App H Capturing Application Traffic with tcpdump

tcpdump is a command-line utility for capturing traffic. It generates packet traces in a format that AppTransaction Xpert can recognize. The syntax for starting a capture is as follows:

```
cmd> tcpdump -s 0 -i <interface_name> -w <capture_file_name> <expression>
```

The following table lists a short description of each required argument. For more information about these and other arguments, refer to the “man” page for tcpdump. (To access this, go to an internet search engine and search on “tcpdump man”.)

Table H-1 Command-Line Arguments to Use with tcpdump

Argument	Description
-c	Stop the capture after **c** packets are captured. It is good practice to specify a maximum number of packets before the capture ends, to avoid the possibility that the accelerator will run out of disk space.

Table H-1 Command-Line Arguments to Use with tcpdump (Continued)

Argument	Description
-s 0	The maximum number of bytes to capture per individual packet. It is good practice to capture the smallest number of bytes per packet for the protocol information that you want to study in AppTransaction Xpert. To capture the entire contents of each packet, specify 0 for this argument.
-i <*interface_name***>**	The name of the interface(s) on which to capture. If this is unspecified, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loopback). Ties are broken by choosing the earliest match. To print a list of all available network interfaces on which tcpdump can capture packets, enter the following command: `tcpdump -D` If you do not know which interface(s) to capture on, see the following: • Identifying the WAE Interfaces for Capturing Traffic (Cisco) • Identifying the Steelhead Interfaces for Capturing Traffic (Riverbed)
-w <*capture_file_name***>**	Write the raw packets to <*capture_file_name*> rather than simply printing them out.
<*packet_filter_expression***>**	A filter expression in Berkeley Packet Filter (BPF) format, used to filter out irrelevant packets. **Note—**You should always specify a packet filter. This will keep the packet trace from becoming unnecessarily large and reduce the amount of filtering required when you import the packet trace into AppTransaction Xpert. The following filters are provided as examples: • `ip host client and ip host server` (capture all IP packets between client and server) • `ip host client.mycompany.com port eth1` (capture all IP packets to or from port GigabitEthernet 2/0 (specified as `eth1`) on host client) For detailed information about BPF, go to the “<expression>” section on the tcpdump man page.