Perform a Packet Capture in a Telemetry Broker Node

Contents

Introduction

This document describes how to perform a packet capture in a Cisco Telemetry Broker (CTB) Broker node.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Linux administration
- Basic Cisco Telemetry Broker architecture
- SSH basic knowledge
- Command Line Interface (CLI) access as **admin** and root is needed to perform the packet capture.

Components Used

The information in this document is based on CTB Broker node running version 2.0.1.

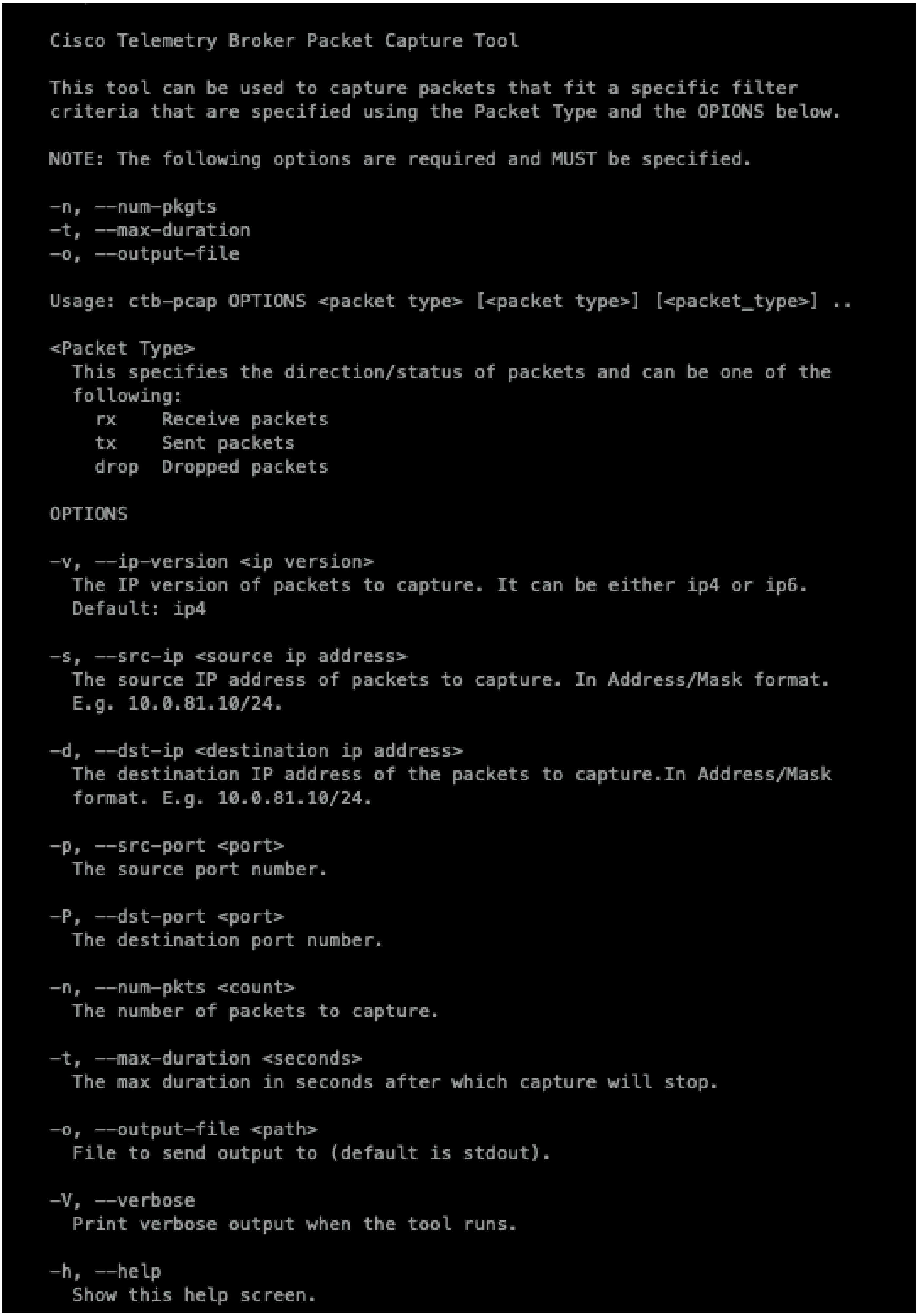
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

The CTB Broker Node has a tool called **ctb-pcap** that is used to perform a network capture from the telemetry interface of the broker node. Note that this tool is not available at the CTB Manager Node.

Before you use the command ctb-pcap, ensure that you first switch to the **root** user with the command sudo su. This tool is available to the root user only.

To view the available options for this tool, run the command **ctb-pcap --help** at the CLI of the Broker node. This image displays the full list of the options:



```
Cisco Telemetry Broker Packet Capture Tool

This tool can be used to capture packets that fit a specific filter
criteria that are specified using the Packet Type and the OPIONS below.

NOTE: The following options are required and MUST be specified.

-n, --num-pkgts
-t, --max-duration
-o, --output-file

Usage: ctb-pcap OPTIONS <packet type> [<packet type>] [<packet_type>] ..

<Packet Type>
  This specifies the direction/status of packets and can be one of the
  following:
    rx    Receive packets
    tx    Sent packets
    drop  Dropped packets

OPTIONS

-v, --ip-version <ip version>
  The IP version of packets to capture. It can be either ip4 or ip6.
  Default: ip4

-s, --src-ip <source ip address>
  The source IP address of packets to capture. In Address/Mask format.
  E.g. 10.0.81.10/24.

-d, --dst-ip <destination ip address>
  The destination IP address of the packets to capture.In Address/Mask
  format. E.g. 10.0.81.10/24.

-p, --src-port <port>
  The source port number.

-P, --dst-port <port>
  The destination port number.

-n, --num-pkts <count>
  The number of packets to capture.

-t, --max-duration <seconds>
  The max duration in seconds after which capture will stop.

-o, --output-file <path>
  File to send output to (default is stdout).

-V, --verbose
  Print verbose output when the tool runs.

-h, --help
  Show this help screen.
```

All available options for CTB packet capture tool

As the output indicates, the number of captured packets, the duration in seconds, and the packet capture outp