

# Risoluzione dei problemi relativi a Network Address Translation con le domande frequenti

## Sommario

[Introduzione](#)

[NAT generico](#)

[D. Che cos'è NAT?](#)

[D. Come funziona NAT?](#)

[D. Come configurare NAT?](#)

[D. Quali sono le differenze principali tra le implementazioni del software Cisco IOS® e delle appliance Cisco Adaptive Security \(ASA\) di NAT?](#)

[D. Su quale hardware di routing Cisco è disponibile Cisco IOS NAT? Come si può ordinare l'hardware?](#)

[D. Il NAT si verifica prima o dopo il routing?](#)

[D. È possibile installare NAT in un ambiente LAN wireless pubblico?](#)

[D. NAT esegue il bilanciamento del carico TCP per i server sulla rete interna?](#)

[D. Posso limitare il numero di traduzioni NAT?](#)

[D. In che modo viene appreso o propagato il routing per le subnet IP o gli indirizzi utilizzati da NAT?](#)

[D. Quante sessioni NAT simultanee sono supportate in Cisco IOS NAT?](#)

[D. Che tipo di prestazioni di routing ci si può aspettare con Cisco IOS NAT?](#)

[D. È possibile applicare Cisco IOS NAT alle sottointerfacce?](#)

[D. È possibile utilizzare Cisco IOS NAT con il protocollo HSRP \(Hot Standby Router Protocol\) per fornire collegamenti ridondanti a un ISP?](#)

[D. Cisco IOS NAT supporta le traduzioni in entrata su un'interfaccia Frame Relay? Supporta le conversioni in uscita sul lato Ethernet?](#)

[D. Un singolo router abilitato NAT può consentire ad alcuni utenti di utilizzare NAT e ad altri utenti sulla stessa interfaccia Ethernet di continuare a utilizzare i propri indirizzi IP?](#)

[D. Quando PAT \(sovraccarico\) è configurato, qual è il numero massimo di traduzioni che possono essere create per ogni indirizzo IP globale interno?](#)

[D. Come funziona PAT?](#)

[D. Cosa sono i pool IP NAT?](#)

[D. Qual è il numero massimo di pool IP NAT configurabili \(ip nat "name"\)?](#)

[D. Qual è il vantaggio di route-map rispetto ad ACL su un pool NAT?](#)

[D. In che modo l'indirizzo IP "si sovrappone" nel contesto di NAT?](#)

[D. Cosa sono le traduzioni NAT statiche?](#)

[D. Cosa si intende per sovraccarico NAT? Si tratta di PAT?](#)

[D. Cosa sono le traduzioni NAT dinamiche?](#)

[D. Che cos'è ALG?](#)

[D. È possibile creare una configurazione con traduzioni NAT sia statiche che dinamiche?](#)

[D. Quando si esegue un traceroute tramite un router NAT, il traceroute deve mostrare l'indirizzo NAT-Globale o deve perdere l'indirizzo NAT-Locale?](#)

[D. In che modo PAT alloca la porta?](#)

[D. Qual è la differenza tra frammentazione IP e segmentazione TCP?](#)

D. Il protocollo NAT supporta la frammentazione IP e la segmentazione TCP in modo non corretto?

D. Come eseguire il debug della frammentazione IP e della segmentazione TCP?

D. È disponibile un MIB NAT supportato?

D. Che cos'è il timeout TCP e come si relaziona al timer TCP NAT?

D. È possibile modificare la quantità di tempo necessaria per una traduzione NAT in modo che scada dalla tabella di conversione NAT?

D. Come arrestare il protocollo LDAP (Lightweight Directory Access Protocol) quando allega byte aggiuntivi a ciascun pacchetto di risposta LDAP?

D. Qual è il percorso consigliato per l'indirizzo IP locale globale/esterno interno nella casella NAT?

D. Cisco IOS NAT supporta gli ACL con una parola chiave log?

#### Voice-NAT

D. NAT supporta Skinny Client Control Protocol (SCCP) v17 fornito con Cisco Unified Communications Manager (CUCM) V7?

D. Quali versioni di caricamento CUCM/SCCP/firmware sono supportate da NAT?

D. In cosa consiste il miglioramento dell'allocazione delle porte PAT del provider di servizi per RTP e RTCP?

D. Che cos'è il protocollo SIP (Session Initiation Protocol) e possono essere indirizzati pacchetti SIP con NAT?

D. In cosa consiste il supporto Hosted NAT Traversal per Session Border Controller (SBC)?

D. Quante chiamate SIP, Skinny e H323 possono gestire la memoria e la CPU di un router con NAT?

D. Un router NAT supporta la segmentazione TCP dei pacchetti Skinny e H323?

D. Ci sono avvertenze da tenere in considerazione quando si utilizza una configurazione di sovraccarico NAT in un'implementazione vocale?

D. Vi sono problemi noti causati quando si usa il comando clear ip nat trans \*o il comando clear ip nat trans in un'implementazione vocale?

D. La tecnologia NAT supporta la soluzione di voice-co-location?

D. Il protocollo NVI supporta Skinny ALG, H323 ALG e TCP SIP ALG?

#### NAT con VRF/MPLS

D. È possibile che un router NAT si supporti nello stesso spazio di indirizzi di un VRF e di uno spazio di indirizzi globale? Al momento, viene visualizzato il seguente messaggio di avviso: "% like static entry (10.1.1.1 —> 10.2.2.2) existing" quando si tenta di configurare il seguente:

D. La tecnologia NAT legacy supporta VRF-Lite (il percorso da un VRF a un VRF diverso)?

#### NAT NVI

D. Che cos'è NAT NVI?

D. È necessario utilizzare NAT NVI per effettuare il routing tra un'interfaccia in modalità globale e un'interfaccia in una VRF?

D. La segmentazione TCP per NAT-NVI è supportata?

D. Il protocollo NVI supporta Skinny ALG, H323 ALG e TCP SIP ALG?

D. La segmentazione TCP è supportata con SNAT?

#### SNAT

D. Che cos'è il protocollo stateful NAT (SNAT)?

D. La segmentazione TCP è supportata con SNAT?

D. La tecnologia SNAT è supportata per il routing asimmetrico?

#### NAT-PT (da v6 a v4)

D. Che cos'è NAT-PT?

[D. Il protocollo NAT-PT è supportato nel percorso CEF \(Cisco Express Forwarding\)?](#)

[D. Quali ALG sono supportati in NAT-PT?](#)

[D. ASR 1004 supporta NAT-PT?](#)

[Cisco 7600/6k dipendente dalla piattaforma](#)

[D. La tecnologia Stateful NAT \(SNAT\) è disponibile su Catalyst 6500 sul treno SX?](#)

[D. NAT con riconoscimento VRF è supportato nell'hardware su 6k?](#)

[D. I modelli 7600 e Cat6000 supportano NAT con riconoscimento VRF?](#)

[Cisco 850 Dipendente Dalla Piattaforma](#)

[D. Cisco 850 supporta Skinny NAT ALG nella versione 12.4T?](#)

[Distribuzione NAT](#)

[D. Come implementare NAT?](#)

[D. Come implementare NAT con la voce?](#)

[D. Come integrare NAT con VPN MPLS?](#)

[D. La mappatura statica NAT supporta HSRP per l'alta disponibilità?](#)

[D. Come implementare NAT NVI?](#)

[D. Come implementare il bilanciamento del carico con NAT?](#)

[D. Come implementare NAT in combinazione con IPSec?](#)

[D. Come implementare NAT-PT?](#)

[D. Come implementare un NAT multicast?](#)

[D. Come implementare un NAT stateful \(SNAT\)?](#)

[Best practice NAT](#)

[D. Esistono best practice NAT?](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive il funzionamento del processo del router Network Address Translation (NAT) e fornisce le risposte ad alcune domande frequenti.

## NAT generico

### D. Che cos'è NAT?

R. Network Address Translation (NAT) è progettato per la conservazione degli indirizzi IP. Consente alle reti IP private che utilizzano indirizzi IP non registrati di connettersi a Internet. Il protocollo NAT funziona su un router, in genere quando si connettono due reti tra loro, e converte gli indirizzi privati (non globalmente univoci) della rete interna in indirizzi legali, prima che i pacchetti vengano inoltrati a un'altra rete.

Come parte di questa funzionalità, NAT può essere configurato per annunciare un solo indirizzo per l'intera rete al mondo esterno. In questo modo l'intera rete interna viene nascosta dietro l'indirizzo che fornisce ulteriore sicurezza. NAT offre la doppia funzione di protezione e conservazione degli indirizzi ed è generalmente implementata in ambienti di accesso remoto.

### D. Come funziona NAT?

R.Fondamentalmente, il protocollo NAT consente a un singolo dispositivo, ad esempio un router, di fungere da agente tra Internet (o rete pubblica) e una rete locale (o rete privata), il che significa che è necessario un solo indirizzo IP univoco per rappresentare un intero gruppo di computer per qualsiasi elemento esterno alla rete.

## D. Come configurare NAT?

A.Per configurare il protocollo NAT tradizionale, è necessario configurare almeno un'interfaccia su un router (esterno NAT) e un'altra interfaccia sul router (interno NAT) e un insieme di regole di conversione per gli indirizzi IP nelle intestazioni dei pacchetti (e nei payload, se lo si desidera). Per configurare l'interfaccia virtuale Nat (NVI), è necessario configurare almeno un'interfaccia con NAT enable e lo stesso gruppo di regole menzionate sopra.

Per ulteriori informazioni, fare riferimento [alla Guida alla configurazione di Cisco IOS IP Addressing Services](#) o alla relativa sezione [sulla configurazione dell'interfaccia virtuale NAT](#).

## D. Quali sono le differenze principali tra le implementazioni del software Cisco IOS® e delle appliance Cisco Adaptive Security (ASA) di NAT?

A.Cisco IOS basato su software non è fondamentalmente diverso dalla funzione NAT nell'appliance Cisco ASA. Le principali differenze includono i diversi tipi di traffico supportati nelle implementazioni e i requisiti di progettazione. Per ulteriori informazioni sulla configurazione di NAT sui dispositivi Cisco ASA (inclusi i tipi di traffico supportati), fare riferimento [agli](#) esempi di configurazione NAT.

## D. Su quale hardware di routing Cisco è disponibile Cisco IOS NAT? Come si può ordinare l'hardware?

R. Lo strumento Cisco Feature Navigator consente ai clienti di identificare una funzionalità (NAT) e di individuare la versione e l'hardware in cui è disponibile questa funzionalità software di Cisco IOS. Per utilizzare questo strumento, consultare [Cisco Feature Navigator](#).

## D. Il NAT si verifica prima o dopo il routing?

A.L'ordine in cui NAT elabora le transazioni si basa sul fatto che un pacchetto viaggi dalla rete interna alla rete esterna o dalla rete esterna alla rete interna. La traslazione dall'interno all'esterno si verifica dopo la stesura e la traslazione dall'esterno all'interno prima della stesura. Per ulteriori informazioni, fare riferimento [all'ordine di funzionamento NAT](#).

## D. È possibile installare NAT in un ambiente LAN wireless pubblico?

R.Sì. La funzione NAT - Supporto IP statico fornisce supporto agli utenti con indirizzi IP statici e consente loro di stabilire una sessione IP in un ambiente LAN wireless pubblico.

## D. NAT esegue il bilanciamento del carico TCP per i server sulla rete interna?

R.Sì. con NAT, è possibile stabilire un host virtuale nella rete interna che coordina i bilanciamenti del carico tra gli host reali.

## D. Posso limitare il numero di traduzioni NAT?

R.Sì. La funzione di conversione NAT per la limitazione della velocità consente di limitare il numero massimo di operazioni NAT simultanee su un router. In questo modo gli utenti hanno un maggiore controllo su come vengono utilizzati gli indirizzi NAT. La funzione di conversione NAT con limitazione della velocità può essere utilizzata per limitare gli effetti di virus, worm e attacchi Denial of Service.

## D. In che modo viene appreso o propagato il routing per le subnet IP o gli indirizzi utilizzati da NAT?

A.Routing per indirizzi IP creati da NAT viene appreso se:

- Il pool di indirizzi globale interno deriva dalla subnet di un router dell'hop successivo.
- La voce del percorso statico viene configurata nel router dell'hop successivo e ridistribuita nella rete di routing.

Quando l'indirizzo globale interno corrisponde all'interfaccia locale, NAT installa un alias IP e una voce ARP, nel qual caso il router **può proxy-arp** per questi indirizzi. Se questo comportamento non è desiderato, utilizzare la parola chiave **no-alias**.

Quando si configura un pool NAT, l'opzione **add-route** può essere utilizzata per l'inserimento automatico della route.

## D. Quante sessioni NAT simultanee sono supportate in Cisco IOS NAT?

A.Il limite di sessione NAT è limitato dalla quantità di DRAM disponibile nel router. Ogni traduzione NAT consuma circa 312 byte in DRAM. Di conseguenza, 10.000 traduzioni (più di quelle che verrebbero generalmente gestite su un singolo router) consumano circa 3 MB. Pertanto, l'hardware di routing tipico dispone di una quantità di memoria più che sufficiente per supportare migliaia di traduzioni NAT. Tuttavia, si consiglia anche di verificare le specifiche della piattaforma.

## D. Che tipo di prestazioni di routing ci si può aspettare con Cisco IOS NAT?

A.Cisco IOS NAT supporta la commutazione Cisco Express Forwarding (CEF), la commutazione rapida e la commutazione di contesto. Nella versione 12.4T e successive, il percorso di commutazione veloce non è più supportato. Per la piattaforma Cat6k, l'ordine di commutazione è NetFlow (percorso di commutazione hardware), CEF, percorso di processo.

Le prestazioni dipendono da diversi fattori:

- Tipo di applicazione e relativo tipo di traffico
- Se gli indirizzi IP sono incorporati
- Scambio e controllo di più messaggi
- Porta di origine obbligatoria
- Numero di traduzioni
- Altre applicazioni in esecuzione in quel momento
- Il tipo di hardware e processore

## D. È possibile applicare Cisco IOS NAT alle sottointerfacce?

**R.Sì.** Le traduzioni NAT di origine e/o destinazione possono essere applicate a qualsiasi interfaccia o sottointerfaccia con un indirizzo IP (incluse le interfacce dialer). Impossibile configurare NAT con l'interfaccia virtuale wireless. L'interfaccia virtuale wireless non esiste al momento della scrittura nella NVRAM. Pertanto, dopo il riavvio, il router perde la configurazione NAT sull'interfaccia virtuale wireless.

**D. È possibile utilizzare Cisco IOS NAT con il protocollo HSRP (Hot Standby Router Protocol) per fornire collegamenti ridondanti a un ISP?**

**R.Sì.** NAT fornisce HSRP ridondante. Tuttavia, è diverso da SNAT (Stateful NAT). NAT con HSRP è un sistema senza stato. La sessione corrente non viene mantenuta quando si verifica un errore. Durante la configurazione NAT statica (quando un pacchetto non corrisponde ad alcuna configurazione delle regole STATICHE), il pacchetto viene inviato tramite senza alcuna conversione.

**D. Cisco IOS NAT supporta le traduzioni in entrata su un'interfaccia Frame Relay? Supporta le conversioni in uscita sul lato Ethernet?**

**R.Sì.** L'incapsulamento non è importante per NAT. Il protocollo NAT può essere eseguito quando sull'interfaccia è presente un indirizzo IP e l'interfaccia è NAT all'interno o NAT all'esterno. Per il funzionamento di NAT è necessario che siano presenti un interno e un esterno. Se si utilizza NVI, deve essere presente almeno un'interfaccia abilitata NAT. Per ulteriori informazioni, vedere la domanda precedente ["Come configurare NAT?"](#).

**D. Un singolo router abilitato NAT può consentire ad alcuni utenti di utilizzare NAT e ad altri utenti sulla stessa interfaccia Ethernet di continuare a utilizzare i propri indirizzi IP?**

**R.Sì.** A tale scopo, è possibile utilizzare un elenco degli accessi che descrive il set di host o reti che richiedono NAT. Tutte le sessioni sullo stesso host possono essere tradotte o passare attraverso il router ma non possono essere tradotte.

Gli elenchi degli accessi, gli elenchi degli accessi estesi e le route map possono essere utilizzati per definire le regole di conversione dei dispositivi IP. È necessario specificare sempre l'indirizzo di rete e la subnet mask appropriata. La parola chiave anynon deve essere usata in sostituzione dell'indirizzo di rete o della subnet mask. Con la configurazione NAT statica, quando il pacchetto non corrisponde ad alcuna configurazione della regola STATICA, il pacchetto può essere inviato tramite senza alcuna conversione.

**D. Quando PAT (sovraccarico) è configurato, qual è il numero massimo di traduzioni che possono essere create per ogni indirizzo IP globale interno?**

**A.PAT (overload)** divide le porte disponibili per indirizzo IP globale in tre intervalli: 0-511, 512-1023 e 1024-65535. PAT assegna una porta di origine univoca per ciascuna sessione UDP o TCP. Tenta di assegnare lo stesso valore di porta della richiesta originale, ma se la porta di origine originale è già stata utilizzata, inizia la scansione dall'inizio dell'intervallo di porte specifico per trovare la prima porta disponibile e la assegna alla conversazione.

**D. Come funziona PAT?**

A.PAT funziona con uno o più indirizzi IP globali.

## PAT con una tabella di indirizzi IP

### Condizione Descrizione

- 1 NAT/PAT controlla il traffico e lo associa a una regola di traduzione.
- 2 La regola corrisponde a una configurazione PAT.
- 3 Se PAT è a conoscenza del tipo di traffico e dispone di "un insieme di porte specifiche che negozia" che può utilizzare, PAT le imposta da parte e non le assegna come identificatori univoci.
- 4 Se una sessione senza requisiti speciali della porta tenta di stabilire una connessione, PAT converte l'indirizzo di origine IP e controlla la disponibilità della porta di origine (ad esempio, 4000). Vedere la **nota**.
- 5 Se la porta di origine richiesta è disponibile, PAT assegna la porta di origine e la sessione continua.
- 6 Se la porta di origine richiesta non è disponibile, PAT inizia la ricerca dall'inizio del gruppo pertinente (inizia da 1 per le applicazioni TCP o UDP e da 0 per ICMP).
- 7 Se una porta è disponibile, viene assegnata e la sessione continua.
- 8 Se non sono disponibili porte, il pacchetto viene scartato.

**Nota:** per i protocolli TCP (Transmission Control Protocol) e UDP (User Datagram Protocol), gli intervalli sono: 1-511, 512-1023, 1024-65535. Per il protocollo ICMP (Internet Control Message Protocol), il primo gruppo inizia da 0.

## PAT con più indirizzi IP

### Condizione Descrizione

- 1-7 Le prime sette condizioni sono le stesse di un singolo indirizzo IP.
- 8 Se nel gruppo corrispondente al primo indirizzo IP non sono disponibili porte, NAT passa all'indirizzo IP successivo nel pool e tenta di allocare la porta di origine richiesta.
- 9 Se la porta di origine richiesta è disponibile, NAT assegna la porta di origine e la sessione continua.
- 10 Se la porta di origine richiesta non è disponibile, NAT inizia la ricerca dall'inizio del gruppo pertinente (inizia da 1 per le applicazioni TCP o UDP e da 0 per ICMP).
- 11 Se una porta è disponibile, viene assegnata e la sessione continua.
- 12 Se non sono disponibili porte, il pacchetto viene scartato, a meno che nel pool non sia disponibile un altro indirizzo IP.

## D. Cosa sono i pool IP NAT?

I pool IP A.NAT sono un intervallo di indirizzi IP allocati per la traduzione NAT in base alle esigenze. Per definire un pool, viene utilizzato il comando di configurazione:

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

### Esempio 1

Nell'esempio seguente viene eseguita la conversione tra gli host interni indirizzati dalla rete 192.168.1.0 o 192.168.2.0 e la rete 10.69.233.208/28, univoca a livello globale:

```

ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

```

## Esempio 2

Nell'esempio successivo, l'obiettivo è quello di definire un indirizzo virtuale, le cui connessioni vengono distribuite tra un set di host reali. Il pool definisce gli indirizzi degli host reali. L'elenco degli accessi definisce l'indirizzo virtuale. Se non esiste ancora una conversione, i pacchetti TCP dell'interfaccia seriale 0 (l'interfaccia esterna) la cui destinazione corrisponde all'elenco degli accessi vengono convertiti in un indirizzo del pool.

```

ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1

```

## D. Qual è il numero massimo di pool IP NAT configurabili (ip nat "name")?

R. Nell'uso pratico, il numero massimo di pool IP configurabili è limitato dalla quantità di DRAM disponibile sul router in questione. (Cisco consiglia di configurare una dimensione di pool di 255.) Ogni pool non deve essere più lungo di 16 bit. Nella versione 12.4(11)T e successive, Cisco IOS ha introdotto il CCE (Common Classification Engine). Ciò ha limitato NAT a un massimo di 255 pool.

## D. Qual è il vantaggio di route-map rispetto ad ACL su un pool NAT?

A. A route-map protegge gli utenti esterni indesiderati da raggiungere agli utenti/server interni. Consente inoltre di mappare un singolo indirizzo IP interno a diversi indirizzi globali interni in base alla regola. Per ulteriori informazioni, fare riferimento [al supporto NAT per più pool che utilizzano le mappe route](#).

## D. In che modo l'indirizzo IP "si sovrappone" nel contesto di NAT?

La sovrapposizione di indirizzi IP A.IP si riferisce a una situazione in cui due percorsi che desiderano interconnettersi utilizzano lo stesso schema di indirizzi IP. Non si tratta di un evento insolito, ma si verifica spesso quando le aziende si fondono o vengono acquisite. Senza un supporto speciale, le due sedi non possono connettersi e stabilire sessioni. L'indirizzo IP

sovrapposto può essere un indirizzo pubblico assegnato a un'altra società, un indirizzo privato assegnato a un'altra società o derivare dall'intervallo di indirizzi privati definito [nella RFC 1918](#).

Gli indirizzi IP privati non sono instradabili e richiedono traduzioni NAT per consentire le connessioni con il mondo esterno. La soluzione prevede l'intercettazione delle risposte alle query dei nomi DNS (Domain Name System) dall'esterno verso l'interno, una configurazione di conversione per l'indirizzo esterno e la correzione della risposta DNS prima dell'inoltro all'host interno. È necessario che un server DNS sia coinvolto su entrambi i lati del dispositivo NAT per risolvere gli utenti che desiderano avere una connessione tra entrambe le reti.

NAT è in grado di ispezionare ed eseguire la traduzione degli indirizzi sul contenuto dei record DNS e PTR, come mostrato [in Utilizzo di NAT in reti sovrapposte](#).

## D. Cosa sono le traduzioni NAT statiche?

Le traduzioni NAT statiche A.000 dispongono di un mapping uno-a-uno tra indirizzi locali e globali. Gli utenti possono inoltre configurare le conversioni degli indirizzi statici a livello di porta e utilizzare la parte restante dell'indirizzo IP per altre conversioni. Ciò si verifica in genere quando si esegue Port Address Translation (PAT).

Nell'esempio seguente viene mostrato come configurare la mappa dei percorsi per consentire la traduzione da esterno a interno per un NAT statico:

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

## D. Cosa si intende per *sovraccarico NAT*; è questo PAT?

R.Sì. Il sovraccarico NAT è PAT, che implica l'uso di un pool con un intervallo di uno o più indirizzi o l'uso di un indirizzo IP di interfaccia in combinazione con la porta. Quando sovraccaricate, create una traslazione completamente estesa. Questa è una voce della tabella di conversione che contiene informazioni sull'indirizzo IP e sulla porta di origine/destinazione, comunemente denominata PAT o overload.

Il PAT (o overload) è una funzionalità di Cisco IOS NAT che viene utilizzata per *tradurre* gli indirizzi privati *interni* (locali interni) in uno o *più indirizzi IP esterni* (interni globali, generalmente registrati). Numeri di porta di origine univoci in ogni traduzione vengono utilizzati per distinguere le conversazioni.

## D. Cosa sono le traduzioni NAT dinamiche?

R. Nelle traduzioni NAT dinamiche, gli utenti possono stabilire una mappatura dinamica tra indirizzi locali e globali. Il mapping dinamico viene eseguito quando si definiscono gli indirizzi locali da convertire e il pool di indirizzi o di indirizzi IP di interfaccia da cui allocare gli indirizzi globali e quando si associano i due indirizzi.

## D. Che cos'è ALG?

**A.**ALG è un ALG (Application Layer Gateway). NAT esegue il servizio di traduzione su qualsiasi traffico TCP/UDP (Transmission Control Protocol/User Datagram Protocol) che non trasporta indirizzi IP di origine e/o destinazione nel flusso di dati dell'applicazione.

Questi protocolli includono FTP, HTTP, SKINNY, H323, DNS, RAS, SIP, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh, rcp. I protocolli specifici che incorporano le informazioni sull'indirizzo IP nel payload richiedono il supporto di un ALG (Application Level Gateway).

Per ulteriori informazioni, fare riferimento [a Utilizzo di gateway a livello di applicazione con NAT](#).

## **D. È possibile creare una configurazione con traduzioni NAT sia statiche che dinamiche?**

**R.**Sì. Tuttavia, lo stesso indirizzo IP non può essere utilizzato per la configurazione statica NAT o nel pool per la configurazione dinamica NAT. Tutti gli indirizzi IP pubblici devono essere univoci. Si noti che gli indirizzi globali utilizzati nelle traduzioni statiche non vengono automaticamente esclusi con i pool dinamici che contengono gli stessi indirizzi globali. È necessario creare pool dinamici per escludere gli indirizzi assegnati da voci statiche. Per ulteriori informazioni, fare riferimento [alla sezione Configurazione simultanea di NAT statico e dinamico](#).

## **D. Quando si esegue un traceroute tramite un router NAT, il traceroute deve mostrare l'indirizzo NAT-Globale o deve perdere l'indirizzo NAT-Locale?**

**A.**Traceroute dall'esterno deve sempre restituire l'indirizzo globale.

## **D. In che modo PAT alloca la porta?**

**A.**NAT introduce funzionalità aggiuntive per le porte: full-range e port-map.

- La funzionalità full-range consente a NAT di utilizzare tutte le porte indipendentemente dal relativo intervallo di porte predefinito.
- Port-map consente a NAT di riservare un intervallo di porte definito dall'utente per un'applicazione specifica.

Per ulteriori informazioni, [fare riferimento a Intervalli di porte di origine definite dall'utente](#).

Nella versione 12.4(20)T2 in poi, NAT introduce la randomizzazione delle porte per L3/L4 e porta simmetrica.

- L'assegnazione casuale delle porte consente a NAT di selezionare in modo casuale qualsiasi porta globale per la richiesta della porta di origine.
- La porta simmetrica consente a NAT di *supportare l'endpoint in modo indipendente*.

## **D. Qual è la differenza tra frammentazione IP e segmentazione TCP?**

**La frammentazione A.IP** avviene sul layer 3 (IP), la segmentazione TCP sul layer 4 (TCP). La frammentazione IP ha luogo quando i pacchetti più grandi della MTU (Maximum Transmission Unit) di un'interfaccia vengono inviati fuori da questa interfaccia. Quando si invia il pacchetto all'interfaccia, il pacchetto deve essere frammentato o scartato. Se il Don't Fragment (DF) bit non è impostato nell'intestazione IP del pacchetto, il pacchetto può essere frammentato. Se il bit DF è impostato nell'intestazione IP del pacchetto, il pacchetto viene scartato e un messaggio di errore

ICMP indica il valore MTU dell'hop successivo restituito al mittente. Tutti i frammenti di un pacchetto IP hanno lo stesso ID nell'intestazione IP, che consente al destinatario finale di ricomporre i frammenti nel pacchetto IP originale. per ulteriori informazioni, fare riferimento a [Risoluzione dei problemi di IP Fragmentation, MTU, MSS e PMTUD con GRE e IPsec](#).

La segmentazione TCP ha luogo quando un'applicazione su una stazione terminale invia dati. I dati dell'applicazione vengono suddivisi in quelli che TCP considera i blocchi di dimensioni migliori da inviare. L'unità di dati passata da TCP a IP viene definita segmento. I segmenti TCP vengono inviati in datagrammi IP. Questi datagrammi IP possono quindi diventare frammenti IP mentre attraversano la rete e incontrano collegamenti MTU inferiori a quelli che possono attraversare.

Il protocollo TCP può segmentare prima questi dati in segmenti TCP (in base al valore TCP MSS), aggiungere l'intestazione TCP e passare questo segmento TCP all'indirizzo IP. Quindi IP può aggiungere un'intestazione IP per inviare il pacchetto all'host remoto. Se il pacchetto IP con il segmento TCP è più grande dell'MTU IP su un'interfaccia in uscita sul percorso tra gli host TCP, l'IP può frammentare il pacchetto IP/TCP per adattarlo. Questi frammenti di pacchetto IP possono essere ricomposti sull'host remoto dal layer IP e il segmento TCP completo (originariamente inviato) può essere consegnato al layer TCP. Il layer TCP non ha idea che l'IP abbia frammentato il pacchetto durante il transito.

NAT supporta i frammenti IP, ma non i segmenti TCP.

## **D. Il protocollo NAT supporta la frammentazione IP e la segmentazione TCP in modo non corretto?**

A.NAT supporta solo frammenti IP non ordinati a causa del **riassembaggio virtuale ofip**.

## **D. Come eseguire il debug della frammentazione IP e della segmentazione TCP?**

A.NAT utilizza la stessa CLI di debug sia per la frammentazione IP che per la segmentazione TCP:**debug ip nat frag**.

## **D. È disponibile un MIB NAT supportato?**

R.No. Non è supportato alcun MIB NAT né CISCO-IETF-NAT-MIB.

## **D. Che cos'è il *timeout* TCP e come si relaziona al timer TCP NAT?**

A.Se l'handshake a tre vie non viene completato e NAT vede un pacchetto TCP, NAT può avviare un timer di 60 secondi. Al termine dell'handshake a tre vie, per impostazione predefinita NAT utilizza un timer di 24 ore per una voce NAT. Se un host terminale invia un comando RESET, NAT cambia il timer predefinito da 24 ore a 60 secondi. Nel caso di FIN, NAT cambia il timer predefinito da 24 ore a 60 secondi quando riceve FIN e FIN-ACK.

## **D. È possibile modificare la quantità di tempo necessaria per una traduzione NAT in modo che scada dalla tabella di conversione NAT?**

R.Sì. È possibile modificare i valori di timeout NAT per tutte le voci o per diversi tipi di conversioni NAT (ad esempio, udp-timeout, dns-timeout, tcp-timeout, finst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout e arp-ping-timeout).

## **D. Come arrestare il protocollo LDAP (Lightweight Directory Access Protocol) quando allega byte aggiuntivi a ciascun pacchetto di risposta LDAP?**

A.LDAP è impostato per aggiungere i byte aggiuntivi (risultati di ricerca LDAP) durante l'elaborazione dei messaggi di tipo Search-Res-Entry. LDAP allega 10 byte di risultati di ricerca a ciascun pacchetto di risposta LDAP. Nel caso in cui i 10 byte di dati in più restituiscano il pacchetto e superino l'MTU (Maximum Transmission Unit) di una rete, il pacchetto viene scartato. In questo caso, Cisco consiglia di disattivare questo comportamento LDAP con il comando **clino ip nat service append-ldap-search-resper** inviare e ricevere i pacchetti.

## **D. Qual è il percorso consigliato per l'indirizzo IP locale globale/esterno interno nella casella NAT?**

A.A route deve essere specificato nella casella NAT configurato per l'indirizzo IP globale interno per funzionalità quali NAT-NVI. Analogamente, è necessario specificare una route nella casella NAT per l'indirizzo IP locale esterno. In questo caso, per qualsiasi pacchetto da una direzione in-to-out con la regola statica esterna, è necessario questo tipo di percorso. In questi scenari, oltre a fornire il percorso per IG/OL, è necessario configurare anche l'indirizzo IP dell'hop successivo. Se la configurazione dell'hop successivo non viene trovata, viene considerato un errore di configurazione e determina un comportamento non definito.

NVI-NAT è presente solo nel percorso della funzionalità di output. Se la subnet è stata connessa direttamente con NAT-NVI o con la regola di conversione NAT esterna configurata nella confezione, in questi scenari sarà necessario fornire un indirizzo IP dell'hop successivo fittizio e un ARP associato per l'hop successivo. Questa operazione è necessaria perché l'infrastruttura sottostante possa consegnare il pacchetto al NAT per la traduzione.

## **D. Cisco IOS NAT supporta gli ACL con una parola chiave *log*?**

A.Quando si configura Cisco IOS NAT per la traduzione NAT dinamica, viene usato un ACL per identificare i pacchetti che possono essere tradotti. L'architettura NAT corrente non supporta ACL con parola chiave **log**.

## **Voice-NAT**

### **D. NAT supporta Skinny Client Control Protocol (SCCP) v17 fornito con Cisco Unified Communications Manager (CUCM) V7?**

A.CUCM 7 e tutti i caricamenti telefonici predefiniti per CUCM 7 supportano SCCPv17. La versione SCCP utilizzata è determinata dalla versione più comune tra CUCM e il telefono al momento della registrazione.

NAT non supporta ancora SCCP v17. Finché non viene implementato il supporto NAT per SCCP v17, è necessario effettuare il downgrade del firmware alla versione 8-3-5 o inferiore in modo che SCCP v16 venga negoziato. CUCM6 non può rilevare il problema NAT con alcun carico telefonico se utilizza SCCP v16. Cisco IOS non supporta attualmente SCCP versione 17.

### **D. Quali versioni di caricamento CUCM/SCCP/firmware sono supportate da NAT?**

**A.**NAT supporta CUCM versione 6.x e versioni precedenti. Queste versioni CUCM vengono rilasciate con il caricamento predefinito del firmware del telefono 8.3.x (o precedente) che supporta SCCP v15 (o precedente).

NAT non supporta CUCM versione 7.x o successive. Queste versioni CUCM vengono rilasciate con il caricamento predefinito del firmware del telefono 8.4.x che supporta SCCP v17 (o versione successiva).

Se si usa CUCM 7.x o versione successiva, è necessario installare un precedente caricamento del firmware sul server CUCM TFTP in modo che i telefoni utilizzino un caricamento del firmware con SCCP v15 o versione precedente per poter essere supportati da NAT.

## **D. In cosa consiste il miglioramento dell'allocazione delle porte PAT del provider di servizi per RTP e RTCP?**

**A.** La funzione Service Provider PAT Port Allocation Enhancement for RTP and RTCP assicura che per le chiamate vocali SIP, H.323 e Skinny. I numeri di porta utilizzati per i flussi RTP sono numeri di porta pari, mentre i flussi RTCP sono i successivi numeri di porta dispari. Il numero di porta viene convertito in un numero compreso nell'intervallo specificato e conforme alla RFC-1889. Una chiamata con un numero di porta compreso nell'intervallo può determinare la conversione di un numero di porta in un altro numero di porta compreso nell'intervallo. Analogamente, una conversione PAT per un numero di porta non compreso nell'intervallo non può determinare la conversione in un numero compreso nell'intervallo specificato.

## **D. Che cos'è il protocollo SIP (Session Initiation Protocol) e possono essere indirizzati pacchetti SIP con NAT?**

**A.**Session Initiation Protocol (SIP) è un protocollo di controllo a livello di applicazione basato su ASCII che può essere utilizzato per stabilire, mantenere e terminare le chiamate tra due o più endpoint. Il SIP è un protocollo alternativo sviluppato dalla Internet Engineering Task Force (IETF) per le conferenze multimediali su IP. L'implementazione SIP di Cisco consente alle piattaforme Cisco supportate di segnalare la configurazione delle chiamate vocali e multimediali sulle reti IP. I pacchetti SIP possono essere NATted.

## **D. In cosa consiste il supporto Hosted NAT Traversal per Session Border Controller (SBC)?**

**A.**La funzionalità Cisco IOS Hosted NAT Traversal per SBC consente a un router Cisco IOS NAT SIP Application-Level Gateway (ALG) di fungere da SBC su un gateway IP-to-IP multiservice di Cisco, che contribuisce a garantire la corretta consegna dei servizi Voice over IP (VoIP).

per ulteriori informazioni, fare riferimento [a Configurazione del Cisco IOS Hosted NAT Traversal per il controller del bordo di sessione](#).

## **D. Quante chiamate SIP, Skinny e H323 possono gestire la memoria e la CPU di un router con NAT?**

**R.**Il numero di chiamate gestite da un router NAT dipende dalla quantità di memoria disponibile nella confezione e dalla potenza di elaborazione della CPU.

## D. Un router NAT supporta la segmentazione TCP dei pacchetti Skinny e H323?

A. Cisco IOS-NAT supporta la segmentazione TCP per H323 e il supporto della segmentazione TCP per SKINNY.

## D. Ci sono avvertenze da tenere in considerazione quando si utilizza una configurazione di sovraccarico NAT in un'implementazione vocale?

R. Sì. Quando si dispone di configurazioni di sovraccarico NAT e di una distribuzione vocale, è necessario che il messaggio di registrazione passi attraverso NAT e crei un'associazione per out->in per raggiungere questo dispositivo interno. Il dispositivo interno invia periodicamente questa registrazione e NAT aggiorna questo pin-hole/associazione dalle informazioni come nel messaggio di segnalazione.

## D. Vi sono problemi noti causati quando si usa il comando `clear ip nat trans *` o il comando `clear ip nat trans` in un'implementazione vocale?

A. Nelle distribuzioni vocali, quando si immette il comando `clear ip nat trans *` o `clear ip nat trans` forzato e si dispone di un NAT dinamico, si elimina il foro/associazione del pin e si deve attendere il successivo ciclo di registrazione dal dispositivo interno per stabilire nuovamente questa condizione. Cisco consiglia di non utilizzare questi comandi clear in una distribuzione vocale.

## D. La tecnologia NAT supporta la soluzione di voice-co-location?

R. No. La soluzione con percorso condiviso non è attualmente supportata. La prossima installazione con NAT (sulla stessa confezione) è considerata una soluzione con sede condivisa: CME/DSP-Farm/SCCP/H323.

## D. Il protocollo NVI supporta Skinny ALG, H323 ALG e TCP SIP ALG?

R. No. Si noti che l'algoritmo UDP SIP ALG (utilizzato dalla maggior parte delle implementazioni) non è interessato.

## NAT con VRF/MPLS

D. È possibile che un router NAT si supporti nello stesso spazio di indirizzi di un VRF e di uno spazio di indirizzi globale? Al momento, viene visualizzato questo avviso: *"% una voce statica simile a % (10.1.1.1 —> 10.2.2.2) esiste già"* quando si tenta di configurare questa voce:

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

A. Legacy NAT supporta la configurazione degli indirizzi sovrapposta su VRF diversi. È necessario configurare la sovrapposizione a una regola con l'opzione `thematch-in-vrfoption` e impostare `upip nat interno/esterno` nello stesso VRF per il traffico su tale VRF specifico. Il supporto della sovrapposizione non include la tabella di routing globale.

È necessario aggiungere la parola chiave `match-in-vrf` per le voci NAT statiche VRF sovrapposte

per VRF diverse. Tuttavia, non è possibile sovrapporre indirizzi NAT globali e VRF.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

**D. La tecnologia NAT legacy supporta VRF-Lite (il percorso da un VRF a un VRF diverso)?**

R.No. È necessario utilizzare da NVI a NAT tra VRF diversi. È possibile utilizzare il protocollo NAT legacy per eseguire NAT da VRF a globale o NAT all'interno dello stesso VRF.

## NAT NVI

**D. Che cos'è NAT NVI?**

A.NVI è l'acronimo di NAT Virtual Interface. Consente la conversione NAT tra due VRF diversi. Questa soluzione deve essere utilizzata al posto di Network Address Translation su Memory Stick.

**D. È necessario utilizzare NAT NVI per effettuare il routing tra un'interfaccia in modalità globale e un'interfaccia in una VRF?**

A.Cisco consiglia di utilizzare il protocollo NAT legacy per VRF sul protocollo NAT globale (ip nat interno/esterno) e tra interfacce nello stesso VRF. NVI viene utilizzato per NAT tra VRF diversi.

**D. La segmentazione TCP per NAT-NVI è supportata?**

R.Non è supportato il supporto della segmentazione TCP per NAT-NVI.

**D. Il protocollo NVI supporta Skinny ALG, H323 ALG e TCP SIP ALG?**

R.No. Si noti che l'algoritmo UDP SIP ALG (utilizzato dalla maggior parte delle implementazioni) non è interessato.

**D. La segmentazione TCP è supportata con SNAT?**

A.SNAT non supporta alcun ALG TCP (ad esempio SIP, SKINNY, H323 o DNS). Pertanto, la segmentazione TCP non è supportata. Tuttavia, sono supportati SIP UDP e DNS.

## SNAT

**D. Che cos'è il protocollo stateful NAT (SNAT)?**

A.SNAT consente a due o più traduttori di indirizzi di rete di funzionare come gruppo di traduzione. Un membro del gruppo di traduzione gestisce il traffico che richiede la traduzione delle informazioni sull'indirizzo IP. Inoltre, informa il traduttore di backup dei flussi attivi man mano che si verificano. Il traduttore di backup può quindi utilizzare le informazioni del traduttore attivo per preparare le voci duplicate della tabella di traduzione. Pertanto, se il convertitore attivo è

ostacolato da un errore critico, il traffico può essere rapidamente passato al backup. Il flusso di traffico continua poiché vengono utilizzate le stesse traduzioni degli indirizzi di rete e lo stato di tali traduzioni è stato definito in precedenza.

#### **D. La segmentazione TCP è supportata con SNAT?**

A.SNAT non supporta alcun ALG TCP (ad esempio SIP, SKINNY, H323 o DNS). Pertanto, la segmentazione TCP non è supportata. Tuttavia, sono supportati SIP UDP e DNS.

#### **D. Il protocollo SNAT è supportato per il routing asimmetrico?**

R. Il routing asimmetrico supporta NAT quando abilita `as-queuing`. Per impostazione predefinita, la funzione di accodamento automatico è abilitata. Tuttavia, a partire dall'articolo 12.4(24)T, `as-queuing` non è più supportato. Per il corretto funzionamento del routing asimmetrico, i clienti devono verificare che i pacchetti siano indirizzati correttamente e che sia stato aggiunto il ritardo corretto.

## **NAT-PT (da v6 a v4)**

#### **D. Che cos'è NAT-PT?**

A.NAT-PT è la traduzione da v4 a v6 per NAT. Protocol Translation (NAT-PT) è un meccanismo di conversione IPv6-IPv4, definito [nelle RFC 2765 e 2766](#), che consente ai dispositivi solo IPv6 di comunicare con i dispositivi solo IPv4 e viceversa.

#### **D. Il protocollo NAT-PT è supportato nel percorso CEF (Cisco Express Forwarding)?**

A.NAT-PT non è supportato nel percorso CEF.

#### **D. Quali ALG sono supportati in NAT-PT?**

A.NAT-PT supporta TFTP/FTP e DNS. NAT-PT non supporta la voce e il protocollo SNAT.

#### **D. ASR 1004 supporta NAT-PT?**

A.Aggregation Services Router (ASR) utilizza NAT64.

## **Cisco 7600/6k dipendente dalla piattaforma**

#### **D. La tecnologia Stateful NAT (SNAT) è disponibile su Catalyst 6500 sul treno SX?**

A.SNAT non è disponibile su Catalyst 6500 sul treno SX.

#### **D. NAT con riconoscimento VRF è supportato nell'hardware su 6k?**

NAT compatibile con A.VRF non supportato nell'hardware di questa piattaforma.

## **D. I modelli 7600 e Cat6000 supportano NAT con riconoscimento VRF?**

R.Sulla piattaforma 65xx/76xx, il protocollo NAT con supporto VRF non è supportato e le CLI sono bloccate.

**Nota:** è possibile implementare un progetto se si utilizza un modulo FWSM eseguito in modalità trasparente del contesto virtuale.

## **Cisco 850 Dipendente Dalla Piattaforma**

### **D. Cisco 850 supporta Skinny NAT ALG nella versione 12.4T?**

R.No. Non c'è supporto per Skinny NAT ALG in 12.4T sulla serie 850.

## **Distribuzione NAT**

### **D. Come implementare NAT?**

A.NAT consente la connessione a Internet di interreti IP private che utilizzano indirizzi IP non registrati. NAT converte l'indirizzo privato (RFC1918) della rete interna in indirizzi instradabili legali prima che i pacchetti vengano inoltrati a un'altra rete.

### **D. Come posso implementare NAT con la voce?**

A.La funzionalità vocale del supporto NAT consente di convertire nuovamente nel pacchetto i messaggi SIP incorporati che passano attraverso un router configurato con Network Address Translation (NAT). Con NAT viene utilizzato un ALG (Application Layer Gateway) per tradurre i pacchetti voce.

### **D. Come integrare NAT con VPN MPLS?**

R.L'integrazione NAT con le VPN MPLS consente di configurare più VPN MPLS su un singolo dispositivo per il funzionamento congiunto. NAT può differenziarsi da quale VPN MPLS riceve il traffico IP anche se le VPN MPLS utilizzano tutte lo stesso schema di indirizzamento IP. Questo miglioramento consente a più clienti VPN MPLS di condividere i servizi e garantisce che ogni VPN MPLS sia completamente separata dall'altra.

### **D. La mappatura statica NAT supporta HSRP per l'alta disponibilità?**

A.Quando viene attivata una query ARP (Address Resolution Protocol) per un indirizzo configurato con il mapping statico Network Address Translation (NAT) e di proprietà del router, NAT risponde con l'indirizzo MAC BIA sull'interfaccia a cui punta ARP. Due router funzionano come HSRP attivo e in standby. Le relative interfacce interne NAT devono essere abilitate e configurate per appartenere a un gruppo.

### **D. Come posso implementare NAT NVI?**

A. La funzionalità dell'interfaccia virtuale NAT (NVI) elimina la necessità di configurare un'interfaccia come NAT interno o NAT esterno.

## D. Come è possibile implementare il bilanciamento del carico con NAT?

R. Con NAT è possibile eseguire due tipi di bilanciamento del carico: è possibile bilanciare il carico in entrata in un set di server per distribuire il carico sui server e bilanciare il carico del traffico utente verso Internet su due o più ISP.

Per ulteriori informazioni sul bilanciamento del carico in uscita, fare riferimento [a Cisco IOS NAT Load-Balancing per Two ISP Connections](#).

## D. Come implementare NAT in combinazione con IPSec?

R. C'è supporto per IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT e IPSec NAT Transparency.

La funzionalità IPSec ESP tramite NAT consente di supportare più tunnel o connessioni IPSec ESP simultanee tramite un dispositivo Cisco IOS NAT configurato in modalità overload o PAT (Port Address Translation). La funzionalità di trasparenza NAT di IPSec introduce il supporto per il traffico IPSec che attraversa punti NAT o PAT nella rete quando viene risolta una serie di incompatibilità note tra NAT e IPSec.

## D. Come implementare NAT-PT?

A. NAT-PT (Network Address Translation—Protocol Translation) è un meccanismo di conversione IPv6-IPv4, definito [nelle RFC 2765 e RFC 2766](#), che consente ai dispositivi solo IPv6 di comunicare con i dispositivi solo IPv4 e viceversa.

## D. Come implementare un NAT multicast?

R. È possibile utilizzare il protocollo NAT per l'IP di origine di un flusso multicast. Impossibile utilizzare una route-map quando viene eseguito un NAT dinamico per multicast. Per questo elemento è supportato solo un elenco degli accessi.

Per ulteriori informazioni, fare riferimento [a Come funziona il multicast NAT sui router Cisco](#). Il gruppo multicast di destinazione utilizza NAT con una soluzione Multicast Service Reflection.

## D. Come implementare un NAT stateful (SNAT)?

A. SNAT abilita il servizio continuo per le sessioni NAT mappate in modo dinamico. Le sessioni definite staticamente ricevono il vantaggio della ridondanza senza la necessità di SNAT. In assenza del protocollo SNAT, le sessioni che utilizzano mapping NAT dinamici verranno interrotte in caso di errore critico e dovranno essere ristabilite. È supportata solo la configurazione SNAT minima. Le distribuzioni future devono essere eseguite solo dopo aver parlato con l'Account Team Cisco per convalidare la progettazione in base alle restrizioni correnti.

SNAT è consigliato per gli scenari successivi:

- La modalità primaria/backup non è consigliata, in quanto alcune funzionalità sono assenti

rispetto a HSRP.

- Per scenari di failover e per la configurazione a 2 router. In altre parole, se un router si blocca, l'altro router subentra senza problemi. (l'architettura SNAT non è progettata per gestire i flap dell'interfaccia.)
- Scenario di routing non asimmetrico supportato. Il routing asimmetrico può essere gestito solo se la latenza nel pacchetto di risposta è superiore a quella tra due router SNAT per lo scambio dei messaggi SNAT.

Attualmente l'architettura SNAT non è progettata per gestire la robustezza, pertanto non è previsto il completamento di questi test:

- Quando le voci NAT vengono cancellate in presenza di traffico.
- Quando i parametri dell'interfaccia (ad esempio, modifica dell'indirizzo IP, chiusura/non chiusura e così via) vengono modificati in presenza di traffico.
- L'esecuzione di `SNAT specificclearorshowcommands` non è prevista in modo corretto e non è consigliata. Di seguito sono riportati alcuni comandi `clearandshow` correlati a SNAT:

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- Se l'utente desidera cancellare le voci, è possibile usare i comandi **clear ip nat trans forced** o **clear ip nat trans \***. Per visualizzare le voci dell'elenco, è possibile usare i comandi **show ip nat translation**, **show ip nat translation verbose** e **show ip nat status**. *Se il servizio è stato configurato*, può visualizzare anche informazioni specifiche SNAT.
- Si sconsiglia di cancellare le conversioni NAT sul router di backup. Cancellare sempre le voci NAT sul router SNAT primario.
- SNAT non è HA; pertanto, le configurazioni su entrambi i router devono essere le stesse. Entrambi i router devono eseguire la stessa immagine. Inoltre, verificare che la piattaforma sottostante utilizzata per entrambi i router SNAT sia la stessa.

## Best practice NAT

### D. Esistono best practice NAT?

R.Sì. Queste sono le best practice NAT:

1. Quando si utilizza un NAT sia dinamico che statico, l'ACL che imposta la regola per il NAT dinamico deve escludere gli host locali statici in modo da evitare sovrapposizioni.
2. Se si usa ACL per NAT **con allow ip any**, si possono ottenere risultati imprevedibili. Dopo la versione 12.4(20)T, NAT può convertire i pacchetti HSRP e del protocollo di routing generati localmente se inviati dall'interfaccia esterna, nonché i pacchetti crittografati localmente che soddisfano la regola NAT.
3. In caso di reti sovrapposte per NAT, utilizzare la parola chiave **thematch-in-vrf**. È necessario

aggiungere la parola chiave **match-in-vrf** per le voci NAT statiche VRF sovrapposte per VRF diverse VRF, ma non è possibile sovrapporre gli indirizzi NAT globali e vrf.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. I pool NAT con lo stesso intervallo di indirizzi non possono essere utilizzati in VRF diversi a meno che non venga utilizzata la parola chiave **thematch-in-vrfkeyword**. Ad esempio:

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

**Nota:** anche se la configurazione CLI è valida, senza la parola chiave **match-in-vrf** la configurazione non è supportata.

5. Quando si distribuisce il bilanciamento del carico degli ISP con sovraccarico dell'interfaccia NAT, la procedura ottimale è utilizzare la route-map con corrispondenza dell'interfaccia su corrispondenza ACL.
6. Quando si usa il mapping del pool, non è necessario usare due mapping diversi (ACL o route-map) per condividere lo stesso indirizzo del pool NAT.
7. Quando si distribuiscono le stesse regole NAT su due router diversi nello scenario di failover, è necessario utilizzare la ridondanza HSRP.
8. Non definire lo stesso indirizzo globale interno in un NAT statico e in un pool dinamico. Questa azione può portare a risultati indesiderati.

## Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)

## 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).