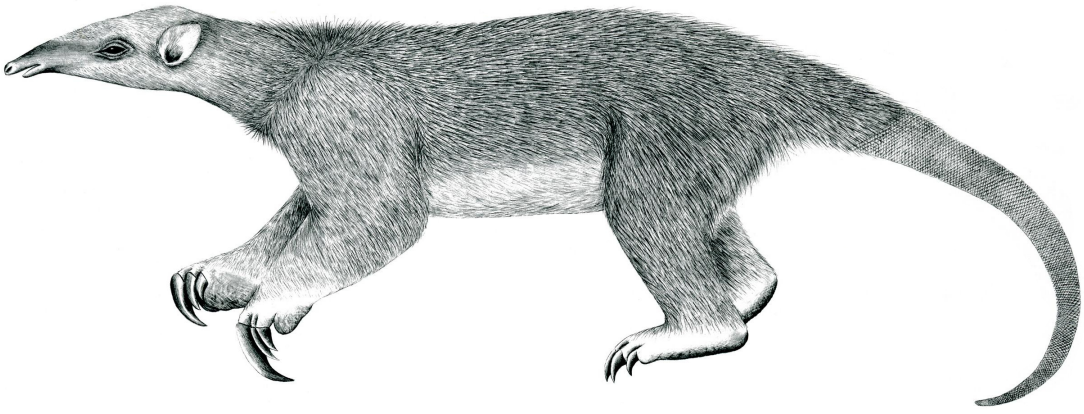
# Tranalyzer2

## cdpDecode

Cisco Discovery Protocol (CDP)



Tranalyzer Development Team

# Contents

**1 cdpDecode** **1**
1.1 Description . . . 1
1.2 Dependencies . . . 1
1.3 Configuration Flags . . . 1
1.4 Flow File Output . . . 1
1.5 Packet File Output . . . 3
1.6 Monitoring Output . . . 4
1.7 Plugin Report Output . . . 4

# 1 cdpDecode

## 1.1 Description

The cdpDecode plugin analyzes CDP traffic.

## 1.2 Dependencies

### 1.2.1 Core Configuration

This plugin requires the following core configuration:

- *$T2HOME/tranalyzer2/src/networkHeaders.h*:
  - `ETH_ACTIVATE>0`

## 1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

| Name | Default | Description |
|---|---|---|
| `CDP_NADDR` | 5 | Maximum number of IPv4 addresses |
| `CDP_NMADDR` | 5 | Maximum number of management addresses |
| `CDP_NIPPG` | 5 | Maximum number of IP prefix gateways |
| `CDP_STRLEN` | 25 | Maximum length of strings to store |
| `CDP_LSTRLEN` | 100 | Maximum length of long strings to store |

## 1.4 Flow File Output

The cdpDecode plugin outputs the following columns:

| Column | Type | Description |
|---|---|---|
| `cdpStat` | H8 | Status |
| `cdpVer` | U8 | Version |
| `cdpTTL` | U8 | Time To Live (sec) |
| `cdpTLVTypes` | H32 | TLV types |
| `cdpDevice` | SC | Device ID |
| `cdpPlatform` | S | Platform |
| `cdpSWVersion` | S | Software Version |
| `cdpPortID` | SC | Port ID |
| `cdpCaps` | H32 | Capabilities |
| `cdpDuplex` | H8 | Duplex |
| `cdpNVLAN` | U16 | Native VLAN |
| `cdpVoipVLAN` | U16 | VoIP VLAN |
| `cdpVTPMngmtDmn` | SC | VTP management domain |
| `cdpMAddrs` | R(IP4) | Management Addresses |
| `cdpAddrs` | R(IP4) | Addresses |

| Column | Type | Description |
|---|---|---|
| cdpIPPref_cdr | R(IP4_U8) | IP Prefix, CIDR |

### 1.4.1 cdpStat

The cdpStat column is to be interpreted as follows:

| cdpStat | Description |
|---|---|
| 0x01 | Flow is CDP |
| 0x02 | — |
| 0x04 | — |
| 0x08 | — |
| 0x10 | — |
| 0x20 | String truncated... increase CDP_STRLEN |
| 0x40 | Invalid TLV length |
| 0x80 | Snapped payload |

### 1.4.2 cdpTLVTypes

The cdpTLVTypes column is to be interpreted as follows:

| cdpTLVTypes | | Description |
|---|---|---|
| $2^0$ | (=0x0000 0001) | — |
| $2^1$ | (=0x0000 0002) | Device ID |
| $2^2$ | (=0x0000 0004) | Addresses |
| $2^3$ | (=0x0000 0008) | Port ID |
| $2^4$ | (=0x0000 0010) | Capabilities |
| $2^5$ | (=0x0000 0020) | Software Version |
| $2^6$ | (=0x0000 0040) | Platform |
| $2^7$ | (=0x0000 0080) | IP Prefixes |
| $2^8$ | (=0x0000 0100) | Protocol Hello |
| $2^9$ | (=0x0000 0200) | VTP Management Domain |
| $2^{10}$ | (=0x0000 0400) | Native VLAN |
| $2^{11}$ | (=0x0000 0800) | Duplex |
| $2^{12}$ | (=0x0000 1000) | — |
| $2^{13}$ | (=0x0000 2000) | — |
| $2^{14}$ | (=0x0000 4000) | VoIP VLAN Reply |
| $2^{15}$ | (=0x0000 8000) | VoIP VLAN Query |

| cdpTLVTypes | | Description |
|---|---|---|
| $2^{16}$ | (=0x0001 0000) | Power Consumption |
| $2^{17}$ | (=0x0002 0000) | MTU |
| $2^{18}$ | (=0x0004 0000) | Trust Bitmap |
| $2^{19}$ | (=0x0008 0000) | Untrusted Port CoS |
| $2^{20}$ | (=0x0010 0000) | System Name |
| $2^{21}$ | (=0x0020 0000) | System OID |
| $2^{22}$ | (=0x0040 0000) | Management Address |
| $2^{23}$ | (=0x0080 0000) | Location |
| $2^{24}$ | (=0x0100 0000) | External Port ID |
| $2^{25}$ | (=0x0200 0000) | Power Requested |
| $2^{26}$ | (=0x0400 0000) | Power Available |
| $2^{27}$ | (=0x0800 0000) | Port Unidirectional |
| $2^{28}$ | (=0x1000 0000) | Energy Wise |
| $2^{29}$ | (=0x2000 0000) | Spare Pair POE |
| $2^{30}$ | (=0x4000 0000) | — |
| $2^{31}$ | (=0x8000 0000) | Any type $\geq 31$ |

### 1.4.3 cdpCaps

The cdpCaps column is to be interpreted as follows:

| cdpCaps | Description |
|---|---|
| 0x0000 0001 | Router |
| 0x0000 0002 | Transparent Bridge |
| 0x0000 0004 | Source Route Bridge |
| 0x0000 0008 | Switch |
| 0x0000 0010 | Host |
| 0x0000 0020 | IGMP capable |
| 0x0000 0040 | Repeater |
| 0x00000100-0x80000000 | Reserved |

### 1.4.4 cdpDuplex

The cdpDuplex column is to be interpreted as follows:

| cdpDuplex | Description |
|---|---|
| 0x0001 | Half |
| 0x0002 | Full |

## 1.5 Packet File Output

In packet mode (-s option), the cdpDecode plugin outputs the following columns:

| Column | Type | Description | Flags |
|---|---|---|---|
| cdpStat | H8 | Status | |
| cdpVer | U8 | Version | |
| cdpTTL | U8 | Time To Live (sec) | |
| cdpTLVTypes | H16 | TLV types | |
| cdpDevice | SC | Device ID | |
| cdpPlatform | S | Platform | |
| cdpPortID | SC | Port ID | |
| cdpCaps | H32 | Capabilities | |
| cdpDuplex | H8 | Duplex | |
| cdpNVLAN | U16 | Native VLAN | |
| cdpVoipVLAN | U16 | VoIP VLAN | |
| cdpVTPMngmtDmn | SC | VTP management domain | |
| cdpMAddrs | IP4 | Management Addresses | |
| cdpAddrs | IP4 | Addresses | |

## 1.6 Monitoring Output

In monitoring mode, the cdpDecode plugin outputs the following columns:

| Column | Type | Description | Flags |
|---|---|---|---|
| cdpPkts | U64 | Number of CDP packets | |

## 1.7 Plugin Report Output

The following information is reported:

- Aggregated cdpStat
- Aggregated cdpTLVTypes
- Aggregated cdpCaps
- Number of CDP packets