Inhoud

VRIJWARING

Dit document verstrekt een samenvatting op hoog niveau van sommige gevestigde beste praktijkaanbevelingen voor OSPF/IS-IS en BGP-routing. Deze aanbevelingen vertegenwoordigen geen door Cisco gevalideerd ontwerp, en de

nodige zorg en aandacht zijn vereist voor implementatie in een specifieke besturingsomgeving. Zij moeten worden gelezen in samenhang met de configuratiehandleidingen en de technische documentatie voor de relevante producten, waarin meer in detail wordt beschreven hoe deze aanbevelingen voor beste praktijken kunnen worden uitgevoerd. Verwijzingen in dit document naar configuratiehandleidingen en technische documentatie voor specifieke producten zijn slechts bedoeld als voorbeelden. Raadpleeg de configuratiehandleidingen en de technische documentatie voor uw specifieke producten.

Inleiding

Dit document schetst een aantal gevestigde best practices en aanbevelingen voor het bouwen van vereenvoudigde, efficiënte en schaalbare netwerken die worden aangedreven door IOS XR-routingplatforms. Dit document concentreert zich op specifieke implementatietechnieken en opties voor functieondersteuning die in IOS XR beschikbaar zijn om te helpen OSPF/IS-IS en BGP-implementaties aan te passen.

OSPF-implementatie

Het OSPF-protocol dat in RFC 2328 is gedefinieerd, is een IGP die wordt gebruikt om routeringsinformatie binnen één autonoom systeem te distribueren. OSPF biedt verscheidene voordelen over andere protocollen, maar een juist ontwerp wordt vereist om tot een schaalbaar en fout-verdraagzaam netwerk te leiden.

Raadpleeg voor meer informatie over OSPF:

- TechNotes over OSPF: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc13
- Configuratiehandleiding voor 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
- Opdrachtreferentie: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/routing/command/reference/b-routing-cr-asr9000-75x/ospf-commands.html#wp2421918195

Belangrijkste concepten

- Hiërarchie: Een hiërarchisch netwerkmodel is een handig hulpmiddel op hoog niveau voor het ontwerpen van betrouwbare netwerkinfrastructuur en helpt complexe netwerkontwerpproblemen te doorbreken in kleinere en beter te beheren gebieden.
- Modulariteit: Door verschillende functies op een netwerk in modules te splitsen, is het netwerk veel gemakkelijker te ontwerpen. Cisco heeft verschillende modules geïdentificeerd, waaronder de bedrijfscampus, servicesblok, datacenter en Internet edge.
- Resiliency: Het netwerk is beschikbaar in zowel normale als abnormale omstandigheden. De normale omstandigheden omvatten verwachte verkeersstromen, patronen, en geplande gebeurtenissen zoals onderhoudsvensters. Abnormale omstandigheden omvatten hardware- of softwarestoringen, extreme

verkeersbelastingen, ongebruikelijke verkeerspatronen, DoS-gebeurtenissen (denial-of-service) en andere geplande of ongeplande gebeurtenissen.

- Flexibiliteit: de mogelijkheid om delen van het netwerk te wijzigen, nieuwe services toe te voegen of de capaciteit te vergroten zonder een aanzienlijke upgrade van de vorkheftruck te moeten ondergaan (bijv. vervanging van belangrijke hardwareapparaten).

Als algemene beste praktijk, zou de netwerkplaatsing van de "spanwijdte"van het netwerk moeten rekenschap geven om de routes binnen een specifieke grens en routes te bevatten die door de routers binnen een domein voor het door:sturen relevant zijn en worden vereist. Het effectieve gebruik van OSPF-gebieden helpt het aantal link-state-advertenties (LSA's) en ander overhead-verkeer dat over het netwerk wordt verzonden te verminderen. Een van de voordelen van het creëren van een hiërarchie is dat deze aanpak helpt ervoor te zorgen dat de grootte van de topologiedatabase die elke router zal moeten onderhouden, beheersbaar is en voldoet aan het geheugenprofiel van de router.

OSPF-domein en BGP-herdistributie

OSPF is ontworpen om slechts een paar duizend routes te dragen. Op een hoog niveau zijn OSPF-gebieden secties van een netwerk waar elke router weet van de routermogelijkheden van elke andere router in het gebied. Dit maakt snelle convergentie mogelijk wanneer een apparaat een probleem heeft, maar ten koste van een verminderde schaalbaarheid. Als zodanig wordt OSPF gebruikt in een Service Provider-kern om de basisconnectiviteit tussen alle kernapparaten te bieden, en worden alle kernapparaten geconfigureerd binnen hetzelfde OSPF-gebied. Dit is een standaardontwerp van een "underlay"-netwerk.

BGP is daarentegen ontworpen om aanzienlijk meer routes te transporteren dan de meeste IGP's, zoals OSPF. Risico's die verbonden zijn aan het herverdelen van BGP-routes in een IGP zoals OSPF. Als een serviceprovider vereist dat BGP-routes voor elk gebruik opnieuw worden gedistribueerd naar het IGP-domein, moet dit worden beheerd door de serviceprovider, met de juiste filtering bij de Autonomous System Boundary Routers (ASBR's) en met de overbelastingsbescherming die op de ontvangende router is geconfigureerd. Als BGP-herdistributie niet in een OSPF-apparaat wordt gefilterd, zal elk OSPF-apparaat in de ASBR beginnen met het ontvangen van routes die veel verder gaan dan de capaciteit om tegelijkertijd te verwerken. Met Cisco IOS XR-routers kunnen bijvoorbeeld alleen 10.000 BGP-routes standaard worden herverdeeld in OSPF. Wanneer BGP-routes in de IGP worden herverdeeld, is het mogelijk dat alle routers binnen het IGP-domein deze routes ontvangen, afhankelijk van het IGP-ontwerp. Overeenkomstig OSPF-protocol RFC moet elke externe route die naar OSPF wordt herverdeeld, worden gedistribueerd naar alle routers in het OSPF-gebied.

Herverdeling in IGP beheren

Als algemene beste praktijk dient herverdeling alleen op een zorgvuldige en geplande manier te gebeuren als er geen andere opties zijn om de routes te leren die een herverdelingsfunctie zal bieden.

In de regel dient u het volgende te doen:

- Vermijd herverdeling
- Vermijd het dragen van routes in een IGP-domein

- Implementeer BGP voor externe bereikbaarheid
- Gebruik IGP om alleen informatie over de volgende hop te dragen; bijvoorbeeld Loopback 0

Beperkingen van OSPF-routeherdistributie

De schaal van prefixes die van BGP naar OSPF worden herverdeeld wordt beheerd met de configuratie van de overbelastingsbescherming (max-lsa). Dit is de enige bescherming tegen het lekken van een groot aantal routes in het domein OSPF. In het geval van herdistributie in één enkel OSPF-gebied moet u meerdere lagen van bescherming tegen routeherdistributie implementeren.

Hier zijn enkele van de opties die beschikbaar zijn voor bescherming tegen routeherverdeling:

- Herdistributie-filtering met ACL
- Herdistributielimiet - wereldwijde instelling om te voorkomen dat meer dan een bepaald aantal routes opnieuw worden gedistribueerd. Als het filter wordt verwijderd, is de mondiale herdistributielimiet de tweede verdedigingslinie die de kernen zal beschermen.
- Max-LSA-configuraties op alle apparaten in het OSPF-gebied - als de in de bovenstaande opsommingen vermelde bescherming niet werkt, dwingt u de ontvangende routers om de inkomende buitensporige LSA's te weigeren.

OSPF Link-State Database Overload-bescherming

De functie OSPF Link-State Database Overload Protection biedt een mechanisme op OSPF-niveau om het aantal niet-zelf gegenereerde LSA’s voor een bepaald OSPF-proces te beperken. Als andere routers in het netwerk verkeerd zijn geconfigureerd, kunnen ze bijvoorbeeld een groot volume LSA's genereren om grote aantallen prefixes te herverdelen in OSPF. Dit beschermingsmechanisme helpt bij het voorkomen dat routers veel LSA's ontvangen en daardoor te maken krijgen met CPU- en geheugentekorten.

Functiegedrag

Dit is hoe de functie zich gedraagt:

- Wanneer deze eigenschap wordt toegelaten, houdt de router een telling van het aantal alle ontvangen (niet zelf-geproduceerde) LSAs bij.
- Wanneer de ingestelde drempelwaarde wordt bereikt, wordt een foutbericht vastgelegd.
- Wanneer het geconfigureerde maximale aantal ontvangen LSA’s wordt overschreden, accepteert de router geen nieuwe LSA’s.

```
max-lsa <max-lsa-count> <%-drempel-naar-log-waarschuwing> negeren-telling <negeren-telling-waarde>
negeren-tijd <negeren-tijd-in-minuten> reset-time <time-to-reset-ignore-count-in-minuten>
```

OSPF-staten

Als de ontvangen LSAs-telling na een minuut hoger is dan het geconfigureerde max-nummer, wordt met het OSPF-proces alle nabijheid uitgeschakeld en wordt de OSPF-database gewist. Deze staat wordt de negestaat genoemd. In deze staat, worden alle OSPF-pakketten die worden ontvangen op alle interfaces die tot de OSPF-instantie behoren, genegeerd en er worden geen OSPF-pakketten gegenereerd op de interfaces. Het OSPF-proces blijft in de negestaat voor de duur van de geconfigureerde negetijd (standaard is 5 minuten). Wanneer de negetijd verloopt, keert het OSPF-proces terug naar de normale werking en bouwt nabijheid op alle interfaces.

Als de LSA-telling het maximale aantal overschrijdt zodra de OSPF-instantie terugkeert van de staat die wordt genegeerd, kan de OSPF-instantie eindeloos oscilleren tussen de normale staat en de staat die wordt genegeerd. Om deze oneindige oscillatie te verhinderen, telt de instantie OSPF hoe vaak het in de negeerstaat is geweest. Deze teller wordt de negetelling genoemd. Als de negetelling (standaard negetelling is 5) de ingestelde waarde overschrijdt, blijft de OSPF-instantie permanent in de negeerstaat.

U moet de duidelijke ospf-opdracht uitgeven om de OSPF-instantie naar de normale status te retourneren. Het negeren-tellen wordt teruggesteld aan nul als het aantal LSA niet het maximumaantal opnieuw tijdens de tijd overschrijdt die door het terugstellen-tijd sleutelwoord wordt gevormd.

Als u het waarschuwing-enige sleutelwoord gebruikt, gaat de instantie OSPF nooit de negeerstaat in. Wanneer de LSA-telling het maximale aantal overschrijdt, wordt met het OSPF-proces een foutbericht vastgelegd en gaat de OSPF-instantie door in de normale werking van de status.

Er is geen standaardwaarde voor max-lsa. De limiet wordt alleen gecontroleerd als deze specifiek is ingesteld.

Zodra max-lsa is geconfigureerd, kunnen andere parameters standaardwaarden hebben:

- standaard %-drempel-naar-log-waarschuwing - 75%
- standaard neutraal-teller-waarde - 5
- standaard negeer-tijd-in-minuten - 5 minuten
- standaard tijd-to-reset-ignore-count - 10 minuten

Hier is een voorbeeld van de implementatie die toont hoe te om de instantie OSPF te vormen om 12000 niet-zelf-geproduceerde LSAs en 1000 niet-zelf-geproduceerde LSAs in VRF V1 goed te keuren.

```
RP/0/RSP0/CPU0:router# configureren
RP/0/RSP0/CPU0:router (configuratie)# 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
```

Het volgende voorbeeld toont hoe de huidige status van de OSPF-instantie te tonen.

```
RP/0/RSP0/CPU0:router# ospf 0 tonen
    Routing-proces "ospf 0" met ID 10.0.0.2
    NSR (non-stop routing) is uitgeschakeld
    Ondersteunt alleen enkele TOS(TOS0) routes
    Ondersteunt ondoorzichtige LSA
    Het is een router aan de gebiedskader
    Maximumaantal niet zelf gegenereerde LSA's 12000
       Huidig aantal niet zelf gegenereerde LSA 1
       Drempelwaarde voor waarschuwingsbericht 75%
       Negeren-tijd 5 minuten, reset-tijd 10 minuten
       Negeren-telling toegestaan 5, stroom negeren-telling 0
```

BGP-implementatie

BGP-adresfamilies maken van de BGP een "multiprotocol" routeringsprotocol. Het is sterk aanbevolen dat u begrijpt hoe de adresfamilies worden gebruikt om schaalbare topologieën te creëren die eenvoudig te implementeren en te beheren zijn. Door gebruik te maken van adresfamilies kan de operator verschillende topologieën maken voor verschillende technologieën, bijvoorbeeld EVPN, Multicast, enzovoort.

Zie de BGP-configuratiegids voor meer informatie over BGP:
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html

BGP en BFD

BGP-convergentie in een netwerk van serviceproviders is belangrijk om te voldoen aan de verwachtingen van klanten voor het bouwen van veerkrachtige en fouttolerante netwerken. Standaard heeft BGP een Keepalive-timer van 60 seconden en een Hold-timer van 180 seconden. Dit alles betekent dat BGP zeer traag zal zijn om samen te komen tenzij er hulp beschikbaar is van ondersteunende protocollen. BFD Bi-directional Forwarding (BFD) is een van deze protocollen die ontworpen is om de clientprotocollen sneller te laten convergeren. Met BFD kunnen protocollen binnen enkele seconden samenkomen.

Aanvullende informatie

- Deze handleiding bevat conceptuele en configuratiegegevens voor de BFD: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/76x/b-routing-cg-ncs5500-76x/implementing-bfd.html
- Dit whitepaper biedt een op serviceproviders gerichte weergave van snelle convergentie met BFD op de routers van Cisco NCS 5500 en Cisco Network Convergence System 500 Series: https://xrdocs.io/ncs5500/tutorials/bfd-architecture-on-ncs5500-and-ncs500/
- Raadpleeg https://xrdocs.io/ voor een dieper inzicht in het gebruik van BFD op Bundle-interfaces en het implementeren van Multipath en MultiHop BFD.

BGP-detectie van langzame peer

Een slow peer is een peer die niet kan bijhouden met de snelheid waarmee de router updateberichten genereert over een langere periode (in de volgorde van minuten) in een updategroep. Wanneer een langzame peer in een updategroep aanwezig is, stijgt het aantal geformatteerde updates hangende transmissie. Wanneer de cachelimiet is bereikt, heeft de groep geen quota meer om nieuwe berichten te formatteren. Om een nieuw bericht te formatteren, moeten sommige bestaande berichten worden verzonden met de slow peer en dan uit het cache worden verwijderd. De rest van de leden van de groep die sneller zijn dan de langzame peer en de transmissie van de geformatteerde berichten hebben voltooid zullen niets nieuws te verzenden hebben, alhoewel er onlangs gewijzigde BGP-netwerken kunnen zijn die wachten om geadverteerd of ingetrokken te worden. Dit effect van het blokkeren van de opmaak van alle peers in een groep wanneer een van de peers traag is in het verwerken van updates is het "slow peer" probleem.

Gebeurtenissen die een significante breuk in de BGP-tabel (zoals verbindingsresets) veroorzaken, kunnen een korte piek in de snelheid van de updategeneratie veroorzaken. Een peer die tijdelijk achterop raakt tijdens dergelijke evenementen, maar zich snel herstelt na de gebeurtenis, wordt niet beschouwd als een traag peer. Voor een peer om als langzaam te worden gemarkeerd, moet het niet in staat zijn om met het gemiddelde tarief van geproduceerde updates over een langere periode (in de orde van een paar minuten) bij te houden.

BGP Slow peer kan worden veroorzaakt door:

- Packet Loss of veel verkeer op de link naar de peer.
- Een BGP-peer kan zwaar worden geladen in termen van CPU en kan daardoor de TCP-verbinding niet op de vereiste snelheid onderhouden.
- In dit geval moeten de hardwaremogelijkheden van het platform en de aangeboden belasting worden gecontroleerd.
- Doorvoerproblemen met de BGP-verbinding
- Voor meer informatie over BGP Slow peer detectie, surf naar 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

Hier zijn sommige matigingen en beste praktijken voor het beheren van langzame edelen:

- End-to-end QoS, die bandbreedte reserveert voor BGP-verkeer van besturingsplane tijdens stremming.
- Gebruik van juiste en geschikte MSS / MTU-waarden met BGP PMTUD en/of TCP MSS instellingen.
- Gebruik de juiste hardware en minimaliseer het aantal routes ten opzichte van de hardware.

Slow-peer detectie is standaard ingeschakeld in Cisco IOS XR vanaf release 7.1.2. Langzame peers zijn peers die traag zijn bij het ontvangen en verwerken van de inkomende BGP-updates en de updates bevestigen aan de afzender. Als de slow peer deel uitmaakt van dezelfde updategroep als andere peers, kan dit het updateproces voor alle peers vertragen. In deze versie, wanneer IOS XR een langzame peer ontdekt, zal het tot een syslog leiden die de details over de specifieke peer heeft.

Snelle convergentie met BGP-prefix onafhankelijke convergentie

Voor BGP-prefixes wordt snelle convergentie bereikt met BGP Prefix Independent Convergence (PIC), waarin BGP een alternatieve beste pad en primaire beste pad berekent en beide paden in de routeringstabel als primaire en back-uppaden installeert.

Als de BGP next-hop remote onbereikbaar wordt, switch BGP onmiddellijk naar het alternatieve pad met BGP PIC in plaats van het pad na de fout opnieuw te berekenen.

Als de BGP next-hop externe PE nog springt, maar er is een padfout, behandelt IGP TI-LFA FRR snelle re-convergentie naar het alternatieve pad en werkt BGP de IGP next-hop voor de externe PE bij.

BGP PIC wordt geconfigureerd onder VRF-adresfamilie voor snelle convergentie van VPN-prefixes als een externe PE onbereikbaar wordt.

Zie voor meer informatie over BGP Prefix Independent Convergence:
https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/bgp-pic.html

BGP-beveiliging met BGP-stroomspecificatie

BGP Flowspec, in een notendop, is een eigenschap die u toestaat om IPv4/IPv6 verkeersstroomspecificaties (bron X, bestemming Y, protocol UDP, bronpoort A, enzovoort) en acties te ontvangen die op dat verkeer (zoals drop, politie, of omleiding) via BGP update moeten worden genomen.
Binnen de BGP update, worden de Flowspec aanpassingscriteria vertegenwoordigd door BGP NLRI, en BGP uitgebreide gemeenschappen vertegenwoordigen de acties.

Deze optie is gebaseerd op RFC 5575 en kan worden gebruikt om DDoS-aanvallen te helpen beperken. Wanneer een bepaalde host binnen een netwerk wordt aangevallen, kunnen we een Flowspec-update naar randrouters sturen zodat aanvalsverkeer kan worden gepoliceerd of weggelaten, of zelfs ergens anders omgeleid, misschien naar een apparaat dat het verkeer kan reinigen (filter het 'slechte' verkeer en doorsturen alleen het 'goede' verkeer naar de aangetaste host).

Zodra Flowspecs door een router worden ontvangen en in toepasselijke lijnkaarten geprogrammeerd, zullen om het even welke actieve L3 havens op die lijnkaarten beginnen toegangsverkeer volgens Flowspec regels te verwerken.

Zie voor meer informatie over het implementeren van BGP FlowSpec:

- Whitepaper met links naar het Cisco IOS XR YouTube-kanaal, zie https://xrdocs.io/ncs5500/tutorials/bgp-flowspec-on-ncs5500/
- BGP-configuratiehandleiding: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html#concept_ugv_bxq_h2b

Beste praktijken en aanbevelingen

De volgende lijst geeft een overzicht van de algemene best practices en aanbevelingen, in niet-specifieke volgorde:

- Netwerkaudit voor de algemene gezondheid van het systeem. Begin met een configuratiecontrole en ga achtereenvolgens van interfaceconfiguraties naar routing en services.
- Zorg voor een monitoringstrategie. Terwijl SNMP standaardpraktijk is, overweeg het opstellen van robuustere en beschrijvende technieken met behulp van streaming telemetrie. Raadpleeg het volgende witboek voor aanbevelingen over beste praktijken bij het implementeren van telemetrie op een IOS XR-router: https://xrdocs.io/telemetry/

OSPF

Hier zijn algemene best practices en aanbevelingen voor OSPF:

- Voer routesamenvatting voor intra-gebied routes voor OSPF uit.
- Configureer de router-ID expliciet binnen OSPF als een van de OSPF-enabled loopback-adressen.
- Ontwerp een hiërarchisch netwerk om de LSA's binnen een gebied voor OSPF te beperken. Houd het aantal ABR's voor een gebied binnen een redelijk bereik (~3 tot 4).
- Voer OSPF "max-lsa"-configuratie voor OSPF of gelijkwaardig uit om de LSA's in de database te beperken om het geheugen van het systeem effectief te gebruiken.
- Beperk het maximale aantal routes dat kan worden gedistribueerd van BGP naar OSPF. In IOS-XR is de standaardlimiet 10K.
- Gebruik routebeleid (RPL) om de routes te herverdelen in OSPF.
- Geef een overzicht van de interzoneroute en de externe type 5-routes, indien van toepassing.
- Gebruik van authenticatie indien nodig.
- Gebruik altijd NSF en NSR.
- Configureer herdistributie filtering aan de bron in plaats van aan de bestemming.
- Gebruik passieve interface waar van toepassing.
- OSPF moet alleen Loopback- en Router-Interface-routes dragen - verwijder elke andere BGP-to-OSPF-herdistributie.
- Overweeg om elke primaire hub naar zijn eigen gebied (NSSA) te verplaatsen.
- Gebruik BFD voor snelle storingsdetectie in vergelijking met de agressieve routeringsprotocoltimers.
- Gebruik de opdracht mtu-negeer niet zoveel mogelijk.
- Overweeg het gebruik van IGP-LDP-synchronisatie in een MPLS-omgeving om te voorkomen dat er verkeer op een niet-gelabeld pad wordt verzonden.
- Overweeg schaal binnen ondersteunde platformgrenzen (aantal prefixes, aantal labels, ECMP, aantal gebieden, enzovoort).
- Vermijd wederzijdse herverdeling op meerdere punten.
- Configureer de administratieve afstand zodat elk prefix van elk protocol of proces via het overeenkomstige protocol of proces van het domein wordt bereikt.
- Beheer de prefixes (met behulp van afstand of prefix-lijstcombinatie), zodat dezelfde prefix niet wordt geadverteerd naar het oorspronkelijke domein.
- Hoewel OSPF-proces-ID lokale betekenis heeft voor de router, wordt aanbevolen dezelfde proces-ID te hebben voor alle routers in hetzelfde OSPF-domein. Dit verbetert de configuratieconsistentie en vergemakkelijkt de automatische configuratietaken.
- Wanneer u OSPF configureert voor hub-and-spoke omgevingen, ontwerp u de OSPF-gebieden met een kleiner aantal routers.
- Configureer de bandbreedte van de OSPF-verwijzing voor automatische kosten in het OSPF-domein naar de hoogste bandbreedte in het netwerk.

- Vanuit een ontwerpperspectief raden we u aan om IGP-peer met domeinen onder dezelfde administratieve of operationele controles te implementeren om te voorkomen dat ongeplande of ondoordachte IGP-update zich over het netwerk verspreidt. Dit zou voor beter nut en gemak van het oplossen van problemen moeten toestaan ingeval de fouten voorkomen. Als een groot IGP-domein een zakelijke noodzaak is, plant dan het gebruik van BGP in die gevallen om het aantal routes in het IGP-netwerkdomein te beperken.
- Als u end-to-end MPLS-connectiviteit nodig hebt, kunt u de hiërarchie/segmentering blijven gebruiken en opties blijven gebruiken zoals RFC3107 BGP-LU of berekeningen van paden tussen domeinen via PCE, of herdistributie/lekken selecteren met beleid als laatste redmiddel.
- OSPF Shortest Path First Throttling feature kan worden gebruikt om SPF-planning te configureren in milliseconde intervallen en om de SPF-berekeningen mogelijk uit te stellen tijdens netwerkinstabiliteit.
- OSPF SPF Prefix Priorisation-functie stelt een beheerder in staat om belangrijke prefixes sneller te converteren tijdens routeinstallatie.

ISIS

Hier zijn algemene best practices en aanbevelingen voor IS-IS:

- Als je een vlak netwerk met één niveau gebruikt, denk dan aan de schaal. Alle routers alleen als L2 configureren. Standaard is de router L1-L2, en lekken van routerinformatie van L1 naar L2 is standaard ingeschakeld. Dit zou tot alle routers kunnen leiden die alle L1 routes naar L2 lekken, die het verbinding-staat gegevensbestand opblazen.
- Als u een netwerk op meerdere niveaus (meerdere gebieden) gebruikt, zorg er dan voor dat Layer 3-topologie de ISIS-hiërarchie volgt. Maak geen backdoor-koppelingen tussen L1-gebieden.
- Als u een netwerk op meerdere niveaus (meerdere gebieden) gebruikt, zorg er dan voor dat de L1- en L2-routers via zowel L1- als L2-gebieden zijn verbonden. Dit vereist geen meervoudige fysieke of virtuele verbindingen tussen hen; stel het verband tussen L1 en L2 routers als L1/L2 kring in werking.
- Als u een netwerk op meerdere niveaus (meerdere gebieden) gebruikt, vat u samen wat u kunt samenvatten - bijvoorbeeld in het geval van MPLS moet de loopback van PE-routers tussen gebieden worden gepropageerd, maar de infrastructurele koppelingsadressen niet.
- Maak en volg het juiste adresseringsplan als dat mogelijk is. Dat maakt samenvatting mogelijk en helpt schaalbaar te zijn.
- Stel de LSP-levensduur in op maximaal 18 uur.
- Vermijd herverdeling op welke manier dan ook. Herdistributie is complex en moet handmatig worden beheerd om routing loops te voorkomen. Gebruik, indien mogelijk, een ontwerp met meerdere gebieden/niveaus.
- Als u herdistributie moet gebruiken, gebruik route tagging tijdens herdistributie en "distribute-list in" filtering gebaseerd op tags om het te beheren. Vat dit zo mogelijk samen tijdens de herverdeling.
- Configureer interfaces als "point-to-point" indien mogelijk. Dit verbetert de prestaties en schaalbaarheid van het protocol.
- Gebruik geen ISIS in een topologie met grote mazen. De verbinding-staat protocollen gedragen zich slecht in hoogst vermaasde milieu's.

- Configureer een hoge standaardmetriek in de submodus van de ISIS-adresfamilie. Dit voorkomt dat nieuwe links verkeer aantrekken als ze per ongeluk zonder metriek worden geconfigureerd.
- Configureer "wijzigingen in lognabijheid" om te helpen bij het oplossen van verbindingsproblemen.
- Gebruik "metric-style wide" onder de submodus van de ISIS-adresfamilie ipv4. Smalle metriek zijn niet erg nuttig en ondersteunen geen functies zoals segmentrouting of flex-algo.
- Als u SR-MPLS TI-LFA gebruikt, moet u "ipv4 unnumed mpls traffic-eng Loopback0" aan de configuratie toevoegen, zodat IS indien nodig TE-tunnels kan toewijzen.
- Laat de "lsp-gen-interval" en "spf-interval" configuraties standaard, tenzij u zeker weet dat snellere native convergentie vereist is. Met Ti-LFA native convergentie is niet zo cruciaal, omdat snel omleiden zal omgaan met enkele topologiewijzigingen in 50 ms of minder.
- Als u "lsp-gen-interval" of "spf-interval" wijzigt, gebruik dan geen initiële vertraging korter dan 50 ms.
- In de meeste gevallen is "set-overload-bit" een betere keuze dan "max-metric" omdat het een atomaire verandering is die wordt ondersteund door fast-reroute.
- Gebruik cryptografische verificatie voor Hellos (hello-password) en LSP's (lsp-password). Keychains bieden de meeste flexibiliteit en kunnen
  geschikt voor hitless key rollovers.
- Configureer "nsf cisco" voor hitless authenticatie van ISIS-procesherstart en installatie via SMU. Ondanks de naam zorgt dit voor een betere interoperabiliteit met andere leveranciers dan "nsf ietf".
- Op een platform met dubbele RP's, configureer OOK "nsr" om RP-switchovers aan te kunnen.
- Gebruik "group" en "application-group" sjablonen om herhaalde configuratiesecties te configureren. Dit is minder foutgevoelig en gemakkelijker te veranderen indien nodig.
- In een netwerk met meerdere niveaus, overweeg zorgvuldig of u "propagate"moet gebruiken om prefixes van Niveau 2 aan Niveau 1 te lekken. Dit kan schaalbaarheid beperken en vaak is de standaard level-1 route die door het Bijgevoegde bit wordt geboden voldoende.
- Als u meerdere ISIS-instanties in dezelfde VRF gebruikt, kunt u overwegen unieke "afstand"-waarden voor deze instanties te configureren. Dit maakt routeinstallatie in de RIB meer deterministisch als elk een route naar hetzelfde prefix heeft.
- Gebruik BFD voor snelle link-down detectie. Omdat de BFD deze functie biedt, kan het ISIS-hello-interval veilig worden verlengd om de schaalbaarheid te verbeteren.

BGP

Hier zijn algemene best practices en aanbevelingen voor BGP:

- Gebruik NSR en NSF / graceful herstart met zorgvuldig afgestemde timers afhankelijk van de verwachte schaal.
- Configureer BGP met de 'always UP' loopback-interface en niet met de fysieke interface voor IBGP-peer.
- Verdeel BGP-routes (groot volume) niet opnieuw in IGP (relatief laag volume) en vice versa zonder juiste RPL, waardoor het aantal geherdistribueerde routes van BGP naar een IGP (OSPF/ISIS) wordt beperkt.

- Het doen van BGP aan IGP herdistributie zonder een juiste, goed-geteste beleid (ACL) kan middel (geheugen) uitputting op de router veroorzaken.
- Gebruik van summiere routes in BGP om de grootte van de routeringstabel en het gebruik van geheugen te verminderen. Aggregaat routes met samenvatting-slechts waar het steek houdt
- Gebruik routefiltering voor efficiënte reclame en ontvangst van routes, met name in BGP.
- We raden het gebruik van Route-Reflector (RR) en confederatie aan om het netwerk op te schalen.
- Enkele overwegingen met betrekking tot het routeweerkaatsingsontwerp zijn:
- De schaal van het pad wordt verhoogd op basis van het aantal clients/niet-clients.
- In hiërarchische RRs, gebruik zelfde cluster-id op het zelfde niveau (overtollige RR) voor lijnpreventie en schaal.
- Besturing MTU binnen het BGP-pad of gebruik het PMTUD-protocol om BGP MSS automatisch aan te passen.
- Gebruik BFD of tune BGP-timers voor snellere foutdetectie.
- BGP-schaal is per configuratie en gebruikscase, en geen enkele grootte past allemaal. Je moet een goed idee hebben over:
- routesnelheid
  - pad schaal (met zachte herconfiguratie, het zal toenemen)
  - kenmerkschaal
- Als het add-path is geconfigureerd, neemt het meer geheugen in beslag.
- Een zorgvuldig begrip van het BGP-buurbeleid:
  - pass-all (vooral bij een grensrouter) kan verwoesting veroorzaken als de geheugenschaal omhoog schiet.
  - Gebruik beleidsconstructies die reguliere expressieovereenkomsten in RPL voorkomen.
- Met NSR zal standby RP ongeveer 30% meer virtueel geheugen gebruiken dan actief. Houd hier rekening mee als er een stand-by is.
- Let op continue karnvorming op een aanzienlijk aantal routes (versiebobbels). Hierdoor kan het geheugen van de updategeneratie hoog watermerk houden.
- Bescherm peers met de max-prefixknop.
- Gebruik next-hop-trigger vertragingsparameters volgens schaal- en convergentiedoelstellingen.
- In het netwerkontwerp, probeer om nieuwe eigenschappen te vermijden. Unieke kenmerken leiden tot inefficiënte verpakking en resulteren in meer BGP-updates.
- Het configureren van multipath over het netwerk kan leiden tot het doorsturen van loops. Gebruik het voorzichtig.
- Gebruik het beleid van de tabel om te vermijden route te installeren om te ribbelen als RR niet inline-RR is (geen next-hop-self)

Monitorsysteemgeheugen voor routingprocessen

Geen apparaat heeft oneindig veel middelen - als we een oneindig aantal routes naar een apparaat verzenden, moet het apparaat kiezen hoe het faalt. De routers zullen proberen om alle routes te onderhouden tot de geheugengrenzen worden uitgeput, en dit kan alle routeringsprotocollen en processen veroorzaken om te mislukken.

Elk proces in de kernrouter heeft een "RLIMIET" gedefinieerd. De "RLIMIET" is de hoeveelheid systeemgeheugen die elk proces mag verbruiken.

In dit gedeelte worden enkele standaardtechnieken beschreven om het systeemgeheugen te controleren dat door het BGP-proces wordt gebruikt.

Procesgeheugen

Toont de hoeveelheid geheugen die door een proces wordt verbruikt.

```
RP/0/RP0/CPU0:NCS-5501#show-proc geheugen
JID Text(KB) Data(KB) Stack(KB) Dynamisch(KB) Proces
------ ---------- ---------- ---------- ----------- ------------------------------
1150/896 368300 136 33462 lspv_server
380 316 1877872 136 32775 parser_server
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 schema_server
1276 4272 1677244 136 20743
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 status_manager_g
```

Elk proces krijgt een maximale hoeveelheid geheugen toegewezen die het mag gebruiken. Dit wordt gedefinieerd als de limiet.

```
RP/0/RP0/CPU0:NCS-5501#show-geheugen
JID Text Stack Dynamic Dyn-Limit Shm-Tot PHY-Tot Proces
================================================================================================
=======
1150 896K 359M 136K 32M 1024M 18M 24M    LSPV_server
1084 2M 2368M 136K 30M 7447M 43M 69M  bgp
1260 1M 1529M 160K 30M 8192M 38M 52M  IPv4_rib
380 316K 1833M 136K 29M 2048M 25M 94M    parser_server
1262 1M 1134M 152K 28M 8192M 22M 31M  IPv6_rib
1277 4M 1445M 136K 21M 1024M 18M 41M  PIM6
1301 80K 222M 136K 20M 300M 5M 33M    schema_server
1276 4M 1637M 136K 20M 1024M 19M 41M  pooien
250 124K 676M 136K 20M 1024M 9M 31M   invmgr_proxy
1294 4M 2024M 136K 19M 1861M 48M 66M  l2v_mgr
211 212K 676M 136K 18M 300M 9M 29M    sdr_invmgr
1257 4K 663M 136K 17M 2048M 20M 39M   statsd_manager_g
288 4K 534M 136K 16M 2048M 15M 33M    statsd_manager_l
...
```

Belangrijkste geheugengebruikers

```
RP/0/RP0/CPU0:NCS-5501#show geheugen-top-consumenten
###########################################################################
 Belangrijkste geheugenconsumenten op 0/0/CPU0 (bij 2022/apr/13/15:54:12)
###########################################################################
    Totale PID-proces (MB) Hoop (MB) gedeeld (MB)
   3469 fia_driver 826 492.82 321
   4091 fib_mgr 175 1094,43 155
   3456 spp.
   4063 dpa_port_mapper 108 1.12 105
   3457 pakket 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 optische driver 62 141.23 22
   4090 ipv6_nd 55 4,13 49
###########################################################################
 Belangrijkste geheugenconsumenten op 0/RP0/CPU0 (bij 2022/apr/13/15:54:12)
###########################################################################
    Totale PID-proces (MB) Hoop (MB) gedeeld (MB)
   3581 spp.
   4352 dpa_port_mapper 106 2,75 102
   4494 fib_mgr 99 7,71 90
   3582 pakket 96 1,48 94
   3684 parser_server 95 64.27 25
   814 te_control 71 15.06 55
   890 bgp 70 27,61 44
   7674 l2vpn_mgr 67 23,64 48
   8376 mibd_interface 65 35.28 28
   3608 sap 65 15,75 48
```

Totaal geheugen - gebruikt en beschikbaar

Systeemcomponenten hebben een vaste hoeveelheid geheugen beschikbaar.

```
RP/0/RP0/CPU0:NCS-5501#show geheugen samenvatting locatie alles
knooppunt: knooppunt0_0_CPU0
------------------------------------------------------------------
 Fysiek geheugen: 8192M totaal (6172M beschikbaar)
 Toepassingsgeheugen: 8192M (6172M beschikbaar)
 Afbeelding: 4M (bootram: 0M)
 Gereserveerd: 0M, IOMem: 0M, flashfsys: 0M
 Totaal gedeeld venster: 226M
knooppunt: knooppunt0_RP0_CPU0
------------------------------------------------------------------
 Fysiek geheugen: 18432M totaal (15344M beschikbaar)
 Toepassingsgeheugen: 18432M (15344M beschikbaar)
 Afbeelding: 4M (bootram: 0M)
 Gereserveerd: 0M, IOMem: 0M, flashfsys: 0M
 Totaal gedeeld venster: 181M
```

Het venster voor gedeeld geheugen biedt informatie over de gedeelde geheugentoewijzingen op het systeem.

```
RP/0/RP0/CPU0:NCS-5501#show geheugen samenvatting detaillocatie 0/RP0/CPU0
knooppunt: knooppunt0_RP0_CPU0
------------------------------------------------------------------
 Fysiek geheugen: 18432M totaal (15344M beschikbaar)
 Toepassingsgeheugen: 18432M (15344M beschikbaar)
 Afbeelding: 4M (bootram: 0M)
 Gereserveerd: 0M, IOMem: 0M, flashfsys: 0M
 Gedeeld venster soasync-app-1: 243.328K
 Gedeeld venster soasync-12: 3.328K
 ...
 Gedeeld venster herschrijven-db: 272.164K
 Gedeeld venster l2fib_brg_shm: 139.758K
 Gedeeld venster im_rules: 384.211K
 Gedeeld venster grid_svr_shm: 44.272M
 Gedeeld venster spp: 86.387M
 Gedeeld venster im_db: 1.306M
 Totaal gedeeld venster: 180.969M
 Toegewezen geheugen: 2,337G
 Programma Tekst: 127.993T
 Programmagegevens: 64.479G
 Programmastack: 2.034G
Systeem RAM: 18432M ( 19327352832)
Totaal gebruikt: 3088M ( 3238002688)
 Tweedehands: 0M ( 0)
 Gebruikt gedeeld: 3088M ( 3238002688)
```

U kunt de deelnemersprocessen met een gedeeld geheugenvenster controleren.

```
RP/0/RP0/CPU0:NCS-5501#sh shmwin spp deelnemers lijst
Gegevens voor Window "spp":
----------------------------
Lijst van huidige deelnemers:-
NAAM PID JID-INDEX
3581 113 0
pakket 3582-345-1
NCD 4362 432 2
Noot 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
...
SNMP 8171 1002 44
8417.1030,45 ospf
MPLS_ldp 7678 1292 46
8980 1084,47 GBP
CDP 9295 337 48
RP/0/RP0/CPU0:BRU-SPCORE-PE6#sh shmwin soasync-1 deelnemerslijst
Gegevens voor venster "soasync-1":
----------------------------
Lijst van huidige deelnemers:-
NAAM PID JID-INDEX
TCP 5584 168 0
8980 1084 BGP
```

Resourcemonitoring en -bewaking

Geheugengebruik wordt bewaakt door een systeem waakhond in cXR en met Resmon in eXR.

```
RP/0/RP0/CPU0:NCS-5501#show-waakhond-geheugenstatus
---- knooppunt0_RP0_CPU0 ----
Geheugeninformatie:
    Fysiek geheugen: 18432,0 MB
    Gratis geheugen: 15348,0 MB
    Geheugenstaat : Normaal
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501#show watchdog drempel geheugen standaardlocatie 0/RP0/CPU0
---- knooppunt0_RP0_CPU0 ----
 Standaardgeheugendrempels:
 Klein: 1843 MB ß—10%
 Ernstig: 1474 MB ß-8%
 Kritisch: 921.599 MB ß-5%
Geheugeninformatie:
    Fysiek geheugen: 18432,0 MB
    Gratis geheugen: 15340,0 MB
    Geheugenstaat : Normaal
RP/0/RP0/CPU0:NCS-5501#
RP/0/RP0/CPU0:NCS-5501(config)#watchdog drempelgeheugen?
  <5-40> geheugenverbruik in percentage
```

Er wordt een waarschuwing afgedrukt als de drempelwaarden worden overschreden.

```
RP/0/RP0/CPU0:Feb 17 23:30:21.663 UTC: resmon[425]: %HA-HA_WD-4-MEMORY_ALARM: Geheugendrempel
overschreden: Klein met 1840.000MB gratis. Vorige staat: Normaal
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_GEBRUIKERS_INFO: Top 5
consumenten van systeemgeheugen (1884160 Kbytes vrij):
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 0: Procesnaam:
bgp[0], pid: 7861, Heap gebruik: 12207392 kbytes.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 1: Procesnaam:
ipv4_rib[0], pid: 4726, Heap gebruik: 708784 kbytes.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 2: Procesnaam:
fib_mgr[0], pid: 3870, Heap gebruik: 584072 kbytes.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 3: Procesnaam:
netconf[0], pid: 9260, Heap gebruik: 553352 kbytes.
RP/0/RP0/CPU0:Feb 17 23:30:21.664 UTC: resmon[425]: %HA-HA_WD-6-TOP_MEMORY_USER_INFO : 4: Procesnaam:
netio[0], pid: 3655, Heap gebruik: 253556 kbytes.
LC/0/3/CPU0:Mar 8 05:48:58.414 PST: resmon[172]: %HA-HA_WD-4-MEMORY_ALARM: Geheugendrempel
overschreden: Ernstig met 600.182MB vrij. Vorige staat: Normaal
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: Top 5
consumenten van systeemgeheugen (624654 Kbytes vrij):
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: 0: Procesnaam:
fib_mgr[0], pid: 5375, Heap gebruik 1014064 Kbytes.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: 1: Procesnaam:
ipv4_mfwd_partner[0], pid: 5324, Heap gebruik 185596 Kbytes.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: 2: Procesnaam:
nfsvr[0], pid: 8357, Heap gebruik 183692 Kbytes.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: 3: Procesnaam:
fia_driver[0], pid: 3542, Heap gebruik 177552 Kbytes.
LC/0/3/CPU0:Mar 8 05:48:58.435 PST: resmon[172]: %HA-HA_WD-4-TOP_MEMORY_USER_WARNING: 4: Procesnaam:
npu_driver[0], pid: 3525, Heap gebruik 177156 Kbytes.
```

Sommige processen kunnen specifieke acties ondernemen op basis van de status van het horlogegeheugen. BGP doet bijvoorbeeld het volgende:

- in de minder belangrijke staat, houdt BGP op nieuwe peers op te voeden
- in de ernstige staat brengt BGP geleidelijk een aantal peers terug.
- in een kritieke toestand wordt het BGP-proces uitgeschakeld.

Processen kunnen geconfigureerd worden om te registreren voor meldingen van geheugenstatus.

```
Toon waakhond of-bewust-proces
```

Gebruikers kunnen automatische processtopzetting uitschakelen vanwege de wachttijd van de waakhond.

```
watchdog herstart geheugen-hog uitschakelen
```

Waar vindt u meer informatie?

- Cisco IOS XR-weblogs en -opslagplaats voor whitepapers (xrdocs.io)
  - Core Fabric Design: https://xrdocs.io/design/blogs/latest-core-fabric-hld: dit artikel gaat over de recente trends en evolutie in core backbone netwerken.
  - Peering Fabric Design: https://xrdocs.io/design/blogs/latest-peering-fabric-hld : Dit whitepaper biedt een uitgebreid overzicht van de uitdagingen en aanbevelingen voor best practices voor peering design met de nadruk op netwerkvereenvoudiging.
- Configuratiehandleiding: Deze handleiding bevat informatie over BGP: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/76x/b-bgp-cg-ncs5500-76x/implementing-bgp.html
- Command Reference Guide: Deze handleiding beschrijft de opdrachten die worden gebruikt om BGP te configureren en te bewaken op Cisco NCS 5500 Series routers met behulp van Cisco IOS XR-software: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/bgp/b-ncs5500-bgp-cli-reference.html

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.