IP Accounting Configuration

Table of Contents

Chapter 1 IP Accounting

IP accounting is used to make statistics of flows. Compared with netflow, IP accounting is simple in functions and also makes statistics of ACL-filtered packets. It is always deployed in small-scale LAN. When attacks such as DOS attack happen, you can use this command to judge which hosts may be triggering these attacks.

Though IP accounting is very useful, it is not so well-known as netflow. Many flow statistics functions of netflow are lack in IP accounting, which is the reason why IP accounting is only used in a few applications. However, IP accounting can obtain the flow statistics results rapidly, which is its advantage.

1.1 IP Accounting Applications

Making statistics of normally forwarded flows based on the source and destination addresses

Making statistics of ACL-filtering flows based on the source and destination addresses

Making statistics of flows based on the MAC address

Making statistics of flows based on the precedence of the IP header

1.2 Advantages of IP Accounting

It can be easily deployed, obtain the current flow statistics information conveniently, and make statistics of ACL-filtering flows.

1.3 Disadvantages of IP Accounting

The statistics information is too simple and the detailed flow information cannot be obtained; what's more, IP accounting is unsuitable to those complicated networks.

IP accounting has no timeout mechanism, so you have to delete the statistics information continuously; if not, the flow statistics entries are fully occupied and the outburst flows cannot be put into statistics.

1.4 Terminologies of IP Accounting

output-packets—the data that are forwarded by equipment

access-violations—the flows that are filtered by ACL

active database—the database to record flows when output-packets or access-violations are put into statistics

Checkpoint database—the database where the deleted output-packets or access-violations are stored and finally released to the memory

Chapter 2 Setting IP Accounting

2.1 Setting Output-Packets Statistics

1. Enabling the statistics function on a corresponding port

The source IP address, destination IP address, packet quantity and byte quantity of all forwarded packets are put into statistics.

Command	Remarks
ip accounting output-packets	Makes statistics of the traffic of output packets on a port.

2. Setting the statistics list and the corresponding transits quantity

To reduce the host quantity in the statistics, you can set a host statistics list. If the source IP address of a host is not in the statistics list, the host will not be put into statistics. The entries of the **Transits** flow mean the entries of the flow that does not comply with the statistics list.

Command	Remarks
ip accounting-list *address netmask*	Opens a host statistics list.
ip accounting-transits *num*	Sets the corresponding **transits** entry quantity.
show ip accounting transits	Displays the information about the flows which are put into **Transits** statistics.
clear ip accounting transits	Deletes the information about flows in Transits.

3. Setting the cache quantity of a statistics flow

Note: **ip accounting access-violation** and **checkpoint database** share the corresponding caches, so this command affects the number of caches for the three commands. If the caches are used up, the following flows have to be dropped and the dropped packets and bytes will be recorded.

Command	Remarks
ip accounting-threshold *num*	Sets the cache quantity of a statistics flow.

4. Active and checkpoint databases

The cache can be classified into the active database and the checkpoint database. All flows are refreshed in the active entry and the checkpoint entry is used to remove the whole active database in a moment to the checkpoint database to observe what traffic each host has in this moment.

Command	Remarks
Show ip accounting output-packets	Displays the statistics information about all output packets.
show ip accounting checkpoint output-packets	Displays the statistics information about the output packets in the checkpoint database.
show ip accounting checkpoint access-violation	Displays the statistics information about the access-violation flows in the checkpoint database.
clear ip accounting	Deletes the contents from the active database to the checkpoint database and at the same time the previous contents in the checkpoint database.
clear ip accounting checkpoint	Deletes the checkpoint database.

2.2 Setting the Access Violation Statistics

1. Enabling the ACL-filtering flows on a corresponding port

   The source and destination IPs, byte quantity, packet quantity and ACL name of all ACL-filtering flows will be put into statistics.

Command	Remarks
ip accounting access-violation	Makes statistics of the ACL-filtering flows.

2. Displaying the active database of access violation

   The access-violation statistics information which is gained after the latest deletion of the active database will be shown.

Command	Remarks
Show ip accounting access-violation	Displays the statistics information about all output packets.

2.3 Setting the Precedence Statistics

1. Enabling flow statistics on a corresponding port based on the IP packet's precedence

   After this command is run, the bytes and packets of 8 precedences are mainly put into statistics, but the IP address and the MAC address will not.

Command	Remarks
ip accounting precedence input	Makes statistics of the precedence of packets received from this port.
ip accounting precedence output	Makes statistics of the precedence of packets that are transmitted from this port.

2. Displaying the precedence statistics information

Command	Remarks
show ip accounting precedence	Displays the precedences on all interfaces.
show ip accounting precedence interface *intf*	Displays the precedences on all interfaces.

3. Deleting the precedence statistics information

Command	Remarks
clear ip accounting precedence	Deletes the precedences on all interfaces.
clear ip accounting precedence interface *intf*	Deletes the precedences on the **intf** interface.

2.4 Setting MAC Statistics

1. Enabling MAC statistics on a port

Each interface has 512 entries to record the received packets and another 512 entries to record the transmitted packets.

As to the input packets, their source MAC addresses, byte quantity and packet quantity are mainly recorded; as to the output packets, their destination MAC addresses, byte quantity and packet quantity are mainly recorded. However, the input packets and the output packets have a timestack, which is used to record the time of receiving recent packets.

Command	Remarks
ip accounting mac-address input	Makes statistics of the packets that are received by a port and records their source MAC addresses.
ip accounting mac-address output	Makes statistics of the packets that are sent from a port and records their destination MAC addresses.

2. Displaying the MAC statistics information

Command	Remarks
show ip accounting mac-address	Displays the MAC addresses that are put into statistics on all interfaces.
show ip accounting mac-address interface *intf*	Displays the MAC addresses that are put into statistics on the **intf** interface.

3. Deleting the MAC statistics information

Command	Remarks
clear ip accounting mac-address	Deletes the MAC addresses that are put into statistics on all interfaces.
clear ip accounting mac-address interface *intf*	Deletes the MAC addresses that are put into statistics on the **intf** interface.

Chapter 3 Configuration Example

1. Setting output packets on interface f0/0

   Router_config_f0/0#ip accounting output-packets

   Router_config#ip accounting-threshold 1024

2. Setting access-violation on interface f0/0

   Router_config_f0/0#ip accounting access-violation

3. Setting precedence statistics on interface f0/0

   Router_config_f0/0#ip accounting precedence input

   Router_config_f0/0#ip accounting precedence output

4. Setting mac-address statistics on interface f0/0

   Router_config_f0/0#ip accounting mac-address input

   Router_config_f0/0#ip accounting mac-address output