ICMP-omleidingsberichten begrijpen

Inhoud

Inleiding

Dit document beschrijft de functionaliteit voor ICMP-pakketomleiding (Internet Control Message Protocol).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Nexus 7000 platform architectuur
- Cisco NX-OS-softwareconfiguratie
- Internet Control Message Protocol, zoals gedocumenteerd in Verzoek om Opmerkingen (RFC) 792

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 7000 switch
- Cisco NX-OS-software

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document bespreekt de functionaliteit voor pakketomleiding die wordt geboden door Internet Control Message Protocol (ICMP). Het document legt uit welke aanwezigheid van ICMP-omleidingsberichten in het netwerk gewoonlijk aangeeft en wat kan worden gedaan om negatieve neveneffecten te minimaliseren die zijn gekoppeld aan netwerkomstandigheden die het genereren van ICMP-omleidingsberichten veroorzaken.

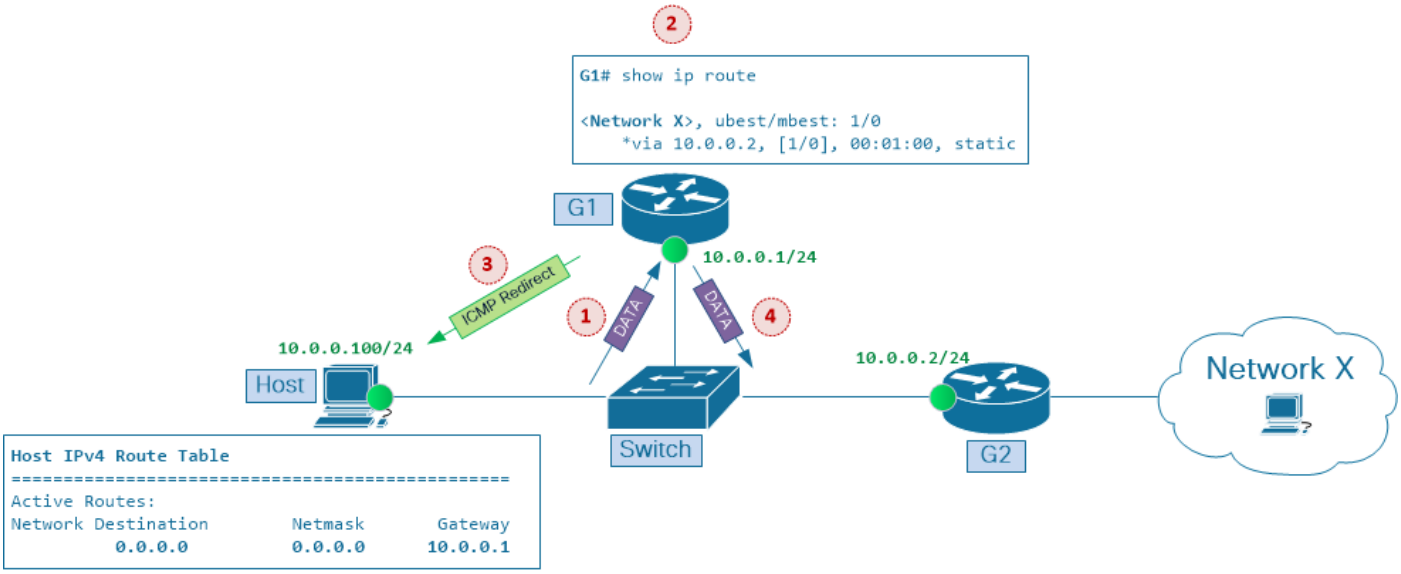
ICMP-omleidingsberichten

De functionaliteit van ICMP-omleiding wordt met dit voorbeeld uitgelegd in RFC 792 Internet Control Message Protocol:

> De gateway stuurt een omleidingsbericht naar een host in deze situatie.
>
> Een gateway, G1, ontvangt een datagram van Internet van een gastheer op een netwerk waaraan de gateway in bijlage is. De gateway, G1, controleert zijn routeringstabel en verkrijgt het adres van de volgende gateway, G2, op de route aan het datagram Internet bestemmingsnetwerk, X
>
> Als G2 en de host die wordt geïdentificeerd door het internetbronadres van het datagram zich op hetzelfde netwerk bevinden, wordt er een omleidingsbericht naar de host verzonden. Het omleiden bericht adviseert de host om zijn verkeer voor netwerk X rechtstreeks naar gateway G2 te verzenden aangezien dit een kortere weg naar de bestemming is.
>
> De gateway verstuurt de oorspronkelijke datagramgegevens naar zijn internetbestemming.

Dit scenario wordt getoond in afbeelding 1. Host en twee routers, G1 en G2, zijn verbonden met een gedeeld Ethernet-segment en hebben IP-adressen in hetzelfde netwerk (10.0.0.0/24)

Afbeelding 1 ICMP-omleidingen in multi-point Ethernet-netwerken



ICMP-omleidingen in multi-point Ethernet-netwerken

De host heeft IP-adres 10.0.0.100. De Host Routing Table heeft een standaard routeingang die naar het IP-adres 10.0.0.1 van de router G1 verwijst als de standaardgateway. De router G1 gebruikt router G2 IP adres 10.0.0.2 als zijn volgende hop wanneer het door:sturen van verkeer aan bestemmingsnetwerk X.

Dit is wat er gebeurt wanneer de host een pakket naar een doelnetwerk verstuurt X:

1. Gateway G1 met IP-adres 10.0.0.1 ontvangt gegevenspakket van host 10.0.0.10 op een netwerk waaraan het is gekoppeld.

2. De gateway, G1, controleert zijn routeringstabel en verkrijgt het IP-adres 10.0.0.2 van de volgende gateway, G2, op de route naar het gegevenspakketbestemmingsnetwerk, X.

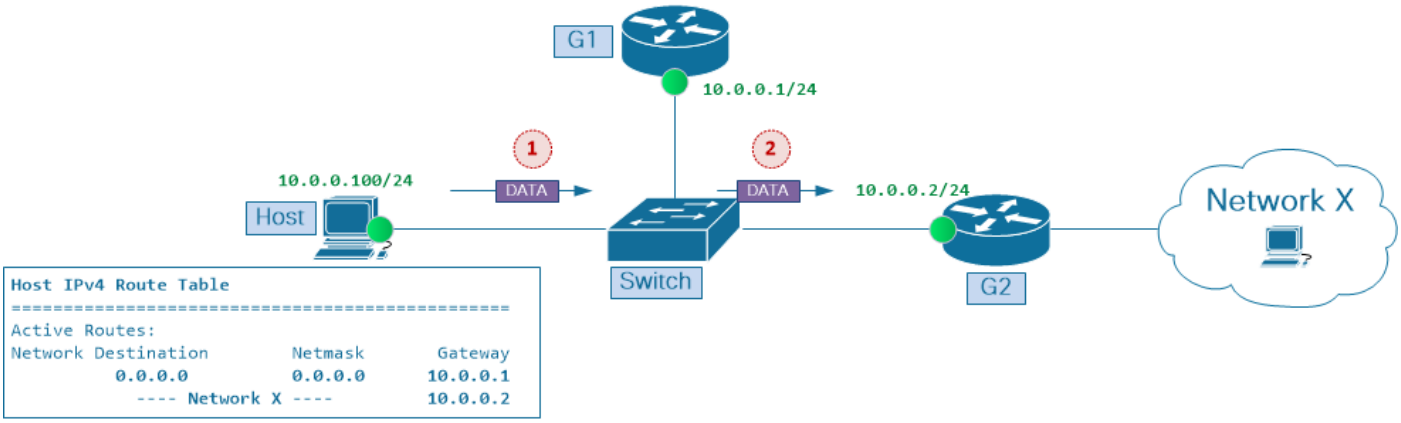
3. Als G2 en de host die wordt geïdentificeerd door het bronadres van IP-pakket zich op hetzelfde netwerk bevinden, wordt het ICMP-omleidingsbericht naar de host verzonden. Het ICMP-omleidingsbericht adviseert de host om zijn verkeer voor netwerk X rechtstreeks naar gateway G2 te sturen, aangezien dit een kortere weg naar de bestemming is.

4. De gateway G1 verstuurt het oorspronkelijke gegevenspakket naar de bestemming.

Afhankelijk van de configuratie van de host kan deze ervoor kiezen ICMP-omleidingsberichten te negeren die G1 naar de host stuurt. Als Host echter ICMP-berichten gebruikt om de routingcache aan te passen en latere gegevenspakketten rechtstreeks naar G2 begint te verzenden, worden deze voordelen in dit scenario bereikt

- optimalisering van het gegevensdoorsturen via het netwerk; het verkeer bereikt zijn bestemming sneller
- Beperking van netwerkgebruik, zoals bandbreedte en router-CPU-belasting

Afbeelding 2: Next Hop G2 geïnstalleerd in Host Routing Cache



Next Hop G2 geïnstalleerd in host routing cache

Zoals in afbeelding 2 wordt getoond, worden deze voordelen in het netwerk gezien nadat de host een route-cachegeheugen heeft gecreëerd voor Network X met G2 als de volgende hop:

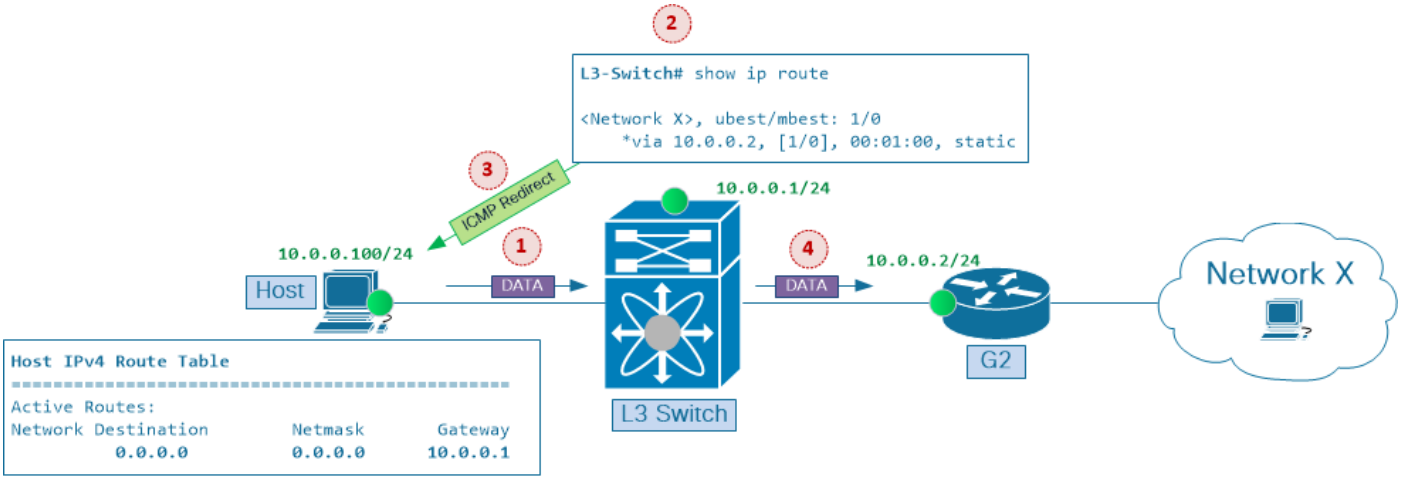
- Het bandbreedtegebruik op het verband tussen Switch en router G1 vermindert in beide richtingen.
- Het gebruik van cpu op router G1 vermindert, omdat de verkeersstroom van Host naar Network X niet deze knoop meer oversteekt.
- De end-to-end netwerkvertraging tussen host en netwerk X verbetert.

Om het belang van het mechanisme van ICMP Redirect te begrijpen, herinner dat de vroege routerimplementaties van Internet hoofdzakelijk op de middelen van CPU vertrouwden om gegevensverkeer te verwerken. Daarom was het wenselijk om het verkeersvolume te verminderen dat door één enkele router moest worden behandeld en ook om het aantal routerhop te minimaliseren dat een bepaalde verkeersstroom op zijn weg naar de bestemming moest oversteken. Tegelijkertijd werd Layer 2 Forwarding (ook bekend als switching) voornamelijk geïmplementeerd in aangepaste Application-Specific Integrated Circuits (ASIC), en vanuit het perspectief van doorsturen van prestaties was relatief 'goedkoop' in vergelijking met Layer 3 Forwarding (ook wel routing genoemd), die, opnieuw, werd uitgevoerd in processors voor algemene doeleinden.

Nieuwe ASIC-generaties kunnen zowel Layer 2 als Layer 3-pakketdoorsturen. Layer 3-tabellen die in hardware worden uitgevoerd, helpen de prestatiekosten te verlagen die door de routers aan pakketverwerking worden gekoppeld. Bovendien, toen Layer 3-doorsturen in Layer 2-switches werd geïntegreerd (die nu Layer 3-switches worden genoemd) pakketdoorsturen efficiënter maakte, was er geen **één-armige routerontwerpopties** (ook bekend als **router op een stok**) meer nodig en werden beperkingen die aan dergelijke netwerkconfiguraties waren gekoppeld, vermeden.

Afbeelding 3 bouwt voort op het scenario in afbeelding 1. Layer 2- en Layer 3-functies, die oorspronkelijk door twee aparte knooppunten, Switch en router G1, worden geleverd, worden geconsolideerd in één Layer 3-Switch, zoals Nexus 7000 Series-platform.

Afbeelding 3. Layer 3 Switch vervangt configuratie van "één-poorts-router"



Layer 3 Switch vervangt configuratie van "één-poorts router"

Dit gebeurt er wanneer de host een pakket naar een doelnetwerk verstuurt X:

1. Gateway L3 Switch met IP-adres 10.0.0.1 ontvangt gegevenspakket van een host 10.0.0.10 op een netwerk waaraan het is gekoppeld.

2. De gateway, L3 Switch, controleert zijn routeringstabel en verkrijgt het adres 10.0.0.2 van de volgende gateway, G2, op het netwerk van de route aan de bestemming van het gegevenspakket, X.

3. Als G2 en de host die wordt geïdentificeerd door het bronadres van IP-pakket zich op hetzelfde netwerk bevinden, wordt het ICMP-omleidingsbericht naar de host verzonden. Het ICMP-omleidingsbericht adviseert de host om zijn verkeer voor Network X rechtstreeks naar gateway G2 te verzenden, aangezien dit een korter pad naar de bestemming is.

4. De gateway verstuurt het oorspronkelijke gegevenspakket naar de bestemming.

Nu Layer 3-switches zowel Layer 2 als Layer 3-pakketdoorsturen op ASIC-niveau kunnen uitvoeren, kan worden geconcludeerd dat beide voordelen van de ICMP Redirect-functionaliteit, (a) een betere vertragingstactiek door het netwerk en (b) een lagere benutting van netwerkbronnen worden bereikt, en dat er niet meer veel aandacht hoeft te worden besteed aan padoptimalisatietechnieken in multi-point Ethernet-segmenten.

Echter, met ICMP Redirect functionaliteit ingeschakeld op Layer 3-interfaces, blijft suboptimaal doorsturen via multi-point Ethernet-segmenten potentiële knelpunten voor prestaties opleveren, ondanks dat om een andere reden, zoals wordt uitgelegd in de sectie Nexus Platform Considerations later in dit document.

> **Opmerking:** ICMP-omleidingen zijn standaard ingeschakeld op Layer 3-interfaces in Cisco IOS en Cisco NX-OS-software.

> **Opmerking:** Samenvatting van voorwaarden wanneer ICMP-omleidingsberichten worden gegenereerd: Layer 3 switch genereert ICMP-omleidingsbericht terug naar de bron van het gegevenspakket, als het gegevenspakket moet worden doorgestuurd naar Layer 3-interface waarop dit pakket is ontvangen.

Suboptimale paden door Ethernet-netwerken

Interior Gateway Protocols (IGP), zoals Open Shortest Path First (OSFP) en Cisco Enhanced Interior Gateway Routing Protocol (EIGRP), zijn ontworpen om routing-informatie tussen routers te synchroniseren en consistent en voorspelbaar pakketdoorstuurgedrag te bieden op alle netwerkknooppunten die dergelijke informatie honoreren. Bijvoorbeeld, met multi-point Ethernet-netwerken, als alle Layer 3-knooppunten op een segment dezelfde routing-informatie gebruiken en het eens zijn over hetzelfde exit point naar de bestemming, is suboptimaal doorsturen over dergelijke netwerken zelden het geval.

Om te begrijpen wat sub-optimale het door:sturen wegen veroorzaakt, herinner dat Layer 3 knopen pakket het door:sturen van besluiten onafhankelijk van elkaar maken. Dat wil zeggen, het pakketdoorsturen van beslissingen die door router B zijn genomen is niet afhankelijk van het pakketdoorsturen van beslissingen die door router A zijn genomen. Dit is een van de belangrijkste principes om te onthouden wanneer u pakketdoorsturen via IP-netwerken probleemoplossing aanbiedt, en een belangrijk principe om in gedachten te houden wanneer u suboptimaal doorsturen pad in multi-point Ethernet-netwerken onderzoekt.

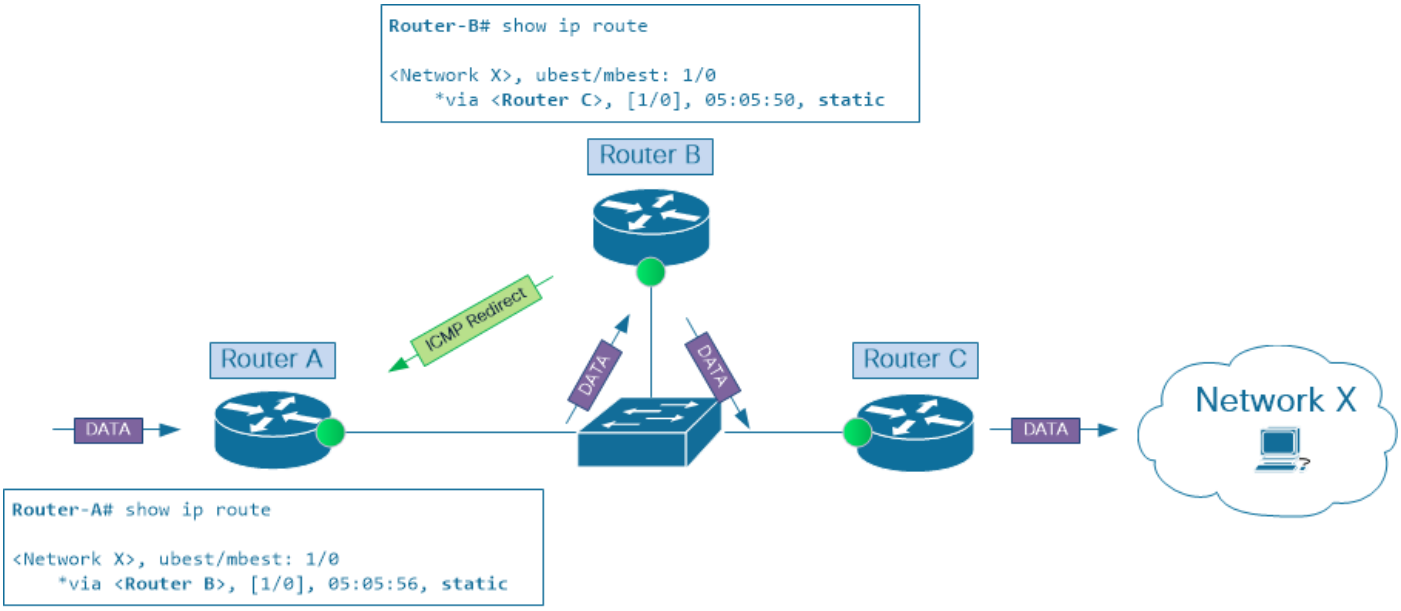
Zoals eerder vermeld, in netwerken waar alle routers op één enkel dynamisch routeringsprotocol vertrouwen om verkeer tussen eindpunten te leveren, moet het suboptimale door multi-point Ethernet segmenten niet gebeuren. In netwerken in de echte wereld is het echter heel gewoon om een combinatie van verschillende mechanismen voor pakketrouting en -doorsturen te vinden. Voorbeelden van dergelijke mechanismen zijn diverse IGP's, statische routing en op beleid gebaseerde routing. Deze functies worden doorgaans samen gebruikt om het gewenste doorsturen van verkeer via het netwerk te realiseren.

Terwijl gecombineerd gebruik van deze mechanismen kan helpen verkeer fijnafstemmen en aan vereisten van een bepaald netwerkontwerp voldoen, overzien zij bijwerkingen die deze hulpmiddelen samen in multi-point Ethernet netwerken kunnen veroorzaken in slechte algemene netwerkprestaties kunnen resulteren.

Statische routing

Om dit te illustreren, overweeg scenario in Figuur 4. Router A heeft statische route aan Netwerk X met router B als zijn volgende-hop. Tezelfdertijd gebruikt router B router C als zijn volgende-hop in statische route naar netwerk X.

Afbeelding 4 Suboptimaal pad met statische routing



Suboptimale pad met statische routing

Terwijl het verkeer dit netwerk bij router A ingaat, verlaat het door router C, en uiteindelijk wordt geleverd aan bestemmingsNetwerk X, moeten de pakketten dit IP netwerk tweemaal op hun manier doorkruisen aan de bestemming. Dit is geen efficiënt gebruik van netwerkbronnen. In plaats daarvan, verzend pakketten van Router A rechtstreeks naar Router C zou de zelfde resultaten, terwijl bereiken en minder netwerkmiddelen verbruiken.

> **Opmerking:** Zelfs als in dit scenario router A en router C worden gebruikt als toegang en uitgang Layer 3-knooppunten voor dit IP-netwerksegment, kunnen beide knooppunten worden vervangen door netwerkapplicaties (zoals taakverdelers of firewalls) als de laatste routeringsconfiguratie hebben die resulteert in hetzelfde pakketdoorsturen gedrag.

Op beleid gebaseerde routing

Op beleid gebaseerde routing (PBR) is een ander mechanisme dat een suboptimaal pad via Ethernet-netwerken kan veroorzaken. In tegenstelling tot Statische of Dynamische routing werkt PBR niet op routingtabelniveau. In plaats daarvan wordt voor het verkeer toegangscontrolelijst (ACL) rechtstreeks in de switch-hardware geprogrammeerd. Hierdoor wordt voor bepaalde verkeersstromen pakketdoorzoeking bij de toegangslijnkaart omzeild door routinginformatie die via Statische of Dynamische routing is verkregen.

In afbeelding 4, ruilen Routers A en B routerinformatie over het doelnetwerk X met een van de dynamische routerprotocollen. Beide zijn het eens over router B is de beste next-hop naar dit netwerk.

Met een PBR-configuratie op router B die routing-informatie die van het routeringsprotocol is ontvangen en router C als volgende hop op netwerk X instelt, wordt echter voldaan aan de voorwaarde om de ICMP-omleidingsfunctie te activeren en wordt het pakket naar de CPU van router B verzonden om het verder te verwerken.

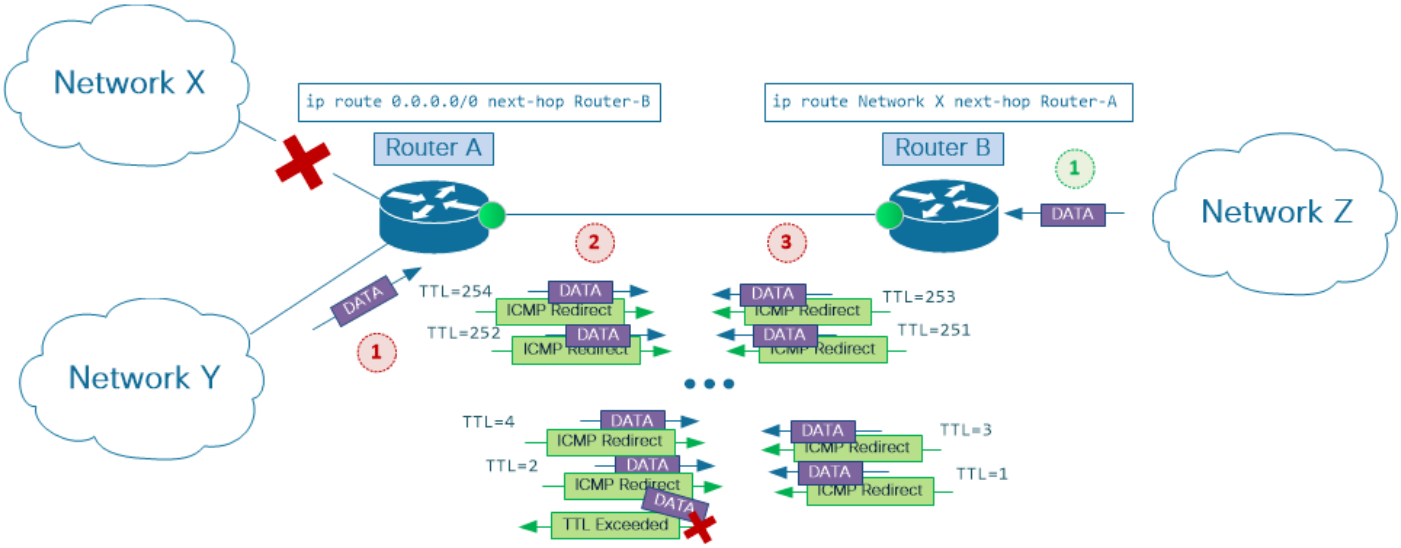
ICMP-omleidingen op point-to-point links

Tot nu toe verwees dit document naar Ethernet-netwerken die drie (of meer) Layer 3-knooppunten

hebben gekoppeld, vandaar de naam multi-point Ethernet-netwerken. Houd er echter rekening mee dat ICMP-omleidingsberichten ook op point-to-point Ethernet-koppelingen kunnen worden gegenereerd.

Overweeg scenario op Figuur 5. Router A gebruikt statische standaardroute om verkeer naar router B te verzenden, terwijl router B een statische route aan netwerk X heeft die aan router A richt.

Afbeelding 5. ICMP-omleidingen op point-to-point links



Suboptimale pad met statische routing

Deze ontwerpoptie, ook wel bekend als single-homed verbinding, is een populaire keuze wanneer u kleine gebruikersomgevingen verbindt met Service Provider netwerken. Hier is router B een Provider Edge (PE)-apparaat en router A is een user Edge (CE) apparaat.

Bericht dat de typische configuratie van Ce de gezamenlijke statische route(s) aan gebruiker IP adresblokken omvat die aan Null0 interface richten. Deze configuratie is een aanbevolen best practice voor single-homed CE-PE connectiviteit optie met statische routing. In dit voorbeeld wordt echter aangenomen dat een dergelijke configuratie niet aanwezig is.

Stel dat router A connectiviteit met netwerk X verliest zoals in de afbeelding. Wanneer pakketten van het gebruikersnetwerk Y of het externe netwerk Z proberen om netwerk X te bereiken, kunnen routers A en B het verkeer tussen elkaar stuiteren, en vermindert het IP Time-To-Live veld in elk pakket tot de waarde 1 bereikt, op welk punt verdere routing van het pakket niet mogelijk is.

Terwijl het verkeer aan Netwerk X heen en weer tussen PE en CE routers stuitert, verhoogt dramatisch (en onnodig) het gebruik van de CE-PE linkbandbreedte, wordt het probleem erger als ICMP-omleidingen aan één of beide kanten van punt-tot-punt PE-CE verbinding worden toegelaten. In dit geval wordt elk pakket in de stroom die naar Network X wordt geleid, meerdere malen in CPU op elke router verwerkt om de ICMP-omleidingsberichten te genereren.

Nexus platform overwegingen

Wanneer ICMP-omleidingen zijn ingeschakeld op Layer 3-switch en een inkomend gegevenspakket deze interface gebruikt om een Layer 3-interface in te voeren en te verlaten, wordt een ICMP-omleidingsbericht gegenereerd. Terwijl Layer 3-pakketdoorsturen in hardware op

Cisco Nexus 7000-platform gebeurt, is het nog steeds de verantwoordelijkheid van de switch-CPU om ICMP-omleidingsberichten te construeren. Hiervoor moet de CPU op Nexus 7000 Supervisor-module IP-adresinformatie verkrijgen van de stroom waarvan het pad door het netwerksegment kan worden geoptimaliseerd. Dit is de reden achter gegevenspakket dat door toegangslijnkaart naar de module van de Supervisor wordt verzonden.

Als ontvangers van een ICMP Redirect-bericht dit negeren en doorgaan met het doorsturen van gegevensverkeer naar Layer 3-switch van Nexus waarop ICMP-omleidingen zijn ingeschakeld, wordt het ICMP Redirect-generatieproces geactiveerd voor elk gegevenspakket.

Op lijnkaartniveau begint het proces in de vorm van hardware-Forwarding-uitzondering. De uitzonderingen worden opgeheven op ASICs wanneer de pakket het door:sturen verrichting niet met succes door de lijnkaartmodule kan worden voltooid. In dit geval moet het gegevenspakket naar de Supervisor-module worden verzonden voor correcte pakketverwerking.

> **Opmerking:** De CPU op de Supervisor module, genereert niet alleen ICMP Redirect-berichten, het behandelt veel andere pakket het door:sturen uitzonderingen, zoals IP pakketten met de waarde van de Tijd te leven (TTL) die aan 1 wordt geplaatst, of IP pakketten die moeten worden gefragmenteerd alvorens het wordt verzonden naar de volgende hop.

Nadat CPU op de Supervisor module verzonden ICMP Redirect bericht naar de bron, voltooit het uitzondering behandeling door gegevenspakket door te sturen naar de volgende hop door uitgang lijnkaartmodule.

Terwijl Nexus 7000 Supervisor modules gebruik maken van krachtige CPU-processors die grote verkeersvolumes kunnen verwerken, is het platform ontworpen om het grootste deel van het dataverkeer op lijnkaartniveau te verwerken zonder de noodzaak om de Supervisor CPU-processor te betrekken bij het pakketdoorsturen proces. Hierdoor kan de CPU zich op zijn kerntaken richten en kan pakketdoorsturen naar speciale hardware-engine op lijnkaarten.

In stabiele netwerken wordt verwacht dat uitzonderingen voor het doorsturen van pakketten, als ze zich voordoen, op een redelijk lage snelheid zullen plaatsvinden. Op basis van deze veronderstelling kunnen ze door Supervisor CPU worden verwerkt zonder dat dit een significant effect heeft op de prestaties ervan. Aan de andere kant kan een CPU die zich bezighoudt met pakketdoorsturen van uitzonderingen die op een zeer hoog tempo voorkomen een negatief effect hebben op de algehele systeemstabiliteit en reactievermogen.

Nexus 7000 platform design biedt een aantal mogelijkheden om switch CPU's te beschermen tegen aanzienlijk verkeer. Deze mechanismen worden op verschillende punten in het systeem toegepast. Op lijnkaartniveau zijn er hardwareresultaten en besturingsplane Policing (CoPP)-functie. Beide vastgestelde verkeersdrempels, die effectief de hoeveelheid verkeer controleert die van elke lijnkaartmodule naar de Supervisor moet worden doorgestuurd.

Deze beveiligingsmechanismen geven de voorkeur aan het verkeer van verschillende controleprotocollen die van cruciaal belang zijn voor netwerkstabiliteit en beheerbaarheid van de switch, zoals OSPF, BGP of SSH, en filteren tegelijkertijd op agressieve wijze verkeerstypen die niet van cruciaal belang zijn om de vliegtuigfunctionaliteit van de switch te regelen. Het grootste deel van het gegevensverkeer wordt, indien dit naar de CPU wordt doorgestuurd als gevolg van uitzonderingen voor het doorsturen van pakketten, zwaar bewaakt door dergelijke mechanismen.

Hardware snelheidsbegrenzers en CoPP policing De mechanismen verstrekken stabiliteit van controlevliegtuig van de switch en sterk geadviseerd om altijd worden toegelaten, kunnen zij één van de belangrijkste redenen van gegevenspakketdalingen, overdrachtvertragingen, en algemene slechte toepassingsprestaties over het netwerk zijn. Dit is waarom het belangrijk is om de wegen te begrijpen die verkeersstromen door het netwerk en het gebruik van hulpmiddelen nemen om netwerkapparatuur te controleren die kan en/of verwacht om functionaliteit ICMP Redirect te gebruiken.

Tools voor bewaking en diagnose van verkeer

IP-verkeer tonen

Zowel Cisco IOS- als Cisco NX-OS-software biedt een manier om statistieken te controleren van het verkeer dat door CPU wordt verwerkt. Dit gebeurt met **show ip traffic** uit. Deze opdracht kan worden gebruikt om ontvangst en/of genereren van ICMP Redirect-berichten te controleren op Layer 3-switch of -router.

```
Nexus7000#show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
----------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

Nexus7000#
```

Voer uit show ip traffic opdracht een paar keer en controleer of ICMP-omleiding tellerstoename.

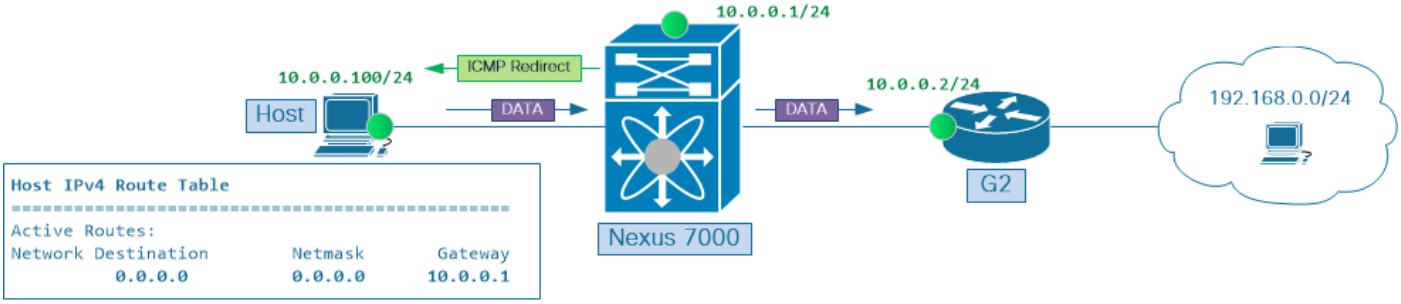
Ethanalyzer

Cisco NX-OS-software heeft een ingebouwde tool om verkeer op te nemen flowing van en naar switch CPU, bekend als Ethanalyzer.

> **Opmerking:** Raadpleeg voor meer informatie over Ethanalyzer de Ethanalyzer op de Nexus 7000 Handleiding voor probleemoplossing.

Afbeelding 6 toont een scenario dat vergelijkbaar is met dat in afbeelding 3. Hier wordt Network X vervangen door 192.168.0.0/24.

Afbeelding 6 Leg de Ethanalyzer Capture uit



Leg ethanalyzer Capture uit

De Host 10.0.0.100 verzendt een continue stroom ICMP Echo-aanvragen naar het IP-adres van de bestemming 192.168.0.1. De Host gebruikt Switch Virtual Interface (SVI) 10 van Nexus 7000 switch als zijn volgende hop naar het externe netwerk 192.168.0.0/24. Voor demonstratiedoeleinden is de Host geconfigureerd om ICMP-omleidingsberichten te negeren.

Gebruik deze volgende opdracht om ICMP-verkeer op te nemen dat is ontvangen en verzonden door Nexus 7000 CPU:

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

Tijdstempels in de vorige uitvoer suggereren dat drie pakketten die in dit voorbeeld zijn gemarkeerd, tegelijkertijd zijn opgenomen, 2018-09-15 23:45:40.128. De volgende is een per-pakketuitsplitsing van deze pakketgroep

- Het eerste pakket is het pakket met toegangsgegevens, dat in dit voorbeeld een ICMP-echo-verzoek is.

    2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 ICMP Echo (ping)-verzoek

- Het tweede pakket is een ICMP Redirect-pakket, gegenereerd door gateway. Dit pakket wordt teruggestuurd naar de host.

  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP Redirect (Redirect voor host)

- Het derde pakket is het gegevenspakket dat in de uitgangsrichting is opgenomen nadat het door de CPU is gerouteerd. Hoewel niet eerder getoond, is de IP TTL van dit pakket verminderd en de controlesom opnieuw berekend.

  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP Echo (ping)-verzoek

Terwijl u door grote Ethanalyzer bladert vangt die vele pakketten van verschillende types en stromen hebben, kan het moeilijk zijn om ICMP te correleren omleiden berichten met het gegevensverkeer dat aan hen beantwoordt.

In deze situaties, focus op ICMP omleiden berichten om informatie op te halen over suboptimaal doorgestuurde verkeersstromen. De ICMP-omleidingsberichten bevatten de internetheader plus de eerste 64 bits van de oorspronkelijke datagramgegevens. Deze gegevens worden gebruikt door de bron van het datagram om het bericht aan het juiste proces aan te passen.

Gebruik het pakketopnamegereedschap van Ethanalyzer met **detailtrefwoord** om de inhoud van ICMP-omleidingsberichten weer te geven en IP-adresinformatie te vinden van de gegevensstroom die suboptimaal wordt doorgestuurd

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
[Time delta from previous displayed frame: 0.000426000 seconds]
[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
```

```
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
 Type: 5 (Redirect)
 Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)
Destination: 192.168.0.1 (192.168.0.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

ICMP-omleidingen uitschakelen

Als het netwerkontwerp vereist dat de verkeersstroom uit dezelfde Layer 3-interface wordt gerouteerd waarop het de switch of router heeft ingevoerd, is het mogelijk om te voorkomen dat de stroom door de CPU wordt gerouteerd als u de ICMP-omleidingsfunctionaliteit op Layer 3-interface die aan deze interface beantwoordt, uitschakelt.

In feite is het voor de meeste netwerken een goede praktijk om ICMP-omleidingen proactief uit te schakelen op alle Layer 3-interfaces, zowel fysiek, zoals Ethernet-interface, als virtueel, zoals Port-Channel- en SVI-interfaces. Gebruik de no ip redirects Cisco NX-OS opdracht op interfaceniveau om ICMP-omleidingen op een Layer 3-interface uit te schakelen. Controleer of de functionaliteit van ICMP Redirect is uitgeschakeld:

- verzekeren**no ip** **omleidt** bevel wordt toegevoegd aan interfaceconfiguratie.

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- Zorg ervoor dat de status van ICMP-omleidingen op de interface "uitgeschakeld" wordt weergegeven.

```
Nexus7000#show ip interface vlan 10 | include redirects
  IP icmp redirects: disabled
```

- Zorg ervoor dat de vlag voor ICMP Redirect Enable/Disable op **0** is ingesteld door de softwarecomponent van Cisco NX-OS die de interfaceconfiguratie van switch Supervisor naar een of meer lijnkaarten duwt.

```
Nexus7000#show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
```

- Zorg ervoor dat ICMP Redirect in-/uitschakelen vlag voor een bepaalde Layer 3-interface is ingesteld op **0** op een of meer lijnkaarten.

```
Nexus7000#attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done
in one of the custom VDCs
module-7#vdc 6

module-7#show system internal iftmc info interface vlan 10 | include icmp_redirect
icmp_redirect : 0x0 ipv6_redirect : 0x1
```

Samenvatting

Het ICMP Redirect-mechanisme, zoals beschreven in RFC 792, is ontworpen om het doorsturen van paden door multipoint netwerksegmenten te optimaliseren. Aan het begin van het internet droeg deze optimalisatie bij aan de bescherming van dure netwerkbronnen, zoals linkbandbreedte en CPU-cycli van routers. Naarmate netwerkbandbreedte goedkoper werd en relatief langzame op CPU gebaseerde pakketrouting evolueerde in snellere Layer 3-pakketdoorsturen in speciale hardware-ASIC's, nam het belang van optimale gegevensdoorvoer door multipoint netwerksegmenten af. Standaard is de functionaliteit ICMP Redirect ingeschakeld op elke Layer 3-interface. De pogingen om netwerkknooppunten op multi-point Ethernet-segmenten te informeren over optimale doorsturen van paden worden echter niet altijd begrepen en door het netwerkpersoneel opgevolgd. In netwerken met gecombineerd gebruik van verschillende doorsturen mechanismen, zoals Statische routing, Dynamic Routing en op beleid gebaseerde routing, kan dit, als u de ICMP Redirect-functionaliteit ingeschakeld laat en deze niet goed bewaakt, leiden tot ongewenst gebruik van doorvoer knooppunt(en) CPU's om het productieverkeer te verwerken. Dit kan op zijn beurt een aanzienlijk effect hebben op zowel de

stromen van productieverkeer als de stabiliteit van het controlevliegtuig van de netwerkinfrastructuur.

Voor de meeste netwerken wordt het beschouwd als een goede praktijk om functionaliteit ICMP Redirect op alle Layer 3-interfaces in netwerkinfrastructuur proactief uit te schakelen. Dit helpt om scenario's van productiegegevensverkeer te voorkomen dat in CPU van Layer 3-switches en -routers wordt verwerkt wanneer er een beter doorsturen pad is door multipoint netwerksegmenten.

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.