UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
INGENIEROS DE SISTEMAS

TEMA:
IMPLEMENTACIÓN DE UNA RED PILOTO QUE MUESTRE EL FUNCIONAMIENTO Y ATRIBUTOS QUE TIENE EL PROTOCOLO OVERLAY TRANSPORT VIRTUALIZATION (OTV) SOBRE UN AMBIENTE VIRTUALIZADO EN GNS3

AUTORES:
KATHERINE PATRICIA RAMOS BASTIDAS
WILSON DAVID COLLAGUAZO MARTÍNEZ

TUTOR:
JORGE ENRIQUE LÓPEZ LOGACHO

Quito, abril de 2016

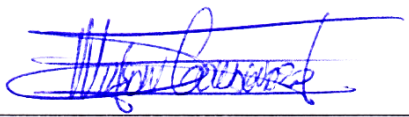
Cesión de derechos de autor

Nosotros, Katherine Patricia Ramos Bastidas y Wilson David Collaguazo Martínez con cédula de identificación N° 1725633703 y 1724481864 respectivamente, manifestamos nuestra voluntad de ceder a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: IMPLEMENTACIÓN DE UNA RED PILOTO QUE MUESTRE EL FUNCIONAMIENTO Y ATRIBUTOS QUE TIENE EL PROTOCOLO OVERLAY TRANSPORT VIRTUALIZATION (OTV) SOBRE UN AMBIENTE VIRTUALIZADO EN GNS3, mismo que ha sido desarrollado para optar por el título de: Ingenieros de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, abril de 2016

Katherine Patricia Ramos Bastidas
CI: 1725633703

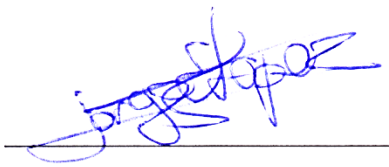


Wilson David Collaguazo Martínez
CI: 1724481864

Declaratoria de coautoría del docente tutor

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación IMPLEMENTACIÓN DE UNA RED PILOTO QUE MUESTRE EL FUNCIONAMIENTO Y ATRIBUTOS QUE TIENE EL PROTOCOLO OVERLAY TRANSPORT VIRTUALIZATION (OTV) SOBRE UN AMBIENTE VIRTUALIZADO EN GNS3 realizado por Katherine Patricia Ramos Bastidas y Wilson David Collaguazo Martínez obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Quito, abril de 2016



Ing. Jorge Enrique López Logacho
CI: 1712082484

DEDICATORIA

A mis padres Manuel Ramos y Victoria Bastidas quienes siempre están apoyándome y aconsejándome incondicionalmente, a mis hermanos Josselyn y Edison por su compresión y palabras de aliento y a todos quienes forman parte de mi vida como mis perrunos que con su inocencia, amor sincero y travesuras siempre están junto a mí.

Katherine Ramos

A mis madres Lilian Martínez y Zoila Díaz quienes siempre han estado guiándome y apoyándome incondicionalmente para convertirme en un buen hombre, a mi tío Roberto Martínez quien con su ejemplo me ha enseñado que con esfuerzo se puede salir adelante aun en las situaciones más duras, a mi hermana Rosi quien me impulsó a seguir adelante al considerarme su guía y a toda mi familia, quienes con palabras de aliento me animaban a continuar y culminar mis estudios.

David Collaguazo

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El siguiente trabajo es un informe técnico en el cual se detalla los procesos para la implementación de un ambiente virtual de una red empresarial en la que se emplea el protocolo Overlay Transport Virtualization (OTV) para integrar de manera lógica centros de datos geográficamente distantes de una manera eficiente y que permita balancear la carga de la red con el fin de manejar grandes volúmenes de datos a bajo costo y en el menor tiempo posible. En este documento se encuentra la información más relevante para dar una explicación clara del protocolo y de sus componentes como son el enrutamiento MAC, Mutihoming, Interfaces virtuales con túneles GRE, Trafico etiquetado basado en la tecnología de MPLS así como su funcionamiento, para establecer las ventajas del protocolo frente a otros del mismo tipo se ha creado tres topologías que permitan resaltar los atributos de OTV, en la primera topología se utiliza el enrutamiento dinámico en los enlaces con el fin de establecer las condiciones iniciales de la red, en la segunda topología se utiliza interfaces virtuales VPN en los enlaces para tomar datos que sirvan para establecer tablas comparativas frente a OTV, en la tercera topología finalmente se implementa la red virtual sobrepuesta para los enlaces, una vez configurada las topologías se pasa a las pruebas que permiten recolectar datos para establecer resultados técnicos y sacar conclusiones.

ABSTRACT

The following work is a technical report in which the processes for implementing a virtual environment of a corporate network in which the protocol Overlay Transport Virtualization (OTV) is used to integrate logically centers geographically distant data from a detailed efficiently and allows load balancing network in order to handle large volumes of data at low cost and in the shortest time possible. This document describes the most relevant information is to give a clear explanation of the protocol and its components such as the MAC, Mutihoming routing, virtual Interfaces with GRE tunnels, traffic labeled based on MPLS technology and its operation, to establish benefits of the protocol against the same type was created three topologies that allow highlight the attributes of OTV, in the first topology dynamic routing is used on links in order to establish the initial conditions of the network, in the second topology virtual interfaces VPN is used on links to take factors used to establish comparative tables against OTV, in the third topology finally the Overlay virtual network for links is implemented, once configured topologies passed the tests to collect data to establish technical results and draw conclusions.

INTRODUCCIÓN

Las redes a nivel mundial en la actualidad se encuentran bajo gran demanda de recursos generada por diversos aplicativos que son creados para la interacción con los usuarios a tiempo real, esto genera a su vez la necesidad de crear nuevos protocolos que permitan el transporte y procesamiento de enormes cantidades de información a la mayor velocidad posible y que sean lo más imperceptibles en el tráfico de la red para incrementar la seguridad e integridad de la información.

A través del tiempo se han creado algunos protocolos que han mitigado la necesidad y se han constituido en soluciones temporales pero debido a la creciente demanda de mayor número de usuarios de la red estos protocolos se han ido tornando insuficientes para manejar el volumen de tráfico, es por eso que protocolos con similar funcionalidad son creados rápidamente con algunas mejoras y nuevas propiedades dejando a sus antecesores como conocimiento obsoleto y que debe ser actualizado.

El presente trabajo se enfoca en el protocolo Overlay Transport Virtualization (OTV) que fue dado a conocer por cisco en el año 2011 y difundido al mundo en el 2012 como una alternativa al protocolo Multiprotocol Label Switching (MPLS) y al manejo de VPN. Este protocolo se basa en el uso de equipos especializados que permiten el intercambio de información a través de tráfico etiquetado como lo realiza MPLS y emplea una infraestructura de transporte virtual como lo hace el uso de VPN.

El protocolo OTV de cisco es un tema relativamente nuevo en Latinoamérica y del que no se dispone de mucha información en idioma español, existen también algunas nuevas terminologías utilizadas que dificultan el entendimiento de la funcionalidad que tiene este protocolo y los beneficios que aporta para el mundo de las redes. Al ser un

protocolo compuesto es necesario conocer algunos de los protocolos que trabajan cooperativamente para el manejo y transporte de la información, esto con el fin de tener una idea clara de cómo funciona y como procesa la información que debe ser transportada.

En este trabajo se pretende realizar la implementación de una red piloto sobre un ambiente virtualizado que permita mostrar el funcionamiento y características del protocolo OTV para mejorar la comprensión de los usuarios que desean tener información sobre esta solución.

Algunos de los temas que se tratan en este trabajo son de gran importancia para la comprensión del funcionamiento del protocolo por lo que se recomienda leer detenidamente la sección del fundamento teórico en el cual se encuentra contenida la información más relevante y por ningún motivo es recomendable ir directamente al diseño pues hay aspectos técnicos que requieren de conocimiento previo para ser comprendidos.

CAPÍTULO 1

FUNDAMENTO TEÓRICO

1.1 Ipv4

Ipv4 corresponde a la cuarta versión del protocolo de Internet (Internet Protocol) que permite la interconexión de redes proporcionando un esquema de transporte para él envió de paquetes entre redes locales o distantes a través de la trasmisión de conjuntos de datos conocidos como datagramas en los cuales se incluye la dirección de origen y la de destino compuestas por identificadores numéricos que se conocen como dirección IP y son únicos para cada dispositivo.

1.1.1 Notaciones

Para representar las direcciones IP existen diferentes tipos de notaciones utilizadas, la más común es utilizar un número decimal dentro del rango de 0 a 255 establecido en concordancia con el valor equivalente en binarios que puede tomar el octeto, entonces una dirección valida seria 192.168.1.1 no así 258.205.23.16 que se encuentra fuera del rango de valores.

Notación decimal

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**=**	**255**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**=**	**1 octeto**

Figura 1. Notación decimal
Fuente: Wilson Collaguazo y Katherine Ramos

En hexadecimal la notación puede ir desde 0 a FF donde una dirección valida seria B2.D2.2.1 y una no valida seria H3.F2.6.5 pues ya quedaría fuera del rango de los octetos.

Notación Hexadecimal

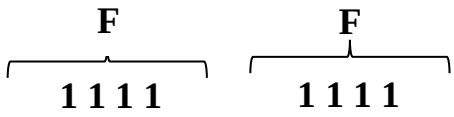


Figura 2. Notación Hexadecimal
Fuente: Wilson Collaguazo y Katherine Ramos

En binario la notación puede ir entre 00000000 a 11111111, entonces la forma de escribirla es:

Notación Binaria

10101010. 11111111. 11110000. 00000000

Figura 3. Notación Binaria
Fuente: Wilson Collaguazo y Katherine Ramos

1.1.2 Aplicaciones

El protocolo IP es utilizado para clasificar las redes y de este modo tener un control de la asignación de IP's a nivel mundial, permitiendo así asegurar que lleguen a cada equipo como una dirección única e irrepetible. Las redes se han clasificado en cinco grupos que son Clase A, Clase B, Clase C, Clase D, Clase E.

1.1.3 Limitantes

En la actualidad IPv4 se considera un protocolo con direcciones insuficientes que deber ser remplazado por IPv6 pues según la LACNIC no hay más direcciones para América latina y el Caribe y han declarado el agotamiento de direcciones.

1.2 Open Shortest Path First (OSPF)

1.2.1 Características

- No presenta limitación para el conteo de saltos.

- El uso apropiado de VLSM es de gran utilidad en el proceso de asignación de direcciones IP.
- OSPF utiliza multidifusión IP para enviar actualizaciones de estado de enlace garantizando un menor procesamiento en los routers que no están a la escucha de paquetes OSPF. Las actualizaciones sólo se envían en caso de cambios de enrutamiento y no de manera periódica. Esto garantiza un mejor uso del ancho de banda.
- Tiene mejor convergencia debido a que los cambios en el enrutamiento se propagan de forma instantánea y no periódica.
- Mejora el balance de carga evaluando el costo de los enlaces y teniendo rutas alternas de respaldo.
- Presenta definiciones lógicas de redes en las que los routers se pueden dividir en áreas. De este modo, se limita el broadcast de actualizaciones de estado de enlace en toda la red, además de proporcionar un mecanismo para agregar rutas y reducir la propagación innecesaria de información de subred.
- Tiene autenticación de enrutamiento a través de distintos métodos de manejo de contraseñas.
- Permite la transferencia y el etiquetado de rutas externas inyectadas en un sistema autónomo. De este modo, se realiza un seguimiento de las rutas externas inyectadas por protocolos exteriores como BGP.

1.2.2 Funcionalidad

OSPF se basa en la existencia de un mapa de la red el cual es conocido por todos los nodos y regularmente actualizado. Para llevar a cabo este propósito la red debe de ser capaz de almacenar en cada nodo el mapa de la red y actuar rápidamente ante cualquier cambio en la estructura de la red tomando en cuenta la seguridad, la creación de bucles innecesarios y siempre teniendo en cuenta posibles particiones o uniones de la red. (Gil, 2013)

Mapa de red local

La creación del mapa de red local en cada router de la red se realiza a través de una tabla donde una fila representa a un router de la red y cualquier cambio que le ocurra a ese router será reflejado en este registro de la tabla a través de los registros de descripción. Una columna de la tabla representa los atributos de un router que son almacenados para cada nodo. (Gil, 2013)

Los atributos de los nodos son el identificador de interface, el número de enlace e información acerca del estado del enlace, o sea, el destino y la distancia o métrica. (Gil, 2013)

Con esta información cada router es capaz de crear su propio mapa de la red idéntico lo cual implicará que no se produzcan bucles y que la creación de este mapa de red local se realiza en los router lo más rápido posible. (Gil, 2013)

Mapa de red Local

Ejemplo

A --- 1 --- B --- 2 --- C --- 3 --- D --- 4 --- A

DE	A	ENLACE	DISTANCIA
A	**B**	**1**	**1**
B	**C**	**2**	**1**
C	**D**	**3**	**1**
D	**A**	**4**	**1**

Figura 4. Mapa de red Local
Fuente: Wilson Collaguazo y Katherine Ramos

Los routers envían periódicamente mensajes HELLO para que el resto de routers, tanto si pertenecen al mapa local como a un circuito virtual sepan que están activos. (Gil, 2013)

Para que un router sepa que sus mensajes se están escuchando los mensajes HELLO incluyen una lista de todos los identificadores de los vecinos cuyos saludos ha oído el emisor. (Gil, 2013)

Respuesta ante un cambio en la topología de la red

Un cambio en la topología de la red es detectado en principio por el nodo que causo el cambio o por los nodos afectados por el enlace que provoco el cambio. El protocolo o mecanismo de actualización de la información de la red debe ser rápido y seguro para esto OSPF utiliza los protocolos de inundación y de intercambio o sincronización. (Gil, 2013)

Protocolo de Inundación (The flooding Protocol)

Este protocolo consiste en el paso de mensajes entre nodos, partiendo el mensaje del nodo o nodos que han advertido el cambio, tal que cada nodo envía el mensaje recibido por todas sus interfaces menos por la que le llega siempre y cuando no haya recibido ese

mensaje, para ello cada mensaje cuenta con un identificador de mensaje o contador de tiempo para constatar su validez.

Ejemplo

Suponiendo que en la red anterior el enlace que va del nodo A al B, queda fuera de servicio de tal manera que la distancia pasa a ser infinito.

El mensaje que A enviara a D será:

Desde A hacia B, enlace 1, distancia infinito, numero 2.

El mensaje que B enviara a C será:

Desde B hacia A, enlace 1, distancia infinito, numero 2.

La base de datos después del protocolo de flooding quedaría:

Mapa de red local después del Flooding

DE	A	ENLACE	DISTANCIA	NÚMERO
A	**B**	**1**	**infinito**	**2**
B	**C**	**2**	**1**	**1**
C	**D**	**4**	**1**	**1**
D	**A**	**3**	**1**	**1**
B	**A**	**1**	**infinito**	**2**
C	**B**	**2**	**1**	**1**
D	**C**	**4**	**1**	**1**
A	**D**	**3**	**1**	**1**

Figura 5. Mapa de red local después del Flooding
Fuente: (Gil, 2013)

Hay que entender que un cambio en un enlace de la red puede dejar aislados a unos nodos de la red, es decir, puede partir la red. Este cambio tal como está planteado el mapa local no es problema ya que aunque todos los nodos de la red inicial no tengan el mismo mapa local este será idéntico para cada uno de los nodos en cada una de sus particiones.

El proceso mediante el cual se produce el chequeo del mapa local de las diferentes subredes para formar uno idéntico para todos los nodos de la nueva red se denomina:

Protocolo de Chequeo de Mapas (Bringing Up Adjacencies)

Se basa en la existencia de identificadores de enlace y número de versiones, a partir de estos OSPF forma unos paquetes de descripción del mapa local e inicializa un proceso de sincronización entre un par de routers de la red que tiene dos fases:

Una de intercambio de paquetes de descripción del mapa local entre los nodos y en la que cada nodo crea una lista de nodos nuevos a tener en cuenta o actualiza su número de versión y el identificador del enlace.

La otra fase es la creación en cada nodo de paquetes con información acerca de esos nodos especiales que se envían a sus vecinos para que corroboren la información.

Tras terminar este intercambio de información, ambos routers conocen los nodos que son obsoletos en su mapa local y los nodos que no existían en su mapa local. Los mensajes que se usan para solicitar todas las entradas que necesiten actualización son los Link State Request o mensajes de petición de estado de enlace y los mensajes de respuesta son los Link State Update. (Gil, 2013)

1.2.3 Aplicaciones

OSPF tiene como ventaja que fue diseñado para adaptarse al máximo a los protocolos TCP/IP permitiendo la conexión de redes locales con un enlace "link to a stub network" que permite asignar a la red local un número de subred y especificar solamente un enlace entre el router y la subred. (Gil, 2013)

1.2.4 Limitantes

La configuración del protocolo debe ser muy cuidadosa, hay que tener en cuenta el área a la que se asignara una determinada red pues si el área de la red es incorrecta ese

enlace quedará excluido del mapa de red local y queda en estado de inalcanzable con valor infinito.

Otra desventaja de este protocolo es que generará una mayor sobrecarga en la asignación de memoria y utilización de la CPU. (Cisco Systems Inc, 2008)

1.3 Multiprotocol Label Switching (MPLS)

MPLS fue creado por la IETF y definido en el RFC 3031, es un híbrido entre ATM e IP que se basa en el envío de paquetes con etiquetado y en la conmutación de los flujos de tráfico a través de la red, opera entre la capa de enlace de datos y la capa de red del modelo OSI por lo tanto se puede definir como la capa 2.5 tal como se muestra en la figura1. (Escalante Gil, 2012)

Modelo de capas para MPLS

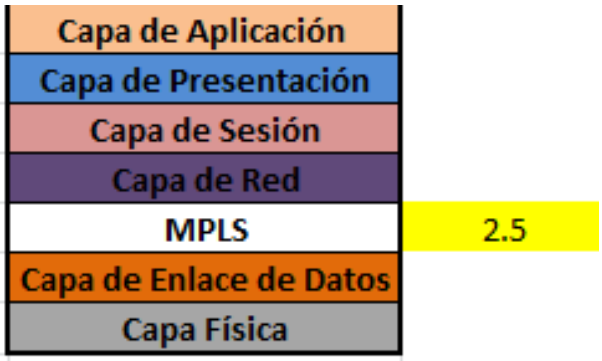


Figura 6. Modelo de capas para MPLS
Fuente: Wilson Collaguazo y Katherine Ramos

1.3.1 Características

- MPLS cuenta con las siguientes características:
- MPLS puede funcionar sobre cualquier tecnología de transporte como ATM, Frame-Relay y Ethernet
- Tiene algunos mecanismo para manejar el flujo de tráfico de tamaños variados
- Es independiente de protocolos de capa 2 y 3

- Interconecta a los protocolos existentes en la red
- Soporta él envió de paquetes tanto unicast como multicast
- Facilita la gestión de VPNs
- Permite el crecimiento constante de la Internet
- Especifica mecanismos para gestionar flujos de tráfico de diferentes tipos
- Es compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP (Cure & Gonzáles , 2012, pág. 11)

1.3.2 Funcionalidad

MPLS se utiliza en el núcleo de las redes de los proveedores de servicio, realiza la transmisión mediante caminos de etiquetas conmutadas (LSP), que forman una cadena de etiquetas en el camino a los nodos desde el emisor al receptor.

MPLS proporciona soporte de QoS (Quality of service) y CoS (Class of service) para diferenciar los servicios, orientado a conexión y a la gestión de tráfico, permite agilizar los procesos de envío de paquetes conservando la flexibilidad de un modelo de red IP.

LSPs (Label-Switched Paths)

La ruta se establece antes que la transmisión de datos empiece para que el paquete que ingresa a la red MPLS pueda ser examinado y así poderle asociar una LSP y una etiqueta adecuada. Esta decisión se debe a factores como:

- La dirección de destino
- QoS
- Estado actual de la red.

Cuando se asigna un LSP a un FEC este va en una sola dirección por lo tanto al tráfico de vuelta se le debe asignar otro LSP para ayudar a distribuir la carga y se asigna un nuevo LSP cuando hay un fallo en la red o cambia la topología para volver a encaminar todo el tráfico.

Hay dos formas de requerir los LSPs que son:

- Antes de la transmisión de datos (control-driven).
- Una vez detectado un cierto flujo de datos (data-driven).

Dominio MPLS

Un dominio MPLS corresponde a un grupo de equipos configurados con MPLS donde se establece un camino para que un paquete siga su recorrido con un determinado FEC.

Existen dos mecanismos para establecer un LSP:

- Encaminamiento salto a salto: El LSR asigna el próximo salto para un FEC, utilizando así cualquier protocolo de enrutamiento disponible en ese momento.
- Encaminamiento explícito: El LER de entrada establece el número de saltos desde el inicio hasta la salida, también permite que un LSP sea encaminado a un área de la red que se encuentre fuera del control administrativo de quien comenzó el LSP mediante la asignación de un identificador de sistema autónomo.

LSR (Label Switched Router)

Son routers de gran velocidad que se encuentra en el núcleo de una red MPLS, también se pueden usar los switches ATM como LSRs sin que tengan que cambiar su hardware.

Cada LSR debe contener (interfaz de entrada, etiqueta asociada) → (interfaz de salida, etiqueta asociada') dentro de sus tablas de envió para poder usar los LSPs.

Sus funciones son las siguientes:

- Participar en la asignación de los LSPs mediante el uso de un protocolo de señalización adecuado.
- Conmutar rápidamente el tráfico de datos entre los caminos establecidos.

LER (Label Edge Router)

Son routers que se encuentran en el borde de la red que pueden conectarse a diversas redes no similares como Frame Relay, ATM y Ethernet. Se encargan de asignar y remover las etiquetas que fueron asignadas a los paquetes, también son responsables de enviar el tráfico que ingresa a la red MPLS mediante el uso de un protocolo de señalización de etiquetas y distribuir el trafico saliente entre las diferentes redes.

LDP (Label Distribution Protocol)

LDP es un método estándar para la distribución de etiquetas de enrutamiento entre los LSRs vecinos que sirven para establecer la comunicación y poder ubicarse con los mismos. Usa pares LDP para el intercambio de etiquetas y mapear información entre los LSRs que utilizan LDP, mediante el inicio de sesión de LDP.

Tipos de mensaje LDP

- Discovery messages: anuncia y mantiene la presencia de un LSR en la red como por ejemplo con él envió de hellos
- Session messages: establece, mantiene, y termina sesiones entre LDP pares como por ejemplo con él envió de keepalive.

- Advertisement messages: crea, cambia, y borra el mapeo de las etiquetas para FECs como por ejemplo con él envió de label mapping.
- Notification messages: provee información de avisos y señalización de errores

FEC (Forward Equivalence Class)

La FEC es un grupo de paquetes IP que comparten mismas características para ser transportadas, se produce cuando el paquete entra en la red, lo que permite que una etiqueta sea negociada entre LSRs vecinos, desde el ingreso hasta la salida de un dominio. (Ferrer Martínez, 2011)

1.3.3 Arquitectura

Nodos MPLS

Un nodo MPLS tiene conocimiento de los protocolos de control, es un punto de interconexión de MPLS que opera en uno o más protocolos de enrutamiento de la capa de red del modelo OSI, lo cual le da la capacidad de volver a enviar paquetes en base a etiquetas.

Tipos de nodos MPLS

- Nodo de tránsito: Recibe el PDU y usa la cabecera MPLS para tomar las decisiones de reenvío, también realiza el intercambio de etiquetas. También llamado LSR interior, o LSR del núcleo.
- Nodo de borde: Conecta un dominio MPLS con un nodo fuera del dominio. Pueden haber dos tipos, de acuerdo al rol que adopten en un momento dado:
- Nodo de egreso: maneja el tráfico que sale del dominio MPLS.
- Nodo de ingreso: maneja el tráfico que ingresa en el dominio MPLS.

Planos de control

Los planos de control permiten anunciar las etiquetas y las direcciones, para asociarlas entre sí, pueden operar más de un protocolo entre ellos LDP.

Los mensajes de control se intercambian entre LSRs para realizar varias operaciones:

- Intercambio de mensajes periódicos de hello.
- Intercambio de mensajes de etiquetas y direcciones para ser asociadas, y usar posteriormente esta asociación en el plano de datos para el reenvío de tráfico.

Planos de datos

Los planos de datos de MPLS examinan el encabezado del paquete MPLS para reenviar el tráfico. Cuando el tráfico es entregado al usuario receptor, la dirección de red es examinada para entregar el paquete y la cabecera de etiquetas es eliminada. (Velásquez)

Etiquetas

Las etiquetas identifican el camino que un paquete puede atravesar. La etiqueta es encapsulada en la cabecera de la capa de enlace. Una vez el paquete ha sido etiquetado viajará a través del backbone mediante conmutación de etiquetas, es decir, cada router examinará la etiqueta, consultará en sus tablas de envío para saber con qué etiqueta y por qué interfaz debe salir, intercambiará las etiquetas y lo enviará por el interfaz correspondiente.

Pasos para la asignación de etiquetas:

- Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.

- Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa 2 para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 pueden servir como etiquetas. Para redes como Ethernet y PPP a la etiqueta se le añade una cabecera shim entre las cabeceras de la capa 2 y la capa 3, que contendrá el campoTTL (Time To Live).
- Las decisiones para la asignación de las etiquetas están basadas en criterios de envío como encaminamiento unicast, multicast, ingeniería de tráfico, VPN y QoS.
- Las etiquetas constan de 32 bits y tienen el siguiente formato:

Formato de etiquetas MPLS

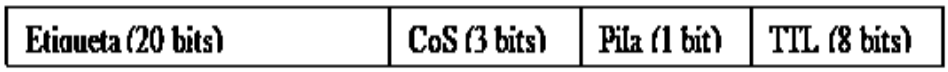


Figura 7. Formato de etiquetas MPLS
Fuente: (Ferrer Martínez, 2011)

- Etiqueta (20 bits): contiene la etiqueta asignada.
- CoS (3 bits): indica la clase de servicio que requiere el paquete.
- Pila (1 bit): permite apilar etiquetas en un paquete para realizar un encaminamiento jerárquico.
- TTL (8 bits): tiene el mismo significado que en IP, se denomina cabecera shim. (Ferrer Martínez, 2011)

1.3.4 Aplicaciones

Sus principales aplicaciones son:

- Ingeniería de tráfico: es el proceso que mejora la utilización de la red mediante la distribución del tráfico en ella de acuerdo con la disponibilidad de los recursos,

el tráfico actual y el esperado. CoS y QoS pueden ser factores a tener en cuenta en este proceso.

- Redes de Alto Rendimiento: las decisiones de encaminamiento tomadas por el router son más sencillas y rápidas.
- VPN: facilita crear y habilitar caminos de conmutación de etiquetas , lo cual hace más sencilla la creación de VPNs
- QoS: asigna a un cliente o a un tipo de trafico un reenvió de equivalencia de clase que se debe asociar a un camino de conmutación de etiqueta (Escalante Gil, 2012, pág. 6)

1.3.5 Limitantes

MPLS mediante el uso de etiquetas beneficia al paquete a llegar a su destino por lo cual se da el aumento de la cabecera transportada contribuyendo así a reducir el rendimiento de la red.

1.4 Overlay Transport Virtualization

Es un protocolo que abarca un conjunto de servicios añadidos en algunos dispositivos de borde (Switch Multicapa) empleados en redes empresariales u organizaciones que manejan gran cantidad de información y que requieren de equipos de alta gama que aporten beneficios a la red. El IOS - Titanium de los Switches CISCO Nexus de la serie 7000 es considerado el primero en implementarlo como una solución para el balance de carga de información transportada a través de los nodos que componen la red de trabajo.

OTV es un protocolo creado con el propósito de interconectar centros de datos separados físicamente a través de una red virtual sobrepuesta conmutada por paquetes permitiendo que estos trabajen con facilidad y como un solo centro de datos lógico

enlazados por los equipos de borde de cada sitio, se considera una mejor solución que cualquier otra tecnología de capaz como VPN, VPLS u otros.

Emplea un esquema de direccionamiento MAC en dentro de paquetes IP donde cada equipo de borde mantiene una tabla de direcciones MAC actualizada periódicamente utilizando anuncios de plano de control para todos los dispositivos del sitio a través del dominio OTV. Los equipos de borde intercambian constantemente información de enrutamiento de L2 entre ellos lo que permite el descubrimiento dinámico de nuevos equipos o el cambio de posición de uno de ellos.

Permite aumentar sin problemas los servicios que ofrecen los centros de datos, eliminando las restricciones de espacio y permitiendo distribuir de forma más rápida la carga de información que necesita enviar desde un lugar a otro a través de los centros de datos, maximiza el balance de carga, gestiona de forma eficiente la utilización de recursos y mejora la respuesta de las aplicaciones logrando así que los usuarios puedan acceder a las aplicaciones, incluso frente a un posible congestionamiento en el tráfico de un sitio.

Trabaja como una subcapa entre las capas L2 y L3 convirtiéndose en una extensión virtual transparente de L2 que provee conectividad multipunto y multisitio, formando una red sobrepuesta a través de la red de transporte y conformada por los equipos de borde que se encuentren con el servicio configurado. Al ser una solución que es configurada en los Switches de la red, los Routers que se utilicen no tienen incidencia en su funcionamiento. Mas esta solución necesita contar con equipos de alta gama que tengan incorporada esta herramienta en el IOS, de no ser así es necesario verificar si los equipos con los que se cuenta tienen soporte para implementarla y de ser así contactar

con un representante de la empresa pues la licencia es pagada, en algunos casos estos equipos pueden llegar a costar muchos dinero pero si se trata de grandes cantidades de información el costo beneficio resulta provechoso.

1.4.1 Características

OTV crea una LAN lógica sobrepuesta a la red de transporte conformada por los equipos de borde autorizados de cada sitio permitiendo algunas de las siguientes características:

- Balancea la carga a través de ECMP (Equal-Cost Multi-Path) del núcleo, para distribuir el tráfico hacia un mismo destino pero utilizando diferentes rutas o caminos.
- Provee multi-homing libre de bucles.
- La red superpuesta tiene un equipo de borde autorizado por sitio (Authoritative Edge Device) y es el único que puede reenviar paquetes a través de la red superpuesta, lo que evita que haya tráfico innecesario como bucles y duplicados.
- La red sobrepuesta se muestra de manera óptima a los equipos de borde interesados.
- Los equipos de borde que conforman la red sobrepuesta aprovechan la funcionalidad del protocolo IS-IS para conocer el estado de los enlaces de capa dos en la red sobrepuesta.
- Utiliza el protocolo de plano de control para el intercambio de la información de accesibilidad entre los diferentes equipos de borde OTV.
- Introduce el concepto de enrutamiento MAC
- Trabaja independientemente de la red de transporte implementada.
- Permite extender el dominio de Vlans a redes remotas.

- Permite unificar nodos que se encuentren en una misma ciudad.

1.4.2 Términos asociados con OTV

Dispositivos de borde

Es un dispositivo multicapa que se encuentra operando con la funcionalidad de un equipo de capa 2 y capa 3, actuando como núcleo de la red al proporcionar control sobre el estado de los enlaces L2 y permitiendo que se gestione el encapsulamiento de la información sobre la red virtualizada.

Dispositivo de borde autoritario o autorizado

Es el único dispositivo en un sitio que tiene el permiso de transmisión en la red sobrepuesta, ya que un sitio puede estar conformado por más de un nodo es necesario que haya un equipo mandatario. Un ejemplo de esto puede ser en el caso cuando en una misma ciudad hay barias sucursales de una empresa, entonces se necesita un equipo mandatario para la conectividad de la ciudad.

Red sobrepuesta

Es la red que conecta las interfaces virtuales creadas por OTV con el fin de establecer la adyacencia de los sitios que componen la red. Esta red puede ser gestionada para brindar servicios a clientes y para mejorar la conectividad con el proveedor ISP.

Interface Join

Es la interfaces de enlace de salida del dispositivo de borde, es la interfaz que se une a las de más interfaces de punto a multipunto de la red sobrepuesta. Se utiliza el encapsulamiento de la dirección IP de esta interfaz para anunciar la accesibilidad de una dirección MAC presentes en este sitio.

Interface interna

Es la interface que proporciona la troncalidad a las Vlans que han sido extendidas sobre la red sobrepuesta, es decir que permite la conexión interna de la red sobrepuesta con los equipos que se encuentran en el sitio.

Direccionamiento MAC

El direccionamiento MAC asocia la dirección MAC de destino del tráfico en L2 con la dirección IP correspondiente a una interface del dispositivo de borde. Las MAC para el direccionamiento IP se anuncia a los dispositivos de borde de cada sitio desde los equipos que lo conforman, a través del protocolo de plano de control de OTV. Este crea una tabla que almacena la posición de los equipos dentro de la red. Los equipos son accesibles a través de la dirección IP asignada desde un dispositivo remoto en el borde.

Direccionamiento MAC

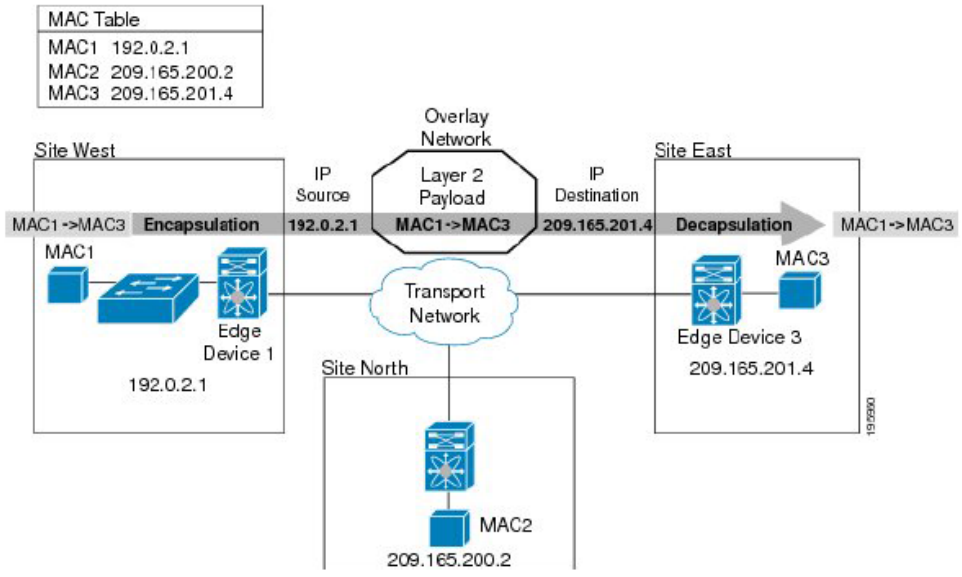


Figura 8. Direccionamiento MAC
Fuente: Cisco Systems, Inc.

Interface Overlay

Es una interfaz virtual de multidifusión con multi-acceso. La interfaz encapsula las tramas de nivel 2 que llegan al equipo borde asignándoles las cabeceras IP unicast o multicast y las transmite por la red sobrepuesta.

Sitio

Se considera un sitio a una red de capa 2 que puede ser individual o conformada por múltiples subredes separadas físicamente y que comparten la misma red de transporte para tener salida a redes remotas.

Sitio de Vlan

Sitio de VLAN envía mensajes que permiten detectar otros dispositivos de borde OTV que contenga la mismas Vlans registradas en el sitio y determina el dispositivo de borde de autoridad para tener conectividad con las VLANs extendidas sobre la red sobrepuesta. La VLAN 1 es la VLAN por defecto del sitio pero puede ser modificada basta con asegurarse de que este activa en al menos uno de los puertos del dispositivo de borde y que el sitio VLAN no se extienda a través de la red como una Vlan de datos.

Tipos de redes OTV

Red con un enlace OTV simple

Topología de una red OTV con enlace simple

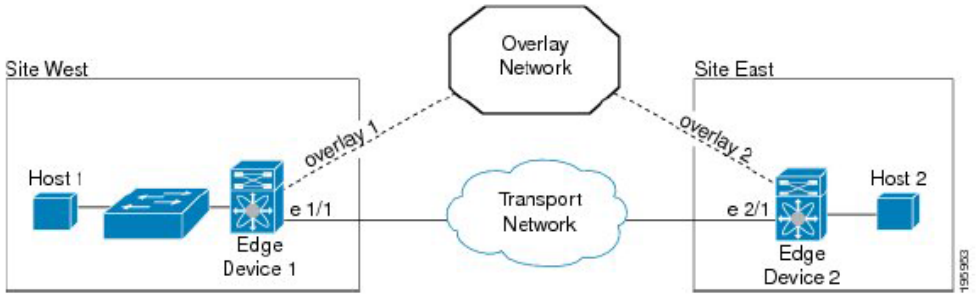


Figura 9. Topología de una red OTV con enlace simple
Fuente: Cisco Systems, Inc.

Está compuesto por dos sitios con un dispositivo de borde cada uno y una red de transporte común, en ambos dispositivos se ha configurado una interface virtual Overlay que permite que se conecten a una red sobrepuesta común que comparte el mismo grupo de control.

Red con múltiples enlaces OTV

Topología de una red con múltiples enlaces OTV

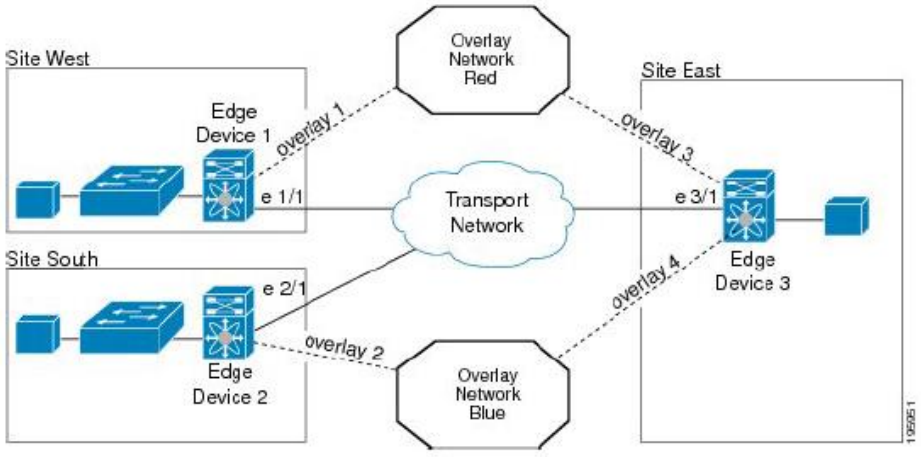


Figura 10. Topología de una red con múltiples enlaces OTV
Fuente: Cisco Systems, Inc.

Se compone por tres sitios con un dispositivo de borde cada uno, conectados a una red de transporte común, en cada equipo se configura una interface virtual Overlay que conecta a una de las dos redes sobrepuestas. El sitio del Oeste se conecta a la red

sobrepuesta Roja en común con el sitio del Este a través de las interfaces Overlay 1 y la Overlay 3, el sitio Este se conecta al sitio Sur por la red común sobrepuesta azul a través de las interfaces Overlay 4 y Overlay 2. Cada red sobrepuesta tiene diferentes direcciones del grupo de control. En esta topología puede haber algunos equipos de borde asociados a diferentes redes sobrepuestas.

Red con multi-homing y enlace simple

Topología de una red con multi-homing y enlace simple

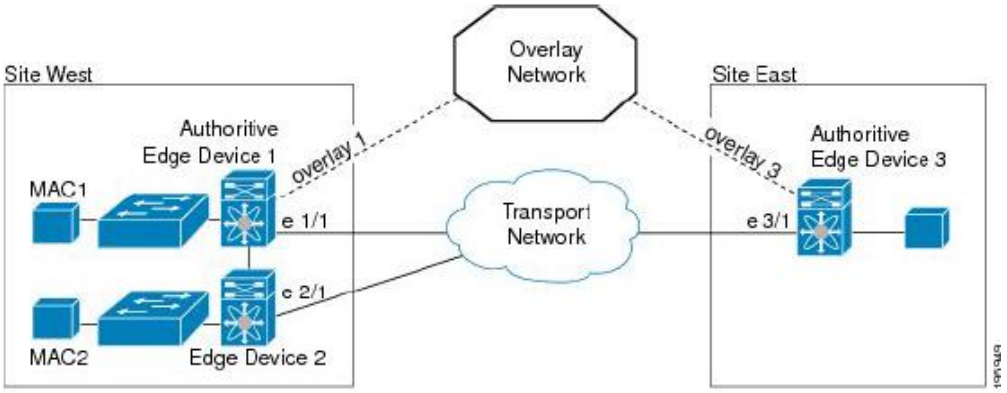


Figura 11. Topología de una red con multi-homing y enlace simple
Fuente: Cisco Systems, Inc.

Se compone de dos sitios con la particularidad de que uno tiene multi-homing o se considera un sitio compuesto, en este caso el sitio Oeste está compuesto por dos subredes cada una con un equipo de borde. Como ya se ha mencionado anteriormente en este caso se vuelve necesario designar un equipo autorizado que establezca la conectividad a la red sobrepuesta para todo el sitio. Los sitios comparten una red de transporte común y una red sobrepuesta común, la conectividad en la red sobrepuesta en este caso se realiza entre el dispositivo autorizado del sitio oeste y el equipo de borde del este por las Interfaces virtuales Overlay 1 y Overlay 3. En caso del sitio Oeste se configura al equipo de borde 2 como una extensión del equipo de borde 1 y de este

modo para la red sobrepuesta se verán lógicamente como si se tratara de un solo equipo de borde del sitio.

Este tipo de topología es muy utilizada por empresas que tienen sucursales en una misma ciudad y que comparten la misma red de transporte para dar salida hacia redes externas, en este caso OTV permite no solo que se unifiquen lógicamente sino que da paso a una nueva propiedad que es el balance de la carga de la red generada por el sitio, pues físicamente la topología está configurada como se muestra en el literal A de la Figura 11, pero lógicamente la red sobrepuesta trabaja como se muestra en el literal B de la Figura 11, esta configuración lógica permite que el tráfico que se transmite por la red sobrepuesta se comparta entre los dos dispositivos y los paquetes sean procesados con mayor rapidez, al pertenecer los equipos a red sobrepuesta siempre tendrán actualizada la tabla de direccionamiento MAC y una vez que los paquetes han sido desencapsulados se envían de inmediato hacia el destino.

Balance de carga

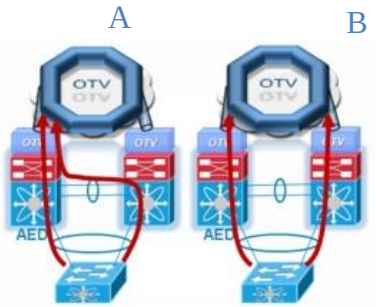


Figura 12. Balance de carga
Fuente: Cisco Systems, Inc.

Red con doble enlace

Se implementa en la misma topología que en la red de enlace simple o cualquier otra, se trata básicamente de configurar una interface virtual Overlay que provea redundancia al enlace con la

red sobrepuesta. En este caso lo que se bebe hacer es crear en cada equipo de borde otra interfaz Overlay adicional a la que se ha creado y conectarla a la red.

1.4.3 Funcionamiento

Actualización de tablas MAC

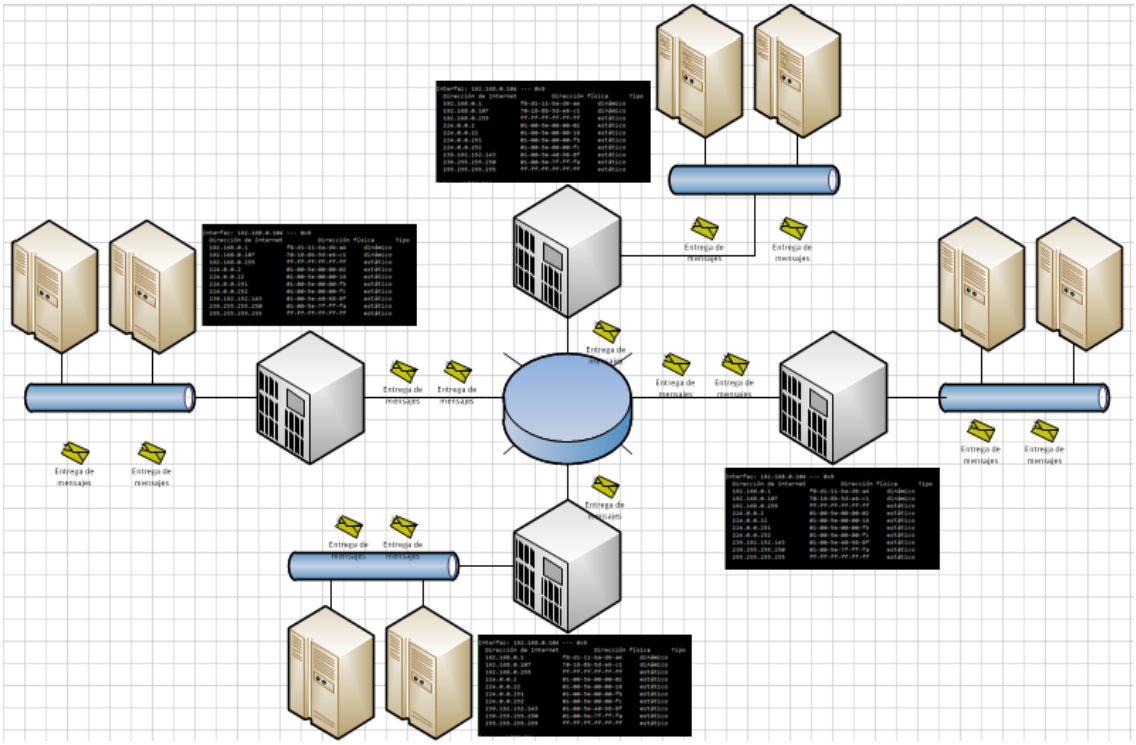


Figura 13. Actualización de tablas MAC
Fuente: Wilson Collaguazo y Katherine Ramos

En los equipos de borde correspondientes en cada sitio se crean interfaces virtuales Overlay que se conectan a la red sobrepuesta creando adyacencias entre los equipos que conforman la red. Una vez que los equipos de borde crean adyacencias mediante el protocolo de plano de control generan una tabla de direccionamiento MAC que se distribuye entre todos los equipos para que estos sepan la ubicación de cada uno en dentro de la red sobrepuesta, de esta manera una vez que los paquetes enviados desde un equipo dentro del sitio llegan hasta el equipo de borde autorizado del sitio, este los procesa y asigna a la interface Overlay correspondiente, la misma que añade las

cabeceras con la MAC del equipo destino dentro del paquete IP y lo reenvía a través de la red sobrepuesta que lo entrega al equipo de borde autorizado del sitio destino, una vez recibido el paquete el equipo de borde en el destino lo procesa y verifica que la MAC destino pertenece a un equipo de su sitio y lo entrega. En la Figura 13 se puede visualizar el envío de información entre los equipos que conforman la red superpuesta y la creación de la tabla de direcciones MAC que albergan los equipos borde de cada sitio.

La actualización de las tablas MAC se realizada constantemente por anuncios de plano de control que automatiza la detección de equipos, esto permite añadir o quitar equipos rápidamente. Los anuncios de plano de control abarcan protocolos de señalización internodos, descubrimiento de la topología, anuncio y reserva de recursos, cálculo para caminos y enrutamiento e información a intercambiar sobre el estado de los enlaces.

El equipo borde autorizado emisor envía un paquete Multicast hacia todos los equipos borde que se encuentran en la red supuesta para establecer las rutas que llevaran el paquete a su destino, una vez que el destino se ha señalado y las rutas se han establecido se realiza el encapsulamiento de los paquetes Unicast y se direccionan sobre la red sobrepuesta.

1.4.4 Arquitectura

Encapsulamiento de paquetes.

OTV realiza el encapsulamiento de los mensajes en paquetes UDP pues es un protocolo no orientado a conexiones fijas, la transferencia de datos en este caso utiliza múltiples caminos por los que los mensajes llegan a su destino utilizando encabezados de puerto origen y destino.

Formato de encapsulamiento de paquete UDP

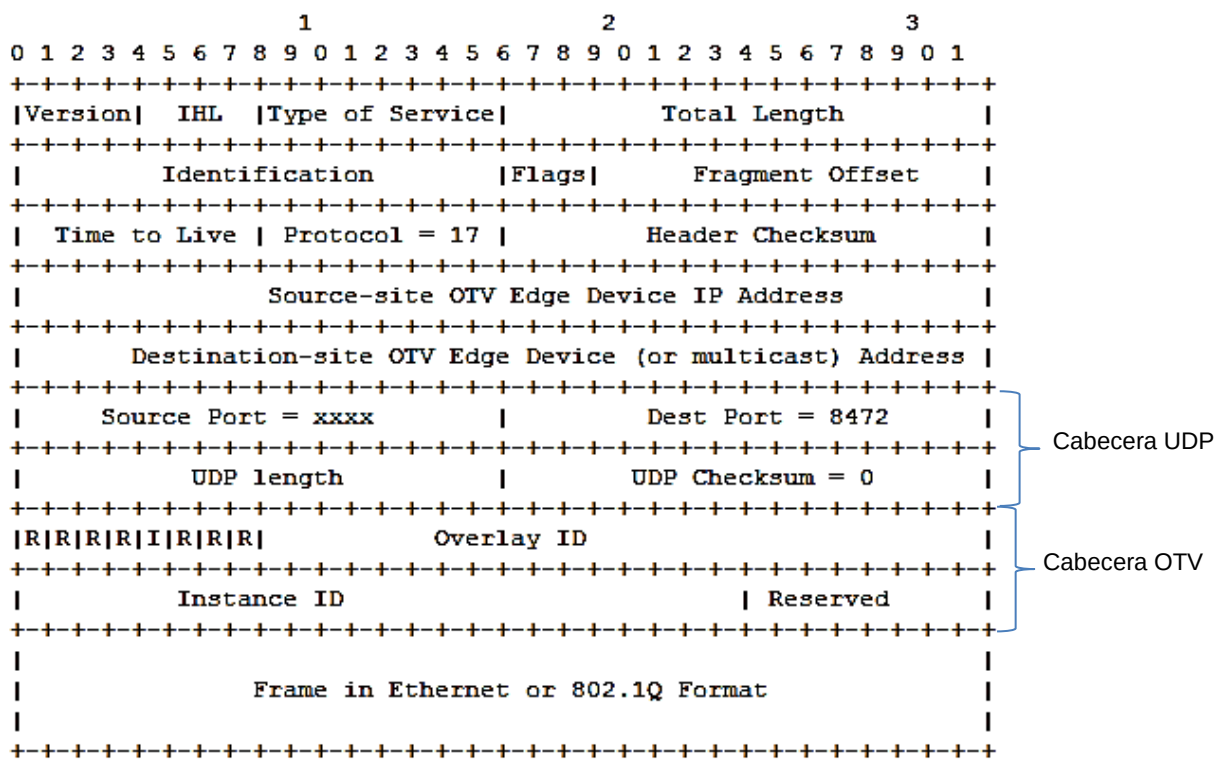


Figura 14. Formato de encapsulamiento de paquete UDP
Fuente: Wilson Collaguazo y Katherine Ramos

Componentes del mensaje:

- Versión (Versión): Configurado al valor de 4 (o 6) en decimal.
- Longitud de cabecera (IHL): Configurado al valor de 5 en decimal, no hay opciones IP presentes en el encapsulado de paquetes OTV.
- Tipo de Servicio / Clase de tráfico (Type of Service/Traffic Class): Los bits 802.1P de Ethernet.
- Longitud total (Total Length:): La longitud total del datagrama IPv4 en bytes. Esta incluye la cabecera IPv4, la cabecera UDP, la cabecera OTV, y la trama de capa dos sin el preámbulo y CRC.

- Identificación (Identification): Configurado aleatoriamente por el dispositivo de borde OTV
- Banderas (Flags): El bit DF (do not fragment) debe configurarse en 1.
- Tiempo de Vida / Límite Hop (Time to Live/Hop Limit): Establecido por el dispositivo de borde OTV y es configurable.
- Protocolo / Siguiente Cabecera (Protocol/Next Header): Dado que el paquete esta encapsulado UDP, este campo se configura al valor de 17 en decimal.
- Cabecera de control (Header Checksum): Debe ser calculado por el dispositivo de borde OTV sobre el campo de encabezado IP.
- Fuente Dirección (Source Address:): La dirección IPv4 del dispositivo de borde OTV hace la encapsulación de la trama de la capa dos.
- Dirección de destino (Destination Address:): La dirección IPv4 unicast o multicast, se configura por el dispositivo de borde OTV que se encapsula en la trama de la capa dos. Los dispositivos de borde deciden cuando la dirección se establece en una dirección unicast o multicast.

Cabecera UDP:

- Puerto de origen (Source Port): Es elegido por el dispositivo de borde OTV que está encapsulando la trama de la capa dos basado en un hash de la trama de capa dos. Esto permite que los paquetes sean uniformemente de carga dividida sobre los LAGs (Lag behind) en los routers de núcleo, son los responsables de la entrega de estos paquetes IP encapsulados.
- Puerto de destino (Destination Port): Este es un valor dado por la IANA, que asigna un número de puerto de usuario bien conocido. Los paquetes

encapsulados por un dispositivo de borde OTV ponen el valor de 8472 en el campo de puerto de destino.

- UDP Longitud (UDP Length): Es la longitud en bytes de la cabecera UDP, del encabezado OTV, y de la trama de capa dos sin el preámbulo y CRC.
- UDP Checksum (UDP Checksum): Se configura a 0 por el dispositivo de borde OTV al hacer encapsulación e ignorar al dispositivo de borde OTV que se está desencapsulando en el lugar de destino.

Cabecera OTV:

- Banderas (Flags):
- 'I' – Instancia ID de bits. Cuando se configura a 1, indica el ID de instancia, se debe utilizar en la búsqueda de reenvío.
- 'R' – Bits reservados.
- Superposición ID (Overlay ID): Se utiliza solo en los paquetes del plano de control, como URP / MRP (IS-IS) para identificar los paquetes para una superposición especifica.
- Instancia ID (Instance ID): Configurado por el dispositivo de borde OTV, hace la encapsulación para especificar una tabla lógica que se debe utilizar para la búsqueda de un dispositivo de borde OTV en el sitio de destino.

Trama de Ethernet:

- Trama de Ethernet (Frame in Ethernet): La trama de capa dos menos el preámbulo y CRC, recibidos en un enlace interno por un dispositivo de borde OTV.

- OTV aprovecha la funcionalidad del protocolo IS-IS para conocer el estado de los enlaces en la red superpuesta, en los equipos de borde que conforman la red superpuesta IS-IS forma parte de OTV por lo que no es necesario configurar ningún otro protocolo de enrutamiento en la red superpuesta bastara con levantar el servicio y configurarlo en cada uno de los nodos involucrados.

IS-IS

El protocolo de enrutamiento IS-IS (Intermediate System - Intermediate System) es un protocolo de estado de enlace, que es opuesto al protocolo de vector distancia. Al tener el estado de los enlaces se tiene varias ventajas sobre los protocolos de vector-distancia como por ejemplo mayor velocidad de convergencia, soporte Internetworks mucho más grandes, y es menos susceptible a los bucles de enrutamiento.

La ventaja de un protocolo de enrutamiento de estado de enlace es que el conocimiento completo de la topología permite que los equipos borde calculen rutas que satisfagan ciertos criterios particulares. Esto puede ser útil para los propósitos de ingeniería de tráfico, pues las rutas pueden ser delimitadas para determinado tipo de servicio.

IS-IS en cada enrutador distribuye información sobre el estado local de sus interfaces usables, vecinos accesibles y costo de la utilización de cada interfaz a otros routers utilizando un mensaje de estado de enlace PDU (LSP).

Cada router utiliza los mensajes recibidos para construir una base de datos idéntica que describe la topología de la red, a partir de esta base de datos, cada router calcula su propia tabla de enrutamiento utilizando un Shortest Path First (SPF) o algoritmo Dijkstra. Esta tabla a su vez contiene todos los destinos que el protocolo de

enrutamiento conoce y los asocia a una dirección IP que se constituye en el siguiente salto, la tabla indica también cuál es la interfaz de salida que le corresponde.

Funcionamiento

IS-IS asigna funcionalidad a los routers donde un dominio de ruteo se puede dividir en uno o más subdominios y cada subdominio se refiere a un área. Los routers de nivel-1 operan dentro del área mientras que los routers de nivel-2 operan en áreas diferentes. IS-IS no requiere de zona cero para pasar todo el tráfico inter-área, crea una topología lógica de una red troncal de routers de nivel-2 con ramas de nivel 1-2 y enrutadores de nivel-1 que forman las áreas individuales tal como se muestra en la Figura 10.

Router nivel-1: Solo enrutan a destinos dentro del área, en base al ID del sistema, usan una ruta por defecto 0.0.0.0 para enrutar hacia destinos fuera del área a través del router nivel 1-2 más cercano y mantiene una única base de datos para rutas del área.

Router nivel-2: Enrutan a destinos en otras áreas, en base al ID de área, mantienen una única base de datos para rutas del backbone.

Router nivel 1-2: Actúa como un vínculo para enrutar hacia dentro y fuera del área, mantiene dos bases de datos separadas, una para rutas del área y otra para rutas externas al área. Si se conecta a otra área se genera un ATT bit hacia el nivel-1. (Lavado, 2015)

Topología lógica de IS-IS

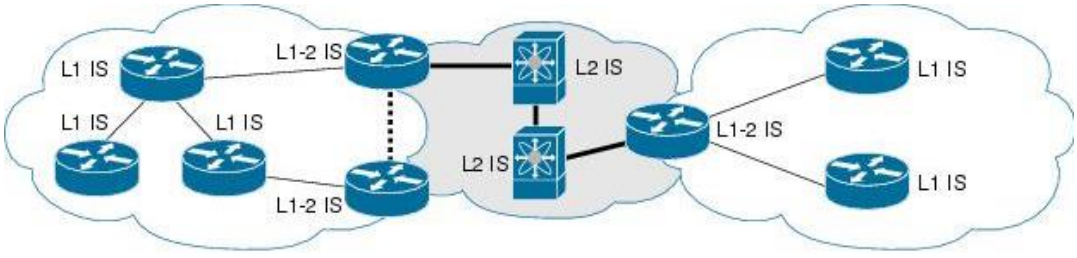


Figura 15. Topología lógica de IS-IS
Fuente: CISCO

Etiquetado IS-IS

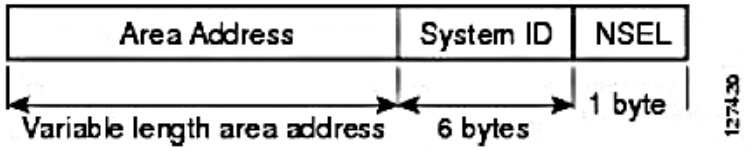


Figura 16. Formato de etiqueta IS-IS
Fuente: CISCO

- Dirección de área (Área Address): definido por la ISO como un área de direccionamiento privado, inicia con un valor de 49.
- ID del sistema (System ID): es un valor fijo de 6 bytes que identifica al router, debe ser único a nivel de área y dominio IS-IS.
- NSEL: si el NSEL es diferente de cero se trata de un NSAP e identifica al servicio dentro de un host IS-IS tradicional, si el NSEL es igual a cero se trata de un NET e identifica al propio host.

Tipos de paquetes

- Hello: usado para formar adyacencias, existen un formato para enlaces ponto a punto que una vez establecido el nivel de routing se pueden enviar las actualizaciones y otro formato para broadcast que son los de nivel-1 y nivel-2.
- LSP: intercambia información de enrutamiento.
- SNP: controla la distribución de los LSP, sirve para sincronizar la base de datos LSBD

Características

- Protocolo de estado de enlace para resolver las rutas cuyos mensajes usan el formato TLV que lo hace flexible a cambios.
- Soporta VLSM, sumarización y autenticación entre áreas.

- Utiliza algoritmo SPF.
- Converge rápidamente cuando hay cambios en la red.
- Forma adyacencias con los routers directamente conectados mediante el intercambio de hello's.
- La métrica usada para comparar rutas depende del costo de casa enlace.

Túneles GRE

OTV utiliza Generic Router Encapsulation (GRE) sobre IP y añade un suplemento a la cabecera OTV para codificar la información de la LAN virtual. La encapsulación OTV es de 42 bytes, que es menor que una LAN privada virtual de servicios (VPLS) sobre GRE. La encapsulación se lleva a cabo en su totalidad por el motor de reenvío en el hardware.

GRE, es un protocolo, que puede encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre dos máquinas que estén comunicándose por este protocolo. Su uso principal es crear túneles VPN, GRE, está definido por los RFC 1701, 1702 y 2784.

Es importante conocer la necesidad a la hora de realizar la configuración de túneles GRE, pues, podrían ser difíciles de manejar si la cantidad de los mismos crece demasiado. Estos túneles resultan ser útiles cuando se necesita trabajar con un protocolo que no es enrutables o con protocolos enrutables diferentes de IP a través de una red IP.

GRE toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, en el siguiente grafico se muestra el formato de encapsulación.

Formato de encabezado GRE

Encabezado de vinculo de datos (D/L)
Encabezado IP
Encabezado GRE
Encabezado PPP
Carga útil de PPP cifrada
Final del vínculo de datos

Figura 17. Formato de encabezado GRE
Fuente: Wilson Collaguazo y Katherine Ramos

A los datos o carga útil que va a atravesar el túnel se le proporciona un encabezado del Protocolo punto a punto (PPP) y, a continuación, se coloca dentro de un paquete GRE.

El paquete GRE lleva los datos entre los dos extremos del túnel. Después de que el paquete GRE llegue al destino final (el extremo del túnel), se descarta y el paquete encapsulado se transmite a continuación a su destino final.

OTV crea múltiples túneles GRE que permiten establecer varias rutas de igual costo entre el equipo origen y destino estableciendo enlaces multipunto multisitio que reducen el tiempo de transmisión de la información.

Topología lógica de GRE

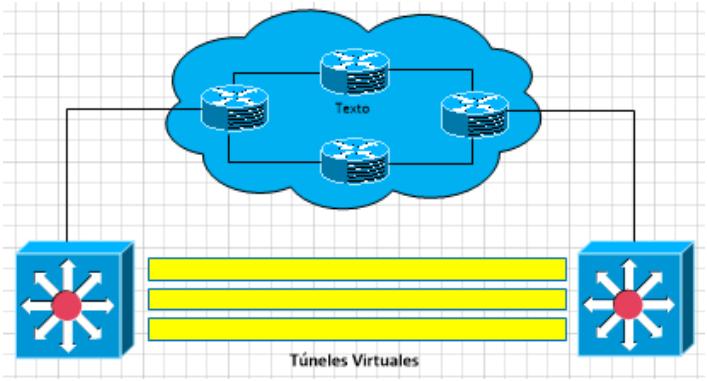


Figura 18. Topología lógica de GRE
Fuente: Wilson Collaguazo y Katherine Ramos

Multihoming

El Multihoming se refiere a la conexión de un sistema autónomo a más de un ISP al mismo tiempo como se muestra en la Figura 14. Para su implementación se necesita

conseguir un conjunto de direcciones independientes del proveedor junto con un número de sistema autónomo y dar a conocer mediante BGP a cada uno de los ISPs conectados el conjunto de direcciones obtenidas del proveedor, si un sitio no es capaz de hacer multihoming con las direcciones independientes del proveedor es posible conseguir un conjunto de direcciones de uno de los ISPs que prestan el servicio, donde el sistema autónomo cliente anuncia su conjunto de direcciones mediante BGP a los ISPs conectados y estos lo anuncian al internet.

Topología lógica de Multihoming

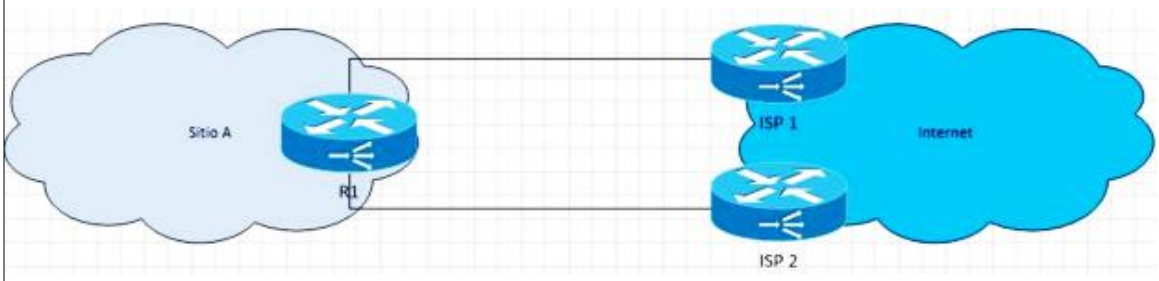


Figura 19. Topología lógica de Multihoming
Fuente: Wilson Collaguazo y Katherine Ramos

Características

- Facilita el balanceo de carga de tráfico entre los diversos proveedores disponibles.
- Distribuye el tráfico entrante y saliente entre los diferentes proveedores disponibles.
- Tolerante a fallos ya que cada sitio debe ser capaz de poder comunicarse con el exterior cuando falle algo en la red.
- Decide que volumen de tráfico enviar a cada ISP basándose en los acuerdos de nivel de servicio.

- Posee independencia de los ISPs por lo que cada sitio puede contratar a distintos ISPs en forma independiente e implementar multihoming por sí mismos.

Funcionamiento

Multihoming mantiene un sistema autónomo para facilitar la conexión a internet, cuando existe alguna falla o se pierde una de sus conexiones, provee un mejor servicio ya que dirige el tráfico a cualquier otro destino utilizando otra conexión y así poder prevenir la saturación en el destino de dicha conexión.

Múltiples conexiones utilizando un solo ISP

Si se produce alguna falla en el ISP se pierde la conexión por completo la salida del cliente al internet.

Multihoming utilizando un solo ISP

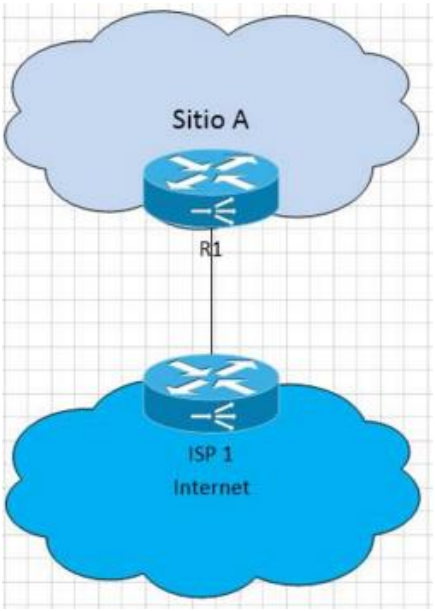


Figura 20. Multihoming utilizando un solo ISP
Fuente: Wilson Collaguazo y Katherine Ramos

Múltiples conexiones con varios ISP

Proporciona una alta disponibilidad de la conexión y permite que la red sea redundante, si algún ISP falla rápidamente se puede acceder al otro ISP y así evitar la pérdida de conexión de un cliente al internet.

Multihoming utilizando varios ISP

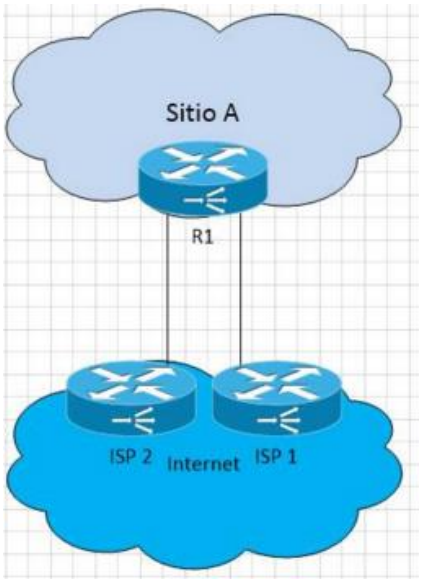


Figura 21. Multihoming utilizando varios ISP
Fuente: Wilson Collaguazo y Katherine Ramos

1.4.5 Configuraciones

Habilitación de las funciones de OTV

Por defecto las funciones vienen deshabilitadas pues se requiere de una licencia para su uso, provisionalmente al habilitar las funciones se tiene un periodo de evaluación del producto por 120 días.

Tabla 1.

Funciones OTV.

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal switch(config)#	Ingreso al modo de configuración global.
Paso 2	**Feature otv** Example: switch(config)# feature otv	Activa las funciones de OTV
Paso 3	**show feature | include otv [interface]** Example: switch(config)# show feature | include otv	Muestra el estado de activación o desactivación de las características de OTV. .
Paso 4	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Activar funciones OTV
Fuente: Cisco Systems, Inc.

Configuración de la interface física que se asocia a la interfaz Overlay

Se asocia una interface física a la interface virtual Overlay para aprovechar el enlace a la red de transporte y el encapsulado IPV4.

Tabla 2.

Interfaz Overlay

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal switch(config)#	Ingreso al modo de configuración global.
Paso 2	**Interface [interface]** Example: switch(config)# interface Ethernet 2/1	Ingreso al modo de configuración de la interface
Paso 3	**ip address [IP] + [mascara red]** Example: switch(config-if)# ip address 12.12.12.1 255.255.255.248	Asigna la dirección ip de la interface
Paso 4	**Ip igmp version 3** Example: switch(config-if)# ip igmp version 3	Activa igmp versión 3 en la interface, de este modo se añade al grupo.

Paso 5	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Asignación de IP a interfaz física
Fuente: Cisco Systems, Inc

Configuración de la interface Overlay

Es la interface que provee la adyacencia a la red virtual sobrepuesta, se encarga de encapsular el direccionamiento MAC entre equipos.

Tabla 3.

Configuración interfaz Overlay

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal switch(config)#	Ingreso al modo de configuración global.
Paso 2	**Interface overlay [numero]** Example: switch(config)# interface overlay 1	Crea una interfaz superpuesta de OTV y entra en el modo de configuración de interfaz. El rango es de 0 a 65535
Paso 3	**Description [nombre]** Example: switch(config-if-overlay)# description sitio_A	Configura una descripción de la red superpuesta, se puede utilizar una cadena alfanumérica entre mayúsculas y minúsculas de hasta 80 caracteres.
Paso 4	**OTV control group [dirección]** Example: switch(config-if-overlay)# otv control-group 239.1.1.1	Permite configurar la dirección del grupo multicast utilizada por el plano de control OTV para esta red superpuesta OTV. La dirección de grupo multicast es una dirección IPv4 en notación decimal con puntos.
Paso 5	**OTV data-group [dirección]** Example: switch# copy running-config startup-config	Configura uno o más rangos de prefijos de grupos locales IPv4 multicast utilizados para el tráfico de datos multicast. Utilizar SSM grupos multicast 232.0.0.0/8. Se pueden definir hasta ocho rangos de grupo.
Paso 6	**OTV join-interface [interface física]** Example: switch(config-if-overlay)# otv join-interface ethernet 2/1	Se une la interfaz superpuesta de OTV con una interfaz física de nivel 3. Se debe configurar una dirección IP en la interfaz física.
Paso 7	**No shutdown** Example: switch(config-if-overlay)# no	Enciende la interface y protocolos de comunicación.

	shutdown	
Paso 8	**Show otv overlay [numero]** Example: switch# show otv overlay 1	Muestra la configuración de la interfaz superpuesta de OTV
Paso	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Asignación IP interfaz Overlay
Fuente: Cisco Systems, Inc

Configuración de Vlan's extendidas

Se asigna las ID's de las Vlan's que se quiere extender sobre la red sobrepuesta, se pueden extender tantas como se haya creado.

Tabla 4.

Configuración Vlans Extendidas

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal switch(config)#	Ingreso al modo de configuración global.
Paso 2	**Otv extend-vlan [Rango]** Example: switch(config)# otv extend-vlan 2,5-34	Asigna el rango de Vlan's que se extienden por la red sobrepuesta
Paso 3	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Asignación de Vlans extendidas
Fuente: Cisco Systems, Inc

Configuración de la VLAN de Sitio

La Vlan de sitio tiene la función de troncalizar la salida de la información del sitio por un solo enlace, evita que se genere tráfico innecesario.

Tabla 5.

Configuración Vlan de sitio

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal	Ingreso al modo de configuración global.

	switch(config)#	
Paso 2	**otv site-vlan [numero]** Example: switch(config)# otv site-vlan 10	Configura una VLAN a la cual todos los dispositivos de borde locales se comunican. Se recomienda que se utilice el mismo ID de VLAN en todos los sitios. El rango es de 1 hasta 3967, y desde 4048 a 4093. El valor predeterminado es 1
Paso 3	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Asignación de Vlans de sitio
Fuente: Cisco Systems, Inc

Configuración de autenticación de OTV PDU

Permite crear un método de autenticación de los paquetes transmitidos por la red sobrepuesta.

Tabla 6.

Configuración autenticación OTV PDU

	Comando	Propósito
Paso 1	**Configure terminal** Example: switch# configure terminal switch(config)#	Ingreso al modo de configuración global.
Paso 2	**Otv-isis default** Example: switch(config)# otv-isis default	Entra en el modo de configuración del router OTV.
Paso 3	**Vpn [nombre]** Example: switch(config-router)# vpn Overlay1	Entra en el modo de configuración OTV de red privada virtual (VPN). El nombre de sobreposición puede ser cualquiera, puede ser una cadena alfanumérica entre mayúsculas y minúsculas de hasta 32 caracteres.
Paso 4	**Authentication-check** Example: switch(config-router-vrf)# authentication-check	Permite la autenticación de PDUs. El valor por defecto está activado
Paso 5	**Authentication-type** Example: switch(config-router-vrf)# authentication-type	Configura el método de autenticación.
Paso 6	**Authentication key-chain [key]**	Configura el key-chain de autenticación para la PDU.

	Example: switch (config-router-vrf)# authentication key-chain OTVKeys	Puede ser cualquier key-chain, debe ser una cadena alfanumérica entre mayúsculas y minúsculas de hasta 16 caracteres.
Paso 7	**Sh otv isis hostname vpn Overlay1** Example: switch# sh otv isis hostname vpn Overlay1	Muestra la configuración OTV VPN
Paso 8	**copy running-config startup-config** Example: switch# copy running-config startup-config	Copia la configuración en ejecución al arranque de configuración.

Nota: Autenticación OTV PDU para la interfaz Overlay
Fuente: Cisco Systems, Inc

1.5 Herramientas utilizadas

1.5.1 NEXUS-IOS 5

Es un sistema operativo de red creado por Cisco Systems para equipos de la serie Nexus Ethernet Switch's y MDS-series. Se desarrolló desde el sistema operativo Cisco SAN-OS utilizado en equipos desde hace algunos años, originalmente creado para conmutadores MDS pero luego de observar las ventajas que presenta se lo ha incluido en equipos Ethernet. Se basa en software Linux y es interoperable con otros sistemas operativos Cisco.

1.5.2 VMware

Permite crear y ejecutar máquinas virtuales con un total de 4 núcleos de procesamiento, el cual puede constar de 4 procesadores de núcleo único, 2 procesadores de doble núcleo o un procesador quad-core, como son las máquinas que poseen un procesador Intel i7. Permite tener la funcionalidad de las interfaces del equipo al igual que el sistema anfitrión.

Funciona tanto en sistemas operativos de 32 bit y 64 bit, soportando así la mayoría de ediciones de escritorio y servidor de Microsoft Windows, Linux, Solaris, Netware y FreeeBSD como sistemas operativos invitados.

1.5.3 GNS3

GNS3 es un emulador gráfico de redes de código abierto que permite crear de manera virtual routers y switches de CISCO en sistemas operativos como Windows, OS X y Linux, para implementar entornos de redes complejas. Es una herramienta excelente para ser utilizada por Ingenieros en redes, administradores de red y cualquier persona que estudie para las certificaciones de CISCO o Juniper.

Es también utilizado para experimentar con nuevas características y verificar configuraciones de la red que van apareciendo a través de los años, para su posterior despliegue en equipos reales.

Para complementar su funcionalidad GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de CISCO Systems.
- Dynagen, un front-end basado en texto para Dynamips
- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de CISCO o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.

  (Neumann , 2014)

CAPÍTULO 2

ANÁLISIS

2.1 Metodología

La metodología empleada para la elaboración de este trabajo es la "Metodología Científica" que tiene definida los procesos de observación o planteamiento del problema, formulación de hipótesis, experimentación, conclusiones y reporte de resultados técnicos.

Los procesos que se siguen en el desarrollo del trabajo son:

- Recolección de la información.
- Análisis de antecedentes.
- Formulación de hipótesis
- Diseño del modelo físico
- Diseño del modelo lógico
- Formulación de hipótesis
- Configuración del ambiente de estudio virtual correspondiente al nodo 1
- Configuración del ambiente de estudio virtual correspondiente al nodo 2
- Configuración del ambiente de estudio virtual correspondiente al nodo 3
- Configuración del ambiente de estudio virtual correspondiente a la nube MPLS.
- Prueba de la red sin protocolos de transmisión
- Prueba de transmisión con VPN
- Prueba de transmisión con OTV
- Análisis de resultados
- Presentación de resultados

- Establecimiento de conclusiones y recomendaciones

2.2 Problemática.

En la actualidad el uso de las redes se ha constituido para las empresas en la columna vertebral del negocio pues como parte fundamental se encuentra el intercambio de información de manera inmediata, bajo esta necesidad es indispensable mejorar la velocidad a la que se trasmite pero sin descuidar la seguridad que debe tener para evitar que está sea receptada por personas ajenas que puedan utilizar esta información para su beneficio o para perjudicar a la empresa. OTV es una solución que se ha dado a conocer por cisco como un protocolo que permite tener una buena velocidad de transmisión y seguridad.

El protocolo OTV de CISCO es un tema relativamente nuevo en Latinoamérica por lo que no se dispone de información clara en idioma español, algunas de las características y terminologías empleadas por este protocolo dificultan el entendimiento de la funcionalidad que tiene y los beneficios que aporta para el mundo de las redes. Al investigar sobre OTV es notable que la información que existe está en su mayoría disponible en otros idiomas, lo que se constituye en una desventaja para aquellos que buscan información sobre el tema y carecen de un buen nivel de manejo del idioma en el que esta presentada la información.

2.3 Justificación

Al tener la información en otros idiomas e intentar traducirla al español en muchos casos se puede tener una idea tergiversada del contenido pues hay terminologías que pueden tener varios significados al traducirlos, esto hace que se pierda el contexto de la idea original o hace que se vuelva confuso. En este caso la información que se tiene sobre el

tema se encuentra en idioma inglés obtenida directamente desde su fuente CISCO que la ha dado a conocer a través de fichas técnicas.

Bajo este antecedente se propone la implementación de una red piloto sobre un ambiente virtualizado que permita mostrar el funcionamiento y características del protocolo OTV para mejorar la comprensión de los usuarios que desean tener información en idioma español sobre esta solución e implementarla en ambientes empresariales.

OTV como una solución de redes permite emplear la funcionalidad y velocidad de transmisión que ofrece el tráfico etiquetado con la seguridad que ofrece el uso de interfaces virtuales como medio de transporte, este protocolo fue creado pensando en ambientes empresariales donde se necesita crear enlaces virtuales directos que permiten que el trafico viaje a mayores velocidades, esto es posible gracias al etiquetado de tráfico que permite que este fluya a través de los diferentes equipos que conforman la red sin necesidad de que cada equipo realice la verificación de los paquetes. Este protocolo es considerado también como una mejora al protocolo MPLS pues se basa en este con la ventaja de una interface virtual similar a VPN que permite seguridad en la trasmisión, esta combinación evita que se tenga que configurar los servicios mencionados por separado para tener la misma funcionalidad en la red.

2.4 Objetivos

2.4.1 General

Implementar una red piloto que permita mostrar el funcionamiento y características del protocolo OTV utilizando un ambiente virtualizado en GNS3 que emule la interconexión de una red compuesta por tres nodos.

2.4.2 Específicos

- Realizar un estudio de la información difundida actualmente sobre el protocolo OTV para obtener el entendimiento necesario para crear una guía de procesos a seguir en la configuración y tener clara su funcionalidad.
- Crear un ambiente virtual de estudio que emule una red empresarial compuesta por tres nodos y una nube MPLS que se toma como la nube de internet por la cual debe viajar la información.
- Monitorear la red sin la intervención de protocolos de encapsulamiento a través de túneles virtuales para establecer las condiciones iniciales de la red.
- Monitorear la red con la intervención del protocolo VPN de encapsulamiento por túneles virtuales para obtener información de las ventajas que implica el uso de este y establecer datos comparativos para el uso de OTV.
- Monitorear la red con la intervención del protocolo OTV de encapsulamiento por una red superpuesta para obtener información de las ventajas que implica el uso de este y establecer datos que sean comparados con los obtenidos con VPN.
- Analizar los resultados técnicos obtenidos en las diferentes pruebas realizadas para generar un informe que refleje lo obtenido en el desarrollo del estudio.

2.5 Hipótesis

- El uso de interfaces virtuales como VPN y OTV para la transferencia de información incrementa la velocidad de transmisión pues los paquetes son etiquetados de tal forma que los primeros en llegar a su destino marcan el camino a los otros que le siguen y no es necesario que posteriormente sean verificados.

- OTV se considera la mejor solución para el trabajo de una red integrada por diferentes nodos pues combina la eficiencia del tráfico etiquetado y el uso de interfaces virtuales de conexión directa, aprovecha la funcionalidad del agregado de cabeceras en los paquetes para distinguir el tráfico y de este modo evitar que equipos que no sean el destino ocupen tiempo en la comprobación de los paquetes. Establece una red virtual superpuesta conformada por equipos de borde especializados que se enlazan sobre la red principal como un anillo lógico en el cual los equipos se miran directamente sin importar cuantos equipos estén conectados entre ellos.

CAPÍTULO 3

DISEÑO DE LA RED

3.1 Diseño físico

El diseño físico de la red está compuesto por tres equipos portátiles y un equipo de escritorio con las siguientes características:

Equipos portátiles:

- Memoria RAM 8 GB
- Procesador Core I7 cuarta generación.
- Win 7 Professional de 64 bits
- Tarjeta de Red Ethernet 10/100/1000 B-TX
- Capacidad de Virtualización (Vtx)

Equipo de escritorio:

- Memoria RAM de 6 GB
- Procesador Core I7 cuarta generación.
- 3 Tarjetas de Red Ethernet 10/100/1000 B-TX
- Capacidad de Virtualización (Vtx)

En cada uno de los equipos portátiles se utiliza WMware version 11.1.0 para crear 3 máquinas virtuales que corresponden a el equipo Switch Nexus 7000, a un equipo servidor WEB – FTP y a un equipo Cliente. Estos equipos tienen también instalada la herramienta GNS3 con versión 1.3.10 para levantar la virtualización del ambiente de un centro de datos.

En el equipo de escritorio se tiene solo la herramienta GNS3 instalada para levantar la virtualización del ambiente de una nube MPLS que emula la nube de internet a la cual se conectan los tres nodos.

Diseño físico de la Red

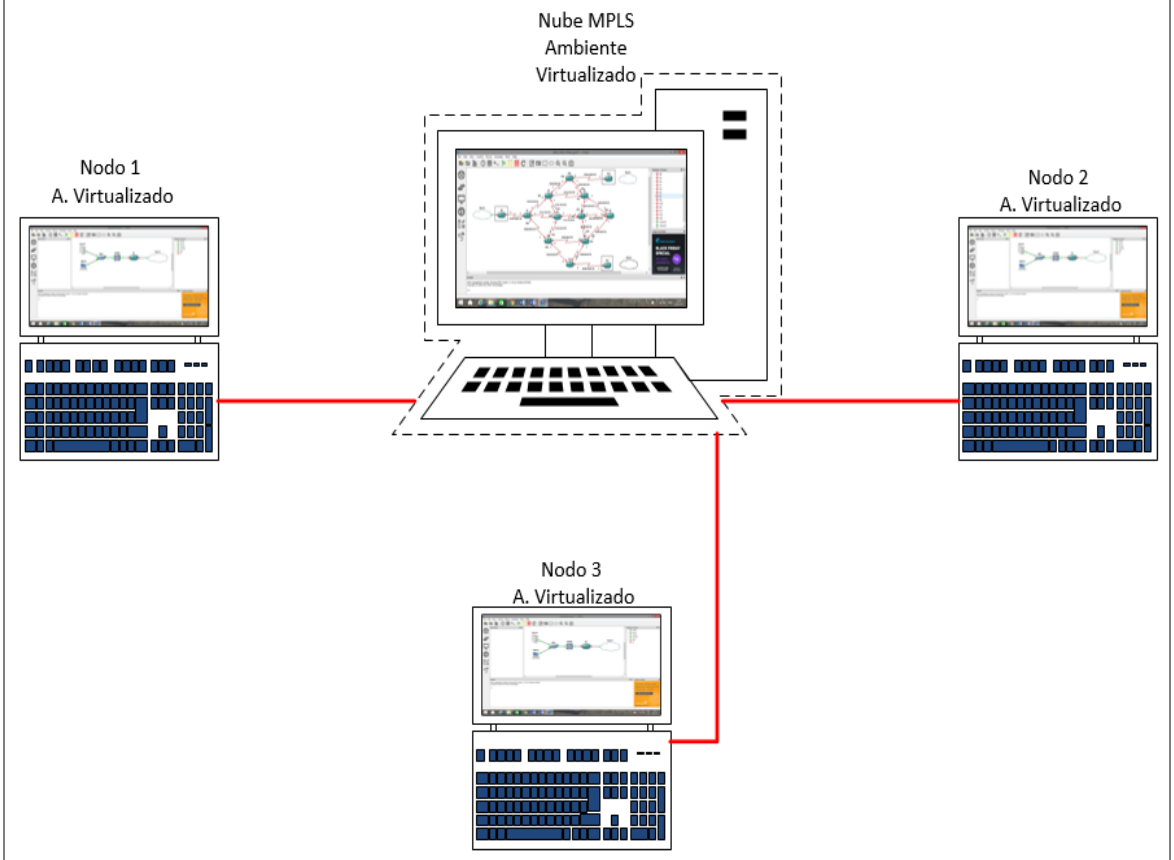


Figura 22. Diseño físico de la Red
Fuente: Wilson Collaguazo y Katherine Ramos

3.2 Diseño lógico

El diseño lógico de la red maneja un esquema de posicionamiento y direccionamiento de los equipos que componen la red, esto permite la administración de las IPS's que se asignan a tal o cual equipo y deja claro su ubicación, con el fin de facilitar el manejo, gestión y mantenimiento que necesite la red para su correcto funcionamiento.

Equipos Utilizados:

- Router C 7200

- Switch Nexus 7000
- Host
- Server

3.2.1 Mapa del diseño lógico de la Red

Diseño lógico de la red

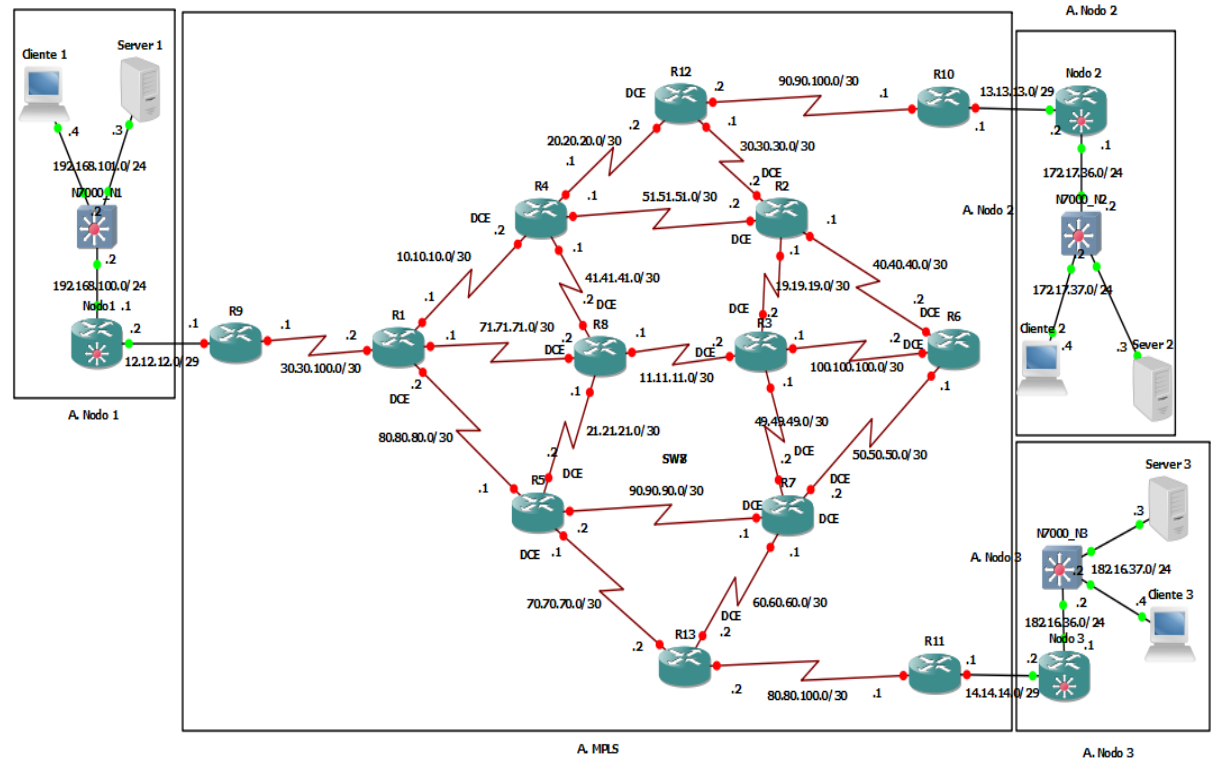


Figura 23. Diseño lógico de la red
Fuente: Wilson Collaguazo y Katherine Ramos

3.2.2 Tablas de direccionamiento

Las tablas de direccionamiento que se muestra a continuación contiene las direcciones IP's que corresponden a cada uno de los equipos que componen la red. Se encuentran también las direcciones de los servidores y host de los nodos en los diferentes equipos.

Tabla 7.

Direccionamiento de la nube MPLS y Router’s ISP

ROUTER	INTERFAZ	IP	MASCARA	RELOJ
R1	S1/0	10.10.10.1	255,255,255,252	
	S1/1	80.80.80.2	255,255,255,252	DCE
	S1/2	71.71.71.1	255,255,255,252	
	S1/3	30.30.100.2	255,255,255,252	
R2	S1/0	19.19.19.1	255,255,255,252	
	S1/1	40.40.40.1	255,255,255,252	
	S1/2	51.51.51.2	255,255,255,252	DCE
	S1/3	30.30.30.2	255,255,255,252	DCE
R3	S1/0	19.19.19.2	255,255,255,252	DCE
	S1/1	49.49.49.1	255,255,255,252	
	S1/2	11.11.11.2	255,255,255,252	DCE
	S1/3	100.100.100.1	255,255,255,252	
R4	S1/0	10.10.10.2	255,255,255,252	DCE
	S1/1	41.41.41.1	255,255,255,252	
	S1/2	51.51.51.1	255,255,255,252	
	S1/3	20.20.20.1	255,255,255,252	
R5	S1/0	21.21.21.2	255,255,255,252	DCE
	S1/1	80.80.80.1	255,255,255,252	
	S1/2	90.90.90.2	255,255,255,252	
	S1/3	70.70.70.1	255,255,255,252	DCE
R6	S1/0	100.100.100.2	255,255,255,252	DCE
	S1/1	40.40.40.2	255,255,255,252	DCE
	S1/2	50.50.50.1	255,255,255,252	
R7	S1/0	50.50.50.2	255,255,255,252	
	S1/1	49.49.49.2	255,255,255,252	DCE
	S1/2	90.90.90.1	255,255,255,252	DCE
	S1/3	60.60.60.1	255,255,255,252	
R8	S1/0	21.21.21.1	255,255,255,252	
	S1/1	41.41.41.2	255,255,255,252	DCE
	S1/2	11.11.11.1	255,255,255,252	
	S1/3	71.71.71.2	255,255,255,252	
R9 (IPS1)	S1/0	30.30.100.1	255,255,255,252	DCE
	F0/0	12.12.12.1	255,255,255,248	
R10 (ISP2)	S1/0	90.90.100.1	255,255,255,252	DCE
	F0/0	13.13.13.1	255,255,255,248	
R11 (ISP3)	S1/0	80.80.100.1	255,255,255,252	DCE
	F0/0	14.14.14.1	255,255,255,248	

R12	S1/0	90.90.100.2	255,255,255,252	
	S1/1	20.20.20.2	255,255,255,252	DCE
	S1/2	30.30.30.1	255,255,255,252	
R13	S1/0	80.80.100.2	255,255,255,252	
	S1/1	60.60.60.2	255,255,255,252	DCE
	S1/2	70.70.70.2	255,255,255,252	

Nota: Asignación de direcciones a la nueve MPLS
Fuente: Wilson Collaguazo y Katherine Ramos

Tabla 8.

Enrutamiento de servidores y host

A. Nodo 1	Nodo1	f0/0	12.12.12.2	255.255.255.248
		f0/1	192.168.100.1	255.255.255.0
	N7000_N1	e2/1	192.168.100.2	255.255.255.0
		e2/2	192.168.101.2	255.255.255.0
	Servidor 1	eth0	192.168.101.3	255.255.255.0
	Cliente 1	eth0	192.168.101.4	255.255.255.0
A. Nodo 2	Nodo2	f0/0	13.13.13.2	255.255.255.248
		f0/1	172.17.36.1	255.255.255.0
	N7000_N2	e2/1	172.17.36.2	255.255.255.0
		e2/2	172.17.37.2	255.255.255.0
	Servidor 2	eth0	172.17.37.3	255.255.255.0
	Cliente 2	eth0	172.17.37.4	255.255.255.0
A. Nodo 3	Nodo3	f0/0	14.14.14.2	255.255.255.248
		f0/1	182.16.36.1	255.255.255.0
	N7000_N3	e2/1	182.16.36.2	255.255.255.0
		e2/2	182.16.37.2	255.255.255.0
	Servidor 3	eth0	182.16.37.3	255.255.255.0
	Cliente 3	eth0	182.16.37.4	255.255.255.0

Nota: Asignación de direcciones a servidores y host
Fuente: Wilson Collaguazo y Katherine Ramos

3.3 Configuración

La configuración de la red se realiza siguiendo los pasos en el orden que se indica, estos procedimientos describen como levantar las áreas virtuales de los nodos en los equipos portátiles y la configuración del equipo de escritorio que contendrá la nube MPLS. También se describe la configuración de los protocolos que aportan prestaciones a la red como son IPv4, OSPF, VPN y OTV.

3.3.1 Ambiente de un Nodo:

Paso 1: Importar a VMware el respaldo de la máquina virtual que contiene el IOS del Switch Nexus 7000.

Importación de la máquina virtual desde WMware

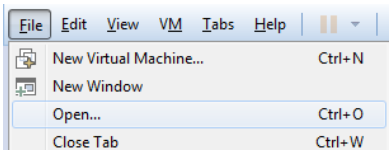


Figura 24. Importación de la máquina virtual desde WMware
Fuente: Wilson Collaguazo y Katherine Ramos

Archivo .vmx contenido en Titanium

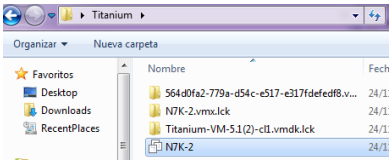


Figura 25. Archivo .vmx contenido en Titanium
Fuente: Wilson Collaguazo y Katherine Ramos

Máquina virtual importada y funcionando

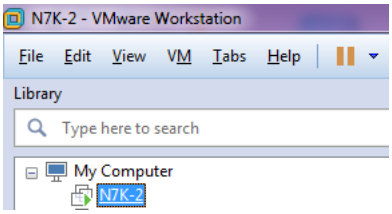


Figura 26. Máquina virtual importada y funcionando
Fuente: Wilson Collaguazo y Katherine Ramos

Paso 2: Configuración de adaptador serial del Switch para tener acceso al plano de configuración por consola. Para esto hay que ingresar a los submenús de la máquina virtual.

Submenú ajustes de la máquina virtual

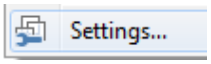


Figura 27. Submenú ajustes de la máquina virtual
Fuente: Wilson Collaguazo y Katherine Ramos

En el submenú ajustes ubicar la opción serial port, en caso que no haya un puerto serial asignado se añade uno como se indica en la sección de anexos. En la ventana de configuración del serial port dejar las opciones como se indica en la Figura 29.

Opción serial ports

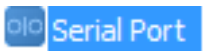


Figura 28. Opción serial ports
Fuente: Wilson Collaguazo y Katherine Ramos

Configuración del adaptador serial

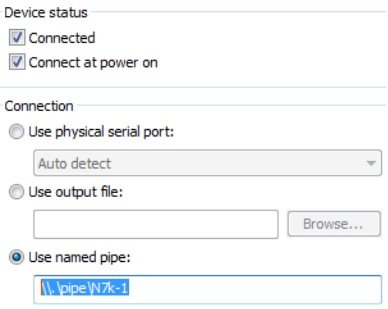


Figura 29. Configuración del adaptador serial
Fuente: Wilson Collaguazo y Katherine Ramos

Paso 3: Crear una máquina virtual para albergar y configurar a los servidores FTP y WEB, utilizando Centos 7 distribución de 64 bit.

Máquina virtual con Centos

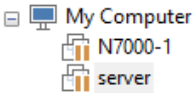


Figura 30. Máquina virtual con Centos
Fuente: Wilson Collaguazo y Katherine Ramos

Con Centos en ejecución lo siguiente es configurar los servidores siguiendo los siguientes pasos en una terminal en modo root:

Servidor FTP

#yum -y install vsftpd // Instalación del paquete de ftp

#systemctl enable vsftpd.service // Habilita el servicio FTP en todos los niveles de ejecución

 # gedit /etc/vsftpd/vsftpd.conf // Acceso al fichero de configuración de vsftpd en donde se edita las siguientes líneas.

anonymous_enable=NO // Deshabilita el ingreso anónimo

ascii_upload_enable=YES // Habilita la carga de archivos al servidor

ascii_download_enable=YES // Habilita la descarga de archivos desde el servidor

use_localtime=YES //Sincroniza el tiempo del servidor al tiempo local

// Cerrar el archivo de configuración con :wq para que se guarde y se cierre

#systemctl restart vsftpd //Reinicia el servicio FTP para que recargue la configuración

#firewall-cmd --permanent --add-service=ftp //Abre el puerto del firewall para que puedan conectarse al servidor FTP

#systemctl restart firewalld.service // Recarga el firewall

#iptables –F //Borrar la regla iptables presentes en el servidor

#iptables –X //Borrar la regla iptables presentes en el servidor

#iptables –Z //Borrar la regla iptables presentes en el servidor

Abrir los puertos 20 y 21 para conexiones pasivas que se haya definido:

#iptables -A INPUT -m state -- NEW -m tcp -p tcp --dport 20 -j ACCEPT

#iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT

#iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 30300:30309 -j ACCEPT

Guardar cambios de los iptables

#service iptables save

Reiniciar el servicio de Iptables con el siguiente comando

 # service iptables restart

Si se quiere subir un archivo, el Selinux podría tirar la conexión alegando que no se tiene los permisos por lo cual para evitar esto se ejecuta el siguiente comando:

#setenforce permissive

Crear usuarios con sus respectivas contraseñas

#useradd adm123

#passwd adm123

Ingresar contraseña nueva:

Ahora queda indicarle a Selinux que permita a los usuarios locales acceder a su home a través del FTP

#setsebool -P ftp_home_dir on

Reiniciar el servicio de FTP

#systemctl restart vsftpd

Comprobar que este levantado el servicio accediendo al navegador e ingresando **ftp://(ip servidor)**. El servidor solicitara el nombre de usuario y contraseña para conectarse y poder acceder a las respectivas carpetas del usuario.

Servidor WEB

#yum -y install httpd // Instalación del paquete de httpd

#systemctl enable httpd // Inicia el servicio

#gedit /var/www/html/index.html // Ingresar al directorio del servidor para crear una página de inicio

La página puede contener un diseño cualquiera para efectos de prueba en este caso se ha utilizado:

```
<HTML>
<HEAD>
<TITLE>UPS</TITLE>
</HEAD>
<BODY>
<marquee><h1>Universidad Politécnica Salesiana </h1></marquee>
<center><h2>Proyecto de Grado</h2>
<h2>Katherine Ramos</h2>
<h2>Wilson Collaguazo</h2></center>
</BODY>
</HTML>
```

Comprobar que este levantado el servicio accediendo al navegador e ingresando **http://(ip servidor)**. El servidor desplegara la página inicial creada.

Paso 4: Crear una máquina virtual cliente, utilizando Ubuntu 14.0 distribución para 64 bits.

Máquina virtual con Ubuntu

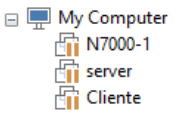


Figura 31. Máquina virtual con Ubuntu
Fuente: Wilson Collaguazo y Katherine Ramos

Paso 5: Configurar y asignar adaptadores genéricos a las máquinas virtuales para tener conexión entre ellas. En este punto es muy importante tener en cuenta como se asignan

los adaptadores pues no solo dan la conectividad entre máquinas virtuales sino que también dan salida a las conexiones con los equipos físicos.

Entrar en la pestaña Edit - Opción Virtual Network Editor y Agregar 2 nuevas interfaces de red genéricas como se muestra en las Figura 28, en este caso los adaptadores genéricos creados son VMnet 11 y VMnet 12 las otras se agregan por defecto al instalar VMware. Reiniciar la máquina física para que las nuevas interfaces sean reconocidas conjuntamente con las otras en el arranque del sistema.

Ajustes de adaptadores virtuales

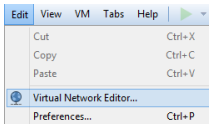


Figura 32. Ajustes de adaptadores virtuales
Fuente: Wilson Collaguazo y Katherine Ramos

Añadido de interfaces genéricas

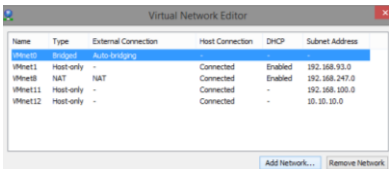


Figura 33. Añadido de interfaces genéricas
Fuente: Wilson Collaguazo y Katherine Ramos

Con las interfaces genéricas reconocidas por el Sistema lo siguientes es asignarles una IP que este dentro del rango de direcciones a la red que pertenecen. En el caso del adaptador que conecta a las máquinas virtuales tanto del servidor como el cliente la IP que le corresponde es una dentro de la red de Lan Local, mientras que la IP que le corresponde al adaptador que conecte al Switch con el Router es una que este dentro del rango de la red de zona restringida.

Lista de Adaptadores en la maquina física

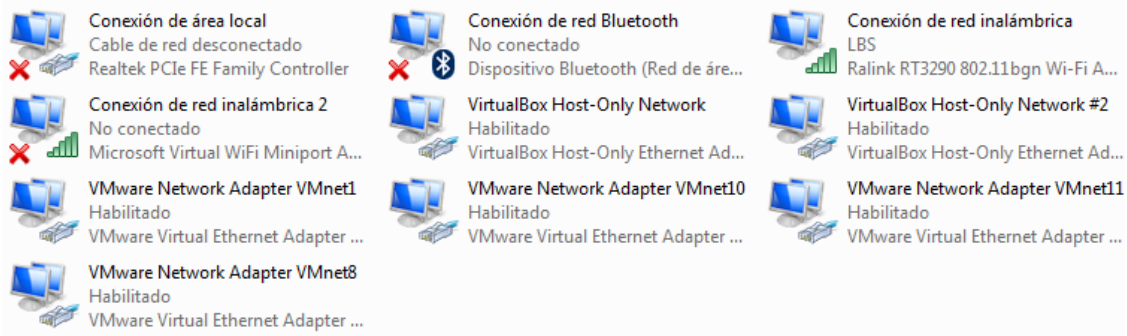


Figura 34. Lista de Adaptadores en la maquina física
Fuente: Wilson Collaguazo y Katherine Ramos

Asignación de IP Lan Local

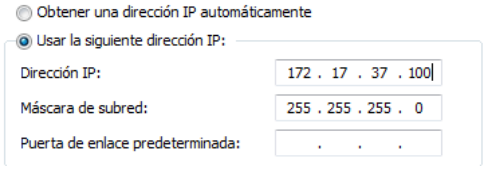


Figura 35. Asignación de IP Lan Local
Fuente: Wilson Collaguazo y Katherine Ramos

Asignación de IP área restringida

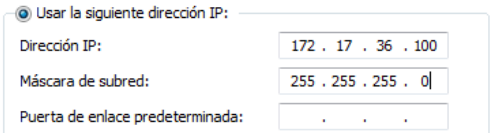


Figura 36. Asignación de IP área restringida
Fuente: Wilson Collaguazo y Katherine Ramos

Con los adaptadores de red añadidos y configurados lo siguiente es asignar los adaptadores a las máquinas virtuales y configurar las IP de las interfaces tanto en el Switch como en las máquinas de servidor y cliente de acuerdo a la Tabla 8.

La configuración empieza en el Switch ingresando a consola con la herramienta Putty que se conecta al Puerto series que se ha configurado previamente. En consola lo siguientes es ingresar los siguientes comandos:

N7K-2# sh interface brief //Permite conocer el detalle de las interfaces que tiene el equipo, se ejecuta fuera del área de configuración o anteponiendo do.
N7K-2# conf ter //Permite ingresar en el área de configuración global del equipo

N7K-2(config)# int e2/1 //Permite ingresar en el área de configuración de la interface
N7K-2(config-if)# ip address 172.17.36.2 255.255.255.0 //Asigna la dirección que le corresponde a la interface.
N7K-2(config-if)# no shutdown //Enciende la interface y levanta el protocolo.
N7K-2(config-if)# exit //Permite salir al área de configuración global
N7K-2(config)# int e2/2 //Permite ingresar en el área de configuración de la interface
N7K-2(config-if)# ip address 172.17.37.2 255.255.255.0 //Asigna la dirección que le corresponde a la
N7K-2(config-if)# no shutdown //Enciende la interface y levanta el protocolo.
N7K-2(config-if)# exit //Permite salir al área de configuración global
N7K-2(config)# exit //Permite salir al menú de raíz

Verificar el estado de los enlaces y que los protocolos se hayan levantado, en caso que no se hayan levantado los enlaces desconectar y reconectar los adaptadores de las máquinas virtuales.

N7K-2# sh ip interface brief //Permite conocer el detalle de las interfaces que tiene el equipo y las IP's asignadas, se ejecuta fuera del área de configuración o anteponiendo do.

Comando sh ip interface brief

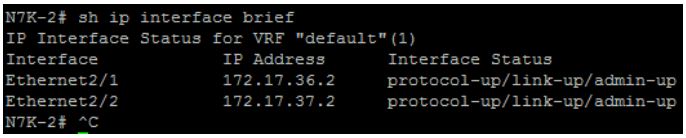


Figura 37. Resultado del comando sh ip interface brief
Fuente: Wilson Collaguazo y Katherine Ramos

El siguiente paso es configurar las IP's en el servidor y en el cliente de acuerdo a la Tabla 8 de direccionamiento.

Asignación de IP al servidor

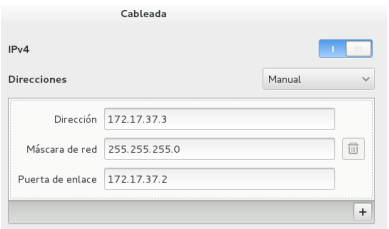


Figura 38. Asignación de IP al servidor
Fuente: Wilson Collaguazo y Katherine Ramos

Asignación de IP al cliente

Figura 39. Asignación de IP al cliente
Fuente: Wilson Collaguazo y Katherine Ramos

Con las interfaces genéricas configuradas accedemos a WMware y asignamos los adaptadores a las máquinas virtuales, esto lo realizamos ingresando a ajustes de cada una de las máquinas en la opción de adaptadores. En el caso de la máquina que corresponde al Switch Nexus 7000 se asignan los dos adaptadores genéricos, mientras que a las máquinas tanto de servidor como de cliente se asigna solo el adaptador correspondiente al puente entre máquinas.

Asignación de adaptadores genéricos

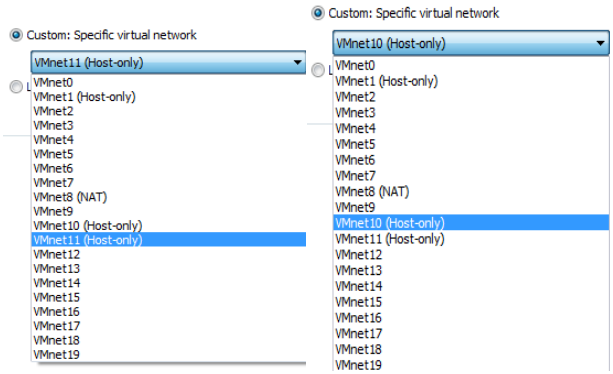


Figura 40. Asignación de adaptadores genéricos
Fuente: Wilson Collaguazo y Katherine Ramos

Una vez que los adaptadores han sido asignados es necesario probar la conectividad entre las máquinas virtuales y los adaptadores genéricos utilizar ping entre interfaces con el fin de comprobar su estado. En caso de algún problema revisar la sección de anexos para mayor información.

Ping de prueba para verificación de adaptadores

```
[server@localhost ~]$ ping 172.17.37.2
PING 172.17.37.2 (172.17.37.2) 56(84) bytes of data.
64 bytes from 172.17.37.2: icmp_seq=1 ttl=255 time=0.856 ms
64 bytes from 172.17.37.2: icmp_seq=2 ttl=255 time=1.64 ms
64 bytes from 172.17.37.2: icmp_seq=3 ttl=255 time=1.57 ms
64 bytes from 172.17.37.2: icmp_seq=4 ttl=255 time=1.51 ms
64 bytes from 172.17.37.2: icmp_seq=5 ttl=255 time=1.58 ms
64 bytes from 172.17.37.2: icmp_seq=6 ttl=255 time=1.60 ms
64 bytes from 172.17.37.2: icmp_seq=7 ttl=255 time=1.02 ms
64 bytes from 172.17.37.2: icmp_seq=8 ttl=255 time=1.53 ms
64 bytes from 172.17.37.2: icmp_seq=9 ttl=255 time=1.73 ms
64 bytes from 172.17.37.2: icmp_seq=10 ttl=255 time=1.02 ms
64 bytes from 172.17.37.2: icmp_seq=11 ttl=255 time=1.54 ms
64 bytes from 172.17.37.2: icmp_seq=12 ttl=255 time=1.85 ms
64 bytes from 172.17.37.2: icmp_seq=13 ttl=255 time=1.48 ms
64 bytes from 172.17.37.2: icmp_seq=14 ttl=255 time=1.01 ms
64 bytes from 172.17.37.2: icmp_seq=15 ttl=255 time=1.59 ms
^C
--- 172.17.37.2 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14053ms
rtt min/avg/max/mdev = 0.856/1.438/1.853/0.293 ms
[server@localhost ~]$
```

Figura 41. Ping de prueba para verificación de adaptadores
Fuente: Wilson Collaguazo y Katherine Ramos

Paso 6: Ultimo paso del levantamiento del nodo es armar la topología en el emulador GNS3 para esto se tomara en cuenta el diseño lógico.

Empezar por ingresar a GNS3 para configurar la red que comprende el área virtual del nodo. Para la arquitectura se emplea 4 nubes que permiten las conexión con los adaptadores de red que dan acceso a las máquinas virtuales, un Router que servirá como Gateway y un Switch Ethernet que permite la conexión de los equipos servidor y cliente con el equipo Nexus 7000.

Topología del nodo en GNS3

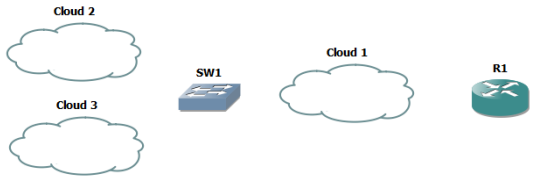


Figura 42. Topología del nodo en GNS3
Fuente: Wilson Collaguazo y Katherine Ramos

Para que se pueda utilizar el Router es necesario cargar la imagen del IOS del Router c7200, esto se lo realiza desde la pestaña Edit opción Preferences – IOS Router – New –

Seleccionar imagen. En la importación del IOS hay que tomar en cuenta las interfaces del Router que se necesita asignar para las conexiones.

Carga del IOS del Router

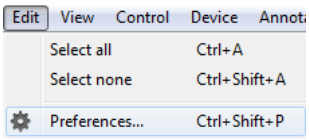


Figura 43. Carga del IOS del Router
Fuente: Wilson Collaguazo y Katherine Ramos

Ventana de configuración del Router

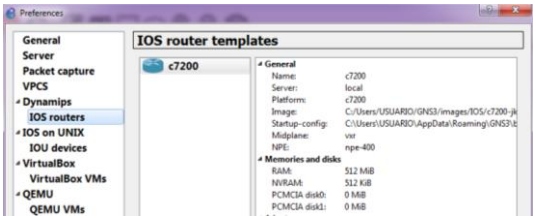


Figura 44. Ventana de configuración del Router
Fuente: Wilson Collaguazo y Katherine Ramos

Una vez la topología armada asignar los adaptadores de las nubes para establecer los enlaces. Para las nubes que conectan al servidor y al cliente utilizar el mismo adaptador genérico que se asignó en las máquinas virtuales, mientras que para la que corresponde al switch asignar los dos adaptadores genéricos.

Asignación de adaptador a la nube

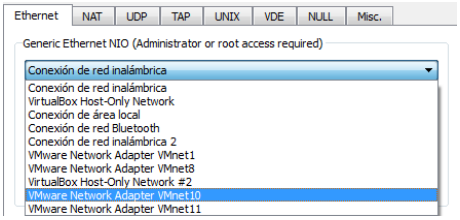


Figura 45. Asignación de adaptador a la nube
Fuente: Wilson Collaguazo y Katherine Ramos

Topología con enlaces establecidos.

Figura 46. Topología con enlaces establecidos.
Fuente: Wilson Collaguazo y Katherine Ramos

Establecidos los enlaces hay que configurar el Router que corresponde al Gateway del nodo para ello es necesario configurar el Router por consola, para ello se ejecuta la simulación y dar doble clic en el Router, así se abrirá la consola que permitirá el acceso a la línea de comandos.

```
Router#sh ip interface brief //Permite visualizar la IP y estado de las interface
Router#conf ter //Ingreso al área de configuración global
Router(config)#int f0/0 //Ingreso al modo de configuración de la interface
Router(config-if)#ip address 172.17.36.1 255.255.255.0 //Asignación de
dirección a la interface
Router(config-if)#no shutdown //Enciende la interface
Router(config-if)#exit //Sale del modo de configuración de la interface
Router(config)#int f0/1 //Ingreso al modo de configuración de la interface
Router(config-if)#ip address 13.13.13.2 255.255.255.248 //Asignación de
dirección a la interface
Router(config-if)#no shutdown //Asignación de dirección a la interface
Router(config-if)#exit //Sale del modo de configuración de la interface
Router(config)# end //Sale al menú de raíz
```

Verificar el estado de los enlaces y que los protocolos se hayan levantado.

```
Router#sh ip interface brief //Permite visualizar la configuración de las interfaces
```

Configurada la topología en GNS3 se realiza pruebas a los enlaces entre máquinas virtuales y GNS3 utilizando ping para verificar su estado.

Nota: Para la configuración de las otras dos áreas de los nodos repetir los pasos que se han realizado en la configuración hasta ahora.

3.3.2 Implementación de la nube MPLS

El siguiente paso en la configuración de la red es levantar la nube MPLS en GNS3, para ello lo primero es añadir la imagen del IOS de los Router que se utilizan, en este caso se emplea el IOS de un Router C7200 que permite la configuración del servicio MPLS, Hay que tomar en cuenta que no todos los IOS permiten el servicio. Lo siguiente es asignar IP's a los Router's y posicionarlos de acuerdo al direccionamiento de la Tabla 1 y al diseño lógico.

Diseño de la nube MPLS

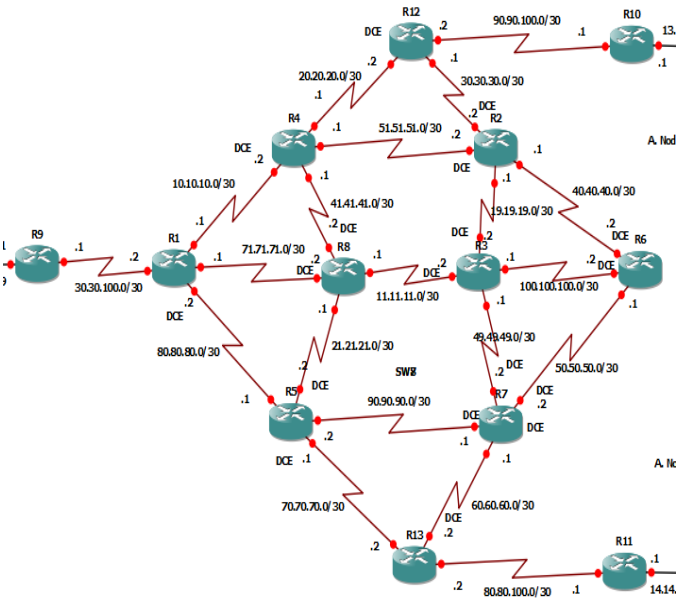


Figura 47. Diseño de la nube MPLS
Fuente: Wilson Collaguazo y Katherine Ramos

Ejemplo:

R1
R1#conf ter //Ingreso a terminal de configuración del Router
R1(config)#int s1/0 //Ingreso a interface serial 1/0
R1(config-if)#ip add 10.10.10.1 255.255.255.252 // Asignación de dirección.
R1(config-if)#no shut //Encendido de la interface
R1(config-if)#exit
R1(config)#int s1/1 //Ingreso a la interface serial 1/0
R1(config-if)#ip add 80.80.80.2 255.255.255.252 // Asignación de dirección.
R1(config-if)#clock rate 64000 //Velocidad del reloj de sincronización

```
R1(config-if)#no shut //Encendido de la interface
R1(config)#int s1/2
R1(config-if)#ip add 71.71.71.1 255.255.255.252
R1(config-if)#no shut
R1(config)#int s1/3
R1(config-if)#ip add 30.30.100.2 255.255.255.252
R1(config-if)#no shut
```

Nota: El mismo procedimiento se lo repite en cada uno de los otros Router's de acuerdo a la tabla de direccionamiento.

Configurar OSPF como protocolo de enrutamiento.

Ejemplo:

```
R1#conf t
R1(config)#router ospf 1 //Agregado de tabla de Ruteo OSPF 1
R1(config-router)#net 110.10.10.0  0.0.0.3 area 0  //Red con conexión directa
R1(config-router)#net 10.10.10.0  0.0.0.3 area 0 //Red con conexión directa
R1(config-router)#net 80.80.80.0  0.0.0.3 area 0 //Red con conexión directa
R1(config-router)#net 71.71.71.0  0.0.0.3 area 0 //Red con conexión directa
R1(config-router)#net 30.30.100.0  0.0.0.3 area 0 //Red con conexión directa
```

Configurar MPLS en la red.

Ejemplo:

```
R1
R1#conf t
R1(config)#int s1/0 //Ingreso a la interface
R1(config-if)#mpls ip //Levantamiento del servicio MPLS
R1(config-if)#int s1/1 //Ingreso a la interface
R1(config-if)#mpls ip //Levantamiento del servicio MPLS
R1(config-if)#int s1/2 //Ingreso a la interface
R1(config-if)#mpls ip //Levantamiento del servicio MPLS
R1(config-if)#int s1/3 //Ingreso a la interface
R1(config-if)#mpls ip //Levantamiento del servicio MPLS
```

La revisión de la configuración de MPLS se la realiza con los siguientes comandos:

```
R# show mpls interfaces // Permite ver que interfaces usan MPLS y su estado
R# show mpls ldp discovery // Permite obtener información de LDP local y de los vecinos
R# show mpls ldp neighbor // Permite ver las adyacencias LDP y conocer su estado
```

R# show mpls ldp bindings // Permite ver la tabla LIB
R# show mpls forwarding-table // Permite ver la tabla LFIB

Comando show mpls interfaces

```
R1#show mpls interfaces
Interface              IP           Tunnel   Operational
Serial1/0              Yes (ldp)    No       Yes
Serial1/1              Yes (ldp)    No       Yes
Serial1/2              Yes (ldp)    No       Yes
Serial1/3              Yes (ldp)    No       Yes
R1#
```

Figura 48. Comando show mpls interfaces
Fuente: Wilson Collaguazo y Katherine Ramos

Comando show mpls ldp discovery

```
R1#sh mpls ldp discovery
 Local LDP Identifier:
    110.10.10.1:0
    Discovery Sources:
    Interfaces:
        Serial1/0 (ldp): xmit/recv
            LDP Id: 113.10.10.1:0
        Serial1/1 (ldp): xmit/recv
            LDP Id: 114.10.10.1:0
        Serial1/2 (ldp): xmit/recv
            LDP Id: 117.10.10.1:0
        Serial1/3 (ldp): xmit/recv
            LDP Id: 120.10.10.1:0
```

Figura 49. Comando show mpls ldp discovery
Fuente: Wilson Collaguazo y Katherine Ramos

Con todos los Router's configurados y con los enlaces en funcionamiento hay que realizar las pruebas de conexión con el comando ping entre equipos. Con la red configurada y una vez que se ha realizado las pruebas de conexión necesarias proceder con los enlaces físicos entres equipos de acuerdo al diseño físico descrito.

Una vez que todos los enlaces han sido probados es necesario sacar respaldos de todo para duplicar la red y proceder con los próximos pasos, para las pruebas que se van a realizar se necesita tener dos redes con topologías similares pues en la una se configura VPN's entre los equipos de Gateway, mientras que en la otra red se configura OTV en los Switch de borde.

3.3.3 Implementación de túneles VPN's

La configuración de los túneles VPN's se realiza entre los Router's de Gateway de cada nodo para reducir el tiempo que los paquetes necesitan para llegar de una Lan a otra. Al utilizar túneles el tráfico se etiqueta y no necesita ser verificado en cada uno delos Router's que conforman la red.

La configuración de los Router's se la realiza de acuerdo al siguiente ejemplo:

Ejemplo:

R1(config)#crypto isakmp enable // Permite habilitar las políticas IKE para seguridad.
R1(config)#crypto isakmp policy 1 // Establece la configuración de las políticas IKE de prioridad 1, al crear una nueva política IKE es necesario identificar cada una con un prioridad definida de 1 a 10000, donde 1 es la prioridad más alta del rango, lo que define que esta política será gestionada de primero.
R1(config-isakmp)#authentication pre-share // Establece el modo de autenticación con clave precompartida.
R1(config-isakmp)#hash md5 // Establece md5 o message digest 5 como algoritmo de hash para garantizar la integridad de los paquetes, MD5 genera una salida de 128 bits a diferencia de SHA que lo hace con 160 bits, convirtiendo a MD5 en el más eficaz
R1(config-isakmp)#group 1 // Especifica el método de intercambio de claves con el identificador de grupo de Diffie-Hellman en la política IKE, las opciones son: 1 para un identificador de grupo de 768 bits, 2 para un identificador de 1024 bits y 5 para un identificador de 1536 bits (ciscoipv6ttechtips, 2011), los grupos 2 y 5 ofrecen una seguridad más efectiva pero su rendimiento es pobre, en este caso se escogido el grupo 1 por el rendimiento que ofrece dentro del túnel IPSec (Watch Guard System Manager Help, 2010).
R1(config-isakmp)#encryption 3des // Especifica 3DES como algoritmo de cifrado
R1(config-isakmp)#lifetime 86400 // Especifica el tiempo de vida en segundos para la SA
R1(config-isakmp)#exi //
R1(config)#crypto isakmp key 0 cisco address 13.13.13.2 255.255.255.248 // Define la clave precompartida, en texto plano, "0", y la IP del que será el extremo remoto del túnel en formato IPv4
R1(config)#crypto keyring ANILLO // Define el nombre del keyring que se usará durante la autenticación
R1(conf-keyring)#pre-shared-key address 13.13.13.2 255.255.255.248 key proyecto //Define la clave precompartida a usar durante la autenticación IKE
R1(conf-keyring)#exit

R1(config)#crypto ipsec transform-set TRANSFORMADA esp-3des // Define un transformset, que es una combinación de protocolos y algoritmos que sean aceptables por routers IPSec
R1(cfg-crypto-trans)#crypto ipsec profile PERFIL // Define los parámetros que se van a usar para el cifrado IPSec entre los Router's
R1(ipsec-profile)#set transform-set TRANSFORMADA // Especifica transform-set a utilizar
R1(ipsec-profile)#exit
R1(config)#int tunnel 1 // Configura un nueva interfaz virtual llamada túnel 1
R1(config-if)#ip add 14.10.10.1 255.255.255.248
R1(config-if)#tunnel source f0/1 // Especifica la interface origen del túnel
R1(config-if)#tunnel destination 13.13.13.2// Especifica la interface destino del túnel 1
R1(config-if)#tunnel mode ipsec ipv4 // Establece el modo de encapsulamiento para la
interfaz tunnel 0
R1(config-if)#tunnel protection ipsec profile PERFIL // Asocia la interfaz túnel 0 con el perfil
R1(config-if)#exit
R1(config)#ip route 172.17.37.0 255.255.255.0 tunnel 1 // Agrega la ruta estática desde la hacia la LAN destino.
R1(config)#do wr // Guarda una copia del fichero de configuración global

Las configuraciones se pueden visualizar utilizando los siguientes comandos:

R1(config)#show Crypto isakmp sa // Muestra el origen, el fin del túnel y estado.
R1(config)#show Crypto ipsec sa // Muestra como resultado las direcciones de las interfaces de entrada y salida de los paquetes encriptados, indica el número de paquetes encriptados y desencriptados, el número de errores durante la encriptación, el túnel virtual que está usando esa ruta, el identificador de la cabecera ESP y de la SA, el identificador del crypto-map, el algoritmo de cifrado así como el tiempo de vida de la clave de encriptación.

Comando show Crypto isakmp sa

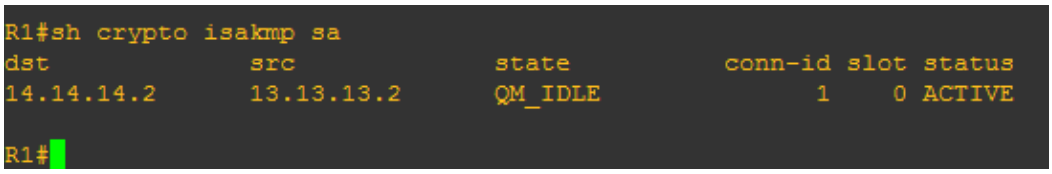


Figura 50. Comando show Crypto isakmp sa
Fuente: Wilson Collaguazo y Katherine Ramos

Comando show Crypto ipsec sa

```
R1#sh crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 13.13.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 12.12.12.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 694, #pkts encrypt: 694, #pkts digest: 694
    #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 13.13.13.2, remote crypto endpt.: 12.12.12.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x8B1DE501(2333992193)
```

Figura 51. Comando show Crypto ipsec sa
Fuente: Wilson Collaguazo y Katherine Ramos

3.3.4 Implementación de OTV

Activación de la función de OTV
N7K-2(config)# feature otv // Permite activar el protocolo OTV
N7K-2(config)# sh feature | include otv // Muestra el estado de activación / desactivación para las características de OTV

Comando sh feature | include otv

```
N7K-1# sh feature | include otv
otv                   1         enabled
N7K-1#
```

Figura 52. Comando sh feature | include otv
Fuente: Wilson Collaguazo y Katherine Ramos

Creación de una interfaz superpuesta
N7K-2(config)# int overlay 1 //Crea una interfaz superpuesta de OTV y entra en el modo de configuración de interfaz. El rango es de 0 a 65535
N7K-2(config-if-overlay)# description NODO_2 //Configura una descripción de la red superpuesta, se puede utilizar una cadena alfanumérica entre mayúsculas y minúsculas de hasta 80 caracteres.
N7K-2(config-if-overlay)# sh otv overlay 1 //Muestra la configuración de la interfaz superpuesta de OTV.

Comando sh otv overlay 1

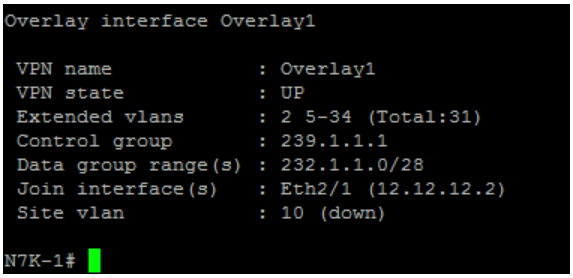


Figura 53. Comando sh otv overlay 1
Fuente: Wilson Collaguazo y Katherine Ramos

Configuración de la dirección de grupo multicast

N7K-2(config-if-overlay)# otv control-group 239.1.1.1 //Permite configurar la dirección del grupo multicast utilizada por el plano de control OTV para esta red superpuesta OTV. La dirección de grupo multicast es una dirección IPv4 en notación decimal con puntos.
N7K-2(config-if-overlay)# otv data-group 232.1.1.0/28 //Configura uno o más rangos de prefijos de grupos locales IPv4 multicast utilizados para el tráfico de datos multicast. Utilizar SSM grupos multicast 232.0.0.0/8. Se pueden definir hasta ocho rangos de grupo.
N7K-2(config-if-overlay)# show otv data-group //Muestra los grupos multicast anunciados
N7K-2(config-if-overlay)# exit //Salir de la interfaz superpuesta

Asignación de una interfaz física a la interfaz superpuesta

N7K-2(config)# int e2/1 //Interfaz física
N7K-2(config-if)# ip igmp version 3 /Activar igmp versión 3 para unir con las demás interfaces
N7K-2(config-if)#exit //salir de la interfaz física
N7K-2(config)# int overlay 1 //Ingresar a la interfaz superpuesta creada
N7K-2(config-if-overlay)# otv join-interface ethernet 2/1 //Se une la interfaz superpuesta de OTV con una interfaz física de nivel 3. Debe configurar una dirección IP en la interfaz física.

Asignación de VLAN de rango extendido

N7K-2(config-if-overlay)# otv extend-vlan 2,5-34 //Extiende un rango de VLAN a través de la interfaz superpuesta y permite anuncios OTV para estas VLAN. El alcance de VLAN es de 1 a 3967, y 4048-4093.
N7K-2(config-if-overlay)# exit //Salir de la interfaz superpuesta

Configuración de la VLAN de Sitio e identificador de sitio

N7K-2(config)# otv site-vlan 10 //Configura una VLAN a la cual todos los dispositivos de borde locales se comunican. Se recomienda que se utilice el mismo ID de VLAN en todos los sitios. El rango es de 1 hasta 3967, y desde 4048 a 4093. El valor predeterminado es 1.
N7K-2(config-site-vlan)# exit //Salir del sitio de VLAN
N7K-2(config)# otv site-identifier 256 //Configura el identificador de sitio. Se debe configurar el mismo identificador de sitio en todos los dispositivos de borde OTV locales.
N7K-2(config)# sh otv site //Muestra la información de sitio de OTV

Configuración de autenticación de OTV PDU

N7K-2(config)# otv-isis default // Entra en el modo de configuración del router OTV.
N7K-2(config-router)# vpn Overlay1 // Entra en el modo de configuración OTV de red privada virtual (VPN). El nombre de superposición puede ser cualquiera, puede ser una cadena alfanumérica entre mayúsculas y minúsculas de hasta 32 caracteres.
N7K-2(config-router-vrf)# authentication-check // Permite la autenticación de PDUs. El valor por defecto está activado.
N7K-2(config-router-vrf)# authentication-type md5 // Configura el método de autenticación.
N7K-2(config-router-vrf)# authentication key-chain OTVKeys // Configura el key-chain de autenticación para la autenticación PDU. El nombre puede ser cualquier key-chain, puede ser una cadena alfanumérica entre mayúsculas y minúsculas de hasta 16 caracteres
N7K-2(config-router-vrf)# sh otv isis hostname vpn Overlay1 // Muestra la configuración OTV VPN.

Comando sh otv isis hostname vpn Overlay

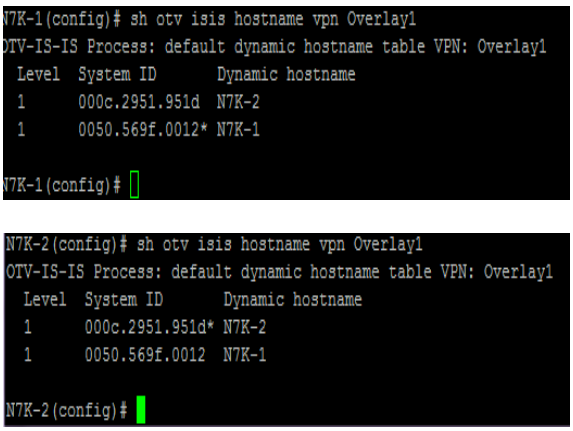


Figura 54. Comando sh otv isis hostname vpn Overlay
Fuente: Wilson Collaguazo y Katherine Ramos

Ejemplo de configuración de un equipo de borde con OTV

```
vrf context management
  ip route 0.0.0.0/0 192.168.1.1
otv site-vlan 10
key chain OTVKeys
  key 1
    key-string 7 070c285f4d06

interface Overlay1
  otv isis authentication-type md5
  otv isis authentication key-chain OTVKeys
  otv join-interface Ethernet2/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  no shutdown

interface Ethernet2/1
  ip address 12.12.12.2/29
  ip igmp version 3
  no shutdown

interface Ethernet2/2
  ip address 192.168.101.1/24
  no shutdown
interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet2/9

interface mgmt0
  vrf member management
  ip address 192.168.1.101/24
line console
line vty
boot kickstart bootflash:/titanium-d1-kickstart.5.1.2.gbin
boot system bootflash:/titanium-d1.5.1.2.gbin
router ospf 1
  network 12.12.12.0/29 area 0.0.0.0
  network 192.168.101.0/24 area 0.0.0.0
otv-isis default
  vpn Overlay1
    authentication-type md5
    authentication key-chain OTVKeys
```

Figura 55. Ejemplo de configuración de un Nexus 7000
Fuente: Wilson Collaguazo y Katherine Ramos

Comprobación de configuración de OTV

N7K-1# show otv adjacency // Muestra las adyacencias creadas y enlazadas a la red sobrepuesta

Comando sh otv isis hostname vpn Overlay

```
Overlay-Interface Overlay1  :
Hostname                       System-ID      Dest Addr       Up Time   State
N7K-1                          000c.2999.80fb 12.12.12.2      00:25:43  UP
N7K-2                          000c.2914.666a 14.14.14.2      00:00:21  UP
N7K-3#
```

Figura 56. Comando show otv adjacency
Fuente: Wilson Collaguazo y Katherine Ramos

N7K-1# show otv site // Muestra las adyacencias creadas y enlazadas a la red sobrepuesta

Comando show otv site

```
N7K-1# sh otv site

Site Adjacency Information (Site-VLAN: 10) (* - this device)

Overlay1 Site-Local Adjacencies (Count: 1)

  Hostname                       System-ID      Up Time   Ordinal
  ------------------------------ -------------- --------- ----------
* N7K-1                          000c.2999.80fb 00:47:15  0

N7K-1#
```

Figura 57. Comando show otv site
Fuente: Wilson Collaguazo y Katherine Ramos

CAPÍTULO 4

PRUEBAS Y RESULTADOS

4.1 Pruebas de ruta

Las primeras pruebas en ser ejecutadas son las rutas que deben seguir los paquetes cuando se crea una solicitud desde un cliente a un servidor en la red local y las rutas a seguir hacia un servidor en una red remota, esto permitirá evidenciar las diferencias entre una ruta con direccionamiento dinámico, una ruta que emplea túneles VPN y una ruta que tiene una red sobrepuesta entre equipos de borde creada por la solución OTV.

Ruta hacia el servidor local sin VPN

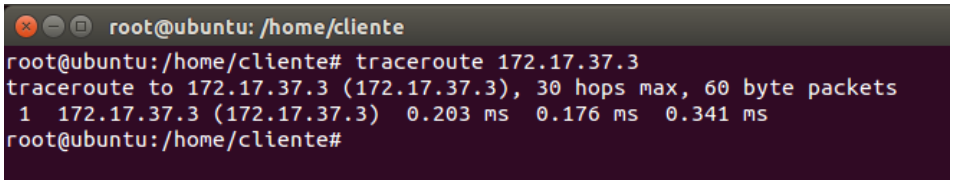


Figura 58. Ruta hacia el servidor local sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada está compuesta por el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 172.17.37.3, esta solicitud es procesada únicamente por el Gateway del sitio.

Ruta hacia el servidor remoto sin VPN

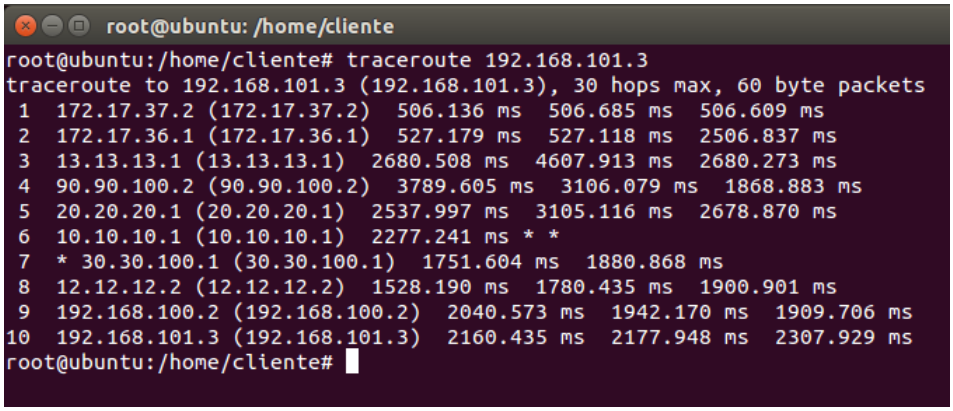


Figura 59. Ruta hacia el servidor remoto sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada está compuesta por el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 192.168.101.3, esta solicitud es procesada por el Gateway del sitio y enviada al siguiente salto hasta alcanzar su destino. Los paquetes deben atravesar por ocho equipos antes de llegar a la ubicación del servidor.

Ruta hacia el servidor local con VPN

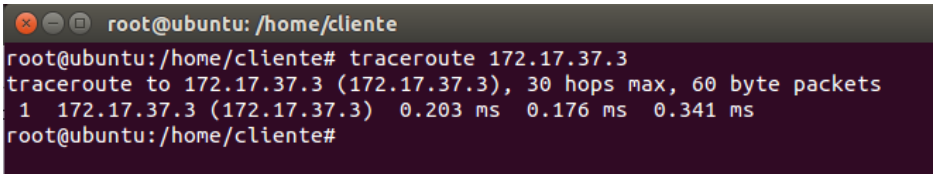


Figura 60. Ruta hacia el servidor local con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada está compuesta por el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 172.17.37.3, esta solicitud es procesada únicamente por el Gateway del sitio al igual que al utilizar el enrutamiento dinámico.

Ruta hacia el servidor remoto con VPN

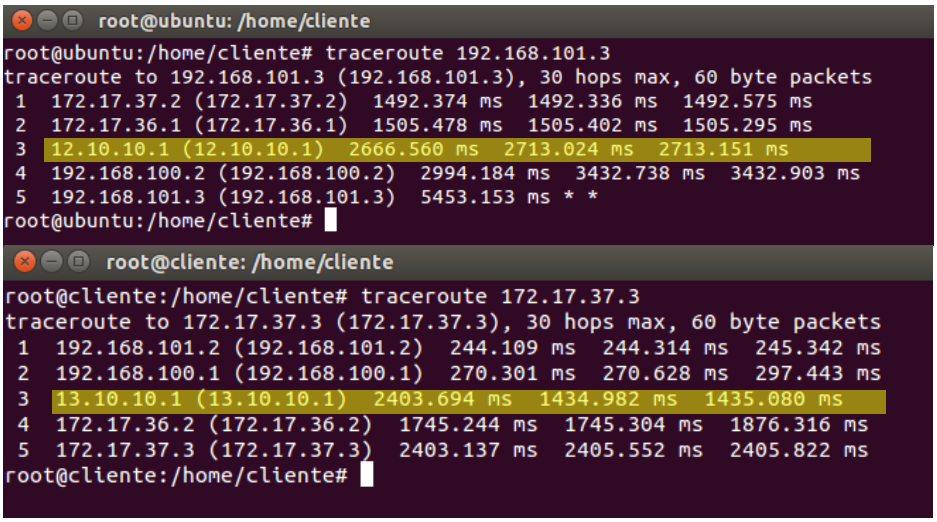


Figura 61. Ruta hacia el servidor remoto con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada está compuesta por el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 192.168.101.3, esta solicitud es procesada por el

Gateway del sitio y enviada a través del túnel VPN compuesto por los extremos 12.10.10.1 y 13.10.10.1 para posteriormente llegar a su destino.

Ruta hacia el servidor local con OTV

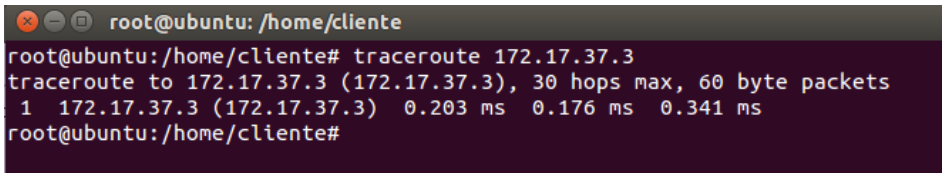


Figura 62. Ruta hacia el servidor local con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada hacia el servidor local está compuesta desde el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 172.17.37.3, esta solicitud es procesada únicamente por el Gateway del sitio al igual que al utilizar el enrutamiento dinámico y túneles VPN.

Ruta hacia el servidor remoto con OTV

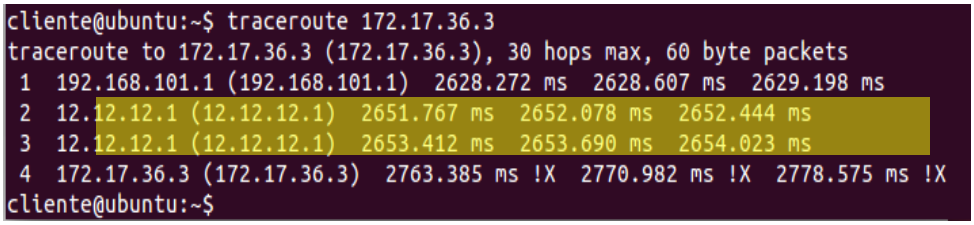


Figura 63. Ruta hacia el servidor remoto con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

La ruta trazada está compuesta por el cliente que realiza la solicitud desde la dirección 172.17.37.4 al servidor con dirección 192.168.101.3, esta solicitud es procesada por el Gateway del sitio y enviada a través de la interface de adyacencia 12.12.12.1 que da acceso a la red sobrepuesta para posteriormente llegar a su destino.

Resultados:

- En las pruebas de ruta realizadas se ha establecido como resultado que en la ruta creada por ruteo dinámico hacia el servidor local sin VPN el número de saltos es

igual que si se utiliza tanto VPN como OTV pues al compartir el mismo Router los paquetes únicamente necesitan trasladarse hacia el Gateway para luego ser direccionados hacia el equipo destino, estableciendo así que no tiene mayor incidencia la utilidad de interfaces virtuales en la red local.

- En la prueba realizada hacia el servidor remoto, la ruta que se crea utilizando direccionamiento dinámico únicamente, está compuesta por 10 saltos entre equipos Router's como se puede apreciar en la Figura 59, en este caso se necesita que cada uno de ellos procese el paquete verificando el siguiente salto, esto genera a su vez la necesidad de emplear un tiempo determinado en cada sitio aumentando así el tiempo total que necesita el envió para llegar a su destino, en comparación con las otras rutas del estudio esta solución es la que presenta mayor latencia.
- En la prueba realizada hacia el servidor remoto, la ruta que se crea con túneles VPN está compuesta por 5 saltos, en la Figura 61 se puede notar las direcciones 12.10.10.1 y 13.10.10.1 que corresponden a los extremos del túnel VPN creado y por donde se transmite la información, al utilizar este túnel se evita que cinco Router's en la ruta realicen la comprobación de los paquetes y aminora el tiempo que necesita él envió para llegar a su destino, la latencia que presenta esta ruta es menor que la de la ruta con direccionamiento dinámico pero mayor que la ruta que emplea OTV.
- En la prueba realizada hacia el servidor remoto, la ruta que se crea con la red sobrepuesta OTV está compuesta por 4 saltos, en la Figura 63 se puede notar la dirección 12.12.12.1 que corresponde a la interface de adyacencia que permite al

equipo integrarse a la red sobrepuesta, una vez que los paquetes llegan a la red sobrepuesta son transmitidos mediante enrutamiento MAC hacia el equipo borde que registra en su tabla de direccionamiento MAC el destino, el empleo de la red sobrepuesta reduce notablemente el tiempo que necesita el envío para llegar a su destino, la latencia en esta ruta es la menor en comparación con las otras rutas.

La segunda parte de las pruebas consiste en obtener el tiempo requerido para cargar una página web solicitada desde el cliente de la red local y el tiempo requerido con la solicitud realizada desde un cliente en una LAN remota, en la primera parte se lo hace sobre la red sin el uso de interfaces virtuales y posteriormente sobre la red con interfaces virtuales, esto con el fin de establecer la diferencia que existe en la latencia al utilizar tecnologías de enlaces directos que emplean trafico etiquetado para agilitar la transmisión de información.

4.2 Pruebas de carga ligera en la red con enrutamiento Dinámico

En las siguientes figuras se indica el tiempo que demora en cargar una página web haciendo la solicitud desde el cliente al servidor en la misma LAN y la solicitud a un servidor ubicado en una LAN remota, esto sobre la red sin emplear interfaces virtuales ni trafico etiquetado.

En este caso la red local es 172.17.37.0/24 donde el cliente tiene la dirección 172.17.37.4 y el servidor la dirección 172.17.37.3. La red remota para la prueba es 192.168.101.0/24 en donde la dirección del servidor es 192.168.101.3

Carga de la web desde LAN local sin VPN

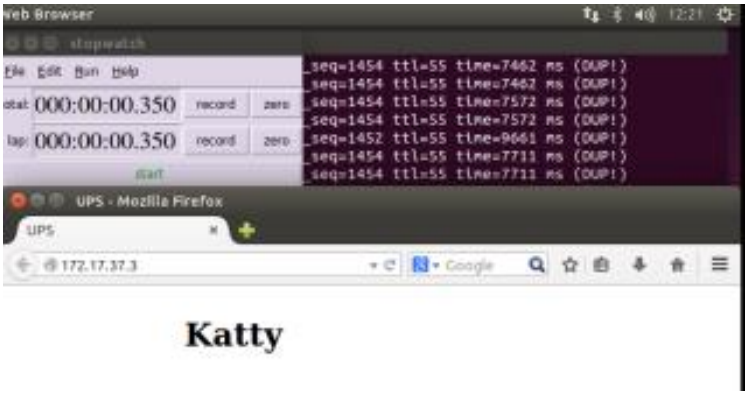


Figura 64. Carga de la web desde LAN local sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red local.

Carga de la web desde LAN remota sin VPN

Figura 65. Carga de la web desde LAN remota sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red remota.

Tabla 9.

Muestreo de carga ligera sin VPN

Iteración (U)	Servidor Local (Segundos)	Servidor Remoto (Segundos)
1 Muestra	0.350	5.032
2 Muestra	0.265	8.911
3 Muestra	0.324	7.956

Promedio	0.313	7.299

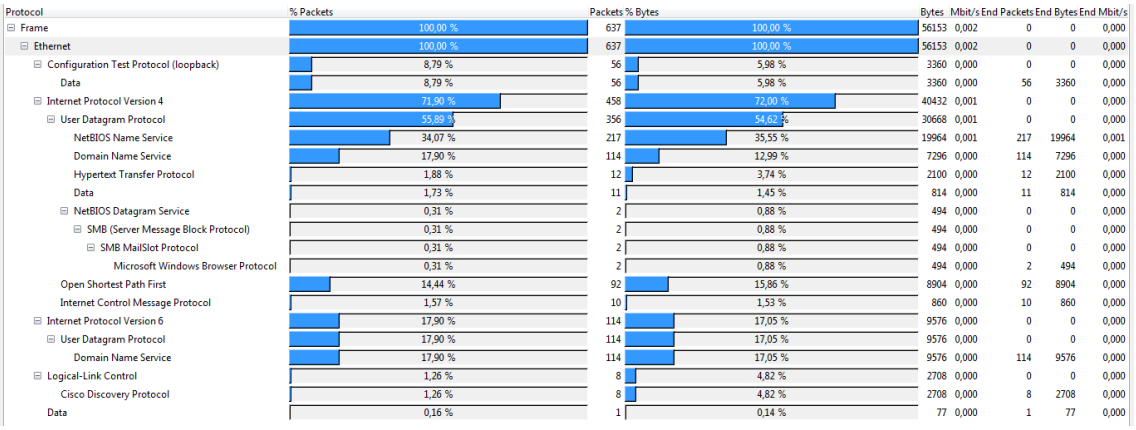
Nota: Muestras para calcular el tiempo de carga ligera sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo en la prueba se ha establecido que para la carga de una web desde un servidor local el tiempo de latencia necesario es de 0.313s, esto debido a que los paquetes no necesitan recorrer gran distancia entre el origen y el destino pues comparten el mismo núcleo y no se necesita de saltos a otras redes.

En la carga de la web desde un servidor remoto el tiempo promedio de latencia necesario es de 7.299s pues en este caso los paquetes necesitan ser dirigidos hacia su destino atravesando 10 saltos en la ruta como se puede apreciar en la Figura 59. El uso de enrutamiento dinámico es útil para redes pequeñas y en donde la cantidad del flujo de tráfico sea bajo pues se generan mucho paquetes Broadcast que aumentan la carga de la red y en determinado caso esto puede significar la pérdida del enlace, en el caso de redes corporativas este tipo de enrutamiento es ineficiente pues no provee la suficiente seguridad tanto en el estado del enlace como en eficiencia de tiempo en la transmisión.

Carga ligera (WEB) inyectada a la red con enrutamiento dinámico



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	637	100,00 %	56153	0,002	0	0	0,000
Ethernet	100,00 %	637	100,00 %	56153	0,002	0	0	0,000
Configuration Test Protocol (loopback)	8,79 %	56	5,98 %	3360	0,000	0	0	0,000
Data	8,79 %	56	5,98 %	3360	0,000	56	3360	0,000
Internet Protocol Version 4	71,90 %	458	72,00 %	40432	0,001	0	0	0,000
User Datagram Protocol	55,89 %	356	54,62 %	30668	0,001	0	0	0,000
NetBIOS Name Service	34,07 %	217	35,55 %	19964	0,001	217	19964	0,001
Domain Name Service	17,90 %	114	12,99 %	7296	0,000	114	7296	0,000
Hypertext Transfer Protocol	1,88 %	12	3,74 %	2100	0,000	12	2100	0,000
Data	1,73 %	11	1,45 %	814	0,000	11	814	0,000
NetBIOS Datagram Service	0,31 %	2	0,88 %	494	0,000	0	0	0,000
SMB (Server Message Block Protocol)	0,31 %	2	0,88 %	494	0,000	0	0	0,000
SMB MailSlot Protocol	0,31 %	2	0,88 %	494	0,000	0	0	0,000
Microsoft Windows Browser Protocol	0,31 %	2	0,88 %	494	0,000	2	494	0,000
Open Shortest Path First	14,44 %	92	15,86 %	8904	0,000	92	8904	0,000
Internet Control Message Protocol	1,57 %	10	1,53 %	860	0,000	10	860	0,000
Internet Protocol Version 6	17,90 %	114	17,05 %	9576	0,000	0	0	0,000
User Datagram Protocol	17,90 %	114	17,05 %	9576	0,000	0	0	0,000
Domain Name Service	17,90 %	114	17,05 %	9576	0,000	114	9576	0,000
Logical-Link Control	1,26 %	8	4,82 %	2708	0,000	0	0	0,000
Cisco Discovery Protocol	1,26 %	8	4,82 %	2708	0,000	8	2708	0,000
Data	0,16 %	1	0,14 %	77	0,000	1	77	0,000

Figura 66. Carga ligera (WEB) inyectada a la red con enrutamiento dinámico
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos de la Figura 66 el número de paquetes transmitidos son 637 con el 100% de éxito en la transmisión, muestra también que se está utilizando como protocolo de transporte Ipv4 y para la comunicación y estabilidad del enlace NetBIOS, se puede apreciar también que al usar solo el enrutamiento dinámico los paquetes son enviados con los encabezados predeterminados y son verificados en cada uno de los puntos por donde atraviesan para seleccionar su próximo destino, esto a su vez se convierte en un aumento de tiempo en la latencia de transmisión.

4.3 Pruebas de carga ligera en la red con túneles VPN

En las siguientes figuras se indica el tiempo que demora en cargar una página web haciendo la solicitud desde el cliente al servidor en la misma LAN sobre la red con túneles VPN y la solicitud a un servidor remoto en una LAN distante.

La red local es 172.17.37.0/24 donde el cliente tiene la dirección 172.17.37.4 y el servidor la dirección 172.17.37.3. La red remota es 192.168.101.0/24 en donde la dirección del servidor es 192.168.101.3

Carga de la web desde LAN local con VPN

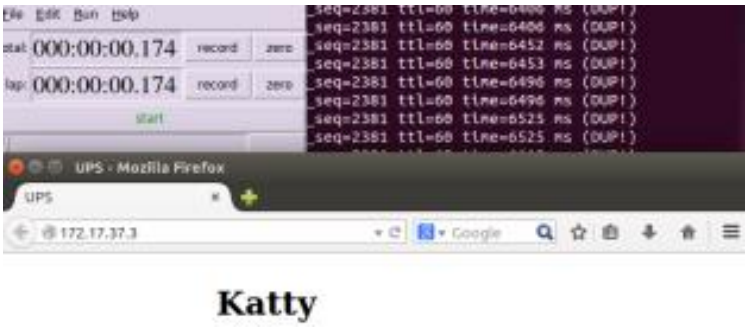


Figura 67. Carga de la web desde LAN local con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red local.

Carga de la web desde LAN remota con VPN

Figura 68. Carga de la web desde LAN remota con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red remota.

Tabla 10.

Muestreo de carga ligera con VPN

Iteración (U)	Servidor Local (Segundos)	Servidor Remoto (Segundos)
1 Muestra	0.174	3.846
2 Muestra	0.188	3.431
3 Muestra	0.185	3.667
Promedio	0.182	3.648

Nota: Muestras para calcular el tiempo con carga ligera con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo se ha establecido que el tiempo promedio de carga de la web es de 0.182s en la red local y de 3.648s para la red remota. Realizando la comparación con los valores obtenidos en la prueba anterior en la red con enrutamiento dinámico es notable que al utilizar túneles VPN el tiempo de carga se reduce debido a que los equipos crean una interface virtual entre dos extremos y se crea una ruta única que se muestra como una conexión lineal por la cual la información es transmitida.

Como se puede apreciar la diferencia de tiempo es mucho más notable en el servidor remoto que en el servidor local, pues como se puede ver en la Figura 61 los extremos del

túnel remplazan a 5 saltos entre equipos lo que se traduce en mayor rapidez en la transmisión de datos.

Carga ligera (WEB) inyectada a la red con VPN

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	775	100,00 %	87855	0,022	0	0	0,000
Ethernet	100,00 %	775	100,00 %	87855	0,022	0	0	0,000
Internet Protocol Version 4	99,10 %	768	99,20 %	87156	0,022	0	0	0,000
Encapsulating Security Payload	97,16 %	753	97,05 %	85266	0,021	753	85266	0,021
Open Shortest Path First	0,77 %	6	0,64 %	564	0,000	6	564	0,000
User Datagram Protocol	1,16 %	9	1,51 %	1326	0,000	0	0	0,000
Hypertext Transfer Protocol	0,77 %	6	1,20 %	1050	0,000	6	1050	0,000
NetBIOS Name Service	0,39 %	3	0,31 %	276	0,000	3	276	0,000
Configuration Test Protocol (loopback)	0,77 %	6	0,41 %	360	0,000	0	0	0,000
Data	0,77 %	6	0,41 %	360	0,000	6	360	0,000
Logical-Link Control	0,13 %	1	0,39 %	339	0,000	0	0	0,000
Cisco Discovery Protocol	0,13 %	1	0,39 %	339	0,000	1	339	0,000

Figura 69. Carga ligera (WEB) inyectada a la red con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos de la Figura 69 el número de paquetes enviados son 775 con el 100% de éxito en la transmisión. Realizando una comparación con la transmisión realizada con enrutamiento dinámico se puede apreciar que a los paquetes que son enviados por el túnel VPN se les agrega un encabezado y se los encapsula etiquetándolos de manera que todos sigan el mismo camino hacia su destino, a comparación de los datos presentados en la Figura 66 el 98.13% de los paquetes toman el mismo camino a través del túnel lo que agiliza la transmisión al crear un camino lineal que no necesita que los paquetes sean verificados en cada uno de los puntos por los que atraviesa.

4.4 Pruebas de carga ligera con OTV

En las pruebas que se realizan con OTV es necesario indicar el cambio realizado en algunos puntos pues al ser una solución que está presente en equipos de alta gama, estos permiten tener funcionalidades adicionales que brindan ventajas a la red.

El primer cambio realizado en la red es la unificación de L2 y L3 en el equipo Switch Nexus 7000 pues al ser un equipo multicapa permite tener las funciones del Router Core y también las funciones del Switch de distribución. Este cambio es notable al observar las Figura 23 del diseño lógico y compararla con la siguiente Figura del diseño con los equipos implementados.

Diseño de la red con equipos Switch Nexus 7000

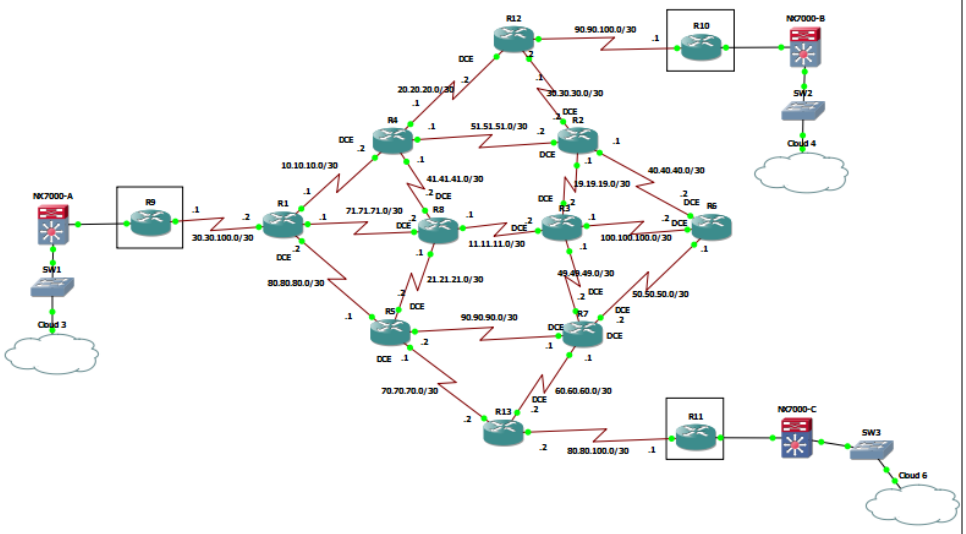


Figura 70. Diseño de la red con equipos Switch Nexus 7000
Fuente: Wilson Collaguazo y Katherine Ramos

Con la unificación las redes LAN, que en el diseño lógico se establecían como dos subredes ahora estas forman una sola, es así que las redes 172.17.36.0/24 y la red 172.17.37.0/24 ahora se representan únicamente con la red 172.17.36.0/24 pues como se indicó los equipos que tenían esta redes se han cambiado por uno solo. Lo mismo sucede con las otras redes LAN que serán representadas por la red 192.168.101.0/24 y 182.16.36.0/24.

En las siguientes figuras se indica el tiempo que demora en cargar una página web haciendo la solicitud desde el cliente al servidor en la misma LAN sobre la red con la solución OTV configurada y la solicitud a un servidor remoto en una LAN distante.

La red local es 192.168.101.0/24 donde el cliente tiene la dirección 192.168.101.4 y el servidor la dirección 192.168.101.3. La red remota es la 172.17.36.0/24 en donde la dirección del servidor es 172.17.36.3

Carga de la web desde LAN local con OTV

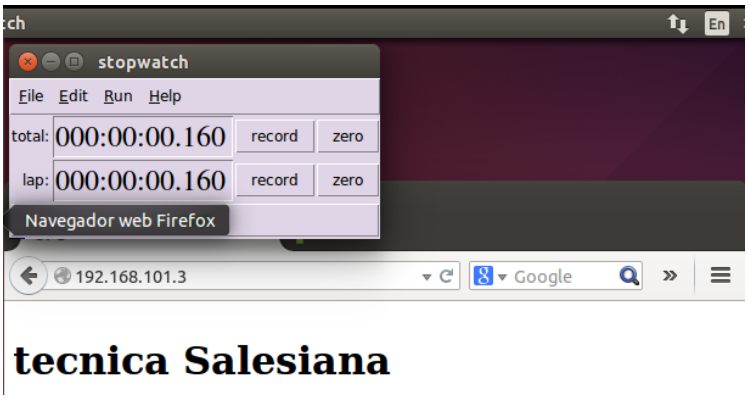


Figura 71. Carga de la web desde LAN local con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red local.

Carga de la web desde LAN remota con OTV

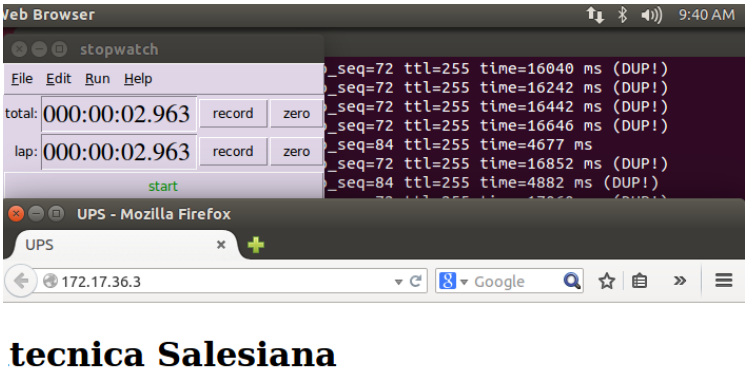


Figura 72. Carga de la web desde LAN remota con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una página web cuando se hace la solicitud desde el cliente en la red remota.

Tabla 11.

Muestreo de carga ligera con OTV

Iteración (U)	Servidor Local (Segundos)	Servidor Remoto (Segundos)
1 Muestra	0.170	2.909
2 Muestra	0.160	3.123
3 Muestra	0.161	2.963
Promedio	0.164	2.998

Nota: Muestras para calcular el tiempo de carga ligera con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo se ha establecido que el tiempo promedio necesario para la carga de la web desde un servidor en la LAN local con OTV es de 0.164s y el tiempo promedio para la carga desde un servidor en una red remota con la red sobrepuesta es de 2.998s.

Los tiempos en este caso son menores que en las otras pruebas, esto debido a que se crean interfaces virtuales de enlace directo como son, la Interface interna para la comunicación desde el interior de la LAN local hacia el equipo de borde, la interface

interna hace que se mantenga una conexión activa entre los equipos que componen el sitio y el equipo borde haciendo que no se necesita crear solicitudes de establecimiento de enlaces y que reduzca el tiempo de latencia en la transmisión. En el caso de la carga web desde un servidor remoto el comportamiento es similar pues como ya se ha mencionado en puntos anteriores el equipo borde crea una interface Join que le da acceso a la red sobrepuesta y permite que los equipos mantengan una conexión activa haciendo que la trasmisión pueda ser enviada por varios caminos con igual costo de ruta hacia el destino disminuyendo de esta manera notablemente la latencia. Si se observa la Figura 62 muestra la ruta compuesta por la dirección IP del equipo emisor, la IP de la interface física asociada a la adyacencia y la dirección IP del destino, esto debido a que una vez que los paquetes llegan al equipo de borde, la interface física los encapsula dentro de los paquetes IPV4 asignándoles cabeceras que contienen el enrutamiento hacia la MAC destino y los envía por la red sobrepuesta hacia el equipo de borde que tenga en la tabla de equipos del sitio la MAC correspondiente y de ahí llega directamente hacia el destino sin ser intervenidos.

Carga ligera (WEB) inyectada a la red con OTV

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	24238	100.0	2215845	39 k	0	0	0
Ethernet	100.0	24238	100.0	2215845	39 k	0	0	0
Logical-Link Control	0.1	31	0.4	9509	168	0	0	0
Cisco Discovery Protocol	0.1	31	0.4	9509	168	31	9509	168
Internet Protocol Version 6	0.2	41	0.2	4652	82	0	0	0
User Datagram Protocol	0.2	38	0.2	4382	77	0	0	0
Link-local Multicast Name Resolution	0.1	20	0.1	1704	30	20	1704	30
Hypertext Transfer Protocol	0.0	1	0.0	179	3	1	179	3
DHCPv6	0.1	17	0.1	2499	44	17	2499	44
Internet Control Message Protocol v6	0.0	3	0.0	270	4	3	270	4
Internet Protocol Version 4	99.3	24073	99.1	2196087	38 k	0	0	0
User Datagram Protocol	12.0	2902	12.7	280353	4966	0	0	0
NetBIOS Name Service	9.9	2394	9.9	220248	3901	2394	220248	3901
Link-local Multicast Name Resolution	0.1	20	0.1	1304	23	20	1304	23
Hypertext Transfer Protocol	0.4	95	1.3	29719	526	95	29719	526
Data	1.6	393	1.3	29082	515	393	29082	515
Open Shortest Path First	0.8	196	0.8	17200	304	196	17200	304
Internet Group Management Protocol	0.1	20	0.1	1152	20	20	1152	20
Internet Control Message Protocol	85.5	20715	72.6	1608474	28 k	20715	1608474	28 k
Generic Routing Encapsulation	1.0	240	13.0	288908	5118	0	0	0
MultiProtocol Label Switching Header	1.0	240	13.0	288908	5118	0	0	0
Data	1.0	240	13.0	288908	5118	240	288908	5118
Data	0.0	1	0.0	77	1	1	77	1
Configuration Test Protocol (loopback)	0.4	90	0.2	5400	95	0	0	0
Data	0.4	90	0.2	5400	95	90	5400	95
Address Resolution Protocol	0.0	2	0.0	120	2	2	120	2

Figura 73. Carga ligera (WEB) inyectada a la red con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos de la Figura 73 el número de paquetes transmitidos son 24238 con el 100% de éxito en la transmisión, muestra que se está utilizando como protocolo de transporte Ipv4. Aunque no se lo puede detector con la captura del tráfico los paquetes son encapsulados con la cabecera OTV lo que hace que un mayor número de paquetes sea transmitidos en el mismo lapso de tiempo mejorando notablemente la latencia.

4.5 Pruebas de carga pesada en la red con enrutamiento Dinámico

En las siguientes figuras se indica el tiempo que demora en cargar la solicitud de acceso FTP desde el cliente al servidor en la misma LAN y la solicitud a un servidor remoto en una LAN distante sobre la red sin interfaces virtuales.

La red local es 172.17.37.0/24 donde el cliente tiene la dirección 172.17.37.4 y el servidor la dirección 172.17.37.3 y la red remota es 192.168.101.0/24 en donde la dirección del servidor es 192.168.101.3

Solicitud conexión FTP red local sin VPN

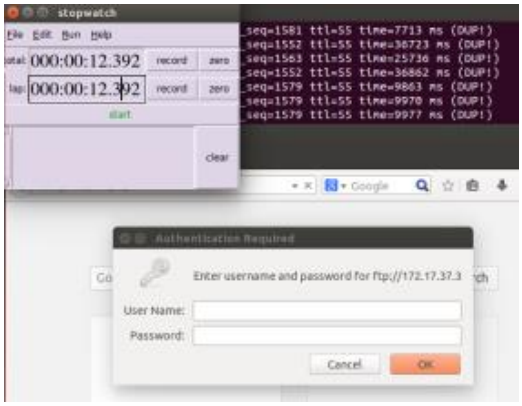


Figura 74. Solicitud conexión FTP red local sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red local.

Solicitud conexión FTP red remota sin VPN

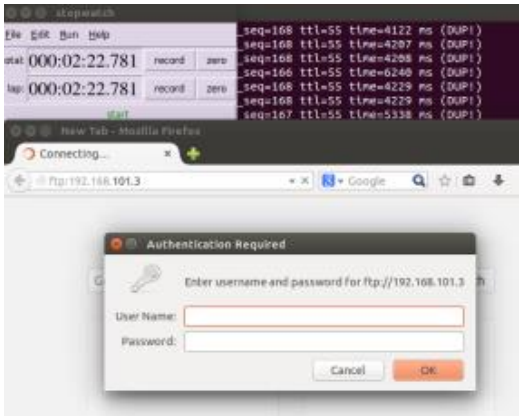


Figura 75. Solicitud conexión FTP red remota sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red remota.

Tabla 12.

Muestreo de carga pesada sin VPN

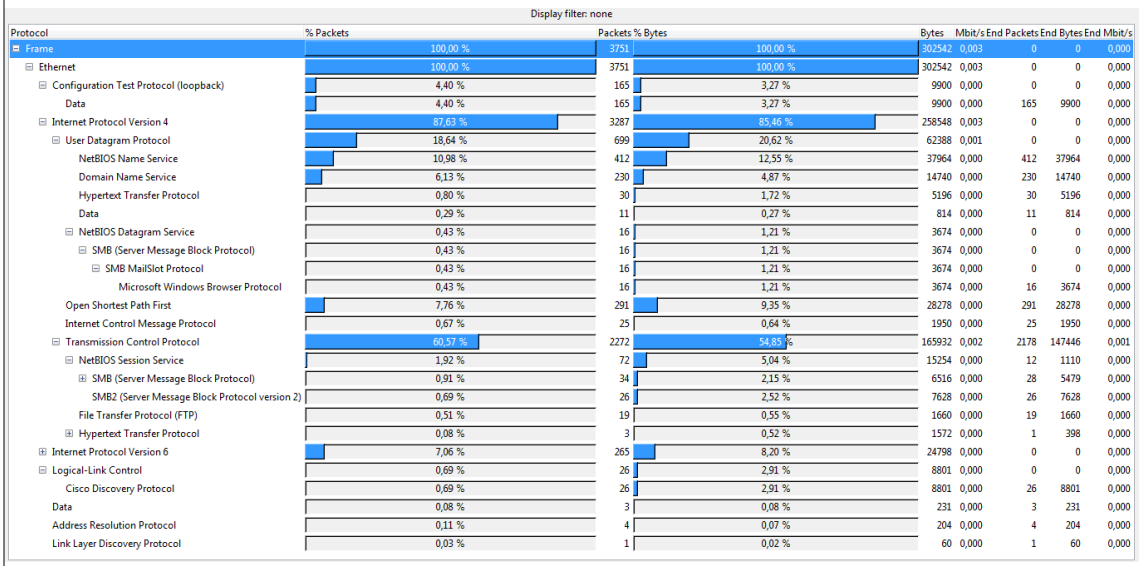
Iteración (U)	Servidor Local (MM:SS)	Servidor Remoto (MM:SS)
1 Muestra	0:12.392	02:22.781
2 Muestra	0:12.445	02:15.866
3 Muestra	0:12.415	02:18.335
Promedio	0:12.417	02:18.994

Nota: Muestras para calcular el tiempo de carga pesada sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo se ha establecido que el tiempo promedio de carga de la conexión remota hacia el servidor FTP es de 0m: 12.417s en la red local y de 02m: 18.994s para la red remota utilizando enrutamiento dinámico. Como se ha mencionado en el principio de la prueba a diferencia de las realizadas anteriormente sobre un servidor web esta necesita transmitir un mayor número de paquetes entre el servidor FTP y el cliente para establecer un enlace remoto que permita gestionar en tiempo real los ficheros que se encuentran albergados en el servidor, esto hace que se requiere un mayor consumo de recursos y el flujo de tráfico de la red se vuelva más pesado. En este caso al utilizar enrutamiento dinámico se requiere de un tiempo excesivamente prolongado para el establecimiento de la conexión remota

Carga pesada (FTP) inyectada a la red sin VPN



Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	3751	100,00 %	302542	0,003	0	0	0,000
Ethernet	100,00 %	3751	100,00 %	302542	0,003	0	0	0,000
Configuration Test Protocol (loopback)	4,40 %	165	3,27 %	9900	0,000	0	0	0,000
Data	4,40 %	165	3,27 %	9900	0,000	165	9900	0,000
Internet Protocol Version 4	87,63 %	3287	85,46 %	258548	0,003	0	0	0,000
User Datagram Protocol	18,64 %	699	20,62 %	62388	0,001	0	0	0,000
NetBIOS Name Service	10,98 %	412	12,55 %	37964	0,000	412	37964	0,000
Domain Name Service	6,13 %	230	4,87 %	14740	0,000	230	14740	0,000
Hypertext Transfer Protocol	0,80 %	30	1,72 %	5196	0,000	30	5196	0,000
Data	0,29 %	11	0,27 %	814	0,000	11	814	0,000
NetBIOS Datagram Service	0,43 %	16	1,21 %	3674	0,000	0	0	0,000
SMB (Server Message Block Protocol)	0,43 %	16	1,21 %	3674	0,000	0	0	0,000
SMB MailSlot Protocol	0,43 %	16	1,21 %	3674	0,000	0	0	0,000
Microsoft Windows Browser Protocol	0,43 %	16	1,21 %	3674	0,000	16	3674	0,000
Open Shortest Path First	7,76 %	291	9,35 %	28278	0,000	291	28278	0,000
Internet Control Message Protocol	0,67 %	25	0,64 %	1950	0,000	25	1950	0,000
Transmission Control Protocol	60,57 %	2272	54,85 %	165932	0,002	2178	147446	0,001
NetBIOS Session Service	1,92 %	72	5,04 %	15254	0,000	12	1110	0,000
SMB (Server Message Block Protocol)	0,91 %	34	2,15 %	6516	0,000	28	5479	0,000
SMB2 (Server Message Block Protocol version 2)	0,69 %	26	2,52 %	7628	0,000	26	7628	0,000
File Transfer Protocol (FTP)	0,51 %	19	0,55 %	1660	0,000	19	1660	0,000
Hypertext Transfer Protocol	0,08 %	3	0,52 %	1572	0,000	1	398	0,000
Internet Protocol Version 6	7,06 %	265	8,20 %	24798	0,000	0	0	0,000
Logical-Link Control	0,69 %	26	2,91 %	8801	0,000	0	0	0,000
Cisco Discovery Protocol	0,69 %	26	2,91 %	8801	0,000	26	8801	0,000
Data	0,08 %	3	0,08 %	231	0,000	3	231	0,000
Address Resolution Protocol	0,11 %	4	0,07 %	204	0,000	4	204	0,000
Link Layer Discovery Protocol	0,03 %	1	0,02 %	60	0,000	1	60	0,000

Figura 76. Carga pesada (FTP) inyectada a la red sin VPN
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos mostrados en la Figura 74, el número de paquetes transmitidos es de 3751 con un 100% de eficiencia de trasmisión, como se indicó anteriormente el tiempo requerido para el transporte de esta carga es excesivo, esto debido a que los paquetes toman varios caminos hacia el destino y se requiere que cada uno de estos sea verificado por el equipo por donde está cruzando.

4.6 Pruebas de carga pesada en la red con túneles VPN

En las siguientes figuras se indica el tiempo que demora en cargar una página web haciendo la solicitud desde el cliente al servidor en la misma LAN y la solicitud a un servidor remoto en una LAN distante sobre la red con túneles VPN. La red local es 172.17.37.0/24 donde el cliente tiene la dirección 172.17.37.4 y el servidor la dirección 172.17.37.3. La red remota es 192.168.101.0/24 en donde la dirección del servidor es 192.168.101.3

Solicitud conexión FTP red local con VPN

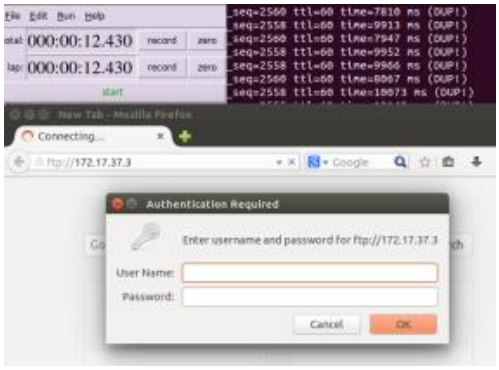


Figura 77. Solicitud conexión FTP red local con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red local.

Solicitud conexión FTP red remota con VPN

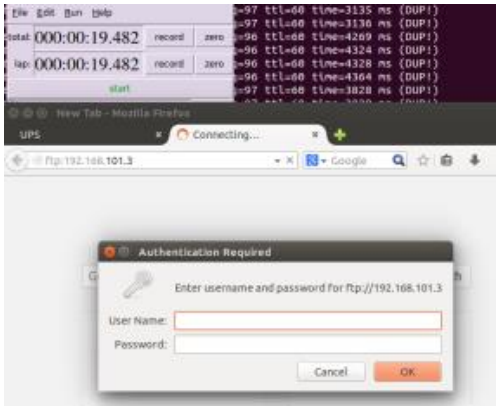


Figura 78. Solicitud conexión FTP red remota con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red remota.

Tabla 13.

Muestreo de carga pesada con VPN

Iteración (U)	Servidor Local (MM:SS)	Servidor Remoto (MM:SS)
1 Muestra	0:12.430	0:19.482
2 Muestra	0:12.076	0:20.509
3 Muestra	0:12.345	0:19.856
Promedio	0:12.284	0:19.949

Nota: Muestras para calcular el tiempo de carga pesada con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo se ha establecido que el tiempo promedio de carga de la conexión remota hacia el servidor FTP es de 0m: 12.284s en la red local y de 0m: 19.999s para la red remota en este caso utilizando VPN. Como se puede ver la diferencia entre utilizar VPN y enrutamiento dinámico es mucho más notable que en las prueba anterior pues hay una diferencia de casi 2 minutos en comparación del tiempo requerido para la conexión a al servidor remoto, mientras que el tiempo que se necesita para la conexión al servidor local no cambia.

Carga pesada (FTP) inyectada a la red con VPN

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	42513	100,00 %	4711137	0,041	0	0	0,000
Ethernet	100,00 %	42513	100,00 %	4711137	0,041	0	0	0,000
Internet Protocol Version 4	97,58 %	41484	96,55 %	4548626	0,039	0	0	0,000
Encapsulating Security Payload	92,83 %	39466	89,49 %	4215868	0,036	39466	4215868	0,036
Open Shortest Path First	0,55 %	233	0,48 %	22382	0,000	233	22382	0,000
User Datagram Protocol	3,56 %	1513	5,81 %	273498	0,002	0	0	0,000
Internet Group Management Protocol	0,15 %	65	0,08 %	3700	0,000	65	3700	0,000
Internet Control Message Protocol	0,11 %	45	0,07 %	3514	0,000	45	3514	0,000
Transmission Control Protocol	0,38 %	162	0,63 %	29664	0,000	150	17964	0,000
Hypertext Transfer Protocol	0,02 %	9	0,19 %	8880	0,000	0	0	0,000
eXtensible Markup Language	0,02 %	9	0,19 %	8880	0,000	9	8880	0,000
Malformed Packet	0,01 %	3	0,06 %	2820	0,000	3	2820	0,000
Configuration Test Protocol (loopback)	0,43 %	184	0,23 %	11040	0,000	0	0	0,000
Data	0,43 %	184	0,23 %	11040	0,000	184	11040	0,000
Logical-Link Control	0,07 %	29	0,21 %	9816	0,000	0	0	0,000
Cisco Discovery Protocol	0,07 %	29	0,21 %	9816	0,000	29	9816	0,000
Internet Protocol Version 6	1,77 %	752	2,93 %	138231	0,001	0	0	0,000
Link Layer Discovery Protocol	0,03 %	14	0,02 %	840	0,000	14	840	0,000
Address Resolution Protocol	0,11 %	48	0,05 %	2430	0,000	48	2430	0,000
Data	0,00 %	2	0,00 %	154	0,000	2	154	0,000

Figura 79. Carga pesada (FTP) inyectada a la red con VPN
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos mostrados en la Figura 79 el número de paquetes es de 42513 con un 100% de eficiencia en la trasmisión, Se puede notar que el número de paquetes en esta trasmisión es mayor que en la anterior prueba de carga con FTP pero sin embargo el tiempo de latencia es menor, esto debido a que los paquetes que se trasmiten por la VPN tienen una menor carga útil al necesitar del agregado de encabezados para marcar el tráfico que es transmitido.

Con menor carga útil es necesario fraccionar la información en un mayor número de partes algo que normalmente se constituiría en un inconveniente pero al utilizar túneles el flujo cruza directamente sin estar sujeto a comprobaciones por equipos fuera de los extremos del túnel y el hecho de tener más paquetes se vuelve trivial.

Al agregar las cabeceras a los paquetes el tráfico se etiqueta de tal manera que el primer paquete enviado marca el camino hacia el destino dejando la libertad a los paquetes que lo siguen para ser trasmitidos sin necesidad de ser sometidos a verificación, esto se traduce entonces en la eliminación del tiempo en el que los paquetes se detienen en cada equipo y son procesados para continuar con su trayecto.

4.7 Pruebas de carga pesada en a la red con OTV

En las siguientes figuras se indica el tiempo que demora en cargar la solicitud de acceso FTP desde el cliente al servidor en la misma LAN y la solicitud a un servidor remoto en una LAN distante sobre la red con la solución OTV configurada.

La red local es 192.168.101.0/24 donde el cliente tiene la dirección 192.168.101.4 y el servidor la dirección 192.168.101.3. La red remota es la 172.17.36.0/24 en donde la dirección del servidor es 172.17.36.3

Solicitud conexión FTP red local con OTV

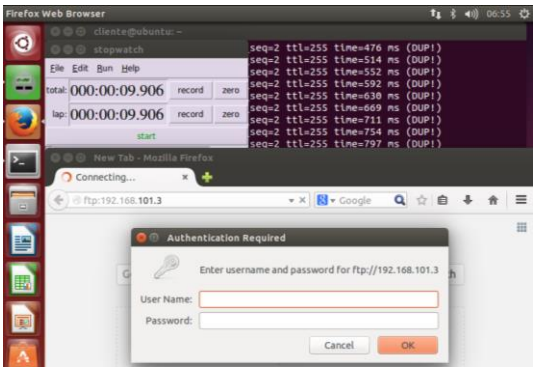


Figura 80. Solicitud conexión FTP red local con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red local.

Solicitud conexión FTP red remota con OTV

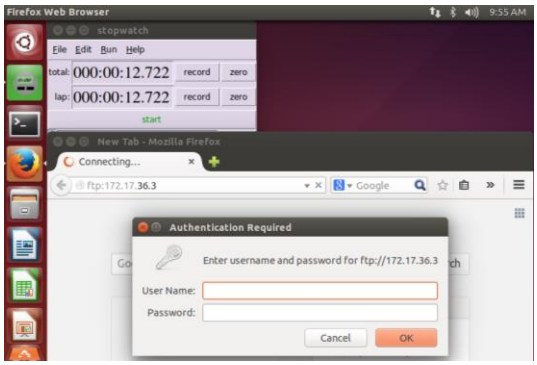


Figura 81. Solicitud conexión FTP red remota con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Toma de una muestra del tiempo que se demora en la carga de una conexión remota al servidor FTP cuando se hace la solicitud desde el cliente en la red local.

Tabla 14.

Muestreo de carga pesada con OTV

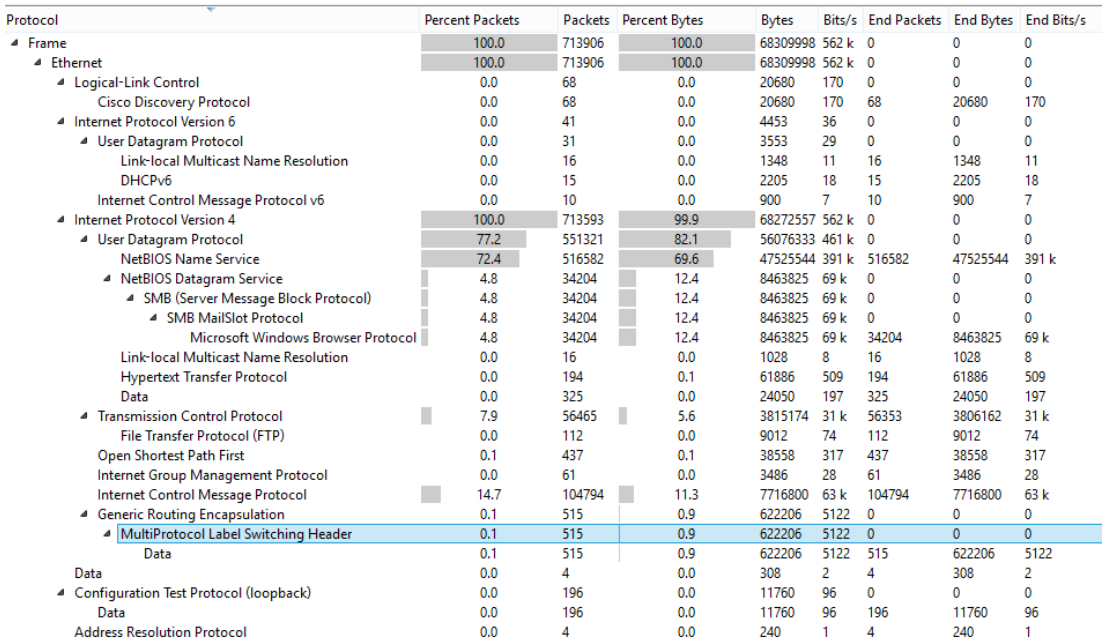
Iteración (U)	Servidor Local (MM:SS)	Servidor Remoto (MM:SS)
1 Muestra	0:10.817	0:12.722
2 Muestra	0:9.906	0:13.226
3 Muestra	0:9.949	0:13.213
Promedio	0:10.224	0:13.054

Nota: Muestras para calcular el tiempo de carga pesada con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

Resultados:

Tomando varias muestras de tiempo se ha establecido que el tiempo promedio de carga de la conexión remota hacia el servidor FTP es de 0m: 10.224s en la red local y de 0m: 13.054s para la conexión al servidor en la red remota en este caso utilizando la red sobrepuesta OTV. Haciendo una comparación entre el enrutamiento dinámico, la utilización de túneles VPN y la red sobrepuesta OTV, es mucho más eficiente emplear OTV pues presenta la menor latencia entre las rutas empleadas.

Carga pesada (FTP) inyectada a la red con OTV



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	713906	100.0	68309998	562 k	0	0	0
Ethernet	100.0	713906	100.0	68309998	562 k	0	0	0
Logical-Link Control	0.0	68	0.0	20680	170	0	0	0
Cisco Discovery Protocol	0.0	68	0.0	20680	170	68	20680	170
Internet Protocol Version 6	0.0	41	0.0	4453	36	0	0	0
User Datagram Protocol	0.0	31	0.0	3553	29	0	0	0
Link-local Multicast Name Resolution	0.0	16	0.0	1348	11	16	1348	11
DHCPv6	0.0	15	0.0	2205	18	15	2205	18
Internet Control Message Protocol v6	0.0	10	0.0	900	7	10	900	7
Internet Protocol Version 4	100.0	713593	99.9	68272557	562 k	0	0	0
User Datagram Protocol	77.2	551321	82.1	56076333	461 k	0	0	0
NetBIOS Name Service	72.4	516582	69.6	47525544	391 k	516582	47525544	391 k
NetBIOS Datagram Service	4.8	34204	12.4	8463825	69 k	0	0	0
SMB (Server Message Block Protocol)	4.8	34204	12.4	8463825	69 k	0	0	0
SMB MailSlot Protocol	4.8	34204	12.4	8463825	69 k	0	0	0
Microsoft Windows Browser Protocol	4.8	34204	12.4	8463825	69 k	34204	8463825	69 k
Link-local Multicast Name Resolution	0.0	16	0.0	1028	8	16	1028	8
Hypertext Transfer Protocol	0.0	194	0.1	61886	509	194	61886	509
Data	0.0	325	0.0	24050	197	325	24050	197
Transmission Control Protocol	7.9	56465	5.6	3815174	31 k	56353	3806162	31 k
File Transfer Protocol (FTP)	0.0	112	0.0	9012	74	112	9012	74
Open Shortest Path First	0.1	437	0.1	38558	317	437	38558	317
Internet Group Management Protocol	0.0	61	0.0	3486	28	61	3486	28
Internet Control Message Protocol	14.7	104794	11.3	7716800	63 k	104794	7716800	63 k
Generic Routing Encapsulation	0.1	515	0.9	622206	5122	0	0	0
MultiProtocol Label Switching Header	0.1	515	0.9	622206	5122	0	0	0
Data	0.1	515	0.9	622206	5122	515	622206	5122
Data	0.0	4	0.0	308	2	4	308	2
Configuration Test Protocol (loopback)	0.0	196	0.0	11760	96	0	0	0
Data	0.0	196	0.0	11760	96	196	11760	96
Address Resolution Protocol	0.0	4	0.0	240	1	4	240	1

Figura 82. Carga pesada (FTP) inyectada a la red con OTV
Fuente: Wilson Collaguazo y Katherine Ramos

De acuerdo a los datos mostrados en la Figura 82 el número de paquetes es de 713906 con un 100% de eficiencia en la trasmisión al utilizar IPv4 para encapsular todos los paquetes, en esta fase el número de paquetes es mayor que en las anteriores pruebas, sin embargo el tiempo de latencia es también el menor de todos, esto debido a que los paquetes que se trasmiten por la red sobrepuesta OTV no están sujetos a verificación en cada uno de los puntos por donde atraviesan permitiendo el trafico libre entre el origen y el destino manejando mejor tiempo de latencia.

Resultados generales:

En los siguientes cuadros y tablas se muestra la estadística comparativa entre las pruebas realizadas para establecer conclusiones acerca del comportamiento de la red en las distintas condiciones sometidas.

La tabla de carga web relaciona el número de saltos en la ruta con los tiempos de latencia promedios obtenidos según la configuración del protocolo de transmisión utilizado.

Tabla 15.

Resultados generales de la carga web

Direccionamiento	# Saltos	Latencia Local	Latencia Remota
Dinámico	10	0.313	7.299
Túneles VPN	5	0.182	3.648
Red OTV	3	0.164	2.998

Nota: Resultados generales con WEB con número de saltos, latencia local y remota
Fuente: Wilson Collaguazo y Katherine Ramos

La gráfica mostrada a continuación describe la comparativa entre el número de saltos y tipo de protocolo de transporte

Comparativa de saltos en la ruta hacia el servidor web

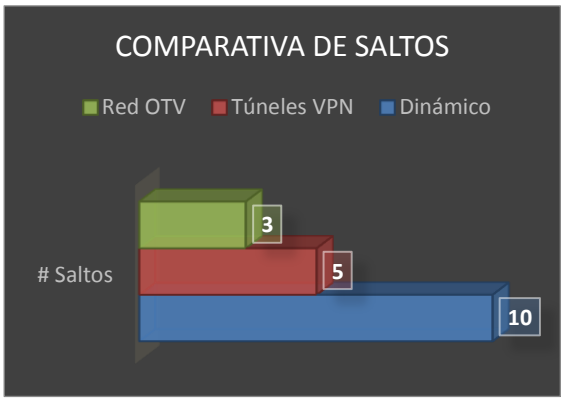


Figura 83. Comparativa de saltos en la ruta hacia el servidor web
Fuente: Wilson Collaguazo y Katherine Ramos

La gráfica mostrada a continuación describe la comparativa entre el tipo de protocolo de transporte y el tiempo de latencia

Comparativa de Latencia en el enlace al servidor web

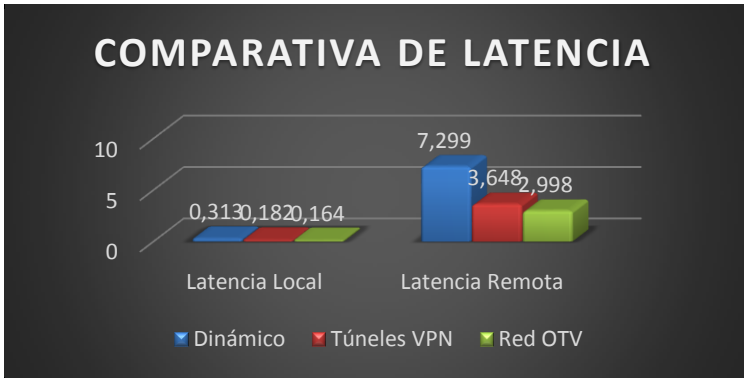


Figura 84. Comparativa de Latencia en el enlace al servidor web
Fuente: Wilson Collaguazo y Katherine Ramos

La tabla de carga FTP relaciona el número de saltos en la ruta con los tiempos de latencia promedios obtenidos según la configuración del protocolo de transmisión utilizado.

Tabla 16.

Resultados generales de la carga FTP

Direccionamiento	# Saltos	Latencia Local	Latencia Remota
Dinámico	10	12.417	138.994
Túneles VPN	5	12.284	19.949
Red OTV	3	10.224	13.054

Nota: Resultados generales con FTP con número de saltos, latencia local y remota
Fuente: Wilson Collaguazo y Katherine Ramos

La gráfica mostrada a continuación describe la comparativa entre el número de saltos y tipo de protocolo de transporte

Comparativa de saltos en la ruta hacia el servidor FTP

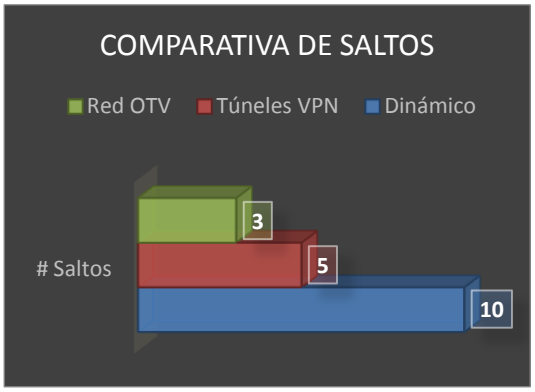


Figura 85. Comparativa de saltos en la ruta hacia el servidor FTP
Fuente: Wilson Collaguazo y Katherine Ramos

La gráfica mostrada a continuación describe la comparativa entre el tipo de protocolo de transporte y el tiempo de latencia

Comparativa de Latencia en el enlace al servidor FTP

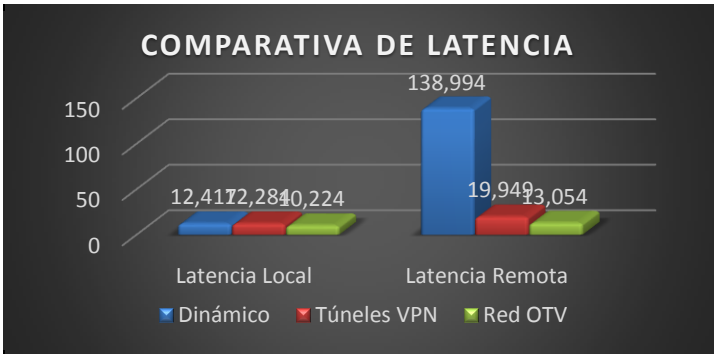


Figura 86. Comparativa de Latencia en el enlace al servidor FTP
Fuente: Wilson Collaguazo y Katherine Ramos

CONCLUSIONES

- El uso interfaces virtuales para transportar la información es una manera de asegurar la integridad de los paquetes enviados pues es muy difícil que personas que son ajenas a la empresa encuentren la forma de captarlos y tener acceso a la información.
- Una vez que se ha analizado los resultados obtenidos se concluye que OTV es una de las mejores soluciones para la interconexión de centros de datos, esto en base a la comparación del uso direccionamiento dinámico y al uso de túnel VPN para transportar la información pues presenta la menor latencia tanto en el tráfico local como en el tráfico hacia una red remota. Mediante la configuración del protocolo OTV en los Switch Nexus 7000 de los nodos se obtiene los siguientes datos, de la carga web la latencia local es de 0,164s y la latencia remota es de 2,998s, de la carga FTP la latencia local es de 10,224s y la latencia remota es de 13,054s estos valores son los más bajos obtenidos en las pruebas y pueden ser vistos con mayor claridad en la Figuras 84 y 85 en la presentación de resultados generales.
- La gran cantidad de paquetes transmitidos que se observan con el uso del protocolo OTV en las pruebas de carga liviana y pesada se debe al encapsulamiento UDP que utiliza el protocolo en sí, el cual no verifica los paquetes que se envían a cada uno de los nodos y esto hace que un mayor número de paquetes se transmitan en el mismo lapso de tiempo que las otras tecnologías toman para transmitir una menor cantidad.
- Con el aprendizaje de direcciones MAC que OTV proporciona por medio del plano de control se logra la comunicación inmediata entre los respectivos nodos de la red sobrepuesta, evitando así que se utilice mecanismos de inundación en la red para dar

a conocer las direcciones de los equipos que la conforman y dejando de generar trafico innecesario.

- La tecnología MPLS forma parte de los servicios de OTV, esta entra en funcionamiento sin necesidad de configuraciones adicionales, se activa conjuntamente con el protocolo. Mediante esta tecnología se hace uso de etiquetas para asignar al tráfico que va dentro de la red sobrepuesta.
- El enrutamiento MAC hace uso del protocolo IS-IS de routing y control de enlaces para realizar el direccionamiento de los paquetes sobre la red sobrepuesta, al igual que MPLS no es necesario configurar el servicio pues esta también embebido en el protocolo OTV. IS-IS se hace notorio si se configura una VPN OTV como se indica en la implementación en el literal 3.3
- OTV es una solución eficiente para la interconexión de centros de datos empresariales ya que provee a la red de algunos beneficios que ahorran recursos y por ende esto se convierte en ahorro de dinero. Ahora si bien se ha demostrado con este trabajo que es una excelente herramienta también hay que decir que la principal desventaja que presenta es que solo se encuentra en equipos de alta agama con costos elevados, por lo que su implementación será beneficiosa solo para empresas grandes donde el flujo de información es alto y se requiere de enlaces de altas prestaciones. Un enlace de alta velocidad proporcionado por un proveedor de servicios tiende en algunos casos a ser mayor que si se invirtieran en este tipo de soluciones por lo que actualmente algunas empresas han optado por manejar sus propios enlaces corporativos.

RECOMENDACIONES

- En la configuración del ambiente físico se recomienda que al montar la imagen del Switch Nexus 7000 en VMware en caso de presentarse un error de incompatibilidad con las interfaces, la solución es eliminar las interfaces embebidas en la imagen desde el fichero de configuración de la máquina virtual en VMware y ejecutar la máquina virtual para posteriormente ir agregando las interfaces con la maquina en funcionamiento. Verificar que las interfaces de los Switch Nexus 7000 en las máquinas virtuales estén levantadas (up), esto se puede realizar ejecutando el comando **#show ip interface brief** en línea de comandos proporcionada por la herramienta Putty, caso contrario si las interfaces se encuentran apagadas (Down) la solución es desactivar y volver activar los adaptadores de red de cada máquina con lo cual las interfaces se levantan y se puede continuar con la configuración. Al utilizar adaptadores de red de USB a RJ45 hay que asegurarse que estos sean compatibles con múltiples plataformas ya que existen muchos en el mercado que no tienen compatibilidad con sistemas Unix - Linux que en este caso son la base de los IOS que se utiliza en los equipos. En las interfaces de las nubes en GNS3 que sirven de conexión con las máquinas virtuales se debe tener en cuenta que sean las mismas que las asignadas en las máquinas en VMware pues de ellos depende la conexión hacia servidores y clientes.
- En la configuración de las condiciones de la red se recomienda levantar la red OTV tomando en consideración que tipo de red sobrepuesta es la que se desea crear para ello es necesario revisar el literal 1.4 del presente trabajo en donde se describe que tipo de redes existentes, tomar en cuenta también que si se va a configurar las

extensiones de las Vlans sobre la red sobrepuesta se debe tener configurado previamente todas las Vlans y troncales para que posteriormente no haya problema de duplicidad.

- En el trascurso del desarrollo de las pruebas se recomienda tener un monitoreo constante sobre los enlaces y procurar que el lugar donde se realiza el armado del ambiente de trabajo no este expuesto a manipulación por terceros ya que esto puede ser razón de errores al momento de tomar muestras y establecer resultados.
- En la toma de muestras de las pruebas se recomienda recoger al menos tres muestras para tener una mejor aproximación al tiempo promedio.
- En el servidor FTP utilizado para pruebas se recomienda compartir previamente un archivo que sirva para probar el enlace con la apertura de este.
- Se recomienda que para futuros trabajos se revise como prioridad la existencia de nuevas versiones del NEXUS-IOS y las actualizaciones que sean publicadas acerca del protocolo OTV en registros oficiales, como tema complementario a este trabajo se puede realizar la factibilidad del protocolo con soporte de IPv6.

REFERENCIAS

Andrade, J., & Súarez, F. (2012). Estudio e implementacion de una solución de virtualización para la Universidad Politécnica Salesiana (Tesis de Pregrado). *Universidad Politécnica Salesiana*, 272.

Cisco Systems Inc. (2008, 03 23). *Guía de diseño de OSPF*. Retrieved from http://www.cisco.com/cisco/web/support/LA/7/73/73214_1.pdf

ciscoipv6ttechtips. (2011). *Cisco Configuration*. Retrieved from http://www.ciscoipv6ittechtips.com/39th-article-the-group-and-hashipv6-

Cure, E., & Gonzáles , J. L. (2012). ANÁLISIS DE LA ARQUITECTURA MPLS (MULTI-PROTOCOL LABEL SWITCHING) PARA EL ESTUDIO Y ESTABLECIMIENTO DE VPN'S Y EL DISEÑO. 55.

Escalante Gil, K. M. (2012, Septiembre 03). *SlideShare*. Retrieved from SlideShare: es.slideshare.net

Ferrer Martínez, M. D. (2011, Mayo 05). MPLS, EL PRESENTE DE LAS REDES IP. . Retrieved from SlidePlayer.

Gil, F. H. (2013). *Introduccion al OSPF*. Retrieved from www.uv.es/~montanan/redes/trabajos/OSPF.doc

Lavado, G. (2015, Enero 29). IS-IS. *CISCO*, 29.

Neumann , J. (2014). *The Book of GNS3.* San Francisco.

Oracle VM VirtualBox. (2015). "About VirtualBox". *VirtualBox.org*, 15.

Velásquez, K. (n.d.). *MPLS, (UCV, Universidad Central de Venezuela).* Venezuela.

Watch Guard System Manager Help. (2010). *About Diffie-Hellman Groups*. Retrieved from http://www.watchguard.com/help/docs/wsm/11/en-US/index_Left.html#CSHID=en-US%2Fbovpn%2Fmanual%2Fdiffie_hellman_c.html|StartTopic=Content%2Fen-US%2Fbovpn%2Fmanual%2Fdiffie_hellman_c.html|SkinName=WSM