L2 Operation: Other Protocols

Blocking unknown unicast/multicast frames

Unfortunately the following will not work in Packet Tracer. These commands are supported on some switches.

Remember how the switch treats its switching table: if it finds the destination address of a frame in the table, then it forwards the frame to the port listed in the table. If it doesn't find it in the table, it floods the frame in a similar way to broadcast. However, this is not desirable in certain circumstances – for security reasons. That's why it's common in some companies to set up unknown unicast blocking on access ports:

```
interface range ….
       switchport block unicast
```

If a frame with an unknown destination address arrives on such a port, it will be discarded. What do you think, what are the implications for network traffic? And what happens when someone tries to attack the MAC table? What exactly can this setup be good for?

Switch does not only have a unicast MAC address table, it also has a multicast MAC address table, which is treated quite similarly, including flooding of unknown MACs. We can also block unknown traffic here:

```
interface range ….
       switchport block multicast
```

Both settings can be made on the same port. To cancel, just put "no" before the command.

How to check the settings:

```
sh int … switchport
sh run | section interface …
```

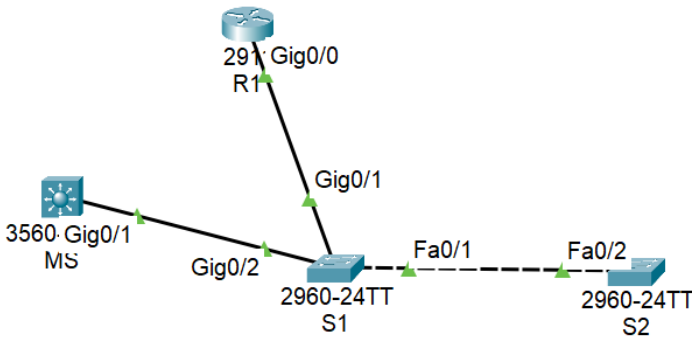
The flood blocking setting is independent of VLANs and applies to all VLANs configured on the port.

Try blocking unicast and multicast flooding on some of the switches.

CDP

This somewhat "chatty" protocol allows Cisco devices to introduce themselves to each other. Its open equivalent is LLDP, supported on devices from various manufacturers.

Create a computer network as shown, including device types, naming and connections on specific ports. Set the IP address 10.0.0.1/8 on router R1 and 172.16.0.1/16 on switch SM.



On the switch, try:

```
sh cdp neighbors    ; do  devices already communicated the changes?
sh cdp entry R1
sh cdp entry *      ; * means all neighbours
```

If we made the last change to the name setting, the switch may see the older name for a while, then even both names for a while (two devices on the same port). Try the command with the entry subcommand on the other device as well.

```
sh cdp interface g0/2     ; timers etc.
```

Also, there is a subcommand that we can't try in Packet Tracer:

```
sh cdp traffic
```

Enable/disable CDP on the whole device – in the global config mode:

```
cdp run
no cdp run
```

Enabling/disabling CDP on the port:

```
cdp enable
no cdp enable
```

Shut down CDP on the switch centrally, check what the corresponding show command says. Then enable it, check the CDP state.

Turn off CDP on the port g0/2 (the router is connected to) and check again, including neighbours. Take into account that there will be some delay.

LLDP

Similar commands for LLDP (an open variant to CDP supported by various vendors):

```
sh lldp
sh lldp neighbors          ; or other variants
lldp run                   ; enabling LLDP on the entire device in the global config
no lldp run                ; disabling…
int f0/1
       lldp receive        ; enabling for one interface, disabling with „no“
       lldp transmit       ; each direction is switched on/off separately
```

LLDP is disabled by default on Cisco devices. Turn it on sequentially on all devices on the network, see what variants of the show command are supported, and look at the output format.

CDP and LLDP communication

CDP multicast address

CDP frames are sent to the target multicast MAC address `01-00-0C-CC-CC-CC`.

Cisco uses `01-00-0C-CC-CC-CC` for multiple purposes (CDP, VTP, DTP,…), inside the LLC/SNAP frame there is the sequence 00:00:0C as the OUI (= Cisco OUI), instead of EtherType there is an identifier of the proper protocol, and inside the LLC/SNAP frame there is a CDP, VTP or other proprietary frame.

The new designation for OUI is MA-L (MAC Address Block Large). These assigned IDs are here:

https://standards-oui.ieee.org/oui/oui.txt

Find the listed OUI from Cisco on this website.

On packetlife.net, find a suitable CDP frame and look at the structure of the frame. Compare it to an LLDP frame (ideally select the LLDP_and_CDP.cap file where both types are present). Next, find a DTP frame and compare.

CDP Spoofing:

This is done by attacker sending CDP frames with the target multicast MAC address `01-00-0C-CC-CC-CC`, the source address is usually spoofed.

If the device cannot defend itself, the only protection is to disable CDP on those ports where there are no "trusted" devices such as switches, routers, etc., especially on access ports.