Capítulo 12

Solución de problemas de red

Documentación de red

Descripción general de la documentación

Se requiere documentación de red precisa y completa para supervisar y solucionar problemas de redes de manera eficaz.

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

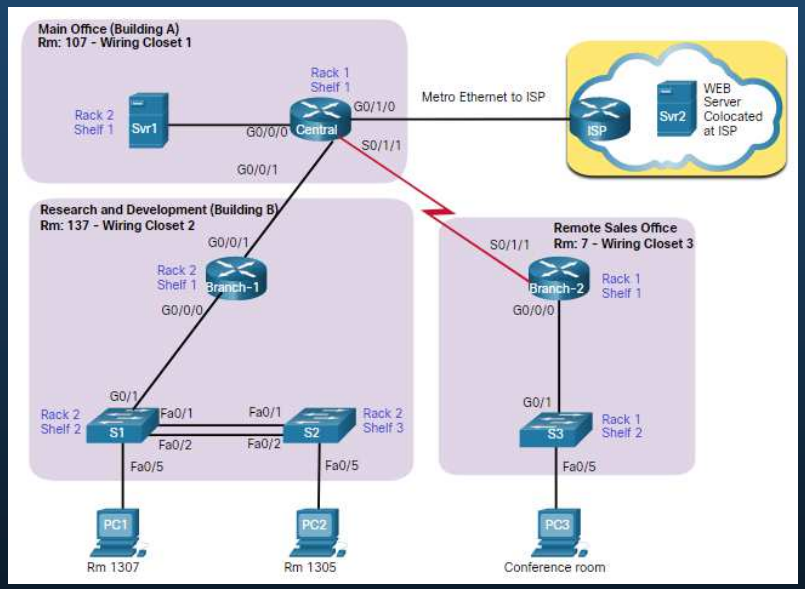
Toda la documentación de la red debe mantenerse en una sola ubicación y la documentación de copia de seguridad debe mantenerse y mantenerse en una ubicación separada.

Documentación de red

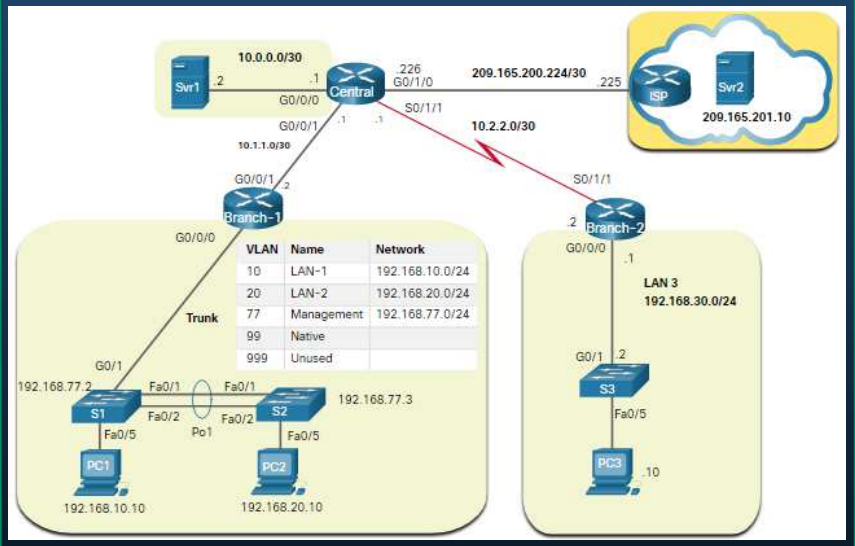
Diagramas de topología de la red

Hay dos tipos de diagramas de topología de la red: la topología física y la topología lógica.

Topología física



Topología lógica



Documentación de red

Documentación de dispositivos de red

La documentación de red debería contener registros precisos y actualizados del hardware y el software usados en una red.

La documentación debe incluir toda la información pertinente sobre los dispositivos de red.

Device	Model	Description	Location	IOS	License
Central	ISR 4321	Central Edge Router	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9

Interface	Description	IPv4 Address	IPv6 Address	MAC Address	Routing
G0/0/0	Connects to SVR-1	10.0.0.1/30	2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3

Device	Model	Description	Mgt. IP Address	IOS	VTP
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 switch	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M	Domain: CCNA Mode: Server

Port	Description	Access	VLAN	Trunk	EtherChannel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1	-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2	-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***	Yes	999	-	-		Shut
Fa0/4	*** Not in use ***	Yes	999	-	-		Shut
Fa0/5	Access port to user	Yes	10	-	-		Yes

Device	OS	Services	MAC Address	IPv4 / IPv6 Addresses	Default Gateway	DNS
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

Documentación de red

Establecer una línea de base de red

Una línea de base de red se utiliza para establecer el rendimiento normal de la red con el fin de 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.

Los datos de referencia son los siguientes:

- Proporcionar información sobre si el diseño actual de la red puede satisfacer los requisitos comerciales.
- Puede revelar áreas de congestión o áreas de la red que están infrautilizadas.

Documentación de red

Determine qué tipos de datos se deben recopilar.

Al establecer la línea de base inicial, comience por seleccionar algunas variables que representen a las políticas definidas.

Si se seleccionan demasiados puntos de datos, la cantidad de datos puede ser abrumadora, lo que dificulta el análisis de los datos reunidos.

Comience de manera simple y realice ajustes a lo largo del proceso.

Algunas medidas útiles son el uso de interfaz y el uso de CPU.

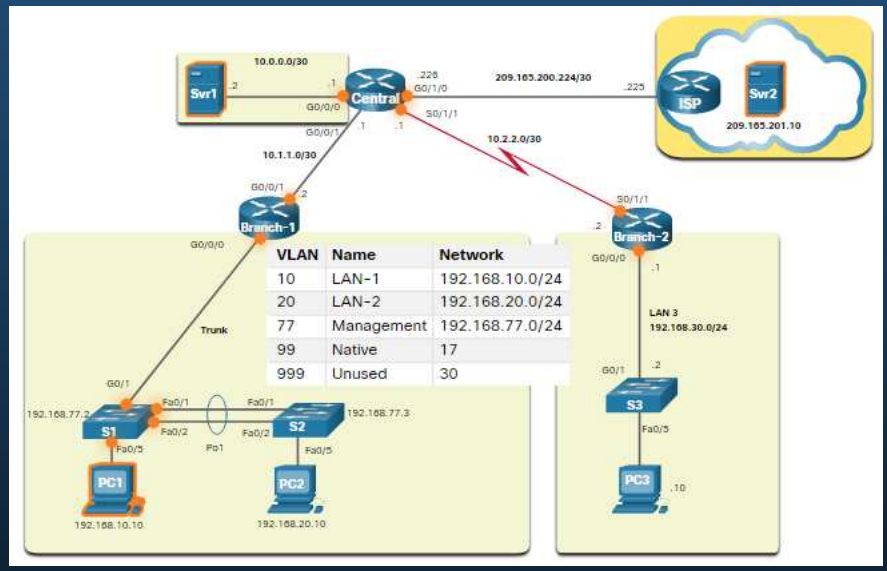
Documentación de red

Identifique los dispositivos y los puertos de interés.

Un diagrama de topología lógica de la red, puede ser útil en la identificación de los dispositivos y los puertos principales que se van a supervisar.

Como se muestra en la topología de ejemplo, los dispositivos y puertos de interés incluyen:

- PC1 (terminal de administración)
- Dos servidores (es decir, Srv1 y Svr2)
- Interfaces de router
- Puertos clave en switches



Documentación de red

Paso 3 - Determine la duración de la línea de base

Al capturar datos para el análisis, el período especificado debe ser:

- Como mínimo, siete días de duración.
- No se deben extender durante más de seis semanas, salvo que se deban medir tendencias específicas a largo plazo.
- Por lo general, una línea de base de dos a cuatro semanas es adecuada.

Realice un análisis anual de toda la red o analice la línea de base de diferentes secciones de la red.

Para entender la forma en que el crecimiento y otros cambios afectan la red, el análisis se debe realizar periódicamente.

Documentación de red

Medición de datos

La figura detalla algunos de los comandos más comunes de Cisco IOS para la recopilación de datos.

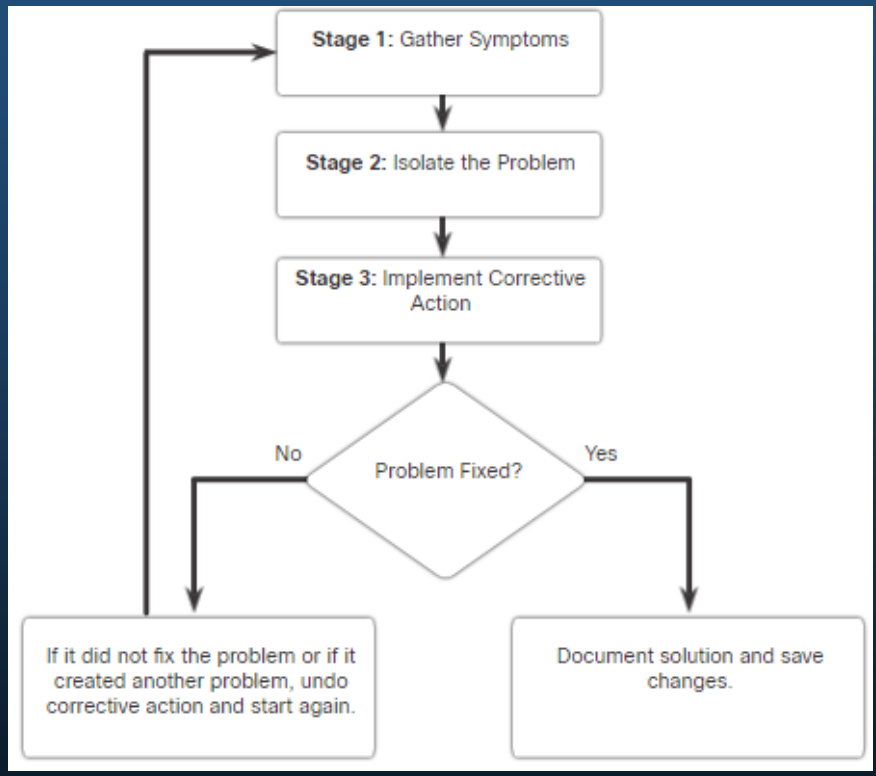
Comando	Descripción
show version	• Muestra el tiempo de actividad, información sobre la versión del software y del hardware del dispositivo.
show ip interface [brief] **show ipv6 interface [brief]**	• Muestra todas las opciones de configuración establecidas en una interfaz.
show interfaces	• Muestra la salida detallada de cada interfaz.
show ip route [static |eigrp |ospf |bgp] **show ipv6 route [static |eigrp |ospf |bgp]**	• La tabla de routing consta de redes conectadas directamente y redes remotas aprendidas.
show cdp neighbors detail	• Muestre información detallada acerca de los dispositivos Cisco conectados directamente.
show arp **show ipv6 neighbors**	• Muestra el contenido de la tabla ARP (IPv4) y la tabla vecina (IPv6).
show running-config	• Muestre la configuración actual.
show vlan	• Muestra el estado de las VLAN en un switch.
show port	• Muestra el estado de los puertos en un switch.
show tech-support	• Se utiliza para recopilar una gran cantidad de información utilizando varios comandos **show** para propósitos de informes de soporte técnico.

Proceso de solución de problemas

Procedimientos generales de solución de problemas

La solución de problemas puede llevar mucho tiempo porque las redes difieren, los problemas difieren y la experiencia de solución de problemas varía.

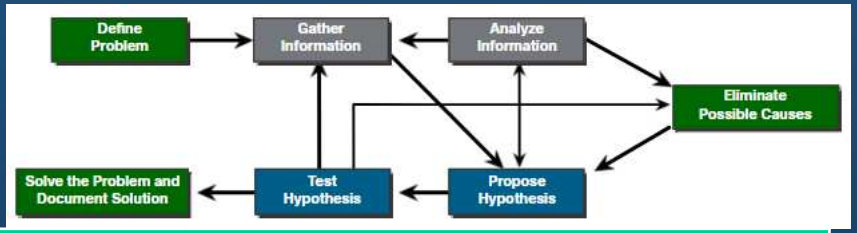
- El uso de un método estructurado de solución de problemas acortará el tiempo general de solución de problemas.
- Existen varios procesos de solución de problemas que se pueden usar para resolver un problema.
- La figura muestra el diagrama de flujo lógico de un proceso simplificado de solución de problemas de tres etapas.



Proceso de solución de problemas

Proceso de siete pasos para la solución de problemas

La figura muestra un proceso de solución de problemas de siete pasos más detallado.



Pasos	Descripción
Defina el problema	• Compruebe que existe un problema y, a continuación, defina correctamente cuál es el problema.
Recopilar información	• Los destinos (es decir, hosts, dispositivos) se identifican, se accede y se recopila información.
Analizar información	• Identifique posibles causas mediante documentación de red, líneas base de red, bases de conocimiento y pares.
Elimine posibles causas	• Elimine progresivamente las posibles causas para eventualmente identificar la causa más probable.
Proponer hipótesis	• Cuando se ha identificado la causa más probable, se debe formular una solución.
Probar la hipótesis	• Evaluar la urgencia del problema, crear un plan de reversión, implementar la solución y verificar el resultado.
Resuelva el problema	• Cuando se resuelva, informe a todos los involucrados y documente la causa y la solución para ayudar a resolver problemas futuros.

Proceso de solución de problemas

Preguntas a los usuarios finales

La tabla de la izquierda proporciona algunas pautas y ejemplos de preguntas para los usuarios finales.

Pautas	Preguntas de ejemplo para los usuarios finales
Haga preguntas pertinentes.	• ¿Qué no funciona? • Exactamente, ¿cuál es el problema? • ¿Qué intenta lograr?
Determine el alcance del problema.	• ¿A quién afecta este problema? ¿Eres solo tú u otros? • ¿En qué dispositivo está pasando esto?
Determine cuándo y con qué frecuencia ocurre o ocurrió el problema.	• ¿Cuándo se produjo el problema exactamente? • ¿Cuándo se advirtió el problema por primera vez? • ¿Se han mostrado mensajes de error?
Determine si el problema es constante o intermitente.	• ¿Puede reproducir el problema? • ¿Puedes enviarme una captura de pantalla o un video del problema?
Determine si algo ha cambiado.	• ¿Qué se ha modificado desde la última vez que funcionó?
Utilizar cada pregunta como un medio para eliminar o descubrir posibles problemas.	• ¿Qué funciona? • ¿Qué no funciona?

Proceso de solución de problemas

Recopilación de información

Comandos de Cisco IOS comunes que se utilizan para recopilar los síntomas de un problema de red.

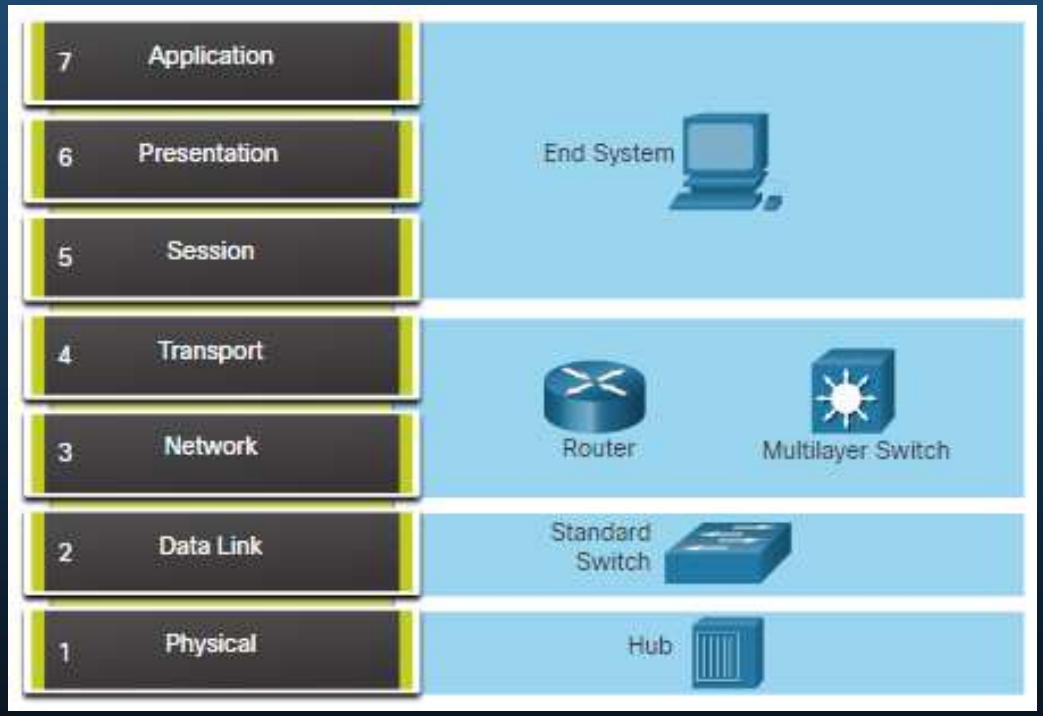
Comando	Descripción
ping {*host* | *ip-address*}	• Envía un paquete de solicitud de eco a una dirección y espera una respuesta.
traceroute *destination*	• Identifica la ruta que recorre un paquete a través de las redes.
telnet {*host* | *ip-address*}	• Se conecta con una dirección IP usando la aplicación Telnet (Nota: Use SSH siempre cuando sea posible).
ssh -l *user-id ip-address*	• Se conecta a una dirección IP con SSH.
show ip interface brief **show ipv6 interface brief**	• Muestra un resumen del estado de todas las interfaces en un dispositivo.
show ip route **show ipv6 route**	• Muestra las tablas de routing IPv4 e IPv6 actuales.
show protocols	• Muestra los estado globales y específicos por interfaz de cualquier protocolo de Capa 3 configurado.
depurar	• Muestra una lista de opciones para habilitar o deshabilitar eventos de depuración.

Proceso de solución de problemas

Solución de problemas con modelos en capas

Los modelos OSI y TCP/IP se pueden aplicar para aislar los problemas de red cuando durante la solución de problemas.

La figura muestra algunos dispositivos comunes y las capas del modelo OSI que se deben examinar durante el proceso de solución de problemas de cada dispositivo.



Proceso de solución de problemas

Métodos estructurados para la solución de problemas

Los diferentes enfoques de solución de problemas que se pueden utilizar incluyen los siguientes.

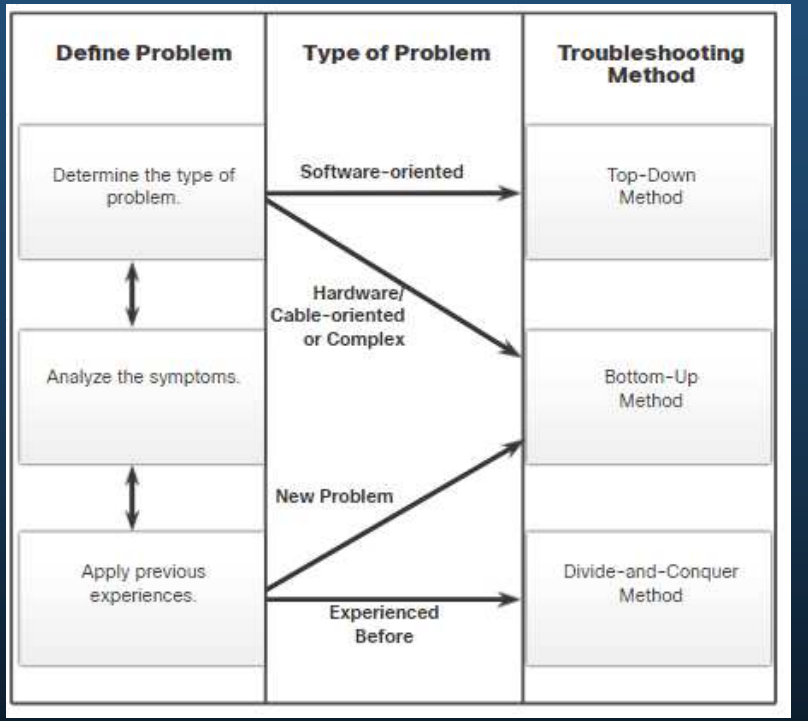
Enfoque para la solución de problemas	Descripción
Ascendente	• Es un buen método para usar cuando se sospecha que el problema es físico.
Descendente	• Use este método para los problemas más simples o cuando crea que el problema está en un software.
Divide y vencerás	• Comience en una capa intermedia (es decir, Capa 3) y realice las pruebas en ambas direcciones desde esa capa.
Seguimiento de la ruta	• Se utiliza para descubrir la ruta de tráfico real de origen a destino para reducir el alcance de la solución de problemas.
Sustitución	• Intercambia físicamente un dispositivo sospechoso problemático por uno conocido y funcional.
Comparación	• Intenta resolver el problema comparando un elemento no operativo con el que funciona.
Deducción informada	• El éxito de este método varía en función de su experiencia y capacidad de solución de problemas.

Proceso de solución de problemas

Pautas para seleccionar un método de solución de problemas

Para resolver rápidamente los problemas de una red, tómese el tiempo para seleccionar el método más eficaz de resolución de problemas de red.

- La figura ilustra qué método se podría utilizar cuando se descubre un cierto tipo de problema.
- Solución de problemas es una habilidad que se desarrolla al hacerlo.
- Cada problema de red que identifique y resuelva se añade a su conjunto de habilidades.



Herramientas de solución de problemas

Herramientas para la solución de problemas de software

Algunas herramientas para la solución de problemas de software incluyen las siguientes:

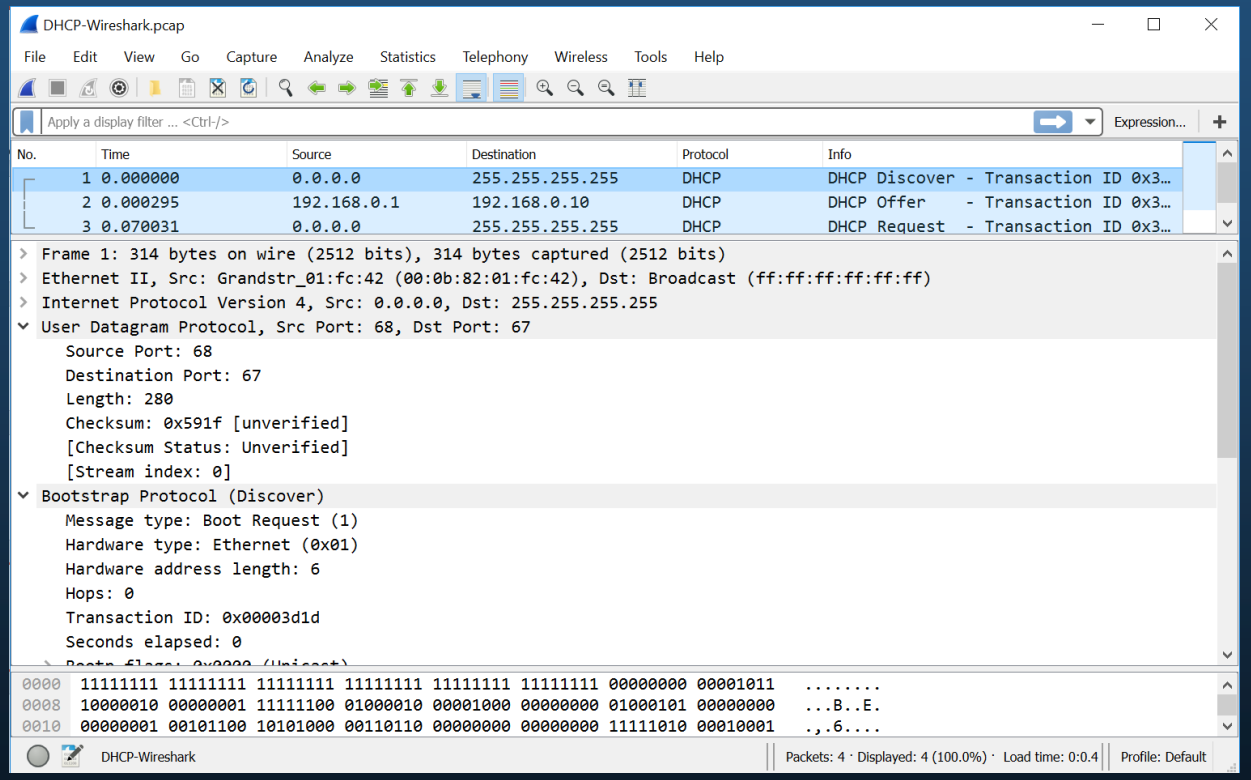
Herramienta de software	Descripción
Herramientas del sistema de administración de red (NMS)	• Software de red incluye las herramientas de monitoreo a nivel de los dispositivos, configuración y administración de fallas. • Estas herramientas se pueden usar para investigar y corregir los problemas de red.
Base de conocimientos	• Las bases de conocimientos en línea de los proveedores de dispositivos de red se volvieron fuentes de información indispensables. • Cuando las bases de conocimientos de los proveedores se combinan con motores de búsqueda de Internet, los administradores de red tienen acceso a una vasta fuente de información fundada en la experiencia.
Herramientas de línea de base	• Hay numerosas herramientas disponibles para automatizar la documentación de red y el proceso de línea de base. • Las herramientas de línea de base pueden ayudar con tareas habituales como diagramas de red, actualizar el registro de software y hardware de una red y medir de forma rentable la línea de base de uso de ancho de banda de la red.

Herramientas de solución de problemas

Analizador de protocolos

Un analizador de protocolos puede capturar y mostrar la capa física a la información de capa de aplicación contenida en un paquete.

Los analizadores de protocolos, como Wireshark, pueden ayudar a resolver problemas de rendimiento de la red.



Herramientas de solución de problemas

Herramientas para la solución de problemas de hardware

Hay varios tipos de herramientas de solución de problemas de hardware.

Herramientas para hardware	Descripción
Multímetro digital	Los dispositivos miden los valores eléctricos de voltaje, corriente y resistencia.
Analizadores de cables	Los portátiles están diseñados para probar los diversos tipos de cables de comunicación de datos.
Analizador de cables	Dispositivos portátiles multifuncionales utilizados para probar y certificar cables de cobre y fibra.
Analizadores de redportátiles	Dispositivo especializado utilizado para solucionar problemas de redes conmutadas y VLAN.
Cisco Prime NAM	Interfaz basada en navegador que muestra el análisis del rendimiento del dispositivo en un entorno conmutado (switched) y enrutado (routed).

Herramientas de solución de problemas

Solución de problemas con un servidor de syslog

Los clientes syslog utilizan Syslog para enviar mensajes de registro basados en texto a un servidor syslog.

- Los mensajes de registro se pueden enviar a la consola, las líneas VTY, el búfer de memoria o el servidor syslog.
- Los mensajes de registro del IOS de Cisco se ubican en uno de ocho niveles.
- Cuanto menor es el número del nivel, mayor es el nivel de gravedad.
- De forma predeterminada, la consola muestra mensajes de nivel 6 (depuración).
- En el comando de salida, los mensajes de sistema del nivel 0 (emergencias) al 5 (notificaciones) se envían al servidor de syslog en 209.165.200.225.

Nivel	Palabra clave
0	Emergencias
1	Alertas
2	Crítico
3	Errores
4	Advertencias
5	Notificaciones
6	Informativo
7	Depuración

```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
R1(config)#
```

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los síntomas comunes de los problemas de red de capas físicas.

Síntoma	Descripción
Rendimiento menor a la línea de base	• Requiere líneas base anteriores para la comparación. • Las razones más frecuentes incluyen servidores sobrecargados o con alimentación insuficiente, configuraciones de router o switch inadecuadas, congestión del tráfico en un enlace de baja capacidad y pérdida crónica de tramas.
Pérdida de conectividad	• La pérdida de conectividad podría deberse a un cable fallido o desconectado. • Se puede verificar mediante una simple prueba **de ping** . • La pérdida intermitente de la conectividad puede indicar una conexión floja u oxidada.
Cuellos de botella o congestión en la red	• Si falla una ruta, los protocolos de enrutamiento podrían redirigir el tráfico a rutas que no sean óptimas. • Esto puede provocar congestión o cuellos de botella en esas partes de la red.
Altos porcentajes de utilización de CPU	• Las altas tasas de utilización de la CPU indican que un dispositivo está funcionando en o excediendo sus límites de diseño. • Si no se aborda rápidamente, la sobrecarga de CPU puede ocasionar que un dispositivo falle o se desactive.
Mensajes de error de la consola	• Los mensajes de error notificados en la consola de dispositivos podrían indicar un problema en la capa física. • Los mensajes de la consola deben registrarse en un servidor syslog central.

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los incidentes que comúnmente causan problemas de red en la capa física incluyen los siguientes:

Causa del problema	Descripción
Relacionadas con la alimentación	Revise el funcionamiento de los ventiladores y asegurarse de que los orificios de entrada y salida de ventilación del bastidor no estén obstruidos.
Fallas de hardware	Archivos de controladores NIC defectuosos o corruptos, cables defectuosos o problemas de conexión a tierra pueden causar errores de transmisión de red, como colisiones tardías, tramas cortas y jabber.
Fallas de cableado	Busque cables dañados, cables incorrectos y conectores mal engarzados. Los cables sospechosos se deben probar o cambiar por un cable que se sepa que funcione.
atenuación	La atenuación puede ocurrir cuando la longitud de un cable supera el límite de diseño para los medios o cuando hay una conexión deficiente que se debe a un cable flojo o a contactos sucios u oxidados.
Ruido	La interferencia electromagnética local (EMI) puede ser generada por muchas fuentes, tales como diafonía, cables eléctricos cercanos, grandes motores eléctricos, estaciones de radio FM, radio policial y más.
Errores de configuración de interfaz	Las causas pueden incluir una frecuencia de reloj incorrecta, una fuente de reloj incorrecta y la interfaz no activada. Esto provoca la pérdida de la conectividad a los segmentos de red conectados.
Límites de diseño excedidos	Un componente podría funcionar de manera subóptima si se utiliza más allá de las especificaciones.
Sobrecarga de CPU	Los síntomas incluyen procesos con altos porcentajes de uso de CPU, descartes de cola de entrada, rendimiento lento, tiempos de espera de SNMP, falta de acceso remoto o respuesta lenta o fallida de servicios como DHCP, Telnet y ping.

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los síntomas comunes de los problemas de red de capa de vínculo de datos.

Síntoma	Descripción
Falta de funcionalidad o conectividad en la capa de red o en capas superiores	Algunos problemas de capa 2 pueden detener el intercambio de tramas a través de un enlace, mientras que otros solo provocan un deterioro del rendimiento de la red.
La red funciona por debajo de los niveles de rendimiento de línea de base	• Las tramas pueden tomar una ruta subóptima a su destino, pero aún así llegan haciendo que la red experimente un uso inesperado de ancho de banda alto en los enlaces. • Un ping extendido o continuo ayuda a revelar si se descartan tramas.
Difusiones excesivas	• Los sistemas operativos utilizan ampliamente difusiones y multidifusión. • Por lo general, las difusiones excesivas son el resultado de aplicaciones programadas o configuradas incorrectamente, grandes dominios de difusión de capa 2 o problemas de red subyacentes.
Mensajes de la consola	• Los routers envía mensajes cuando detecta un problema con la interpretación de las tramas entrantes (problemas de encapsulación o entramado) o cuando se esperan keepalives pero no llegan. • El mensaje de la consola más común que indica que existe un problema de Capa 2 es un mensaje que indica que el protocolo de línea está desactivado.

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los problemas que suelen causar problemas de red en la capa de vínculo de datos.

Causa del problema	Descripción
Errores de encapsulación	Se produce cuando los bits colocados en un campo por el remitente no son lo que el receptor espera ver.
Errores de asignación de direcciones	Se produce cuando el direccionamiento de capa 2 y capa no están disponibles.
Errores de entramado	Los errores de tramas pueden deberse al ruido en la línea serial, un cable mal diseñado, una falla de NIC, una diferencia entre dúplex o un error de configuración de reloj de línea de unidad de servicio de canal (CSU).
Fallas o bucles de STP	La mayoría de los problemas de STP se relacionan con el reenvío de bucles, que se produce cuando no se bloquean puertos en una topología redundante y el tráfico se reenvía en círculos indefinidamente, lo que implica una saturación excesiva provocada por una tasa elevada de cambios en la topología STP.

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los síntomas comunes de los problemas de red de capa.

Síntoma	Descripción
Falla de red	• Se produce cuando esta no funciona o funciona parcialmente, lo que afecta a todos los usuarios y a todas las aplicaciones en la red. • Los usuarios y los administradores de red normalmente detectan estas fallas en seguida, las que sin dudas son fundamentales para la productividad de la empresa.
Rendimiento inferior al óptimo	• Estos incluyen un subconjunto de usuarios, aplicaciones, destinos o un tipo de tráfico. • Es difícil detectar los problemas de optimización, y es incluso más difícil aislarlos y diagnosticarlos. • Esto se debe a que varias capas suelen verse involucradas o incluso una sola computadora de host. • Puede llevar tiempo determinar que el problema se encuentra en la capa de red.

Solución de problemas de red

Solución de problemas de la capa física

La tabla enumera los síntomas comunes de los problemas de red de capa.

Causa del problema	Descripción
Problemas generales de red	• A menudo, un cambio en la topología puede, sin saberlo, tener efectos en otras áreas de la red. • Determine si algún elemento de la red cambió de manera reciente y si hay alguna persona trabajando en la infraestructura de la red en ese momento.
Problemas de conectividad	Compruebe si hay problemas de equipo y conectividad, incluidos problemas de alimentación, problemas ambientales y problemas de nivel 1, como problemas de cableado, puertos defectuosos y problemas de ISP.
Tabla de routing	Revise la tabla de routing para ver si existe algo inesperado, como rutas faltantes o imprevistas.
Problemas de vecinos	Compruebe si hay algún problema con los routers que forman adyacencias vecinas.
Base de datos de topología	Revise la tabla de routing para ver si existe algo inesperado, como rutas faltantes o imprevistas.

Solución de problemas de red

Solución de problemas de la capa de transporte: ACL

La tabla enumera las áreas donde las configuraciones incorrectas ACL ocurren comúnmente.

Configuraciones incorrectas	Descripción
Selección del flujo de tráfico	Se debe aplicar la ACL a la interfaz correcta en el sentido de tráfico apropiado.
Orden de las entradas de control de acceso	El orden de las entradas en una ACL debe ir de lo específico a lo general.
deny any implícita	La ACE implícita puede ser la causa de una configuración incorrecta de ACL.
Dirección y máscaras wildcard IPv4	Las máscaras de comodín IPv4 complejas son más eficientes, pero están más sujetas a errores de configuración.
Selección del protocolo de la capa de transporte	Es importante que sólo se especifique el protocolo de capa de transporte correcto en una ACE.
Puertos de origen y destino	Asegurarse de que los puertos entrantes y salientes correctos se especifican en un ACE
Uso de la palabra clave established	La palabra clave **establecida** aplicada incorrectamente, puede proporcionar resultados inesperados.
Protocolos poco frecuentes	Las ACL configuradas incorrectamente suelen causar problemas en protocolos distintos de TCP y UDP.

Solución de problemas de red

Solución de problemas de la capa de transporte - NAT para IPv4

La tabla enumera áreas frecuentes de interoperabilidad con NAT.

Síntoma	Descripción
BOOTP y DHCP	• El paquete de solicitud de DHCP tiene la dirección IPv4 de origen 0.0.0.0. • Debido a que la NAT requiere direcciones IPv4 de origen y de destino válidas, BOOTP y DHCP pueden tener dificultades para operar a través de un router que ejecuta una NAT estática o dinámica. • La configuración de la característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.
DNS	• Un servidor DNS fuera del router NAT no tiene una representación precisa de la red dentro del enrutador. • La configuración de la característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.
SNMP	• Una administración SNMP en un lado de un router NAT no pueda comunicarse con los agentes SNMP del otro lado del router NAT. • La configuración de la característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.
Protocolos de tunneling y cifrado	Los protocolos de cifrado y tunneling suelen requerir que el tráfico se origine en un puerto UDP o TCP específico o usan un protocolo en la capa de transporte que la NAT no puede procesar.

Solución de problemas de red

Solución de problemas de la capa física

La tabla proporciona una breve descripción de estos protocolos de capa de aplicación.

Aplicaciones	Descripción
SSH/Telnet	Permite a los usuarios establecer conexiones de sesión de terminal a los hosts remotos.
HTTP	Admite el intercambio de texto, gráficos, sonido, video y otros archivos multimedia en la Web.
FTP	Realiza transferencias interactivas de archivos entre los hosts.
TFTP	Realiza transferencias interactivas básicas de archivos, generalmente, entre hosts y dispositivos de red.
SMTP	Admite servicios básicos de entrega de mensajes.
POP	Conecta a los servidores de correo electrónico y descarga correo electrónico.
SNMP	Recopila información de administración de dispositivos de red.
DNS	Asigna direcciones IP a los nombres asignados a los dispositivos de red.
NFS	Sistema de archivos de red (NFS): habilita las computadoras para montar unidades en hosts remotos y operarlas como si fueran unidades locales.

Solución de problemas de conectividad IP

Componentes de la solución de problemas de conectividad de extremo a extremo

Los pasos de enfoque ascendente cuando no hay conectividad end-to-end son los siguientes:

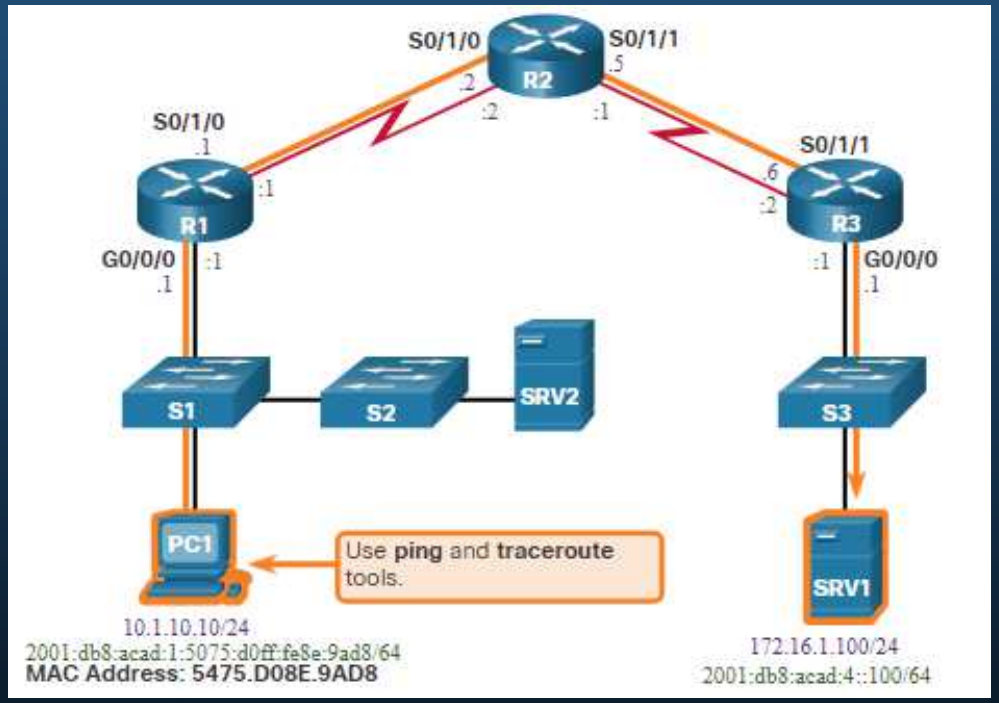
1. Revisar la conectividad física en el punto donde se detiene la comunicación de red.
2. Revisar las incompatibilidades de dúplex.
3. Revisar el direccionamiento de las capas de enlace de datos y de red en la red local.
4. Verificar que el gateway predeterminado sea correcto.
5. Asegurarse de que los dispositivos determinen la ruta correcta del origen al destino.
6. Verificar que la capa de transporte funcione correctamente.
7. Verificar que no haya ACL que bloqueen el tráfico.
8. Asegurarse de que la configuración del DNS sea correcta.

Solución de problemas de conectividad IP

Problema de conectividad de extremo a extremo, inicio a la solución de problemas

Generalmente, lo que da inicio a un esfuerzo de resolución de problemas es la detección de un problema con la conectividad de extremo a extremo.

Dos de las utilidades más comunes que se utilizan para verificar un problema con la conectividad de extremo a extremo son **ping** y **traceroute**.



Solución de problemas de conectividad IP

Paso 1: Verificar la capa física

El comando **show interfaces** es útil al solucionar problemas relacionados al rendimientos en los que se sospecha que el hardware es la causa.

De interés en la salida son los:

- Estado de la interfaz
- Descartes de cola de entrada
- Descartes de cola de salida
- Errores de entrada
- Errores de salida

```
R1# show interfaces GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0(bia d48c.b5ce.a0c0)
Internet address is 10.1.10.1/24
(Output omitted)
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
 Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
85 packets input, 7711 bytes, 0 no buffer
Received 25 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 5 multicast, 0 pause input
10112 packets output, 922864 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
11 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R1#
```

Solución de problemas de conectividad IP

Paso 2 - Revisar las incompatibilidades de dúplex

El estándar Gigabit Ethernet IEEE 802.3ab exige el uso de la autonegociación, para velocidad, dúplex y prácticamente todos los NICs Fast Ethernet también usan autonegociación predeterminadamente.

Pueden producirse problemas cuando hay una discrepancia dúplex.

```
S1# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Full-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S1#
```

```
S2# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96d2.4001 (bia 0cd9.96d2.4001)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Half-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S2(config)# interface fa 0/20
S2(config-if)# duplex auto
S2(config-if)#
```

Solución de problemas de conectividad IP

Paso 3 - Verificar el direccionamiento en la red local

El comando **arp** de Windows muestra y modifica las entradas en la caché ARP, que se usan para almacenar las direcciones IPv4 y sus direcciones físicas de Ethernet (MAC) resueltas.

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  10.1.10.1             d4-8c-b5-ce-a0-c0     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

Solución de problemas de conectividad IP

Solucionar problemas de asignación de VLAN Ejemplo

Al resolver problemas de conectividad de extremo a extremo, otro problema que se debe considerar es la asignación de VLAN.

Por ejemplo, la dirección MAC en Fa0/1 debe estar en VLAN 10 en lugar de VLAN 1.

```
S1# show mac address-table
             Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type     Ports
All       0100.0ccc.cccc      STATIC   CPU
All       0100.0ccc.cccd      STATIC   CPU
 1        d48c.b5ce.a0c0      DYNAMIC  Fa0/1
10        000f.34f9.9201      DYNAMIC  Fa0/5
10        5475.d08e.9ad8      DYNAMIC  Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

La siguiente configuración cambia Fa0/1 a VLAN 10 y verifica el cambio.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1#
S1# show mac address-table
             Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type     Ports
All       0100.0ccc.cccc      STATIC   CPU
All       0100.0ccc.cccd      STATIC   CPU
10        d48c.b5ce.a0c0      DYNAMIC  Fa0/1
10        000f.34f9.9201      DYNAMIC  Fa0/5
10        5475.d08e.9ad8      DYNAMIC  Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

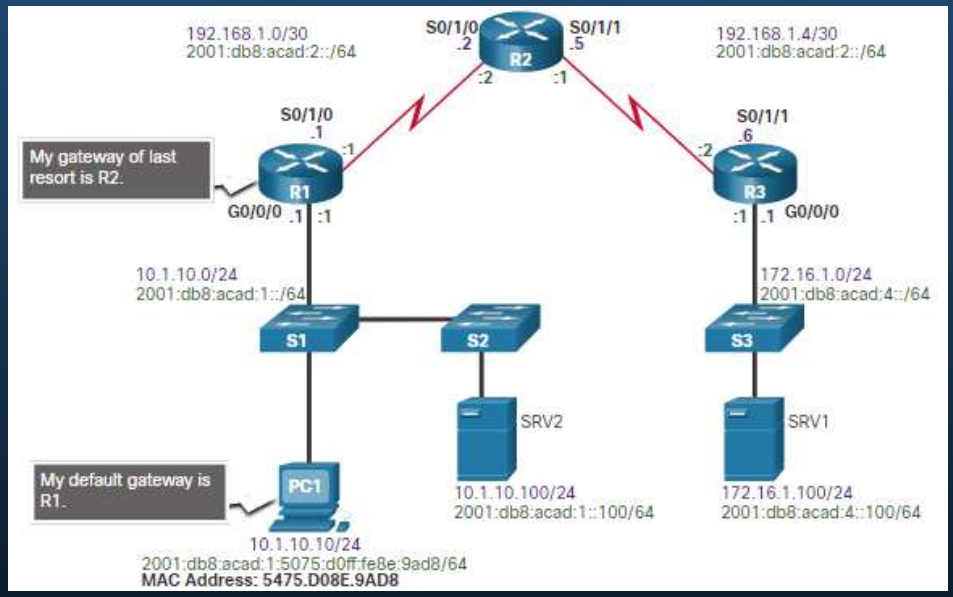
Solución de problemas de conectividad IP

Paso 4: Verificar el gateway predeterminado

Las puertas de enlace predeterminadas mal configuradas o que faltan pueden causar problemas de conectividad.

En la figura, por ejemplo, las puertas de enlace predeterminadas para:

- R1 es 192.168.1.2 (R2)
- PC1 es 10.1.10.1 (R1 G0/0/0)



Comandos útiles para verificar la puerta de enlace predeterminada en:

- R1: **show ip route**
- PC1: **impresión de ruta** (o **netstat —r**)

Solución de problemas de conectividad IP

Solucionar problemas de puerta de enlace predeterminada de IPv6

Un gateway IPv6 predeterminado puede configurarse manualmente usando SLAAC o con DHCPv6.

Por ejemplo, un PC no puede adquirir su configuración IPv6 mediante SLAAC. El resultado del comando falta el grupo de multidifusión de todos IPv6-router (FF02: :2).

```
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
      FF02:: 1
      FF02::1:FF00:1

(Output omitted)
R1#
```

R1 está habilitado como un router IPv6 y ahora la salida verifica que R1 sea miembro de ff02: :2, el grupo multidifusión de routers todos-IPV6.

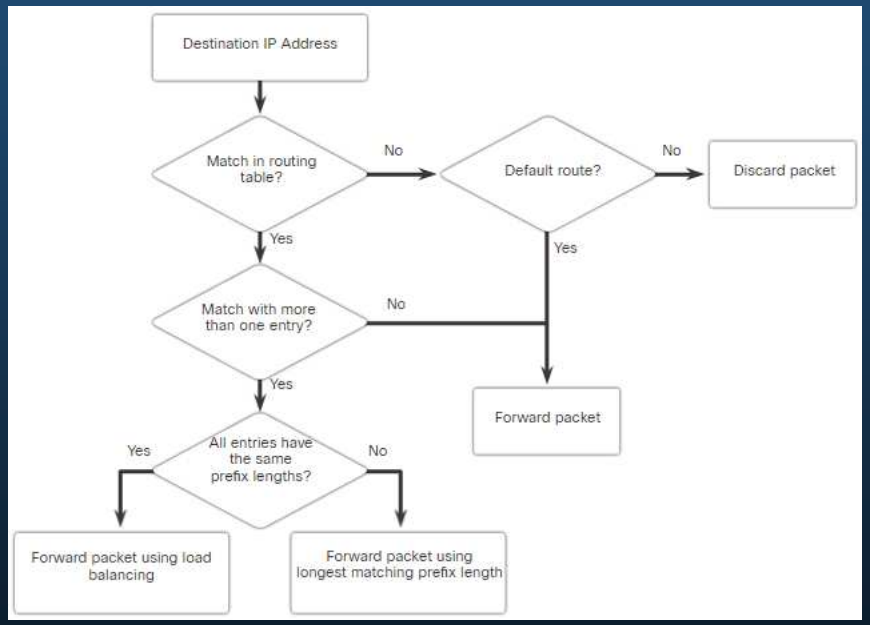
```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1# show ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
      FF02:: 1
      FF02:: 2
      FF02::1:FF00:1
(Output omitted)
R1#
```

Solución de problemas de conectividad IP

Paso 5: Verificar la ruta correcta

Al resolver problemas, con frecuencia es necesario verificar la ruta hacia la red de destino.

- La figura describe el proceso de las tablas de routing IPv4 e IPv6.
- El proceso de reenvío de paquetes IPv4 e IPv6 se basa en la coincidencia más larga de bits o de prefijos.
- El proceso de la tabla de routing intenta reenviar el paquete mediante una entrada en la tabla de routing con el máximo número de bits coincidentes en el extremo izquierdo.
- La longitud de prefijo de la ruta indica el número de bits coincidentes.



Solución de problemas de conectividad IP

Paso 6: Verificar la capa de transporte

Dos de los problemas más frecuentes que afectan la conectividad de la capa de transporte incluyen las configuraciones de ACL y de NAT.

- Una herramienta frecuente para probar la funcionalidad de la capa de transporte es la utilidad Telnet.

- Por ejemplo, el administrador intenta Telnet a R2 usando el puerto 80.

```
R1# telnet 2001:db8:acad:2::2 80
Trying 2001:DB8:ACAD:2::2, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Mon, 04 Nov 2019 12:34:23 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

Solución de problemas de conectividad IP

Paso 7 - Verificar las ACL

En los routers, puede haber ACL configuradas que prohíben a los protocolos atravesar la interfaz en sentido entrante o saliente.

En este ejemplo, ACL 100 se ha configurado incorrectamente como entrante en el G0/0/0 en lugar de como entrante en S0/1/1.

```
R3# show ip interface serial 0/1/1 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
R3#
R3# show ip interface gig 0/0/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is 100
R3#
```

La ACL se elimina de G0/0/0 y se configura como entrante en S0/1/1.

```
R3(config)# interface GigabitEthernet 0/0/0
R3(config-if)# no ip access-group 100 in
R3(config-if)# exit
R3(config)#
R3(config)# interface serial 0/1/1
R3(config-if)# ip access-group 100 in
R3(config-if)# end
R3#
```

Solución de problemas de conectividad IP

Paso 8: Verificar DNS

El protocolo DNS controla el DNS, una base de datos distribuida mediante la cual se pueden asignar nombres de host a las direcciones IP.

- Cuando configura el DNS en el dispositivo, puede reemplazar el nombre de host por la dirección IP con todos los comandos IP, como ping o telnet.
- Utilice el comando **ip host** global configuration para introducir un nombre que se utilizará en lugar de la dirección IPv4 del switch o router, como se muestra en la salida del comando.

```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
R1#

R1# ping ipv4-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R1#
```

- Para visualizar la información de asignación de nombre a dirección IP en una computadora con Windows, use el comando **nslookup**.

Capítulo 13

Virtualización de Red

Computación en la nube

Computación en la nube

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

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

Computación en la nube

Servicios en la nube

Los tres servicios principales de computación en la nube definidos por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos en la Publicación especial 800-145 son:

- Software como un Servicio (SaaS)**: El proveedor de la nube es responsable del acceso a los servicios, que se proporcionan por Internet.**
- 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.**
- Infraestructura como un 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.**

Los proveedores de servicios en la nube han extendido este modelo y también proporcionan asistencia de TI para cada uno de los servicios de computación en la nube (ITaaS). Para las empresas, ITaaS puede ampliar la capacidad de la red, sin requerir inversiones en nueva infraestructura, capacitación de personal, ni licencias de software nuevas.

Computación en la nube

Computación en la nube

Los cuatro modelos principales en la nube son:

- Nubes públicas**: Las aplicaciones basadas en la nube y los servicios que se ofrecen en una nube pública están a disposición de la población en general.**
- Nubes privadas**: Las aplicaciones y los servicios basados en una nube privada que se ofrecen en una nube privada están destinados a una organización o una entidad específica, como el gobierno.**
- Nubes híbridas**: Una nube híbrida consta de dos o más nubes (por ejemplo, una parte privada y otra parte pública); donde cada una de las partes sigue siendo un objeto separado, pero ambas están conectadas a través de una única arquitectura.**
- Nubes comunitarias: Una nube comunitaria se crea para el uso exclusivo de una comunidad específica. Las diferencias entre nubes públicas y las comunitarias son las necesidades funcionales que han sido personalizadas para la comunidad. Por ejemplo, las organizaciones de servicios de salud deben cumplir las políticas y leyes (por ejemplo, la HIPAA) que requieren una autenticación y una confidencialidad especiales.

Computación en la nube

Computación en la Nube versus Centro de Datos

A continuación se brindan las definiciones correctas de "centro de datos" y "computación en la nube":

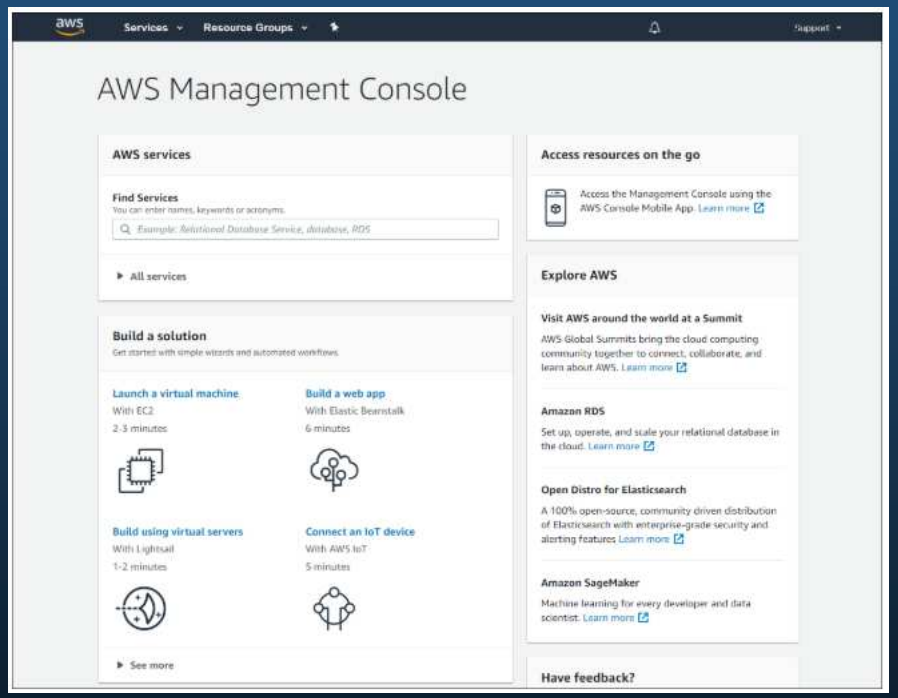
- Centro de datos: Habitualmente es una instalación de procesamiento y almacenamiento de datos que es ejecutada por un departamento de TI interno o arrendado fuera de las instalaciones. Por lo general, la creación y el mantenimiento de centros de datos son muy costosos.
- Computación en la nube: Habitualmente es un servicio fuera de las instalaciones que ofrece acceso a solicitud de un grupo y donde son compartidos recursos de computación, los mismos son configurables. Estos recursos se pueden aprovisionar y liberar rápidamente con un esfuerzo mínimo de administración.

Los centros de datos son las instalaciones físicas que proporcionan las necesidades informáticas, de red y de almacenamiento de los servicios de cloud computing. Los proveedores de servicios en la nube usan los centros de datos para alojar los servicios en la nube y los recursos basados en la nube.

Virtualización

Computación en la nube y virtualización

- Los términos "computación en la nube" y "virtualización" suelen usarse de manera intercambiable; no obstante, significan dos cosas distintas. La virtualización es la base de la computación en la nube. Sin esta base, la computación en la nube que se implementa masivamente no sería posible.
- La virtualización separa el sistema operativo del hardware. Varios proveedores ofrecen servicios virtuales en la nube que permiten aprovisionar servidores de manera dinámica según sea necesario. Estas instancias virtualizadas de los servidores se crean a pedido.

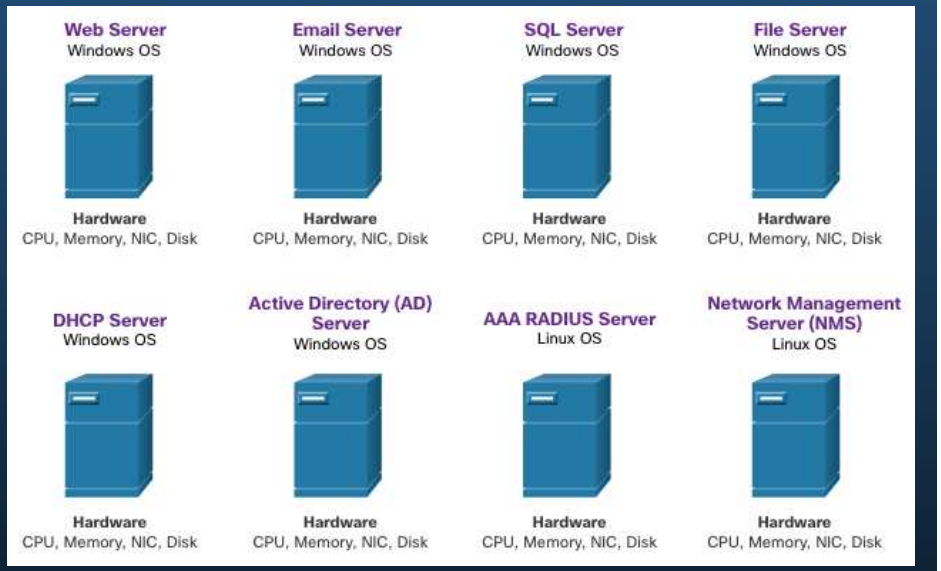


Virtualización

Virtualización Servidores dedicados

Antes, los servidores empresariales estaban formados por un sistema operativo (SO) de servidor, como Windows Server o Linux Server, instalado en hardware específico. Toda la RAM, la potencia de procesamiento y todo el espacio del disco duro de un servidor se dedicaban al servicio proporcionado (por ejemplo, red, servicios de correo electrónico, etc).

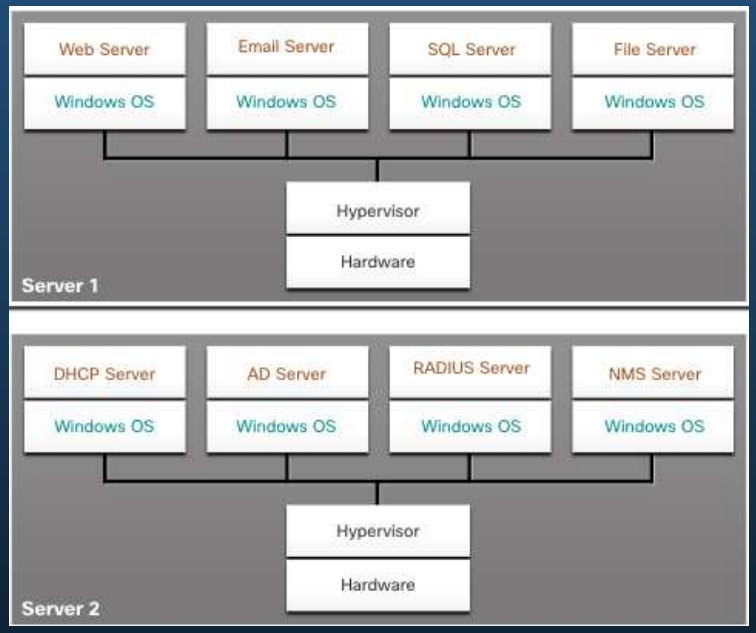
- El principal problema con esta configuración es que cuando falla un componente, el servicio proporcionado por este servidor no se encuentra disponible. Esto se conoce como punto único de falla.
- Por lo general, los servidores dedicados estaban sub-utilizados. A menudo, los servidores dedicados estaban inactivos durante largos períodos de tiempo, esperando hasta que hubiera una necesidad de ofrecer un servicio específico que estos proporcionaban. Estos servidores malgastaban energía y ocupaban más espacio del que estaba garantizado por la cantidad de servicio. Esto se conoce como proliferación de servidores.



Virtualización

Virtualización de servidores

- La virtualización de servidores saca provecho de los recursos inactivos y consolida el número de servidores requeridos. Esto también permite que múltiples sistemas operativos existan en una sola plataforma de hardware.
- El uso de la virtualización normalmente incluye redundancia para brindar protección desde un punto único de falla.
- El Hypervisor es un programa, un firmware o un hardware que suma una capa de abstracción a la parte superior del hardware físico real. La capa de abstracción se utiliza para crear máquinas virtuales que tienen acceso a todo el hardware de la máquina física, como CPU, memoria, controladores de disco y NIC.



Virtualización

Ventajas de la virtualización de servidores

Una de las ventajas más importantes de la virtualización es un menor costo total:

- Se requieren menos equipos
- Se consume menos energía
- Se requiere menos espacio

Estos son los beneficios adicionales de la virtualización:

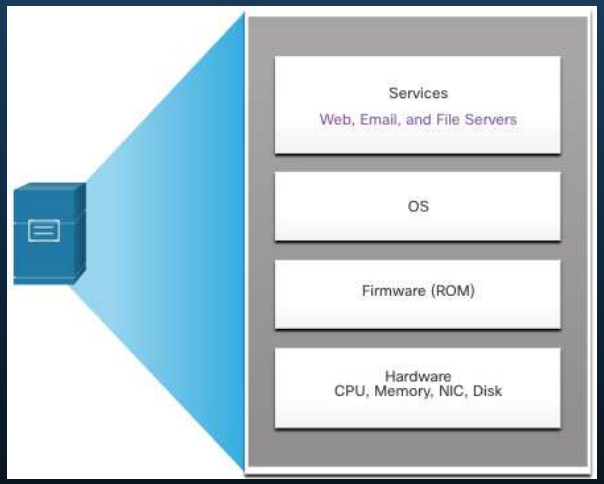
- Facilita la creacion de prototipos
- Provisionamiento más rápido de servidores
- Incremento del tiempo de actividad del servidor
- Mejor recuperación tras desastres
- Soporte heredado (Legacy)

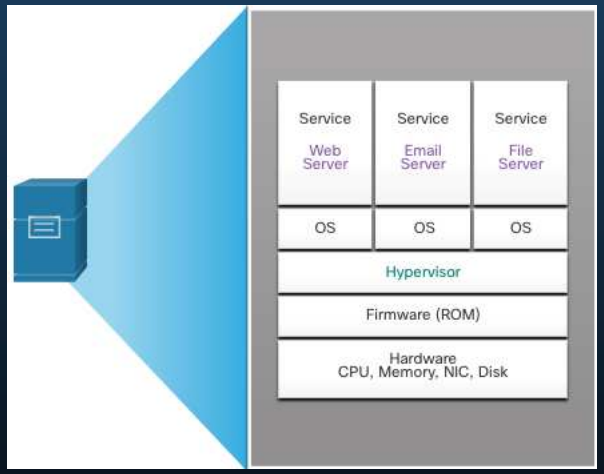
Virtualización

Capas de abstracción

Un sistema informático consta de las siguientes capas de abstracción: aplicaciones, SO, firmware y hardware.

- En cada una de estas capas de abstracción, se utiliza algún tipo de código de programación como interfaz entre la capa inferior y la capa superior.
- Un hypervisor se instala entre el firmware y el OS. El hypervisor puede admitir varias instancias de SO.

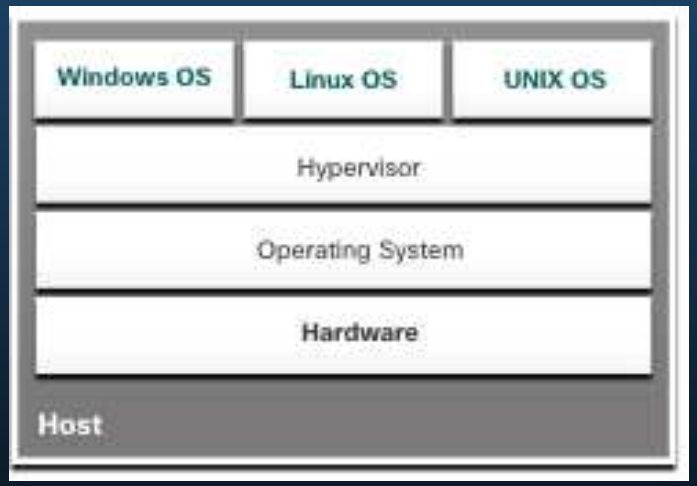




Virtualización

Hypervisores de Tipo 2

- Un hypervisor, tipo 2, es un software que crea y ejecuta instancias de VM. La computadora, en la que un hypervisor está ejecutando una o más VM, es un host. Un hypervisor de tipo 2 también se denomina alojado (hosted hypervisor).
- Una gran ventaja de el hypervisor de tipo 2 es que el software de consola de administración no es necesario.



Infraestructura de red virtual

Hypervisor de tipo 1

- El hypervisor de tipo 1 también se denomina infraestructura física (bare metal), porque el hypervisor está instalado directamente en el hardware. Generalmente este tipo de hypervisor se instala en los servidores empresariales y los dispositivos de redes para centros de datos.
- El hypervisor de tipo 1, se instala directamente en el servidor o en el hardware de red. Luego, las instancias de SO se instalan sobre el hipervisor, como se muestra en la figura. Los hipervisores de tipo 1 tienen acceso directo a los recursos de hardware. Por lo tanto, son más eficientes que las arquitecturas alojadas. Los hipervisores de tipo 1 mejoran la escalabilidad, el rendimiento y la solidez.

Infraestructura de red virtual

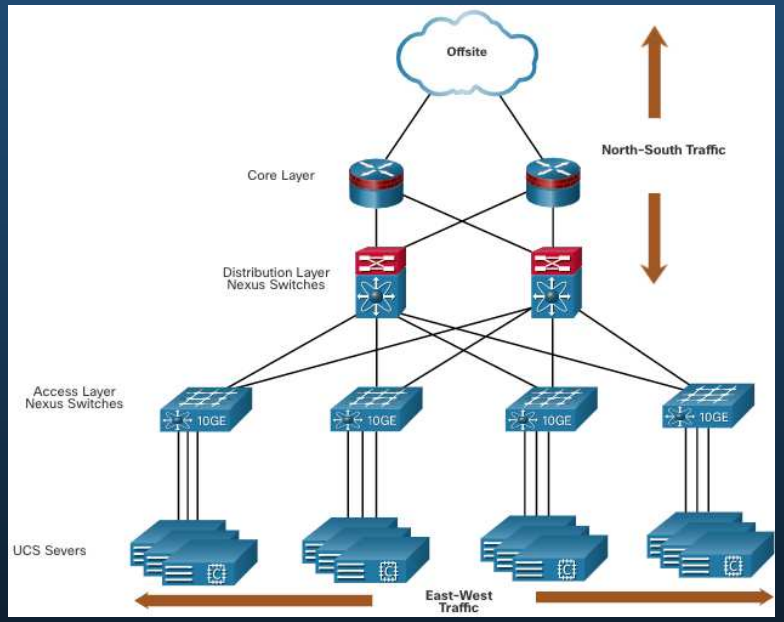
Instalación de una VM en un Hypervisor

- El hypervisor de tipo 1 requiere una “consola de administración” para administrarlo. El software de administración se utiliza para administrar varios servidores con el mismo hypervisor. La consola de administración puede consolidar los servidores automáticamente y encender o apagar los servidores, según sea necesario.
- La consola de administración proporciona la recuperación ante las fallas de hardware. Si falla un componente del servidor, la consola de administración mueve la VM a otro servidor automáticamente y sin inconvenientes. Cisco UCS Manager controla varios servidores y administra los recursos de miles de VM.
- Algunas consolas de administración también permiten la sobre-asignación. La sobre-asignación se produce cuando se instalan varias instancias de SO, pero su asignación de memoria excede la cantidad total de memoria que tiene un servidor. Este tipo de asignación excesiva es habitual porque las cuatro instancias de SO requieren todo el recurso.

Infraestructura de red virtual

La Complejidad de la Virtualización de la Red

- La virtualización del servidor oculta los recursos del servidor. Esta práctica puede crear problemas si el centro de datos está utilizando las arquitecturas de red tradicionales.
- Sin embargo, las VM son trasladables, y el administrador de la red debe poder agregar, descartar y cambiar los recursos y los de la red, para soportar esta característica. Este proceso sería manual y llevaría mucho tiempo con los switches de red tradicionales.
- Otro problema es que los flujos de tráfico difieren considerablemente del modelo cliente-servidor tradicional. Normalmente, hay una cantidad considerable de tráfico que se intercambia entre servidores virtuales (tráfico Este-Oeste) que cambia de ubicación e intensidad a lo largo del tiempo. El tráfico Norte-Sur suele ser el tráfico destinado a ubicaciones fuera del sitio, como otro centro de datos, otros proveedores de nube o Internet.



Infraestructura de red virtual

La Complejidad de la Virtualización de la Red

- El tráfico dinámico en constante cambio requiere un enfoque flexible para la administración de recursos de red. Las infraestructuras de red existentes pueden responder a los requisitos cambiantes relacionados con la administración de los flujos de tráfico utilizando las configuraciones de calidad de servicio (QoS) y de ajustes de nivel de seguridad para los flujos individuales. Sin embargo, en empresas grandes que utilizan equipos de varios proveedores, cada vez que se activa una nueva VM, la reconfiguración necesaria puede llevar mucho tiempo.
- La infraestructura de red también puede verse beneficiada gracias a la virtualización. Funciones de Red que pueden ser virtualizadas. Cada dispositivo de red se puede segmentar en varios dispositivos virtuales, los cuales funcionan como dispositivos independientes. Entre los ejemplos se incluyen subinterfaces, interfaces virtuales, VLAN y tablas de enrutamiento. El enrutamiento virtualizado se denomina enrutamiento y reenvío virtuales (VRF).

Redes definidas por software

Plano de control y plano de datos

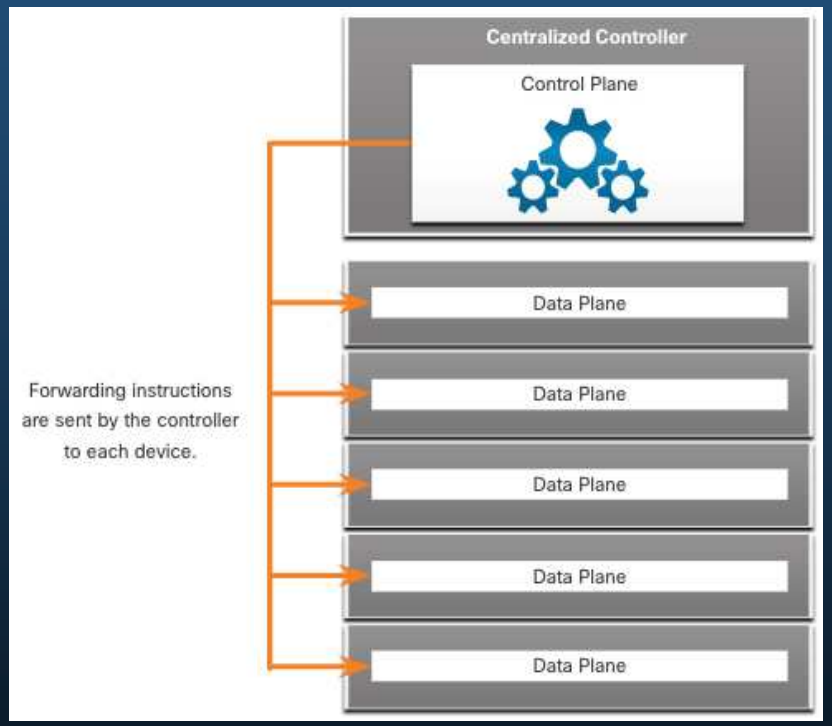
Un dispositivo de red contiene los siguientes planos:

- **Plano de control** - Suele considerarse el cerebro del dispositivo. Se utiliza para tomar decisiones de reenvío. El plano de control contiene los mecanismos de reenvío de ruta de Capa 2 y Capa 3, como las tablas de vecinos de protocolo de routing y las tablas de topología, las tablas de routing IPv4 e IPv6, STP, y la tabla ARP. La información que se envía al plano de control es procesada por la CPU.
- **Plano de datos** - También conocido como plano de reenvío, este plano suele ser la estructura de switch que conecta lo varios puertos de red de un dispositivo. El plano de datos de cada dispositivo se utiliza para reenviar los flujos de tráfico. Los routers y los switches utilizan la información del plano de control para reenviar el tráfico entrante desde la interfaz de egreso correspondiente. Por lo general, la información del plano de datos es procesada por un procesador especial del plano de datos, sin que se involucre a la CPU.

Redes definidas por software

Plano de control y plano de datos

- CEF es una tecnología de switching de IP de capa 3 que permite que el reenvío de los paquetes ocurra en el plano de datos sin que se consulte el plano de control.
- SDN consiste básicamente en la separación del plano de control y el plano de datos. La función del plano de control es eliminada de cada dispositivo, y la misma es realizada desde un controlador central. El controlador centralizado comunica las funciones del plano de control a cada dispositivo. Cada dispositivo ahora puede enfocarse en el envío de datos mientras el controlador centralizado administra el flujo de datos, mejora la seguridad y proporciona otros servicios.



Redes definidas por software

Plano de control y plano de datos

- El **plano de administración** se utiliza para administrar un dispositivo a través de su conexión a la red.
- Los administradores de red utilizan aplicaciones como Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), Secure FTP y Secure Hypertext Transfer Protocol (HTTPS) para acceder al plano de administración y configurar un dispositivo.
- El plano de administración es la forma en que ha accedido y configurado los dispositivos en sus estudios de redes. Además, protocolos como Simple Network Management Protocol (SNMP), utilizan el plano de administración.

Redes definidas por software

SDN

Se han desarrollado dos arquitecturas de red principales para admitir la virtualización de la red:

- **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.
- 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.**

Redes definidas por software

Tecnologías de Virtualización

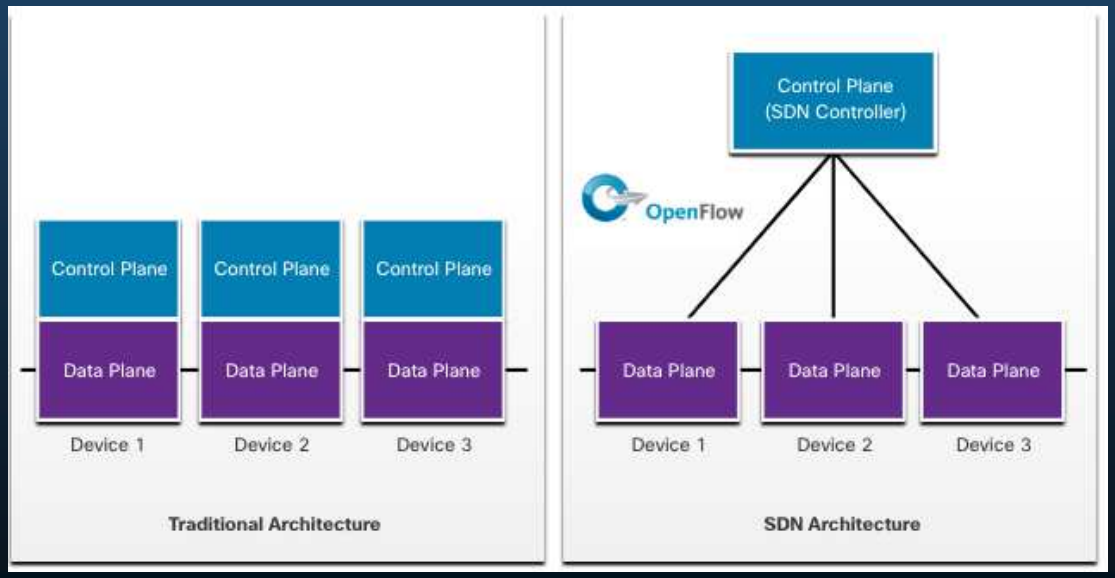
Los componentes de SDN pueden incluir los siguientes:

- OpenFlow: Este enfoque se desarrolló en la Universidad de Stanford para administrar el tráfico entre routers, switches, puntos de acceso inalámbrico y un controlador. El protocolo OpenFlow es un elemento básico en el desarrollo de soluciones de SDN.
- OpenStack: Este enfoque es una plataforma de virtualización y coordinación disponible para armar entornos escalables en la nube y proporcionar una solución de infraestructura como servicio (IaaS). OpenStack se usa frecuentemente en conjunto con Cisco ACI. La organización en la red es el proceso para automatizar el aprovisionamiento de los componentes de red como servidores, almacenamiento, switches, routers y aplicaciones.
- Otros componentes: **otros componentes incluyen la interfaz a Routing System (I2RS), la interconexión transparente de varios enlaces (TRILL), Cisco FabricPath (FP) e IEEE 802.1aq Shortest Path Bridging (SPB).**

Redes definidas por software

Arquitectura de SDN

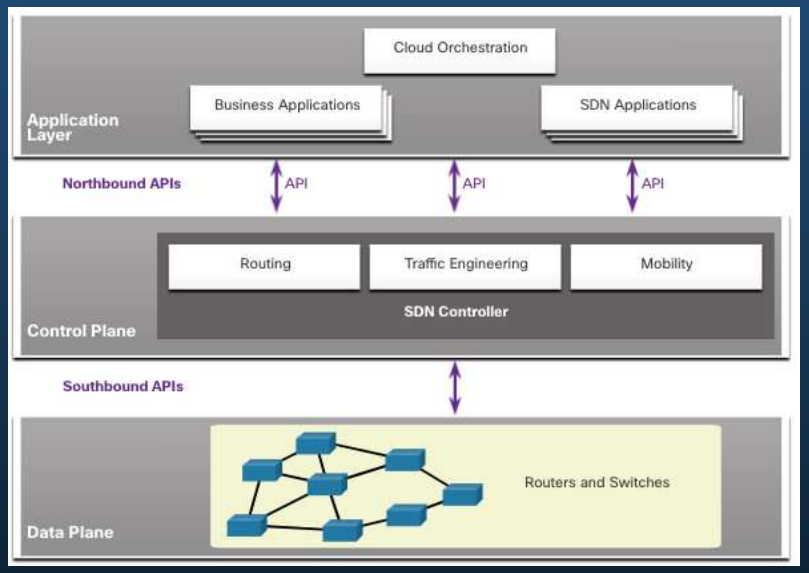
En un router o una arquitectura de switches tradicionales, el plano de control y las funciones del plano de datos se producen en el mismo dispositivo. Las decisiones de routing y el envío de paquetes son responsabilidad del sistema operativo del dispositivo. En SDN, la administración del plano de control se mueve a un controlador SDN centralizado. La figura compara la arquitectura tradicional contral SDN.



Redes definidas por software

Arquitectura tradicional y de SDN

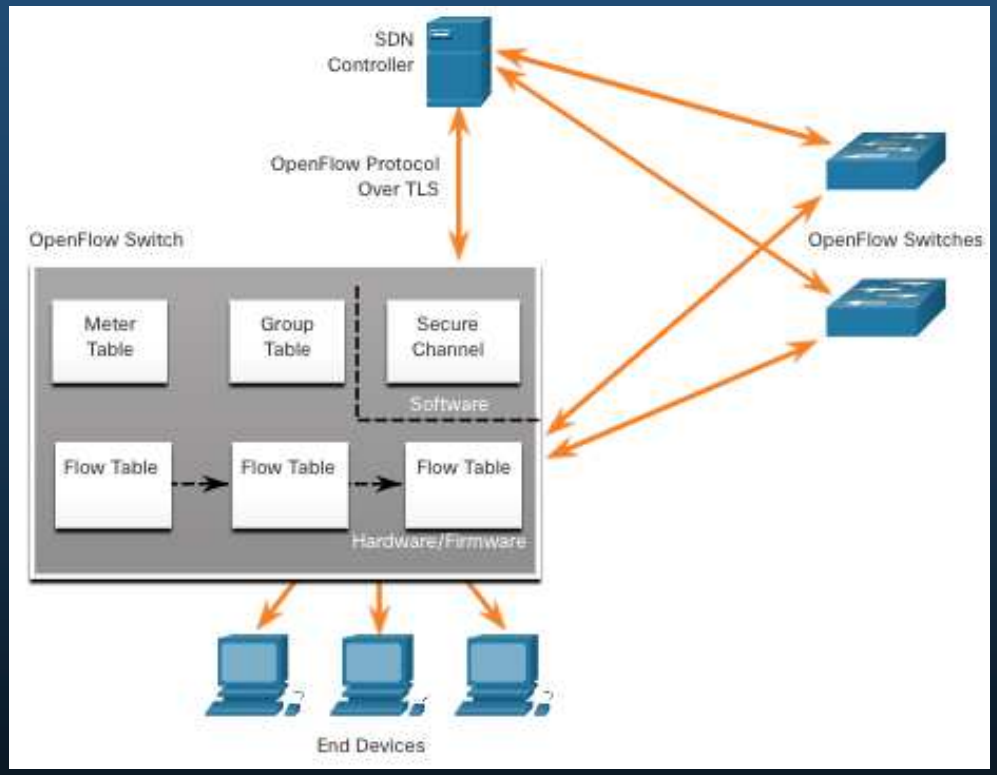
- El controlador de SDN es una entidad lógica que permite que los administradores de red administren y determinen cómo el plano de datos de switches y routers debe administrar el tráfico de red. Coordina, media y facilita la comunicación entre las aplicaciones y los elementos de red.
- El marco SDN completo se muestra en la figura. Observe el uso de interfaces de programación de aplicaciones (API) Una API es un conjunto de solicitudes estandarizadas que definen la forma adecuada para que una aplicación solicite servicios de otra aplicación.
- El controlador de SDN usa los API ascendentes para comunicarse con las aplicaciones ascendentes, ayudando al administrador a configurar servicios. El controlador de SDN también utiliza interfaces API descendentes para definir el comportamiento de los switches y routers virtuales descendentes. OpenFlow es la API original descendente ampliamente implementada.



Controladores

Controlador de SDN y operaciones

- El controlador SDN define los flujos de datos entre el plano de control centralizado y los planos de datos en routers y switches individuales.
- Cada flujo que viaja por la red debe primero obtener permiso del controlador SDN, que verifica que la comunicación esté permitida según la política de red.
- El controlador realiza todas las funciones complejas. El controlador completa las tablas de flujo. Los switches administran las tablas de flujo.



Controladores

Controlador de SDN y operaciones

Dentro de cada switch, se utiliza una serie de tablas implementadas en el hardware o el firmware para administrar flujos de paquetes a través del switch. Para el switch, un flujo es una secuencia de paquetes que coincide con una entrada específica en una tabla de flujo.

Los tres tipos de tablas que se muestran en la figura anterior son los siguientes:

- **Tabla de flujo** - Esta tabla asigna los paquetes entrantes a un flujo determinado y especifica las funciones que deben realizarse en los paquetes. Puede haber tablas de flujo múltiples que funcionan a modo de canalización.
- **Tabla de grupos** - Una tabla de flujo puede dirigir un flujo a una tabla de grupos, que puede alimentar una variedad de acciones que afecten a uno o más flujos.
- **Tabla de medidor** - Esta tabla activa una variedad de acciones relacionadas con el funcionamiento en un flujo**.**

Controladores

Vídeo de controladores - Cisco ACI

- Muy pocas organizaciones tienen realmente el deseo o las habilidades para programar la red utilizando las herramientas de SDN. Sin embargo, la mayoría de las organizaciones desea automatizar la red, acelerar la implementación de aplicaciones y alinear sus infraestructuras de TI para cumplir mejor con los requisitos empresariales. Cisco desarrolló la Infraestructura centrada en aplicaciones (ACI) para alcanzar los siguientes objetivos de maneras más avanzadas y más innovadoras que antes los enfoques de SDN.
- Cisco ACI es una solución de hardware diseñada específicamente para integrar la computación en la nube con la administración de centros de datos. En un nivel alto, el elemento de políticas de la red se elimina del plano de datos. Esto simplifica el modo en que se crean redes del centro de datos.

Controladores

Componentes principales de ACI

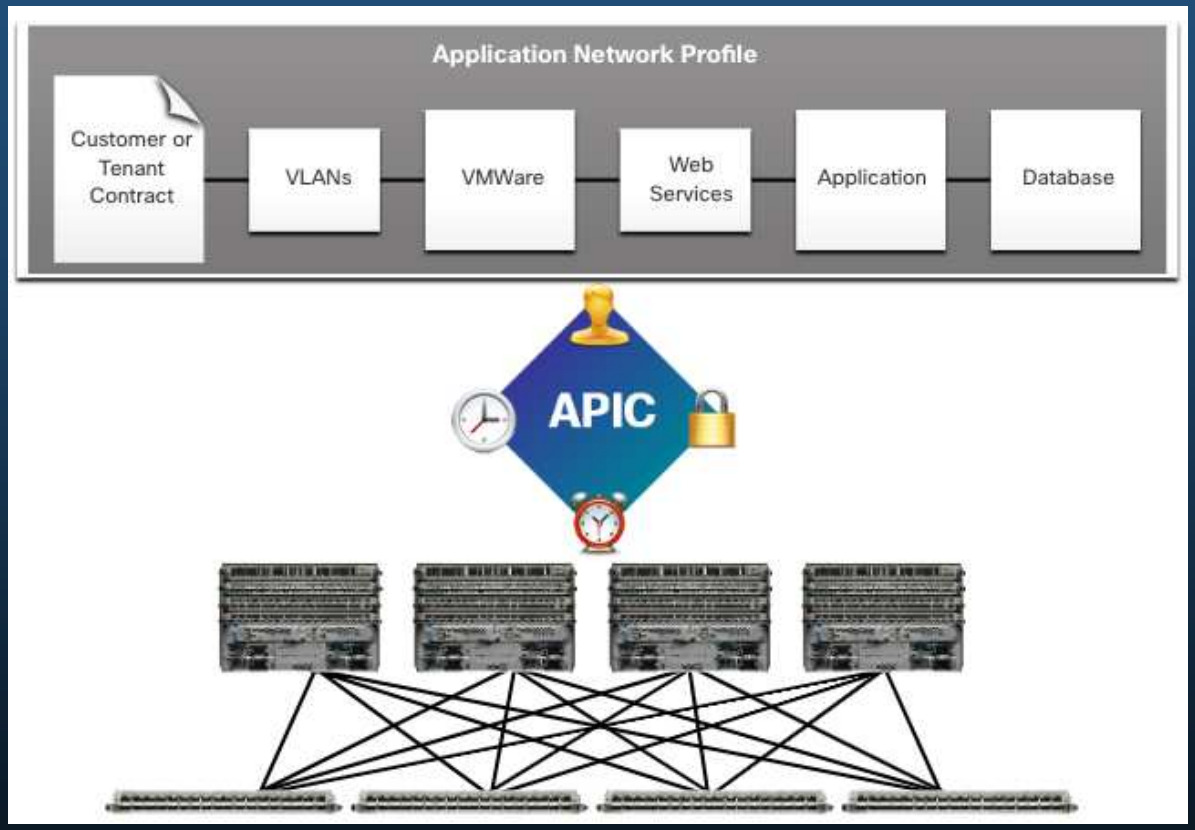
Estos son los tres componentes principales de la arquitectura de ACI:

- **Perfil de aplicación de red (ANP)** - Un ANP es una colección de grupos de terminales (EPG) con sus conexiones y las políticas que definen dichas conexiones.
- **Controlador de infraestructura de política de aplicación (APIC)** - El APIC es un controlador centralizado de software que administra y opera una estructura agrupada ACI escalable. Está diseñado para la programabilidad y la administración centralizada. Traduce las políticas de las aplicaciones a la programación de la red.
- **Switches de la serie 9000 de Cisco Nexus** - Estos switches proporcionan una estructura de switching con reconocimiento de aplicaciones y operan con un APIC para administrar la infraestructura virtual y física de la red.

El APIC se ubica entre el APN y la infraestructura de red habilitada con ACI. El APIC traduce los requisitos de aplicaciones a una configuración de red para cumplir con esas necesidades.

Controladores

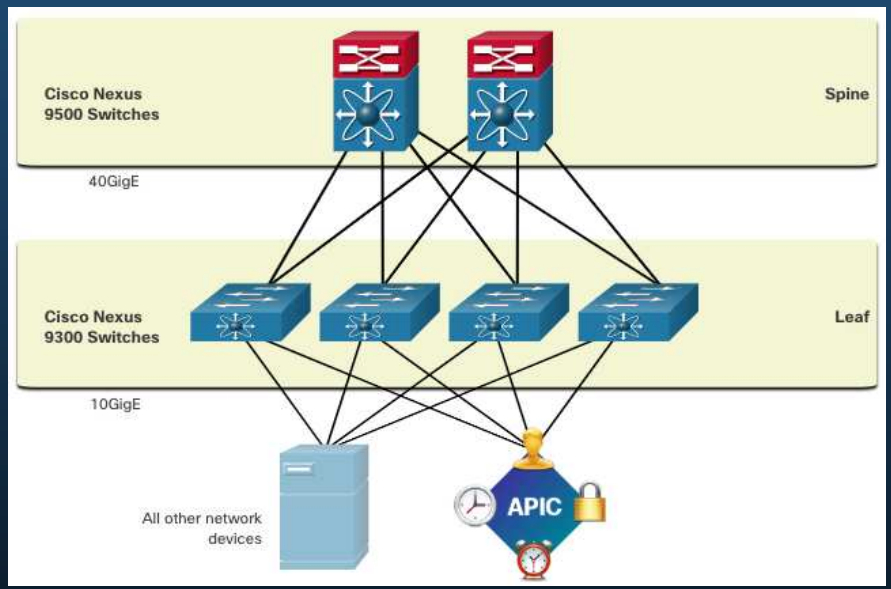
Componentes principales de ACI



Controladores

Topología Spine-Leaf

- La estructura Cisco ACI está compuesta por la APIC y los switches de la serie 9000 de Cisco Nexus mediante topología de nodo principal y secundario de dos niveles, como se muestra en la figura. Los switches de nodo secundario siempre se adjuntan a los nodos principales, pero nunca se adjuntan entre sí. De manera similar, los switches principales solo se adjuntan a la hoja y a los switches de núcleo (no se muestran). En esta topología de dos niveles, todo está a un salto de todo lo demás.
- En comparación con una SDN, el controlador de APIC no manipula la ruta de datos directamente. En cambio, el APIC centraliza la definición de políticas y programas a los que cambia el nodo secundario para reenviar tráfico según las políticas definidas.

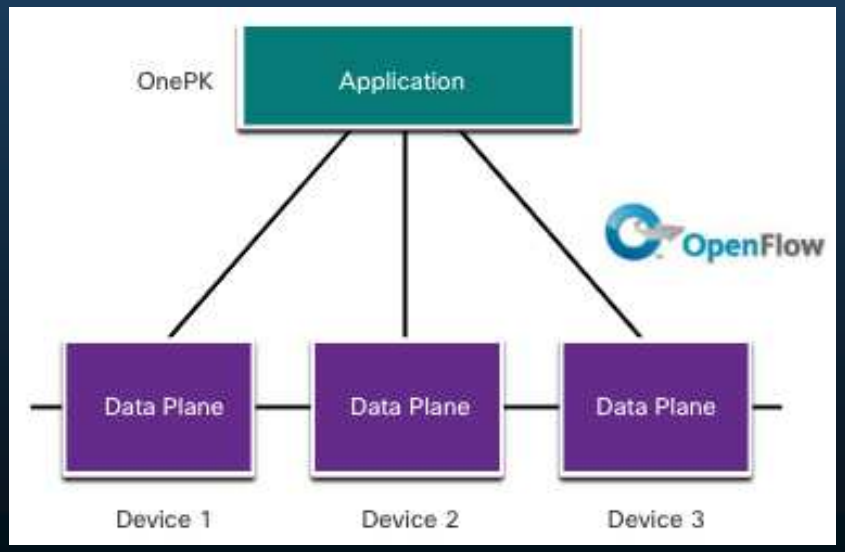


Controladores

Tipos de SDN

El Módulo empresarial del Controlador de infraestructura de política de aplicación (APIC-EM) de Cisco amplía las capacidades de ACI para las instalaciones empresariales y de campus. Para entender mejor APIC-EM, es útil obtener una perspectiva más amplia de los tres tipos de SDN:

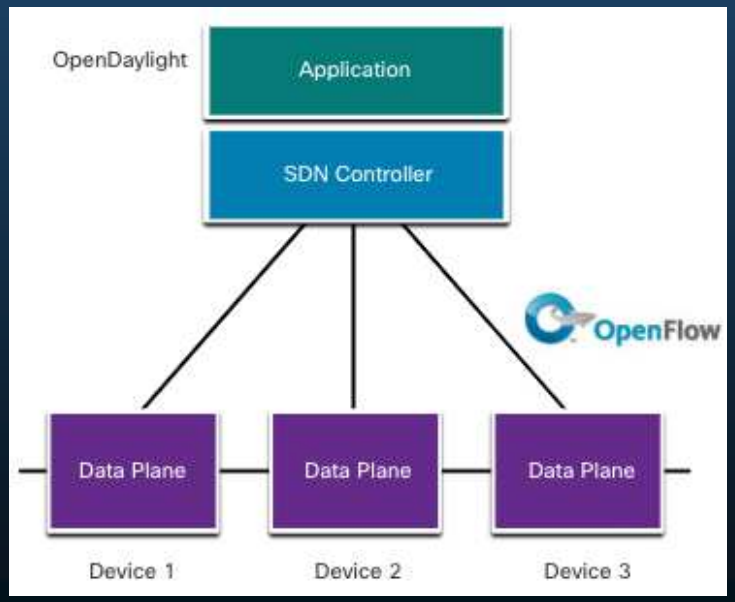
- **SDN basada en dispositivos:** Los dispositivos son programables mediante aplicaciones que se ejecutan en el dispositivo mismo o en un servidor en la red, como se muestra en la figura.



Controladores

Tipos de SDN

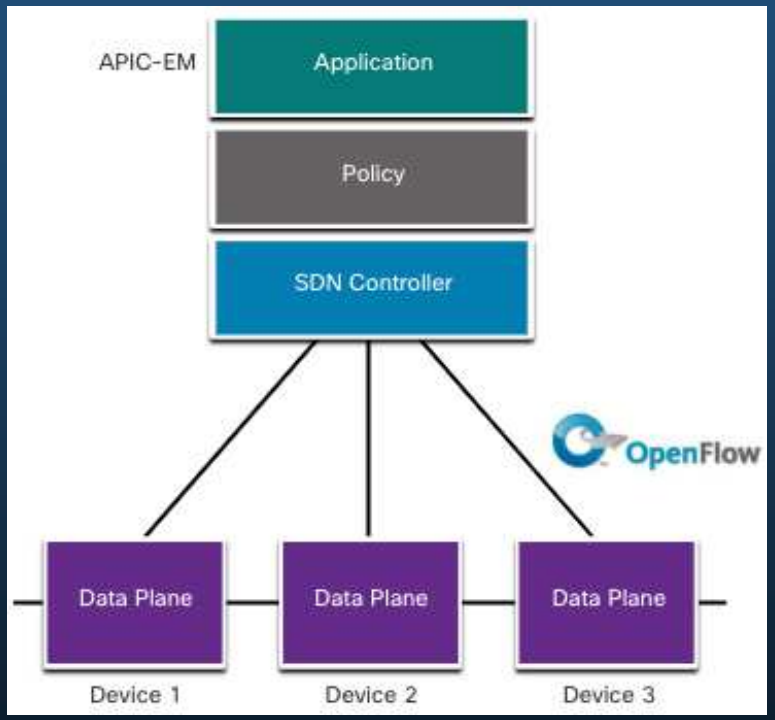
SDN basado en controlador: Este tipo de SDN usa un controlador centralizado que tiene conocimiento de todos los dispositivos de la red, como se ve en la figura. Las aplicaciones pueden interactuar con el controlador responsable de administrar los dispositivos y de manipular los flujos de tráfico en la red. El controlador SDN Cisco Open es una distribución comercial de Open Daylight.



Controladores

Tipos de SDN

SDN basada en políticas: Este tipo de SDN es parecido al SDN basado en controlador, ya que un controlador centralizado tiene una vista de todos los dispositivos de la red, como se ve en la figura El SDN basado en políticas incluye una capa de políticas adicional que funciona a un nivel de abstracción mayor. Usa aplicaciones incorporadas que automatizan las tareas de configuración avanzadas mediante un flujo de trabajo guiado y una GUI fácil de usar. No se necesitan conocimientos de programación. Cisco APIC-EM es un ejemplo de este tipo de SDN.

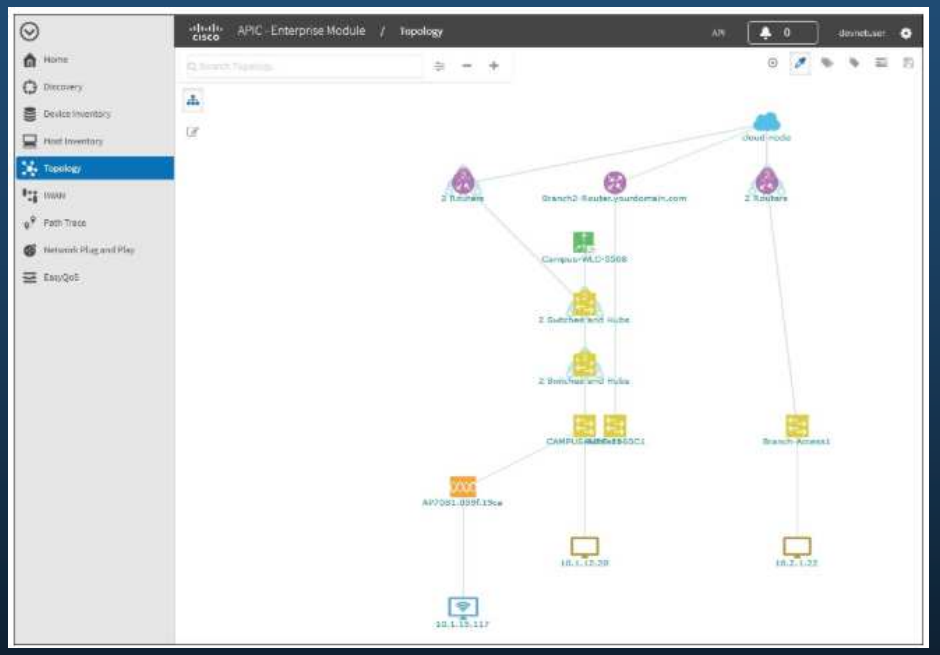


Controladores

Funciones de APIC-EM

Cisco APIC-EM proporciona una interfaz única para la administración de red que incluye:

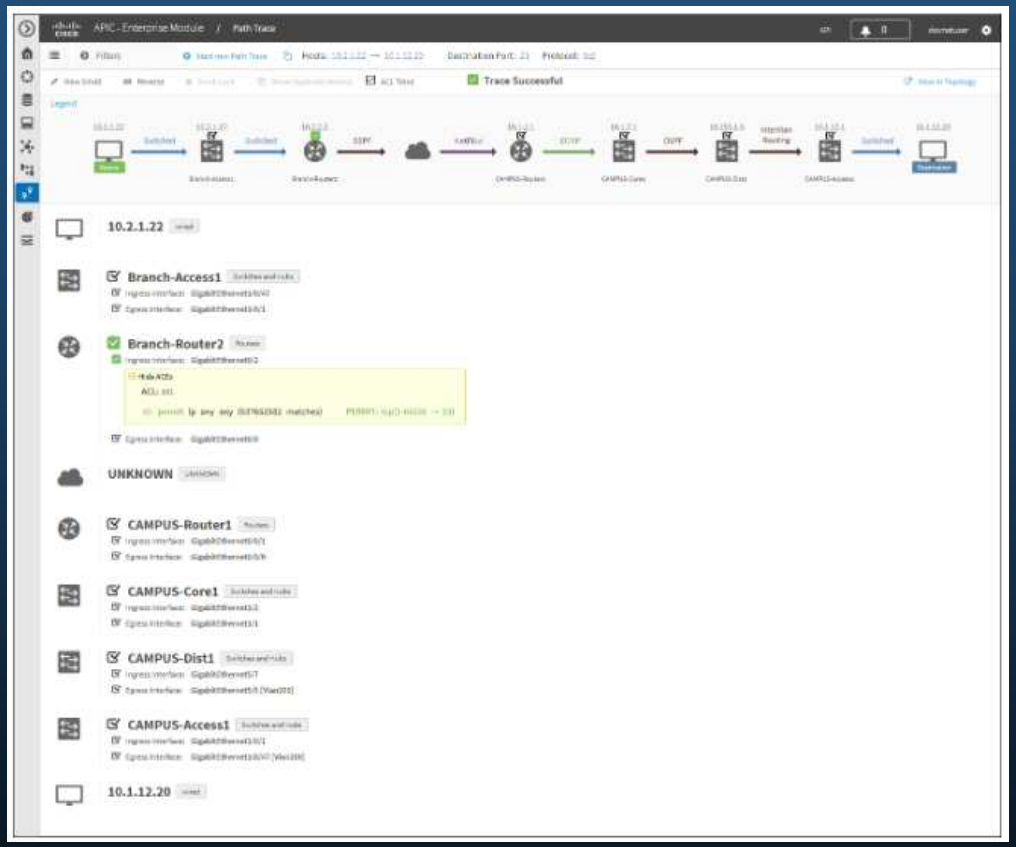
- Descubrir y acceder a inventarios de dispositivos y hosts.
- Visualización de la topología (como se muestra en la figura).
- Rastreo de una ruta entre los puntos finales.
- Establecer directivas.



Controladores

Seguimiento de ruta de APIC-EM

El análisis y el seguimiento de ruta de las ACL permiten que el administrador visualice fácilmente flujos de tráfico y descubra las entradas de ACL conflictivas, duplicadas o sombreadas. Esta herramienta examina las ACL específicas en la ruta entre dos nodos finales y muestra todos los problemas potenciales. Puede ver dónde las ACL a lo largo de la ruta permitieron o denegaron el tráfico, como se muestra en la figura. Observe cómo Branch-Router2 permite todo el tráfico. El administrador de red ahora puede realizar ajustes, si es necesario, para filtrar mejor el tráfico.



Capítulo 14

Automatización de la red

Descripción general de la automatización

El aumento de la automatización

Estos son algunos de los beneficios de la automatización:

- Las máquinas pueden trabajar las 24 horas sin interrupciones, por ende brindan una mayor producción.
- Las máquinas proporcionan un resultado más uniforme.
- La automatización permite la recolección de grandes cantidades de datos, los cuales pueden analizarse rápidamente, para proporcionar información que guíe un evento o proceso.
- Los robots se utilizan en condiciones peligrosas como la minería, la lucha contra incendios y la limpieza de accidentes industriales. Esto reduce el riesgo para las personas.
- Bajo ciertas circunstancias, los dispositivos inteligentes pueden alterar su uso de energía, realizar diagnósticos médicos y mejorar la conducción de los automóviles para que sea más segura.

Descripción general de la automatización

Dispositivos de pensamiento

- Actualmente muchos dispositivos incorporan tecnologías inteligentes que ayudan a determinar su comportamiento. Esto puede ser tan simple como cuando un dispositivo inteligente reduce su consumo de energía durante períodos de alta demanda o tan complejo como conducir un auto de manera autónoma.
- Cada vez que un dispositivo toma una decisión, en función de información externa, dicho dispositivo se conoce como un dispositivo inteligente. En la actualidad muchos dispositivos con los que interactuamos llevan la palabra inteligente en el nombre. Esto indica que el dispositivo tiene la capacidad para alterar su comportamiento según su entorno.
- Para que un dispositivo pueda "pensar" el mismo debe ser programado utilizando herramientas de automatización de red.

Formato de datos

El concepto de Formato de Datos

- Los formatos son simplemente una manera de almacenar e intercambiar datos de una manera estructurada. Uno de esos formatos es el Lenguaje de marcas de hipertexto (Hypertext Markup Language - HTML). HTML es un estándar que describe la estructura de las páginas web, como se aprecia en la imagen.
- Existen algunos formatos de datos comunes que son usados en muchas aplicaciones incluidas automatización de la red y programación:
  - Notación de objeto de JavaScript (JavaScript Object Notation - JSON)
  - Lenguaje de marcado extensible (XML)
  - YAML no es un lenguaje de marcado (YAML)
- El formato de datos seleccionado dependerá del formato que es usado por la aplicación, herramienta o las instrucciones que usted esté usando. Muchos sistemas pueden soportar más de un formato, lo que le permite al usuario elegir el preferido.

Formato de datos

Reglas de formato de datos

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:

- La sintaxis, la cual incluye diferentes tipos de símbolos como [], ( ), { }, el uso de espacio, o sangría, comillas, comas y más.
- Cómo se representan los objetos como caracteres, una cadena de caracteres, una lista y vectores.
- Cómo se representan los pares llave/valor (key/value). La llave (key) usualmente se encuentra al lado izquierdo e identifica o describe los datos. El valor (value) 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.


```
{"message": "success", "timestamp": 1560789216, "iss_position": {"latitude": "25.9990",
"longitude": "-132.6992"}}
```

Formato de datos

Comparar formato de datos

```
{
 "mensaje": "éxito",
         "marca de tiempo":
1560789260,
         "iss_position": {
 "latitud": "25.9990", "longitud":
"-132.6992"
         }
}
```

Formato JSON

```
mensaje: éxito
marca de tiempo: 1560789260
iss_position:
         latitud: '25.9990'
longitud:: '-132.6992'
```

Formato YAML

```
<?xml version="1.0" encoding="UTF-8" ?>
<root>
<message>success</message>
<timestamp>1560789260</timestamp>
<iss_position>
   <latitude>25.9990</latitude>
   <longitude>-132.6992</longitude>
</iss_position>
</root>
```

Formato XML

Formato de datos

Formatos de dato JSON

- JSON es un formato legible para humanos, usado por aplicaciones para almacenar, transferir y leer información. JSON es relativamente popular y es usado por servicios web y API para brindar información pública. Esto se debe a que es fácil de analizar y puede ser usado con la mayoría de lenguajes de programación moderno, entre ellos Python.

Formato de datos

Formatos de dato JSON

```
GigabitEthernet0/0/0 is up, line protocol is up (connected)
   Description: Wide Area Network
   Internet address is 172.16.0.2/24
```

Compare la salida IOS anterior a la salida en formato JSON. Nótese que cada objecto (cada par de llave/valor) es una porción de información diferente acerca de las interfaces, incluyendo su nombre, una descripción, y si se encuentra habilitada.

```
{
"ietf-interfaces:interface": {
 "name": "GigabitEthernet0/0/0",
         "description": "Wide Area Network”,
         "enabled": true,
         "ietf-ip:ipv4": {
                  "address": [
                           {
                           "ip": "172.16.0.2",
                           "netmask": "255.255.255.0"
                           }
                  ]
         }
  }
}
```

Formato de datos

Reglas de sintaxis JSON

Estas son algunas de las características de el formato JSON:

- JSON utiliza una estructura jerárquica y contiene valores anidados.
- Utiliza llaves { } para almacenar objetos y corchetes [ ] para almacenar vectores.
- Su información es escrita en pares llave/valor (key/value).

En JSON, la información conocida como objetos consiste en uno o más pares de llaves/valores (key/value) contenidos dentro de llaves { }. La sintaxis de un objeto JSON incluye:

- Las llaves deben ser cadenas de caracteres contenidas dentro de comillas " ".
- Los valores deben ser un tipo de información válida (cadena de caracteres, números, vectores, valores booleanos, caracteres nulos u otro objeto).
- Las llaves y los valores son separados por dos puntos (:).
- Múltiples pares de llaves/valores dentro de un objeto se separan mediante comas.
- El espacio en blanco no es significativo.

Formato de datos

Reglas de sintaxis JSON

En ocasiones una llave puede tener mas de un valor. Esto es conocido como un vector. Un vector en JSON es una lista ordenada de valores. Las características de un vector en JSON incluyen:

- La llave debe estar seguida por dos puntos (:) y una lista de valores contenidos dentro de corchetes [].
- Un vector en JSON es una lista ordenada de valores.
- Un vector puede almacenar diferentes tipos de valores como caracteres, números, valores booleanos, objetos u otro vector.
- Cada valor dentro del vector es separado por una coma.

Formato de datos

Reglas de sintaxis JSON

Por ejemplo, una lista de direcciones IPv4 podría verse de la siguiente manera. La llave es “addresses”. Cada entrada de la lista es un objecto independiente, separado por llaves { }. Los objetos son dos pares de llaves/valores: una dirección IPv4 ("ip") y una máscara de red ("netmask") separados por una coma. El vector es una lista separada por una coma seguido de una llave de cierre.

```
{
   "addresses": [
       {
 "ip": "172.16.0.2",
 "netmask": "255.255.255.0"
       },
       {
 "ip": "172.16.0.3",
 "netmask": "255.255.255.0"
       },
       {
 "ip": "172.16.0.4",
 "netmask:": "255.255.255.0"
       }
   ]
}
```

Formato de datos

Formato de datos YAML

YAML es otro tipo de formato usado por aplicaciones para almacenar, transferir y leer información, el cual es legible por humanos. Algunas de las características de YAML incluyen:

- Es considerado una versión mejorada de JSON.
- Tiene un formato minimalista, lo cual lo hace fácil de leer y escribir.
- Utiliza la sangría para definir su estructura, sin utilizar.

Formato de datos

Formato de datos YAML

```
{
   "ietf-interfaces:interface": {
 "name": "GigabitEthernet2",
 "description": "Wide Area Network",
 "enabled": true,
      "ietf-ip:ipv4": {
         "address": [
            {
 "ip": "172.16.0.2",
 "netmask": "255.255.255.0"
            },
            {
 "ip": "172.16.0.3",
 "netmask": "255.255.255.0"
            },
            {
 "ip": "172.16.0.4",
 "netmask": "255.255.255.0"
            }
         ]
      }
   }
}
```

- La salida IOS en JSON está a la izquierda. Los mismos datos en formato YAML están abajo. Es más fácil de leer.
- Similar a JSON, un objeto en YAML se compone de uno o más pares de llaves/valores. Las llaves y los valores, son separados por medio de dos puntos sin el uso de comillas. En YAML, un guion es usado para separar cada elemento de un lista.

```
ietf-interfaces:interface:
 name: GigabitEthernet2
 description: Wide Area Network
 enabled: true
   ietf-ip:ipv4:
      address:
         - ip: 172.16.0.2
 netmask: 255.255.255.0
 - ip: 172.16.0.3
 netmask: 255.255.255.0
 - ip: 172.16.0.4
           netmask: 255.255.255.0
```

Formato de datos

Formato de datos XML

XML es un formato que es más legible para humanos y se utiliza para almacenar, transferir y leer información desde aplicaciones. Algunas de las características de XML incluyen:

- Es similar a HTML , el cual es el lenguaje de mercado generalizado para la creación de páginas y aplicaciones web.
- Es auto-descriptivo, contiene información dentro de un conjunto de etiquetas: **<tag>data</tag>**
- A diferencia de HTML, XML no utiliza etiquetas predefinidas, ni una estructura de documento.

Los objetos XML son uno o más pares clave / valor, con la etiqueta de inicio utilizada como nombre de la clave: **<key>value</key>**

Formato de datos

Formato de datos XML

El siguiente ejemplo muestra la misma información de GigabitEthernet2 en formato XML. Nótese como los valores están contenidos dentro de las etiquetas de objeto. En este ejemplo, cada par de llave/valor está en una línea separada y en algunas se utiliza sangría. Esto último no es requerido, pero se utiliza para mejorar la lectura. La lista utiliza instancias repetidas de **<tag></tag>** para cada elemento de la lista. Los elementos dentro de estas instancias representan uno o más pares de llave/valor.

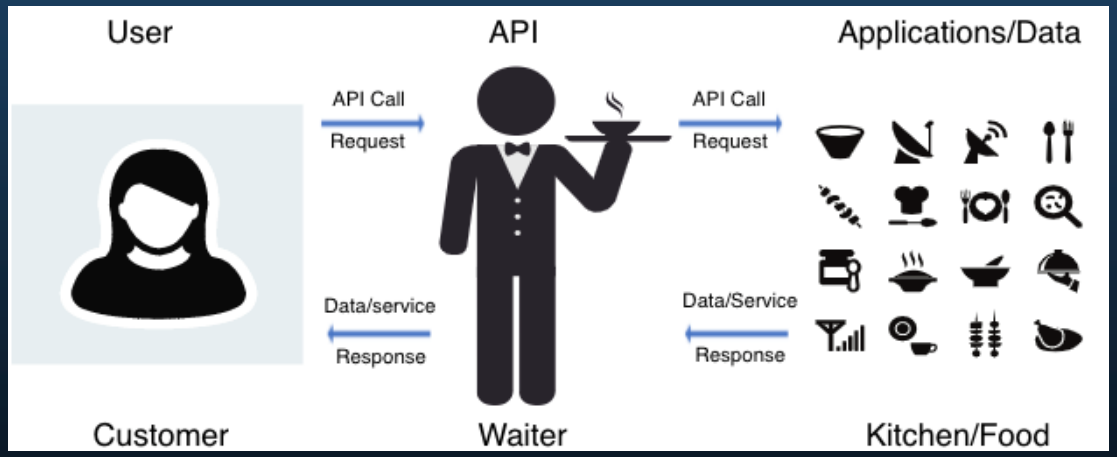
```
<?xml version="1.0" encoding="UTF-8" ?>
<ietf-interfaces:interface>
   <name>GigabitEthernet2</name>
   <description>Wide Area Network</description>
   <enabled>true</enabled>
   <ietf-ip:ipv4>
      <address>
         <ip>172.16.0.2</ip>
         <netmask>255.255.255.0</netmask>
      </address>
      <address>
         <ip>172.16.0.3</ip>
 <netmask>255.255.255.0</netmask>
      </address>
      <address>
         <ip>172.16.0.4</ip>
         <netmask>255.255.255.0</netmask>
      </address>
   </ietf-ip:ipv4>
</ietf-interfaces:interface>
```

14.3 APIs

APIs

El concepto de API

- API es un programa que permite a otras aplicaciones accesar a su información o a sus servicios. Es un conjunto de reglas que describe como 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.
- Una API es similar a un mesero en un restaurante, como se muestra en el siguiente ejemplo.



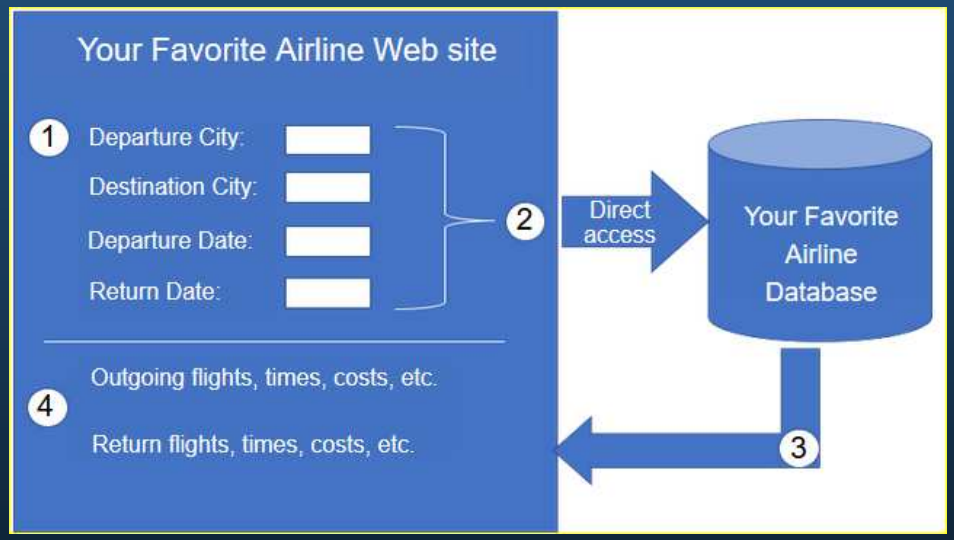
APIs

Un ejemplo de API

Para entender realmente cómo se pueden utilizar las API para proporcionar datos y servicios, veremos dos opciones para generar reservas de aerolíneas.

La primera opción utiliza el sitio web de una aerolínea específica, como se muestra en la figura. Mediante el sitio web de la aerolínea, el usuario ingresa la información para realizar una solicitud de reserva.

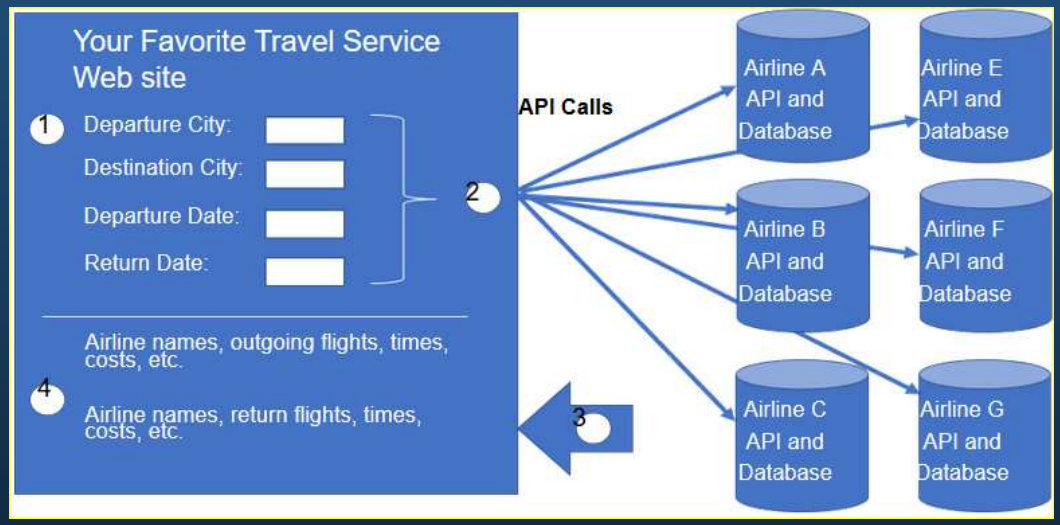
El sitio web interactúa directamente con la propia base de datos de la aerolínea y proporciona al usuario información que coincide con la solicitud del usuario.



APIs

Un ejemplo de API

Los usuarios pueden utilizar un sitio de viaje para acceder a esta misma información, no sólo desde una aerolínea específica, sino una variedad de aerolíneas. En este caso, el usuario introduce información de reserva similar. El sitio web del servicio de viajes interactúa con las diversas bases de datos de aerolíneas mediante las API proporcionadas por cada aerolínea. El servicio de viajes utiliza el API de cada aerolínea para solicitar información de esa aerolínea específica y luego muestra la información de todas las aerolíneas en su página web.



La API actúa como una especie de mensajero entre la aplicación solicitante y la aplicación en el servidor que proporciona los datos o el servicio. El mensaje de la aplicación solicitante al servidor donde residen los datos se conoce como una llamada a la API.

APIs

API abiertas, internas y de socios

Una consideración importante al desarrollar una API es la distinción entre API abiertas, internas y APIs de partner:

- **API abiertas o API públicas -** Estas API están disponibles públicamente y se pueden usar sin restricciones. Dado que estas API son públicas, muchos proveedores de API, como Google Maps, requieren que el usuario obtenga una clave gratuita, o token, antes de usar la API. Esto es para ayudar a controlar la cantidad de solicitudes API que reciben y procesan.
- **API internas o privadas -** Estas son API que utiliza una organización o empresa para acceder a datos y servicios solo para uso interno. Un ejemplo de una API interna es permitir a los vendedores autorizados acceder a los datos de ventas internos en sus dispositivos móviles.
- **API de socios:-** son APIs que se utilizan entre una empresa y sus socios comerciales o contratistas para facilitar el negocio entre ellos. El socio comercial debe tener una licencia u otra forma de permiso para usar la API. Un servicio de viaje que utiliza la API de una aerolínea es un ejemplo de una API de socio.

APIs

Tipos de APIs de servicios web

Un servicio web es un servicio que está disponible a través de Internet, utilizando la World Wide Web. Existen cuatro tipos de APIs de servicios web:

- Protocolo Simple de Acceso a Objetos (SOAP)
- Transferencia de Estado Representacional (REST)
- Llamada a procedimiento remoto de lenguaje de marcado extensible (XML-RPC)
- Llamada a procedimiento remoto de notación de objetos JavaScript (JSON-RPC)

Característica	SOAP	REST	XML-RPC	JSON-RPC
Formato de datos	XML	JSON, XML, YAML y otros	XML	JSON
Año de lanzamiento	1998	2000	1998	2005
Puntos fuertes	Bien establecido	Formateo flexible y más utilizado	Bien establecida, simplicidad	Simplicidad

REST

REST y RESTful API

- Los exploradores web utilizan HTTP o HTTPS para solicitar (GET) una página web. Si se solicita correctamente (código de estado HTTP 200), los servidores web responden a las solicitudes GET con una página web codificada HTML, como se muestra en la figura.
- 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.
- El cumplimiento de las restricciones de la arquitectura REST generalmente se conoce como "RESTful". Una API puede considerarse "RESTful" si tiene las siguientes características:
  - **Cliente-Servidor:** - el cliente maneja el front-end y el servidor maneja el back-end. Cualquiera de los dos puede ser reemplazado independientemente del otro.
  - **Sin estado** - No se almacenan datos del cliente en el servidor entre solicitudes. El estado de la sesión se almacena en el cliente.
  - **Cacheable** - los clientes pueden almacenar en caché las respuestas localmente para mejorar el rendimiento.

REST

Implementación RESTful

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

- Identificador uniforme de recursos (URI) base para el servicio web, como http://example.com/resources.
- 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.
- El conjunto de operaciones admitidas por el servicio web utilizando métodos HTTP.
- La API debe estar controlada por hipertexto.

Las API RESTful utilizan métodos HTTP comunes, como POST, GET, PUT, PATCH y DELETE. Como se muestra en la tabla siguiente, se corresponden con operaciones RESTful: Crear, Leer, Actualizar y Eliminar (o CRUD).

Método HTTP	Operación RESTful
POST	Crear (Create)
GET	lectura (Read)
PUT/PATCH	Actualizar (Update)
DELETE	Eliminar (Delete)

REST

URI, URN, y URL

Los recursos web y los servicios web, como las API RESTful, se identifican mediante un URI. Un URI es una cadena de caracteres que identifica un recurso de red específico. Un URI tiene dos especializaciones:

- **Nombre uniforme de recursos (URL):**-identifica solo el espacio de nombres del recurso (página web, documento, imagen, etc.) sin referencia al protocolo.
- **Localizador uniforme de recursos (URL)**- - define la ubicación de red de un recurso específico en la red. HTTP or HTTPS URLs se usan típicamente con navegadores web. Otros protocolos como FTP, SFTP, SSH y otros pueden usar una dirección URL. Una URL que usa SFTP podría tener el siguiente aspecto: sftp://sftp.example.com

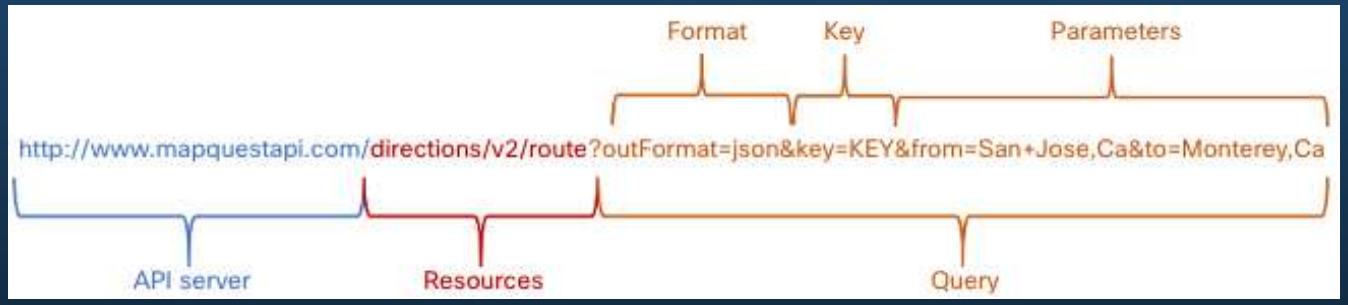
Estas son las partes del URI https://www.example.com/author/book.html#page155:

- **Protocolo/esquema:**– HTTPS u otros protocolos como FTP, SFTP, mailto, y NNTP
- **Nombre de host**-www.example.com
- Ruta y nombre de archivo **- /author1a/book2.html**
- **Fragmento**- #page155

REST

Anatomía de una solicitud RESTful

- En un servicio web RESTful, una solicitud realizada al URI de un recurso obtendrá una respuesta. La respuesta será una carga normalmente formateada en JSON, pero podría ser HTML, XML o algún otro formato. La figura muestra el URI de la API de direcciones de MapQuest. La solicitud de API es para indicaciones desde San José, California hasta Monterey, California.

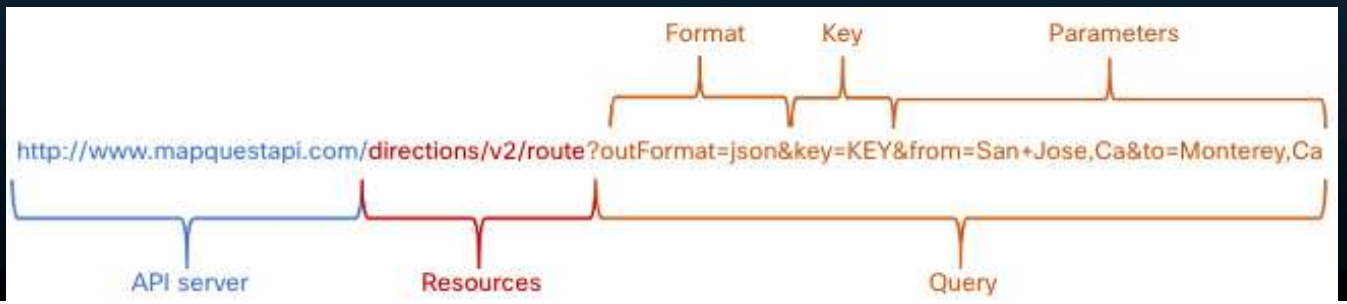


REST

Anatomía de una solicitud RESTful

Estas son las diferentes partes de la solicitud de API:

- **Servidor API:**- es la dirección URL del servidor que responde a las solicitudes REST. En este ejemplo es el servidor de la API de MapQuest.
- **Recursos**- - específica la API que se está solicitando. En este ejemplo es la API de direcciones de MapQuest.
- **Consulta**-específica el formato de datos y la información que el cliente solicita al servicio de API. Las consultas pueden incluir:
  - **Formato:**– Esto suele ser JSON, pero puede ser YAML o XML. En este ejemplo se solicita JSON.
  - **Clave:**- La clave es para autorización, si es necesario. MapQuest requiere una clave para su API de direcciones. En el URI anterior, deberá reemplazar "KEY" por una clave válida para enviar una solicitud válida.
  - **Parámetros**- - los parámetros se utilizan para enviar información relativa a la solicitud. En este ejemplo, los parámetros de consulta incluyen información acerca de las direcciones que necesita la API para que sepa qué direcciones devolver: "from-San+Jose,Ca" y "to-Monterey,Ca".



REST

Anatomía de una solicitud RESTful

Muchas API RESTful, incluidas las API públicas, requieren una clave. La clave se utiliza para identificar el origen de la solicitud a través de la autenticación. Estas son algunas razones por las que un proveedor de API puede requerir una clave:

- para autenticar la fuente y asegurarse de que esté autorizada para usar la API
- para limitar el número de personas que usan la API
- Para limitar el número de solicitudes por usuario.
- para capturar y rastrear mejor los datos que solicitan los usuarios
- para recopilar información sobre las personas que usan la API

Nota: La API MapQuest requiere una clave. Busque en Internet la URL para obtener una clave MapQuest. Utilice los parámetros de búsqueda: developer.mapquest. También puede buscar en Internet la URL actual que describe la política de privacidad de MapQuest.

REST

Aplicación RESTful API

- Muchos sitios web y aplicaciones utilizan las API para acceder a la información y proporcionar el servicio a sus clientes.
- Algunas solicitudes de API RESTful se pueden realizar escribiendo el URI desde un explorador web. La API de direcciones de MapQuest es un ejemplo de esto. Una solicitud de API RESTful también se puede realizar de otras maneras.
  - **Sitio web del desarrollador**: Los desarrolladores a menudo mantienen sitios web que incluyen información sobre la API, información de parámetros y ejemplos de uso. Estos sitios también pueden permitir al usuario realizar la solicitud de API dentro de la página web del desarrollador introduciendo los parámetros y otra información.
  - **Postman**:Postman es una aplicación para probar y usar las API de REST. Contiene todo lo necesario para construir y enviar solicitudes de API REST, incluida la introducción de claves y parámetros de consulta.
  - **Python**: Las API también se pueden invocar desde un programa Python. Esto permite una posible automatización, personalización e integración de aplicaciones de la API.
  - **Sistemas operativos de red**: Utilizando protocolos como NETCONF (NET CONFiguration) y RESTCONF, los sistemas operativos de red están comenzando a proporcionar un método alternativo para la configuración, el monitoreo y la administración.

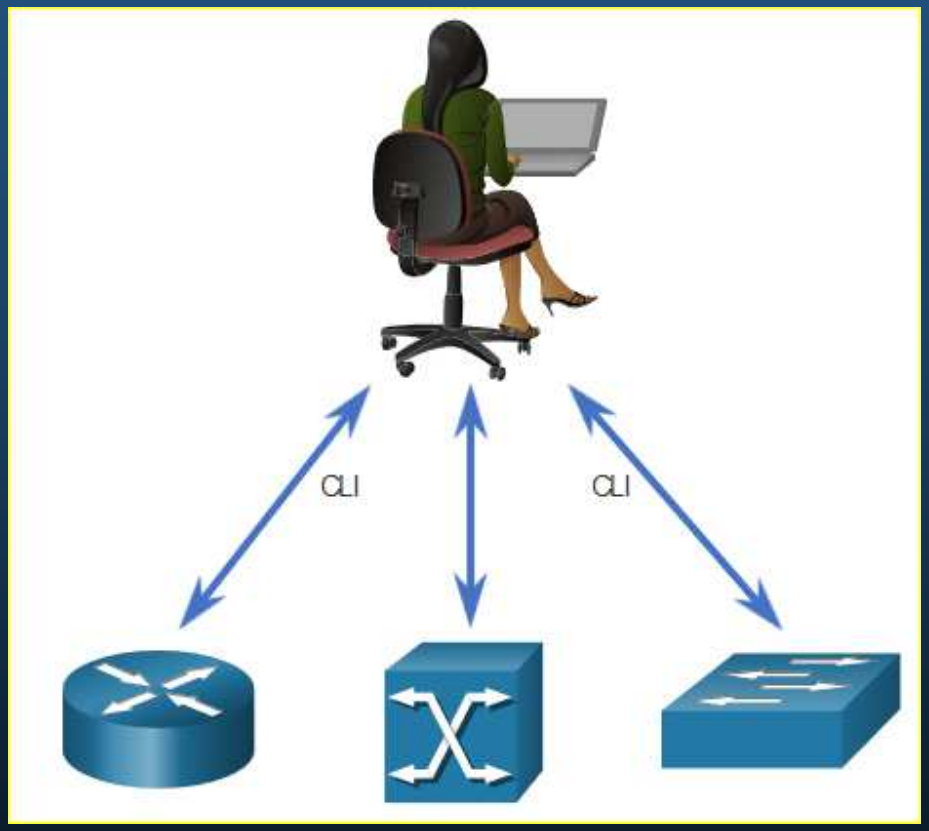
Herramientas de configuración

Configuración de red tradicional

Los dispositivos de red han sido configurados tradicionalmente por un administrador de red utilizando la CLI.

Siempre que haya un cambio o una nueva característica, los comandos de configuración necesarios se deben ingresar manualmente en todos los dispositivos apropiados.

Esto se convierte en un problema importante en redes más grandes o con configuraciones más complejas.

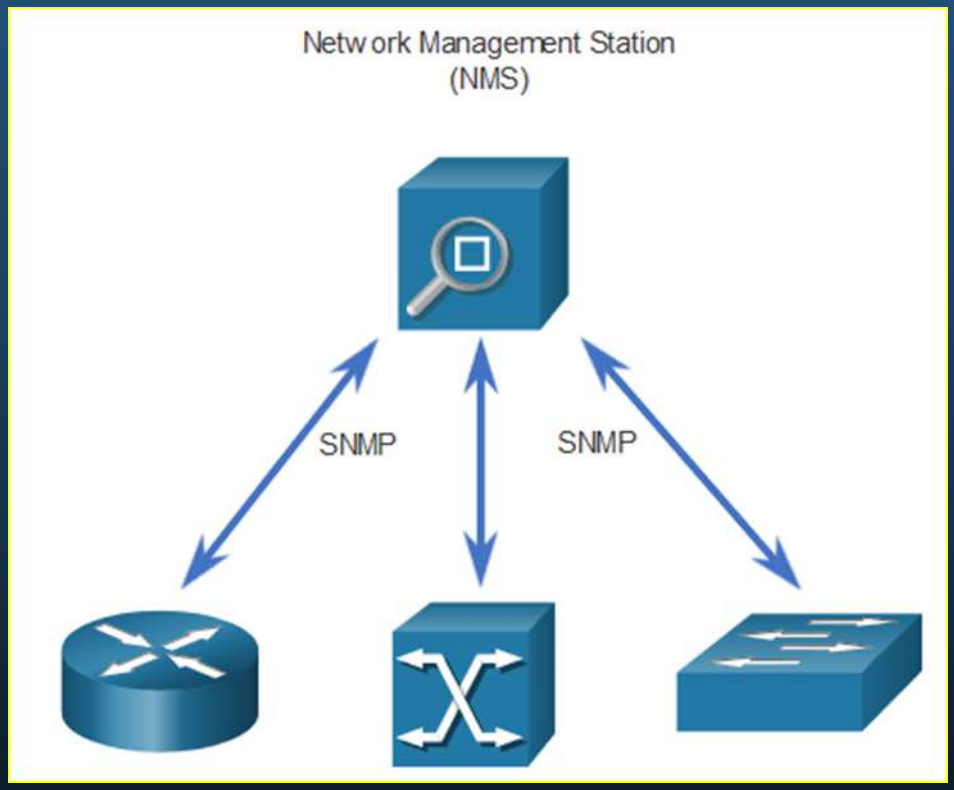


Herramientas de configuración

Configuración de red tradicional

El Protocolo simple de administración de red (SNMP) permite a los administradores gestionar nodos en una red IP. Mediante una estación de administración de red (NMS), que se muestra en la figura siguiente, SNMP permite a los administradores de red supervisar y administrar el rendimiento de la red, buscar y resolver problemas de red y realizar consultas para estadísticas. Sin embargo, no se utiliza normalmente para la configuración debido a problemas de seguridad y dificultad en la implementación.

También puede usar las API para automatizar la implementación y administración de recursos de red. En lugar de configurar manualmente puertos, listas de acceso, QoS y políticas de equilibrio de carga, puede usar herramientas para automatizar las configuraciones.

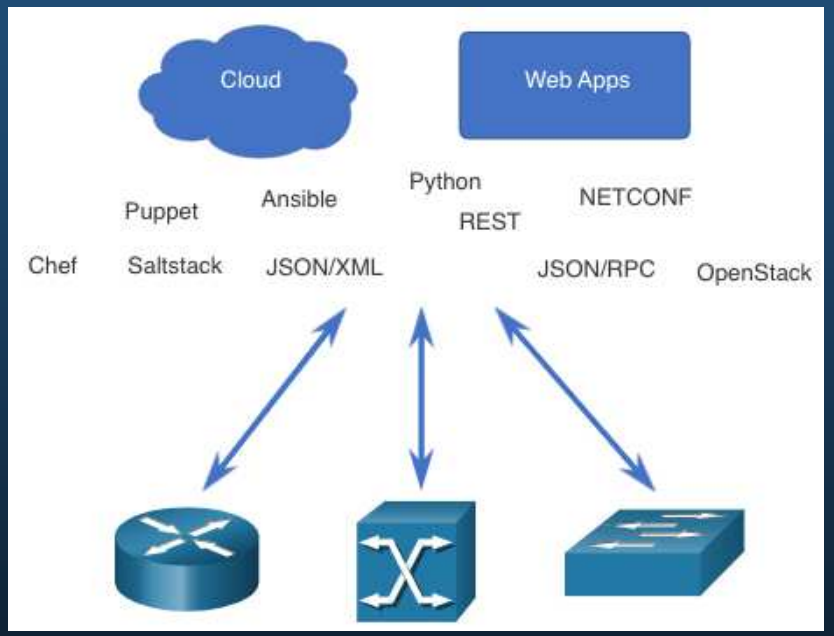


Herramientas de configuración

Automatización de redes

Nos estamos alejando rápidamente de un mundo en el que un administrador de red administra unas pocas docenas de dispositivos de red, a uno en el que están implementando y administrando cientos, miles e incluso decenas de miles de dispositivos de red complejos (tanto físicos como virtuales) con la ayuda de software. Esta transformación se está extendiendo rápidamente a todos los lugares de la red.

Existen métodos nuevos y diferentes para que los operadores de red supervisen, administren y configuren automáticamente la red. Como se muestra en la figura, estos incluyen protocolos y tecnologías como REST, Ansible, Puppet, Chef, Python, JSON, XML y más.



Herramientas de configuración

Clave para autorización, si es necesario

Las herramientas de administración de configuración utilizan las solicitudes de API RESTful para automatizar tareas y pueden escalar en miles de dispositivos. Estas son algunas características de la red que los administradores se benefician de la automatización:

- Control de versión de software
- Atributos del dispositivo, como nombres, direccionamiento y seguridad
- Configuración de protocolos
- Configuraciones de ACL

Las herramientas de gestión de la configuración suelen incluir automatización y orquestación. La automatización realiza automáticamente una tarea en un sistema. La orquestación organiza un conjunto de tareas automatizadas que dan como resultado un proceso de coordenadas o un flujo de trabajo.

Herramientas de configuración

Herramientas de administración de configuración

Hay varias herramientas disponibles para facilitar la gestión de la configuración:

- Ansible
- Chef
- Puppet
- SaltStack

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.

Herramientas de configuración

Puppet, Chef, Ansible y SaltStack

Ansible, Chef, Puppet y SaltStack vienen con documentación de API para configurar solicitudes de API RESTful. Todos ellos admiten JSON y YAML, así como otros formatos de datos. En la tabla siguiente se muestra un resumen de una comparación de las principales características de las herramientas de administración de configuración de Ansible, Puppet, Chef y SaltStack.

Característica	Ansible	Chef	Puppet	SaltStack
Lenguaje de programación	Python + YAML	Ruby	Ruby	Python
¿Basado en agentes o sin agente?	Sin agente	Basado en agentes	Soporta ambos	Soporta ambos
¿Cómo se administran los dispositivos?	Cualquier dispositivo puede ser "controlador"	Chef Master	Puppet Master	Salt Master
¿Qué crea la herramienta?	Cuaderno de estrategias	Cookbook	Manifesto	Pilar

IBN y Cisco DNA Center

Descripción general de redes basadas en intención

- IBN es el modelo de industria emergente para la próxima generación de redes. IBN se basa en las redes definidas por software (SDN), transformando un enfoque manual y centrado en el hardware para diseñar y operar redes en uno que esté centrado en el software y totalmente automatizado.
- Los objetivos comerciales de la red se expresan como intenciones. IBN captura la intención comercial y utiliza análisis, aprendizaje automático y automatización para alinear la red de forma continua y dinámica a medida que cambian las necesidades comerciales.
- IBN captura y traduce la intención empresarial en políticas de red que se pueden automatizar y aplicar de forma coherente en toda la red.

IBN y Cisco DNA Center

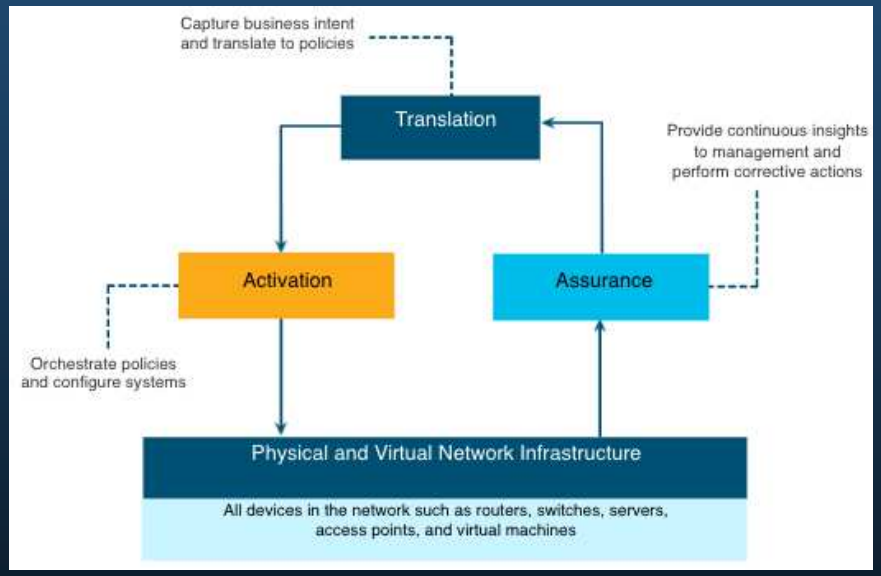
Descripción general de redes basadas en intención

Cisco considera que IBN tiene tres funciones esenciales: traducción, activación y seguridad. Estas funciones interactúan con la infraestructura física y virtual subyacente, como se muestra en la figura.

Traducción:-La función de traducción permite al administrador de la red expresar el comportamiento de red esperado que mejor respaldará la intención comercial.

Activación- La intención capturada debe interpretarse en políticas que se pueden aplicar a través de la red. La función de activación instala estas directivas en la infraestructura de red física y virtual mediante la automatización en toda la red.

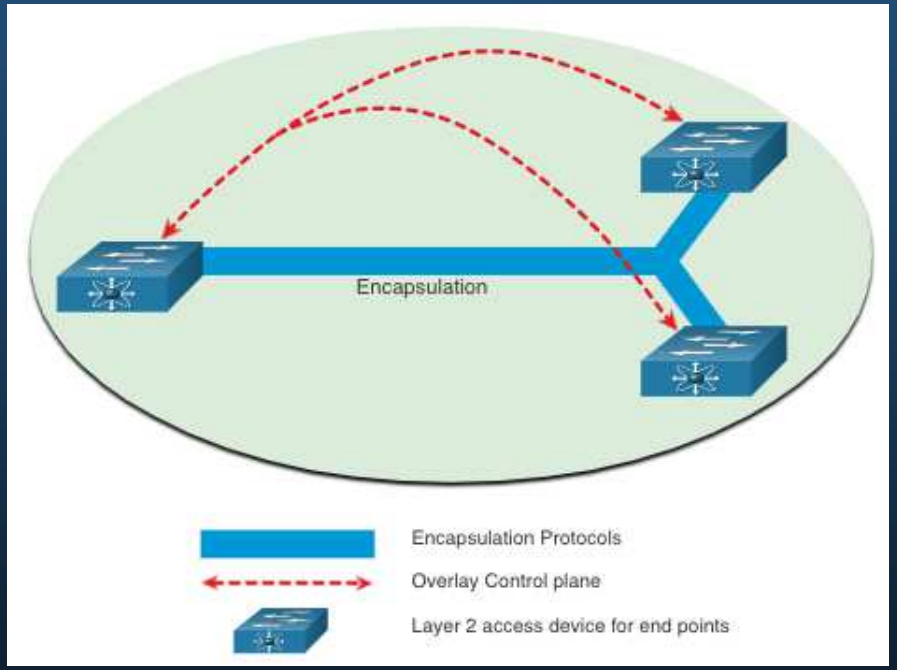
Aseguramiento-Para comprobar continuamente que la red respeta la intención expresada en cualquier momento, la función de aseguramiento mantiene un bucle continuo de validación y verificación.



IBN y Cisco DNA Center

Infraestructura de red como tejido

- Desde la perspectiva de IBN, la infraestructura de red física y virtual es un tejido; una superposición que representa la topología lógica utilizada para conectarse virtualmente a los dispositivos. La superposición limita la cantidad de dispositivos que el administrador de red debe programar y proporciona servicios y métodos de reenvío alternativos que no controlan los dispositivos físicos subyacentes.
- La superposición es donde se producen los protocolos de encapsulación como IPsec y CAPWAP. Mediante una solución IBN, el administrador de red puede especificar a través de directivas exactamente lo que sucede en el plano de control de superposición. Observe que cómo los switches están conectados físicamente no es una preocupación de la superposición.



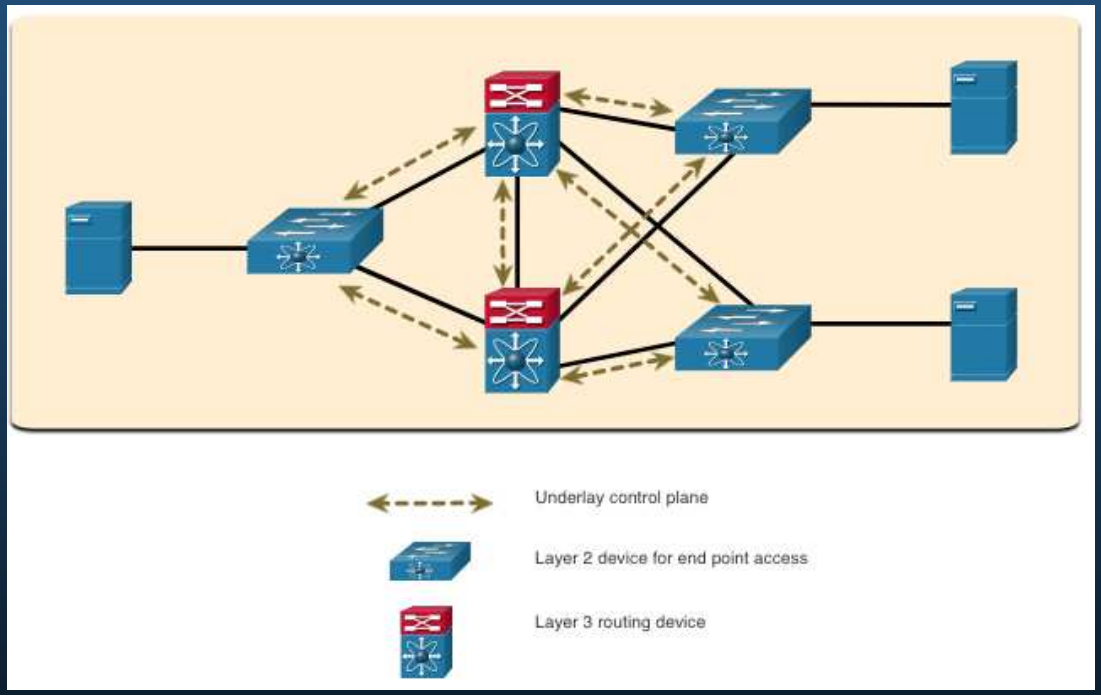
IBN y Cisco DNA Center

Infraestructura de red como tejido

La red subyacente es la topología física que incluye todo el hardware requerido para cumplir con los objetivos comerciales. La capa subyacente revela dispositivos adicionales y especifica cómo están conectados estos dispositivos, como se muestra en la figura.

Los puntos finales, como los servidores de la figura, acceden a la red a través de los dispositivos de Capa 2.

El plano de control subyacente es responsable de las tareas de reenvío simple.



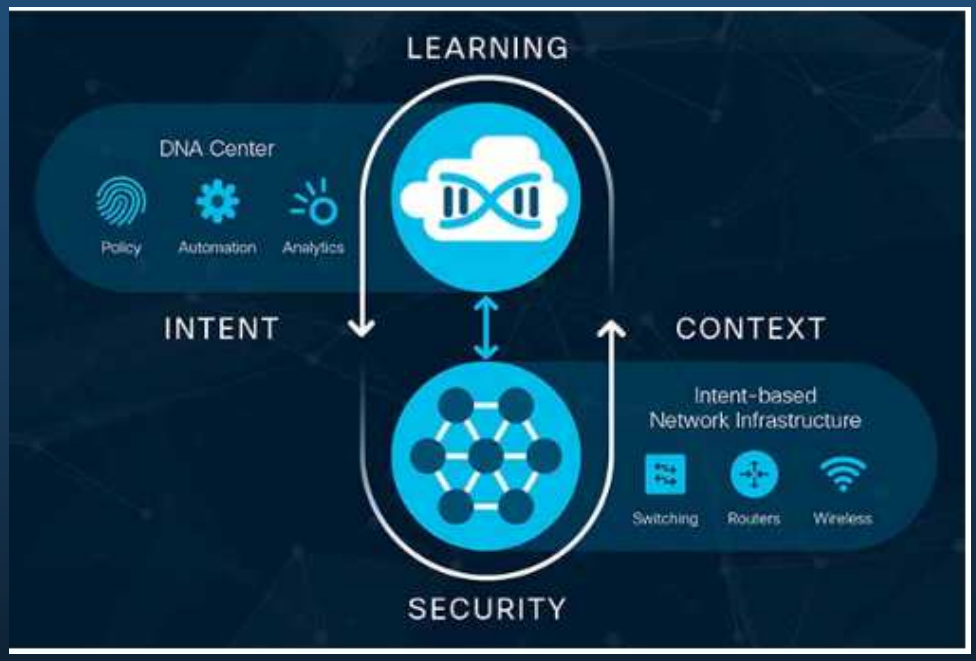
IBN y Cisco DNA Center

Arquitectura de red digital de Cisco (DNA)

Cisco implementa el tejido IBN utilizando Cisco DNA. Como se muestra en la figura, la intención comercial se implementa de forma segura en la infraestructura de red (la estructura).

Cisco DNA entonces recopila continuamente los datos de una multitud de fuentes (dispositivos y aplicaciones) para proporcionar un contexto rico de información.

Esta información puede analizarse para asegurarse de que la red se desempeña de manera segura en su nivel óptimo y de acuerdo con la intención comercial y las políticas de red.



IBN y Cisco DNA Center

Arquitectura de red digital de Cisco (DNA)

Soluciones Cisco DNA	Descripción	Beneficios
Acceso definido por software	•Primera solución de red empresarial basada en la intención construida con Cisco DNA. •Utiliza una estructura de red única a través de LAN y WLAN para crear una experiencia de usuario consistente y altamente segura. •Segmenta el tráfico de usuarios, dispositivos y aplicaciones y automatiza las políticas de acceso de usuarios para establecer la política correcta para cualquier usuario o dispositivo, con cualquier aplicación, a través de una red.	Habilite el acceso de cualquier usuario o dispositivo a cualquier aplicación en minutos sin poner en riesgo la seguridad.
SD-WAN	•Utiliza una arquitectura segura entregada en la nube para administrar centralmente las conexiones WAN. •Simplifica y acelera la entrega de servicios WAN seguros, flexibles y ricos para conectar centros de datos, sucursales, campus e instalaciones de colocación.	•Ofrece mejores experiencias de usuario para aplicaciones que residen en las instalaciones o en la nube. •Logre una mayor agilidad y ahorro de costos a través de implementaciones más fáciles e independencia de transporte.

IBN y Cisco DNA Center

Arquitectura de red digital de Cisco (DNA)

Soluciones Cisco DNA	Descripción	Beneficios
Cisco DNA Assurance	•Se utiliza para solucionar problemas y aumentar la productividad de TI. •Aplica análisis avanzados y aprendizaje automático para mejorar el rendimiento y la resolución de problemas, y predecir para asegurar el rendimiento de la red. •Proporciona notificaciones en tiempo real para condiciones de red que requieren atención.	•Le permite identificar las causas raíz y proporciona soluciones recomendadas para una resolución de problemas más rápida. •Cisco DNA Center proporciona un panel único y fácil de usar con información y capacidades de desglose. •El aprendizaje automático mejora continuamente la inteligencia de la red para predecir problemas antes de que ocurran.
Cisco DNA Center Security	•Se utiliza para proporcionar visibilidad mediante el uso de la red como sensor para análisis e inteligencia en tiempo real. •Proporciona un mayor control granular para aplicar políticas y contener amenazas en toda la red.	•Reduzca el riesgo y proteja a su organización contra amenazas, incluso en tráfico encriptado. •Obtenga visibilidad de 360 grados a través de análisis en tiempo real para una inteligencia profunda en toda la red. •Menor complejidad con seguridad de extremo a extremo.

IBN y Cisco DNA Center

Cisco DNA Center

- Cisco DNA Center es el controlador básico y la plataforma de análisis es la clave de Cisco DNA. Admite la expresión de intenciones para múltiples casos de uso, incluidas las capacidades básicas de automatización, el aprovisionamiento de estructuras y la segmentación basada en políticas en la red empresarial. Cisco DNA Center es un centro de comando y administración de red para el aprovisionamiento y la configuración de dispositivos de red. Es una plataforma de hardware y software que proporciona un "panel de vidrio único" (interfaz única) que se centra en la garantía, el análisis y la automatización.

- La página de inicio de la interfaz de DNA Center le ofrece un resumen general del estado y una captura instantánea de red. Desde aquí, el administrador de la red puede profundizar rápidamente en áreas de interés.

IBN y Cisco DNA Center

Cisco DNA Center

En la parte superior, los menús le brindan acceso a las cinco áreas principales de DNA Center. Como se muestra en la figura, los pasos son:

- **Diseño:**- Modele toda la red, desde sitios y edificios hasta dispositivos y enlaces, tanto físicos como virtuales, en todo el campus, la sucursal, la WAN y la nube.
- **Política:**- Utilice políticas para automatizar y simplificar la administración de la red, lo que reduce el costo y el riesgo al tiempo que acelera la implementación de servicios nuevos y mejorados.
- **Aprovisionamiento:**- Proporcione nuevos servicios a los usuarios con facilidad, velocidad y seguridad en toda la red empresarial, independientemente del tamaño y la complejidad de la red.
- **Aseguramiento:**- Utilice monitoreo y perspectivas proactivas de la red, los dispositivos y las aplicaciones para predecir los problemas con mayor rapidez y asegurarse de que los cambios en la configuración y la política logren la intención comercial y la experiencia del usuario que usted desea brindar.
- **Plataforma**- Utilice las API para integrarse con sus sistemas de TI preferidos para crear soluciones de extremo a extremo y agregar soporte para dispositivos de múltiples proveedores.