Hewlett Packard Enterprise

HPE IMC NTA
Probe Traffic Analysis Configuration Examples

Part number: 5200-4111
Software version: IMC NTA 7.3 (E0503)

Contents

Introduction

This document provides examples for configuring NTA to work with probes to monitor the traffic of devices that do not support NetStream or sFlow.

On a device that does not support NetStream or sFlow, configure port mirroring on the device to mirror the traffic to be analyzed to the probe server. The probe server collects statistics of the received mirrored traffic and generates probe traffic logs. Then, the probe server uploads the probe traffic logs to the NTA server by using FTP. NTA analyzes the network traffic based on the received probe traffic logs.

Prerequisites

Before you configure NTA and a probe to monitor the network traffic, make sure the following requirements are met:

- The probe application program has been correctly installed on a dedicated server.

  For more information, see *HPE Intelligent Management Center Probe Installation Guide*.
- An FTP server has been set up on the same host as the NTA server and the FTP server is running correctly.

  This example uses TYPSoft to set up the FTP server. If you use other software to set up the FTP server, see related documentation.

Example: Configuring NTA and a probe to monitor the network traffic

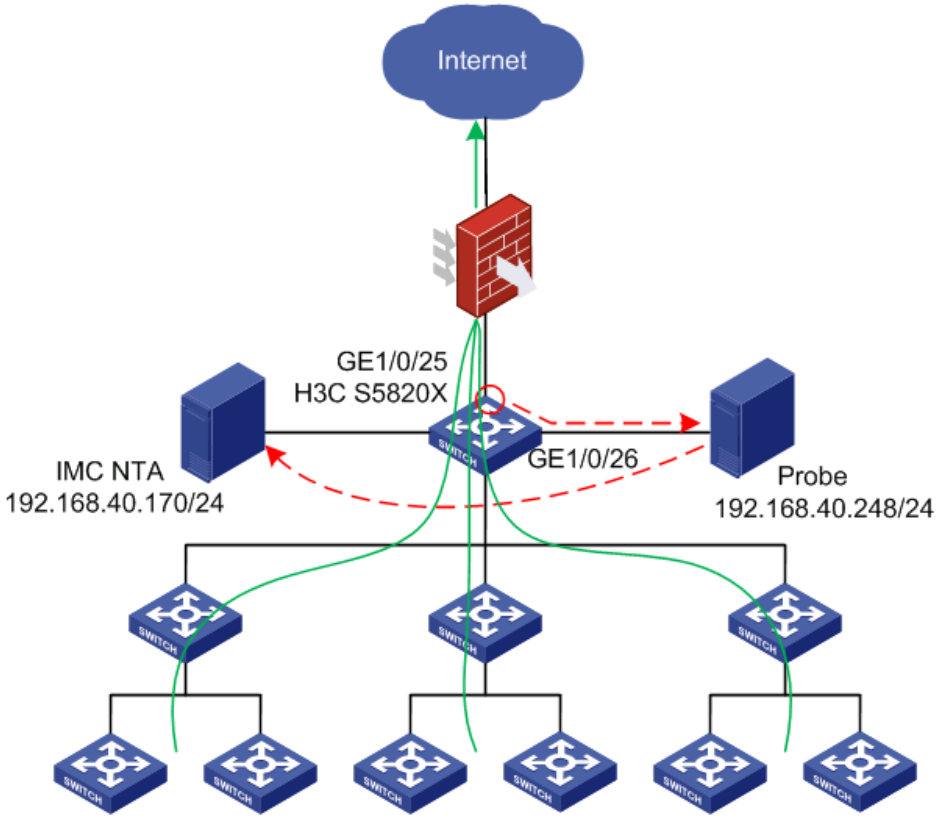
Network configuration

As shown in Figure 1, GigabitEthernet 1/0/25 and GigabitEthernet 1/0/26 on the H3C S5820X-28S switch are connected to the Internet and the probe server, respectively.

Configure GigabitEthernet 1/0/25 as the source port and GigabitEthernet 1/0/26 as the monitor port of a local mirroring group. Then, the following events occur:

- GigabitEthernet 1/0/25 can mirror all received and sent packets to GigabitEthernet 1/0/26.
- The probe server sends probe traffic logs to the IMC NTA server at 192.168.40.170/24 for traffic analysis.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on H3C S5820X-28S, Comware Software, Version 5.20, Release 1808P12.

Restrictions and guidelines

When you configure a probe to monitor the network traffic, follow these restrictions and guidelines:

- Make sure the password you configure when you install the probe is the same as the probe configurations on the NTA server.
- Make sure the username and the password settings you configure for the FTP server match the server configuration on the NTA server.
- Make sure **Enable Layer 7 Application Identification** is enabled, so that NTA can identify applications that use dynamically assigned port numbers such as BT, DC, eDonkey Gnutella, Kazaa, MSN, QQ, AIM.

Configuring port mirroring on the H3C S5820X-28S switch

Create local mirroring group 1.

```
<Switch> system-view
```

```
[Switch] mirroring-group 1 local
```

Configure local mirroring group 1 to monitor the bidirectional traffic of GigabitEthernet 1/0/25.

```
[Switch] mirroring-group 1 mirroring-port gigabitethernet 1/0/25 both
```

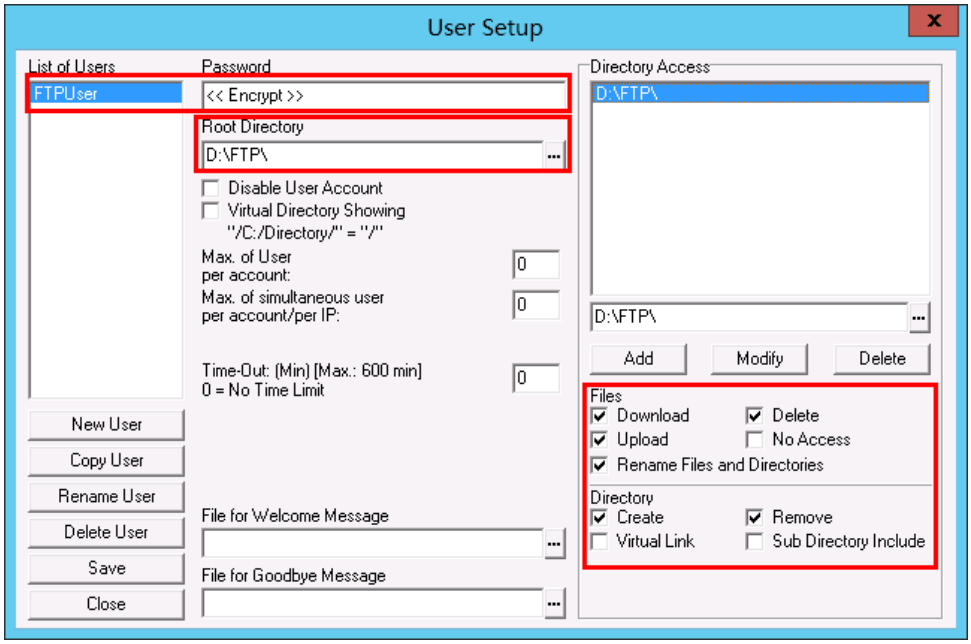
Configure GigabitEthernet 1/0/26 as the monitor port for local mirroring group 1.

```
[Switch] mirroring-group 1 monitor-port gigabitethernet 1/0/26
```

Configuring FTP on the same host as NTA

1. Create an FTP server.
2. Configure the username, password, root directory, and user permissions, as shown in Figure 2. This example uses **FTPUser** as the username.

Figure 2 Configuring FTP

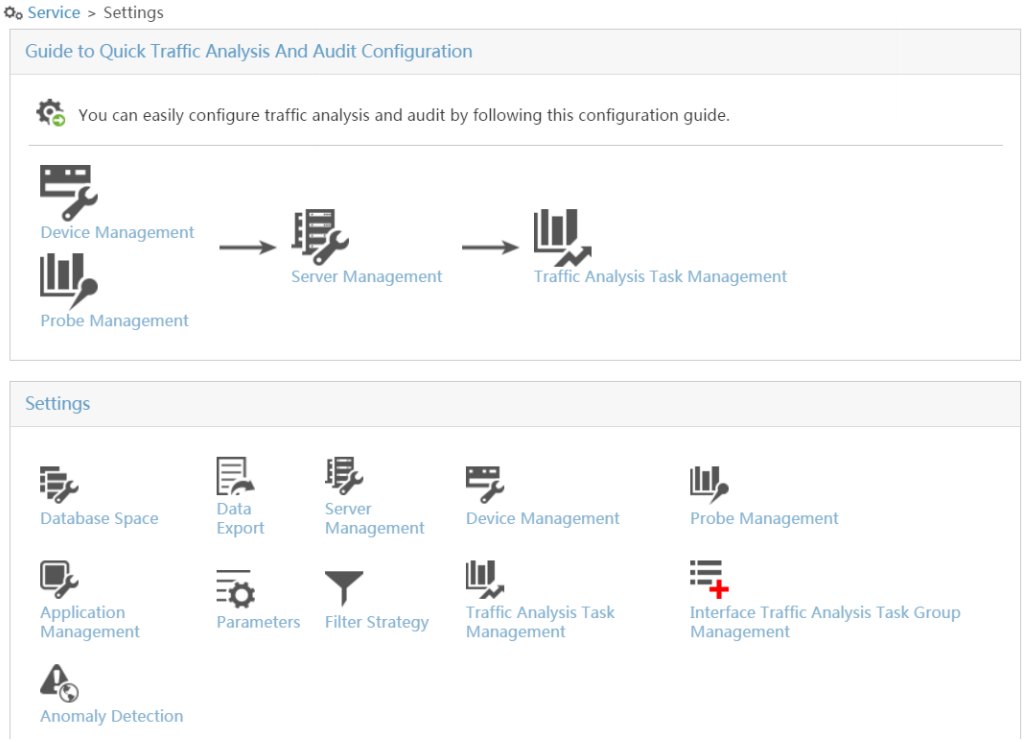


Configuring the NTA server

Adding a probe

1. Click the **Service** tab.
2. From the left navigation tree, select **Traffic Analysis and Audit** > **Settings**. The **Settings** page opens, as shown in Figure 3.

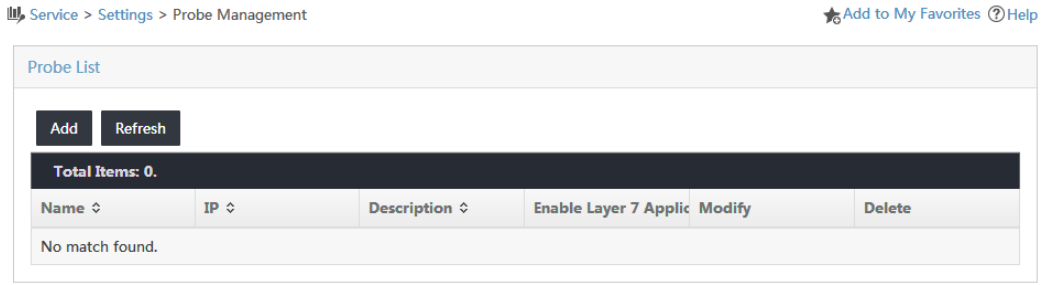
Figure 3 Accessing the traffic analysis and audit settings page



3. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **Probe Management**.

   The **Probe Management** page opens, as shown in Figure 4.

Figure 4 Accessing the Probe Management page



4. In the probe list, click **Add**.

   The **Add Probe** page opens.

5. Configure probe parameters, as shown in Figure 5:

   a. Enter a name in the **Name** field.

   This example uses **192.168.40.248**.

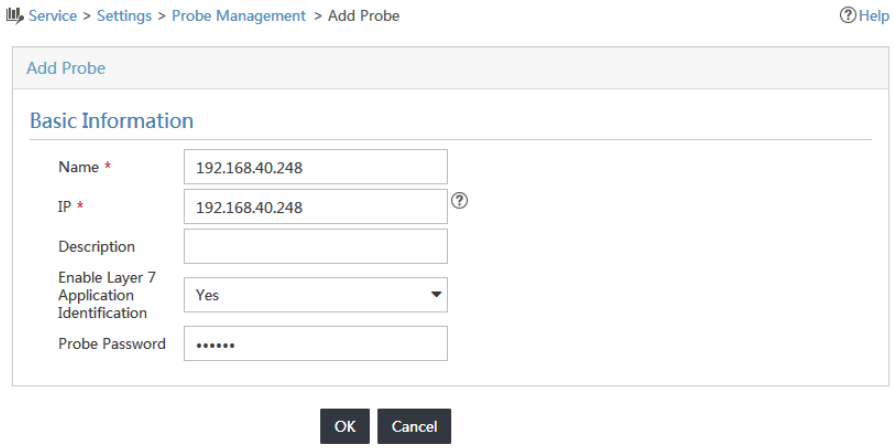
   b. Enter **192.168.40.248** in the **IP** field.

   c. Enter the probe password in the **Probe Password** field.

   d. Select **Yes** from the **Enable Layer 7 Application Identification** list.

   e. Use the default values of other parameters.

Figure 5 Adding a probe



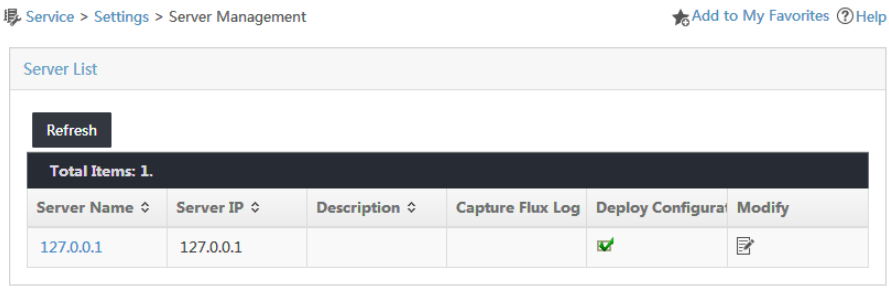
6. Click **OK**.

Deploying server configuration

1. Access the **Settings** page.
2. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **Server Management**.

   The **Server Management** page opens, as shown in Figure 6.

   Figure 6 Accessing the Server Management page

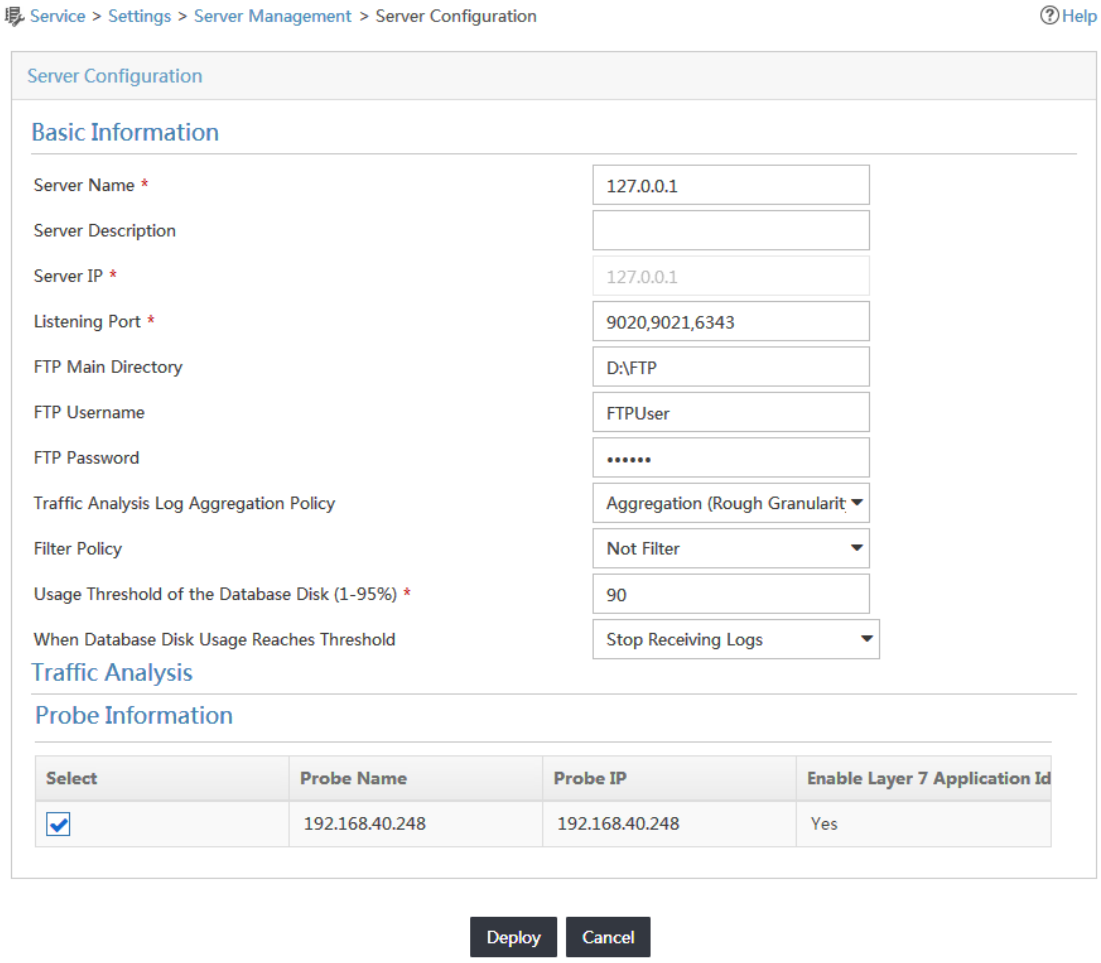


3. Click the **Modify** icon for the NTA server.

   The **Server Configuration** page opens.
4. Modify the server parameters as needed, as shown in Figure 7:
   a. Enter a name in the **Server Name** field.

      This example uses **127.0.0.1**.
   b. Enter **D:\FTP** in the **FTP Main Directory** field.
   c. Enter **FTPUser** in the **FTP Username** field.
   d. Enter the FTP password in the **FTP Password** field.
   e. In the **Probe Information** area, select the probe named **192.168.40.248**.
   f. Use the default values of other parameters.

Figure 7 Configuring the NTA server



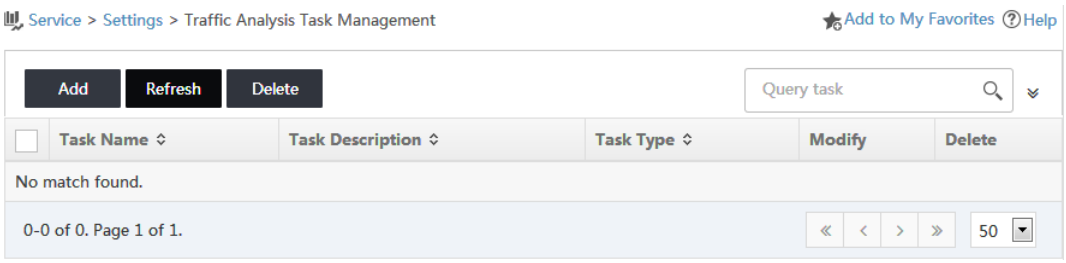
5. Click **Deploy**.

Adding a probe traffic analysis task

1. Access the **Settings** page.
2. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **Traffic Analysis Task Management**.

   The **Traffic Analysis Task Management** page opens, as shown in Figure 8.

Figure 8 Accessing the Traffic Analysis Task Management page



3. In the traffic analysis task list, click **Add**.

   The **Select Task Type** page opens.
4. Select **Probe** and click **Next**.

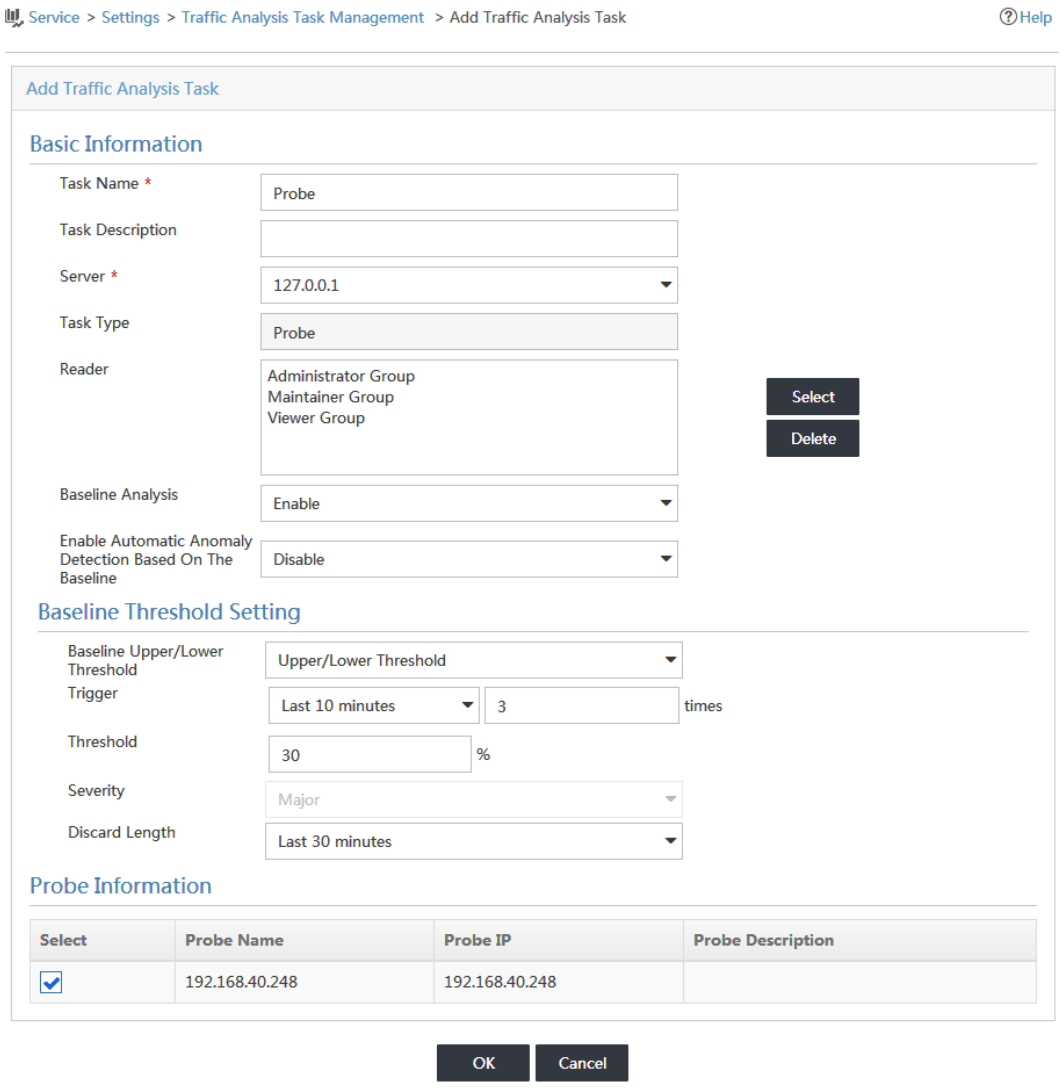
The **Add Traffic Analysis Task** page opens.

5. Configure traffic analysis task parameters, as shown in Figure 9:
   a. Enter a task name in the **Task Name** field.

      This example uses **Probe**.
   b. Select **127.0.0.1** from the **Server** list.
   c. Click **Select** next to the **Reader** field. On the window that opens, select operator groups that have the right to view the task, and then click **OK**.
   d. Select **Enable** from the **Baseline Analysis** list.

      The **Enable Automatic Anomaly Detection Based On The Baseline** field and the **Baseline Threshold Setting** area are displayed.
   e. Select **Disable** form the **Enable Automatic Anomaly Detection Based On The Baseline** list.
   f. In the **Baseline Threshold Setting** area, enter **30** in the **Threshold** field.
   g. In the **Probe Information** area, select the probe named **192.168.40.248**.
   h. Use the default values of other parameters.

Figure 9 Adding a probe traffic analysis task



6. Click **OK**.

Verifying the configuration

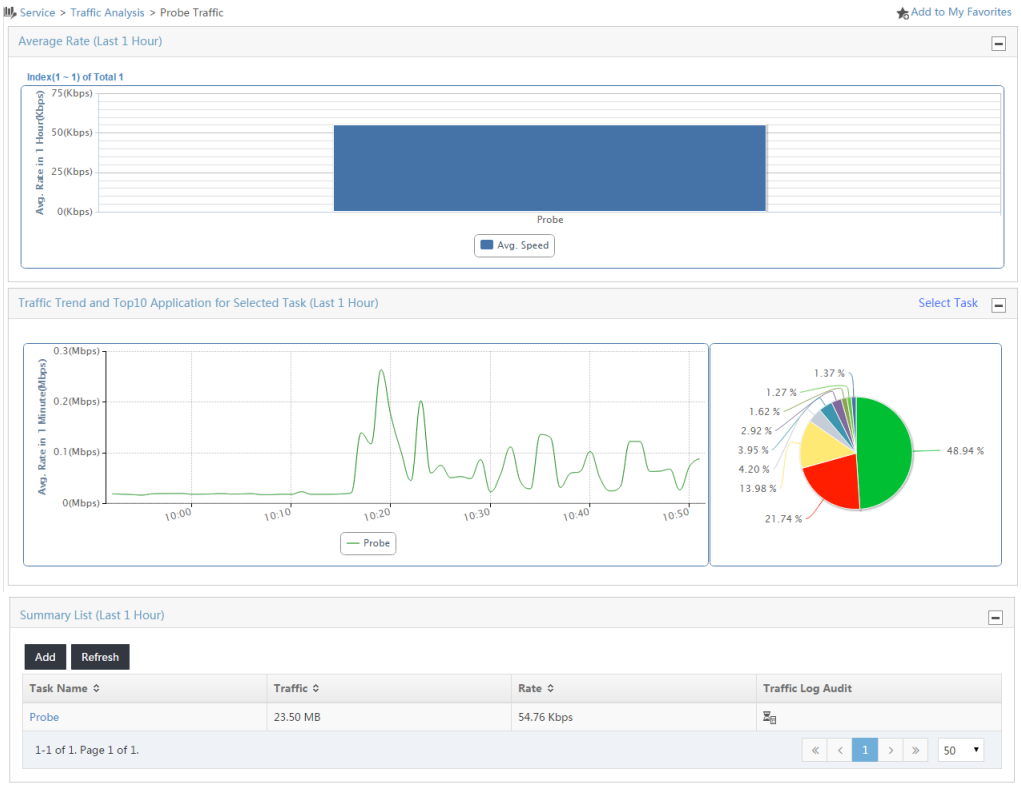
NTA enables you to view the summary report of all probe traffic analysis tasks and the report of an individual probe traffic analysis task.

Viewing the summary report of all probe analysis tasks

1. Click the **Service** tab.
2. From the left navigation tree, select **Traffic Analysis and Audit** > **Probe Traffic Analysis Task**.

   The **Probe Traffic** page opens and displays the summary report of all probe analysis tasks, as shown in Figure 10.

Figure 10 Summary information about probe traffic tasks



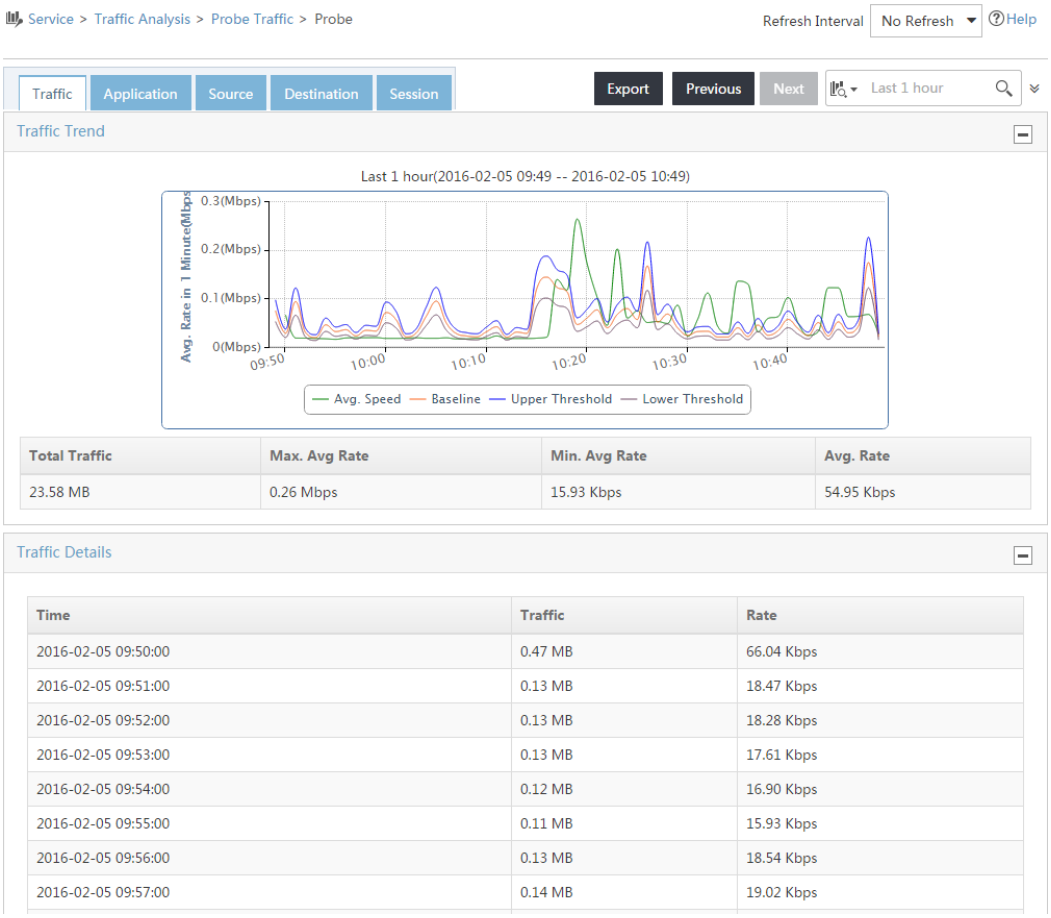
Viewing the report of an individual probe traffic analysis task

Viewing traffic information for the probe traffic analysis task named Probe

1. Access the **Probe Traffic** page.
2. In the **Summary List** area, click **Probe**.

   The **Probe** page opens, as shown in Figure 11. By default, the **Probe** page displays the **Traffic** tab. The tab displays the traffic trend and details for the probe traffic analysis task named **Probe**.

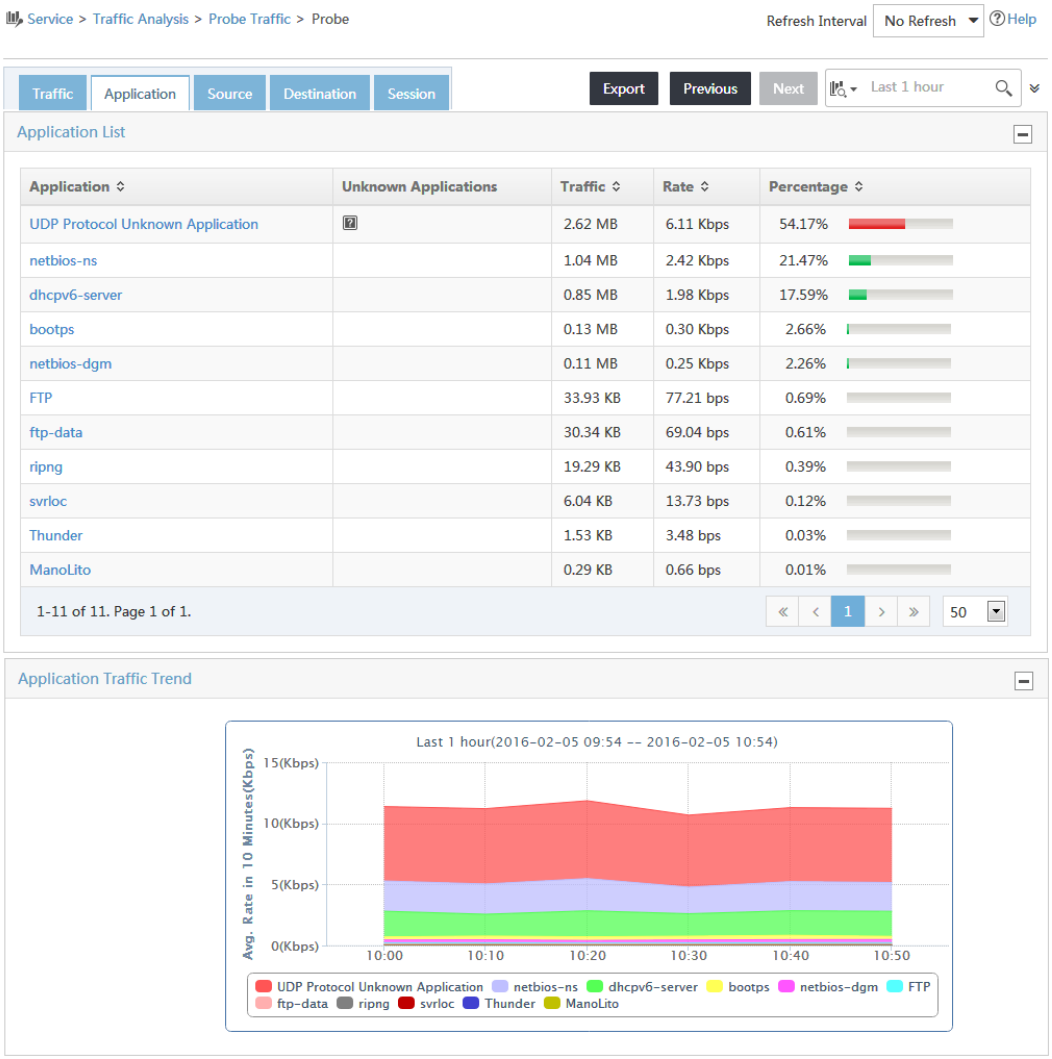
Figure 11 Traffic information for the probe traffic analysis task



Viewing application traffic information for the probe traffic analysis task named Probe

On the **Probe** page, click the **Application** tab. The tab displays the application traffic information for the probe traffic analysis task named **Probe**, as shown in Figure 12.

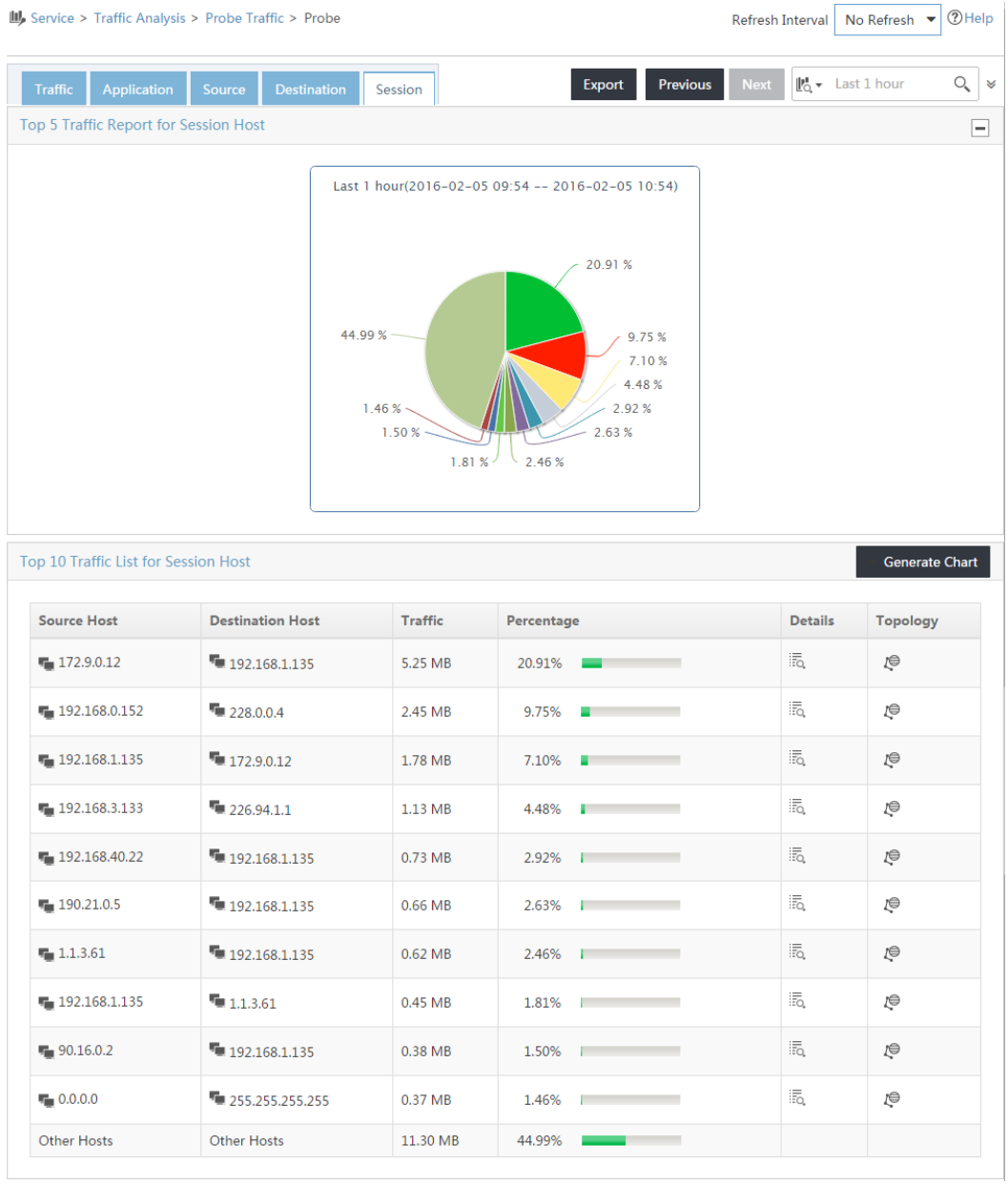
Figure 12 Application traffic information for the probe traffic analysis task



Viewing the session traffic information for the probe traffic analysis task named Probe

On the **Probe** traffic page, click the **Session** tab. The tab displays the session traffic information for the probe traffic analysis task named **Probe**, as shown in Figure 13.

Figure 13 Session traffic information for the probe traffic analysis task



Source Host	Destination Host	Traffic	Percentage	Details	Topology
172.9.0.12	192.168.1.135	5.25 MB	20.91%		
192.168.0.152	228.0.0.4	2.45 MB	9.75%		
192.168.1.135	172.9.0.12	1.78 MB	7.10%		
192.168.3.133	226.94.1.1	1.13 MB	4.48%		
192.168.40.22	192.168.1.135	0.73 MB	2.92%		
190.21.0.5	192.168.1.135	0.66 MB	2.63%		
1.1.3.61	192.168.1.135	0.62 MB	2.46%		
192.168.1.135	1.1.3.61	0.45 MB	1.81%		
90.16.0.2	192.168.1.135	0.38 MB	1.50%		
0.0.0.0	255.255.255.255	0.37 MB	1.46%		
Other Hosts	Other Hosts	11.30 MB	44.99%		