NAME

ciscodump − Provide interfaces to capture from a remote Cisco router through SSH.

SYNOPSIS

ciscodump [**−−help**] [**−−version**] [**−−extcap−interfaces**] [**−−extcap−dlts**]
[**−−extcap−interface**=<interface>] [**−−extcap−config**] [**−−extcap−capture−filter**=<capture filter>]
[**−−capture**] [**−−fifo**=<path to file or pipe>] [**−−remote−host**=<IP address>]
[**−−remote−port**=<TCP port>] [**−−remote−username**=<username>]
[**−−remote−password**=<password>] [**−−remote−filter**=<filter>] [**−−sshkey**=<public key path>]
[**−−remote−interface**=<interface>]

ciscodump −−extcap−interfaces

ciscodump −−extcap−interface=<interface> **−−extcap−dlts**

ciscodump −−extcap−interface=<interface> **−−extcap−config**

ciscodump −−extcap−interface=<interface> **−−fifo**=<path to file or pipe> **−−capture**
−−remote−host=remoterouter −−remote−port=22 −−remote−username=user
−−remote−interface=<the router interface>

DESCRIPTION

Ciscodump is an extcap tool that relies on Cisco EPC to allow a user to run a remote capture on a Cisco router in a SSH connection. The minimum IOS version supporting this feature is 12.4(20)T. More details can be found here:
https://www.cisco.com/c/en/us/products/collateral/ios−nx−os−software/ios−embedded−packet−capture/datasheet_c78−50

Supported interfaces:

1. cisco

OPTIONS

−−help

Print program arguments.

−−version

Print program version.

−−extcap−interfaces

List available interfaces.

−−extcap−interface=<interface>

Use specified interfaces.

−−extcap−dlts

List DLTs of specified interface.

−−extcap−config

List configuration options of specified interface.

−−capture

Start capturing from specified interface and save it in place specified by −−fifo.

−−fifo=<path to file or pipe>

Save captured packet to file or send it through pipe.

−−remote−host=<remote host>

The address of the remote host for capture.

−−remote−port=<remote port>

The SSH port of the remote host.

−−remote−username=<username>

The username for ssh authentication.

−−remote−password=<password>

The password to use (if not ssh−agent and pubkey are used). WARNING: the passwords are stored in plaintext and visible to all users on this system. It is recommended to use keyfiles with a SSH agent.

−−remote−filter=<filter>

The remote filter on the router. This is a capture filter that follows the Cisco IOS standards (https://www.cisco.com/c/en/us/support/docs/ip/access−lists/26448−ACLsamples.html). Multiple filters can be specified using a comma between them. BEWARE: when using a filter, the default behavior is to drop all the packets except the ones that fall into the filter.

Examples:

```
permit ip host MYHOST any, permit ip any host MYHOST (capture the traffic for

deny ip host MYHOST any, deny ip any host MYHOST, permit ip any any (capture a
```

−−sshkey=<SSH private key path>

The path to a private key for authentication.

−−remote−interface=<remote interface>

The remote network interface to capture from.

−−extcap−capture−filter=<capture filter>

Unused (compatibility only).

EXAMPLES

To see program arguments:

```
ciscodump −−help
```

To see program version:

```
ciscodump --version
```

To see interfaces:

```
ciscodump --extcap-interfaces
```

Only one interface (cisco) is supported.

Example output

```
interface {value=cisco}{display=SSH remote capture}
```

To see interface DLTs:

```
ciscodump --extcap-interface=cisco --extcap-dlts
```

Example output

```
dlt {number=147}{name=cisco}{display=Remote capture dependent DLT}
```

To see interface configuration options:

```
ciscodump --extcap-interface=cisco --extcap-config
```

Example output

```
ciscodump --extcap-interface=cisco --extcap-config
arg {number=0}{call=--remote-host}{display=Remote SSH server address}
    {type=string}{tooltip=The remote SSH host. It can be both an IP address or a
    {required=true}
arg {number=1}{call=--remote-port}{display=Remote SSH server port}{type=unsigned}
    {default=22}{tooltip=The remote SSH host port (1-65535)}{range=1,65535}
arg {number=2}{call=--remote-username}{display=Remote SSH server username}{type=s
    {default=<current user>}{tooltip=The remote SSH username. If not provided, th
    user will be used}
arg {number=3}{call=--remote-password}{display=Remote SSH server password}{type=s
    {tooltip=The SSH password, used when other methods (SSH agent or key files) a
arg {number=4}{call=--sshkey}{display=Path to SSH private key}{type=fileselect}
    {tooltip=The path on the local filesystem of the private ssh key}
arg {number=5}{call--sshkey-passphrase}{display=SSH key passphrase}
    {type=string}{tooltip=Passphrase to unlock the SSH private key}
arg {number=6}{call=--remote-interface}{display=Remote interface}{type=string}
    {required=true}{tooltip=The remote network interface used for capture}
arg {number=7}{call=--remote-filter}{display=Remote capture filter}{type=string}
    {default=(null)}{tooltip=The remote capture filter}
arg {number=8}{call=--remote-count}{display=Packets to capture}{type=unsigned}{re
    {tooltip=The number of remote packets to capture.}
```

To capture:

```
ciscodump --extcap-interface cisco --fifo=/tmp/cisco.pcap --capture --remote-host
    --remote-username user --remote-interface gigabit0/0
    --remote-filter "permit ip host 192.168.1.1 any, permit ip any host 192.168.1
```

Note

Packet count is mandatory, hence the capture will start after this number.

KNOWN ISSUES

The configuration of the capture on the routers is a multi−step process. If the SSH connection is interrupted during it, the configuration can be in an inconsistent state. That can happen also if the capture is stopped and ciscodump can’t clean the configuration up. In this case it is necessary to log into the router and manually clean the configuration, removing both the capture point (WIRESHARK_CAPTURE_POINT), the capture buffer (WIRESHARK_CAPTURE_BUFFER) and the capture filter (WIRESHARK_CAPTURE_FILTER).

Another known issues is related to the number of captured packets (−−remote−count). Due to the nature of the capture buffer, ciscodump waits for the capture to complete and then issues the command to show it. It means that if the user specifies a number of packets above the currently captured, the show command is never shown. Not only is the count of the maximum number of captured packets, but it is also the *exact* number of expected packets.

SEE ALSO

wireshark(1), tshark(1), dumpcap(1), extcap(4), sshdump(1)

NOTES

ciscodump is part of the **Wireshark** distribution. The latest version of **Wireshark** can be found at https://www.wireshark.org.

HTML versions of the Wireshark project man pages are available at https://www.wireshark.org/docs/man−pages.

AUTHORS

Original Author

Dario Lombardo <lomato[AT]gmail.com>