Informazioni sui messaggi di reindirizzamento ICMP

Sommario

Introduzione

In questo documento viene descritta la funzionalità di reindirizzamento dei pacchetti ICMP (Internet Control Message Protocol).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Architettura della piattaforma Nexus 7000
- Configurazione del software Cisco NX-OS
- Protocollo RFC (Request for Comments) 792

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Nexus 7000
- Software Cisco NX-OS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene descritta la funzionalità di reindirizzamento dei pacchetti offerta dal protocollo ICMP (Internet Control Message Protocol). Il documento spiega cosa indica in genere la presenza di messaggi di reindirizzamento ICMP nella rete e cosa è possibile fare per ridurre al minimo gli effetti collaterali negativi associati alle condizioni di rete che causano la generazione di messaggi di reindirizzamento ICMP.

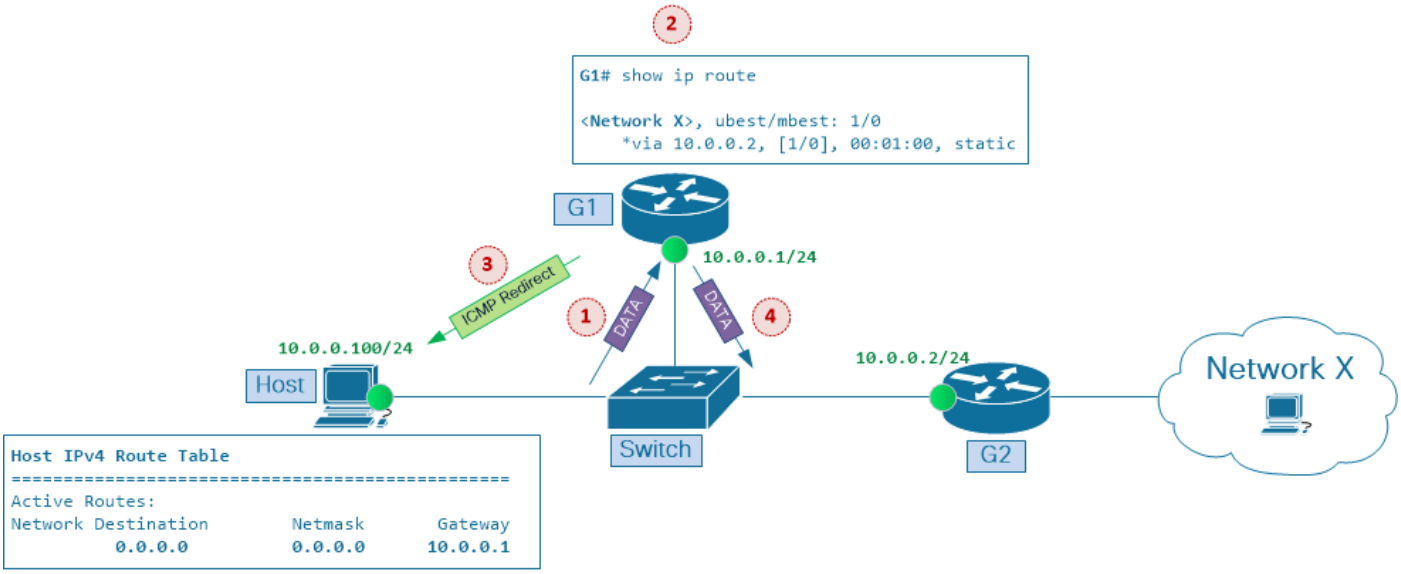
Messaggi di reindirizzamento ICMP

La funzionalità di reindirizzamento ICMP è spiegata nella RFC 792 - Protocollo Internet Control Message in questo esempio:

> In questa situazione, il gateway invia un messaggio di reindirizzamento a un host.
>
> Un gateway, G1, riceve un datagramma Internet da un host di una rete a cui è collegato. Il gateway G1 controlla la relativa tabella di routing e ottiene l'indirizzo del gateway successivo G2 sul percorso verso la rete di destinazione Internet del datagramma, X
>
> Se G2 e l'host identificato dall'indirizzo di origine Internet del datagramma si trovano sulla stessa rete, viene inviato un messaggio di reindirizzamento all'host. Il messaggio di reindirizzamento indica all'host di inviare il traffico della rete X direttamente al gateway G2, poiché si tratta di un percorso più breve verso la destinazione.
>
> Il gateway inoltra i dati del datagramma originale alla relativa destinazione Internet.

Questo scenario è mostrato nella Figura 1. L'host e i due router, G1 e G2, sono collegati a un segmento Ethernet condiviso e hanno indirizzi IP nella stessa rete 10.0.0.0/24

Figura 1 Reindirizzamenti ICMP in reti Ethernet multipoint



Reindirizzamenti ICMP in reti Ethernet multipoint

L'host ha l'indirizzo IP 10.0.0.100. La tabella di routing dell'host ha una voce di route predefinita che punta all'indirizzo IP 10.0.0.1 del router G1 come gateway predefinito. Il router G1 usa l'indirizzo IP 10.0.0.2 del router G2 come hop successivo quando inoltra il traffico alla rete di destinazione X.

Questo è quello che succede quando l'host invia un pacchetto alla rete di destinazione X:

1. Il gateway G1 con indirizzo IP 10.0.0.1 riceve il pacchetto dati dall'host 10.0.0.100 sulla rete a cui è collegato.

2. Il gateway G1 controlla la relativa tabella di routing e ottiene l'indirizzo IP 10.0.0.2 del gateway successivo G2 sul percorso verso la rete di destinazione del pacchetto dati X.

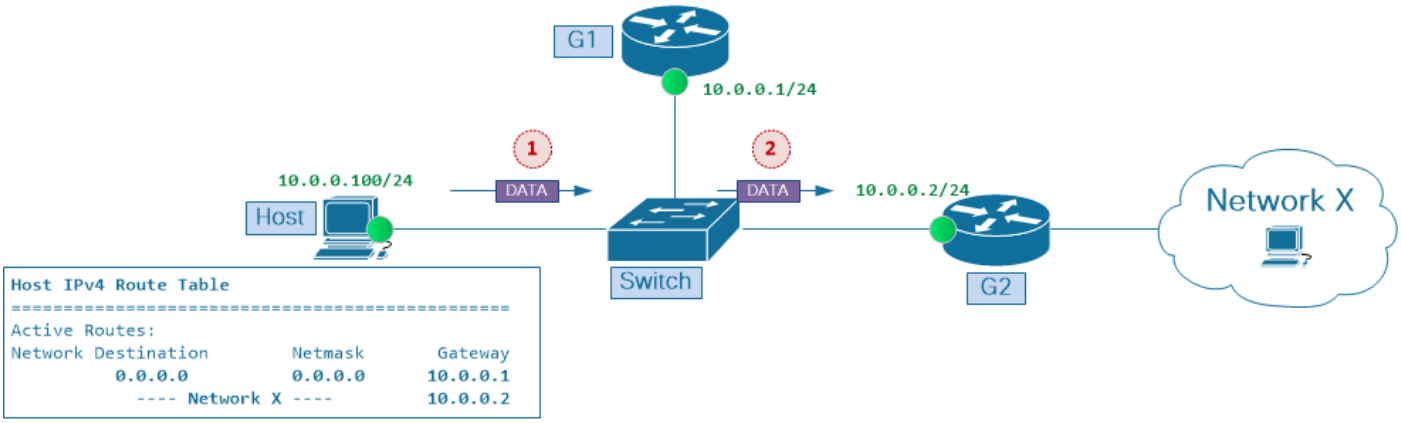
3. Se G2 e l'host identificato dall'indirizzo di origine del pacchetto IP si trovano sulla stessa rete, all'host viene inviato un messaggio di reindirizzamento ICMP. Il messaggio di reindirizzamento ICMP consiglia all'host di inviare il traffico della rete X direttamente al gateway G2, poiché si tratta di un percorso più breve verso la destinazione.

4. Il gateway G1 inoltra il pacchetto dati originale alla destinazione.

A seconda della configurazione dell'host, può scegliere di ignorare i messaggi di reindirizzamento ICMP inviati dal G1. Tuttavia, se l'host utilizza i messaggi di reindirizzamento ICMP per regolare la propria cache di routing e inizia a inviare i pacchetti di dati successivi direttamente al server G2, in questo scenario vengono ottenuti questi vantaggi

- Ottimizzazione del percorso di inoltro dei dati attraverso la rete; il traffico raggiunge la sua destinazione più rapidamente
- Riduzione dell'utilizzo delle risorse di rete, ad esempio larghezza di banda e carico della CPU del router

Figura 2 Hop successivo G2 installato nella cache di routing dell'host



Hop successivo G2 installato nella cache di routing dell'host

Come mostrato nella Figura 2, dopo che l'host ha creato la voce route cache per la rete X con G2 come hop successivo, la rete presenta i seguenti vantaggi:

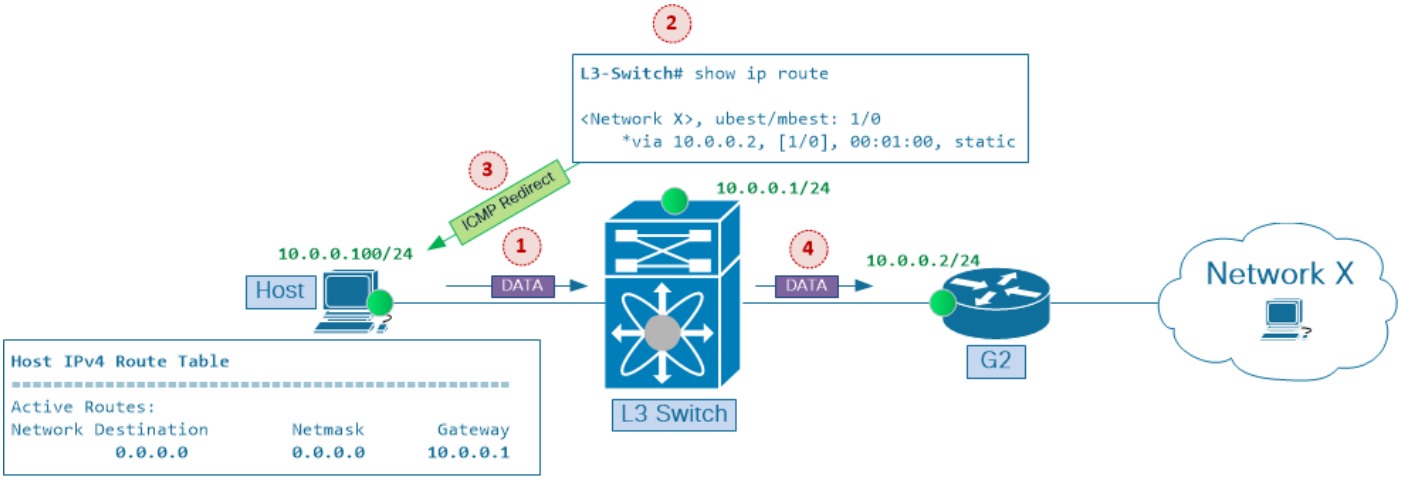
- L'utilizzo della larghezza di banda sul collegamento tra lo switch e il router G1 diminuisce in entrambe le direzioni.
- L'utilizzo della CPU sul router G1 si riduce perché il flusso di traffico dall'host alla rete X non attraversa più questo nodo.
- Il ritardo di rete end-to-end tra l'host e la rete X migliora.

Per comprendere l'importanza del meccanismo di reindirizzamento ICMP, tenere presente che le prime implementazioni di router Internet si sono basate principalmente sulle risorse della CPU per elaborare il traffico di dati. Era quindi auspicabile ridurre il volume del traffico che doveva essere gestito da un singolo router e ridurre al minimo il numero di hop su router che un particolare flusso di traffico doveva attraversare lungo il percorso verso la destinazione. Allo stesso tempo, l'inoltro di layer 2 (noto anche come switching) è stato implementato principalmente in circuiti integrati specifici dell'applicazione (ASIC) personalizzati e, dal punto di vista delle prestazioni, è stato relativamente "economico" rispetto all'inoltro di layer 3 (detto anche routing), che, ancora una volta, è stato eseguito in processori generici.

Le nuove generazioni ASIC possono eseguire sia l'inoltro di pacchetti di layer 2 che di layer 3. La ricerca nella tabella di layer 3 eseguita nell'hardware consente di ridurre i costi delle prestazioni associati alla gestione dei pacchetti da parte dei router. Inoltre, quando è stata integrata la funzionalità di inoltro di layer 3 negli switch di layer 2 (ora denominati switch di layer 3), il funzionamento dell'inoltro dei pacchetti è diventato più efficiente, **non è** più necessario utilizzare opzioni di progettazione di **router con un solo braccio** (noto anche come **router su stick**) e si evitano i limiti associati a tali configurazioni di rete.

La Figura 3 si basa sullo scenario illustrato nella Figura 1. Ora le funzioni di layer 2 e layer 3, fornite originariamente da due nodi separati, switch e router G1, sono consolidate in un unico switch di layer 3, ad esempio la piattaforma Nexus serie 7000.

La Figura 3 sostituisce la configurazione di uno switch di layer 3 con un router



Lo switch di layer 3 sostituisce la configurazione con un router

Questo è quello che succede quando l'host invia un pacchetto alla rete di destinazione X:

1. Lo switch L3 gateway con indirizzo IP 10.0.0.1 riceve un pacchetto dati da un host 10.0.0.100 su una rete a cui è collegato.

2. Lo switch L3 del gateway controlla la tabella di routing e ottiene l'indirizzo 10.0.0.2 del gateway successivo, G2, sul percorso verso la rete di destinazione del pacchetto dati, X.

3. Se G2 e l'host identificato dall'indirizzo di origine del pacchetto IP si trovano sulla stessa rete, all'host viene inviato un messaggio di reindirizzamento ICMP. Il messaggio di reindirizzamento ICMP consiglia all'host di inviare il traffico per la rete X direttamente al gateway G2, in quanto si tratta di un percorso più breve verso la destinazione.

4. Il gateway inoltra il pacchetto dati originale alla destinazione.

Con gli switch di layer 3, ora in grado di eseguire sia l'inoltro di pacchetti di layer 2 che di layer 3 a livello ASIC, si può concludere che vengono raggiunti entrambi i vantaggi della funzionalità di reindirizzamento ICMP, (a) miglioramento del ritardo nella rete e (b) riduzione dell'utilizzo delle risorse di rete, e che non c'è più bisogno di prestare molta attenzione alle tecniche di ottimizzazione dei percorsi nei segmenti Ethernet multi-point.

Tuttavia, con la funzionalità di reindirizzamento ICMP abilitata sulle interfacce di layer 3, l'inoltro subottimale attraverso i segmenti Ethernet multi-point continua a presentare potenziali colli di bottiglia delle prestazioni, anche se per un motivo diverso, come spiegato nella sezione Considerazioni sulla piattaforma Nexus più avanti in questo documento.

> **Nota:** I reindirizzamenti ICMP sono abilitati per impostazione predefinita sulle interfacce di layer 3 nei software Cisco IOS e Cisco NX-OS.

> **Nota:** Riepilogo delle condizioni in cui vengono generati i messaggi di reindirizzamento ICMP: Lo switch di layer 3 genera un messaggio ICMP Redirect verso l'origine del pacchetto dati, se il pacchetto dati deve essere inoltrato fuori dall'interfaccia di layer 3 su cui viene ricevuto.

Percorsi subottimali tramite reti Ethernet

I protocolli IGP (Interior Gateway Protocol), come Open Shortest Path First (OSFP) e Cisco Enhanced Interior Gateway Routing Protocol (EIGRP), sono progettati per sincronizzare le informazioni di routing tra i router e per fornire un comportamento coerente e prevedibile di inoltro dei pacchetti su tutti i nodi di rete che rispettano tali informazioni. Ad esempio, nelle reti Ethernet multi-punto, se tutti i nodi di layer 3 di un segmento utilizzano le stesse informazioni di routing e concordano sullo stesso punto di uscita verso la destinazione, l'inoltro non ottimale su tali reti si verifica raramente.

Per comprendere la causa dei percorsi di inoltro non ottimali, tenere presente che i nodi di layer 3 prendono le decisioni di inoltro dei pacchetti in modo indipendente l'uno dall'altro. Vale a dire che la decisione di inoltro dei pacchetti presa dal router B non dipende dalla decisione di inoltro dei pacchetti presa dal router A. Questo è uno dei principi chiave da ricordare quando si risolvono i problemi di inoltro dei pacchetti tramite le reti IP ed è importante da tenere presente quando si analizza il percorso di inoltro non ottimale nelle reti Ethernet multi-punto.

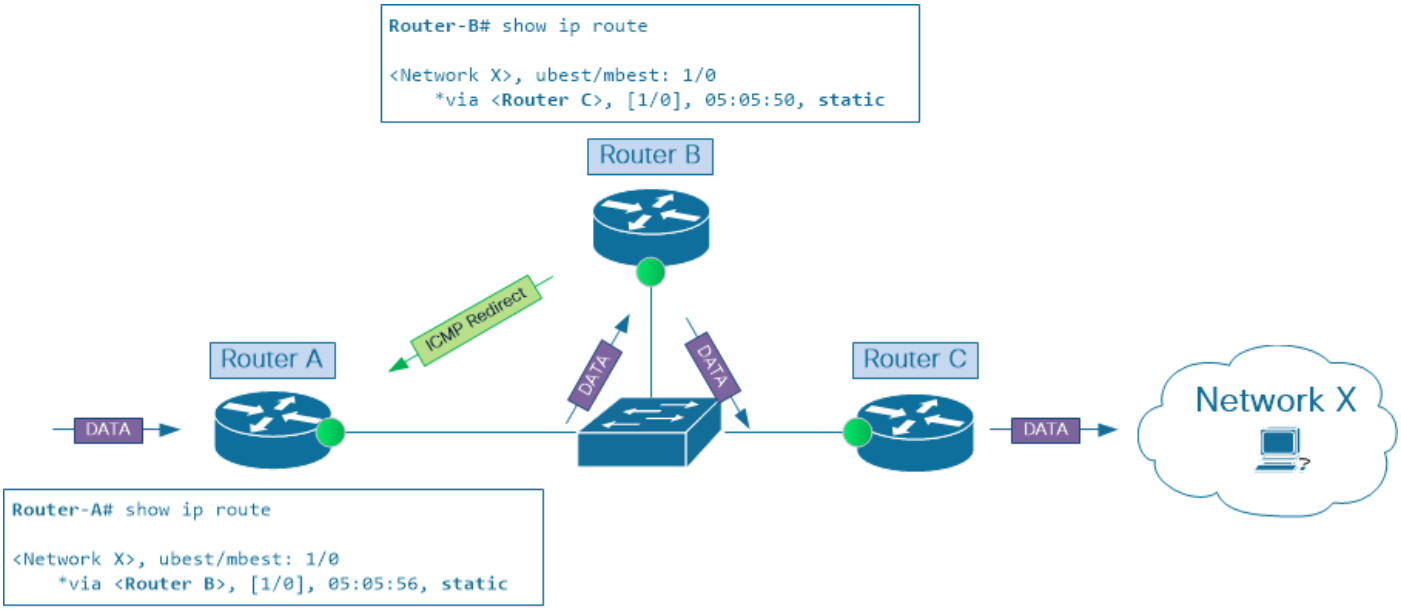
Come accennato in precedenza, nelle reti in cui tutti i router si basano su un unico protocollo di routing dinamico per distribuire il traffico tra gli endpoint, l'inoltro non ottimale attraverso i segmenti Ethernet multi-punto non deve verificarsi. Nelle reti reali, tuttavia, è molto comune trovare una combinazione di vari meccanismi di routing e inoltro dei pacchetti. Esempi di tali meccanismi sono vari IGP, il routing statico e il routing basato su criteri. Queste funzionalità vengono in genere utilizzate insieme per ottenere l'inoltro del traffico desiderato attraverso la rete.

Anche se l'uso combinato di questi meccanismi può aiutare a ottimizzare il flusso del traffico e a soddisfare i requisiti di una particolare progettazione di rete, essi trascurano gli effetti collaterali che questi strumenti insieme possono causare nelle reti Ethernet multi-point e possono causare prestazioni complessive di rete insoddisfacenti.

Routing statico

Per illustrare questo scenario, considerare la figura 4. Il router A ha un percorso statico alla rete X con il router B come hop successivo. Allo stesso tempo, il router B usa il router C come hop successivo nel percorso statico alla rete X.

Figura 4 Percorso non ottimale con routing statico



Mentre il traffico entra in questa rete dal router A, la lascia attraverso il router C e alla fine viene consegnato alla rete di destinazione X, i pacchetti devono attraversare questa rete IP due volte nel percorso verso la destinazione. Questo non è un uso efficiente delle risorse di rete. Al contrario, l'invio di pacchetti dal router A direttamente al router C avrebbe gli stessi risultati, mentre l'invio di pacchetti e il consumo di risorse di rete sarebbero inferiori.

> **Nota:** Anche se in questo scenario il router A e il router C vengono utilizzati come nodi di livello 3 in entrata e in uscita per questo segmento di rete IP, entrambi i nodi possono essere sostituiti da accessori di rete (ad esempio, load balancer o firewall) se questi ultimi hanno una configurazione di routing che determina lo stesso comportamento di inoltro dei pacchetti.

Policy-Based Routing

Il Policy Based Routing (PBR) è un altro meccanismo che può causare un percorso non ottimale attraverso le reti Ethernet. Tuttavia, a differenza del routing statico o dinamico, PBR non opera a livello di tabella di routing. Al contrario, programma il reindirizzamento del traffico dell'Access Control List (ACL) direttamente nell'hardware dello switch. Di conseguenza, per flussi di traffico selezionati, la ricerca dell'inoltro pacchetti sulla scheda di linea in entrata ignora le informazioni di routing ottenute tramite il routing statico o dinamico.

Nella Figura 4, i router A e B scambiano informazioni di routing sulla rete di destinazione X con uno dei protocolli di routing dinamico. Entrambi concordano sul fatto che il router B è l'hop successivo migliore per questa rete.

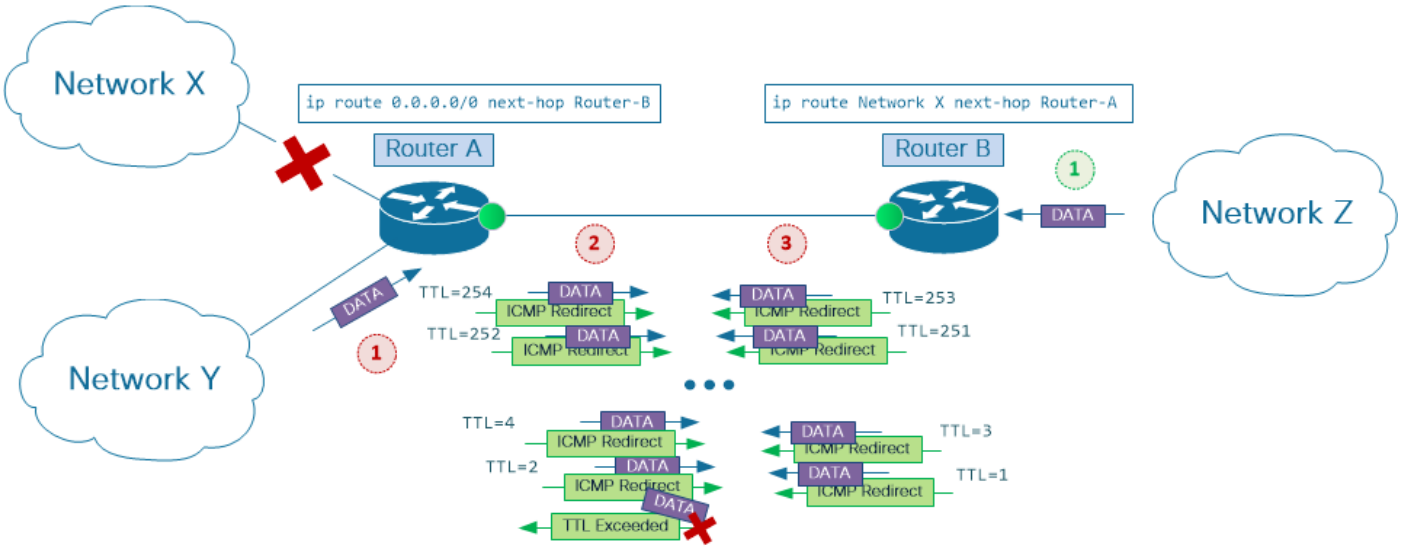
Tuttavia, con una configurazione PBR sul router B che ignora le informazioni di routing ricevute dal protocollo di routing e imposta il router C come hop successivo sulla rete X, viene soddisfatta la condizione per attivare la funzione di reindirizzamento ICMP e il pacchetto viene inviato alla CPU del router B per essere elaborato ulteriormente.

Reindirizzamenti ICMP su collegamenti point-to-point

Finora questo documento si riferiva alle reti Ethernet a cui sono collegati tre (o più) nodi di layer 3, da cui il nome reti Ethernet multipunto. Tenere presente, tuttavia, che i messaggi di reindirizzamento ICMP possono essere generati anche su collegamenti Ethernet point-to-point.

Si prenda in considerazione lo scenario della Figura 5. Il router A utilizza un percorso statico predefinito per inviare il traffico al router B, mentre il router B dispone di un percorso statico alla rete X che punta al router A.

Figura 5. Reindirizzamenti ICMP su collegamenti point-to-point



Percorso non ottimale con routing statico

Questa opzione di progettazione, nota anche come connessione con una sola casa, è una scelta diffusa quando si connettono ambienti utente di piccole dimensioni a reti di provider di servizi. Qui il router B è un dispositivo Provider Edge (PE), mentre il router A è un dispositivo User Edge (CE).

Si noti che la configurazione CE tipica include route statiche aggregate ai blocchi di indirizzi IP utente che puntano all'interfaccia Null0. Questa configurazione è una procedura consigliata per l'opzione di connettività CE-PE single-homed con routing statico. Tuttavia, ai fini del presente esempio, si presume che tale configurazione non sia presente.

Si supponga che il router A perda la connettività alla rete X, come mostrato nella Figura. Quando i pacchetti provenienti dalla rete utente Y o dalla rete remota Z tentano di raggiungere la rete X, i router A e B possono far rimbalzare il traffico tra di loro e diminuiscono il campo IP Time-To-Live in ciascun pacchetto finché il suo valore non raggiunge 1, nel qual caso non è possibile effettuare un ulteriore routing del pacchetto.

Mentre il traffico diretto alla rete X rimbalza avanti e indietro tra i router PE e CE, aumentando significativamente (e inutilmente) l'utilizzo della larghezza di banda del collegamento CE-PE, il problema diventa peggiore se i reindirizzamenti ICMP sono abilitati su uno o entrambi i lati della connessione PE-CE point-to-point. In questo caso, ciascun pacchetto del flusso diretto alla rete X viene elaborato più volte nella CPU di ciascun router per contribuire alla generazione dei messaggi di reindirizzamento ICMP.

Considerazioni sulla piattaforma Nexus

Quando i reindirizzamenti ICMP sono abilitati sull'interfaccia di layer 3 e un pacchetto di dati in ingresso utilizza questa interfaccia sia per entrare che per uscire da uno switch di layer 3, viene generato un messaggio di reindirizzamento ICMP. Mentre l'inoltro dei pacchetti di layer 3 viene eseguito nell'hardware della piattaforma Cisco Nexus 7000, la CPU dello switch ha comunque la responsabilità di creare messaggi di reindirizzamento ICMP. A tale scopo, la CPU del modulo Supervisor Nexus 7000 deve ottenere le informazioni sull'indirizzo IP del flusso il cui percorso attraverso il segmento di rete può essere ottimizzato. Questo è il motivo per cui il pacchetto dati viene inviato dalla scheda di linea in entrata al modulo Supervisor.

Se i destinatari del messaggio di reindirizzamento ICMP lo ignorano e continuano a inoltrare il traffico di dati all'interfaccia di layer 3 dello switch Nexus su cui sono abilitati i reindirizzamenti

ICMP, per ogni pacchetto dati viene attivato il processo di generazione del reindirizzamento ICMP.

A livello di scheda di linea il processo ha inizio sotto forma di eccezione di inoltro hardware. Le eccezioni vengono generate sugli ASIC quando l'operazione di inoltro dei pacchetti non può essere completata correttamente dal modulo della scheda di linea. In questo caso, il pacchetto dati deve essere inviato al modulo Supervisor per una gestione corretta.

> **Nota:** La CPU del modulo Supervisor non solo genera messaggi di reindirizzamento ICMP, ma gestisce molte altre eccezioni di inoltro dei pacchetti, come i pacchetti IP con valore TTL (Time To Live) impostato su 1 o i pacchetti IP che devono essere frammentati prima di essere inviati all'hop successivo.

Dopo che la CPU del modulo Supervisor ha inviato un messaggio di reindirizzamento ICMP all'origine, completa la gestione delle eccezioni inoltrando il pacchetto di dati all'hop successivo tramite il modulo della scheda di linea in uscita.

Mentre i moduli Supervisor Nexus 7000 utilizzano potenti processori CPU in grado di elaborare grandi volumi di traffico, la piattaforma è progettata per gestire la maggior parte del traffico di dati a livello di scheda di linea senza la necessità di coinvolgere il processore CPU Supervisor nel processo di inoltro dei pacchetti. Ciò consente alla CPU di concentrarsi sulle attività principali e lascia l'operazione di inoltro dei pacchetti a motori hardware dedicati sulle schede di linea.

Nelle reti stabili, si prevede che le eccezioni di inoltro dei pacchetti, se si verificano, si verifichino a velocità ragionevolmente basse. Con questo presupposto, possono essere gestite dalla CPU Supervisor senza un impatto significativo sulle prestazioni. D'altra parte, una CPU che gestisce le eccezioni di inoltro dei pacchetti che si verificano ad una velocità molto elevata può avere un effetto negativo sulla stabilità e sulla velocità di risposta globali del sistema.

La progettazione della piattaforma Nexus 7000 fornisce una serie di meccanismi per proteggere la CPU dello switch da quantità significative di traffico. Questi meccanismi vengono applicati in punti diversi del sistema. A livello di scheda di linea, sono disponibili limitatori di velocità hardware e Control Plane Policing (CoPP). Entrambe impostano le soglie di velocità del traffico, che controllano in modo efficace la quantità di traffico da inoltrare al Supervisor da ciascun modulo di scheda di linea.

Questi meccanismi di protezione danno la preferenza al traffico di vari protocolli di controllo che sono critici per la stabilità della rete e la gestibilità dello switch, come OSPF, BGP o SSH, e allo stesso tempo filtrano in modo aggressivo i tipi di traffico che non sono critici per il controllo della funzionalità del piano dello switch. La maggior parte del traffico di dati, se inoltrato alla CPU come risultato di eccezioni di inoltro dei pacchetti, è fortemente controllato da tali meccanismi.

Mentre i limitatori di velocità hardware e il policing i meccanismi garantiscono la stabilità del control plane dello switch e si consiglia di abilitarli sempre. Questi meccanismi possono essere una delle cause principali delle perdite di pacchetti di dati, dei ritardi di trasferimento e, in generale, delle prestazioni insoddisfacenti delle applicazioni in rete. Ecco perché è importante comprendere i percorsi usati dai flussi di traffico attraverso la rete e l'uso di strumenti per monitorare le apparecchiature di rete che possono e/o devono usare la funzionalità ICMP Redirect.

Strumenti per monitorare e diagnosticare il traffico

show ip traffic

Sia il software Cisco IOS che Cisco NX-OS consentono di controllare le statistiche del traffico gestito dalla CPU. Questa operazione viene eseguita con **show ip traffic** Questo comando può essere usato per verificare la ricezione e/o la generazione di messaggi di reindirizzamento ICMP da parte dello switch di layer 3 o del 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#
```

Lanciare show ip traffic del reindirizzamento ICMP e verificare se i contatori di reindirizzamento ICMP vengono incrementati.

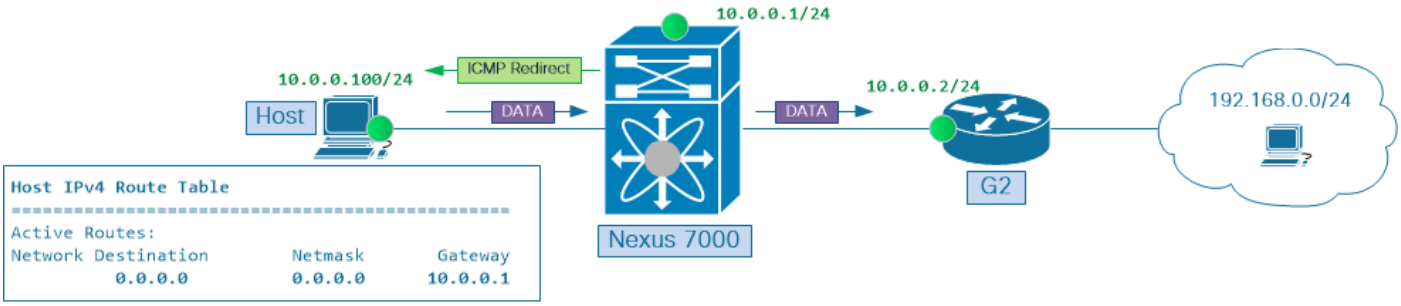
Etanalizzatore

Il software Cisco NX-OS è dotato di uno strumento integrato per l'acquisizione del traffico flowing alla e dalla CPU dello switch, nota come Ethanalyzer.

> **Nota:** Per ulteriori informazioni su Ethanalyzer, consultare la guida alla risoluzione dei problemi di Ethanalyzer su Nexus 7000.

La Figura 6 mostra uno scenario simile a quello della Figura 3. In questo caso, la rete X è sostituita dalla rete 192.168.0.0/24.

Figura 6 Esecuzione di Ethanalyzer Capture



Esegui acquisizione Ethanalyzer

L'host 10.0.0.100 invia un flusso continuo di richieste echo ICMP all'indirizzo IP di destinazione 192.168.0.1. L'host utilizza l'interfaccia virtuale dello switch (SVI) 10 di Nexus 7000 come hop successivo sulla rete remota 192.168.0.0/24. A scopo dimostrativo, l'host è configurato in modo da ignorare i messaggi di reindirizzamento ICMP.

Utilizzare questo comando per acquisire il traffico ICMP ricevuto e inviato dalla CPU Nexus 7000:

```
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

...
```

L'indicatore orario nell'output precedente suggerisce che tre pacchetti evidenziati in questo esempio sono stati acquisiti contemporaneamente, 2018-09-15 23:45:40.128. Il successivo è un'analisi stratificata per pacchetto di questo gruppo di pacchetti

- Il primo pacchetto è il pacchetto dati in entrata, che in questo esempio è una richiesta Echo ICMP.

  2018-09-15 23:45:40.128348 10.0.0.100 -> Richiesta echo (ping) 192.168.0.1 ICMP

- Il secondo pacchetto è un pacchetto di reindirizzamento ICMP, generato dal gateway. Il pacchetto viene rimandato all'host.

2018-09-15 23:45:40.128611 10.0.0.1 -> Reindirizzamento ICMP 10.0.0.100 (reindirizzamento per l'host)

- Il terzo pacchetto è il pacchetto dati acquisito in direzione di uscita, dopo essere stato instradato dalla CPU. Anche se non mostrata in precedenza, il valore TTL IP di questo pacchetto è diminuito e il checksum è stato ricalcolato.
  2018-09-15 23:45:40.128659 10.0.0.100 -> Richiesta echo (ping) 192.168.0.1 ICMP

Mentre si naviga attraverso grandi acquisizioni Ethanalyzer che hanno molti pacchetti di tipi e flussi diversi, può essere difficile correlare i messaggi ICMP Redirect con il traffico di dati che a essi corrisponde.

In queste situazioni, è consigliabile concentrarsi sui messaggi di reindirizzamento ICMP per recuperare le informazioni sui flussi di traffico inoltrati in modo non ottimale. I messaggi di reindirizzamento ICMP includono l'intestazione Internet più i primi 64 bit dei dati del datagramma originale. Questi dati vengono utilizzati dall'origine del datagramma per far corrispondere il messaggio al processo appropriato.

Usare lo strumento di acquisizione dei pacchetti Ethanalyzer con la parola chiave **detail** per visualizzare il contenuto dei messaggi di reindirizzamento ICMP e trovare le informazioni sull'indirizzo IP del flusso di dati inoltrato in modo non ottimale

```
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)

...
```

Disabilita reindirizzamenti ICMP

Se la progettazione della rete richiede che il flusso del traffico venga indirizzato dall'interfaccia di layer 3 su cui è stato immesso nello switch o nel router, è possibile impedire che il flusso venga indirizzato attraverso la CPU se si disabilita la funzionalità di reindirizzamento ICMP sull'interfaccia di layer 3 corrispondente.

Di fatto, per la maggior parte delle reti è buona norma disabilitare proattivamente i reindirizzamenti ICMP su tutte le interfacce di layer 3, sia fisiche, come l'interfaccia Ethernet, che virtuali, come le interfacce Port-Channel e SVI. Utilizzare il no ip redirects Comando a livello di interfaccia Cisco NX-OS per disabilitare i reindirizzamenti ICMP su un'interfaccia di layer 3. Per verificare che la funzionalità di reindirizzamento ICMP sia disabilitata:

- Garantire**no ip** il comando **redirects** viene aggiunto alla configurazione dell'interfaccia.

```
Nexus7000#show run interface vlan 10

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

- Verificare che lo stato dei reindirizzamenti ICMP sull'interfaccia sia "disabled".

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

- Verificare che il flag di abilitazione/disabilitazione del reindirizzamento ICMP sia impostato su **0** dal componente software Cisco NX-OS che trasferisce la configurazione dell'interfaccia dal Supervisor dello switch a una o più schede di linea.

```
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
```

- Verificare che il flag di abilitazione/disabilitazione del reindirizzamento ICMP per una particolare interfaccia di layer 3 sia impostato su **0** su una o più schede di linea.

```
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
```

Riepilogo

Il meccanismo di reindirizzamento ICMP, descritto nella RFC 792, è stato progettato per ottimizzare il percorso di inoltro attraverso i segmenti di rete multipunto. All'inizio di Internet, questa ottimizzazione ha contribuito a proteggere risorse di rete costose, come la larghezza di banda dei collegamenti e i cicli della CPU dei router. Con l'aumento dei costi della larghezza di banda della rete e la relativa lentezza del routing dei pacchetti basato sulla CPU, che si è evoluto in un inoltro più rapido dei pacchetti di layer 3 negli ASIC hardware dedicati, l'importanza di un transito ottimale dei dati attraverso i segmenti di rete multipunto è diminuita. Per impostazione predefinita, la funzionalità di reindirizzamento ICMP è abilitata su ogni interfaccia di layer 3. Tuttavia, i suoi tentativi di notificare ai nodi di rete su segmenti Ethernet multipunto i percorsi di inoltro ottimali non sono sempre compresi ed eseguiti dal personale di rete. Nelle reti con l'uso combinato di vari meccanismi di inoltro, come il routing statico, il routing dinamico e il routing basato su criteri, se si lascia abilitata la funzionalità di reindirizzamento ICMP e non la si controlla correttamente, potrebbe verificarsi un uso indesiderato della CPU dei nodi di transito per gestire il traffico di produzione. Ciò, a sua volta, può causare un impatto significativo sia sui flussi di traffico di produzione che sulla stabilità del control plane dell'infrastruttura di rete.

Per la maggior parte delle reti, è buona norma disabilitare proattivamente la funzionalità di reindirizzamento ICMP su tutte le interfacce di layer 3 dell'infrastruttura di rete. Questo aiuta a prevenire scenari di traffico dei dati di produzione che viene gestito nella CPU degli switch e dei router di layer 3 quando c'è un miglior percorso di inoltro attraverso segmenti di rete multipunto.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).