Cdp

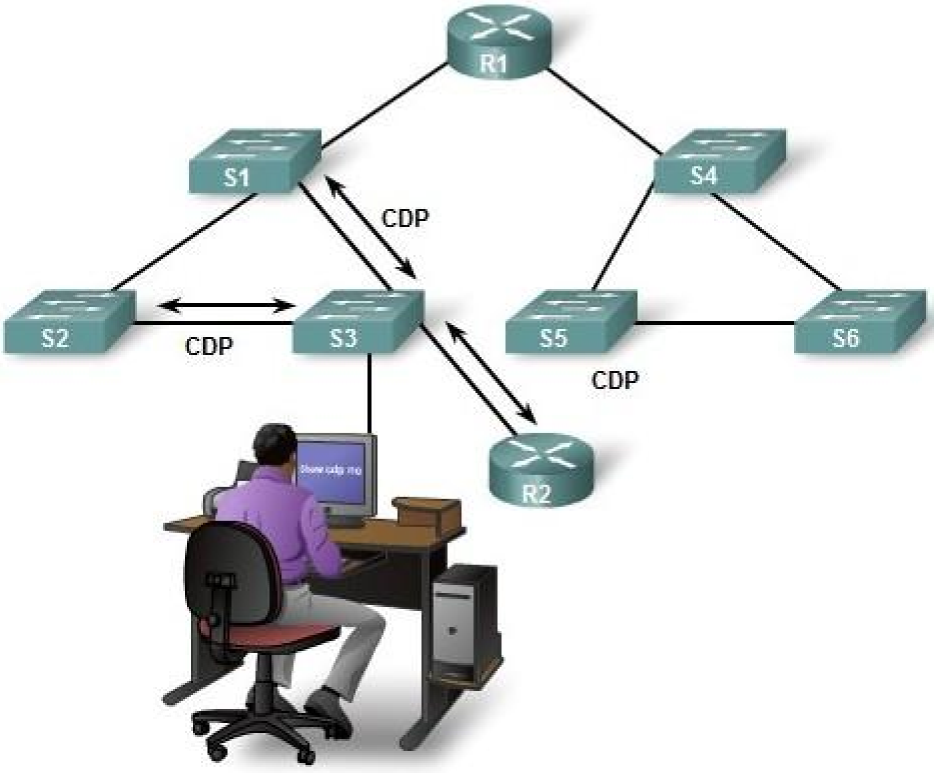
Cdp是一款可自动生成思科发现协议（CDP，Cisco Discovery Protocol）数据包的路由分析工具

一，帮助手册

```
cdp [-v] -i <接口> -m{0,1}…

洪水模式(- m0):
-n <number> 数量的数据包
-l <number> 设备id的长度
-c <char>字符来填充设备id</char>
-r 随机化设备id字符串

恶搞模式(- m1):
-D <string>     设备标识
-P <字符串>      端口id
-L <字符串>      平台
-S <字符串>      软件版本
-F <string>     IP地址

-c <功能>
    这些都是:
        R -路由器，T -跨桥，B -源路由桥
        S -开关，H -主机，I - IGMP，r -中继器
```

```
cdp [-v] -i <interface> -m {0,1} ...

Flood mode (-m 0):
-n <number>     number of packets
-l <number>     length of the device id
-c <char>       character to fill in device id
-r              randomize device id string

Spoof mode (-m 1):
-D <string>     Device id
-P <string>     Port id
-L <string>     Platform
-S <string>     Software
-F <string>     IP address
-C <capabilities>
        these are:
        R - Router, T - Trans Bridge, B - Source Route Bridge
        S - Switch, H - Host, I - IGMP, r - Repeater
```

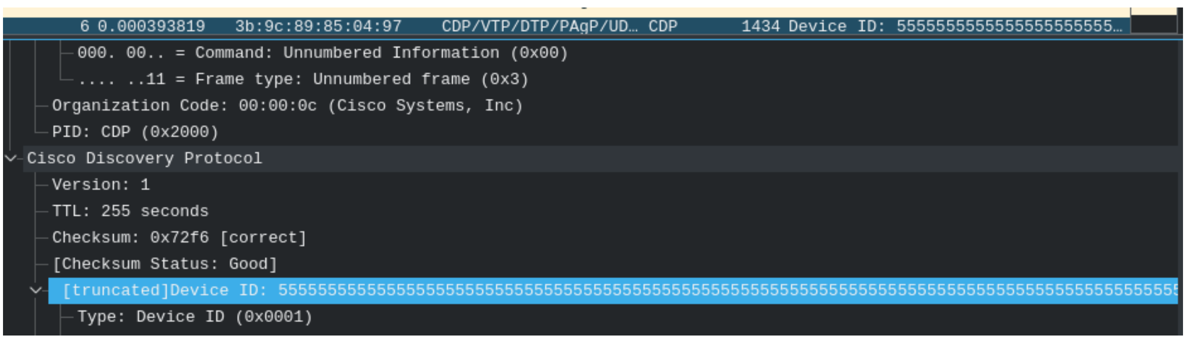
思科发现协议（CDP，Cisco Discovery Protocol）



思科发现协议（Cisco Discovery Protocol）主要用来获取相邻设备的协议地址及发现这些设备的平台。

二，命令实例

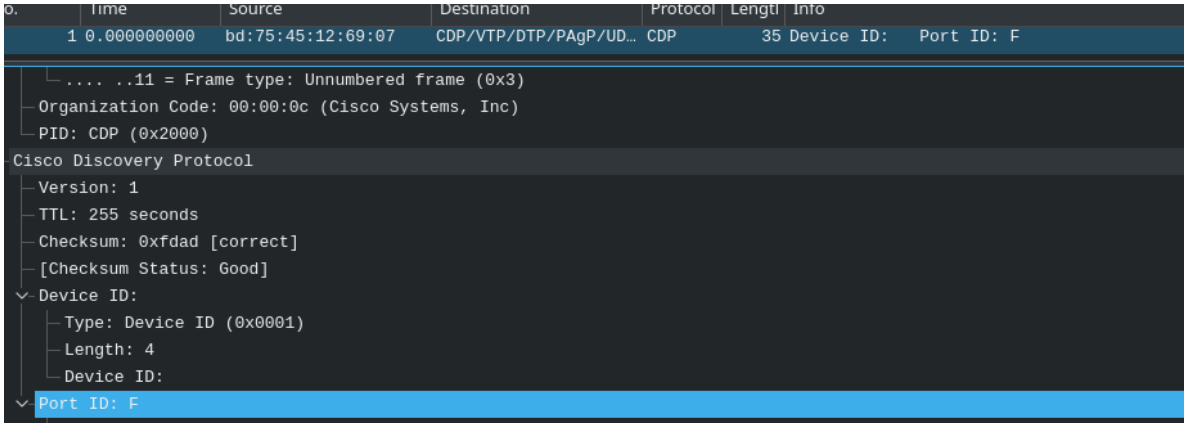
洪水模式



```
6 0.000393819   3b:9c:89:85:04:97   CDP/VTP/DTP/PAgP/UD… CDP   1434 Device ID: 5555555555555555555555…
    000. 00.. = Command: Unnumbered Information (0x00)
    .... ..11 = Frame type: Unnumbered frame (0x3)
  Organization Code: 00:00:0c (Cisco Systems, Inc)
  PID: CDP (0x2000)
Cisco Discovery Protocol
  Version: 1
  TTL: 255 seconds
  Checksum: 0x72f6 [correct]
  [Checksum Status: Good]
  [truncated]Device ID: 55555555555555555555555555555555555555555555555555555555555555555555555555555555555555555
    Type: Device ID (0x0001)
```

cdp -i vmnet8 -n 10 -c 5 -F 192.168.11.137

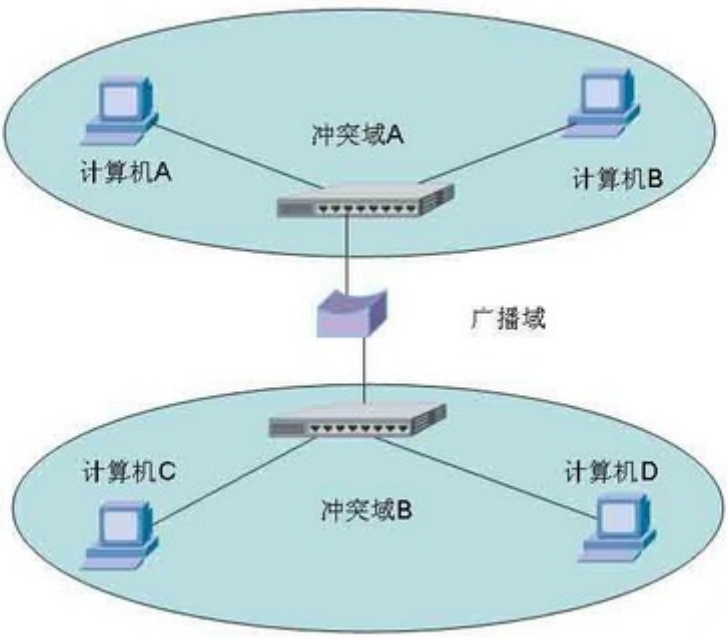
指定网卡对目标主机发送十个数据包，设备字符全部由"5"字符进行添加



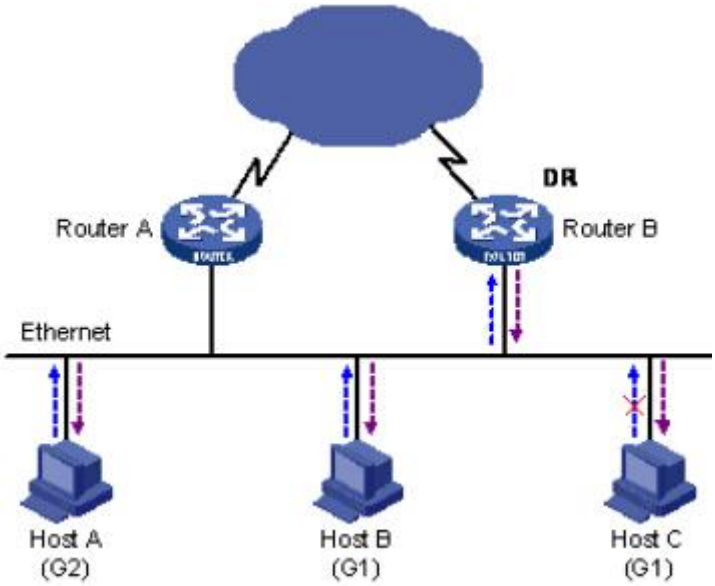
cdp -i vmnet8 -n 1 -l 1 -r -F 192.168.11.137

指定网卡为vmnet8，并指定设备ID长度为1，且随机设备ID字符串对目标发送数据包

欺骗模式（恶搞模式)



桥接（Bridging）的定义就是通过一台设备或多台设备，把几个网络串连起来而形成的连接，通过桥接来实现无路由上网的解决方案



IGMP（Internet Group Mangement Protocol）组管理协议，是因特网家族协议中的一个组播协议，主要运行在主机和组播路由器之间。通过IGMP协议通知路由器希望接收或离开某个特定的组播组的信息。

主要分为三个版本：IGMPv1、IGMPv2、IGMPv3

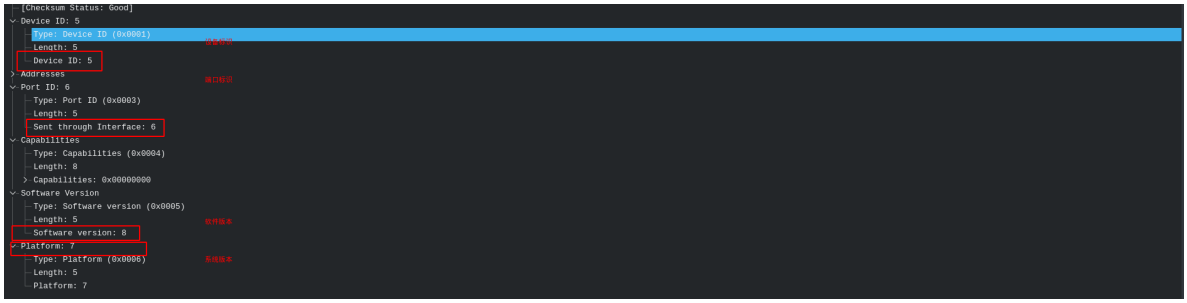
IGMP主要负责路由器之间交互信息的组播树，IGMP属于交互。是组播路由器用来维护组播成员信息的协议，运行与主机和路由器之间，IGMP封装在IP报文之中，协议号一般为2.

比如一个主机想要发送到一个特定的组播数据包、他需要监听发往那个特定组的所有数据包、为解决internet上组播路径上的选择，主机需要通知其子网中的组播路由来加入或离开一个组，而这项任务主要有IGMP来完成

中继器（RP REPEATER）

中继器，主要工作在物理层上的连接设备，主要对信号进行再生和还原的网络设备。

其作用是在局域网环境下用来延长网络距离并对线路上的信号具有放大和再生的功能，可用于扩展局域网网段长度。



cdp -i vmnet8 -m1 -D -P -C -L -S -F -D 5 -P 6 -L 7 -S 8 -F 192.168.11.137

设置设备标识为5，端口标识clear为6，系统平台为7，软件版本为8的数据包请求

> CDP有趣的地方有很多，比如 -C 命令下的功能

-c <功能>
这些都是:
R -路由器，T -跨桥，B -源路由桥
S -开关，H -主机，I - IGMP, r -中继器