



**REDISEÑAR LA RED LAN Y WAN BASADO EN EL PROTOCOLO VXLAN PARA
MEJORAR LA COMUNICACIÓN DE TODAS LAS SEDES DE LA COMPAÑÍA CRC, EN
LA CIUDAD DE BOGOTÁ**

INTEGRANTES

**JONATHAN MORENO
HAROLD GARCIA**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES**

SECCIONAL BOGOTÁ D.C.

DICIEMBRE 2019



**REDISEÑAR LA RED LAN Y WAN BASADO EN EL PROTOCOLO VXLAN PARA
MEJORAR LA COMUNICACIÓN DE TODAS LAS SEDES DE LA COMPAÑÍA CRC, EN
LA CIUDAD DE BOGOTA**

INTEGRANTES

**JONATHAN MORENO
HAROLD GARCIA**

**MODALIDAD DE GRADO SEMINARIO DE PERFECCIONAMIENTO CCNA
Requisito parcial para optar al título de Ingeniero de Telecomunicaciones**

**DIRECTOR
YOVANNY L. VELA SAENZ**

**UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES
SECCIONAL BOGOTÁ D.C.
DICIEMBRE 2019**

NOTA DE ACEPTACIÓN

PRIMER JURADO

SEGUNDO JURADO

OBSERVACIONES

Bogotá, Mes, Año

CONTENIDO

RESUMEN	6
INTRODUCCION	7
GLOSARIO	8
1.Descripción del problema	10
1.1 Planteamiento del Problema	10
1.2 Justificación	12
1.3 Objetivos	13
Generales:	13
Específicos:	13
2.Marcos de referencia	13
2.1 Teórico	13
Trama VXLAN	14
Comunicación Unicast y Multicast	17
2.2 Marco institucional	19
Plataforma estratégica de la empresa CRC	19
Visión:	20
Misión:	20
Estrategia misional:	20
Líneas de servicios o productos	21
3. Metodología	22
3.1 Población	22
3.2 Técnicas para la recolección y análisis de la información	22
3.3 Tipo de investigación	22
4. Diagnóstico de las condiciones actuales de la empresa CRCS S.A.S.	23
4.1 Estado de las condiciones actuales	23
Caída de sistema CRC	23
4.2 Determinación de factores críticos	24
4.3 IDENTIFICACION DE HALLAZGOS SIGNIFICATIVOS	25
5. Diseño de ingeniería	25
5.1 PROPONER REDISEÑO DE LA RED LAN Y WAN QUE SOPORTA SERVICIO AL CLIENTE, BASADO EN LA APLICACIÓN DE LA ESTANDAR CCNA-CISCO, EN EL AREA DE GESTION INFORMATICA DE LA EMPRESA CRC S.A.S EN LA CIUDAD DE BOGOTA	26

5.1.1 Etapa 1.....	26
5.1.2 Etapa 2.....	26
5.1.3 Etapa 3.....	28
CONCLUSIONES	31
BIBLIOGRAFÍA.....	32

RESUMEN

La presente investigación tiene como referencia planear y ejecutar una reestructuración robusta y escalable para operar sobre la infraestructura de red existente en la compañía CRC, prestando bastante importancia y enfoque en el protocolo VLAN que opera sobre redes de entorno capa 2.

El protocolo VLAN tiene una posición importante en las comunicaciones de la compañía CRC, ya que estas brindan flexibilidad en la operación del día a día y tienden a facilitar y escalar rápidamente requerimientos demandantes orientados en los entornos de segmentación por áreas.

Entonces, en el siguiente trabajo se presentará el uso, limitaciones e investigaciones que han realizado los equipos investigativos de las marcas que son predominantes en el mercado mundial, la idea consiste en componer y ofrecer una estabilización en la comunicación y acceso de los servicios sin afectar el rendimiento de las redes convergentes que intervienen en esta compañía, por tal motivo se ofrece esta solución después de haber detectado la necesidad del cliente.

Es de importancia aclarar que la presente investigación es de tipo descriptiva y exploratoria puesto que tiene prioridad identificar los elementos y características del objetivo principal.

INTRODUCCION

Es importante brindar conocimiento de los constantes cambios que surgen en las redes, siempre teniendo en cuenta la creciente demanda y la diversificación de los servicios, no hay duda que la evolución de las aplicaciones tienden a tener la necesidad de contar con servicios disponibles 7x24, para cumplir con este requerimiento surge la tolerancia a fallos que han hecho que sean dedicados demasiados recursos con el fin de cumplir con estos requerimientos que garantizan la productividad de la de la compañía, su sostenibilidad y participación en el mercado mundial.

Hacemos referencia a la capa de enlace de datos que rige el modelo OSI el cual tiene un papel importante en las comunicaciones de la compañía, ya que en esta capa se realiza toda la transferencia de los datos en tramas por el enlace físico, desde este punto se tiene un control de errores, transmisión y flujo de datos.

Notamos que en el transcurso de la historia se han desarrollado y proporcionado diferentes alternativas de comunicación estos se denominan protocolos (VLAN, VTP, STP, LLDP, etc.) estos son estándares que operan en la capa del modelo OSI y permiten obtener rendimiento, convergencia y escalabilidad en las redes.

Aun así, se evidencia un problema que se mantiene al mencionar que la evolución de las redes hace a un lado los protocolos anteriormente mencionados ya que no pueden ser funcionales para las tecnologías actuales, por esta y muchas más razones, se reúnen los esfuerzos necesarios para investigar y desarrollar nuevos protocolos que garantizan el funcionamiento de las nuevas tecnologías.

Para nuestro caso es muy importante conocer cómo opera el protocolo VLAN ya que es parte fundamental de la segmentación y organización de áreas en la compañía. Se reconoce abiertamente que el no tener las redes segmentadas de acuerdo con la demanda de servicios, afecta el desempeño y funcionamiento de la operación, se pretende dar a conocer el funcionamiento de este tipo de plataformas para asegurar que la compañía logre tomar la decisión de migrar esta variedad de tecnologías, representando un ahorro económico y ambiental a un largo plazo.

GLOSARIO

- VXLAN: Virtual Extensible Local Área Network, método de superposición de redes capa 2 en redes capa 3.
- VLAN: Virtual Local Área Network, mecanismo que utilizan los switches para segmentar el tráfico entre hosts usando una única infraestructura física.
- Multicast: Es el envío de información a múltiples destinos simultáneamente.
- ISP's: Internet service provider (proveedor de servicios de Internet) es la empresa que brinda conexión a Internet a sus clientes.
- SLAs: (Service Level Agreement).
- Tramas: Es una serie sucesiva de bits, organizados en forma cíclica que transportan información a través de la red.
- 802.1Q: Desarrollo que permite interconectar múltiples redes compartiendo un mismo medio físico sin interferencias.
- VTP: VLAN Trunking Protocol, facilita la administración de una red conmutada realizando distribución de Vlan`s por todos los SW`s del mismo dominio.
- Payload: Corresponde al área de datos que se desean transportar en una trama.
- Hypervisor: Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar al mismo tiempo diferentes sistemas operativos sobre el mismo hardware.
- VSM (Virtual Supervisor Module): Módulo que controla varias VEMs como un switch virtual distribuido.
- LLDP: Link Layer Discovery Protocol, este protocolo se encargó de reconocer los dispositivos en la red, adicionalmente permite compartir información detallada

acerca de ellos mismos a otros dispositivos que también están conectados directamente a la red.

- STP: Spanning Tree Protocol, su función es identificar y eliminar lazos en enlaces redundantes.
- VEM (Virtual Ethernet Module): Hace parte del software del hypervisor, toman la configuración del VSM y realiza las tareas de capa 2 y funciones de red como un switch físico.
- Token Ring: Consolidado en el estándar 802.5, se define como una topología física en anillo que utiliza la técnica de control de acceso al medio para poder establecer una comunicación entre hosts.
- Server Sprawl: Expansión del servidor es una situación en la que varios servidores subutilizados ocupan más espacio y consumen más recursos de los que pueden justificarse por su carga de trabajo.
- SDN: Una categoría de tecnologías que separa el plano de control de la red del plano de reenvío para permitir un aprovisionamiento más automatizado y una gestión de recursos de red basada en políticas.
- VNI (VXLAN Network Identifier): La ID de VXLAN (llamada Identificador de red de VXLAN o VNI) tiene una longitud de 24 bits en comparación con la ID de VLAN de 12 bits. Por lo tanto, proporciona más de 16 millones de ID únicos.
- VM: Virtual machine o alojador de una maquina virtual.
- Overlay Network: Una red superpuesta es una red de telecomunicaciones que se construye sobre otra red y es compatible con su infraestructura.
- VTEP: Punto terminal virtual (Virtual Terminal Endpoint)

1. Descripción del problema

1.1 Planteamiento del Problema

VXLAN es un método de superposición que extiende el tráfico de capa 2 sobre una capa 3 basada en IP

A través de su encapsulación es posible aumentar considerablemente el número de redes que se desea transportar, sin importar el alcance geográfico para la implementación de redes capa 2.

VXLAN se basa en la multidifusión, esta extensión de la funcionalidad de VLAN nos permite alcanzar un máximo de 16 millones de redes que pueden converger en una misma implementación de VXLAN. El uso de VXLAN simplifica notablemente la gestión de los segmentos de red y el Routing, a la vez que elimina la necesidad de realizar cambios a la red física cuando nos encontramos en el proceso de aprovisionamiento.

Actualmente vemos como las grandes y medianas organizaciones migran sus servicios e infraestructura a Datacenters, se realiza con el objetivo de disminuir costos y recibir grandes beneficios (Disponibilidad, atención 7 x 24 x 365, mayor eficiencia, menor costo de operación, velocidad del negocio, opción de crecimiento y escalabilidad).

El mejor negocio que adoptan estas empresas las cuales su CORE de negocio no es administrar las redes ni el desarrollar aplicaciones, es contratar estos servicios a través de proveedores consultoría que realmente si garantizan el funcionamiento de las aplicaciones que utilizan estas grandes y medianas organizaciones.

Estos se encargan de administrar y distribuir servicios de Datacenter cuentan con el personal y la infraestructura dedicada he idónea para mantener la disponibilidad de los servicios, dando tranquilidad y garantía a sus clientes, regidos por los acuerdos de servicio o SLAs.

En lo que va de la historia, hasta nuestros días, los ingenieros han implementado en los Datacenters redes de conexión interna para todos sus clientes, estas redes internas son compartidas y son construidas de esta manera con el objetivo de reducir gastos (Hardware, administración de equipos).

El desarrollo de protocolos de red permite que estos esquemas compartidos funcionen correctamente, como lo es el protocolo VLAN, el cual logra realizar una segmentación lógica de una red sobre un entorno físico compartido, las diferentes estaciones se combinan en una solución de red independiente de su ubicación, garantizando exclusividad en la transmisión de datos para cada uno de los clientes que se incluyen dentro de este esquema compartido.

En cuanto a los servicios y aplicaciones de una compañía, convierten los entornos en áreas compartidas que tienden a surgir con el desarrollo de la era de la virtualización, esta era surge como necesidad lo que comúnmente denominamos proliferación de servidores. Al mantener cantidad de servidores alojados en una infraestructura es inferir en costos y complejidad para administrar dicha red.

Los administradores de Datacenter se enfrentan a problemas como: el aumento de personal, lo que genera crecimiento en la virtualización de servidores, con el fin, de desplegar plataformas de servicios en la nube y esto ha hecho, aumentar las exigencias de la infraestructura de red física interna para publicar los aplicativos. Actualmente, con la fuerte demanda y basados en los protocolos de comunicaciones, los clientes exigen conexiones alternas y de contingencia, haciendo que se dificulte la labor de ejecutar despliegues de redes en la segunda capa del modelo OSI, de acuerdo a cada servicio solicitado.

Teniendo en cuenta lo anterior se presenta un alto consumo de procesamiento en los dispositivos Switches, afectando directamente la administración de las tablas MAC, los switches operan en un entorno compartido que garantiza la conectividad a cientos o miles de servidores que comparten estos recursos físicos.

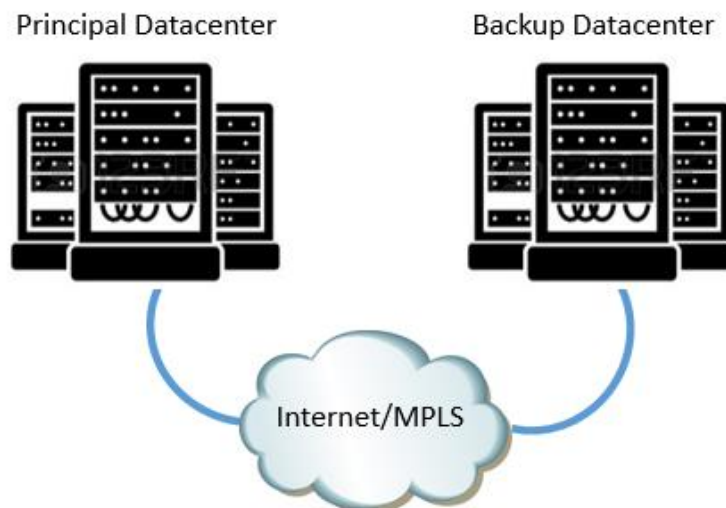


Ilustración 1, Esquema de redundancia en Datacenter

Se debe aclarar que el protocolo VLAN ha tenido una larga trayectoria en la utilización de los entornos compartidos que facilitan el escalamiento de la red, siempre garantizando la seguridad e integridad en los servicios que se prestan al cliente. La composición de las

VLANs está dada por tan sólo 12 Bits para diferenciación e identificación de la VLAN, teniendo en cuenta que siempre debe de cumplir con el etiquetado de las tramas referentes del estándar 802.1Q, es decir, que la longitud desarrolla una capacidad de 4096 VLAN disponibles dentro de nuestro entorno de red.

A cada VLAN se le asigna su propia identificación única haciendo que esto sea una limitante, ya que la mayoría de los clientes adquieren varias VLAN ID para la segmentación de los servicios.

Hablando un poco de las limitantes para las VLAN, cabe resaltar que estas fueron diseñadas para ser implementadas en redes físicas con diferentes ambientes corporativos, su limitante es, la configuración y administración se realizada en los dispositivos físicos de la red de la organización. Los entornos virtualizados pueden hacer uso de estas VLANs, pero solamente de VLANs que ya existen en la red física, por lo que desde los entornos virtualizados no se pueden definir nuevas VLANs sin intervención en los dispositivos de red física.

Aquí es donde vemos que el protocolo VXLAN opera bajo el modelo de SDN (Software Defined Network) enfoque aplicado a la administración de los sistemas de interconexión de red y a la centralización de una forma eficiente para un mejor rendimiento. SDN garantiza que el administrador de red pueda gestionar los servicios de interconexión a través de comandos de bajo nivel, minimizando los errores y fallas humanas.

1.2 Justificación

La finalidad de este trabajo es dar a conocer las ventajas de aplicar he utilizar los protocolos de comunicaciones, para así, poder comprender que a medida que avanzan los desarrollos tecnológicos, los protocolos y los estándares mundiales, podemos mejorar el rendimiento de las redes de comunicaciones, proveer nuevos servicios, garantizar una mayor estabilidad, escalabilidad, estando a la vanguardia, ya que esto implica cambios positivos para las organizaciones, y esto conlleva a facilitar la administración de la red.

Los ambientes virtualizados serán el futuro de las redes de comunicaciones, por lo cual, podemos afirmar que existen varios protocolos que cumplen con los estándares de calidad que los clientes exigen y necesitan. En este trabajo investigativo hablaremos específicamente del protocolo VXLAN el cual es uno de los más importantes para los nuevos entornos de virtualización.

A medida que surgen nuevas tecnologías, que es cada vez más rápido, la demanda es mucho más exigente para los ingenieros, diseñadores, etc. el tener que estar actualizados para así, proponer nuevas mejoras que ayuden a la efectividad del transporte de la información. Por esta razón se realiza este trabajo, queremos dar a conocer esta tecnología, su aplicabilidad, con el fin de estar a la vanguardia de los grandes proveedores de servicios. Es importante entender el funcionamiento del protocolo VXLAN ya que podremos comprender el procesamiento de la red en un entorno de virtualización. VXLAN es creado para el tipo de ambientes virtualizados, facilita los servicios y flexibiliza la distribución de los recursos en ambientes compartidos. Ha llegado a ser un papel clave en los nuevos

ambientes de Datacenter hoy en día, permitiendo alojar y brindar servicio a miles de usuarios evitando el enmascaramiento de protocolos y la implementación de túneles, este tipo de modelos generan retrasos y reprocesos significativos en la red.

1.3 Objetivos

Generales:

- Rediseñar la Red LAN y WAN basado en el protocolo VXLAN para mejorar la comunicación de todas las sedes de la compañía CRC.

Específicos:

- Analizar la actividad del protocolo VXLAN en su aplicación, requerimientos y ventajas.
- Diseñar los servicios de CRC en la nube para optimizar el rendimiento de la red interna y externa.
- Ejecutar un modelo de pruebas en capa 2 y 3 usando VXLAN en un ambiente virtualizado.

2. Marcos de referencia

2.1 Teórico

La tecnología de protocolo de LAN virtual extensible VXLAN, hace que las redes admitan más VLAN, siendo un esquema de expansión de redes capa 2 sobre redes capa 3, es decir, que a través de la encapsulación de paquetes se podrá encapsular tramas de capa 2 en tramas de capa 3. Esta tecnología se considera “Overlay Network”, ya que, debe de ser primero que todo una red lógica, es decir, que permita segmentar redes de forma lógica, segundo, debe de contar con un proceso de encapsulamiento y des encapsulamiento, VXLAN encapsula la trama Ethernet original en un paquete UDP. tercero, debe haber una comunicación establecida a través de un túnel entre las dos terminales, modulo llamado VTEP. Basados en todo lo anterior VXLAN cumple perfectamente con cada una de las especificaciones.

La VXLAN tienen una capa de identificador que se denominan un segmento y sólo las máquinas virtuales asociadas a este identificador pueden comunicarse entre sí, estos identificadores se conocen como VNI, el cual tiene una longitud de 24 bits. Lo que hace permitir que hasta 16 millones de segmentos puedan ser desplegados en el mismo dominio administrativo.

Una de las ventajas de VXLAN es que a través de su VNI se puede aislar el tráfico de cada segmento de red, sin importar si una dirección MAC se encuentra repetida o duplicada al interior de cada segmento. Esto se debe porque su VNI encapsula la dirección física de cada VM en una trama que finalmente procesa el módulo VTEP, de esta forma los switches no entraran en conflicto cuando se ejecuten los procesos sobre su tabla MAC.

Trama VXLAN

En la siguiente imagen observamos la trama del protocolo VLAN y las adiciones técnicas para el funcionamiento de la trama VXLAN

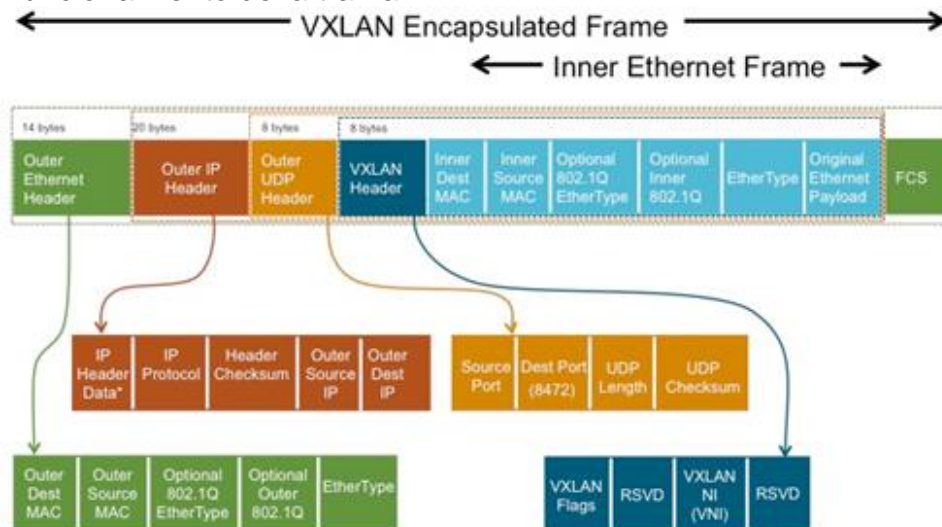


Ilustración 2, Trama VXLAN.

Fuente: Posted in Cisco, Data Center, NexusTagged Cloud.

La trama original Ethernet VLAN de capa 2 se denomina **Inner Ethernet Frame** la cual tiene los siguientes campos:

- **Inner Destination Mac (4 bytes):** Dirección MAC de destino o a la cual va dirigida la trama, esta puede ser de un dispositivo físico o virtual y puede estar ubicada dentro o fuera de la red.
- **Inner Source Mac (4 bytes):** Esta es la dirección MAC del dispositivo que envía la trama.
- **Optional 802.1Q Ether Type (2 bytes):** Campo referente al taggeado de la trama, el cual indica que la trama ethernet ha sido modificada para llevar una VLAN ID según el protocolo 802.1Q este valor puede ser entre 1 y 4094.
- **Optional inner 802.1Q (2 bytes):** Este campo se refiere al VLAN ID y se encuentra compuesto por 3 campos.
 - **User Priority (3 bits):** Suministra la calidad de servicio.
 - **Canonical Format Indicator (1 bit):** Este campo nos ayuda a identificar si el campo siguiente (VLAN ID) está destinado. Puede ser para el protocolo Ethernet (0) o Token Ring (1).

- **VLAN ID (12 bits):** Identificar la VLAN (Tag). Al tener 12 bits, da la posibilidad de tener hasta 4096 VLANs.
- **Ether Type (2 bytes):** Este campo indica el tipo de protocolo que contiene los Datos o denominado Payload. Si estos están basados en IPv4, este campo será 0x0800. Si fuese por ejemplo IPv6 sería 0x86DD.
- **Original Ethernet Payload (1500 bytes):** Aquí viene los datos que entrega la capa 3 o capa de red del modelo OSI. Los fragmentos tendrán un tamaño de 1500 bytes, esta será la cantidad útil de información que podrá transporta la trama.
- **FCS (4 bytes):** El Frame Check Sequence es el encargado de hacer el código de redundancia cíclica (CRC). El cual vela por la integridad de la información.

VXLAN Header (Cabecera de la trama VXLAN)

- **VXLAN Flags (1 byte):** Banderas empleadas para algún propósito en VXLAN.
- **RSVD (3 bytes):** Reservado para el futuro. Campo puesto en ceros.
- **VXLAN NI (VNI) (3 bytes):** El campo de VNI o VXLAN Number Identifier es quien lleva el identificar de red. VNI está compuesto por 24 bits, proporcionando más de 16 millones de ID`s o redes posibles, sin embargo, se ha decidido comenzar desde el número 5000 con el fin de no duplicar los valores de la VLAN ID.
- **RSVD (3 bytes):** Reservado para el futuro. Campo puesto en ceros.

Outer UDP Header

Estos campos tienen como propósito especificar información de capa 4 o capa de transporte para los VTEP`s.

- **Source Port (2 bytes):** El puerto de origen es escogido por el VTEP que está encapsulando la trama original de ethernet. VTEP calcula este puerto utilizando un algoritmo hash. El hash emplea el header de la trama original de ethernet (Inner L2 Header).
- **Dest Port (2 bytes):** El puerto de destino predeterminado es el 8472. Sin embargo, este valor puede ser cambiado por el software de administración de los equipos.
- **UDP Length (2 bytes):** Especifica la longitud en bytes del header de este segmento UDP.
- **UDP Checksum (2 bytes):** Este valor siempre será 0x0000. El VTEP que enviará la trama establecerá este valor. Si el VTEP que recibe la trama nota que este valor es distinto, rechazara la solicitud.

Outer IPV4 Header

Estos campos tienen como propósito especificar información de capa 3 o capa de red acerca de los VTEP`s.

- **IP Header Data (9 bytes):** Son una combinación de varios campos, como:
- **Versión (4 bits):** Si este valor es 4 significa que la versión de IP es IPv4.
- **IHL (4 bits):** Internet Header Length se encarga de avisar si el campo de "Options" será o no utilizado.
- **Type of Service (1 byte):** Permite establecer calidad de servicio de capa 3.
- **Total Length (2 bytes):** Establece el tamaño total del paquete, incluyendo el header. Este valor es de 20 Bytes para el caso de IPv4.
- **TTL (1 byte):** Time to Live, encargado de eliminar bucles de capa 3.
- **Options (3 bytes):** Permite ampliar las opciones de IPv4.
- **Padding (1 byte):** Se encarga de garantizar que la longitud del paquete sea múltiplo de 32.
- **Protocolo IP (1 byte):** Indica si se está utilizando el protocolo UDP, si su valor es 0x11.
- **Header Checksum (2 bytes):** Chequeo de cabecera, este valor permite verificar la integridad de los datos.
- **Source IP (4 bytes):** En este campo se refleja la dirección IPv4 del VTEP de origen (el VTEP que estará encapsulando).
- **Destination IP (4 bytes):** Refleja la dirección IPv4 del VTEP de destino (el VTEP que estará des encapsulando).

Outer Mac Header

Estos campos tienen como propósito especificar información de capa 2 o capa de enlace de datos acerca de los VTEP`s.

- **Outer Dest MAC (4 bytes):** Dirección MAC de destino (dirección MAC del VTEP a quien va dirigida la trama) con la cual el VTEP de origen se desea comunicar, si el destino se encuentre en otra red en este caso la dirección MAC podría ser de un dispositivo de capa 3 que se encargue de enrutar el tráfico.
- **Outer Source MAC (4 bytes):** Esta es la dirección MAC del VTEP que enviará la trama.

- **Optional 802.1Q Ether Type (2 bytes):** Es opcional en VXLAN. Podría ser que una o varias VXLAN viaje a través de una VLAN.
- **Optional Outer 802.1Q (2 bytes):** Utilizar VLAN es opcional en una implementación de VXLAN, de ser empleado el valor de la VLAN irá en este campo.
- **Ethernet Type (2 bytes):** Este campo indica el tipo de protocolo que VTEP empleará en capa 3. Si VTEP emplea IPv4, este campo será 0x0800.

En la siguiente sección se describirá el escenario de flujo de tráfico en un ambiente VXLAN utilizando un plano de control y plano de datos. Enseguida describiremos cómo se asocia la dirección MAC de la máquina virtual a la dirección IP del VTEP, función y operación de Multicast para el aprendizaje de destinos desconocidos, y tramas Multicast enfocados al tema de servicios. Se describirá también la forma en que VXLAN utiliza el plano de control, utilizando varios esquemas para el aprendizaje y distribución de las direcciones IP de los VTEP'S hacia las direcciones MAC de las máquinas virtuales.

Comunicación Unicast y Multicast

Para cada servidor es totalmente transparente el esquema lógico de conexión. Al realizar una conexión tipo Multicast y Unicast se realiza el siguiente proceso de conexión tal y como se observa en la ilustración número 3:

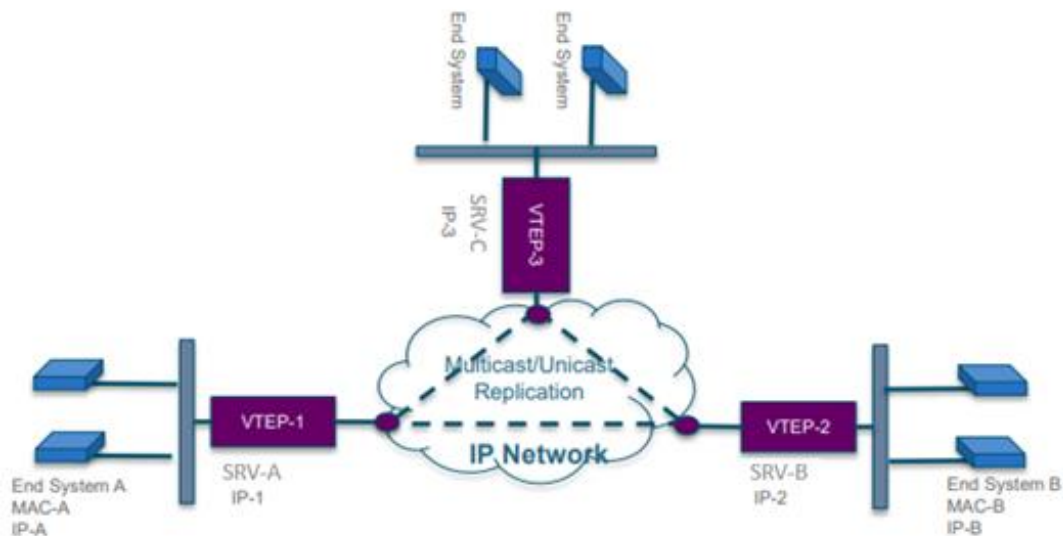


Ilustración 3 - Paso 1 esquema de conexión.

Fuente: Cisco live, Berlin, Germany Date: February 15–19, 2016 - A Summary of Cisco VXLAN MP-BGP EVPN.

- El servidor SRV-A es clasificado en un segmento VXLAN, el hypervisor o monitor de la máquina virtual notifica al Virtual Ethernet Module (VEM).

- El VEM agrega la dirección MAC virtual en la tabla local del VTEP.

En la ilustración número 4 se describe el segundo estado de conexión:

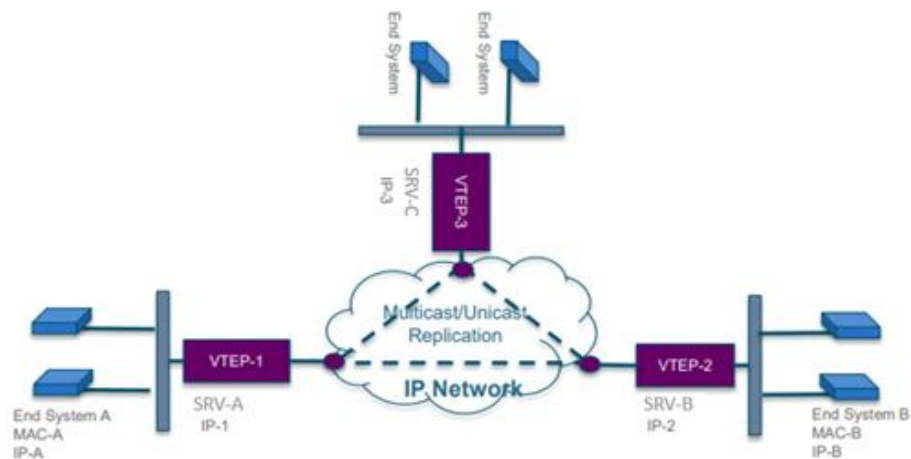


Ilustración 4 - Paso 2 esquema de conexión.

Fuente: Cisco live, Berlin, Germany Date: February 15–19, 2016 - A Summary of Cisco VXLAN MP-BGP EVPN.

- El VSM (Virtual Supervisor Module) continúa alimentando la tabla local de VTEP, de acuerdo con la información entregada por sus vecinos.
- El VSM envía la tabla de mapeo a todos los VEMs.

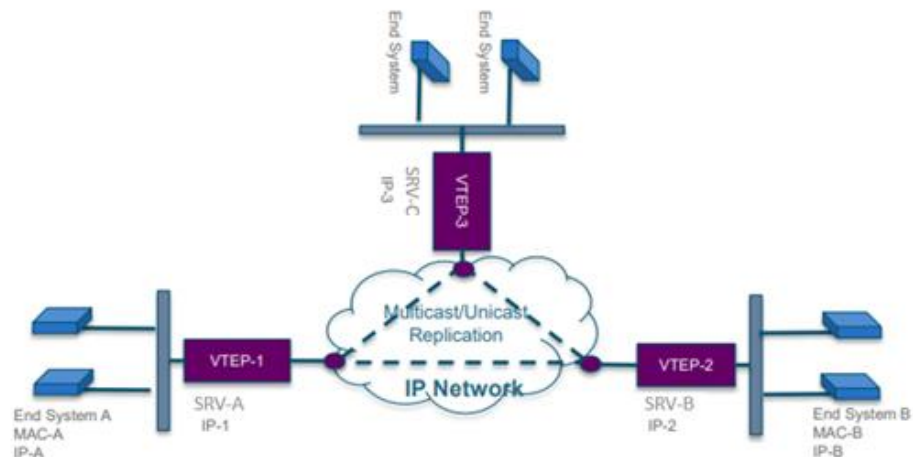


Ilustración 5 - Paso 3 esquema de conexión.

Fuente: Cisco live, Berlin, Germany Date: February 15–19, 2016 - A Summary of Cisco VXLAN MP-BGP EVPN.

- Cuando SRV-A envía peticiones ARP en busca del servidor SRV-B el VEM generará la respuesta ARP ya que este contiene la información en su tabla local, si la MAC

destino no se encuentra en la tabla, la petición ARP se reenviará a las VTEPs de forwarding-incapable o reenvío incapaz.

- El tráfico desde el servidor SRV-A destinado al servidor SRV-B estará encapsulado por el VTEP1 y enviado al VTEP2.
- VTEP2 desencapsulará el paquete y lo entregará localmente.
- SRV-B recibirá la trama original.

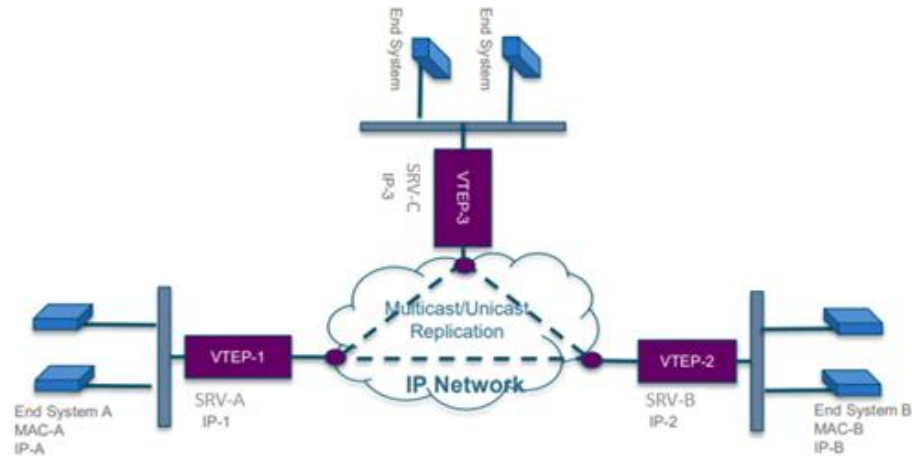


Ilustración 6 - Paso 4 esquema de conexión.

Fuente: Cisco live, Berlin, Germany Date: February 15–19, 2016 - A Summary of Cisco VXLAN MP-BGP EVPN.

- Si el servidor SRV-A envía tráfico Multicast, entonces el VEM replicará y enviará una copia a cada VEM con un VTEP asociado a cada segmento VXLAN.
- El VEM remoto recibirá los paquetes Multicast enviarán una copia a cada destino local sobre el segmento particular de VXLAN

2.2 Marco institucional

Plataforma estratégica de la empresa CRC

El punto de llegada al implementar la propuesta de renovación en el aspecto de configuración está dado por la interconexión que se lleva a cabo en cada una de las sedes según los objetivos planteados, los esfuerzos están dirigidos a ejecutar la solución del planteamiento del problema.

La línea de productos y servicios se establece de acuerdo a mitigar la necesidad unificando la comunicación en la compañía CRC, partiendo del hecho que se ofrece una misma conexión de red en diferentes ubicaciones geográficas.

Permitiendo de alguna manera poder ofrecer la disponibilidad de los servicios que ofrece el área de tecnología, esta vez apoyando fuertemente los procesos de los servicios tecnológicos que se interactúan a diario en la compañía.

Es así como se despliega el alcance del plan de acción en mejora planteado en este documento, proyectando así a la ejecución del mismo y determinando estabilidad en salida a producción, de igual manera haciendo un enfoque en el comportamiento para determinar si se continua con la ejecución del servicio o se realiza un rollback de configuración.

Si la implementación marcha bien se dará por hecho la finalización del alcance que se ha planteado para contrarrestar el problema.

Visión:

Apoyamos a diferentes entidades del Sector Financiero y Real Colombiano en la recuperación de cartera.

Misión:

En el 2025 CRC será una empresa que promueva la interacción y el empoderamiento sobre la decisión de crédito, administra todas las etapas del ciclo: radicación de las solicitudes, estudio, aprobación, administración y control de tarjetas.

Estrategia misional:

Su interés estratégico está concentrado en evolucionar muy rápido hacia la prestación de servicios de tercerización del proceso de crédito en todas las etapas del ciclo, sin embargo tiene una necesidad central y es el funcionamiento de la compañía bajo un esquema de red tecnológica que actualmente interfiere en la prestación de los servicios que ofrece a nivel interno y externo de la compañía, es así como se provee una fuerte inclinación de tener una estructura que mantenga la disponibilidad de los servicios en el momento que se requiera.

CRC Cuenta con varias áreas que estructuran la operación y permiten que la empresa pueda surgir sin problema alguno, las áreas demandan servicios de conexión a red, telefonía y periféricos, que demandan requerimientos e incidencias que tienen alcance desde soporte nivel 1, 2, y 3, junto con la tercerización si así se requiere, las solicitudes recibidas se deben atender con bastante prioridad, se puede afirmar que CRC tiene claramente estipulado en sus procesos de soporte, unos ANS que se deben cumplir con riguridad, de lo contrario se pueden acarrear multas ya establecidas por medio de contratos con sus clientes.

Es así como se reitera la importancia de tener una estructura robusta a nivel tecnológico que posea la configuración correcta, ya que la demanda de servicios es bastante alta y depende directamente de área de sistemas responder por la estabilidad y continuidad de las demás dependencias de la compañía de acuerdo a la caracterización de los servicios tecnológicos que se prestan.

Se debe garantizar que los servicios se mantengan sin interrupción para una breve ejecución de todas las tareas operativas como entrega del plástico al cliente, facturación, administración de la cartera, control de documentos y actividades de servicio al cliente, la configuración precisa y robusta en tecnología ayuda para que estas labores se simplifiquen y se puedan llevar a cabo sin inconveniente.

Como empresa prestadora de servicios de Fábrica de Crédito, Recuperación de Cartera y BPO, recibe información de sus clientes para que la misma sea tratada con el único objetivo de brindar los servicios específicamente contratados y recopila información con la finalidad de realizar diversas gestiones sobre su cartera propia.

De esta manera CRC SAS, puede actuar como responsable o encargado de la información respectivamente de acuerdo a sus contratos.

Política y principios de la empresa CRC

La política de la empresa CRCS S.A.S. está orientada a la protección de datos personales, para que toda persona pueda conocer, actualizar y rectificar la información contenida en las bases de datos o demás archivos y generar reclamos de acuerdo con lo definido en el artículo 15 de la Ley Estatutaria 1581 del 17 de octubre del 2012, así como los demás derechos, obligaciones y responsabilidades, contenidas en la normatividad vigente.

CRC SAS, como empresa prestadora de servicios de Fábrica de Crédito, Recuperación de Cartera y BPO, recibe información de sus clientes para que la misma sea tratada con el único objetivo de brindar los servicios específicamente contratados y recopila información con la finalidad de realizar diversas gestiones sobre su cartera propia. De esta manera CRC SAS, puede actuar como responsable o encargado de la información respectivamente.

DISEÑO Y AUTOMATIZACION DE PROCESOS BACKOFFICE: Procesos modernos, Eficientes y Efectivos que permiten generar valor a nuestros clientes.

FABRICA DE CREDITO.

ADMINISTRACION DE CARTERA: Ejecución de procesos tales como causación de intereses, cobros adicionales, facturación, aplicación de pagos, reporte a centrales de información, interfaz contable.

RECUPERACION DE CARTERA: Diseño de estrategia según portafolio. Gestión preventiva y prejurídica

Líneas de servicios o productos

Carrera 7 No.155C-30 Piso 26.
Centro Empresarial North Point Torre E
Bogotá Colombia.

Teléfono: 57 1 4895000

Línea ética: 57 1 4088365
buzonpqr@crc.com.co.

3. Metodología

3.1 Población

La población muestra del presente trabajo, hace referencia a todo el personal involucrado en el Sistema de Gestión de Calidad implementado en la compañía, se constituye por las áreas que responden a la fuerte operación, es de aclarar que se debe ofrecer alta disponibilidad de servicio.

CRC cuenta con un equipo especializado en atender y solucionar todas las solicitudes e incidencias que surjan a lo largo de la ejecución de procesos, se ha evidenciado una fuerte demanda de requerimientos que se sitúa en brindar comunicación de voz y datos entre las sedes o puntos que posee CRC, este es el punto de partida ideal, con el fin de cumplir el objetivo de poder centralizar las conexiones, teniendo en cuenta que existen áreas que necesitan interactuar para efectuar los procesos que rigen el SGC.

3.2 Técnicas para la recolección y análisis de la información

Las técnicas inician a partir de observar las estadísticas de los datos que se transfieren por medio de las redes que interactúan con servidores y son capaces de comunicar a CRC.

Inspección en cada estado actual de toda la infraestructura que se encuentra en la organización.

Estado actual de hardware, se debe recolectar toda la información de los dispositivos físicos que se encuentran en la red.

Estado actual de software, Se debe recolectar cada una de las configuraciones actuales de cada dispositivo conectado a la red.

Estado actual de la red física, Se debe obtener información los servicios que se manejan frente a los requeridos de la organización.

El análisis y constatación se relacionan en los estudios realizados en el marco teórico.

3.3 Tipo de investigación

Para diseñar y definir las actividades necesarias para el mejoramiento de la red de la organización CRC, asegurando la excelencia de los servicios Cisco, describe una opción llamada ciclo de vida de redes PPDIOO (Preparar–Planear–Diseñar–Implementar–Operar–Optimizar). La cual vamos a utilizar en esta investigación, enfocándonos solo en las tres primeras etapas.

Etapa 1 - Preparación

Aquí en la etapa se establecen las actividades requeridas para brindar el mejor servicio, identificar la tecnología que soportará la arquitectura y optimizar el ciclo de vida de la red.

Etapa 2 - Planeación

En esta etapa se identifican los requisitos de la red mediante una evaluación de la infraestructura de la red de la organización, como está actualmente, deficiencias y de sus aplicaciones, se realiza un análisis de área donde la red podría implementarse.

Etapa 3 - Diseño

Desarrollar un diseño detallado que comprenda requerimientos técnicos y de negocios, con base en las anteriores etapas. Esta etapa incluye diagramas de red y lista de equipos.

4. Diagnóstico de las condiciones actuales de la empresa CRCS S.A.S.

4.1 Estado de las condiciones actuales

La compañía cuenta con un sistema tecnológico orientado a la gestión de servicios de tecnología de la información, esta plataforma es capaz de brindar en tiempo real la demanda de requerimientos e incidencias que se presentan en el día a día de la operación.

La gestión se ejerce en todas las áreas de la compañía siendo estas segmentadas por VLAN'S que representan la comunicación de cada área, por lo tanto, se ha visto afectada la operación debido a fallas recurrentes.

Las fallas se tienen identificadas y básicamente son intermitencias en la comunicación de voz y datos de las distintas áreas entre las sedes que conforman el anillo de comunicación de CRC.

Actualmente CRC cuenta con 150 usuarios que están distribuidos en tres sedes, cada una de las sedes se encuentra conectada por una red MLPS que realiza la conectividad entre ellas.

Pero al realizar el análisis de fallas se evidencia el siguiente ejemplo.

Caída de sistema CRC

Los usuarios se conectan por medio de un navegador WEB a un host que se encuentra alojado en la sede A de la compañía, por lo tanto, los usuarios de la sede B y C pueden presentar inconsistencia de servicio de acuerdo con las fallas de proveedor.

Es allí donde ejecutan el proceso de radicación de incidencia por medio de la herramienta corporativa GLPI.



Ilustración 7 - Evidencia de requerimientos.

Fuente: Plataforma de servicios GLPI perteneciente a CRC - <http://gpi.crcsas.local>

La solicitud es entregada al grupo de IT quien se encarga de realizar su respectiva identificación y atención para priorizar una solución.

Si nos enfocamos nuevamente en el análisis de las fallas recurrentes podríamos observar la solución definitiva que se relaciona en el estudio realizado que da cita al marco teórico.

Actualmente la infraestructura de la compañía se encuentra distribuida de la siguiente forma:

Áreas	Cantidad de Dispositivos	Segmentación de Red	VLAN ID	Sede A	Sede B	Sede C
Servicio al cliente	15	192.168.20.0/25	20X	X		
Contabilidad	5	192.168.30.0/26	30X	X		
Colocación de crédito	30	192.168.40.0/27	40X			X
Cobranzas	70	192.168.50.0/28	50X	X		
Crédito	20	192.168.60.0/29	60X	X		X
Sistemas	15	192.168.70.0/30	70X			
Gerencia	3	192.168.80.0/31	80X			
Total:	158					

Ilustración 8 – Distribución de áreas de CRC

Fuente: Plataforma de servicios de enrutamiento y seguridad perteneciente a CRC - <http://fw.crcsas.local>

Podemos determinar que CRC tiene una alta demanda de conexión a dispositivos que se encuentran en distintos lugares físicos, lo que requiere la implementación de lo propuesto.

4.2 Determinación de factores críticos

Observando la llegada de la virtualización en los centros de datos, aparece una facilidad de escalabilidad bastante importante, ya que gracias a las posibilidades de la virtualización el número de conexiones que aumenta rápidamente.

Con el número de servidores se aumenta obviamente el número de MACs y el número de VLANs. Esto hace que la tabla de MACs crezca y que el número de VLANs permitido por

protocolo (12 bits para el VLAN ID en IEEE 802.1Q – 4094) se agoten. Eso sin contar los problemas con el STP, recordad que por ejemplo RSTP sólo soporta 127 instancias.

Por otro lado, la gestión tradicional en este tipo de entornos se complica enormemente y se tenía que encontrar una solución que permitiera escalar en servidores, en VLANs y solventar el problema del STP en la medida de lo posible.

4.3 IDENTIFICACION DE HALLAZGOS SIGNIFICATIVOS

En el siguiente párrafo mencionaremos algunos de los requerimientos identificados para realizar la nueva configuración en switches Nexus 7000:

- Espacio en racks para realizar la instalación física de los nuevos equipos en el Datacenter de proveedor.
- Conexiones físicas de datos, Cableado UT para los nuevos equipos.
- Nuevo direccionamiento IP para ser asignado a los nuevos equipos a instalar.
- Servidores para alojar el software que comunica la compañía.
- Creación de un usuario con roll de administrador para los nuevos switches Nexus 7000.
- El proveedor de hosting debe garantizar el aprovisionado en la nube de los nuevos equipos pertenecientes a CRC.
- Se debe garantizar que la granja de maquina virtuales VM no debe superar el espacio de direcciones IP pero desea preservar la arquitectura de la red del centro de datos para garantizar seguridad.
- El proveedor de servicios en la nube que tiene múltiples inquilinos necesita garantizar el escalamiento de las VLAN 802.1q.
- Elaboración y entrega de un nuevo certificado digital de seguridad para cada uno de los equipos que componen la solución, esto será utilizado únicamente para la administración de la solución.
- Documentación de la solución implementada requerida por CRC al proveedor.

5. Diseño de ingeniería

5.1 PROPONER REDISEÑO DE LA RED LAN Y WAN QUE SOPORTA SERVICIO AL CLIENTE, BASADO EN LA APLICACIÓN DE LA ESTANDAR CCNA-CISCO, EN EL AREA DE GESTION INFORMATICA DE LA EMPRESA CRC S.A.S EN LA CIUDAD DE BOGOTA

5.1.1 Etapa 1

Al observar el análisis realizado y las muestras tomadas, podemos afirmar que las sedes se necesitan comunicar entre sí para lograr una mejor producción.

Se observa que se debe realizar una mejor administración de las VLAN'S para poder brindar la comunicación interna de la compañía sin importar donde se encuentren localizadas las áreas que la conforman.

Por eso se determina realizar la configuración de VXLAN en los nuevos equipos para la compañía CRC que se implementan en el proveedor.

5.1.2 Etapa 2

Escenario de Implementación para VXLAN en la compañía CRC

VXLAN será implementado en los centros de datos del proveedor y los servidores contarán con virtualización del software que actualmente se encuentra en ejecución en los Datacenter locales de la empresa CRC S.A.S. Cabe resaltar que el servicio de data center es tercerizado y se comprende que los equipos son propiedad de CRC, el proveedor debe garantizar que los equipos se alojen en los racks con las condiciones adecuadas para prestar un óptimo servicio sostenible y con recuperación de fallos.

Los racks deben ser individuales y pueden ser parte de una red de capa 3 diferente o podrían ser en una sola red de capa 2. Los segmentos VXLAN se superponen en la parte superior de estas Capas, capa 2 o Capa 3 de la red y se configuran en los equipos.

“Vemos en la siguiente figura que representa por dos servidores virtualizados conectados en la infraestructura de capa 3 que ofrece el proveedor a CRC.

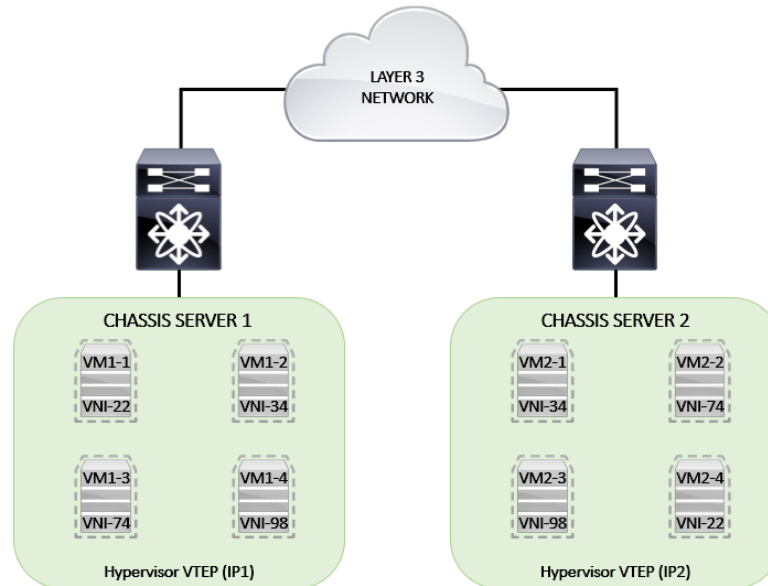


Ilustración 9 - Despliegue de VXLAN - VTEPs a través de una red capa 3

Hay cuatro redes superpuestas VXLAN identificados por el VNIs 22, 34, 74, y 98. Considere el caso de VM1-1 en el servidor 1 y VM2-4 en el servidor 2, que están en la misma red superpuesta VXLAN identificado por VNI 22. Las máquinas virtuales no saben acerca de las redes superpuestas y método de transporte desde la encapsulación y des encapsulación suceda de forma transparente a los VTEPs en servidores de 1 y 2.

“Las otras redes superpuestas y las máquinas virtuales correspondientes son VM1-2 en el servidor 1 y VM2-1 en el servidor 2, tanto en VNI 34; VM1-3 en el servidor 1 y VM2-2 en el servidor 2 de VNI 74; y, finalmente, VM1-4 en el servidor 1 y VM2-3 en el servidor 2 de 98 VNI.

Análisis del Proyecto

Teniendo en cuenta toda la información que se analiza y comparte en los capítulos anteriores, podremos realizar la implementación de un ambiente de pruebas virtualizado en donde se pondrá a prueba el funcionamiento de VXLAN en el proveedor que ofrece el alojamiento de los servicios de datos.

Un objetivo claro en este ambiente de pruebas es no simular del todo la transmisión de datos generada que genera CRC, la idea es poder realizar migraciones por hosts o servidores virtuales segmentados en grupos, se quiere dar a entender cómo opera el proceso de encapsulamiento y des encapsulamiento de cada trama VXLAN generada por interfaces virtuales concebidas por la arquitectura que se implemente en el proveedor.

Análisis y Definiciones de Requerimientos

En este caso utilizaremos la plataforma gratuita de virtualización oVirt y sobre esta plataforma vamos a virtualizar los routers firewalls marca pfsense.

Descargar oVirt

oVirt 4.3.7 está destinado para uso en producción y está disponible para las siguientes plataformas:

- Red Hat Enterprise Linux 7.7 o posterior pero <8
- CentOS Linux 7.7 o posterior pero <8
- Scientific Linux 7.7 o posterior pero <8
- oVirt Node (basado en CentOS)

Consulte las [Notas de la versión de oVirt 4.3.7](#).

Instalar oVirt con Cockpit

oVirt se instala utilizando un instalador gráfico en Cockpit.

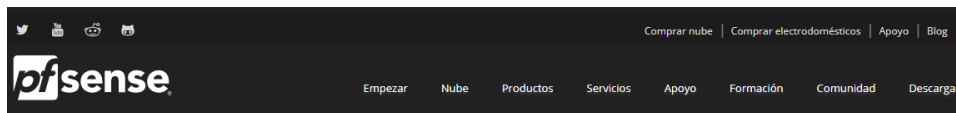
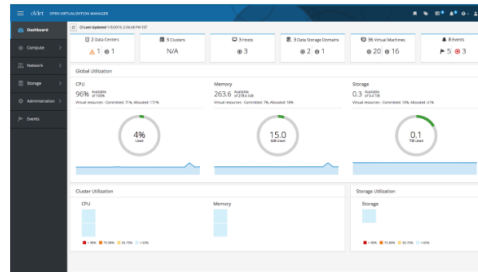
oVirt Engine y un host se instalan junto con el motor que se ejecuta como una máquina virtual en ese host. Una vez que instale un segundo host, la máquina virtual del motor estará altamente disponible. Consulte la [Guía del motor independiente](#) para obtener todos los detalles.

Opciones alternativas de descarga

oVirt admite dos tipos de hosts :

- [oVirt Node](#) , un sistema operativo de hipervisor mínimo basado en CentOS
- [Enterprise Linux \(como CentOS o RHEL\)](#)

Ilustración 10 - Portal de descarga del oVirt – Software de virtualización.



Descargar

Casa | Descargar

Última versión estable (edición comunitaria)

Esta es la versión estable más reciente y la versión recomendada para todas las instalaciones. Consulte la documentación para obtener [Guías de actualización](#) y [Guías de instalación](#) . Para sistemas preconfigurados, consulte los [dispositivos de firewall pfSense® de Netgate](#) .

[NOTAS DE LANZAMIENTO](#)

[CÓDIGO FUENTE](#)

Seleccionar imagen para descargar

Versión: 2.4.4-p3

Arquitectura:

Espejo:

Supported by

Suscríbase al boletín de Netgate

Información del producto, anuncios de software pfSense y ofertas especiales. Vea nuestro [archivo de boletines](#) para avisos pasados.

Email *

Entiendo que me estoy registrando para recibir el boletín, los anuncios de

Ilustración 11 - Descarga de plataforma pfSense – Software de seguridad y enrutamiento.

5.1.3 Etapa 3

Definición del laboratorio

Se utilizarán 4 nodos de oVirt para virtualizar y ejecutar las máquinas virtuales de enrutamiento y seguridad, junto con los servidores de aplicaciones y bases de datos que proveen el servicio para la compañía.

Se van a Utilizar Switches Nexus 7000 que posee el proveedor en la configuración de hardware que posee su Datacenter

Se tomará en cuenta la documentación que describe el fabricante Cisco para poder implementar VxLAN para conectar los servidores de virtualización y generar así comunicación en la compañía CRC en diferentes puntos.

Documentación de la configuración:



Ilustración 12 - Cisco Nexus 7000 VxLAN Configuration Guide

Detalle de solución a implementar:

Para la solución a implementar de conectividad y virtualización, se realizará la instalación, configuración y puesta en marcha de cuatro (4) servidores del modelo UCS marca Cisco línea 240, en alta disponibilidad en estado activo – activo, con lo cual se logrará tener un balanceo de carga entre ambos equipos, permitiendo la integración con la infraestructura actual del CRC, sin olvidar la seguridad y la disponibilidad de un servicio que no se verá afectado en ningún momento.

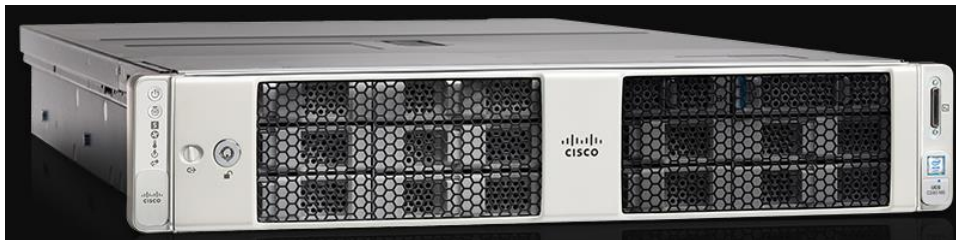


Ilustración 13 - Servidores del modelo UCS marca Cisco línea 240

Para poder lograr este balanceo el proveedor de alojamiento posee equipos balanceadores de carga, los nuevos servidores serán alojados detrás de un clúster de equipos de la marca F5 (balanceadores), los cuales se encargarán de repartir el tráfico hacia los nuevos equipos.

Topología Lógica de Conexión a implementar

Mostraremos el diagrama de conexión y flujo de datos de la solución que se solicita al proveedor de alojamiento donde se va a implementar toda la solución. En la imagen No. 14, se pueden observar a que equipos y puertos se encontraran conectados los diferentes elementos que componen la solución a implementar.

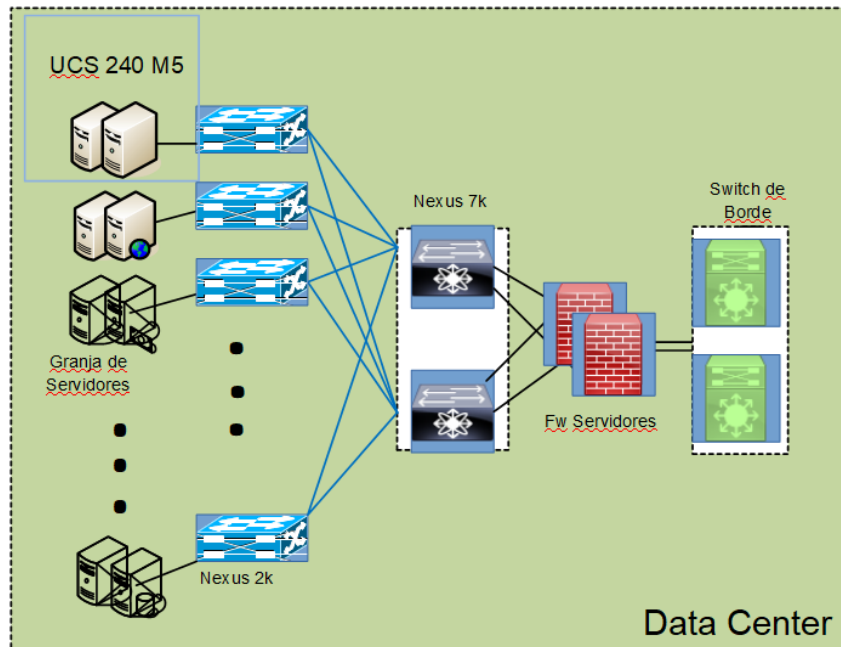


Ilustración 14 – Topología de red escalable

Esta es una breve descripción del flujo de datos del funcionamiento de la nueva solución de proxy a implementar:

Cuando un usuario realice una consulta a los aplicativos utilizando el navegador de su ordenador o las aplicaciones, la solicitud será enviada a una dirección IP que se encontrara configurada en los balanceadores de carga de la marca F5 en la red del Datacenter de la sede principal del proveedor, los dispositivos anteriormente mencionados se encargarán de enviar la petición a los nuevos servidores de virtualización.

Y garantizando un funcionamiento de igual carga a estos equipos, cuando el requerimiento llegue a los servidores de virtualización, se podrán realizar consultas de los servicios que se ofrece en el modelo piloto.

Diagrama de Topología Física de instalación

Topología de instalación física, la cual es propuesta de la siguiente manera:

- Conectar los servidores en diferentes racks y realizar las interconexiones hacia los switches a través de los FEX que se encuentran en los mismos racks.

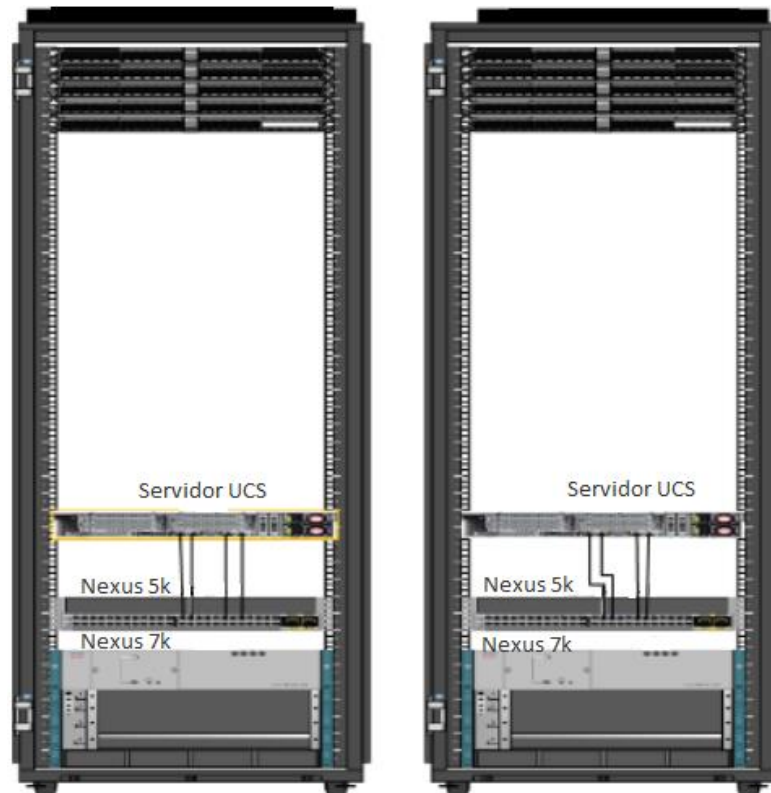


Ilustración 15 - Topología Física de instalación

CONCLUSIONES

Este trabajo demuestra el funcionamiento técnico y lógico de la tecnología VXLAN partiendo de una estructura de red robusta, se puede concluir que podemos realizar implementaciones en nuestros entornos de red virtualizado para garantizar el escalamiento y la disponibilidad de los servicios y las redes.

Si bien VXLAN ofrece beneficios significativos en términos de escalabilidad y seguridad de redes virtualizados, existe también un efecto secundario donde existe un importante procesamiento adicional de paquetes, VXLAN usa una capa de encapsulamiento adicional, y, por lo tanto, descargas de NIC tradicionales no se pueden utilizar. El resultado es el consumo altos niveles de costosos cursos de procesamiento de CPU, así como una reducción significativa en el rendimiento de la red.

En la parte de Seguridad, en el caso de tener acceso al ambiente virtualizado el atacante podría empezar a emitir tramas de IGMP que puedan unirse al grupo de Multicast o multidifusión que se utiliza en los segmentos VXLAN específicos, le permitiría al intruso poder tener información completa de los mensajes que cruzan a través de la red.

Al contar con un esquema de encapsulamiento sobre redes capa 3, nuestros sistemas se vuelven vulnerables desde cualquier segmento de red que sea alcanzable por cualquier enrutador.

Al presentarse un escenario de red Overlay el escaneo de puertos y análisis de paquetes se complejiza ya que la red se encuentra “Rota”, es decir, VXLAN rompe el esquema básico de red plana y el análisis de red tomará analizarlo en más tiempo.

BIBLIOGRAFÍA

- Caban-Babilonia, W. (2015, Marzo 12). A Summary of Cisco VXLAN Control Planes: Multicast, Unicast, MP-BGP EVPN. Retrieved from <http://blogs.cisco.com/perspectives/a-summary-of-cisco-vxlan-control-planes-multicast-unicast-mp-bgp-evpn-2>
- IETF. (2014, Agosto). Virtual eXtensible Local Area Network (VXLAN). Retrieved from <https://tools.ietf.org/html/rfc7348>
- Cisco live, Berlin, Germany Date: February 15–19, 2016 - A Summary of Cisco VXLAN MP-BGP EVPN. Retrieved from <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/LTRDCT-2223.pdf>
- oVirt, Document. (4.3.6 / 26 de septiembre de 2019). VMware NSX – Introducción a la VXLAN. Retrieved from <https://www.ovirt.org/documentation/>
- Epping, D. (2017, August 31). VXLAN Innovations on the Nexus OS Tony Antony. Retrieved from <https://blogs.cisco.com/datacenter/vxlan-innovations-on-the-nexus-os-part-1-of-2?dtid=osscdc000283>

Productos y servicios, Interruptores, Interruptores de centro de datos, Retrieved from <https://www.cisco.com/c/en/us/products/switches/nexus-7000-series-switches/index.html#~stickynav=2>

ANEXOS

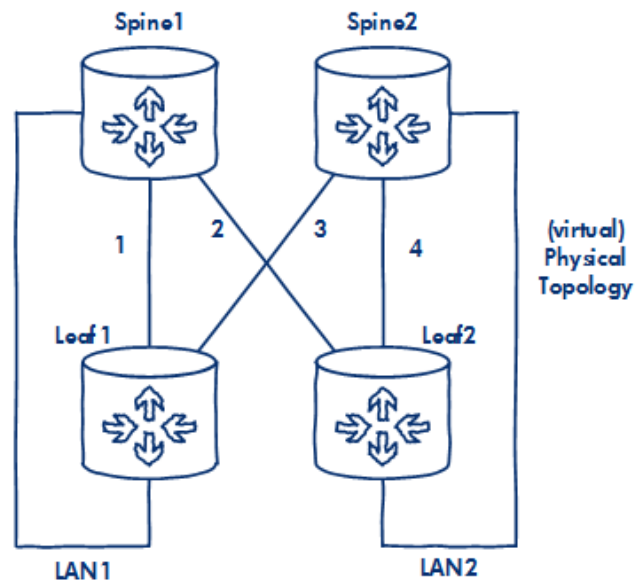


Ilustración 16 - Topología de Laboratorio VXLAN

Fuente: Joe Neville February 23, 2016 - Lab on a Laptop - Building a VXLAN Leaf Spine Network with HPE VSRs.

Outer Mac Header		Outer IPv4 Header		Outer UDP Header		VXLAN Header		Inner L2 Header & Payload		FCS
Outer Mac Header	Bytes	Outer IPv4 Header	Bytes	Outer UDP Header	Bytes	VXLAN Header	Bytes	Inner L2	Bytes	
Destination Address	6	Misc Data	9	Source Port	2	VXLAN Flags	1	Destination Address	6	
Source Address	6	Protocol 0x11	1	VXLAN Port	2	Reserved	3	Source Address	6	
VLAN Type 0x8100	2	Header Checksum	2	UDP Length	2	VNI	3	VLAN Type 0x8100	2	
VLAN Tag	2	Source IP	4	Checksum 0x0000	2	Reserved	1	VLAN Tag	2	
Ethernet Type 0x0800	2	Destination IP	4	Total	8	Total	8	Ethernet Type 0x0800	2	
Total (with Tag)	14	Total	20					Total (with Tag)	14	
Total (No Tag)	18							Total (No Tag)	18	

Total (With Tag) = 18+20+8+8+18=72 bytes + Payload = 72 bytes + 1500 bytes = 1572 bytes
 Total (No tag) = 14+20+8+8+14 = 64 bytes + Payload = 64 bytes + 1500 bytes = 1564 bytes

Ilustración 17 - VXLAN Encapsulated Frame for IPv4

Fuente: Andrés Araque Date: February 15, 2015 - VMware NSX – Introducción a la VXLAN

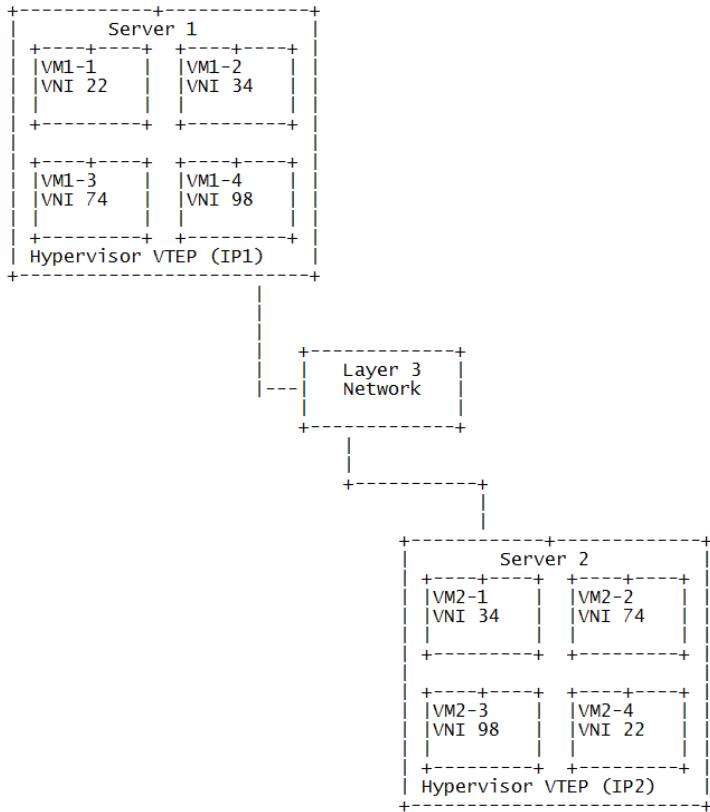


Ilustración 18 - VXLAN Deployment - VTEPs across a Layer 3 Network

Fuente: IETF Date: August 2014 - Virtual eXtensible Local Area Network (VXLAN) – Page 15