Carrier Grade Network Address Translation

Carrier Grade Network Address Translation (CGN) is a large-scale NAT that translates private IPv4 addresses into public IPv4 addresses. CGN employs Network Address and Port Translation methods to aggregate multiple private IPv4 addresses into fewer public IPv4 addresses.

This module provides an overview of CGN and describes how to configure CGN.

Restrictions for Carrier Grade Network Address Translation

- Asymmetric routing with box-to-box (B2B) redundancy is not supported in Carrier Grade Network Address Translation (CGN) mode.
- B2B redundancy is not supported on broadband with CGN; B2B is supported on standalone CGN.
- Broadband is not supported with traditional NAT.
- CGN does not support IP sessions.
- NAT outside mappings are disabled automatically when CGN operating mode is configured using the **ip nat settings mode cgn** command.
- CGN does not support integration with Cisco Performance Routing (PfR). Commands with the **oer** keyword are not supported. For example, the **ip nat inside source route-map pool overload oer** and the **ip nat inside source list pool overload oer** commands are not supported.
- The **match-in-vrf** keyword for intra-VPN NAT is not supported with CGN.
- If you specify a destination port to configure timeout in CGN mode, the destination port is ignored and the local port is considered for timeout.
- The **ip nat settings log-destination** command is not supported in a Box-to-Box High-Availability set up.

Information About Carrier Grade Network Address Translation

Carrier Grade NAT Overview

Network Address Translation (NAT) is positioned between a private and public IP network and uses nonglobal, private IP addresses and a public IP address for translation. NAT dynamically maps one or more private IP addresses into one or more public (globally routable) IP addresses that use Network Address and Port Translation (NAPT) techniques. Traditionally, NAT boxes are deployed in residential home gateways (HGWs) to translate multiple private IP addresses that are configured on multiple devices inside the home to a single public IP address that is configured and provisioned on the HGW by the service provider. Service providers deploy NAT in such a way that multiple subscribers can share a single global IP address. The service provider NAT scales to several millions of NAT translations, making it a Carrier Grade NAT (CGN).

In CGN, packets that traverse from inside the network to outside require only the source address port translation; destination address port translation is not required. CGN can be standalone like traditional NAT or you can use it along with broadband access aggregation. CGN coexists with Intelligent Services Gateway (ISG) features such as Layer 4 Redirect and subscriber services such as traffic classes.

You can configure CGN by using the **ip nat settings mode cgn** command. Use the **ip nat settings mode default** command to change to the default or traditional NAT operating mode. In the CGN mode, you cannot configure any NAT outside mappings. Mode changes on an active NAT device are not allowed. However, when you change from the default NAT mode to CGN mode, all existing outside mappings have to be removed. Use the **no ip nat settings support mapping outside** command to remove all outside mappings and to prevent any new outside mappings from being configured. You can also remove outside mappings by using the **no** form of commands used to configure NAT outside. In case there are specific ports configured with TCP or UDP timeout values, remove the configuration of **ip nat translation port** *protocol port timeout* completely and configure the timeout values for these protocols using the same command. Alternatively, reload the device. Note, if you specify a destination port to configure timeout in CGN mode, the destination port is ignored and the local port is considered for timeout.

CGN increases the scalability of the number of NAT translations that can be supported because destination information is not stored.

CGN supports the following:

- All application-level gateways (ALGs) that are supported by traditional NAT. For more information about supported ALGs, see the *Using Application-Level Gateways with NAT* module of the *IP Addressing: NAT Configuration Guide*.
- Endpoint independent mapping and endpoint independent filtering.
- Hairpinning by using VRF-Aware Software Infrastructure (VASI) and policy-based routing (PBR). Hairpinning occurs when two subscribers are behind the same NAT device but can see each other only by using the global IP address.
- Interbox and intrabox redundancy.
- Lawful intercept.
- Logging of NAT high-speed logging (HSL) records. For more information about HSL, see the section "High-Speed Logging for NAT" in the *Maintaining and Monitoring NAT* module of the *IP Addressing: NAT Configuration Guide*.

- Multihoming, which is the ability to support multiple outside interfaces to provide connectivity through redundant or standby exit points. Depending on the configured routing topology, any exit interface that is marked as an outside interface can use a translation that was created previously.
- TCP timeout value of 2 hours and 4 minutes.
- VPN routing and forwarding (VRF)-aware NAT.
- CGN NAT can scale to higher number of translations on ESP200 using the **ip nat settings scale bind** command.

Carrier Grade NAT Support for Broadband Access Aggregation

You can configure Carrier Grade Network Address Translation (CGN) as an independent feature or use CGN along with broadband access aggregation.

Broadband access aggregation enables connections between multiple technologies such as cable, digital subscriber line (DSL), Ethernet, ISDN, and wireless devices that are connected to corporate VPNs, third-party applications, and the Internet.

PPP over Ethernet (PPPoE) connects hosts on a network over a simple bridging device to a remote aggregation concentrator. PPPoE is the predominant access protocol in broadband networks worldwide.

For PPPoE to work with CGN, either the virtual templates or the RADIUS server must provide the Network Address Translation (NAT) inside configuration. The NAT inside configuration can be downloaded as part of the RADIUS authentication or alternatively configure the **ip nat inside** command on the virtual template. This gets cloned into a virtual access interface that inherits the ip nat inside configuration. For the RADIUS server to provide the NAT inside configuration, configure the **aaa policy interface-config allow-subinterface** global command or configure the Cisco attribute-value pairs (AV pairs) lcp:allow-subinterface=yes and then include lcp:interface-config=ip nat inside in the RADIUS profile on a per-subscriber basis.

You can terminate a PPPoE session either in the global routing table or at a VRF instance.

CGN supports dual-stack (IPv4 and IPv6) PPP sessions. However, only IPv4 traffic is subject to NAT. The IPv6 traffic is not translated; it is routed as per the IPv6 routing configuration.

How to Configure Carrier Grade Network Address Translation

Based on your network configuration, you can configure static, dynamic, or dynamic PAT Carrier Grade NAT.

Note You must use at least one of the configurations described in the following tasks for Carrier Grade NAT to work.

Configuring Static Carrier Grade NAT

Static address translation (static NAT) allows one-to-one mapping between local and global addresses. Use the **ip nat inside source static** command to enable static NAT of the inside source address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **ip nat inside source static** *local-ip global-ip*
5. **interface gigabitethernet** *card/spaslot/port.subinterface-number*
6. **ip nat inside**
7. **exit**
8. **interface** *type number*
9. **ip nat outside**
10. **end**
11. **show ip nat translations** [**verbose**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat settings mode cgn** **Example:** `Device(config)# ip nat settings mode cgn`	Enables CGN operating mode.
Step 4	**ip nat inside source static** *local-ip global-ip* **Example:** `Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2`	Enables static Carrier Grade NAT of the inside source address.
Step 5	**interface gigabitethernet** *card/spaslot/port.subinterface-number* **Example:** `Device(config)# interface gigabitethernet 0/0/4`	Configures an interface and enters interface configuration mode. **Note** The NAT inside network can be applied to interface virtual-template when the router is used for broadband aggregation deployment.
Step 6	**ip nat inside** **Example:** `Device(config-if)# ip nat inside`	Indicates that the interface is connected to the inside network (the network that is subject to NAT translation).

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 9	**ip nat outside** **Example:** `Device(config-if)# ip nat outside`	Indicates that the interface is connected to the outside network.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 11	**show ip nat translations** [**verbose**] **Example:** `Device# show ip nat translations`	Displays active NAT translations.

Example

The following is sample output from the **show ip nat translations** command:

```
Device# show ip nat translations

Pro  Inside global         Inside local          Outside local         Outside global
udp  10.5.5.1:1025          192.0.2.1:4000        ---                    ---
udp  10.5.5.1:1024          192.0.2.3:4000        ---                    ---
udp  10.5.5.1:1026          192.0.2.2:4000        ---                    ---

Total number of translations: 3
```

The following is sample output from the **show ip nat translations verbose** command:

```
Device# show ip nat translations verbose

Pro  Inside global         Inside local          Outside local         Outside global
udp  10.5.5.1:1025          192.0.2.1:4000        ---                    ---
  create: 02/15/12 11:38:01, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
  entry-id: 0x0, use_count:1

udp  10.5.5.1:1024          192.0.2.3:4000        ---                    ---
  create: 02/15/12 11:38:00, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
  entry-id: 0x0, use_count:1

udp  10.5.5.1:1026          192.0.2.2:4000        ---                    ---
  create: 02/15/12 11:38:00, use: 02/15/12 11:39:02, timeout: 00:00:00
  Map-Id(In): 1
```

```
  Mac-Address: 0000.0000.0000    Input-IDB: TenGigabitEthernet1/1/0
  entry-id: 0x0, use_count:1

Total number of translations: 3
```

Configuring Dynamic Carrier Grade NAT

Dynamic address translation (dynamic NAT) maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **access-list** *standard-access-list-number* **permit** *source wildcard*
5. **access-list** *standard-access-list-number* **permit** *source wildcard*
6. **route-map** *map-tag*
7. **match ip address** [*access-list-number*]
8. **match ip next-hop** [*access-list-number*]
9. **exit**
10. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
11. **ip nat inside source route-map** *name* **pool** *name*
12. **interface gigabitethernet** *card/spaslot/port.subinterface-number*
13. **ip nat inside**
14. **exit**
15. **interface** *type number*
16. **ip nat outside**
17. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat settings mode cgn** **Example:** `Device(config)# ip nat settings mode cgn`	Enables CGN operating mode.

	Command or Action	Purpose
Step 4	**access-list** *standard-access-list-number* **permit** *source wildcard* **Example:** `Device(config)# access-list 1 permit 10.1.1.0 0.0.0.255`	Defines a standard access list and specifies a host. • Access list 1 defined in this step is used by the **match ip address** command.
Step 5	**access-list** *standard-access-list-number* **permit** *source wildcard* **Example:** `Device(config)# access-list 2 permit 10.5.5.0 0.0.0.255`	Defines a standard access list and specifies a host. • Access list 2 defined in this step is used by the **match ip next-hop** command.
Step 6	**route-map** *map-tag* **Example:** `Device(config)# route-map nat-route-map`	Defines conditions for redistributing routes from one routing protocol into another or enables policy routing and enters route-map configuration mode.
Step 7	**match ip address** [*access-list-number*] **Example:** `Device(config-route-map)# match ip address 1`	Distributes any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list or performs policy routing on packets.
Step 8	**match ip next-hop** [*access-list-number*] **Example:** `Device(config-route-map)# match ip next-hop 2`	Redistributes any routes that have a next-hop router address passed by one of the specified access lists.
Step 9	**exit** **Example:** `Device(config-route-map)# exit`	Exits route-map configuration mode and enters global configuration mode.
Step 10	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 prefix-length 16`	Defines a pool of IP addresses for NAT.
Step 11	**ip nat inside source route-map** *name* **pool** *name* **Example:** `Device(config)# ip nat inside source route-map nat-route-map pool nat-pool`	Enables dynamic NAT of the inside source address.
Step 12	**interface gigabitethernet** *card/spaslot/port.subinterface-number* **Example:** `Device(config)# interface gigabitethernet 0/0/5`	Configures an interface and enters interface configuration mode. **Note** The NAT inside network can be applied to interface virtual-template when the router is used for broadband aggregation deployment.

	Command or Action	Purpose
Step 13	**ip nat inside** **Example:** `Device(config-if)# ip nat inside`	Indicates that the interface is connected to the inside network (the network that is subject to NAT translation).
Step 14	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 15	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/1`	Configures an interface and enters interface configuration mode.
Step 16	**ip nat outside** **Example:** `Device(config-if)# ip nat outside`	Indicates that the interface is connected to the outside network.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuring Dynamic Port Address Carrier Grade NAT

Port Address Translation (PAT) or overloading is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many-to-one mapping) by using different ports. PAT enables thousands of users to connect to the Internet by using only one real global IP address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat settings mode cgn**
4. **ip nat inside source list** *number* **pool** *name* [**overload**]
5. **ip nat pool** *name start-ip end-ip* **netmask** *netmask*
6. **access-list** *standard-access-list-number* **permit** *source wildcard*
7. **interface gigabitethernet** *card/spaslot/port.subinterface-number*
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip nat outside**
12. **end**
13. **show ip nat statistics**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip nat settings mode cgn** **Example:** `Device(config)# ip nat settings mode cgn`	Enables CGN operating mode.
Step 4	**ip nat inside source list** *number* **pool** *name* [**overload**] **Example:** `Device(config)# ip nat inside source list 1 pool nat-pool overload`	Enables the router to use one global address for many local addresses. • When you configure the **overload** keyword, the TCP or UDP port number of each inside host distinguishes between multiple conversations using the same local IP address. • The **overload** keyword configures overloading or PAT.
Step 5	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* **Example:** `Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 netmask 255.255.0.0`	Defines a pool of IP addresses for NAT.
Step 6	**access-list** *standard-access-list-number* **permit** *source wildcard* **Example:** `Device(config)# access-list 1 permit 172.16.0.0 255.255.0.0`	Defines a standard access list and specifies a host.
Step 7	**interface gigabitethernet** *card/spaslot/port.subinterface-number* **Example:** `Device(config)# interface gigabitethernet 0/0/6`	Configures an interface and enters interface configuration mode. **Note** The NAT inside network can be applied to interface virtual-template when the router is used for broadband aggregation deployment.
Step 8	**ip nat inside** **Example:** `Device(config-if)# ip nat inside`	Indicates that the interface is connected to the inside network (the network that is subject to NAT translation).

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/2`	Configures an interface and enters interface configuration mode.
Step 11	**ip nat outside** **Example:** `Device(config-if)# ip nat outside`	Indicates that the interface is connected to the outside network.
Step 12	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 13	**show ip nat statistics** **Example:** `Device# show ip nat statistics`	Displays NAT statistics.

Example

The following is sample output from the **show ip nat statistics** command:

```
Device# show ip nat statistics

Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  TenGigabitEthernet2/0/0, TenGigabitEthernet2/1/0, TenGigabitEthernet2/2/0
  TenGigabitEthernet2/3/0
Inside interfaces:
  TenGigabitEthernet1/0/0, TenGigabitEthernet1/1/0, TenGigabitEthernet1/2/0
  TenGigabitEthernet1/3/0
Hits: 59230465  Misses: 3
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 102 pool mypool refcount 3
 pool mypool: netmask 255.255.255.0
        start 10.5.5.1 end 10.5.5.5
        type generic, total addresses 5, allocated 1 (20%), misses 0
nat-limit statistics:
 max entry: max allowed 2147483647, used 3, missed 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

Logging Destination IP Address and Port Details in Carrier Grade NAT (CGN) Mode

In the Carrier Grade NAT (CGN) mode, the destination IP address and port details are not logged when High Speed Logging (HSL) records are generated. You can still log the destination IP address and destination port details using the classic NAT mode, but that does not support Endpoint-independent filtering (EIF).

Once the **ip nat settings log-destination** command is configured in the Carrier Grade NAT (CGN) mode, the destination IP address and destination port details are included in the add and delete HSL records.

To enable including the destination IP and destination port information in the HSL messages for Carrier Grade NAT (CGN) mode, use the following **ip nat settings log-destination** command.

Example

```
Device# show run | in log
ip nat settings log-destination
ip nat log translations flow-export v9 udp ipv6-destination 2001::2 30000 source
GigabitEthernet0/0/3
ip nat log translations flow-export v9 udp destination 172.27.61.85 20000
```

Configuration Examples for Carrier Grade Network Address Translation

Example: Configuring Static Carrier Grade NAT

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat inside source static 192.168.2.1 192.168.34.2
Device(config)# interface gigabitethernet 0/0/6
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip nat outside
Device(config-if)# end
```

Example: Configuring Dynamic Carrier Grade NAT

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Device(config)# access-list 2 permit 10.5.5.0 0.0.0.255
Device(config)# route-map nat-route-map
Device(config-route-map)# match ip address 1
Device(config-route-map)# match ip next-hop 2
Device(config-route-map)# exit
Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 prefix-length 16
Device(config)# ip nat inside source route-map nat-route-map pool nat-pool
```

```
Device(config)# interface gigabitethernet 0/0/5
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ip nat outside
Device(config-if)# end
```

Example: Configuring Dynamic Port Address Carrier Grade NAT

```
Device# configure terminal
Device(config)# ip nat settings mode cgn
Device(config)# ip nat inside source list 1 pool nat-pool overload
Device(config)# ip nat pool nat-pool 10.1.1.1 10.1.254.254 netmask 255.255.0.0
Device(config)# access-list 1 permit 172.16.0.0 255.255.0.0
Device(config)# interface gigabitethernet 0/0/4
Device(config-if)# ip nat inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/3
Device(config-if)# ip nat outside
Device(config-if)# end
```

Additional References for Carrier Grade Network Address Translation

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
NAT commands	IP Addressing Command Reference
NAT ALGs	“Using Application-Level Gateways with NAT”
HSL messages	“Monitoring and Maintaining NAT”

Standards and RFCs

Standard/RFC	Title
RFC 4787	*Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
RFC 5582	*Location-to-URL Mapping Architecture and Framework*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Carrier Grade Network Address Translation

Table 1: Feature Information for Carrier Grade Network Address Translation

Feature Name	Releases	Feature Information
Carrier Grade Network Address Translation	Cisco IOS XE Release 3.6S	Carrier Grade Network Address Translation (CGN) is a large-scale NAT that translates private IPv4 addresses into public IPv4 addresses. CGN employs Network Address and Port Translation methods to aggregate multiple private IPv4 addresses into fewer public IPv4 addresses. The following commands were introduced or modified: **ip nat settings mode** and **ip nat settings support mapping outside**. **Note** This feature is not supported on ISR 4000 platform.