

Bulk Logging and Port Block Allocation

The Bulk Logging and Port Block Allocation feature allocates a block of ports for translation instead of allocating individual ports. This feature is supported only in carrier-grade Network Address Translation (CGN) mode.

This module provides information about the feature and how to configure it.

- Prerequisites for Bulk Logging and Port Block Allocation, on page 1
- Restrictions for Bulk Logging and Port Block Allocation, on page 1
- Information About Bulk Logging and Port Block Allocation, on page 2
- How to Configure Bulk Logging and Port Block Allocation, on page 4
- Configuration Examples for Bulk Logging and Port Block Allocation, on page 6
- Additional References for Bulk Logging and Port Block Allocation, on page 8

Prerequisites for Bulk Logging and Port Block Allocation

- Enable the carrier-grade Network Address Translation (CGN) mode before enabling the Bulk Logging and Port Block Allocation feature.
- Enable paired-address pooling for this feature to work.

Restrictions for Bulk Logging and Port Block Allocation

- The Bulk Logging and Port Block Allocation feature is not supported on interface overload configurations because Network Address Translation (NAT) does not own the port space, the device owns it. You can configure an interface-overload mapping with this feature; however, no messages will be logged for the configuration.
- Destination information is not logged.
- Application layer gateways (ALGs) that require consecutive port pairings only work when bulk-port allocation is configured with a step size of one. For more information on step size, see "Bulk Logging and Port Block Allocation Overview, on page 2."
- Only bulk logging of messages is performed when this feature is enabled.

- ALG ports can be used for bulk-port allocation; however, this can cause degraded performance in sessions associated with these ports. If your configuration does not need ALGs, we recommend that you disable ALGs using the CLI.
- Syslog is not supported.
- Low ports, ports below 1024, are not supported; any application that requires a low port does not work with this feature.
- Bulk-port allocation pools must not overlap with static NAT mappings (particularly static mappings with ports) for this feature to work.
- The **ip nat service full-range** command is not supported.
- Enabling Port Block Allocation on Cisco Catalyst 8500 Series may raise QFP utilization and reduce device performance.

Information About Bulk Logging and Port Block Allocation

Bulk Logging and Port Block Allocation Overview

The Bulk Logging and Port Block Allocation feature allocates ports to users in blocks, instead of allocating individual ports. When a session is started from inside the network, instead of allocating a single global IP address and a global port, multiple global ports of a single global IP address are allocated for Network Address Translation (NAT) of traffic. Based on the volume of translations, additional blocks of ports can be allocated.

To allocate port sets, you can use either the consecutive port-set method or the scattered port-set method. In the consecutive port-set method, a user is allocated a set of ports with consecutive port numbers. It is easy to determine the port numbers in the consecutive method and this as a result, can be a security threat.

The Bulk Logging and Port Block Allocation feature uses the scattered port-set method, which allows you to define a start port number, a step value, and the number of ports to allocate. For example, if the starting port number is 4000, the step value is four, and the number of ports is 512, then the step value of four is added to 4000 to get the second port number. Four is added again to 4004 to get the third port number and this process repeats until you have 512 ports in the port set. This method of port-set allocation provides better security.

Some application layer gateways (ALGs) require two consecutive global ports to operate correctly. These ALGs are supported with this feature only when a step value of one is configured, which allocates a consecutive port set.

You must enable NAT paired-address pooling support for this feature to work. This feature also supports Point-to-Point Tunneling Protocol (PPTP).



Note This feature is supported only in carrier-grade NAT (CGN) mode; therefore only source information is logged when this feature is configured. Destination information is not logged. For more information about CGN, see the “Carrier-Grade Network Address Translation" module in *IP Addressing: NAT Configuration Guide*.

Port Size in Bulk Logging and Port Block Allocation

Port size is configurable and determines the number of ports allocated in each port set. However, ports below 1024, also known as low ports, will not work when bulk logging and port-block allocation is configured.

The first port that is allocated is always the first port in the set. Initially, ports are likely to be allocated in a linear method; however, as sessions are released and ports are freed, the allocation is semi-random. A port set is freed when the last session referencing it is freed.

A few port sets are reserved for users using a specific global IP address. Therefore, when allocated ports are used up, a session can use a reserved port set. If all reserved port sets are used, the session is dropped.

The default port size is 512 ports, but it can differ based on the configured paired-address pooling limit. The following table provides information of the default port size when various paired-address pooling limits are configured:

Table 1: Default Port Size Based on Paired-Address Pooling Support

Paired-Address Pooling Limit	Default Bulk-Port Allocation Port Size	Maximum Port Step Size
120	512 ports	8
30	2048 ports	2
60	1024 ports	4
250	256 ports	4
500	128 ports	8
1000	64 ports	16

High-Speed Logging in Bulk Logging and Port Block Allocation

The Bulk Logging and Port Block Allocation feature reduces the volume of Network Address Translation (NAT) high-speed logging (HSL). The reduction is accomplished by dynamically allocating a block of global ports instead of a single global port.

Messages are usually logged when a session is created and destroyed. In bulk port allocation, messages are logged when a port set is allocated or freed.

The following table provides information about HSL fields, their format and value:

Table 2: HSL Field Description

Field	Format	ID	Value
Source IP address	IPv4 address	8	Varies
Translated source address	IPv4 address	225	Varies
VRF[1] ID	32-bit ID	234	Varies
Protocol	8-bit value	4	Varies

Field	Format	ID	Value
Event	8-bit value	230	• 0—Invalid • 1—Add event • 2—Delete event
UNIX timestamp in milliseconds	64-bit value	323	Varies
Port block start	16-bit port	361	Varies
Port block step size	16-bit step size	363	Varies
Number of ports in the block	16-bit number	364	Varies

[1] virtual routing and forwarding

How to Configure Bulk Logging and Port Block Allocation

Configuring Bulk Logging and Port-Block Allocation

Before you configure bulk logging and port-block allocation, you must:

- Enable carrier-grade Network Address Translation (CGN) mode.
- Enable NAT paired-address pooling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **interface** *type number*
7. **ip nat outside**
8. **exit**
9. **ip nat settings mode cgn**
10. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
11. **access-list** *access-list-number* **permit source** [*source-wildcard*]
12. **ip nat inside source list** *access-list-number* **pool** *name*
13. **ip nat settings pap bpa set-size 512 step-size 8**
14. **ip nat log translations flow-export v9 udp destination** *addr port*
15. **end**
16. **show ip nat translations**

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	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip nat inside** **Example:** `Device(config-if)# ip nat inside`	Connects the interface to the inside network, which is subject to Network Address Translation (NAT).
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Specifies an interface and enters interface configuration mode.
Step 7	**ip nat outside** **Example:** `Device(config-if)# ip nat outside`	Connects the interface to the outside network.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**ip nat settings mode cgn** **Example:** `Device(config)# ip nat settings mode cgn`	Enables CGN mode.
Step 10	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **Example:** `Device(config)# ip nat pool net-208 192.168.202.129 192.168.202.132 prefix-length 24`	Defines a pool of global addresses to be allocated as needed.

	Command or Action	Purpose
Step 11	**access-list** *access-list-number* **permit source** [*source-wildcard*] **Example:** `Device(config)# access-list 1 permit source 192.168.34.0 0.0.0.255`	Defines a standard access list that permits addresses that are to be translated.
Step 12	**ip nat inside source list** *access-list-number* **pool** *name* **Example:** `Device(config)# ip nat inside source list 1 pool net-208`	Establishes dynamic NAT by specifying the access list and the IP address pool defined in Step 10 and Step 11.
Step 13	**ip nat settings pap bpa set-size 512 step-size 8** **Example:** `Device(config)# ip nat settings pap bpa set-size 512 step-size 8`	Configures bulk-port allocation.
Step 14	**ip nat log translations flow-export v9 udp destination** *addr port* **Example:** `Device(config)# ip nat log translations flow-export v9 udp destination 10.1.1.1 2055`	Enables the high-speed logging (HSL) of all NAT translations.
Step 15	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 16	**show ip nat translations** **Example:** `Device# show ip nat translations`	Displays active NAT translations.

Configuration Examples for Bulk Logging and Port Block Allocation

Example: Configuring Bulk Logging and Port Block Allocation

In the following example, dynamic carrier-grade NAT (CGN) and paired-address pooling is configured for bulk-port allocation.

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

```
Device(config-if)# exit
Device(config)# ip nat settings mode cgn
Device(config)# ip nat pool net-208 192.168.202.129 192.168.202.132 prefix-length 24
Device(config)# access-list 1 permit source 192.168.34.0 0.0.0.255
Device(config)# ip nat inside source list 1 pool net-208
Device(config)# ip nat settings pap bpa set-size 512 step-size 8
Device(config)# ip nat log translations flow-export v9 udp destination 10.1.1.1 2055
Device(config)# end
```

Verifying Bulk Logging and Port Block Allocation

SUMMARY STEPS

1. **show ip nat bpa**
2. **show ip nat pool name***pool-name*

DETAILED STEPS

Procedure

Step 1 **show ip nat bpa**

Example:

```
Device# show ip nat bpa
```

Displays Network Address Translation (NAT) bulk logging and port-block allocation settings.

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

```
Device# show ip nat bpa

Paired Address Pooling (PAP)
Limit: 120 local addresses per global address
Bulk Port Allocation (BPA)
Port set size: 1024 ports in each port set allocation
Port step size: 1
Single set: True
```

Step 2 **show ip nat pool name***pool-name*

Example:

```
Device# show ip nat pool name pool1
```

Displays NAT pool and port statistics.

The following is sample output from the **show ip nat pool name pool1** command:

```
Device# show ip nat pool name pool1

NAT Pool Statistics
Pool name pool1, id 1
Assigned Available
Addresses 0 5
UDP Low Ports 0 0
TCP Low Ports 0 0
UDP High Ports 0 150
```

```
TCP High Ports 0 150
(Low ports are less than 1024. High ports are greater than or equal to 1024.)
```

The following is sample output from the **show ip nat pool name pool3** command:

```
Device# show ip nat pool name pool3

NAT Pool Statistics
Pool name pool3, id 4
Assigned Available
Addresses 0 9
UDP Low Ports 0 0
TCP Low Ports 0 0
UDP High Ports 0 1080
TCP High Ports 0 1080
(Low ports are less than 1024. High ports are greater than or equal to 1024.)
```

Additional References for Bulk Logging and Port Block Allocation

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Master Command List
NAT commands	Cisco IOS IP Addressing Services Command Reference
Carrier-grade NAT	"Carrier-Grade Network Address Translation" module in the *IP Addressing NAT Configuration Guide*
Paired-address pooling support	"Paired-Address Pooling Support in NAT" module in the *IP Addressing NAT Configuration Guide*

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