Cisco CGR2010 Ports Reference

Contents

Introduction

This document describes the TCP and UDP ports that Cisco CGR2010 platform uses for applications and intranetwork communications.

Default Ports

Cisco CGR2010 has these ports enabled by default :

```
Router#show control-plane host open-ports
Active internet connections (servers and established)
Prot            Local Address              Foreign Address                Service    State
 tcp                     *:23                          *:0                 Telnet    LISTEN


Router#
```

In case that SSH is enabled in the router, port 22 is open in the CGR 2010:

```
Router#show control-plane host open-ports
Active internet connections (servers and established)
Prot Local Address Foreign Address Service State
tcp *:22 *:0 SSH-Server LISTEN
tcp *:23 *:0 Telnet LISTEN
```

Use Nmap to verify the ports that are enabled in the router.

```
C:\Program Files (x86)\Nmap>nmap -sS -p1-10000 10.31.126.137
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-06 20:05 Central Standard Time (Mexico)
Nmap scan report for 10.31.126.137
Host is up (0.0054s latency).
Not shown: 9998 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds

C:\Program Files (x86)\Nmap>
```

When a switch module is installed on the CGR2010, the router opens the ports 2003, 4003, 6003 and 9003. Take a look at the Table.

```
C:\Program Files (x86)\Nmap>nmap -sS -p1-10000 10.31.126.137
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-06 20:22 Central Standard Time (Mexico)
Nmap scan report for 10.31.126.137
Host is up (0.0067s latency).
Not shown: 9994 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
2003/tcp open finger
4003/tcp open pxc-splr-ft
6003/tcp open X11:3
9003/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 12.54 seconds

C:\Program Files (x86)\Nmap>
```

Table of Reverse Port Services

Service Name	Reserved Port Range
Normal Telnet	2000-2xxx
Raw TCP	4000-4xxx
Telnet Binary Mode	6000-6xxx
Reverse Xremote	9000-9xxx

This behavior is addressed in these
CDETS: https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsh95539