Internal Legal Disclaimer

The information in this document has been compiled solely for purposes of supporting the proposal of a licensing program(s). All statements and figures are assumptions based on available market data collected to date and assume negotiated terms. They are to be used solely for planning purposes, and are subject to change as more detailed data is received, more detailed analysis is performed, client’s business changes, or due to other factors. Stated royalty rate assumptions are illustrative, and are not a projection of actual royalty rates to be achieved in connection with specific negotiation or litigation. Valuations do not take into account revenue/value that could be derived in other business units, or by this business unit, if using a different business plan.
U.S. Pat. No. 9,407,548 B2 – PATENT OVERVIEW
21. A method for providing redundant network address translation (ReNAT) communications, comprising:

- initiating a virtual private connection with a private network;
- translating between a customer-assigned private internet protocol (IP) address and a unique private IP (UPIP) address, wherein the UPIP overlaps with the customer-assigned private IP address and wherein the UPIP is unique within a network operations center (NOC) in which the UPIP is utilized;
- facilitating communication between a user workstation that includes a ReNAT twin NAT client and the private network, wherein address translation has been performed by the ReNAT twin NAT client;
- mapping addresses in the data to customer-defined IP addresses; and
- encrypting the data and transferring the data to the private network.
U.S. Pat. No. 9,407,548 B2 – REPRESENTATIVE PRODUCT

Cisco Nexus 9000 Series Switches Cisco NX-OS

Build a next-generation automated data center

Prepare your data center for growing number of users and complicated applications. Our Nexus 9000 Series data center switches deliver proven high performance and density up to 400G, as well as low latency and exceptional power efficiency in a range of form factors. The switches are highly programmable and offer industry-leading software-defined networking for data center automation.

Watch video (2:18)

Compare Nexus 9000 models

Cloud Scale ASIC enables ACI leaf-spine architecture and NX-OS VXLAN Fabric with diverse modular and fixed portfolio.

Source:
Open, extensible operating system for data center

**Open Cisco NX-OS Software** is the industry’s most extensible, open, and programmable network operating system. It enables network automation and allows customers to programatically provision and configure switches through comprehensive APIs, utilizing tools provided by Cisco and open-source third party solutions. Powerful capabilities include zero touch provisioning and network telemetry for top notch security.


Products supported by NX-OS

- Cisco MDS 9000 Series Multilayer Switches
- Cisco Nexus 9000 Series Switches
- Cisco Nexus 7000 Series Switches
Figure 35: Native VLAN Hazard

- Tag not added for VLAN 40
- Tag removed
- Packet tagged for VLAN 30

Switch A
- Customer X
- 802.1Q trunk port VLANs 30-40 Native VLAN 40

Switch B
- Tunnel port Access VLAN 40

Service provider

VLANs 5-50

Tunnel port Switch C
- Native VLAN 40

Tunnel port Access VLAN 30

Switch D
- Customer X VLANs 30-40 Native VLAN 40

Switch E
- Customer Y

Q = 802.1Q trunk ports

Confidential - Subject to NDA see restrictions on title page
U.S. Pat. No. 9,407,548 B2 – Cisco Nexus 9000 Series NX-OS Interfaces (Release 9.3x) SUMMARY

Problem over prior art: Gateway routers in commercial environments is the creation of a virtual private network (VPN) to connect external users to the internal private network. The VPN provides an envelope or wrapper protocol to hide the internal IP addresses and data while the packet is routed across the public Internet to the user. Prior invention provides a mechanism for multiple organizations using a VPN with private address realms to share a public software resource on the Internet. Each organization uses a VPN to communicate with remote users over the public Internet. In this way, the VPN creates a virtual tunnel between the organization's private IP network and servers and the remote user. Each VPN provides two functions to enable secure communication. The first function is that information in the virtual tunnel may be encrypted to protect it from unauthorized access. The second function is that organization's private IP network is extended to the user workstation. While the use of private IP addresses and VPN allows users to securely access private networks, these two facts mean that organizations using VPNs cannot make use of software functions on the public Internet.

Solution over prior art: The invention describes the method Cisco Nexus 9000 Series NX-OS Interfaces which supported Network address translation function in addition with Virtual private network function (ReNAT) which allows remote users to securely access the Private networks of Corporate data centre (remote computing device). Cisco Nexus 9000 Series NX-OS Interfaces supported static and dynamic twin NAT (Twice NAT) function which perform translation between private IP address and unique private IP address. The private IP address of Remote user (User workstation) comprises source IP address and destination IP address. The Cisco Nexus 9000 Series NX-OS Interfaces (ReNAT) supported Twin NAT (twice NAT) translates the private IP address of Remote user (user workstation) into unique IP address (translated IP). The unique private IP address (Registered IP address) is the IP address of Cisco Nexus 9000 Series NX-OS comprises source UPIP and destination UPIP. The UPIP is map (overlap) with the private IP address (registered IP address) of the Remote user (user workstation) in a datagram. The Cisco Nexus 9000 Series installed with NX-OS which supported generic routing protocol (VPN) securely connects the user workstation (Remote user) to remote computing device (destination) through an IP tunnel by encapsulating the data packet. The VLAN (cots VPN client) encrypt the Outbound datagram comprise source IP and destination IP address from user workstation (remote user) and send the data packet to the private network of remote computing device (destination). User workstation (Remote user) and the corporate office (remote computing device) see only respective internal private IP addresses. The Cisco Nexus 9000 Series Switch router are enterprise-class devices that supported NX-OS (virtual software) that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services over the public internet as similar to ReNAT technology of Patent (548B2).
U.S. Pat. No. 9,407,548 B2 – LEADING PLAYERS IN NAT ROUTER

- NETGEAR
- tp-link
- ZTE
- HUAWEI
- Franklin Wireless
- SAMSUNG
- ARISTA
- SIERRA WIRELESS
- NEC
- VERSA NETWORKS
- DIGI
- iDirect
- ADVANTECH
- cradlepoint
- peplink
- CISCO
- BROADCOM
- JUNIPER NETWORKS
- RAD
- F5

CONFIDENTIAL - SUBJECT TO NON-DISCLOSURE AGREEMENT

PRELIMINARY CLAIM CHART
**U.S. Pat. No. 9,407,548 B2 – Cisco Nexus 9000 Series NX-OS Interfaces (Release 9.3x)**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>21. A method for providing redundant network address translation (ReNAT) communications, comprising: (Preamble)</td>
<td>Embodiments described herein include ReNAT systems and methods for facilitating communication between a user computing device in a private realm and a remote computing device over a wide area network (or other network). Specifically, the user computing device may communicate with the remote computing device via a satellite network or other network that may have slower than desired connection speeds. While the user may utilize a virtual private network, the communication may be routed from a user workstation, which includes a ReNAT twin NAT (network address translation) client and a commercial off the shelf (COTS) VPN client to a network operations center (NOC). The NOC includes a COTS VPN, COTS clear text software, a ReNAT Twin NAT, and a ReNAT VPN.</td>
<td><strong>Researcher Comment:</strong> Evidence demonstrates Cisco Nexus 9000 Series NX-OS interface which supported VPN (VLAN/VPC) and NAT function (ReNAT) for facilitating secure communications between user computing device (Client side) and remote computing device (corporate office) over a wide area network (internet).</td>
</tr>
</tbody>
</table>

---

**Build a next-generation automated data center**

Prepare your data center for growing number of users and complicated applications. Our Nexus 9000 Series data center switches deliver proven high performance and density up to 400G, as well as low latency and exceptional power efficiency in a range of form factors. The switches are highly programmable and offer industry-leading software-defined networking for data center automation.

**Source:**

Open, extensible operating system for data center

Open Cisco NX-OS Software is the industry’s most extensible, open, and programmable network operating system. It enables network automation and allows customers to programatically provision and configure switches through comprehensive APIs, utilizing tools provided by Cisco and open-source third party solutions. Powerful capabilities include zero touch provisioning and network telemetry for top notch security.

Source:
For Broadcom-based Cisco Nexus 9000 Series switches, if the route to your inside global address on the translating device is reachable via the outside interface, packets for Network Address Translated flows coming from outside to inside get software forwarded, duplicated, and looped in the network. For this situation, you must enter the add-route CLI argument on the end of the NAT configuration for this flow. For example, `ip nat inside source static 192.168.1.1 172.16.1.1 add-route`.

IP packets without TCP/UDP/ICMP headers are not translated with dynamic NAT.

In dynamic twice NAT, if dynamic NAT flows are not created before creating static NAT flows, dynamic twice NAT flows are not created correctly.

When an empty ACL is created, the default rule of `permit ip any any` is configured. The NAT-ACL does not match further ACL entries if the first ACL is blank.

Enabling Static NAT for an Inside Source Address

For inside source translation, the traffic flows from inside interface to the outside interface. NAT translates the inside local IP address to the inside global IP address. On the return traffic, the destination inside global IP address gets translated back to the inside local IP address.

Note

When the Cisco Nexus device is configured to translate an inside source IP address (Src:ip1) to an outside source IP address (newSrc:ip2), the Cisco Nexus device implicitly adds a translation for an outside destination IP address (Dst: ip2) to an inside destination IP address (newDst: ip1).
Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows.

Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it.

With dynamic NAT and Port Address Translation (PAT), each host uses a different address or port for each subsequent translation. The main difference dynamic NAT does not.

Source:
https://www.cisco.com/c/en/us/td/docs/s...
Pool Support for Dynamic NAT
Cisco NX-OS provides pool support for dynamic NAT. Dynamic NAT allows the configuration of a pool of global addresses that can be used to dynamically allocate a global address from the pool for every new translation. The addresses are returned to the pool after the session ages out or is closed. This allows for a more efficient use of addresses based on requirements.

Network Address Translation Overview
Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into local IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.

Source:
PRELIMINARY CLAIM CHART

NAT/PAT on Cisco Nexus Switches

As far as I know, there are no NAT capabilities on Cisco Nexus 7000 Series Switches.

NAT is only supported on below Nexus Switches

- Nexus 9300 Series
- Nexus 6000 Series
- Nexus 5600 Series
- Nexus 3448 Series

ILT support for SLB NAT on Nexus Switches

In SLB-NAT deployment, client can send traffic to a virtual IP address, and need not know about the IP of the underlying servers. NAT provides additional security in hiding the real server IP from the outside world. In the case of Virtualized server environments, this NAT capability provides increased flexibility in moving the real servers across the different server pools without being noticed by the their clients. With respect health monitoring and traffic reassignment, SLB-NAT helps applications to work seamlessly without client being aware of any IP change.

<table>
<thead>
<tr>
<th>NAT Support on various Nexus Switches Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus Switches</td>
</tr>
<tr>
<td>Static NAT</td>
</tr>
<tr>
<td>Dynamic NAT</td>
</tr>
<tr>
<td>PAT</td>
</tr>
<tr>
<td>Twice NAT</td>
</tr>
<tr>
<td>VRF-Aware NAT</td>
</tr>
</tbody>
</table>

Source:
https://www.slideshare.net/PratikBhide/natfinal
Nexus 9000:
Recent feature additions

Roadmap Features under evaluation:
- Destination-NAT SLB

ITD – SLB with Destination NAT

- NAT Functionality is limited to ITD for SLB, not for Carrier-grade NAT as a feature itself.

Source:

Source:
**Clause 1**

- **initiating a virtual private connection with a private network:**

  FIG. 2 depicts yet another computing environment, utilizing a twin NAT configuration, according to embodiments described herein. As illustrated, the user workstation 202 may send data to an NOC 204 by translating private IP addresses into UPIP addresses. The data may then be translated back to private addresses before being sent to a corporate office 206. The user workstation 202 includes user applications 208, as well as client software 209. The client software 209 includes a ReNAT twin NAT client 210, a COTS clear text process (CTP) COTS CTP client 212, a COTS VPN client 214, a client login manager 216, and a client session manager 218. Specifically, the user applications 208 may instruct the user workstation 202 to send data to the remote computing device 234 on the corporate office 206. As such, the client login manager 216 may facilitate the communication of login credentials for the NOC 204. Upon logging the user into the NOC, the client session manager 218 may provide user interfaces and/or other data for identifying and/or accessing the desired computing device (in this case the remote computing device 234).

**Researcher comment:** The evidence demonstrates Cisco Nexus 9000 Series NX-OS Interfaces supported VPN (VLAN) function which create GRE tunnel to securely connect the user workstation (customer switch A) to private network (LAN) of remote computing device (Customer Switch D).

IP tunnels can encapsulate a same-layer or higher layer protocol and transport the result over IP through a tunnel created between two devices.

You can use generic routing encapsulation (GRE) as the carrier protocol for a variety of passenger protocols.

The following figure shows the IP tunnel components for a GRE tunnel. The original passenger protocol packet becomes the GRE payload and the device adds a GRE header to the packet. The device then adds the transport protocol header to the packet and transmits it.

The point-to-point IP-in-IP encapsulation and decapsulation is a type of tunnel that you can create to send encapsulated packets from a source tunnel interface to a destination tunnel interface. This type of tunnel will carry both inbound and outbound traffic.

---

**Multiple IP-in-IP/GRE tunnel interfaces on a same Cisco Nexus Device:** can be sourced from or destined to the same IP Address across different VRFs. This is supported on Cisco Nexus N92xx N93xx-EX/FX/FX2 platforms. This is not supported on Cisco Nexus N9300-GX and N9500 platforms.
Accordingly, the ReNAT twin NAT client 210 assigns data received from the user applications 208 UPIP. The ReNAT twin NAT client 210 may be configured to translate both source and destination IP addresses in the clear text packets to/from assigned UPIP. The COTS CTP client 212 receives and processes the data using clear text processing (or other protocol). The COTS VPN client 214 receives the data and creates a VPN tunnel for securely communicating the data to the NOC 204.

A VLAN interface, or switch virtual interface (SVI), is a virtual routed interface that connects a VLAN on the device to the Layer 3 router engine on the same device. Only one VLAN interface can be associated with a VLAN, but you need to configure a VLAN interface for a VLAN only when you want to route between VLANs or to provide IP host connectivity to the device through a virtual routing and forwarding (VRF) instance that is not
The management VRF. When you enable VLAN interface creation, Cisco NX-OS creates a VLAN interface for the default VLAN (VLAN 1) to permit remote switch administration. The VRF aware NAT feature enables a switch to understand an address space in a VRF (virtual routing and forwarding instances) and to translate the packet. This allows the NAT feature to translate traffic in an overlapping address space that is used between two VRFs.

- Carrier protocol—The protocol that is used to encapsulate the passenger protocol. Cisco NX-OS supports GRE as a carrier protocol.
- Cisco NX-OS supports the following maximum number of tunnels:
  - IP tunnels – 8 tunnels.
  - GRE and IP-in-IP regular tunnels – 8 tunnels, (7.0(3)112 and later)
  - On Cisco Nexus 9200 Series switches, GRE packets that are received on an IP-in-IP tunnel are not dropped as expected and are instead forwarded to the packet destination.

Point-to-Point IP-in-IP Tunnel Encapsulation and Decapsulation

For 6.1(2)i3(4), 7.0(3)i12, and later, point-to-point IP-in-IP encapsulation and decapsulation is a type of tunnel that you can create to send encapsulated packets from a source tunnel interface to a destination tunnel interface. This type of tunnel will carry both inbound and outbound traffic.

Figure 1. GRE PDU
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>translating</strong> between a customer-assigned private internet protocol (IP) address and a unique private IP (UPIP) address, wherein the UPIP overlaps with the customer-assigned private IP address and wherein the UPIP is unique within a network operations center (NOC) in which the UPIP is utilized;</td>
<td>FIG. 2 depicts yet another computing environment, utilizing a twin NAT configuration, according to embodiments described herein. As illustrated, the user workstation 202 may send data to an NOC 204 by translating private IP addresses into UPIP addresses. The data may then be translated back to private addresses before being sent to a corporate office 206. The user workstation 202 includes user applications 208, as well as client software 209. The client software 209 includes a ReNAT twin NAT client 210, a COTS clear text process (CTP) COTS CTP client 212, a COTS VPN client 214, a client login manager 216, and a client session manager 218. Specifically, the user applications 208 may instruct the user workstation 202 to send data to the remote computing device 234 on the corporate office 206. As such, the client login manager 216 may facilitate the communication of login credentials for the NOC 204. Upon logging the user into the NOC, the client session manager 218 may provide user interfaces and/or other data for identifying and/or accessing the desired computing device (in this case the remote computing device 234). Accordingly, the ReNAT twin NAT client 210 assigns data received from the user applications 208 UPIP. The ReNAT twin NAT</td>
<td><strong>Researcher comment:</strong> Evidence demonstrates Cisco Nexus 9000 Series NX-OS interfaces supported Static and dynamic twice NAT function which perform translation between private IP address (Local IP address) and unique private IP address (Public IP address/global IP address). The private IP address of (user workstation) comprises source IP address and destination IP address. The Cisco Nexus 9000 Series NX-OS Interfaces supported Twin NAT function translates the Source IP address (local IP address) into inside unique IP address (global IP address). The unique private IP address is the IP address of NAT comprises source UPIP and destination UPIP. In return Path, The destination inside global IP address (unique IP address/UPIP) is translated back to local IP address (private IP address). The UPIP (unique IP address/Registered IP address) is map (overlap) with the private IP address (unregistered IP address) in a datagram.</td>
</tr>
</tbody>
</table>

**Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into legal IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.**

A device configured with NAT has at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit router between a stub domain and a backbone. When a packet leaves the domain, NAT translates the locally significant source IP
Client 210 may be configured to translate both source and destination IP addresses in the clear text packets to/from assigned UPIP. The COTS CTP client 212 receives and processes the data using clear text processing (or other protocol). The COTS VPN client 214 receives the data and creates a VPN tunnel for securely communicating the data to the NOC 204.

<p>| address into a globally unique IP address. When a packet enters the domain, NAT translates the globally unique destination IP address into a local IP address. If more than one exit point exists, NAT configured at each point must have the same translation table. Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows. Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it. With dynamic NAT and Port Address Translation (PAT), each host uses a different address or port for each subsequent translation. The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not. The figure shows a typical static NAT scenario. The translation is always active so both translated and remote hosts can originate connections, and the mapped address is statically assigned by the static command. |</p>
<table>
<thead>
<tr>
<th>PRELIMINARY CLAIM CHART</th>
</tr>
</thead>
<tbody>
<tr>
<td>When both the source IP address and the destination IP address are translated as a single packet that goes through a Network Address Translation (NAT) device, it is referred to as twice NAT. Twice NAT is supported for static and dynamic translations.</td>
</tr>
<tr>
<td>Twice NAT allows you to configure two NAT translations (one inside and one outside) as part of a group of translations. These translations can be applied to a single packet as it flows through a NAT device. When you add two translations as part of a group, both the individual translations and the combined translation take effect.</td>
</tr>
<tr>
<td>A NAT inside translation modifies the source IP address and port number when a packet flows from inside to outside. It modifies the destination IP address and port number when the packet returns from outside to inside.</td>
</tr>
<tr>
<td>A NAT outside translation modifies the source IP address and port number when the packet flows from outside to inside, and it modifies the destination IP address and port number when the packet returns from inside to outside.</td>
</tr>
<tr>
<td>Without twice NAT, only one of the translation rules is applied on a packet, either the source IP address and port number or the destination IP address and port number. Static NAT translations that belong to the same group are considered for twice NAT configuration. If a static configuration does not have a configured group ID, the twice NAT configuration will not work. All inside and outside NAT translations that belong to a single group that is identified by the group ID are paired to form twice NAT translations.</td>
</tr>
<tr>
<td>Dynamic twice NAT translations dynamically select the source IP address and port number information from pre-defined ip nat pool or interface overload configurations. Packet filtration is done by configuring ACLs, and traffic must originate from the dynamic NAT translation rule direction such that source translation is done by using dynamic NAT rules.</td>
</tr>
</tbody>
</table>
Dynamic twice NAT allows you to configure two NAT translations (one inside and one outside) as part of a group of translations. One translation must be dynamic and other translation must be static. When these two translations are part of a group of translations, both the translations can be applied on a single packet as it goes through the NAT device either from inside to outside or from outside to inside.

Source: https://www.cisco.com/

The following restrictions apply to dynamic Network Address Translation (NAT):

• For Broadcom-based Cisco Nexus 9000 Series switches, if the route to your inside global address on the translating device is reachable via the outside interface, packets for Network Address Translated flows coming from outside to inside get software forwarded, duplicated, and looped in the network. For this situation, you must enter the add-route CLI argument on the end of the NAT configuration for this flow. For example, ip nat inside source static 192.168.1.1 172.16.1.1 add-route.

Source: https://www.cisco.com/

Enabling Static NAT for an Inside Source Address

For inside source translation, the traffic flows from inside interface to the outside interface. NAT translates the inside local IP address to the inside global IP address. On the return traffic, the destination inside global IP address gets translated back to the inside local IP address.

Note: When the Cisco Nexus device is configured to translate an inside source IP address (Src: ip1) to an outside source IP address (newSrc: ip2), the Cisco Nexus device implicitly adds a translation for an outside destination IP address (Dst: ip2) to an inside destination IP address (newDst: ip1).

Source: https://www.cisco.com/
**Dynamic Network Address Translation (NAT)** translates a group of **real IP addresses** into **mapped IP addresses** that are routable on a destination network. Dynamic NAT establishes a **one-to-one mapping** between unregistered and registered IP addresses; however, the mapping can vary depending on the registered IP address that is available at the time of communication.

A **dynamic NAT** configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact.

**Dynamic NAT translations** do not exist in the NAT translation table until a device receives traffic that requires translation. Dynamic translations are cleared or timed out when not in use to make space for new entries. Usually, **NAT translation entries** are cleared when the ternary content addressable memory (TCAM) entries are limited. The default minimum timeout for dynamic NAT translations is 30 minutes.

3 ways to NAT on a Cisco Router

- **Inside to Outside**
  - Static NAT translating inside private IP to outside public IP
    - example: assigning outside, public IP to internal web server
  - Outside to Inside
    - Translating outside public IP to inside private IP
      - example: port-forwarding specific port to inside host from the outside interface IP

### Inside to Outside

For inside to outside NAT, imagine you have an internal web server you want to NAT to an outside, public IP. Here are what those commands would look like:

```
ip nat inside source static 192.168.1.5 22.33.44.55
```

With that command, the internal device @ 192.168.1.5 would be NAT’ed to the public IP 22.33.44.55. This is referred to as static NAT.

### Outside to Inside

Outside to inside NAT involves translating a public IP back to a private, inside IP address. This is commonly done with a specific port involved as well. It’s all dependant on your situation, not required by any means. First off, your configuration would look like this:

```
ip nat outside source static tcp 22.33.44.55 22 192.168.1.5 22
```

What you are seeing is that all tcp/22 traffic sourcing in the outside interface from the IP 22.33.44.55 will be translated to 192.168.1.5. That way, the destination device will reply to 192.168.1.5, not the public IP 22.33.44.55. This is useful in cases where devices may not have a default route, etc.

**Source:** [https://www.theroutingtable.com/3-ways-to-nat-on-a-cisco-router/](https://www.theroutingtable.com/3-ways-to-nat-on-a-cisco-router/)
Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into legal IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.

Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows.

Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, a persistent translation rule exists. Static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it.

NAT Inside and Outside Addresses

NAT inside refers to networks owned by an organization that must be translated. When NAT is configured, hosts within this network will have addresses in one space (known as the local address space) that will appear to those outside the network as being in another space (known as the global address space).

Dynamic NAT Overview

Dynamic Network Address Translation (NAT) translates a group of real IP addresses into mapped IP addresses that are routable on a destination network. Dynamic NAT establishes a one-to-one mapping between unregistered and registered IP addresses; however, the mapping can vary depending on the registered IP address that is available at the time of communication.

A dynamic NAT configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact.

Static NAT translations that belong to the same group are considered for twice NAT configuration. If a static configuration does not have a configured group ID, the twice NAT configuration will not work. All inside and outside NAT translations that belong to a single group that is identified by the group ID are paired to form twice NAT translations.

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into legal IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.

Source:
facilitating communication between a user workstation that includes a ReNAT twin NAT client and the private network, wherein address translation has been performed by the ReNAT twin NAT client;

(Clause 3)

FIG. 2 depicts yet another computing environment, utilizing a twin NAT configuration, according to embodiments described herein. As illustrated, the user workstation 202 may send data to an NOC 204 by translating private IP addresses into UPIP addresses. The data may then be translated back to private addresses before being sent to a corporate office 206. The user workstation 202 includes user applications 208, as well as client software 209. The client software 209 includes a ReNAT twin NAT client 210, a COTS clear text process (CTP) COTS CTP client 212, a COTS VPN client 214, a client login manager 216, and a client session manager 218. Specifically, the user applications 208 may instruct the user workstation 202 to send data to the remote computing device 234 on the corporate office 206. As such, the client login manager 216 may facilitate the communication of login credentials for the NOC 204. Upon logging the user into the NOC, the client session manager 218 may provide user interfaces and/or other data for identifying and/or accessing the desired computing device (in this case the remote computing device 234).

Researcher comment: Evidence demonstrates User workstation (Host) that includes ReNAT twin NAT client (Cisco Nexus 9000 Series NX-OS Interfaces) which offers network address translation solution in communication with private networks of Other host (remote computing device).
Accordingly, the ReNAT twin NAT client 210 assigns data received from the user applications 208 UPIP. The ReNAT twin NAT client 210 may be configured to translate both source and destination IP addresses in the clear text packets to/from assigned UPIP. The COTS CTP client 212 receives and processes the data using clear text

COTS VPN client 214 receives the data and creates a VPN tunnel for securely communicating the data to the NOC 204.

Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows.

Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it.

With dynamic NAT and Port Address Translation (PAT), each host uses a different address or port for each subsequent translation. The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not.

Source:
Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus 9000 Series device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows.

Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it.

With dynamic NAT and Port Address Translation (PAT), each host uses a different address or port for each subsequent translation. The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not.

Source:
Inside to Outside
- **Static NAT** translating inside private IP to outside public IP
- *example:* assigning outside, public IP to internal web server

Outside to Inside
- **Translating outside public IP to inside private IP**
- *example:* port-forwarding specific port to inside host from the outside interface IP

### Inside to Outside

For inside to outside NAT, imagine you have an internal web server you want to NAT to an outside, public IP. Here are what those commands would look like:

```bash
ip nat inside source static 192.168.1.5 22.33.44.55
```

With that command, the internal device @ 192.168.1.5 would be NAT’ed to the public IP 22.33.44.55. This is referred to as static NAT.

### Outside to Inside

Outside to inside NAT involves translating a public IP back to a private, inside IP address. This is commonly done with a specific port involved as well. It’s all dependant on your situation, not required by any means. First off, your configuration would look like this:

```bash
ip nat outside source static tcp 22.33.44.55 22 192.168.1.5 22
```

What you are seeing is that all tcp/22 traffic sourcing in the outside interface from the IP 22.33.44.55 will be translated to 192.168.1.5. That way, the destination device will reply to 192.168.1.5, not the public IP 22.33.44.55. This is useful in cases where devices may not have a default route, etc.

**US Patent 9,407,548**

**Patent Specification Support**

<table>
<thead>
<tr>
<th>Clause 4</th>
<th><strong>Researcher comment:</strong> Evidence demonstrates Cisco Nexus 9000 Series NX-OS Interfaces (ReNAT twin NAT) perform mapping of UPIP address (Registered IP address) in the datagram to customer-defined IP address (unregistered IP address).</th>
</tr>
</thead>
<tbody>
<tr>
<td>mapping addresses in the data to customer-defined IP addresses; and</td>
<td>Dynamic Network Address Translation (NAT) translates a group of real IP addresses into mapped IP addresses that are routable on a destination network. Dynamic NAT establishes a one-to-one mapping between unregistered and registered IP addresses; however, the mapping can vary depending on the registered IP address that is available at the time of communication.</td>
</tr>
</tbody>
</table>

**Cisco Nexus 9000 Series NX-OS Interfaces (Release 9.3x)**

**FIG. 7 depcts a flowchart that includes actions that a NOC may perform in facilitating communication between a user workstation and a remote computing device, according to embodiments described herein.** As illustrated in block 750, the datagram may be processed by the NOC and a different datagram may be generated for sending to the remote computing device. In block 752, UPIP addresses may be mapped in the datagram to customer-defined private IP addresses. In block 754, the datagram may be encrypted and transferred to the remote computing device. **A dynamic NAT configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact.**

**Dynamic NAT translations do not exist in the NAT translation table until a device receives traffic that requires translation. Dynamic translations are cleared or timed out when not in use to make space for new entries. Usually, NAT translation entries are cleared when the ternary content addressable memory (TCAM) entries are limited. The default minimum timeout for dynamic NAT translations is 30 minutes.**
Cisco NX-OS provides pool support for dynamic NAT. Dynamic NAT allows the configuration of a pool of global addresses that can be used to dynamically allocate a global address from the pool for every new translation. The addresses are returned to the pool after the session ages out or is closed. This allows for a more efficient use of addresses based on requirements.

Dynamic NAT Overview

Dynamic Network Address Translation (NAT) translates a group of real IP addresses into mapped IP addresses that are routable on a destination network. Dynamic NAT establishes a one-to-one mapping between unregistered and registered IP addresses; however, the mapping can vary depending on the registered IP address that is available at the time of communication.

A dynamic NAT configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact.

Dynamic NAT translations do not exist in the NAT translation table until a device receives traffic that requires translation. Dynamic translations are cleared or timed out when not in use to make space for new entries. Usually, NAT translation entries are cleared when the ternary content addressable memory (TCAM) entries are limited. The default minimum timeout for dynamic NAT translations is 30 minutes.

Source:
encrypting the data and transferring the data to the private network.

(Clause 5)

FIG. 7 depicts a flowchart that includes actions that a NOC may perform in facilitating communication between a user workstation and a remote computing device, according to embodiments described herein. As illustrated in block 750, the datagram may be processed by the NOC and a different datagram may be generated for sending to the remote computing device. In block 752, UPIP addresses may be mapped in the datagram to customer-defined private IP addresses. In block 754, the datagram may be encrypted and transferred to the remote computing device.

Researcher comment: Evidence demonstrates Cisco Nexus 9000 Series NX-OS Interfaces Supported Generic routing encapsulation to perform encrypting (encapsulating) the data packet and transferring the data to the private network of Destination (remote computing device).

The point-to-point IP-in-IP encapsulation and decapsulation is a type of tunnel that you can create to send encapsulated packets from a source tunnel interface to a destination tunnel interface. This type of tunnel will carry both inbound and outbound traffic.

You can use generic routing encapsulation (GRE) as the carrier protocol for a variety of passenger protocols. The following figure shows the IP tunnel components for a GRE tunnel. The original passenger protocol packet becomes the GRE payload and the device adds a GRE header to the packet. The device then adds the transport protocol header to the packet and transmits it.
• Carrier protocol—The protocol that is used to encapsulate the passenger protocol. Cisco NX-OS supports GRE as a carrier protocol.
• Cisco NX-OS supports the following maximum number of tunnels:
  • IP tunnels - 8 tunnels.
  • GRE and IP-in-IP regular tunnels - 6 tunnels, (7.0(3)I(2) and later)
• On Cisco Nexus 9200 Series switches, GRE packets that are received on an IP-in-IP tunnel are not dropped as expected and are instead forwarded to the packet destination.

Point-to-Point IP-in-IP Tunnel Encapsulation and Decapsulation

For 6.1(2)I(4), 7.0(3)I(2), and later, point-to-point IP-in-IP encapsulation and decapsulation is a type of tunnel that you can create to send encapsulated packets from a source tunnel interface to a destination tunnel interface. This type of tunnel will carry both inbound and outbound traffic.

GRE Tunnels

You can use generic routing encapsulation (GRE) as the carrier protocol for a variety of passenger protocols.

The following figure shows the IP tunnel components for a GRE tunnel. The original passenger protocol packet becomes the GRE payload and the device adds a GRE header to the packet. The device then adds the transport protocol header to the packet and transmits it.

Source:
Tunnelling provides a mechanism to transport packets of one protocol within another protocol. The protocol that is carried is called as the passenger protocol, and the protocol that is used for carrying the passenger protocol is called as the transport protocol. **Generic Routing Encapsulation (GRE)** is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

To configure the tunnel source and destination, issue the `tunnel source` (ip-address | interface-type) and `tunnel destination` (host-name | ip-address) commands under the interface configuration mode for the tunnel.

```plaintext
interface Tunnel0
ip address 10.0.0.2 255.255.255.252
tunnel source 65.17.89.11
tunnel destination 64.45.15.17
```

End of report 😊😊😊😊😊