Entrega: Proyecto de Investigación

Redes Definidas por Software

Alumno: Alejandro Vargas Mena

20160110239

Universidad Latina de Costa Rica

San Pedro

Sistemas Operativos 2 – BIT-28

Profesor: Ing. Carlos Andrés Méndez

20-4-2024

Introducción

La configuración de redes en las empresas medianas y grandes a sido de mucha importancia para la segmentación, virtualización y envío de tráfico a la red global utilizando medios de traducción y distribución para el eficiente manejo y la trayectorias mas cortas que se pueden acceder durante el desplazamiento de las tramas a través de las redes mundiales con el propósito de enlazar y comunicar dispositivos, sean de almacenamiento, presentación de información mediante navegadores o aplicaciones disponibles en los dispositivos sean teléfonos celulares computadoras, con o sin interfaz grafica, con la disponibilidad de ejecutar programas configurados para funciones específicas, en las redes se implementan practicas o pruebas de configuración de dispositivos encargados de dirigir el tráfico de red usando programación para simular diversos dispositivos de una red y fluir trafico de red por medio de ellos para generar tratamientos especializados de calidad, enrutamiento entre varias funciones, para beneficio de todos, hoy en día el software basado en redes toma una gran importancia, en Costa Rica el pasado Enero en el día 5, se inauguro la primer torre 5G en el campus de la Universidad de Costa Rica liderada por equipos del ICE, este tipo de tecnología involucra a un volumen más amplio la el software basado en redes para el monitoreo de inmensa cantidad de dispositivos, motivo por el cual está diseñado la red 5G.

Método

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

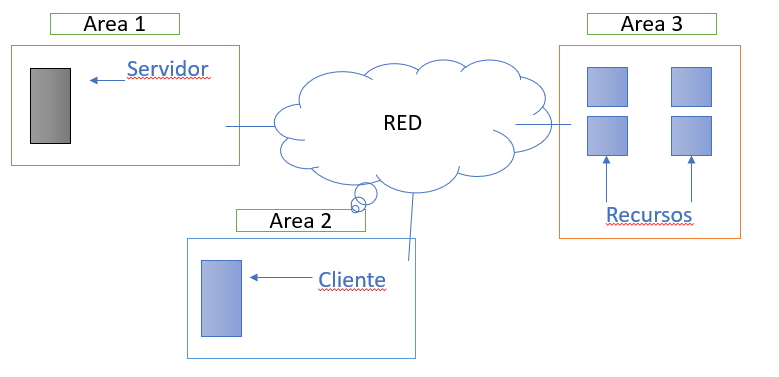


Ilustración 1 - Sistema distribuido Cliente-Servidor

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.

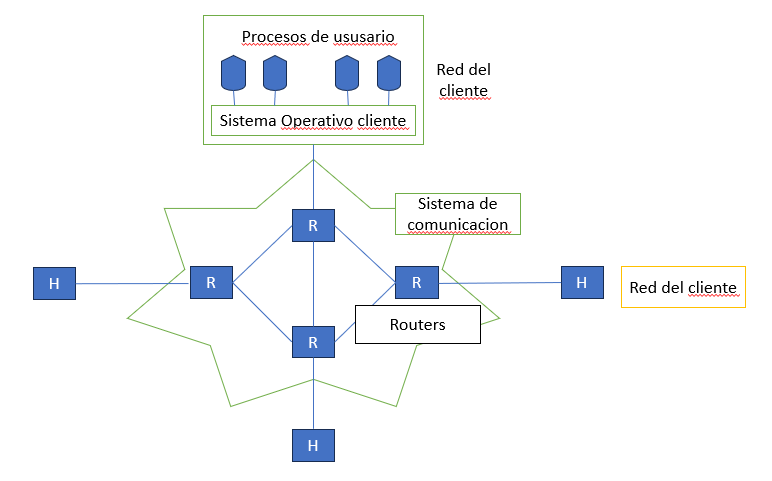


Ilustración 2 - Proceso de comunicación en red de área amplia

Estructura de comunicación

Resolución de nombres de dominio DHCP

Protocolos de comunicion

TCPO/IP

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

Nota\*\* Arquitectura CISCO ACE

Las redes definidas por software son un conjunto de técnicas relacionadas con el área de redes computacionales, cuyo objetivo es facilitar la implementación e implantación de servicios de red de manera determinista, dinámica y escalable. Todo esto se consigue mediante la separación de los planos control y de datos.

Utilizan un enfoque pensado para el sector empresarial que pueda optimizar los recursos disponibles y mejore las comunicaciones al momento de enrutar el tráfico, esto mediante el uso de software para priorizar y ordenar el tráfico de la red, que de forma general envía el uso de ciertas aplicaciones a través de determinadas conexiones, considerando métricas como la velocidad, latencia y consumo que demandan estas aplicaciones. El flujo de la información y la tecnología SD-WAN es la autoridad encargada de poner orden asegurando un flujo adecuado ahorrando recursos.

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.

Historia

Gracias a SDN, el diseño y gestión de redes se ha vuelto más innovador en los últimos años.

Sin embargo, esta tecnología no es resultado de una súbita aparición, sino de una larga historia de innovaciones dirigidas a hacer más programables las redes.

La historia de SDN comienza 20 años atrás, más o menos en el comienzo de lo que hoy conocemos como Internet, el cual, debido a su éxito, intensificó la necesidad de gestionar y evolucionar las infraestructuras de redes, es decir, hacerlas programables.

A partir de este momento, la historia se divide en tres etapas diferenciadas:

\* redes activas (1995 a 2000 aprox.),

\* separación de planos de control y datos (2001-2007 aprox.)

\* la aparición de la interfaz de programación de aplicaciones de Openflow (2007-2010 aprox.).

​ En 2014 Avaya hizo una demostración de redes definidas por software usando Shortest Path Bridging y OpenStack, eliminando la configuración manual

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.

¿Porque SDN?

Limitaciones en las tecnologías de redes actuales

Hacer frente a los requerimientos de telecomunicaciones por parte del público mundial, es imposible con las redes tradicionales. Los departamentos de IT de infinidad de empresas y proveedores de servicios de redes, están intentando aprovechar al máximo sus redes, invirtiendo gran parte de sus beneficios en esta tarea. Sin embargo, esta es una solución temporal, ya que de ninguna manera las arquitecturas de red actuales están diseñadas para conocer los requerimientos actuales de usuarios, empresas y proveedores. Las limitaciones de las redes actuales incluyen:

\* Complejidad: para acomodar las redes a las necesidades de sus usuarios en general, la industria ha mejorado los protocolos de red para ser más seguros y eficientes.

Los protocolos tienden a ser definidos en aislamiento, sin embargo, con cada uno resolviendo un problema específico y sin el beneficio de una acción conjunta (abstracciones).

\* Políticas incoherentes: para implementar una política que abarque a la red completamente, los administradores de red, deben configurar miles de mecanismos y aparatos.

**Por ejemplo**, todas las veces que una nueva máquina virtual se introduce en la red, puede llevar (en el peor de los casos) horas, hasta que el administrador encargado reconfigura las listas de acceso (ACL) en toda la red.

\* Imposibilidad de escalabilidad: a la vez que las demandas de centros de datos aumentan rápidamente, la red debe crecer de la misma forma. Sin embargo, la red se vuelve más compleja con la suma de cientos de miles de aparatos de red que deben ser configurados y gestionados.

\* Dependencia del vendedor: las nuevas capacidades y servicios perseguidas por proveedores y empresas en respuesta rápida a las necesidades dinámicas de negocios y demanda de clientes, se ven frenadas por los ciclos de producción de los equipamientos por parte de los vendedores, que pueden abarcar hasta más de tres años.

Necesidad de una nueva red arquitectónica

Los servicios de red surgidos en los últimos tiempos, están llevando a las redes tradicionales a sus límites. Algunos de los elementos que están llevando a la necesidad de una nueva arquitectura de red son los siguientes:

\* Heterogeneidad en los patrones de tráfico: en contraposición con las aplicaciones cliente-servidor en las que la gran parte de la comunicación ocurre entre un cliente y un servidor, las aplicaciones modernas crean tráfico máquina a máquina mediante accesos a bases de datos y servidores, antes del retorno de los datos al usuario final. Además, los usuarios están cambiando los patrones de tráfico, al poder conectarse desde cualquier punto en cualquier momento en determinadas redes inalámbricas.

\* Aumento de carga de trabajo considerable de los administradores de red: los administradores se ven bajo presión a la hora de proteger los datos de los usuarios y mantener la seguridad en las redes, mientras nuevos dispositivos móviles, como teléfonos inteligentes y tabletas, acceden a la red.

\* El aumento de los servicios basados en la nube: este aumento, principalmente debido a la gran acogida por parte de las empresas en el plano público y privado, junto a la necesidad actual de aumentar la agilidad de acceso a aplicaciones, infraestructuras y otros recursos de telecomunicaciones y junto a la complejidad de mejorar la seguridad de estos servicios, requieren una escalabilidad dinámica de la capacidad de cómputo, almacenamiento y recursos de red.

\* Big data y el aumento de ancho de banda requerido: manejar un big data actualmente requiere procesamiento masivo por parte de miles de servidores y su aumento demanda ancho de banda a los ISP.

Beneficios SDN

Además de ofrecer redes centralizadas programables que pueden atender dinámicamente las necesidades de las empresas, SDN provee los siguientes beneficios:

\* Reduce el Capex (Capital Expenditures): mediante la posibilidad de reutilizar el hardware existente, SDN limita la necesidad de invertir en hardware nuevo.

\* Reduce el Opex (Operating Expense): SDN permite control algorítmico de la red, en enrutadores y puentes (hardware y software) que cada vez son más programables, haciendo más sencillo la configuración y gestión de las redes. Además, esto permite una reducción del tiempo de gestión por parte de los administradores, lo que reduce la probabilidad de error humano.

\* Agilidad y flexibilidad: SDN permite a las organizaciones desplegar aplicaciones, servicios e infraestructuras rápidamente para alcanzar los objetivos propuestos por empresas en el menor tiempo posible.

\* Permite innovación: permite crear nuevos tipos de aplicaciones y modelos de negocio por parte de las empresas, que las beneficia y aumenta el valor de sus redes.

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.

Arquitectura SDN

Aunque la ONF está continuamente modificando la terminología, los términos más comunes para los componentes de esta arquitectura son los siguientes:

\* Aplicación SDN (SDN App): las aplicaciones SDN son programas que directamente comunican las necesidades y los comportamientos deseados de su red al controlador SDN a través de los NBI. Están formadas por una lógica de aplicación y uno o más NBI.

\* Controlador SDN (SDN Controller): entidad lógica de control encargada de traducir las peticiones de la aplicación SDN a las rutas de datos más abajo, dando a la capa de aplicación una visión abstracta de la red mediante estadísticas y posibles eventos. Un controlador SDN consiste en uno o más NBIs, la lógica de control SDN y el CDPI driver.

\* Ruta de datos SDN (SDN Datapath): componente lógico que expone visibilidad y control sobre sus capacidades de reenvío y procesamiento. La representación lógica, por lo tanto, puede abarcar todos o un subconjunto de los recursos físicos. Está formado por un agente CDPI, un conjunto de motores de reenvío y de funciones de procesamiento, que incluyen simples reenvíos entre interfaces externas de esta y procesamiento interno del tráfico. Las rutas de datos pueden contenerse en un único elemento de red (físico).

Interfaz SDN del plano de control al plano de datos (SDN Control to Data-Plane Interface, CDPI): interfaz entre el controlador y la ruta de datos, que provee programabilidad a la hora del reenvío, anuncio de capacidades, reporte estadístico y notificación de eventos.

Interfaces hacia el norte SDN (NBI): son interfaces entre las aplicaciones SDN y los controladores que proveen vistas abstractas del comportamiento de la red y sus requerimientos.

Conductores y agentes de interfaz (Interface Drivers & Agents): cada interfaz es implementada por un par de este tipo, que representa el fondo (relacionado con la infraestructura) y la cima (relacionada con la aplicación).

Gestión y administración (Management & Admin): el plano de gestión cubre tareas estáticas, manejadas mejor fuera de los planos de aplicación, control y datos, como la asignación de recursos a los clientes, la configuración de equipos físicos y la concordancia entre alcanzabilidad y credenciales entre entidades físicas y lógicas.

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

Resultados

Discusión

Referencias

Notas

Tablas

Figuras

Apendice

Errores encontrados

Error al emplear repositorios de Docker en el JA\_PC



Error al crear un nodo en el plano: Intalar TigerVNC server después de usar el soporte VNC

