

Conmutación y redes.

Luis Alberto Vargas González.

Ensayo Administración de una red.

Fecha: 03/05/2022

**QoS en la red.**

En las modernas redes de internet y conexiones de telecomunicaciones se deben de considerar 4 partes para poder llevar a cabo una inspección de calidad de dichas redes, ellos son:

1. Bandwidth (ancho de banda).
2. Delay(retardo).
3. Jitter (Fluctuación).
4. Loss (perdida de paquetes. )

Esto nos indica que con cada uno de estos aspectos cuidadosamente seleccionados y depurados, podremos brindar una calidad de servicio (como su nombre lo indica) de la interconexión de datos y además indican la habilidad, pericia, y buena atención por parte del técnico o ingeniero en redes sobre como ha resuelto las necesidades de dicho cliente o clientes acerca de la interconexión de dicha red.

Todo esto aunado además a la facilidad de escalabilidad que debe de tener una red, pues como sabemos las redes y las necesidades de los usuarios de las mismas, irán evolucionando, cada vez se requerirán mas datos que interconectar, mas datos que analizar o mandar, o mas usuarios simultáneos que conectar por igual, por lo que la exigencia de dichas redes por igual subirá de categoría y será necesario actualizar equipos de la infraestructura, como hardware y software de los mismos, así como los routers, switches pueden necesitar ser aumentados o disminuidos según sea el caso.

Además se cuenta con el beneficio de poder disfrutar de un servicio bien integrado de opciones de conectividad en cada caso.

**Administración de redes**

Para poder administrar de una manera efectiva nuestras redes de telecomunicaciones; existen distintas herramientas con las cuales podremos de una manera efectiva medir, identificar, corregir cierta cantidad de errores y analizar dispositivos en la red entre otros propósitos.

CDP:

Se usa para descubrir y detallar otros dispositivos conectados a la misma fuente de conexión y cableado de la red, y además de eso, envía mensajes entre ellos para la verificación de su conexión y estado.

Puede ayudar a tomar mejores decisiones en el diseño y depuración de la red en sí, y para analizar dichos dispositivos en red.

LLDP:

A diferencia del método anterior, lldp no se limita a uso exclusivo de dispositivos cisco, por lo que se puede usar en prácticamente cualquier desarrollador de telecomunicaciones y en sus dispositivos.

NTP:

Es un servidor que funciona para poder verificar, actualizar o corregir (según sea el caso) la hora y fecha determinada en un dispositivo, debido a que es más preciso y fácil de utilizar que el método manual.

Esta es una actividad muy importante que realizar y verificar ya que muchos problemas de conectividad requieren del uso del reloj del software para poder hacer mediciones y para correcciones.

SNMP:

Llamado Protocolo Simple de Administración de redes es un protocolo de capa de aplicación y da una forma de comunicación entre administradores y agentes.

Consta de 3 elementos:

* 1. Administradores
  2. Agentes
  3. Base de información de admin.

Los hay de 3 versiones, la SNMPv1, v2 y v3.

Los agentes SNMP que residen en los dispositivos administrados recopilan y almacenan información sobre los dispositivos y su funcionamiento. El agente almacena esta información localmente en la MIB. El administrador de SNMP luego usa el agente SNMP para tener acceso a la información dentro de la MIB.

Existen dos solicitudes principales de administrador de SNMP: get y set. NMS usa una solicitud get para solicitar datos al dispositivo. NMS usa una solicitud "set" para cambiar las variables de configuración en el dispositivo de agente. Una solicitud set también puede iniciar acciones dentro de un dispositivo. Por ejemplo, una solicitud set puede hacer que un router se reinicie, que envíe o que reciba un archivo de configuración. El administrador de SNMP utiliza las acciones de las solicitudes get y set para realizar las operaciones descritas en la tabla.

Syslog:

Este es un notificador de mensajes y errores o posibles errores de los componentes de una red; analógicamente se puede comparar a la luz de un salpicadero de auto, donde se informa de algún error en especial.

El servicio de registro de syslog proporciona tres funciones principales:

* 1. La capacidad de recopilar información de registro para el control y la solución de problemas
  2. La capacidad de escoger el tipo de información de registro que se captura
  3. La capacidad de especificar los destinos de los mensajes de syslog capturados

Hay varios lugares donde se muestran los mensajes:

1. Bufer de registro.
2. Linea de consola
3. Linea de terminal
4. Servidor de syslog.

**Diseño de red.**

El diseño de una red es uno de los aspectos mas vitales e importantes para poder implementar una funcionalidad correcta a pequeño, mediano y largo plazo de esa misma red, teniendo así en cuenta que la escalabilidad es el aspecto fundamental de dicho tema.

Cisco tiene una implementación llamada: Redes conmutadas sin límites, la cual puede combinar intranets y subredes dentro de una misma área y esas mismas subredes e intranets se pueden interconectar a otras en distintas áreas geográficas.

1. Jerarquía - facilita la comprensión de la función de cada dispositivo en cada nivel, simplifica la implementación, el funcionamiento y la administración, y reduce los dominios de error en cada nivel.
2. Modularidad - permite la expansión de la red y la habilitación de servicios integrados sin inconvenientes y a petición.
3. Capacidad de recuperación - satisface las expectativas del usuario al mantener la red siempre activa.
4. Flexibilidad - permite compartir la carga de tráfico de forma inteligente mediante el uso de todos los recursos de red.

Existen 3 capas de funcionamiento de dicha tecnología.

1. Capa de acceso

La capa de acceso representa el perímetro de la red, por donde entra o sale el tráfico de la red del campus.

1. Capa de disribución

La capa de distribución interactúa entre la capa de acceso y la capa de núcleo para proporcionar muchas funciones importantes, incluidas las siguientes:

Agregar redes de armario de cableado a gran escala.

Agregar dominios de broadcast de Capa 2 y límites de enrutamiento de Capa 3.

Proporcionar funciones inteligentes de switching, de enrutamiento y de política de acceso a la red para acceder al resto de la red.

Proporcionar una alta disponibilidad al usuario final mediante los switches de capa de distribución redundantes, y rutas de igual costo al núcleo. Proporcionar servicios diferenciados a distintas clases de aplicaciones de servicio en el perímetro de la red.

1. Capa de núcleo central

La capa de núcleo es el backbone. Esta conecta varias capas de la red de campus

Como se pudo constatar el diseño de la red es uno de los elementos fundamentales de la implementación de la red, un correcto diseño de red nos dará a futuro soluciones de escalabilidad de red para requerimientos futuros.

**Resolución de problemas de red.**

Documentacion de red:

La documentación de red común incluye lo siguiente:

Diagramas lógicos y físicos de topología de la red

Documentación de dispositivos de red que registra toda la información pertinente del dispositivo

Documentación de referencia del rendimiento de la red

Diagramas de topología:

1. Topología física
2. Topología lógica ipv4
3. Topología lógica ipv6

Línea base:

Una línea de base se utiliza para establecer el rendimiento normal de la red o del sistema, para determinar la "personalidad" de una red en condiciones normales.

Para establecer una línea de base de rendimiento de la red, es necesario reunir datos sobre el rendimiento de los puertos y los dispositivos que son esenciales para el funcionamiento de la red.

Una línea de base debería responder las siguientes preguntas:

¿Cómo funciona la red durante un día normal o promedio?

¿Dónde ocurre la mayoría de los errores?

¿Qué parte de la red se usa con más frecuencia?

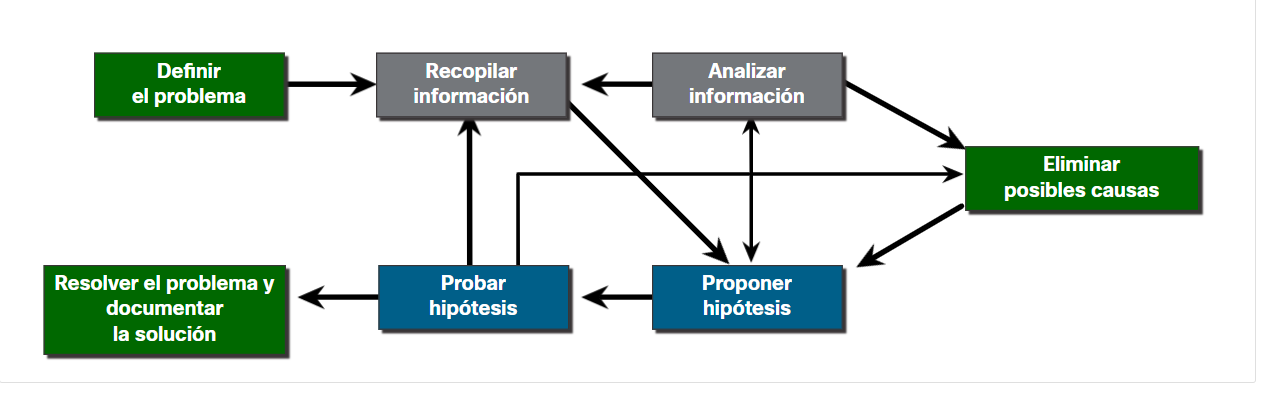
¿Qué parte de la red se usa con menos frecuencia?

Existen 3 pasos para determinar esta tarea:

1. Determinar el tipo de info a recopilar.
2. Identificar dispositivos y puertos de interés.
3. Determinar la duración de la línea base.

Proceso de resolución de problemas:

Se explica a grandes rasgos la metodología por la cual se hace la solución de problemas de redes:



1. Definir el problema: se trata de hacer el análisis adecuado del problema a tratar, este al ser el paso fundamental, es un paso de extrema importancia ya que sin el, los demás pasos no pueden ser hechos.
2. Recopilar información: se refiere a la colección y análisis de datos de dicho problema dado, como las bases de datos implicadas en el proceso de hardware o software, así como comportamientos de los mismos.
3. Analizar información: proceso mediante el cual se trata de definir a detalle el o los problemas dados.
4. Proponer hipótesis: es el proceso mediante el cual se da una solución aproximada a la ideal para poder dar una solución.
5. Probar hipótesis: proceso donde se pone a prueba dicha solución, en caso de Los routers también cumplen otras funciones útiles:

Ofrecen contención de broadcast limitando estos a la red local Interconectan sitios separados geográficamente.

Puede agrupar usuarios de manera lógica, ya sea por aplicación o departamento, los cuales requieren acceso a los mismos recursos.

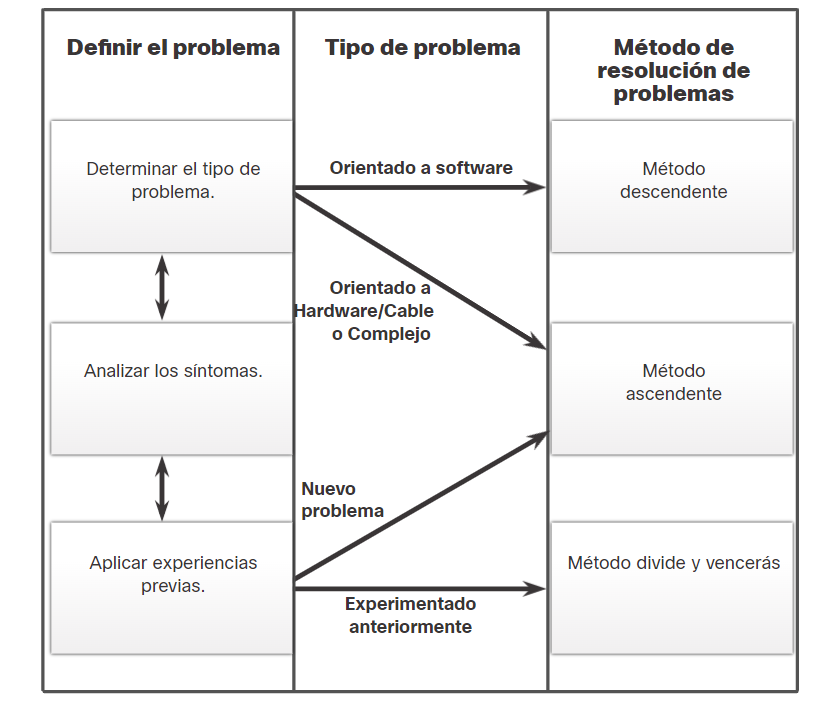
Ellos brindan seguridad mejorada, mediante el uso de ACL para filtrar el trafico no deseado.

1. Resolver el problema y documentarlo: es necesario que después de resolver el problema se adhiera a una base de datos del problema para su futura revisión en caso de ser necesario.

Métodos estructurados de resolución de problemas:

1. Ascendente.
2. Descendente.
3. Divide y vencerás.
4. Seguimiento de ruta
5. Sustitución.
6. Comparación.
7. Deducción informada.

**Pautas para seleccionar un método de resolución de problemas.**

****

**Herramientas para resolución de problemas.**

Existen varias herramientas para poder generar una solución a problemas entre ellas:

1. NMS; Herramientas del sistema de administración de red
2. Bases de conocimientos.
3. De línea de base.
4. Analizador de protocolos.
5. De hardware:
   1. Multimetro digital.
   2. Comprobadores de cables.
   3. Analizador de cables.
   4. Analizadores de red portátiles.
   5. Cisco prime NAM
6. Servidor Syslog.

**Síntomas y causas de problemas en la red.**

Existen muchos tipos de problemas relacionados a una red, cada uno de ellos esta catalogado en distintas partes de las capas de telecomunicaciones del modelo osi.

**Virtualización en la red.**

Como se pudo constatar en este tema de virtualización, la computación en la nube es uno de los avances tecnológicos más importantes de la última década del siglo 21, debido a que el término de “computación en la nube “es relativamente nuevo, muchas personas lo conocen y lo han utilizado, sin embargo, no es un término difundido alrededor del mundo, existe aun un gran porcentaje de desconocimiento de dicha tecnología.

La computación en la nube aborda una variedad de problemas de administración de datos:

1. Permite el acceso a los datos de organización en cualquier momento y lugar.
2. Optimiza las operaciones de TI de la organización suscribiéndose únicamente a los servicios necesarios.
3. Elimina o reduce la necesidad de equipos, mantenimiento y administración de TI en las instalaciones.
4. Reduce el costo de equipos y energía, los requisitos físicos de la planta y las necesidades de capacitación del personal.
5. Permite respuestas rápidas a los crecientes requisitos de volumen de datos

Existen además 3 tipos de servicios en la nube, cada uno de ellos se diferencia del otro en cuanto sus características se refieren:

1. Software como servicio (SaaS) - El proveedor de la nube es responsable del acceso a los servicios, como correo electrónico, comunicaciones y Office 365, que se proporcionan por Internet. El usuario no administra ningún aspecto de los servicios en la nube, excepto la configuración limitada de la aplicación específica del usuario. El usuario sólo necesita proporcionar sus datos.
2. Plataforma como un Servicio (PaaS) - El proveedor de la nube es responsable del acceso a las herramientas y los servicios de desarrollo utilizados para distribuir las aplicaciones. Estos usuarios suelen ser programadores y pueden tener control sobre la configuración del entorno de alojamiento de aplicaciones del proveedor de nube.
3. Infraestructura como servicio (IaaS) - El proveedor de la nube es responsable del acceso a los equipos de la red, los servicios de red virtualizados y el soporte de infraestructura de la red. El uso de este servicio en la nube permite a los administradores de TI implementar y ejecutar código de software, que puede incluir sistemas operativos y aplicaciones.

Además hay 4 modelos generales de nube:

1. Publica.
2. Privada
3. Comunitaria
4. Híbrida

La virtualización es la base de la computación en la nube esto no es al revés como mucha gente cree. Sin esta base, la computación en la nube que se implementa masivamente no sería posible.

La virtualización separa el sistema operativo (SO) del hardware. Varios proveedores ofrecen servicios virtuales en la nube que permiten aprovisionar servidores de manera dinámica según sea necesario.

Además de todas estas características definidas; la virtualización tiene sus ventajas; que; están definas en sectores de sus consumos de distintas fuentes y de tiempo de procesos; entre ellas:

1. Menos cantidad de equipos necesarios: La virtualización permite la consolidación de servidores, lo que reduce la cantidad necesaria de servidores físicos, dispositivos de red e infraestructura de soporte. También significa menores costos de mantenimiento.
2. Menor consumo de energía: La consolidación de servidores reduce los costos mensuales de alimentación y refrigeración. El consumo reducido ayuda a las empresas a alcanzar una huella de carbono más pequeña.
3. Menos espacio necesario: La consolidación de servidores con virtualización reduce la huella total del centro de datos. Menos servidores, dispositivos de red y racks reducen la cantidad de espacio de piso requerido.

Existen además una tecnología de red y de virtualización llamada Hipervisores, los cuales hay de 2 tipos; los de versión 1 y de versión 2, los cuales son una herramienta que ayuda a controlar ya sea el hardware de servidores de la virtualización en el tipo 1, o a emular los componentes físicos de los mismos para poder crear instancias de VM (máquinas virtuales) y de esta manera poder crear varios servicios de software estructurados en una misma computación.

Hay 2 tecnologías de virtualización de redes específicamente las cuales son:

1. Redes definidas por software (SDN): una arquitectura de red que virtualiza la red, ofreciendo un nuevo enfoque para la administración y administración de redes que busca simplificar y optimizar el proceso de administración.
2. Infraestructura centrada en aplicaciones (ACI) de Cisco - Solución de hardware diseñada específicamente para integrar la computación en la nube con la administración de centros de datos.

El controlador de SDN es una entidad lógica que permite que los administradores de red administren y determinen cómo el plano de datos de switches y Reuters debe administrar el tráfico de red. Coordina, media y facilita la comunicación entre las aplicaciones y los elementos de red.

Hay 3 tipos de sdn:

1. Basados en dispositivos.
2. Basados en controladores.
3. Basados en políticas.

Cisco APIC-EM es un ejemplo de SDN basado en políticas. Cisco APIC-EM proporciona una interfaz única para la administración de red que incluye:

1. descubrir y acceder a los inventarios de dispositivos y hostes,
2. ver la topología (como se muestra en la figura),
3. trazar una ruta entre los puntos finales, y establecer políticas.

**Automatización de la red.**

Como se pudo revisar en el tema, la automatización de la red es una de las tantas aplicaciones lógicas que se tienen implementadas en las actuales tecnologías de automatización, por lo cual en este tema se revisa solo y exclusivamente el uso de la automatización en reses, sin embargo, la automatización se puede aplicar a un sinfín de actividades extra y sin ninguna relación a la red o a conmutación.

Existen además una cantidad muy grande formatos de presentación de datos, los cuales van desde simple información lanzada a granel y al pantallazo, hasta datos con estructuras muy bien definidas y que pasan de ser simples textos a complejas estructuras de control y redes.

El formato de datos posee reglas y estructuras similares a los que tenemos en programación y lenguajes escritos. Cada formato va a tener características específicas:

1. La sintaxis, incluye diferentes tipos de símbolos, tales como [], (), {}, el uso de espacio o sangría, comillas, comas, y más.
2. ¿Cómo se representan los objetos?, como caracteres, una cadena de caracteres, una lista, y vectores.
3. ¿Cómo se representan los pares llave/valor (ley/valué)? La llave (ley) usualmente se encuentra al lado izquierdo e identifica o describe los datos. El valor (valué) que se encuentra al lado derecho, consiste en los datos, los cuales pueden ser caracteres, cadenas de caracteres, números, listas o cualquier otro tipo de información.

Hay además 3 grandes clases de formatos:

1. Formatos JSON.
2. Formatos YAML.
3. Formatos XML.

Cabe destacar que el formato mas lógico y entendible es el de XML el cual es usado para una gran variedad de aplicaciones como; formatos y estructurados lógicos de archivos contables, archivos fiscales, formatos de archivos bancarios y numerales, además de contener una estructura per sé fácil de aprender y entender.

Una API es un sitio donde se aloja información clave contenida sobre un cierto tema o herramienta en específico el cual puede definirse como una base de datos

API es un programa que permite a otras aplicaciones acceso a su información o sus servicios. Es un conjunto de reglas que describe cómo una aplicación puede interactuar con otra, y las instrucciones para que esa interacción ocurra. El usuario envía una solicitud API a un servidor solicitando información específica y recibe una respuesta API desde el servidor con la información solicitada. Alojada generalmente en un sitio web:

Los hay de 3 tipos:

1. API públicas.
2. Privadas.
3. De socios.

REST es un estilo arquitectónico para diseñar aplicaciones de servicio web. Se refiere a un estilo de arquitectura web que tiene muchas características subyacentes y gobierna el comportamiento de los clientes y servidores. En pocas palabras, una API REST es una API que funciona encima del protocolo HTTP. Define un conjunto de funciones que los desarrolladores pueden usar para realizar solicitudes y recibir respuestas a través del protocolo HTTP como GET y POST.

Un servicio web RESTful se implementa mediante HTTP. Es una colección de recursos con cuatro aspectos definidos:

1. Identificador uniforme de recursos (URI) base para el servicio web, como http://example.com/resources.
2. El formato de datos admitido por el servicio web. A menudo es JSON, YAML o XML, pero podría ser cualquier otro formato de datos que sea un estándar de hipertexto válido.
3. El conjunto de operaciones admitidas por el servicio web mediante métodos HTTP.
4. La API debe estar controlada por hipertexto.

Al investigar un poco sobre las herramientas de automatización en redes se encontraron que existen una gran multitud de ellas; sin embargo se destacan 4:

1. Chef
2. Ansible
3. Puppet
4. SaltStack

Estas herramientas sirven para varios propósitos en red , cada una de ellas se diferencia mas en la manera en como estructuran dicha red, mas que en sus funcionalidades, sirven para:

1. Control de versión de software’
2. Atributos del dispositivo, como nombres, direccionamiento y seguridad
3. Configuración de protocolos
4. Configuraciones de ACL

El objetivo de todas estas herramientas es reducir la complejidad y el tiempo que implica configurar y mantener una infraestructura de red a gran escala con cientos, incluso miles de dispositivos. Estas mismas herramientas también pueden beneficiar a redes más pequeñas.