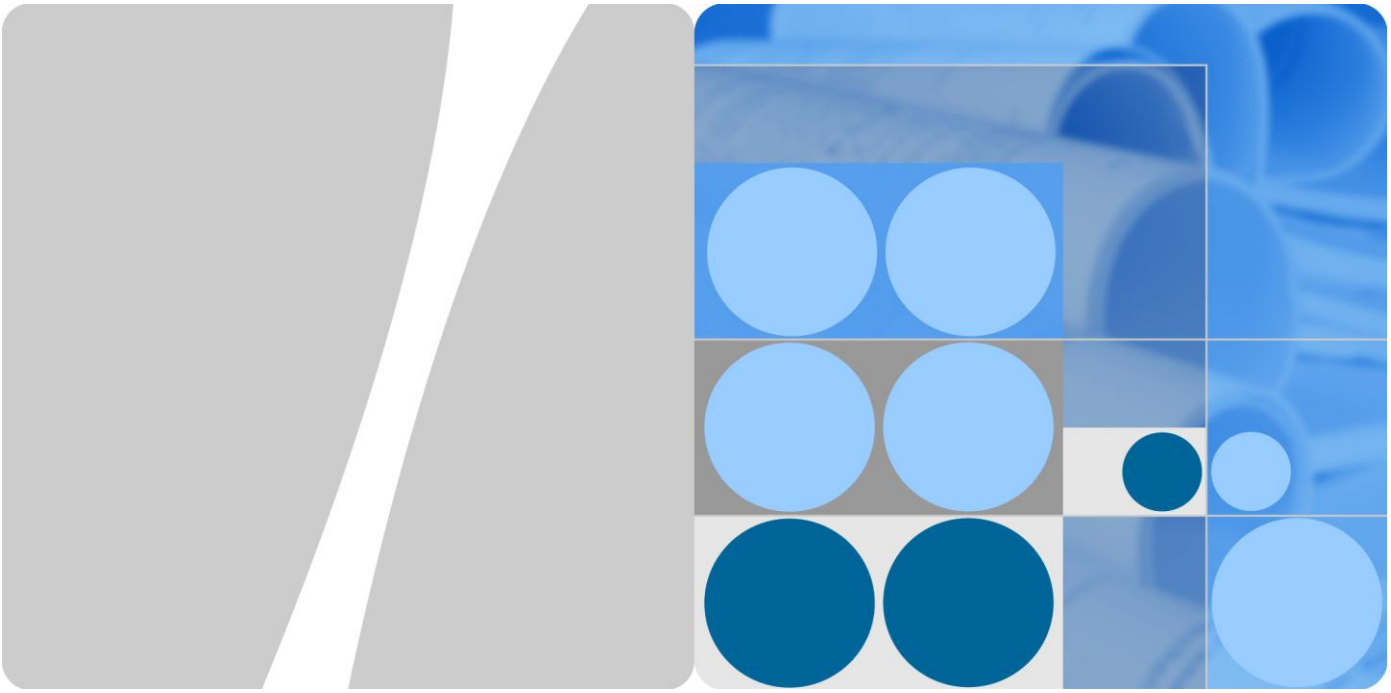


NetStream (Integrated) Technology White Paper

Issue 01

Date 2012-9-6

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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://www.huawei.com

Email: support@huawei.com

Contents

NetStream

About This Chapter

1.1 Introduction

Definition

NetStream is a traffic statistics and analysis technology.

Purpose

The Internet provides users with high bandwidth and supports more services and applications. Enterprises require fine-grained management and accounting, which poses higher requirements on traffic statistics and analysis. Traditional traffic statistics technologies such as SNMP and port mirroring cannot meet these requirements because of their limitations (see Table 1-1). A new technology is required to better support network traffic statistics.

NetStream has been developed to address this problem. NetStream collects classified statistics about service traffic and resource usage, and sends the statistics to a dedicated server or a network management system (NMS) that has NetStream software installed for further analysis.

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

Traffic Statistics Method	Implementation	Limitation
Statistics based on	Saves counter indexes in the routing table on a device to count the number	This method applies to collection of statistics about simple information

Traffic Statistics Method	Implementation	Limitation
IP packets	of bytes and packets that pass through the device.	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.
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 because a dedicated server is required to collect statistics. In addition, this method occupies a port. Statistics cannot be collected on a port 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 server and dedicated hardware devices are required.

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 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.

- User monitoring and analysis

NetStream allows network administrators to obtain network resource usage of users so that they can efficiently plan and allocate network resources and ensure network running security.

NOTE

The NetStream function is incompatible with the IP Source Trail function and you cannot configure them simultaneously.

Currently, only E-series boards support NetStream.

1.2 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	-

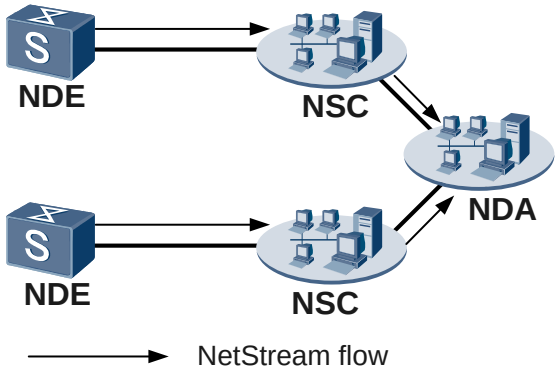
1.3 Principles

1.3.1 Basic Principles of NetStream

Components of a NetStream System

As shown in Figure 1-1, three roles are involved in a NetStream system: NetStream data exporter (NDE), NetStream collector (NSC), and NetStream data analyzer (NDA).

Figure 1-1 Networking diagram of a NetStream system



- 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 switch 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.

NOTE

In practice, the NSC and NDA are integrated on a NetStream server.

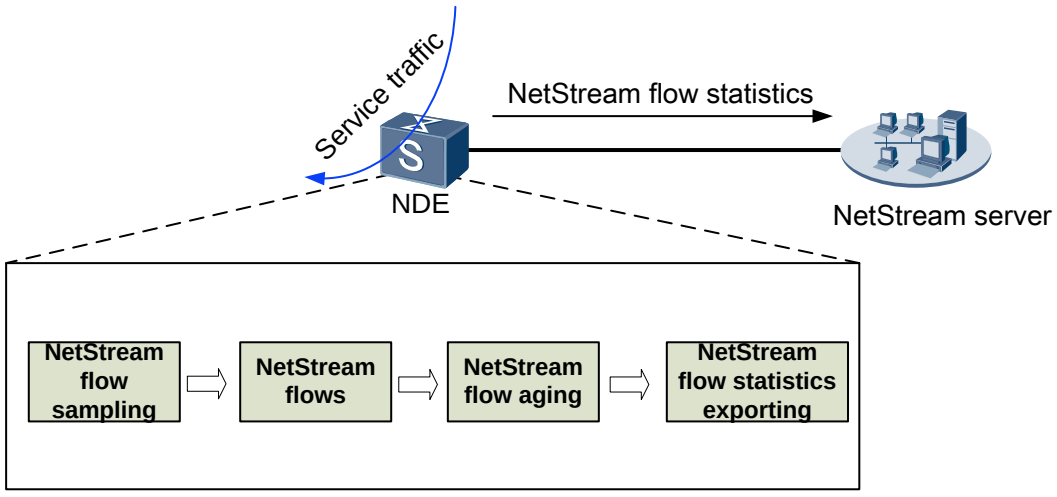
NetStream Working Mechanism

A NetStream system works as follows:

1. An NDE periodically exports detailed data about flows to an NSC.
2. The NSC processes the data and sends it to an NDA.
3. The NDA analyzes the data for applications such as accounting and network planning.

   In most cases, datacom products function as NDEs in a NetStream system. This document mainly describes NDE implementation.

Figure 1-1 Diagram for implementing NetStream



As shown in Figure 1-1, a switch configured with NetStream functions as the NDE and is properly forwarding service traffic. The NetStream module on the NDE samples packets (see1.3.2 NetStream Packet Sampling), creates a flow based on the collected data (see You can sample incoming traffic on an interface only after running the **ip netstream inbound** command on the interface to enable NetStream flow statistics collection for incoming traffic.

), ages out the flow (see NetStream Flow Aging), and exports the flow statistics (see NetStream Flow Statistics Exporting). In this manner, the NDE periodically exports detailed data about flows to the NSC.

1.3.2 NetStream Packet Sampling

Incoming traffic and outgoing traffic are sampled for statistics. You can set an interval for sampling packets so that only statistics about sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces NetStream impact on device performance.

The following sampling modes are available:

- Packet-based random sampling

  The NDE randomly samples a packet from a specified number of packets transmitted. For example, if the number of packets is set to 100, the NDE randomly samples a packet from every 100 packets. This mode applies to sampling regular traffic.

- Packet-based regular sampling

  The NDE samples a packet every time when a specified number of packets are transmitted. For example, if the number of packets is set to 100, the NDE samples a packet after every 100 packets are transmitted. If the NDE samples the fifth packet at the first time, the NDE samples the 105th packet, the 205th packet, and so on. This mode applies to network traffic accounting.

- Time-based random sampling

  The NDE randomly samples a packet in a specified interval. For example, if the interval is set to 100, the NDE randomly samples a packet in every 100 ms. This mode applies to sampling regular traffic.

- Time-based regular sampling

  The NDE samples a packet at a specified interval. For example, the interval is set to 100. If the NetStream module samples a packet at the fifth millisecond at the first time, the NDE samples a packet at the 105th millisecond, the 205th millisecond, and so on. This mode applies to networks with a large volume of traffic.

Currently, the switches support only packet-based regular sampling for incoming and outgoing traffic. You can configure one direction or both.

You can run the following commands to configure the packet-based regular sampling on GE1/0/1 and set the sampling ratio to 1:1200 for incoming traffic:

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] ip netstream sampler fix-packets 1200 inbound
[Quidway-GigabitEthernet1/0/1] ip netstream inbound
```

NOTE

You can sample incoming traffic on an interface only after running the **ip netstream inbound** command on the interface to enable NetStream flow statistics collection for incoming traffic.

1.3.3 NetStream Flows

NetStream provides packet statistics based on flows. NetStream supports statistics about IP packets (including UDP, TCP, and ICMP packets).

- For IPv4 packets, IPv4 NetStream defines a flow based on the destination IP address, source IP address, destination port number, source port number, protocol number, ToS,

and inbound or outbound interface. Packets with the same 7-tuple information are marked as one flow.

- For IPv6 packets, IPv6 NetStream defines a flow based on the destination IP address, source IP address, destination port number, source port number, protocol number, traffic class, flow label, and inbound or outbound interface. Packets with the same 8-tuple information are marked as one flow.

1.3.4 NetStream Flow Aging

NetStream flow aging is the prerequisite for exporting flow statistics to the NSC. After NetStream is enabled on a device, flow statistics are stored in the NetStream cache on the device. When a NetStream flow is aged out, the NDE exports the flow statistics in the cache to the NSC using NetStream packets of a specified version.

NetStream flows are aged out in the following modes:

- Regular aging
  - Active aging

    Packets are added to a flow continuously in a specified period since the first packet is added to the flow. After the active aging timer expires, the flow statistics are exported. Active aging enables the NDE to periodically export the statistics about the flows that last for a long period.
  - Inactive aging

    If no packet is added to a flow in a specified period after the last packet is added to the flow, the NDE exports flow statistics to the NetStream server. Inactive aging clears unnecessary entries in the NetStream cache so that the system can fully leverage statistical entries. Inactive aging enables the NDE to export the statistics about flows that last for a short period. Once adding packets to a flow stops, the NDE exports the flow statistics to save memory space.

  Currently, the switch supports only inactive aging. You can run the following command to set the inactive aging time to 20s:

  ```
  [Quidway] ip netstream timeout inactive 20
  ```

- FIN- or RST-based aging

  The FIN or RST flag in a TCP packet indicates that a TCP connection is terminated. When receiving a packet with the FIN or RST flag, the NDE immediately ages the corresponding NetStream flow.

  It is recommended that you enable this aging mode. You can run the following command to enable FIN- or RST-based aging:

  ```
  [Quidway] ip netstream tcp-flag enable
  ```

- Byte-based aging

  The number of bytes is recorded for each flow in the NetStream cache. When the number of bytes of a flow exceeds the specified upper limit, the flow overflows. Therefore, when finding that the number of bytes of a flow exceeds the specified upper limit, the NDE immediately ages the flow to prevent a byte counting error. The hardware byte counter is a 64–bit counter, and the upper limit for bytes is 4294967295 bytes (about 3.9 GB).

  This aging mode is enabled by default, which requires no configuration and cannot be disabled.

- Forced aging

You can run commands to forcibly age all flows in the NetStream cache. Forced aging is used when existing flows do not meet aging conditions but the latest statistics are required or when some flows fail to be aged out due to abnormal NetStream services.

You can run the following command to forcible aging flows in the cache of slot 3:

```
[Quidway] reset ip netstream cache slot 3
```

1.3.5 NetStream Flow Statistics Exporting

After aging flows in the NetStream cache, the NDE exports the flow statistics to a specified NSC for further analysis. Original, aggregation, and flexible flow statistics are exported as packets of V5, V8, or V9.

I. Flow Statistics Exporting Modes

Original flow statistics exporting

In original flow statistics exporting mode, the NDE collects statistics about all flows. After the aging timer expires, the NDE exports statistics about each flow to the NetStream server.

This mode enables the NetStream server to obtain detailed statistics about each flow. However, this mode increases the network bandwidth and CPU usage. In addition, these statistics occupy much memory space of the NDE, which increases the cost.

After NetStream sampling and aging are configured, the NDE can export original flow statistics only when you configure the exported packet attributes including the source address, destination IP address, and destination UDP port number.

You can run the following commands to set the source address of the exported packets carrying original flow statistics to 1.1.1.1, destination IP address to 1.1.1.2, and destination UDP port number to 6000.

```
[Quidway] ip netstream export source 1.1.1.1
[Quidway] ip netstream export host 1.1.1.2 6000
```

Aggregation flow statistics exporting

The NDE aggregates flow statistics with the same aggregation entry values and exports the aggregation flow statistics to a specified NetStream server. This mode greatly saves network bandwidth. The NDE supports the aggregation modes described in Table 1-1.

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 1-1 Aggregation modes

Aggregation Mode	Aggregation Entries
as	Source AS number, destination AS number, inbound interface index, and outbound interface index
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

Aggregation Mode	Aggregation Entries
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
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

After NetStream sampling and aging are configured, you must configure aggregation keywords and exported packet attributes, and enable the aggregation function in the aggregation view.

You can run the following commands to configure exporting of aggregation flow statistics (This example uses the protocol-port aggregation mode):

```
[Quidway] ip netstream aggregation protocol-port
[Quidway-aggregation-protport] ip netstream export source 1.1.1.1
[Quidway-aggregation-protport] ip netstream export host 1.1.1.2 6000
[Quidway-aggregation-protport] enable
```

NOTE

If you configure the exported packet attributes both in the aggregation view and system view, the configuration in the aggregation view takes effect.

Only when the exported packet attributes are not configured in the aggregation view, the configuration in the system takes effect. In this case, statistics about original flows and aggregation flows are both exported.

Flexible flow statistics exporting

Similar to exporting of aggregation flow statistics, statistics about flexible flows are exported only after an aggregation keyword is set. The difference lies in that statistics about flexible flows are exported based on the hardware and flows matching aggregation keywords are directly aggregated, while in the exporting of aggregation flow statistics, original flows are aggregated. Flexible flows are established based on the customized configuration. Users can configure flow statistics collection based on the protocol type, DSCP field, source IP address, destination IP address, source port number, destination port number, or flow label as required. The NDE then exports the flow statistics to the NetStream server. Compared to original flow statistics exporting, flexible flow statistics exporting occupies less traffic and provides users with a flexible way to collect NetStream statistics.

After NetStream sampling and aging are configured, you must configure a flexible flow statistics template and bind the template to the interface in addition to configuring the exported packet attributes.

You can run the following commands to configure flexible flow statistics exporting (The source IP address is used in the flexible flow statistics template):

```
[Quidway] ip netstream export source 1.1.1.1
[Quidway] ip netstream export host 1.1.1.2 6000
[Quidway] ip netstream record test
Info: Creating the new record succeeded.
[Quidway-record-test] match ip source-address
[Quidway-record-test] collect counter bytes
[Quidway-record-test] collect counter packets
[Quidway-record-test] collect interface input
[Quidway-record-test] collect interface output
[Quidway-record-test] quit
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] port ip netstream record test
Info: Configuring a record on the interface succeeded.
[Quidway-GigabitEthernet1/0/1] ip netstream inbound
[Quidway-GigabitEthernet1/0/1] ip netstream outbound
```

NOTE

- When configuring a flexible flow statistics template, you can configure one or more keywords. When you configure multiple keywords such as the source IP address and destination IP address, only the packets with the same source IP address and same destination IP address are added to the flow.
- You must bind the flexible flow statistics template to the interface before enabling the NetStream statistics collection function on the interface. Therefore, you need to run the **port ip netstream record** command before the **ip netstream** command. If you run the **ip netstream** command first on the interface, the interface collects statistics about original flows.

II. Versions of Exported Packets

At present, the versions of NetStream exported packets are V5, V8, and V9. Other versions are in the experimental stage and have not been put to commercial use. 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 version 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. V9 supports the exporting of BGP next hop information and IPv6 statistics.

Exported packets of V9 are easy to expand and can be flexibly exported based on the template. V9 supports the exporting of IPv6 and BGP next-hop information. It is recommended that you set the version of exported packets to V9.

For exporting statistics about original and flexible flows, you can run the following command to set the version of exported packets to V9:

```
[Quidway] ip netstream export version 9
```

For exporting statistics about aggregation flows, you can run the following commands to set the version of exported packets to V9 (This example uses the protocol-port aggregation mode):

```
[Quidway] ip netstream aggregation protocol-port
[Quidway-aggregation-protport] export version 9
```

III. Mapping Between Flow Statistics Exporting Modes and Packet Versions

Statistics about a NetStream flow are exported based on a specified flow statistics exporting mode and a specified packet version. Each flow exporting mode maps a packet version, as described in Table 1-1

Table 1-1 Mapping between flow statistics exporting modes and packet versions

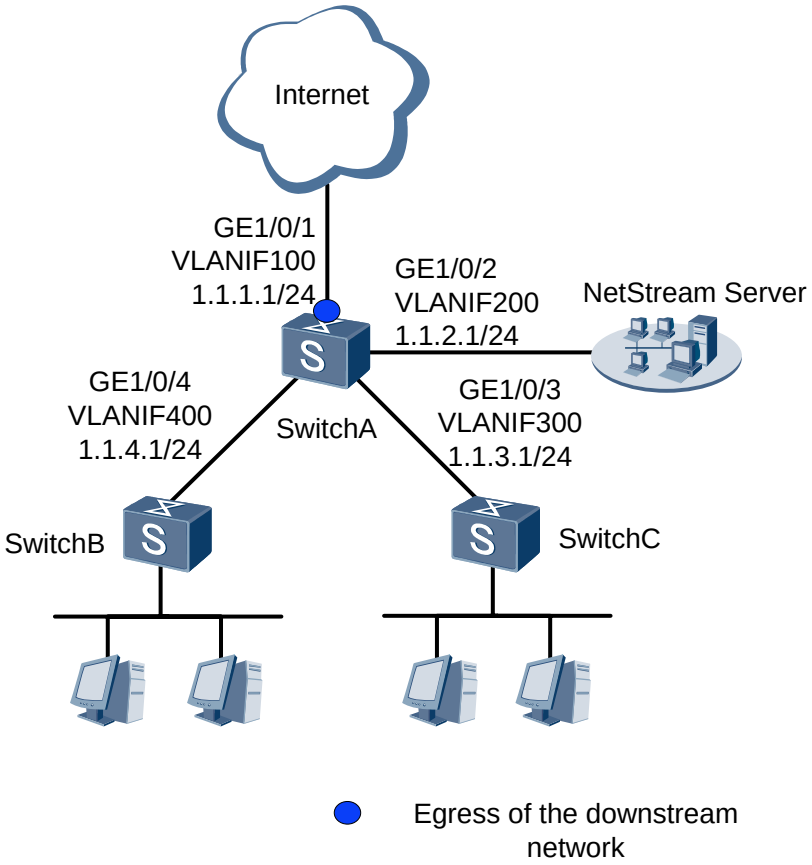
Flow Statistics Exporting Mode	Packet Version
Original flow statistics exporting	V5 and V9 By default, the version of exported packets carrying IPv4 flow statistics is V5, and the version of exported packets carrying IPv6 flow statistics is V9.
Aggregation flow statistics exporting	V8 and V9 By default, V8 supports exported packets carrying IPv4 aggregation flow statistics.
Flexible flow statistics exporting	V9

1.4 Applications

1.4.1 Typical Applications of NetStream for Network Monitoring

On a network shown in Figure 1-1, SwitchA connects the downstream network to the Internet. A large number of communication packets are stored on SwitchA. Network administrators want to know the bandwidths occupied by services. The NetStream function needs to be configured on SwitchA to monitor real-time traffic on the interface connecting to the Internet. The traffic monitoring information helps network administrators determine the network running status and discover inappropriate network structures or performance bottlenecks on networks.

Figure 1-1 Networking diagram of NetStream



Configuration roadmap:

You can configure IPv4 NetStream flow statistics exporting on GE1/0/1 of SwitchA, collect statistics about incoming and outgoing traffic on the interface, and send the statistics to the NetStream server for further analysis. In this way, you can monitor communication between downstream network and the Internet.

The configuration file of SwitchA is as follows. You can configure original flow statistics exporting, aggregation flow statistics exporting, or flexible flow statistics exporting. The following configuration file takes the original flow statistics exporting as an example.

```
#
sysname SwitchA
#
vlan batch 100 200 300 400
#
ip netstream export version 9
ip netstream export source 1.1.2.1
ip netstream export host 1.1.2.2 6000
ip netstream timeout inactive 100
#
ip netstream tcp-flag enable
#
interface Vlanif100
 ip address 1.1.1.1 255.255.255.0
#
interface Vlanif200
```

```
 ip address 1.1.2.1 255.255.255.0
#
interface Vlanif300
 ip address 1.1.3.1 255.255.255.0
#
interface Vlanif400
 ip address 1.1.4.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 ip netstream inbound
 ip netstream outbound
 ip netstream sampler fix-packets 1200 inbound
#
interface GigabitEthernet1/0/2
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface GigabitEthernet1/0/3
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface GigabitEthernet1/0/4
 port hybrid pvid vlan 400
 port hybrid untagged vlan 400
#
return
```

1.5 Troubleshooting

1.5.1 NSC Cannot Export the Flow Statistics

Fault Description

After the NetStream function is configured, the NSC cannot export the statistics packets to the NDA.

Procedure

1. Check whether the NSC can parse statistics packets.
   - If the NSC cannot parse statistics packets, run the **display netstream all** command on the NDE to check whether the version of the exported packets is supported by the NSC. The following assumes that the NSC supports the exported packets of V9.
     - If the version is not V9, run the **ip netstream export version 9** command to set the version to V9. To set the exported packet version of aggregation flows, run the **export version 9** command in the aggregation view.
     - If the version is V9, wait for 30 minutes or run the **ip netstream** { **inbound** | **outbound** } command to enable the NetStream function again.

- If the NSC can parse statistics packets, go to step 2.

NOTE

The interval for exporting the statistics packets of V9 is 30 minutes. The NSC can parse V9 packets only after the device sends the V9 template to the NSC. If you enable the NetStream function again, the device immediately sends the V9 template to the NSC.

2. Verify the NetStream configurations.

Run the **display netstream all** command to check NetStream configurations.

```
<Quidway> display netstream all
system
 ip netstream export version 9
 ip netstream export host 70.1.1.2 6000
 ipv6 netstream export version 9
 ipv6 netstream export host 70.1.1.3 6000
ip netstream aggregation destination-prefix
 ip netstream export host 70.1.1.5 6000
 enable
 export version 9

slot 0
GigabitEthernet1/0/1
 ip netstream inbound
```

Verify the NetStream configurations according to the following tables:

- Table 1-1 describes the configuration items for original flows.
- Table 1-2 describes the configuration items for aggregation flows.
- The method of checking flexible NetStream configuration is the same as the method of checking the NetStream configuration of original flows. In addition, flexible NetStream requires that:
  - The **port ip netstream record** be run in the interface view.
  - IPv4 or IPv6 NetStream be enabled on the interface.
  - The exported packet version be set to V9.

Table 1-1 Configuration items of original flows

Item	Method	Solution
NetStream is enabled on the interface.	Check whether the output contains **ip netstream inbound**, **ip netstream outbound**, **ipv6 netstream inbound**, or **ipv6 netstream outbound**.	Original flows are classified into IPv4 flows and IPv6 flows. To collect statistics on a certain type of flows, the NetStream function must be enabled for the flows. • To enable NetStream for IPv4 original flows, run the **ip netstream** { **inbound** | **outbound** } command in the interface view. • To enable NetStream for IPv6 original flows, run the **ipv6 netstream** { **inbound** | **outbound** } command in the interface view.
The aging time is	Check whether the output contains **ip**	The default aging time is recommended. The

Item	Method	Solution
set properly.	**netstream timeout inactive** *inactive-interval*. • If so, check the value of *inactive-interval*. • If not, the default aging time is in use.	default aging time is 30 seconds. To restore the default aging time, run the **ip netstream timeout inactive** command in the system view.
The destination address and destination port of the exported packets are correctly configured.	Check whether the output contains **ip netstream export host** *ip-address port-number* and **ipv6 netstream export host** *ip-address port-number*.	• To configure NetStream for IPv4 original flows, run the **ip netstream export host** *ip-address port-number* command in the system view. • To configure NetStream for IPv6 original flows, run the **ipv6 netstream export host** *ip-address port-number* command in the system view. **NOTE** *The destination is the NSC address.*

Table 1-2 Configuration items of aggregation flows

Item	Method	Solution
Flexible NetStream is configured.	Check whether the output contains **port ip netstream record** *record-name*.	If flexible NetStream is configured, NetStream for aggregation flows is invalid. Run the **port ip netstream record** command to disable flexible NetStream.
NetStream is enabled for IPv4 flows on the interface.	Check whether the output contains **ip netstream inbound** or **ip netstream outbound**.	Currently, only IPv4 flows can be aggregated. To enable NetStream, run the **ip netstream** { **inbound** | **outbound** } command in the interface view.
The aging time is set properly.	Check whether the output contains **ip netstream timeout inactive** *inactive-interval*. • If so, check the value of *inactive-interval*. • If not, the default aging time is in use.	The default aging time is recommended. The default aging time is 30 seconds. To restore the default aging time, run the **ip netstream timeout inactive** command in the system view.
Aggregation NetStream is enabled.	Check whether the output in the NetStream aggregation view contains **enable**.	To enable aggregation NetStream, run the **enable** command in the NetStream aggregation view.
The destination address and	Check whether the output in the NetStream	The destination NSC address configured in the aggregation view takes precedence

Item	Method	Solution
destination port of the exported packets are correctly configured.	aggregation view contains **ip netstream export host** *ip-address port-number*.	over that configured in the system view. After the destination NSC address is configured: • Original flow statistics are exported only to the destination NSC address configured in the system view. • Aggregation flows are exported to the destination NSC address configured in the corresponding aggregation view. • If no destination NSC address is configured in the aggregation view, aggregation flows are exported to the destination NSC address configured in the system view. To configure the destination IP address and destination port number, run the **ip netstream export host** *ip-address port-number* command in the NetStream aggregation view.

----End

1.6 Terms and Abbreviations

Abbreviations

Acronyms	Full Spelling
NDE	NetStream Data Exporter
NSC	NetStream Collector
NDA	NetStream Data Analyzer