OG 150

www.og150.com

Follow @theog150

CDP Prank

TABLE OF CONTENTS

CDP Prank v1.0
Author: Darren Johnson

Introduction To CDP (Cisco Discovery Protocol).

CDP (Cisco Discovery Protocol) is a proprietary Data Link Layer and Network Layer protocol developed by Cisco Systems (www.cisco.com). It is used to share information about other directly connected Cisco equipment, such as the operating system version and IP address. CDP can also be used for On-Demand Routing, however this functionality is rarely used in real life and is not investigated as part of this tutorial.

Cisco devices, such as switches and routers, send CDP announcements to the multicast destination address 01-00-0c-cc-cc-cc, out of each connected network interface. These multicast packets may be received by Cisco switches and other networking devices that support CDP into their connected network interface. By default, CDP announcements are sent every 60 seconds and the holdtime is 180 seconds (if no announcements are received from a device for a period in excess of the holdtime, the device information is discarded). Each Cisco device that supports CDP stores the information received from other devices in a table that can be viewed using the ‘show cdp neighbors’ command.

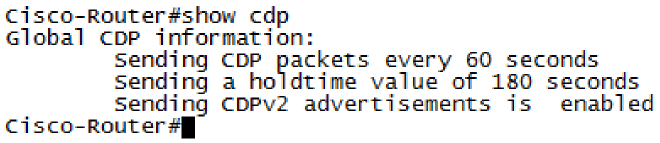
‘The CDP Prank’, Setting The Scene.....

This tutorial will use the OG150 to spoof CDP messages as a prank, however it could also be used for malicious purposes. This prank is best performed against your Network Admin or Network Support peers who maintain Cisco infrastructure devices such as routers, switches, access-points, etc. Once the OG150 is connected to the network, you will learn how to create and send CDP messages to confuse and frustrate your Network Admin or Network Support peers ☺ During my own testing, this had no adverse affect on the functionality of the Cisco infrastructure devices. This tutorial uses an extremely basic layout, a single Cisco router (hostname ‘Cisco-Router’) with an OG150 directly plugged into the routers FastEthernet0/0 interface.

Implementing The Prank.

The first task is to verify that CDP is enabled on your network infrastructure device(s). Screenshot 1 illustrates the command to do this and the output that is observed when CDP is correctly enabled. If CDP is disabled, it can be enabled using the command ‘cdp run’ in global configuration mode.

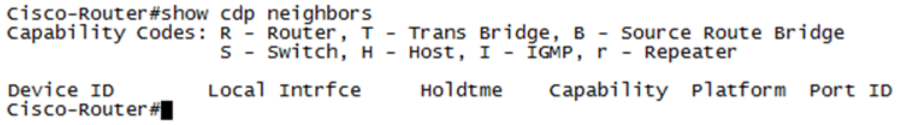
Screenshot 1 – Verify CDP is enabled on the Cisco infrastructure device(s)



```
Cisco-Router#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
Cisco-Router#
```

Next, you can check the CDP table before you start the prank. Screenshot 2 shows how this is done and you can see that there are no CDP neighbors in the CDP cache of device ‘Cisco-Router’.

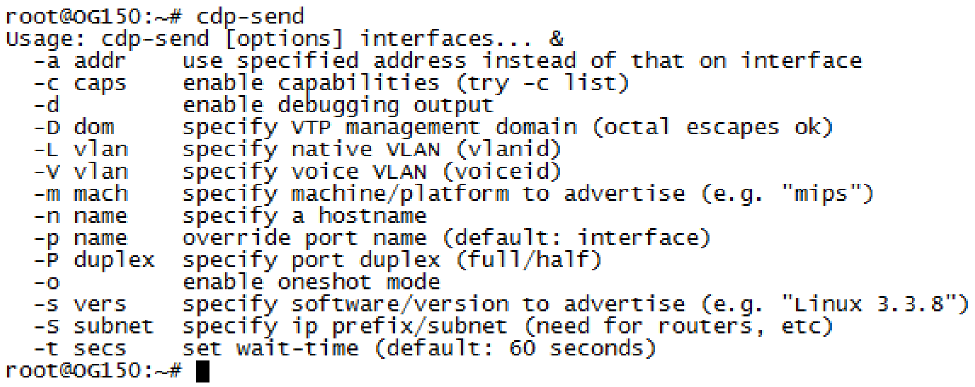
Screenshot 2 – No CDP neighbours in the existing CDP cache of device ‘Cisco-Router’



```
Cisco-Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Cisco-Router#
```

Connect to your OG150 via SSH. ‘CDP-Tools’ has been pre-installed, so you simply need to launch the program ‘cdp-send’. The options available in ‘cdp-send’ can be seen in Screenshot 3.

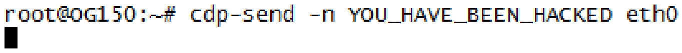
Screenshot 3 – Options available with ‘cdp-send’



```
root@OG150:~# cdp-send
Usage: cdp-send [options] interfaces... &
  -a addr    use specified address instead of that on interface
  -c caps    enable capabilities (try -c list)
  -d         enable debugging output
  -D dom     specify VTP management domain (octal escapes ok)
  -L vlan    specify native VLAN (vlanid)
  -V vlan    specify voice VLAN (voiceid)
  -m mach    specify machine/platform to advertise (e.g. "mips")
  -n name    specify a hostname
  -p name    override port name (default: interface)
  -P duplex  specify port duplex (full/half)
  -o         enable oneshot mode
  -s vers    specify software/version to advertise (e.g. "Linux 3.3.8")
  -S subnet  specify ip prefix/subnet (need for routers, etc)
  -t secs    set wait-time (default: 60 seconds)
root@OG150:~#
```

I will now demonstrate two separate ‘tests’ to demonstrate the flexibility of this tool. The first test is the most simplistic - we simply send a CDP message (out of the OG150 eth0 interface) with the hostname set to ‘YOU_HAVE_BEEN_HACKED’ as shown in Screenshot 4.

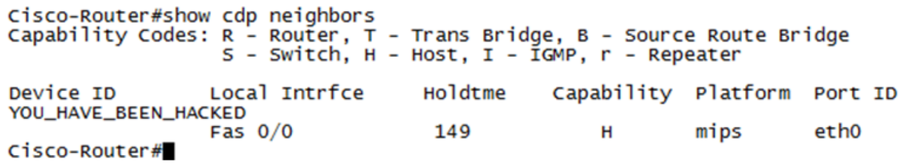
Screenshot 4 – Test#1 – spoof CDP message



```
root@OG150:~# cdp-send -n YOU_HAVE_BEEN_HACKED eth0
```

You can verify this was received correctly on your Cisco network infrastructure device as shown in Screenshot 5. At this point, you would ask your Network Admin or Network Support peer ‘what the hell is going on?’ whilst pointing at the output shown in Screenshot 5....and then sit back whilst they look at the screen in disbelief ☺ Note: To cease sending CDP messages from the OG150, enter ‘CTRL+C’.

Screenshot 5 – Test#1 – verify CDP message is displayed on device 'Cisco-Router'



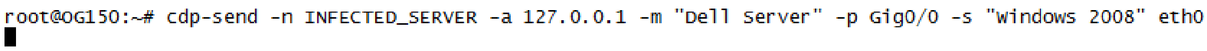
```
Cisco-Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
YOU_HAVE_BEEN_HACKED
                 Fas 0/0            149          H        mips      eth0
Cisco-Router#
```

The second test configures additional fields within the CDP message. This makes the prank look more legitimate and it should arouse further suspicion amongst your peers.......

In Screenshot 6, the OG150 will send CDP messages with the following parameters set:

- The **hostname** is set to **'INFECTED_SERVER'**
- The **IP address** set to **127.0.0.1** (this overrides the IP address of the OG150 eth0 interface which is used by default)
- The **platform** is set to **'Dell Server'**
- The **port** used by the OG150 is set to **'Gig0/0'** (this doesn't exist on the OG150, but you can set this to whatever you like)
- The **software version** is set to **'Windows 2008'**
- Finally, the command is appended with 'eth0' to instruct the OG150 to send CDP messages out its eth0 interface

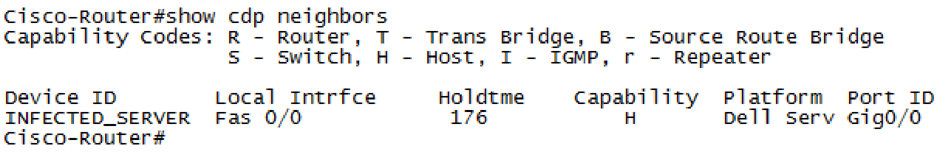
Screenshot 6 – Test#2 – spoof CDP message



```
root@OG150:~# cdp-send -n INFECTED_SERVER -a 127.0.0.1 -m "Dell Server" -p Gig0/0 -s "Windows 2008" eth0
```

As you can see in Screenshot 7, the device 'Cisco-Router' has successfully detected a CDP neighbour named 'INFECTED_SERVER'.

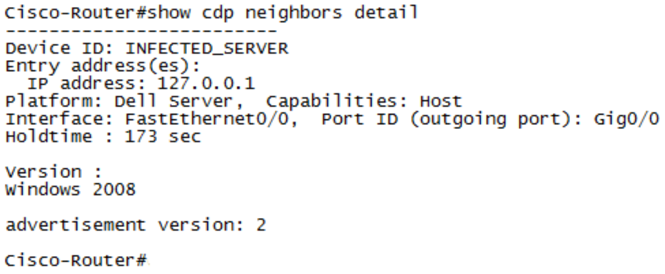
Screenshot 7 – Test#2 – verify CDP message is displayed on device 'Cisco-Router'



```
Cisco-Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
INFECTED_SERVER  Fas 0/0            176          H        Dell Serv Gig0/0
Cisco-Router#
```

Finally, we can append the keyword 'detail' to the command shown in Screenshot 7 to display additional detail about the CDP neighbour(s). Screenshot 8 confirms that the settings configured in Screenshot 6 are being correctly displayed on device 'Cisco-Router'. At this point, speak to Network Admin or Network Support – see what they say and try to keep a straight face whilst they troubleshoot ☺

Screenshot 8 – Test#2 – display additional details about CDP neighbours seen by device ‘Cisco-Router’



```
Cisco-Router#show cdp neighbors detail
-------------------------
Device ID: INFECTED_SERVER
Entry address(es):
  IP address: 127.0.0.1
Platform: Dell Server,  Capabilities: Host
Interface: FastEthernet0/0,  Port ID (outgoing port): Gig0/0
Holdtime : 173 sec

Version :
Windows 2008

advertisement version: 2

Cisco-Router#
```