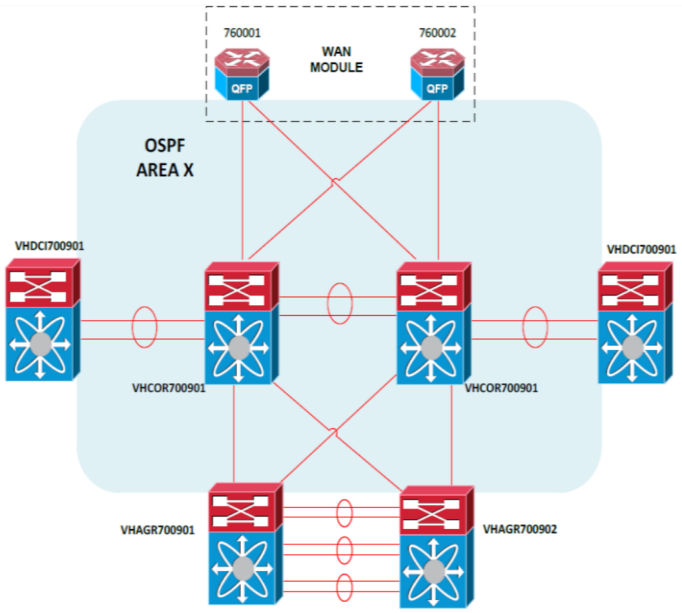


Figura 3.5 Diseño de capa de Red

3.9 Direccionamiento

En la figura 3.6 se muestra el direccionamiento IP considerado para el diseño de Core de la Empresa.

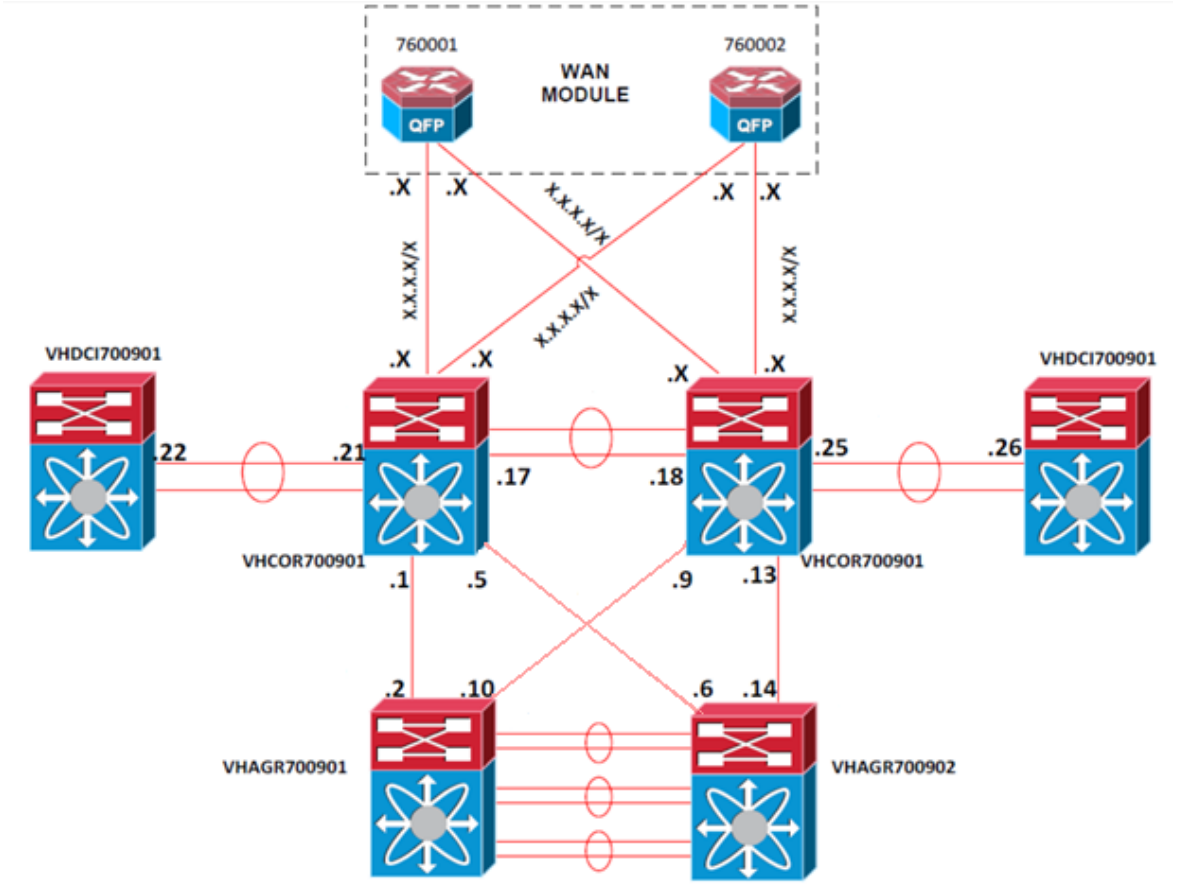


Figura 3.6 Direccionamiento CORE

3.10 Ruteo OSPF

El protocolo Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado-enlace utilizado para el intercambio de información de accesibilidad de la red dentro de un sistema autónomo. Cada router OSPF anuncia información sobre sus enlaces activos a sus routers vecinos. La información de enlace consiste en el tipo de enlace, la métrica, y el router vecino que está conectado al enlace. Los anuncios que contienen esta información de los vínculos se llaman anuncios de estado-enlace.

3.10.1 Alta disponibilidad OSPF

Una plataforma con dos supervisores que ejecutan Cisco NX-OS puede experimentar un supervisor de transición estable. Antes de que ocurra el cambio de conexión, OSPFv2 inicia un reinicio (activado por default) anunciando que OSPFv2 no estará disponible por algún tiempo. Cuando ocurre un cambio de conexión, la red continúa para reenviar el tráfico y mantener el sistema en la topología de la red.

Después de una conmutación, en el Cisco NX-OS se aplica la configuración en ejecución y OSPFv2 informa a los vecinos que es de nuevo operativo. Los vecinos ayudan a restablecer las adyacencias.

OSPFv2 se reinicia automáticamente si el proceso experimenta problemas. Tras la reanudación, OSPFv2 inicia un reinicio natural por lo que la plataforma no se saca de la topología de red. Si se reinicia manualmente OSPF, se realiza un reinicio natural, que es similar a una conmutación de estado. La configuración en ejecución se aplica en ambos casos.

Un desvío de reinicio, o reenvío sin escalas (NSF), permite a OSPFv2 permanecer en la ruta de transmisión de datos a través de un proceso de reinicio. Cuando OSPFv2 tiene que reiniciar, primero envía un enlace local (tipo 9) LSA, llamado LSA natural. Este reinicio de la plataforma OSPFv2 se llama NSF competente.

El LSA natural incluye un período de gracia, en un periodo de tiempo determinado en el que las interfaces OSPFv2 vecinas esperan hasta que la LSA de la interfaz reinicie OSPFv2. (Normalmente, OSPFv2 derriba la adyacencia y descarta todas las LSA desde abajo o reinicia la interfaz OSPFv2.) Los vecinos participantes son llamados ayudantes NSF y mantienen todos los LSA que se originan desde el reinicio de la interfaz OSPFv2 como si la interfaz siguiera siendo adyacente.

Cuando la interfaz OSPFv2 reinicia y vuelve a ser operativa, se redescubren sus vecinos, establece adyacencia, y comienza a enviar sus actualizaciones LSA de nuevo. En este punto, los ayudantes NSF reconocen que el reinicio natural ha terminado.

3.10.2 OSPF BFD

Esta función admite la detección de reenvío bidireccional (BFD). BFD es un protocolo de detección que proporciona un reenvío rápido de la ruta en tiempo de detección de fallos. BFD proporciona una segunda detección de fallos entre dos dispositivos adyacentes y puede ser menos CPU-intensivo que los mensajes de protocolo de saludo porque algunos BFD de carga pueden ser distribuidos sobre el plano de datos en los módulos soportados.

En la figura 3.7 se muestra la plantilla de configuración para el OSPF BFD

```
Nexus7k(config)#feature bfd
Please disable the ICMP redirects on all interfaces running BFD sessions using the command below [no ip redirects] |
Nexus7K(config)#int e1/1
Nexus7K(config-if)#no ip redirects
Nexus7K(config-if)#ip ospf bfd
```

Figura 3.7 Configuración BFD

3.10.3 OSPF Área 0

En todos los enlaces ascendentes de los módulos de agregación, DNI y WAN del Core se ejecutará OSPFv2, y también formarán parte de la red troncal OSPF, Área 0.

- ➔ Los dispositivos Core Nexus 7009 se conectarán a la agregación, DNI y módulos WAN, y las conexiones L3 serán en la zona 0.

- ➔ OSPF sólo se ejecutará entre los dispositivos L3 de red de Cisco. En los firewalls no se ejecutará OSPF.

En el Core VDC sólo se ejecuta el proceso de OSPF Zona 0 a través de la agregación, DCI y los módulos WAN.

3.10.4 Proceso de ruteo OSPF

La activación de OSPF requiere que una instancia de enrutamiento de OSPF sea creada mediante la configuración de un proceso de OSPF. Es de gran ayuda y también una buena práctica asignar un nombre fácil de recordar y un número de proceso distinto para la red básica, por ejemplo 0. El número de procesos es significativo a nivel local con el router en un dominio OSPF. El ID de proceso para la capa de Core de la empresa es 100.

En la figura 3.8 se muestra la configuración del proceso de ruteo.

```
router ospf <process-id>
```

Figura 3.8 Configuración del proceso de ruteo OSPF en los Nexus 7000

Nota:

En el OSPF NX-OS la función debe estar habilitada para configurar OSPF.

3.10.5 OSPF ID del ruteador

Cada router que ejecuta OSPF en una red debe tener un ID único de router. El ID del router es utilizado por la base de datos de estado de enlace OSPF (LSDB) como un método de monitoreo de cada router en el dominio y sus enlaces asociados. Por default OSPF utiliza la dirección IP más alta de una de las interfaces activas del router como router-id. Si se configuran las interfaces loopback con una dirección IP, el software Cisco NxOS usará direcciones más altas de bucle como su ID de router, a pesar de que otras interfaces que tienen direcciones IP superior. Principalmente, las interfaces loopback no se ven afectados por la falta de circuitos. Mediante la configuración de bucle invertido de dirección IP de la interfaz como router-id, se logra una mayor estabilidad en la tabla de enrutamiento. Se recomienda disponer de direcciones de bucle configurados en todos los dispositivos con el fin de tener un determinista OSPF ID del router.

En la figura 3.9 se muestra la configuración del ID del router

```
router ospf <number>
router-id <router_id>
```

Figura 3.9 Configuración del ID del router OSPF en Nexus 7009

En la tabla 3.7 se muestra los router ID utilizados en el equipo Core

Tabla 3.7 OSPF – Router IDS usados en el Core de la empresa

Nombre del Dispositivo	Router ID
COR700901_CORE	172.28.F.193
COR700902_CORE	172.28.F.194

3.10.6 Referencia del ancho de banda de OSPF

Por default el NX-OS calcula el costo del enlace mediante el uso de ancho de banda de referencia de 40 Gbps. El Cisco NX-OS ejecuta automáticamente un ancho de banda de referencia más razonable por default de 40,000 Mbps. Este valor proporciona una mayor flexibilidad en el desarrollo de interfaces 40 Gbps y 100 Gbps en la plataforma de los Nexus 7000.

Nota:

En la red del Data Center tanto con NX-OS y dispositivos IOS, el de ancho de banda de referencia debe ajustarse de modo que todos los dispositivos dentro de un área OSPF puedan utilizar un valor consistente. La configuración de ancho de banda de referencia para OSPF en Cisco NX-OS es idéntica a Cisco IOS, y se realiza con el uso del comando de referencia de ancho de banda de auto-coste.

El valor por default para la métrica OSPF se basa en el ancho de banda normalizado. Por defecto OSPF calculará la métrica OSPF para una interfaz de acuerdo con el ancho de banda de la interfaz.

OSPF usa un ancho de banda de referencia de 100 Mbps para el cálculo de host. La fórmula para calcular el costo es el ancho de banda de referencia dividido por el ancho de banda de la interfaz. Por ejemplo, en el caso de Ethernet, es 100 Mbps/10 Mbps = 10.

En el caso de redes con gran ancho de banda (es decir, un gigabit Ethernet), se debe utilizar un número mayor para diferenciar el costo de los enlaces frente a otros (siempre y cuando dichos enlaces estén disponibles, por ejemplo, diez gigabit Ethernet o Fast Ethernet podrían considerarse suficientes).

Si el ancho de banda de referencia se deja en su valor por default, entonces el costo de un Fast Ethernet, Gigabit Ethernet y enlaces de diez Gigabit Ethernet sería 1, siempre y cuando no exista diferenciación de OSPF para las distintas velocidades de enlace.

Para superar esto, el ancho de banda de referencia debe ser cambiado en todos los dispositivos para el enlace más rápido que pudiera existir en la red. En la actualidad, las interfaces más rápidas disponibles para los dispositivos de la empresa son Ethernet 10 Gigabit, pero es importante estar preparados para el futuro de 40GB.

Sin embargo todo el enrutamiento OSPF dentro de la empresa tiene el ancho de banda de referencia por default de 100 Mbps si se requiere cambiar el ancho de banda de referencia a 40 Gbps,see necesitaríacambiar la configuración de todos los routers que ejecutan OSPF.

En la figura 3.10 se muestra la configuración de referencia de Ancho de banda.

```
Router(config)#router ospf <Process ID>
Router(config-router)#auto-cost reference-bandwidth 40000 →sets the ref-bw to 40 gigabit
```

Figura 3.10 Configuración de referencia de ancho de banda

Nota:

El valor establecido por el comando *ip ospf cost*anula el costo resultante del comando OSPF auto-cost.

Nota:

El ancho de banda de referencia debe establecerse en todos los routers para proporcionar la asignación de costos coherentes en toda la red. También debe asegurarse de que el ancho de banda de la interfaz correcta se refleja en la interfaz física.

3.10.7 Red tipo OSPF

Las interfaces Ethernet son ***broadcast***de forma predeterminada. Se recomienda el uso de red de tipo punto a punto en todos los dispositivos con el fin de evitar el proceso de elección del router para la designación de OSPF.

En la figura 3.11 se muestra la configuración de red tipo OSPF

```
interface Ethernet slot#/type#  ip ospf network point-to-point
```

Figura 3.11 Configuración de red tipo OSPF en los Nexus 7009

3.10.8 Convergencia OSPF

En la empresa el proceso OSPF 100 va a cambiar a la configuración por default de los valores que mostrados a continuación:

En la tabla 3.8 muestra la relación de temporizadores OSPF

Tabla 3.8 Temporizadores OSPF

Temporizadores	Valor Defult Broadcast/Punto a Punto	OSPF de la Empresa
ip ospf dead-interval	4 x hello interval (40 seg/120 seg)	3 seg
ip ospf hello-interval	10 seg/ 30 seg	1 seg
ip ospf retransmit-interval	5 seg	5 seg
ip ospf transmit-delay	1 seg	1 seg

Cada uno de estos temporizadores afecta el rendimiento de OSPF y se pueden ajustar para efectuar tanto el tiempo de convergencia como la utilización de recursos de red. Si bien es posible utilizar los valores más pequeños para los intervalos muertos y saludos, estos valores deben ser evaluados en relación con la estabilidad de la red y con la utilización general de los recursos.

En la figura 3.12 se muestra la configuración de los temporizadores OSPF.

```
interface Ethernet slot#/type#
    ip ospf dead-interval 3
    ip ospf hello-interval 1
ip ospf mtu-ignore
```

Figura 3.12 Configuración de los temporizadores en los Nexus 7009

Nota:

El enlace con el módulo WAN será utilizado como predeterminado con los temporizadores de OSPF.

3.10.9 Autenticación OSPF

La autenticación de paquetes MD5 se considera una buena práctica y se puede configurar en la Empresa.

Para cada mensaje OSPFv2, Cisco NX-OS crea un mensaje MD5 unidireccional dirigido, basado en su propio mensaje y la contraseña cifrada. La interfaz envía este resumen con el mensaje OSPFv2. El vecino OSPFv2 al recibir, valida el resumen utilizando la misma contraseña cifrada. Si el mensaje no ha cambiado, el cálculo del resumen es idéntico y el mensaje OSPFv2 se considera válido.

La autenticación MD5 incluye un número de secuencia con cada mensaje OSPFv2 para asegurar que ningún mensaje se repite en la red.

En la figura 3.13 se muestra la configuración OSPF MD5 para autenticación.

```
interface Ethernet slot#/type#
      ip ospf dead-interval 3
    ip ospf hello-interval 1
ip ospf mtu-ignore
```

Figura 3.13 Configuración OSPF MD5 para autenticación en los Nexus 7009

Nota:

Cualquier cambio de autenticación tiene que ser configurado en todos los routers dentro del proceso OSPF.

3.10.10 Límites de configuración OSPF

La siguiente tabla resume los valores de escalabilidad OSPF v2 verificados para los switches Cisco Nexus 7000.

Tabla 3.10 OSPFv2- Límites de configuración

Parámetros	Límite verificado (Cisco NX-OS 5.2)
Number of active interfaces	300
Number of passive interfaces	500
Number of process instances per VDC	4
Number of neighbors/total routes with aggressive timers (1s/3s)	16/6000

3.10.11 Resumen de diseño OSPF

Con base en la red de la empresa y el enfoque jerárquico se resumen las configuraciones en:

- ➔ El área OSPF 0 se ejecutará en el Corede la empresa.
- ➔ Todas las interfaces físicas en el área 0 deben tener vecinos OSPF.
- ➔ Todas las interfaces físicas en el área 0 deben ser redes punto a punto.
- ➔ Todos los routers OSPF deben asignar una dirección de loopback (loopback0), que se utilizará para el ID del router.
- ➔ Se tiene que ajustar el auto-cost reference-bandwidth a 100 Mbps en todos los routers durante el uso de enlaces de alta velocidad.
- ➔ Se debe asegurar que el ancho de banda de todas las interfaces físicas se reflejan en función de su velocidad.
- ➔ Los saludos y tiempos muertos deben ser cambiados a 1 y 3 para mejorar los tiempos de convergencia.

3.10.12 Plantilla de configuraciones OSPF

La siguiente configuración OSPF es un ejemplo de un switch core de la red. La misma configuración se puede usar para el otro switch core. Sólo el router-ID y las interfaces de red necesitan ser cambiadas.

En la figura 3.14 se muestra la plantilla de configuración.

```
Router(config)#interface Loopback0
Router(config-if)#ip address <address><subnet mask>
Router(config-if)#no ip directed-broadcast
Router(config)#interface Type <slot#/port#>
Router(config-if)#ip address <address><subnet mask>
Router(config-if)#no ip directed-broadcast
Router(config-if)#udld aggressive
Router(config-if)#ip ospf network point-to-point
Router(config-if)#ip ospf hello-interval 1
Router(config-if)#ip ospf dead-interval 3
Router(config-if)#ip ospf mtu-ignore
Router(config-if)#ip router ospf 100 area 0
Router(config)#router ospf <process-id>
Router(config-router)#router-id <address>
Router(config-router)#log-adjacency-changes
```

Figura 3.14 Plantilla de configuración OSPF

3.11 Flujos de tráfico

Una vez que los usuarios de la Empresa obtengan acceso a red de la cloud a través del módulo deWAN, el Core enviará paquetes al módulo de agregación usando enrutamiento OSPF.

Conectividad entre Core y agregación es parte de OSPF área 0 y también utilizan ECMP al tráfico y balancear la carga en los múltiples caminos.

En la figura 3.5 observaremos un diagrama que nos explicara el flujo del tráfico en los equipos CORE

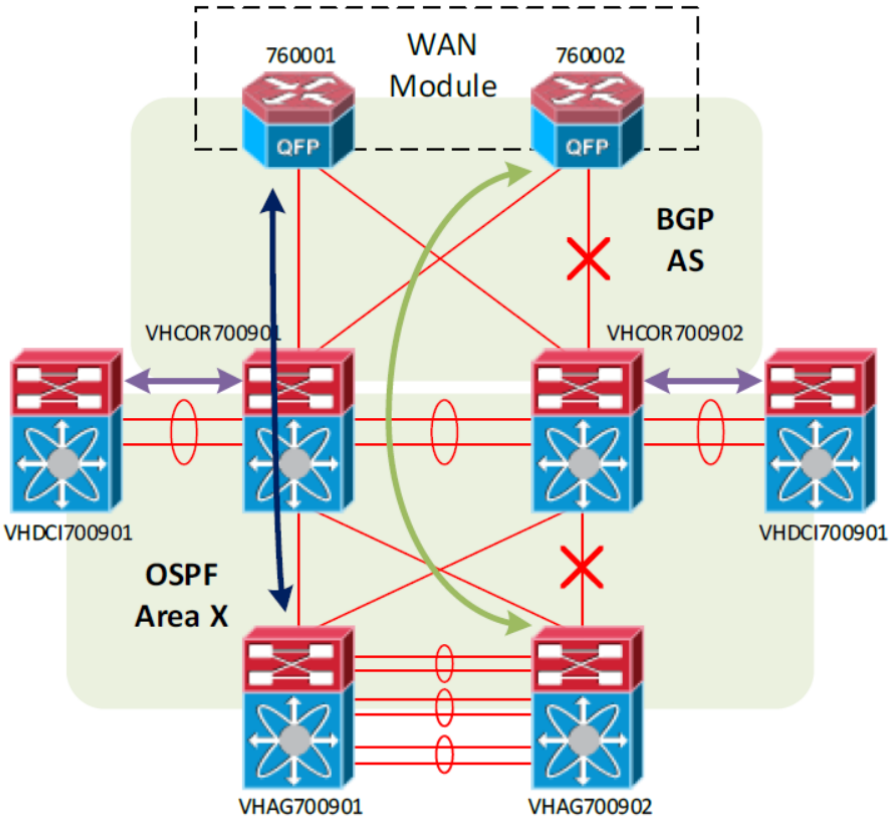


Figura 3.15 Diagrama de flujos de tráfico del CORE

Capítulo 4: Módulo de agregación

4.1 Descripción general

El módulo de agregación tiene muchas capas de acceso a enlaces ascendentes conectados a ella, tiene la responsabilidad principal de la agregación de las miles de sesiones que entran y salen del Data Center. Los switches de agregación son capaces de soportar múltiples enlaces de Ethernet a 10 Gigabit y Gigabit Ethernet. El bloque de agregación también ofrece conectividad a la capa de servicios, que proporciona seguridad y optimización de aplicaciones.

4.2 Componentes de hardware

Las siguientes tablas muestran los módulos y tarjetas de línea que se utilizarán para los Switches Nexus 7009.

La Tabla 4.1 muestra la ubicación de los slots del Switch Nexus 7009

Tabla 4.1 Ubicación de los slots del Nexus 7009

Puerto	Módulo	Descripción
1	N7K-SUP2	Nexus 7000 - Supervisor 2 Includes External 8GB USB Flash
2	N7K-SUP2	Nexus 7000 - Supervisor 2 Includes External 8GB USB Flash
3	N7K-M108X2-12L x	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)
4	N7K-M108X2-12L x	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)
5	N7K-M108X2-12L x	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)
6	N7K-M108X2-12L x	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)
7	Empty	Empty
8	N7K-F132XP-15	Nexus 7000 - 32 Port 1G/10G Ethernet Module SFP/SFP+
9	N7K-F132XP-15	Nexus 7000 - 32 Port 1G/10G Ethernet Module SFP/SFP+
FM1	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module
FM2	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module
FM3	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module
FM4	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module
FM5	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module
PS1	N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module
PS2	N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module

Nota:

Los Módulos X2 son 10GBBASE-SR, SFP son GLC-SX-MMD o SFP-10G-SR o GLC-T, cada supervisor tiene 1 puerto de administración de GE.

La figura 4.1 muestra la vista frontal y trasera del switch Nexus 7009.

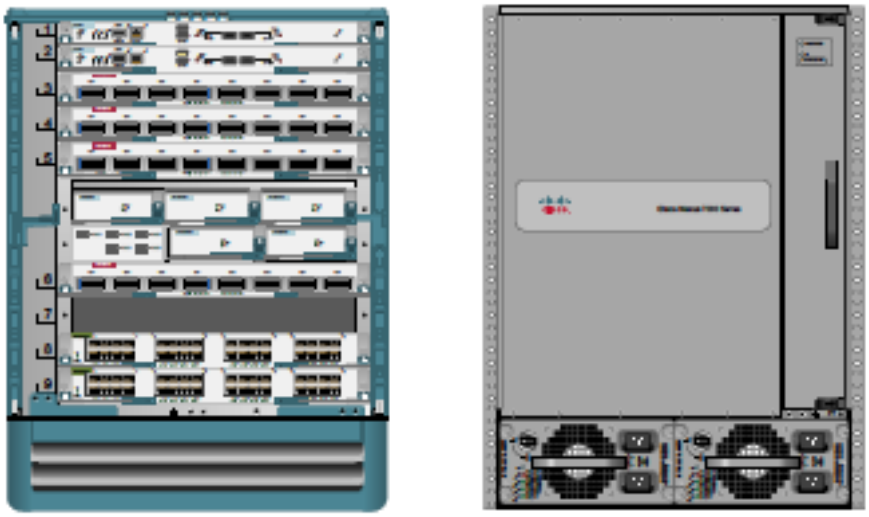


Figura 4.1 Vista frontal y trasera en los Nexus 7009

La Tabla 4.2 muestra los módulos del switch Nexus 7009 SFP

Tabla 4.2 Módulos del Nexus 7009 SFP

Cantidad	Módulo	Descripción
64	X2-10GB-SR	10GBASE-SR X2 Module
40	GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM
88	SFP-10G-SR	10GBASE-SR SFP Module

4.3 Sistema de alta disponibilidad

Los Switches Nexus 7009 de Cisco proporcionan varias características de redundancia de hardware a nivel de sistema que incluyen las siguientes capacidades:

- Redundancia doble supervisor que ofrece capacidades tales como stateful, supervisor de conmutación y proporciona la base para la actualización de software en servicio (ISSU).

- ➔ Los módulos redundantes de fábrica proporcionan protección contra las fallas de módulos de fábrica individuales.
- ➔ Fuentes de alimentación redundantes que protegen el sistema contra cualquier falla en el suministro de energía o interrupción de la red.
- ➔ Posibilidad de instalar múltiples módulos de E/S que permiten construir redes con rutas y diversidad de módulos de E/S para el Canal de Puertos (PortChannel) y enlaces múltiples con costos iguales(ECMP).

4.4 Especificaciones de software

En el chasis del Nexus 7009 corre el NX-OS, software de Cisco NX-OS, una clase de sistema operativo de tipo de Data Center construido con modularidad, flexibilidad y capacidad de servicio. La licencia Enterprise está obligada a proporcionar enrutamiento IP, y un conjunto de características OSPF v2 (IPv4). La Overlay Transport Virtualization (OTV) será soportada con la Licencia de Servicios de Transporte. La Tabla 3 proporciona el software recomendado para switches Nexus. La licencia Enterprise LAN Advanced proporciona capacidades de virtualización como VDC´S.

La Tabla 4.3 muestra el software utilizado por el switch Nexus 7009.

Tabla 4.3 Software de Nexus 7009

Dispositivo	Software	Description
VHAGR700901	NxOS EPLD 6.1(2a), NxOS Kick Start 6.1.2, NxOS System Software 6.1.2	Nexus 7000 Release 6.1.2
VHAGR700902	NxOS EPLD 6.1(2a), NxOS Kick Start 6.1.2, NxOS System Software 6.1.2	Nexus 7000 Release 6.1.2

La Tabla 4.4 muestra el control de licencias del switchNexus 7009.

Tabla 4.4 Licenciamiento del Nexus 7009

Cantidad	Licencia	Descripción
2	DCNM-PAK	DCNM Advanced License kit for Nexus and MDS witches
4	N7K-FCOEF132XP	FCoE License for Nexus 7000 32-port 10G SFP+ (F1)
2	N7K-SBUN-P1	Includes LAN ADV TRS EL2 DCNM License – Promotion
2	DCNM-N7K-K9-SBUN	DCNM for LAN Enterprise License for one Nexus 7000
2	N7K-ADV1K9-SBUN	Nexus 7000 Advanced LAN Enterprise License (VDC CTS Only)
2	N7K-EL21K9-SBUN	Nexus 7000 Enhanced Layer 2 Licences (FabricPath)

2	N7K-LAN1K9-SBUN	Nexus 7000 LAN Enterprise License (L3 protocols)
2	N7K-TRS1K9-SBUN	Nexus 7000 Transport Services License
2	N7K-SAN1K9	Nexus 7000 SAN Enterprise License

4.5 Diseño físico de la red

Lafigura 4.2muestrael diagrama de conectividad física de agregación al Core.

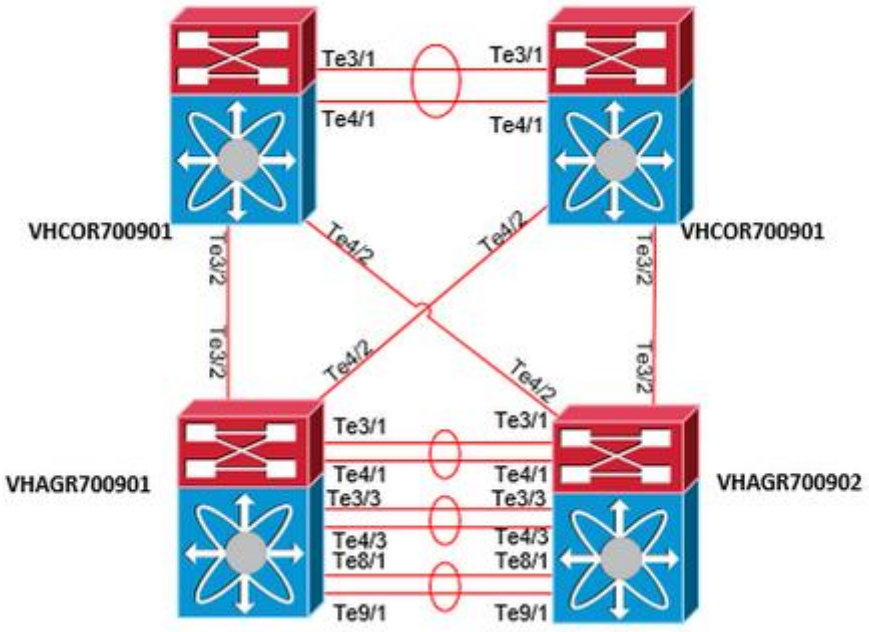


Figura 4.2 Agregación del Core de conectividad física

La figura 4.3 muestrael diagrama de conectividad física de agregación al módulo DCI.

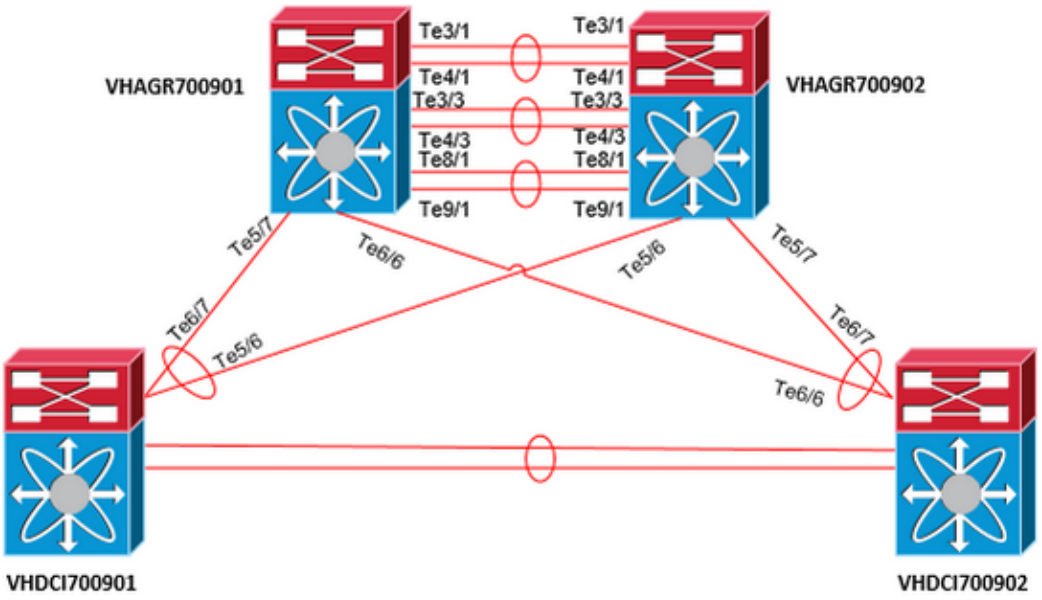


Figura 4.3 Agregación al módulo DCI de conectividad física

La figura 4.4 muestra el diagrama de conectividad física de agregación al módulo de servicios.

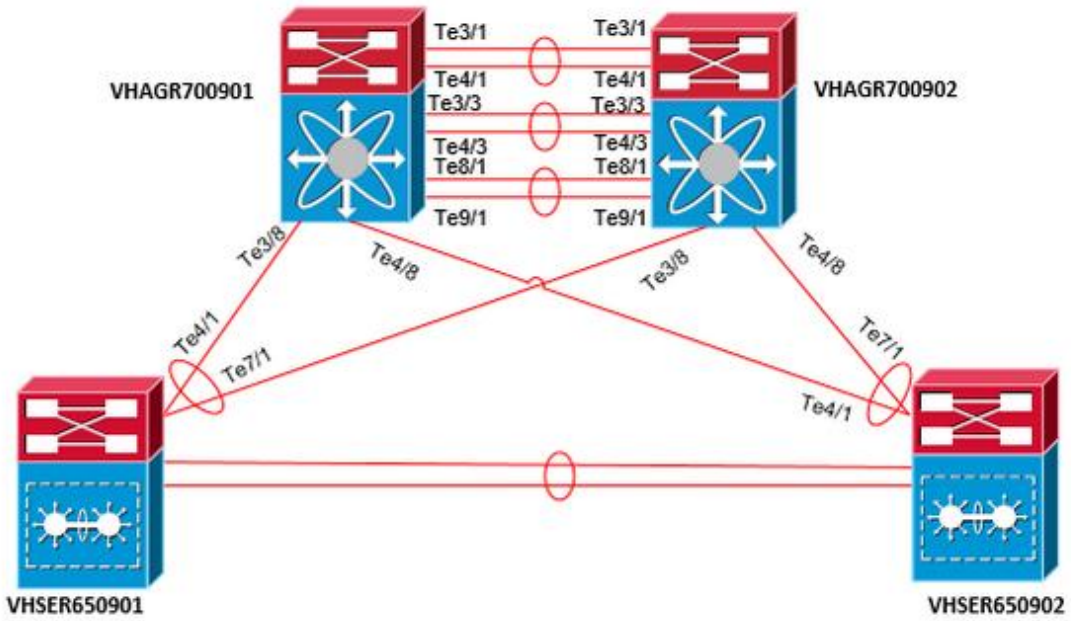


Figura 4.4 Agregación al módulo de servicios de la conectividad física

La figura 4.5 muestra el diagrama de conectividad física de agregación al módulo de acceso.

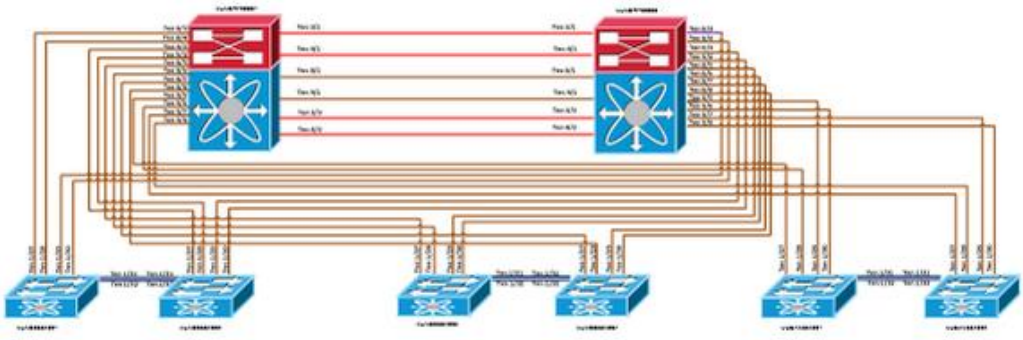


Figura 4.5 Agregación al módulo de la conectividad física

4.6 Virtualización

El switch de Cisco Nexus 7009 tiene la capacidad de dividir un switch físico único en un máximo de cuatro conmutadores virtuales. Estos conmutadores virtuales llevan el nombre de contextos de dispositivo virtual (VDC), donde cada VDC opera como un switch independiente con un archivo de configuración independiente, puertos físicos asignados al mismo y las instancias separadas de necesarios protocolos del plano de control, tales como protocolos de enrutamiento y el árbol de expansión. Los switches físicos Nexus 7009 en la empresa se dividirán en entidades lógicas (VCD).

En el diseño propuesto para la empresa, los VCD´s se pueden aprovechar para proporcionar:

- ➔ Escalabilidad del hardware disponible para múltiples datos lógicos de bloques centrales
- ➔ Capa 2, Capa 3 y seguridad en la zona de segmentación
- ➔ Una infraestructura de gestión independiente y controles de acceso en los VCD´s.

Cada uno de los dos switches Nexus 7009 en el core se divide en los VCD´s lógicos, siguiendoel diseño se muestra en el siguiente diagrama.

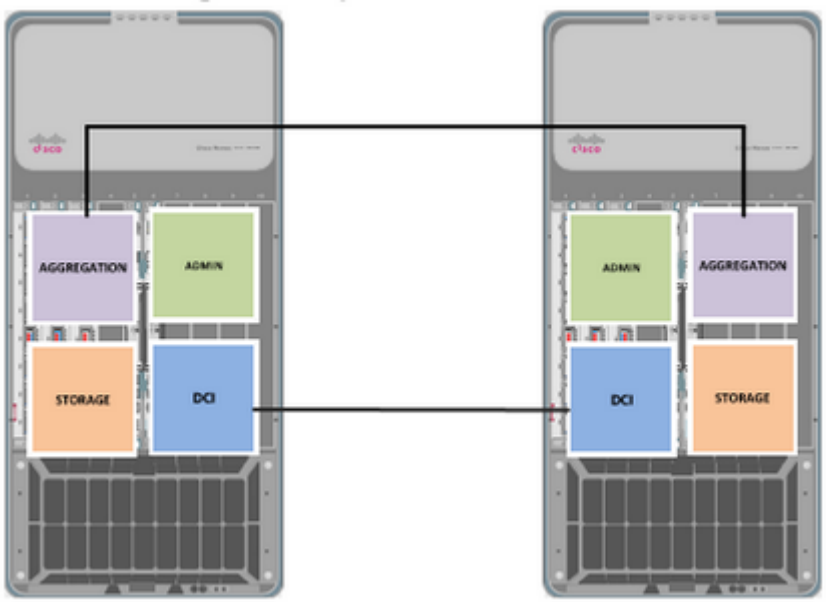


Figura 4.6 Desglose de contexto lógico de dispositivo Virtual

La versión 6.1 Cisco NX-OS introduce un nuevo tipo de VDC que proporciona aislamiento de fallas para las funciones de switch-administrativas. El nuevo VDC se llama VDC administrador.

Se puede activar el VDC administrador en el arranque inicial del sistema a través de un script de configuración. El administrador VDC se utiliza sólo para las funciones administrativas. El VDC administrador es compatible con supervisor 2 y sólo módulos de Supervisor 2E. Cuando unVDC administrador está activado, sólo el puerto mgmt0 se asigna al VDC administrador. Una licencia no es necesaria para habilitar VDC administrador.

Tres VDC´S se crearán en la red de producción de agregación, DNI y almacenamiento.

Los siguientes puntos se refieren a la topología física de la agregación VDC:

- ➔ Distribución VDC´s, VHCOR700901-agregación y VHCOR700902_AGGREGATION, estarán conectados entre sí por medio de enlaces 2 x 10GE para non-VLANs y Layer 3.
- ➔ 10 enlaces GE se utilizarán para conectarse al VCC Core a través de la capa 3.
- ➔ 10 enlaces GE se pueden utilizar para conectar al DCI VCC a través de la capa 2.
- ➔ Agregación VDC tendrán vínculos iguales vivos con dos enlaces de 10GE como parte de la configuración vPC, también dos 10GE formarán el peer-link vPC
- ➔ 10 enlaces GE de agregación al Access Nexus 5548 con FabricPath.
- ➔ Conectividad con el módulo de Servicios (firewall, IPS, balanceo de carga) se proporcionará a través de dos 10GE capa 2 enlaces en vPC.

Los siguientes puntos se refieren a la topología física del almacenamiento:

- ➔ El almacenamiento VDC´s, VHCOR700901-STORAGE y VHCOR700902-STORAGE, no se conectan entre sí, VHCOR700901-STORAGE actuará como Fabric A y VHCOR700902-STORAGE actuará como Fabric B.
- ➔ 10 enlaces GE se utilizarán para conectar el VDC de almacenamiento con la capa de acceso.
- ➔ FCoE se utilizará para la comunicación entre servidores y dispositivos de almacenamiento.
- ➔ 10 enlaces GE se utilizarán para conectar el VDC de almacenamiento con los dispositivos de almacenamiento.

4.6.1 VDC Función asignación

Cada VDC proporcionará un conjunto único de funcionalidad de la red como se describe a continuación:

Tabla 4.5 VDC Función asignación

VDC	Disco Físico	Default	Redundante	Función
Admin	VHAGR700901 VHAGR700902	Yes	Yes	Management switch
Aggregation	VHAGR700901 VHAGR700902	No	Yes	Data Center Core
DCI	VHAGR700901 VHAGR700902	No	Yes	Storage IP Replication
Storage	VHAGR700901 VHAGR700902	No	Yes	Future Use
Future Use 2	VHAGR700901 VHAGR700902	No	Yes	Future Use

Las siguientes consideraciones deben ser respetadas en el diseño VDC:

- ➔ La agregación y el almacenamiento son los contextos más críticos y el diseño deben apoyar su disponibilidad.
- ➔ El VDC administrador predeterminado en un dispositivo tiene ciertas características especiales:
- ➔ Parámetros de todo el sistema, tales como las políticas del plano de control, la asignación de recursos VDC, y el Protocolo de Tiempo de Red (NTP) se pueden configurar desde el VDC default.
- ➔ Las licencias del switch para las características del software se controlan desde el VDC default.
- ➔ Los algoritmos de puerto de canal hash se configuran desde el VDC predeterminado y se aplican a todo el sistema. Estos se pueden establecer específicamente por módulo.
- ➔ La instalación del software se debe realizar desde el VDC por default; todos los VDC´S ejecutan la misma versión de software.
- ➔ Los reinicios del sistema o recargas sólo se emiten desde el VDC default.

Nota:

Las comunicaciones entre los VDC´s en una sola máquina física sólo pueden ocurrir a través de cable físico externo.

Nota:

Cada módulo tiene su propio espacio de memoria L2 y L3 en la tabla de re-envío (forwarding table), por lo tanto si los puertos que pertenecen a una sola tarjeta de línea son

cuidadosamente asignados a los VCD´s individuales, en lugar de compartirlos, es posible dedicar todos los recursos en una tarjeta de línea a un VDC y disponer con un VDC con el espacio de memoria más disponible.

4.6.2 NxOS compatibilidad de características en los VDC´s

El soporte VDC para las características del software NX-OS de Cisco varía, dependiendo de la función. Para la mayoría de las características del software NX-OS de Cisco, la configuración y operación son locales para el VDC actual.

Sin embargo tenemos las siguientes excepciones:

- **Políticas del planeación de control (CoPP Control Plane Policing).** Debido al soporte de hardware, se puede configurar las políticas CoPP sólo en el VDC default. Las políticas CoPP se aplican a través de todos los VDC´s en el dispositivo físico.
- **Fabricación extendida (Fabric Extender).** Se debe instalar en el Nexus 2000 Series Cisco la función Fabricación extendida establecida en el VDC predeterminado antes de poder activar el extensor de fabricación de cualquier VDC (incluido el VDC default).
- **Tasa de límites.**Debido al soporte de hardware se pueden configurar límites de frecuencia sólo en el VDC default. Los límites de velocidad se aplican a todos los VDC en el dispositivo físico.
- **Túneles-IP.** En Cisco NX-OS las versiones anteriores a la 4.2, pueden crear túneles VDC´s sólo en el VDC default. Sin embargo, a partir de Cisco NX-OS versión 4.2 (1), se pueden poner interfaces de túnel en los VDC´S no predeterminados y VRFs.

- **Canal de fibra sobre Ethernet (Fibre Channel Over Ethernet FCoE).** A partir de la versión Cisco NX-OS 5.2 (1) para los dispositivos de la Serie Nexus 7000, VDC´S tienen soporte FCoE para proporcionar, a los usuarios de la red de área local (LAN)/red de área de almacenamiento(SAN), la gestión de separarse en una interfaz física Ethernet. Cisco NX-OS es compatible con Ethernet y FCoE sólo en los VDC´S no predeterminados que controlan las partes Ethernet y almacenamiento de la red. Usted puede tener un solo VDC almacenamiento configurado en el dispositivo.

Los VDC´S admin tienen las siguientes consideraciones para la configuración y limitaciones:

- No hay funciones o conjuntos de características que se pueden habilitar en el VDC administrador.
- Sin interfaces de cualquier módulo de tarjeta de línea, se pueden asignar al VDC administrador. Sólo mgmt0 pueden asignarse a la administración VDC. Esto significa que para el admin VDC, sólo administración fuera de banda es posible a través de la interfaz mgmt0.
- Cuando el VDC administrador está activado en el arranque, se sustituye el VDC default.
- Una vez creado el VDC de administración, no se puede eliminar y no se puede cambiar de nuevo el VDC default. Para cambiar de nuevo a los valores de VDC, se requiere un arranque de refresh.

4.6.3 Alta disponibilidad VDC

En un solo despliegue de VDC estándar, la serie de switches Nexus 7000 con supervisores duales utilizan un modelo de alta disponibilidad (HA) de transición supervisora, es decir, si hay un fallo de nivel de supervisor, todos los procesos se cambiarán al supervisor espera. En una situación en la que no es posible, por ejemplo, el supervisor espera no está listo porque está recargando, el sistema hace un supervisor reinicio del supervisor activo.

Si bien la política de HA no se puede cambiar para el VDC default, la política puede ser cambiada por los VDC´s no predeterminados en un sistema supervisor de simple y doble. Las opciones para las políticas de HA VDC´s no predeterminados se encuentran en un entorno de doble supervisor:

- ➔ **Bringdown -** Pone el VDC en el estado fallido. Para recuperarse del Estado fallido, debe volver a cargar el dispositivo físico.
- ➔ **Restart -** Toma y establece los procesos VDC e interfaces y lo reinicia con la configuración de inicio.
- ➔ **Conmutación-Switchover (predeterminado para sistemas duales de supervisor) -** Inicia un módulo de conmutación de supervisor.

El diseño del 7009 Nexus VDC en la empresa, agregación, DCI y almacenamiento VDC´S realizarán la función supervisor de conmutación en caso de fallo de nivel supervisor. Esta opción de diseño es para apoyar el funcionamiento agregación, DNI y almacenamiento VDC, al no permitir la conmutación supervisor VDC no crítica, al tiempo que permite a reiniciar VDC fallado. Si hay un problema de supervisor de sistemática, un supervisor de conmutación se puede realizar desde el VDC default.

```
Nexus7k(config)#vdc xxxx

Nexus7k (config)#ha-policy dual-sup
switchover

Nexus7k (config)# show vdc xxxx detail
```

Figura 4.7 Configuración de alta disponibilidad VDC

4.7 Asignación de interfaces

Posiblemente el aspecto más importante de la asignación de recursos a los VDC´s, es la asignación de las interfaces a los contextos de dispositivos virtuales. Para permitir que un VDC pueda comunicarse con otros dispositivos en la red, el administrador debe asignar explícitamente interfaces para un VDC, excepto por el VDC por default que tendrá el control de todas las interfaces que no están ocupadas de otra manera.

Los siguientes módulos Ethernet 7009 Series Cisco Nexus pertenecen a la capa de agregación y tienen el siguiente número de grupos de puertos e interfaces:

- ➔ N7K-M108X2-12L (1 interfaz de x 8 grupos de puertos = 8 interfaces) - No hay restricciones en la asignación de interfaz entre los VDC´s.
- ➔ N7K-F132XP-15 - Debe asignar las interfaces del dispositivo físico en la combinación especificada. Este módulo cuenta con 16 grupos de soporte formados por 2 puertos cada uno (2 x 16 grupos de interfaces de puerto = 32 interfaces). Interfaces pertenecientes a un mismo grupo de puertos deben pertenecer al mismo VDC.

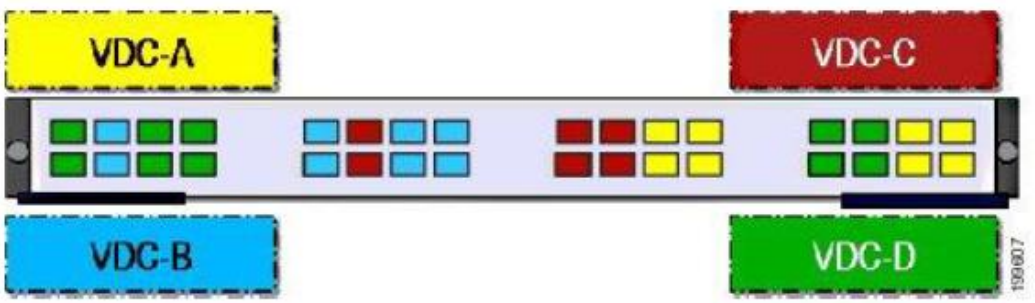


Figura 4.8 Asignación de interfaz para grupo de puertos en el módulo N7K-F132XP-15

La tabla 4.6 muestra la numeración de puertos por cada grupo de puertos:

Tabla 4.6 Número de puertos por grupo en el módulo N7K-F132XP-15

Grupo de puertos	Números de puerto
Group 1	1 and 2
Group 2	3 and 4
Group 3	5 and 6
Group 4	7 and 8
Group 5	9 and 10
Group 6	11 and 12
Group 7	13 and 14
Group 8	15 and 16
Group 9	17 and 18
Group 10	19 and 20
Group 11	21 and 22
Group 12	23 and 24
Group 13	25 and 26
Group 14	27 and 28
Group 15	29 and 30
Group 16	31 and 32

Tabla 4.7 Asignación de puertos VDC

Chassis	VDC	Puertos
Nexus 7009	VHAR700901_AGGREGATION	Te3/1-3, Te3/5-8 Te4/1-2, Te4/5-8 Te5/1-5/5 Te6/1-6/5 Te7/1-7/8 Te8/1-8, Te8/15-32 Te9/1-8, Te9/15-32
Nexus 7009	VHAR700902_AGGREGATION	Te3/1-3, Te3/5-8 Te4/1-2, Te4/5-8 Te5/1-5/5 Te6/1-6/5 Te7/1-7/8 Te8/1-8, Te8/15-32 Te9/1-8, Te9/15-32
Nexus 7009	VHAR700901_DCI	Te3/4 Te4/4 Te5/6-8 Te6/6-8
Nexus 7009	VHAR700902_DCI	Te3/4 Te4/4 Te5/6-8 Te6/6-8
Nexus 7009	VHAR700901_STORAGE	Te8/9-14 Te9/9-14
Nexus 7009	VHAR700902_STORAGE	Te8/9-14 Te9/9-14
Nexus 7009	VHAR700901	Mgt 1 Mgt 2
Nexus 7009	VHAR700902	Mgt 1 Mgt 2

4.8 Capa 3

Todos los enlaces de Agregación alVDC Core son enlaces de Capa 3. Las cuales son rutas redundantes de igual costo,además de que todas las conexiones que estén por debajo del bloque de Agregación se encontrarán a nivel de Capa 2 en el dominio de FabricPath. La autenticación MD5 se utiliza para minimizar la posibilidad de dirigir las relaciones con los routers desconocidos.

La funcionalidad de enrutamiento en la capa de agregación será proporcionada por el protocolo de enrutamiento OSPF.

En la figura 4.9 se reflejara la conectividad involucrada a nivel de la Capa 3 del modelo OSI

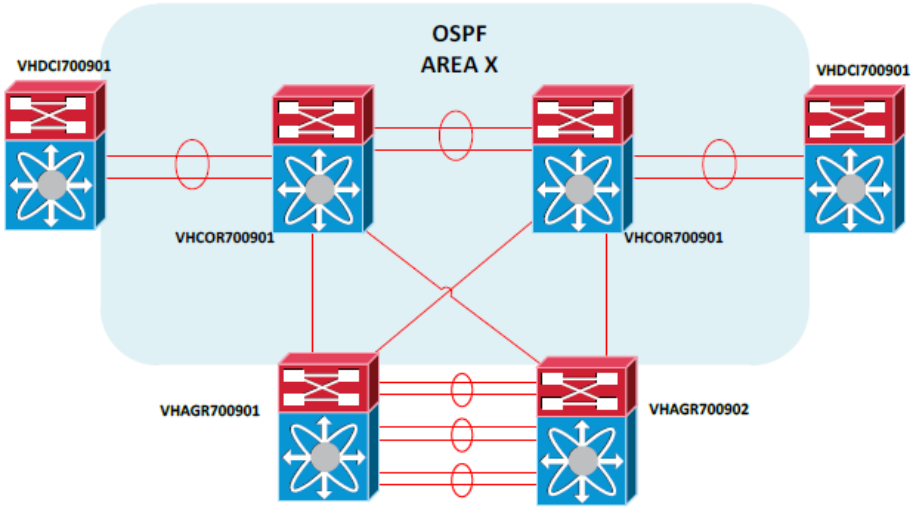


Figura 4.9 Diseño de Capa 3

Los puntos clave relativos a la capa 3 de enrutamiento son los siguientes:

- El VDC Core recibirá una ruta por default a los VDC´S de Agregación. Estos valores serán de igual costo, por lo que cada VDC Core realizará ECMP (CEF based) repartiendo la carga sobre ambos enlaces principales.
- La autenticación MD5 se configurará en todos los enlaces en OSPF que se estén ejecutando.
- El ancho de banda de referencia OSPF auto-cost se configurará a 100 Mbps para alinearse con el resto de la infraestructura de OSPF (Nexus 7000 por default es 40 Gbps - un valor superior a IOS).

A menos que se especifique lo contrario, los servidores fuera de la cloud de VLAN tendrán una interfaz de capa 3 asociado a un SVI para actuar como puerta de enlace predeterminada para las granjas de servidores. Estas interfaces SVI se pueden configurar para ejecutar HSRP y proporcionar redundancia de primero salto para los servidores.

Los puntos clave relativos a la configuración de SVI son las siguientes:

- El par HSRP activo se configura para que coincida con el Spanning-tree del puente raíz para la VLAN de que se trate.
- Interfaz OSPF pasiva.
- La interfaz SVI se configurará para residir en el lado de la cloud de vlan´s.
- HSRP la interfaz SVI activa se puede configurar con una prioridad de 110.
- HSRP la interfaz en espera SVI se pueden configurar con una prioridad de 90.
- Los temporizadores de HSRP se quedarán en sus valores por default debido a la presencia de supervisores duales del chasis Nexus 7000. Poner a punto de temporizadores HSRP a valores más bajos podría interferir con el proceso de conmutación en el caso de un fallo supervisor primario.

A menos que se especifique lo contrario, los servidores dentro de la cloud de VLANs tendrán un gateway predeterminado asociado que apuntará al router virtual Citrix, la interfaces SVI de agregación de capa3 actuarán como puerta de enlace predeterminada en el router virtual Citrix. Estas interfaces SVI se pueden configurar para ejecutar HSRP con el fin de proporcionar redundancia de primer salto para los servidores.

El VDC Agregación y el Servicio de enrutamiento virtual no ejecutarán ningún protocolo de enrutamiento, el tráfico de la WAN a la cloud se hará por proxy arp

4.8.1 Direccionamiento IP

La figura 4.10 se muestra la distribución del direccionamiento IP entre bloques

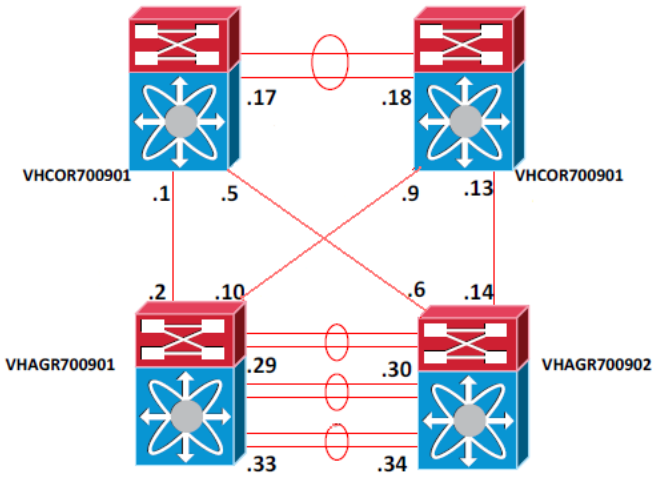


Figura 4.10 Direccionamiento VDC agregación al VDC Core

4.8.2 Ruteo OSPF

El protocolo Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado-enlace utilizado para el intercambio de información de la accesibilidad de la red dentro de un sistema autónomo. OSPF publica la información de sus enlaces activos a sus enrutadores vecinos. La información de enlace consiste en el tipo de vínculo, la métrica de enlace y el router vecino que se conecta al enlace. Los anuncios que contienen la información de este enlace se denominan anuncios de estado-enlace.

El enrutamiento OSPF en elVDC agregación se realiza sobre la base de las rutas de filtro en el área 0 por todos los módulos de conexión al Core. En resumen se utiliza siempre que sea posible para mantener las rutas en el VDC Agregación al mínimo.

4.8.2.1 Alta disponibilidad OSPF

Una plataforma con dos supervisores que ejecutan Cisco NX-OS puede experimentar una conmutación de estado en el supervisor. Antes de que ocurra la conmutación, OSPFv2 inicia un reinicio consistente(habilitado por default) al anunciar que OSPFv2 no estará disponible por algún tiempo. Durante una conmutación, la red continúa reenviando tráfico y mantiene el sistema en la topología de red.

Después de una conmutación, Cisco NX-OS aplica la configuración en ejecución y OSPFv2 informa a los vecinos que es de nuevo operativo. Los vecinos ayudan a restablecer las adyacencias.

OSPFv2 reinicia automáticamente, cuando el proceso comienza a experimenta problemas. Tras la reanudación, OSPFv2 se reiniciapara que la plataforma no sea sacada de la topología de red. Si esta se reinicia manualmente OSPF,realizara un reinicio consistente, que es similar a una conmutación de estado. La configuración en ejecución se aplica en ambos casos.

Un desvío de reinicio consistente, o sin detención de reenvío(NSF), permite que OSPFv2 permanezca en la ruta de transmisión de datos a través de un proceso de reinicio. Cuando OSPFv2 tiene que reiniciar, primero envía un enlace local (tipo 9), llamado LSA.

El LSA incluye un período de consistencia, que tiene un plazo determinado en la que los vecinos de las interfacesdirectamente conectadas se aferran a la LSA provocando el reinicio de OSPFv2. (Normalmente, OSPFv2 derriba la adyacencia y descarta todas las LSA.) Los vecinos participantes, llamados ayudantes NSF, mantienen todas las LSA´s que se originan en la interfaz OSPFv2 como si la interfaz siguiera siendo adyacente.

Cuando la interfaz OSPFv2 reinicia, este vuelve a su estado operativo, redescubre a sus vecinos, establece la adyacencia, y comienza a enviar sus actualizaciones de LSA de nuevo. En este punto, los ayudantes NSF reconocen que el reinicio ha terminado.

4.8.2.2 OSPF BFD

Esta función admite la detección de reenvío bidireccional (BFD). BFD es un protocolo de detección que proporciona el reenvío de la ruta de tiempos rápidos de detección de fallos. BFD proporciona detección de fallos debajo del segundo entre dos dispositivos adyacentes y puede ser menos CPU-intensivo del que los mensajes de protocolo de saludo, porque algunos de la carga BFD, puede ser distribuida sobre el plano de datos en módulos soportados.

La figura 4.11 mostrara la configuración OSPF BFD

```
Nexus7K (config)#feature bfd
Please disable the ICMP redirects on all interfaces running BFD sessions using the command below [no ip redirects]
Nexus7K (config)#int e1/1
Nexus7K (config-if)#no ip redirects
Nexus7K (config-if)#ip ospf bfd
```

Figura 4.11 Configuración OSPF BFD

4.8.2.3 OSPF área 0

Todos los enlaces ascendentes desde el módulo de agregación a la base se ejecutarán con el protocolo OSPFv2, y formarán parte de la red troncal OSPF, área 0.

➔ OSPF sólo se ejecutará entre los dispositivos de red de Cisco L3. Los firewalls no ejecutarán OSPF.

El VDC de Agregación sólo se ejecuta en el proceso de OSPF área 0 a través de los módulos del Core.

4.8.2.4 Proceso de ruteo OSPF

La habilitación de OSPF requerirá que una instancia de enrutamiento de OSPF se cree mediante la configuración de un proceso de OSPF. Es de gran ayuda y también buena práctica asignar un nombre fácil de recordar y número de proceso distinto para la red básica, por ejemplo 0.

Número de procesos es significativo a nivel local con el router en un dominio OSPF. El proceso de enrutamiento para los switches de agregación de la empresa es de 100.

La figura 4.12 muestra la configuración del proceso de ruteo OSPF en Nexus 7000

```
router ospf <process-id>
```

Figura 4.12 Configuración del proceso de ruteo OSPF en Nexus 7000

Nota:

En función OSPF NX-OS debe estar habilitado, para configurar OSPF "característica ospf".

4.8.2.5 OSPF router ID

Cada router que ejecuta OSPF en una red debe tener un ID único. El ID del router es utilizado por la base de datos de estado- enlace OSPF (LSDB) como un método de monitoreo para cada router en el dominio y enlaces asociados. Por default OSPF utiliza la dirección IP más alta de una de las interfaces activas del router como router-id. Si se configuran las interfaces loopback con una dirección IP, el software Cisco IOS usará las direcciones más altas de bucle como su ID de router, a pesar de otras interfaces que tengan direcciones IP superior.

Principalmente, las interfaces loopback no se ven afectados por la falta de circuitos. Mediante la configuración de bucle invertido de dirección IP de la interfaz como router-id, se logra una mayor estabilidad en la tabla de enrutamiento. Se recomienda disponer de direcciones de bucle configurados en todos los dispositivos con el fin de tener un router ID OSPF determinista.

La figura 4.13 muestra la configuración OSPF Router ID en Nexus 7009

```
router ospf <number>
router-id <router_id>
```

Figura 4.13 Configuración OSPF router ID en Nexus 7009

La tabla 4.8 muestra el router ID asignado para los dispositivos Nexus 7000

Tabla 4.8 OSPF router Ids usan en la Empresa

Nombre del Dispositivo	Router ID
VHAGR700901_AGGREGATION	172.28.F.xxx
VHAGR700902_AGGREGATION	172.28.F.xxx

4.8.2.6 Referencia de ancho de banda OSPF

Por default NX-OS calcula el costo del enlace mediante el uso de ancho de banda de referencia de 40 Gbps. Cisco NX-OS ejecuta automáticamente un ancho de banda de referencia por default de 40.000 Mbps. Este valor proporciona una mayor flexibilidad en el desarrollo de interfaces de 40 Gbps y 100 Gbps en la plataforma Nexus 7000.

Nota:

En una red de Data Centercon equipos NX-OS y dispositivos IOS, el ajuste de ancho de banda de referencia debe ajustarse de modo que todos los dispositivos dentro de una OSPF puedan utilizar un valor constante. La configuración de ancho de banda de referencia para OSPF en Cisco NX-OS es idéntica a Cisco IOS, y se realiza con el uso delcomando de referencia de ancho de banda auto-cost.

El valor por default para la métrica OSPF se basa en el ancho de banda normalizado. Por default OSPF calcular la métrica OSPF para una interfaz de acuerdo con el ancho de banda de la interfaz.

La métrica para OSPF se calcula de la división de la referencia de ancho de banda entre el ancho de banda de la interface, esta referencia de ancho de banda tiene un valor predeterminado a 10^8, y el valor del ancho de banda de la interface se puede obtener por el comando bandwidth.

El cálculo de FDDI (Fiber Distributed Data Interface) utiliza una métrica de 1 (es decir 100Mbps.

En el caso de redes con gran ancho de banda (es decir, un gigabit Ethernet), se debe utilizar un número mayor de costo en los enlaces frente a otros enlaces (siempre y cuando dichos enlaces estén disponibles, por ejemplo, 10 gigabit Ethernet o Fast Ethernet estos casos pueden considerarse suficientes).

Si el ancho de banda de referencia se deja en su valor por default, entonces el costo de un Fast Ethernet, Gigabit Ethernet y enlaces de 10 Gigabit Ethernet sería de un valor de 1, siempre y cuando no exista diferenciación de OSPF para las distintas velocidades de enlace.

Para superar esto, el ancho de banda de referencia debe ser cambiado en todos los dispositivos para el enlace más rápido que pudiera existir en la red. En la actualidad, las interfaces más rápidas disponibles para los dispositivos de la empresa son Ethernet 10 Gigabit, pero es importante estar preparados para el futuro de 40GB.

Sin embargo todo el enrutamiento OSPF dentro de la Empresa se tiene de un ancho de banda de referencia por default de 10 Mbps. Si la Empresa quiere cambiar el ancho de banda de referencia a 40 Gbps se necesitará hacer la configuración de todos los routers que ejecutan OSPF.

En la figura 4.14 se muestra la configuración de referencia para el ancho de banda

```
Router(config)#router ospf <Process ID>
Router(config-router)#auto-cost reference-bandwidth 40000 ------->sets the ref-bw to 40 gigabit
```

Figura 4.14 Configuración de referencia de ancho de banda

Nota:

El valor establecido por el comando ip ospf cost invalida el costo resultante del comando OSPF auto-cost.

Nota:

El ancho de banda de referencia debe establecerse en todos los routers para proporcionar la asignación de costos coherente en toda la red. También debe asegurarse de que el ancho de banda de la interfaz correcta se refleje en la interfaz física.

4.8.2.7 Tipo de red OSPF

Interfaces Ethernet se transmiten de forma predeterminada. En la empresa se recomienda el uso del tipo de red de punto a punto en todos los dispositivos con el fin de evitar que el proceso de elección del enrutador designado OSPF.

En la figura 4.15 se muestra la configuración OSPF del tipo de red punto a punto

```
interface Ethernet slot#/type#
ip ospf network point-to-point
```

Figura 4.15 Configuración OSPF para el tipo de red en Nexus 7009

4.8.2.8 Convergencia OSPF

En la empresa el proceso OSPF 100 va a cambiar su configuración por default dependiendo los valores que se muestran en la tabla 4.9 a continuación:

Tabla 4.9 OSPF temporizadores

Temporizadores	Valor Default Broadcast/Point-to-point	OSPF
Ip ospf dead-interval	4 x hello interval (40 sec/120 sec)	3 sec
Ip ospf hello-interval	10 sec/ 30 sec	1 sec
Ip ospf retransmit-interval	5 sec	5 sec
Ip ospf transmit-delay	1 sec	1 sec

Cada uno de estos temporizadores afectará el rendimiento de OSPF y se puede ajustar para efectuar tanto el tiempo de convergencia como la utilización de recursos de red. Si bien es posible utilizar los valores más pequeños para los intervalos muertos y de saludo, estos valores deben ser evaluados en relación con la estabilidad de la red y la utilización general de los recursos.

La figura 4.16 muestra la configuración de temporizadores de OSPF

```
interface Ethernet slot#/type#
ip ospf dead-interval 3
ip ospf hello-interval 1
ip ospf mtu-ignore
```

Figura 4.16 Configuración OSPF temporizadores de tiempo en interfaces Nexus 7000

4.8.2.9 Autenticación OSPF

Para cada mensaje OSPFv2, Cisco NX-OS crea un mensaje unidireccional MD5 one-way (un camino) basado en el mensaje en sí mismo y la contraseña cifrada. La interfaz envía este resumen con el mensaje OSPFv2. El vecino OSPFv2 lo valida utilizando la misma contraseña cifrada. Si el mensaje no ha cambiado, el cálculo del resumen es idéntico y el mensaje OSPFv2 se considera válido.

La autenticación MD5 incluye un número de secuencia con cada mensaje OSPFv2 para asegurar que ningún mensaje se repite en la red.

En la figura 4.17 se muestra la configuración para la autenticación MD5

```
router ospf <process-id>
area 0 authentication message-digest
interface Ethernet slot#/port#
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 OSPF_4A#XX
```

Figura 4.17 Configuración OSPF MD5 – Autenticación en Nexus 7000

Nota:

Cualquier cambio de autenticación debe estar configurado en todos los routers dentro del proceso de OSPF.

4.8.2.10 Límites de configuración OSPF

La tabla 4.10 resume los valores de escalabilidad OSPF v2 verificados para los switches Cisco Nexus 7000.

Tabla 4.10 OSPFv2 configuración de límites

Parámetro	Límite Verificado (Cisco NX-OS 6.1)
Number of active interfaces	300
Number of passive interfaces	500
Number of process instances per VDC	4
Number of neighbors/total routes with aggressive timers (1s/3s)	16/6000

4.8.2.11 Resumen de diseño OSPF

En base a la red de la empresa y con el enfoque jerárquico, tenemos que resumir las configuraciones en:

- ➔ El área OSPF 0 se ejecutará en la distribución de la empresa
- ➔ Todas las interfaces físicas en el área 0 deben tener vecinos OSPF.
- ➔ Todas las interfaces físicas en el área 0 debe ser punto a punto.
- ➔ Todos los routers OSPF deben asignar una dirección de loopback (loopback0), que se utilizará para la identificación del router

.

- ➔ Ajustar el auto-cost reference-bandwidth a 100 Mbps en todos los routers durante el uso de enlaces de alta velocidad.

- ➔ Asegurarse de que el ancho de banda en todas las interfaces físicas se refleja en función de su velocidad.

- ➔ Bienvenida y temporizadores muertos deben ser cambiados a 1 y 3 para mejorar los tiempos de convergencia.

4.8.2.12 Plantilla de configuración OSPF

La figura 4.18 muestra la plantilla de configuración de OSPF en un equipo Nexus 7000 de la capa de Agregación. La misma configuración se puede usar para el otro switch de Agregación - sólo el router-ID y las interfaces de red necesitan ser cambiadas.

```
Router(config)#interface Loopback0
Router(config-if)#ip address <address><subnet mask>
Router(config-if)#no ip directed-broadcast
Router(config)#interface Type <slot#/port#>
Router(config-if)#ip address <address><subnet mask>
Router(config-if)#no ip directed-broadcast
Router(config-if)#udld aggressive
Router(config-if)#ip ospf network point-to-point
Router(config-if)#ip ospf hello-interval 1
Router(config-if)#ip ospf dead-interval 3
Router(config-if)#ip ospf mtu-ignore
Router(config-if)#ip router ospf 100 area 0
Router(config)#router ospf <process-id>
Router(config-router)#router-id <address>
Router(config-router)#log-adjacency-changes
```

Figura 4.18 Plantilla de configuración OSPF

4.8.3 Protocolo de ruteo Hot standby (HSRP)

El Protocolo Hot Standby Router proporciona un mecanismo que está diseñado para soportar la conmutación por error no disruptiva de tráfico IP en ciertas circunstancias. En particular, el protocolo protege contra el fallo de la primera hop router cuando el host de origen no puede aprender la dirección IP de la primera hop router dinámicamente. HSRP proporciona una dirección "siempre" default gateway IP de máquinas host (granja de servidores). Ambos switches comparten esta dirección "siempre" IP y con vPC los dos switches con el tráfico hacia adelante para la dirección IP a la vez.

- ➔ Sub-segundo - temporizadores FHRP no se recomiendan para un sistema de doble apoyo Hello (1s) y para Hold (3s) se recomienda el temporizador. Temporizadores agresivos no son necesarios con vPC.

- ➔ Configurar HSRP extendida y mantener temporizadores para apoyar conmutaciones NSF en emi / Sup. No aplican temporizadores con menos de un segundo. Configurar en todos los routers HSRP con el mismo temporizador (default / mínima es 10 s).

- ➔ Configurar HSRP retraso Preemption.

- ➔ Desactivar proxy ARP IP para evitar problemas con la expedición de un mal funcionamiento del servidor (por default).
- ➔ Configurar "sin redirecciones IP" para desactivar supervisora de generar redirecciones ICMP.
- ➔ Para ECMP, utilizar por flujo de balanceo de carga (por default) para evitar los paquetes fuera de orden.

4.8.3.1 Prioridad HSRP

HSRP interfaces SVI activas se pueden configurar con una prioridad de 120 y las interfaces HSRP en espera SVI se pueden configurar con una prioridad de 90.

La figura 4.19 muestra la configuración de prioridad HSRP

```
Interface VLAN <VLANID>
Hsrp<group>
Priority 120
```

Figura 4.19 Configuración prioridad HSRP

4.8.3.2 HSRP Preempt (Adelantarse a HSRP)

El HSRP de suscripción preferente se utiliza en la red de la Empresa con el fin de mantener la topología determinista, lo que significa que en cualquier momento dado HSRP interfaz activa podría ser identificado basándose en el dispositivo activo. HSRP preempt asegura que el router con los más altos esfuerzos prioritarios HSRP asume el control como el router activo.

La prioridad se determina en primer lugar por el valor de prioridad configurado, y luego por la dirección IP. En cada caso un valor más alto es de mayor prioridad.

Tenga en cuenta también que, cuando un router se integra por primera vez no tiene una tabla de enrutamiento completa. Si está configurado para adelantarse y tiene una prioridad más alta que el actual router activo se convertirá en el router activo, sin embargo, es incapaz de proporcionar servicios de enrutamiento adecuados lo que significa que el tráfico estaría escondido. El retraso se debe configurar para que todo zigzag sólo tenga lugar una vez que el enrutamiento adyacencias y enlaces físicos sean estables ante el router primario y se haga cargo de nuevo.

La función de retardo mínimo preempt permite preferencia a que se retrase durante un período de tiempo configurable.

Preemption sólo se inicia cuando una prioridad del router no activo más alto recibe un paquete de un enrutador activo de menor prioridad. Si el router de mayor prioridad no recibe los paquetes de protocolo HSRP desde el router activo de menor prioridad, entonces se convertirá en activo.

En la figura 4.20 se muestra la configuración HSRP preemption

```
Interface VLAN <VLANID>
Hsrp <group>
Preempt delay minimum 180
```

Figura 4.20 Configuración HSRP prempt

El algoritmo de autenticación MD5 HSRP protege contra paquetes spoofing HSRP. Se recomienda habilitar la autenticación entre todos los switches Nexus.

Esta configuración se muestra en la figura 4.21.

```
Interface VLAN <VLAN ID>
Hsrp <group>
Authentication md5 key-string <string>
```

Figura 4.21 Autenticación HSRP

4.8.3.3 Configuración HSRP

Para el enrutador primario la configuración de HSRP se muestra en la figura 4.22 a continuación.

```
Nexus7K(config)#feature hsrp
Nexus7K (config)#feature interface-VLAN
!
VLAN <VLAN>
!
Hsrp timers extended-hold <time>
!
Interface VLAN <VLAN ID>
No shutdown
Description “description”
Ip address X.X.X.X
No ip redirects
Hsrp version 2
Hsrp <group>
Preempt delay minimun 120
Priority 110
Ip Y.Y.Y.Y
```

Figura 4.22 Configuración de router primario HSRP

Para el enrutador secundario la configuración para HSRP se muestra en la figura 4.23 a continuación:

```
Interface VLAN <VLAN ID>
No shutdown
Description “description”
No ip redirects
Ip address X.X.X.X
Hsrp version 2
Hsrp <group>
Preempt delay minimum 120
Priority 95
Ip Y.Y.Y.Y
```

Figura 4.23 Configuración de router secundario HSRP

4.9 Capa 2

Uno de los objetivos de diseño de la empresa para este proyecto es reducir al mínimo la dependencia de Spanning-tree Protocol (STP) en la red. A tal fin, la agregación VDC del Data Center se basará en la FabricPath y Virtual Puerto Canal + (vPC +) función dentro del Nexus 7000.

FabricPath es una innovación en Cisco NX-OS Software que trae la estabilidad y la escalabilidad de enrutamiento de capa 2. El dominio conmutado no tiene que ser segmentado más y el suministro de datos de movilidad carga de trabajo en todo el centro. Dado que el tráfico ya no se transmite a lo largo de un árbol de expansión, el ancho de banda biseccional de la red no está limitado en escalabilidad y ahora es posible.

La característica vPC permite hacer EtherChannel Multi-Chassis entre el acceso y la capa de agregación, y permite enlaces de los miembros de un EtherChannel para abarcar chasis de doble Nexus 7000. Los beneficios clave de vPC son la capacidad de utilizar cada enlace ascendente desde el acceso a la agregación (es decir, sin puertos bloqueados), así como la eliminación de la dependencia del STP.

La capa de agregación VDC es el punto de demarcación entre la capa 2 y capa 3 - todos los enlaces a la capa de acceso operan en la capa 2.

Los siguientes puntos se refieren a la capa 2 del diseño del Proyecto de la empresa:

- ➔ Rapid Per VLAN Spanning-tree Protocol (rPVST +) funcionará como un mecanismo de seguridad solamente. Debido a la presencia de FabricPath y vPC, sin bucles se construirán en la topología, sin embargo RSTP funcionará sólo como un mecanismo para evitar bucles en el caso de una mala configuración, cableado incorrecto, etc La excepción serán las conexiones del módulo Servicios, que dependen de conexiones Spanning-tree tradicionales.

- ➔ VTP no se activará en cualquier capa de la red y la configuración de la VLAN se llevará a cabo manualmente en cada switch.
- ➔ Detección de enlace unidireccional (UDLD) se configura en cada enlace para los switches de capa de acceso como mecanismo a prueba de fallos adicionales.
- ➔ El diseño de la red de capa 2 tiene uplinks redundantes de los switches de capa de acceso y se configura dentro del dominio FabricPath.

En la empresa, el switch de agregación primaria (VHAGR700901_AGGREGATION) está configurado como raíz principal STP para toda la producción de VLAN, el switch de agregación secundaria (VHAGR700902_AGGREGATION) como root secundaria para la producción de VLAN, por único mecanismo a prueba de fallos.

Los vínculos entre el VDC de agregación y el Core VDC son enlaces capa 3. Los puertos de borde en el que se conectan los servidores tienen puerto rápido y BPDU habilitados. La característica de puerto rápido utiliza un puerto para saltar los estados de escucha y aprendizaje, reduciendo de este modo el retardo para un puerto de conmutación de bloqueo para el reenvío.

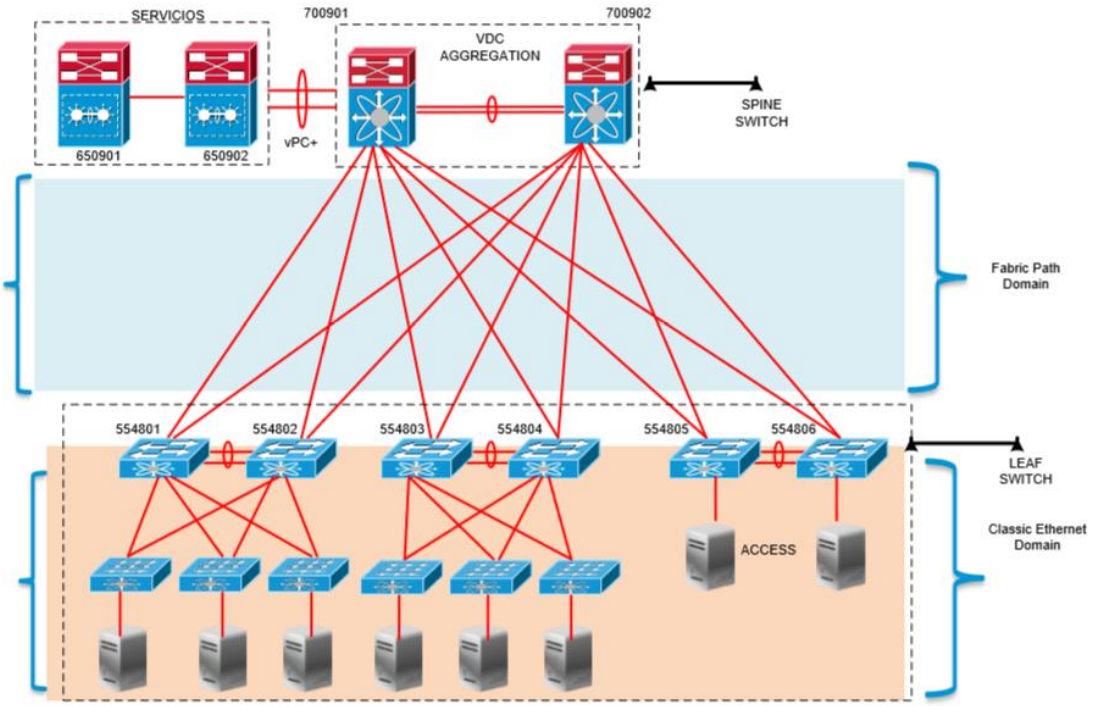


Figura 4.24 Diseño para el proyecto de la Empresa

4.9.1 Fabrics con FabricPath en Capa 2

La tendencia de virtualización comenzó en el borde del Data Center. La virtualización de servidores permite la consolidación de varios servidores como máquinas virtuales en un único host físico para aumentar su utilización. FabricPath proporciona la base para la construcción de un fabric escalable una red que sí se parece a un único switch virtual desde la perspectiva de sus usuarios. Esta propiedad se consigue proporcionando ancho de banda óptimo entre dos puertos, independientemente de sus ubicaciones físicas. Además, debido a FabricPath no sufre de las limitaciones de escala de puente transparente tradicional, una VLAN particular puede ser extendida a través de todo el fabric, lo que refuerza esta noción de un único conmutador virtual.

Nota:

Tenga en cuenta que si FabricPath es una tecnología de capa 2, el fabric sigue manteniendo las capacidades de Capa 3 de la familia de switches Cisco Nexus y proporciona integración de enrutamiento.

Las vías de circulación FabricPath dentro de Fabric trae la estabilidad y el rendimiento de enrutamiento de capa 2. FabricPath se hace cargo tan pronto como haya una transición de trama de Ethernet de una red Ethernet (denominado Clásica Ethernet) a un fabric FabricPath. Principios de extrapolación Ethernet no dictan la topología y los principios de reenvío en un fabric FabricPath. El marco se encapsula con un encabezado FabricPath, que consiste de fuente enrutable y direcciones de destino. Estas direcciones son simplemente la dirección del cambio

en que se recibe la trama y la dirección del cambio de destino a la que la trama se dirige. A partir de ahí, la trama se encamina hasta que se alcanza el switch de control remoto, donde se des-encapsula y es entregado en su formato original de Ethernet.

La siguiente figura 4.25 ilustra este proceso simple:

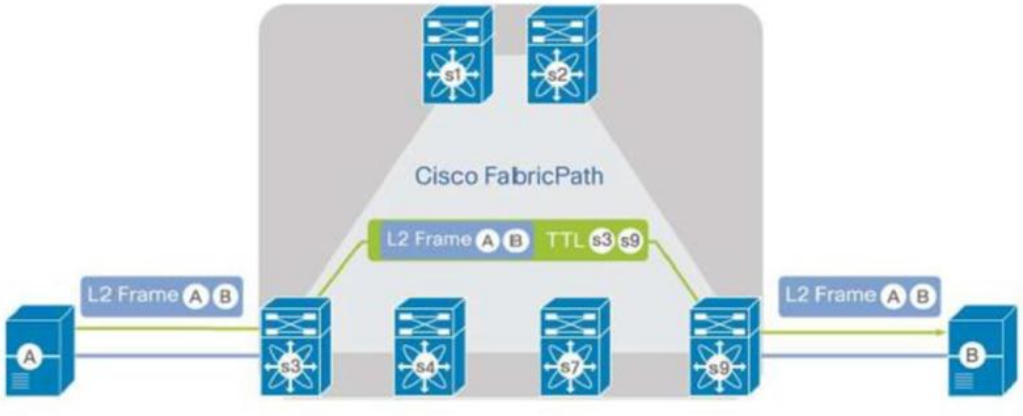


Figura 4.25 Frame transportando usando FabricPath

La diferencia fundamental entre FabricPath y Ethernet clásico es que con FabricPath, la trama es siempre enviada en el core con una dirección de destino conocido. Las direcciones de los bridges se asignan automáticamente, y una tabla de enrutamiento se calcula para todos los destinos unicast y multicast. La solución resultante todavía proporciona el comportamiento simple y flexible de la capa 2, mientras que, el uso de los mecanismos de enrutamiento IP se hacen fiables y escalables.
FabricPath introduce un cambio dramático en el plano de datos, y no se requiere hardware dedicado para implementar las funciones con baja latencia. Los módulos Cisco Nexus 7000 F-Series E / S y la Plataforma Nexus 5500 de Cisco son capaces de ejecutar FabricPath así IEEE Data Center Bridging (DCB) y Fibre Channel over Ethernet (FCoE). Debido a que los switches Cisco Nexus también integran de forma transparente con enrutamiento de nivel 3, el fabric resultante puede ejecutar todos los datos de diferentes tecnologías de centro de I / O al mismo tiempo y de manera eficiente.

4.9.2 Beneficios de un Ethernet Fabric

Con FabricPath, se puede crear una estructura Ethernet flexible que elimina muchas de las limitaciones del protocolo Spanning-tree. En el plano de control, FabricPath utiliza un protocolo de enrutamiento Shortest-Path First (SPF) para determinar la accesibilidad y selecciona la mejor ruta o rutas a cualquier destino que figura en el dominio FabricPath. Además, el plano de datos FabricPath introduce capacidades que ayudan a garantizar que la red se mantiene estable, y proporciona escalabilidad, el aprendizaje basado en hardware y capacidades de reenvío que no esté obligada por el software o la capacidad de la CPU.

- ➔ Soporte Legacy

Un dispositivo que no es compatible FabricPath se puede conectar de forma redundante con dos puentes FabricPath separadas con una mayor PortChannel virtual (vPC +) y es la tecnología, que proporciona una ruta de migración fácil. Al igual que vPC, vPC + se basa en la tecnología PortChannel proporcionar múltiples rutas y redundancia sin recurrir a Spanning-tree Protocol

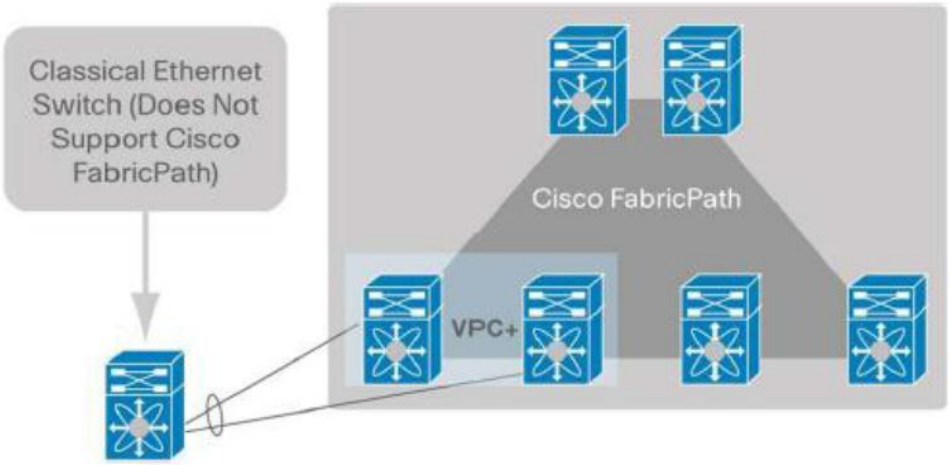


Figura 4.26 Conectando dispositivos que no soportan FabricPath con vPC+

➔ **Escalabilidad basada en tecnología**

FabricPath utiliza un protocolo de control construido en la cima del sistema (IS-IS) protocolo de enrutamiento, un estándar del sector que proporciona una convergencia rápida y que se ha demostrado para escalar hasta los más grandes entornos de proveedores de servicios.

Prevención y mitigación de Loop están disponibles en el plano de datos, ayudando a asegurar el reenvío seguro y que no puede ser igualada por ninguna tecnología de transición transparente. Los marcos FabricPath incluyen un campo similar a la utilizada en IP tiempo de vida (TTL), y un Reverse Path Forwarding (RPF) .

➔ **Eficiencia y alto rendimiento**

Porque en igual costo multitrayecto (ECMP) se puede utilizar el plano de datos, la red puede utilizar todos los enlaces disponibles entre dos dispositivos. La primera generación de hardware FabricPath de soporte puede realizar de 16 vías ECMP, que, cuando se combina con 16 canales de puerto-puerto 10-Gbps, representa un potencial de ancho de banda de 2,56 terabits por segundo (Tbps) entre los conmutadores.

Las tramas se reenvían a lo largo del camino más corto a su destino, incluyendola reducción de la latencia de los intercambios entre estaciones finales en comparación con una solución basada en árbol de expansión.

Direcciones MAC se obtienen selectivamente en el borde, lo que permite la ampliación de la red más allá de los límites de la tabla de direcciones MAC de los switches individuales.

En otras palabras, mientras que los beneficios FabricPath el servidor y los equipos de aplicación, proporcionan una estructura de red transparente que rompe silos de aplicaciones, permite la movilidad de la carga de trabajo, y proporciona un alto nivel de flexibilidad de implementación, también beneficia al equipo de operaciones de la red mediante la reducción de las dependencias InterTeam con la racionalización implementación y configuración, simplificando el mantenimiento y la solución de problemas de red.

4.9.3 Interfaces FabricPath

Cada interfaz en FabricPath de conmutación corresponde a una de dos categorías:

- ➔ FabricPath puerto de borde: Los puertos borde FabricPath son interfaces en el borde del dominio FabricPath. Estas interfaces Ethernet funcionan de forma Clásica y se comportan exactamente igual que los puertos Ethernet normales. Puede conectar cualquier dispositivo Ethernet clásico a la fabric FabricPath conectándolo a un puerto borde FabricPath. Switches FabricPath realizan dirección MAC de aprendizaje en los puertos de borde y las tramas transmitidas en los puertos de borde son marcos estándar IEEE 802.3 Ethernet. Se puede configurar un puerto de borde como un puerto de acceso o como un enlace troncal 802.1Q IEEE.

- ➔ Puerto base FabricPath: Son puertos principales FabricPath de tramas Ethernet siempre adelante y encapsulan en un encabezado FabricPath. Como regla general, sin aprendizaje de direcciones MAC se producen en los puertos centrales FabricPath; decisiones de envío basadas exclusivamente en operaciones de búsqueda en la tabla de switch. Tramas Ethernet en una interfaz de transmisión FabricPath siempre llevan una etiqueta IEEE 802.1Q, y por lo tanto los puertos pueden ser considerados un puerto de enlace troncal.

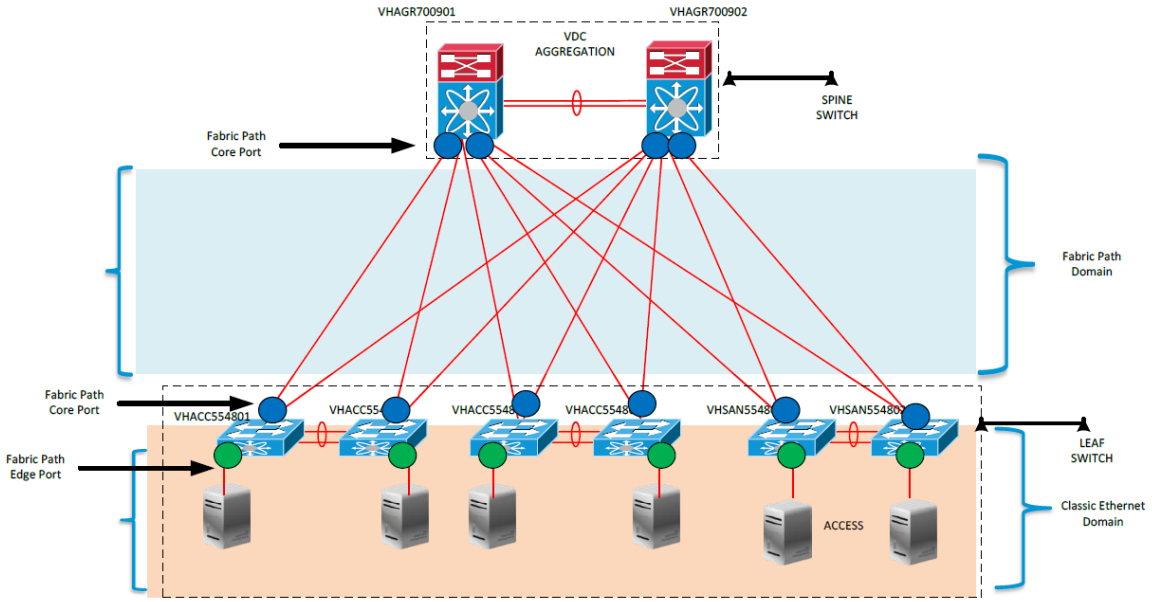


Figura 4.27 Puerto FabriPath edge y puertos Core

Tabla 4.11 FabricPath Core – Puertos de agregación

Switch	Fabricpath - Puertos Core
VHAGR700901_AGGREGATION	8/1-8, 9/1-8
VHAGR700901_AGGREGATION	8/1-8, 9/1-8

Tabla 4.12 FabricPath Edge – Puertos de agregación

Switch	Fabricpath - Puertos Core
VHAGR700901_AGGREGATION	3/8, 4/8
VHAGR700901_AGGREGATION	3/8, 4/8

Todos los puertos en los que se están llevando tráfico FabricPath se definen como tipo FabricPath. Con FabricPath, no se configura trunking y pruning de las VLAN en los puertos FabricPath. La configuración se muestra en la figura 4.28 para declarar un puerto como puerto FabricPath:

```
DC1-Agg1(config)#interface Ethernet 8/3
DC1-Agg1(config-if)#description FP Link to DC1-5500-1
DC1-Agg1(config-if)#switchport mode fabricpath
DC1-Agg1(config-if)#no shutdown
```

Figura 4.28 Puertos declarados como puertos Fabric

4.9.4 FabricPath VLANs

De forma predeterminada, al crear las VLAN en el Cisco Nexus 7000 Series, la VLAN Ethernet funciona en modo Clásica. Una de las primeras tareas que se realizan en la configuración FabricPath es definir una o más VLAN como VLANs que operan en modo FabricPath.

Tenga en cuenta que el modo (Clásico Ethernet o FabricPath) de una VLAN determinada es significativa sólo de los VDC´s locales. Otros VDC´s u otros switches en la red, no tienen conocimiento de la forma de una VLAN en otros switches. Si se define un rango de VLAN en un switch Ethernet Clásica y luego se conecta ese cambio a un puerto de borde FabricPath, los switches FabricPath tendrán el mismo ID de VLAN definido, pero con el modo VLAN configurado como FabricPath, como se muestra en la tabla 4.13:

Tabla 4.13 **FabricPath Edge – Puertos de agregación**

Vlans	Modo
1801-1900	fabricpath
2701-2800	fabricpath
2801-2900	fabricpath
1950-1999	fabricpath
2087-2094	fabricpath
2000-2086	fabricpath
2901-3000	fabricpath
2401-2500	fabricpath
2501-2600	fabricpath
2601-2700	fabricpath
Rest of vlans	Classical Ethernet

Nota:

Hay que tener en cuenta que a partir de la versión de Software 5.2 (1) Cisco NX-OS, sólo los puertos en un módulo de F1 I / O (N7K-F132XP-15) pueden pertenecer a VLANs FabricPath. Por lo tanto, ambos puertos borde FabricPath y puertos principales FabricPath deben ser interfaces de F1 en VLANs FabricPath; interfaces de módulos M1 familia de E / S no se pueden configurar como puertos de switch en una VLAN configuradas con el modo FabricPath.

El comando necesario para configurar una VLAN en el modo FabricPath es:

```
DC1-Agg1(config)#vlan 101
DC1-Agg1(config-if)#mode fabricpath
```

Figura 4.29 VLAN en modo FabricPath

Las VLANs FabricPath se envían en enlaces principales FabricPath utilizando MAC-in-MAC con cabecera de encapsulación y en los enlaces borde FabricPath sin el encabezado MAC-in-MAC. VLAN FabricPath se pueden agrupar en topologías para la ingeniería de tráfico. Por default, todas las VLAN FabricPath pertenecen a la topología de base 0.

VLAN y VLAN FabricPath CE no pueden compartir un enlace a menos que el enlace es un puerto de borde FabricPath.

4.9.5 Encapsulado de FabricPath

Los switches FabricPath encapsulan todas las tramas Ethernet que atraviesan al fabric dentro de una cabecera FabricPath de 16 bytes. La siguiente figura muestra los detalles de la cabecera FabricPath.

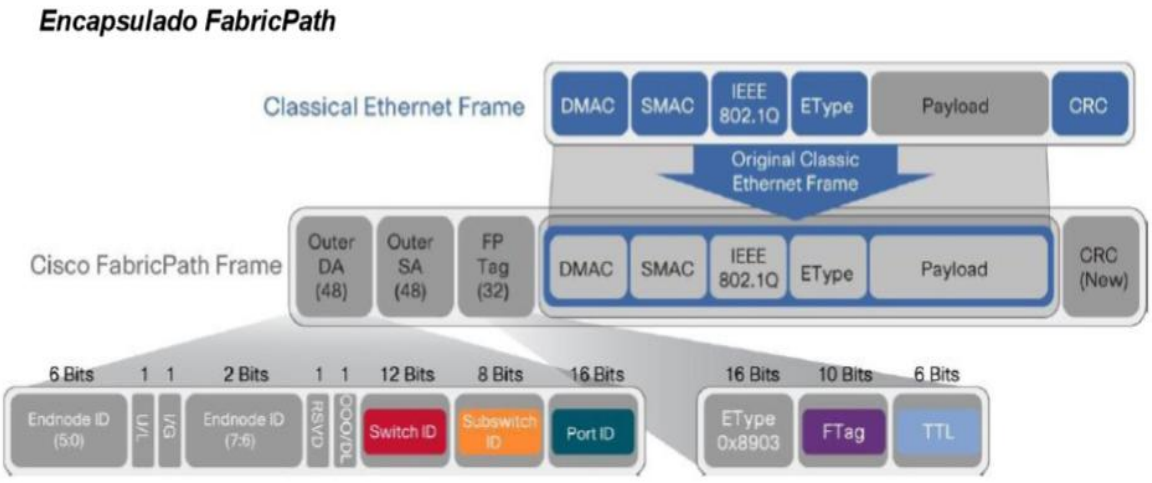


Figura 4.30 Encapsulado FabricPath

La encapsulación FabricPath utiliza un formato encapsulado de dirección en MAC. La trama Ethernet original, junto con una etiqueta IEEE 802.1Q, se antepone por una dirección de 48 bits externa de origen (SA), una dirección de destino exterior 48-bit (DA), y una etiqueta FabricPath 32-bit (FP). Mientras que la dirección de origen y dirección de destino exterior pueden aparecer como direcciones MAC de 48 bits, switches FabricPath que reciben dichos marcos en un puerto core FabricPath analizan estos campos de acuerdo con el formato que se muestra en la figura 4.29.

4.9.6 Switch ID

Cada switch en el dominio FabricPath es asignado a un ID de switch de 12 bits único (SID). En la dirección de origen exterior, este campo identifica el switch FabricPath que se originó (típicamente el switch de borde FabricPath entrada). En la dirección de destino exterior, este campo identifica el switch FabricPath destino.

En el caso de marcos de multidestino, este valor en la dirección de destino exterior se establece en un valor específico en función del tipo de marco multidestino:

- ➔ Para las tramas de multidifusión, este campo se rellena con los bits correspondientes de la barra de direcciones MAC destino de la trama original de Ethernet (encapsulado).
- ➔ Para las tramas unicast desconocidas, este campo se rellena con los bits correspondientes de una dirección multicast reservada (01:00 F: FF: C1: 01: C0).
- ➔ Para las tramas con una dirección MAC de destino interno conocido, con una fuente desconocida, este campo se rellena con los bits correspondientes de una dirección multicast reservada (01:00 F: FF: C2: 02: C0) para facilitar las actualizaciones de tabla de direcciones MAC en el borde de FabricPath en los switches.

En la tabla 4.14 se muestran los switches ID Fabric Path

Tabla 4.14 FabricPath switch-ID

Switch	FabricPath Switch-ID
VHAGR700901-AGGREGATION	121
VHAGR700902-AGGREGATION	122

Los valores de conmutador-id se asignan de forma predeterminada para cada dispositivo FabricPath a través del protocolo DRAP. Sin embargo, puede ser una buena práctica asignarlos manualmente con el fin de proporcionar un esquema de numeración más significativa.

4.9.7 VLAN Trunking

En las redes de árbol que se abarca, el usuario tiene que especificar qué VLAN pertenecen a qué puerto mediante el uso del comando **switchport trunk allowed vlan**. Con FabricPath, el usuario no tiene que especificar explícitamente qué VLAN se realiza en un vínculo FabricPath habilitado (VLANs, obviamente, deben ser definidos en los switches). La configuración de un puerto core FabricPath se lleva a cabo con el comando **switchport mode fabricpath**. El comando **switchport mode trunk** pone un puerto Ethernet en modo tradicional en lugar del modo FabricPath.

4.9.8 Métricas

La ruta preferida a cualquier switch-ID se calcula en base en la métrica a cualquier destino dado.

La métrica es como sigue:

- ➔ Enlaces de 1 Gbps Ethernet tienen un costo de 400
- ➔ Enlaces • 10-Gigabit Ethernet tienen un costo de 40
- ➔ 20-Gbps tienen un costo de 20

4.9.9 Balanceo de carga de múltiples rutas

El Unicast en capa 2 de rutas múltiples está activado por default, pero se puede configurar el mecanismo de balanceo de carga (por default se utiliza la capa 2, capa 3 o capa 4 con sus respectivas IP de origen y destino así como su respectiva VLAN) para el tráfico de la capa 2 con el siguiente comando:

La figura 4.25 muestra el comando para configurar el balanceo de carga de múltiples rutas.

```
DC-700901(config)#fabricpath load-balance unicast < destination, include-vlan, layer-3, layer4, mixed, source, source-destination>
```

Figura 4.31 Configuración de balanceo de carga Multipath

4.9.10 Árboles multidestino

En el tráfico FabricPath de multidifusión, los mensajes broadcast y el tráfico de inundación se transmiten a lo largo de un árbol multidestino. FabricPath permite múltiples árboles multidestino con el fin de lograr el balanceo de carga de tráfico para las tramas multidestino. Esto se logra mediante el uso de una etiqueta especial presente en el marcoFabricPath, que se denomina reenvío Tag o FTag.

El FTag, junto con el tipo de dirección de destino de la trama (unicast desconocido, broadcast o multicast), selecciona un gráfico de reenvío, que es el conjunto de posibles switches y las interfaces a través de las cuales se envía la trama. En cada switch, el FTag en el encabezado de la trama se utiliza para reenviar el marco a lo largo de las interfaces que se encuentran en el gráfico de reenvío.

FabricPath utiliza un protocolo de estado-enlace para determinar los árboles de reenvío en la red. La tecnología FabricPath permite la definición de múltiples topologías.

La figura 4.26 muestra la topología soportada para dos árboles multidestino, FTags: FTag1 y FTag2. Cada uno de estos árboles multidestino tiene sus raíces en una de las espinas.

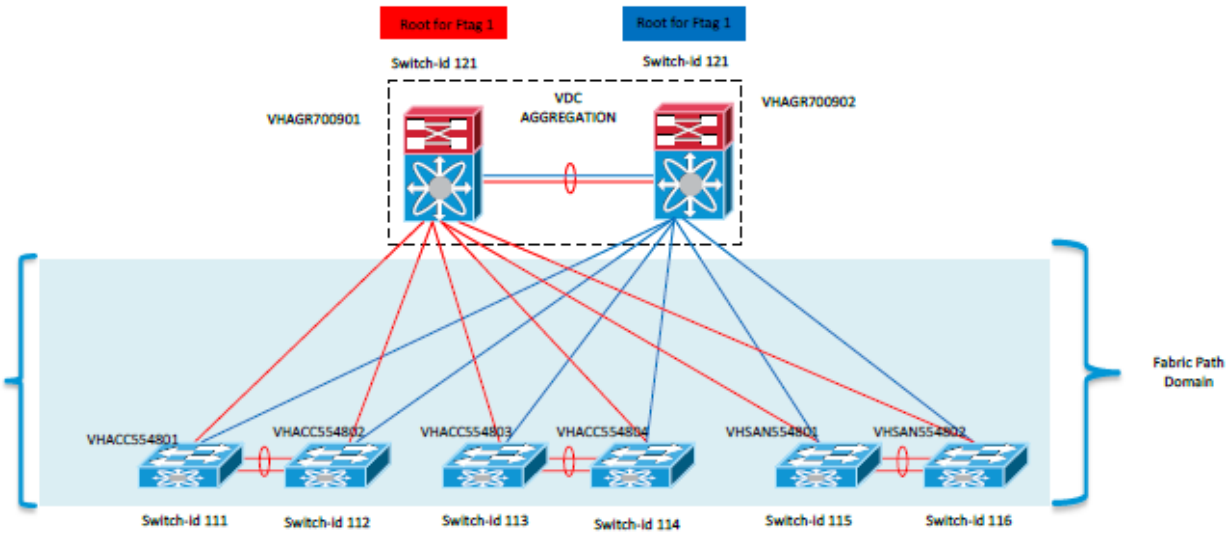


Figura 4.32 Árboles FTag – Asignación en FabricPath

FTag 1 se utiliza para el primer árbol multidestino y FTag2 se utiliza para el segundo árbol multidestino. Los árboles FTag se utilizan de la siguiente manera:

- ➔ FTag1 se utiliza para unicast, broadcast y multicast desconocidos. El switch de la más alta prioridad en la topología FabricPath es elegido como la raíz de FTag1. Es posible modificar el valor de prioridad raíz FabricPath predeterminada con el fin de colocar la raíz para FTag1o FTag2 en un dispositivo determinado. Si se mantiene la prioridad por default en todos los switches como parte del dominio FabricPath, el valor del ID del sistema del switch se utiliza para determinar la raíz con la prioridad más alta.
- ➔ FTag2 se utiliza sólo para el tráfico de multicast. El segundo switch de más alta prioridad en la topología FabricPath es elegido como la raíz de FTag2.

En el dominio FabricPath, un switch se convierte en la raíz del primer árbol muticast(árbol 1). Los switches FabricPath comparan tres parámetros para seleccionar la raíz del árbol 1, los valores más altos son mejores en todos los casos. Los parámetros, en orden de preferencia, son:

- ➔ Prioridad Root: Un valor de 8 bits entre 0 y 255, con un valor predeterminado de 64.
- ➔ ID del sistema: Un valor de 48 bits formado por la dirección MAC VDC (tomado del plano medio del rango de direcciones MAC chasis).
- ➔ Switch ID: El único SID es de12 bits.

Después de que un switch se convierte en la raíz para el árbol 1, se selecciona una raíz de cada árbol adicional de tipo multicast (sobre la base de los parámetros anteriores) y asigna a cada árbol multicast un valor FTag único.

Aunque FabricPath IS-IS automáticamenteseleccionará los switches por cada árbol multicast, puede influir en la selección de raíz mediante el comando root con prioridad en el modo de configuración de dominio FabricPath. El enfoque recomendado es configurar más switches centralmente conectados como las raíces. (Por ejemplo, utilizar la agregación o lo switches tipo columna vertebral como las raíces en lugar de ser accesos o switches de hoja).

La Tabla 4.15 muestra la prioridad de la raíz Fabricpath.

Tabla 4.15 Prioridad de la raíz FabricPath

Switch	Prioridad de la raíz Fabricpath
VHAGR700901-AGGREGATION	1
VHAGR700902-AGGREGATION	2

4.9.11 Topología 0

La topología 0, es la topología por default y no puede ser eliminada, se encuentra configurada por default:

La figura 4.26 muestra la topología del Fabricpath.

```
DC1-Agg1 (config)#fabricpath topology ?
<1-63> Fabricpath Topology ID 1-63
DC1-Agg1#show fabricpath isis topology?
<0-63> Specific topology information
Summary Display summaty topology information
```

Figura 4.33 Topología FabricPath

La única configuración que es posible modificar con el fin de optimizar la distribución del tráfico, es la opción de la raíz de los árboles multidestino.

4.9.12 Subswitch ID

El campo del ID del subswitch (sSID) identifica la fuente o el destino vPC+ de la interfaz del PortChannel asociado con un par de conmutadores vPC+ en particular. FabricPath ejecuta vPC+ que utiliza este campo para identificar el vPC+ del PortChannel específico en el que el tráfico va a ser reenviado. El valor sSID es significativo a nivel local para cada par de conmutadores vPC+. En ausencia de vPC +, este campo se establece en 0.

La Tabla 4.16 muestra el cómo se identifican los switch´s con sus respectivos Subswitch's

Tabla 4.16 FabricPath del subswitch ID

Switch	SubSwitch-ID
VHAGR700901-AGGREGATION	1000
VHAGR700902-AGGREGATION	1000

4.9.13 El protocolo IS-IS de FabricPath

El protocolo FabricPath IS-IS sustituye al Protocolo Spanning-tree (SPT) como el protocolo del plano de control en el dominio FabricPath. En otras palabras, el protocolo FabricPath IS-IS determina la topología de reenvío en lugar de que lo haga SPT.

IS-IS es un protocolo estándar de enrutamiento de estado de enlace de la industria. La implementación del FabricPath IS-IS se basa en la especificación ISO / IEC 10589, implementado como un solo nivel de dominio IS-IS y se extiende a través de la definición de *Tipo-Longitud-Valor* (TLV) de los campos específicos para el FabricPath.

Varias características del protocolo IS-IS hacen que sea ideal para su uso como un protocolo de reenvío de capa 2:

- **No tiene dependencia IP**: IS-IS no requiere accesibilidad IP para formar adyacencia entre dispositivos. Aunque la mayoría de las redes modernas ofrecen conectividad IP para la infraestructura de la red, el uso de IS-IS asegura que no existe ningún requisito estricto para la conectividad IP en banda entre los switches.

- **Se puede extender fácilmente:**Usando TLVs personalizados, Los dispositivosIS-IS pueden intercambiar información sobre casi cualquier cosa. En el caso de la capa 3, los routers intercambian accesibilidad del prefijo IP. En el caso de FabricPath, los switches intercambianaccesibilidad SID.

- **Proporciona enrutamiento SPF:**Los protocolos de enrutamientoSPF han demostrado ser escalables, flexibles y de rápida convergencia. Además, IS-IS soporta el reenvío de ECMP, permitiendo que los paquetes de datos puedan seguir cualquier camino paralelo disponible en lugar de restringir el reenvío a un solo camino.

Aunque IS-IS es la base de FabricPath, permitiendo que el FabricPath de la red no requiera ningún conocimiento específico de IS-IS: la configuración es plug-and-play. Por mucho que un operador de red, utilice el Protocolo Spanning-tree e interconecte switches, se puede habilitar FabricPath en las interfaces para comenzar el reenvío a través de FabricPath con poca configuración.

4.10 Fabric Path: Interacción con Spanning-tree

FabricPath no sólo soporta conexionestradicionales directasde Ethernet, sino también de conexión tradicionales spanning-tree de los switches a los puertos FabricPath. Por default, los conmutadores FabricPath transmiten y procesan el protocolo Bridge Protocol Data Units (BPDs) en los puertos de borde FabricPath (se puede modificar este comportamiento mediante características tales como BPDU guardia y BPDU filtro), y por lo tanto participar en la construcción del árbol de topología de reenvío del Protocolo Spanning en cada dominio Spanning-tree Protocol conectado.

Sin embargo, las BPDU, incluyendo las notificaciones de cambio de topología (TCN), no se transmiten en los puertos principales del FabricPath y los BPDU no son enviados o tunelizados a través del dominio FabricPath por default. Por lo tanto, FabricPath aísla cada dominio del protocolo Spanning-tree, y los cambios en el dominio de la topología STP no se propagan a otros ámbitos relacionados con el mismo FabricPath.

Este aislamiento se logra haciendo que todo el dominio FabricPath aparezca como un solo puente STP a todos los dominios de STP conectados. Para aparecer como un puente STP, todos los puentes FabricPath comparten un ID de puente común (BID): C84C.75FA.6XXX. Este ID de puente se define estáticamente y no puede ser configurado por el usuario.

La figura 4.27 muestra el dominio FabricPath como un solo Puente Lógico, para cada dominio STP.

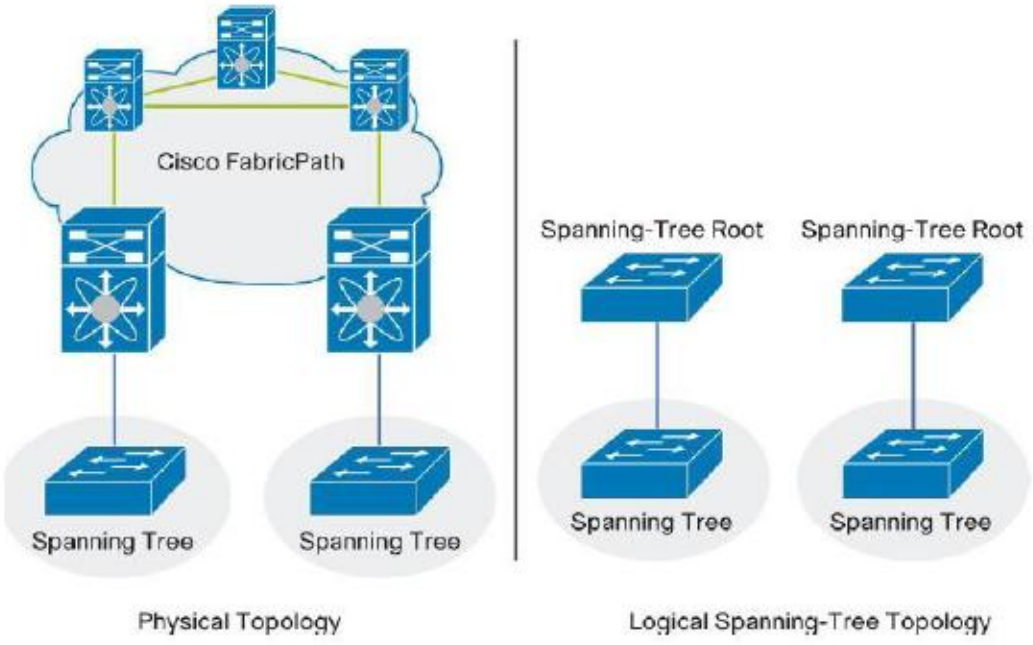


Figura 4.34 Dominio FabricPath como un puente lógico a cada dominio STP

Cada Switch de acceso FabricPath debe configurarse como la raíz de todas las VLAN FabricPath. Si se conectan dispositivos STP a FabricPath, se debenconfigurar todos los switches de borde como la raíz de STP con el comando **spanning-tree vlan x raíz primaria** (o configurar manualmente la prioridad del puente en cada switch para forzar alswith a ser la raíz). Además, si hay varios switches FabricPath se conectan al mismo dominio STP, en este punto se debe asegurar que los switches de acceso utilizan el mismo valor de prioridad del puente.

Para asegurarse que el FabricPath actúa como la raíz de STP, todos los puertos de borde FabricPath tienen la función de raíz STP habilitada implícitamente. Si una BPDU superior es recibida en un puerto de borde FabricPath, el puerto es colocado en la “puerta de enlace de capa 2” y el estado se elimina hasta que la condición es cumplida.

4.11 Diseño para la capa central o agregación

La topología FabricPath de la empresa consiste en un par de dispositivos conectados a múltiples dispositivos de borde. La plataforma del Cisco Nexus 7009 es utilizada como dispositivo de la columna vertebral, mientras que los Cisco Nexus 5548 detectores están conectados en el borde.

La columna vertebral en este diseño también se utiliza para realizar la función de enrutamiento entre la cloud FabricPath y el resto de la red. La puerta de enlace predeterminada para los servidores se encuentra en la capa de la columna vertebral, que siendo también el router en la topología, realiza la función de ventaja en el FabricPath.

La topología que se muestra en la figura 4.35, es la capa de la columna vertebral, que también es la capa de agregación, ya que los agregados de los switches de borde, operan simultáneamente en dos modalidades:

- ➔ Se envía el tráfico de nivel 2 entre los dispositivos de última generación basados exclusivamente en el destino del conmutador-id, y sin la necesidad de aprender las direcciones MAC (tráfico este-oeste).
- ➔ Aprender las direcciones MAC exclusivamente con el fin de encapsular tráfico encaminado en tramas FabricPath

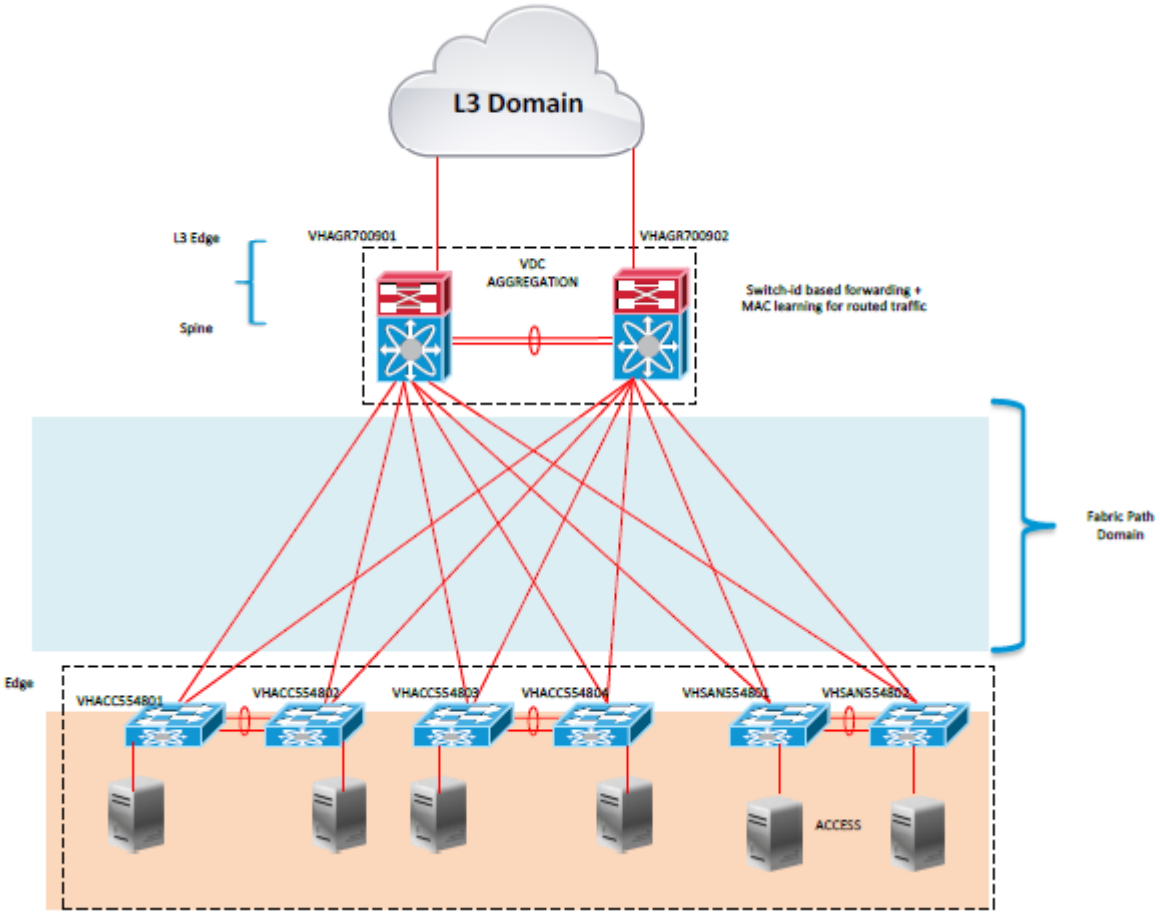


Figura 4.35 Capa de agregación

En comparación con un diseño del árbol de expansión o un diseño vPC, este diseño incluye las siguientes ventajas:

- ➔ Facilidad de configuración
- ➔ Desvío de múltiples rutas unicast y multicast de las capas “Capa 2 y Capa 3” del tráfico.
- ➔ Tiempos de convergencia más rápida

4.11.1Construcción de una espina enrutada

En el diseño de la empresa, la Espina también realiza funciones de enrutamiento, y como resultado se debe configurar por default la puerta de enlace. Cuando la Espina se construye con la familia de productos de la serie Nexus 7009 de Cisco, es necesaria la integración de las tarjetas F1 y M1. Esta integración proporciona los beneficios combinados de un switch FabricPath para el tráfico de la Capa 2, eldes-encapsulamiento y la encapsulación de tráfico de Capa 3 en la cloud FabricPath, sin necesidad de ningún cableado externo o equipo adicional.

4.11.2 Conexión del FabricPath de borde o la capa de hoja a la capade la espina

Al conectar la capa de borde FabricPath a la capa de espina, se puede usar cualquier puerto de la capa de espina para conectar la tarjeta F1, a menos que la escalabilidad de direcciones MAC en la topología sea un factor clave en el diseño. En este caso, se debe maximizar el uso de la SoC en la tarjeta de F1.

Para lograr esto, se tienen que distribuir los switches de borde de manera que utilicen diferentes SoCs. Un ejemplo sería, conectar el switch de borde-1 a los puertos 1 y 2 de la tarjeta de F1, elswitch se borde 2 a los puertos 3 y 4, y así sucesivamente.

En la figura 4.36 se muestra la forma de conectar la espina de borde a la tarjeta F1.

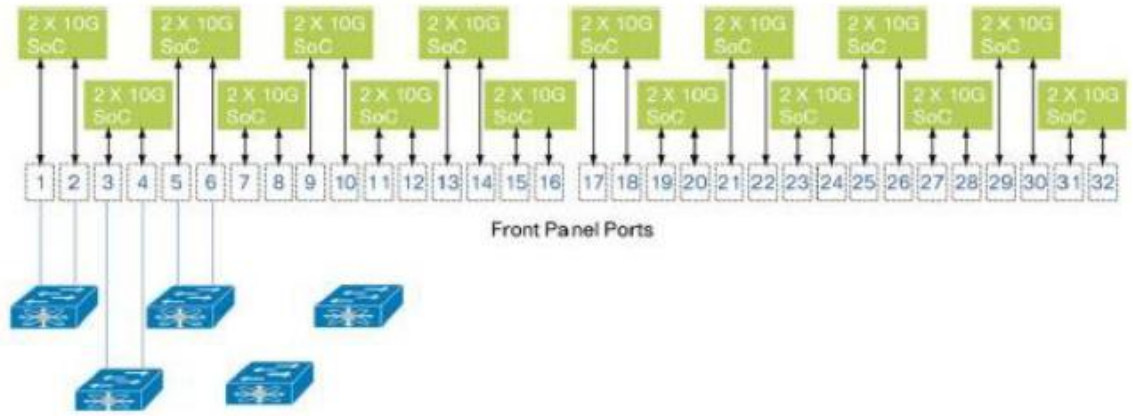


Figura 4.36 Conexión entre la espina con la tarjeta F1

4.11.3 Evitar saturación por la sincronización del protocolo ARP y la tabla de Capa 2

El tiempo de caducidad por default en la tabla de reenvío de Capa 2 en la serie Nexus 7000 de Cisco es de 1800 segundos. El Protocolo de Resolución de Direcciones (ARP) predeterminado, tiene un tiempo de espera de 1500 segundos. Con el fin de evitar la saturación de tráfico enrutado, es una buena práctica asegurarse de que en la espina, el tiempo de espera ARP es más agresivo que la Capa 2 de la tabla de reenvío, que es normalmente el valor predeterminado.

No es necesario sincronizar la tabla de direcciones MAC en el dispositivo de borde ya que en esta arquitectura, el borde no realiza el aprendizaje basado en el protocolo ARP. El dispositivo

de borde en una topología FabricPath que aprende las direcciones MAC sólo para las conversaciones activas.

En la espina, la presencia de la tarjeta de M1 en el mismo VDC requiere la tarjeta de F1 para obtener direcciones MAC con el único propósito de volver a escribir el tráfico encaminado con la información FabricPath. En este caso específico, los SoCs aprenden direcciones MAC basados en ARP, pero no usan la información MAC para el reenvío de tráfico de la Capa 2.

4.11.4 Consideraciones de ruteo Multicast

Ruteo Multicast y el switcheo FabricPath no requieren una configuración especialo ajuste de los dispositivos de la capa de agregación. Sólo PIM puede requerir ajuste si se desea reducir el tiempo de conmutación por error, como se haría en diseños enrutados.

4.11.5 Reenvío Multicast en FabricPath

Como se mencionó anteriormente, FabricPath construye dos árboles multidestino con dos raíces diferentes: una para Ftag1 y otro para Ftag2. En la Capa 2, al tráfico Multicast se le aplica un algoritmo hash a cualquier árbol. El hash de cualquier árbol multidestino es dependiente de la plataforma, por ejemplo, se puede incluir el campo VLAN o los campos de dirección IP.

Con el fin de maximizar la eficiencia de la distribución del tráfico, es recomendable ajustar manualmente la prioridad de la raíz para la Ftag1 y Ftag2 en espina:

En la figura 4.37 se muestra el código para el reenvío Multicast.

```
Agg1:
fabricpath domain default
root-priority 66
Agg2:
fabricpath domain default
root-priority 65

Traffic load-balancing can be configured with the following command:

DC1-Agg1(config)# fabricpath load-balance multicast ?
destination Include destination parameters
[…[
source-destination Include source and destination parameters
symmetric Symmetric (default)
xor Include ex-or of source and destination parameters
```

Figura 4.37 Reenvío Multicast

IGMP se utiliza para construir la capa 2 multicast de la tablaMAC de reenvío en los switch de borde. La información se utiliza para eliminar el tráfico en función de cada VLAN en los dos árboles multidestino.

4.11.6 Configuración de enrutamiento Multicast

El enrutamiento multicast, sigue las mismas reglas que un diseño no FabricPath:

- ➔ Habilitar PIM bajo la interfaz de SVI.

- ➔ IGMP se habilita automáticamente en el SVI cuando PIM está habilitado.
- ➔ Definir los puntos de encuentro (RP) en la red y / o configurar el dispositivo de la columna vertebral para auto-RP. NX-OS proporciona una funcionalidad específica, basado en el RFC 4610, llamada Anycast-RP con el Protocolo de Independencia Multicast (PIM). Esta funcionalidad hace que sea posible proporcionar redundancia RP de una manera más simple que cuando se despliega el Protocolo Fuente de Descubrimiento Multicast (MSDP).

En la figura 4.38 se muestra el código para configurar el protocolo PIM.

```
ip pim anycast-rp 1.1.1.100 1.1.1.1
ip pim anycast-rp 1.1.1.100 1.1.1.2
ip pim rp-address 1.1.1.100 group-list 224.0.0.0/4
interface loopback100
description anycast-RP
ip address 1.1.1.100/32
ip router ospf 10 area 0.0.0.0
ip pim sparse-mode
```

Figura 4.38 Configuración del protocolo PIM

Nota:

La selección Ftag para el tráfico de ruteo multicast puede cambiar después del enrutamiento. El tráfico de pos-ruteo puede ser enviado a un árbol Ftag diferente que el tráfico pre-ruteado.

Los tiempos para el protocolo PIM están configurados por default, y son la causa de los tiempos de convergencia más lenta que se miden para el tráfico multicast. Se pueden modificar y disminuir estos tiempos significativamente por cualquiera de los temporizadores PIM o mediante el uso de la Detección de Reenvío Bidireccional (BFD) de PIM.

En la figura 4.39 se muestra el código para configurar el protocolo PIM usando BFD.

```
bfd interval 50 min_rx 100 multiplier 3
interface Vlan101
[...]
ip pim sparse-mode
ip pim bfd-instance
ip pim dr-priority 10
ip pim hello-interval 1000
```

Figura 4.39 Configuración del protocolo PIM usando BFD

Nota:

El intervalo de sincronización del protocolo PIM debe ser configuradotomando precauciones porque cuando se despliega en demasiadas interfaces, puede aumentar la utilización del CPU. Es recomendable utilizar las escalas de BFD.

4.12 Resumen de recomendaciones

En esta sección se resume la recomendación para la construcción de una capa de 3 columna vertebral en una topología FabricPath. La siguiente figura ilustra estas recomendaciones:

- ➔ Configurar las VLAN en el modo FabricPath.
- ➔ Considere el uso de configuración manual switch-ids. Esto puede ayudar con la gestión y funcionamiento de la topología ya que se puede utilizar el esquema de numeración.
- ➔ Configurar SVI y HSRP como de costumbre.
- ➔ Configurar vPC + definiendo un vPC pares de enlace y un conmutador-id emulado en el dominio vPC. Esto es para permitir la integración del legado de dispositivos de la capa de borde (no FabricPath habilitados) y para proporcionar la funcionalidad de los datos del plano DefaultGateway.
- ➔ Configurar Capa 3 entre los routers mirando más de una VLAN FabricPath (por ejemplo, en el mismo enlace que se utiliza para interconectar los dispositivos de la columna vertebral, tales como el peer-enlace vPC +). Esto es necesario para reencaminar tráfico destinado a la capa en dirección norte dominio 3 si uno de los dispositivos de agregación pierde la conectividad física de los dispositivos aguas arriba.
- ➔ Utilice los vínculos FabricPath habilitados con fines peer-enlace VPC.
- ➔ Configurar dual-active exclude vlan para la lista de SVI (a menos que el uso de los dispositivos conectados VPC).
- ➔ Distribuir conmutadores de estado a diferentes SoC de la tarjeta de F1 para una 131ritic escalabilidad dirección MAC.
- ➔ Aunque esta es la configuración por default, en la columna, es probable que desee comprobar que el envejecimiento timeout ARP es más rápido que el tiempo de espera de reenvío de nivel capa 2.

En la figura 4.40 se muestra el resumen de recomendaciones para el diseño FabricPath

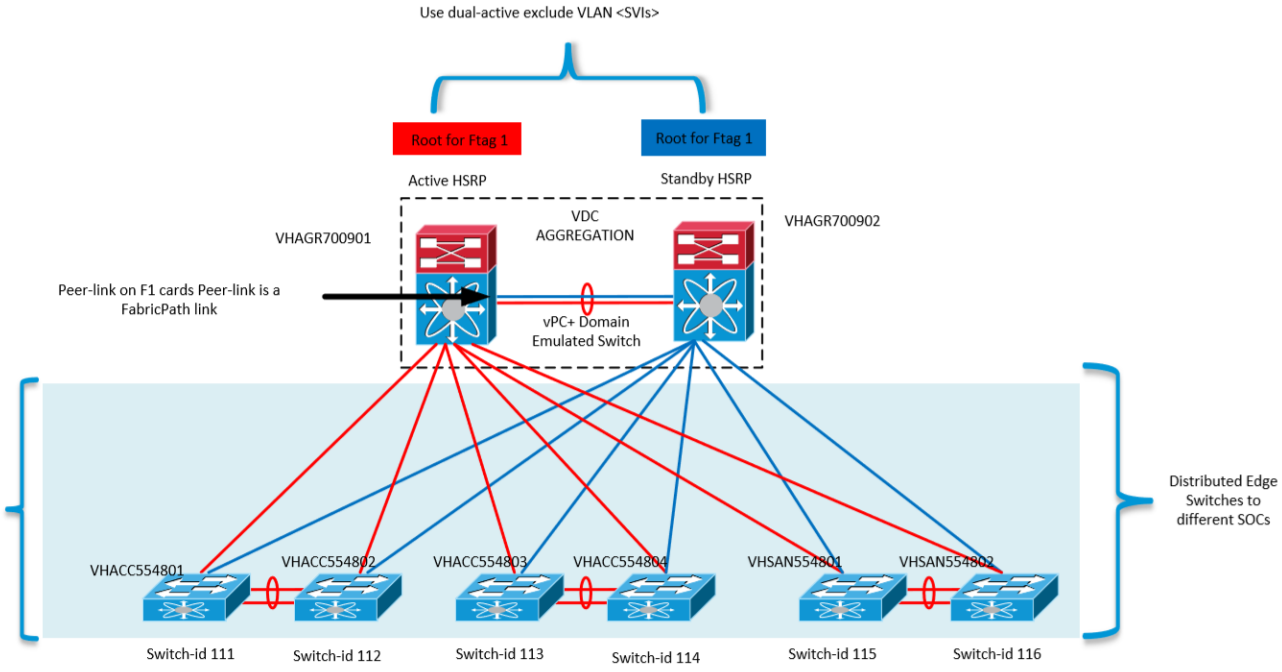


Figura 4.40 Resumen de recomendaciones para el diseño FabricPath

4.12.1 Escalabilidad y consideraciones de FabricPath

En la escalabilidad de FabricPath, hay tres elementos que deben considerarse para un dominio FabricPath:

- ➔ Número de switches
- ➔ Número de VLANs
- ➔ Número de direcciones MAC

El número máximo de switches y VLAN compatibles (es decir, probado por GC) en el mismodominio FabricPath aumenta continuamente en cada nueva versión del software NX-OS deCisco. En el momento de escribir este documento, estos son los valores soportados esperados:

- ➔ Cisco Nexus 7000 Series (NX-OS versión 6.0): 128 switch-ids y entre 2000 y 4000VLANs
- ➔ Cisco Nexus 5500 Switches (NX-OS versión 5.1 (3) N1 (1)): 128 switch-ids y entre 2000y 4000 VLAN´s.

Uno de los beneficios de la FabricPath es la escalabilidad tanto en términos de direcciones MAC y en términos de relaciones de rendimiento / sobresuscripción.

En cuanto a la dirección MAC escalabilidad, debemos diferenciar entre el borde y los dispositivos de la columna vertebral. Los conmutadores de extremo aprenden solamente direcciones MAC para los que hay conversaciones activas establecidas (aprendizaje conversacional). El objetivo de este documento es sobre el uso de los Switches Cisco Nexus 5500 en el borde de la red FabricPath. El valor máximo actual de direcciones MAC soportado sobre estos dispositivos es 24k.

La tabla 4.17 muestra los límites de configuraciones para FabricPath

Tabla 4.17 Límites de configuración para FabricPath

Feature	Límite Verificado(Cisco NX-OS 6.1)
Number of VLANs per switch	200 (Cisco NX-OS 6.1.1) 400 (Cisco NX-OS 6.1.2
Number of core ports per switch	256
Number of edge ports per switch	256
Number of trees per switch	2
Number of topologies per switch	1
Number of multicast groups per switch	10, 000
Number of Layer 2 IS-IS adjacencies per switch	256
Number of switch IDs	200 (Cisco NX-OS 6.1.1) 400 (Cisco NX-OS 6.1.2

4.12.2 Convergencia FabricPath Times

FabricPath mejora significativamente en los tiempos de convergencia de cualquier fallo determinado. Para la mayoría de las fallas unicast, la pérdida de tráfico se encuentra a unos pocos cientos de milisegundos. Para el tráfico enrutado, el peor tiempo de convergencia es el tiempo que le toma a los routers para hacer un cálculo de SPF. Teniendo en cuenta los diversos mecanismos de limitación, esto equivale a 5 segundos, lo que se puede bajar aún más mediante el cambio de los temporizadores OSPF por default en los dispositivos de encaminamiento adyacentes.

La configuración necesaria para lograr esto es muy simple:

```
Router ospf 10
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
```

Figura 4.41 FabricPath – Tiempos de convergencia

Para la capa 2, el tiempo de convergencia de multidifusión también se encuentran a unos pocos cientos de milisegundos, mientras que para enrutado multicast, PIM debe sintonizarse a través de BFD y / o temporizadores más agresivos que los valores por default. Enrutado multicast con ajuste adecuado puede converger en un par de segundos.

Tenga en cuenta que estos tiempos de convergencia más lenta no se deben a FabricPath sino temporizadores predeterminados de protocolos de enrutamiento. FabricPath tiene tiempos de convergencia de fracaso de unos pocos cientos de milisegundos. Para obtener mejores tiempos de conmutación por error, tenga en cuenta lo siguiente:

- ➔ Utilice vPC + en la columna para que HSRP a ser objeto de publicidad con el emulado conmutador-id.
- ➔ Considere la posibilidad de ajuste de los temporizadores OSPF por default SPF para evitar nuevos cálculos SPF estrangulación demasiado.
- ➔ Considere la posibilidad de ajuste de los temporizadores PIM predeterminada y, o utilizando BFD.

Para mejorar la convergencia de FP, que se puede recomendar para reducir el tiempo máximo de intervalo de SPF. El intervalo de tiempo predeterminado SPF es esperar 50 ms para el primer disparo, 50 ms para cada disparo adicional y 8000ms como la cantidad máxima.

La figura 4.42 muestra la convergencia SPF para FabricPath

```
s2(config-fabricpath-isis)#spf-interval ?
<50-120000> Maximun wait betweem trigger and SPF computatio (mili-secs)
*default value is 8000

fabricpath domain default
        spf-interval 50 50 50
        lsp-en-interval 50 50 50
```

Figura 4.42 SPF FabricPath – Intervalos de convergencia

4.12.3 Configuraciones ejemplo

En esta sección se explica cómo configurar los switches de la serie Nexus 7000 de Cisco y Switches Cisco Nexus 5500 para un diseño de vanguardia con base que también proporciona la funcionalidad de puerta de enlace de capa 3. Las muestras de configuración se refieren a la topología de la red se muestra la siguiente figura 4.43.

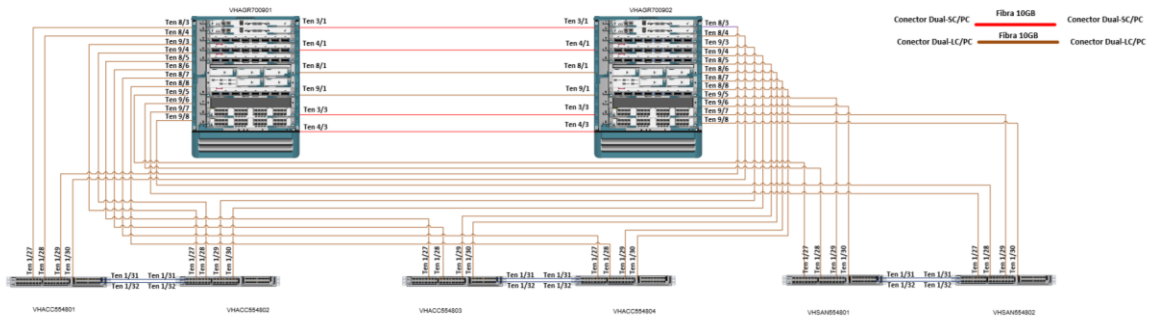


Figura 4.43 Referencia topológica - Configuración

La figura 4.44 muestra el resumen de configuración FabricPath

Cisco Nexus 7000 Series Spine 1 (VHAGR700901)

```
install feature-set fabricpath
hostname VHAGR700901
vdc AGGREGATION id 1
allow feature-set fabricpath
[…]
feature-set fabricpath
[…]
feature ospf
feature pim
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature bfd
bfd interval 50 min_rx 100 multiplier 3
vlan X
mode fabricpath
name FP_VLAN_101
vlan XX
mode fabricpath
name FP_VLAN_102
vlan XXX
mode fabricpath
name FP_VLAN_103
vpc domain 1
role priority 110
peer-keepalive destination X.X.X.X
delay restore 3600
dual-active exclude interface-vlan 101-104
fabricpath switch-id 1000
interface X
no shutdown
ip address X.X.X.2/16
ip ospf passive-interface
ip router ospf 10 area 0.0.0.0
ip pim sparse-mode
ip pim bfd-instance
ip pim dr-priority 10
ip pim hello-interval 1000
hsrp 1
preempt delay reload 300
priority 110
ip X.X.X.1

interface port-channelX
description FP Link to VHACC55480X
switchport
switchport mode fabricpath
interface port-channel2
description vPC+ Peer-Link
switchport
switchport mode fabricpath
vpc peer-link
interface Ethernet8/1
description vPC+ Peer-Link Member 1
switchport mode fabricpath
channel-group 2 mode active
no shutdown
interface Ethernet9/1
description vPC+ Peer-Link Member 2
switchport mode fabricpath
channel-group 2 mode active
no shutdown
```

```
interface Ethernet8/4
description Port-channel to VHACC55480X
switchport mode fabricpath
channel-group 1 mode active
no shutdown
fabricpath domain default
root-priority 66
topology 1
ip pim rp-address 3.3.3.3 group-list 224.0.0.0/4
ip pim ssm range 232.0.0.0/8
fabricpath switch-id 121
```

Cisco Nexus 7000 Series Spine 2 (VHAGR700902)

```
install feature-set fabricpath
hostname VHAGR700902
vdc AGGREGATION id 1
allow feature-set fabricpath
[…]
feature-set fabricpath
cfs eth distribute
feature ospf
feature pim
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature bfd
bfd interval 50 min_rx 100 multiplier 3
vrf context management
ip route 0.0.0.0/0 10.60.17.254
vlan X
mode fabricpath
name FP_VLAN_101
vlan XX
mode fabricpath
name FP_VLAN_102
vlan XXX
mode fabricpath
name FP_VLAN_103
vpc domain 1
peer-keepalive destination X.X.X.Z
delay restore 3600
dual-active exclude interface-vlan 101-104
fabricpath switch-id 1000
interface X
no shutdown
no ip redirects
ip address X.X.X.3/16
ip ospf passive-interface
ip router ospf 10 area 0.0.0.0
ip pim sparse-mode
ip pim bfd-instance
ip pim hello-interval 1000
hsrp 1
ip X.X.X.1
interface port-channelX
```

```
description FP Link to VHACC554802
switchport
switchport mode fabricpath
interface port-channel2
description vPC+ Peer-Link
switchport
switchport mode fabricpath
vpc peer-link
interface Ethernet8/1
description vPC+ Peer-Link Member 1
switchport mode fabricpath
channel-group 2 mode active
no shutdown
interface Ethernet9/1
description vPC+ Peer-Link Member 2
switchport mode fabricpath
channel-group 2 mode active
no shutdown
interface Ethernet8/3
description FP Link to VHACC554802
switchport mode fabricpath
channel-group X mode active
no shutdown
interface Ethernet8/4
description FP Link to VHACC554802
switchport mode fabricpath
channel-group 2 mode active
no shutdown
fabricpath domain default
root-priority 65
topology 1
ip pim rp-address 3.3.3.3 group-list 224.0.0.0/4
fabricpath switch-id 122
```

Figura 4.44 Resumen de configuración FabricPath

4.13 vPC+

FabricPath extiende los beneficios de vPC a un entorno FabricPath con la introducción de vPC +. Al igual que vPC, vPC + proporciona una capacidad de enlace ascendente 136ritic-activo para los hosts de base dual, así como para la infraestructura de red Ethernet clásico tradicional, como Spanning-tree Protocol switches, routers y servicios (como por ejemplo firewalls y balanceadores de carga). Mientras el dispositivo conectado admite PortChannels (también conocido como EtherChannel, agregación de enlaces, etc), el dispositivo puede beneficiarse de vPC +. vPC + soporta dinámico (negociado a través de Link Protocolo de control de agregación [LACP]) y PortChannels estáticas que se conectan desde un único dispositivo Ethernet clásico a un par de switches FabricPath.

4.13.1 Bases de vPC+

La configuración de hardware y software para vPC + es casi idéntica a la de vPC tradicional.

Sólo hay algunas diferencias importantes:

- ➔ Debe configurar un SID FabricPath bajo el dominio vPC (FabricPath conmutador-idx).
- ➔ Este SID actúa como un conmutador virtual que los pares + VPC a la red (más detallesse proporcionan más adelante en esta sección).
- ➔ Deben utilizarse interfaces F1 como los + enlaces pares VPC.
- ➔ El vPC + enlace entre pares se debe configurar como un puerto principal FabricPath(modo switchport FabricPath).

La figura 4.45muestra cómo vPC + introduce un conmutador virtual en la red FabricPath:

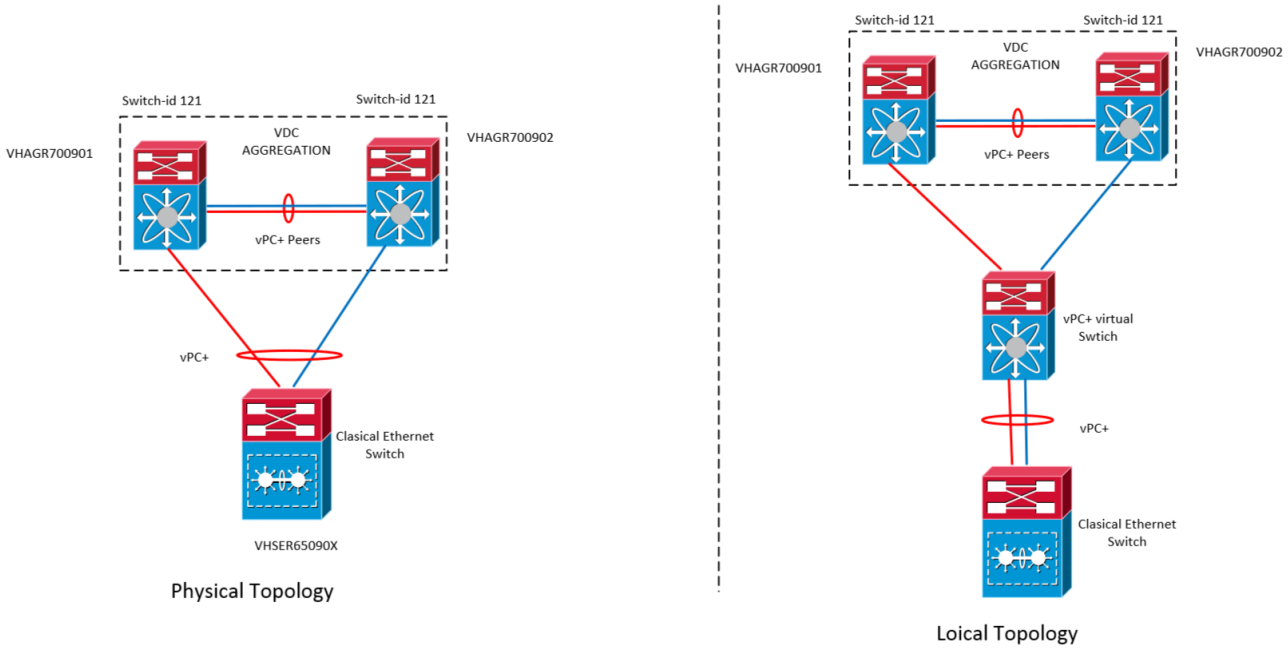


Figura 4.45 vPC+ Introduce un switch virtual dentro de la topología FabricPath

VHAGR700901-agregación y VHAGR700902-agregación son los switches + pares VPC. Tanto un vínculo entre pares y un enlace keepalive se requieren entre estos switches (al igual que envPC). El vPC + enlace entre pares debe constar de las interfaces de los módulos de F1 de E / S y debe ser configurado como puerto base FabricPath.
El + SID virtuales vPC configurado bajo el dominio vPC debe ser único en el dominio FabricPath. Ningún otro cambio físico debe usar ese SID, y ningún otro dominio vPC deben utilizar el mismo SID virtual.

4.13.2 Configuración vPC+ Peer Keepalive

El enlace keepalive vPC + pares (peers) Citirix puede para cualquiera de los métodos habituales para la conectividad keepalive (conexión directa, la interfaz de supervisor de mgmt0, etc.) Para las conexiones directas, las interfaces de módulos M1 I / O, si tiene módulos M1 en el VDC, o F1 interfaces de módulos de E / S.

Cuando el uso de conexiones es directa en las interfaces de M1, se configuran las direcciones IP en cada una de las conexiones, y si es una instancia VRF dedicada esta es para la conectividad entre pares Keepalive (nota que la configuración VRF utiliza una licencia de servicios empresariales Capa 3).

Al utilizar conexiones directas en las interfaces F1 definir una VLAN dedicada ID de conectividad keepalive compañeros y luego definir una interfaz virtual del switch VLAN (SVI) en cada switch y configurar una dirección IP y, si es posible, una instancia VRF dedicado. Además, asegúrese de añadir el comando de configuración de dirección en las SVI para permitir que el SVI se mantenga en el estado hasta incluso si no hay módulos M1 I / O están presentes.

La siguiente figura, 4.46, muestra una topología que utiliza interfaces de módulos F1 de E / S para el enlace keepalive pares:

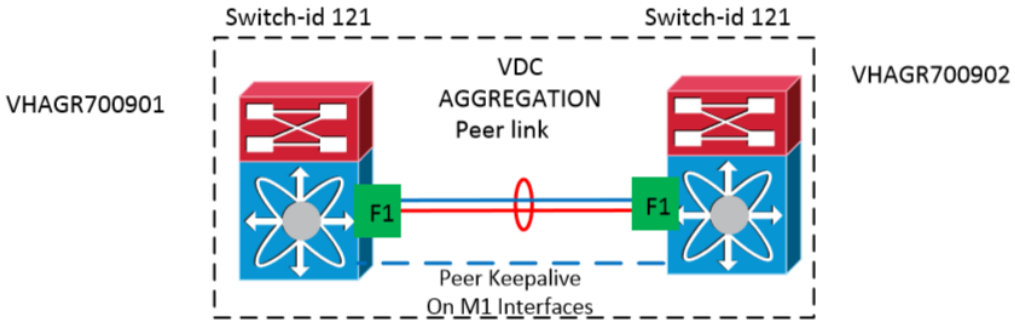


Figura 4.46 Usando interfaces M1 para conectividad vPC+ Peer Keepalive

Sí se está utilizando M1 o interfaces de módulos F1 de E / S para el keepalive pares, hay que tener cuidado si se es incapaz de aislar las interfaces mediante una instancia VRF específico (por ejemplo, no se instala una licencia de Capa 3). Sin una configuración dedicada VRF, el switch trata la interfaz de capa 3 o SVI utilizado para la keepalive pares como cualquier otra interfaz y enrutar el tráfico de mayo sobre ella, lo que probablemente no es deseable.

4.13.2.1 Roles y prioridad de vPC

Un dominio necesita ser definido (como se indica por el ID de dominio), así como las prioridades para definir las funciones primarias y secundarias en la configuración vPC. Además, estos roles son non-preemptive, por lo que un dispositivo pueden ser operativamente primaria, secundaria, pero desde la perspectiva de configuración.

Para dos switches (pares VPC) para formar un sistema vPC, los ID de dominio de estos switches deben coincidir. Como se ha descrito anteriormente, el ID de dominio se utiliza para generar la LAGID en la negociación LACP.

En la siguiente tabla, 4.18, se muestra el dominio vPC en el módulo de agregación.

Tabla 4.18 Dominio vPC en el módulo de agregación

Switch	SubSwitch-ID
vPC domain ID	100
Role Primary	5500
Role Secundary	6000
System priotity primary	4000
System priority secondary	4000

La figura 4.47 muestra la configuración para el rol y prioridad vPC

```
Switch1(config)# vpc domain <domain-id>
Switch1 (config-vpc-domain)# role priority xxxx
Switch2 (config)# vpc domain <domain-id -- same as Switch1>
Switch2 (config-vpc-domain)# role priority xxxx
```

Figura 4.47 Rol y prioridad vPC

4.13.2.2 Enlace vPC Peer

El vínculo entre pares vPC es una troncal de 2 capas 802.1Q estándar que lleva potencialmente todas las VLAN. También lleva a regular de tráfico de plano de control, tales como HSRP hellos, STP BPDU, etc El vPC Peer Link también lleva el CFS crítico (Cisco tela Servicios) de tráfico, tales como las BPDU y HSRP hellos y la sincronización de dirección MAC entre los pares VPC, que son marcada con un valor CoS de 6.

El enlace vPC Peer se considera crítico para la operación vPC. A pesar de su fracaso no interrumpe los flujos VPC existente, el incumplimiento puede poner en peligro el establecimiento de nuevos flujos y aislar puertos huérfanos. Configurar el enlace entre pares de una manera redundante ayuda a garantizar la conectividad esencialmente ininterrumpida entre los compañeros VPC. Como tal, las recomendaciones generales de enlaces de pares son como sigue:

- ➔ El enlace vPC Peer debe estar formado por un mínimo de 2 x conexiones 10GE en linecards separados
- ➔ Los puertos 10GE deben ser configurados para funcionar en modo de ancho de banda dedicado
- ➔ Configurar VPC puertos Peer enlace como puertos 'Red' STP para permitir Spanning-tree Assurance Puente en estos enlaces (suponiendo que BA se habilita globalmente).
- ➔ Habilitar UDLD en VPC Peer Enlaces

La recomendación de utilizar un mínimo de 2 x 10GE enlaces para el enlace entre pares vPC asegura que un solo fallo linecard 10GE no dará lugar a una situación de conmutación por error vPC, por lo que la dependencia de las características de seguridad tales como el enlace Peer-Keepalive o Spanning-tree pueda entrar en jugar.

La recomendación sobre el modo de tasa específica se hace para asegurar que sobresuscripción no debería ser un problema en el vPC Peer Link.

El modo de velocidad en un puerto puede ser configurado mediante los siguientes comandos CLI como se muestran en las figuras 4.48 y 4.49:

```
Interface Ethernet <slot/port>
Rate-mode dedicated
```

Figura 4.48 Configuración modo dedicado

```
switch(config)# interface port-channel10
switch(config-if)# vpc peer-link
switch(config-if)# switchport trunk allowed VLAN <all access VLANs>
```

Figura 4.49 Configuración vPC Peer-Link

La configuración de la conexión entre pares (peers) se instala automáticamente con el aseguramiento de puente en el enlace entre pares. Esta configuración es compatible con ISSU, así que se puede mantener Puente Assurance activa en este enlace.

El enlace entre pares lleva una copia del tráfico de multidifusión, independientemente de si existen puertos huérfanos que necesitan para recibirlo. Usted debe aprovisionar el ancho de banda para el enlace entre pares en consecuencia.

La tabla 4.19 muestra los puertos peer link para la agregación vPC

Tabla 4.19 Agregación vPC Peer-Link ports

Dispositivo	Puertos	Portchannel
VHAGR700901 - AGGREGATION	8/1, 9/1	2
VHAGR700902 - AGGREGATION	8/1, 9/1	2

La figura 4.50 muestra el comando que muestra el Levante la FP IS-IS métrica para VPC+ Peer-Link a preferir otros enlaces Core FP:

```
switch(config)# interface port-channel10
switch(config-if)# fabricpath isis metric 200
```

Figura 4.50 Configuración vPC Peer-Link

4.13.2.3 vPC Peer-Keepalive

Otro eslabón clave en la cadena de gestión de ciclo vPC es el vínculo peer-keepalive. Este enlace proporciona una ruta de comunicación secundaria entre los dispositivos de pares VPC con el fin de detectar un posible escenario activo / activo en el caso de un fallo catastrófico de las múltiples conexiones entre pares de enlaces de VPC. Si bien esta clase de fallo es muy poco probable (pérdida de múltiples tarjetas de línea y puertos al mismo tiempo tiene una muy pequeña probabilidad de ocurrencia), todavía es un caso de error que necesita ser protegida contra. Con el fin de hacer esto, los sistemas de vPC enviar un mensaje hola el uno al otro una vez cada 2 segundos. Los mensajes son sólo 96 bytes de longitud, y no tienen ningún tráfico de datos, de hecho, sólo llevan el ID del dispositivo, vPC ID de dominio y la información de origen y destino, a fin de validar que los paquetes son recibidos por el vPC apropiado dispositivo par.

La recomendación es ejecutar el enlace peer-keepalive vPC a través de un enlace punto 2 puntos por separado entre los compañeros VPC, probablemente en un puerto de 1 GbE si hay alguno disponible. También es posible configurar un canal de puertos entre los dos switches con el fin de proporcionar la resistencia física adicional a la ruta de transmisión de mensajes entre keepalive, pero esto no se requiere específicamente.

El vPC Peer-keepalive Link (PK-link) se utiliza para proporcionar protección contra escenarios activos duales en el caso de la primaria Peer Enlace perderse. Si la pérdida de la Peer Enlace se lleva a cabo, el enlace de PK se utiliza para determinar el estado del par opuesto (en otras palabras, para determinar si la pérdida de conectividad es debida a fallo en liga o error en el nodo).

El PK-Link utiliza un latido simple entre sus compañeros VPC - estos mensajes se envían cada 2 segundos y utiliza el enlace de 3 segundos de tiempo de espera dominio sobre la pérdida de la Peer primaria Link.

La tabla 4.20 muestra los puertos keep alive para la agregación vPC

Tabla 4.20 Agregación vPC Keep Alive link ports

Dispositivos	Puertos	Portchannel	Dirección IP
VHAGR700901 - AGGREGATION	3/3, 4/3	3	172.28.184.X1
VHAGR700902 - AGGREGATION	3/3, 4/4	3	172.28.184.X2

La configuración de la figura 4.51ilustra el uso de una interfaz de Ethernet Gigabit dedicado para este propósito:

```
vrf context vpc-keepalive
interface Ethernet8/16
description vPC Heartbeat Link
vrf member vpc-keepalive
ip address x.x.x.x/y
no shutdown
vpc domain 1
peer-keepalive destination x.x.x.x source x.x.x.x vrf vpc-keepalive
```

Figura 4.51 vPC Peer Keepalive

No debe usarse la interfaz mgmt0 para una conexión de back-to-back directa entre los sistemas de Cisco Nexus 7000 Series, porque no se puede determinar qué supervisor está activo en un momento dado.

La interfaz mgmt0 se puede utilizar tanto para la gestión y para el encaminamiento de la keepalive pares a través de la red de gestión fuera de banda. En este caso, cada uno de Cisco Nexus 7009 Conmutador de la serie está conectado a la red de gestión a través de mgmt0 de supervisor de ranuras 1 y 2.

Siguiendo este enfoque, independientemente de qué supervisor está activo, el Nexus 7009 Conmutador de la serie Cisco tiene una de las interfaces mgmt0 conectados a la red de gestión, que luego se pueden utilizar para los propósitos de mantenimiento de conexión por pares.

4.13.3 Reenvío Active-Active HSRP

Al igual que con vPC tradicional vPC + ofrece reenvío HSRP activo-activo cuando los pares VPC+ han formado una relación activo-standby HSRP, es decir, cualquiera de los switches vPC+ pares (peers) realizará una expedición de capa 3 para el tráfico destinado a la dirección virtual MAC HSRP (VMAC).

El vPC+ par (peer), con la instancia del control-plane HSRP activa, transmite HSRP saludos procedentes de la dirección VMAC HSRP y destinados a la dirección de todos los routers HSRP (VMAC). Cuando éstos saludos se envían en puertos centrales FabricPath, el campo exterior SA contiene el SID virtual de vPC+, causando conmutadores de extremo FabricPath para aprender la dirección de VMAC HSRP como una dirección MAC remota utilizando el + SID virtual de vPC y no el SID del switch particular, vPC+ pares. Los conmutadores tradicionales Ethernet, conectados detrás de vPC+ PortChannels, aprenden la dirección VMAC en la interfaz PortChannel conectándose así a los pares VPC+.

La siguiente figura ilustra la topología física y lógica de una configuración vPC +:

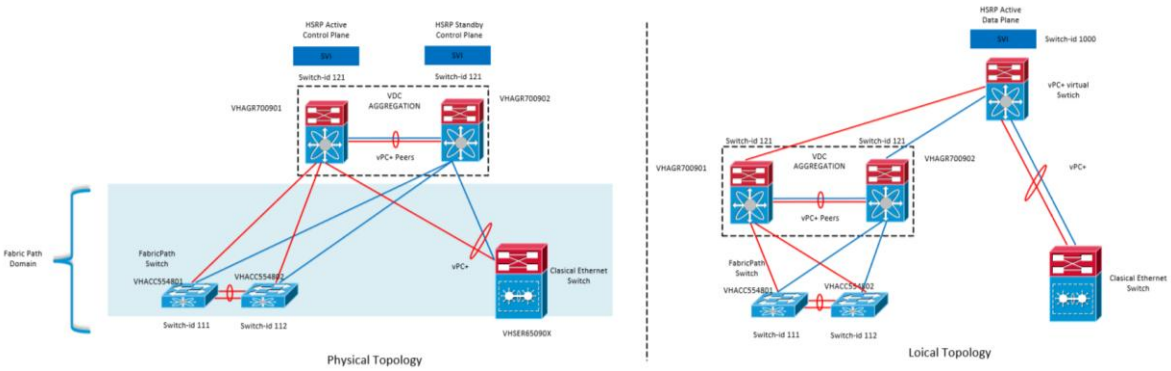


Figura 4.52 Active HSRP con vPC+

Esta técnica permite a todos los dispositivos, independientemente de si están conectados a través de PortChannels VPC+ o puertos nativos FabricPath, usar la función de reenvío de HSRP activo-activo de vPC + y utilizar varias rutas a la puerta de enlace predeterminada.

Cuando un conmutador de acceso FabricPath debe enviar una trama a la dirección VMAC HSRP, la tabla de direcciones MAC de búsqueda devuelve el SID + virtuales vPC como la dirección central de destino. Cuando un dispositivo Ethernet conectado a un tradicional vPC+ PortChannel debe enviar una trama a la dirección VMAC HSRP. El tráfico puede tener cualquier vínculo físico en el PortChannel, al llegar a cualquiera de los switches vPC+ pares, cualquiera de los cuales puede enrutar el paquete.

4.13.4 Configuración de vPC

La figura 4.53 muestra la configuración inicial para vPC

```
switch# config t ->Enables vPC, LACP and Udld
switch(config)# feature vPC
switch(config)# feature lacp
switch(config)# feature udld
switch(config)# spanning-tree VLAN 1-4093 root <primary/secondary>
switch(config)# spanning-tree VLAN 1-4093 hello-time 4
```

Figura 4.53 Configuración inicial vPC

Se debe habilitar la característica vPC para poder configurar o ejecutar la funcionalidad vPC.

Después de habilitar la funcionalidad vPC, se debe crear el vínculo peer-keepalive que envía mensajes de control entre los dispositivos pares (peers) VPC.

La tabla 4.21 muestra los puertos vPC Peer-keepalive en la empresa.

Tabla 4.21 vPC Peer-Keepalive ports en la Empresa

Dispositivo	vPC Peer-Keepalive link port
VHAGR700901-AGGREGATION	3/3, 4/3
VHAGR700902-AGGREGATION	3/3, 4/3

La figura 4.54 ilustra la configuración peer-keepalive link

```
switch(config)# vrf context pkalVRF for the vPC peer-keepalive link
switch(config-vrf)# exit
switch(config)# interface portchannel 3
switch(config-if)# vrf member pkal
switch(config-if)# ip address <ip address>
switch(config-if)# no shutdown
switch(config)# interface ethernet 3/3
switch(config-if)# channel group 3 mode active
switch(config-if)# no shutdown
```

Figura 4.54 Configuración Peer-Keepalive link

La tabla 4.22 muestra vPC Peer-Keepalive en la empresa

Tabla 4.22 vPC Peer-Keepalive link ports en la Empresa

Dispositivo	vPC Peer-Keepalive link port
VHAGR700901-AGGREGATION	8/1, 9/1
VHAGR700902-AGGREGATION	8/1, 9/1

La figura 4.55 ilustra la configuración Peer-Keepalive link

```
switch(config)# interface ethernet 8/1
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 9/1
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 8/1 ! Peer links in portchannel LACP
switch(config-if)# switchport
switch(config-if)# switchport mode fabricpath
switch(config-if)# spanning-tree port type network
ilustrswitch(config)# interface ethernet 9/1 ! Peer links in portchannel LACP
switch(config-if)# switchport
switch(config-if)# switchport mode fabricpath
switch(config-if)# channel-group 2 mode active
switch(config-if)# exit
switch(config)# interface port-channel 2 ! vPC peer link
switch(config-if)# vpc peer-link
switch(config-if)# exit
```

Figura 4.55 Configuración Peer-Keepalive link

El dominio vPC incluye dispositivos VPC pares (peers), el vínculo peer-keepalive vPC, el vínculo entre pares vPC, y todos los canales de puerto en el dominio vPC conectado al dispositivo de transmisión hacia abajo. Se puede tener un solo vPC ID de dominio en cada dispositivo.

Siempre hay que conectar todos los dispositivos vPC utilizando los canales del puerto a dispositivos vPC pares (peers).

La figura 4.56 muestra las configuraciones de Links a vPC de transmisiones hacia abajo

```
switch(config)# interface ethernet X/Y ! links to vPC downstream
switch(config-if)# switchport mode trunk
switch(config-if)# allowed VLAN X-Y
switch(config-if)# native VLAN Z
switch(config-if)# channel-group XX mode active
switch(config-if)# exit
switch(config)# interface port-channel XX
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# vpc XXX
switch(config-if)# exit
switch(config)#
```

Figura 4.56 Configuraciones links a vPC Downstream

El tercer dispositivo, o el dispositivo de downstream, puede ser un switch, el servidor o cualquier otro dispositivo de red que utiliza un canal de escala habitual para conectarse a la vPC. Se tiene que utilizar LACP para el puerto de canal de los dispositivos de acceso y los switches de servicios que se conectan a la capa de agregación.

La tabla 4.23 muestra los puertos vPC Peer link en la Empresa.

Tabla 4.23 vPC Peer link ports ports en la Empresa

Dispositivo de agregación	Puerto de agregación	vPC	Tercer Dispositivo
VHAGR700901-AGGREGATION	3/8	10	VHSER650901 VHSER650902
VHAGR700902-AGGREGATION	3/8	10	VHSER650901 VHSER650902
VHAGR700901-AGGREGATION	4/8	11	VHSER650901 VHSER650902
VHAGR700902-AGGREGATION	4/8	11	VHSER650901 VHSER650902
VHAGR700901-AGGREGATION	4/8	20	VHDCI700901 VHDCI700902
VHAGR700902-AGGREGATION	4/8	20	VHDCI700901 VHDCI700902
VHAGR700901-AGGREGATION	4/8	21	VHDCI700901 VHDCI700902
VHAGR700902-AGGREGATION	4/8	21	VHDCI700901 VHDCI700902
VHAGR700901-AGGREGATION	8/21	30	Data mover 01
VHAGR700902-AGGREGATION	8/21	30	Data mover 01
VHAGR700901-AGGREGATION	8/24	31	Data mover 01
VHAGR700902-AGGREGATION	8/24	31	Data mover 01
VHAGR700901-AGGREGATION	8/22	32	Data mover 02
VHAGR700902-AGGREGATION	8/22	32	Data mover 02
VHAGR700901-AGGREGATION	8/25	33	Data mover 02
VHAGR700902-AGGREGATION	8/25	33	Data mover 02
VHAGR700901-AGGREGATION	8/23	34	Data mover 03
VHAGR700902-AGGREGATION	8/23	34	Data mover 03
VHAGR700901-AGGREGATION	8/26	35	Data mover 04
VHAGR700902-AGGREGATION	8/26	35	Data mover 04
VHAGR700901-AGGREGATION	5/2	36	ISILON x400
VHAGR700902-AGGREGATION	5/2	36	ISILON x400
VHAGR700901-AGGREGATION	5/3	37	ISILON x400
VHAGR700902-AGGREGATION	5/3	37	ISILON x400
VHAGR700901-AGGREGATION	5/4	38	ISILON x400
VHAGR700902-AGGREGATION	5/4	38	ISILON x400
VHAGR700901-AGGREGATION	6/2	39	ISILON x400
VHAGR700902-AGGREGATION	6/2	39	ISILON x400
VHAGR700901-AGGREGATION	6/3	40	ISILON x400
VHAGR700902-AGGREGATION	6/3	40	ISILON x400
VHAGR700901-AGGREGATION	6/4	41	ISILON x400
VHAGR700902-AGGREGATION	6/4	41	ISILON x400
VHAGR700901-AGGREGATION	8/15	42	ISILON NL400
VHAGR700902-AGGREGATION	8/15	42	ISILON NL400
VHAGR700901-AGGREGATION	8/16	43	ISILON NL400
VHAGR700902-AGGREGATION	8/16	43	ISILON NL400
VHAGR700901-AGGREGATION	9/23	44	ISILON NL400
VHAGR700902-AGGREGATION	9/23	44	ISILON NL400
VHAGR700901-AGGREGATION	9/24	45	ISILON NL400
VHAGR700902-AGGREGATION	9/24	45	ISILON NL400
VHAGR700901-AGGREGATION	9/25	46	ISILON NL400
VHAGR700902-AGGREGATION	9/25	46	ISILON NL400

4.14 Jumbo Frames

Nota:

Si un paquete Jumbo tiene que atravesar un Nexus 5548 y Nexus 7010, es necesario configurar la política-mapa en el Nexus 5548 y establecer el tamaño jumbomtu sistema en el Nexus 7010 Series Switch.

Si se va a enviar el tráfico al SVI entonces se necesita una mtu configurada en el SVI.

En la figura 4.57Se muestra la configuración para establecer el tamaño de Jumbo frame en equipos N5K

```
switch(config)#policy-map type network-qos jumbo
switch(config-pmap-nq)#class type network-qos class-default
switch(config-pmap-c-nq)#mtu 9216
switch(config-pmap-c-nq)#multicas-optimize
switch(config-pmap-c-nq)#exit
switch(config-pmap-nq)#exit
switch(config)#system qos
switch(config-sys-qos)#service-policy type network-qos jumbo
```

Figura 4.57 Configuración Jumbo Frame para N5K

En la figura 4.58Se muestra la configuración para establecer el tamaño de Jumbo frame en equipos N7K

```
switch(config)#system jumbomtu 9216
switch(config)#interface ethernet x/x
switch(config-if)#switchport
switch(config-if)#mtu 9216
switch(config-if)#exit
switch(config)#interface vlan <number>
switch(config-if)#mtu 9216
switch(config-if)#exit
```

Figura 4.58 Configuración Jumbo Frame para N7K

4.15 Flujo de tráfico de agregación

El módulo de agregación recibirá el tráfico que viene desde el Core, y exportará este tráfico a al nivel de servicios requerido.
En la figura 4.59Se observa el flujo del tráfico.

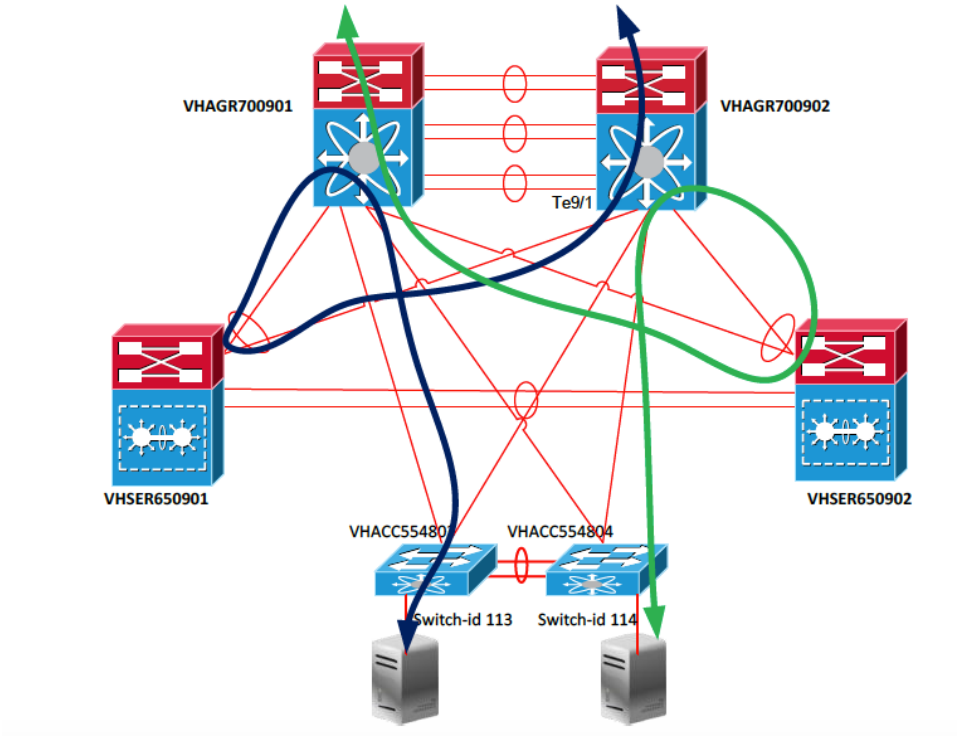


Figura 4.59 Flujos de tráfico de Agregación a Servicios

En cada nivel se aplicarán IPS y las políticas de balanceo de carga, luego eltráfico regresaráa los dispositivos de agregación para que el tráfico pueda seguir su camino haciala capa de acceso.

Capítulo 5: Acceso

5.1 Descripción general

El nivel de acceso brinda la conectividad física de red a los servidores y sistemas del Data Center. En la capa de acceso se juega un rol crítico, el cual consta de cubrir requerimientos particulares tales como NIC teaming, clustering y contención de transmisión. La capa de acceso es el primer punto de Oversubscription en el Data Center porque conjunta el tráfico de los servidores a una velocidad de 10 Gigabit Ethernet en los enlaces hacia la capa de agregación. Para la producción de la solución de la capa de acceso se ha tomado en cuenta la agilidad de negocio, los requerimientos de conectividad, y la característica de los sets de soporte para las granjas de servidoresexistentes y futuras de la empresa. La solución del nivel acceso provee:

- **Arquitectura de nivel de acceso flexible**—la cual respalda la ubicación lógica de los servidores a través de la Infraestructura del Data Center.
- Opera en el ambiente de Capa 2.
- Radios de densidad de puertos yOversubscription.
- Apoyo para Unified fabric y entradas/salidas consolidadas.
- Opciones de conectividad para mantener las plataformas de los servidores de la Empresa, incluyendo Legacy y los requerimientos de conectividad de las plataformas de la Citrix Cloud. La solución brinda el apoyo para la conectividad de equipos a 10GE. También provee la opción de conectividad de sistemas blade FCoE y FC.
- Opción estandarizada para la ubicación de dispositivos de acceso a nivel de red.
- Soporte para NIC teaming, clustering, etc.
- Facilidad de administración con un número reducido de puntos de administración.

5.2 Requerimientos de conectividad de capa de acceso

Los servidores en uso, de la Empresa, utilizan actualmente NICs para la conectividad de la red y HBAs para la conectividad de almacenamiento. Típicamente, cada servidor utiliza un par dedicado de NICs para la producción, despliegue, respaldo y manejo. Estos servidores tienen normalmente interfaces múltiples, las cuales son acomodadas para realizar las funciones específicas siguientes:

Interfaces de producción – se usan para transportar el tráfico con información de aplicaciones,desde y hacia los servidores. El tráfico de respaldo basado en la red se dirige también a estas interfaces. La mayoría de los servidores en la empresa están equipados con interfaces en velocidades de 10Gig Ethernet. El número de interfaces usado por el servidor varía con base en el hardware, en la aplicación y en la plataforma del sistema operativo.

5.3 Componentes del hardware

Se implementarán switches para la capa de acceso en el Data Center, emparejados en grupos de dos para habilitar las conexiones redundantes de servidores en donde estén disponibles. En

el Data Center de Villahermosa, se instalará un total de seis switches Cisco Nexus 5548UP. Dos de esos switches se utilizarán para la inter-conexión SAN.

La Tabla 5.1 enlista el chasis y los módulos que se utilizarán para los switches de la plataforma de capa de acceso en Villahermosa.

Tabla 5.1 Especificación de Hardware de nivel de Acceso para Ethernet y FCoE

Cantidad	Equipo	Descripción
6	Cisco Nexus 5548UP Switch	1RU 10 Gigabit Ethernet, Fibre Channel, and FCoE switch ofreciendo hasta 960 Gbps de rendimiento y hasta 48 puertos. El switch tiene 32 puertos unificados y un espacio de expansión.
4	N55-M16UP	Nexus 5500 Unified Module con 16 puertos 10GE Eth/FCoE o 16 puertos 8/4/2/1G FC

El switch Cisco Nexus 5548UP se basa en el software de Cisco NX-OS, y es un switch Rack-Unit 10 Gigabit Ethernet y FCoE que ofrece un rendimiento de hasta 960-Gbps, provee hasta 48 puertos: 32 fijos unificados de 1/10-Gbps SFP+ Ethernet y puertos FCoE, y un espacio de expansión.

En la figura 5.1 se muestra el equipo físico del switch Cisco Nexus 5548UP

Figura 5.1 Vista física frontal de switch Cisco Nexus 5548UP

Con los módulos de expansión N55--M16UP, el switch Cisco Nexus 5548UP puede brindar un puerto de 16 unificado con 10-Gbps SFP+ Ethernet y FCoE o 1/2/4/8-Gbps Fiber Channel nativo. Este módulo se utiliza para interconectar el Nivel de Acceso al ambiente de SAN con el puerto FC conectado al Switch MDS 9506.

En la tabla 5.2 se muestra la cantidad de SFP de los módulos para el equipo Nexus 5548UP

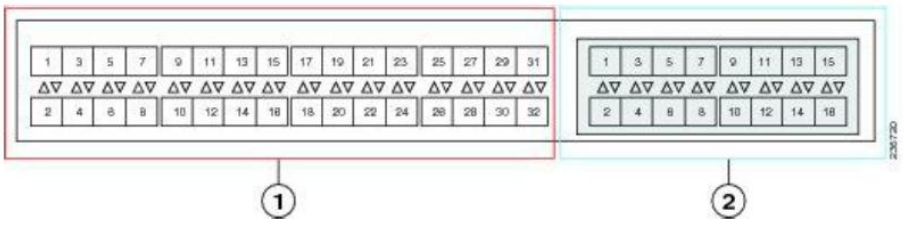
Tabla 5.2 Módulos Cisco Nexus 5548UP SFP

Cantidad	*Modulo*	*Descripción*
12	DS-SFP-FC8G-SW	8 GbpsFibreChannelSWSFP+LC
144	SFP-10G-SR	10GBASE-SR SFPModule
40	GLC-T	1000BASE-TSFP

5.3.1 Puertos de datos

Cada puerto de datos en el switch Cisco Nexus 5548 y los grupos de puertos están numerados basados en su función. Los puertos se enumeran de arriba hacia abajo, y de izquierda a derecha.

Se observa en la figura 5.2 la numeración de los puertos para el switch Cisco Nexus 5548



1	32 fixed ports	2	16-port expansion module (N55 M16UP)

Figura 5.2 Numeración de puertos del switch Cisco Nexus 5548 con un módulo de expansión

5.4 Alto nivel de disponibilidad del sistema

Las siguientes características se encontrarán disponibles en las plataformas Cisco Nexus 5548UP en el Data Center de la empresa para su alta disponibilidad:

- Mejora del Software In-Service (ISSSU) para Capa 2
- Insumos de energía hot-swappable y field-replaceable, módulos de extracción y módulos de expansión.
- Potencia de redundancia 1:1
- 2 Módulos extractores

Nota:

El switch Cisco Nexus 5548 requiere de dos módulos extractores. Cada módulo extractor tiene cuatro extractores. Si más de un extractor falla en uno de estos módulos, el módulo deberá ser cambiado.

5.5 Especificación del software

La tabla 5.3 nos muestra la versión de software recomendada para switches Access Cisco Nexus 5548UP.

Tabla 5.3 Especificación para software de switches

Actualización de Software	Descripción	Nombre del archivo	Tamaño
6.0(2N1(1)	Nexus 5548UP Release 6.0(2)N1(1) Kick Start image Nexus 5548UP Release 6.0(2)N1(1) System Image	n5000-uk9-kickstart 6.0.2.N1.1bin n5000-uk9.6.0.2.N1.1.bin	33.07 MB (34676224 bytes) 226.80 MB (237821046)

5.5.1 Instalación de software NX-OS

Los switches Nexus 5548UP para el Data Center Villahermosa son habilitados con una memoria Bootflash de 2GB. La verión recomendada NX-OS 6.0(2)N1(1), (imágenes kick start y del sistema) utilizan un total de 260 MB(272497270 bytes) de memoria bootflash. La figura 5.3 muestra la memoria la memoria interna bootflash disponible.

```
switch# dir
             1211 Dec 28 12:34:52 2012 license_SSI16420TS4_13.lic
             4096 Mar 07 05:30:59 2013 lost+found/
             2208 Mar 07 11:03:23 2009 mts.log
34358272 Dec 28 12:27:21 2012 n5000-uk9-kickstart.5.1.3.N1.1a.bin
147420604 Dec 28 12:28:44 2012 n5000-uk9.5.1.3.N1.1a.bin
             4096 Jan 01 12:31:39 2009 vdc_2/
             4096 Jan 01 12:31:40 2009 vdc_3/
             4096 Jan 01 12:31:40 2009 vdc_4/
             4096 Mar 08 13:40:43 2009 virt_strg_pool_bf/

Usage for bootflash://
299753024 bytes used
1351152064 bytes free
1650905088 bytes total
```

Figura 5.3 Memoria bootflash interna

Existen varios procedimientos disponibles para descargar un archivo en la memoria bootflash. Para copiar la versión NX-OS 6.0(2)N1(1), (imágenes kick start y del sistema) en la memoria bootflash, se puede usar una memoria USB conectada al puerto USB disponible en el Nexus 5500 Series que se encuentra ubicado en la parte trasera del chasis, fácil de identificar al costado del puerto de la consola. La figura 5.4 muestra el comando para descargar los archivos con la memoria USB.

```
switch# copy usb1: bootflash:n5000-uk9-kickstart.6.0.2.N1.1.bin
Enter source filename: n5000-uk9-kickstart.6.0.2.N1.1.bin
switch# copy usb1: bootflash: n5000-uk9.6.0.2.N1.1.bin
Enter source filename: n5000-uk9.6.0.2.N1.1.bin
```

Figura 5.4 Descargando la versión kickstart y sistema NX-OS

Es recomendable ampliamente que se firme en el puerto de consola para comenzar el proceso de upgrade.

No se puede entrar en modo de configuración durante un upgrade. Se debe guardar, consignar o descartar cualquier sesión activa de configuración antes del upgrading o downgrading la imagen del software Cisco NX-OS. Se borrará la sesión activa de configuración sin previo aviso durante una recarga. Hay que utilizar el comando summary session para verificar que no haya sesiones activas de configuración. La figura 5.5 muestra dicho comando.

```
switch# show configuration session summary
There are no active configuration sessions
```

Figura 5.5 Comando para verificar sesiones activas de configuración

Se tienen que evitar interrupciones de energía durante un procedimiento de instalación. Las interrupciones de energía pueden corromper la imagen de software.

Para el upgrade del sistema NX-OS se utiliza el comando "**install all".** El comando acciona los ISSSU en switches Cisco Nexus 5000 Series.
ISSU significa Actualización de los servicios de Software (In-Service Software Upgrade). Con esto, es posible el upgrade de capa de acceso Nexus sin causar ninguna disrupción en el tráfico de los servidores.

Tradicionalmente, ISSU ha sido puesto en sistemas modulares de doble supervisión como los switches Cisco Nexus 7000 y Cisco Catalizador 6500. Con un solo supervisor como el switch Cisco Nexus 5000 Series, el proceso de ISSU trabaja de manera diferente, pero brinda los mismos beneficios que un sistema de supervisor dual. El ISSU en el switch de Cisco Nexus 5000 Serie causa que el supervisor CPU restablezca y cargue la nueva versión del software. El plano de control se encuentra inactivo en este lapso, pero el plano de información sigue mandando paquetes, llevándolo hacia un upgrade sin irrumpir en el servicio. Después de que el CPU carga la versión actualizada de NX-OS, el sistema restablece el plano de control a su configuración previa y a su estado de tiempo y se sincroniza con el plano de datos, completando entonces el proceso ISSU. Ya que el plano de datos continuó mandando paquetes mientras el plano de control se actualizaba, cualquier servidor conectado al switch acceso capa de Cisco Nexus 5000 Series, no deberá mostrar disrupción en el tráfico.

Se utiliza el comando ***"show install all impact***" para identificar al impacto de upgrade. Este comando despliega información que describe el impacto del upgrade así como las versiones actuales y upgrade de la imagen. Este comando también muestra si el upgrade es destructivo, o la razón por la cual e upgrade es destructivo.

La figura 5.6 muestra el uso del comando para el update del software versión 6.0(2)N1(1) de Cisco NX-OS. Las siguientes imágenes son actualizadas durante la instalación:

- ➔ Imagen Kickstart
- ➔ Imagen del Sistema
- ➔ Imagen Fabric Extender
- ➔ Sistema BIOS
- ➔ Secuenciadores de poder en el sistema

```
switch# install all kickstart bootflash:n5000-uk9-kickstart.6.0.2.N1.1.bin system bootflash:n5000-uk9.6.0.2.N1.1.bin
Verifying image bootflash:/ n5000-uk9-kickstart.6.0.2.N1.1.bin for boot variable "kickstart".
...
```

Figura 5.6 Comando para instalar el NX-OS 6.0(2)N1(1) kickstart y el software del sistema

Después del upgrade del sistema, la nueva versión del Software se encuentra ya en uso. Para verificar la nueva versión del software NX-OS se usa el comando “show versión”. Este comando también conoce el archivo de imagen de kickstart y de sistema el modelo del chasis y la memoria interna del CPU, la cual es de 8GB, así como también la memoria bootflash y la última razón del reset. La figura 5.7 muestra la verificación de la nueva versión de software.

```
switch#  sh  version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
        BIOS: versión 3.6.0
        loader: versión N/A
        kickstart: versión 6.0(2)N1(1)
        system: versión 6.0(2)N1(1)
        Power Sequencer Firmware:
                Module 1: versión v1.0
                Module 2: versión v1.0
                Module 3: versión v2.0
        Microcontroller Firmware: versión v1.2.0.1
        SFP uC: Module 1: v1.0.0.0
        QSFP uC: Module not detected
        BIOS compile time: 05/09/2012
        kickstart image file is: bootflash:///n5000-uk9-kickstart.6.0.2.N1.1.bin
        kickstart compile time: 1/29/2013 7:00:00 [01/29/2013 09:40:46]
        system image file is: bootflash:///n5000-uk9.6.0.2.N1.1.bin
        system compile time: 1/29/2013 7:00:00 [01/29/2013 11:44:48]

Hardware
        cisco Nexus5548 Chassis ("O2 32X10GE/Modular Universal Platform Supervisor")
        Intel(R) Xeon(R) CPU with 8262952 kB of memory.
        Processor Board ID FOC16495L4N

        Device name: switch
        bootflash: 2007040 kB
Kernel uptime is 0 day(s), 12 hour(s), 33 minute(s), 37 second(s)
Last reset
        Reason: system upgrade
        System versión: 5.1(3)N1(1a)

        Service:
        plugin
            Core Plugin, Ethernet Plugin, Fc Plugin
```

Figura 5.7 **Verificación de la nueva versión del sistema NX-OS en uso**

5.5.2 Licencia de Nexus

El paquete de software para Cisco Nexus 5000 series ofrece flexibilidad y un set de características integrales, siendo consistente con los switches de acceso de Cisco Nexus. El software de sistema predeterminado posee un set de características Capa 2 integral que contiene características amplias de seguridad y administración. Para habilitar el Capa 3 IP unicast y funciones de routing multicast, es necesario instalar licencias adicionales.
La implementación de Cisco Nexus 5548UP para el Data Center de la empresa de Villahermosa tiene una licencia diferente para Capa 2 y características de almacenamiento, también, para la licencia del Sistema de Administración DCNM-SAN Fabric Manager Server. La tabla 5.4 enlista las licencias disponibles.

Tabla 5.4 Licenciamiento Nexus 5548UP

Licencia	Basado en Chasis o puerto	N° de parte	Características soportadas y plataformas
Cisco Nexus 5500 Storage Protocols Services License, 8 ports	Puerto	N55-8PSSK9	Canal de fibra y FCoE y FCoE NPV características soportadas en cualquier Cisco Nexus 5548 y 5596 de 8 puertos
Cisco Nexus 5500 Layer 3 Enterprise Software License	Chassis	N55-LAN1K9	Full EIGRP, OSPF con escalabilidad de 8000 rutas, BGP, y VRF-lite (IP-VPN); rutas máximas soportadas por hardware de Capa 3: 8000 entradas
Cisco Nexus 55000 VM-FEX Software License	Chassis	N55-VMFEXK9	Cisco Data Center VM-FEX soportado en Cisco Nexus y Cisco Nexus 5596
Cisco Nexus 5548 Enhanced Layer 2 Software License	Chassis	N5548-EL2-SSK9	Cisco FabricPath soportado en Cisco Nexus 5548
Cisco DCNM SAN Software License	Chassis	DCNM-SAN-N5K-K9	Cisco DCNM para edición avancada SAN para Nexus 5000 series
Cisco Nexus 5500 Nexus Storage protocols Services License, 8 ports	Puerto	N55-8P-SSK9	Características de canal de fibra y FCoE y FCoE NPV soportadas en cualquier Cisco Nexus 5548 y 5596 de 8 puertos

Las licencias mostradas previamente en la tabla 5.4 pueden ser instaladas de fábrica, de cualquier manera, es posible realizar la instalación manual de la licencia.
Se firma en el dispositivo a través del puerto de la consola y se realiza la instalación utilizando el comando “install license”. La figura 5.8 muestra dicho comando.

```
switch# install license bootflash: license_file.lic
Installing license ..done
```

Figura 5.8 Comando para instalar la licencia en Nexus

Para desplegar la información sobre el uso de la licencia se utiliza el comando “license usage”. La figura 5.9 muestra el uso del comando license usage.

```
switch# sh license usage
Feature Ins Lic Status Expiry Date Comments
Count
--------------------------------------------------------------------------------
FCOE_NPV_PKG No - Unused            Grace 119D 15H
FM_SERVER_PKG No - Unused -
ENTERPRISE_PKG Yes - Unused Never -
FC_FEATURES_PKG Yes - In use Never -
VMFEX_FEATURE_PKG Yes - Unused Never -
ENHANCED_CAPA2_PKG Yes - In use Never -
LAN_BASE_SERVICES_PKG No - Unused -
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------
```

Figura 5.9 Comando para verificar el uso de la licencia

5.6 Hostname y administración de la dirección IP de Access Nexus Switches.

La tabla 5.5 enlista el Hostname y la administración de la Dirección IP que se usa para cada switch Access Nexus 5548UP. El puerto de administración de Cisco Nexus 5548UP se conecta a una red de administración OOB que brinda servicios esenciales a la red, tales como autenticación de proxys, colecciones de syslogs, colecciones de trampas Simple Network Management Protocol (SNMP) e interconexión a los sistemas de administración tales como Cisco Prime DCNM y el servidor de sincronización (NTP).

Tabla 5.5 Hostname y administración de la dirección IP

Hostname	Dirección IP	Máscara de subnet	Puerta de enlace	VLAN
VHACC554801	172.28.183.3X	255.255.255.0	172.28.18X.254	2087
VHACC554802	172.28.183.3X	255.255.255.0	172.28.18X.254	2087
VHACC554803	172.28.183.3X	255.255.255.0	172.28.18X.254	2087
VHACC554804	172.28.183.3X	255.255.255.0	172.28.18X.254	2087
VHACC554801	172.28.183.3X	255.255.255.0	172.28.18X.254	2087
VHACC554802	172.28.183.3X	255.255.255.0	172.28.18X.254	2087

La interfaz mgmt0 en los dispositivos Cisco NX-OS proporciona administración out-of-band, la cual le permite administrar el dispositivo a través de su dirección IPv4. La interface mgmt0 utiliza Ethernet 10/100/1000 y brinda una conexión predeterminada al contexto de “administración” configurado de vrf, en el Nexus. La figura 5.10 muestra la configuración para la seguridad y administración esenciales de los switches Access Nexus 5548UP.

```
Switch# configuration terminal
Switch(config)# hostname VHACC554801
interface mgmt0
ip address 172.28.183.33/24
vrf context management
ip route 0.0.0.0/0 172.28.183.254
VHACC554801(config)#
```

Figura 5.10 Configuración para el hostname y la dirección IP de administración

Algunos servicios se encuentran habilitados por default como el servidor SSH con una clave de duración 1024-bit. Telnet se deshabilita y se configura el comando "***password strength-check***" para mejores prácticas de seguridad.
Los marcos Jumbo están permitidos en el sistema con un mtu de 9216 bytes. La autenticación AAA se implementará para todos los dispositivos de Cisco en la nueva infraestructura para la Empresa. Los servicios TACACS+ serán proporcionados por un Servidor ACS. Todos los servicios esenciales de administración serán provistos por sistemas localizados en el Data Center de la empresa en Reynosa. La figura 5.11 muestra el comando para verificar el uso de la licencia en Nexus.

```
switch# no feature telnet
feature tacacs+
feature interface-vlan
feature lacp
feature vpc
logging level vpc 6
logging level aaa 5
logging level cdp 6
logging level monitor 6
logging level radius 5
logging level session-mgr 6
logging level spanning-tree 6
logging level tacacs 5
logging level track 6
username admin password 5 $1$YrOlOOqK$eC1Bzc/b0ylfUjrc6nMi4. role network-admin
username vhsnmpuserro password 5 $1$Fq3V4aku$VUT.UPMbkJKnQ2vhKZXb11 role network-
operator
username vhsnmpuserrw password 5 $1$ze558OxL$wCoYo1dTN2U6XJfMESzPt/ role network-
operator
password strength-check
banner motd #
**************************************************************************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access this device. All activities
performed on this device are logged and violations of this policy
result in disciplinary action.
**************************************************************************
#
ip domain-lookup
tacacs-server host 172.20.62.11 key 7 "6bdvx$ozW$"
tacacs-server host 172.20.62.12 key 7 "6bdvx$ozW$"
aaa group server tacacs+ EMPRESA-ACS
server 172.20.62.11
server 172.20.62.12
use-vrf management
source-interface mgmt0
policy-map type network-qos jumbo
class type network-qos class-default
mtu 9216
multicast-optimize
system qos
service-policy type network-qos jumbo
snmp-server contact EMPRESA
snmp-server location Villahermosa Tabasco
snmp-server source-interface trap mgmt0
snmp-server user admin network-admin auth md5 0x990697685a6dc571a1621bcd7cf9d378
priv 0x990697685a6dc571a1621bcd7cf9d378 localizedke
y
snmp-server       user       vhsnmpuserro       network-operator       auth       sha
0x13091d58dcb440751ad02523bfe8ee2c12744125 priv aes-128 0xf46106512ddbfe1605
8c0c8561d499725c86dfc0 localizedkey
snmp-server       user       vhsnmpuserrw       network-operator       auth       sha
0x13091d58dcb440751ad02523bfe8ee2c12744125 priv aes-128 0xf46106512ddbfe1605
8c0c8561d499725c86dfc0 localizedkey
snmp-server host 172.20.62.13 traps version 3 auth vhsnmpuserro
snmp-server enable traps
snmp-server community 5CAcDTiRw group network-admin
snmp-server community 5CAcDTiR group network-operator
ntp server 172.28.183.254 use-vrf management
ntp source-interface mgmt0
aaa authentication login default group EMPRESA-ACS none
aaa authentication login console group EMPRESA-ACS none
aaa accounting default group CIES-ACS
```

Figura 5.11 Comando para verificar el uso de la licencia en Nexus

5.7 Diseño de la red física para acceso

La capa de acceso del Data Center proporciona el nivel físico de anexado a los recursos delservidor, y opera en Capa 2. La capa de acceso juega un rol crítico en cubrir los requerimientos particulares del servidor, tales como NIC teaming, clustering, y broadcast containment. La capa de acceso es el primer punto de sobresuscripción en el Data Center porque conjunta el tráfico del servidor en 10 uplinks Gigabit Ethernet a la capa de conjunto. El diseño propone la implementación de los switches dela capa de acceso en grupos de pares de manera lógica para trabajar con las conexiones redundantes del servidor o para trabajar con diversas conexiones de interfaces Ethernet para producción, respaldo, y administración. La nivel de acceso consiste en switches Nexus 5548UP que se interconectan usando links Ethernet de alta velocidad de 10 GB a los switches de conjunto.

5.7.1 Conexiones físicas

La función principal dela capa de acceso es proporcionar una conexión confiable a los servidores del Data Center.Para lograrlo y para la red de Legacy Ethernet, cada switch Nexus 5548UP utilizará cuatro interfaces dedicadas 10 GigE conectando dos interfaces dedicadas de 10GigE para cada uno de los dos switches de conjunto Nexus 7009. La figura 5.12 muestra el conjunto para Legacy Ethernet.

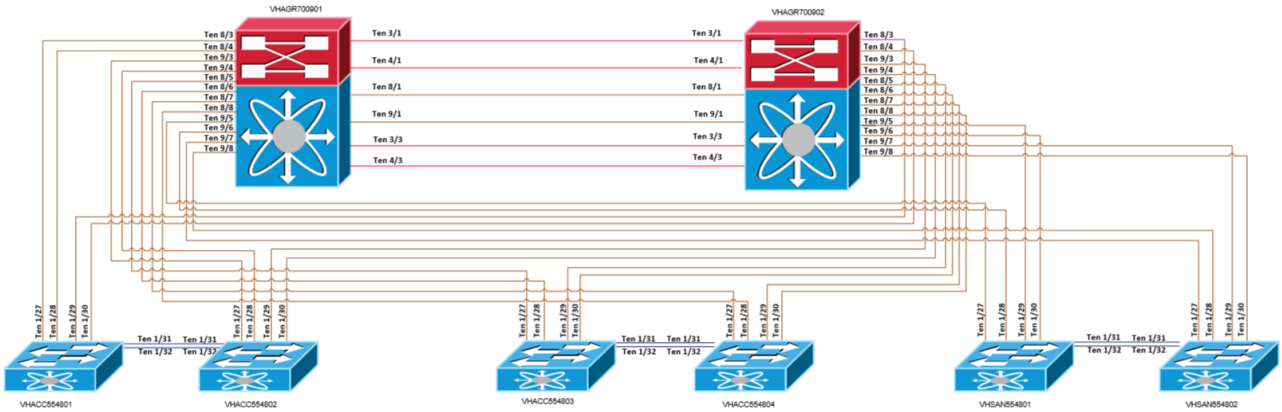


Figura 5.12 Conjunto para Legacy Ethernet de conectividad física de capa de acceso

Cada par de switches Nexus 5548UP estará interconectado espalda-a-espalda usando dos ligas 10 GigE que se utilizan para proporcionar la unión hacia VPC+ Peer-link. Todos los servidores estarán basados de manera doble a los dispositivos de nivel de acceso y serán capaces de sobrevivir a fallas a nivel link o a nivel del dispositivo de red.

Para la red FCoE que se usa para transportar el tráfico Primary Storage, existen dos 10GigE extra utilizado por cada Cisco Nexus 5548UP e interconectar así al "Storage" VDC del switch de conjunto Nexus 7009. El "Storage" VDC del switch de Conjunto "VHAGR700901" se designa como el Fabric A y tiene la responsabilidad de conectar vía FCoE a los switches nones de acceso Nexus 5548UP, y el "Storage" VDC en el switch de Conjunto "VHAGR700902" se designa como Fabric B y tiene la responsabilidad de conectar vía FCoE a los switches pares de acceso Nexus 5548UP, tal y como se muestra en la figura 5.13. Se proporcionará una conexión confiable de los servidores, basada en que cada servidorque estará conectado a cada par de switches de acceso Nexus 5548UP de forma espalda-con-espalda.

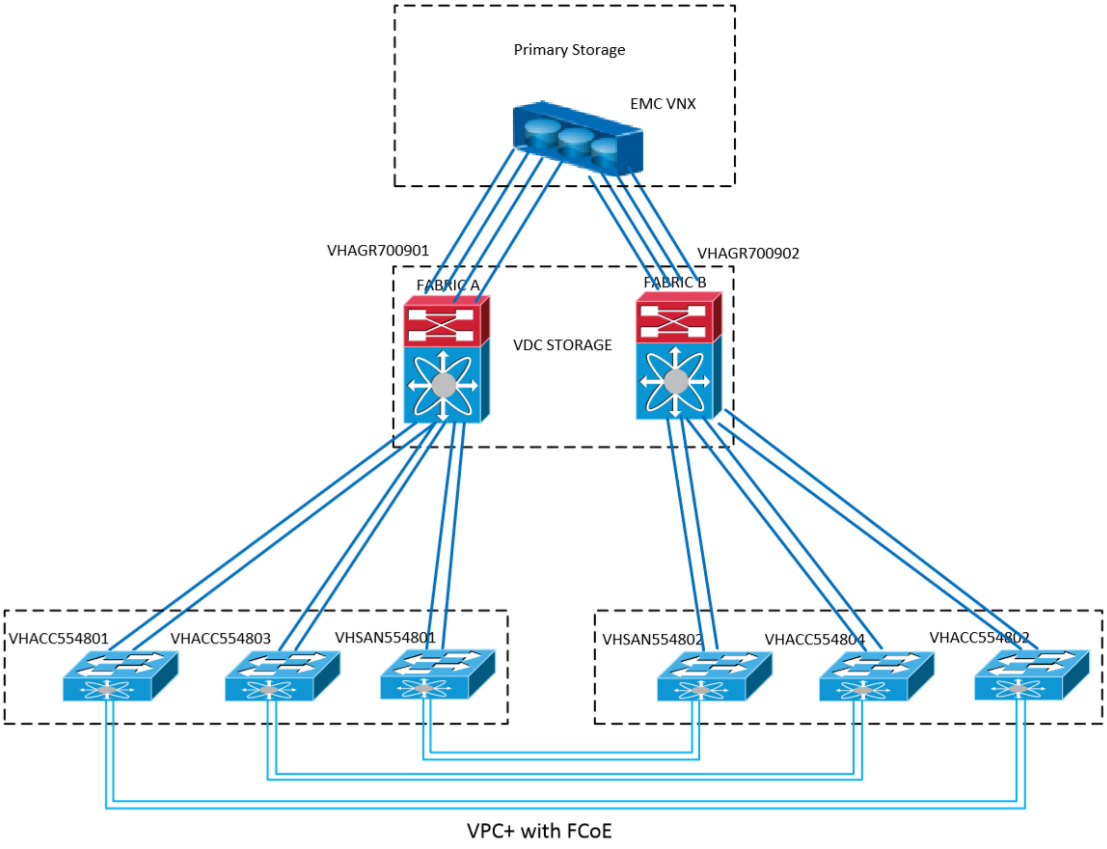


Figura 5.13 Almacenamiento primario FcoE de la Empresa

La figura 5.14muestra el uso de la configuración para los puertos FCoE conectados al sitio de ALMACENAMIENTO (STORAGE) en los switches de conjunto Nexus. La interface "VFC" Virtual Fabric-channel es creada en cada uno de los switches de acceso que se encuentran unidos auna interface Port-channel. Se utiliza Vlan 2083 para "Fabric A" para transportar el tráfico FCoE

utilizando Vsan 10y para “Fabric B” se utiliza Vlan 2084 para transportar el tráfico FCoE utilizando VSAN20.

```
VHACC554801(config)# feature npv
vsan database
vsan 10
vlan 2083
fcoe vsan 10
interface Ethernet1/25
description **** LINK TO VHAGR700901 Ten8/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
interface Ethernet1/26
description **** LINK TO VHAGR700901 Ten9/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
interface port-channel11
description **** FCoE LINK TO VHAGR700901-SAN ****
interface vfc11
bind interface port-channel11
switchport mode NP
switchport trunk allowed vsan 10
switchport description **** FCoE LINK TO VHAGR700901-SAN ****
switchport trunk mode on
no shutdown
VHACC554802(config)# feature npv
vsan database
vsan 20
vlan 2084
fcoe vsan 20
interface Ethernet1/25
description **** LINK TO VHAGR700902 Ten8/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
interface Ethernet1/26
description **** LINK TO VHAGR700902 Ten9/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
interface port-channel22
description **** FCoE LINK TO VHAGR700902-SAN ****
interface vfc22
bind interface port-channel22
switchport mode NP
switchport trunk allowed vsan 20
switchport description **** FCoE LINK TO VHAGR700902-SAN ****
switchport trunk mode on
no shutdown
```

Figura 5.14 **Configuración de interfaces FcoE hacie el contexto Storage (Almacenamiento)**

La tabla 5.6 muestra los puertos utilizados para interconectar la plataforma FCoE.

Tabla 5.6 Puertos Access upstream hacia Storage

Hostname	Interfaz física	Port-Channel/Bind vfc	VLAN/VSAN
VHACC554801	Ethernet1/25 Ethernet1/26	port-channel11/ interface vfc11	VLAN 2083 / VSAN 10
VHACC554802	Ethernet1/25 Ethernet1/26	port-channel22/ interface vfc22	VLAN 2084 / VSAN 20
VHACC554803	Ethernet1/25 Ethernet1/26	port-channel13/ interface vfc13	VLAN 2083 / VSAN 10
VHACC554804	Ethernet1/25 Ethernet1/26	port-channel24/ interface vfc24	VLAN 2084 / VSAN 20
VHSAN554801	Ethernet1/25 Ethernet1/26	port-channel15/ interface vfc15	VLAN 2083 / VSAN 10
VHSAN554802	Ethernet1/25 Ethernet1/26	port-channel26/ interface vfc26	VLAN 2084 / VSAN 20

Como se muestra previamente, existen seis switches Nexus 5548UP que administran lasinterfaces Ethernet y FCoE, en donde dos de estos switches también están dedicados aadministrar interfaces Fabric-Channel, utilizadas para interconectar a la red de almacenamiento(SAN), esta red es mayormente proporcionada por el Switch Cisco MDS9506. Estos dosswitches son identificados por su hostname “VHSAN554801” y “VHSAN554802”. La figura 5.15 muestra la ubicación de los dos switches descritos anteriormente.

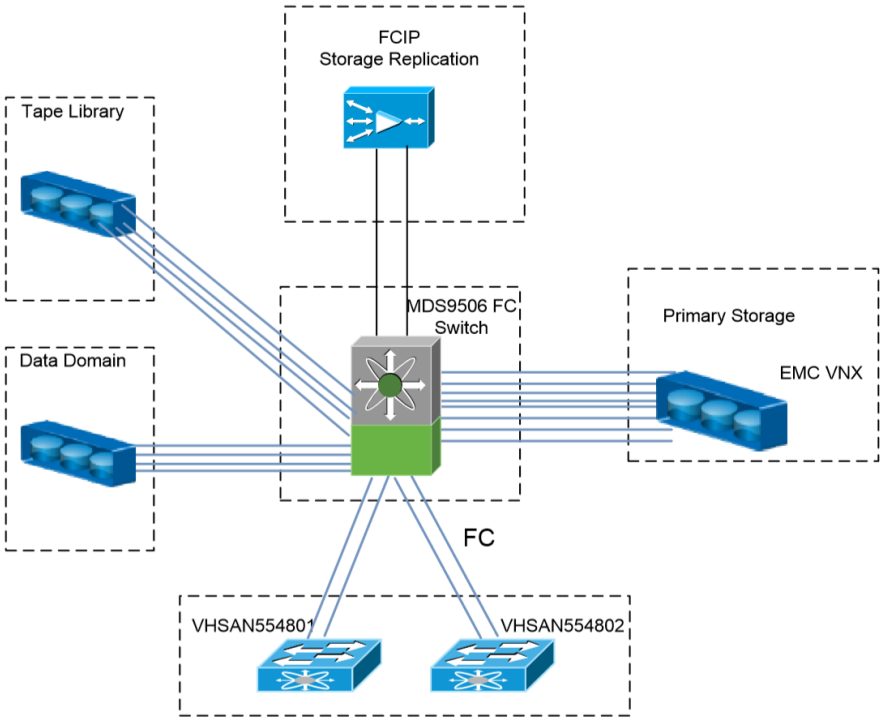


Figura 5.15 Conectividad física, capa FC de acceso para plataforma SAN

Los puertos unificados le permiten configurar puertos como Ethernet, Fiber Channel nativo o Fiber Channel sobre puertos Ethernet (FCoE).Por default, los puertos son puertos Ethernet, pero se puede cambiar el modo del puerto a Fiber Channel o a cualquier puerto en el switch Cisco Nexus 5548UP o los puertos del módulo de expansión Cisco N55-M16UP que se encuentra instalado en los switches Cisco Nexus 5548UP. Para configurar un puerto unificado en switch Cisco Nexus 5548UP, use el comando de puerto. La figura 5.16 muestra la configuración para puertos unificados en Cisco Nexus 5548UP.

```
VHACC554801(config)# slot 1
        Port 31-32 type fc
```

Figura 5.16 Configuración para puertos unificados en Cisco Nexus 55480IP

La siguiente figura, 5.17, muestra el uso de la configuración para los puertos FCoE conectados al nivel "STORAGE" en los switches Nexus de conjunto. Se crea la interface virtual Fabric channel "vfc" en cada uno de los switches de acceso que se encuentran unidos a la interfaceport-channel. Para "Fabric A" se utiliza Vlan 2083 para transportar el tráfico FCoE utilizando Vsan 10, y para "Fabric B" se utiliza Vlan 2084 para transportar el tráfico FCoE usando Vsan 20.

```
VHACC554801(config)# interface fc1/31
switchport trunk mode auto
channel-group 31 force
no shutdown

interface fc1/32
switchport trunk mode auto
channel-group 31 force
no shutdown

interface san-port-channel 31
channel mode active
switchport mode E
switchport trunk allowed vsan 10
switchport description **** FC LINK TO VHSAN950601 ****
switchport speed 4000
switchport trunk mode auto
```

Figura 5.17 Configuración para las interfaces FC

5.7.2 Distribución de rack

El número de servidores que se requieren por rack no es lo suficientemente grande para garantizar el despliegue de los switches TOR o EoR. Cada interface del servidor NIC o HBA será conectada directamente a Cisco Nexus 5548UP, el cual se ubicará en Rack 5, tal y como se muestra en la tabla 5.7

Tabla 5.7 Distribución para rack 5

Distribución de rack	Dispositivo	Función	Hostname
Top	Nexus 5548-1	Acceso	VHACC554801
	Nexus 5548-2	Acceso	VHACC554802
	Nexus 5548-3	Acceso	VHACC554803
	Nexus 5548-4	Acceso	VHACC554804
	Nexus 5548-1	SAN	VHSAN554801
	Nexus 5548-2	SAN	VHSAN554802
	MDS 9506	SAN	VHSAN950601
	WAE 7541	Optimización de tráfico	VHREP754101
Bottom	Catalyst 2960-S	OOB network (Mgmt)	VHADM296005

5.7.3 Asignación del puerto

Como se muestra en la figura 5.2 cada puerto de datos en el switch Cisco Nexus 5548 y los grupos de puertos están numerados basados en su función. Los puertos se numeran de arriba hacia abajo, y de izquierda a derecha.

Los puertos Gigabit Ethernet numerados de arriba hacia abajo, y de izquierda a derecha, comenzando con el puerto 1/1 se encuentra asignado a los servidores y puertos de abajo hacia arriba y de derecha a izquierda, comenzando con puerto 10GB 1/32 son asignados a los dispositivos de interconexión de red tales como la conexión espalda-con-espalda e interconexión upstream con dispositivos de conjunto.

Se deben configurar los puertos Ethernet y FC en un orden específico: Los puertos FC deben ser configurados desde el último puerto del módulo y los puertos Ethernet deben ser configurados desde el primer puerto del módulo. En los dos switches de acceso dedicados para la interconexión SAN, los últimos 4 puertos del chasis se reservan para puertos FC. Entonces, en estos casos la interconexión espalda-con espalda entre los switches SAN son realizados por las primeras interfaces Ethernet (Ethernet 1/1 and Ethernet 1/2).

Se advierte que solo los primeros 4 switches Cisco Nexus 5548UP son proporcionados con el “N55-M16UP”, el cual contiene los 16 puertos reservados para los servidores que requirieron interfaces 10GE Ethernet / FCoE o 8/4/2/1G Fiber-channel.

5.8 Capa 2

Los switches de las capas de Agregación y Acceso establecerán la comunicación L2 por medio de las ventajas de la tecnología Cisco FabricPath. Cisco FabricPath es una innovación en software que combina la simplicidad de plug-and-play de Ethernet con la confiabilidad y escalabilidad del routeode Capa 3. Usando FabricPath, se puede construir redes multipath en Capa 2 de alta escalabilidad sin necesitad de utilizar el protocolo de Spanning-tree. Los enlaces utilizados por los switches Nexus 7009 y el Nexus 5548UP se unirán para formar conexiónes en Capa 2 de FabricPath, en las que los switches Nexus 7009 seran la columna deltallo y los switches Nexus 5548 las hojas.

5.8.1 Distribución VLAN

La capa de Acceso es casi siempre de L2 (Capa 2), en el que las VLANS se utilizan extensivamente. La tabla 5.8muestra el ID de VLANs que serán desplegadas en el Data Center.

Tabla 5.8 ID VLAN utilizada en la capa de Acceso

DESCRIPTION	VLAN	DOMAIN	TYPE
Base de Datos	1801-1900	ACCESS CAPA	FABRICPATH
FW Context	1950-1979	NOT ACCESS CAPA	CE
FW Context	1980-1999	ACCESS CAPA	FABRICPATH
Gestion Eq Comunicaciones	2000-2082	ACCESS CAPA	FABRICPATH
Gestion Eq Comunicaciones	2082-2086	ACCESS CAPA	CE
FCoE implementación	2083-2084	ACCESS CAPA	CE
Gestion Eq Comunicaciones	2085-2086	ACCESS CAPA	FABRICPATH
Gestion	2087-2094	NOT ACCESS CAPA	CE
PI	2401-2500	ACCESS CAPA	FABRICPATH
Respaldos	2501-2600	ACCESS CAPA	FABRICPATH
WEB	2601-2700	ACCESS CAPA	FABRICPATH
Cliente-Servidor (1)	2701-2800	ACCESS CAPA	FABRICPATH
Cliente-Servidor (2)	2801-2900	ACCESS CAPA	FABRICPATH
Legacy	2901-3000	ACCESS CAPA	FABRICPATH
NAS	3001-3100	ACCESS CAPA	FABRICPATH
HPC	3101-3112	ACCESS CAPA	FABRICPATH
HPC	3113-3200	ACCESS CAPA	CE

5.8.2 FabricPath

Con Cisco FabricPath, se puede crear un tejido Ethernet flexible que elimina muchas de las restricciones del Protocolo Spanning-tree. En el plano de control, Cisco FabricPath utiliza un protocolo de ruteo Shortest-Path First (SPF) para determinar el alcance, y selecciona el mejor path (camino) o paths a cualquier destino dado en el dominio de Cisco FabricPath. Además, presenta habilidades que ayudan a asegurar que la red se mantenga estable, y proporciona capacidades de escalabilidad y aprendizaje y reenvío basadas en hardware que no se encuentran ligadas al software o a la capacidad del CPU.

El despliegue de FabricPath para el Data Centerse muestra en la Figura 5.18

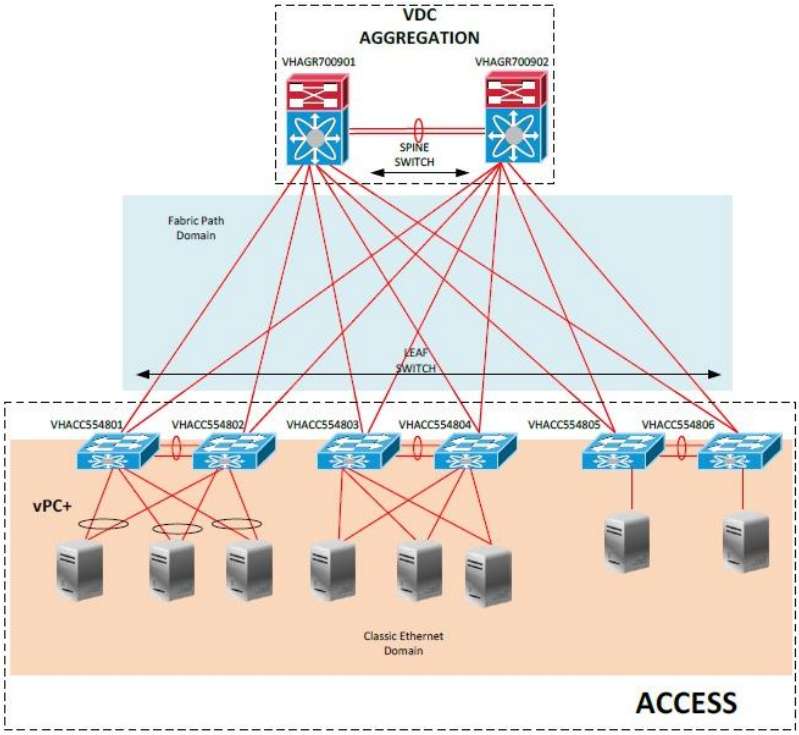


Figura 5.18 Topología de FabricPath

Para habilitar las características de FabricPath en los switches de Acceso Nexus 5548UP, es necesaria la Licencia N5548-EL2-SSK9" (Enhanced Capa 2 license). Esta se debe instalar y habilitar FabricPath antes de que se pueda configurar los componentes que integran al set de características.

Figura 5.19 se muestra los comandos utilizados para instalar y habilitar la característica FabricPath

```
VHACC554801# configuration terminal
VHACC554801(config)# install feature-set fabricpath
feature-set fabricpath
VHACC554801(config)#
```

Figura 5.19 Configuración de características FabricPath

De manera predeterminada, FabricPath asigna un únicoswitch ID después de que este se haya habilitado en el switch. Sin embargo, se puede cambiar manualmente el switch ID si así se prefiere. Para una mejor administración y operación de red, el switch ID se define de la siguiente manera en la tabla 5.9

Tabla 5.9 Switch ID de FabricPath

SYSTEM	SWITCH-ID	TYPE
VHAGR700901	121	STATIC
VHAGR700902	122	STATIC
VHAGR7009-VPC12	1000	EMULATED
VHACC554801	111	STATIC
VHACC554802	112	STATIC
VHACC5548-VPC12	1001	EMULATED
VHACC554803	113	STATIC
VHACC554804	114	STATIC

VHACC5548-VPC34	1002	EMULATED
VHSAN554801	115	STATIC
VHSAN554802	116	STATIC
VHSAN5548-VPC12	1003	EMULATED

El sistema "emulado" es parte de una característica introducida para combinar los beneficios de la combinación entre FabricPah y VPC+.
La configuración de los parámetros del dominio FabricPath y switch ID para el "VHACC5548UP" se muestra en la Figura 5.20

```
VHACC554801# configuration terminal
VHACC554801(config)# fabricpath domain default
spf-interval 50 50 50
lsp-gen-interval 50 50 50
fabricpath switch-id 111
VHACC554801(config)#
```

Figura 5.20 Definiendo el switch ID de FabricPath

Existen dos port-channels definidos en los switches de acceso que contienen, cada uno, dos interfaces Ethernet y son usados como la interconexión upstream hacia la capa de Agregación, como se muestra en la Figura 5. Estos port-channels se definen como la conexión de FabricPath hacia los Switches de Tallo.
Hay también otro par de interfaces que forman un port-channel que interconecte el par consecutivo de equipos Nexus de acceso.
La Figura 5.21 muestra la configuración de estos port-channels para el switch "VHACC554801".

```
VHACC554801# configuration terminal
VHACC554801(config)# interface port-channel3
description **** LINK TO VPC+ Peer-Link ****
switchport mode fabricpath
fabricpath isis metric 200
interface port-channel101
description **** FabricPath LINK TO VHAGR700901
****
switchport mode fabricpath
speed 10000
interface port-channel201
description **** FabricPath LINK TO VHAGR700902
****
switchport mode fabricpath
speed 10000
interface Ethernet1/27
description **** LINK TO VHAGR700901 Ten8/3 ****
switchport mode fabricpath
channel-group 101 mode active
interface Ethernet1/28
description **** LINK TO VHAGR700901 Ten8/4 ****
switchport mode fabricpath
channel-group 101 mode active
interface Ethernet1/29
description **** LINK TO VHAGR700902 Ten8/3 ****
switchport mode fabricpath
channel-group 201 mode active
interface Ethernet1/30
description **** LINK TO VHAGR700902 Ten8/4 ****
switchport mode fabricpath
channel-group 201 mode active
interface Ethernet1/31
description **** LINK TO VHACC554802 Ten1/31 ****
switchport mode fabricpath
```

```
channel-group 3 mode active
interface Ethernet1/32
description **** LINK TO VHACC554802 Ten1/32 ****
switchport mode fabricpath
channel-group 3 mode active
VHACC554801(config)#
```

Figura 5.21 Configuración de port-channel para la interconexión FabricPath

La tabla 5.10 Muestra las interfaces de los equipos de Acceso que intervienen en Fabric-path

Tabla 5.10 Interfaces para Acceso FabricPath

Dispositivo	Interface	Dispositivo	Interface	Port-channel
VHACC554801	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet8/3 Ethernet8/4	port-channel101
VHACC554801	Ethernet1/29 Ethernet1/30	VHAGR700902	Ethernet8/3 Ethernet8/4	port-channel201
VHACC554801	Ethernet1/31 Ethernet1/32	VHACC554802	Ethernet1/31 Ethernet1/32	port-channel3
VHACC554802	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet9/3 Ethernet9/4	port-channel102
VHACC554802	Ethernet1/29 Ethernet1/30	VHAGR700902	Ethernet9/3 Ethernet9/4	port-channel202
VHACC554802	Ethernet1/31 Ethernet1/32	VHACC554801	Ethernet1/31 Ethernet1/32	port-channel3
VHACC554803	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet8/5 Ethernet8/6	port-channel103
VHACC554803	Ethernet1/29 Ethernet1/30	VHAGR700902	Ethernet8/5 Ethernet8/6	port-channel203
VHACC554803	Ethernet1/31 Ethernet1/32	VHACC554804	Ethernet1/31 Ethernet1/32	port-channel3
VHACC554804	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet8/7 Ethernet8/8	port-channel104
VHACC554804	Ethernet1/29 Ethernet1/30	VHAGR700902	Ethernet8/7 Ethernet8/8	port-channel204
VHACC554804	Ethernet1/31	VHACC554803	Ethernet1/31	port-channel3

	Ethernet1/32		Ethernet1/32	
VHSAN554801	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet9/5 Ethernet9/6	port-channel105
VHSAN554801	Ethernet1/3 Ethernet1/4	VHAGR700902	Ethernet9/5 Ethernet9/6	port-channel205
VHSAN554801	Ethernet1/31 Ethernet1/32	VHSAN554802	Ethernet1/1 Ethernet1/2	port-channel3
VHSAN554802	Ethernet1/27 Ethernet1/28	VHAGR700901	Ethernet9/7 Ethernet9/8	port-channel105
VHSAN554802	Ethernet1/3 Ethernet1/4	VHAGR700902	Ethernet9/7 Ethernet9/8	port-channel205
VHSAN554802	Ethernet1/31 Ethernet1/32	VHSAN554801	Ethernet1/1 Ethernet1/2	port-channel3

FabricPath construye dos árboles multidestino con dos raíces diferentes: una para FTag 1 y otra para FTag2. En Capa2, el tráfico multicast es encriptado a alguno de los árboles para que los dos sean utilizados. La encriptación a cualquiera de los árboles multidestino depende de la plataforma, por ejemplo, puede incluir el campo VLAN o el campo de la dirección IP.
Con el fin de maximizar la eficiencia en la distribución de tráfico, es recomendable establecer de manera manual la ruta prioritaria de la raíz para Ftag1 y FTag2.

Cuando se configure FabricPath Forwarding, solamente aquellos VLANS que estén configurados como FP VLANs pueden pertenecer a la topología FabricPath. De manera predeterminada, todos los FP VLANs e interfaces están asignados a la topología FabricPath, FabricPath topo 0.
Cuando se utiliza la topología predeterminada, necesita solamente establecer el modo VLAN para aquellas VLANs que quiere que atraviesen la red FabricPath hacia el FP VLAN.
Debido a que el sistema crea de manera automática los múltiples caminos, una vez que ha especificado los modos e interfaces VLAN, solo se requiere configurar estos aspectos de FabricPath. Usted designa aquellos VLANs que quiere carguen el tráfico FabricPath en la red por medio de su configuración como FP VLANs. Por default, todas las VLANS e interfaces FabricPath, son añadidas a la topología FabricPath.
Con base en la asignaciónde VLAN, mostrada en la Tabla 5.20 la Figura 5.22representa el modo FabricPathconfigurado para las VLAN de los equipos de Acceso.

```
VHACC554801# vlan 1801-1900,1980-2082,2085-2086,2088-2091,2401-3112
mode fabricpath
VHACC554801(config)#
```

Figura 5.22 Configuración de modo VLAN FabricPath

5.8.3 Conexión de acceso de almacenamiento primario con FCoE

Fiber Channel over Ethernet (FCoE) es la próxima evolución de la creación de redes Fiber Channel y del modelo de conectividad en bloques de almacenamiento Small Computer System Interface (SCSI). FCoE mapea Fiber Channel hacia Capa2 Ethernet, permitiendo la combinación del tráfico LAN y SAN hacia un enlace y habilitando a los usuarios de SAN para que puedan tomar ventaja de la economía de escala, comúnidad robusta y el roadmap de Ethernet. La combinación del tráfico LAN y SAN en un enlace se denomina unified fabric. Unified fabric elimina adaptadores, cables y dispositivos, resultando en ahorros que pueden extender la vida del Data Center. FCoE potencializa las iniciativas de virtualización del servidor con la disponibilidad del servidor estándar I/O, el cual funciona con LAN y todas las formas de almacenamiento en red basadas en Ethernet, eliminando redes especializadas del Data Center.

Actualmente Nexus 5548UP funciona con Unified I/O, ayudan a FCoE a transportar el tráfico Fiber Channel y Ethernet en un transporte Ethernet del Data Center. La tecnología Unified I/P reduce mucho los requerimientos de cableo masivo por medio de la utilización de la misma infraestructura física de transporte para las dos comunicaciones LAN y SAN.
Los switches de acceso en el Data Center en Villahermosa, habilitan FCoE y después las características NPV para el despliegue de Storage.- este método requieren que se habilite FCoE, primero utilizando el comando de características FCoE y después habilite NPV utilizando el comando de características npv. Cuando FCoE se encuentre habilitado, el modo de operación predeterminada es switching FC, y cuando se habilite NPV, el modo cambia a modo NPV. El cambio a modo NPV, automáticamente realiza un write erase y recarga el sistema. Después de la recarga, el sistema aparece en modo NPV. Para salir del modo NPV y regresar al modo switching FC, se introduce el comando no feature npv. El modo NPV existente también desencadena un borrado de escritura y una recarga del switch. Este método requiere la licencia Storage Protocols Services Package (FC_FEATURES_PKG). En la figura 5.23 Se muestra la configuración de habilitación de FCOE y NPV.

```
VHACC554801# feature fcoe
feature npv
VHACC554801(config)#
```

Figura 5.23 Habilitando FcoE y la característica NPV

Como se muestra en la Figura 5.24, los VLAN 2083 y VLAN 2084 son utilizados por los servidores para transportar el tráfico FCoE; estos VLANs existen en el VDC “Almacenamiento” en los switches de Agregación. Y los vsan relacionados para el FCoE son VSAN 10 and VSAN 20 respectivamente, para cada uno de los caminos hacia VDC Almacenamiento.

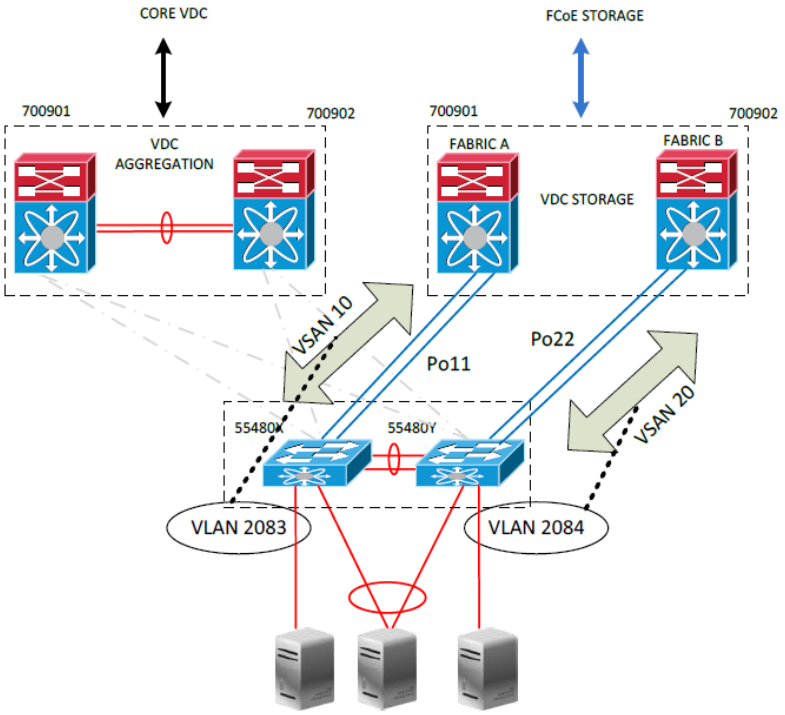


Figura 5.24 Conectividad FCoE de la plataforma de almacenamiento

Se configura un port-channel en cada uno de los switches de acceso para enlazar las dos conexiónes upstream hacia el VDC Almacenamiento, y posteriormente, se ligan a las interfaces vfc correspondidas que pertenecen al VSAN 10 o al VSAN 20, dependiendo del camino utilizado. La figura 5.25 Muestra la configuración del equipo de Agregacion primario FCOE

```
VHACC554801# vlan 2083
fcoe vsan 10
vsan database
vsan 10
interface port-channel11
description **** FCoE LINK TO VHAGR700901-SAN ****
switchport mode trunk
switchport trunk allowed vlan 2083
interface vfc11
bind interface port-channel11
switchport mode NP
switchport trunk allowed vsan 10
switchport description **** FCoE LINK TO VHAGR700901-SAN ****
switchport trunk mode on
no shutdown
interface Ethernet1/25
description **** LINK TO VHAGR700901 Ten8/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
interface Ethernet1/26
description **** LINK TO VHAGR700901 Ten9/11 ****
switchport mode trunk
switchport trunk allowed vlan 2083
channel-group 11 mode active
VHACC554801(config)#
```

Figura 5.25 Configuración del equipo Agregación primario FCoE en la capa de Acceso

5.8.4 VPC+ conectividad del servidor

La topología del Data Center en Villahermosa posee solamente Cisco Nexus 5548UP en el módulo de acceso. Los servidores formarán una VPC+ con los dos Nexus 5548UP.
En el caso de los despliegues de Unified Fabric (Fiber Channel over Ethernet [FCoE]), es importante distinguir los Host VPCs de 4+ puertos, de los Host VPCs de 2 Puertos como se presenta en lafigura 5.26. Para que FCoE pueda funcionar, el adaptador del servidor necesita visualizar dos tejidos Fiber Channel separadas.

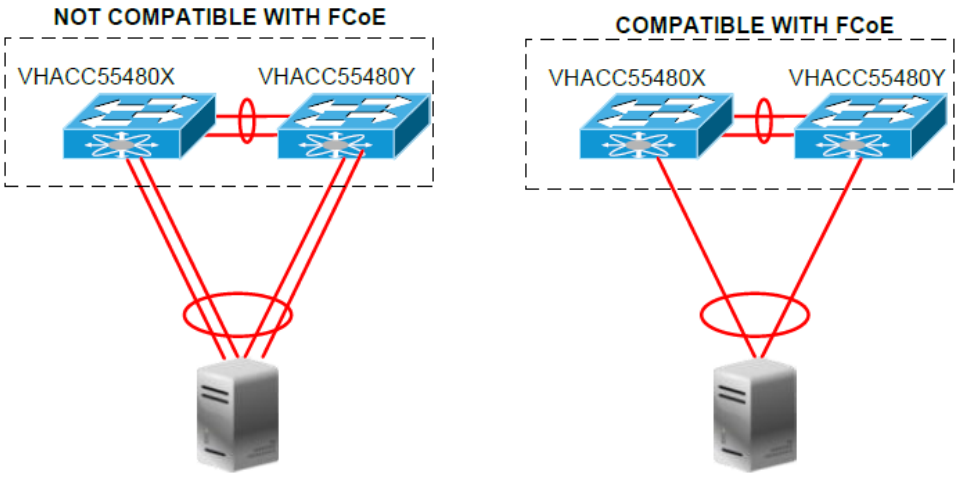


Figura 5.26 4 Puertos vPC y 2 puertos vPC y FCoE

La conexión ala capa de acceso puede ahora ser implementada como un Port-channel virtual librede loop. Ya no es necesario que Spanning-tree bloqueé cualquier puerto en esta topología libre de loop.
Cada servidor será conectado double enlace upstream a los switches de Acceso Nexus 5548UP. Cada par de Switches Nexus 5548UP que acogen la conectividad redundante a los servidores, se configuran para funcionar con VPC+ y proporcionan la utilización de recursos de conexión máxima y simple.
Para configurar una interconexión redundante VPC+ hacia un servidor se aplica el procedimiento que se muestra a continuación.
Primero es necesario crear el dominio VPC, la configuración de la administración de la Dirección IP se configura como el destino de la Dirección IP “peer-keepalive”, y el Po3 como el “vpc-peer-link”, como se muestra en la figura 5.27. El switch-id FabricPath emulado se define para la característica VPC+.

```
VHACC554803# vpc domain 201
role priority 110
peer-keepalive destination 172.X.X.X
fabricpath switch-id 1002
interface port-channel3
description **** LINK TO VPC+ Peer-Link ****
vpc peer-link
VHACC554804# vpc domain 201
peer-keepalive destination 172.X.X.X
fabricpath switch-id 1002
interface port-channel3
description **** LINK TO VPC+ Peer-Link ****
vpc peer-link
VHACC554804(config)#
```

Figura 5.27 Configurando el dominio vPC

Posteriormente, el Vsan 10 y el Vsan 20 son definidos para el transporte upstream del tráfico FCoE, y las vlan de acceso 2083 y 2084 son asignadas para unirse a la Vsan previamente creada, como se muestra en la figura 5.28

```
VHACC554803# vsan database
vsan 10
vlan 2083
fcoe vsan 10
VHACC554803(config)#
VHACC554804# vsan database
vsan 20
vlan 2084
fcoe vsan 20
VHACC554804(config)#
```

Figura 5.28 Definiendo los IDs para VSAN y VLAN

Finalmente, la unión del port-channel se crea hacia el vpc y se liga hacia las interfaces FC que pertenecen a la Vsan correspondiente, como se muestra en la figura 5.29

```
VHACC554803# interface port-channel301
description **** vPC+ TO Server 10G FCoE Ten2/1 ****
switchport mode trunk
switchport trunk allowed vlan 2083,3103
vpc 301
interface Ethernet2/1
description **** LINK TO Server 10G FCoE Ten ****
switchport mode trunk
switchport trunk allowed vlan 2083,3103
spanning-tree port type edge trunk
channel-group 301 mode active
interface vfc301
bind interface port-channel301
switchport trunk mode on
no shutdown
vsan database
vsan 10 interface vfc301
VHACC554804# interface port-channel301
description **** vPC+ TO Server 10G FCoE Ten2/1 ****
switchport mode trunk
switchport trunk allowed vlan 2084,3103
vpc 301
interface Ethernet2/1
description **** LINK TO Server 10G FCoE Ten ****
switchport mode trunk
switchport trunk allowed vlan 2084,3103
spanning-tree port type edge trunk
channel-group 301 mode active
interface vfc301
bind interface port-channel301
switchport trunk mode on
no shutdown
vsan database
vsan 20 interface vfc301
VHACC554804(config)#
```

Figura 5.29 Configuración de vPC+ para conexiones del servidor

5.8.5 Recomendaciones para interconexión del servidor FCoE.

Hay algunas recomendaciones disponibles para lograr una interconexión exitosa entre un Switch Cisco y un servidor con interfaces FCoE. Para el servidor se pueden seguir las siguientes recomendaciones:

- ➔ Verificar y actualizar, si aplica el software firmware del Administrador Onboard del Chasis HP
- ➔ Habilitar la característica FCoE en el HP CNA desde el BIOS

Para un Chasis HP C7000:

- ➔ HP Onboard Administrator firmware: 3.21
- ➔ Pass-Thru firmware: 1.0.7.0

Para HP BL465 G7 Blade Server

- ➔ System ROM: A19
- ➔ iLO3 firmware: 1.10

Adaptador de red HP NC551i Dual Port FlexFabric 10Gb (CNA LoM)

- ➔ Windows 2008 Server (64-bit) Network driver: 2.102.517.0
- ➔ Windows 2008 Server (64-bit) FCoE driver: 7.2.33.8
- ➔ Windows 2008 Server (64-bit) firmware (bootcode): 2.702.517.7
- ➔ Windows 2008 Server (64-bit) Teaming driver: 10.20.0.0

Adaptador de red HP NC551m Dual Port FlexFabric 10Gb (CNA Mezzanine)

- ➔ Windows 2008 Server (64-bit) Network driver: 2.102.517.0
- ➔ Windows 2008 Server (64-bit) FCoE driver: 7.2.33.8
- ➔ Windows 2008 Server (64-bit) firmware (bootcode): 2.702.485.4
- ➔ Windows 2008 Server (64-bit) Teaming driver: 10.20.0.0

La Figura 5.30 muestra un ejemplo del procedimiento a seguir para habilitar la característica FCoE en un Servidor NIC HP.

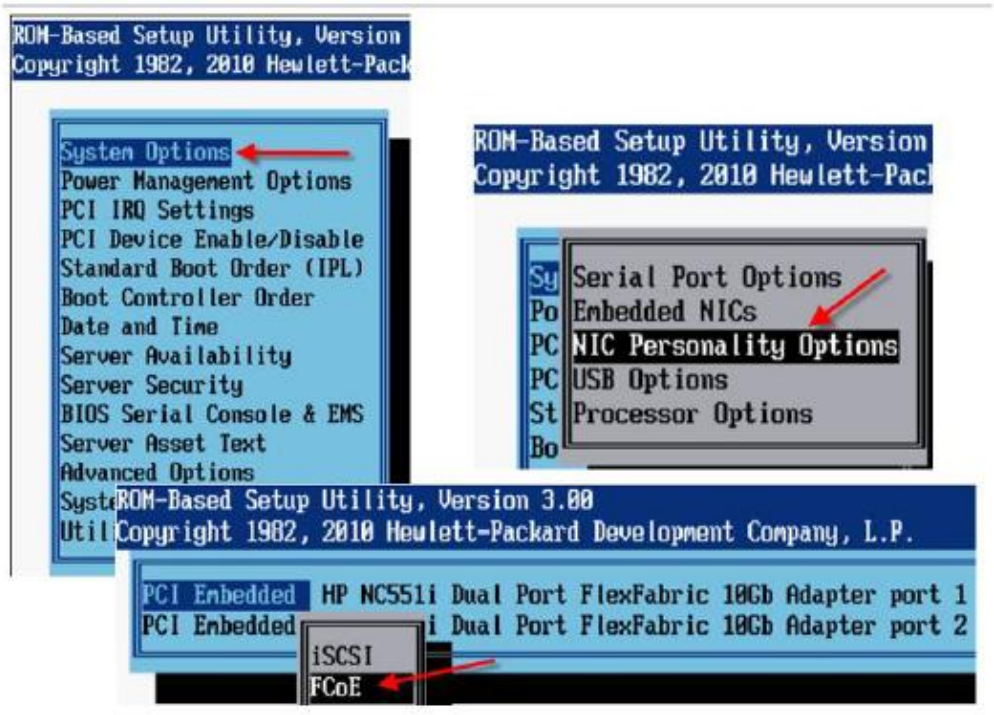


Figura 5.30 Procedimiento a seguir para habilitar la característica FCoE en un servidor NIC HP

5.8.6 Solución de CITRIXCloud

Existe un requerimiento de CITRIX para proporcionar la conectividad de Capa dentro de las redes de las granjas de servidores. Tomando esto en cuenta, CITRIX recomienda que todos los puertos de acceso se configuren en modotrunk, dando permiso a todas las vlans en la cloud del Data Center, y el uso de la vlan nativa predeterminada (vlan 1), es decir, que no habrá una vlan removiendo, en la capa de acceso de conjunto. La Figura 5.31 muestra la topología lógica que se utiliza para interconectar la solución de CITRIX cloud a la nivel de Acceso y Agregación.

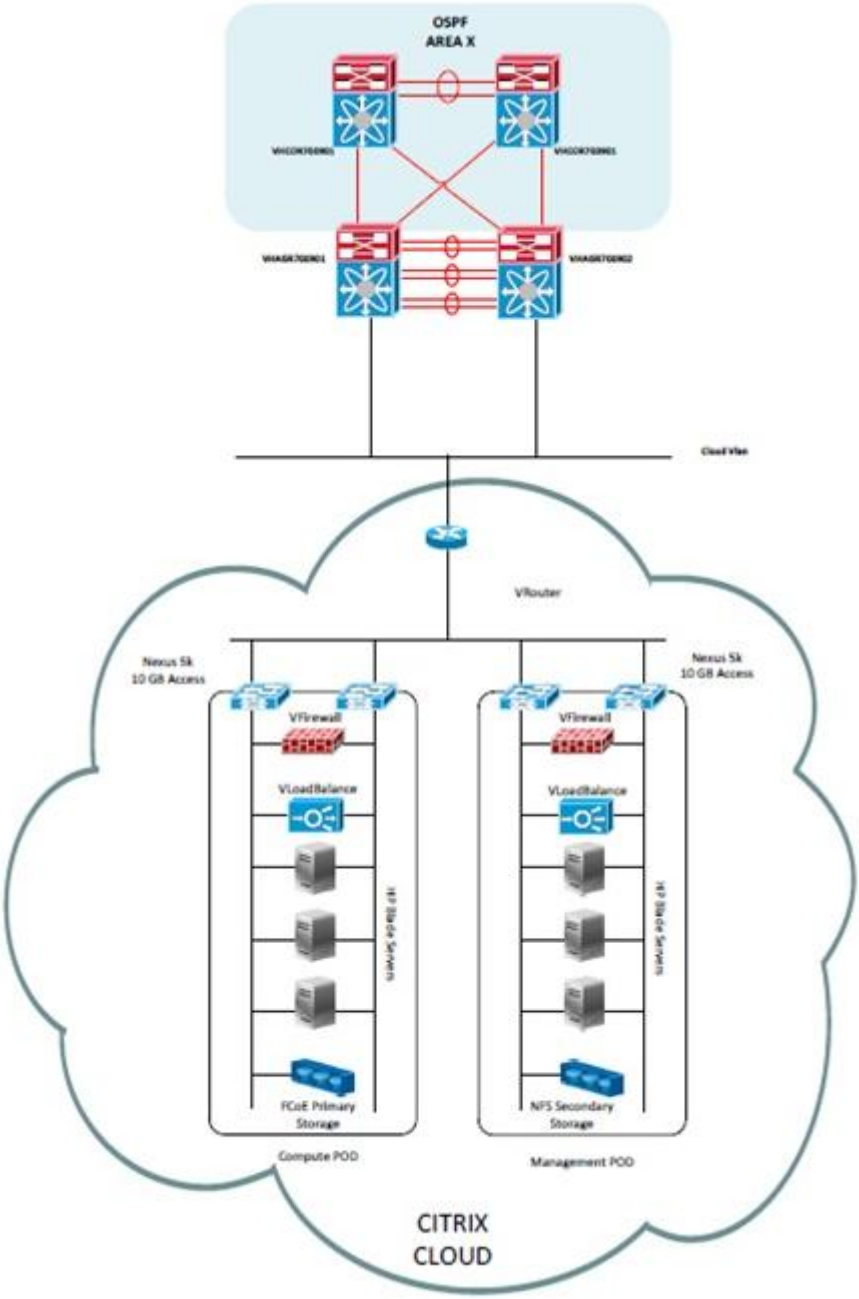


Figura 5.31 Interconexión de la capa de Acceso para la solución CITRIX cloud

Capítulo 6: Servicios

6.1 Topología de la red de servicios

En esta sección se proporciona la arquitectura de enrutamiento y conmutación del Data Center de Villahermosa. Los dispositivos utilizados son un par de switchesCatalyst6509, que se implementan sólo como dispositivos de capa 2. La Capa 3 esta conformada por los dispositivos de firewall y los switches Nexus.

La figura 6.1 muestra una topología general de servicios:

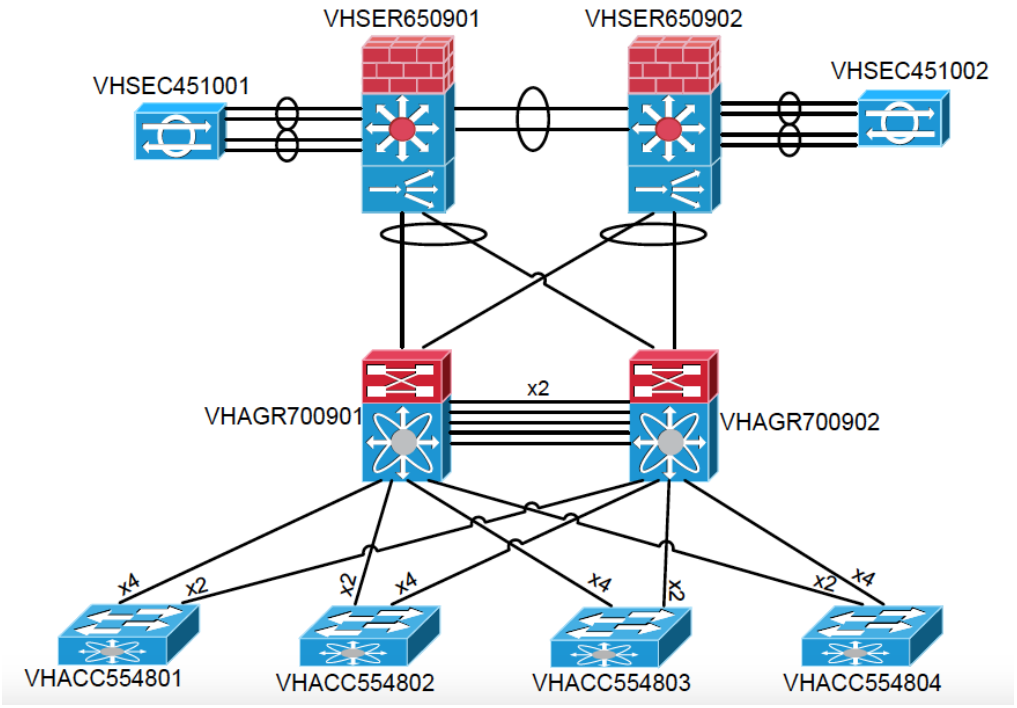


Figura 6.1 Descripción general de la topología de la red de servicios

Nota:

La etiqueta x(n) en la topología representa el número de enlaces conectados bajo un único enlace lógico.

6.2 Diseño de Capa 2

En esta sección se describirá la configuración de la Capa 2 (Desde las VLANs hasta los protocolos VTP, STP, etcétera. Este capítulo provee las configuraciones de los dispositivos y la información necesaria para hacerlo.

6.2.1 VLAN

Múltiples VLANs fueron incluidas en el diseño, cada una de ellas con una función específica dentro de los nivelesen las que están siendo propagadas. Los niveles en esteData Center son:

1. Web
2. Base de datos
3. Aplicación
    - ➔ Cliente-Servidor 1
    - ➔ Cliente-Servidor 2
    - ➔ Legalidad
    - ➔ PI
    - ➔ Respaldos
    - ➔ HPC
    - ➔ Citrix Lab

Además, hay diferentes escenarios, que son:

1. Firewall, balanceo de carga e IPS
2. Firewall y balanceo de carga
3. Firewall e IPS
4. Firewall sólo
5. No hay servicios

Nota:

En el caso del tráfico que va a la Citrix cloud, los serviciosno son utilizados. Algunas de estas aplicaciones sólo pueden utilizar IDS.

La figura 6.2 ilustra los escenarios mencionados anteriormente, nótese como las VLANs son mapeadas dependiendo del dispositivo que atraviesan.

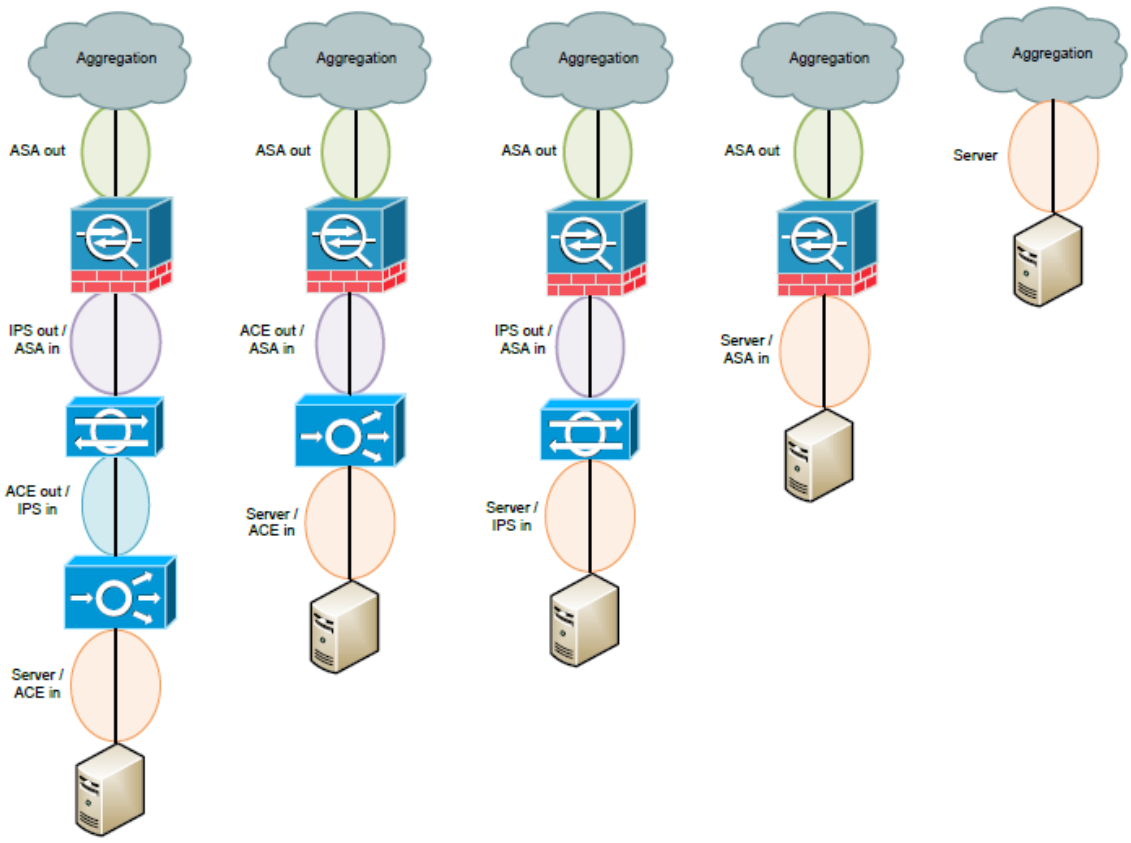


Figura 6.2 Mapeo de VLANs

La tabla 6.1 muestra la distribución de VLAN para cada nivel.

Tabla 6.1 Distribución de VLANs po nivel

Nivel	Rango de VLAN	Red
Web	2601 – 2700	172.28.178.0/24
Base de Datos	1801 – 1900	172.28.179.0/24
Aplicación (Cliente-Servidor 1)	2701 – 2800	172.28.180.0/24
Aplicación (Cliente-Servidor 2)	2801 – 2900	172.28.181.0/24
Aplicación (Legalidad)	2901 – 3000	172.28.175.0/24
Aplicación (PI)	2401 – 2500	172.28.176.0/24
Aplicación (Respaldos)	2501 – 2600	172.28.177.0/24
HPC	3101 – 3200	172.28.186.0/24
Citrix Lab	3201 – 3300	172.28.187.0/24

6.2.2 VTP

VTP (VLAN Trunking Protocol) es un protocolo usado para configurar y administrar VLANs en equipos CISCO, permite la propagación automática de VLANs a través de los diferentes switches dentro del mismo dominio. VTP está disponible en la mayor parte de la serie de switches Cisco Catalyst.

VTP se puede configurar en 3 modos diferentes, los cuales se describen a continuación:

- ➔ Servidor: Permite crear, modificar y eliminar redes VLAN, así como también especificar otros parámetros como la versión VTP. Los servidores VTP anuncian la configuración de las VLAN. Este es el modo predeterminado.
- ➔ Cliente: Se comporta de la misma manera que los servidores VTP, pero las VLANs no se pueden crear, cambiar o modificar. El cliente está a la espera de lo que anuncia el servidor VTP.
- ➔ Transparente: No participa en VTP. Por lo tanto, no manda mensajes de advertencias o sincroniza su base de datos de VLANs. Sin embargo, los switches en modo transparente reenvían los mensajes VTP que reciben de otros switches.

Mientras VTP puede reducir los esfuerzos de la administración, también puede dar lugar a importantes problemas si se elimina una VLAN. En el Data Center de uno de los sitios, el protocolo VTP está configurado en modo transparente. Además, el nombre de host del dispositivo se utiliza como dominio VTP.

La tabla 6.2 muestra los parámetros de configuraciones que deben aplicarse al protocolo VTP en uno de los Data Center para los switches de servicios:

Tabla 6.2 **VTP resumen**

Modo VTP	Transparente
Dominio VTP	Nombre del host
Versión VTP	2 (Por defecto)
Contraseña VTP	******** (Por lo menos 8 caracteres)

La figura 6.3 muestra un ejemplo de la configuración del protocolo VTP. Teniendo en cuenta que los valores actuales se deben modificar de acuerdo con los datos reales.

```
vtp domain VHSER650901
vtp mode transparent
vtp password HvN#&!95ab1L
```

Figura 6.3 **Configuración VTP**

6.2.3 STP

El Protocolo Spanning-tree permite crear topologíasL2 redundantes, mediante el bloqueo de los puertos que crean un bucle L2. Los dispositivos de Cisco utilizan VLAN STP (protocolo propiedad de Cisco), esto significa que las instancias de STP son para una VLAN en particular, lo que permite una mayor flexibilidad en el diseño.

VHSER650901 y VHSER650902 utilizan el protocolo Rapid Per VLAN Spanning-tree Protocol (RPVSTP).

La figura 6.4 muestra la configuración necesaria para habilitar RPVSTP:

```
spanning-tree mode rapid-pvstp
spanning-tree extend system-id
```

Figura 6.4 Configuración RPVSTP

Nota:

Debido a que el Fabric Path de las VLANs raíces son dispositivos Nexus 7009 de dominio, los switches Cat6509 son la prioridad por defecto.

6.2.4 VLAN Troncal

Una VLAN Troncal permite transportar el tráfico de múltiples VLANs a través de una capa de 2 enlaces punto-a-punto. Esta VLAN Troncal en dispositivos de conmutación utiliza la encapsulación 802.1Q (dot1q), que es un estándar IEEE y que permite a múltiples redes compartir de forma transparente el mismo medio físico.

Desde una perspectiva de seguridad, la VLAN Troncal en un Data Center usa VLAN 999 y VLAN nativa.

De forma predeterminada, la VLAN 1 es la VLAN nativa, sin embargo, es una buena práctica utilizar una VLAN diferente y sin usar, con el fin de evitar los ataques de salto de VLAN.

Adicionalmente a lo mencionado anteriormente, EL DTP (protocolo de enlace troncal dinámico) se desactiva en un Data Center.

La tabla 6.3muestra el resumen para un truncamiento detallado:

Tabla 6.3 Resumen troncal

Encapsulado	802.1Q
VLAN nativa	999
DTP	Deshabilitado

La figura 6.5 muestra los comandos para configurar los enlaces troncales de las VLANs bajo una interfaz de configuración.

```
Interface#<interface type>#<ifSlot/ifPort>
#switchport
#switchport trunk encapsulation dot1q
#switchport trunk native VLAN <VLANID>
#switchport trunk allowed VLAN <VLANID>
#switchport mode trunk
#switchportnonegotiate
```

Figura 6.5 Configuración troncal

Nota:

La MTU (Unidad de Transmisión Máxima) para todos los puertos troncales fueron cambiados para soportar los marcos "Jumbo" de 9216 bytes.

6.2.5 Etherchannel

EtherChannel permite agrupar múltiples enlaces físicos en un único enlace lógico. La ventaja de usar etherchannel es el aumento de ancho de banda mediante el intercambio de la carga de tráfico a través de los diferentes enlaces físicos, así como la redundancia en caso de que uno de los enlaces físicos falle.

Nota:

El balanceo de carga en etherchannel no es necesariamente igual en todos los enlaces, ya que no utiliza la metodología round-robin como resultado de un hash, se basa principalmente en los patrones de tráfico de carga.

La tabla 6.4 muestra la configuración etherchannel así como los pares de dispositivos.

Tabla 6.4 Configuraión Etherchannel

Puerto – canal	Dispositivo	Interfaz	Dispositivo	interfaz
1	VHSER650901	Ten4/4 Ten7/4	VHSER650902	Ten4/4 Ten7/4
2	VHSER650901	Ten4/1 Ten7/1	VHSER650902	Ten3/8 Ten3/8
3	VHSER650901	Ten4/2 Ten4/3	VHSER650902	Ten0/6 Ten0/7
4	VHSER650901	Ten7/2 Ten7/3	VHSER650902	Ten0/8 Ten0/9
1	VHSER650902	Ten4/4 Ten7/4	VHSER650901	Ten4/4 Ten7/4
2	VHSER650902	Ten4/1 Ten7/1	VHSER650901	Ten4/8 Ten4/8
3	VHSER650902	Ten4/2 Ten4/3	VHSER650901	Ten0/6 Ten0/7
4	VHSER650902	Ten4/4 Ten7/4	VHSER650901	Ten0/8 Ten0/9

El diagrama 6.6 ilustra cómo están distribuidos los etherchannel.

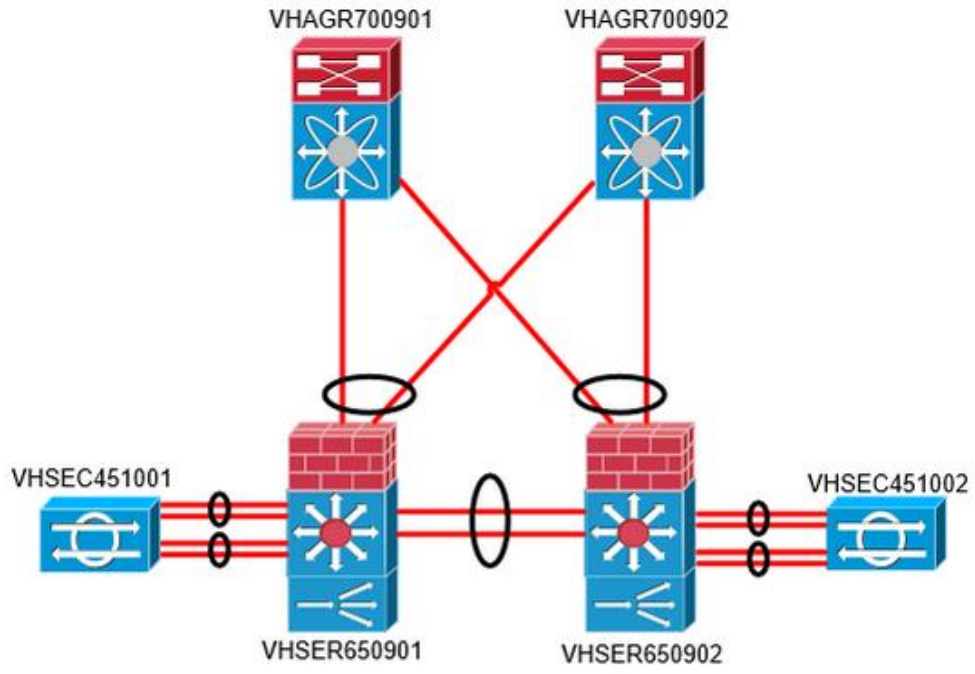


Figura 6.6 Distribución Etherchannel

La figura 6.7 muestra un ejemplo de configuración de Etherchannel.

```
interface Port-channel <ifSlot/ifPort>
description¡<Etherchannel to xxxx>
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 999
switchport trunk allowed VLAN <VLANID>
switchport mode trunk
¡¡¡¡¡¡¡switchportnonegotiate
```

Figura 6.7 Configuración Etherchannel

La figura 6.8 muestra la configuración para el balanceo de cargas en los etherchannels.

```
port-channel load-balance src-dst-ip exclude vlan
```

Figura 6.8 Configuración del balanceo de carga para Etherchannel

6.2.6 SPAN

Switched Puerto Analyzer (SPAN) permite el envío de una copia del tráfico de una interfaz o VLAN a otro puerto del switch. SPAN no afecta a la conmutación del tráfico de red en los puertos de origen. Excepto para el tráfico que se requiere para la sesión de SPAN, puertos de reflector y de destino no reciben o reenvíen tráfico.

SPAN se utiliza en VHSER650901 y VHSER650902 para enviar la copia del tráfico a sus respectivos sistemas de IPS (cuando se trabaja como IDS). Para obtener mayor información, en la sección de seguridad de este documento para obtener más detalles sobre la operación IDS.

La figura 6.9 muestra la configuración para SPAN.

```
monitor session <session_id> source interface <interface>
monitor session <session_id> destination interface <interface>
```

Figura 6.9 Configuración SPAN

Capítulo 7 Interconexión del Data Center

7.1 OTV

En el diseño del Data Center Interconect (DCI) para el Data Center de la cloud, se utilizará una OTV para interconectar los tres Data Center (Villahermosa, Poza Rica y Reynosa). Algunos de los beneficios de utilizar OTV, en lugar de otras tecnologías de extensión Capa 2, se mencionan a continuación:

- ➔ No se necesita el despliegue de EoMPLS o VPLS
- ➔ Proporciona conectividad Capa 2 y Capa 3, potencializando las mismas conexiónes de medios.
- ➔ Aislamiento STP Nativo: no se requiere configurar el filtrado BPDU de manera explícita
- ➔ Aislamiento de la inundación Unicast Nativa Desconocida: unicast desconocida no mandada al Overlay
- ➔ Optimización de ARP con el Cache OTV ARP
- ➔ Aprovisiónamiento simplificado de aislamiento FHRP
- ➔ Fácil adición de Sitios

El diseño de OTV de la Empresa se enfoca principalmente en la nivel de Conjunto para aquellas aplicación es fuera de la Cloud CITRIX, en las cuales residen, las VDCs como la de Conjunto y la OTV.

Nota:

La aplicación dentro de la nube CITRIX, no será extendida entre los Data Centers. El despliegue de la nube CITRIX, no funciona con la extensión vlan entre DC.

7.1.1 Descripción general del diseño

El diseño lógico consiste en tres niveles DC–Core, Aggregation y Access. El propósito de los diseños utilizados, es usar extensiónes Capa 2 entre los Data Centers, en vez de capa 2 o capa 3 DCI. El enfoque de este capítulo se limita al nivel de Conjunto (Aggregation), la cual contiene los elementos funcionales que proporcionan DCI. Enivel de Aggregation en cada Data Center, consiste en dos switches Nexus 7009 desplegados de manera redundante. Elnivel de Aggregation se configura para sostener VDCs múltiples. El uso de VDCs permite la segmentación virtualizada de los planos de control y datos, y se usa en multi-tenancy. Cada uno de los switches Nexus 7009 tiene tres VDCs configurados, los cuales son el Storage VDC, Aggregation VDC, y el OTV VDC. Los VDCs Aggregation fungen como el routeador de límite de Capa 3 en ambos Data Centers, como se muestra en la siguiente Figura. El OTV se configura en modo “appliance” en su propio VDC.

La función del OTV VDC es servir como switch capa 2 en el que las otras VDCs o switches físicos capa 2, pueden extender sus dominios capa 2 a través de DCI hacia otros Data Centers.

En este diseño, el Aggregation VDC conecta vía vPC, hacia el OTV VDC. Se debe remarcar que en un ambiente multi.tenancy, el mismo OTV VDC puede ser configurado con múltiples capas para proporcionar una extensión segmentada capa 2 para distintos tenedores o aplicación es. También debe tomarse en cuenta, que cuando se interconectan múltiples sitios del Data Center, las operaciones OTV pueden beneficiarse de la presencia de multicast en el core.

El diseño global para el Data Center de Villahermosa, Poza Rica y Reynosa, se muestra en la Figura 7.1.

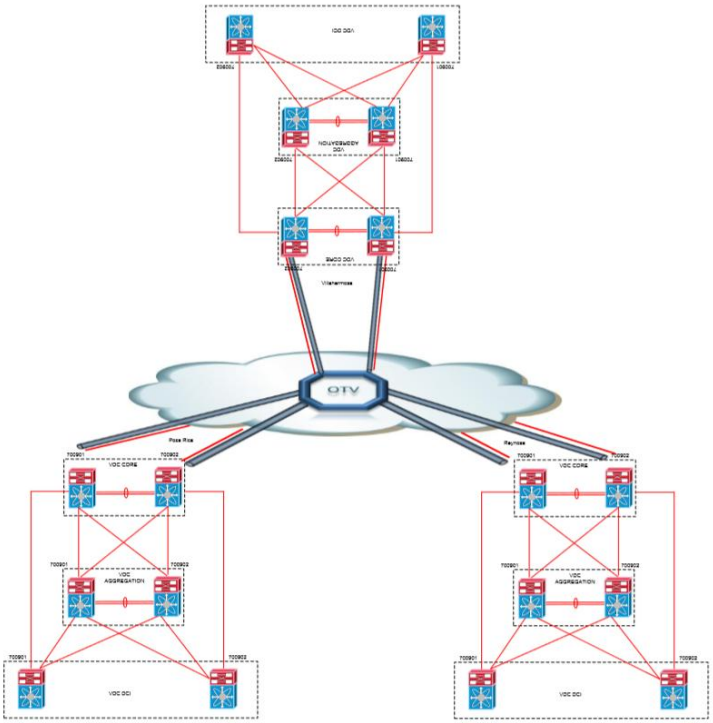


Figura 7.1 Diseño OTV

7.1.2 Nivel Agregación y Panorama DCI

Las niveles aggregation de los Data Centers de Villahermosa, Poza Rica y Reynosa sonidénticas, por lo que solamente describiremos uno de los Data Centers: Villahermosa. La capa de aggregation consiste en dos switches Nexus 7009, VHAGR700901_AGGREGATION yVHAGR700902_AGGREGATION, los cuales proporcionan alta disponibilidad. Cada uno de losswitches Nexus 7009 se configura para tener 3 VDCs: VDC Storage, VDC Aggregation, y el VDC OTV. Los OTVs que residen en los switches agregación, se despliegan como una "aplicaciónOTV en una vara" para brindar una extensión capa 2 entre los Data Centers.

Esto significa que el VDC OTV actúa como el dispositivo de filo para las extensiónes capa 2 y se encuentra enel camino directo del flujo de datos capa 2, entre los dos Data Centers. Se debe remarcar que el VDC OTV se encuentra a un salto de los routers de límite capa 3, proporcionandoconectividad VDC.
La interconexión física entre los Data Centers de Villahermosa, Poza Rica y Reynosa, son proporcionados por el uso de la cloud WAN MPLS. En términos de routing, los centros de datos corren OSPF, así que se provee multi-path desde la perspectiva de capa 3.

7.1.3 Nivel Core.Panorama Capa 3

La CORE capa consiste en dos switches Nexus 7009, VHCOR700901_CORE yVHCOR700902_CORE, los cuales proporcionan alta disponibilidad a los diseños de capa 3. El VDC CORE que corre OSPF, actúa como router de límite capa 3 para la funcionalidad de capa3 DCI, además de funcionar como un switch de nivel Core. El VDCCORE se conecta en unatipología completa capa 3 engranado a los routers upstream WAN. Debe mencionarse que en elambiente ruteado OSPF, el Capa 3 completo engranado ofrece una convergencia más rápida enrelación con una conectividad de forma cuadrada, debido a la existencia de sucesoresrealizables en un diseño completo engranado.

7.1.4 Panorama del nivel agregación capa 2

El nivel agregación de AGR VDCs provee conectividad de capa2 y capa 3 hacia los hosts en el nivel de acceso. Por otro lado, el OTV VDC provee extensión capa 2, conectando a los hostsen las VLANs que están virtualmente extendidas a través de los dos DCs. El VDC AGR enVHAGR700901_AGGREGATION y VHAGR700902_AGGREGATION se configura utilizandovPC para conectar hacia los switches en la nivel de acceso como se muestra en la figura 7.2.

Como mejores prácticas de vPC, se establece un link separado capa 3 entre los dosswitches de agregación para llevar tráfico de capa 3. Por favor tome en cuenta que un SVIpuede ser también utilizado para servir como link de un punto virtual a un punto L3 entre los dosswitches de Nexus para asemejar OSPF y agrupar sobre Vpc peer-link port-channel.

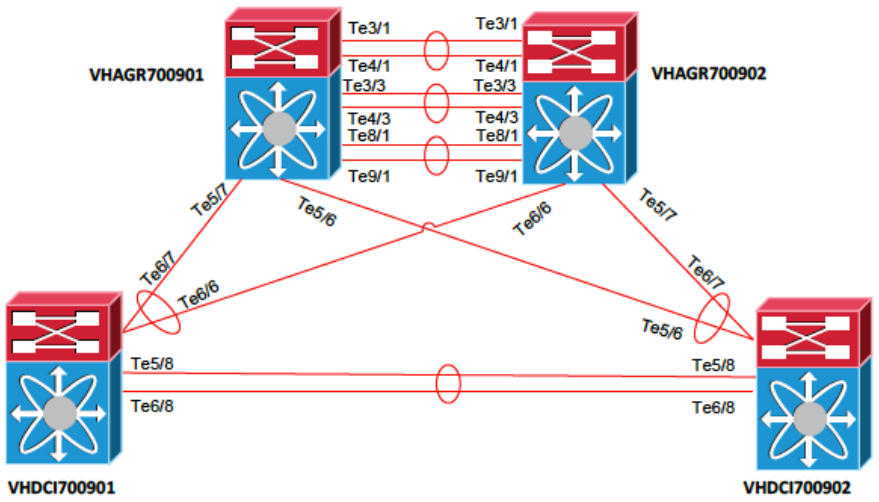


Figura 7.2 Agregación a conectividad OTV

7.1.5 Panorama de la superposición de la Virtualización del Transporte (Overlay Transport Virtualization OTV)

El diseño de OTV en un modo de aplicación virtual, y por ende, OTV se configura en un VDC separado. El VDC de agregación levanta el VDC DCI como un switch de capa 2 para extender las VLANs capa 2 a través de los tres Data Centers. Para lograr una disponibilidad alta d DCI, los VCCs de configuran en ambos VHAGR700901_DCI y VHAGR700902_DCI para proporcionar capacidades multi-homing. Los OTV VDCs en _DCI y VHAGR700902_DCI se encuentran conectados vía vPC a los VCDs de agragación. El uso de vPC permite la redundancia del path capa 2 desde el VDC DCI a los VCDs de agregación.

Como se muestra en la figura 7.3, OTV tiene tres tipos de interfaces: Join, Overlay y la interface Interna.
Las interfaces internas OTV llevan a las VLANs a ser extendidas y a la VLAn del sitio OTV (utilizado dentro del Data Center para proporcionar multi-homig). Se comportan como interfaces switchport trunk capa 2 regulares; de hecho, mandan, reciben y procesan el árbol Spanning BPDUs como lo harían en un dispositivo puente LAN regular.

Las interfaces Overlay encapsulan los marcos L2 en paquetes IP unicast o multicast y son interfaces lógicas multi-access multicast-capable.
Las interfaces Join son interfaces ruteadas punto-apunto que son utilizadas por dispositivos con filo OTV para adjuntarse a la red Overlay. Actualmente la implementación OTV utiliza la dirección IP de la interfaz física Join para promover el alcance de Direcciónes MAC presentes en el sitio. Para versiónes futuras, el plan es usar la dirección loopback para este propósito.
Los mismos VDCs DCI pueden ser levantados por múltiples VDCs desplegadas en el nivel agregación, así como también por otros switches capa 2 conectados a las VDCs DCI. Esto se logra por medio de la configuración de Overlays OTV múltiples. Es importante remarcar que las VLANs extendidas dentro de estos overlays múltiples no deben de empalmarse.

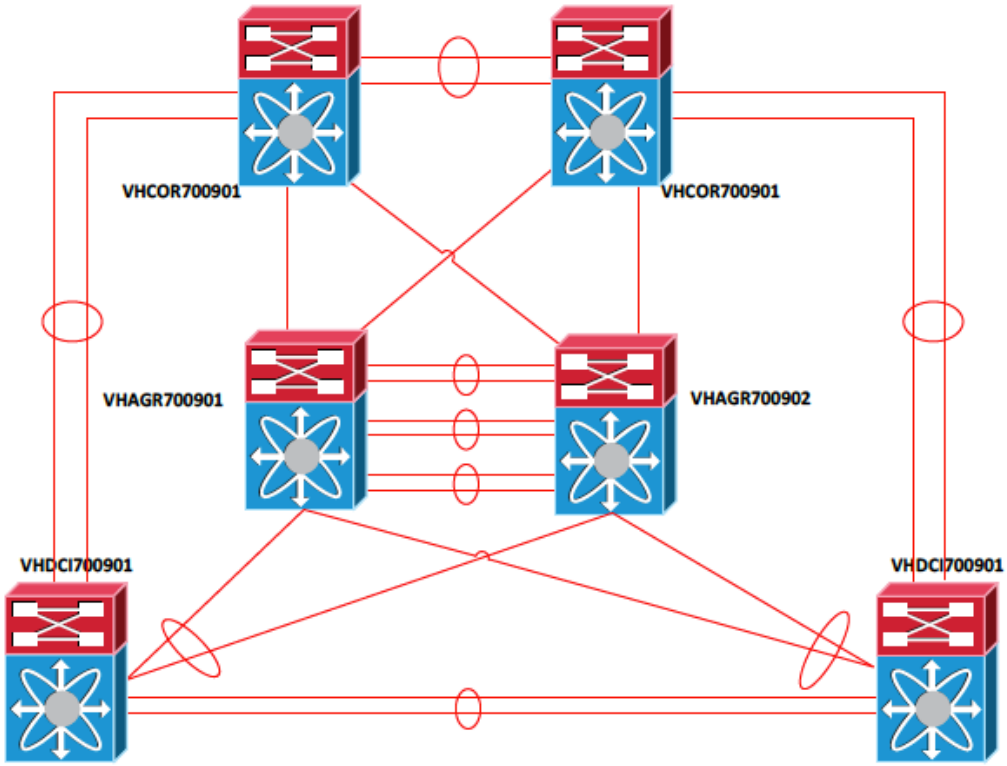


Figura 7.3 OTV – Descripción general

7.1.6 Ruteo OSPF

OSPF escala bien y provee tiempos de convergencia extremadamente rápidos. Para este Data Center, OSPF es utilizado como el protocolo de ruteo para proporcionar la conectividad y una convergencia alta, dentro los Data Centers.

En todos los Data Centers, los switches Nexus 7009 se configuran de tal manera que los procesos OSPF área 0, corra en el link inter-switch y la interface OTV Join. El protocolo Bidirectional Forwarding Detection (BFD) es también utilizado para proveer tiempos de detección rápidos de reenvío de fallas en la ruta para OSPF.

```
interface port-channel1
description **** lint L3 to VHCOR700901 ****
no switchport
mtu 9216
no ip redirects
ip address 172.X.X.X/30
ip ospf authentication message-digest
ip ospf authentication-key 3 a5db8223e1eaa637
ip ospf dead-interval 3
ip ospf hello-interval 1
ip ospf network point-to-point
ip ospf mtu-ignore
ip router ospf 100 area 0.0.0.0
ip ospf bfd
ip pim sparse-mode
ip igmp version 3
```

Figura 7.4 Configuración DCI VDC OSPF

7.2 Replicación de datos

El tráfico de replicación de datos posee características únicas que requiere de recursos dedicados y especializados. Normalmente este tipo de tráfico es alto en volumen con un número reducido de conexiónes TCP; adicionalmente, estas conexiones tienen una vida larga por sesión y probablemente persisten por un periodo largo de tiempo.
El adaptador de red Cisco WAE Inline intercepta el tráfico de manera transparente fluyendo a través de él o puentea el tráfico que no necesita ser optimizado. También utiliza un mecanismo con diseño a prueba de fallas que puentea automáticamente el tráfico en caso de que ocurra una falla de energía, hardware o de software irrecuperable.
La figura 7.5 muestra la Interconexión Lógica propuesta para dos Data Centers

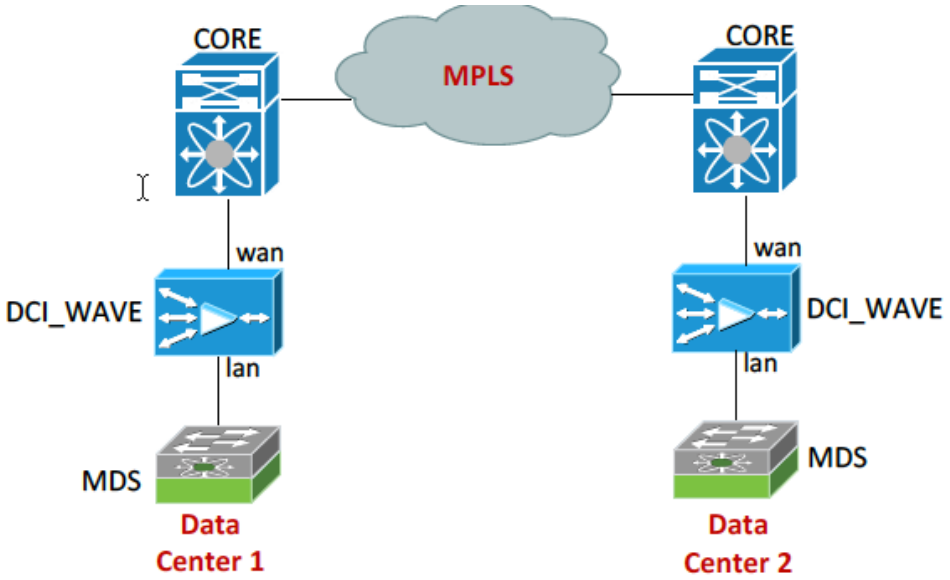


Figura 7.5 Escenario de despliegue WAVE

Cuando el WAVE en línea alcanza las conexiónes máximas permitidas, aquellas conexiónes subsecuentes serían establecidas como conexiónes “pass-through” (de paso) y manejadas directamente por el CORE switch, y enviadas fuera sin optimización.
No hay un mecanismo HA adicional a parte de la característica a prueba de fallas de los dispositivos WAVE; debido a que el Data Center sólo usa una aplicación.

Nota:

En este punto de la implementación, debido a que se necesita otro sitio, no se pueden realizar pruebas de replicación, el WAVE de Villahermosa estará activo y listo para comenzar a optimizar el tráfico tan pronto como uno de los otros sitios esté funcionando con la WAVE respectiva configurada en el Administrador Central.

7.3 WAVE en el Capa DCI

El Adaptador de Red Cisco WAE Inline intercepta el tráfico de manera transparente fluyendo a través de los puentes de tráfico que no necesita ser optimizados. También utiliza una mecánica a prueba de fallas que automáticamente puentea el tráfico en caso de que ocurra una falla de energía, de hardware o de software irrecuperable.

La figura 7.6 muestra la conexión física entre el MDS y la infraestructura CORE, utilizando un adaptador interlínea, dos rutas estarán disponibles al tráfico proveniente del ambiente SAN, una vía la Lan0 y Wan0; y la otra vía la Lan1 y Wan1:

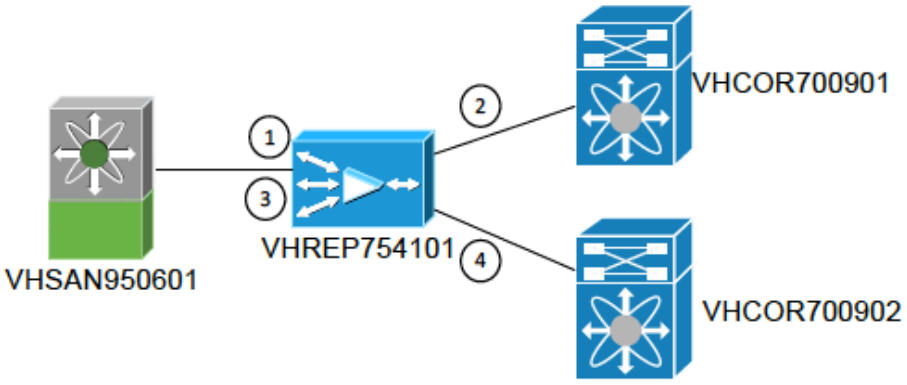


Figura 7.6 Interconexión serial del clúster

Tabla 7.1 Interface de interconexiones seriales del clúster

Identificación	Descripción
1	Inline LAN0 port on VHREP754101
2	Inline WAN0 port on VHREP754101
3	Inline LAN1 port on VHREP754101
4	Inline WAN1 port on VHREP754101

7.3.1 Direccionamiento VLAN e IP

La siguiente tabla muestra el direccionamiento vlan e IP seleccionados para las WAES ubicadas en el Capa WAN:

Tabla 7.2 Capa DCI de direccionamiento VLAN e IP en Villahermosa

Dispositivo	Vlan	IP Address
VHREP754101	N/A	172.X.X.A
Default Gateway	N/A	172.X.X.B

7.3.2 Flujo de Tráfico

Para el Capa DCI, todo el tráfico que sale de Cada Data Center sería optimizado y con carga balanceada entre los puertos WAVE conectado a un MDS específico como se muestra en la siguiente figura:

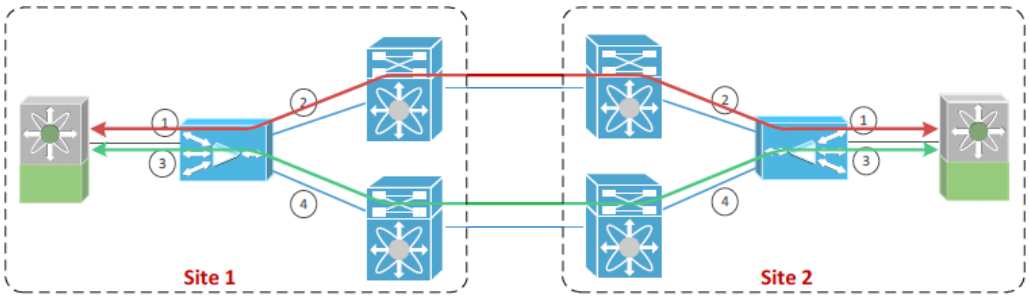


Figura 7.7 Flujo de optimización DCI

7.3.3 Configuración Inline

El siguiente script muestra las configuraciones que se requieren para la integración inline con el Data Center:

```
!
hostname VHREP754101
!
ip domain-name TBD!
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
ip address TBD
exit
interface GigabitEthernet 2/0
shutdown
exit
!
interface InlineGroup 1/0
inline vlan all
exit
interface InlineGroup 1/1
inline vlan all
exit
!
ip default-gateway TBD
!
```

Figura 7.8 Escenario de despliegue WAVE

Nota:

Las interfaces inline van a permitir a todas las vlans asegurar todo el tráfico que necesite ser optimizado, sea aceptado. Las configuraciones requeridas para el Data Center Remoto, será similar para la intercepción Inline.

7.3.4 Registrar WAE en el administrador central

En la configuración, de cada dispositivo WAVE, las direcciónes IP primarias y secundarias del administrador central deben ser expedidas con el fin de registrar los dispositivos. Con el fin de utilizar el servidor DNS name, el nombre de host del administrador central necesita ser creado manualmente en el servidor DNS.

```
wave (config)# central-manager address TBD
wave (config)# cms enable
```

Figura 7.9 Registrando dispositivos WAE en CM

Capítulo 8: SAN y almacenamiento unificado

La infraestructura de Storage Area Network (SAN) es una de las piezas críticas de cualquier diseño de Data Center. Esta sección proporciona los detalles para el diseño propuesto para la infraestructura de Storage Area Network (SAN)
La infraestructura de Storage (Almacenamiento) proporcionará un número de servicios de datos a la cloud, incluyendo servicios para la misma infraestructura de la cloud.
El modulo SAN es en donde casi toda la información será almacenada. Típicamente esta es una red separada, por sí misma, y es la red SAN más comúnmente utilizada es construida usando la tecnología Fiber Channel.
Con Unified Fabric y Fiber Channel over Ethernet (FCoE), no hay necesidad de tener una red SAN separada. El diseño SAN propuesto en este documento utiliza una mezcla de los componentes tradicionales de SAN (como la red fiber channel basada en directores Fiber Channel) y los componentes Unificados I/O dentro de los servidores blade HP (por ejemplo los switches top del nexus 5548UP combinan el tráfico de Ethernet y Fiber Channel sobre una infraestructura de transporte Ethernet convergente).
Es muy importante que en la selección del almacenaje, cada máquina virtual obtenga el desempeño requerido que se necesita. La métrica primaria que se utiliza para determinar las demandas del sistema SAN es operaciones I/O por segundo (IOPS). Cada aplicación de Nube tendrá diferentes requerimientos máximos de IOPS. La creación del almacén de datos SAN debe considerar estos valores máximos para asegurarse de que los almacenes de datos (y LUNs) puedan trabajar con las aplicación es de la cloud.
La confiabilidad y la disponibilidad son dos elementos críticos que necesitan formar parte integral del diseño de SAN en el Data Center. Cualquier falla en la infraestructura de almacenamiento tiene el potencial de causar la corrupción de datos. Teniendo este requerimiento en mente, los diseños propuestos de SAN tienen dos tejidos completamente redundantes e independientes para la confiabilidad y alta disponibilidad. El diseño también toma en cuenta los requerimientos de escalabilidad de la empresa.

8.1 Descripción general

La confiabilidad y la disponibilidad son dos elementos críticos que necesitan formar parte integral del diseño de SAN en el Data Center. Cualquier falla en la infraestructura de almacenamiento tiene el potencial de causar la corrupción de datos. Teniendo este requerimiento en mente, los diseños propuestos de SAN tienen dos tejidos completamente redundantes e independientes para la confiabilidad y alta disponibilidad. El diseño también toma en cuenta los requerimientos de escalabilidad de la empresa.

Como con otras tecnologías de red, la red de almacenamiento basada en FCoE se implementará en el diseño de la CITRIX cloud. La implementación se va a determinar por diversos factores incluyendo los progresos en los estándares y la disponibilidad de los conductores de hardware y software interoperables.

El Servidor Blade HP en esta propuesta trabaja con Unified I/O (FCoE) utilizando los adaptadores de red convergentes (CNAs) y el Nexus 7009 y Nexus 5548UP. El soporte de FCoE para el almacenamiento y soporte de FCoE multi hop entre los switches que se espera estén disponibles en el Data Center.

La Citrix cloud estará basada en la infraestructura SAN FCoE con Fiber Channel (protocolo) utilizando la Infraestructura Ethernet del Data Center para transportar y eliminar lentamente los requerimientos de una infraestructura de transporte Fiber Channel separada.

El tejido de replicación de Almacenaje en la infraestructura MDS 9506 utilizará VSAN y su propio port-channel en una red de replicación de almacenaje aislado. Los puertos existentes de legado FC y EMC FC estarán interconectados a la infraestructura MDS 9506.

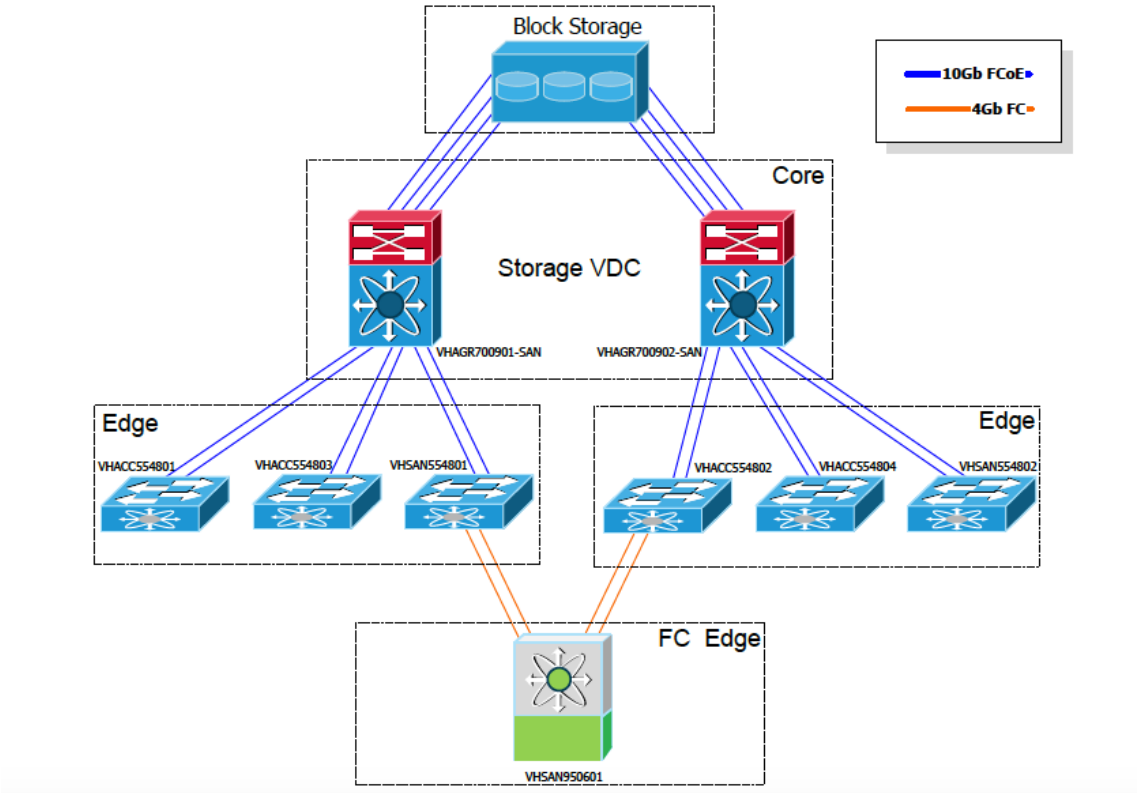


Figura 8.1 Diagrama panorama de SAN en la empresa

8.2 Resumen de requerimientos

La nueva infraestructura SAN del Data Center de la Empresa, necesita soportar lainfraestructura actual y futura de SAN. Los requerimientos se resumen a continuación:

- ➔ Infraestructura SAN confiable, disponible, escalable y redundante
- ➔ La SAN debe ser flexible en diseño con el fin de adaptar los cambios en los requerimientosdel negocio, desempeño y redistribución de servicios
- ➔ Debe aprovechar las habilidades de tejidos unificados
- ➔ Respaldar la consolidación de I/O en el capa de acceso
- ➔ Respaldar el puerto FC para los servidores de legado
- ➔ Habilidad de estirar los tejidos SAN a través de los Data Centers
- ➔ Respaldar la replicación de datos.
- ➔ Respaldar la configuración active-active / active-standby del Data Center.
- ➔ Respaldar SANs múltiples y lógicas en un solo tejido SAN físico
- ➔ SAN debe respaldar características integradas avanzadas como la aceleración de escribir de Fiber Channel, FCIP, NPV, NPIV y respaldo de virtualización en el tejido.

8.3 Componentes de hardware

Las siguientes Tablas enlistan los módulos y las tarjetas de línea que se usarán para las dos Cisco Nexus 7009, seis Cisco Nexus 5548UP y un Switch Cisco MDS 9506 en Villahermosa.

Tabla 8.1 Componentes Nexus 7000

Slot	Módulo	Descripción
1	N7K-SUP2	Nexus 7000 – Supervisor 2 Includes External 8GB USB Flash
2	N7K-SUP2	Nexus 7000 – Supervisor 2 Includes External 8GB USB Flash
3	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
4	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
5	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
6	N7K-M108X2-12L	Nexus 7000 – 8 Port 10GbE with XL option (req. X2)
7	Empty	Empty
8	N7K-F132XP-15	Nexus 7000 – 32 Port 1G/10G Ethernet Module SFP/SFP+
9	N7K-F132XP-15	Nexus 7000 – 32 Port 1G/10G Ethernet Module SFP/SFP+
FM1	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM2	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM3	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM4	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
FM5	N7K-C7009-FAB-2	Nexus 7000 – 9 Slot Chassis – 110Gbps/Slot Fabric Module
PS1	N7K-AC-6.0KW	Nexus 7000 – 6.0KW AC Power Supply Module
PS2	N7K-AC-6.0KW	Nexus 7000 – 6.0KW AC Power Supply Module

Note: Los módulos X2 son 10GBASE-SR, SFP son GLC-SX-MDD o SFP-10G-SR o GLC-T, cada supervisor tienen un puerto de administración 1 GE.

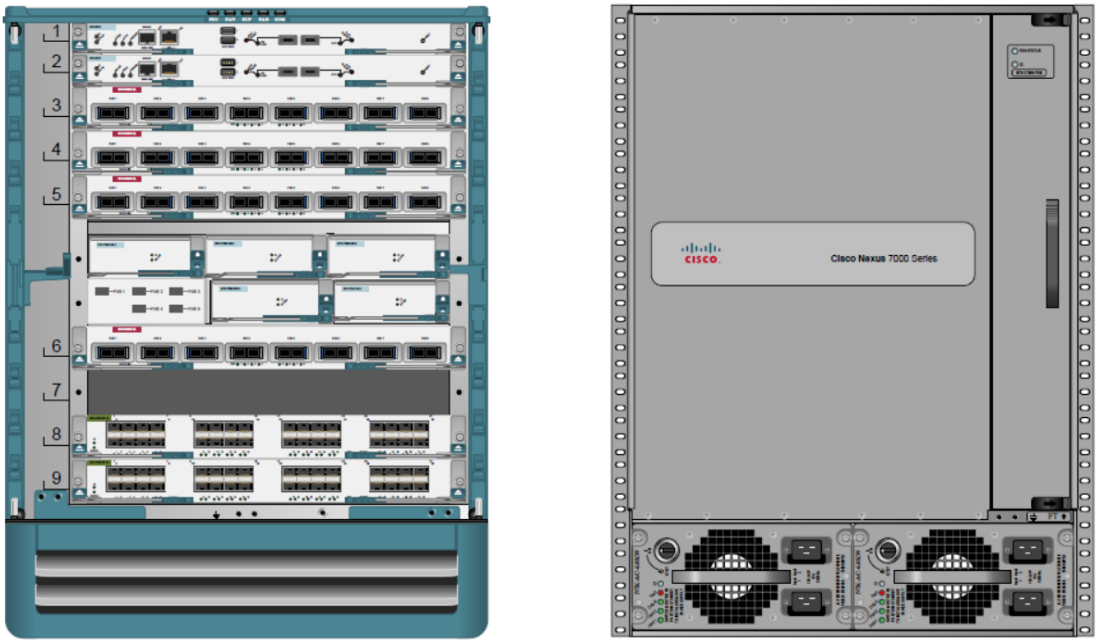


Figura 8.2 Vista física frontal y trasea Nexus 7009

La tabla 8.2 muestra los módules SFP para Nexus 7009

Tabla 8.2 Módulos Nexus 7009 SFP

Cantidad	Módulo	Descripción
64	X2-10GB-SR	10GBASE-SR X2 Module
40	GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM
88	SFP-10G-SR	10GBASE-SR SFP Module

La tabla 8.3 Muestra los componentes Nexus 5548UP

Tabla 8.3 Componentes de Nexus 5548UP

Cantidad	Equipamiento	Descripción
6	Cisco Nexus 5548UP Switch	1RU 10 Gigabit Ethernet, Fibre Channel, and FCoE switch offering up to 960 Gbps of throughput and up to 48 ports. The switch has 32 unified ports and one expansion slot.
4	N55-M16UP	Nexus 5500 Unified Module with 16 ports 10GE Eth/FCoE or 16 port 8/4/2/1G FC

El Switch Cisco Nexus 5548UP está basado en el Software Cisco NX-OS, es un switch FCoE y Ethernet de 1 Unidad-Rack 10 Gigabits, que ofrece una producción de hasta 960-Gbps, proporciona hasta 48 puertos: 32 puertos fijos “unificados” 1/10-Gbps SFP+ Ethernet y FCoE y un espacio de expansión.
La figura 8.3 muestra una vista del switch Cisco Nexus 5548UP

Figura 8.3 Vista frontal física del switch Cisco Nexus 5548UP

Con los módulos de expansión N55-M16UP, el Switch Cisco Nexus 5548UP puede proporcionar un puerto unificado con /10-Gbps SFP+ Ethernet y FCoE o 1/2/4/8-Gbps Fiber Channel nativo.
320
Este módulo se utiliza para interconectar la Hilera de Acceso al ambiente SAN con el puerto FC conectado al Switch MDS 9506.
La tabla 8.4 muestra los módulos SFP de Nexus 5548UP

Tabla 8.4 Módulos SFP de Cisco Nexus 5548UP

Cantidad	Módulo	Descripción
12	DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+ LC
144	SFP-10G-SR	10GBASE-SR SFP Module
40	GLC-T	1000BASE-T SFP

La tabla 8.5 muestra los componentes MDS

Tabla 8.5 Componentes MDS 9506

Slot	Módulo	Descripción
1	DS-X9316-SSNK9	16x1GE, Storage Services Node
3	DS-X9232-256K9	32-Port 8-Gbps Advanced Fibre Channel Switching Module
4	DS-X9232-256K9	32-Port 8-Gbps Advanced Fibre Channel Switching Module
5	DS-X9530-SF2AK9	MDS 9500 Series Supervisor-2A
6	DS-X9530-SF2AK9	MDS 9500 Series Supervisor-2A
1	DS-X9316-SSNK9	16x1GE, Storage Services Node

La tabla 8.6 muestra los módulos SPF para MDS 9506

Tabla 8.6 Módulos SPF de Cisco MDS 9506

Cantidad	Módulo	Descripción
64	DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+ LC
16	DS-SFP-FCGE-SW	1 Gbps Ethernet, 2 Gbps Fibre Channel SW SFP LC

La figura 8.4 muestra a vista frontal y trasera de MDS 9506

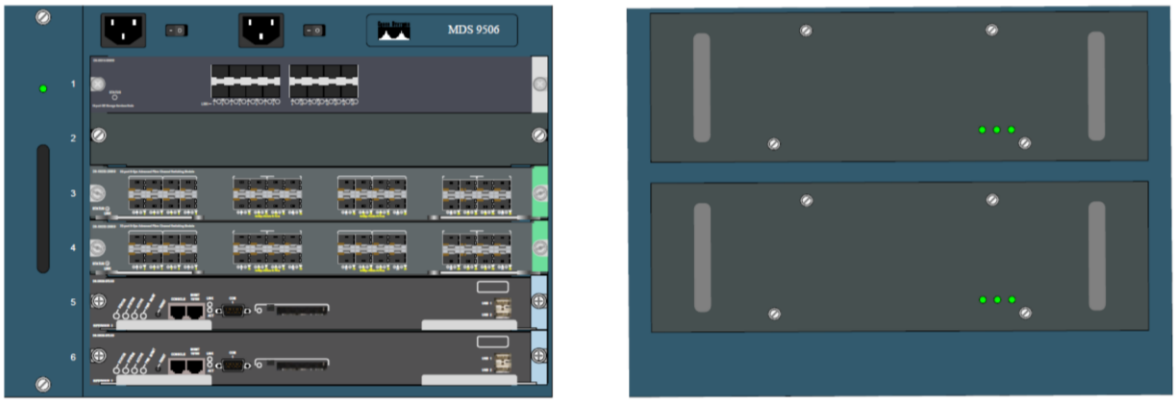


Figura 8.4 Vista física frontal y trasera de MDS 9506

8.4 Conectividad Física

Los switches Nexus 5548UP proporcionan hasta 48 puertos: 32 puertos fijos “unificados” 1/10-Gbps SFP+ Ethernet y FCoE y un espacio de expansión. Cuando se asignan puertos para el Fiber Channel nativo, los puertos FC deben ser asignados en un bloque contiguo comenzando desde los últimos puertos en el switch.

Todos los 6 Nexus 5548UP están conectados a Nexus 7000 del SAN core, utilizan dos puertos configurados como canales de puerto (port cannel). Los dos últimos puertos en los switches Nexus VHSAN554801 y VHSAN554802 están conectados a un switch upstream MDS 9506 utilizando canales de puerto SAN.
Los dos puertos Fiber Channel adyacentes están reservados en Nexus VHSAN554801 y VHSAN554802 para un posible crecimiento futuro.
Cuatro puertos 10GbE en cada Nexus 7009 proporcionarán conectividad FCoE a los procesadores de Almacenaje VNX. Todo el load-balancing y la redundancia de la ruta será

proporcionada por servidores que operan sistemas o en software de terceras partes (por ejemplo: EMC Power Path), entonces las interfaces de almacenaje no participan en canales de puerto.

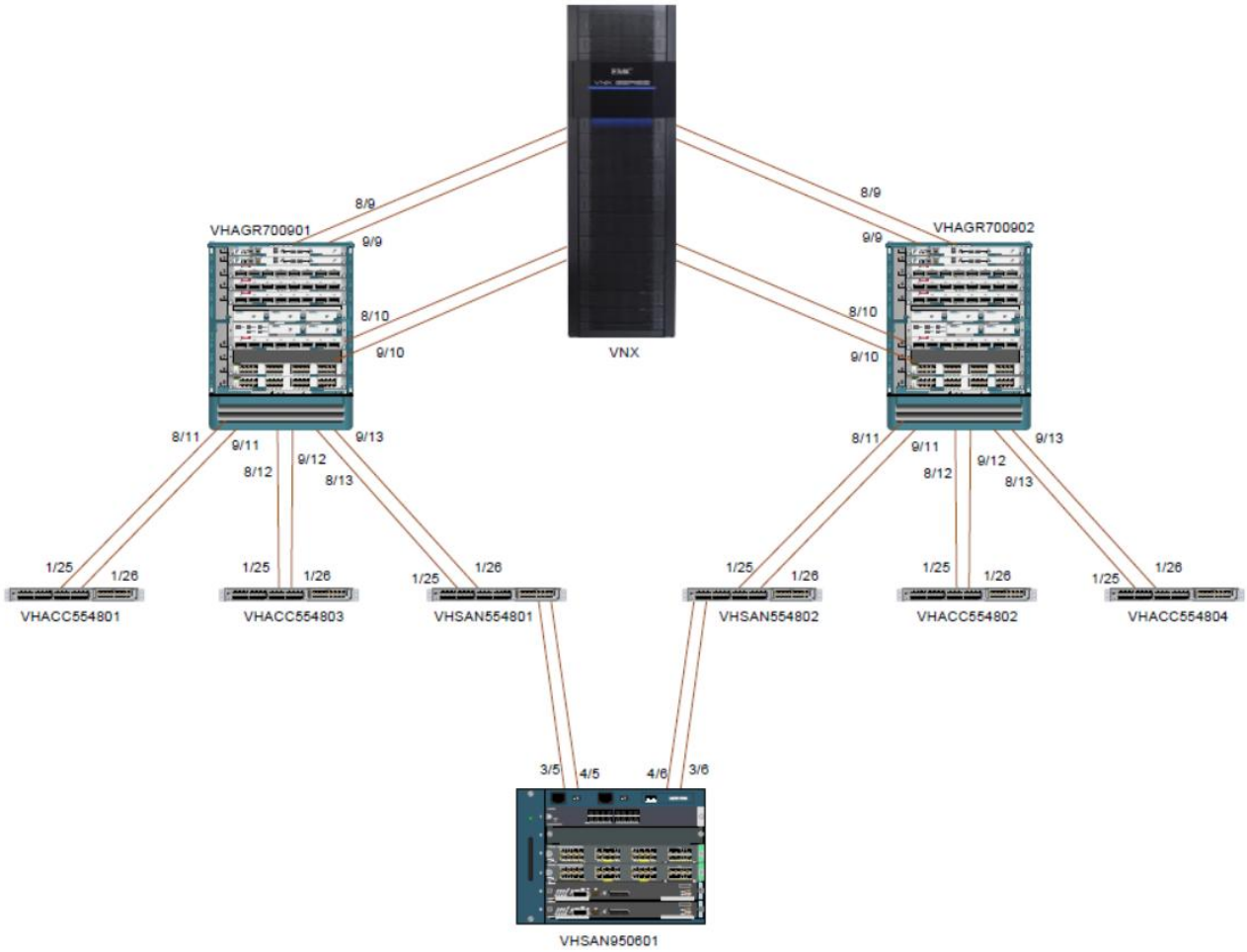


Figura 8.5 Panorama de la conectividad de SAN en la Empresa

8.4.1 Asignación de Puertos

Las siguientes tablas, 8.7 y 8.8, proporcionan información de interfaces para la conectividad entre dispositivos SAN (Nexus 7009, Nexus 5548UP y MDS 9506) así como entre dispositivos SAN y puertos de almacenaje (Nexus 7009 y VNX).

Tabla 8.7 Asignación de puertos Nexus 7009 VHAGR700901-SAN

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth8/9	To EMC VNX disk array	EMC VNX 5205	SPA4
Eth9/9	To EMC VNX disk array	EMC VNX 5205	SPB5
Eth8/10	To EMC VNX disk array	EMC VNX 5205	SPA6
Eth9/10	To EMC VNX disk array	EMC VNX 5205	SPB7
Eth8/11	To VHACC554801 (PO 11)	VHACC554801	Eth1/25
Eth9/11	To VHACC554801 (PO 11)	VHACC554801	Eth1/26
Eth8/12	To VHACC554802 (PO 13)	VHACC554803	Eth1/25
Eth9/12	To VHACC554802 (PO 13)	VHACC554803	Eth1/26
Eth8/13	To VHSAN554801 (PO 15)	VHSAN554801	Eth1/25
Eth9/13	To VHSAN554801 (PO 15)	VHSAN554801	Eth1/26

Tabla 8.8 Asignación de puertos Nexus 7009 VHAGR700902-SAN

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth8/9	To EMC VNX disk array	EMC VNX 5205	SPB4
Eth9/9	To EMC VNX disk array	EMC VNX 5205	SPA5
Eth8/10	To EMC VNX disk array	EMC VNX 5205	SPB6
Eth9/10	To EMC VNX disk array	EMC VNX 5205	SPA7
Eth8/11	To VHACC554802 (PO 22)	VHACC554802	Eth1/25
Eth9/11	To VHACC554802 (PO 22)	VHACC554802	Eth1/26
Eth8/12	To VHACC554804 (PO 24)	VHACC554804	Eth1/25
Eth9/12	To VHACC554804 (PO 24)	VHACC554804	Eth1/26
Eth8/13	To VHSAN554802 (PO 26)	VHSAN554802	Eth1/25
Eth9/13	To VHSAN554802 (PO 26)	VHSAN554802	Eth1/26

Tabla 8.9 Asignación de puertos Nexus 5548UP VHACC554801

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 11)	VHAGR700901-SAN	Eth8/11
Eth1/26	To Core Switch (PO 11)	VHAGR700901-SAN	Eth9/11

Tabla 8.10 Asignación de puertos Nexus 5548UP VHACC554802

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 22)	VHAGR700902-SAN	Eth8/11
Eth1/26	To Core Switch (PO 22)	VHAGR700902-SAN	Eth9/11

Tabla 8.11 Asignación de puertos Nexus 5548UP VHACC554803

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 13)	VHAGR700901-SAN	Eth8/12
Eth1/26	To Core Switch (PO 13)	VHAGR700901-SAN	Eth9/12

Tabla 8.12 Asignación de puertos Nexus 5548UP VHACC554804

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 24)	VHAGR700902-SAN	Eth8/12
Eth1/26	To Core Switch (PO 24)	VHAGR700902-SAN	Eth9/12

Tabla 8.13 Asignación de puertos Nexus 5548UP VHSAN554801

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 15)	VHAGR700901-SAN	Eth8/13
Eth1/26	To Core Switch (PO 15)	VHAGR700901-SAN	Eth9/13
Fc1/31	To MDS 9506 (PO 31)	VHSAN950601	Fc3/5
Fc1/32	To MDS 9506 (PO 31)	VHSAN950601	Fc4/5

Tabla 8.14 Asignación de puertos Nexus 5548UP VHSAN554802

Interface local	Descripción	Dispositivo remoto	Interface remota
Eth1/25	To Core Switch (PO 26)	VHAGR700902-SAN	Eth8/13
Eth1/26	To Core Switch (PO 26)	VHAGR700902-SAN	Eth9/13
Fc1/31	To MDS 9506 (PO 42)	VHSAN950601	Fc3/6
Fc1/32	To MDS 9506 (PO 42)	VHSAN950601	Fc4/6

Tabla 8.15 Asignación de puertos MDS 9506 VHSAN950601

Interface local	Descripción	Dispositivo remoto	Interface remota
Fc3/5	To Nexus 5548UP (PO 31)	VHSAN554801	Fc1/31
Fc4/5	To Nexus 5548UP (PO 31)	VHSAN554801	Fc1/32
Fc3/6	To Nexus 5548UP (PO 42)	VHSAN554802	Fc1/31
Fc4/6	To Nexus 5548UP (PO 42)	VHSAN554802	Fc1/32

8.5 Configuración de switches SAN Nexus 5500

8.5.1 Modo Switch vs. Modo NPV

Los switches Nexus 5500 pueden operar bajo dos modos diferentes para el reenvío de tráfico SAN, modo switch y modo NPV.

El modo Switch– El Nexus 5500 proporciona nativamente todos los servicios de tejido como Fabric Shortest Path First (FSPF), zonificación, etc. El dispositivo Nexus maneja todas las decisiónes de reenvío y consume un ID de dominio FC dentro del tejido.

El modo N-Port Virtualizer (NPV) – El Nexus 5000 actúa como un proxy para Fabric logins (FLOGIs) y decisiónes de reenvío). El switch upstream maneja todos los servicios de tejido y el Nexus no consume un ID de dominio dentro del tejido.

Habilitar el modo NPV es un proceso disruptivo que requiere de un reinicio y borra la configuración actual funcionando.

El SAN de la Empresa utiliza un modo NPV para el Nexus 5548UP: VHACC554801, VHACC554802, VHACC554803 y VHACC554804, y Modo Switch para el Nexus 5548UP:

VHSAN554801 y VHSAN554802, que se encuentran conectados a MDS: VHSAN950601, ya que la Empresa ha expresado la posibilidad de conectar un servidor de legado HBA a el MDS y tener acceso a los puertos de almacenaje FCoE en Nexus 7009.

8.5.2 Habilitando FCoE

FCoE se habilita utilizando el comando siguiente, mostrado en la figura 8.6

```
switch# configuration terminal
switch(config)# feature fcoe
```

Figura 8.6 Comando para habilitar FCoE

8.5.3 Creación de VSAN

La base de datos de VSAN se utiliza para crear el VSAN en el Nexus 5500. Este ID y nombre VSAN va a coincidir con aquellos configurados en los switches Cisco Nexus 7009 y Cisco MDS. VSAN se habilita con el siguiente comando, mostrado en la figura 8.7:

```
switch# configuration terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan <vsan_id>
```

Figura 8.7 Comando para habilitar VSAN

8.5.4 ID de dominio FC domain

Los ID de dominio FC deben ser únicos para cada switch dentro del tejido. En la figura 8.8 se muestra como se establece dicho ID.

```
switch# configuration terminal
switch(config)# fcdomain domain <domain_id> static vsan <vsan_id>
```

Figura 8.8 Estableciendo el ID de dominio FC

La tabla 8.16 muestra la asignación de dichos ID.

Tabla 8.16 Table de asignación del ID de dominio

VSAN	Dominio ID (Decimal)	Dominio ID(Hexadecimal)	Dispositivo
10	10	A	VHAGR700901-SAN
10	11	B	VHSAN554801
10	13	D	VHSAN950601
20	20	14	VHAGR700901-SAN
20	22	16	VHSAN554801
20	24	18	VHSAN950601

8.5.5 Creación VLAN FCoE

Una VLAN única es creada por cada tejido para el tráfico FCoE y unida a la VSAN. Esta VLAN debe ser única en la LAN y debe coincidir con la configuración de los dispositivos FCoE upstream.

Las siguientes líneas de comando en la figura 8.9, muestran la creación de VLAN FcoE

```
switch# configuration terminal
switch(config)# vlan <vlan_id>
switch(config-vlan)# fcoe vsan <vsan_id>
```

Figura 8.9 Creación de VLAN FCoE

8.5.6 Trunking de Port-Channel F

Para brindar la capacidad de crear port channels SAN para nodos finales, se habilitará la característica de trunking de Port-Channel F.
En la figura 8.11 se muestra la forma en que se habilita la característica anteriormente mencionada.

```
switch# configuration terminal
switch(config)# feature fport-channel-trunk
```

Figura 8.10 Habilitando fport.channel-trunk

8.5.7 Asignación de Puerto Fibre Channel

Los últimos 2 puertos de los switches VHSAN554801 y VHSAN554802 serán configurados para Fibre Channel nativo para proporcionar conectividad con el switch SAN MDS.

```
switch# configuration terminal
switch(config)# slot 1
switch(config-slot)# port 31-32 tupe fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

Figura 8.11 Asignación de puertos FC

Para que estos cambios se pongan en vigor, se requiere una recarga del switch.

8.5.8 Configuración del Port Channel SAN

Un Port Channel SAN será configurado para la conectividad entre el Nexus 5500 y el switch Cisco MD5. Este Port Channel proporcionará un conjunto de ancho de banda y balance de carga para ISL (puerto E) o EISL (puerto TE) entre los switches.

- **Modo Channel** – El Modo Channel se configura como activo. Los puertos miembro inician una negociación del protocolo de port channel con el switch semejante.

- **Modo Trunk** – El trunking de VSAN permite al switch transmitir el tráfico a más de una VSAN. Aunque el despliegue inicial utilizará una sola VSAN por tejido, el trunking de VSAN estará habilitado para futura capacidad.

La figura 8.12 muestra la creación de san-port-channnel.

```
switch# config t
switch(config)# interface san-port-channel <san-port-channel_id>
switch(config-if)# switchport description <description>
switch(config-if)# switchport mode e
switch(config-if)# switchport trunk mode auto
switch(config-if)# switchport trunk allowed vsan <vsan_id>
```

Figura 8.12 Creación SAN-port-channel

8.5.9 Crear interfaces virtuales de Fibre Channel

Las interfaces virtuales de Fibre Channel se crean para mapear las interfaces físicas de Ethernet o port channels hacia las VSANs respectivas. La figura 8.13 muestra la configuración para el mapeo.

```
switch# config t
switch(config)# interface vfc <vfc_id>
switch(config-if)# bind interface <interface_id>
switch(config-if)# switchport description <description>
switch(config-if)# switchport trunk allowed vsan <vsan_id>
switch(config-if)# no shut
```

Figura 8.13 Interfaces VFC

8.5.10 Asignando las interfaces a la VSAN

La base de datos de VSAN se usa para asignar interfaces físicas, virtuales y port-channel a la VSAN.

```
switch# config t
switch(config)# vsan database
switch(config-vsan-db)# vsan <vsan_id> interface san-port-channel <san-port-channel_id>
switch(config-vsan-db)# vsan <vsan_id> interface vfc <vfc_id>
switch(config-vsan-db)# vsan <vsan_id> interface fc<slot/port>
```

Figura 8.14 Asignación de la interfaz de la base de datos VSAN

8.5.11 Añadiendo interfaces al Port Channel de SAN

La figura 8.15 muestra como añadir interfaces físicas de Fibre Channel al Port Channel de SAN.

```
switch# config t
switch(config)# interface fc<slot/port>
switch(config-if)# switchport description <description>
switch(config-if)# switchport mode e
switch(config-if)# switchport trunk mode on
switch(config-if)# switchport trunk allowed vsan <vsan_id>
switch(config-if)# channel-group <channel-group_id> force
switch(config-if)# no shut
```

Figura 8.15 Agregar interfaces a los port channels de SAN

8.5.12 Alias del dispositivo

Como solicitud de la Empresa, el alias de dispositivo se encuentra en uso para configurar nombres amigables para identificar los dispositivos de wwpns.

```
switch# config t
switch(config)# Dispositivo-alias database
switch(config-device-alias-db)# device-alias name <name> pwwn <pwwn>
switch(config-device-alias-db)# device-alias commit
```

Figura 8.16 Configuración de alias del dispositivo

8.5.13 Zonificación

Para asegurar la seguridad dentro de la SAN, los dispositivos pueden conectarse entre sí, solamente si es que pertenecen a una zona activa (la zona predeterminada es inactiva).

```
switch# config t
switch(config)# zone name <servername_hbaport_storagename_port>
switch(config-zone)# member pwwn <can_wwpn/hba_wwpn> vsan <vsan_id>
switch(config-zone)# member pwwn <storage_wwpn> vsan <vsan_id>
switch(config-zone)# zoneset name <zoneset_name> vsan <vsan_id>
switch(config-zoneset)# member <servername_hbaport_storagename_port>
switch(config-zoneset)# exit
switch(config)# zone commit vsan <vsan_id>
switch(config)# zoneset activate name <zoneset_name> vsan <vsan_id>
switch(config)# zone commit vsan <vsan_id>
```

Figura 8.17 Configuración de Zona/zoneset

La tabla 8.17 muestra los elementos del zoneset

Tabla 8.17 Elementos del zoneset

VSAN	Zoneset	Zona	Dispositivos en la zona
10	ZS_Fabric_A	Z1_HP-BL460c-stivhfhpc01_SPA-VNX-5205	stivhfhpc01_fcoe_pto1_E5AFEE51 VNX-5205_FCoE_SPA4_Slot2Pto0_50060164
10		Z2_HP-BL460c-stivhfhpc01_SPB-VNX-5205	stivhfhpc01_fcoe_pto1_E5AFEE51 VNX-5205_FCoE_SPB5_Slot2Pto1_5006016D
20	ZS_Fabric_B	Z3_HP-BL460c-stivhfhpc01_SPB-VNX-5205	stivhfhpc01_fcoe_pto1_E5C1F231 VNX-5205_FCoE_SPA5_Slot2Pto1_50060165
20		Z4_HP-BL460c-stivhfhpc01_SPB-VNX-5205	stivhfhpc01_fcoe_pto1_E5C1F231 VNX-5205_FCoE_SPB4_Slot2Pto0_5006016C

8.5.14 Modo Zona

Existen dos tipos de características de zonificación en NX-OS: zonificación básica y mejorada. La característica de zonificación cumple con los estándares de FC-GS-4 y FC-SW-3. El Modo Zoning predeterminado en los switches MDS es "básico". Sin embargo, Cisco sugiere la utilización de zonificación "mejorada".

La zonificación mejorada puede ser activada bajo una base per-VSAN, permitiendo a algunas VSANs utilizar las características de zonificación mejorada y a otras VSANs utilizar las características de zonificación básica.
La zonificación mejorada proporciona, entre otras cosas, candado de sesión para que dos administradores de SAN no puedan modificar la base de datos de zonificación dentro de un VSAN al mismo tiempo. La zonificación mejorada continúa utilizando las mismas técnicas y herramientas que la zonificación básica, con una pequeña cantidad de comandos adicionales.

El modo zonificación está configurado como mejorado para VSANs 10 y 20.

```
switch# config t
switch(config)# zone mode enhanced vsan <vsan_id>
```

Figura 8.18 Configuración de zona/zoneset FC

8.6 Replicación

La replicación de datos entre sitios utilizará FCIP a través de WAN para extender la SAN entre sitios y proporcionar comunicación entre puertos VNXs Block FC hacia el MDS 9506 Director en diferentes sitios.
Para este propósito, dos interfaces Ethernet están conectadas al backbone. Esta sección incluye un diseño físico y lógico de la solución FCIP propuesta para la Empresa.

Con la plataforma Cisco MDS 9000 Family los servicios de replicación de almacenaje tales como EMC Mirror View /SANCopy pueden ser extendidas de distancias metro a global utilizando una infraestructura IP omnipresente, la cual simplifica las estrategias de continuación del negocio. Cisco MEDS integra transparentemente FC y Fiber Channel sobre IP (FCIP) en un sistema.
La siguiente tabla, 8.18, enlista la infraestructura que soportará la implementación de FCIP en la Empresa:

Tabla 8.18 Infraestructura de FCIP

Hardware	Software	Rol
Cisco MDS 9000 16x1GE, Storage Services Node - DS-X9316-SSNK9	NX-OS 5.2(1)	FC to IP bridge

El nodo de servicios de almacenaje Cisco MDS 9000 con 16 puertos acoge cuatro motores de servicio independientes, los cuales pueden ser habilitados, cada uno, individualmente o en escala ascendente tal y como cambien los requerimientos del negocio, o pueden ser configurados para trabajar aplicaciones separadas. Basado en un solo motor de servicio, en el módulo multiservicio Cisco MDS 9000 18/4-Port, con una consolidación cuatro-a-uno logra ahorros significativos en hardware y libera espacios valiosos en el chasis Cisco MDS 9500 Series Multicapa Directors.
Cada uno de los cuatro motores de servicio, soporta 4 puertos de servicio de almacenaje IP Gigabit Ethernet, para un total de 16 puertos de Fibre Channel sobre la conectividad IP (FCIP). El tráfico puede ser cambiado entre un puerto IP y cualquier puerto Fibre Channel en un switch Cisco MDS 9000 Family.

El nodo de servicios de almacenaje Cisco MDS 9000 con 16 Puertos soporta el rango completo de servicios disponibles los otros módulos switching Cisco MDS 9000 Family Fibre Channel, incluyendo SANs (VSANs) virtuales, seguridad, y administración del tráfico.
La figura 8.19 ilustra la conectividad de replicación.

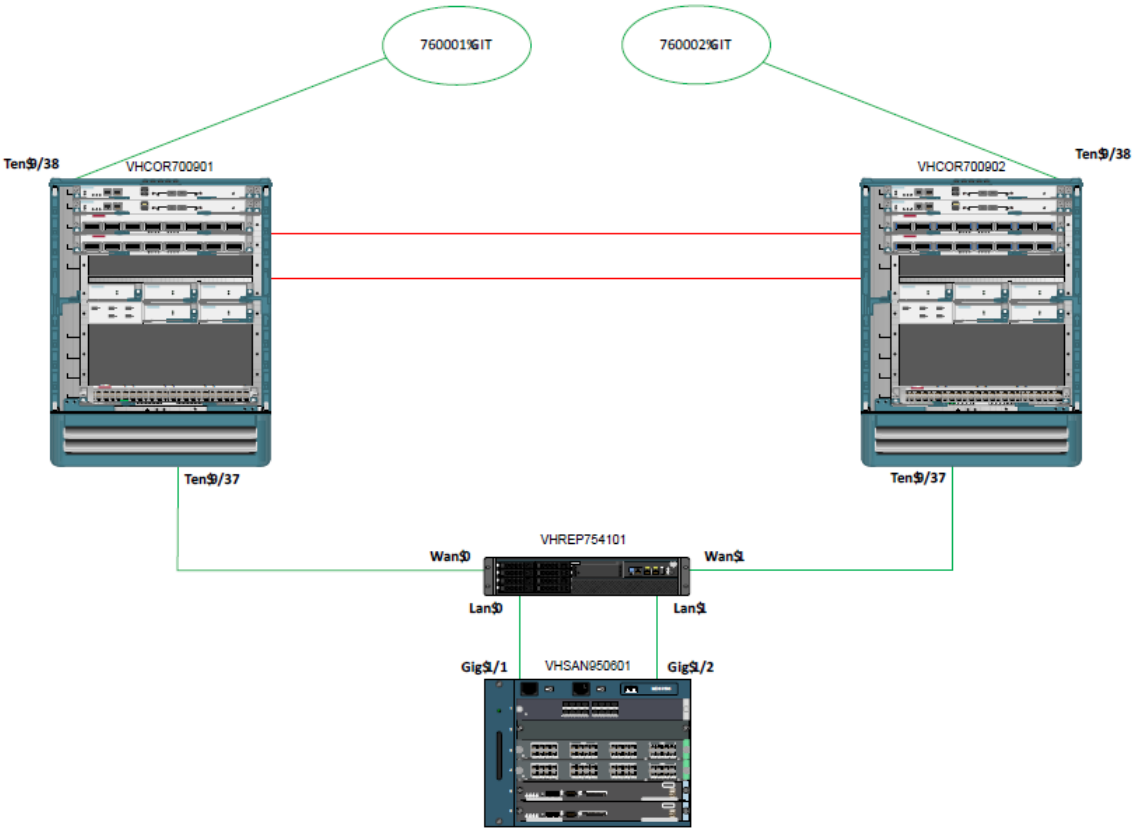


Figura 8.19 Conectividad de replicación

8.6.1 Diseño Físico

La figura 8.20 muestra la topología física del FCIP en el Data Center de Villahermosa, basándose en las mejores prácticas de Cisco y en las necesidades del cliente. Los puertos Ethernet Gigabit del MDS serán conectados a la aplicación WAVE para optimizar el tráfico, que estará conectado a los switches Nexus 7000 y a la WAN. Para propósitos de redundancia la aplicación WAVE estará conectada a dos switches Nexus 7000.

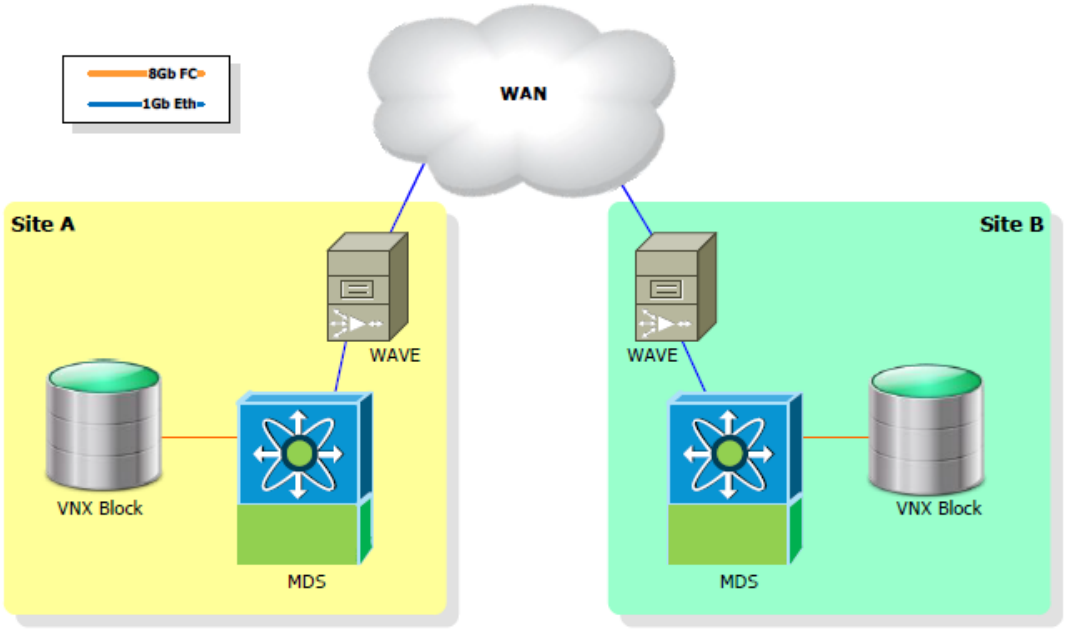


Figura 8.20 Topología de replicación

8.6.2 Diseño Lógico

La figura anterior, 8.20, muestra la topología lógica de FCIP para la SAN de la Empresa. Una configuración IP y FCIP más detallada puede ser encontrada en la siguiente sección, configuración FCIP. Para propósitos de redundancia cada switch SAN será configurado para tener acceso a dos switches diferentes de Ethernet.

8.6.2.1 Replicación VSAN ID de Dominio

Una VSAN exclusiva será usada con propósitos de replicación. Esta VSAN se creará solamente en los switches MDS que sean parte de la topología de replicación y se fusionarán dentro de replicadores semejantes.
Los IDs de Dominio FC deben ser únicos para cada switch dentro de la replicación VSAN.

Tabla 8.19 Asignación de ID de dominio para replicación

VSAN ID	Domain ID(Decimal)	Domain ID (Hexadecimal)	Dispositivo
1000	50	32	VHSAN950601

8.6.3 Configuración FCIP

La asignación de Dirección IP para a configuración de FCIP en la Empresa se basa en la asignación de dirección IP descrita en la tabla 8.20, que también enlista la configuración básica de FCIP.

Tabla 8.20 Configuración FCIP

Switch	Interface	IP Address	IP Peer Info	FCIP	Perfil
VHSAN950601	Ge1/1	172.28.XX.XX	TDB	1	1
VHSAN950601	Ge1/2	172.28.XX.XX	TBD	2	2

8.6.3.1 Habilitando FCIP

En la figura 8.21 se muestra el comando para habilitar FCIP.

```
switch# configuration terminal
switch(config)# feature fcip
```

Figura 8.21 Comando para habilitar FCIP

9 Administración de red

La red de administración se utilizará para proporcionar servicios de monitoreo y administración a los dispositivos de red de Cisco y a algunos equipos de terceras partes dentro del Data Center.

9.1 Consideraciones de Diseño

El diseño general para la red de administración seguirá un diseño “Collapsed Core”: Las capas Core y de distribución se colapsan en un solo par de dispositivos.

La arquitectura de la red de administración estará compuesta por dos switches Catalyst 4503-E que fungirán como el core/distribución, un firewall central que sirve de límite de seguridad, y cinco Catalyst 2960-Sque proporcionan los puertos de acceso.

Los siguientes puntos mencionan las principales premisas del diseño de la red de administración:

- ➔ Alta Disponibilidad: dispositivos y conexiónes redundantes.
- ➔ Seguridad: ambiente protegido con firewall; SNMP v3, AAA
- ➔ Basado en las Mejores Prácticas de Cisco
- ➔ La red de administración dará acceso estrictamente a través de la red privada de la Empresa.

Note: Aun cuando la red de administración puede actuar como una red de administración fuera de banda (OOB), no es completamente independiente del ambiente de producción (como se describe en sesiónes posteriores). Es por eso que el término OOB se usa de manera discrecional.

Note: Existe un total de ocho switches Cat2960 disponibles, pero solamente cinco fueron implementados por Cisco.

9.2 Diseño físico de la red

El diseño físico del módulo de administración de muestra en la siguiente Figura.

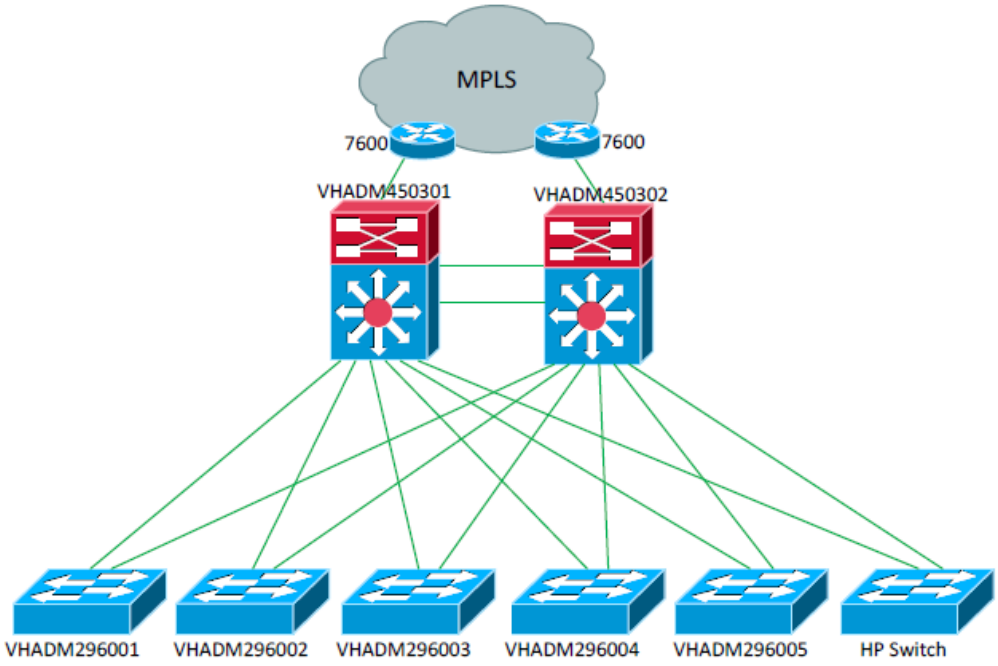


Figura 9.1 Diagrama físico de la administración general

9.2.1 Topología física de la Red

La topología física de la Red de Administración se compone de dos Catalyst 4503-E (VHADM450301, VHADM450302) para la capa Core, cinco Catalyst 2960-S (VHADM29600X) para la capa de acceso, y un switch de tercera parte (HP). Las conexiones entre los dispositivos Core y Access son links Ethernet de 1GB; similarmente, las conexiones entre los dos dispositivos Catalyst 4503-E para redundancia y los uplinks para la red MPLS consisten en links Ethernet de 1GB.

Además, existe una conexión redundante desde el core de administración hasta el Catalyst 6500's en el capa se Servicios del Data Center. Esta conexión tiene el propósito de dar conectividad al contexto de firewall que fungirá como límite de seguridad para la VLANs de administración.

9.2.2 Tabla de Liberación de Hardware/Software

Los dos switches Catalyst 4503-E funcionarán con la versión imagen de IOS 12.2 (54) SG1 con un motor supervisor Sup6L. Para el Catalyst 2960-S Cisco recomienda usar la versión imagen IOS 12.2(58)SE2, ya que resuelve muchas advertencias que aparecen en las versiones más recientes. Las figuras 9.2 y 9.3 ilustran el hardware de los switches descritos anteriormente.

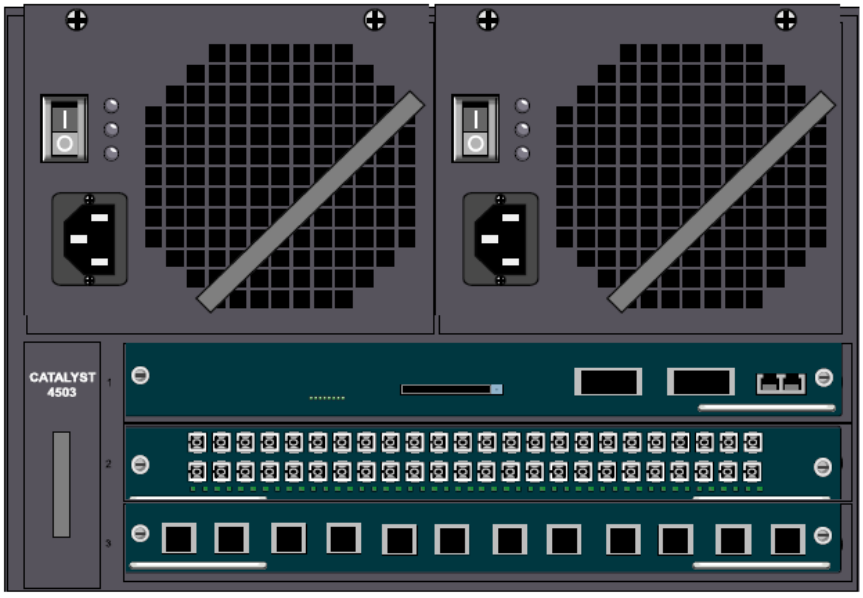


Figura 9.2 Catalyst 4503-E Hardware

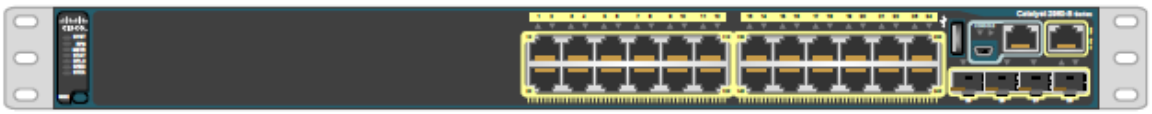


Figura 9.3 Catalyst 2960-S Hardware

La distribución de cuchillas de Cisco para los switches Catalyst se muestra en la tabla 9.1:

Tabla 9.1 Liberación de hardware

Modelo	Slot	Descripción
WS-X45-SUP6L-E	1	Catalyst 4500 E-Series Sup 6-E Lite 2x10GE(X2) w/ Twin Gig
WS-X4612-SFP-E	3	Catalyst 4500 E-Series 12-Port GE (SFP)
WS-X4648-RJ45-E	2	Catalyst 4500 E-Series 48-Port 10/100/1000 (RJ45)

Las recomendaciones de IOS de Cisco para los switches Catalyst se muestran en la siguiente tabla, 9.2.

Tabla 9.2 Tabla de liberación de software

Modelo	IOS	Imagen
Catalyst 4503-E	12.2(54)SG1	cat4500e-entservicesk9-mz.122-54.SG1.bin
Catalyst 2960-S	12.2(58)SE2	c2960s-universalk9-mz.122-58.SE2.bin

9.2.3 Conectividad LAN

La figura 9.4 muestra la conectividad física LAN

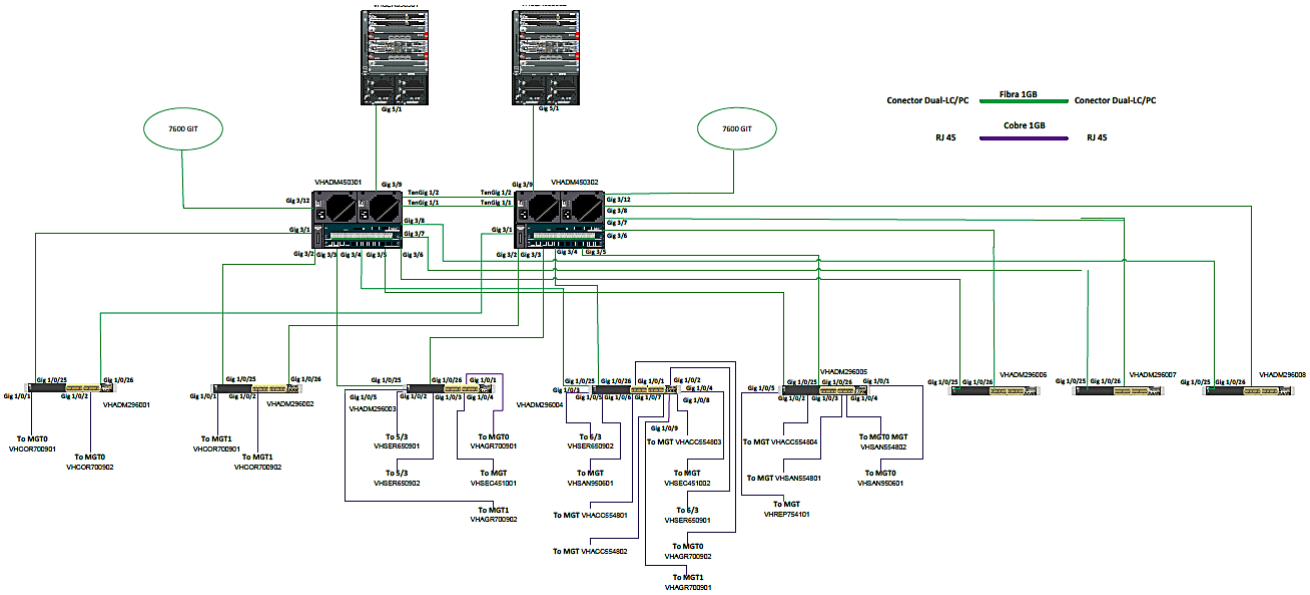


Figura 9.4 LAN – Conectividad física

9.3 Diseño de ruteo y switching lógico de red

9.3.1 Diseño de Capa 2

Esta sección describirá los aspectos considerados en el diseño de Capa para el Data Center de la red de administración. Este diseño incluye todos los mecanismos L2 para evitar lagunas e incrementar el desempeño y la estabilidad.

Un diseño de módulo de red de administración lógica Capa 2 se muestra en la siguiente figura, 9.5.

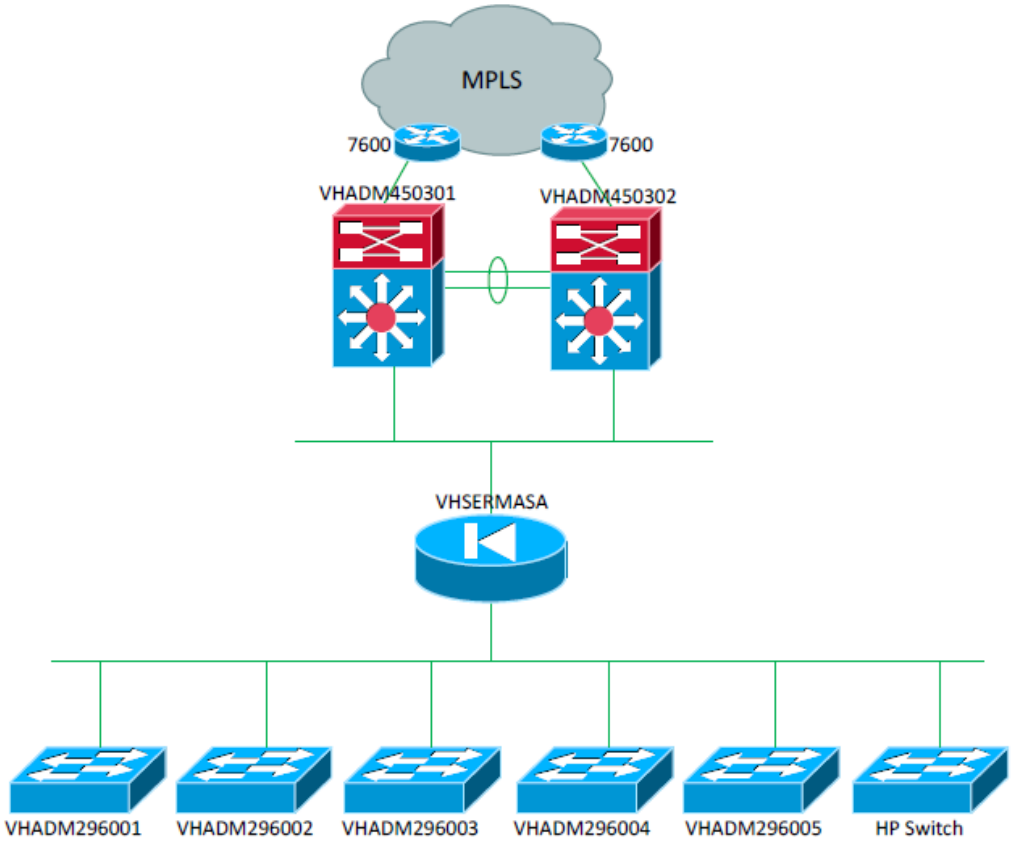


Figura 9.5 Diagrama de la red de administración L2 general

Como se vio en la figura anterior, el diseño lógico muestra un firewall entre las capas de acceso y Core de la red de administración. Lógicamente, una VLAN se extenderá desde administración a la capa de servicios en el Data Center con el fin de proporcionar conectividad. El contexto de firewall ASA fungirá como la entrada predeterminada de todos los dispositivos administrados.

9.3.1.1 VLAN

Se incluirán en el diseño de múltiples VLANs. Estas VLANs tienen funciones específicas con el fin de proporcionar el flujo de tráfico al servicio necesario.
Para el nódulo de administración, una VLAN diferente tendrá como propósito la administración de un tipo de dispositivo específico.

Tabla 9.3 Tabla de VLANs

VLAN	VLAN Name	VLAN Description
2092	MGT4500 to MGTASA	VLAN between 4500 and ASA devices
2087	Mgmt_IT	VLAN for Cisco devices and third party
2093	Failover	ASA Service Module Failover VLAN
2094	Stateful	ASA Service Module Stateful VLAN
1950	VHSERMASA01_CTX01	VLAN for ASA Context 1
1951	VHSERMASA01_CTX02	VLAN for ASA Context 2
1952	VHSERMASA01_CTX03	VLAN for ASA Context 3
1953	VHSERMASA01_CTX04	VLAN for ASA Context 4
1954	VHSERMASA01_CTX05	VLAN for ASA Context 5
1955	VHSERMASA01_CTX06	VLAN for ASA Context 6
1956	VHSERMASA01_CTX07	VLAN for ASA Context 7

1957	VHSERMASA01_CTX08	VLAN for ASA Context 8
1958	VHSERMASA01_CTX09	VLAN for ASA Context 9
1959	VHSERMASA01_CTX10	VLAN for ASA Context 10
1960	VHSERMASA01_CTX11	VLAN for ASA Context 11
1961	VHSERMASA01_CTX12	VLAN for ASA Context 12
1962	VHSERMASA01_CTX13	VLAN for ASA Context 13
1963	VHSERMASA01_CTX14	VLAN for ASA Context 14
1964	VHSERMASA01_CTX15	VLAN for ASA Context 15
1965	VHSERMASA01_CTX16	VLAN for ASA Context 16
1966	VHSERMASA01_CTX17	VLAN for ASA Context 17
1967	VHSERMASA01_CTX18	VLAN for ASA Context 18
1968	VHSERMASA01_CTX19	VLAN for ASA Context 19
1970	VHSERMASA01_CTX20	VLAN for ASA Context 20
1977	DC_ADMINISTRATORS	VLAN for DC Administrators

En la figura 9.6 se describe la configuración correcta de VLAN.

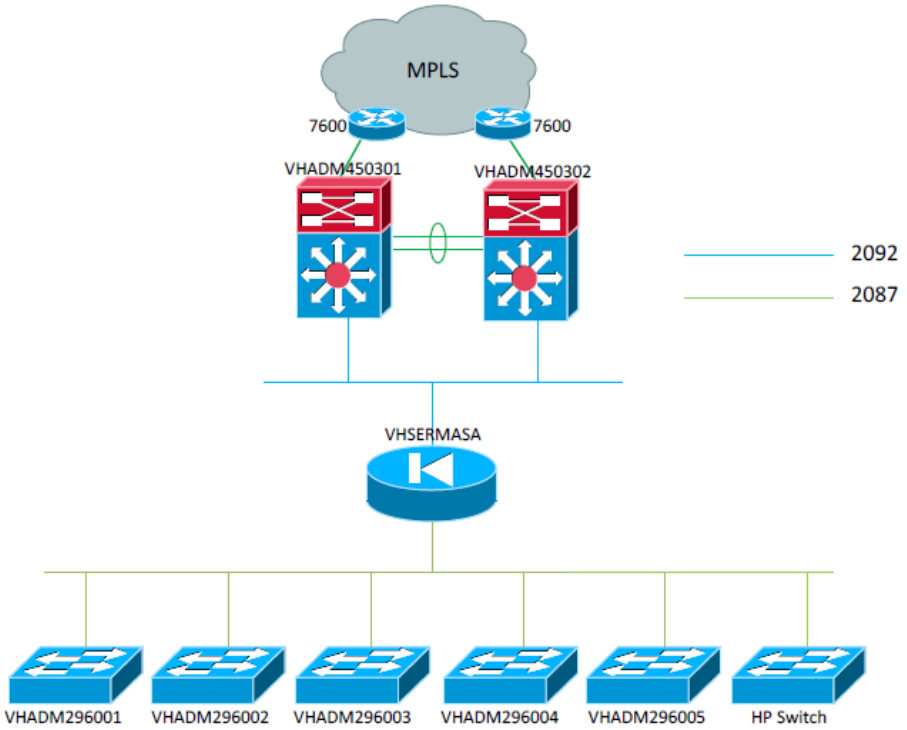


Figura 9.6 Asignación de VLAN capa 2

9.3.1.2 VLAN Trunking de VLAN

Trunking es una manera de llevar el tráfico de múltiples VLANS sobre un link capa 2 punto a punto. El estándar de encapsulación más popular utilizado en los Trunkings de VLANs es el 802.IQ (encapsulación trun estándar IEEE).
Los links de trunk capa 2 802.1Q deben ser configurados entre Catalyst 4503-E así como para los links entre ambos Catalyst 4503-E y el resto de Catalyst 2960-S.
No se implementará ningún protocol de truncking dinámico; los trunks serán definidos estáticamente.

Las mejores prácticas de Cisco no recomiendan el uso de VLAN 1 como el VLAN nativo de los trunks. Para este diseño, una VLAN (999) "dummy" se utilizará como el VLAN nativo en los puertos de trunk.

```
interface <interface type><ifSlot/ifPort>
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
end
```

Figura 9.7 Configuración de puertos Trunk

Todos los uplinks de 2960 se van a configurar como puertos trunk.

9.3.1.3 Protocolo de Trunking Virtual (VTP)

VTP significa Protocolo de Trunk VLAN (VTP), el cual se usa para reducir los esfuerzos de administración en una red switcheada. Cuando se configura una nueva VLAN en un servidor VTP, la VLAN se distribuye a través de todos los switches en el dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes en todos los switches en el dominio.

El modo definido para este proyecto será Transparente; también es importante mencionar que, de acuerdo con las mejores prácticas de Cisco, se debe configurar un nombre de dominio y contraseña.

Note: Un switch VTP transparente no anuncia su configuración VLAN y no sincroniza su configuración VLAN basado en anuncios recibidos, pero los switches transparentes sí reenvían anuncios VTP que reciben por fuera de sus puertos trunk en VTP.

Note: El nombre de dominio VTP a ser usado en el proyecto será el hostname correspondiente del dispositivo.

La tabla 9.4 describe la correcta asignación del nombre dependiendo del Dispositivo:

Tabla 9.4 Configuración de VTP

VTP Mode	Transparent
VTP Domain	<HOST_NAME>
VTP Password	JvN#&!95P%1L

La figura 9.8 demuestra la configuración correcta de VTP para el modo, dominio y contraseña:

```
switch(config)#vtp mode transparent
switch(config)#vtp domain <Domain name>
switch(config)#vtp password <vtpPassword>
```

Figura 9.8 Configuración de modo transparente de VTP

9.3.1.4 Protocolo del Árbol de Expansión (STP)

RPVST+ brinda una convergencia rápida del árbol de expansión. MSTP, que utiliza RSTP para brindar una convergencia rápida, habilita la agrupación de las VLANs dentro de una instancia de árbol de expansión, provee para múltiples rutas de reenvío para el tráfico de datos, y habilita el load-balancing. Mejora la tolerancia a fallas de la red ya que una falla en una instancia (ruta de reenvío) no afecta a otras instancias (rutas de reenvío).
El protocolo de árbol de Expansión (STP) 802.1D tiene una desventaja de convergencia lenta. Los switches Catalyst de Cisco soportan los tres tipos de STPs, los cuales con PVST+, PVST+ rápido y MST. PVST+ está basado en el estándar IEEE802.1D e incluye extensiones del propietario Cisco tales como BackboneFast, UplinkFast, y PortFast.

PVST+ Rápido está basado en el estándar IEEE 802.1w y posee una convergencia más rápida que 802.ID. RSTP (IEEE 801.w) incluye nativamente la mayoría de las mejoras del propietario Cisco para el árbol de expansión 802.1D, tales como BackboneFast y UplinkFast. PVST+ Rápido contiene estas características únicas:

- ➔ Utiliza Bridge Protocol Data Unit (BPDU) versión 2 que es compatible al revés con 802.1D STP, el cual utiliza BDPU versión 0.
- ➔ Todos los switches general BDPUs y envían a todos los puertos cada 2 segundos, mientras en 802.1D STP, solamente el bridge de raíz envía los BDPUs de configuración.
- ➔ Roles de Puerto: puerto raíz, puerto designado, puerto alterno y puerto respaldo.
- ➔ Estados de Puerto: Descartar, Aprender, y Reenviar.
- ➔ Tipos de Puerto: Puerto Orilla (PortFast), Punto-a-Punto y puerto compartido.

El RPVST+ toma ventaja del cableado punto-a-punto y proporciona una convergencia rápida del árbol de expansión. La reconfiguración del árbol de expansión puede ocurrir en menos de 1 segundo (en contraste con 50 segundos con los ajustes predeterminados en el árbol de expansión 801.1D), el cual es crítico para las redes que llevan tráfico sensible a retrasos como los de voz y video.

```
(config)#spanning-tree mode rapid-pvst
```

Figura 9.9 Configuración de modo PVST rápido

El siguiente comando, en la figura 9.10 de configuración de la interfaz asegura que un puerto opere como un puerto orilla RSTP:

```
switch(config)# interface <interface type><ifSlot/ifPort>
switch(config-if)#spanning-tree0020 portfast
```

Figura 9.10 Configuración de puerto orilla RSTP

STP puede interferir con la configuración actual si las prioridades del puerto no están establecidas correctamente. Esta configuración errónea puede causar una pérdida de conexión, interfiriendo con la integridad de la red.
Para guiar hacia la configuración prioritaria de puerto, el seguir las mejores prácticas de Cisco requerirá un puente raíz definido con prioridad de 0 y un switch de respaldo definido con prioridad de 4096 (ambos dispositivos Catalyst 4503-E), garantizando así la integridad de la red con una funcionalidad correcta de STP.

La figura 9.11 describe la asignación del puerto por cada conexión a los switches Catalyst 2960-S.

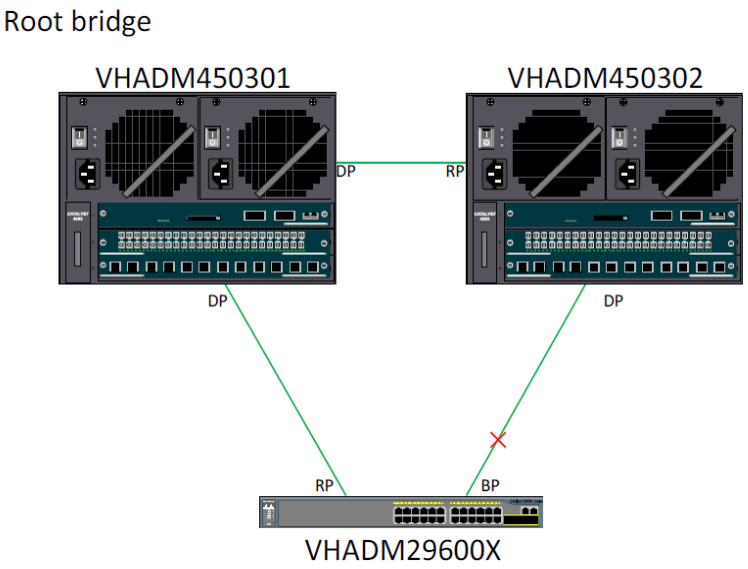


Figura 9.11 Asignación de puerto Catalyst 4503-E

La tabla 9.5 define la asignación prioritaria correcta para la configuración de STP hacia el dispositivo Catalyst.

Tabla 9.5 Configuraciones prioritarias STP

Dispositivo	STP Priority	VLAN Range
VHADM450301	0	2087-2094
VHADM450302	4096	2087-2094
VHADM296001	Default	2087
VHADM296002	Default	2087
VHADM296003	Default	2087
VHADM296004	Default	2087
VHADM296005	Default	2087

9.3.1.4.1 Resguardo raíz STP

La característica de Resguardo Raíz STP es un mecanismo utilizado para proteger la topología STP. A diferencia del Resguardo BPDU, el Resguardo Raíz STP permite la participación en STP siempre y cuando el sistema adjunto no intente convertirse en la raíz. Si el Resguardo de Raíz es activado, entonces el puerto se recupera automáticamente después de que deja de recibir los BDPUs superiores que lo haría la raíz. Resguardo raíz puede ser aplicado a uno o más puertos en los switches de orilla y en switches internos en una red. En general, se aplica esta característica a aquellos puertos en cada switch que no debe convertirse en la raíz.

```
interface <interface-name>
spanning-tree guard root
```

Figura 9.12 Habilitando resguardo de raíz

La característica de resguardo raíz será implementada como un rasgo de seguridad con el fin de prevenir switches “rogue” que reclamen el rol de switch de raíz.

9.3.1.4.2 Portfast STP

Portfast STP usa un puerto LAN Capa 2 configurado como un puerto de acceso para entrar inmediatamente en estado de reenvío, evitando los estados de escuchar y aprender. Puede utilizar PortFast en los puertos de acceso Capa 2 conectados a una sola estación de servicio o servidor para permitir a aquellos dispositivos conectarse a la red inmediatamente, en vez de esperar a que STP converja. Las interfaces conectadas a una sola estación de servicio o servidor no deben de recibir unidades de datos de protocolo de puente (BPDUs). Cuando se configura para PortFast, un puerto aun trabaja el protocolo del árbol de expansión. Un puerto habilitado con PortFast puede hacer la transición inmediatamente al estado de bloqueo si es necesario (esto puede pasar en recepción de un BDPU superior. PortFast puede ser habilitado en puertos trunk. PortFast puede tener un valor operacional que es diferente al valor configurado. Debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar para que STP converja, debe ser solamente utilizado en puertos de acceso (edge). Si habilita PortFast en un puerto conectado a un switch (un puerto de red), puede ser que cree una laguna de puenteo temporal.

```
switch(config)# interface <interface type><ifSlot/ifPort>
switch(config-if)#spanning-tree portfast
```

Figura 9.13 Configuración de portfast

9.3.1.5 EtherChannel

Un EtherChannel consiste en ligas Fast Ethernet individuales, Ethernet Gigabit o 10 Ethernet Gigabit unidos en un sólo link lógico. El EtherChannel brinda un ancho de banda full-duplex combinando múltiples Fast Ethernet hasta 800Mbps, Ethernet Gigabit hasta 8Gbps, y Ethernet Gigabit hasta 80 Gbps.
Cada EtherChannel puede formarse de hasta ocho interfaces Ethernet compatiblemente configuradas. Todas las interfaces en cada EtherChannel debe tener la misma velocidad, y todas deben estar configuradas ya sea como interfaces Capa 2 o Capa 3.

Note: El dispositivo de red al que su switch está conectado puede imponer sus propios límites para el número de interfaces en el EtherChannel.

Si falla un link dentro de un EtherChannel, el trafico llevado anteriormente sobre aquel link fallido se cambia a los links sobrantes dentro del EtherChannel. Se envía una trampa para la falla, identificando el switch, el EtherChannel, y el link fallido. Los paquetes interiores de broadcast y multicast en un link en un EtherChannel se encuentran bloqueados para regresar a cualquier otro link en el EtherChannel.

Una configuración de EtherChannel entre ambos dispositivos Catalyst 4503-E se muestra en la figura 9.14

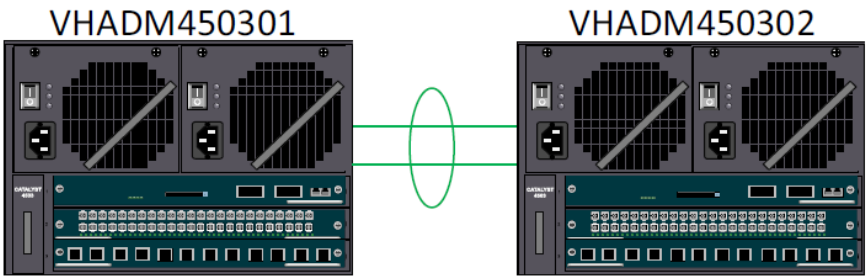


Figura 9.14 Diagrama de configuración de EtherChannel

La configuración de Port-Channel asignada para este proyecto entre los switches Catalyst 4503-E se describe en la tabla 8.26

Tabla 9.6 Configuración de Port-Channel

Port-Channel	Dispositivo	Ports	Dispositivo	Port
1	MGT450301	Gig 1/3, Gig 1/5	MGT450302	Gig 1/3, Gig 1/5

Para este proyecto, el protocolo LACP se utilizará como el método preferido para formar un EtherChannel. El método de carga se modificará para incluir las direcciónes IP fuente y de destino en el algoritmo. La figura 8.37 describe la configuración requerida para la interfaz física que se convertirá en parte de EtherChannel.

```
port-channel load-balance src-dst-ip exclude vlan
interface <interface type> x/y/z
channel-protocol lacp
channel-group <Same EtherChannel number> mode active
exit
```

Figura 9.15 Ejemplo de la configuración de EtherChannel

La siguiente plantilla, en la figura 9.16, muestra la configuración correcta para una interfaz lógica EtherChannel

```
interface port-channel <EtherChannel number>
description <Etherchannel description>
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan <VLAN ID>
switchport trunk allow vlan <VID>
switchport mode trunk
```

Figura 9.16 Continuación de ejemplo de configuración de EtherChannel

9.3.2 Diseño Capa 3

Esta sección describe todos los aspectos considerados en el diseño de Capa 3 para la red de administración del Data Center. Este diseño incluye todos los mecanismos L3 para evitar lagunas e incrementar el desempeño y la estabilidad.

9.3.2.1 OSPFv2

Open Shortest Path First versión dos (OSPF) es un protocolo de entrada interior (IGP) que rutea los paquetes IP solamente dentro de un dominio (sistema autónomo) de ruteo. Recoge información del estado del link de los ruteadores disponibles y construye un mapa de topología de la red. La topología determina la tabla de ruteo presentada a las Capas, quienes toman decisiones de ruteo basadas solamente en la dirección IP de destino encontrada en los paquetes IP. OSPF fue diseñado para soportar modelos de dirección Variable-Length Subnet Masking (VLSM) o Classless Inter-Domain Routing (CIDR).
OSPF detecta cambios en la topología, tales como fallas en el link, de manera rápida y converge en una estructura nueva libre de lagunas, en segundos.
Puede dividir las redes OSPFv2 en áreas. Una red OSPF puede ser estructurada, o subdividida, en áreas de ruteo para simplificar la administración y optimizar el tráfico y la utilización de recursos. Las áreas identificadas con los números 32-bit, expresadas ya sea simplemente en decimal, o muy seguido en notación punto decimal basada en octeto, familiar a notación de dirección IPv4.
Para este proyecto, se tiene la intención de usar OSPF entre los switches core de administración y los ruteadores orilla en el sitio para brindar conectividad a las redes remotas.

La información básica y parámetros a ser usados en los dominios OSPF se muestran en la tabla 9.7:

Tabla 9.7 Parámetro básico en la red de administración OSPF

Process ID	1
Router ID	Loopback 1 interface
Authentication	MD5
Logging adjacency changes	Yes
Cost	Default
Timers	1,3
MTU	Ignore
Redistribution	Yes

9.3.2.2 Estática

Las rutas estáticas definen caminos específicos entre dos ruteadores. Estas ruta no pueden ser actualizadas automáticamente; Usted debe reconfigurar las rutas estáticas de manera manual cuando ocurran cambios en la red. Las rutas estáticas utilizan menos ancho de banda que las rutas dinámicas. No se utilizan ciclos CPU para calcular y analizar las actualizaciones de ruteo.
Sólo debe usar rutas estáticas en ambientes en donde el tráfico de red es predecible y en donde el diseño de la red es simple. No debe usar rutas estáticas en redes grandes cambiantes porque las rutas estáticas no pueden reaccionar a los cambios en la red. La mayoría de las redes utilizan rutas dinámicas para comunicarse entre ruteadores, pero tienen una o dos rutas estáticas configuradas para casos especiales. Las rutas estáticas también son útiles para especificar una entrada de último recurso (un routeador predeterminado al cual se envían todos los paquetes enrutables).
El ruteo entre el Firewall ASA y el Catalyst 4500's será estático. Estas rutas van a mandar todo el tráfico destinado a las diferentes VLANs de administración por detrás del firewall ASA, y por consiguiente a la Red de Administración.
En relación con el segmento de administración de red (definido en el documento dirección IP como 172.28.183.0/24), una ruta estática señalará la interfaz externa del ASA.

La figura 9.17 representa la configuración necesaria para la ruta estática definida en la Red de administración.

```
ip route 172.28.183.0 255.255.255.0 172.28.182.3 name TO_MGT_NETWORK
ip route 172.28.182.240 255.255.255.240 172.28.182.3 name TO_MGT_NETWORK
```

Figura 9.17 Configuración de ruta esática para la red de Administración

9.3.2.3 Redistribución de ruta

La redistribución de ruta es necesaria para anunciar los segmentos de red detrás del módulo ASA. Un mapa de ruta será configurado para controlar las rutas estáticas anunciadas al dominio OSPF.

```
ip prefix-list STATIC_to_OSPF seq 5 permit 172.28.183.0/24
!
route-map STATIC_to_OSPF permit 10
match ip address prefix-list STATIC_to_OSPF
!
router ospf 1
redistribute static metric 100 subnets route-map STATIC_to_OSPF
```

Figura 9.18 Redistribución OSPF de ruta estática

La lista de prefijo STATIC_to_OSPF será el filtro utilizado en la redistribución. Cuando una nueva ruta estática necesita ser anunciada, una nueva línea en esta lista de prefijo necesita ser añadida.

9.3.2.4 Control dinámico del protocolo del host (Dynamic Host Control Protocol DHCP)

El Dynamic Host Control Protocol (DHCP) consiste en dos componentes: un protocol para la entrega de parámetros de configuración específicos del host desde un Servidor DHCP a un host, y un mecanismo para la asignación de las direcciones de red para los hosts. DHCP se construye en un modelo cliente/servidor, en donde los hosts del servidor DHCP designado asignan las direcciones de red y entregan los parámetros de configuración para hosts dinámicamente configurados.
De manera predeterminada, los ruteadores de Cisco que trabajan con software Cisco IOS incluyen el servidor DHCP y el software de agente de retransmisión.
DHCP lo hace capaz de asignar automáticamente direcciones IP reusables para clientes DHCP. La característica del servidor Cisco IOS DHCP es la completa implementación del servidor DHCP que asigna y administra las direcciones IP desde direcciones especificadas dentro del ruteador a los clientes DHCP. Si el servidor Cisco IOS DHCP no puede satisfacer una solicitud de DHCP de su propia base de datos, puede reenviar la solicitud a uno o más servidores DHCP secundarios definidos por el administrador de red.

La figura 9.19 muestra los pasos básicos que suceden cuando un cliente DHCP solicita una dirección IP de un servidor DHCP.

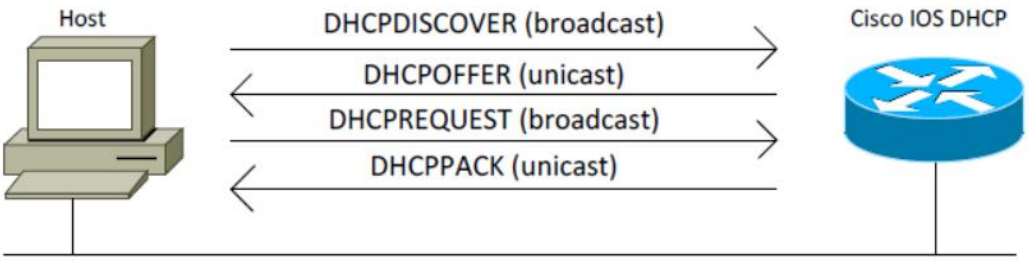


Figura 9.19 Flujo de solicitud DHCP

El cliente, host A, manda un mensaje broadcast DHCPDISCOVER para ubicar al servidor Cisco IOS DHCP. Un servidor DHCP ofrece los parámetros de configuración (tales como la dirección IP, la dirección MAC, un nombre de dominio, y un alquiler para la dirección IP) al cliente en un mensaje unicast DHCPOFFER.
En relación con el proyecto de la Empresa, DHCP tiene el propósito de ser utilizado para dar una dirección IP dinámica a las PCs del administrador del Data Center. Los administradores se van a conectar a un puerto reservado en los switches 2960 y tendrán una IP de los servidores DHCP (en este caso, los switches core de administración).

Tabla 9.8 Parámetros DHCP para la red de Administración

DHCP Pool Name	VH_ADMIN_POOL
Network	172.28.xxx.xxx/28
Default Gateway	172.28.xxx.xxx
VLAN	1976
Domain Name	Empresa.com
Excluded addresses	172.28.xxx.xxx-254

9.3.2.5 Protocolo de ruteo en espera (Hot Standby Routing Protocol HSRP)

El Hot Standby Router Protocol (HSRP) es el método estándar de Cisco para proporcionar alta disponibilidad de red por medio de brindar redundancia first-hop para los hosts IP en una LAN IEEE 802 configurada con una dirección IP predeterminada de entrada. HSRP rutea el tráfico de IP sin depender de la disponibilidad de ningún ruteador. Habilita una serie de interfaces de router para trabajar juntos y proyectar la apariencia de un router virtual o entrada predeterminada a los hosts en la LAN.

Cuando HSRP es configurado en una red o segmento, provee una dirección virtual Media Acces Control (MAC) o una dirección IP que es compartida por un grupo de ruteadores configurados. HSRP permite a dos o más ruteadores de configuración HSRP utilizar la dirección MAC y la dirección de red IP de un ruteador virtual. El ruteador virtual no existe; representa el objetivo común para los ruteadores que han sido configurados para proporcionarse respaldo unos a otros. Uno de los ruteadores es seleccionado para ser el ruteador activo y otro para ser el ruteador standby, el cual asume el control del grupo de dirección MAC o dirección IP en caso de que el router activo designado falle.
Para minimizar el tráfico de red, solamente los ruteadores activo y Standby envían mensajes HSRP periódicos una vez que el protocolo ha completado el proceso de elección. Si falla el ruteador activo, el ruteador Standby toma el lugar del ruteador activo. Si el ruteador falla o se convierte en el ruteador Activo, entonces otro ruteador es seleccionado como ruteador Standby.

Las siguientes configuraciones, en las figuras 9.9 y 9.10 de HSRP se encuentran presentes en el Módulo de administración de red:

Tabla 9.9 Parámetros HSRP en VHADM4500

Interface	Virtual IP	Preempt	Timers	Coment
VLAN 2092	Last IP of the segment	Yes	Hello time 1 sec, hold time 3 sec	LINK BETWEEN 4500'S AND ASA FIREWALLS
VLAN 1950 to 1969	Last IP of the segment	Yes	Hello time 1 sec, hold time 3 sec	LINK BETWEEN 4500'S AND ASA FIREWALLS

Tabla 9.10 Más parámetros HSRP en VHADM4500

Primary device	VHADM450301
Secondary device	VHADM450302
Authentication	MD5
Authenticacion password	H#$%466Cd
Primary priority	110
Secondary Priority	100

Para habilitar HSRP bajo la Red de Administración, se debe aplicar la siguiente configuración mostrada en la figura 9.20:

```
interface <interface type> x/y/z
standby <group-number><ip><virtual-ip-address>
! priority
standby <group-number> priority <priority-number>
! preempt
standby <group-number> preempt
exit
```

Figura 9.20 Ejemplo de configuración HSRP

La prioridad de respaldo entre el dispositivo Catalyst Primario y Secundario debe ser establecido con un valor de prioridad +10 desde el Switch principal. Una configuración adquirida por adelantado debe ser aplicada para asegurar la redundancia entre el grupo HSRP, en caso de fallas.
La autenticación entre los grupos HSRP también debe der aplicada siguiendo las plantillas que se muestran en la figura 9.21.

```
interface <interface type> x/y/z
standby <group-number> authentication md5 key-string <key-string> key <timeout seconds>
exit
```

Figura 9.21 Ejemplo de autenticación HSRP

9.3.3 Resistencia

La configuración física definida requiere de comunicación a todas horas para una implementación redundante exitosa. Siguiendo las mejores prácticas de Cisco aplicables, una línea primaria y una de respaldo son prácticamente un requerimiento permanente para este tipo de topologías.
Los dos Switches Cisco Catalyst 4503-E, responsables del Capa Core, comparten una conexión entre ellos de dos links de 10GB. Este escenario está respaldado por la configuración del puerto de ambos ocho Catalyst 2960-S, en donde todos comparten una conexión a ambos Switches Core Catalyst 4503-E.
La figura 9.22 contiene un diagrama que detalla el tipo de conexión previamente mencionada.

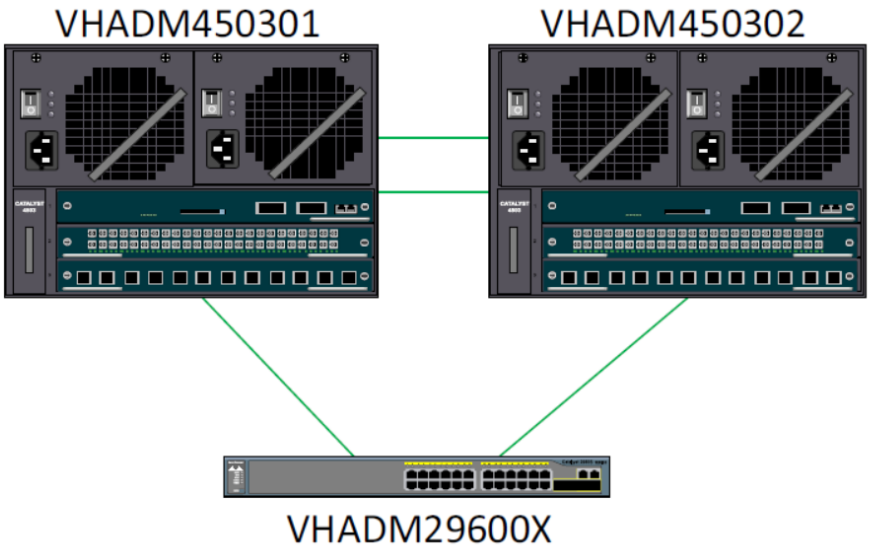


Figura 9.22 Configuración redundante para dispositivos Catalyst

9.4 Flujos de Tráfico

Una descripción completa de la topología de flujos de tráfico, se describe en la figura 9.23.

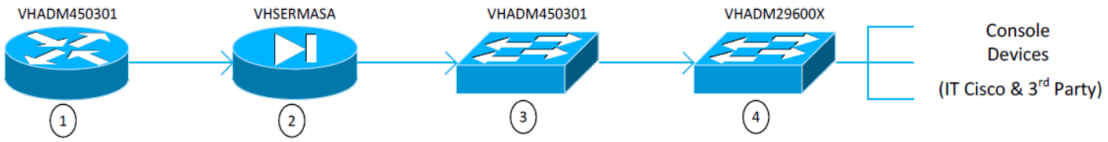


Figura 9.23 Flujo de tráfico

1. El tráfico llega a los Switches Catalyst 4503-E a través de la red MPLS
2. El tráfico es reenviado al Firewall ASA para inspección
3. El tráfico es regresado a los Switches Catalyst 4503-E (solamente en L2)
4. El tráfico es reenviado a los Switches Catalyst 2960-S y alcanza las IT de Cisco y las VLANs de administración de terceras partes.

El mismo escenario se aplica de modo inverso cuando el tráfico es enviado a través de Catalyst 2960-S desde los dispositivos de la consola.

9.5 Escenarios de Errores

La figura 9.24 tiene por objeto describir los posibles escenarios de error que se presenten en la actual topología disponible para la administración de redes.

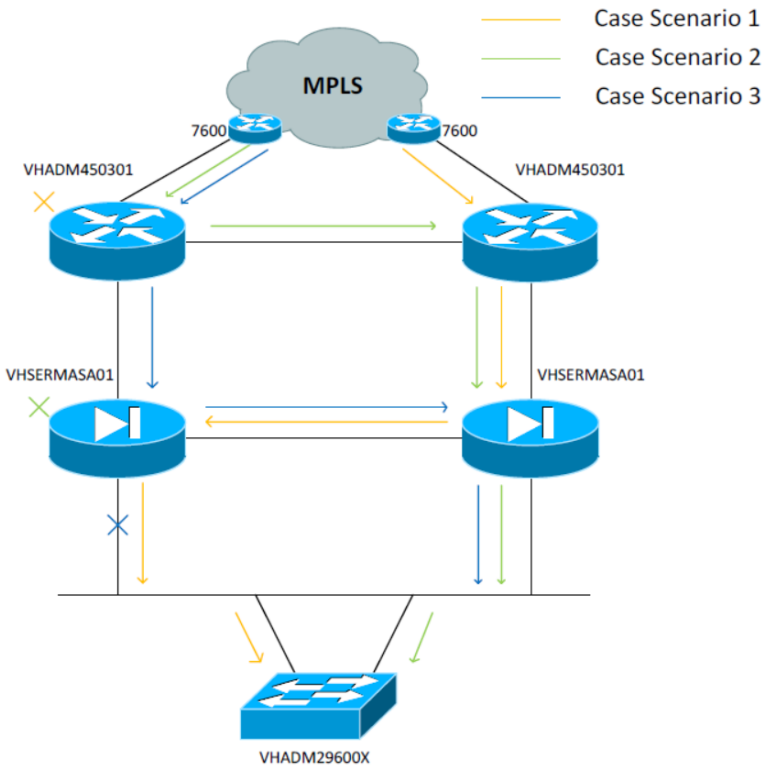


Figura 9.24 Escenarios de errores

Escenario caso 1
El tráfico llega al switch del catalizador 4503-E a través de la conexión de red MPLS, pero el switch del catalizador 4503-E Switch falla inesperadamente. La red redundante diseñada para la administración de red reconoce este error y reenvía el tráfico a través del switch del catalizador 4503-E funcionando como copia de seguridad. El tráfico se envía entonces al ASA Firewall 2 donde se reenvía al principal enlace conFigurad (The ASA Firewall 1). El tráfico a continuación funciona como se esperaba en el diseño, alcanzando los switches de catalizador 2906-S.

Escenario caso 2
El tráfico llega al principal switch del catalizador 4503-E a través de la conexión de red MPLS como se espera tomando en cuenta el diseño actual. En caso de que ASA Firewall 1 deje de funcionar, ASA Firewall 2 toma el papel principal en el flujo de la red. El tráfico se reenvía a ASA Firewall 2 por medio de la redundancia de capa 2.

Escenario caso 3
El tráfico llega al principal switch de catalizador 5403-E a través de la conexión a la red MPLS, y luego es enviada a ASA Firewalls como es lo esperado debido al diseño actual. Si el nexo

principal entra el catalizador 2960-S y ASA Firewalls falla, el tráfico es reenviado a la unidad de ASA Firewall2 como copia de seguridad teniendo en cuanta la configuración de red redundante.Se aplican los mismos escenarios de casos si se presentan fallas en un flujo inverso.

9.6 Calidad de Servicio (QoS)

Una red de comunicaciones es la columna vertebral de cualquier organización exitosa. Estas redes transportan una gran cantidad de aplicación es de datos, incluyendo videos de alta calidad y datos sensible al retraso como la voz en tiempo real. Las aplicación es intensivas para el ancho de banda estiran los recursos y las capacidades pero también complementan, agregan valor y mejoran todos los procesos del negocio. Las redes deben proporcionar servicios seguros, predecibles, medibles, y a veces garantizados. Alcanzar la calidad requerida de servicio (QoS) mediante la gestión de configuraciones específicas se convierte en el secreto de una solución de negocio. Por lo tanto, QoS es el conjunto de técnicas para administrar los recursos de red.

Para este proyecto, Cisco seguirá las políticas de QoS aplicadas por la Empresa. En el momento de escribir este LLD, no hay ninguna información acerca de las políticas de QoS.

Referencias

Zacker Craig, Redes. Manual de referencia. Madrid, España, Editorial McGRAW-HILL,1ª edición, traduccción de Manuel Carracedo Cadierno, Ángel Moreno Blázquez y Felipe Lesmes Zabalegui, 2002,1007 págs.

A. Hallberg Bruce, Fundamentos de redes. CDMX, México, Editorial McGraw-Hill, 4ª edición, traducción de Carlos Roberto Cordero Pedraza, 2007, 444 págs.

C.Sackett George, Manual de Router Cisco. Madrid, España.Editorial McGRAW-HILL, 2ª edición, traducción de Ricardo de Córdoba Herralde, 2002, 868 págs.

CISCO Systems Inc, Cisco. San Jose, CA [en linea].[fecha de consulta: 12 octubre 2015] Disponible en: http://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9700-series-multilayer-directors/guide-c07-732733.html

CISCO Systems Inc, Cisco. San Jose, CA [en linea].[fecha de consulta: 12 octubre 2015] Disponible en: http://www.cisco.com/c/en/us/products/switches/nexus-7000-series-switches/index.html

CISCO Systems Inc, Cisco. San Jose, CA [en linea].[fecha de consulta: 12 octubre 2015] Disponible en: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/solution_overview_c22-574939.html

CISCO Systems Inc, Cisco. San Jose, CA [en linea].[fecha de consulta: 12 octubre 2015] Disponible en:http://www.ciscopress.com/articles/article.asp?p=2294214

CISCO Systems Inc, Cisco. San Jose, CA [en linea].[fecha de consulta: 12 octubre 2015] Disponible en:http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

CONCLUSIONES

CONCLUSIONES

El sector de la industria, desde los inicios de la modernización tecnológica, se ha enfrentado a grandes retos para modificar sus procesos de operación y logística, los cuales aumentan su complejidad día a día, pues se requiere ofrecer servicios de red de una forma segura y controlada. Estos servicios deben de estar disponibles de modo coherente además de tener la capacidad de crecer proporcionalmente a los requisitos del negocio. Para cumplir estos objetivos, un grupo selecto de empresas que se encarga de desarrollar nuevas soluciones tecnológicas, tales como CISCO, IBM, HP, DELL, entre otras, han creado soluciones en Data Center que funcionan como elementos intermedios entre la nube pública y el entorno corporativo privado para proveer a los usuarios un entorno confiable, seguro y de fácil administración. Para lograr esto, los Data Center requieren de un conjunto de herramientas, tecnologías, procedimientos y recomendaciones para que la implementación de la arquitectura e infraestructura de los Data Center pueda ser eficaz. Sin lugar a dudas la implementación de un Data Center no debe de dejar de lado el diseño lógico de la infraestructura de la empresa, pues el éxito radica en la buena adaptación de los componentes de un Data Center o la renovación de ciertas áreas para integrar la mayor parte de los recursos y las aplicaciones de la empresa y así optimizar costos y evitar pérdidas.

Se ha demostrado que un mal diseño lógico o no seguir las recomendaciones de implementación de los componentes que conforman la infraestructura del Data Center, puede provocar la mayoría de los errores Post – Liberación del proyecto. Tales como sobrecarga de tráfico, colisiones, pérdida de información, errores de conexión entre los dispositivos de red, entre otros. Este tipo de incidentes provoca que la administración de un Data Center sea cada vez más complicada.

Es por ello que para disminuir la mayor parte de los incidentes durante la implementación, es necesario apegarse a los *objetivos esenciales* de la arquitectura de un Data Center, estos objetivos son: Escalabilidad, disponibilidad, seguridad y fácil administración. De esta forma podemos atender la demanda creciente de las aplicaciones, usuarios y tecnología con un rendimiento aceptable. Un Data Center debe de tener la capacidad de atender la demanda creciente de los servicios que ofrece la empresa y a sus respectivos usuarios con un nivel de rendimiento aceptable en todos sus componentes. Como administradores de la infraestructura del Data Center, se requiere prestar principal atención en los componentes que requieren escalabilidad y como experiencia durante el proyecto los componentes de red (Acceso y Distribución), la infraestructura, el almacenamiento y los dispositivos para administración son los que están sujetos a constantes cambios y por ser la estructura medular son los que requieren escalabilidad.

La *escalabilidad* se aplica a dimensiones distintas en cada componente. En el caso de los medios conectados a la red, se trata por ejemplo el ancho de banda y el incremento de los puertos, para los servidores es la capacidad de procesamiento y para el almacenamiento es el tamaño y la velocidad de las operaciones de entrada / salida al disco.

Para ampliar un componente de forma eficaz es esencial identificar la naturaleza del incremento de la demanda, el impacto en los distintos dispositivos, así como el coste – beneficio de modificar los componentes. Una vez identificado el problema se puede emplear una estrategia de escalabilidad de aumento o de ampliación.

La *disponibilidad* depende en gran parte de la disciplina informática y de las políticas internas corporativas, las cuales deben someter a los dispositivos de red a pruebas rigurosas y mecanismos ágiles de actualización y configuración, además de incluir un manual de control de cambios.

La clave de la disponibilidad se basa en aislar la funcionalidad del servicio, de los errores de cada componente individual. Esto puede lograrse mediante la eliminación de las dependencias en espacio o tiempo que un servicio pueda tener con respecto a un componente individual de la arquitectura del Data Center. Es por ello que para lograr la alta disponibilidad de los equipos del Data Center es necesario tener en cuenta los posibles eventos que pudieran afectar su funcionamiento, además de configurar por cada nivel un equipo o enlace redundante, así estamos asegurando la disponibilidad de las capas de acceso y distribución del Core. Como se mencionó anteriormente la disponibilidad de los servicios dependen en gran parte de la disciplina informática de la empresa y las reglas que rigen dicha disciplina se encuentran definidas en la seguridad.

Cualquier Data Center debe contemplar un módulo de *seguridad* que defina las estrategias de administración de riesgos y que incluya una adecuada protección de la confidencialidad, integridad y disponibilidad de la información. La clave de implementar mecanismos correctos de seguridad consiste en el diseño de una arquitectura y una estrategia que defina múltiples niveles de seguridad. Es por ello que la arquitectura se divide en redes físicas o segmentos de red independientes, de este modo el sistema consigue que una exposición parcial no provoque la pérdida de datos.

Es por ello que la atención principal de las tareas de seguridad debe recaer en dos áreas distintas:

- Seguridad en la red.
- Seguridad basada en host.

Debido a que la Empresa contaba con la problemática de unificar las tecnologías de Almacenamiento, Red y Virtualización de sus servicios hacia la red, es decir, la comunicación e interacción entre estas tecnologías, se decidió realizar como solución la implementación de un Data center el cual utilizando los equipos especializados como los Nexus 7000 y 5000, diseñados para manejar el procesamiento, comunicación y operación de dichas tecnologías, se redujo el uso de dispositivos de red y minimizo los costos. Con los equipos Nexus se logró crear ambientes virtuales independientes destinados a permitir la conectividad de los múltiples servidores de la empresa, los cuales a su vez soportan diferentes servidores virtuales alojando diferentes servicios y recursos de la empresa. De esta forma se logró distribuir los recursos físicos de los equipos de red para optimizar su funcionalidad y lograr la convivencia de diferentes clases de tecnologías como la de almacenamiento y red en un solo ambiente.

Por último la administración de un Data Center y de todos sus módulos requiere ser homologada a una herramienta que te permita gestionar, controlar y monitorear las operaciones de los dispositivos de red tanto físicos como virtuales y que esta a su vez sea de *fácil administración*. Cada tecnología ofrece distintas soluciones, pero para nuestro caso Cisco ofrece una solución en software para este fin.

Glosario

Arquitectura de red. Es la forma en que están interconectados y distribuidos de forma física y lógica los dispositivos que conforman la red.

ASA: Se refiere a un tipo de seguridad en Cisco, enfocada principalmente en la alta seguridad para el acceso de datos y redes de recursos.

DCI (Data Center Interconnect). Tecnologías que se usan para interconectar a nivel 2, Data Centers.

End to End. Utiliza una visión holística del proceso de monitoreo, ya que realiza las mediciones con la red en operación, observando la red de la misma forma en que la aplicación mira la infraestructura de red instalada. Permite encontrar y diagnosticar problemas de desempeño de manera rápida y remota, sin necesidad de dispositivos o agentes remotos, sin impactar significativamente el desempeño de la red, aunque ésta no sea una red propia.

Front-End. Es responsable de recoger entradas de los usuarios, y ser procesadas de tal manera que cumplan las especificaciones para que el back-end pueda usarlas. La conexión entre front-end y el back-end es un tipo de interfaz.

IDS: Es un dispositivo que manda una alarma informando un ataque pero no bloquea la conexión comprometida.

Middleware. Es un software de computadora que conecta componentes de software o aplicaciones para que puedan intercambiar datos entre éstas. Es utilizado a menudo para soportar aplicaciones distribuidas. Esto incluye servidores web, servidores de aplicaciones, sistemas de gestión de contenido y herramientas similares.

MPLS. (Multi-Protocol Label Switching) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o y la fiabilidad, y seguridad de los servicios Prívate Line, Frame Relay o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia.

Oversubscription. En un entorno SAN (red de área de almacenamiento) cambio de medio ambiente, es la práctica de conectar varios dispositivos al mismo puerto de conmutador para optimizar el uso de interruptor. Cada puerto SAN puede soportar una velocidad de comunicación particular y un switch Fibre Channel puede ofrecer puertos FC 1 Gb, 2 Gb o 4 Gb.

OVT (Overlay Transport Virtualization). Tecnología usada para extender redes de datos de nivel 2 entre Data Center distribuidos.

Servicio. Desde el punto de vista de redes, un servicio es toda aquella tecnología que puede ser accedida desde cualquier nodo o terminal y que permite a sus usuarios realizar eficazmente su trabajo con el fin de mejorar el rendimiento global de la organización.

SSL. Son las siglas en inglés de Secure Socket Layer (en español capa de conexión segura). Es un protocolo criptográfico (un conjunto de reglas a seguir relacionadas a seguridad, aplicando criptografía) empleado para realizar conexiones seguras entre un cliente (como lo es un navegador de Internet) y un servidor (como lo son las computadoras con páginas web).

Stateful firewalls. Son firewalls que actúan en **layer 3** del modelo OSI/ISO (network) donde su punto fuerte es el poder de inspeccionar estados, y saber si los mismos corresponden a una conexión ya

existente o no. Esto es posible lograrlo en Linux mediante connectrion tracking utilizando los módulos *conntrack*, y así mantener un record de los estados existentes en el sistema operativo.

SSH: Protocolo que brinda seguridad de acceso remoto.

Trunk: Es una configuración que lleva el tráfico de múltiples VLANs sobre un único link para que puedan comunicarse entre sí.

VLAN: Red virtual de área local

WAN. (Wide Area Network, redes de área extensa) son redes punto a punto que interconectan países y continentes. Por ejemplo, un cable submarino entre Europa y América, o bien una red troncal de fibra óptica para interconectar dos países. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

Índice de tablas y figuras