------------------------------------------------------------------------------------------------------------------------------------------

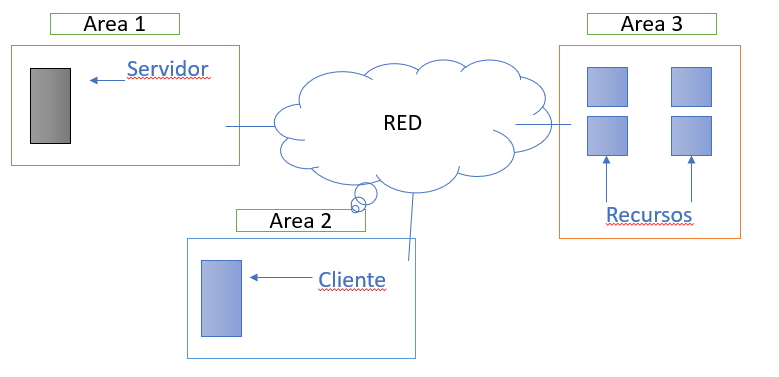


Ilustración 1 - Sistema distribuido Cliente-Servidor

Hay básicamente dos tipos de redes, redes de área local (LAN) y redes de área amplia (WAN). La diferencia entre ambos es la manera en que se encuentran conectadas geográficamente. Las redes de área local están compuestas por los clientes distribuidos en pequeñas áreas y redes de área amplia esta compuesta por sistemas distribuidos en extensas zonas, estas diferencias implican mayor variación en la velocidad y fiabilidad de las redes de comunicaciones.

Redes de área amplia

Este compuesto típicamente por líneas telefónicas, cables ópticos, enlaces de microondas, ondas de radio, canales satelitales y líneas de arrendamiento. La comunicación esta controlada por routers que son responsables del direccionamiento de trafico a otros Reuter o redes y el conjunto de transferencia de información hacia varios sitios.

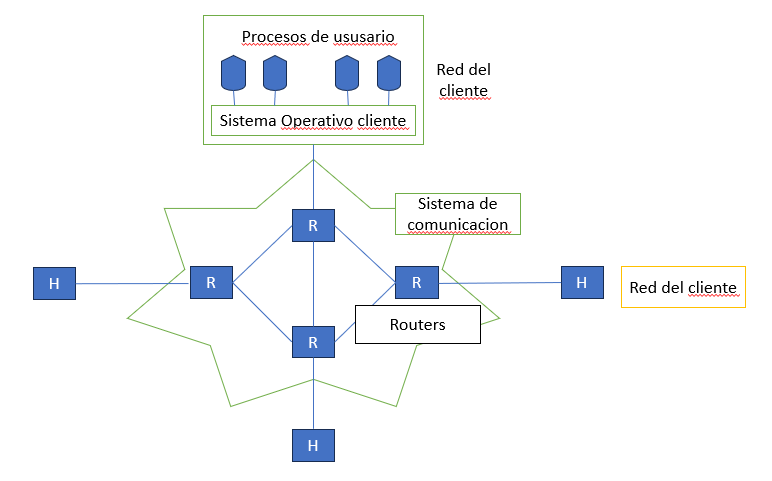


Ilustración 2 - Proceso de comunicación en red de área amplia

Estructura de comunicación

Resolución de nombres de dominio DHCP

Protocolos de comunicion

TCPO/IP

------------------------------------------------------------------------------------------------------------------------------------------

Nota\*\* Arquitectura CISCO ACE

La gestión de una WAN de gran tamaño se ha caracterizado siempre por ser costosa e inflexible, pero las características de la tecnología SD-WAN hacen más simple y barata la administración de los dispositivos de red, permite configuraciones de forma remota y están diseñadas para que el sistema ejecute de forma automática la elección de la ruta más eficiente tomando decisiones inteligentes, reduciendo costos y mejorando el rendimiento de la red.

Redes Activas

El despegue de Internet, a principio de los 90, provocó que las aplicaciones antiguas fueran superadas por otras más novedosas. El aumento del uso de estas llevó a los investigadores a diseñar y probar nuevos protocolos de red. Sin embargo, después de este proceso, estos protocolos debían ser estandarizados por el IETF, proceso muy lento que frustraba a muchos investigadores.

Como respuesta, algunos investigadores apostaron por un enfoque de apertura del control de las redes, análogo a reprogramar un PC autónomo con relativa facilidad.

Como las redes convencionales no son programables, surgieron las redes activas orientadas hacia el control de la red, conceptualizando una interfaz de programación (API) que expone los recursos (procesamiento, almacenamiento, colas de paquetes, etc) en nodos de red individuales y soporta la construcción de funcionalidades personalizadas para aplicar a un subconjunto de paquetes que pasan a través del nodo.

Sin embargo, había muchos otros que defendían la simplicidad de la red como única forma de que Internet tuviese éxito.

El programa de investigación de las redes activas se dedicó por lo tanto, a explorar alternativas a los servicios proporcionados por Internet vía IP o ATM.

El impulso tecnológico que alentó a las redes activas permitió reducir el coste computacional, avanzar en lenguajes de programación y en la tecnología de máquinas virtuales. Un catalizador importante en este ecosistema fue el aumento de interés de agencias, que supuso la creación de programas como el Active Networks program del DARPA, desde mediados de los 90 hasta principios de los 2000.

Las redes activas, por lo tanto, aunque no tuvieron un despliegue extendido, ofrecieron contribuciones relacionadas con SDN como funciones programables en la red, virtualización de redes y la visión de una arquitectura unificada en distintos aparatos de red como cortafuegos, IDS, NAT, etc.

Separación de plano de control y datos

Los enrutadores y conmutadores convencionales, tenían una estrecha integración entre los planos de control y de datos, que realizaba depuración de problemas de configuración o control del comportamiento del enrutamiento, una tarea muy desafiante y complicada. La separación de ambos planos tiene distintos enfoques.

Debido al crecimiento de Internet, las empresas de equipos hardware comenzaron a implementar la lógica de reenvío de paquetes en hardware (plano de datos), separada del plano de control y los ISPs a luchar para poder gestionar sus redes crecientes y poder aportar a sus clientes servicios que las hiciesen más seguras (como las VPN).

Todo esto dio lugar a dos innovaciones principales: una interfaz abierta entre ambos planos, como ForCES (separación del elemento de control y reenvío) estandarizada por la IETF y la interfaz Netlink a la funcionalidad de reenvío de paquetes a nivel de núcleo Linux; y un control lógico centralizado de la red, como con RCP (plataforma de control de enrutamiento), arquitecturas SoftRouter y el protocolo PCE (Path Computation Element) del IETF, ambos conceptos clave en diseños futuros de SDN.

Aparición de la API

Para abordar la visión de separación de plano de datos y de control, se empezó a investigar nuevas arquitecturas para control lógico centralizado. El proyecto 4D, uno de los frutos de estas investigaciones, establecía cuatro capas principales: el plano de datos, para procesar paquetes basándose en reglas configurables; el plano de descubrimiento, encargado de coleccionar medidas topológicas y del tráfico; el plano de diseminación, para instalar reglas de procesado de paquetes; y el plano de decisión, que consistía en controladores lógicos centralizados que convertían objetivos a nivel de red en estado de manejo de paquetes. Numerosos grupos de investigación comenzaron el desarrollo de sistemas basados en este enfoque, y en particular, el proyecto Ethane, y su predecesor directo SANE. El despliegue operacional de este proyecto en la universidad de Stanford, comenzó la etapa de creación de Openflow, y en particular, el diseño simple de switch del proyecto Ethane, se convirtió en la base de la API de Openflow.

A mediados de la primera década del siglo xxi, diversos grupos de investigación y empresas empezaron a interesarse por la experimentación de redes a escala, debido al éxito de infraestructuras experimentales como PlanetLab y Emulab, y la disponibilidad de más fondos por parte del gobierno para invertir en este sector. Uno de los resultados de este entusiasmo fue la creación de GENI (Global Environment for Networking Innovations) y el programa EU FIRE. Al mismo tiempo, en la universidad de Stanford, un grupo de investigadores creó el Clean Slate Program, enfocado en la experimentación en redes universitarias más tratables y locales, que dio lugar al protocolo Openflow.

Gracias a la adopción de Openflow en las empresas, que abrieron sus API para permitir a los programadores controlar ciertos comportamientos de reenvío, la versión inicial de este protocolo se estableció en los switches a través de una simple actualización de firmware, sin necesidad de actualizar el hardware.

Openflow, aunque utilice muchos de los principios de anteriores trabajos en la separación de planos, también aporta bastantes contribuciones como la generalización de dispositivos de red y funciones, la visión de un sistema operativo de red y técnicas de gestión distribuida del estado de aparatos de red entre otras.

Beneficios SDN

SDN no es OpenFlow

OpenFlow es un estándar abierto para un protocolo de comunicaciones que permite al plano de control interactuar con el plano de datos, no es el único protocolo disponible o en desarrollo para SDN y se está convirtiendo en el modelo estándar de implementación.

Conceptos SDN

Las redes definidas por software (SDN) constan de una arquitectura de red cuyo dinamismo, manejabilidad, rentabilidad y adaptabilidad permiten que sea adecuada para la naturaleza dinámica y de alto consumo de ancho de banda de las aplicaciones modernas. Como hemos visto en apartados anteriores, SDN separa el control de la red de las funciones de reenvío con una API bien definida entre ambos, permitiendo la programabilidad del control de red y la abstracción de la infraestructura subyacente.

Funcionamiento del SND

Los proveedores de redes SDN ofrecen una amplia variedad de arquitecturas competentes, centradas en el objetivo comentado anteriormente: separar el plano de control del plano de datos, y formadas por un controlador SDN, una API hacia el sur (southbound API) y una API hacia el norte (northbound API).

Controlador SDN

Los proveedores de redes SDN ofrecen una amplia variedad de arquitecturas competentes, centradas en el objetivo comentado anteriormente: separar el plano de control del plano de datos, y formadas por un controlador SDN, una API hacia el sur (southbound API) y una API hacia el norte (northbound API).

Northbound y southbound

Como comentábamos en el subapartado anterior, estas interfaces sirven para conectar el controlador SDN a los aparatos de red por debajo (sur) y por otro a los servicios y aplicaciones por encima (norte). Las API sur facilitan el control en la red, permitiendo al controlador realizar cambios dinámicos de acuerdo a las demandas en tiempo real y las necesidades. Openflow, desarrollado por la ONF (Open Networking Foundation) es la primera y más conocida de estas interfaces. Además de esta, Cisco OpFlex es otra bien conocida.

Las API norte en cambio, pueden ser usadas para facilitar la innovación y permitir la organización y automatización de la red para suplir las necesidades de las diferentes aplicaciones a través de la programabilidad de la red SDN. Se podría decir que estas interfaces son las más críticas en un entorno SDN, debido a que soportan una gran variedad de aplicaciones y servicios por encima y por lo tanto con algunas de ellas no funciona correctamente. Hay una amplia variedad de posibles interfaces de este tipo situadas en diferentes lugares de la pila para controlar los diferentes tipos de aplicaciones a través del controlador SDN. Sin embargo, estas interfaces son el componente más indeterminado de todo el entorno SDN, lo que ha resultado en un enfoque por parte de la ONF hacia este componente.

Modelos de despliegue de SDN

Hay dos modelos: proactivo y reactivo. Cuando un flujo llega a un switch se realiza un mapeo de la tabla de flujos. En el caso de que no se encuentre coincidencia, se envía una petición al controlador para instrucciones más extensas. En modo reactivo, el controlador actúa después de estas peticiones y crea una regla en la tabla de flujos para el paquete correspondiente si es necesario. En modo proactivo, sin embargo, el controlador llena entradas de la tabla de flujos para cada posible coincidencia de tráfico para ese switch, algo parecido con las típicas entradas de tablas de enrutamiento. Además de estos modelos por separados, se puede combinar en una red ambos modelos en forma de un híbrido, para aportar las ventajas de ambos.

Programabilidad de modelos SDN

Gran parte de la programabilidad en SDN, reside en las API abiertas norte y sur. La promesa de SDN de crear una infraestructura mucho más ágil y flexible es desarrollada principalmente mediante la transformación de la red a una más programable. Existen tres ejemplos principales de uso, para establecer qué significa programabilidad para las redes SDN:

Ajustar los flujos. Este caso se centra en protocolos, como Openflow, que permiten a los controladores SDN interacción con los aparatos de red en el plano de datos para ajustar cómo el tráfico fluye por la red, ayudando a resolver las demandas en esta.

Soporte de aplicaciones. Este caso, se preocupa por la coordinación, automatización (para poder desplegar rápidamente gran número de aplicaciones y servicios nuevos) y el manejo de excepciones de una red, para acompasar mejor las necesidades de las aplicaciones que corren en ella.

Automatización de las redes. Este último caso, se centra en la no interferencia del administrador de la red en las acciones que realiza la red de forma automática cuando algún problema sucede (cuando algo sucede, la inteligencia de la red se debe encargar de ello).

Desafios de seguridad en entornos SDN

La seguridad, como en todo tipo de redes, es un aspecto crucial en redes SDN, para proteger la disponibilidad, integridad y privacidad de la información que transporta. La seguridad en estas redes, aunque existen enfoques competentes, todavía está en juego, ya que estos enfoques no convergen en una idea común. A pesar de estas diferencias, es claro, que las soluciones deben crear un entorno escalable, eficiente y seguro. Además, la seguridad debe ser simple de configurar (debido al dinamismo de la red) y efectiva (para asegurar que pueda desplegarse en cualquier parte). En la arquitectura, hay varios elementos que deben ser protegidos y acciones a llevar a cabo:

Asegurar y proteger el controlador. Debido a que es el centro de control y decisión de la red, debe ser cuidadosamente controlado. Además, si se produce por ejemplo un ataque DDoS al controlador y cae víctima de este, la red cae con él, por lo que debe estar protegido con los mecanismos de seguridad necesarios para afianzar su disponibilidad continua.

Privacidad e integridad. La protección de las comunicaciones en la red es crítica, por lo que se debe asegurar el controlador, las aplicaciones que carga y los dispositivos de red que gestiona y autenticar, estableciendo unos mecanismos que permitan que son quien dicen ser y además funcionan correctamente.

Crear un entorno de desarrollo de política robusto. Es necesario estar seguro de que el controlador (y demás dispositivos) están haciendo lo que queremos que hagan, por lo que habrá que realizar comprobaciones continuas de los sistemas en general.

Llevar a cabo análisis forenses de la red. Para poder determinar, en caso de un ataque, quién lo realizó, reportarlo y proteger la red de cara al futuro.14​

Open network fundation

La Open Networking Foundation (ONF) es una organización impulsada por los usuarios dedicada a la promoción y adopción de SDN a través del desarrollo de estándares abiertos. Esta organización, enfatiza la colaboración y el proceso abierto de desarrollo conducido por los usuarios, dando como resultado el mantenimiento del estándar abierto Openflow, el primer estándar SDN y un elemento vital para las arquitecturas abiertas de SDN.

Hoy en día las comunidades de esta organización siguen analizando los requerimientos de SDN y mejorando el estándar Openflow, para beneficiar SDN con nuevos estándares y suplir las necesidades de despliegues comerciales.

Bibliografia

https://es.wikipedia.org/wiki/Redes\_definidas\_por\_software