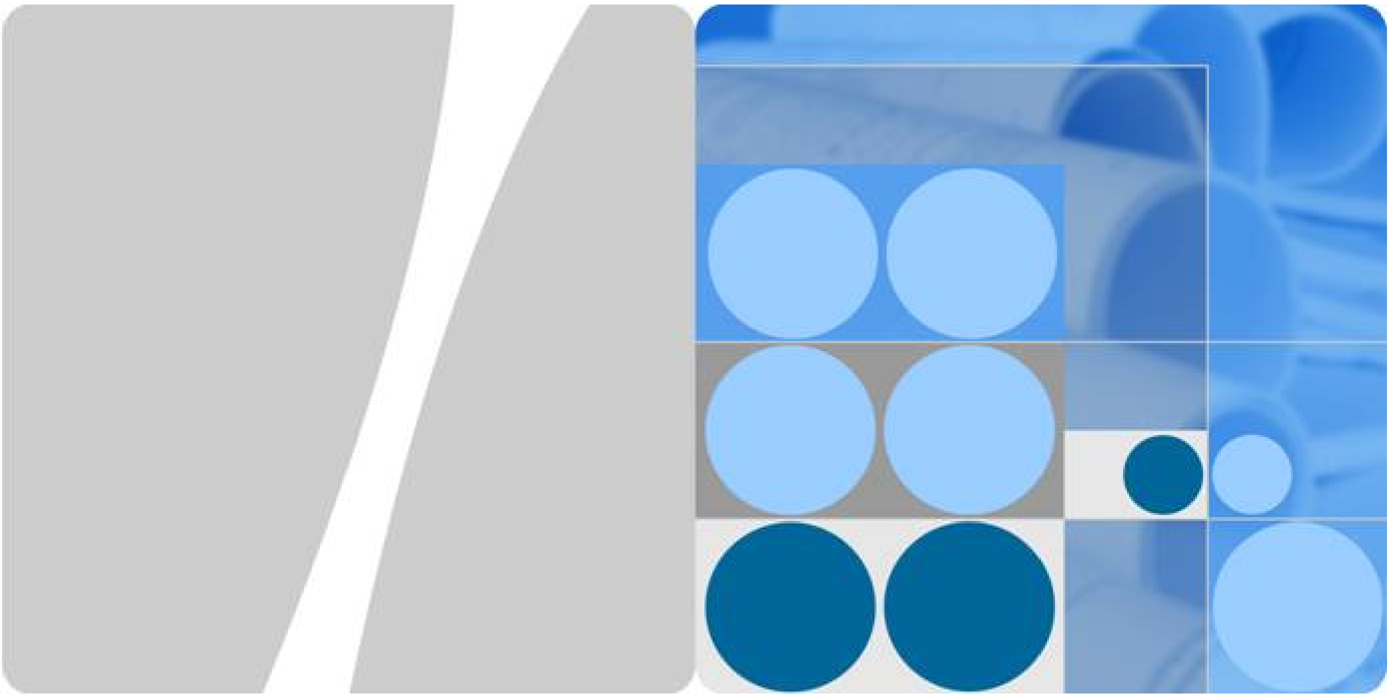


CloudEngine 12800 Series Switches

V100R006C00

NetStream Technology White Paper

Issue	**02**
Date	**2016-06-21**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 NetStream Overview

Definition

NetStream is a technology that collects statistics on and analyzes service traffic on networks.

Purpose

As technologies fast develop, the Internet needs to carry more services and applications. Service deployment and maintenance on the network become complex. A new traffic statistics collection technology is required to collect and analyze traffic statistics. With this technology, network management is precise and optimized.

Traditional traffic statistics collection technologies are not flexible and have limitations (as shown in **Table 1-1**), so they cannot meet current service requirements. To solve this problem, NetStream, which is a precise traffic monitoring and analysis technology, is introduced.

Table 1-1 Implementation and limitations of the traditional traffic statistics methods

Traffic Statistics Method	Implementation	Limitation
Statistics based on IP packets	Saves counter indexes in the routing table on a device to count the number of bytes and packets that pass through the device.	This method applies to collection of statistics about simple information instead of various information.
Statistics based on access control lists (ACLs)	Precisely matches flows based on ACLs and then collects statistics.	This method requires large capacity of ACLs and cannot collect statistics about flows that match no ACL rule.

Traffic Statistics Method	Implementation	Limitation
Statistics using SNMP	Uses SNMP to implement simple statistics functions, such as interface statistics, IP packet statistics, and the ACL matching statistics.	The statistics function is not strong enough and collects statistics from the NMS using continuous polling, wasting CPU and network resources.
Statistics based on port mirroring	Duplicates traffic passing through a port and sends the duplicated traffic to a dedicated server for statistics and analysis.	This method requires high costs. In addition, this method occupies an interface. Statistics cannot be collected on an interface that does not support port mirroring.
Statistics based on the traffic duplication at the physical layer	Duplicates traffic using an optical splitter or other devices at the physical layer and then sends the duplicated traffic to a dedicated server for statistics.	This method requires high costs because a dedicated hardware devices must be purchased.

Benefits

- Accounting

  NetStream provides detailed data for accounting based on resource usage (such as usage of links, bandwidths, and time segments). The data includes the number of packets, number of bytes, IP addresses, time, types of service (ToSs), and application types. An enterprise can calculate expenses of each department and distribute operation costs based on the data to effectively use resources.

- Network monitoring

  NetStream monitors network traffic almost in real time. NetStream can be deployed on an interface connected to the Internet to monitor outgoing traffic almost in real time and analyze bandwidth usage of services. The traffic monitoring information helps network administrators determine the network running status and discover inappropriate network structures or performance bottlenecks on networks. Enterprises can easily plan and allocate network resources.

2 Principles

About This Chapter

2.1 NetStream System Components

A typical NetStream system consists of the NetStream Data Exporter (NDE), NetStream Collector (NSC), and NetStream Data Analyzer (NDA).

- NDE

  An NDE analyzes and processes network flows, extracts flows that meet conditions for statistics, and exports the statistics to the NSC. The NDE can perform operations (such as aggregation) over the statistics before exporting them to the NSC. A device configured with NetStream functions as the NDE in a NetStream system.

- NSC

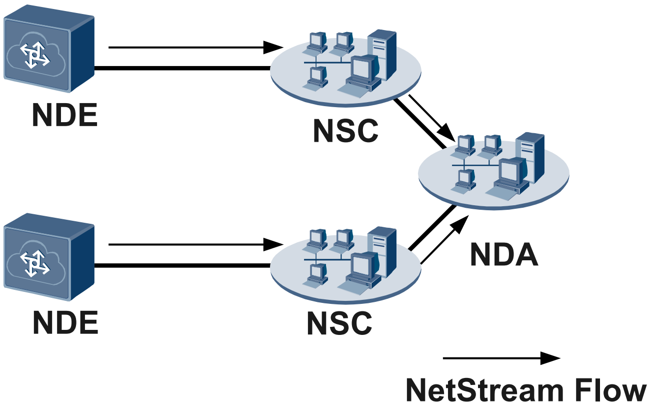
  An NSC is a program running on the Unix or Windows operating system. The NSC parses packets from the NDE and saves statistics to the database. The NSC can collect data exported from multiple NDEs, and filter and aggregate the data.

- NDA

  An NDA is a traffic analysis tool. It extracts statistics from the NSC, processes the statistics, and generates a report. This report provides a basis for services such as traffic accounting, network planning, and attack monitoring. The NDA provides a graphical user interface (GUI) for users to easily obtain, check, and analyze the collected data.

In real networking, the NSC and NDA are integrated on one NetStream server, as shown in **Figure 2-1**. The NDE samples packets to obtain outbound traffic information on 10GE1/0/1 and creates NetStream flows based on conditions. When the NetStream cache is full or a NetStream flow is aged out, the NDE encapsulates statistics in NetStream packets and sends the packets to the NetStream server. The NetStream server analyzes the NetStream packets and shows analysis results.

Figure 2-1 Networking diagram of a NetStream system



NetStream working process

As shown in **Figure 2-1**, the NetStream system works as follows:

1. The device with NetStream configured (that is, NDE) periodically sends collected traffic statistics to the NSC.
2. The NSC processes the traffic statistics, and sends them to NDA.

3. The NDA analyzes the traffic statistics and stores them as the basis of accounting and network planning.

The device functioning as an NDE implements the following functions:

1. The NDE samples service traffic in certain sampling mode and creates NetStream flows. For details, see **2.2 NetStream Flow Creation**.
2. The NetStream flows age out when meeting certain conditions. For details about flow aging, see **2.3 NetStream Flow Aging**.
3. When NetStream flows age out, the device outputs the aging flows. For details about flow exporting, see **2.4 NetStream Flow Exporting**.

2.2 NetStream Flow Creation

The NetStream module on a device samples service traffic in certain modes, and then creates NetStream flows for the sampled traffic.

NetStream Sampling

By cooperating with the sampler, NetStream samples service traffic based on a certain sampling ratio.

NetStream only analyzes flow information of sampled packets. This reduces number of sampled packets and impact on device performance. In addition, the statistics can accurately reflect traffic conditions on the network.

The device supports packet-based random sampling. That is, packets are randomly sampled within the specified packet interval. For example, if the interval is 100 packets, one packet is sampled from every 100 packets.

NetStream Flows

NetStream is a technology that collects packet statistics based on flows. After sampling packets, the NetStream module analyzes the sampled packets and creates flows based on key information in packets. The key information is as follows:

- For Layer 2 information, the packets with five identical attributes are considered as a flow. The five attributes refer to destination MAC address, source MAC address, VLAN ID, Ethernet type, inbound interface, and outbound interface.
- For IPv4 packets, the packets with seven identical attributes are considered as a flow. The seven attributes refer to destination IP address, source IP address, destination port number, source port number, protocol, ToS, and the index of the inbound or outbound interface of IPv4 packets.
- For IPv6 packets, the packets with eight identical attributes are considered as a flow. The eight attributes refer to destination IPv6 address, source IPv6 address, destination port number, source port number, protocol, ToS, flow label, and the index of the inbound or outbound interface of IPv4 packets.
- For MPLS packets, NetStream collects the MPLS label information or IP information in MPLS packets. When collecting IP statistics, NetStream determines a flow according to MPLS label stack and IP attributes.

2.3 NetStream Flow Aging

The device outputs flows to NSC only after the flows age out. After the NetStream function is enabled, NetStream flows are stored in the buffer. When the flows in buffer meet the aging condition, the device outputs the aging flows in the buffer to the NSC.

NetStream flows are aged out in the following modes:

- Aging based on customized conditions
  - Active aging

    After the first packet of a flow is sampled, a flow can always be sampled within specified period. When the aging time of a flow exceeds the specified period, statistics about this flow are output. Active aging enables the device to periodically output the statistics about the flows that last for a long period.
  - Inactive aging

    If the device does not sample a flow until the last packet is sent, that is, the number of packets does not increase within the specified period, the device outputs statistics about this flow to the NetStream server. Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to output statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device outputs flow statistics to conserve memory space.
  - FIN or RST-based aging: A flow is aged when the FIN or RST bit is detected in the packets of the flow.

    The FIN or RST flag in a TCP packet indicates that the TCP connection is terminated.
- Oversized aging
  - NetStream flow table oversized aging

    The device limits the size of the NetStream flow table. When the number of entries in the NetStream flow table exceeds the limit, the system automatically ages the excess flows to ensure accurate statistics.
  - Byte oversized aging

    The NetStream flows in the buffer record the number of passing bytes. When the number of bytes exceeds a limit (4294967295 bytes, about 3.9 GB), recording new statistics will cause buffer overflow and statistics will be inaccurate. Therefore, when detecting that the number of bytes in a flow exceeds the limit, the system immediately ages the flow.
- Forcible aging

  You can run the related commands to age out all flows in the NetStream buffer. The forcible aging is used when the aging conditions are not met but new flows need to be added to the buffer or when the NetStream service becomes abnormal, causing flows in the buffer not to be aged.

2.4 NetStream Flow Exporting

After aging flows in the NetStream cache, the NDE exports the flow statistics to a specified NSC for further analysis.

Flow Statistics Exporting Modes

Original flow statistics exporting

When the flow aging time expires, statistics about every flow are output to the NSC. In flexible flow statistics exporting, the NSC can obtain details about each flow.

Aggregation flow statistics exporting

In aggregation flow statistics exporting, the device summarizes the original flows with the same aggregation keywords, and obtains statistics on the aggregation flow. The aggregation flow statistics obviously reduce bandwidth occupation. The supported aggregation modes are described in **Table 2-1**.

For example, there are four original TCP flows. They have the same source port number, destination port number, and destination IP address, but different source IP addresses. The **protocol-port** mode is used. Aggregation entries in this mode include protocol number, source port number, and destination port number. The four TCP flows have the same protocol number, source port number, and destination port number, so only one aggregation flow statistical record is recorded in the aggregation flow statistics table.

Table 2-1 Aggregation modes

Aggregation Mode	Aggregation Entries
as	Source AS number, destination AS number, index of the inbound interface, and index of the outbound interface
as-tos	Source AS number, destination AS number, inbound interface index, outbound interface index, and ToS
protocol-port	Protocol number, source port number, and destination port number
protocol-port-tos	Protocol number, source port number, destination port number, ToS, inbound interface index, and outbound interface index
source-prefix	Source AS number, source mask length, source prefix, and inbound interface index
source-prefix-tos	Source AS number, source mask length, source prefix, ToS, and inbound interface index
destination-prefix	Destination AS number, destination mask length, destination prefix, and outbound interface index
destination-prefix-tos	Destination AS number, destination mask length, destination prefix, ToS, and outbound interface index
prefix	Source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, inbound interface index, and outbound interface index

Aggregation Mode	Aggregation Entries
prefix-tos	Source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, ToS, inbound interface index, and outbound interface index
bgp-nexthop-tos	BGP next hop, source AS number, destination AS number, inbound interface index, and outbound interface index
index-tos	Inbound interface index, outbound interface index, and ToS
mpls-label (aggregation based on MPLS labels)	First layer label, second layer label, third layer label, TopLabelIpAddress, Bottom-of-Stack flag in the first layer label, and EXP field in the first layer label
source-index-tos	Inbound interface index, ToS, and BGP next hop
vlan-id	VLAN ID, inbound interface index

Flexible flow statistics exporting

Flexible flows are created based on customized configuration. Users can collect flow statistics based on the protocol type, ToS field, source IP address, destination IP address, source port number, destination port number, or flow label as required. The NDE exports the flow statistics to the NSC. Compared to original flow statistics exporting, flexible flow statistics exporting occupies less traffic and provides users with a flexible way to collect NetStream statistics.

Layer 2 NetStream flow statistics exporting

The device only collects statistics on Layer 2 attributes in packets, and sends statistics to the NSC for analysis.

Versions of Exported Packets

At present, the versions of NetStream exported packets are V5, V8, and V9. NetStream exported packets of all the versions are transmitted using UDP.

- V5: The packet format is fixed. NetStream packets in this format contain the original flow statistics collected based on 7-tuple information.
- V8: The packet format is fixed. NetStream packets in this format support the aggregation exporting format.
- V9: The NetStream packet format is defined in profiles. Statistical items can be combined, and therefore statistics are exported more flexibly.

2.5 NetStream Top Talkers

A typical NetStream system consists of three roles: NetStream data exporter (NDE), NetStream collector (NSC), and NetStream data analyzer (NDA). The NSC and NDA are configured on a NetStream server. The NDE with NetStream configured periodically sends traffic statistics to the NetStream server, and the NetStream server analyzes the statistics and shows statistics reports for you to monitor network traffic in real time. If a NetStream server is not located on a network or traffic statistics cannot be exported to the network where a NetStream server resides due to customers' security requirements, the NetStream Top Talkers function can be configured to allow customers to monitor network running status in real time.

NetStream Top Talkers filters traffic based on user-defined keywords, collects statistics on filtered traffic, sorts the traffic in a certain order, and displays only the top N traffic lines on screen. (N is the number of traffic lines recorded in the NetStream Top Talkers template). These N traffic lines are called Top Talkers.

NetStream Top Talkers can filter traffic according to the following keywords: source port number, destination port number, source IP address, destination IP address, next-hop IP address, source Autonomous System (AS), destination AS, packet precedence, protocol type, number of packets, and number of bytes.

NetStream Top Talkers sorts traffic in either of the following orders:

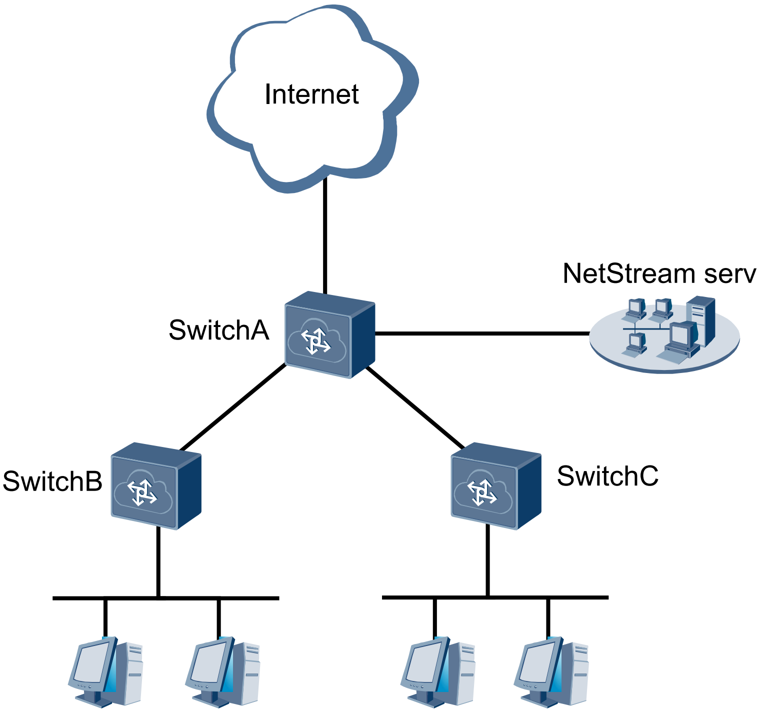
- Descending order of bytes: The Top Talker with the most bytes is listed on the top line.
- Descending order of packets: The Top Talker with the most packets is listed on the top line.

3 Applications

NetStream Usage Scenario

In **Figure 3-1**, SwitchA connects to the Internet, and stores a large number of communication packets. Network administrators intend to monitor bandwidths occupied by services, so NetStream needs to be configured to monitor real-time traffic statistics on the interface connecting to the Internet. The traffic statistics help network administrators determine the network running status and discover inappropriate network structures or performance bottlenecks.

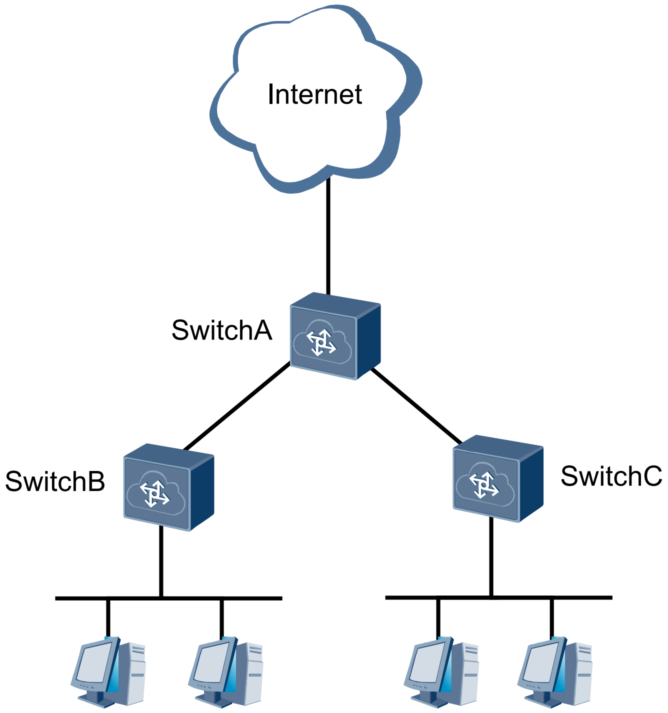
Figure 3-1 NetStream networking diagram



NetStream Top Talkers Usage Scenario

In **Figure 3-2**, SwitchA connects to the Internet, and stores a large number of communication packets. Network administrators intend to monitor bandwidths occupied by services; however, no NetStream server is located on the network. To monitor real-time traffic statistics on interfaces of SwitchA, the NetStream Top Talkers function can be configured on SwitchA. The traffic statistics help network administrators determine the network running status and discover inappropriate network structures or performance bottlenecks. In addition, the network administrators can detect network attacks according to traffic statistics on each interface.

Figure 3-2 NetStream Top Talkers networking diagram



4 Configuration Notes

Involved Network Elements

The switch needs to work with a NetStream server.

License Support

The NetStream IPv6 function is controlled by a license. By default, this function is disabled on new purchased CE12800 series switches. To use the NetStream IPv6 function, apply for and purchase the license from the equipment supplier.

Version Support

Table 4-1 Products and minimum versions supporting NetStream

Series	Product	Minimum Version Required
CE12800	CE12804/CE12808/ CE12812	V100R002C00
	CE12816	V100R003C00
	CE12804S/CE12808S	V100R005C00

Feature Dependencies and Limitations

Conflicts between NetStream and other features

- NetStream and sFlow cannot be configured on the same LPU of a VS.
- If NetStream has been configured on an Eth-Trunk, sFlow or port mirroring cannot be configured on the member interfaces of the Eth-Trunk. If sFlow or port mirroring has been configured on member interfaces of an Eth-Trunk, NetStream cannot be configured on the Eth-Trunk.
- By default, NetStream sampling uses mirroring resources; therefore, NetStream and port mirroring cannot be configured on the same interface. NetStream conflicts with MQC-based traffic mirroring and VLAN mirroring. After NetStream is configured on an

interface, you are advised not to configure any MQC-based traffic mirroring or VLAN mirroring to contain this interface.

- When inbound NetStream sampling uses snoop resources, port mirroring and inbound NetStream can be configured on the same interface.
- NetStream Top Talkers, NetStream IP traffic statistics collection, and NetStream Layer 2 flow statistics collection cannot be configured on the same interface.
- Modular + fixed switch SVF:
  - After the leaf switch collects statistics on the traffic to be sent to the parent switch for Layer 3 forwarding, the flow table generated for the traffic does not contain routing information. To collect such routing information, you are advised to configure NetStream on the FNI interface of the parent switch.
  - If routing information (next-hop IP address and AS) is specified in a NetStream Top Talkers template applied to an interface of a leaf switch, the NetSteram Top Talkers template cannot collect statistics on or sort the traffic to be sent to the parent switch for routing. To collect statistics on and sort such traffic, you are advised to apply the NetStream Top Talkers template to the FNI interface of the parent switch.
  - When inbound NetStream sampling uses snoop resources, the configuration takes effect only on the parent switch, but cannot take effect on leaf switches.
  - A CE5855EI supports NetStream IPv6 when functioning as a leaf switch.

NetStream use restriction

- NetStream cannot sample TRILL packets, or packets encapsulated in MPLS TE tunnel.
- In V100R006C00 and earlier versions, NetStream can sample the original Ethernet frame information in VXLAN packets. Since V200R001C00, NetStream can sample the original Ethernet frame information in VXLAN packets.
- On an FCoE network, the device can only collect Layer 2 statistics about packets.
- In NetStream sampling service, there may be a difference of 5% or lower between collected statistics and actual traffic statistics.
- The recommended NetStream sampling ratio is 8192, which can be manually set. When NetStream sampling ratio is set to a small value, many sampled packets will be sent to the CPU, causing a high CPU usage. If the CPU is overloaded, sampled packets are discarded. When NetStream sampling ratio is set to a small value, many sampled packets will be sent to the CPU, causing a high CPU usage. If the CPU is overloaded, sampled packets are discarded.
- When sampling outgoing packets, the device does not record source VLAN information in the packets. Source VLAN information is recorded as 0. When sampling incoming packets, the device does not record destination VLAN information. Destination VLAN information is recorded as 0.
- NetStream sampling is on the basis of original packets. After the forwarding behavior is modified (for example, policy routing is applied) or information about the packets to be forwarded is modified (for example, ACL or QoS is applied), the modification cannot be shown in the NetStream statistics.
- When sampling packets, NetStream does not resolve the option fields in IPv4 packets and extended headers in IPv6 packets.
- Only inbound NetStream sampling can be configured to use snoop resource. When a switch uses snoop resource to perform NetStream sampling, inbound NetStream sampling rate cannot be configured on interfaces, but only the global NetStream sampling rate can be used to perform inbound sampling on interfaces.

NetStream Top Talkers use restriction

- A device in non-VS mode supports a maximum of 16 NetStream Top Talkers templates. When a device works in VS mode, a VS supports a maximum of 16 NetStream Top Talkers templates.
- After the NetStream Top Talkers function is enabled, modifying the NetStream Top Talkers template within the statistics collection period will make the NetStream Top Talkers function invalid.
- After an ISSU is complete, statistics in the NetStream Top Talkers templates are cleared.

5 Configuring the NetStream

About This Chapter

screen. (N is the number of traffic lines recorded in the NetStream Top Talkers template). These N traffic lines are called Top Talkers.

5.1 Configuring Exporting of IPv4 Original Flow Statistics

Once exporting of IPv4 original flow statistics is configured, the NDE collects statistics about IPv4 flows and exports each flow statistics to the NetStream server for further analysis.

Pre-configuration Tasks

Before configuring exporting of IPv4 original flow statistics exporting, complete the following tasks:

- Set physical parameters of interfaces.
- Set the link-layer attributes of each interface.

Configuration Process

The configuration tasks of IPv4 original flows can be performed in any sequence.

5.1.1 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.1.2 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

  a. Run the **interface** *interface-type interface-number* command to enter the interface view.

  b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

     By default, packet sampling is not configured on any interface.

     If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.1.3 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC.

NetStream flow aging modes include regular aging, FIN- and RST-based aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- FIN- and RST-based aging

An FIN or RST flag in a TCP packet indicates the termination of a TCP connection. When receiving a packet with the FIN or RST flag, the device immediately ages out the corresponding NetStream flow. It is recommended that you enable this mode.

- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.
  b. Run the **netstream timeout ip active** *active-interval* command to set the active aging time of IPv4 flows.

     By default, the active aging time of IPv4 flows is 30 minutes.
  c. Run the **commit** command to commit the configuration.

  Configure inactive aging.

  a. Run the **system-view** command to enter the system view.
  b. Run the **netstream timeout ip inactive** *inactive-interval* command to set the inactive time of IPv4 flows.

     By default, the inactive aging time of IPv4 flows is 30 seconds.
  c. Run the **commit** command to commit the configuration.
- Configure FIN- and RST-based aging.
  a. Run the **system-view** command to enter the system view.
  b. Run the **netstream timeout ip tcp-session** command to age NetStream flows according to the FIN or RST flag in the TCP packet header.

     By default, NetStream flows are not aged according to the FIN or RST flag in the TCP packet header.
  c. Run the **commit** command to commit the configuration.
- Configure forced aging.
  a. Run the **reset netstream cache ip slot** *slot-id* command in the user view to forcibly age out all IPv4 flows on the card.

----End

5.1.4 (Optional) Configuring an MPLS Network to Carry Original Flow Statistics for IPv4 Packets

MPLS IPv4 packet statistics help you understand the usage information about MPLS networks.

Context

Before configuring flow statistics collection for IPv4 packets over an MPLS network, enable MPLS on the device and interfaces to set up an MPLS network. Select one method to sample MPLS packets:

- To sample only the IP packets encapsulated in the MPLS packets.
- To sample only labels in the MPLS packets.
- To sample both labels and IP packets encapsulated in the MPLS packets.

NOTE

Only V9 format is supported when an MPLS network carries original flow statistics for IPv4 packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream mpls-aware** { **ip-only** | **label-and-ip** | **label-only** } **ip** command to configure MPLS packet sampling.

By default, only the IP packets encapsulated in the MPLS packets are sampled.

Step 3 Run:

```
commit
```

The configuration is committed.

----End

5.1.5 Configuring NetStream Original Flow Statistics Exporting

Context

Original flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and one destination UDP port number for the exported packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ip source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying IPv4 original flow statistics.

By default, the source IP address of the exported packets carrying IPv4 original flow statistics is not configured.

NOTE

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying IPv4 original flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 3 Run the **netstream export ip host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying IPv4 original flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying IPv4 original flow statistics are not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

Step 4 Run the **commit** command to commit the configuration.

----End

5.1.6 Configuring the AS Number Format and Interface Index Length on an IPv4 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.
- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv4 network, pay attention to the following points:

- On a network using 32-bit AS numbers, the NMS must be able to identify the 32-bit AS numbers; otherwise, the NMS cannot identify inter-AS traffic.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ip index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv4 flow statistics.

By default, 16-bit interface indexes are contained in the exported packets carrying IPv4 flow statistics. To change the interface index length from 16-bit to 32-bit, ensure that the following requirements are met:

- The export version of original flows is V9.
- The export version of all aggregation flows is V9.

Step 4 Run the **commit** command to commit the configuration.

----End

5.1.7 Configuring Versions for Exported Packets

Context

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The exported packets in V5 have fixed format and are difficult to expand. The format of exported packets in V9 is defined in templates and is easy to expand. The statistics are exported flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets to V9.

The version of exported packets carrying IPv4 original flows must be set to V9 in the following situations:

- Exported packets need to carry BGP next-hop information.
- Exported packets need to carry 32-bit interface indexes.
- Statistics about MPLS IPv4 packets need to be collected.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ip version** { **5** [**origin-as** | **peer-as**] | **9** [**origin-as** | **peer-as**] [**bgp-nexthop**] } command to set the version of exported packets carrying IPv4 original flow statistics.

By default, the packets carrying IPv4 original flow statistics are exported in the format of V5.

Step 3 (Optional) Run the **netstream export ip template timeout-rate** *timeout-interval* command to set the interval at which the template for exporting original flows in V9 format is refreshed.

By default, the output template of IPv4 original flows is refreshed every 30 minutes.

Step 4 Run the **commit** command to commit the configuration.

----End

5.1.8 Enabling NetStream Original Flow Statistics Collection on an Interface

Context

IPv4 original flow statistics can be exported only if flow statistics collection is enabled on an interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream** { **inbound** | **outbound** } **ip** command to enable NetStream on the interface to collect statistics about IPv4 flows.

By default, NetStream for IPv4 flows is disabled on the interface.

Step 4 Run the **commit** command to commit the configuration.

----End

5.1.9 Checking the Configuration

Context

You can run commands to verify that IPv4 original flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ip origin** [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv4 original flowsdetailed on the card.
- Run the **display netstream export ip template** command to check the exported template information.
- Run the **display netstream statistics ip slot** *slot-id* command to check NetStream statistics about IPv4 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.2 Configuring IPv6 Original Flow Statistics Exporting

After IPv6 original flow statistics exporting is configured, the NDE collects statistics about IPv6 flows and exports the statistics about each flow to the NetStream server for further analysis.

Pre-configuration Tasks

Before configuring IPv6 original flow statistics exporting, complete the following tasks:

- Set physical parameters of interfaces.
- Set the link-layer attributes of each interface.

Configuration Process

The configuration tasks of IPv6 original flows can be performed in any sequence.

5.2.1 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.2.2 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

NOTE

When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

a. Run the **interface** *interface-type interface-number* command to enter the interface view.

b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

   By default, packet sampling is not configured on any interface.

   If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.2.3 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, FIN- and RST-based aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- FIN- and RST-based aging

  An FIN or RST flag in a TCP packet indicates the termination of a TCP connection. When receiving a packet with the FIN or RST flag, the device immediately ages out the corresponding NetStream flow. It is recommended that you enable this mode.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

a. Run the **system-view** command to enter the system view.

b. Run the **netstream timeout ipv6 active** *active-interval* command to set the active aging time of IPv6 flows.

   By default, the active aging time of IPv6 flows is 30 minutes.

c. Run the **commit** command to commit the configuration.

Configure inactive aging.

a. Run the **system-view** command to enter the system view.

b. Run the **netstream timeout ipv6 inactive** *inactive-interval* command to set the inactive time of IPv6 flows.

   By default, the inactive aging time of IPv6 flows is 30 seconds.

c. Run the **commit** command to commit the configuration.

- Configure FIN- and RST-based aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ipv6 tcp-session** command to configure the NetStream flows to age according to the FIN or RST flag in the TCP packet header.

     By default, NetStream flows are not aged according to the FIN or RST flag in the TCP packet header.

  c. Run the **commit** command to commit the configuration.

- Configure forced aging.

  a. Run the **reset netstream cache ipv6 slot** *slot-id* command in the user view to forcibly age out all IPv6 flows on the card.

----End

5.2.4 Configuring NetStream Original Flow Statistics Exporting

Context

Original flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and destination UDP port number for the exported packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ipv6 source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying IPv6 original flow statistics.

By default, the source IP address of the exported packets carrying IPv6 original flow statistics is not configured.

NOTE

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying IPv6 original flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 3 Run the **netstream export ipv6 host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying IPv6 original flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying IPv6 original flow statistics are not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ipv6 host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

Step 4 Run the **commit** command to commit the configuration.

----End

5.2.5 Configuring the AS Number Format and Interface Index Length on an IPv6 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.
- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv6 network, pay attention to the following points:

- On a network using the 32-bit AS number format, the NMS must be able to identify the 32-bit AS numbers. Otherwise, the NMS cannot identify inter-AS flows sent from devices.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ipv6 index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv6 flow statistics

By default, 16-bit interface indexes are contained in the exported packets carrying IPv6 flow statistics.

Step 4 Run the **commit** command to commit the configuration.

----End

5.2.6 Configuring Versions for Exported Packets

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ipv6 version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**] command to set the version of the exported packets carrying IPv6 original flow statistics.

By default, the version of exported packets carrying IPv6 original flow statistics is not specified.

NOTE

The version of exported packets carrying IPv6 original flow statistics is fixed as V9.

Step 3 (Optional) Run the **netstream export ipv6 template timeout-rate** *timeout-interval* command to set the interval at which the template for exporting IPv6 original flows in V9 format is refreshed.

By default, the output template is refreshed every 30 minutes.

Step 4 Run the **commit** command to commit the configuration.

----End

5.2.7 Enabling NetStream Original Flow Statistics Collection on an Interface

Context

IPv6 original flow statistics can be exported only when you have enabled flow statistics collection on an interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream** { **inbound** | **outbound** } **ipv6** command to enable the NetStream function on the interface to collect statistics about IPv6 flows.

By default, the NetStream function for IPv6 flows is disabled on the interface.

Step 4 Run the **commit** command to commit the configuration.

----End

5.2.8 Checking the Configuration

Context

You can run commands to verify the configuration of IPv6 flow statistics exporting.

Procedure

- Run the **display netstream cache ipv6 origin** [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ipv6** *ipv6-address* | **source port** *port-number* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv6 original flows on the card.
- Run the **display netstream export ipv6 template** command to check the exported template information.
- Run the **display netstream statistics ipv6 slot** *slot-id* command to check NetStream statistics about IPv6 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.3 Configuring IPv4 Aggregation Flow Statistics Exporting

After the IPv4 aggregation flow statistics exporting is configured, the NDE aggregates statistics about IPv4 flows with the same aggregation entries and exports flow statistics to the NetStream server for further analysis.

Pre-configuration Tasks

Before configuring the IPv4 aggregation flow statistics exporting, complete the following tasks:

- Set physical parameters of interfaces.
- Set the link-layer attributes of each interface.

Configuration Process

The configuration tasks are mandatory and can be performed in any sequence.

5.3.1 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.3.2 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

  a. Run the **interface** *interface-type interface-number* command to enter the interface view.

  b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

     By default, packet sampling is not configured on any interface.

     If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.3.3 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the original flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream aggregation timeout ip active** *active-interval* command to set the active aging time of IPv4 aggregation flows.

     By default, the active aging time of IPv4 aggregation flows is 5 minutes.

  c. Run the **commit** command to commit the configuration.

  Configure inactive aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream aggregation timeout ip inactive** *inactive-interval* command to set the inactive time of IPv4 aggregation flows.

     By default, the inactive aging time of IPv4 aggregation flows is 300 seconds.

  c. Run the **commit** command to commit the configuration.
- Configure forced aging.

  a. Run the **reset netstream cache ip slot** *slot-id* command in the user view to forcibly age out all IPv4 flows on the card.

----End

5.3.4 (Optional) Configuring an MPLS Network to Carry Aggregation Flow Statistics for IPv4 Packets

MPLS IPv4 packet statistics help you understand the usage information about MPLS networks.

Context

Before configuring flow statistics collection for IPv4 packets over an MPLS network, enable MPLS on the device and interfaces to set up an MPLS network. Select one method to sample MPLS packets:

- To sample only the IP packets encapsulated in the MPLS packets.
- To sample only labels in the MPLS packets.
- To sample both labels and IP packets encapsulated in the MPLS packets.

NOTE

Only V9 format is supported when an MPLS network carries aggregation flow statistics for IPv4 packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream mpls-aware** { **ip-only** | **label-and-ip** | **label-only** } **ip** command to configure MPLS packet sampling.

By default, only the IP packets encapsulated in the MPLS packets are sampled.

NOTE

When the MPLS packet sampling method is set to **ip-only**, you cannot enable MPLS-label aggregation using the **netstream aggregation ip** command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.3.5 Configuring NetStream Aggregation Flow Statistics Exporting

Context

Aggregation flow statistics can be exported only when you have specified a source address and at least one destination address and one destination UDP port number for the exported packets.

The device with NetStream aggregation flow statistics enabled can classify and aggregate original flows according to certain rules, and export the aged flows to the NSC. Aggregation of original flows will decrease network bandwidth, CPU usage, and memory space occupation.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream aggregation ip** { **as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **index-tos** | **mpls-label** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** | **source-index-tos** | **vlan-id** } command to configure a NetStream aggregation method and enter the NetStream aggregation view.

For details about aggregation modes, see **netstream aggregation ip** in the Command Reference.

Step 3 (Optional) Run the **mask** { **destination** | **source** } **minimum** *mask-length* command to configure an aggregation mask.

By default, the aggregation mask is 24.

The configured aggregation mask is valid for six aggregation modes: prefix, prefix-tos, destination-prefix, destination-prefix-tos, source-prefix, and source-prefix-tos, in which:

- The parameter **source** is used in prefix, prefix-tos, source-prefix, and source-prefix-tos aggregation method.
- The parameter **destination** is used in prefix, prefix-tos, destination-prefix, and destination-prefix-tos aggregation method.

Step 4 Run the **netstream export ip source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source address for the exported packets carrying IPv4 aggregation flow statistics.

By default, the source address of the exported packets carrying IPv4 aggregation flow statistics is not configured. After the aggregation method is set, the source address configured in the aggregation view is used first. If no source address is configured for an aggregation method, the source address configured by the **netstream export ip source** command in the system view is used.

If the source address is not specified, packets are not exported. The source address of the exported packets carrying IPv4 aggregation flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source address and destination address (NSC address). Two source addresses can be specified: one IPv4 address and one IPv6 address.

Step 5 Run the **netstream export ip host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination address and destination UDP port number for the exported packets carrying IPv4 aggregation flow statistics.

By default, the destination address and UDP port number of the exported packets carrying IPv4 aggregation flow statistics is not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of destination addresses is exceeded and the configuration fails.

After the aggregation method is set, the destination address configured in the aggregation view is used first. If no destination address is configured for an aggregation method, the destination address configured by the **netstream export ip host** command in system view is used.

Step 6 Run the **enable** command to enable the NetStream aggregation function.

By default, the aggregation function is disabled.

Step 7 Run the **commit** command to commit the configuration.

----End

5.3.6 Configuring the AS Number Format and Interface Index Length on an IPv4 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.
- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv4 network, pay attention to the following points:

- On a network using 32-bit AS numbers, the NMS must be able to identify the 32-bit AS numbers; otherwise, the NMS cannot identify inter-AS traffic.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ip index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv4 flow statistics.

By default, 16-bit interface indexes are contained in the exported packets carrying IPv4 flow statistics. To change the interface index length from 16-bit to 32-bit, ensure that the following requirements are met:

- The export version of original flows is V9.
- The export version of all aggregation flows is V9.

Step 4 Run the **commit** command to commit the configuration.

----End

5.3.7 Configuring Versions for Exported Packets

Context

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The exported packets in V8 have fixed format and are difficult to expand. The format of exported packets in V9 is defined in templates and is easy to expand. The statistics are exported flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets carrying aggregation flow statistics to V9.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream aggregation ip** { **as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **index-tos** | **mpls-label** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** | **source-index-tos** | **vlan-id** } command to enter the NetStream aggregation view.

The aggregation view must be the same as the aggregation view in **5.3.5 Configuring NetStream Aggregation Flow Statistics Exporting**.

Step 3 Run the **export version** { **8** | **9** } command to set the version of exported packets carrying aggregation flow statistics.

For the aggregation modes as, as-tos, destination-prefix, destination-prefix-tos, prefix, prefix-tos, protocol-port, protocol-port-tos, source-prefix, and source-prefix-tos, the default version is V8. You can specify the version of exported packets.

For the aggregation modes vlan-id, bgp-nexthop-tos, index-tos, mpls-label and source-index-tos the default version is fixed as V9, and these aggregation modes do not support the **export version** command.

Step 4 (Optional) Run the **template timeout-rate** *timeout-interval* command to set the interval at which the template for exporting aggregated flows in V9 format is refreshed.

By default, the output template of aggregated flows is refreshed every 30 minutes.

Step 5 Run the **commit** command to commit the configuration.

----End

5.3.8 Enabling NetStream Aggregation Flow Statistics Collection on an Interface

Context

Aggregation flow statistics can be exported only when you have enabled flow statistics collection on an interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream** { **inbound** | **outbound** } **ip** command to enable the NetStream function on the interface to collect statistics about IPv4 flows.

By default, the NetStream function for IPv4 flows is disabled on the interface.

Step 4 Run the **commit** command to commit the configuration.

----End

5.3.9 Checking the Configuration

Context

You can run commands to verify that aggregation flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ip aggregation** { **as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **index-tos** | **mpls-label** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-index-tos** | **source-prefix** | **source-prefix-tos** | **vlan-id** } **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv4 aggregation flows on the card.
- Run the **display netstream export ip template** command to check the exported template information.
- Run the **display netstream statistics ip slot** *slot-id* command to check NetStream statistics about IPv4 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.4 Configuring IPv6 Aggregation Flow Statistics Exporting

After the IPv6 aggregation flow statistics exporting is configured, the NDE aggregates statistics about IPv6 flows with the same aggregation entries and exports flow statistics to the NetStream server for further analysis.

Pre-configuration Tasks

Before configuring the IPv6 aggregation flow statistics exporting, complete the following tasks:

- Setting physical parameters of interfaces
- Configuring link layer attributes for interfaces

Configuration Process

The configuration tasks are mandatory and can be performed in any sequence. The function takes effect only when all configuration tasks are completed.

5.4.1 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.4.2 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

NOTE

When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

a. Run the **interface** *interface-type interface-number* command to enter the interface view.

b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

   By default, packet sampling is not configured on any interface.

   If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.4.3 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream aggregation timeout ipv6 active** *active-interval* command to set the active aging time of IPv6 aggregation flows.

By default, the active aging time of IPv6 aggregation flows is 5 minutes.

c. Run the **commit** command to commit the configuration.

Configure inactive aging.

a. Run the **system-view** command to enter the system view.

b. Run the **netstream aggregation timeout ipv6 inactive** *inactive-interval* command to set the inactive time of IPv6 aggregation flows.

   By default, the inactive aging time of IPv6 aggregation flows is 300 seconds.

c. Run the **commit** command to commit the configuration.

- Configure forced aging.
  a. Run the **reset netstream cache ipv6 slot** *slot-id* command in the user view to forcibly age out all IPv6 flows on the card.

----End

5.4.4 Configuring NetStream Aggregation Flow Statistics Exporting

Context

Original flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and one destination UDP port number for the exported packets.

The device with NetStream aggregation flow statistics enabled can classify and aggregate original flows according to certain rules, and export the aged flows to the NSC. Aggregation of original flows will decrease network bandwidth, CPU usage, and memory space occupation.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream aggregation ipv6** { **as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **index-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** | **vlan-id** } command to configure a NetStream aggregation method and enter the NetStream aggregation view.

Step 3 (Optional) Run the **mask** { **destination** | **source** } **minimum** *mask-length* command to configure an aggregation mask.

By default, the aggregation mask is 64.

The aggregation mask is only valid for six aggregation methods: prefix, prefix-tos, destination-prefix, destination-prefix-tos, source-prefix, and source-prefix-tos.

- The parameter **source** is used in the following aggregation methods: prefix, prefix-tos, source-prefix, and source-prefix-tos.
- The parameter **destination** is used in the following aggregation methods: prefix, prefix-tos, destination-prefix, and destination-prefix-tos.

Step 4 (Optional) Run the **template timeout-rate** *timeout-interval* command to set the interval at which the template is refreshed when the packets are exported in the format of V9.

By default, the template refresh interval is 30 minutes.

The version of exported packets carrying IPv6 aggregation flow statistics is fixed as V9, and the **export version** command is not supported.

Step 5 Run the **netstream export ipv6 source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying IPv6 aggregation flow statistics.

By default, the source IP address of the exported packets carrying IPv6 aggregation flow statistics is not configured. After the aggregation method is set, the source address configured in the aggregation view is used first. If no source address is configured for an aggregation method, the source address configured in the **netstream export ipv6 source** command is used.

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying IPv6 aggregation flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 6 Run the **netstream export ipv6 host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying IPv6 aggregation flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying IPv6 aggregation flow statistics are not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ipv6 host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

After the aggregation method is set, the destination address configured in the aggregation view is used first. If no destination address is configured for an aggregation method, the destination address configured in the **netstream export ipv6 host** command is used.

Step 7 Run the **enable** command to enable the NetStream aggregation function.

The aggregation function is disabled by default.

Step 8 Run the **commit** command to commit the configuration.

----End

5.4.5 Configuring the AS Number Format and Interface Index Length on an IPv6 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.

- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv6 network, pay attention to the following points:

- On a network using the 32-bit AS number format, the NMS must be able to identify the 32-bit AS numbers. Otherwise, the NMS cannot identify inter-AS flows sent from devices.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ipv6 index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv6 flow statistics

By default, 16-bit interface indexes are contained in the exported packets carrying IPv6 flow statistics.

Step 4 Run the **commit** command to commit the configuration.

----End

5.4.6 Enabling NetStream Aggregation Flow Statistics Collection on an Interface

Context

Aggregation flow statistics can be exported only when you have enabled flow statistics collection on an interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream** { **inbound** | **outbound** } **ipv6** command to enable the NetStream function on the interface to collect statistics about IPv6 flows.

By default, the NetStream function for IPv6 flows is disabled on the interface.

Step 4 Run the **commit** command to commit the configuration.

----End

5.4.7 Checking the Configuration

Context

You can run commands to verify that flexible flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ipv6 aggregation** { **as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **index-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** | **vlan-id** } **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv6 aggregation flows on the card.
- Run the **display netstream export ipv6 template** command to check the exported template information.
- Run the **display netstream statistics ipv6 slot** *slot-id* command to check NetStream statistics about IPv6 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.5 Configuring IPv4 Flexible Flow Statistics Exporting

After flexible flow statistics exporting is configured, the NDE classifies and collects statistics about packets based on the protocol type, ToS, source IP address, destination IP address, source port number, and destination port number.

Pre-configuration Tasks

Before configuring the IPv4 flexible flow statistics exporting, complete the following tasks:

- Set physical parameters of interfaces.
- Set the link-layer attributes of each interface.

Configuration Process

Configuring a Flexible Flow Statistics Template must be performed before **Enabling NetStream Flexible Flow Statistics Collection on an Interface**. The other configuration tasks are mandatory and can be performed in any sequence.

5.5.1 Configuring a Flexible Flow Statistics Template

Context

You need to configure a flexible flow statistics template before applying it to an interface. To obtain more detailed flow statistics, you can configure whether flexible flow statistics contain the number of packets and bytes, and the indexes of the inbound and outbound interfaces.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream record** *record-name* **ip** command to create IPv4 flexible flow statistics template and enter the IPv4 flexible flow statistics template view.

Step 3 (Optional) Run the **description** *description-information* command to configure the description of IPv4 flexible flows.

By default, the description of IPv4 flexible flows is not configured.

Step 4 Run the **match ip** { **destination-address** | **destination-port** | **tos** | **protocol** | **source-address** | **source-port** } command to configure the aggregation keywords for the IPv4 flexible flow statistics template.

By default, no aggregation keyword is configured in a flexible IPv4 flow statistics template. If you run the command multiple times, multiple keywords are configured to aggregate the flows according to all these keywords.

Step 5 Run the **collect counter** { **bytes** | **packets** } command to add the number of packets and bytes to the flexible flow statistics exported to the NSC.

By default, the flexible flow statistics that are exported to the NSC do not contain the number of packets or bytes.

Step 6 (Optional) Run the **collect interface** { **input** | **output** } command to add the indexes of the inbound and outbound interfaces to the flexible flow statistics exported to the NSC.

By default, the flexible flow statistics exported to the NSC do not contain the index of the inbound or outbound interface.

Step 7 Run the **commit** command to commit the configuration.

----End

5.5.2 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.5.3 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

  a. Run the **interface** *interface-type interface-number* command to enter the interface view.

  b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

     By default, packet sampling is not configured on any interface.

     If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.5.4 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the original flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ip active** *active-interval* command to set the active aging time of IPv4 flows.

     By default, the active aging time of IPv4 flows is 30 minutes.

  c. Run the **commit** command to commit the configuration.

  Configure inactive aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ip inactive** *inactive-interval* command to set the inactive time of IPv4 flows.

     By default, the inactive aging time of IPv4 flows is 30 seconds.

  c. Run the **commit** command to commit the configuration.
- Configure forced aging.

  a. Run the **reset netstream cache ip slot** *slot-id* command in the user view to forcibly age out all IPv4 flows on the card.

----End

5.5.5 Configuring NetStream Flexible Flow Statistics Exporting

Context

Flexible flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and one destination UDP port number for the exported packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ip source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying IPv4 flexible flow statistics.

By default, the source IP address of the exported packets carrying IPv4 flexible flow statistics is not configured.

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying IPv4 flexible flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 3 Run the **netstream export ip host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying IPv4 flexible flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying IPv4 flexible flow statistics are not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

Step 4 Run the **commit** command to commit the configuration.

----End

5.5.6 Configuring the AS Number Format and Interface Index Length on an IPv4 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.
- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv4 network, pay attention to the following points:

- On a network using 32-bit AS numbers, the NMS must be able to identify the 32-bit AS numbers; otherwise, the NMS cannot identify inter-AS traffic.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ip index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv4 flow statistics.

By default, 16-bit interface indexes are contained in the exported packets carrying IPv4 flow statistics. To change the interface index length from 16-bit to 32-bit, ensure that the following requirements are met:

- The export version of original flows is V9.
- The export version of all aggregation flows is V9.

Step 4 Run the **commit** command to commit the configuration.

----End

5.5.7 Configuring Versions for Exported Packets

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ip version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**] command to set the version and AS option of the exported packets carrying IPv4 flexible flow statistics.

By default, the version of the exported packets carrying IPv4 flexible flow statistics is not configured.

NOTE

The version of the exported packets carrying IPv4 flexible flow statistics is fixed as V9.

Step 3 (Optional) Run the **netstream export ip template timeout-rate** *timeout-interval* command to set the interval at which the template is refreshed when packets carrying IPv4 flexible flow statistics are exported in the format of V9.

By default, the template is refreshed every 30 minutes.

Step 4 Run the **commit** command to commit the configuration.

----End

5.5.8 Enabling NetStream Flexible Flow Statistics Collection on an Interface

Context

When configuring flexible NetStream, you must enable flow statistics collection and apply a flexible flow statistics template on an interface to ensure that statistics are exported successfully.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream record** *record-name* **ip** command to apply the IPv4 flexible flow statistics template to the interface.

Each interface can be configured with only one IPv4 flexible flow statistics template. Before modifying the IPv4 flexible flow statistics template in the same interface view, run the **undo netstream record ip** command to delete the existing configuration.

If an IPv4 flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Step 4 Run the **netstream** { **inbound** | **outbound** } **ip** command to enable the NetStream function on the interface to collect statistics about IPv4 flows.

By default, the NetStream function for IPv4 flows is disabled on the interface.

Step 5 Run the **commit** command to commit the configuration.

----End

5.5.9 Checking the Configuration

Context

You can run commands to verify that flexible flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ip record** *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv4 flexible flows on the card.
- Run the **display netstream export ip template** command to check the exported template information.
- Run the **display netstream statistics ip slot** *slot-id* command to check NetStream statistics about IPv4 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.6 Configuring IPv6 Flexible Flow Statistics Exporting

After the flexible flow statistics exporting is configured, the NDE classifies and collects statistics about packets based on the protocol type, ToS, source IPv6 address, destination IPv6 address, source port number, destination port number, or flow labels.

Pre-configuration Tasks

Before configuring the IPv6 flexible flow statistics exporting, complete the following tasks:

- Setting physical parameters of interfaces
- Configuring link layer attributes for interfaces

Configuration Process

The configuration tasks can be performed in any sequence except that the **5.6.1 Configuring a Flexible Flow Statistics Template** task must be performed before **5.6.8 Enabling Flexible Flow Statistics Collection on an Interface**.

5.6.1 Configuring a Flexible Flow Statistics Template

Context

You must configure a flexible flow statistics template before applying it to an interface. To obtain more detailed flow statistics, you can configure whether flexible flow statistics contain the number of packets and bytes, and the indexes of the inbound and outbound interfaces.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream record** *record-name* **ipv6** command to create an IPv6 flexible flow statistics template and enter the template view.

Step 3 (Optional) Run the **description** *description-information* command to configure the description of IPv6 flexible flows.

By default, the description of IPv6 flexible flows is not configured.

Step 4 Run the **match ipv6** { **destination-address** | **destination-port** | **tos** | **flow-label** | **protocol** | **source-address** | **source-port** } command to configure the aggregation keywords for the flexible IPv6 flow statistics template.

By default, no aggregation keyword is configured in a flexible IPv6 flow statistics template. If you run the command multiple times, multiple keywords are configured to aggregate the flows according to all these keywords.

Step 5 Run the **collect counter** { **bytes** | **packets** } command to add the number of packets and bytes to the flexible flow statistics exported to the NSC.

By default, the flexible flow statistics that are exported to the NSC do not contain the number of packets or bytes.

Step 6 (Optional) Run the **collect interface** { **input** | **output** } command to add indexes of the inbound and outbound interfaces to the flexible flow statistics exported to the NSC.

By default, the flexible flow statistics exported to the NSC do not contain the indexes of the inbound or outbound interface.

Step 7 Run the **commit** command to commit the configuration.

----End

5.6.2 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.6.3 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

a. Run the **interface** *interface-type interface-number* command to enter the interface view.

b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

   By default, packet sampling is not configured on any interface.

   If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.6.4 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ipv6 active** *active-interval* command to set the active aging time of IPv6 flows.

     By default, the active aging time of IPv6 flows is 30 minutes.

  c. Run the **commit** command to commit the configuration.

  Configure inactive aging.

a. Run the **system-view** command to enter the system view.

b. Run the **netstream timeout ipv6 inactive** *inactive-interval* command to set the inactive time of IPv6 flows.

   By default, the inactive aging time of IPv6 flows is 30 seconds.

c. Run the **commit** command to commit the configuration.

- Configure forced aging.

  a. Run the **reset netstream cache ipv6 slot** *slot-id* command in the user view to forcibly age out all IPv6 flows on the card.

----End

5.6.5 Configuring NetStream Flexible Flow Statistics Exporting

Context

Flexible IPv6 flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and one destination UDP port number for the exported packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ipv6 source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying IPv6 flexible flow statistics.

By default, the source IP address of the exported packets carrying IPv6 flexible flow statistics is not configured.

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying IPv6 flexible flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 3 Run the **netstream export ipv6 host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying IPv6 flexible flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying IPv6 flexible flow statistics are not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ipv6 host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

Step 4 Run the **commit** command to commit the configuration.

----End

5.6.6 Configuring the AS Number Format and Interface Index Length on an IPv6 Network

Context

The AS number format and interface index length configured on the NDE must be the same as those configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

- **AS number format**: According to RFC recommendations, IP packets carry 16-bit AS numbers; however, in some networks, IP packets carry 32-bit AS numbers. To ensure that the NDE can collect flow statistics between ASs, you may need to set the AS number format on the NDE.
- **Interface index**: The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Before configuring the AS number format and interface index length on an IPv6 network, pay attention to the following points:

- On a network using the 32-bit AS number format, the NMS must be able to identify the 32-bit AS numbers. Otherwise, the NMS cannot identify inter-AS flows sent from devices.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream as-mode** { **16** | **32** } command to set the AS number format.

By default, a device uses 16-bit AS numbers.

Step 3 Run the **netstream export ipv6 index-switch** *index-switch* command to set the interface index length in the exported packets carrying IPv6 flow statistics

By default, 16-bit interface indexes are contained in the exported packets carrying IPv6 flow statistics.

Step 4 Run the **commit** command to commit the configuration.

----End

5.6.7 Configuring Versions for Exported Packets

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ipv6 version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**] command to set the version of the exported packets carrying IPv6 flexible flow statistics.

By default, the version of the exported packets carrying IPv6 flexible flow statistics is not configured.

NOTE

The version of the exported packets carrying IPv6 flexible flow statistics is fixed as V9.

Step 3 (Optional) Run the **netstream export ipv6 template timeout-rate** *timeout-interval* command to set the interval at which the template is refreshed when the packets are exported in the format of V9.

By default, the template is refreshed every 30 minutes.

Step 4 Run the **commit** command to commit the configuration.

----End

5.6.8 Enabling Flexible Flow Statistics Collection on an Interface

Context

When configuring flexible NetStream, you need to enable flow statistics collection on an interface and apply a flexible flow statistics template on the interface to ensure successful statistics exporting.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream record** *record-name* **ipv6** command to apply the IPv6 flexible flow statistics template to the interface.

Each interface can be configured with only one IPv6 flexible flow statistics template. To modify the flexible flow statistics template in an interface view, run the **undo netstream record ipv6** command to delete the existing configuration, and then recreate one.

If an IPv6 flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Step 4 Run the **netstream** { **inbound** | **outbound** } **ipv6** command to enable the NetStream function on the interface to collect statistics about IPv6 flows.

By default, the NetStream function for IPv6 flows is disabled on the interface.

Step 5 Run the **commit** command to commit the configuration.

----End

5.6.9 Checking the Configuration

Context

You can run commands to verify that flexible flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ipv6 record** *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* |

source ipv6 *ipv6-address* | **source port** *port-number* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**] command to check detailed NetStream statistics on IPv6 flexible flows on the card.

- Run the **display netstream export ipv6 template** command to check the exported template information.
- Run the **display netstream statistics ipv6 slot** *slot-id* command to check NetStream statistics about IPv6 flows on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.7 Configuring Layer 2 NetStream Flow Statistics Exporting

After the Layer 2 NetStream flow statistics exporting is configured, the NDE collects Layer 2 NetStream flow statistics and exports statistics to the NetStream server for further analysis.

Pre-configuration Tasks

Before configuring the Layer 2 NetStream flow statistics exporting, complete the following tasks:

- Setting physical parameters of interfaces
- Configuring link layer attributes for interfaces

Configuration Process

The configuration tasks of Layer 2 NetStream flows can be performed in any sequence.

5.7.1 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.7.2 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

  a. Run the **interface** *interface-type interface-number* command to enter the interface view.

  b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

     By default, packet sampling is not configured on any interface.

     If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.7.3 Configuring NetStream Flow Aging

Context

When a NetStream flow is aged out, the device exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flow aging modes include regular aging, byte-based aging, and forced aging. By default, the byte-based aging is enabled.

- Regular aging
  - Active aging

    Active aging requires the device to periodically export statistics about the flows that persist for a long period. This aging mode is enabled on the device by default, and you only need to set the aging time.
  - Inactive aging

    Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistics entries. Inactive aging requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space. This aging mode is enabled on the device by default, and you only need to set the aging time.
- Forced aging

  Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the flows in the cache and export the flow statistics.

Procedure

- Configure regular aging.

  Configure active aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ethernet active** *active-interval* command to set the active aging time of Layer 2 NetStream flow statistics.

     By default, the active aging time of Layer 2 NetStream flow statistics is 30 minutes.

  c. Run the **commit** command to commit the configuration.

  Configure inactive aging.

  a. Run the **system-view** command to enter the system view.

  b. Run the **netstream timeout ethernet inactive** *inactive-interval* command to set the inactive time of Layer 2 NetStream flow statistics.

     By default, the inactive aging time of Layer 2 NetStream flow statistics is 30 seconds.

  c. Run the **commit** command to commit the configuration.
- Configure forced aging.

  a. Run the **reset netstream cache ethernet slot** *slot-id* command in the user view to forcibly age out all Layer 2 NetStream flow statistics on the card.

----End

5.7.4 Configuring NetStream Layer 2 NetStream Flow Statistics Exporting

Context

Layer 2 NetStream flow statistics can be exported only when you have specified a source IP address and at least one destination IP address and one destination UDP port number for the exported packets.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ethernet source** { *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address for the exported packets carrying Layer 2 NetStream flow statistics.

By default, the source address of the exported packets carrying Layer 2 NetStream flow statistics is not configured.

If the source IP address is not specified, packets are not exported. The source address of the exported packets carrying Layer 2 NetStream flow statistics can be an IPv4 or IPv6 address. There must be a reachable route between the source IP address and destination IP address (NSC address). Two source IP addresses can be specified: one IPv4 address and one IPv6 address.

Step 3 Run the **netstream export ethernet host** { *ip-address* | **ipv6** *ipv6-address* } *port-number* [**vpn-instance** *vpn-instance-name*] command to configure the destination IP address and destination UDP port number for the exported packets carrying Layer 2 NetStream flow statistics.

By default, the destination IP address and destination UDP port number of the exported packets carrying Layer 2 NetStream flow statistics is not configured.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ethernet host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of IP addresses is exceeded and the configuration fails.

Step 4 Run the **commit** command to commit the configuration.

----End

5.7.5 Configuring the Interface Index Length in Layer 2 NetStream Flows

Context

The interface index length configured on the NDE must be the same as that configured on the NSC; otherwise, the NSC cannot resolve the NetStream packets sent from the NDE.

The NMS obtains interface information of exported packets according to the interface indexes in NetStream packets. Interface index formats include 16-bit and 32-bit. The NMS devices of different vendors may use different interface index formats. The interface index format used by the NDE must be the same as the interface index format used by the NMS. For example, if the NMS can parse 32-bit interface indexes, set the format of the interface indexes contained in exported NetStream packets to 32-bit.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ethernet index-switch** *index-switch* command to set the number of digits in the interface index contained in an exported packet carrying Layer 2 NetStream statistics.

By default, 16-bit interface indexes are contained in the exported packets carrying Layer 2 NetStream flow statistics.

Step 3 Run:

```
commit
```

The configuration is committed.

----End

5.7.6 Configuring Versions for Exported Packets

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream export ethernet version 9** command to set the version of exported packets carrying Layer 2 NetStream flow statistics.

By default, the export version for Layer 2 NetStream flow statistics is not set.

NOTE

The export version for Layer 2 NetStream flow statistics is fixed as V9.

Step 3 (Optional) Run the **netstream export ethernet template timeout-rate** *timeout-interval* command to set the interval at which the template is refreshed when the packets are exported in the format of V9.

By default, the template is refreshed every 30 minutes.

Step 4 Run the **commit** command to commit the configuration.

----End

5.7.7 Enabling Layer 2 NetStream Flow Statistics Collection on an Interface

Context

Layer 2 NetStream flow statistics can be exported only when you have enabled flow statistics on an interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream** { **inbound** | **outbound** } **ethernet** command to enable Layer 2 NetStream flow statistics collection on the interface.

By default, Layer 2 NetStream flow statistics collection is disabled on interfaces.

Step 4 Run the **commit** command to commit the configuration.

----End

5.7.8 Checking the Configuration

Context

You can run commands to verify that Layer 2 NetStream flow statistics exporting has been configured correctly.

Procedure

- Run the **display netstream cache ethernet** [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source mac-address** *mac-address* | **ethernet-type** *ethernet-type* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**] command to check detailed statistics about Layer 2 NetStream flows on the card.
- Run the **display netstream export ethernet template** command to check the exported template information.
- Run the **display netstream statistics ethernet slot** *slot-id* command to check Layer 2 NetStream flow statistics on the card.
- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.

----End

5.8 Configuring NetStream Top Talkers

NetStream Top Talkers filters traffic based on user-defined keywords, collects statistics on filtered traffic, sorts the traffic in a certain order, and displays only the top N traffic lines on screen. (N is the number of traffic lines recorded in the NetStream Top Talkers template). These N traffic lines are called Top Talkers.

Pre-configuration Tasks

Before configuring NetStream Top Talkers, complete the following task:

- Configuring link layer attributes of interfaces to ensure that the interfaces work properly

Configuration Process

Among all the NetStream Top Talkers configuration tasks, the task **Configuring a NetStream Top Talkers Template** should be performed before **Applying a NetStream Top Talkers Template to Interfaces**, and the task **Applying a NetStream Top Talkers Template to Interfaces** should be performed before **Starting the NetStream Top Talkers Function**. Other tasks can be performed in any sequence.

5.8.1 Configuring a NetStream Top Talkers Template

Context

When configuring the NetStream Top Talkers function, you need to configure a NetStream Top Talkers template first, and then apply the template to an interface. You can define the keywords used to filter traffic and traffic sorting order in the template.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream top-talkers** *talker-name* **ip** command to create a NetStream Top Talkers template and enter the template view.

By default, no NetStream Top Talkers template exists.

Step 3 (Optional) Run the **match ip** { **source-address** *ip-address* [*mask*] | **destination-address** *ip-address* [*mask*] | **nexthop-address** *ip-address* [*mask*] | **source-port** { **min** *port-number* | **max** *port-number* } | **destination-port** { **min** *port-number* | **max** *port-number* } | **source-as** *as-number* [**origin** | **peer**] | **destination-as** *as-number* [**origin** | **peer**] | **tos** *tos-value* | **dscp** *dscp-value* | **precedence** *precedence-value* | **protocol** { *protocol-number* | **tcp** | **udp** } | **packet-range** { **min** *minimum-range* | **max** *maximum-range* } | **byte-range** { **min** *minimum-range* | **max** *maximum-range* } } command to specify the keywords used to filter traffic.

By default, no keyword is specified in a NetStream Top Talkers template. If you run the command multiple times, multiple keywords are configured to filter traffic. The keywords **tos**, **dscp**, and **precedence** cannot be configured together in a NetStream Top Talkers template; otherwise, the filtering result may be unexpected. For example, if you specify **tos**, and then specify **dscp**, the device filers traffic based on the DSCP field of packets.

Step 4 Run the **cache-timeout** *millisecond* command to set the traffic statistics collection period in the NetStream Top Talkers template.

By default, the traffic statistics collection period in a NetStream Top Talkers template is not set. You are advised to set the period longer than 600000 ms (10 minutes). If the period is too short, the collected traffic statistics may be incomplete.

Step 5 Run the **top number** *number* command to set the number of Top Talkers that can be recorded in the NetStream Top Talkers template.

By default, the number of Top Talkers that can be recorded in a NetStream Top Talkers template is not set. A NetStream Top Talkers template can record a maximum of 200 Top Talkers.

Step 6 Run the **sort-by** { **bytes** | **packets** } command to specify the Top Talkers sorting order in the NetStream Top Talkers template.

By default, the Top Talkers sorting order is not specified in a NetStream Top Talkers template. Top Talkers can be sorted in either of the following orders in a NetStream Top Talkers template:

- Descending order of bytes: The Top Talker with the most bytes is listed on the top line.
- Descending order of packets: The Top Talker with the most packets is listed on the top line.

Step 7 Run the **commit** command to commit the configuration.

----End

5.8.2 Configuring NetStream Sampling Resources

Context

NetStream sampling can use mirroring or snoop resources. If NetStream sampling uses mirroring resources, NetStream and port mirroring cannot be configured on the same interface. If NetStream sampling uses snoop resources, NetStream and port mirroring can be configured on the same interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **netstream sampler inbound resource snoop** command to configure NetStream sampling to use snoop resources.

By default, NetStream sampling uses mirroring resources.

After this command is executed, inbound NetStream sampling cannot be configured in an interface view. If inbound NetStream sampling has been configured in an interface view, run the **undo netstream sampler** [**random-packets** *packet-interval*] **inbound** command to disable inbound NetStream sampling first, and then use this command.

Step 3 Run the **commit** command to commit the configuration.

----End

5.8.3 Configuring NetStream Sampling

Context

You can set the intervals for sampling packets so that only statistics of sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces the impact of NetStream on device performance.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 NetStream sampling can be configured in two ways:

- Configure NetStream sampling in the system view. The sampling configuration will take effect on all interfaces.

  Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on all interfaces.

  By default, packet sampling is not configured on any interface.

- Configure NetStream sampling in the interface view. The sampling configuration will take effect on this interface.

  NOTE

  When NetStream sampling uses snoop resources, inbound NetStream sampling cannot be configured in an interface view.

  a. Run the **interface** *interface-type interface-number* command to enter the interface view.

  b. Run the **netstream sampler random-packets** *packet-interval* { **inbound** | **outbound** } command to configure packet sampling on the interface.

     By default, packet sampling is not configured on any interface.

     If NetStream sampling is configured in both system view and interface view, the configuration in the interface view takes effect.

Step 3 Run the **commit** command to commit the configuration.

----End

5.8.4 Applying a NetStream Top Talkers Template to Interfaces

Context

NetStream Top Talkers can collect incoming and outgoing traffic statistics on an interface separately. It can collect traffic statistics, sort traffic, and display statistics results only after the NetStream sampling function is enabled on an interface and a NetStream Top Talkers template is applied to the interface.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **netstream top-talkers** *talker-name* **ip** { **inbound** | **outbound** } command to apply a NetStream Top Talkers template to the interface.

By default, a NetStream Top Talkers template is not applied to any interface. A maximum of two NetStream Top Talkers templates can be applied to one interface, which are used to collect and sort incoming and outgoing traffic separately.

Step 4 Run the **commit** command to commit the configuration.

----End

5.8.5 Starting the NetStream Top Talkers Function

Context

After a NetStream Top Talkers template is applied to an interface, the NetStream Top Talkers function must be started using a command; otherwise, the function does not take effect. The NetStream Top Talkers function can be started in either of the following ways:

- Scheduled start: The NetStream Top Talkers function is started at the specified time point.
- Immediate start.

Procedure

- Start the NetStream Top Talkers function on schedule.
  a. Run the **system-view** command to enter the system view.
  b. Run the **netstream top-talkers** *talker-name* **ip** command to enter the NetStream Top Talkers template view.
  c. Run the **starting time** *time date* command to set the time when the NetStream Top Talkers function will be started.

     By default, the time when the NetStream Top Talkers function will be started is not set.

NOTE

- The NetStream Top Talkers start time must be later than the system time; otherwise, the NetStream Top Talkers function cannot be started.
- The NetStream Top Talkers function can be started at the specified time only when the NetStream Top Talkers template is applied to an interface.
- When the NetStream Top Talkers function has been started on an interface, the NetStream Top Talkers template applied to this interface can also be applied to another interface. In this situation, traffic statistics on the later interface can only be collected in remaining time.
- If you run the **netstream top-talkers ip starting** command after the **starting time** *time date* command, the NetStream Top Talkers function is started immediately. When the specified time is reached, collected traffic statistics are deleted, traffic is not sorted in order, and this function is restarted.
- If you modify the NetStream Top Talkers template while the NetStream Top Talkers function is running, the NetStream Top Talkers function becomes invalid, collected traffic statistics are deleted, and traffic is not sorted in order.

d. Run the **commit** command to commit the configuration.

- Start the NetStream Top Talkers function immediately.

  Run the **netstream top-talkers** *talker-name* **ip starting** command to start the NetStream Top Talkers function.

  By default, the NetStream Top Talkers function is not started.

  NOTE

  - The NetStream Top Talkers function can be immediately started only when the NetStream Top Talkers template is applied to an interface.
  - When the NetStream Top Talkers function has been started on an interface, the NetStream Top Talkers template applied to this interface can also be applied to another interface. In this situation, traffic statistics on the later interface can only be collected in remaining time.
  - If you modify the NetStream Top Talkers template while the NetStream Top Talkers function is running, the NetStream Top Talkers function becomes invalid, collected traffic statistics are deleted, and traffic is not sorted in order.
  - If you restart the NetStream Top Talkers function while the NetStream Top Talkers function is running, collected traffic statistics are deleted, traffic is not sorted in order, and the NetStream Top Talkers function restarts.

----End

5.8.6 Checking the Configuration

Context

After all the configurations of NetStream Top Talkers are complete, you can check the configurations.

Procedure

- Run the **display netstream** { **all** | **global** | **interface** *interface-type interface-number* } command to check the NetStream configuration.
- Run the **display netstream top-talkers** *talker-name* **ip** [**interface** *interface-type interface-number*] **slot** *slot-id* command to check the traffic statistics and sorting results.

----End

6 Maintaining NetStream

About This Chapter

6.1 Clearing NetStream Statistics

Context

NOTICE

The statistics cannot be restored after being deleted.

Procedure

- Run the **reset netstream statistics ethernet** [**slot** *slot-id*] command in the user view to clear NetStream statistics on the specified card.
- Run the **reset netstream statistics ip** [**slot** *slot-id*] command in the user view to clear IPv4 flow statistics on the specified card.
- Run the **reset netstream statistics ipv6** [**slot** *slot-id*] command in the user view to clear IPv6 flow statistics on the specified card.

----End

7 Configuration Examples

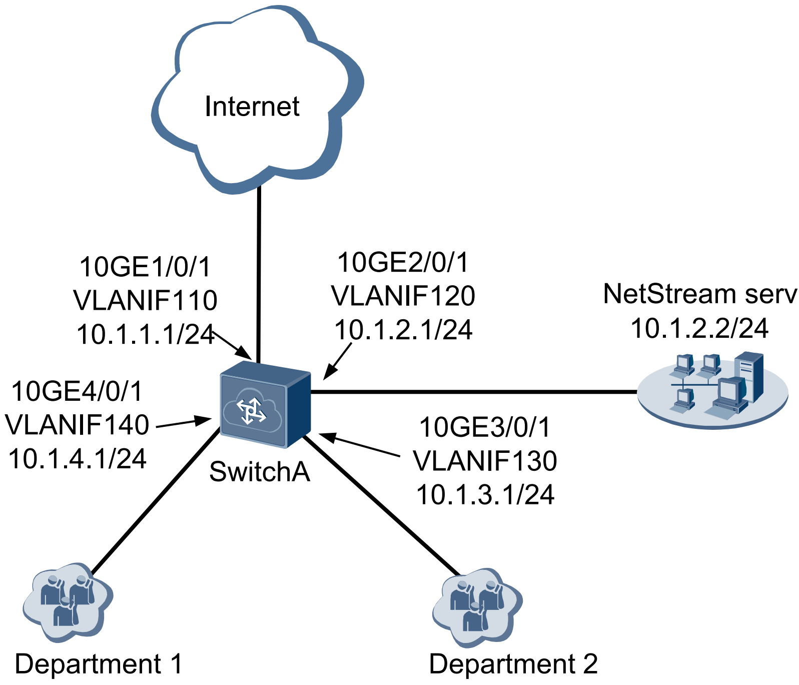
About This Chapter

7.1 Example for Configuring Original Flow Statistics Exporting

Networking Requirements

In **Figure 7-1**, departments 1 and 2 connect to the Internet through SwitchA. Network administrators want to collect statistics about traffic between the two departments and the Internet for network planning.

Figure 7-1 NetStream networking diagram



Configuration Roadmap

You can configure IPv4 original flow statistics exporting on 10GE1/0/1 of SwitchA. Configure SwitchA to collect statistics about incoming and outgoing traffic on the interface, and to send the statistics to the NetStream server for further analysis. The analysis result helps you plan the network.

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces on SwitchA.
2. Configure NetStream sampling.
3. Configure NetStream flow aging.
4. Configure original flow statistics exporting.
5. Configure the version for exported packets.
6. Enable original flow statistics collection on interfaces.

Procedure

Step 1 Configure IP addresses for interfaces on SwitchA as shown in **Figure 7-1**.

# Assign IP addresses to the interfaces of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 110
[*SwitchA-vlan110] quit
[*SwitchA] interface vlanif 110
[*SwitchA-Vlanif110] ip address 10.1.1.1 24
[*SwitchA-Vlanif110] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 110
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 110
[*SwitchA-10GE1/0/1] quit
[*SwitchA] vlan 120
[*SwitchA-vlan120] quit
[*SwitchA] interface vlanif 120
[*SwitchA-Vlanif120] ip address 10.1.2.1 24
[*SwitchA-Vlanif120] quit
[*SwitchA] interface 10ge 2/0/1
[*SwitchA-10GE2/0/1] port link-type trunk
[*SwitchA-10GE2/0/1] port trunk pvid vlan 120
[*SwitchA-10GE2/0/1] port trunk allow-pass vlan 120
[*SwitchA-10GE2/0/1] quit
[*SwitchA] vlan 130
[*SwitchA-vlan130] quit
[*SwitchA] interface vlanif 130
[*SwitchA-Vlanif130] ip address 10.1.3.1 24
[*SwitchA-Vlanif130] quit
[*SwitchA] interface 10ge 3/0/1
[*SwitchA-10GE3/0/1] port link-type trunk
[*SwitchA-10GE3/0/1] port trunk pvid vlan 130
[*SwitchA-10GE3/0/1] port trunk allow-pass vlan 130
[*SwitchA-10GE3/0/1] quit
[*SwitchA] vlan 140
[*SwitchA-vlan140] quit
[*SwitchA] interface vlanif 140
[*SwitchA-Vlanif140] ip address 10.1.4.1 24
[*SwitchA-Vlanif140] quit
[*SwitchA] interface 10ge 4/0/1
[*SwitchA-10GE4/0/1] port link-type trunk
[*SwitchA-10GE4/0/1] port trunk pvid vlan 140
[*SwitchA-10GE4/0/1] port trunk allow-pass vlan 140
[*SwitchA-10GE4/0/1] quit
```

Step 2 Configure NetStream sampling.

# Configure NetStream sampling for the incoming and outgoing packets on 10GE1/0/1 and set the sampling interval to 8192.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream sampler random-packets 8192 inbound
[*SwitchA-10GE1/0/1] netstream sampler random-packets 8192 outbound
[*SwitchA-10GE1/0/1] quit
```

Step 3 Configure NetStream flow aging.

# Set the inactive aging time to 100 seconds and enable FIN- and RST-based aging.

```
[*SwitchA] netstream timeout ip inactive 100
[*SwitchA] netstream timeout ip tcp-session
```

Step 4 Configure NetStream original flow statistics exporting.

# Set the source IP address of the exported packets carrying original flow statistics to 10.1.2.1, destination IP address to 10.1.2.2, and destination port number to 6000.

```
[*SwitchA] netstream export ip source 10.1.2.1
[*SwitchA] netstream export ip host 10.1.2.2 6000
```

Step 5 Configure the version for exported packets.

# Set the version of exported packets to V9.

```
[*SwitchA] netstream export ip version 9
```

Step 6 Enable original flow statistics collection on the interface.

# Enable NetStream statistics collection on 10GE1/0/1 for incoming and outgoing packets.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream outbound ip
[*SwitchA-10GE1/0/1] netstream inbound ip
[*SwitchA-10GE1/0/1] quit
[*SwitchA] commit
```

Step 7 Verify the configuration.

# View flow statistics.

```
[~SwitchA] display netstream statistics ip slot 1
 Time statistics were last cleared: -
 -------------------------------------------------------------------------------
 Packet Length    : Number
 -------------------------------------------------------------------------------
 1      ~    64   : 0
 65     ~    128  : 12
 129    ~    256  : 0
 257    ~    512  : 0
 513    ~    1024 : 0
 1025   ~    1500 : 0
 longer than 1500 : 0
 -------------------------------------------------------------------------------
 StreamType
      Current           Aged        Created       Exported       Exported
      (streams)         (streams)   (streams)     (streams)      (Packets)
 -------------------------------------------------------------------------------
 origin
            1              3              3              3              3
 -------------------------------------------------------------------------------
 as
            0              0              0              0              0
 -------------------------------------------------------------------------------
 as-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 protocol-port
            0              0              0              0              0
 -------------------------------------------------------------------------------
 protocol-port-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 mpls-label
            0              0              0              0              0
 -------------------------------------------------------------------------------
 vlan-id
            0              0              0              0              0
 -------------------------------------------------------------------------------
 bgp-nexthop-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

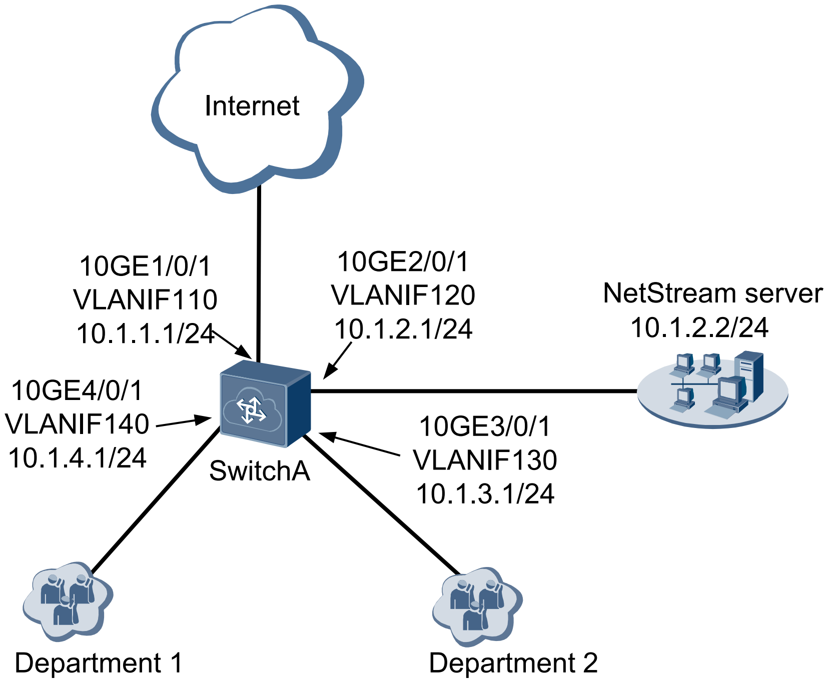
```
#
sysname SwitchA
#
vlan batch 110 120 130 140
#
netstream timeout ip inactive 100
netstream timeout ip tcp-session
netstream export ip version 9
netstream export ip source 10.1.2.1
netstream export ip host 10.1.2.2 6000
#
interface Vlanif110
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif130
 ip address 10.1.3.1 255.255.255.0
#
interface Vlanif140
 ip address 10.1.4.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
 netstream inbound ip
 netstream outbound ip
 netstream sampler random-packets 8192 inbound
 netstream sampler random-packets 8192 outbound
#
interface 10GE2/0/1
 port link-type trunk
 port trunk pvid vlan 120
 port trunk allow-pass vlan 120
#
interface 10GE3/0/1
 port link-type trunk
 port trunk pvid vlan 130
 port trunk allow-pass vlan 130
#
interface 10GE4/0/1
 port link-type trunk
 port trunk pvid vlan 140
 port trunk allow-pass vlan 140
#
return
```

7.2 Example for Configuring Aggregation Flow Statistics Exporting

Networking Requirements

In **Figure 7-2**, departments 1 and 2 connect to the Internet through SwitchA. Network administrators want to obtain key information exchange between the two departments and the Internet to understand communication status and traffic sources.

Figure 7-2 NetStream networking diagram



Configuration Roadmap

You can configure IPv4 aggregation flow statistics exporting on 10GE1/0/1 of SwitchA. Configure SwitchA to collect statistics about incoming and outgoing traffic on the interface, and to send the statistics to the NetStream server for further analysis. The analysis result helps you understand communication status and traffic sources.

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces on SwitchA.
2. Configure NetStream sampling.

3. Configure NetStream aggregation flow statistics exporting.
4. Configure the version for exported packets.
5. Enable aggregation flow statistics collection on interfaces.

Procedure

Step 1 Configure IP addresses for interfaces on SwitchA as shown in **Figure 7-2**.

# Assign IP addresses to the interfaces of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 110
[*SwitchA-vlan110] quit
[*SwitchA] interface vlanif 110
[*SwitchA-Vlanif110] ip address 10.1.1.1 24
[*SwitchA-Vlanif110] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 110
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 110
[*SwitchA-10GE1/0/1] quit
[*SwitchA] vlan 120
[*SwitchA-vlan120] quit
[*SwitchA] interface vlanif 120
[*SwitchA-Vlanif120] ip address 10.1.2.1 24
[*SwitchA-Vlanif120] quit
[*SwitchA] interface 10ge 2/0/1
[*SwitchA-10GE2/0/1] port link-type trunk
[*SwitchA-10GE2/0/1] port trunk pvid vlan 120
[*SwitchA-10GE2/0/1] port trunk allow-pass vlan 120
[*SwitchA-10GE2/0/1] quit
[*SwitchA] vlan 130
[*SwitchA-vlan130] quit
[*SwitchA] interface vlanif 130
[*SwitchA-Vlanif130] ip address 10.1.3.1 24
[*SwitchA-Vlanif130] quit
[*SwitchA] interface 10ge 3/0/1
[*SwitchA-10GE3/0/1] port link-type trunk
[*SwitchA-10GE3/0/1] port trunk pvid vlan 130
[*SwitchA-10GE3/0/1] port trunk allow-pass vlan 130
[*SwitchA-10GE3/0/1] quit
[*SwitchA] vlan 140
[*SwitchA-vlan140] quit
[*SwitchA] interface vlanif 140
[*SwitchA-Vlanif140] ip address 10.1.4.1 24
[*SwitchA-Vlanif140] quit
[*SwitchA] interface 10ge 4/0/1
[*SwitchA-10GE4/0/1] port link-type trunk
[*SwitchA-10GE4/0/1] port trunk pvid vlan 140
[*SwitchA-10GE4/0/1] port trunk allow-pass vlan 140
[*SwitchA-10GE4/0/1] quit
```

Step 2 Configure NetStream sampling.

# Configure NetStream sampling for the incoming and outgoing packets on 10GE1/0/1 and set the sampling interval to 1200.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 inbound
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 outbound
[*SwitchA-10GE1/0/1] quit
```

Step 3 Configure NetStream aggregation flow statistics exporting.

# Configure protocol-port aggregation, and set the source IP address of the exported packets to 10.1.2.1, destination IP address to 10.1.2.2, and destination port number to 6000.

```
[*SwitchA] netstream aggregation ip protocol-port
[*SwitchA-netstream-aggregation-protport] netstream export ip source 10.1.2.1
[*SwitchA-netstream-aggregation-protport] netstream export ip host 10.1.2.2 6000
[*SwitchA-netstream-aggregation-protport] enable
```

Step 4 Configure the version for exported packets.

# Set the version of the exported packets carrying aggregation flow statistics to V9.

```
[*SwitchA-netstream-aggregation-protport] export version 9
[*SwitchA-netstream-aggregation-protport] quit
```

Step 5 Enable aggregation flow statistics collection on the interface.

# Enable NetStream statistics collection on 10GE1/0/1 for incoming and outgoing packets.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream inbound ip
[*SwitchA-10GE1/0/1] netstream outbound ip
[*SwitchA-10GE1/0/1] quit
[*SwitchA] commit
```

Step 6 Verify the configuration.

# View flow statistics.

```
[~SwitchA] display netstream statistics ip slot 1
 Time statistics were last cleared: -
 -------------------------------------------------------------------------------
 Packet Length    : Number
 -------------------------------------------------------------------------------
 1      ~    64   : 0
 65     ~    128  : 439
 129    ~    256  : 0
 257    ~    512  : 0
 513    ~    1024 : 0
 1025   ~    1500 : 0
 longer than 1500 : 0
 -------------------------------------------------------------------------------
 StreamType
      Current           Aged        Created       Exported       Exported
      (streams)         (streams)   (streams)     (streams)      (Packets)
 -------------------------------------------------------------------------------
 origin
            4              3              3              0              0
 -------------------------------------------------------------------------------
 as
            0              0              0              0              0
 -------------------------------------------------------------------------------
 as-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 protocol-port
            3              0              3              0              0
 -------------------------------------------------------------------------------
 protocol-port-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 mpls-label
            0              0              0              0              0
 -------------------------------------------------------------------------------
 vlan-id
            0              0              0              0              0
 -------------------------------------------------------------------------------
 bgp-nexthop-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 110 120 130 140
#
interface Vlanif110
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif130
 ip address 10.1.3.1 255.255.255.0
#
interface Vlanif140
 ip address 10.1.4.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
 netstream inbound ip
 netstream outbound ip
 netstream sampler random-packets 1200 inbound
 netstream sampler random-packets 1200 outbound
#
interface 10GE2/0/1
 port link-type trunk
 port trunk pvid vlan 120
 port trunk allow-pass vlan 120
#
interface 10GE3/0/1
 port link-type trunk
 port trunk pvid vlan 130
 port trunk allow-pass vlan 130
#
interface 10GE4/0/1
 port link-type trunk
 port trunk pvid vlan 140
 port trunk allow-pass vlan 140
#
```

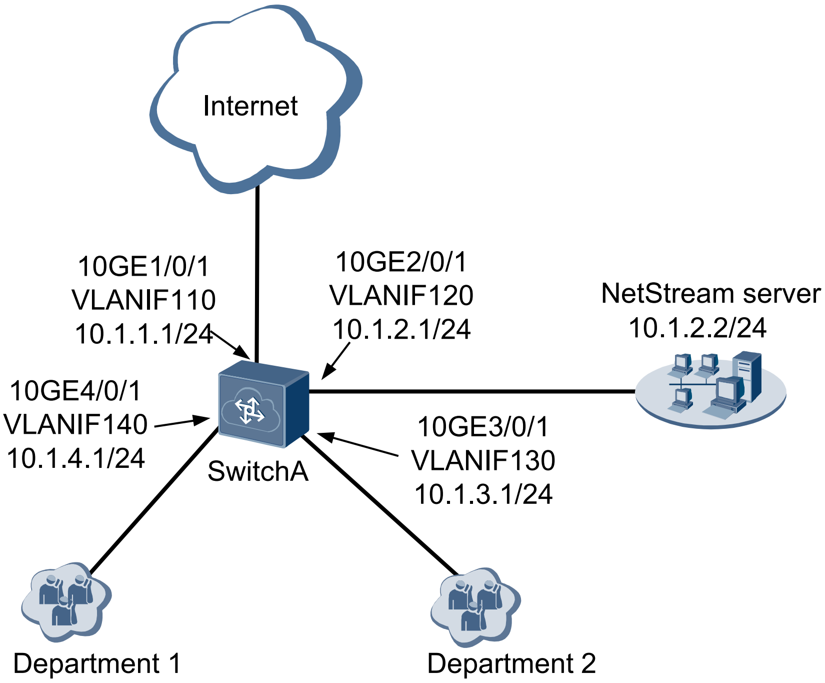
```
netstream aggregation ip protocol-port
 enable
 export version 9
 netstream export ip source 10.1.2.1
 netstream export ip host 10.1.2.2 6000
#
return
```

7.3 Example for Configuring Flexible Flow Statistics Exporting

Networking Requirements

In **Figure 7-3**, departments 1 and 2 connect to the Internet through SwitchA. Network administrators want to monitor communication between departments and the Internet and the websites often visited by the two departments.

Figure 7-3 NetStream networking diagram



Configuration Roadmap

You can configure IPv4 flexible flow statistics exporting on 10GE1/0/1 of SwitchA. Configure SwitchA to collect statistics about incoming and outgoing traffic on the interface, and to send the statistics to the NetStream server for further analysis. The analysis result helps you monitor the websites often visited by the two departments.

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces on SwitchA.
2. Configure a flexible flow statistics template.
3. Configure NetStream sampling.

4. Configure NetStream flexible flow statistics exporting.
5. Configure the version for exported packets.
6. Enable flexible flow statistics collection on interfaces.

Procedure

Step 1 Configure IP addresses for interfaces on SwitchA as shown in **Figure 7-3**.

# Assign IP addresses to the interfaces of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 110
[*SwitchA-vlan110] quit
[*SwitchA] interface vlanif 110
[*SwitchA-Vlanif110] ip address 10.1.1.1 24
[*SwitchA-Vlanif110] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 110
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 110
[*SwitchA-10GE1/0/1] quit
[*SwitchA] vlan 120
[*SwitchA-vlan120] quit
[*SwitchA] interface vlanif 120
[*SwitchA-Vlanif120] ip address 10.1.2.1 24
[*SwitchA-Vlanif120] quit
[*SwitchA] interface 10ge 2/0/1
[*SwitchA-10GE2/0/1] port link-type trunk
[*SwitchA-10GE2/0/1] port trunk pvid vlan 120
[*SwitchA-10GE2/0/1] port trunk allow-pass vlan 120
[*SwitchA-10GE2/0/1] quit
[*SwitchA] vlan 130
[*SwitchA-vlan130] quit
[*SwitchA] interface vlanif 130
[*SwitchA-Vlanif130] ip address 10.1.3.1 24
[*SwitchA-Vlanif130] quit
[*SwitchA] interface 10ge 3/0/1
[*SwitchA-10GE3/0/1] port link-type trunk
[*SwitchA-10GE3/0/1] port trunk pvid vlan 130
[*SwitchA-10GE3/0/1] port trunk allow-pass vlan 130
[*SwitchA-10GE3/0/1] quit
[*SwitchA] vlan 140
[*SwitchA-vlan140] quit
[*SwitchA] interface vlanif 140
[*SwitchA-Vlanif140] ip address 10.1.4.1 24
[*SwitchA-Vlanif140] quit
[*SwitchA] interface 10ge 4/0/1
[*SwitchA-10GE4/0/1] port link-type trunk
[*SwitchA-10GE4/0/1] port trunk pvid vlan 140
[*SwitchA-10GE4/0/1] port trunk allow-pass vlan 140
[*SwitchA-10GE4/0/1] quit
```

Step 2 Configure a flexible flow statistics template.

# Create a template named **record1** to aggregate flows based on destination and source IP addresses, and configure the exported packets to include the number of octets and packets.

```
[*SwitchA] netstream record record1 ip
[*SwitchA-netstream-record-record1] match ip destination-address
[*SwitchA-netstream-record-record1] match ip source-address
[*SwitchA-netstream-record-record1] collect counter bytes
[*SwitchA-netstream-record-record1] collect counter packets
[*SwitchA-netstream-record-record1] quit
```

Step 3 Configure NetStream sampling.

# Configure NetStream sampling for the incoming and outgoing packets on 10GE1/0/1 and set the sampling interval to 1200.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 inbound
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 outbound
[*SwitchA-10GE1/0/1] quit
```

Step 4 Configure NetStream flexible flow statistics exporting.

# Set the source IP address of the exported packets carrying flexible flow statistics to 10.1.2.1, destination IP address to 10.1.2.2, and destination port number to 6000.

```
[*SwitchA] netstream export ip source 10.1.2.1
[*SwitchA] netstream export ip host 10.1.2.2 6000
```

Step 5 Configure the version for exported packets.

# Set the version of exported packets to V9.

```
[*SwitchA] netstream export ip version 9
```

Step 6 Enable flexible flow statistics collection on the interface.

# Enable flexible flow statistics exporting for incoming and outgoing traffic on 10GE1/0/1, and apply the flexible flow statistics template to the interface.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream record record1 ip
[*SwitchA-10GE1/0/1] netstream inbound ip
[*SwitchA-10GE1/0/1] netstream outbound ip
[*SwitchA-10GE1/0/1] quit
[*SwitchA] commit
```

Step 7 Verify the configuration.

# View flow statistics.

```
[~SwitchA] display netstream statistics ip slot 1
 Time statistics were last cleared: -
 -------------------------------------------------------------------------------
 Packet Length    : Number
 -------------------------------------------------------------------------------
 1      ~    64   : 0
 65     ~    128  : 100
 129    ~    256  : 0
 257    ~    512  : 0
 513    ~    1024 : 0
 1025   ~    1500 : 0
 longer than 1500 : 0
 -------------------------------------------------------------------------------
 StreamType
      Current           Aged        Created       Exported       Exported
      (streams)         (streams)   (streams)     (streams)      (Packets)
 -------------------------------------------------------------------------------
 origin
            0              0              0              0              0
 -------------------------------------------------------------------------------
 as
            0              0              0              0              0
 -------------------------------------------------------------------------------
 as-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 protocol-port
            0              0              0              0              0
 -------------------------------------------------------------------------------
 protocol-port-tos
```

```
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 destination-prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix
            0              0              0              0              0
 -------------------------------------------------------------------------------
 prefix-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 mpls-label
            0              0              0              0              0
 -------------------------------------------------------------------------------
 vlan-id
            0              0              0              0              0
 -------------------------------------------------------------------------------
 bgp-nexthop-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 source-index-tos
            0              0              0              0              0
 -------------------------------------------------------------------------------
 record1
            5              1              2              0              0
 -------------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
vlan batch 110 120 130 140
#
netstream export ip version 9
netstream export ip source 10.1.2.1
netstream export ip host 10.1.2.2 6000
#
netstream record record1 ip
 collect counter bytes
 collect counter packets
 match ip destination-address
 match ip source-address
#
interface Vlanif110
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif130
 ip address 10.1.3.1 255.255.255.0
#
```

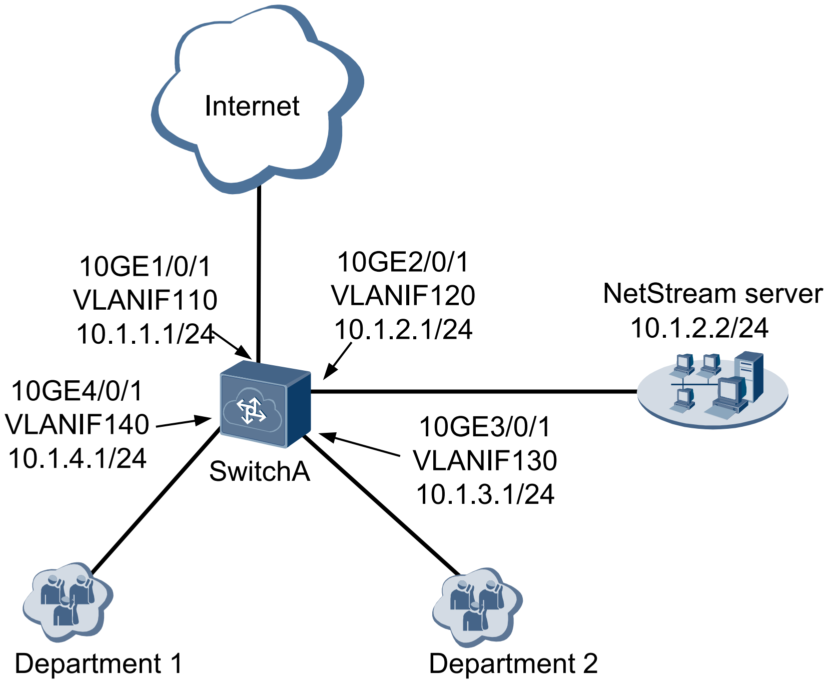
```
interface Vlanif140
 ip address 10.1.4.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
 netstream inbound ip
 netstream outbound ip
 netstream sampler random-packets 1200 inbound
 netstream sampler random-packets 1200 outbound
 netstream record record1 ip
#
interface 10GE2/0/1
 port link-type trunk
 port trunk pvid vlan 120
 port trunk allow-pass vlan 120
#
interface 10GE3/0/1
 port link-type trunk
 port trunk pvid vlan 130
 port trunk allow-pass vlan 130
#
interface 10GE4/0/1
 port link-type trunk
 port trunk pvid vlan 140
 port trunk allow-pass vlan 140
#
return
```

7.4 Example for Configuring Layer 2 NetStream Flow Statistics Exporting

Networking Requirements

In **Figure 7-4**, departments 1 and 2 connect to the Internet through SwitchA. Network administrators want to monitor communication between the two departments and the Internet, and perform accounting for each department.

Figure 7-4 NetStream networking diagram



Configuration Roadmap

You can configure Layer 2 NetStream flow statistics exporting on 10GE1/0/1 of SwitchA. Configure SwitchA to collect statistics about incoming and outgoing traffic on the interface, and to send the statistics to the NetStream server for further analysis. In this way, you can monitor communication between the two departments and the Internet, and perform accounting for each department.

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces on SwitchA.
2. Configure NetStream sampling.
3. Configure Layer 2 NetStream flow statistics exporting.
4. Configure the version for exported packets.
5. Enable Layer 2 statistics collection on the interface.

Procedure

Step 1 Configure IP addresses for interfaces on SwitchA as shown in **Figure 7-4**.

# Assign IP addresses to the interfaces of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan 110
[*SwitchA-vlan110] quit
[*SwitchA] interface vlanif 110
[*SwitchA-Vlanif110] ip address 10.1.1.1 24
[*SwitchA-Vlanif110] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 110
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 110
```

```
[*SwitchA-10GE1/0/1] quit
[*SwitchA] vlan 120
[*SwitchA-vlan120] quit
[*SwitchA] interface vlanif 120
[*SwitchA-Vlanif120] ip address 10.1.2.1 24
[*SwitchA-Vlanif120] quit
[*SwitchA] interface 10ge 2/0/1
[*SwitchA-10GE2/0/1] port link-type trunk
[*SwitchA-10GE2/0/1] port trunk pvid vlan 120
[*SwitchA-10GE2/0/1] port trunk allow-pass vlan 120
[*SwitchA-10GE2/0/1] quit
[*SwitchA] vlan 130
[*SwitchA-vlan130] quit
[*SwitchA] interface vlanif 130
[*SwitchA-Vlanif130] ip address 10.1.3.1 24
[*SwitchA-Vlanif130] quit
[*SwitchA] interface 10ge 3/0/1
[*SwitchA-10GE3/0/1] port link-type trunk
[*SwitchA-10GE3/0/1] port trunk pvid vlan 130
[*SwitchA-10GE3/0/1] port trunk allow-pass vlan 130
[*SwitchA-10GE3/0/1] quit
[*SwitchA] vlan 140
[*SwitchA-vlan140] quit
[*SwitchA] interface vlanif 140
[*SwitchA-Vlanif140] ip address 10.1.4.1 24
[*SwitchA-Vlanif140] quit
[*SwitchA] interface 10ge 4/0/1
[*SwitchA-10GE4/0/1] port link-type trunk
[*SwitchA-10GE4/0/1] port trunk pvid vlan 140
[*SwitchA-10GE4/0/1] port trunk allow-pass vlan 140
[*SwitchA-10GE4/0/1] quit
```

Step 2 Configure NetStream sampling.

# Configure NetStream sampling for the incoming and outgoing packets on 10GE1/0/1 and set the sampling interval to 1200.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 inbound
[*SwitchA-10GE1/0/1] netstream sampler random-packets 1200 outbound
[*SwitchA-10GE1/0/1] quit
```

Step 3 Configure Layer 2 NetStream flow statistics exporting.

# Set the source IP address of the exported packets carrying Layer 2 NetStream flow statistics to 10.1.2.1, destination IP address to 10.1.2.2, and destination port number to 6000.

```
[*SwitchA] netstream export ethernet source 10.1.2.1
[*SwitchA] netstream export ethernet host 10.1.2.2 6000
```

Step 4 Configure the version for exported packets.

# Set the version of exported packets to V9.

```
[*SwitchA] netstream export ethernet version 9
```

Step 5 Enable Layer 2 statistics collection on the interface.

# Enable NetStream statistics collection on 10GE1/0/1 for incoming and outgoing packets.

```
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] netstream inbound ethernet
[*SwitchA-10GE1/0/1] netstream outbound ethernet
[*SwitchA-10GE1/0/1] quit
[*SwitchA] commit
```

Step 6 Verify the configuration.

# View flow statistics.

```
[~SwitchA] display netstream statistics ethernet slot 1
 Time statistics were last cleared: -
 -------------------------------------------------------------------------------
 Packet Length    : Number
 -------------------------------------------------------------------------------
 1      ~    64   : 0
 65     ~    128  : 20
 129    ~    256  : 0
 257    ~    512  : 0
 513    ~    1024 : 0
 1025   ~    1500 : 0
 longer than 1500 : 0
 -------------------------------------------------------------------------------
 StreamType
      Current           Aged        Created       Exported       Exported
      (streams)         (streams)   (streams)     (streams)      (Packets)
 -------------------------------------------------------------------------------
 ethernet
            1             15             15             15             15
 -------------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

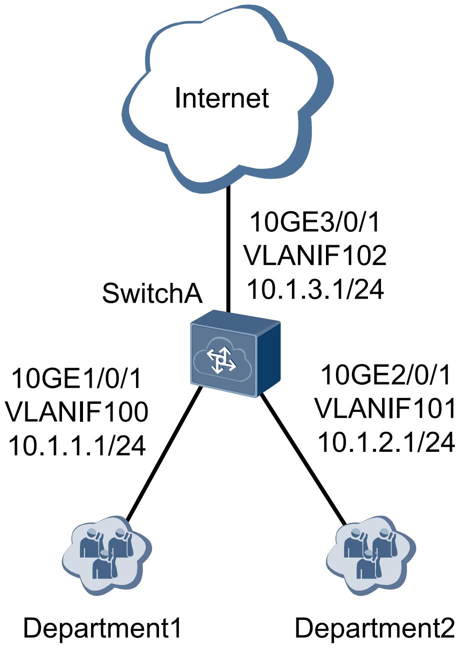
```
#
sysname SwitchA
#
vlan batch 110 120 130 140
#
netstream export ethernet version 9
netstream export ethernet source 10.1.2.1
netstream export ethernet host 10.1.2.2 6000
#
interface Vlanif110
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif130
 ip address 10.1.3.1 255.255.255.0
#
interface Vlanif140
 ip address 10.1.4.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
 netstream inbound ethernet
 netstream outbound ethernet
 netstream sampler random-packets 1200 inbound
 netstream sampler random-packets 1200 outbound
#
interface 10GE2/0/1
 port link-type trunk
 port trunk pvid vlan 120
 port trunk allow-pass vlan 120
#
interface 10GE3/0/1
 port link-type trunk
 port trunk pvid vlan 130
 port trunk allow-pass vlan 130
#
interface 10GE4/0/1
 port link-type trunk
 port trunk pvid vlan 140
 port trunk allow-pass vlan 140
#
return
```

7.5 Example for Configuring NetStream Top Talkers

Networking Requirements

In **Figure 7-5**, departments 1 and 2 of an enterprise connect to the Internet through SwitchA, and no NetStream server is located on the network. To monitor traffic transmitted between the two departments and the Internet, the network administrator intends to configure NetStream Top Talkers on 10GE3/0/1 of SwitchA. The NetStream Top Talkers function can collect statistics on incoming and outgoing traffic on the interface separately, sort the Top Talkers, and displays results.

Figure 7-5 NetStream Top Talkers networking diagram



Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to the interfaces of SwitchA.
2. Configure a NetStream Top Talkers template.
3. Configure NetStream sampling.
4. Apply the NetStream Top Talkers template to an interface.
5. Start the NetStream Top Talkers function.

Procedure

Step 1 Assign IP addresses to the interfaces of SwitchA.

# Assign IP addresses to the interfaces of SwitchA.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] vlan batch 100 101 102
[*SwitchA] interface vlanif 100
[*SwitchA-Vlanif100] ip address 10.1.1.1 24
[*SwitchA-Vlanif100] quit
[*SwitchA] interface vlanif 101
[*SwitchA-Vlanif101] ip address 10.1.2.1 24
[*SwitchA-Vlanif101] quit
[*SwitchA] interface vlanif 102
[*SwitchA-Vlanif102] ip address 10.1.3.1 24
[*SwitchA-Vlanif102] quit
[*SwitchA] interface 10ge 1/0/1
[*SwitchA-10GE1/0/1] port link-type trunk
[*SwitchA-10GE1/0/1] port trunk pvid vlan 100
[*SwitchA-10GE1/0/1] port trunk allow-pass vlan 100
[*SwitchA-10GE1/0/1] quit
[*SwitchA] interface 10ge 2/0/1
[*SwitchA-10GE2/0/1] port link-type trunk
[*SwitchA-10GE2/0/1] port trunk pvid vlan 101
[*SwitchA-10GE2/0/1] port trunk allow-pass vlan 101
[*SwitchA-10GE2/0/1] quit
[*SwitchA] interface 10ge 3/0/1
[*SwitchA-10GE3/0/1] port link-type trunk
[*SwitchA-10GE3/0/1] port trunk pvid vlan 102
[*SwitchA-10GE3/0/1] port trunk allow-pass vlan 102
[*SwitchA-10GE3/0/1] quit
[*SwitchA] commit
```

Step 2 Configure a NetStream Top Talkers template.

# Create a NetStream Top Talkers template named **test**, specify the traffic filtering keyword as destination IP address, set the number of Top Talkers that can be recorded in the NetStream Top Talkers template to 200, set the traffic statistics collection period to 1200000 ms (20 minutes), and specify the Top Talker sorting order as number of packets.

```
[~SwitchA] netstream top-talkers test ip
[*SwitchA-netstream-top-talkers-test] match ip destination-address 10.1.3.2 24
[*SwitchA-netstream-top-talkers-test] top number 200
[*SwitchA-netstream-top-talkers-test] cache-timeout 1200000
[*SwitchA-netstream-top-talkers-test] sort-by packets
[*SwitchA-netstream-top-talkers-test] quit
[*SwitchA] commit
```

Step 3 Configure NetStream sampling.

# Configure NetStream sampling for the incoming and outgoing packets on 10GE3/0/1 and set the sampling interval to 8192.

```
[~SwitchA] interface 10ge 3/0/1
[~SwitchA-10GE3/0/1] netstream sampler random-packets 8192 inbound
[*SwitchA-10GE3/0/1] netstream sampler random-packets 8192 outbound
[*SwitchA-10GE3/0/1] quit
[*SwitchA] commit
```

Step 4 Apply the NetStream Top Talkers template to an interface.

# Enable NetStream Top Talkers statistics collection on 10GE3/0/1 for incoming and outgoing traffic.

```
[~SwitchA] interface 10ge 3/0/1
[~SwitchA-10GE3/0/1] netstream top-talkers test ip inbound
[*SwitchA-10GE3/0/1] netstream top-talkers test ip outbound
```

```
[*SwitchA-10GE3/0/1] quit
[*SwitchA] commit
[~SwitchA] quit
```

Step 5 Start the NetStream Top Talkers function.

# Start the NetStream Top Talkers function immediately.

```
<SwitchA> netstream top-talkers test ip starting
```

Step 6 Verify the configuration.

# After the configurations are complete, view the Top Talkers statistics and sorting results on 10GE3/0/1.

```
<SwitchA> display netstream top-talkers test ip interface 10ge 3/0/1 slot 3
Top-Talkers Name   : test
Flow Type          : IPv4
Top Number         : 200
Sort-By            : PACKETS
Cache-Timeout      : 1200000
BeginCache Time    : 2014-12-10 09:59:44
match DstIP/Mask   : 10.1.3.2/255.255.255.0
 --------------------------------------------------------------------------------
 SrcIP                     SrcPort  Bytes              BPS         BPM
 DstIP                     DstPort  Packets            PPS         PPM
 Interface                 Protocol Direction
 --------------------------------------------------------------------------------

 10.1.1.2                   0        62762800           2096200     125777100
 10.1.3.2                   0        729800             24300       1462500
 10GE3/0/1                  114      Inbound

 10.1.2.2                   0        61894200           2067200     124036400
 10.1.3.2                   0        719700             24000       1442200
 10GE3/0/1                  114      Inbound

 --------------------------------------------------------------------------------
 2 of 200 top talkers shown. 2 flows processed.
 --------------------------------------------------------------------------------
```

----End

Configuration Files

SwitchA configuration file

```
#
sysname SwitchA
#
netstream top-talkers test ip
 match ip destination-address 10.1.3.2 255.255.255.0
 top number 200
 sort-by packets
 cache-timeout 1200000
#
vlan batch 100 to 102
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif101
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif102
 ip address 10.1.3.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100
#
interface 10GE2/0/1
 port link-type trunk
 port trunk pvid vlan 101
 port trunk allow-pass vlan 101
#
interface 10GE3/0/1
 port link-type trunk
 port trunk pvid vlan 102
 port trunk allow-pass vlan 102
 netstream sampler random-packets 8192 inbound
 netstream sampler random-packets 8192 outbound
 netstream top-talkers test ip inbound
 netstream top-talkers test ip outbound
#
return
```

8 References

The following table lists the references of this document.

Document	Description	Remarks
RFC 3917	Requirements for IP Flow Information Export (IPFIX)	-
RFC 3954	Cisco Systems NetFlow Services Export Version 9	-