# Configuring NetFlow Aggregation Caches

This module contains information about and instructions for configuring NetFlow aggregation caches. The NetFlow main cache is the default cache used to store the data captured by NetFlow. By maintaining one or more extra caches, called aggregation caches, the NetFlow Aggregation feature allows limited aggregation of NetFlow data export streams on a router. The aggregation scheme that you select determines the specific kinds of data that are exported to a remote host.

NetFlow is a Cisco IOS XE application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Prerequisites for Configuring NetFlow Aggregation Caches

Before you enable NetFlow you must:

- Configure the router for IP routing
- Ensure that either Cisco Express Forwarding or fast switching is enabled on your router and on the interfaces on which you want to configure NetFlow.
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

If you need autonomous system (AS) information from the aggregation, make sure to specify either the **peer-as**or **origin-as** keyword in your export command if you have not configured an export format version.

You must explicitly enable each NetFlow aggregation cache by entering the **enabled** keyword from aggregation cache configuration mode.

Router-based aggregation must be enabled for minimum masking.

# Restrictions for Configuring NetFlow Aggregation Caches

### Performance Impact

Configuring Egress NetFlow accounting with the **ip flow egress** command might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

# NetFlow Data Export Restrictions

### Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets). The increase in bandwidth usage varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

# Information About Configuring NetFlow Aggregation Caches

## NetFlow Aggregation Caches

### NetFlow Aggregation Cache Benefits

Aggregation of export data is typically performed by NetFlow collection tools on management workstations. Router-based aggregation allows limited aggregation of NetFlow export records to occur on the router. Thus, you can summarize NetFlow export data on the router before the data is exported to a NetFlow data collection system, which has the following benefits:

- Reduces the bandwidth required between the router and the workstations
- Reduces the number of collection workstations required
- Improves performance and scalability on high flow-per-second routers

### NetFlow Aggregation Cache Schemes

Cisco IOS XE NetFlow aggregation maintains one or more extra caches with different combinations of fields that determine which flows are grouped together. These extra caches are called aggregation caches. The combinations of fields that make up an aggregation cache are referred to as schemes.

You can configure each aggregation cache with its individual cache size, cache ager timeout parameter, export destination IP address, and export destination UDP port. The normal flow ager process runs on each active aggregation cache the same way it runs on the main cache. On-demand aging is also supported. Each aggregation cache contains different field combinations that determine which data flows are grouped. The default aggregation cache size is 4096 bytes.

You configure a cache aggregation scheme through the use of arguments to the **ip flow-aggregation cache** command. NetFlow supports the following five non-ToS based cache aggregation schemes:

- Autonomous system (AS) aggregation scheme
- Destination prefix aggregation scheme
- Prefix aggregation scheme
- Protocol port aggregation scheme
- Source prefix aggregation scheme

The NetFlow Type of Service-Based Router Aggregation feature introduced support for additional cache aggregation schemes, all of which include the Type of Service (ToS) byte as one of the fields in the aggregation cache. The following are the six ToS-based aggregation schemes:

- AS-ToS aggregation scheme
- Destination prefix-ToS aggregation scheme
- Prefix-port aggregation scheme

- Prefix-ToS aggregation scheme
- Protocol-port-ToS aggregation scheme
- Source prefix-ToS aggregation scheme

**Note** Additional export formats (for instance, Version 9) are also supported. If you are using Version 9, the formats will be different from those shown in the figures. For more information about Version 9 export formats, see the "Configuring NetFlow and NetFlow Data Export" module.

## NetFlow Aggregation Scheme Fields

Each cache aggregation scheme contains field combinations that differ from any other cache aggregation scheme. The combination of fields determines which data flows are grouped and collected when a flow expires from the main cache. A flow is a set of packets that has common fields, such as the source IP address, destination IP address, protocol, source and destination ports, type-of-service, and the same interface on which the flow is monitored. To manage flow aggregation on your router, you need to configure the aggregation cache scheme that groups and collects the fields from which you want to examine data. The two tables below show the NetFlow fields that are grouped and collected for non-ToS and ToS based cache aggregation schemes.

The table below shows the NetFlow fields used in the non-ToS based aggregation schemes.

***Table 1: NetFlow Fields Used in the Non-ToS Based Aggregations Schemes***

| Field | AS | Protocol Port | Source Prefix | Destination Prefix | Prefix |
|---|---|---|---|---|---|
| Source prefix | | | X | | X |
| Source prefix mask | | | X | | X |
| Destination prefix | | | | X | X |
| Destination prefix mask | | | | X | X |
| Source app port | | X | | | |
| Destination app port | | X | | | |
| Input interface | X | | X | | X |
| Output interface | X | | | X | X |
| IP protocol | | X | | | |

| Field | AS | Protocol Port | Source Prefix | Destination Prefix | Prefix |
|---|---|---|---|---|---|
| Source AS | X | | X | | X |
| Destination AS | X | | | X | X |
| First time stamp | X | X | X | X | X |
| Last time stamp | X | X | X | X | X |
| Number of flows[1] | X | X | X | X | X |
| Number of packets | X | X | X | X | X |
| Number of bytes | X | X | X | X | X |

1 For the Cisco ASR 1000 series router, this value is always 0. This is because on the Cisco ASR 1000 series router, aggregation caches are managed not by extracting data from main cache flow records as they are aged out, but rather by examining each packet, independently of any main cache processing.

The table below shows the NetFlow fields used in the ToS based aggregation schemes.

***Table 2: NetFlow Fields Used in the ToS Based Aggregation Schemes***

| Field | AS-ToS | Protocol Port-ToS | Source Prefix-ToS | Destination Prefix-ToS | Prefix-ToS | Prefix-Port |
|---|---|---|---|---|---|---|
| Source prefix | | | X | | X | X |
| Source prefix mask | | | X | | X | X |
| Destination prefix | | | | X | X | X |
| Destination prefix mask | | | | X | X | X |
| Source app port | | X | | | | X |
| Destination app port | | X | | | | X |
| Input interface | X | X | X | | X | X |
| Output interface | X | X | | X | X | X |

| Field | AS-ToS | Protocol Port-ToS | Source Prefix-ToS | Destination Prefix-ToS | Prefix-ToS | Prefix-Port |
|---|---|---|---|---|---|---|
| IP protocol | | X | | | | X |
| Source AS | X | | X | | X | |
| Destination AS | X | | | X | X | |
| ToS | X | X | X | X | X | X |
| First time stamp | X | X | X | X | X | X |
| Last time stamp | X | X | X | X | X | X |
| Number of flows[2] | X | X | X | X | X | X |
| Number of packets | X | X | X | X | X | X |
| Number of bytes | X | X | X | X | X | X |

2 For the Cisco ASR 1000 series router, this value is always 0. This is because on the Cisco ASR 1000 series router, aggregation caches are managed not by extracting data from main cache flow records as they are aged out, but rather by examining each packet, independently of any main cache processing.

## NetFlow AS Aggregation Scheme

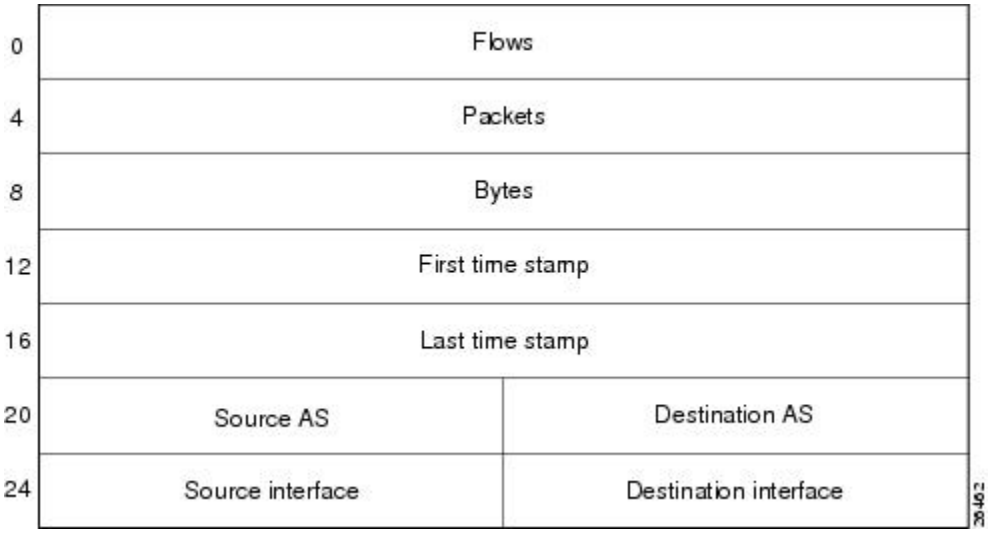
The NetFlow AS aggregation scheme reduces NetFlow export data volume substantially and generates AS-to-AS traffic flow data. The scheme groups data flows that have the same source BGP AS, destination BGP AS, input interface, and output interface.

The aggregated NetFlow data export records report the following:

- Source and destination BGP AS
- Number of packets summarized by the aggregated record
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Source interface
- Destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the AS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 1: Data Export Format for AS Aggregation Scheme***




The table below lists definitions for the data export record fields used in the AS aggregation scheme.

***Table 3: Data Export Record Field Definitions for AS Aggregation Scheme***

| Field | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source AS | Autonomous system of the source IP address (peer or origin) |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |

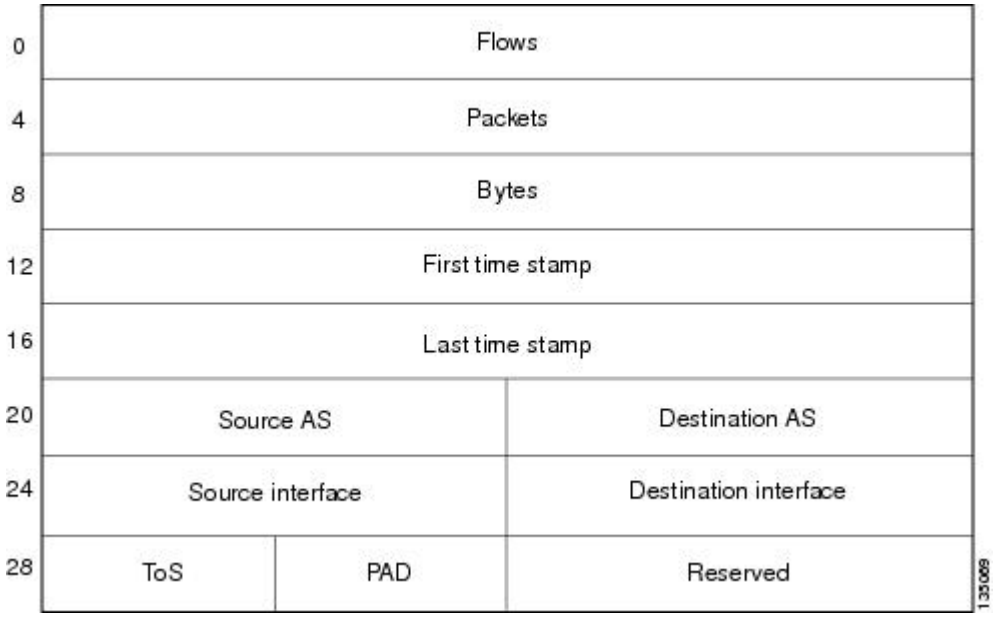
## NetFlow AS-ToS Aggregation Scheme

The NetFlow AS-ToS aggregation scheme groups flows that have the same source BGP AS, destination BGP AS, source and destination interfaces, and ToS byte. The aggregated NetFlow export record based on the AS-ToS aggregation scheme reports the following:

- Source BGP AS
- Destination BGP AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by this aggregated record
- Number of packets summarized by this aggregation record
- Source and destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for generating AS-to-AS traffic flow data, and for reducing NetFlow export data volume substantially. The figure below shows the data export format for the AS-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 2: Data Export Format for AS-ToS Aggregation Scheme***




The table below lists definitions for the data export record terms used in the AS-ToS aggregation scheme.

*Table 4: Data Export Record Term Definitions for AS-ToS Aggregation Scheme*

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source AS | Autonomous system of the source IP address (peer or origin) |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |
| ToS | Type of service byte |
| PAD | Zero field |
| Reserved | Zero field |

## NetFlow Destination Prefix Aggregation Scheme

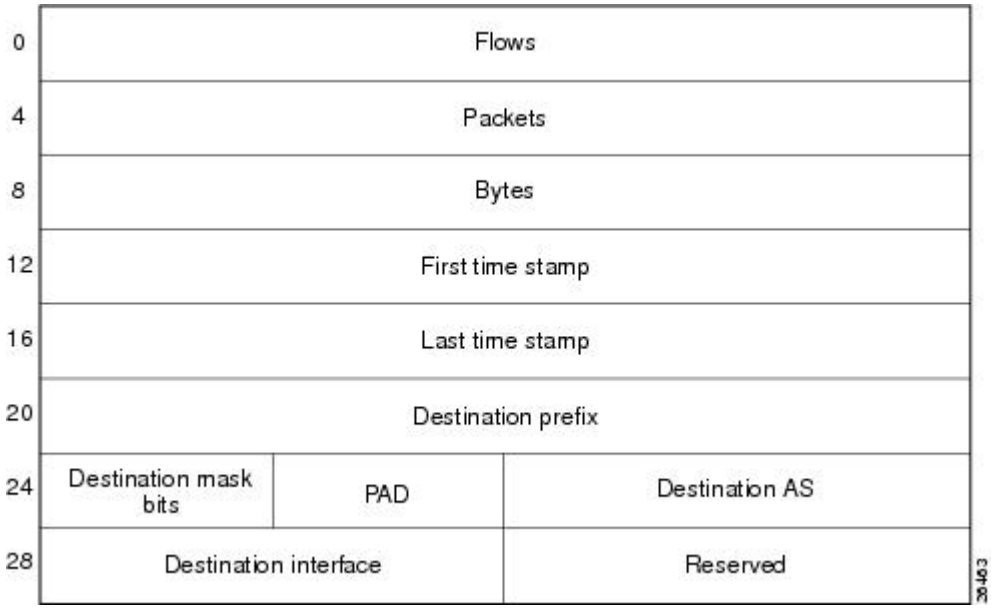
The destination prefix aggregation scheme generates data so that you can examine the destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same destination prefix, destination prefix mask, destination BGP AS, and output interface.

The aggregated NetFlow data export records report the following:

- Destination prefix
- Destination prefix mask
- Destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the destination prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 3: Destination Prefix Aggregation Data Export Record Format***




The table below lists definitions for the data export record terms used in the destination prefix aggregation scheme.

***Table 5: Data Export Record Term Definitions for Destination Prefix Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Destination prefix | Destination IP address ANDed with the destination prefix mask |
| Destination mask bits | Number of bits in the destination prefix |
| PAD | Zero field |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |

| Term | Definition |
|---|---|
| Destination interface | SNMP index of the output interface |
| Reserved | Zero field |

## NetFlow Destination Prefix-ToS Aggregation Scheme

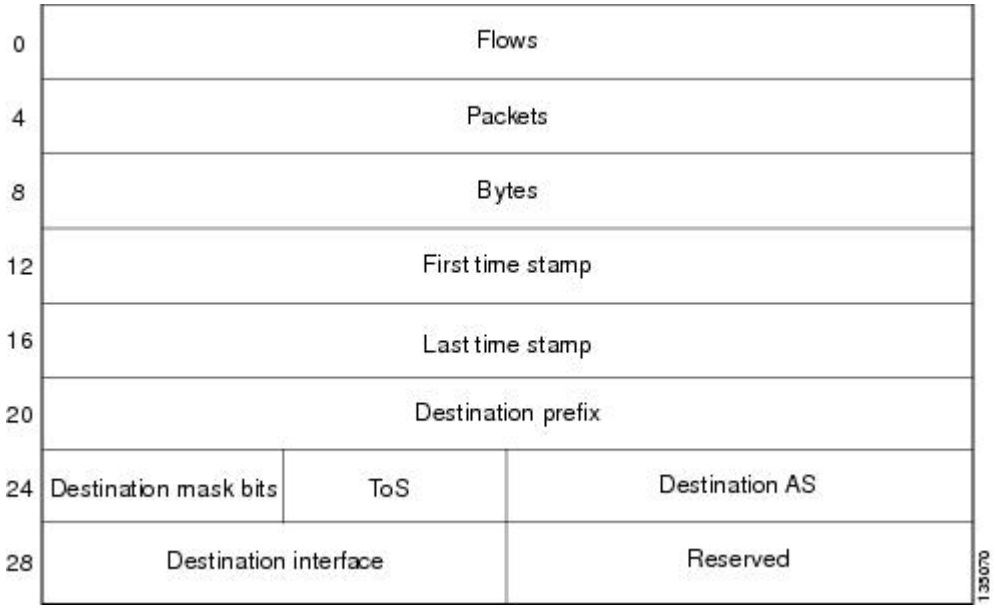
The NetFlow destination prefix-ToS aggregation scheme groups flows that have the same destination prefix, destination prefix mask, destination BGP AS, ToS byte, and output interface. The aggregated NetFlow export record reports the following:

- Destination IP address
- Destination prefix mask
- Destination AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the data export format

for the Destination prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 4: Data Export Format for Destination Prefix-ToS Aggregation Scheme***




The table below lists definitions for the data export record terms used in the destination prefix-ToS aggregation scheme.

***Table 6: Data Export Record Term Definitions for Destination Prefix-ToS Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Destination prefix | Destination IP address ANDed with the destination prefix mask |
| Dest mask bits | Number of bits in the destination prefix |
| ToS | Type of service byte |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |

| Term | Definition |
|---|---|
| Destination interface | SNMP index of the output interface |
| Reserved | Zero field |

## NetFlow Prefix Aggregation Scheme

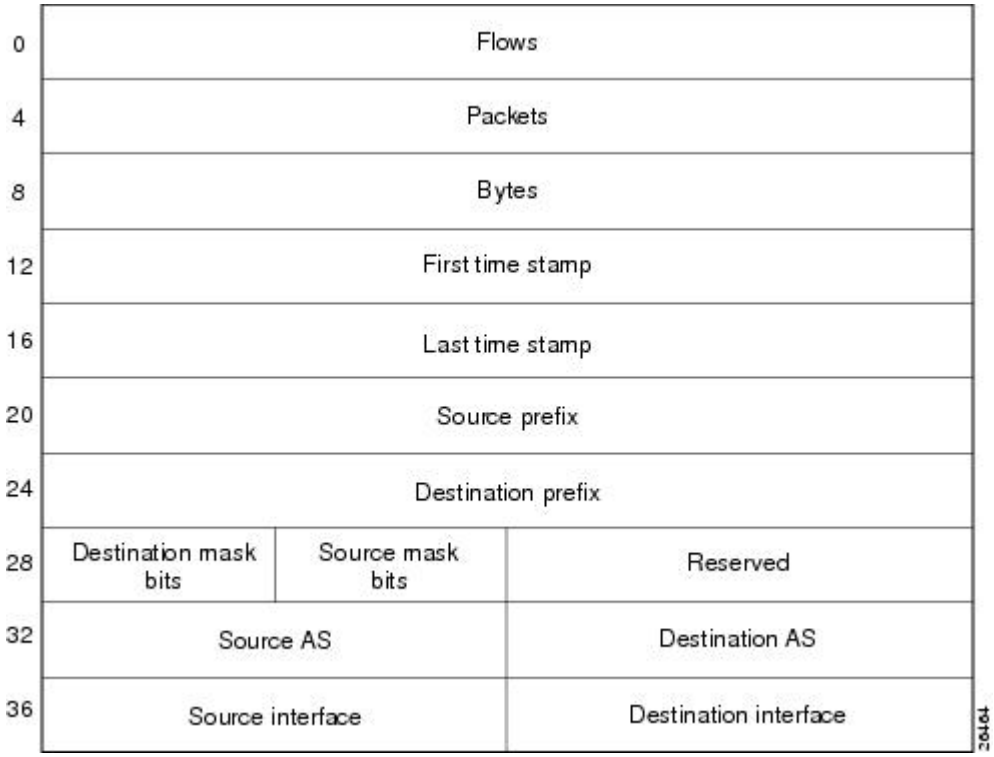
The NetFlow prefix aggregation scheme generates data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface, and output interface. See the figure below.

The aggregated NetFlow data export records report the following:

- Source and destination prefix
- Source and destination prefix mask
- Source and destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input and output interfaces
- Time stamp when the first packet is switched and time stamp when the last packet is switched

The figure below shows the data export format for the prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 5: Data Export Format for Prefix Aggregation Scheme***




The table below lists definitions for the data export record terms used in the prefix aggregation scheme.

***Table 7: Data Export Record Terms and Definitions for Prefix Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source prefix | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs |
| Destination prefix | Destination IP address ANDed with the destination prefix mask |

| Term | Definition |
|---|---|
| Destination mask bits | Number of bits in the destination prefix |
| Source mask bits | Number of bits in the source prefix |
| Reserved | Zero field |
| Source AS | Autonomous system of the source IP address (peer or origin) |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |

## NetFlow Prefix-Port Aggregation Scheme

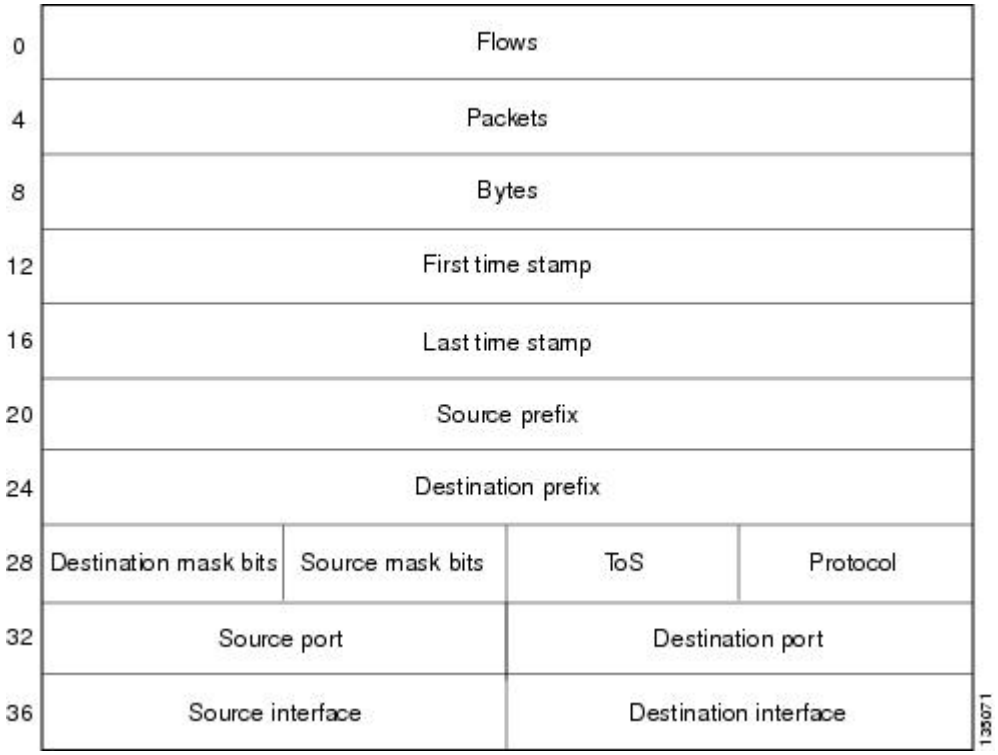
The NetFlow prefix-port aggregation scheme groups flows that have a common source prefix, source mask, destination prefix, destination mask, source port and destination port when applicable, input interface, output interface, protocol, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source port
- Destination port
- Source interface
- Destination interface
- Protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the

data export record for the prefix-port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 6: Data Export Record for Prefix-Port Aggregation Scheme***




The table below lists definitions for the data export record terms used in the prefix-port aggregation scheme.

***Table 8: Data Export Record Term Definitions for Prefix-Port Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source prefix | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs |
| Destination prefix | Destination IP address ANDed with the destination prefix mask |

| Term | Definition |
|---|---|
| Destination mask bits | Number of bits in the destination prefix |
| Source mask bits | Number of bits in the source prefix |
| ToS | Type of service byte |
| Protocol | IP protocol byte |
| Source port | Source UDP or TCP port number if applicable |
| Destination port | Destination User Datagram Protocol (UDP) or TCP port number |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |

## NetFlow Prefix-ToS Aggregation Scheme

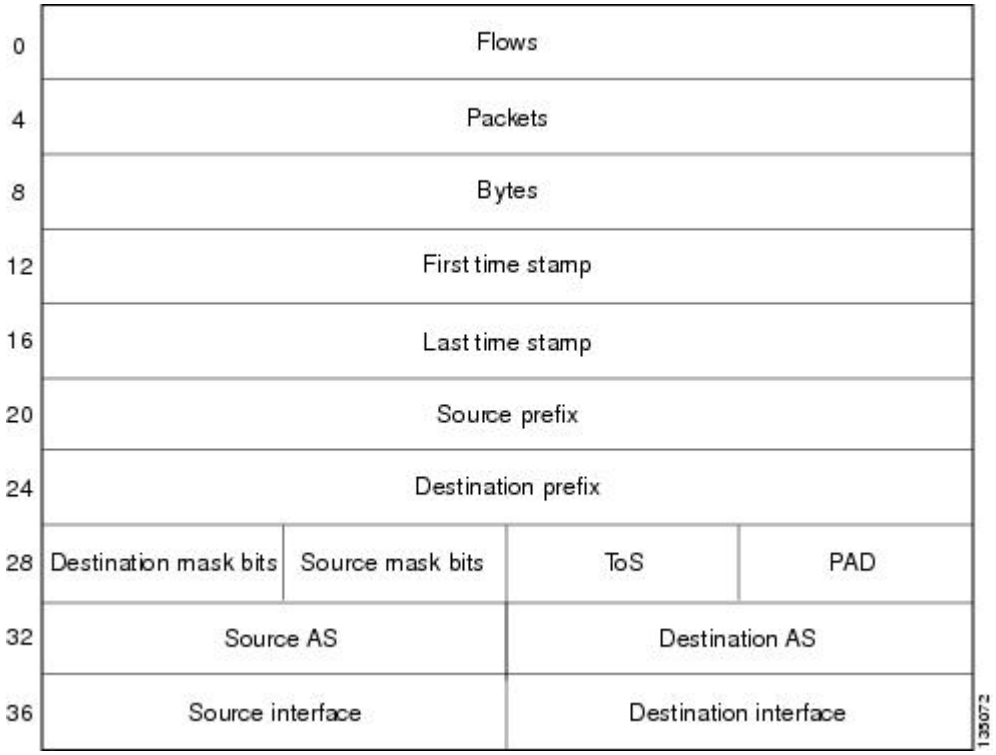
The NetFlow prefix-tos aggregation scheme groups together flows that have a common source prefix, source mask, destination prefix, destination mask, source BGP AS, destination BGP AS, input interface, output interface, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source AS
- Destination AS
- Source interface
- Destination interface
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below displays the data

export format for the prefix-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 7: Data Export Format for Prefix-ToS Aggregation Scheme***




The table below lists definitions for the data export record terms used in the prefix-ToS aggregation scheme.

***Table 9: Data Export Record Term Definitions for Prefix-ToS Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source prefix | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs |
| Destination prefix | Destination IP address ANDed with the destination prefix mask |

| Term | Definition |
|---|---|
| Destination mask bits | Number of bits in the destination prefix |
| Source mask bits | Number of bits in the source prefix |
| ToS | Type of service byte |
| Pad | Zero field |
| Source AS | Autonomous system of the source IP address (peer or origin) |
| Destination AS | Autonomous system of the destination IP address (peer or origin) |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |

## NetFlow Protocol Port Aggregation Scheme

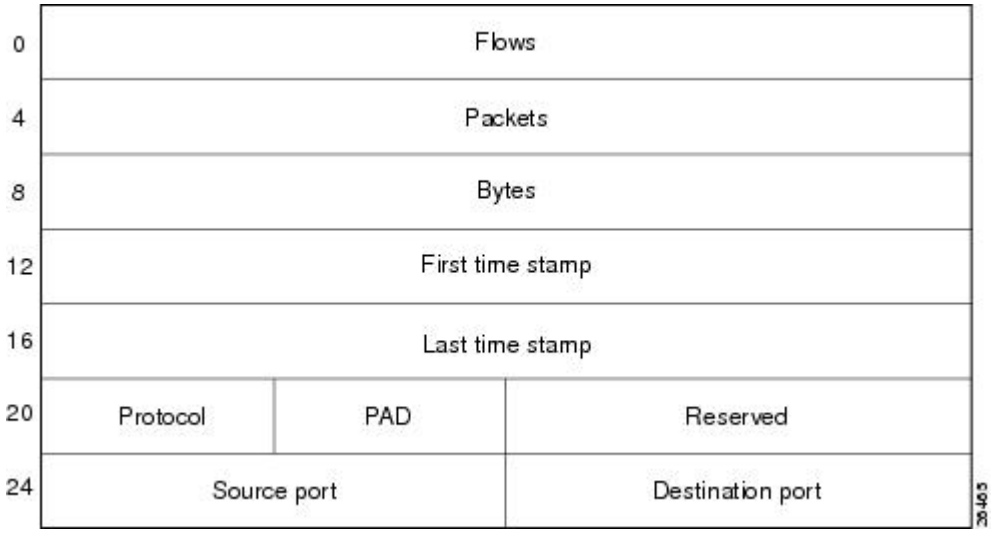
The NetFlow protocol port aggregation scheme captures data so that you can examine network usage by traffic type. The scheme groups data flows with the same IP protocol, source port number, and (when applicable) destination port number.

The aggregated NetFlow data export records report the following:

- Source and destination port numbers
- IP protocol (where 6 = TCP, 17 = UDP, and so on)
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the protocol port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 8: Data Export Format for Protocol Port Aggregation Scheme***




The table below lists definitions for the data export record terms used in the protocol port aggregation scheme.

***Table 10: Data Export Record Term Definitions for Protocol Port Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Protocol | IP protocol byte |
| PAD | Zero field |
| Reserved | Zero field |
| Source port | Source UDP or TCP port number if applicable |
| Destination port | Destination User Datagram Protocol (UDP) or TCP port number |

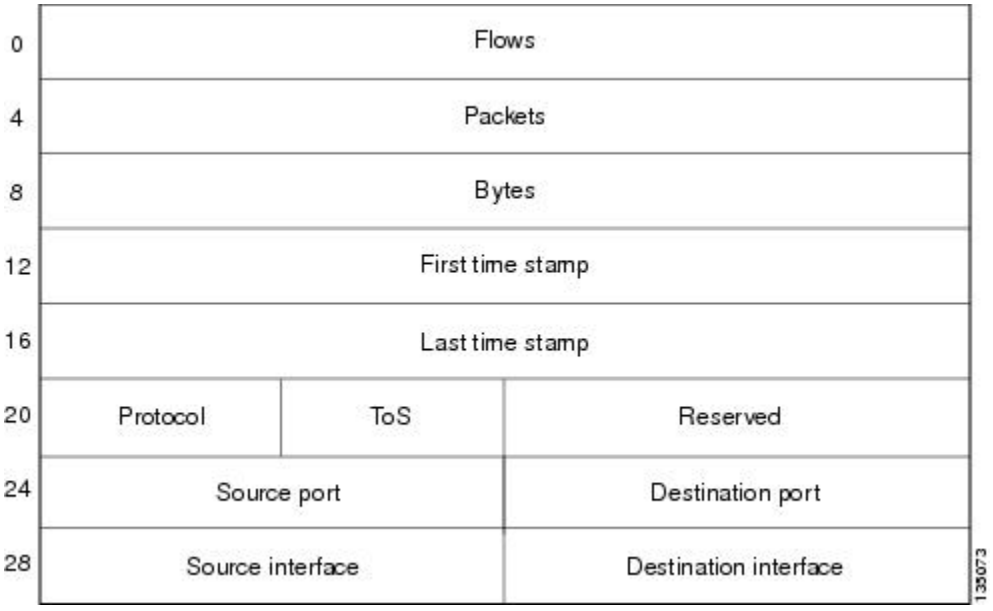
## NetFlow Protocol-Port-ToS Aggregation Scheme

The NetFlow protocol-port-tos aggregation scheme groups flows that have a common IP protocol, ToS byte, source and (when applicable) destination port numbers, and source and destination interfaces. The aggregated NetFlow Export record reports the following:

- Source application port number
- Destination port number
- Source and destination interface
- IP protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine network usage by type of traffic. The figure below shows the data export format for the protocol-port-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 9: Data Export Format for Protocol-Port-ToS Aggregation Scheme***




The table below lists definitions for the data export record terms used in the protocol-port-ToS aggregation scheme.

*Table 11: Data Export Record Term Definitions for Protocol-Port-ToS Aggregation Scheme*

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Protocol | IP protocol byte |
| ToS | Type of service byte |
| Reserved | Zero field |
| Source port | Source UDP or TCP port number if applicable |
| Destination port | Destination User Datagram Protocol (UDP) or TCP port number |
| Source interface | SNMP index of the input interface |
| Destination interface | SNMP index of the output interface |

## NetFlow Source Prefix Aggregation Scheme

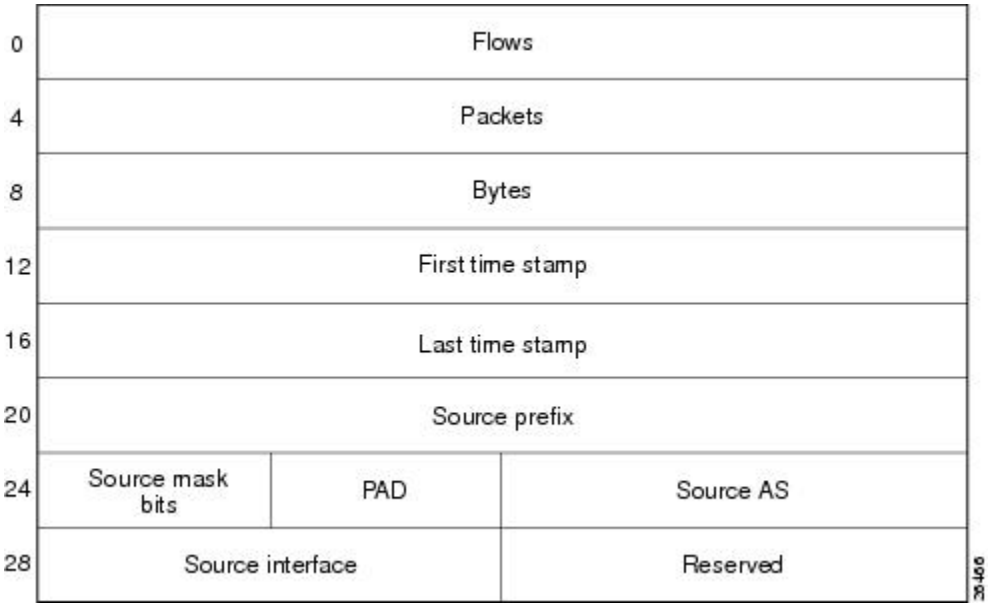
The NetFlow source prefix aggregation scheme captures data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, source prefix mask, source BGP AS, and input interface.

The aggregated NetFlow data export records report the following:

- Source prefix
- Source prefix mask
- Source BGP AS
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the source prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

***Figure 10: Data Export Format for Source Prefix Aggregation Scheme***




The table below lists definitions for the data export record terms used in the source prefix aggregation scheme.

***Table 12: Data Export Record Term Definitions for Source Prefix Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source prefix | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs |
| Source mask bits | Number of bits in the source prefix |
| PAD | Zero field |
| Source AS | Autonomous system of the source IP address (peer or origin) |

| Term | Definition |
|---|---|
| Source interface | SNMP index of the input interface |
| Reserved | Zero field |

## NetFlow Source Prefix-ToS Aggregation Scheme

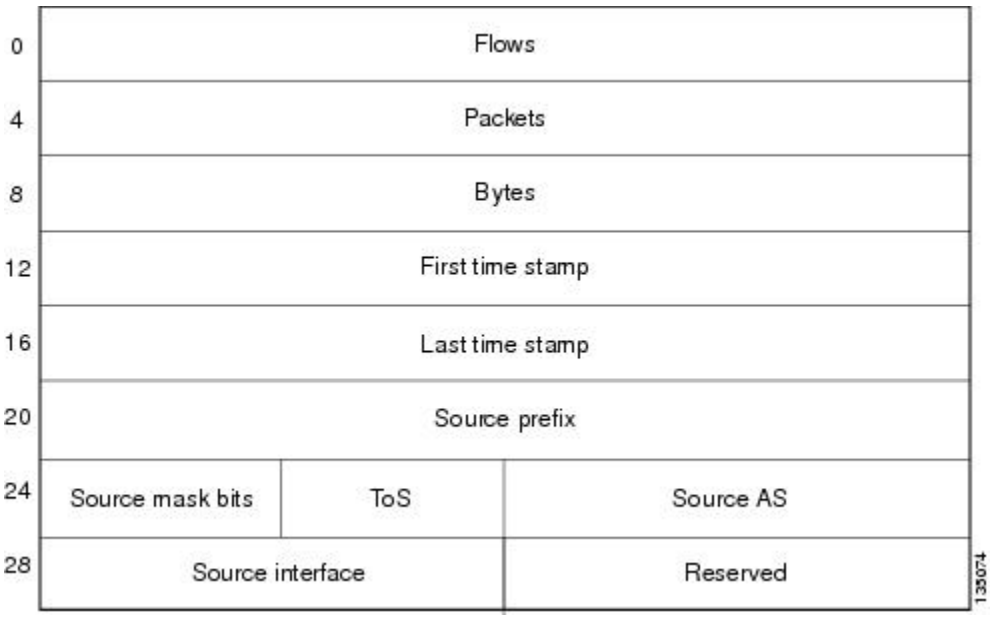
The NetFlow source prefix-ToS aggregation scheme groups flows that have a common source prefix, source prefix mask, source BGP AS, ToS byte, and input interface. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Source AS
- ToS byte
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The figure below shows the data export format for the source prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

**Note** When a router does not have a prefix for the source IP address in the flow, NetFlow uses 0.0.0.0 with 0 mask bits rather than making /32 entries. This prevents DOS attacks that use random source addresses from thrashing the aggregation caches. This is also done for the destination in the destination prefix-ToS, the prefix-ToS, and prefix-port aggregation schemes.

***Figure 11: Data Export Format for Source Prefix-ToS Aggregation Scheme***




The table below lists definitions for the data export record terms used in the source prefix-ToS aggregation scheme.

***Table 13: Data Export Record Term Definitions for Source Prefix-ToS Aggregation Scheme***

| Term | Definition |
|---|---|
| Flows | Number of main cache flows that were aggregated |
| Packets | Number of packets in the aggregated flows |
| Bytes | Number of bytes in the aggregated flows |
| First time stamp | System uptime when the first packet was switched |
| Last time stamp | System uptime when the last packet was switched |
| Source prefix | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs |

| Term | Definition |
|---|---|
| Source mask bits | Number of bits in the source prefix |
| ToS | Type of service byte |
| Source AS | Autonomous system of the source IP address (peer or origin) |
| Source interface | SNMP index of the input interface |
| Reserved | Zero field |

# NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview

Export formats available for NetFlow aggregation caches are the Version 9 export format and the Version 8 export format.

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme. Version 8 is the default export version for aggregation caches when data export is configured.

The Version 9 export format is flexible and extensible, which provides the versatility needed for the support of new fields and record types. You can use the Version 9 export format for both main and aggregation caches.

The Version 8 export format was added to support data export from aggregation caches. This format allows export datagrams to contain a subset of the Version 5 export data that is valid for the cache aggregation scheme.

Refer to the NetFlow Data Export section for more details.

# How to Configure NetFlow Aggregation Caches

## Configuring NetFlow Aggregation Caches

Perform this task to enable NetFlow and configure a NetFlow aggregation cache.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
4. **cache entries** *number*
5. **cache timeout active** *minutes*
6. **cache timeout inactive** *seconds*
7. **export destination** {{*ip-address* | *hostname*} *udp-port*}
8. Repeat Step 7 to configure a second export destination.
9. **export version** [**9**]
10. **enabled**
11. **exit**
12. **interface** *interface-type interface-number*
13. **ip flow** {**ingress** | **egress**}
14. **exit**
15. Repeat Steps 12 through 14 to enable NetFlow on other interfaces
16. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip flow-aggregation cache** {**as** \| **as-tos** \| **destination-prefix** \| **destination-prefix-tos** \| **prefix** \| **prefix-port** \| **prefix-tos** \| **protocol-port** \| **protocol-port-tos** \| **source-prefix** \| **source-prefix-tos**}<br><br>**Example:** | Specifies the aggregation cache scheme and enables aggregation cache configuration mode.<br>• The **as** keyword configures the AS aggregation cache.<br>• The **as-tos**keyword configures the AS ToS aggregation cache.<br>• The **destination-prefix** keyword configures the destination prefix aggregation cache.<br>• The **destination-prefix-tos** keyword configures the destination prefix ToS aggregation cache. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# ip flow-aggregation cache destination-prefix` | • The **prefix** keyword configures the prefix aggregation cache.<br>• The **prefix-port** keyword configures the prefix port aggregation cache.<br>• The **prefix-tos** keyword configures the prefix ToS aggregation cache.<br>• The **protocol-port** keyword configures the protocol port aggregation cache.<br>• The **protocol-port-tos** keyword configures the protocol port ToS aggregation cache.<br>• The **source-prefix** keyword configures the source prefix aggregation cache.<br>• The **source-prefix-tos** keyword configures the source prefix ToS aggregation cache. |
| **Step 4** | **cache entries** *number*<br>**Example:**<br>`Device(config-flow-cache)# cache entries 2048` | (Optional) Configures aggregation cache operational parameters.<br>• The **entries** *number* keyword-argument pair is the number of cached entries allowed in the aggregation cache. The range is from 1024 to 2000000. The default is 4096. |
| **Step 5** | **cache timeout active** *minutes*<br>**Example:**<br>`Device(config-flow-cache)# cache timeout active 15` | (Optional) Configures aggregation cache operational parameters.<br>• The **timeout** keyword dissolves the session in the aggregation cache.<br>• The **active** *minutes* keyword-argument pair specifies the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes. |
| **Step 6** | **cache timeout inactive** *seconds*<br>**Example:**<br>`Device(config-flow-cache)# cache timeout inactive 300` | (Optional) Configures aggregation cache operational parameters.<br>• The **timeout** keyword dissolves the session in the aggregation cache.<br>• The **inactive** *seconds*keyword-argument pair specifies the number of seconds that an inactive entry stays in the aggregation cache before the entry times out. The range is from 10 to 600 seconds. The default is 15 seconds. |
| **Step 7** | **export destination** {{*ip-address* \| *hostname*} *udp-port*}<br>**Example:**<br>`Device(config-flow-cache)# export destination 172.30.0.1 991` | (Optional) Enables the exporting of information from NetFlow aggregation caches.<br>• The *ip-address* \| *hostname*argument is the destination IP address or hostname.<br>• The *port* argument is the destination UDP port. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | Repeat Step 7 to configure a second export destination. | (Optional) You can configure a maximum of two export destinations for each NetFlow aggregation cache. |
| **Step 9** | **export version** [**9**]<br>**Example:**<br>`Device(config-flow-cache)# export version 9` | (Optional) Specifies data export format Version.<br>• The **version 9** keyword specifies that the export packet uses the Version 9 format. |
| **Step 10** | **enabled**<br>**Example:**<br>`Device(config-flow-cache)# enabled` | Enables the aggregation cache. |
| **Step 11** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits NetFlow aggregation cache configuration mode and returns to global configuration mode. |
| **Step 12** | **interface** *interface-type interface-number*<br>**Example:**<br>`Device(config)# interface fastethernet 0/0/0` | Specifies the interface that you want to enable NetFlow on and enters interface configuration mode. |
| **Step 13** | **ip flow** {**ingress** \| **egress**}<br>**Example:**<br>`Device(config-if)# ip flow ingress` | Enables NetFlow on the interface.<br>• **ingress** --captures traffic that is being received by the interface<br>• **egress** --captures traffic that is being transmitted by the interface. |
| **Step 14** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | (Optional) Exits interface configuration mode and returns to global configuration mode.<br>**Note** You only need to use this command if you want to enable NetFlow on another interface. |
| **Step 15** | Repeat Steps 12 through 14 to enable NetFlow on other interfaces | (Optional) -- |
| **Step 16** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

# Verifying the Aggregation Cache Configuration

To verify the aggregation cache configuration, use the following show commands. These commands allow you to:

- Verify that the NetFlow aggregation cache is operational.
- Verify that NetFlow Data Export for the aggregation cache is operational.
- View the aggregation cache statistics.

## SUMMARY STEPS

1. **enable**
2. **show ip cache flow aggregation** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
3. **show ip flow export**
4. **end**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Device>enable
```

Device#

**Step 2** **show ip cache flow aggregation** {**as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

Use the **show ip cache flow aggregation destination-prefix** command to verify the configuration of an destination-prefix aggregation cache. For example:

**Example:**

```
Device# show ip cache flow aggregation destination-prefix
IP Flow Switching Cache, 139272 bytes
  5 active, 2043 inactive, 9 added
  841 ager polls, 0 flow alloc failures
  Active flows timeout in 15 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 11144 bytes
  5 active, 507 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Null           0.0.0.0         /0   0         5    13    52   138.9
Et0/0.1        172.16.6.0      /24  0         1     1    56     0.0
Et1/0.1        172.16.7.0      /24  0         3    31K 1314   187.3
Et0/0.1        172.16.1.0      /24  0        16   104K 1398   188.4
Et1/0.1        172.16.10.0     /24  0         9    99K 1412   183.3
```

Use the **show ip cache verbose flow aggregation source-prefix** command to verify the configuration of a source-prefix aggregation cache. For example:

**Example:**

```
Device# show ip cache verbose flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  51 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  4 active, 1020 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src Prefix      Msk  AS    Flows  Pkts B/Pk  Active
FEt1/0/0.1      172.16.10.0     /24  0        4    35K 1391    67.9
FEt0/0/0.1      172.16.6.0      /24  0        2     5    88    60.6
FEt1/0/0.1      172.16.7.0      /24  0        2  3515  1423    58.6
FEt0/0/0.1      172.16.1.0      /24  0        2    20K 1416    71.9
```

Use the **show ip cache verbose flow aggregation protocol-port** command to verify the configuration of a protocol-port aggregation cache. For example:

**Example:**

```
Device# show ip cache verbose flow aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  158 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
  0x01       0x0000      0x0000      6       52K     1405        104.3
  0x11       0x0208      0x0208      1        3        52         56.9
  0x01       0x0000      0x0800      2      846      1500         59.8
  0x01       0x0000      0x0B01      2       10        56         63.0
```

**Step 3** **show ip flow export**

Use the **show ip flow export** command to verify that NetFlow Data Export is operational for the aggregation cache. For example:

**Example:**

```
Device# show ip flow export
Flow export v1 is disabled for main cache
  Version 9 flow records
  Cache for protocol-port aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for source-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for destination-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  40 flows exported in 20 udp datagrams
  0 flows failed due to lack of export packet
  20 export packets were sent up to process level
```

```
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

**Step 4** **end**

Use this command to exit privileged EXEC mode.

**Example:**

```
Device# end
```

# Configuration Examples for Configuring NetFlow Aggregation Caches

## Configuring an AS Aggregation Cache Example

The following example shows how to configure an AS aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal
!
ip flow-aggregation cache as
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

## Configuring a Destination Prefix Aggregation Cache Example

The following example shows how to configure a destination prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
```

```
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring a Prefix Aggregation Cache Example

The following example shows how to configure a prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring a Protocol Port Aggregation Cache Example

The following example shows how to configure a protocol port aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache protocol-port
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring a Source Prefix Aggregation Cache Example

The following example shows how to configure a source prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring an AS-ToS Aggregation Cache Example

The following example shows how to configure an AS-ToS aggregation cache with a cache active timeout of 20 minutes, an export destination IP address of 10.2.2.2, and a destination port of 9991:

```
configure terminal

!

ip flow-aggregation cache as-tos
 cache timeout active 20
 export destination 10.2.2.2 9991
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring a Prefix-ToS Aggregation Cache Example

The following example shows how to configure a prefix-ToS aggregation cache with an export destination IP address of 10.4.4.4 and a destination port of 9995:

```
configure terminal

!

ip flow-aggregation cache prefix-tos
 export destination 10.4.4.4 9995
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring the Minimum Mask of a Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache prefix
 mask source minimum 24
 mask destination minimum 28
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a destination prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 mask destination minimum 32
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a source prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 mask source minimum 30
 enabled
!
interface Fastethernet0/0/0
 ip flow ingress
!
 end
```

# Configuring NetFlow Version 9 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 9 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export template refresh-rate 10
 export version 9
 export template timeout-rate 60
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS master command list, all releases | Cisco IOS Master Command List, All Releases |
| NetFlow commands | Cisco IOS NetFlow Command Reference |
| Overview of NetFlow | *Cisco IOS NetFlow Overview* |
| Overview of NBAR | *Classifying Network Traffic Using NBAR* |
| Configuring NBAR | *Configuring NBAR Using the MQC* |
| Configuring NBAR using protocol-discovery | *Enabling Protocol Discovery* |
| Capturing and exporting network traffic data | *Configuring NetFlow and NetFlow Data Export* |
| Information for installing, starting, and configuring the CNS NetFlow Collection Engine | Cisco CNS NetFlow Collection Engine Documentation |

### Standards and RFCs

| Standards/RFCs | Title |
|---|---|
| RFC 5103 | Bidirectional Flow Export Using IP Flow Information Export (IPFIX) |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/techsupport |

# Feature Information for Configuring NetFlow Aggregation Caches

*Table 14: Feature Information for Configuring NetFlow Aggregation Caches*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| NetFlow ToS-Based Router Aggregation | Cisco IOS XE Release 2.1 | The NetFlow ToS-Based Router Aggregation feature enables you to limit router-based type of service (ToS) aggregation of NetFlow export data. The aggregation of export data provides a summarized NetFlow export data that can be exported to a collection device. The result is lower bandwidth requirements for NetFlow export data and reduced platform requirements for NetFlow data collection devices.<br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.<br>The following commands were modified by this feature: **ip flow-aggregation cache**, **show ip cache verbose flow aggregation**, **show ip flow export**. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| NetFlow Minimum Prefix Mask for Router-Based Aggregation | Cisco IOS XE Release 2.1 | The NetFlow Minimum Prefix Mask for Router-Based Aggregation feature allows you to set a minimum mask size for prefix aggregation, destination prefix aggregation, and source prefix aggregation schemes.<br>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.<br>The following commands were modified by this feature: **ip flow-aggregation cache**, **mask destination**, **mask source**, **show ip cache flow aggregation**. |

# Glossary

**BGP** --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

**BGP/MPLS/VPN** --A Virtual Private Network (VPN) solution that uses Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) to allow multiple remote customer sites to be connected over an IP backbone. Refer to RFC 2547 for details.

**CE router** --A customer edge router. A router that is part of a customer network and interfaces to a provider edge (PE) router.

**customer network** --A network that is under the control of an end customer. A customer network can use private addresses as defined in RFC 1918. Customer networks are logically isolated from each other and from the provider network. A customer network is also known as a C network.

**egress PE** --The provider edge router through which traffic moves from the backbone to the destination Virtual Private Network (VPN) site.

**flow** --A set of packets with the same source IP address, destination IP address, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

**ingress PE** --The provider edge router through which traffic enters the backbone (provider network) from a Virtual Private Network (VPN) site.

**label** --A short, fixed length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

**MPLS** --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

**PE route** r--A provider edge router. A router at the edge of a provider network that interfaces to customer edge (CE) routers.

**provider network** --A backbone network that is under the control of a service provider and provides transport among customer sites. A provider network is also known as the P network.

**VPN** --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --Virtual Private Network (VPN) routing/forwarding instance. The VRF is a key element in the MPLS VPN technology. VRFs exist on PEs only. A VRF is populated with VPN routes and allows one PE to have multiple routing tables. One VRF is required per VPN on each PE in the VPN.