

12 Internet Access

[12.1 DHCP Emulation](#)

In a DHCP Emulation test, an access node simulates the DHCP client to implement remote acceptance for services that obtain IP addresses in DHCP mode (such as IPTV, IPoE, and VoIP services) and to locate faults.

[12.2 PPPoE Dialup Emulation](#)

[12.3 Traffic Burst Detection](#)

Traffic burst detection is a feature of identifying traffic burst points by deploying detection points on the network and detecting the traffic at the detection points to obtain traffic information.

12.1 DHCP Emulation

In a DHCP Emulation test, an access node simulates the DHCP client to implement remote acceptance for services that obtain IP addresses in DHCP mode (such as IPTV, IPoE, and VoIP services) and to locate faults.

12.1.1 DHCP Emulation Overview

In a DHCP emulation test, an access node emulates a DHCP client to apply for an IP address from a DHCP server. By doing so, the access node can test the connectivity between the access node and DHCP server and therefore the validity of DHCP configurations on the DHCP relay agent, DHCP agent, and DHCP server. In addition, the access node can ping a remote server to test the connectivity between them.

 NOTE

- During DHCP simulation, certain DHCP simulation packets can be sent in a specified mode. Improper use of some simulation fields (such as source MAC address) may cause service abnormality. Therefore, use this feature only when you understand the impact of the simulation packets.
- The access node can be an OLT, MDU, or ONT.
- The remote server is an upstream network device, for example, an IPTV server or softswitch.
- The difference between a DHCP emulation test and the actual DHCP process is the initiator. In a DHCP emulation test, the access node functions as the initiator; in the actual DHCP process, the user terminal (for example, a PC, STB, or VoIP service terminal) functions as the initiator.

Mainly used for deployment acceptance and fault locating, a DHCP emulation test resolves the known issues in the traditional method. For details, see [Table 12-1](#).

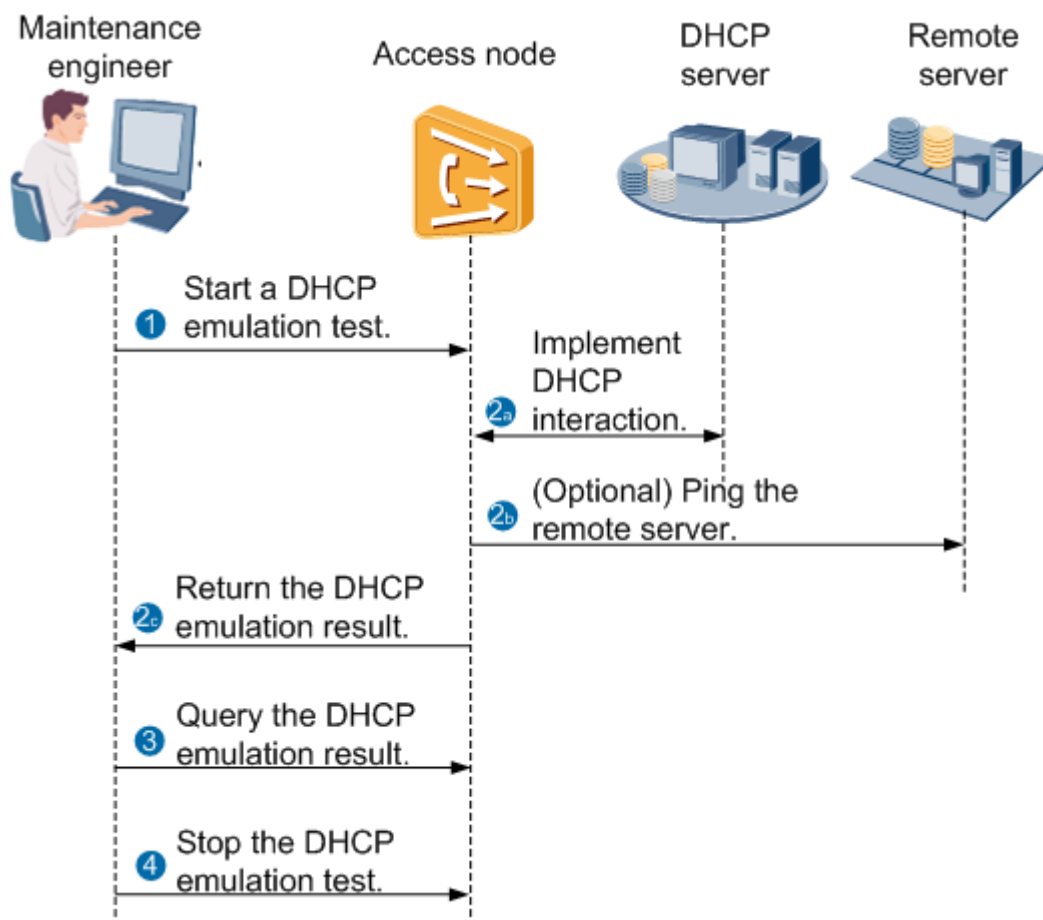
Table 12-1 Comparison between the traditional method and DHCP emulation test

Application Scenario	Traditional Method	DHCP Emulation Test
Deployment acceptance	At the device installation site, a test instrument is connected to the device and the process of users going online in batches is emulated. Alternatively, a laptop is connected to the device to test services on each port. The O&M costs are high.	A remote node implements an acceptance test for services, which does not require site visits and reduces the O&M costs.
Fault locating	When a user reports a fault, the maintenance engineer cannot remotely locate the specific network segment in a timely manner. The maintenance engineer needs to ask for the user's cooperation or go to the user's house to locate the fault, bringing about inconvenience to the user and incurring high O&M costs.	Faults can be remotely located and the specific network segment can be quickly located. Then a work order is assigned to the corresponding maintenance engineer. In this way, the efficiency is improved and the O&M costs are reduced.

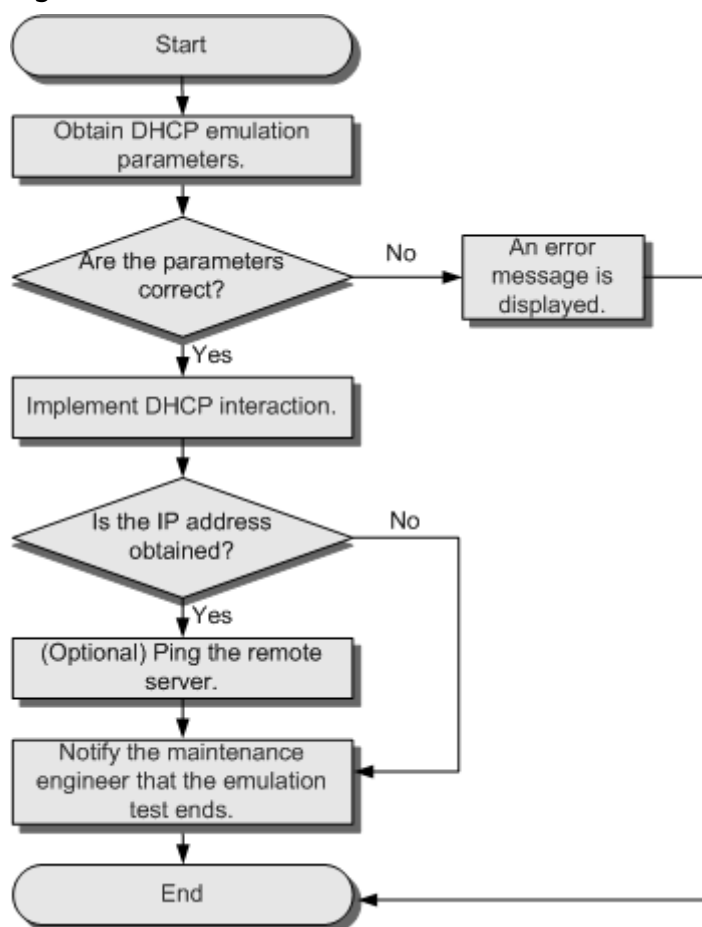
12.1.2 DHCP Emulation Principles

The principles of DHCP emulation.

Figure 12-1 Principles of DHCP emulation



1. The maintenance engineer remotely logs in to the access node and starts a DHCP emulation test.
2. The DHCP emulation process starts. [Figure 12-2](#) shows the DHCP emulation process.
 - a. DHCP interaction is implemented between the access node and DHCP server, which tests the link connectivity between them.
 - b. After obtaining an IP address, the access node pings the remote server if **hostip** (a DHCP emulation parameter indicating the IP address of the remote server) is set. This tests the link connectivity between the access node and remote server.
 - c. The DHCP emulation is completed and the DHCP emulation result is returned.

Figure 12-2 DHCP emulation flow

3. The maintenance engineer queries the DHCP emulation result.
4. The maintenance engineer manually stops the DHCP emulation test to release system resources in a timely manner.

NOTE

A DHCP emulation test automatically stops when the default timeout interval (210s) elapses and the emulation result will be deleted.

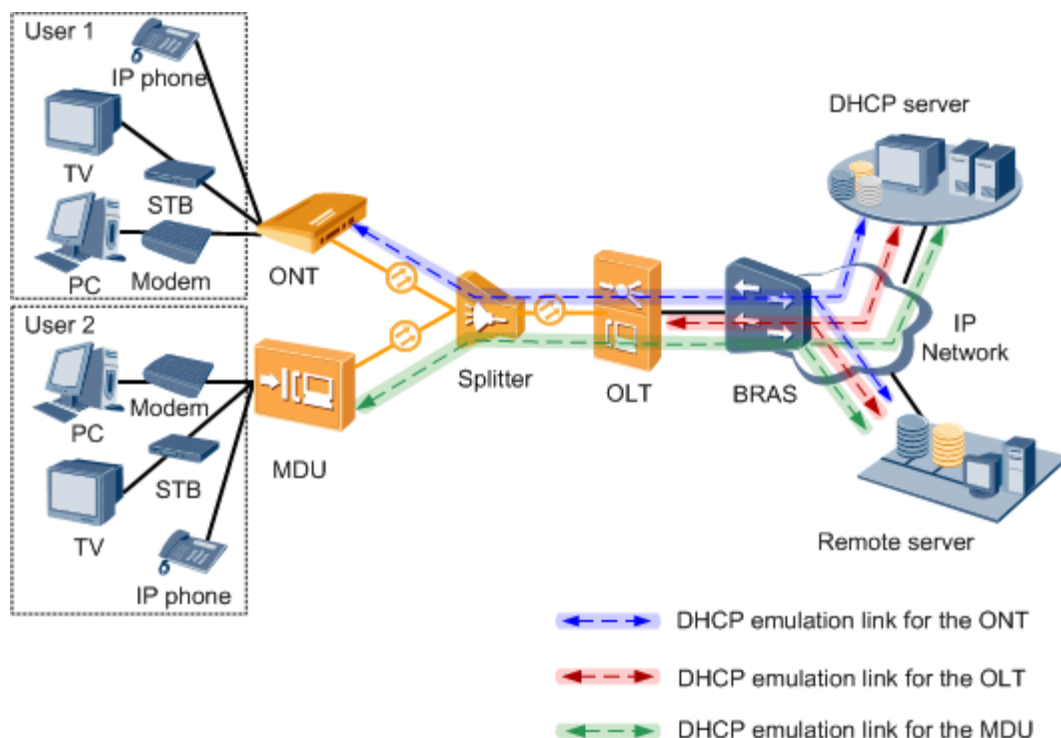
12.1.3 DHCP Emulation Usage Scenario

On an FTTx network, access nodes are close to user terminals and are widely deployed. In a DHCP emulation test, an access node emulates the DHCP client to implement remote acceptance for services that obtain IP addresses in DHCP mode (such as IPTV, IPoE, and VoIP services) and locate faults, which reduces the O&M costs.

FTTx Network Application Scenarios

Figure 12-3 shows typical application scenarios of DHCP emulation on an FTTx network.

Figure 12-3 Typical application scenarios of DHCP emulation on an FTTx network



NOTE

In [Figure 12-3](#):

- Users 1 and 2 receive IP services (such as IPTV, IPoE, and VoIP services) and are authenticated through the BRAS.
- User 1, an FTTH user, receives IP services through the ONT; user 2, an FTTB/FTTC user, receives IP services through the MDU.

When a user receives IPTV, IPoE, or VoIP services and implements deployment acceptance or fault locating through a DHCP emulation test, only the user terminals and remoter servers differ and the operation methods are the same. The following uses receiving IPTV services as an example.

When IPTV services are undergoing deployment acceptance or faulty:

- If the STB cannot obtain an IP address, network connectivity between the STB and DHCP server is abnormal. Perform a DHCP emulation test on the access node device to test the connectivity of each network segment.
- If the STB obtains an IP address successfully, network connectivity between the STB and DHCP server is normal. If users 1 and 2 still cannot watch IPTV programs, ping the remote server (for example, an IPTV server) to test the connectivity between the STB and remote server.

Fault Locating

Locate the fault based on the obtained DHCP emulation result, as shown in [Table 12-2](#).

Table 12-2 Mapping between the emulation result and fault range

emulation Result	Description	Fault Scope
send packet fail	The access node failed to send packets to the DHCP server.	The access node is faulty.
DHCP server not found	After sending DHCP Discover packets, the access node did not receive response packets from the DHCP server.	The network segment between the access node and DHCP server is faulty.
DHCP server refuse request	The DHCP server rejected the DHCP request from the access node.	The DHCP server is faulty.
get IP overtime	After sending a DHCP request, the access node did not receive confirmation packets from the DHCP server.	The network segment between the access node and DHCP server is faulty.
get IP successful	The access node obtained an IP address from the DHCP server, indicating that the DHCP interaction was successful.	The possible fault scopes are as follows: • The network segment between the user terminal and access node is faulty. • The network segment between the BRAS and remote server is faulty.
all ping succeed	The access node succeeded in pinging all the specified remote servers.	The network segment between the user terminal and access node is faulty.
partial ping succeed	The access node succeeded in pinging some of the specified remote servers.	The network segment between the BRAS and remote server that failed to be pinged is faulty.
all ping fail	The access node failed to ping all the specified remote servers.	Network segments between the BRAS and all remote servers are faulty.
system resource not enough	On the access node, resources for DHCP emulation are insufficient.	On the access node, resources for DHCP emulation are insufficient.

emulation Result	Description	Fault Scope
unknown	-	-

12.1.4 Configuring DHCP Emulation

Context

Maintenance engineers can log in to the access node and perform DHCP emulation configurations through the CLI or NMS. The following uses operations through the CLI as an example.

- For FTTB or FTTC scenario, a DHCP emulation test can be directly performed on the OLT or MDU.
- For FTTH scenario, a DHCP emulation test can be started on the ONT through the OLT.

Procedure

Step 1 Run the **simulate dhcp start** command to start a DHCP emulation test.

Step 2 Run the **display simulation dhcp** command to query the specified DHCP emulation result.

NOTE

When the default timeout interval (210s) for the DHCP emulation test elapses or the DHCP emulation test is manually stopped, the DHCP emulation result will be deleted. Therefore, after the DHCP emulation test is completed, query the DHCP emulation result in a timely manner.

Locate the fault based on the obtained DHCP emulation result, as shown in [Table 12-2](#).

Step 3 Run the **simulate dhcp stop** command to stop the DHCP emulation test.

----End

Example

In the FTTB or FTTC scenario: Log in to the OLT or MDU and start a DHCP emulation test on it.

- ID of the service port: 0
 - MAC address of the simulated server: 00e0-fc00-0001
 - Option 60: HW
 - Option 61 type corresponding to the option 61 field: 1; client ID: 00e0-fc00-0002
 - IP address of the to-be-pinged remote server: 192.168.3.99
1. Start a DHCP emulation test.

```
huawei(config)#simulate dhcp start service-port
{ service-portid<U><0,131071> }:0
{ mac-address<P><H-H-H> }:00e0-fc00-0001
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option60<K>|option61<K>|user-vlan<K> }:option60
{ option60<S><Length 1-64> }:HW
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option61<K> }:option61
{ mac-addr<K>|string<K> }:mac-addr
{ mac_clientid<P><XXXX-XXXX-XXXX> }:00e0-fc00-0002
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:host-ip1
{ ipaddr1<I><X.X.X.X> }:192.168.3.99
{ <cr>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|overtime<K> }:
```

Command:

```
simulate dhcp start service-port 0 00e0-fc00-0001 option60 HW
option61 mac-addr 00e0-fc00-0002 host-ip1 192.168.3.99
```

Please check whether the input flow ID and MAC address are correct. Incorrect parameters may affect the services of normal users.

You are suggested to use the MAC address of the actual user.

Are you sure to continue?(y/n)[n]:y

2. Query the DHCP emulation result.

```
huawei(config)#display simulation dhcp
{ <cr>|service-port<K>|<K>|><K>|>><K> }:service-port
{ service-portid<U><0,131071> }:0
{ mac-address<P><XXXX-XXXX-XXXX> }:00e0-fc00-0001
```

Command:

```
display simulation dhcp service-port 0 00e0-fc00-0001
Total : 1
```

```
----- common info -----
FlowID          : 0
User MAC        : 00e0-fc00-0001
User VLAN       : 10
Optin60         : HW
Option61 type   : 1
Option61 client : 00e0-fc00-0002
Simulate status : finished
Simulate result : all ping succeed
Simulate start time : 2019-01-17 16:51:59+08:00
User IP         : 192.168.3.100/24
DHCP server IP  : 192.168.3.8
Primary DNS server IP : -
Secondary DNS server IP : -
Relay gateway   : 0.0.0.0
Default gateway : 192.168.3.201
----- route info -----
Route:1 Destination IP : 192.168.5.0/24 Next hop IP : 192.168.3.66
      Next hop MAC : - Local interface : -
Route:2 Destination IP : 192.168.4.0/24 Next hop IP : 192.168.3.88
      Next hop MAC : 00e0-fc00-dbba Local interface : Y
Route:3 Destination IP : - Next hop IP : -
      Next hop MAC : - Local interface : -
----- ping info -----
Host:1 IP : 192.168.3.99 Total count : 3 Succeed count : 3
Host:2 IP : - Total count : 0 Succeed count : 0
Host:3 IP : - Total count : 0 Succeed count : 0
Host:4 IP : - Total count : 0 Succeed count : 0
Host:5 IP : - Total count : 0 Succeed count : 0
-----
```

3. Stop the DHCP emulation test.

```
huawei(config)#simulate dhcp stop service-port 0 00e0-fc00-0001
```

In the FTTH scenario, log in to the OLT and start a DHCP emulation test on the ONT.

 NOTE

During the DHCP emulation, the IP address obtained can be used for multicast emulation.

- ID of the subrack/slot/port of the OLT connected to the ONT: 0/2/0
 - ID of the ONT enabled with DHCP emulation: 1
 - VLAN ID in the VLAN tag in packets: 10
 - Option 61 type corresponding to the option 61 field: 0; client ID: user
 - IP address of the to-be-pinged remote server: 192.168.3.99
 - IP address of the multicast program: 224.1.1.1
1. Issue commands on the OLT to start a DHCP emulation test on the ONT.

```
huawei(config)#simulate dhcp start ont
{ frameid/slotid/portid<S><Length 5-18> }:/2/0
{ ontid<U><0,255> }:/1
{ eth<K>|outer-vlan<K>|untag<K>|vlan<K> }:/vlan
{ vlanid<U><1,4095> }:/10
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option60<K>|option61<K>|priority1<U><0,7>|usermac<K> }:/option61
{ mac-addr<K>|string<K> }:/string
{ string_clientid<S><Length 1-64> }:/user
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:/host-ip1
{ ipaddr1<I><X.X.X.X> }:/192.168.3.99
{ <cr>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|groupid<K> }:/groupid
{ip-addr<I><X.X.X.X>|<cr> }:/224.1.1.1
{igmp-version<K> }:/igmp-version
{v2<K>|v3<K>}:/v2
```

```
Command:
    simulate dhcp start ont 0/2/0 1 vlan 10 option61 string user host-ip1
192.168.3.99 groupid 224.1.1.1 iqmp-version v2
```

2. Query the ONT DHCP emulation result.

```
huawei#display simulation dhcp
{ <cr>|ont<K>|service-port<K>||<K>|><K>|>><K> } :ont
{ <cr>|frameid/slotid/portid<S><Length 5-18> } :0/2/0
{ ontid<U><0,255> } 1
```

Command:
display simulation dhcp ont 0/2/0 1

```

----- common info -----
simulation instance      : F/S/P: 0/2/0  ONTId:1  ONTPort WAN
simulation VLAN tag num : 1
simulation outer VLANID : 10
simulation inner VLANID : -
Option60                : -
Option61 type           : 0
Option61 client         : user
Simulate status         : finished
Simulate result         : succeed
Simulate start time     : 2013-01-17 15:49:20+09:00
User IP                 : 192.168.3.100/24
DHCP server IP         : 192.168.3.99
Primary DNS server IP   : 10.72.55.81
Secondary DNS server IP : 10.72.255.100
Relay gateway          : 192.168.3.99
Default gateway         : 192.168.3.99
----- route info -----
Route:1  Destination IP : 192.168.5.0/24  Next hop IP : 192.168.3.66
        Next hop MAC   : -                Local interface : -
Route:2  Destination IP : 192.168.4.0/24  Next hop IP : 192.168.3.88
        Next hop MAC   : 00e0-fc00-dbba   Local interface : Y
Route:3  Destination IP : -                Next hop IP : -
        Next hop MAC   : -                Local interface : -
----- ping info -----

```

```
Host:1 IP : 192.168.3.99      Total count : 3   Succeed count : 3
Host:2 IP : -                Total count : 0   Succeed count : 0
Host:3 IP : -                Total count : 0   Succeed count : 0
Host:4 IP : -                Total count : 0   Succeed count : 0
Host:5 IP : -                Total count : 0   Succeed count : 0
-----
Multicast group IP   : 224.1.1.1
Multicast source IP  : -
Multicast version    : IGMPv2
Data rate(kbps)      : 1500
-----
```

3. Stop the ONT DHCP emulation test.
huawei(config)#simulate dhcp stop ont 0/2/0 1

12.1.5 DHCP Emulation Reference Standards and Protocols

- IETF RFC 2131: Dynamic Host Configuration Protocol
- IETF RFC 1533: DHCP Options and BOOTP Vendor Extensions

12.2 PPPoE Dialup Emulation

12.2.1 PPPoE Dialup Emulation Introduction

In PPPoE dialup emulation, an access device emulates an end user and initiates PPPoE dialup. According to the PPPoE dialup emulation result (successful or failed), users can determine the network connectivity between the access device and the broadband remote access server (BRAS). If a fault has occurred in the network, PPPoE dialup emulation helps users quickly identify whether the fault is on the network side or user side.

NOTE

During PPPoE simulation, certain PPPoE simulation packets can be sent in a specified mode. Improper use of some simulation fields (such as source MAC address) may cause service abnormality. Therefore, use this feature only when you understand the impact of the simulation packets.

PPPoE dialup emulation is used for remote fault location and acceptance tests. [Table 12-3](#) lists the comparison between the method of performing a PPPoE dialup emulation test and the method of performing a traditional PPPoE dialup test.

Table 12-3 Comparison between the method of performing a PPPoE dialup emulation test and the method of performing a traditional PPPoE dialup test

Scenario	Task	Method of Performing a Traditional PPPoE Dialup Test	Method of Performing a PPPoE Dialup Emulation Test
Acceptance test	After an access device is installed, a test engineer needs to check whether the PPPoE dialup service on the access device has been provisioned properly.	The test engineer visits the site where the access device is installed and uses an external tester or a portable computer to perform a PPPoE dialup test for each port.	The test engineer remotely logs in to the access device to perform a PPPoE dialup emulation test and determines the service status based on the test result. NOTE A PPPoE dialup emulation test cannot check the status of the line between an end user and an access device.
Fault location	A maintenance engineer needs to locate a fault on an access network that covers a large area and contains geographically dispersed network devices.	The maintenance engineer visits all sites where the access devices are installed and performs a PPPoE dialup test.	The maintenance engineer preliminarily determines the network segment where the fault occurs and remotely logs in to the access devices to perform a PPPoE dialup emulation test. Based on the test result, the maintenance engineer determines the fault cause and rectifies the fault.

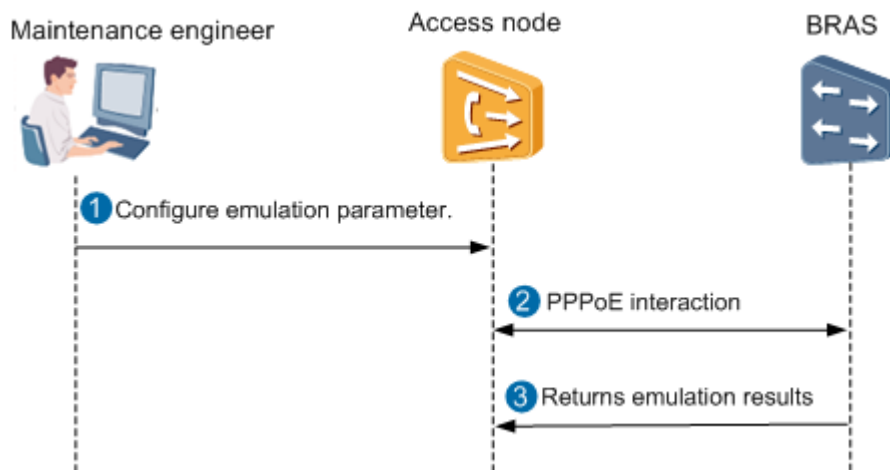
12.2.2 PPPoE Dialup Emulation Principles

PPPoE dialup emulation differs from PPPoE dialup in the following aspects:

- The PPPoE dialup emulation process is initiated by an access device, while the PPPoE dialup is initiated by a PC, modem, or home gateway.
- The MAC address carried in the packet in PPPoE dialup emulation is the bridge MAC of an access device, while the MAC address carried in the packet in the PPPoE dialup is that of a PC, modem, or home gateway.

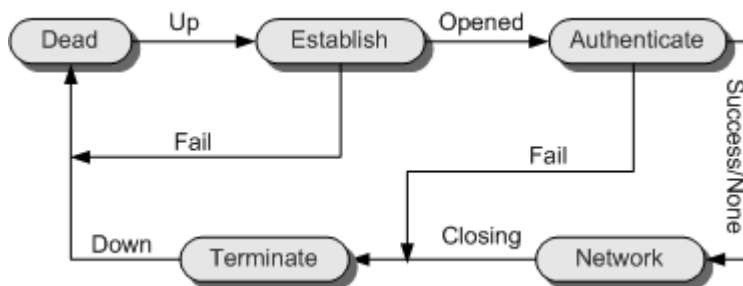
The principles of PPPoE dialup emulation.

Figure 12-4 Principles of PPPoE dialup emulation



1. A maintenance engineer can start a PPPoE dialup emulation on an access node, the access node emulates an end user and initiates PPPoE dialup.
Enter parameters required for the PPPoE dialup emulation, including service flow ID (identifying the user), MAC address, user name, password, authentication mode, and timeout time.
2. Access node interacts with the BRAS.
The emulated PPPoE dialup includes two phases:
 - a. PPPoE discovery phase.
The source host discovers the MAC address of the destination host (in this case, the BRAS), and a point-to-point PPP session is set up.
 - b. PPPoE session phase.
A point-to-point connection has been set up and carries PPP packets for link negotiation, as shown in [Figure 12-5](#).

Figure 12-5 PPPoE session flow



3. The maintenance engineer can stop a PPPoE dialup emulation on an access node.

12.2.3 PPPoE Dialup Emulation Usage Scenario

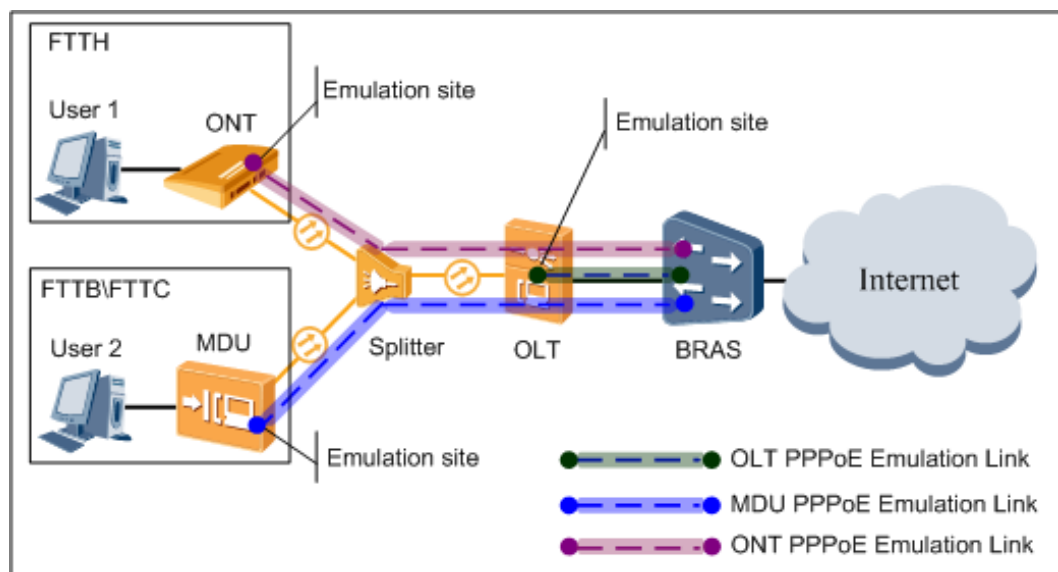
Context

On networks, access devices are closer to terminals and widely distributed. If a PPPoE dialup fault occurs, PPPoE dialup tests performed onsite increase fault location costs. To resolve this issue, PPPoE dialup emulation tests can be performed remotely.

Scenario

Figure 12-6 shows the typical networking.

Figure 12-6 Typical networking



In the preceding figure, users use the PPPoE dialup service and they are authenticated in PPPoE mode through the broadband remote access server (BRAS).

- For ONT user, perform the PPPoE dialup emulation on the ONT.
- For MDU user, perform the PPPoE dialup emulation on the MDU.
- For OLT user, perform the PPPoE dialup emulation on the OLT.

Fault Location

The troubleshooting roadmap based on the test result is as follows:

Table 12-4 PPPoE dialup emulation results

Emulation Result	Corresponding Windows Error Code	Description	Handling Guide
Success	-	• The link between the access node and the BRAS is functional. • The service configuration of the PPPoE user is correct. • Parameters such as the user name, password, and authentication mode of the PPPoE user are correct.	-
Parameter negotiation fail	732 Your computer and the remote computer could not agree on PPP control protocols.	PPPoE dialup emulation has entered the link setup phase of the PPP session, but parameter negotiation fails, causing the link failure.	Check whether the Policy Information Transfer Protocol (PITP) configuration is correct.
Link unnormal	638 The remote server is not responding in a timely fashion.	PPPoE dialup emulation has entered the link setup phase of the PPP session, but the creation of the LCP link is abnormal.	Check whether an access control list (ACL) that does not allow transmission of PPPoE packets is configured on the access node.

Emulation Result	Corresponding Windows Error Code	Description	Handling Guide
Authentication fail	691 The connection was denied because the username or password you specified is not valid or because the selected authentication protocol is not permitted on the remote server.	PPPoE dialup emulation has entered the user authentication phase of the PPP session, but username or password mismatch occurs between the client and server.	• The user's account is configured on the access node is not correct. • The user's account is configured on the BRAS is not correct.
Time out	721 The remote computer is not responding.	PPPoE dialup emulation exceeds the preset emulation timeout time.	• The present emulation time out time is too short. • The link between access node and BRAS is abnormal, transmission delay is too large.
Peer down request	668 The connection was terminated.	The server forcibly terminates the PPPoE dialup emulation.	The user's account is restricted on the BRAS.
Other error	635 There was an unknown error.	Unknown errors.	-

12.2.4 Configuring PPPoE Dialup Emulation

Context

If a PPPoE dialup fault occurs, a PPPoE dialup emulation test can be performed on the ONT or MDU to check the connection between the ONT or MDU and the BRAS and locate the fault according to the test result.

Procedure

- Step 1** Run the **simulate pppoe start** command to perform a PPPoE dialup emulation.
- Step 2** Run the **display simulation pppoe** command to query the status of the PPPoE dialup emulation.

 NOTE

Query the status of the PPPoE dialup emulation only after the test is started. The status cannot be queried if the emulation is stopped.

Step 3 Run the **simulate pppoe stop** command to stop PPPoE dialup emulation.

 NOTE

Another PPPoE dialup emulation can be performed only after the current PPPoE dialup emulation is stopped.

----End

Example

In FTTB or FTTC scenario, remotely log in to the access node device and perform PPPoE dialup emulation on it.

- Service port ID: 0
- MAC address of the emulation user: 00e0-fc00-1111

1. Start PPPoE dialup emulation.

```
huawei(config)#simulate pppoe start
Service-port(index<0-1999>):0
Mac-address(P)<XXXX-XXXX-XXXX>[default 5623-5987-dead]:00e0-fc00-1111
User Name(length<1,65>):user-0
User Password(length<0,16>):*****
Authentication Mode:
1. Chap 2. Pap [default 1]:1
Overtime Time(5-60s)[default 5]:10
```

2. Query the status of PPPoE dialup emulation.

```
huawei(config)#display simulation pppoe
PPPoE simulate information is:
```

```
-----
Service-port: 0
Mac-address: 00e0-fc00-1111
User name: user-0
Current phase: -
Result: Success
Start time: 2019-03-06 08:20:23+08:00
End time: 2019-03-06 08:23:36+08:00
Session ID: 591
User IP: 192.168.1.172
Gateway IP: 192.168.1.1
-----
```

3. Stop PPPoE dialup emulation.

```
huawei(config)#simulate pppoe stop
```

In FTTH scenario, remotely log in to the OLT and perform PPPoE dialup emulation on the ONT.

 NOTE

During the PPPoE dialup emulation, the IP address obtained can be used for multicast emulation.

- Port to which the ONT connects: 0/2/0
- ONT ID: 0
- Ethernet port: 1
- VLAN ID: 100

- IP address of the multicast program: 225.0.0.1
- IP address of the multicast source: 10.2.3.4

1. Start PPPoE dialup emulation.

```
huawei(config-if-gpon-0/2)#pppoe simulate start
{ portid<U><0,3>}:0
{ ontid<U><0,63>}:0
{ eth<K>|untagged<K>|vdsl<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,24>}:1
{ untagged<K>|vlanid<K> }:100
{ priority<U><0,7>|user-name<K> }:2
{user-name<K> }:user-name
{user-name<S><Length 1-64> }:pppoe
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:password
{ authentication-mode<K> }:authentication-mode
{ protocol<U><chap,pap> }:chap
{ <cr>|group-ip-address<K> }:group-ip-address
{ group-ip-address<I><X.X.X> }:225.0.0.1
{ <cr>|igmp-version<K> }:igmp-version
{v2<K>|v3<K>}:v3
{ <cr>|source-ip-address<K> }:source-ip-address
{ source-ip-address<I><X.X.X> }:10.2.3.4
```

Command:

```
pppoe simulate start 0 0 eth 1 100 2 user-name pppoe user-password password authentication-
mode chap groupip 225.0.0.1 igmp-version v2 source-ip-address 10.2.3.4
```

ONT PPPoE Test Result

```
F/S/P      : 0/2
ONT-ID     : 0
ONT ETH Port ID : 1
ONT Vlan ID : 100
Vlan Priority : 2
Multicast group IP : 225.0.0.1
Multicast source IP : 10.2.3.4
Multicast version : v2
Multicast traffic(kbps) : 1500
Emulator result : Multicast test fail
Session ID : 0
User IP : 192.168.1.1
Gateway IP : 255.255.255.0
```

2. Query ONT PPPoE dialup emulation results of port 0/2.

```
huawei(config-if-gpon-0/2)#display pppoe simulate 0
{<cr>|ontid<U><0,127>}
```

Command:

```
display pppoe simulate 0
```

```
F/S/P      : 0/2
ONT-ID     : 0
ONT ETH Port ID : 1
ONT Vlan ID : 100
Vlan Priority : 2
Multicast group IP : 225.0.0.1
Multicast source IP : 10.2.3.4
Multicast version : v2
Multicast Data rate(kbps): 1500
Emulator result : Multicast test fail
Session ID : 0
User IP : 192.168.1.1
Gateway IP : 255.255.255.0
```

3. Run the **simulate pppoe stop** command to stop PPPoE dialup emulation.

```
huawei(config)#simulate pppoe stop
```

12.2.5 PPPoE Dialup Emulation Reference Standards and Protocols

IETF RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE)

IETF RFC 1661: The Point-to-Point Protocol (PPP)

12.3 Traffic Burst Detection

Traffic burst detection is a feature of identifying traffic burst points by deploying detection points on the network and detecting the traffic at the detection points to obtain traffic information.

12.3.1 Traffic Burst Detection Overview

In the high bandwidth era, traffic burst occurs irregularly in peak hours of network services, causing congestion or committed access rate (CAR)-triggered packet loss and affecting the performance of the end-to-end (E2E) network. Therefore, it is important to identify traffic burst points on the network.

Conventional detection methods are complex and time-consuming and do not apply to Gigabit Ethernet (GE)-level traffic burst.

Traffic burst detection enables you to easily monitor gigabit-level traffic burst on the E2E network and identify traffic burst points.

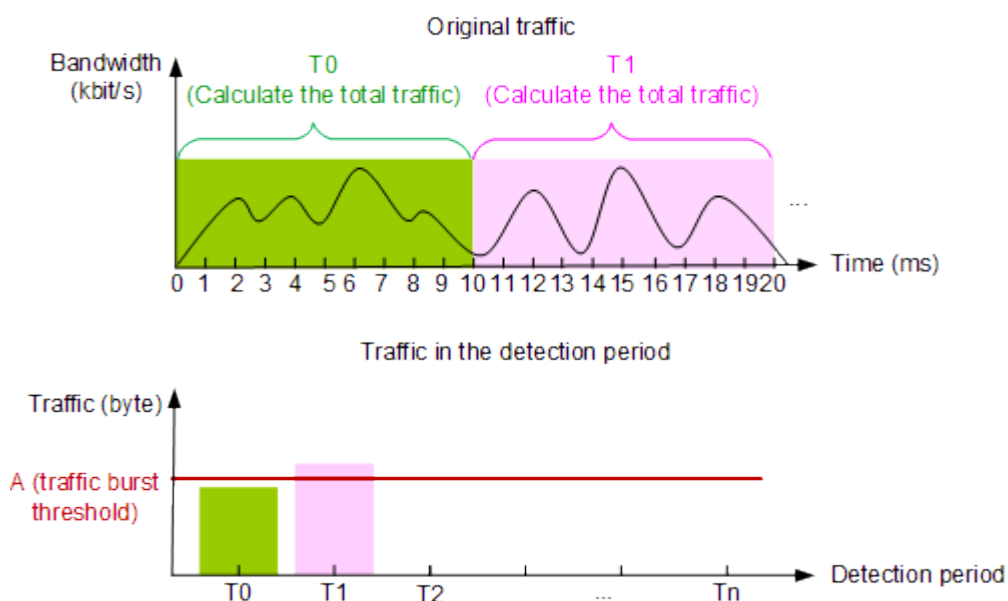
12.3.2 Traffic Burst Detection Principle

Traffic burst detection enables you to monitor traffic status in the detection period and determine whether traffic burst occurs in the detection period. Traffic burst detection can be performed based on either of the following factors:

- Periodic traffic
- Rate limitation threshold

Traffic Burst Detection Based on Periodic Traffic

Figure 1 shows the operating principle of traffic burst detection based on periodic traffic.

Figure 12-7 Operating principle of traffic burst detection based on periodic traffic

In this scenario, the traffic in each detection period (for example, $T = 10$ ms) is calculated, and the system determines whether the traffic in each detection period exceeds the threshold.

- If the traffic in the detection period (for example, T0) does not exceed the threshold, the system checks the traffic in the next detection period (for example, T1).
- If the traffic in the detection period (for example, T1) exceeds the threshold, the system generates a traffic burst record and checks the traffic in the next detection period (for example, T2).

Traffic Burst Detection Based on the Rate Limitation Threshold

Figure 2 shows the operating principle of traffic burst detection based on the rate limitation threshold.

Figure 12-8 Operating principle of traffic burst detection based on the rate limitation threshold

In this scenario, a virtual rate limitation threshold (not actually taking effect) is set for the to-be-detected traffic. The system determines whether traffic burst occurs

in each detection period (for example, $T = 1s$) based on whether virtual packet loss is identified.

- If no packet loss is identified, no traffic burst occurs, and the system checks the traffic in the next detection period.
- If packet loss is identified, traffic burst occurs, and the system generates a traffic burst record and checks the traffic in the next detection period.

 NOTE

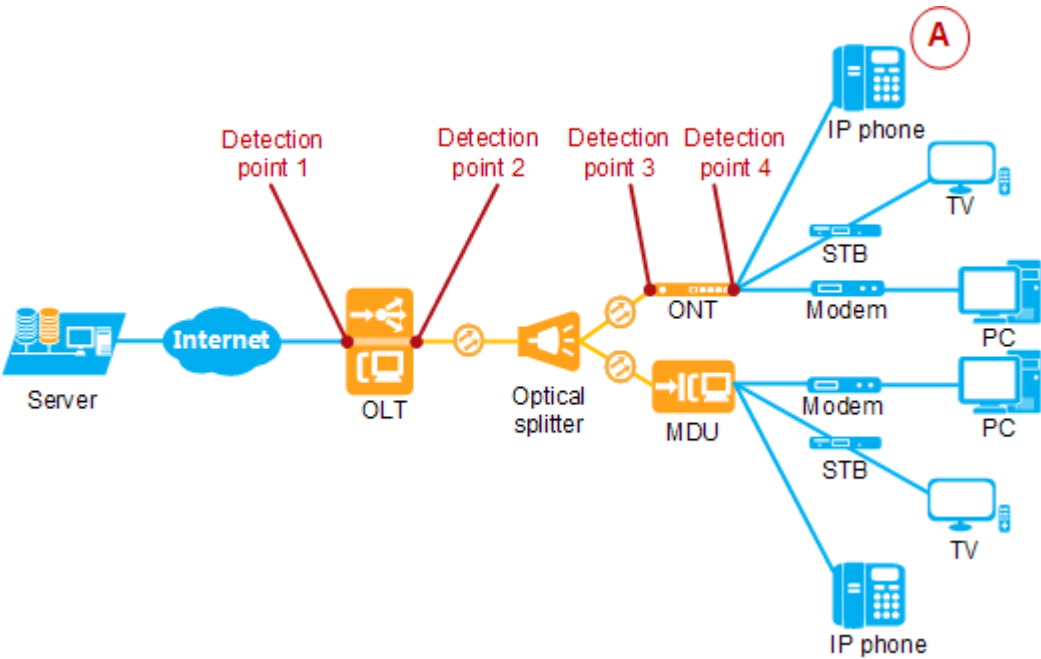
In traffic burst detection based on the rate limitation threshold, the system determines only whether traffic burst occurs, but cannot identify the specific traffic burst value.

12.3.3 Traffic Burst Detection Application Scenario

Scenario Description

Figure 1 shows the application scenario of traffic burst detection on the network.

Figure 12-9 Application scenario of traffic burst detection



Traffic burst detection is performed on different ports of the devices, to identify the traffic burst points on the network. Table 1 describes the detection points and detection directions supported on the devices.

Table 12-5 Detection points and detection directions on different devices

Device	Detection Point	Detection Direction
OLT	Upstream port(Detection point 1)	Upstream and downstream

Device	Detection Point	Detection Direction
	User port(Detection point 2)	Upstream and downstream
ONT	WAN port (Detection point 3)	Upstream and downstream
	User port(Detection point 4)	Upstream and downstream

 NOTE

Traffic burst detection is not limited to specific structures of the upstream network of the optical line terminal (OLT) or the user network.

Detection Point Deployment

Scenario description: In the upstream direction, traffic burst occurs on an intermediate device, causing congestion- or committed access rate (CAR)-triggered packet loss on the device at point A.

Detection point deployment: Deploy detection points at the detection point 1 and detection point 2 and at the detection point 4, to identify the device where traffic burst occurs. Functions of the detection points are as follows:

- The detection point 1 is used to identify whether traffic burst occurs on the upstream network or occurs on the OLT and its downstream network.
- The detection point 2 is used to identify whether traffic burst occurs on the OLT and its upstream network or occurs on the ONT and its downstream network.
- The detection point 4 is used to identify whether traffic burst occurs on the ONT and its upstream network or occurs on the user network.

 NOTE

Traffic burst detection points in the egress direction of the ports do not cover queue scheduling. Traffic burst caused by queue scheduling in the egress direction can be identified only on the downstream device, instead of on this device.

12.3.4 Configure Traffic Burst Detection

Procedure

- Step 1** Run the **traffic-burst-detect instance** command to configure traffic burst detection instances.

 NOTE

You can configure instances for the optical network terminal (ONT) after logging in to the optical line terminal (OLT).

- Step 2** Run the **traffic-burst-detect start** command to modify the start/end time of traffic burst detection instances.

- Step 3** During traffic burst detection, run the **traffic-burst-detect stop** command to stop the detection as required.
- Step 4** Query traffic burst detection instances.
- Run the **display traffic-burst-detect instance all** command to query all configured traffic burst detection instances in batches.
 - Run the **display traffic-burst-detect instance instance-id** command to query a single traffic burst detection instance.
- Step 5** Run the **display traffic-burst-detect result** command to query traffic burst detection records.
- Step 6** Run the **undo traffic-burst-detect** command to delete traffic burst detection instances.

 NOTE

In a service stream, delete the original traffic burst detection instance when you attempt to configure a new instance in the same direction at a port.

----End

Example

Provided that the service stream ID is 11 and a traffic burst detection instance needs to be configured at the downstream input port 0/9/0, detailed parameter settings are as follows:

- Access control list (ACL) rule ID of the service stream: 2000
- ACL filtering rule ID of the service stream: 5
- Traffic burst detection period (ms): 10
- Traffic burst detection threshold (kbit/s): 1000

1. Configure the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect instance 11
{ inbound<K>|outbound<K> } :inbound
{ ip-group<K>|ipv6<K>|link-group<K>|period<K>|user-group<K> } :ip-group
{ access-list-number2<U><2000,3999> } :2000
{ rule<K> } :rule
{ rule-id<U><0,4294967294> } :5
{ link-group<K>|period<K> } :period
{ period<U><1,100> } :1
{ threshold<K> } :threshold
{ threshold<U><64,10240000> } :1000
{ link-aggregation<K>|ont<K>|port<K>|protect-group<K> } :port
{ frameid/slotid/portid<S><Length 5-18> } :0/9/0
{ <cr>|detect-time<K>|from<K>|to<K> } :
```

Command:

```
traffic-burst-detect instance 11 inbound ip-group 2000 rule 5 period 10 threshold 1000
port 0/9/0
```

2. Modify the start/end time of the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect start instance 11
{ <cr>|detect-time<K>|from<K>|to<K> } :from
{ time1<T><hh:mm:ss> } :10:03:10
{ data1<D><yyyy-mm-dd> } :2019-09-15
{ <cr>|detect-time<K>|to<K> } :to
{ time2<T><hh:mm:ss> } :10:04:10
{ data2<D><yyyy-mm-dd> } :2019-09-15
```

Command:

```
traffic-burst-detect start instance 11 from 10:03:10 2019-09-15 to 10:04:10 2019-09-15
```

3. Stop the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect stop instance 11
```

4. Query traffic burst detection instances.

– Query all traffic burst detection instances.

```
huawei(config)#display traffic-burst-detect instance all
```

ID	Direction	F/S/P	ONT	ONT_PORT (ms)	Period (Kbps)	Threshold	state
11	inbound	0/9/0	-	-	10	1000	running

Note: The detection instance based on service-port.
The F/S/P contains the service flow ID.

– Query a single traffic burst detection instance.

```
huawei(config)#display traffic-burst-detect instance 11
```

```
Instance ID      : 11
Direction        : inbound
Position         : port 0/9/0
Period           : 10 ms
Threshold        : 1000 Kbit/s
State            : stopped
Start time       : 2019-09-15 10:03:10+08:00
End time         : 2019-09-15 10:04:10+08:00
ACL match information:
Matches: ACL 2000 rule 5
```

5. Query the traffic burst detection record.

```
huawei(config)#display traffic-burst-detect result instance 11
```

It will take some time, please wait...

```
Instance ID      : 11
Direction        : inbound
Position         : port 0/9/0
Period           : 10 ms
Threshold        : 1000 Kbit/s
State            : stopped
Start time       : 2019-09-15 10:03:10+08:00
End time         : 2019-09-15 10:04:10+08:00
ACL match information:
Matches: ACL 2000 rule 5
```

Total traffic burst records: 2

Time	Traffic BandWidth(Kbit/s)
2019-09-15 10:03:41.0 +08:00	-
2019-09-15 10:03:40.0 +08:00	-

6. Delete the traffic burst detection instance.

```
huawei(config)#undo traffic-burst-detect instance 11
```