Prácticas recomendadas de implementación de Cisco IOS XR para OSPF/IS-IS y routing BGP

Contenido

DESCARGO

Este documento proporciona un resumen de alto nivel de algunas recomendaciones de prácticas recomendadas establecidas para el ruteo OSPF/IS-IS y BGP. Estas recomendaciones no representan un diseño validado de Cisco, y se requiere el cuidado y la atención debidos para la implementación en cualquier entorno operativo específico. Deben leerse junto con las guías de configuración y la documentación técnica de los productos correspondientes, que describen con mayor detalle cómo se pueden implementar estas recomendaciones de prácticas recomendadas. Las referencias que se hacen en este documento a las guías de configuración y a la documentación técnica de productos específicos se consideran sólo como ejemplos. Consulte las guías de configuración y la documentación técnica de sus productos específicos.

Introducción

Este documento describe algunas prácticas recomendadas y recomendaciones establecidas para crear redes simplificadas, eficientes y escalables impulsadas por plataformas de ruteo IOS XR. Este documento se centra en las técnicas de implementación específicas y las opciones de soporte de funciones disponibles en IOS XR para ayudar a personalizar las implementaciones OSPF/IS-IS y BGP.

Implementación de OSPF

El protocolo OSPF, definido en RFC 2328, es un IGP utilizado para distribuir información de ruteo dentro de un único sistema autónomo. OSPF ofrece varias ventajas sobre otros protocolos, pero se requiere un diseño adecuado para crear una red escalable y tolerante a fallas.

Para obtener más información sobre OSPF, consulte:

- Nota técnica sobre OSPF: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc13
- Guía de configuración para OSPF: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-6/routing/configuration/guide/b-routing-cg-asr9000-76x/implementing-ospf.html
- Referencia de comandos: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/routing/configuration/guide/b-routing-cg-asr9000-711x/implementing-ospf.html?dtid=osscdc000283

'Conceptos clave'

■ Jerarquía: un modelo de red jerárquico es una herramienta útil de alto nivel para diseñar una infraestructura de red fiable y ayuda a dividir los problemas de diseño de red complejos en áreas más pequeñas y manejables.

■ Modularidad: al dividir varias funciones de una red en módulos, la red es mucho más fácil de diseñar. Cisco ha identificado varios módulos, incluidos el campus empresarial, el bloque de servicios, el Data Center y la frontera de Internet.

■ Resistencia: la red está disponible en condiciones normales y anormales. Las condiciones normales incluyen flujos de tráfico esperados, patrones y eventos programados como ventanas

de mantenimiento. Entre las condiciones anómalas se incluyen fallos de hardware o software, cargas de tráfico extremas, patrones de tráfico inusuales, eventos de denegación de servicio (DoS) y otros eventos planificados o no planificados.

■ Flexibilidad: la capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin pasar por una actualización a gran escala (es decir, sustituir los principales dispositivos de hardware).

Como práctica recomendada general, la implementación de red debe tener en cuenta el "tramo" de la red para contener las rutas dentro de un límite específico y las rutas que son relevantes y requeridas por los routers dentro de un dominio para el reenvío. El uso eficaz de las áreas OSPF ayuda a reducir el número de anuncios de estado de link (LSA) y otro tráfico de sobrecarga enviados a través de la red. Una de las ventajas de crear una jerarquía es que este enfoque ayuda a garantizar que el tamaño de la base de datos de topología que cada router deberá mantener sea manejable y se ajuste al perfil de memoria del router.

Redistribución de BGP y Dominio OSPF

OSPF está diseñado para transportar solo unos pocos miles de rutas. En un nivel alto, las "áreas" OSPF son secciones de una red donde cualquier router conoce la capacidad de ruteo de cada otro router en el área. Esto permite una convergencia rápida cuando cualquier dispositivo tiene un problema, pero con el costo de una escalabilidad reducida. Como tal, OSPF se utiliza en un núcleo de Proveedor de Servicios para proporcionar la conectividad de nivel base entre todos los dispositivos de núcleo, y todos los dispositivos de núcleo se configuran dentro de la misma área OSPF. Este es un diseño estándar de una red "subyacente".

Por el contrario, BGP está diseñado para transportar significativamente más rutas que la mayoría de los IGP, como OSPF. Riesgos asociados con la redistribución de rutas BGP en un IGP como OSPF. Si un proveedor de servicios requiere que las rutas BGP se redistribuyan en el dominio IGP para cualquier caso de uso, el proveedor de servicios debe administrar esto con un filtrado adecuado en los routers de límite del sistema autónomo (ASBR) y con la protección contra sobrecarga configurada en el router receptor. Si la redistribución de BGP no se filtra en un OSPF, cada dispositivo OSPF en el ASBR comenzará a recibir rutas mucho más allá de su capacidad de manejar al mismo tiempo. Los routers Cisco IOS XR, por ejemplo, solo permitirán que 10,000 rutas BGP se redistribuyan en OSPF de forma predeterminada. Cuando las rutas BGP se redistribuyen en el IGP, es posible que todos los routers dentro del dominio IGP reciban estas rutas, dependiendo del diseño IGP. De acuerdo con el protocolo OSPF RFC, cualquier ruta externa que se redistribuya en OSPF debe distribuirse a todos los routers en el área OSPF.

Administración de la redistribución en IGP

Como mejor práctica general, la redistribución sólo debe hacerse de manera cuidadosa y planificada cuando no haya otras opciones para aprender las rutas de accesibilidad que proporcionará una función de redistribución.

Como práctica general, debe:

■ Evitar la redistribución
■ Evite transportar rutas en un dominio IGP
■ Implementación de BGP para accesibilidad externa

■ Utilice IGP para transportar información de salto siguiente solamente; por ejemplo, Loopback 0

Limitaciones de Redistribución de Rutas OSPF

La escala de prefijos redistribuidos de BGP a OSPF se administra con la configuración de protección contra sobrecarga (max-lsa). Esta es la única protección contra fugas de una gran cantidad de rutas en el dominio OSPF. En caso de redistribución en un solo área OSPF, debe implementar varias capas de protección contra la redistribución de rutas.

Estas son algunas de las opciones disponibles para la protección contra la redistribución de rutas:

■ Filtrado de redistribución mediante ACL
■ Límite de redistribución: configuración global para evitar que se redistribuya más de un número específico de rutas. Si se elimina el filtro, el límite de redistribución global es la segunda línea de defensa y protegerá los núcleos.
■ Configuraciones Max-LSA en todos los dispositivos en el área OSPF: si las protecciones mencionadas en las viñetas anteriores fallan, fuerce a los routers de recepción a rechazar los LSA excesivos entrantes.

Protección contra Sobrecarga de la Base de Datos de Estado de Link OSPF

La función OSPF Link-State Database Overload Protection proporciona un mecanismo en el nivel OSPF para limitar el número de LSA no autogenerados para un proceso OSPF dado. Si otros routers en la red han sido mal configurados, pueden generar un alto volumen de LSAs, por ejemplo, para redistribuir grandes cantidades de prefijos en OSPF. Este mecanismo de protección ayuda a evitar que los routers reciban muchos LSA y, por lo tanto, experimenten escasez de memoria y CPU.

Comportamiento de funciones

Este es el comportamiento de la función:

■ Cuando se habilita esta función, el router mantiene un conteo del número de todos los LSA recibidos (no autogenerados).
■ Cuando se alcanza el valor de umbral configurado, se registra un mensaje de error.
■ Cuando se excede el número máximo configurado de LSA recibidos, el router deja de aceptar nuevos LSA.

```
max-lsa <max-lsa-count> <%-threshold-to-log-warning> ignore-count <ignore-count-value> ignore-time <ignore-time-in-minutes> reset-time <time-to-reset-ignore-count-in-minutes>
```

Estados OSPF

Si el recuento de LSA recibidos es mayor que el número máximo configurado después de un minuto, el proceso OSPF desactiva todas las adyacencias y borra la base de datos OSPF. Este estado se denomina estado ignorado. En este estado, se ignoran todos los paquetes OSPF recibidos en todas las interfaces que pertenecen a la instancia OSPF y no se generan paquetes OSPF en las interfaces. El proceso OSPF permanece en el estado ignore durante el tiempo de ignorar configurado (el valor predeterminado es 5 minutos). Cuando caduca el tiempo de ignorar, el proceso OSPF vuelve al funcionamiento normal y genera adyacencias en todas sus interfaces.

Si el conteo de LSA excede el número max tan pronto como la instancia OSPF regresa del estado ignore, la instancia OSPF puede oscilar sin cesar entre su estado normal y el estado ignore. Para evitar esta oscilación infinita, la instancia OSPF cuenta cuántas veces ha estado en el estado ignore. Este contador se denomina ignore-count. Si ignore-count (default ignore-count is 5) excede su valor configurado, la instancia OSPF permanece permanentemente en el estado ignore.
Debe ejecutar el comando clear ospf para devolver la instancia OSPF a su estado normal. El ignore-count se restablece a cero si el conteo LSA no excede el número máximo nuevamente durante el tiempo configurado por la palabra clave reset-time.
Si utiliza la palabra clave warning-only, la instancia OSPF nunca ingresa en el estado ignore. Cuando el conteo de LSA excede el número máximo, el proceso OSPF registra un mensaje de error y la instancia OSPF continúa en su operación de estado normal.
No hay ningún valor predeterminado para max-lsa. El límite solo se comprueba si está configurado específicamente.

Una vez configurado max-lsa, otros parámetros pueden tener valores predeterminados:

- advertencia %-threshold-to-log predeterminada: 75%
- default ignore-count-value - 5
- default ignore-time-in-minutes - 5 minutes
- tiempo predeterminado para restablecer-ignorar-contar - 10 minutos

Este es un ejemplo de la implementación que muestra cómo configurar la instancia OSPF para aceptar 12000 LSA no autogenerados y 1000 LSA no autogenerados en VRF V1.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 0
RP/0/RSP0/CPU0:router(config-ospf)# max-lsa 12000
RP/0/RSP0/CPU0:router(config-ospf)# vrf V1
RP/0/RSP0/CPU0:router(config-ospf)# max-lsa 1000
```

El siguiente ejemplo muestra cómo visualizar el estado actual de la instancia OSPF.

```
RP/0/RSP0/CPU0:router# show ospf 0
    Proceso de ruteo "ospf 0" con ID 10.0.0.2
    El NSR (enrutamiento ininterrumpido) está desactivado
    Solo admite rutas TOS (TOS0) únicas
    Admite LSA opaco
    Es un router de borde de área
    Número máximo de LSA no autogenerados permitidos 12000
       Número actual de LSA 1 no autogenerados
       Umbral de mensaje de advertencia 75%
       Ignore-time 5 minutes, reset-time 10 minutes
       Ignore-count allowed 5, current ignore-count 0
```

Implementación de BGP

Las familias de direcciones BGP hacen del BGP un protocolo de ruteo "multiprotocolo". Se recomienda encarecidamente conocer cómo se utilizan las familias de direcciones para crear topologías escalables que sean fáciles de implementar y administrar. Mediante las familias de direcciones, el operador puede crear diferentes topologías para diferentes tecnologías, por ejemplo, EVPN, multidifusión, etc.

Para obtener más información sobre BGP, consulte la guía de configuración de BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html

BGP y BFD

La convergencia BGP en una red de proveedor de servicios es importante para satisfacer las expectativas de los clientes en cuanto a la creación de redes resistentes y tolerantes a fallos. De forma predeterminada, BGP tiene un temporizador Keepalive de 60 segundos y un temporizador Hold de 180 segundos. Todo esto significa que BGP será muy lento para converger a menos que haya ayuda disponible de los protocolos de soporte. El reenvío bidireccional (BFD) de BFD es uno de esos protocolos que está diseñado para ayudar a que los protocolos del cliente converjan más rápidamente. Con BFD, los protocolos pueden converger en cuestión de segundos.

Additional Information

■ Esta guía proporciona información conceptual y de configuración para BFD: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b-routing-cg-ncs5500-76x/implementing-bfd.html

■ Este informe técnico presenta una visión centrada en los proveedores de servicios sobre la convergencia rápida mediante BFD en los routers Cisco NCS 5500 y Cisco Network Convergence System 500 Series: https://xrdocs.io/ncs5500/tutorials/bfd-architecture-on-ncs5500-and-ncs500/

■ Para profundizar en el uso de BFD en interfaces Bundle e implementar Multipath y MultiHop BFD, consulte el repositorio https://xrdocs.io/.

Detección de peer lento BGP

Un par lento es un par que no puede mantenerse al día con la velocidad a la que el router está generando mensajes de actualización durante un período prolongado (en el orden de minutos) en un grupo de actualización. Cuando un par lento está presente en un grupo de actualización, el número de actualizaciones formateadas pendientes de transmisión se acumula. Cuando se alcanza el límite de caché, el grupo no tiene más cuotas para dar formato a los nuevos mensajes. Para formatear un mensaje nuevo, algunos mensajes existentes deben transmitirse mediante el par lento y, a continuación, eliminarse de la caché. El resto de los miembros del grupo que son más rápidos que el par lento y que han completado la transmisión de los mensajes formateados no tendrán nada nuevo que enviar, aunque puede haber redes BGP recién modificadas esperando ser anunciadas o retiradas. Este efecto de bloquear el formato de todos los pares de un grupo cuando uno de los pares consume las actualizaciones con lentitud es el problema del "par lento".

Los eventos que causan una agitación significativa en la tabla BGP (como los reinicios de conexión) pueden causar un breve pico en la velocidad de generación de actualizaciones. Un

par que se queda atrás temporalmente durante estos eventos pero que se recupera rápidamente después del evento no se considera un par lento. Para que un par se marque como lento, debe ser incapaz de mantenerse al día con la velocidad promedio de las actualizaciones generadas durante un período más prolongado (en el orden de unos minutos).

El par lento BGP puede ser causado debido a:

■ Pérdida de paquetes o tráfico alto en el link al par.
■ Un peer BGP podría estar cargado en términos de CPU y, por lo tanto, no puede mantener la conexión TCP a la velocidad requerida.
■ En este caso, se debe comprobar la capacidad del hardware de la plataforma y la carga ofrecida.
■ Problemas de rendimiento con la conexión BGP
■ Para obtener más información sobre la detección de pares lentos BGP, consulte: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_ir5_j4w_p4b

A continuación se indican algunas mitigaciones y prácticas recomendadas para administrar pares lentos:

■ QoS de extremo a extremo, que reserva ancho de banda para el tráfico del plano de control BGP durante la congestión.
■ Uso de valores correctos y apropiados de MSS / MTU mediante la configuración BGP PMTUD y/o TCP MSS.
■ Utilice el hardware correcto y minimice el número de rutas con respecto al hardware.

La detección de par lento está habilitada de forma predeterminada en Cisco IOS XR a partir de la versión 7.1.2. Los peers lentos son peers que tardan en recibir y procesar las actualizaciones de BGP entrantes y en reconocer las actualizaciones al remitente. Si el par lento está participando en el mismo grupo de actualización que otros pares, esto puede ralentizar el proceso de actualización para todos los pares. En esta versión, cuando IOS XR detecta un par lento, creará un syslog que tiene los detalles sobre el par específico.

Convergencia rápida mediante la convergencia independiente de prefijos BGP

Para los prefijos BGP, la convergencia rápida se logra mediante la Convergencia independiente de prefijos BGP (PIC), en la que BGP calcula una mejor trayectoria alternativa y una mejor trayectoria principal e instala ambas trayectorias en la tabla de ruteo como trayectorias principales y de respaldo.

Si el BGP next-hop remote se vuelve inalcanzable, BGP inmediatamente cambia a la trayectoria alternativa usando BGP PIC en lugar de recalcular la trayectoria después de la falla.

Si el PE remoto de siguiente salto BGP está activo, pero hay una falla de trayectoria, IGP TI-LFA FRR maneja la reconvergencia rápida a la trayectoria alternativa y BGP actualiza el siguiente salto IGP para el PE remoto.

BGP PIC se configura bajo la familia de direcciones VRF para la convergencia rápida de los prefijos VPN si un PE remoto se vuelve inalcanzable.

Para obtener más información sobre la convergencia independiente de prefijos BGP, consulte: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/bgp-pic.html

Seguridad BGP con BGP Flowspec

BGP Flowspec, en pocas palabras, es una función que le permite recibir especificaciones de flujo de tráfico IPv4/IPv6 (origen X, destino Y, protocolo UDP, puerto de origen A, etc.) y acciones que deben llevarse a cabo en ese tráfico (como descartar, supervisar o redirigir) a través de la actualización de BGP.

Dentro de la actualización de BGP, los criterios de coincidencia de Flowspec están representados por BGP NLRI, y las comunidades BGP extendidas representan las acciones.

Esta función se basa en RFC 5575 y se puede utilizar para ayudar a mitigar ataques DDoS. Cuando un host determinado dentro de una red está siendo atacado, podemos enviar una actualización de Flowspec a los routers de borde para que el tráfico de ataque pueda ser controlado o descartado, o incluso redirigido a otro lugar, tal vez a un dispositivo que pueda limpiar el tráfico (filtrar el tráfico 'malo' y reenviar solo el tráfico 'bueno' hacia el host afectado).

Una vez que un router recibe las especificaciones de flujo y las programa en las tarjetas de línea correspondientes, cualquier puerto L3 activo de esas tarjetas de línea comenzará a procesar el tráfico de entrada según las reglas de Flowspec.

Para obtener más información sobre la implementación de BGP FlowSpec, consulte:

- Informe técnico de BGP FlowSpec: https://xrdocs.io/ncs5500/tutorials/bgp-flowspec-on-ncs5500/
- Guía de configuración de BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_uqv_bxq_h2b

Función BGP Maximum Prefix

La función Maximum-Prefix es útil cuando, en un cambio de política saliente en el sitio de peering remoto, un router comienza a recibir más prefijos que los recursos del router de peering pueden manejar pero también para proteger los recursos o los peers BGP internos donde estos prefijos externos serán reenviados. Estos gastos generales de recursos podrían ser perjudiciales.

La función de prefijo máximo BGP impone un límite máximo en el número de prefijos que se reciben de un vecino para una familia de direcciones dada. De forma predeterminada, cada vez que el número de prefijos recibidos excede el número máximo configurado, la sesión BGP envía una notificación de cese al vecino y la sesión finaliza. Una familia de direcciones que cruza el prefijo máximo hará que toda la sesión BGP caiga, impactando a todas las otras familias de direcciones habilitadas en esa sesión BGP.

Esta función se utiliza comúnmente para que los peers BGP externos protejan la infraestructura interna de un proveedor de servicios. Sirve como barandilla para evitar el agotamiento de los recursos del router que podría ser causado por una configuración incorrecta, ya sea localmente o en el vecino remoto. Se recomienda encarecidamente configurar el prefijo máximo para

protegerlo contra errores de configuración locales o remotas que podrían desencadenar la inundación de la tabla de rutas. Esto también protege contra ataques de desagregación de prefijos.

La configuración del prefijo máximo de BGP se debe habilitar explícitamente en todos los routers eBGP para limitar el número de prefijos que debe recibir de un vecino determinado, ya sea cliente o AS de peering. Se recomienda que el operador configure un margen aceptable de prefijos adicionales que el sistema pueda mantener después de una cuidadosa evaluación de la memoria del sistema disponible. Debe tenerse en cuenta que no existe una configuración única que se pueda aplicar a todos los routers y que el umbral debe ajustarse cuidadosamente en función de la función del dispositivo en la red. Por ejemplo, si el prefijo máximo BGP se va a configurar en los vecinos BGP, el valor del prefijo máximo debe ser menor en los vecinos configurados en el reflector de ruta que en los vecinos configurados en los clientes reflectores de ruta. El reflector de ruta agrega los prefijos recibidos de varios routers de peering y luego vuelve a anunciar la tabla completa a los clientes reflectores de ruta. Por lo tanto, el reflector de ruta anunciará más prefijos a sus clientes que los que recibe de cada peer individual. De manera similar, un router de peering también puede volver a anunciar más prefijos hacia el reflector de ruta que los que recibe de cada peer externo individual.

En resumen, se recomienda revisar y configurar cuidadosamente la acción apropiada a tomar cuando se alcanza el umbral de prefijo máximo en un dispositivo de producción. Algunos atributos de las opciones del comando maximum-prefix se describen de la siguiente manera:

- Cuando una sesión BGP se configura explícitamente con la función de prefijo máximo sin ninguna palabra clave adicional (como sólo advertencia o reinicio potencial), la sesión se cerrará como comportamiento predeterminado. La acción predeterminada de la sesión de peer que se desactiva sin recuperación automática podría provocar una interrupción prolongada en el núcleo.

  ```
  %ROUTING-BGP-5-ADJCHANGE_DETAIL: neighbor 10.10.10.10 Down - BGP
  Notification received, maximum number of prefixes reach (VRF: default;
  AFI/SAFI: 1/1, 1/128, 2/4, 2/128, 1/133, 2/133) (AS: 65000) "
  %ROUTING-BGP-5-NBR_NSR_DISABLED_STANDBY: NSR deshabilitado en el vecino
  10.10.10.10 en el RP en espera debido a que el par excede el límite
  máximo de prefijos (VRF: predeterminado)
  ```

- La configuración de la opción descartar trayectos adicionales descarta todos los prefijos en exceso recibidos del vecino por encima del umbral de valor máximo configurado. Esta caída no produce inestabilidad en la sesión. Las ventajas de esta opción incluyen limitar la utilización de la memoria de proceso BGP y detener el inestabilidad de los peers dentro de la red principal. Sin embargo, esto puede dar lugar a que se descarten los loops de reenvío para los prefijos ya que las entradas de reenvío pueden volverse inconsistentes entre los routers en la red.
- Cuando se utiliza add-path, el valor de prefijo máximo configurado se aplica a las trayectorias en lugar de a los prefijos, ya que el NLRI está formado por el prefijo y los atributos de la trayectoria. Consulte la siguiente referencia de comandos para obtener más información:

https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/b-ncs5500-bgp-cli-reference/b-ncs5500-bgp-cli-reference_chapter_01.html

Recomendación: Evalúe cuidadosamente las siguientes opciones al configurar el comando maximum-prefix:

- No se ha definido ninguna acción explícita: el router cerrará la sesión y mantendrá la relación de vecino BGP inactiva hasta que el operador borre manualmente la sesión BGP. [clear bgp command]
- Restart [time-interval]: interrumpa la sesión e intente un reinicio automático de la sesión BGP periódicamente después de un temporizador configurado. Esto será exitoso si el peer remoto deja de anunciar los prefijos excesivos de lo contrario la sesión BGP se apagará nuevamente (causando así inestabilidad periódica).
- Discard-extra-paths: Con la opción discard-extra-paths, la sesión BGP permanece activa pero se descartan los prefijos sobre el límite máximo de prefijos. Esta opción no afecta a otras familias de direcciones en las que no se ha alcanzado el prefijo máximo y garantiza que no se agoten los recursos locales, pero esto puede llevar a que se descarten bucles de reenvío para los prefijos. Tenga en cuenta que la opción de descartar rutas adicionales no puede coexistir con el botón de reconfiguración por software.
- Solo advertencia: registre una advertencia solo cuando se alcance el umbral, de modo que el operador pueda realizar acciones manuales para borrar la condición.

Para obtener más información, consulte la Guía de configuración de routing de la siguiente manera:

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-3/routing/configuration/guide/b-routing-cg-asr9000-73x/implementing-BGP.html#concept_5AF38064B1D044B7B5F439C10BCF9808

Prácticas recomendadas y recomendaciones

La siguiente lista proporciona una descripción general de las mejores prácticas y recomendaciones generales, que no se enumeran en un orden específico:

■ Auditoría de la red para el estado general del sistema. Comience con una auditoría de la configuración y pase secuencialmente de las configuraciones de la interfaz al routing y los servicios.
■ Disponer de una estrategia de supervisión. Aunque SNMP es una práctica estándar, considere la posibilidad de implementar técnicas más sólidas y descriptivas mediante la telemetría de transmisión. Consulte el siguiente informe técnico para obtener recomendaciones de prácticas recomendadas sobre la implementación de la telemetría en un router IOS XR: https://xrdocs.io/telemetry/

OSPF

A continuación se detallan las prácticas recomendadas y recomendaciones generales para OSPF:

■ Implemente el resumen de ruta para las rutas dentro del área para OSPF.
■ Configure el ID del router explícitamente dentro de OSPF como una de las direcciones de loopback habilitadas para OSPF.
■ Diseñe una red jerárquica para limitar los LSA dentro de un área para OSPF. Mantenga el número de ABR para un área dentro de un rango razonable (~3 a 4).
■ Implemente la configuración "max-lsa" OSPF para OSPF, o equivalente, para limitar los LSA en la base de datos para utilizar eficazmente la memoria del sistema.
■ Limite el número máximo de rutas que se pueden distribuir de BGP a OSPF. En IOS-XR, el límite predeterminado es 10K.
■ Utilice la política de rutas (RPL) para redistribuir las rutas en OSPF.
■ Resuma la ruta entre áreas y las rutas externas de tipo 5 donde corresponda.
■ Uso de autenticación cuando sea necesario.
■ Utilice siempre NSF y NSR.
■ Configure el filtrado de redistribución en el origen en lugar del destino.
■ Use una interfaz pasiva donde corresponda.
■ OSPF sólo debe transportar rutas de loopback y de interfaz de router; elimine cualquier otra redistribución de BGP a OSPF.
■ Considere la posibilidad de trasladar cada hub principal a su propia área (NSSA).
■ Utilice BFD para una detección rápida de fallas en comparación con los temporizadores de protocolo de ruteo agresivo.
■ No utilice el comando mtu-ignore tanto como sea posible.
■ Considere el uso de la sincronización IGP-LDP en un entorno MPLS para evitar el envío de tráfico en una trayectoria sin etiqueta.
■ Considere la posibilidad de escalar dentro de los límites de plataforma admitidos (número de prefijos, número de etiquetas, ECMP, número de áreas, etc.).
■ Evitar la redistribución mutua en múltiples puntos.
■ Configure la distancia administrativa de modo que cada prefijo nativo de cada protocolo o proceso se alcance a través del protocolo o proceso del dominio correspondiente.
■ Controle los prefijos (utilizando la combinación de distancia o lista de prefijos) para que el mismo prefijo no se anuncie de nuevo al dominio de origen.
■ Aunque el ID de proceso OSPF tiene importancia local para el router, se recomienda tener el mismo ID de proceso para todos los routers en el mismo dominio OSPF. Esto mejora la coherencia de la configuración y facilita las tareas de configuración automática.
■ Al configurar OSPF para entornos de hub y radio, diseñe las áreas OSPF con un número menor de routers.
■ Configure el ancho de banda de referencia de costo automático OSPF en todo el dominio OSPF al link de ancho de banda más alto de la red.
■ Desde una perspectiva de diseño, le recomendamos implementar el peering IGP con dominios bajo los mismos controles administrativos u operativos para ayudar a evitar una actualización IGP no planificada o no autorizada que se propague por la red. Esto debe permitir una mayor facilidad de mantenimiento y de resolución de problemas en caso de que se produzcan errores. En caso de que un dominio IGP grande sea una necesidad comercial, planifique el uso de BGP en esos casos para limitar el número de rutas en el dominio de red IGP.

■ Si necesita conectividad MPLS de extremo a extremo, continúe usando la jerarquía/segmentación y utilice opciones como RFC3107 BGP-LU o cálculo de ruta entre dominios a través de PCE, o seleccione la redistribución/fuga con la política como último recurso.
■ La función OSPF Shortest Path First Throttling se puede utilizar para configurar la programación SPF en intervalos de milisegundos y para retrasar potencialmente los cálculos SPF durante la inestabilidad de la red.
■ La función OSPF SPF Prefix Prioritization permite que un administrador converja prefijos importantes más rápido durante la instalación de la ruta.

IS-IS

Estas son las mejores prácticas y recomendaciones generales para IS-IS:

■ Si ejecuta una red plana de un solo nivel, piense en la escala. Configure todos los routers como L2 solamente. De forma predeterminada, el router es L1-L2, y la fuga de información de ruteo de L1 a L2 está habilitada de forma predeterminada. Esto podría llevar a que todos los routers fuguen todas las rutas L1 a L2, inflando la base de datos de estado de link.
■ Si ejecuta una red multinivel (de varias áreas), asegúrese de que la topología de capa 3 sigue la jerarquía de ISIS. No cree enlaces de puerta trasera entre áreas L1.
■ Si ejecuta una red multinivel (varias áreas), asegúrese de que los routers L1 y L2 estén conectados a través de las áreas L1 y L2. Esto no requiere múltiples conexiones físicas o virtuales entre ellos; ejecute el link entre los routers L1 y L2 como un circuito L1/L2.
■ Si ejecuta una red multinivel (de varias áreas), resuma lo que se puede resumir; por ejemplo, en el caso de MPLS, el bucle invertido de los routers PE debe propagarse entre áreas, pero las direcciones de enlace de infraestructura no lo hacen.
■ Cree y siga el plan de direccionamiento adecuado si es posible. que permite el resumen y ayuda a ampliar.
■ Establezca la duración de LSP en un máximo de 18 horas.
■ Evitar la redistribución por cualquier medio. La redistribución es compleja y debe gestionarse manualmente para evitar bucles de routing. Si es posible, utilice un diseño de varias áreas/niveles.
■ Si debe utilizar la redistribución, utilice el etiquetado de ruta durante la redistribución y el filtrado "distribute-list in" basado en etiquetas para administrarla. Resuma durante la redistribución si es posible.
■ Configure las interfaces como "punto a punto" siempre que sea posible. Esto mejora el rendimiento y la escalabilidad del protocolo.
■ No utilice ISIS en topología de malla alta. Los protocolos de estado de link se comportan de manera deficiente en entornos altamente mallados.
■ Configure una métrica predeterminada alta en el submodo de familia de direcciones de ISIS. Esto evita que los links recién agregados atraigan tráfico si se configuran inadvertidamente sin una métrica.
■ Configurar "cambios de adyacencia de registro" para ayudar con la resolución de problemas de conexión.
■ Use "metric-style wide" bajo el submodo ipv4 de la familia de direcciones de ISIS. Las métricas estrechas no son muy útiles y no soportan funciones como segmento-routing o flex-algo.

■ Si está utilizando SR-MPLS TI-LFA recuerde agregar "ipv4 unnumbered mpls traffic-eng Loopback0" a la configuración para permitir que ISIS asigne túneles TE cuando sea necesario.
■ Deje que las configuraciones "lsp-gen-interval" y "spf-interval" sean predeterminadas a menos que esté seguro de que se requiere una convergencia nativa más rápida. Con TI-LFA la convergencia nativa no es tan crítica, ya que el reroute rápido manejará cambios de topología únicos en 50 ms o menos.
■ Si modifica "lsp-gen-interval" o "spf-interval", no utilice un retardo inicial inferior a 50 ms.
■ En la mayoría de los casos, "set-overload-bit" es una mejor opción que "max-metric", ya que es un cambio atómico soportado por fast-reroute.
■ Usar autenticación criptográfica para Hellos (hello-password) y LSPs (lsp-password). Los llaveros proporcionan la mayor flexibilidad y pueden
acomodar rollovers de llave sin impacto.
■ Configure "nsf cisco" para la autenticación sin impacto de los reinicios del proceso ISIS y la instalación de SMU. A pesar del nombre, esto proporciona una mejor interoperabilidad con otros proveedores que "nsf ietf".
■ En una plataforma con RP duales, TAMBIÉN configure "nsr" para gestionar switchovers RP.
■ Utilice las plantillas "group" y "apply-group" para configurar secciones de configuración repetidas. Esto es menos propenso a errores y más fácil de cambiar si es necesario.
■ En una red multinivel, considere cuidadosamente si necesita utilizar "propagar" para filtrar prefijos desde el Nivel 2 al Nivel 1. Esto puede limitar la escalabilidad y, a menudo, la ruta predeterminada de nivel 1 proporcionada por el bit conectado es suficiente.
■ Si está utilizando varias instancias de ISIS en el mismo VRF, considere la posibilidad de configurar valores de "distancia" únicos para ellas. Esto hará que la instalación de la ruta en la RIB sea más determinística si cada una tiene una ruta al mismo prefijo.
■ Utilice BFD para la detección rápida de link caído. Con BFD proporcionando esta función, el intervalo hello de ISIS puede aumentarse de forma segura para mejorar la escalabilidad.

BGP

A continuación, se detallan las mejores prácticas y recomendaciones generales para BGP:

■ Utilice NSR y NSF / reinicio sin errores con temporizadores ajustados cuidadosamente en función de la escala esperada.
■ Configure BGP usando la interfaz de loopback 'siempre ACTIVA', no la interfaz física para el peering IBGP.
■ No redistribuya rutas BGP (de gran volumen) en IGP (de volumen comparativamente bajo) y viceversa sin RPL adecuado, restringiendo el número de rutas redistribuidas de BGP a IGP (OSPF/ISIS).
■ Realizar una redistribución de BGP a IGP sin una política (ACL) adecuada y bien probada puede causar agotamiento de los recursos (memoria) en el router.
■ Uso de rutas de resumen en BGP para disminuir el tamaño de la tabla de ruteo y el uso de memoria. Agregue rutas con summary-only donde tenga sentido
■ Utilice el filtrado de rutas para anunciar y recibir rutas de manera eficiente, especialmente en BGP.
■ Recomendamos el uso del reflector de ruta (RR) y la confederación para ampliar la red.
■ Algunas de las consideraciones de diseño de Route Reflector son:

■ La escala de rutas aumenta en función del número de clientes/no clientes.
■ En RR jerárquicos, utilice el mismo cluster-id en el mismo nivel (RR redundante) para la prevención de loops y la escalabilidad.
■ Controle la MTU dentro de la trayectoria BGP o utilice el protocolo PMTUD para ajustar el MSS BGP automáticamente.
■ Utilice BFD o ajuste los temporizadores BGP para una detección de fallas más rápida.
■ La escalabilidad de BGP se realiza en función de la configuración y el caso práctico, y no existe un tamaño que se ajuste a todos los requisitos. Debe tener una buena idea sobre:
■ escala de ruta
— escala de trayectoria (con reconfiguración suave, aumentará)
— escala de atributos
■ Si se configura el add-path, consume más memoria.
■ Comprensión cuidadosa de las políticas de vecino BGP:
— pass-all (especialmente en un router de frontera) puede causar estragos ya que la escala de memoria se disparará.
— Utilice construcciones de políticas que eviten coincidencias de expresiones regulares en RPL.
■ Con el NSR, el RP en espera utilizará un 30% más de memoria virtual que la activa. Tenga esto en cuenta si hay un RP en espera.
■ Preste atención a la agitación continua en un número significativo de rutas (baches en la versión). Esto puede mantener la memoria de generación de actualizaciones en una marca de agua alta.
■ Proteja a sus pares con el botón max-prefix.
■ Utilice los parámetros de retardo del disparador del siguiente salto según la escala y los objetivos de convergencia.
■ En el diseño de red, intente evitar nuevos atributos. Los atributos únicos conducen a un empaquetado ineficiente y resultan en más actualizaciones de BGP.
■ La configuración de múltiples trayectorias a través de la red puede conducir a loops de reenvío. Utilícelo con cuidado.
■ Use la política de tabla para evitar la instalación de la ruta en el nervio si RR no está en línea-RR (no next-hop-self)

Supervisión de la memoria del sistema para procesos de routing

Ningún dispositivo tiene recursos infinitos - si enviamos un número infinito de rutas a un dispositivo, el dispositivo debe elegir cómo falla. Los routers intentarán dar servicio a todas las rutas hasta que se agoten los límites de memoria, y esto puede hacer que todos los protocolos y procesos de ruteo fallen.

Cada proceso del router de núcleo tiene definido un "RLIMIT". El "RLIMIT" es la cantidad de memoria del sistema que cada proceso puede consumir.

Esta sección describe algunas técnicas estándar para monitorear y verificar la memoria del sistema utilizada por el proceso BGP.

Memoria de proceso

Muestra la cantidad de memoria consumida por un proceso.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory
```

```
Proceso dinámico (KB) de pila(KB) de datos(KB) de texto JID (KB)
------ ---------- ---------- ---------- ---------- ----------------------------
-
1150 896 368300 136 33462 lspv_server
380 316 1877872 136 32775 servidor_analizador
1084 2092 2425220 136 31703 bgp
1260 1056 1566272 160 31691 ipv4_rib
1262 1304 1161960 152 28962 ipv6_rib
1277 4276 1479984 136 21555 pim6
1301 80 227388 136 21372 servidor_esquema
1276 4272 1677244 136 20743 pim
250 124 692436 136 20647 invmgr_proxy
1294 4540 2072976 136 20133 l2vpn_mgr
211 212 692476 136 19408 sdr_invmgr
1257 4 679752 136 17454 statsd_manager_g
```

A cada proceso se le asigna una cantidad máxima de memoria que se le permite consumir. Esto se define como el límite.

```
RP/0/RP0/CPU0:NCS-5501#show proc memory detail
Proceso dinámico Dyn-Limit Shm-Tot Phy-Tot de la pila de datos de texto JID
================================================================================
============================
1150 896K 359M 136K 32M 1024M 18M 24M lspv_server
1084 2 M 2368 M 136 K 30 M 7447 M 43 M 69 M bgp
1260 1 M 1529 M 160 K 30 M 8192 M 38 M 52 M ipv4_rib
380 316K 1833M 136K 29M 2048M 25M 94M servidor_analizador
1262 1M 1134M 152K 28M 8192M 22M 31M ipv6_rib
1277 4M 1445M 136K 21M 1024M 18M 41M pim6
1301 80 000 222 M 136 000 20 M 300 M 5 M 33 M servidor_esquema
1276 4M 1637M 136K 20M 1024M 19M 41M pim
250 124 K 676 M 136 K 20 M 1024 M 9 M 31 M invmgr_proxy
1294 4M 2024M 136K 19M 1861M 48M 66M l2vpn_mgr
211 212K 676M 136K 18M 300M 9M 29M sdr_invmgr
1257 4000 663 MB 136 000 17 MB 2048 MB 20 MB 39 MB statsd_manager_g
288 4000 534 MB 136 000 16 M 2048 M 15 M 33 MB statsd_manager_l
...
```

Principales consumidores de memoria

```
RP/0/RP0/CPU0:NCS-5501#show memory-top-users
##########################################################################
 Principales consumidores de memoria en 0/0/CPU0 (en 2022/13/abr/15:54:12)
##########################################################################
    PID Proceso total(MB) Pila(MB) Compartido(MB)
   3469 fia_driver 826 492,82 321
   4091 fib_mgr 175 1094.43 155
   3456 spp 130 9,68 124
   4063 dpa_port_mapper 108 1.12 105
   3457 packet 104 1.36 101
   5097 l2fib_mgr 86 52.01 71
   4147 bfd_agent 78 6,66 66
   4958 eth_intf_ea 66 4,76 61
   4131 optics_driver 62 141.23 22
   4090 ipv6_nd 55 4,13 49
##########################################################################
 Principales consumidores de memoria en 0/RP0/CPU0 (a 20xx/MMM/HH:MM:SS)
##########################################################################
    PID Proceso total(MB) Pila(MB) Compartido(MB)
   3581 spp 119 9,62 114
   4352 dpa_port_mapper 106 2.75 102
   4494 fib_mgr 99 7,71 90
   3582 paquetes 96 1,48 94
   3684 parser_server 95 64,27 25
   8144 te_control 71 15,06 55
   8980 bgp 70 27,61 44
   7674 l2vpn_mgr 67 23.64 48
   8376 mibd_interface 65 35.28 28
   3608 gsp 65 15,75 48
```

Memoria total: usada y disponible

Los componentes del sistema tienen una cantidad fija de memoria disponible.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary location all
nodo: node0_0_CPU0
----------------------------------------------------------------
 Memoria física: 8192 millones en total (6172 millones disponibles)
```

```
 Memoria de la aplicación: 8192M (6172M disponibles)
 Imagen: 4M (bootam: 0M)
 Reservado: 0M, IOMem: 0M, flashfsys: 0M
 Ventana compartida total: 226 millones
nodo: node0_RP0_CPU0
----------------------------------------------------------------
 Memoria física: 18432M en total (15344M disponibles)
 Memoria de la aplicación: 18432M (15344M disponibles)
 Imagen: 4M (bootam: 0M)
 Reservado: 0M, IOMem: 0M, flashfsys: 0M
 Ventana compartida total: 181 millones
```

La ventana de memoria compartida proporciona información sobre las asignaciones de memoria compartida en el sistema.

```
RP/0/RP0/CPU0:NCS-5501#show memory summary detail location 0/RP0/CPU0
nodo: node0_RP0_CPU0
----------------------------------------------------------------
 Memoria física: 18432M en total (15344M disponibles)
 Memoria de la aplicación: 18432M (15344M disponibles)
 Imagen: 4M (bootam: 0M)
 Reservado: 0M, IOMem: 0M, flashfsys: 0M
 Ventana compartida soasync-app-1: 243,328K
 Shared window soasync-12: 3,328 K
 ...
 Shared window rewrite-db: 272.164K
 Ventana compartida l2fib_brg_shm: 139.758K
 im_rules de ventana compartida: 384 211 K
 grid_svr_shm de ventana compartida: 44,272 millones
 Ventana compartida spp: 86,387M
 im_db de ventana compartida: 1,306 millones
 Ventana compartida total: 180,969 millones
 Memoria asignada: 2,337 G
 Texto del programa: 127.993T
 Datos del programa: 64,479G
 Pila de programas: 2,034G
RAM del sistema: 18432M ( 19327352832)
```

```
Total utilizado: 3088 millones (3238002688)
 Usado Privado: 0M ( 0)
 Usado compartido: 3088M ( 3238002688)
```

Puede comprobar los procesos de los participantes con una ventana de memoria compartida.

```
RP/0/RP0/CPU0:NCS-5501#sh shmwin spp participate list
Datos para Window "spp":
----------------------------
Lista de participantes actuales:-
NOMBRE PID JID INDEX
spp 3581 113 0
packet 3582 345 1
ncd 4362 432 2
netio 4354 234  3
nsr_ping_reply 4371 291 4
aib 4423 296 5
ipv6_io 4497 430 6
ipv4_io 4484 438 7
fib_mgr 4494 293 8
...
snmpd 8171 1002 44
ospf 8417 1030 45
mpls_ldp 7678 1292 46
bgp 8980 1084 47
cdp 9295 337 48
RP/0/RP0/CPU0:NCS-5501#sh shmwin soasync-1 participate list
Datos para la ventana "soasync-1":
----------------------------
Lista de participantes actuales:-
NOMBRE PID JID INDEX
tcp 5584 168 0
bgp 8980 1084
```

Vigilancia y supervisión de recursos

La utilización de la memoria se monitorea a través de un sistema de vigilancia en cXR y con Resmon en eXR.

```
RP/0/RP0/CPU0:NCS-5501#show watchdog memory-state

---- node0_RP0_CPU0 ----

Información de memoria:

    Memoria física: 18432 MB

    Memoria libre: 15348 MB

    Estado de memoria: Normal

RP/0/RP0/CPU0:NCS-5501#

RP/0/RP0/CPU0:NCS-5501#show watchdog threshold memory defaults location
0/RP0/CPU0

---- node0_RP0_CPU0 ----

 Umbrales de memoria predeterminados:

 Menor: 1843 MB ß-10%

 Grave: 1474 MB ß-8%

 Crítico: 921,599 MB ß-5%

Información de memoria:

    Memoria física: 18432 MB

    Memoria libre: 15340 MB

    Estado de memoria: Normal

RP/0/RP0/CPU0:NCS-5501#

RP/0/RP0/CPU0:NCS-5501(config)#watchdog threshold memory minor ?

  <5-40> consumo de memoria en porcentaje
```

Si se superan los umbrales, se imprime una advertencia.

```
RP/0/RP0/CPU0:Feb 17 23:30:21.663 UTC: resmon[425]: %HA-HA_WD-4-MEMORY_ALARM:
Umbral de memoria cruzado: Menor con 1840.000 MB libres. Estado anterior:
Normal

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USERS_INFO: 5 consumidores principales de memoria del sistema (1884160
Kbytes libres):

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 0: Nombre del proceso: bgp[0], pid: 7861, Uso del montón:
12207392 kbytes.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 1: Nombre del proceso: ipv4_rib[0], pid: 4726, Uso del
montón: 708784 kbytes.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 2: Nombre del proceso: fib_mgr[0], pid: 3870, Uso del
montón: 584072 kbytes.
```

```
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 3: Nombre del proceso: netconf[0], pid: 9260, Uso del
montón: 553352 kbytes.

RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-
TOP_MEMORY_USER_INFO : 4: Nombre del proceso: netio[0], pid: 3655, Uso del
montón: 253556 kbytes.

LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172]: %HA-HA_WD-4-MEMORY_ALARM: Umbral
de memoria cruzado: Grave con 600.182MB libres. Estado anterior: Normal

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USERS_WARNING: 5 consumidores principales de memoria del sistema
(624654 Kbytes libres):

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 0: Nombre del proceso: fib_mgr[0], pid: 5375, uso del
montón 1014064 Kbytes.

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 1: Nombre del proceso: ipv4_mfwd_partner[0], pid: 5324,
uso del montón 185596 Kbytes.

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 2: Nombre del proceso: nfsvr[0], pid: 8357, uso del
montón 183692 Kbytes.

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 3: Nombre del proceso: fia_driver[0], pid: 3542, uso
del montón 177552 Kbytes.

LC/0/3/CPU0:8 de marzo 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-
TOP_MEMORY_USER_WARNING : 4: Nombre del proceso: npu_driver[0], pid: 3525, uso
del montón 177156 Kbytes.
```

Algunos procesos pueden tomar acciones específicas basadas en el estado de memoria de vigilancia. Por ejemplo, BGP hace lo siguiente:

- en el estado menor, BGP deja de traer nuevos peers
- en el estado severo, BGP gradualmente derriba algunos peers.
- en un estado crítico, el proceso BGP se apaga.

Los procesos se pueden configurar para que se registren para las notificaciones de estado de memoria.

Show watchdog or-aware-process

Los usuarios pueden desactivar el cierre automático de procesos debido al tiempo de espera de vigilancia.

watchdog restart memory-hog disable

¿Dónde puede encontrar más información?

- Repositorio de informes técnicos y blogs de Cisco IOS XR (xrdocs.io)
    - Core Fabric Design: https://xrdocs.io/design/blogs/latest-core-fabric-hld: este informe técnico trata sobre las tendencias recientes y la evolución de las redes troncales de núcleo.

■ Peering Fabric Design: https://xrdocs.io/design/blogs/latest-peering-fabric-hld: este informe técnico ofrece una completa descripción general de los retos y recomendaciones de prácticas recomendadas para el diseño de iguales, con un enfoque en la simplificación de la red.

■ Referencia de la Guía de Configuración: Implementación de BGP https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/710x/b-bgp-cg-ncs5500-710x/implementing-bgp.html

Mejoras de funciones

Aislamiento del Router de Límite del Sistema Autónomo y Control de Adyacencia para Desbordamientos LSA	Introducido en 7.10.1 en los routers de puerto fijo NCS 5500: routers de puerto fijo NCS 5700 En una red que emplea un router de límite del sistema autónomo (ASBR) y otros routers, ahora se le garantiza un flujo de tráfico ininterrumpido incluso si el ASBR genera LSA que exceden el límite configurado. Esto es posible ya que ahora puede aislar ASBR y también controlar la duración de la adyacencia en la fase EXCHANGE o LOADING. Al aislar el ASBR de sus vecinos inmediatos, la topología de red restante puede continuar funcionando sin interrupciones, lo que evita eficazmente cualquier impacto adverso en el flujo de tráfico. Este enfoque también simplifica el proceso de recuperación, ya que la intervención manual solo es necesaria para los vecinos inmediatos de los routers ASBR. Esta función introduce estos cambios: CLI: • max-external-lsa • exchange-timer Modelo de datos YANG: • Cisco-IOS-XR-ipv4-ospf-cfg.yang • Cisco-IOS-XR-ipv4-ospf-oper.yang • Cisco-IOS-XR-um-router-ospf-cfg.yang (consulte GitHub, YANG Data Models Navigator)
Restablecimiento Automático de una Sesión de Vecino BGP	Presentado en esta versión en: routers de puerto fijo NCS 5500; routers de puerto fijo NCS 5700; routers modulares NCS 5500 (tarjetas de línea NCS 5500; tarjetas de línea NCS 5700 [Modo: Compatibilidad; nativo]) Ahora puede configurar el router para restablecer automáticamente una sesión de vecino BGP que se haya inhabilitado porque se ha excedido el límite máximo de prefijos. La función introduce estos cambios: CLI • maximum-prefix-restart-time Modelo de datos YANG: • Nuevas XPath para openconfig-bgp-neighbor.yang(consulte GitHub, YANG Data Models Navigator)

Especificación de flujo BGP en interfaces virtuales de grupo de puentes	Presentado en la versión 7.10.1 en: Routers modulares NCS 5500 (tarjetas de línea NCS 5700 [Modo: nativo]) Ahora puede emplear BGP Flowspec de forma eficaz en la interfaz virtual de grupo de puentes (BVI) para conectarse a dominios de difusión que alojen dispositivos host, como en el caso de las redes empresariales. Esta compatibilidad significa que sus clientes pueden proteger sus redes de amenazas de red, como los ataques de denegación de servicio distribuida (DDoS) que entran a través de BVI.
Descartar mensaje de actualización de BGP entrante	Presentado en la versión 7.10.1 en: routers de puerto fijo NCS 5500; routers de puerto fijo NCS 5700; routers modulares NCS 5500 (tarjetas de línea NCS 5500; tarjetas de línea NCS 5700 [Modo: Compatibilidad; nativo]) Ahora puede evitar el restablecimiento de sesión cuando una sesión BGP encuentra errores mientras analiza el mensaje de actualización recibido. Esto es posible porque la función permite descartar el mensaje de actualización entrante como un mensaje de retirada. CLI: • actualización en tratamiento de errores de tratar como retirar Modelo de datos YANG: • Nuevos XPath para openconfig-bgp-neighbor.yang (consulte GitHub, YANG Data Models Navigator)
Exclusión de Asignación de Etiquetas para Rutas no Anunciadas	Presentado en la versión 7.10.1 en: routers de puerto fijo NCS 5500; routers de puerto fijo NCS 5700; routers modulares NCS 5500 (tarjetas de línea NCS 5500; tarjetas de línea NCS 5700 [Modo: Compatibilidad; nativo]) Hemos mejorado la gestión del espacio de etiquetas y la utilización de recursos de hardware al flexibilizar la asignación de etiquetas MPLS. Esta flexibilidad significa que ahora puede asignar estas etiquetas sólo a aquellas rutas que se anuncian a sus rutas pares, lo que garantiza una mejor gestión del espacio de etiquetas y una mejor utilización de los recursos de hardware. Antes de esta versión, la asignación de etiquetas se realizaba independientemente de si las rutas se anunciaban o no. Esto dio lugar a un uso ineficiente del espacio de etiquetas.
Protección de Vecinos EBGP Conectados Directamente a través del Identificador LPTS Basado en Interfaz	Presentado en la versión 7.10.1 en: Routers de puerto fijo NCS 5500 Hemos mejorado la seguridad de la red para los vecinos eBGP conectados directamente asegurándonos de que solo los paquetes que se originan en vecinos eBGP designados puedan atravesar a través de una sola interfaz, evitando así la suplantación de IP. Esto es posible gracias a que hemos agregado un identificador de interfaz para los servicios de transporte de paquetes locales (LPTS). LPTS filtra y controla los paquetes en función del tipo de caudal que configure.

	La función presenta lo siguiente: CLI: • bgp lpts-secure-binding Modelo de datos YANG: • Cisco-IOS-XR-um-router-bgp-cfg (consulte GitHub, YANG Data Models Navigator)
Reduzca las recursiones para el Peering eBGP en la Dirección Loopback en la Interfaz Virtual del Grupo de Bridge	Presentado en la versión 7.10.1 en: Routers modulares NCS 5500 (tarjetas de línea NCS 5700 [Modo: nativo]) Ahora puede lograr el peering eBGP en las interfaces Loopback en la Interfaz Virtual de Grupo de Puentes (BVI) y reducir el nivel de recursividad de tres a dos. Esta reducción en el nivel de recursividad, que se logra al eliminar la necesidad de utilizar el nombre BVI en la configuración de rutas estáticas, permite un reenvío de paquetes más rápido y una mejor utilización de los recursos de red.
BGP Policy Accounting	Introducido en la versión 7.9.1: el protocolo de gateway fronterizo (BGP) mide la contabilización de políticas y clasifica el tráfico IP que se recibe de diferentes peers. Puede identificar y dar cuenta de todo el tráfico por cliente y facturar según corresponda. La contabilización de políticas se habilita en base a una interfaz de entrada individual. Con la contabilización de políticas BGP, ahora puede contabilizar el tráfico según la ruta que atraviesa. Esta función ahora es compatible con routers que tienen tarjetas de línea basadas en Cisco NC57 con TCAM externo (eTCAM) y funcionan en modo nativo. Esta función introduce estos cambios: • CLI: La función introduce el comando hw-module fib bgppa stats-mode. • YANG Data Model: nuevas XPath para Cisco-IOS-XR-um-hw-module-profile-cfg.yang (consulte GitHub, YANG Data Models Navigator)
Detección de Peer Lento en un Grupo BGP	Introducido en la versión 7.9.1: los peers BGP procesan los mensajes de actualización de BGP entrantes a diferentes velocidades. Un peer lento es un peer que está procesando mensajes de actualización BGP entrantes muy lentamente durante un largo período de tiempo comparado con otros peers en el subgrupo de actualización. La gestión lenta de pares es importante cuando las rutas cambian constantemente durante un largo período de tiempo. Es importante limpiar la información obsoleta en la cola y enviar solo el estado más reciente. Es útil saber si hay un par lento, lo que indica que hay un problema de red, como una congestión de red sostenida o un receptor que no procesa las actualizaciones a tiempo, que el administrador de red puede resolver.

Limitación de los números LSA en una Base de Datos de Estado de Link OSPF	Introducido en la versión 7.9.1: los anuncios de estado de link (LSA) no generados automáticamente para un proceso OSPF (Open Shortest Path First) determinado están limitados a 500000. Este mecanismo de protección evita que los routers reciban muchos LSA, evitando fallos de CPU y escasez de memoria, y está habilitado de forma predeterminada a partir de esta versión. Si tiene más de 500000 LSAs en su red, configure el comando max-lsa con la escala LSA esperada antes de actualizar a esta versión o posterior. Esta función modifica los siguientes comandos: • show ospf para mostrar el número máximo de prefijos redistribuidos. • show ospf database-summary detail para mostrar el número de recuentos de LSA por router. • show ospf database-summary adv-routerrouter ID para mostrar la información del router y los LSA recibidos de un router determinado.
Limitación del Máximo de Prefijos LSA Tipo 3 Redistribuidos en OSPF	Introducido en la versión 7.9.1: De forma predeterminada, el máximo de prefijos LSA de tipo 3 redistribuidos para un proceso OSPF determinado está ahora limitado a 100000. Este mecanismo evita que OSPF redistribuya una gran cantidad de prefijos como LSA de tipo 3 y, por lo tanto, evita el uso elevado de la CPU y la escasez de memoria. Una vez que el número de prefijos redistribuidos se alcanza o excede el valor de umbral, se genera el mensaje de registro del sistema y no se redistribuyen más prefijos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).