Objectives:

- Explain the role of Data Link layer protocols in data transmission.
- Explain the purpose of encapsulating packets into frames to facilitate media access.

Intro:

ACME Inc. needs you again. According to the phone call, its network is behaving strangely: the network connections are extremely slow.

The Scenario:

You get to ACME office and go take a look on the server and since all the native services and ACME software are up and running, you conclude the server is not the problem. Using proper tools, you check the cabling. According to your cable tester results, the cabling is also ok.

You move up to OSI Layer 2 and go check the central switch. From the Wiring Closet's door, you notice something is wrong with the switch: all its LEDs are flashing very fast.

You connect your laptop on ACME's network and try a telnet to the switch. After a few minutes, the switch refuses the connection. Since this is unexpected, you connect your laptop to the switch's console port and the access is granted. (**Note:** Cisco IOS saves an amount of process power to the device's console session to improve troubleshooting in situations like this.)

From the switch console shell, you issue a `show process cpu` command. The output reveals 2 uncommon (and probably related) points: the switch's CPU use is over 90% and the ARP input process is the process which is creating the high CPU usage.

Since ACME's regular traffic is not enough to create such amount trouble to the Central Switch, you conclude something is wrong. Below is the command output:

Output 1: `show process cpu` output (part of the output was omitted)

```
ACMECentralSW>sh proc cpu

CPU utilization for five seconds: 95%/94%; one minute: 92%; five minutes: 91%

 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process

   1          44        43       1023  0.00%  0.00%  0.00%   0 Chunk Manager

   2          76    336978          0  0.00%  0.02%  0.02%   0 Load Meter

   3         104   1915943          0  0.00%  0.04%  0.04%   0 Spanning Tree

   4           4         2       2000  0.00%  0.00%  0.00%   0 EDDRI_MAIN
```

```
  5     1138132    200311       5681  0.00%  0.09%  0.06%   0 Check heaps
  6         208       218        954  0.00%  0.00%  0.00%   0 Pool Manager
  7           0         2          0  0.00%  0.00%  0.00%   0 Timers
  8           0     28083          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  9           0         1          0  0.00%  0.00%  0.00%   0 IPC Zone Manager
 10          12   1684880          0  0.08%  0.00%  0.00%   0 IPC Periodic Tim
 11           4   1684880          0  0.00%  0.00%  0.00%   0 IPC Deferred Por
 12           0         1          0  0.00%  0.00%  0.00%   0 IPC Seat Manager
 13           0         1          0  0.00%  0.00%  0.00%   0 IPC BackPressure
 14           0         1          0  0.00%  0.00%  0.00%   0 OIR Handler
 15           0         1          0  0.00%  0.00%  0.00%   0 Crash writer
 16           4     56164          0  0.00%  0.00%  0.00%   0 Environmental mo
 17    96943584  229384416     519236 91.24% 87.40% 88.49%  0 ARP Input
 18           0         2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
 19           4         2       2000  0.00%  0.00%  0.00%   0 AAA high-capacit
 20           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
 21           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
```

A process called ARP Input is keeping the switch really busy. This is reflected by the high processing values (over than 90%). Such high use of the switch's CPU explains why the telnet from your laptop to the switch failed and the strange switch LED behavior. Now you need to find out what is generating such high amount of traffic and leading ARP Input process to be invoked so many times?

Because the problem seems to be created by ARP Input process, you decided to check the switch's MAC Address Table.

As you know, the MAC Address Table is where a Cisco switch stores the 'MAC address/destination port' mappings, dynamically created by the switch. The `show mac-address-table` command lists all the entries stored on the MAC Address table.

Output 2: `show mac-address-table` output (part of the output was omitted)

```
ACMECentralSW#sh mac-address-table

Destination Address  Address Type  VLAN  Destination Port
```

```
----------------  -----------  ----  -------------------
0014.699d.aac8          Self          1     Vlan1
001c.2701.baba          Dynamic       1     FastEthernet0/0
003c.2711.ca02          Dynamic       1     FastEthernet0/3
00dd.2707.43df          Dynamic       1     FastEthernet0/3
00a1.edf1.ab3f          Dynamic       1     FastEthernet0/3
003c.56d4.0045          Dynamic       1     FastEthernet0/3
002e.3145.abb5          Dynamic       1     FastEthernet0/3
001d.61d2.2622          Dynamic       1     FastEthernet0/3
001a.6640.2124          Dynamic       1     FastEthernet0/3
0121.23e1.3e21          Dynamic       1     FastEthernet0/0
01c4.aae4.a851          Dynamic       1     FastEthernet0/0
004d.5532.654d          Dynamic       1     FastEthernet0/0
002b.12c5.54c1          Dynamic       1     FastEthernet0/0
001f.ac12.78d2          Dynamic       1     FastEthernet0/0
0c12.dde3.6531          Dynamic       1     FastEthernet0/0
001e.eed4.54de          Dynamic       1     FastEthernet0/3
00ed.053d.ab01          Dynamic       1     FastEthernet0/3
00c6.acde.9823          Dynamic       1     FastEthernet0/0
0b34.45d2.87de          Dynamic       1     FastEthernet0/0
001d.32ed.3ed2          Dynamic       1     FastEthernet0/0
002e.4242.82f1          Dynamic       1     FastEthernet0/0
003c.aab3.54ed          Dynamic       1     FastEthernet0/3
007f.34d1.17dc          Dynamic       1     FastEthernet0/3
004e.9a3d.432d          Dynamic       1     FastEthernet0/3
003d.65ea.12ef          Dynamic       1     FastEthernet0/3
002f.32ce.02cd          Dynamic       1     FastEthernet0/3
```

The problem:

The output shows different MAC addresses being learnt from the interfaces FastEthernet0/0 and FastEthernet0/3 but since ACME network has no more than 1 device (user PC, router or server) per switch port, you conclude something is wrong.

You go take a look on the devices connected to the mentioned ports (both user PCs). Their MAC addresses are not the same listed on the MAC Address Table of the switch. An anti-virus scan reveals a virus running on those PCs.

After a quick search on the internet, you learn more about this virus: once the computer is infected, it starts to generate millions of frames per second with fake source MAC addresses and opens a backdoor on the infected PC.

ACME Central Switch is learning different MAC address from ports FastEthernet0/0 and FastEthernet0/3 and populating the CAM table with fake information

The impact of this virus on the network is serious: The switch detects the fake-source-MAC frames and populates its CAM table with that fake information. Since millions of fake-source-MAC address frames are being sent in a short time interval and the CAM is limited in size, the switch has no opportunity to populate the CAM with a valid source MAC address frame (the frames sent by the rest of ACME network). The CAM table gets full of fake addresses (randomly generated by the virus) and because ACME Central Switch is no longer able to switch frames to their correct destination (no valid MAC/destination port present on the CAM), it sends them out to all of its ports (except the port from where the frame was received). In other words, the virus transformed ACME Central Switch in a hub.

Once the switch is acting as a hub, the backdoor function becomes clear: using the backdoor created by the virus, a malicious user could capture ACME's internal corporate traffic even though the network has a switch.

The Solution:

Once the problem is identified, your first step is to disconnect the infected computers from the network. This move ensures no more infections will take place while you clean the PCs and gives to you the opportunity to monitor the MAC Address Table on the switch. Since the virus is no longer able to send fake information to ACME's switch, the switch should eventually purge the malicious information injected into its CAM and re-learn the internal's ACME valid MACs.

Question 1:

Is there a way to configure a Cisco Switch in order to avoid this kind of attack? Explain.

Answers

Q1. Yes. The answer should vary around the Switch Port Security features.