



Monitoreo y Supervisión

Troubleshooting

2021

Joaquín García
Álvaro Sánchez

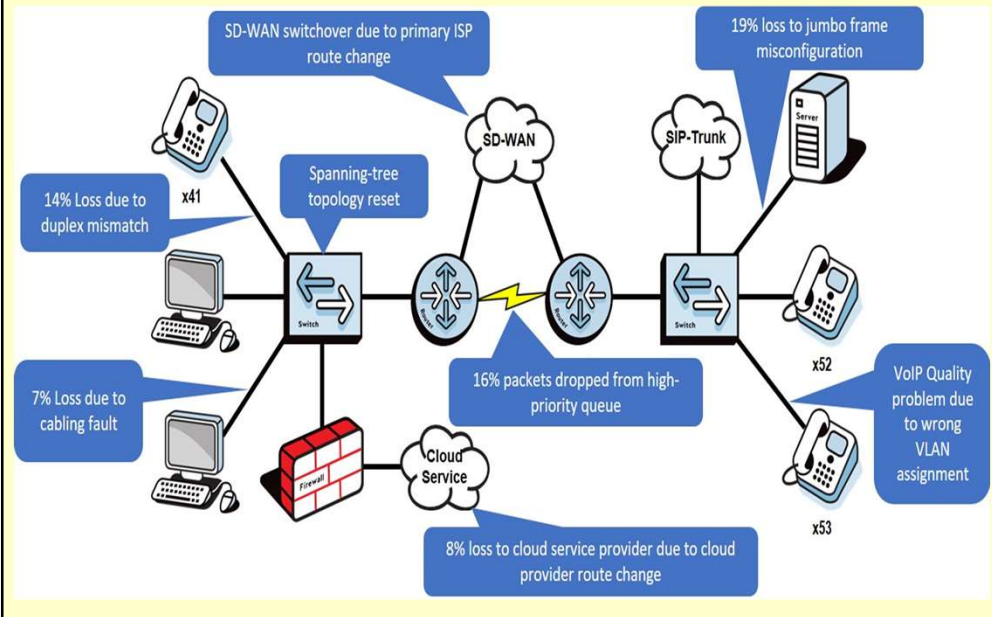
Herramientas de diagnóstico

Temas

- Diagnóstico de problemas (troubleshooting)
- Herramientas
 - Análisis de tráfico (NetFlow)
 - Registros de información (Syslog)
 - Sincronismo de red (NTP)

Diagnóstico de problemas

Diagnóstico (troubleshooting) de problemas



Diagnóstico de problemas

Pasos para diagnosticar un problema

1. Identificar el problema
2. Desarrollar una hipótesis
3. Verificar la hipótesis
4. Preparar un plan "A" de acción, y un plan "B" alternativo
5. Implementar la solución del plan "A"
6. Verificar los resultados y corregir si es necesario
7. Registrar lo sucedido

Diagnóstico de problemas

Problemas comunes

1.- Conflictos con direcciones IP

Los servicios DHCP en general, poseen sistemas que les ayuda a prevenir que asignen una IP repetida a un equipo en la red. Sin embargo ocasionalmente puede ocurrir que 2 equipos tengan la misma IP, ya que uno de ellos puede estar configurado estáticamente. Este hecho se conoce como IP Duplicada.

Lo primero es mantener nuestra red ordenada, eso nos evita problemas y nos ayuda a detectar la falla rápidamente si se presenta. Después podemos verificar que no tenemos 2 servidores DHCP funcionando, por ejemplo nuestro servidor de datos que actúa también como servidor DHCP y un router, que esté actuando como servidor DHCP.

Diagnóstico de problemas

Problemas comunes

2.- Fallas en switches o Routers

En algunos casos las fallas en la red no tienen una causa aparente. Por ejemplo, nuestra máquina puede enviar y recibir correos sin problemas pero no tiene acceso a Internet, o estamos tranquilamente navegando en la red cuando de un momento a otro se pierde el acceso, y pasados algunos minutos hay Internet de nuevo.

Cuando los problemas de conectividad son locales el problema puede solucionarse reiniciando el switch de acceso o router.

Si estos problemas se repiten demasiado frecuentemente, es necesario revisar la calidad de nuestra fuente de energía, cambios del suministro eléctrico puede provocar equipos apagados o incluso daños en nuestros routers o switches. Después de todas estas verificaciones sería bueno probar con otro switch.

Diagnóstico de problemas

Problemas comunes

3.- Conectar equipos desordenadamente

La necesidad de conectividad suele crecer demasiado rápido, y esto provoca que se terminen conectando equipos simplemente al “switch más cercano” o conectar un switch al “switch más cercano” y así sucesivamente.

Cuando esto ocurre los datos deben recorrer largas distancias antes de llegar a su destino, además de aumentar los lugares que podrían causar fallas.

Una buena práctica es anticiparse al crecimiento y evitar estos parches en nuestra red por nuevos usuarios, o reorganizar procurando consolidar lo disperso en un sistema potente y estable.

Diagnóstico de problemas

Problemas comunes

4.- Problemas con NetBIOS

NetBIOS es un protocolo de Windows que permite a las computadoras en una red “hablar”. Sin embargo frecuentemente no trabaja adecuadamente provocando lentitud en nuestra red o generando errores al acceder los archivos compartidos y a veces el corte del servicio.

Una opción es identificar los equipos con conflictos y renombrar uno de ellos. Para analizar los nombres de la red se puede utilizar una herramienta como AngryIpScanner.

Comportamientos extraños en los recursos de la red pueden ser causados cuando los hosts tienen el mismo nombre. Deshabilitar el servicio de resolución de nombres WINS/NetBT podría solucionar este problema.

Diagnóstico de problemas

Problemas comunes

5.- Tarjetas de red defectuosas

Un problema común es la presencia de este tipo de fallas. Cuando un equipo produce errores esporádicos o intermitentes, sobre todo cuando están relacionados con una estación de trabajo en particular. Una manera sencilla de verificar el funcionamiento de nuestra tarjeta es prestar atención al LED verde o blanco que viene en cada una de ellas, que debe parpadear o permanecer encendido, si no, se debe verificar que el cable está conectado correctamente y en buenas condiciones.

Diagnóstico de problemas

Problemas comunes

6.- Insuficiente Ancho de Banda

Puede ocurrir que simplemente el ancho de banda que tenemos no alcance para todas las exigencias de la red, puede ser de manera local como de Internet. Un cable Cat5E puede ser insuficiente si las exigencias son muy altas, tenemos cables Cat6 o incluso Cat7 que se pueden utilizar en la red. También nuestro ancho de banda en la red local puede ser afectada por la calidad de nuestros switches o routers: 1 solo switch 10/100 puede hacer lenta una red de 10/100/1000.

Diagnóstico de problemas

Problemas comunes

7.- Errores DNS

Puede darse el caso en que Windows informe que tenemos acceso a internet, pero al intentar acceder a alguna Web nos dé error NAME NOT RESOLVED.

El comando “nslookup” es una herramienta útil en estos casos.

Diagnóstico de problemas

Problemas comunes

8.- Infecciones SpyWare

En esencia un virus de este tipo transmite información de un host a una entidad externa, obviamente sin permiso del usuario.

Esto podría saturar la red compartiendo datos sin que el usuario lo perciba, por lo que es necesario mantener el antivirus activo y actualizado.

Diagnóstico de problemas

Problemas comunes

9.- Infecciones de Virus

En este punto son clave las normas o políticas de la empresa en cuanto al uso de Internet, la disciplina puede ahorrarnos muchísimos problemas.

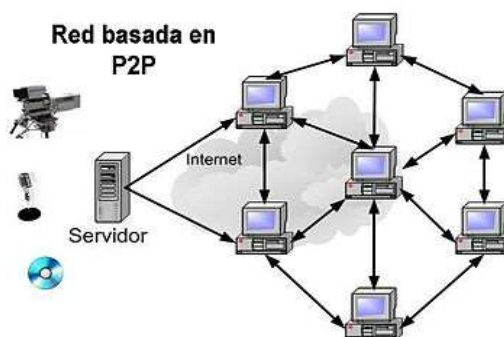
Ante una falla repentina, nunca está de más un escaneo de virus en cada terminal de la red. Una sola terminal infectada puede estar generando miles de correos SPAM que congestionan nuestra red.

Diagnóstico de problemas

Problemas comunes

10.- Demasiadas aplicaciones que operan sobre la red.

En muchos casos desde internet se instalan programas que se conectan a internet, software P2P (peer to peer), etc., que sobrecargan inútilmente la red. Identificarlos y desactivar los que no son esenciales es crítico.

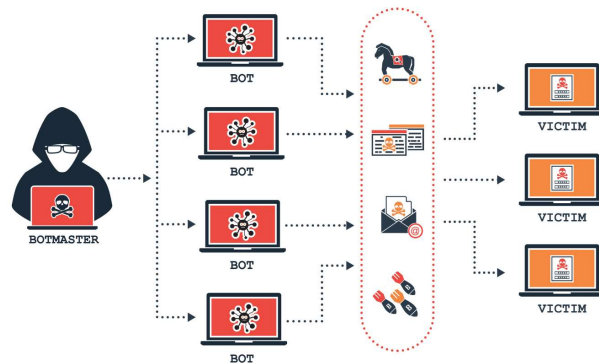


Diagnóstico de problemas

Problemas comunes

11.- Ataques de denegación de servicio (DOS y DDOS).

Envío de tráfico a efectos de consumir recursos.



Diagnóstico de problemas

Herramientas

A efectos de diagnosticar y encaminar la solución adecuada, a continuación vamos a revisar algunas herramientas utilizadas frecuentemente en redes.

Herramientas

Herramientas

1. NetFlow
2. Syslog
3. NTP

NetFlow

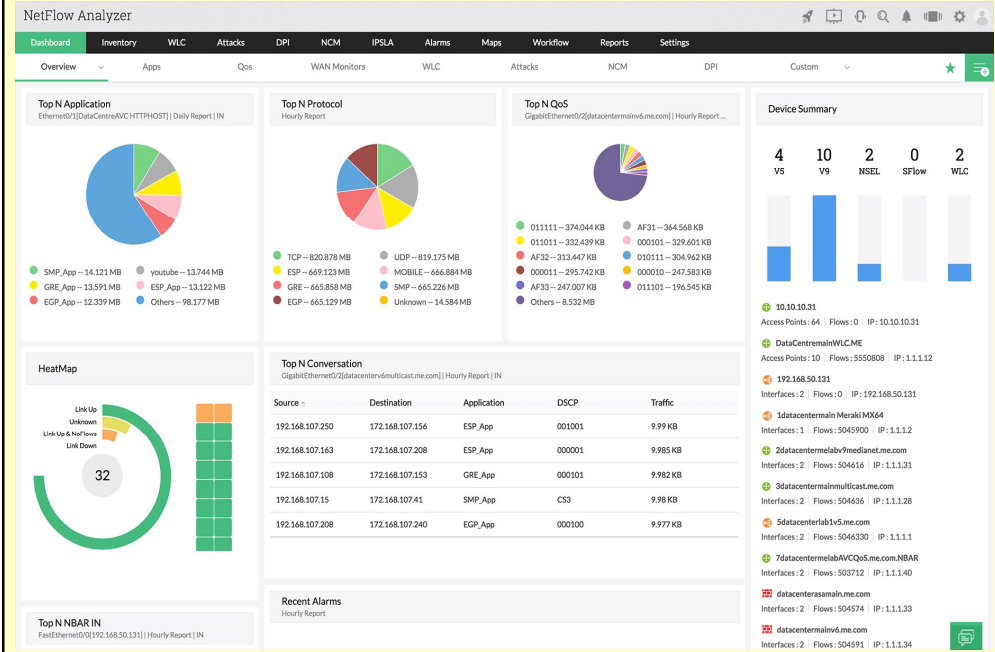
NetFlow

NetFlow es una aplicación que permite caracterizar el funcionamiento de la red. En respuesta a los nuevos requisitos y presiones, a los operadores de red les resulta fundamental comprender cómo se comporta la red, lo que incluye:

- Uso de aplicaciones y redes
- Productividad de la red y utilización de los recursos de la red
- El impacto de los cambios en la red
- Anomalías de la red y vulnerabilidades de seguridad
- Problemas de cumplimiento a largo plazo

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow



NetFlow

NetFlow crea un entorno donde los administradores tienen las herramientas para comprender quién, qué, cuándo, dónde y cómo fluye el tráfico de la red. Cuando se comprende el comportamiento de la red, el proceso comercial mejora y quedan disponibles registros de auditoría de cómo se utiliza la red.

Esta mayor comprensión reduce la vulnerabilidad de la red en relación con la interrupción y permite un funcionamiento más eficiente. Las mejoras en la operación de la red reducen los costos y generan mayores ingresos comerciales mediante una mejor utilización de la infraestructura de la red.

Las empresas dependen en gran medida de NetFlow para cumplir con sus objetivos comerciales.

Es importante destacar que NetFlow no toma información de los datos contenidos en el “payload” de los paquetes, por lo que no vulnera la privacidad de las comunicaciones.

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Versiones

NetFlow Version	Comments
1	Original
5	Estándar y el más utilizado
7	Específico de los conmutadores Cisco Catalyst 6500 y 7600 Similar a versión 5 pero no incluye información AS, interfaz, TCP Flag & TOS
8	Hasta 11 esquemas de agregación Reduce los recursos requeridos al sistema
9	Formato de trama flexible y extensible que facilita el soporte de campos de información adicionales (por ejemplo BGP next Hop y MPLS "aware")

NetFlow

Versión 5

Ofrece los siguiente campos de información de los flujos de tráfico en la red:

Dirección IP origen

Dirección IP destino

Puerto UDP/TCP origen

Puerto UDP/TCP destino

Tipo de protocolo de nivel 3

TOS byte (Type of Service)

Interfaces lógicas de entrada
y de salida (ifIndex)

Flags TCP

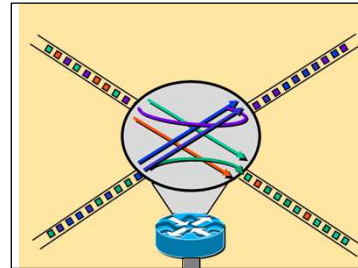
¿Quién habla
con quién?

¿Qué protocolos
y aplicaciones?

Tráfico según su
tipo de priorización

¿Dónde?

¿Ataques DoS?



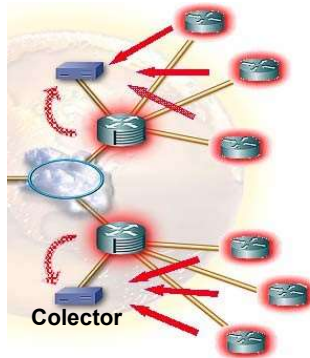
Datos exportados
via paquetes UDP

NetFlow

Versión 5

- Los routers exportan la información de los flujos mediante Netflow a un sistema de colectores.
- Las tramas se exportan vía UDP. Las tramas son típicamente de 1500 bytes y cada una contiene información de entre 20 y 50 flujos

Colector



NetFlow

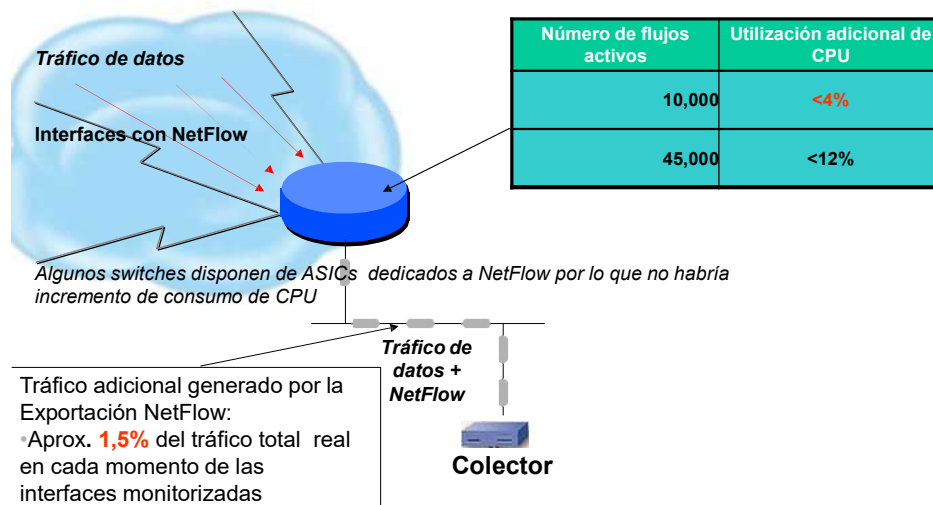
Versión 5

Configurar NetFlow en router Cisco:

- En la configuración global
 - ip flow-export source loopback
 - ip flow-export version 5
 - ip flow-cache timeout active 1
 - ip flow-export destination [*harvesterIP*] 9995
- Para cada interfaz a monitorizar
 - ip route-cache flow

NetFlow

Impacto de habilitar NetFlow



NetFlow

Uso de SNMP

- Los operadores y administradores de red utilizan herramientas que se basan en el protocolo SNMP para obtener información de las interfaces de un dispositivo
- Estos datos son visibles mediante gráficos disponibles en páginas web
- Representan el ancho de banda que atraviesa dicha interfaz en ambos sentidos (in/out)
- Esta información es muy útil para la toma de decisiones que hacen al funcionamiento y la planificación para el futuro, al observar por ejemplo la saturación de la capacidad de un enlace en diferentes momentos del día

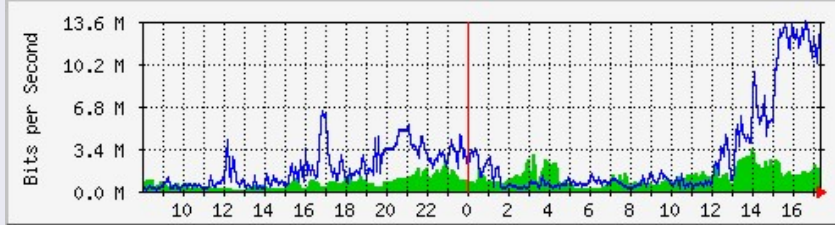
NetFlow

Uso de SNMP

Herramientas basadas en consultas SNMP

- MRTG
- Cacti
- Zabbix
- Cricket
- Pandora

Imagen generada



NetFlow

Uso de SNMP

- SNMP es la forma tradicional de monitorear el ancho de banda
- Un conocimiento más detallado de cómo se está utilizando el ancho de banda es muy importante hoy en las redes IP
- Contadores de paquetes y bytes de interfaz son útiles
- Pero SNMP no permite conocer qué direcciones IP son el origen y destino del tráfico, qué protocolos atraviesan los enlaces y qué aplicaciones están generando el tráfico

NetFlow

Monitoreo de desempeño SNMP tradicional

Tradicionalmente, los clientes confiaban casi exclusivamente en SNMP para monitorear el ancho de banda. Aunque SNMP facilita la planificación de la capacidad, hace poco para caracterizar las aplicaciones y los patrones de tráfico, lo que es esencial para comprender qué tan bien la red respalda el negocio. Una comprensión más detallada de cómo se usa el ancho de banda es extremadamente importante en las redes IP de hoy. Los contadores de interfaz de paquetes y bytes son útiles, pero comprender qué direcciones IP son el origen y el destino del tráfico y qué aplicaciones generan el tráfico es invaluable.

Comprensión de red basada en NetFlow

La capacidad de caracterizar el tráfico IP y comprender cómo y dónde fluye es fundamental para la disponibilidad, el rendimiento y la resolución de problemas de la red. La supervisión de los flujos de tráfico IP facilita una planificación de la capacidad más precisa y garantiza que los recursos se utilicen de forma adecuada en apoyo de los objetivos de la organización. Ayuda a TI a determinar dónde aplicar la calidad de servicio (QoS), optimizar el uso de recursos y desempeña un papel vital en la seguridad de la red para detectar ataques de denegación de servicio (DoS), gusanos propagados por la red y otros eventos de red no deseados.

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

NetFlow facilita soluciones a muchos problemas comunes

- Analizar nuevas aplicaciones y su impacto en la red.
Identificar nuevas cargas de red de aplicaciones, como VoIP o adiciones a sitios remotos.
- Reducción del tráfico máximo de WAN
Utilizar las estadísticas de NetFlow para medir la mejora del tráfico WAN a partir de cambios en la política de aplicaciones; comprender quién está utilizando la red y los principales interlocutores de la red.
- Solución de problemas y comprensión de los puntos débiles de la red
Diagnosticar el rendimiento lento de la red, los acaparadores del ancho de banda y la utilización del ancho de banda, rápidamente con la interfaz de línea de comandos o las herramientas de informes.
- Detección de tráfico WAN no autorizado
Evitar costosas actualizaciones identificando las aplicaciones que causan congestión.
- Seguridad y detección de anomalías
NetFlow se puede utilizar para la detección de anomalías y el diagnóstico de gusanos junto con aplicaciones como CiscoCS-Mars.
- Validación de parámetros de QoS
Confirmar que se haya asignado el ancho de banda apropiado a cada clase de servicio (CoS) y que ninguna CoS tenga una suscripción excesiva o insuficiente.

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

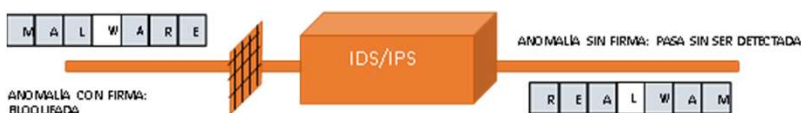
NetFlow

Detección de anomalías de red

Una de las mayores amenazas para las organizaciones de hoy en día está relacionada con la seguridad de la red. Muchos problemas de seguridad de la red están causados por malware, ataques distribuidos de denegación de servicio (DDoS) y aplicaciones desconocidas que se ejecutan en puertos conocidos; todo esto puede ser difícil de detectar. Para combatir estas amenazas contra la seguridad, los administradores de red pueden usar NetFlow y otras tecnologías de flujo a fin de monitorear y detectar patrones de tráfico de red anormales que puedan afectar el desempeño de la red.

¿Qué puede provocar anomalías en la red?

Comúnmente, pueden introducirse anomalías en la red a través del teletrabajo y los usuarios que llevan sus propios dispositivos (Bring Your Own Device, BYOD). Ambos aumentan el riesgo de que se introduzca malware directamente en la red después de haberse infectado a través de una fuente externa. Además, la red puede estar alojando un bot que se introdujo a través de una de dichas fuentes.



https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Detección de anomalías

En una empresa, los administradores intentan asegurar la red mediante un sistema de detección y prevención de intrusiones (IDS/IPS), que recopila datos y funciona con firmas para identificar amenazas, mientras que los routers y firewalls funcionan según reglas de control de acceso definidas por usuarios. Si un malware de día cero se introduce en la red, puede ser muy difícil que lo detecten los routers, los firewalls o, incluso, los sistemas IDP/IPS. Un bot alojado en una red no puede ser detectado por los firewalls ni los IDS/IPS porque rastrean solo el tráfico de entrada, mientras que los bots contribuyen más al tráfico de salida. Un sistema IDS/IPS sin firma es una alternativa costosa.

Puede resultar difícil encontrar una anomalía en la red, pero existen indicios que se pueden identificar, como un aumento abrupto del tráfico de red, un comportamiento del tráfico de red fuera de la línea de base, picos inusuales y tráfico enfocado de manera anormal en ciertas partes de la red, los puertos o las direcciones IP, y aplicaciones nuevas que acaparan casi todo el ancho de banda o generan patrones de tráfico anormales.

NetFlow

Detección de anomalías

Algunos casos específicos que se deben vigilar son un volumen elevado de tráfico SMTP de salida, oleadas breves e intermitentes de paquetes UDP, conversaciones de un host a muchos en el mismo puerto, tráfico en puertos desconocidos, demasiados marcadores TCP SYN, tráfico entre direcciones IP reservadas por IANA, etc.

Al recopilar datos de flujo de todos los dispositivos en un punto único, analizar los patrones de tráfico y buscar comportamientos de tráfico inesperados, los administradores de red pueden detectar un comportamiento de tráfico de red anómalo. Se pueden diagnosticar períodos específicos en los registros de NetFlow para encontrar la causa de una interrupción que ocurrió, por ejemplo, durante el fin de semana o cuando no había nadie en la oficina.

NetFlow

Rastreo del rendimiento de la nube

La demanda creciente de aplicaciones basadas en la nube y la velocidad incrementada de adopción tienen como resultado una presión inmensa sobre los administradores de red. Al implementar servicios en la nube, resulta imprescindible que las empresas tengan un tiempo de actividad de red continuo para los procesos operativos necesarios. Cualquier problema con la red o la velocidad del servicio puede tener un efecto adverso en los negocios. Uno de los elementos que se ve más afectado por las aplicaciones y servicios en la nube es el ancho de banda de una red. Los enfoques basados en la nube y en software como servicio (SaaS) implican que tiene que garantizar que haya un ancho de banda suficiente disponible para que las aplicaciones críticas para los negocios puedan ejecutar procesos ininterrumpidos 24x7. Cualquier tiempo de inactividad de la red puede ocasionar una enorme pérdida operativa en toda la empresa y potencialmente afectar a los resultados de la organización. Algunos de los problemas a los que se enfrentan los administradores de red al usar aplicaciones en la nube incluyen los siguientes:

- Impacto en el ancho de banda por parte de aplicaciones en la nube
- Pérdida operativa si una aplicación de misión crítica en la nube deja de funcionar
- Cuellos de botella en la red empresarial
- Acaparamientos de ancho de banda por parte de otras aplicaciones
- Usos no autorizados de protocolos y aplicaciones

NetFlow

Cómo asegurar un uso continuo de las aplicaciones en la nube



Analizar los datos de NetFlow ayuda a monitorear el desempeño de la red dado que el tiempo de actividad continuo es una necesidad absoluta para las empresas que usan o alojan aplicaciones en la nube. Resulta imprescindible que los administradores de red encuentren los cuellos de botella, los acaparamientos del ancho de banda y la prioridad no autorizada de protocolos y aplicaciones. Los datos de NetFlow contienen información acerca de lo siguiente:

- Causa de los cuellos de botella de tráfico
- Diferentes puntos finales que usan ancho de banda empresarial
- Aplicaciones que se usan en la red
- Prioridad de conversaciones dentro de la red

NetFlow

Cómo asegurar un uso continuo de las aplicaciones en la nube

NetFlow ofrece una perspectiva a los administradores de red y les ayuda a establecer prioridades para aplicaciones alojadas y a implementar políticas de calidad de servicio (QoS).

Proporciona los medios para rastrear el uso acumulativo de una aplicación determinada de manera conjunta, hasta regiones específicas, si es necesario.

Como resultado, la información de NetFlow se puede usar para comprobar si el comportamiento de uso en la nube coincide con el acuerdo de nivel de servicio, asignando la actividad real entre la nube y la red. Medir la latencia es un desafío mientras se opera en la nube, pero al usar exportadores de flujo como nProbe™, se pueden identificar cuellos de botella al analizar los datos a través de los recopiladores de NetFlow y se puede exigir que los proveedores de nube entreguen el servicio prometido.

NetFlow

Validación de QoS y ToS

Las aplicaciones no autorizadas pueden saturar el ancho de banda de la red, lo cual a su vez puede producir una interrupción de las aplicaciones empresariales importantes. Por este motivo, es importante definir la calidad de servicio (QoS) y establecer prioridades para las distintas aplicaciones. Establecer prioridades para el ancho de banda según las necesidades es una estrategia crucial para los administradores de red. Por ejemplo, el 50 % de su ancho de banda puede fijarse para aplicaciones de VoIP que sean sensibles para el negocio, mientras que a otras aplicaciones no críticas se les asigna un ancho de banda menor. Así, definiendo las clases de QoS y asignando políticas, los administradores de red pueden establecer acciones predefinidas que se desencadenan en casos específicos.



Como se explica en la imagen anterior, las aplicaciones compiten entre sí cuando atraviesan la WAN y, dado que el ancho de banda no es infinito ni gratuito, es perfectamente entendible que quiera ver cómo se usa. Dado que los datos de NetFlow informan acerca del tipo de servicio (ToS) y los campos DSCP de conversaciones de tráfico, se puede monitorear el uso del ancho de banda por aplicación y medir la efectividad de las políticas de QoS.

NetFlow

Planificación de capacidad

NetFlow ayuda a los administradores a planificar la capacidad de la red con mayor precisión a medida que las organizaciones crecen, mediante la implementación de un ancho de banda mayor para los servicios de red avanzados. Con NetFlow, se puede comprobar fácilmente si el crecimiento del ancho de banda está alineado con los recursos utilizados en el entorno actual y prepararse para el futuro. Esto permite a los administradores de red monitorear con mayor facilidad el ancho de banda que consumen las aplicaciones.

La planificación de capacidad mediante el uso de NetFlow también puede ayudar a los administradores de red a implementar políticas de QoS y establecer prioridades para aplicaciones de misión crítica al categorizar el tráfico. Al distinguir diferentes tipos de tráfico de red como voz, correo electrónico y otras aplicaciones, los administradores pueden analizar y comprender las políticas de QoS que implementaron. Las aplicaciones y conversaciones principales según datos de NetFlow se pueden almacenar para su referencia, a diferencia de PCAP, que requiere almacenamiento extensivo.

La planificación de capacidad ayuda a las empresas a recopilar más datos históricos de NetFlow y comparar las tendencias con la red de la organización. Esto ayuda a calcular suficiente ancho de banda para las aplicaciones críticas y evitar que cualquier anomalía se introduzca en la red. Contar con NetFlow para la planificación de capacidad también ayuda en la ampliación de la red según las necesidades y utiliza el ancho de banda disponible de una mejor forma, lo cual asegura una buena alineación de recursos y una buena planificación de capacidad.

NetFlow

¿Cómo proporciona NetFlow la información de la red?

¿Qué es un IP Flow?

Cada paquete que se reenvía dentro de un router o switch se examina en busca de un conjunto de atributos de paquete IP. Estos atributos son la identidad del paquete IP o la huella digital del paquete y determinan si el paquete es único o similar a otros paquetes.

Tradicionalmente, un flujo de IP se basa en un conjunto de 5 y hasta 7 atributos de paquetes IP.

Atributos de paquetes IP utilizados por NetFlow:

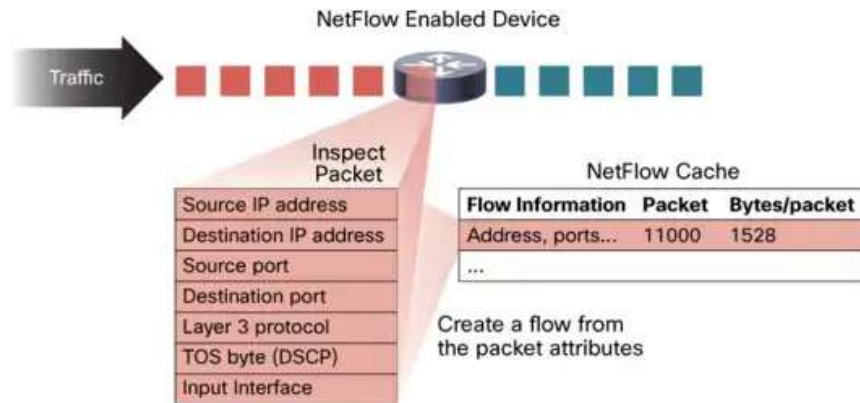
- Dirección de origen IP
- Dirección IP de destino
- Puerto de origen
- Puerto de destino
- Tipo de protocolo de capa 3
- Clase de servicio
- Interfaz de router o switch

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

¿Qué es un IP Flow?

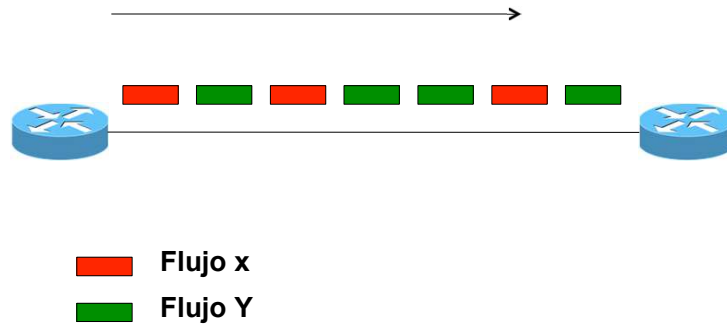
Todos los paquetes con la misma dirección IP de origen / destino, puertos de origen / destino, interfaz de protocolo y clase de servicio se agrupan en un flujo y luego se cuentan los paquetes y bytes. Esta metodología de toma de huellas digitales o determinación de un flujo es escalable porque una gran cantidad de información de red se condensa en una base de datos de información de NetFlow llamada caché de NetFlow.



https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Flujos simples



https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

¿Cuáles de estos paquetes son del mismo flujo?

	<i>Src IP</i>	<i>Dst IP</i>	<i>Protocol</i>	<i>Src Port</i>	<i>Dst Port</i>
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	6 (TCP)	22	4001
C	1.2.3.4	5.6.7.8	6 (TCP)	4002	80
D	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
E	1.2.3.4	8.8.8.8	17 (UDP)	65432	53
F	8.8.8.8	1.2.3.4	17 (UDP)	53	65432

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

¿Cuáles de estos paquetes son del mismo flujo?

	Src IP	Dst IP	Protocol	Src Port	Dst Port
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	6 (TCP)	22	4001
C	1.2.3.4	5.6.7.8	6 (TCP)	4002	80
D	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
E	1.2.3.4	8.8.8.8	17 (UDP)	65432	53
F	8.8.8.8	1.2.3.4	17 (UDP)	53	65432

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Todos los paquetes con la misma dirección IP de origen / destino, puertos de origen / destino, interfaz de protocolo y clase de servicio se agrupan en un flujo y luego se cuentan los paquetes y bytes. Esta metodología de toma de huellas digitales o determinación de un flujo es escalable porque una gran cantidad de información de red se condensa en una base de datos de información de NetFlow llamada caché de NetFlow.

Esta información de flujo es extremadamente útil para comprender el comportamiento de la red.

- La dirección de origen permite comprender quién origina el tráfico.
- La dirección de destino indica quién recibe el tráfico.
- Los puertos caracterizan la aplicación que utiliza el tráfico.
- La clase de servicio examina la prioridad del tráfico.
- La interfaz del dispositivo indica cómo el dispositivo de red utiliza el tráfico
- Los paquetes y bytes contabilizados muestran la cantidad de tráfico

La información adicional agregada a un flujo incluye

- Marcas de tiempo de flujo para comprender la vida de un flujo; las marcas de tiempo son útiles para calcular paquetes y bytes por segundo
- Direcciones IP de siguiente salto que incluyen sistemas autónomos (AS) de enrutamiento BGP
- Máscara de subred para las direcciones de origen y destino para calcular prefijos
- Indicadores de TCP para examinar los apretones de manos de TCP

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

¿Cómo acceder a los datos producidos por NetFlow?

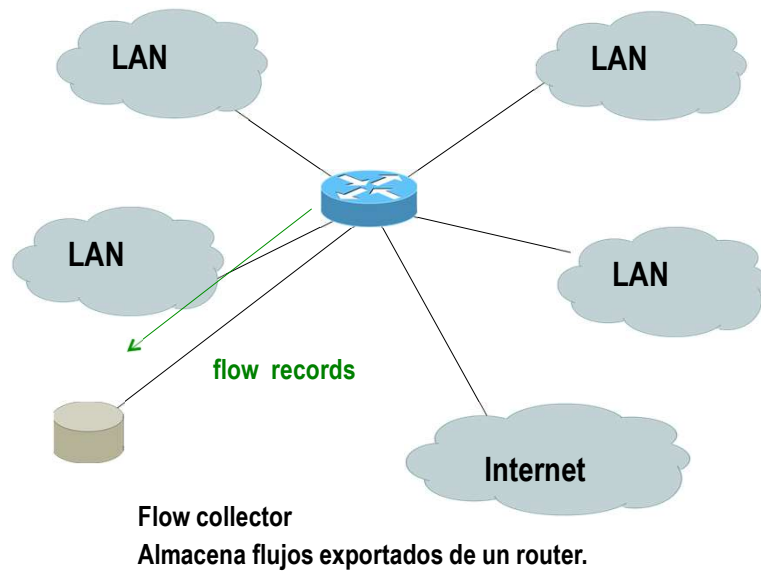
Hay dos métodos principales para acceder a los datos de NetFlow: la interfaz de línea de comandos (CLI) con comandos show o utilizando una herramienta de informes de aplicaciones. Si se está interesado en una vista inmediata de lo que está sucediendo en su red, se puede utilizar la CLI. NetFlow CLI es muy útil para solucionar problemas.

La otra opción es exportar NetFlow a un servidor de informes o lo que se denomina "recopilador de NetFlow". El recopilador de NetFlow tiene la función de ensamblar y comprender los flujos exportados y combinarlos o agregarlos para producir los valiosos informes utilizados para el análisis de tráfico y seguridad. La exportación de NetFlow, a diferencia del sondeo SNMP, envía información periódicamente al recopilador de informes de NetFlow. En general, la caché de NetFlow se llena constantemente de flujos y el software del router o switch busca en la caché los flujos que han terminado o expirado y estos flujos se exportan al servidor recolector de NetFlow. Los flujos finalizan cuando termina la comunicación de red (es decir, un paquete contiene el indicador TCP FIN).

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Recolección de flujos



NetFlow

Informes de NetFlow

Los siguientes pasos se utilizan para implementar los informes de datos de NetFlow:

- NetFlow está configurado para capturar flujos en caché de NetFlow
- La exportación de NetFlow permite enviar flujos al colector.
- Se busca en el caché de NetFlow los flujos que han terminado y estos se exportan al servidor de recopilación de NetFlow.
- Aproximadamente de 30 a 50 flujos se agrupan y normalmente se transportan en formato UDP al servidor recolector de NetFlow
- El software de recopilación NetFlow crea informes históricos o en tiempo real a partir de los datos

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

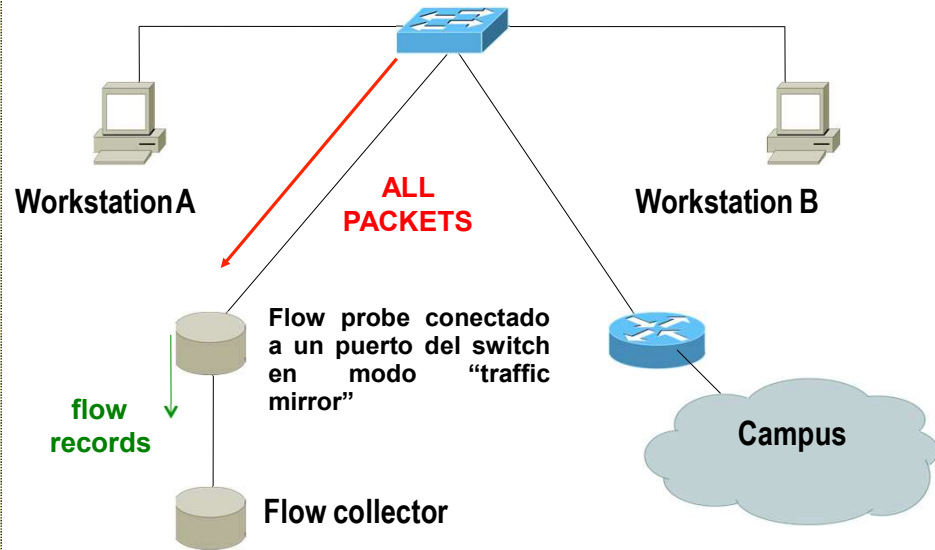
¿Cómo determina el router o el switch qué flujos exportar al servidor NetFlow Collector?

Un flujo está listo para exportarse cuando está inactivo durante un cierto tiempo (es decir, no se reciben nuevos paquetes para el flujo); o si el flujo es de larga duración (activo) y dura más que el temporizador activo (es decir, descarga FTP larga). Además, el flujo está listo para la exportación cuando un indicador TCP indica que el flujo ha terminado (es decir, indicador FIN, RST). Son temporizadores para determinar si un flujo está inactivo o si un flujo es de larga duración y el valor predeterminado para el temporizador de flujo inactivo es de 15 segundos y el temporizador de flujo activo es de 30 minutos. Todos los temporizadores para la exportación son configurables, pero los valores predeterminados se utilizan en la mayoría de los casos, excepto en la plataforma de conmutadores Cisco Catalyst 6500 Series. El recolector puede combinar flujos y tráfico agregado. Por ejemplo, una descarga FTP que dure más que el temporizador activo puede dividirse en varios flujos y el recopilador puede combinar estos flujos mostrando el tráfico ftp total a un servidor a una hora específica del día.

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Passive Monitor Collection



NetFlow

Passive Monitor Collection

- Ejemplos
 - softflowd (Linux/BSD)
 - pfflowd (BSD)
 - ng_netflow (BSD)
- El collector ve todo el tráfico de la red en el punto en el que está conectado y genera flujos. Le evita al router el procesamiento, crea flujos y los exporta.

NetFlow

¿Cuál es el formato de los datos de exportación?

Existen varios formatos para el paquete de exportación y estos se denominan comúnmente “versión de exportación”.

Las versiones de exportación son formatos bien documentados, incluidas las versiones 5, 7 y 9.

El formato más común utilizado es la versión 5 de exportación de NetFlow, pero la versión 9 es el formato más reciente y tiene algunas ventajas para tecnologías clave como seguridad, análisis de tráfico y multidifusión.

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

La Figura 2 a continuación es un ejemplo de los datos disponibles en una caché de NetFlow.

1. Flow cache—The first unique packet creates a flow

SrcIf	SrcPAddr	DstIf	DstPAddr	Protocol	TOS	Flags	Pkts	Src Port	Src Mask	Src AS	Dst Port	Dst Mask	Dst AS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Flow Aging Timers

- Inactive Flow (15 sec is default)
- Long Flow (30 min (1800 sec) is default)
- Flow ends by RST or FIN TCP Flag

SrcIf	SrcPAddr	DstIf	DstPAddr	Protocol	TOS	Flags	Pkts	Src Port	Src Mask	Src AS	Dst Port	Dst Mask	Dst AS	NextHop	Bytes/Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Flows packaged in export packet

Non-aggregated Flows—Export Version 5 or 9

4. Transport Flows to Reporting Server



https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Protocolos de exportación de flujos

- **Cisco Netflow**, diferentes versiones
 - v5: muy usado
 - v9: Más nuevo, incluye soporte de IPv6
- **IP Flow Information Export (IPFIX)**:
 - IETF standard, basado en Netflow v9
- **sFlow**: Usado en switches
- **jFlow**: Juniper

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Cisco Netflow

- Flujos unidireccionales
- IPv4 unicast y multicast
 - (IPv6 en Netflow v9)
- Flujos exportados via UDP
 - Choose a port. No particular standard, although 2055 and 9996 are commonly used
- En todas las variantes de IOS, en viejas versiones de ASA and CatOS

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Configuración de Cisco IOS

- Se configura en cada interfaz
 - Inbound y outbound
 - Versiones viejas de IOS sólo permiten inbound
- Se define la versión
- Se define la dirección IP y el puerto del colector (dónde enviar los flujos)
- Opcionalmente configurar timeout para flujos, y tamaño de tabla de flujos (v5)
- Opcionalmente configurar velocidad de muestreo

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

NetFlow

Configuración de Netflow: en viejas plataformas

- Habilitar CEF

```
ip cef ipv6  
cef
```

- Habilitar low en cada interfaz

```
ip route-cache flow
```

 (pre IOS 12.4)

O

```
ip flow ingress ipflow  
egress
```

 (IOS 12.4 en adelante)

- Exportar Flows a un colector

```
ip flow-export version [5|9] [origin-as|peer-as] ip flow-  
export destination <x.x.x.x> <udp-port>
```

NetFlow

Netflow "Top-talkers"

- Se pueden agregar flujos en el router
 - Configurar los top-talkers

```
ip flow-top-talkers top 50
sort-by bytes
match input-interface GigabitEthernet0/0
```

- Mostrará a los 50 mayores generadores de flujos en la interfaz GigabitEthernet0/0
- Mostrar los top-talkers:

```
show ip flow top-talkers
```

NetFlow

Configuración de Flexible Netflow

- Definir uno or más "exporters":

```
flow exporter EXPORTER-1 destination  
192.0.2.99  
transport udp      9996 source Loopback0  
template data timeout 300
```

NetFlow

Configuración de Flexible Netflow

- Definir uno o más “flow monitors”:

```
flow monitor FLOW-MONITOR-V4 exporter  
EXPORTER-1  
cache timeout active 300  
record netflow    ipv4 original-input
```

```
flow monitor FLOW-MONITOR-V6 exporter  
EXPORTER-1  
cache timeout active 300  
record netflow    ipv6 original-input
```

NetFlow

Configuración de Flexible Netflow

- Aplicar "flow monitors" a las interfaces activas

```
interface GigabitEthernet0/0/0
ip    flow monitor FLOW-MONITOR-V4 input
ip    flow monitor FLOW-MONITOR-V4 output
ipv6  flow monitor FLOW-MONITOR-V6 input
ipv6  flow monitor FLOW-MONITOR-V6 output
```


NetFlow

Configuración de Flexible Netflow

- Se pueden agregar flujos en el router

```
show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source  
address ipv4 destination address sort counter bytes top 50
```

- O en plataformas más nuevas:

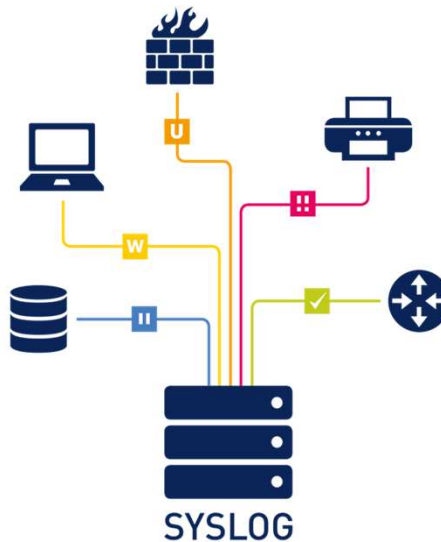
```
show flow monitor FLOW-MONITOR-V4 cache sort highest ipv4 source  
address top 50 format table
```

Syslog

Syslog

Los dispositivos de red, los hosts y los servidores, generan avisos ante incidentes que ocurran, con la finalidad de su análisis posterior, a efectos de diagnosticar posibles problemas.

El protocolo Syslog permite centralizar la información anterior, de modo de protegerla ante fallos de los dispositivos, ataques a vulnerabilidades de los equipos, virus, etc.



Syslog

El término Syslog se utiliza tanto para describir un estándar, como también para describir el protocolo desarrollado para ese estándar.

El protocolo syslog se desarrolló para sistemas UNIX en la década de 1980, pero IETF lo documentó por primera vez como RFC 3164 en 2001.

Syslog usa el puerto UDP 514 para enviar mensajes de notificación de eventos a través de redes IP a los recolectores de mensajes de eventos.

Muchos dispositivos de red admiten syslog, incluidos: routers, switches, servidores de aplicaciones, firewalls y otros dispositivos de red.

El protocolo syslog permite que los dispositivos de red envíen sus mensajes del sistema operativo a través de la red a los servidores syslog.

Hay varios paquetes de software de servidor syslog diferentes para Windows y UNIX. Muchos de ellos son gratuitos.

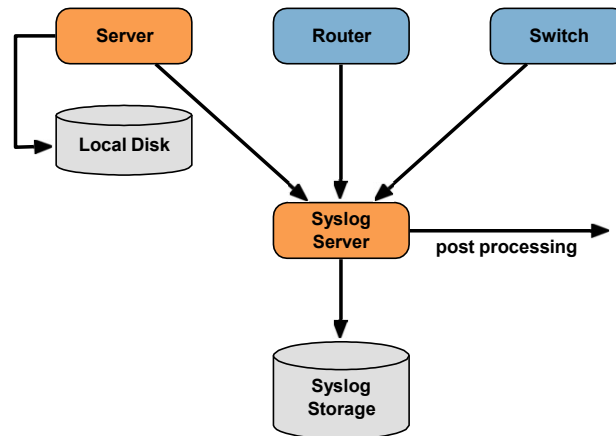
Syslog

El servicio de registro de syslog proporciona tres funciones principales:

- La capacidad de recopilar información de registro para monitorear y solucionar problemas
- La capacidad de seleccionar el tipo de información de registro que se captura.
- La capacidad de especificar los destinos de los mensajes syslog capturados En los dispositivos de red de Cisco, el protocolo syslog comienza enviando mensajes del sistema y la salida de depuración a un proceso de registro local interno al dispositivo.

Syslog

Registro Centralizado



Syslog

Estos mensajes se pueden recuperar sin necesidad de acceder al dispositivo real.

Los mensajes de syslog y las salidas almacenadas en el servidor externo se pueden incorporar a varios informes para facilitar la lectura.

Alternativamente, los mensajes de syslog pueden enviarse a un búfer interno. Los mensajes enviados al búfer interno solo se pueden ver a través de la CLI del dispositivo.

Finalmente, el administrador de la red puede especificar que sólo se envíen ciertos tipos de mensajes del sistema a varios destinos. Por ejemplo, el dispositivo puede configurarse para reenviar todos los mensajes del sistema a un servidor syslog externo.

Sin embargo, los mensajes de nivel de debug se reenvían al búfer interno y sólo el administrador puede acceder a ellos desde la CLI. Los niveles numéricos más pequeños son las alarmas de syslog más críticas. El nivel de gravedad de los mensajes se puede configurar para controlar dónde se muestra cada tipo de mensaje (es decir, en la consola o en otros destinos).

Syslog

La lista completa de niveles de syslog:

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	2	Critical condition
Error	3	Error Condition
Warning	4	Warning Condition
Notification	5	Normal, but significant Condition
Informational	6	Information Message
Debugging	7	debugging message

Cada nivel de syslog tiene su propio significado:

Nivel de advertencia - Nivel de emergencia: estos mensajes son mensajes de error sobre fallas de software o hardware; este tipo de mensajes significa que la funcionalidad del dispositivo se ve afectada. La gravedad del problema determina el nivel de syslog real aplicado.

Syslog

Nivel de depuración (debug): este nivel indica que los mensajes se generan al emitir varios comandos de debug.

Nivel de notificación: el nivel de notificaciones es sólo para información, la funcionalidad del dispositivo no se ve afectada. Las transiciones de interfaz hacia arriba o hacia abajo y los mensajes de reinicio del sistema se muestran en el nivel de notificaciones.

Además de especificar la gravedad, los mensajes de syslog también contienen información sobre la instalación. Las instalaciones de Syslog son identificadores de servicio que identifican y categorizan los datos de estado del sistema para informar de mensajes de error y eventos. Las opciones de la función de registro que están disponibles son específicas del dispositivo de red. Por ejemplo, los switches Cisco de la serie 2960 que ejecutan Cisco IOS versión 15.0 (2) y los routers Cisco 1941 que ejecutan Cisco IOS versión 15.2 (4) admiten 24 opciones de instalaciones que se clasifican en 12 tipos.

Syslog

Algunas funciones comunes de mensajes de Syslog informadas en los routers Cisco IOS abarcan:

- IP
- Protocolo OSPF
- Sistema operativo SYS
- Seguridad IP (IPsec)
- IP de interfaz (IF)

Por defecto, el formato de los mensajes de syslog en el software Cisco IOS es el siguiente:

seq no: timestamp:% installation-severity-MNEMONIC: description

Syslog

Timestamp

Los mensajes de log pueden tener una marca o etiqueta de tiempo (timestamp) y se puede incluir la dirección de origen de los mensajes de Syslog. Esto mejora la depuración y la gestión en tiempo real.

Cuando se da el comando “service timestamps log uptime”, la cantidad de tiempo desde la última vez que se inició el dispositivo se incluye en los logs.

Una versión más útil de este comando se obtiene si se emplea la palabra clave “datetime” en lugar de la palabra clave “uptime”, esto obliga a incluir en cada log la fecha y la hora asociadas con el evento.

Cuando se usa la palabra clave datetime, se debe configurar el reloj en el dispositivo de red. Esto se puede lograr de dos formas:

- Configurarlos manualmente, usando el comando “clock set”
- Configurarlos automáticamente, usando el protocolo de sincronismo de red (NTP)

Syslog

Para habilitar los timestamps se pueden emplear los siguientes comandos:

```
router (config) #service timestamps debug datetime msec
```

```
router (config) #service timestamps log datetime msec
```

Estos comandos agregan timestamps a los debugs en el formato MMM DD HH: MM: SS, indicando la fecha y la hora según el reloj del sistema. Si no se ha configurado el reloj del sistema, la fecha y la hora están precedidas por un asterisco (*) para indicar que probablemente la fecha y la hora no sean correctas.

En general, es aconsejable configurar timestamps en milisegundos, ya que esto proporciona un alto nivel de claridad al mirar las salidas de debug, ya que brindan una mejor indicación de la sincronización de los diversos eventos de debug en relación con los demás. Sin embargo, hay que tener en cuenta que, cuando el puerto de la consola emite muchos mensajes, es posible que no se correlacionen con el momento real del evento. Por lo tanto, no conviene utilizar timestamps en mseg para probar problemas de rendimiento, sino para obtener información relativa sobre cuándo ocurren los eventos.

Los timestamps en milisegundos (mseg) se habilitan mediante el comando "service timestamps".

Syslog

Configuración de Syslog

Para ver los mensajes de syslog, se debe instalar un servidor de syslog en una estación de trabajo de la red.

El servidor de syslog proporciona una interfaz relativamente fácil de usar para ver la salida de mensajes. El servidor analiza la salida y coloca los mensajes en columnas predefinidas para facilitar la interpretación. Si los timestamps están configurados en el dispositivo de red que genera los mensajes de syslog, la fecha y hora de cada mensaje se muestran en la salida del servidor de syslog.

Por defecto, los routers y switches de Cisco envían a la consola mensajes de log para todos los niveles de gravedad.

En algunas versiones de IOS, el dispositivo también almacena por defecto los mensajes de log. Para habilitar estas dos funciones, se pueden utilizar los comandos "logging console" y "logging buffered" en el modo de configuración global.

El comando "show logging" muestra las configuraciones de logging. A continuación se muestra un ejemplo.

Syslog

Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 32 messages logged, xml disabled, filtering disabled

Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled

Buffer logging: level debugging, 32 messages logged, xml disabled, filtering disabled

Exception Logging: size (4096 bytes)

Count and timestamp logging messages: disabled

Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 34 message lines logged

Logging Source-Interface: VRF Name:

Log Buffer (8192 bytes):

*Jan 2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted

*Jan 2 00:00:02.621: %IOS_LICENSE_IMAGE_APPLICATION_6 LICENSE LEVEL: Module

Syslog

El resultado del ejemplo anterior, señala que se han registrado 32 mensajes de este tipo.

La segunda línea resaltada indica que en este router se registra en un búfer interno.

Debido a que este router tiene habilitado el registro en un búfer interno, el comando show logging también enumera los mensajes en ese búfer.

Configuración del cliente syslog

Son tres los pasos para configurar el router para que envíe mensajes del sistema a un servidor syslog donde se pueden almacenar, filtrar y analizar:

Paso 1. Configurar el nombre de host de destino o la dirección IP del servidor syslog en el modo de configuración global:

```
R1 (config) # logging 192.168.1.3
```

Syslog

Paso 2. Controlar los mensajes que se enviarán al servidor de syslog con el comando en modo de configuración global “logging trap *level*”. Por ejemplo, para limitar los mensajes a los niveles 4 e inferiores (0 a 4), utilizar uno de los dos comandos equivalentes:

R1 (config) # logging trap 4

R1 (config) # logging trap warning

Paso 3. Opcionalmente, configurar la interfaz de origen con el comando de modo en configuración global “logging source-interface *interface-type interface number*”. Esto especifica que los paquetes syslog contienen la dirección IPv4 o IPv6 de una interfaz específica, independientemente de la interfaz que utilice el paquete para salir del router. Por ejemplo, para configurar la interfaz de origen g0 / 0, usar el siguiente comando:

R1 (config) # logging source-interface g0 / 0

Syslog

Verificar syslog

Se puede utilizar el comando “show logging”, con algunas opciones de “pipe”:

```
show logging | include changed state
```

```
show logging | begin June 12
```

Si se desea crear un mensaje de syslog sin apagar una interfaz u otra acción, alcanza con utilizar la sintaxis:

```
send log [severity] [text to send]
```

```
ej .: send log 4 ¡Advertencia!
```

Caso particular

El siguiente ejemplo habilita timestamps en los mensajes de syslog, mostrando la fecha y hora actuales en relación con la zona horaria local, con el nombre de la zona horaria incluido:

```
service timestamps log datetime localtime show-timezone
```

Syslog

Seguridad

Los routers Cisco pueden registrar información sobre cambios de configuración, descargas de ACL, estado de interfaces, uso de la CPU y muchos otros tipos de eventos.

Por ejemplo, utilizar los comandos “memory free low-watermark threshold io *valor_en KB*” y “memory free low-watermark processor *valor_en_KB*” para establecer los umbrales de memoria (de memoria de entrada-salida, y de memoria de procesador, respectivamente).

El router enviará notificaciones, especificadas en kilobytes, al servidor syslog cuando la memoria libre disponible caiga por debajo del umbral.

El router enviará notificaciones nuevamente cuando la memoria libre disponible se eleve al cinco por ciento por encima del umbral.

NTP

NTP

Network Timing Protocol (NTP) permite distribuir señal de reloj en una red, y sincronizar de ese modo los dispositivos.

NTP sincroniza la hora normal entre un conjunto de clientes y servidores de tiempo distribuidos. Con esta sincronización, se pueden correlacionar los eventos con la hora en que se crearon los registros del sistema y la hora en que ocurren otros eventos específicos. Cada dispositivo debe poder acceder a un servidor NTP.

NTP utiliza UDP como su protocolo de transporte. Todas las comunicaciones NTP utilizan la hora universal coordinada (UTC), que es la misma que la hora media de Greenwich. Una red NTP generalmente obtiene su hora de una fuente de hora autorizada, como un reloj de radio o un reloj atómico que está conectado a un servidor de hora. NTP distribuye este tiempo a través de la red. NTP es extremadamente eficiente; no se necesita más de un paquete por minuto para sincronizar dos máquinas con un milisegundo de diferencia entre sí.

NTP utiliza una medida en estratos para describir a cuántos saltos NTP se encuentra una máquina de una fuente de tiempo autorizada. Un servidor de tiempo de estrato 1 tiene un reloj de radio o atómico que está conectado directamente. Un servidor de tiempo de estrato 2 recibe su tiempo de un servidor de tiempo de estrato 1. Y así sucesivamente. Una máquina que ejecuta NTP elige automáticamente como fuente de tiempo la máquina con el número de estrato más bajo con la que está configurada para comunicarse a través de NTP.

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html>

NTP

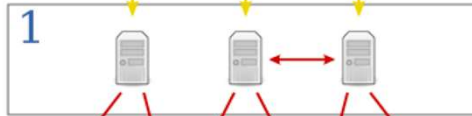
Cómo trabaja NTP

Estrato 0

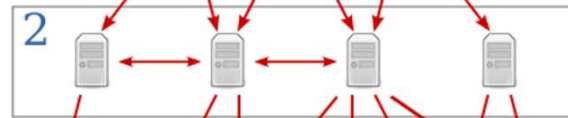


GPS/CDMA

Estrato 1



Estrato 2



Estrato 3



NTP

Estrato 0

Los servidores NTP Stratum 1 utilizan fuentes de tiempo Stratum 0

El estrato 0 son dispositivos de cronometraje de alta precisión también conocidos como relojes de referencia

Las fuentes de transmisión de tiempo del Estrato 0 incluyen;

Relojes atómicos

Relojes de radio

Sistema de posicionamiento global (GPS)

Los servidores de estrato 0 son extremadamente caros.

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html>

NTP

NTP tiene dos formas de evitar la sincronización con una máquina cuya hora puede ser ambigua:

- NTP nunca se sincroniza con una máquina que no está sincronizada.
- NTP compara el tiempo que informan varias máquinas y no se sincroniza con una máquina cuyo tiempo es significativamente diferente de los demás, incluso si su estrato es menor.

Las **comunicaciones entre máquinas que ejecutan NTP**, conocidas como **asociaciones**, suelen estar configuradas estáticamente; cada máquina recibe las direcciones IP de todas las máquinas con las que debe formar asociaciones. Un par de máquinas asociadas pueden mantener la hora exacta intercambiando mensajes NTP entre sí. Sin embargo, en un entorno LAN, se puede configurar NTP para utilizar mensajes de broadcast IP. Con esta alternativa, se puede configurar la máquina para enviar o recibir mensajes de broadcast, pero la precisión del cronometraje se reduce ligeramente porque el flujo de información es unidireccional.

La implementación de Cisco de NTP no admite el servicio de estrato 1; no es posible conectarse a un radio o reloj atómico. Se recomienda obtener el servicio de hora para la red de los servidores NTP públicos disponibles en Internet IP.

Si la red está aislada de Internet, la implementación de NTP de Cisco permite configurar una máquina para que actúe como si estuviera sincronizada mediante NTP, cuando en realidad ha determinado la hora mediante otros métodos. Otras máquinas se sincronizan con esa máquina mediante NTP.

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html>

NTP

Modo de servidor NTP

En este modo, el router lee la hora de la fuente NTP. A menos que definamos manualmente la fuente NTP, el router usa su propio reloj como fuente NTP. Según lo que se requiera, es posible configurar el reloj del router o bien usar un reloj externo como fuente NTP. Una vez que se configura la fuente NTP, el router del servidor NTP anuncia esta vez en la red. En este modo, el router sólo anuncia actualizaciones NTP. No acepta ninguna actualización NTP para otros servidores NTP.

Modo cliente / servidor NTP

En este modo, el router recibe actualizaciones del servidor NTP y las anuncia desde sus propias interfaces. De esta manera, el enrutador juega ambos roles. Como cliente NTP recibe actualizaciones NTP y como servidor NTP anuncia actualizaciones NTP.

En este modo, como servidor NTP, en lugar de utilizar su propia fuente NTP, el enrutador utiliza las actualizaciones NTP recibidas de otro servidor NTP para anunciar las actualizaciones NTP. Esta característica nos permite utilizar una única fuente NTP centralizada en el servidor NTP.

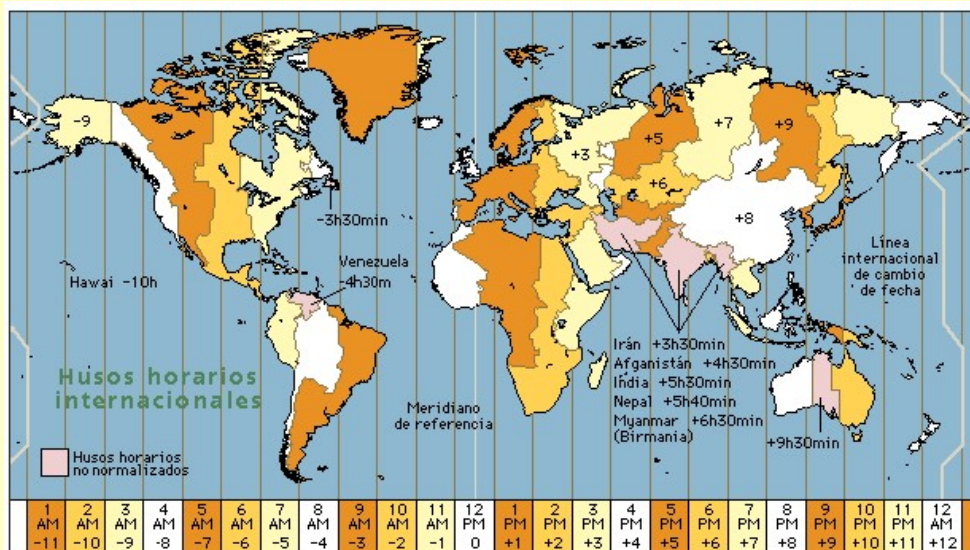
Modo de cliente NTP

En este modo, el router solo recibe actualizaciones NTP. No anuncia las actualizaciones recibidas. Los usa para sincronizar su propio reloj.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Mapa de zonas horarias



NTP

Configuración del servidor NTP

La configuración del servidor NTP es sencilla. Solo se necesitan dos comandos para implementar un router como servidor NTP.

Router (config) #ntp master [nivel de estrato]

Router (config) #ntp source [Interfaz / nombre de host o dirección IP de la fuente NTP]

En el primer comando, la indicación del nivel de estrato es opcional. Si no lo especificamos, el router usará el valor predeterminado. El nivel de estrato predeterminado del reloj interno es 7.

En el segundo comando, tenemos que especificar la fuente NTP. Podemos utilizar cualquier fuente NTP válida aquí.

Para configurar la zona horaria, puede emplearse el comando

Router(config)#clock timezone *Palabra diferencia_horaria*

donde la Palabra permite recordar a qué corresponde la zona horaria, y la diferencia:horaria corresponde a la diferencia en horas respecto de la hora de Greenwich.

Ejemplo:

R3(config)#clock timezone EST -20

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Para utilizar un servidor NTP público, el router debe estar conectado a Internet y el puerto UDP 123 debe estar permitido en el firewall.

Para utilizar otro servidor NTP de la red interna, escribir la dirección IP de ese servidor.

Para usar el reloj interno de un router, usar cualquier dirección IP configurada en cualquier interfaz del mismo.

Si se utiliza el reloj interno del router como fuente NTP, podemos usar la dirección IP de cualquier interfaz. Si hay definida una interfaz loopback, el único beneficio de usar su dirección IP es que esa interfaz de loopback permanece siempre encendida.

```
R1(config)#ntp master
R1(config)#ntp source loopback 0
R1(config)#
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Configurar interfaces para que actúen como NTP Server only

Por defecto, el router funciona en modo NTP server / client. En ese modo el router anuncia y escucha mensajes NTP en todas las interfaces activas. Si queremos implementar este router NTP Server only, tenemos que configurar todas las interfaces activas de manera que solo difundan el mensaje NTP. Por suerte, este proceso también es muy sencillo. Solo requiere el siguiente comando en cada interfaz activa.

Router(config-if)ntp broadcast

Veamos un ejemplo:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0
R1(config-if)#ntp broadcast
R1(config-if)#exit
R1(config)#interface serial 0/1
R1(config-if)#ntp broadcast
R1(config-if)#exit
R1(config)#exit
R1#
Mar  1 05:57:17.481: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Configurar NTP Server client

Por defecto, los routers funcionan en este modo. Por lo tanto, no se requiere ninguna configuración adicional. Pero hay un aspecto a considerar.

Por defecto, en este modo, el router usa su propio reloj como fuente NTP.

Entonces, si queremos construir una jerarquía donde este router reciba sincronismo de otro servidor NTP, debemos cambiar la fuente NTP en este router.

El siguiente comando se usa para cambiar la fuente NTP

```
Router (config) #ntp server [dirección IP de origen NTP]
```

Para forzar que un router tome sincronismo de una dirección IP se puede dar el comando (en el ejemplo, la dirección de la fuente de referencia es 100.0.0.1):

```
R2 (config) #ntp server 100.0.0.1
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Configurar la dirección IP del servidor NTP y guardar la configuración

```
*Mar 1 00:00:14.195: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3,
R2#show clock
*00:08:24.118 UTC Fri Mar 1 2002
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 100.0.0.1
R2(config)#exit
R2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#show clock
00:09:56.702 UTC Fri Mar 1 2002
R2#show clock
23:28:11.152 UTC Thu Apr 5 2018
R2#
```

Updating process usually takes 2 to 3 minutes

Es normal que no se visualice inmediatamente la actualización de la fecha y la hora, lo cual puede llevar 2 o 3 minutos. Pero una vez sincronizado el reloj, se actualizará automáticamente.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Configurar NTP Client only

Para configurar un router sólo como cliente NTP, necesitamos dos comandos.

```
Router(config)#ntp server [NTP Server IP address]
```

```
Router(config-if)#ntp broadcast client
```

Como se explicó anteriormente, el primer comando insiste en que el router use la hora del servidor NTP en lugar de su propia hora local y el segundo comando configura la interfaz activa para escuchar sólo el mensaje de transmisión NTP.

Como ejemplo, configuremos R3 y R4 como clientes NTP únicamente. Podemos usar cualquier dirección IP configurada desde el router del servidor NTP para obtener las actualizaciones NTP. Para entenderlo más claramente, esta vez usaremos la dirección IP de la interfaz serial de R2 para conectarnos con el servidor NTP.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Configurar NTP Client only

La siguiente figura muestra comandos paso a paso para configurar R3 como cliente NTP únicamente

```
R3#show clock
00:36:37.450 UTC Fri Mar 1 2002
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 30.0.0.2
R3(config)#interface serial 0/2
R3(config-if)#ntp broadcast client
R3(config-if)#exit
R3(config)#exit
R3#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Testing y troubleshooting de problemas de configuración de NTP

Para realizar pruebas y solucionar problemas, NTP ofrece dos comandos show; de ntp status y de ntp associations. Veamos estos dos comandos en detalle.

`show ntp status`

Este comando lista mucha información. La primera línea contiene tres columnas; clock status, nivel de estrato y fuente ntp. Veamos estas columnas en detalle.

Clock status: -

Esta columna muestra si el reloj está sincronizado o no. En ella se mostrará la hora actualizada solo cuando el reloj esté sincronizado.

Nivel de estrato: -

Esta columna muestra después de la sincronización, en qué nivel de confiabilidad se encuentra el reloj del router. Si el router no está conectado con ningún servidor NTP o el reloj no está sincronizado con ninguna fuente NTP, esta columna siempre mostrará el valor 16. Si el router está sincronizado con cualquier fuente NTP, esta columna mostrará el nivel de estrato de este router en la jerarquía NTP. Por lo general, permanece un nivel por debajo de la fuente NTP a menos que se modifique manualmente.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Aspectos clave

El estrato 0 representa el reloj atómico y no se usa en el router Cisco

Los estratos 1-15 son niveles válidos. 1 es la fuente NTP más confiable y 15 es la peor (pero aún válida) fuente NTP.

El estrato 16 representa una situación en la que el router no está conectado con ninguna fuente NTP o aún no está sincronizado con ningún servidor NTP.

Por defecto, después de la sincronización, el router mantiene su reloj un nivel por debajo de la fuente o servidor NTP. Nos permite construir una jerarquía adecuada.

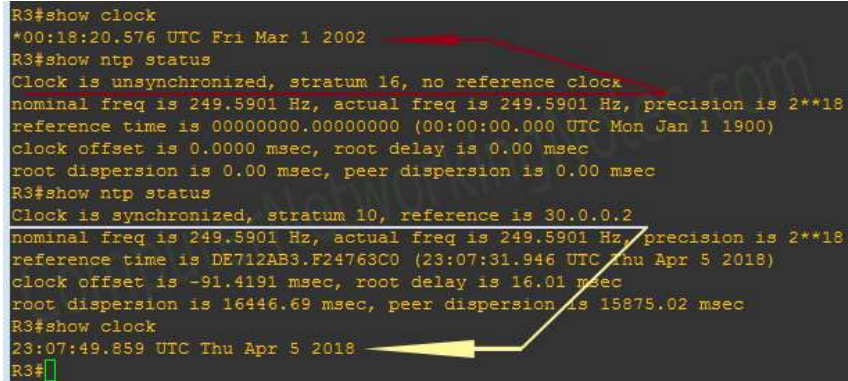
El nivel de estrato por defecto del reloj interno del router es 7.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Fuente NTP: -

Esta columna muestra la fuente o referencia de la fuente NTP desde donde se sincroniza esta hora.



```
R3#show clock
*00:18:20.576 UTC Fri Mar 1 2002
R3#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**18
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
R3#show ntp status
Clock is synchronized, stratum 10, reference is 30.0.0.2
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**18
reference time is DE712AB3.F24763C0 (23:07:31.946 UTC Thu Apr 5 2018)
clock offset is -91.4191 msec, root delay is 16.01 msec
root dispersion is 16446.69 msec, peer dispersion is 15875.02 msec
R3#show clock
23:07:49.859 UTC Thu Apr 5 2018
R3#
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Show ntp associations

Al igual que el comando show ntp status, este comando también proporciona mucha información. Nuevamente, a partir de esta información, solo necesitamos centrarnos en las tres primeras columnas; dirección, ref reloj y st. Entendamos estas columnas en detalle

address:-

Esta es la dirección del servidor NTP desde donde este router recibió actualizaciones NTP. Esta columna puede contener dos símbolos adicionales; * y ~. El * muestra el modo NTP en el que está funcionando el servidor NTP y ~ muestra cómo NTP obtiene tiempo de la fuente NTP.

ref clock: -

Esta es la fuente NTP desde donde el servidor NTP recibió la hora.

s t:-

Este es el nivel de estrato de la fuente NTP.

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

La siguiente figura muestra la salida de este comando para dos casos:

```
R1#show ntp status
Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**18
reference time is DE7133BE.CEEB94AE (19:46:06.808 EDT Thu Apr 5 2018)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
R1#show ntp association
```

address	ref clock	st	when	poll	reach	delay	offset	disp
*~127.127.7.1	127.127.7.1	7	40	64	377	0.0	0.00	0.0

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
R1#

```
R2#show ntp status
Clock is synchronized, stratum 9, reference is 100.0.0.1
nominal freq is 249.5901 Hz, actual freq is 249.5898 Hz, precision is 2**18
reference time is DE713349.D9125FC9 (23:44:09.847 UTC Thu Apr 5 2018)
clock offset is 475.3939 msec, root delay is 4.00 msec
root dispersion is 996.32 msec, peer dispersion is 520.90 msec
R2#show ntp association
```

address	ref clock	st	when	poll	reach	delay	offset	disp
*~100.0.0.1	127.127.7.1	8	107	256	377	4.0	475.39	520.9

* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
R2#

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

La siguiente figura muestra la salida de este comando para otros dos casos:

```
R3#show ntp status
Clock is synchronized, stratum 10, reference is 30.0.0.2
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**18
reference time is C0294B47.6B15D286 (00:35:19.418 UTC Fri Mar 1 2002)
clock offset is 508028451548.9979 msec, root delay is 8.01 msec
root dispersion is 6628445.16 msec, peer dispersion is 7883.09 msec
R3#show ntp associations

      address          ref clock      st when poll re  Both NTP client received
*~30.0.0.2             100.0.0.1      9   43   64  NTP updates from same NTP
* master (syncd), # master (unsyncd), + selected, server but they used different
                                     IP addresses of NTP server
R3#
Both stand one level
```

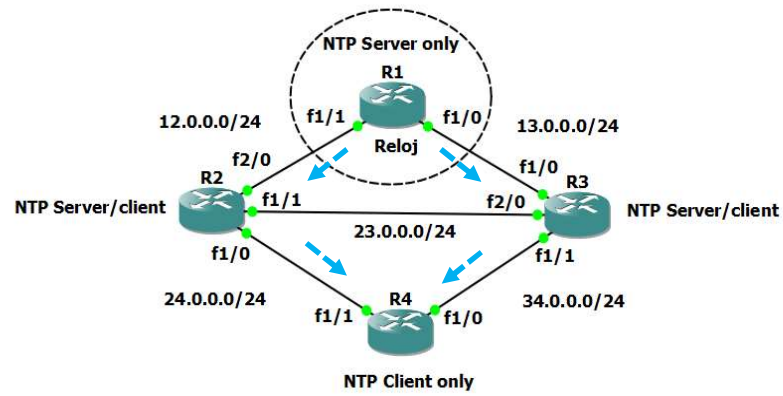
```
R4#show ntp status down from their master to get them
Clock is synchronized, stratum 10, reference is 40.0.0.2
nominal freq is 249.5901 Hz, actual freq is 249.5901 Hz, precision is 2**18
reference time is C0294BE0.92C81302 (00:37:52.573 UTC Fri Mar 1 2002)
clock offset is 508028577117.4387 msec, root delay is 32.03 msec
root dispersion is 6502835.17 msec, peer dispersion is 7875.09 msec
R4#show ntp associ
R4#show ntp associations

      address          ref clock      st when poll reach delay offset disp
*~40.0.0.2             100.0.0.1      9   13   64  377   20.0 508028 7875.1
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
R4#
Shows this address is configured as NTP server
```

<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-ntp-in-cisco-router.html>

NTP

Topología de ejemplo:



Funciones de gestion y herramientas

:	Función	Área funcional	Herramientas
	Detección de fallos		
	Definición de indicadores		
	Definiciones de funciones		
	Gestión de SLA		
	Prevención de fallos (monitoreo de tendencias)		
	Gestión de topología		
	Recursos usados		
	Uso de backups		
	Registro de eventos		
	Activación de recursos		
	Monitoreo de indicadores		
	Gestión de inventario		
	Aislamiento del fallo		
	Implantación de sistemas de seguridad		
	Diagnóstico		
	Gestión de servicios de directorio		
	Análisis de riesgos		
	Gestión de incidencias		
	Gestión de cambios de configuración		
	Reportes de violaciones		
	Perfiles de usuarios		
	Análisis de indicadores		
	Funciones de protección		
	Áreas funcionales: Configuration, Security, Fault, Performance, Accounting		