

Using the tcpdump Command in ACNS Software

Document ID: 27608

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Capturing Packets

- Options
- FTP
- Ethereal

Related Information

Introduction

Cisco Application and Content Networking Software (ACNS) 4.2.1 introduced the **tcpdump** command. This command enables you to gather a sniffer trace on the Content Engine, Content Router, or Content Distribution Manager for the purpose of troubleshooting, when asked to gather the data by the Cisco Technical Support. This utility is very similar to the Linux/Unix **tcpdump** command.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- FTP
- ACNS
- Command-line interface (CLI) of ACNS

Components Used

The information in this document is based on the software and hardware versions:

- ACNS 4.2.1 software and later
- All platforms that run ACNS 4.2.X and above

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Capturing Packets

The CLI on ACNS now allows the administrator (must be user admin) to capture packets from the Ethernet. On the Content Engine 500 series, the interface names are eth0 and eth1. On all ACNS platforms, it is recommended that you specify a path/filename in the local1 directory.

You can do a straight packet header dump to the screen if you issue the **tcpdump** command on the CLI. Press **Ctrl-C** in order to stop the dump.

Options

The **tcpdump** command has these options:

- **-w filename** Writes the raw packet capture output to a file.
- **-s count** Captures the first <count> bytes of each packet.
- **-i interface** Allows you to specify a specific interface to use for capturing the packets.
- **-c count** Limits the capture to *count* packets.

This is a sample command:

```
tcpdump -w /local1/dump.pcap -i eth0 -s 1500 -c 10000
```

This command captures the first 1500 bytes of the next 10,000 packets from interface Ethernet 0, and puts the output in a file named **dump.pcap** in the local1 directory on the Content Engine.

Note: Ensure that you specify option **s** to set the packet snaplength. The default value captures only 64 bytes, and this saves only packet headers into the capture file. For troubleshooting of redirected packets or higher level traffic (HTTP, authentication, and so forth), a copy of complete packets is needed.

You can also run **tcpdump** and filter on a particular IP address:

- Add **host 10.255.1.34** to the end of the **tcpdump** line.

Note: Replace **10.255.1.34** with the IP address that the client is using.

- Also, use 1600 as the size in order to catch bad packets that can be larger than 1500 bytes.

Here is an example:

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

After the TCP dump has been collected, you need to move the file from the Content Engine to a PC so that it can be viewed by a sniffer decoder.

```
ftp <ip address of the CE>
```

```
!--- Log in with the admin username and password.
```

```
cd local1
bin
hash
get <name of the file>
```

!--- Using the previous example, it is `dump.pcap`.

bye

Ethereal

Ethereal is the recommended software application for reading the TCP dump, due to the extent of its features and their use with content networking, including the ability to decode packets that are encapsulated into a GRE tunnel, used by WCCP redirection. Refer to the Wireshark website for more information.

Note: In most cases, redirected packets captured by the **tcpdump** facility available with the ACNS CLI differ from the data received on the interface. Due to internal implementation and handling of redirected packets, the destination IP address and TCP port number are modified to reflect the device IP address and the port number 8999.

Related Information

- **Cisco Application and Content Networking Software (ACNS) Software Support**
- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 31, 2006

Document ID: 27608
