61700544G1-44.1A
March 2010

ADTRAN

Troubleshooting Guide

Network Forensics in AOS

This troubleshooting guide provides instructions for using the network forensics feature in ADTRAN Operating System (AOS) products to gather Dynamic Host Configuration Protocol (DHCP) information on clients connected through the network. Included in this guide is an overview of the network forensics functionality, steps to enable the feature, a description of the information gathered, and how to clear the information from the system. Steps to use this feature are provided in both the Web-based graphical user interface (GUI) and the command line interface (CLI).

This guide consists of the following sections:

Introduction to Network Forensics

Network forensics is a method of collecting information about the network in which the AOS device resides. Network administrators can gain network insight by monitoring DHCP messages. The information gathered identifies clients connected to the AOS device and provides information about them, such as their location in the network. Once network forensics is enabled, the AOS device passively monitors DHCP message exchanges between the server and the client. The following information is collected:

- Client MAC address
- Client IP address
- Client VLAN ID
- Client host name
- Client lease time
- Client source port
- Client vendor class identifier
- Server MAC address
- Server IP address
- Date and time DHCP information last updated

Hardware and Software Requirements and Limitations

The Network forensics feature is available on AOS products as outlined in the ADTRAN knowledge base article number 2272, *Product Feature Matrix*. This matrix is available online at http://kb.adtran.com.

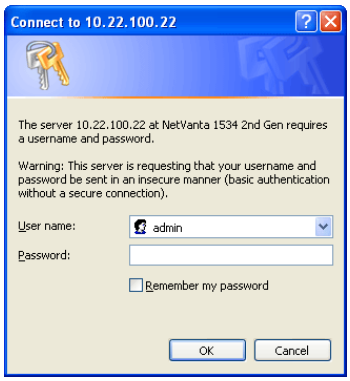
Enabling Network Forensics Using the GUI

To begin using network forensics through the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Enter your AOS product's IP address in the Internet browser's address field in the following form:

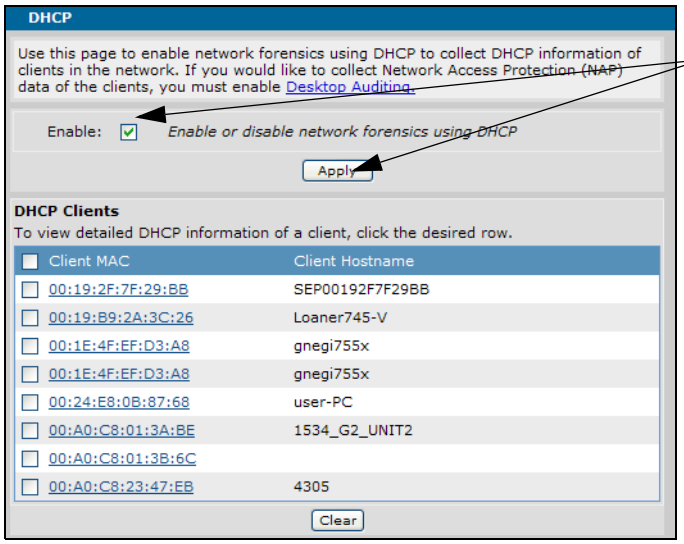
   http://<*ip address*>.

   For example: **http://10.22.100.22**
3. At the prompt, enter your user name and password and select **OK**. The default user name is **admin** and the default password is **password**.



4. Navigate to **Data** > **Switch** > **Network Forensics**.

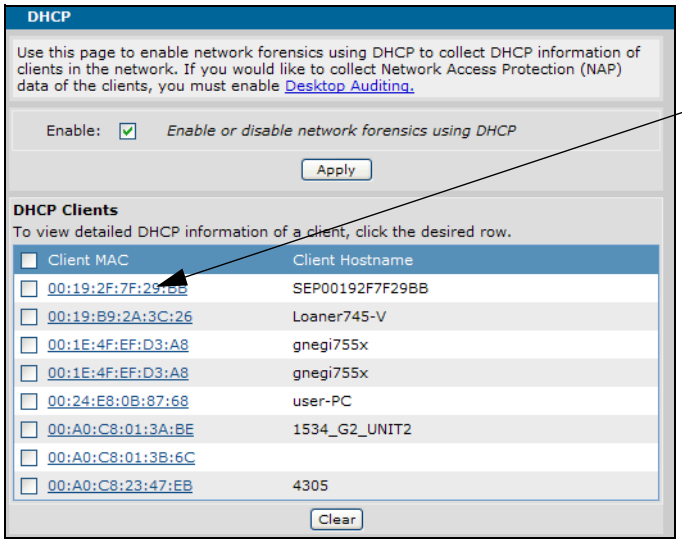
5. Enable network forensics by checking the box next to **Enable** (by default, network forensics is disabled). Select **Apply**.



Check **Enable** and select **Apply** to enable this feature.

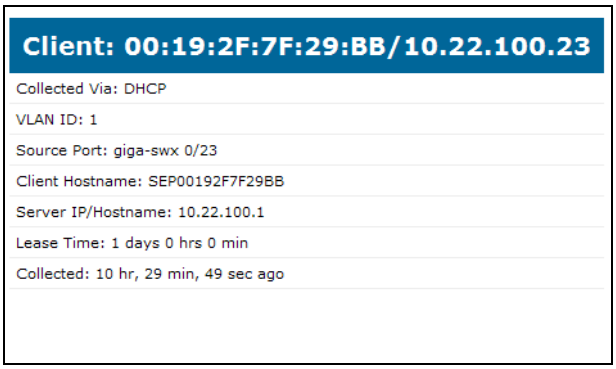
Viewing Client DHCP Information Using the GUI

Once network forensics is enabled, the AOS unit gathers DHCP information from the clients. The DHCP information can be viewed from the GUI by navigating to the **Data** > **Switch** > **Network Forensics** menu. All connected clients, currently being monitored, are displayed in the **DHCP Clients** list. To view a specific client's DHCP information, select the MAC address.



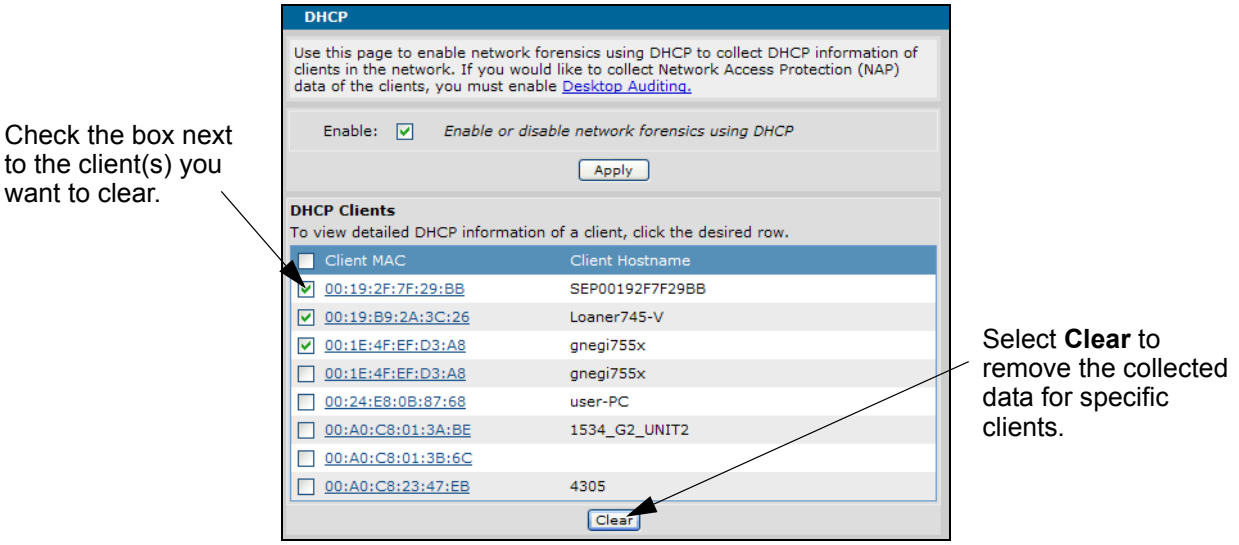
Select the client's MAC address to view the collected DHCP information.

The specific DHCP information collected for that client is displayed in a separate dialog box.



Clearing Client Information Using the GUI

The DHCP message information being collected can be cleared. To clear data for specific clients, check the box next to the client(s) and select **Clear** at the bottom of the **DHCP** menu. To clear the data for all clients, select the checkbox next to **Client MAC** which selects all clients and select **Clear** at the bottom of the client **DHCP** menu.



> NOTE *Information for a particular client will not be repopulated until the client requests a new IP address via DHCP.*

Enabling Network Forensics Using the CLI

Network forensics is enabled using the **network-forensics ip dhcp** command. This command specifies that the AOS unit will monitor DHCP message exchanges between the server and the client. By default, this feature is disabled. Using the **no** form of this command disables network forensics.

To enable network forensics, enter the **network-forensics ip dhcp** command from the Global Configuration mode prompt as follows:

(config)**#network-forensics ip dhcp**

Viewing Client DHCP Information Using the CLI

Once network forensics is enabled, the AOS unit gathers DHCP information from the clients. To view the DHCP information, use the **show network-forensics ip dhcp** command issued from Enable mode. This command can display all DHCP information collected, or filtered by a specific client using the client host name, interface, ip address, or MAC address. By using these additional parameters, the show command output is limited to the specific client matching the **hostname** <*hostname*>, **interface gigabit-switchport** <*slot/port*>, **ip** <*ip address*>, or **mac** <*mac address*>. IP addresses are specified in dotted decimal notation, for example, **10.10.10.1**. MAC addresses are specified in HH:HH:HH:HH:HH format.

The following is sample output from the **show network-forensics ip dhcp** command:

```
#show network-forensics ip dhcp
Client MAC/IP/Host: 00:E0:29:0E:D5:E3 / 10.23.220.1 / xpsp3-host
    VLAN ID: 100
    Source Port: gigabit-switchport 0/2
    Server Mac/IP: 00:E0:29:0E:D5:E5 / 10.23.220.254
    Lease from Time Collected: 3 days from 25 Aug 2009 10:33:42
    Client Vendor Class: unknown
```

> NOTE
> *The preceding output is for one client. This same information will be displayed for all connected clients unless one of the filtering parameters is used in conjunction with the* ***show network-forensics ip dhcp*** *command.*

To view the DHCP information for specific clients, use one of the following variations of this command:

show network-forensics ip dhcp hostname <*hostname*>
show network-forensics ip dhcp interface gigabit-switchport <*slot/port*>
show network-forensics ip dhcp ip <*ip address*>
show network-forensics ip dhcp mac <*mac address*>

Clearing Client Information Using the CLI

The collected DHCP message information can be cleared from the AOS unit using the **clear network-forensics ip dhcp** command. Data can be cleared for all clients or for a specific client using the optional parameters. Using the optional parameters clears the DHCP data collected for the specific client matching the **hostname** <*hostname*>, **interface gigabit-switchport** <*slot/port*>, **ip** <*ip address*>, **mac** <*mac address*>, or VLAN interface <*vlan id*>. IP addresses are specified in dotted decimal notation, for example, **10.10.10.1**. MAC addresses are specified in HH:HH:HH:HH:HH format.

For example, to clear all data for all connected clients from the AOS unit, enter the following command:

```
#clear network-forensics ip dhcp
```

To clear data for the specific client at MAC address **00:E0:29:0E:D5:E3**, enter the following command:

```
#clear network-forensics ip dhcp mac 00:E0:29:0E:D5:E3
```


Command Summary

The following table includes configuration, **show**, **clear**, and **debug** commands necessary for using the network forensics feature. The debug commands are explained in *Troubleshooting Using the CLI on page 8*.

Table 1. Network Forensics Command Summary

Prompt	Command	Description
(config)#	**[no] network-forensics ip dhcp**	Enables network forensics. Using the **no** form of this command disables network forensics.
#	**show network-forensics ip dhcp [mac** <*mac address*> | **ip** <*ip address*> | **hostname** <*hostname*> | **gigabit-switchport** <*slot/port*>**]**	Displays general client information collected by monitoring DHCP messages. This output can be for all clients, or limited to specific clients by indicating the client host name, interface, IP address, or MAC address.
#	**clear network-forensics ip dhcp [mac** <*mac address*> **| ip** <*ip address*> **| hostname** <*hostname*> **| interface gigabit-switchport** <*slot/port*> | **vlan** <*vlan id*>**]**	Clears the collected information for either all clients or a specific client. Clients are specified by host name, interface, IP address, MAC address, or VLAN.
#	**[no] debug network-forensics ip dhcp [mac** <*mac address*> **| ip** <*ip address*> **| hostname** <*hostname*> **| gigabit-switchport** <*slot/port*>**]**	Displays DHCP messages that have been monitored and some of the information included in those messages. The debug messages can be enabled for all clients or limited to specific clients by indicating the client host name, interface, IP address, or MAC address.

Troubleshooting

There are two methods for troubleshooting network forensics. Troubleshooting can be done from either the GUI or the CLI. Only the CLI will be covered in this document.

*Using **debug** commands to troubleshoot network forensics can be initiated from the GUI by navigating to the **Utilities** > **System** > **Debug Unit** menu.*

Troubleshooting Using the CLI

The **debug network-forensics ip dhcp** command can be beneficial in viewing details about connected clients in the network. The command is issued from the Enable mode in the CLI to assist in troubleshooting, and can specify if debug information for all clients is displayed or if information for a specific client is displayed. Clients can be specified by host name, interface, IP address, or MAC address. **Debug** commands display the collected information in real time.

*Using **debug** commands can be very processor intensive, and should be used with caution.*

The following sample output displays when debug messages are enabled for all clients connected to the network:

#debug network-forensics ip dhcp

2009.08.31 14:30:30 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/5 Discover from 00:E0:29:0E:D5:E3 (xpsp3-host)
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/24 Offer from 00:E0:29:0E:D5:E5/10.23.220.254 to 00:E0:29:0E:D5:E3 of 10.23.220.1/255.255.255.0(xpsp3-host)
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/5 Request from 00:E0:29:0E:D5:E3 10.23.220.1/255.255.255.0 (xpsp3-host) to 00:E0:29:0E:D5:E5/10.23.220.254
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/24 Ack from 00:E0:29:0E:D5:E5/10.23.220.254 to 00:E0:29:0E:D5:E3 of 10.23.220.1/255.255.255.0 (xpsp3-host)

To view the DHCP information for specific clients, use one of the following variations of this command:

debug network-forensics ip dhcp hostname <*hostname*>
debug network-forensics ip dhcp interface gigabit-switchport <*slot/port*>
debug network-forensics ip dhcp ip <*ip address*>
debug network-forensics ip dhcp mac <*mac address*>

By using these additional parameters, the debug messages are limited to the specific client matching the **hostname** <*hostname*>, **interface gigabit-switchport** <*slot/port*>, **ip** <*ip address*>, or **mac** <*mac address*>. IP addresses are specified in dotted decimal notation, for example, **10.10.10.1**. MAC addresses are specified in HH:HH:HH:HH:HH format.

