Experimental report

Experiment name: Experiment 3.3.1: Broadcast storm and MAC address table shock analysis

College: Beijing Institute of Technology

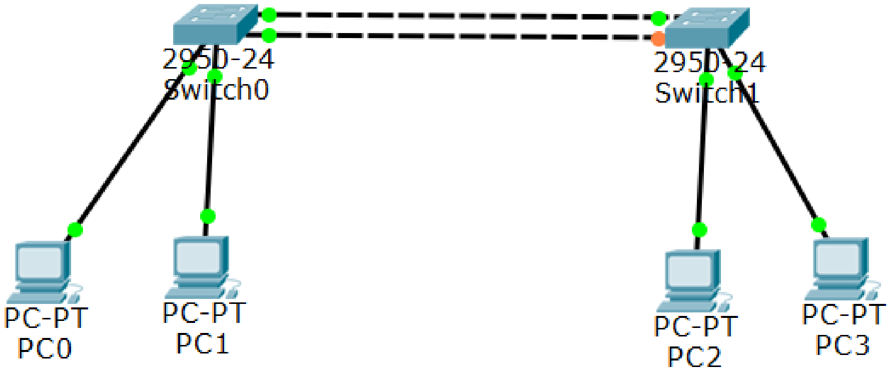
Class: Computer Networks

Student ID: 1820243077

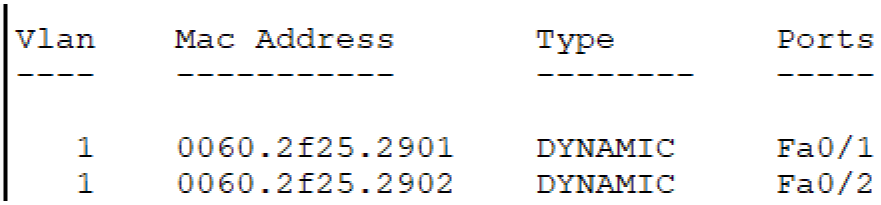
Name: Pimenov Gleb

1. Topology

Topology made with Cisco Packet Tracer (simulations are also conducted through this program)

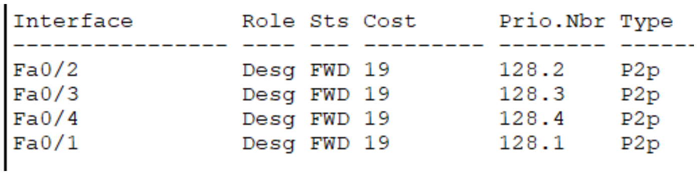


2. Switch 1 MAC address table



```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2f25.2901    DYNAMIC     Fa0/1
   1    0060.2f25.2902    DYNAMIC     Fa0/2
```

3. Switch 1 information
   Spanning tree info:

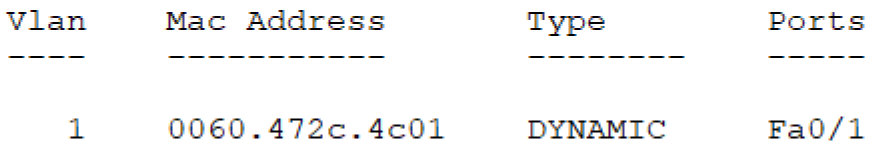


```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/1            Desg FWD 19        128.1    P2p
```

Other info:

Switch Interface	Destination Mac-address	Destination Interface
Fa 0/1	0001.c74e.eb47	Fa 0/1
Fa 0/2	0001.c74e.eb47	Fa 0/2
Fa 0/3	000A.F3ED.4D76	Fa 0
Fa 0/4	0010.11DD.9B4D	Fa 0

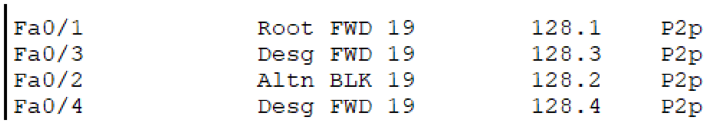
4. Switch 2 MAC address table



```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.472c.4c01    DYNAMIC     Fa0/1
```

5. Switch 2 information

Spanning tree info:



```
Fa0/1            Root FWD 19         128.1    P2p
Fa0/3            Desg FWD 19         128.3    P2p
Fa0/2            Altn BLK 19         128.2    P2p
Fa0/4            Desg FWD 19         128.4    P2p
```

Other info:

Switch Interface	Destination Mac-address	Destination Interface
Fa 0/1	0000.0cbd.39dc	Fa 0/1
Fa 0/2	0000.0cbd.39dc	Fa 0/2
Fa 0/3	0001.428A.EDE5	Fa 0
Fa 0/4	0002.1631.3C24	Fa 0

Root: The Root role is assigned to the port on the root bridge itself. This port is responsible for forwarding traffic towards the root bridge.

Designated (Desg): The Designated role is assigned to the port that has been elected as the designated port for its segment. The designated port is responsible for forwarding traffic towards the root bridge for that segment.

Alternate (Alt): The Alternate role is assigned to backup ports that are in a blocking state but can quickly take over forwarding duties if the designated port fails.

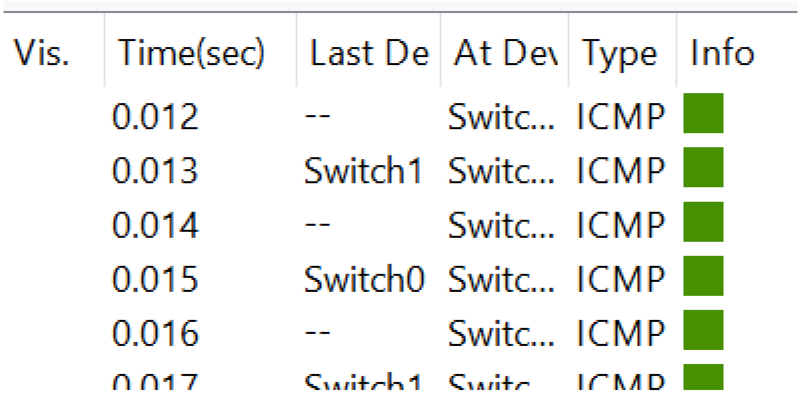
Backup (Backup): The Backup role is assigned to redundant ports that are in a blocking state. These ports are available to take over forwarding duties if the designated port fails, but they do not participate actively in forwarding traffic under normal conditions.

Disabled: The Disabled role is assigned to ports that have been manually disabled or administratively shut down. These ports do not participate in the spanning tree algorithm and do not forward traffic.

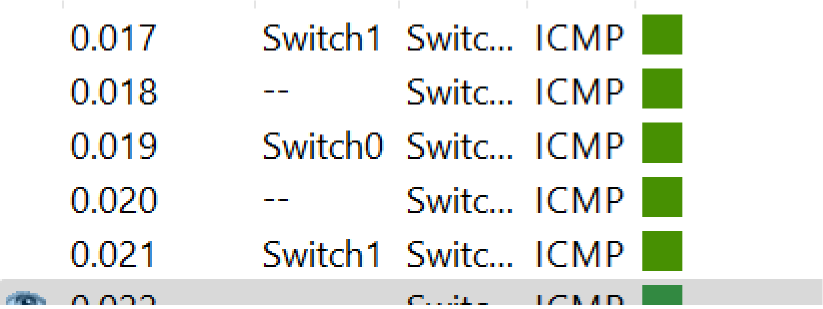
6. Broadcast Storm

To start broadcast storm, we need to disable STP in both switches: no spanning-tree vlan <vlan_id>

As we can see here, after PC1 pings PC4, packet of information went into the loop



Vis.	Time(sec)	Last De	At Dev	Type	Info
	0.012	--	Switc...	ICMP	🟩
	0.013	Switch1	Switc...	ICMP	🟩
	0.014	--	Switc...	ICMP	🟩
	0.015	Switch0	Switc...	ICMP	🟩
	0.016	--	Switc...	ICMP	🟩
	0.017	Switch1	Switc	ICMP	🟩

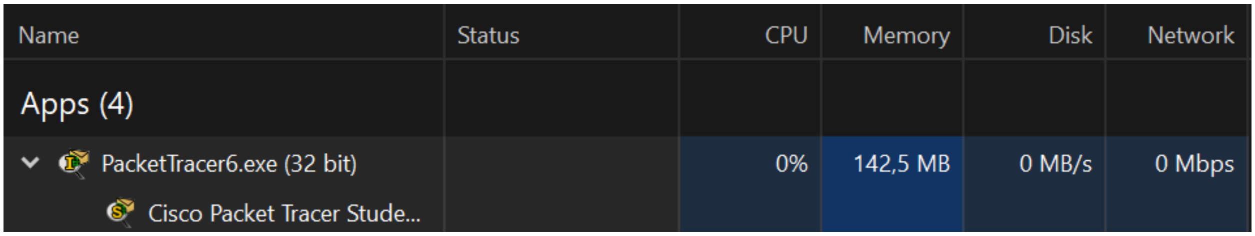


	0.017	Switch1	Switc...	ICMP	🟩
	0.018	--	Switc...	ICMP	🟩
	0.019	Switch0	Switc...	ICMP	🟩
	0.020	--	Switc...	ICMP	🟩
	0.021	Switch1	Switc...	ICMP	🟩
	0.022		Switc	ICMP	🟩

7. Utilization Rate

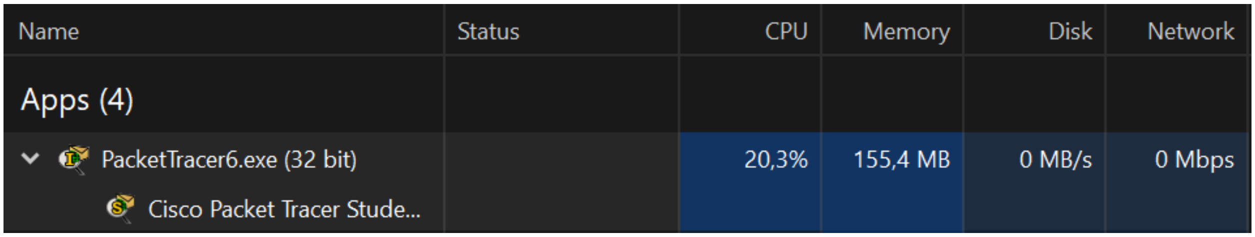
Cisco packet tracer does not provide information about Switch CPU utilization, but we can say that it increased because of increasing utilization of the Cisco Packet Tracer Application in windows

Without broadcast storm



Name	Status	CPU	Memory	Disk	Network
Apps (4)					
PacketTracer6.exe (32 bit)		0%	142,5 MB	0 MB/s	0 Mbps
Cisco Packet Tracer Stude...					

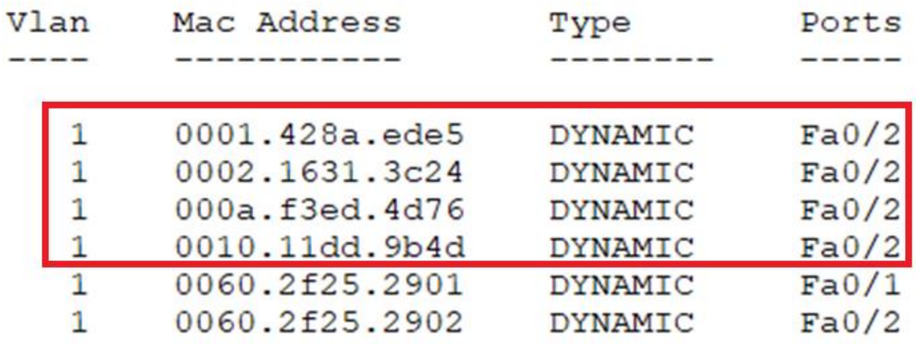
With broadcast storm



Name	Status	CPU	Memory	Disk	Network
Apps (4)					
PacketTracer6.exe (32 bit)		20,3%	155,4 MB	0 MB/s	0 Mbps
Cisco Packet Tracer Stude...					

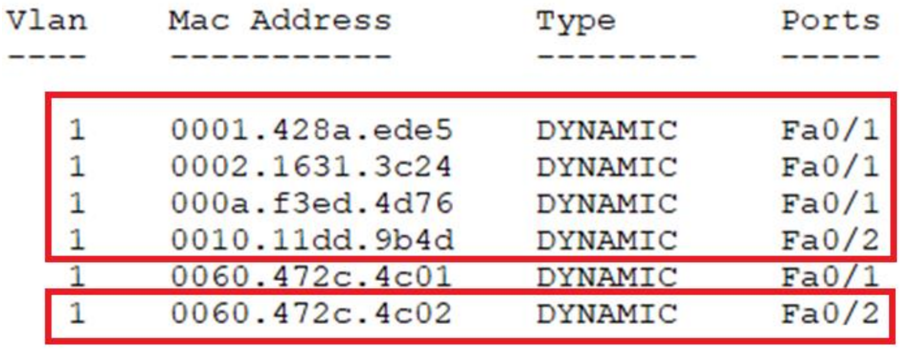
8. Switch 1 Mac-address table after broadcast storm

Red square – new ones



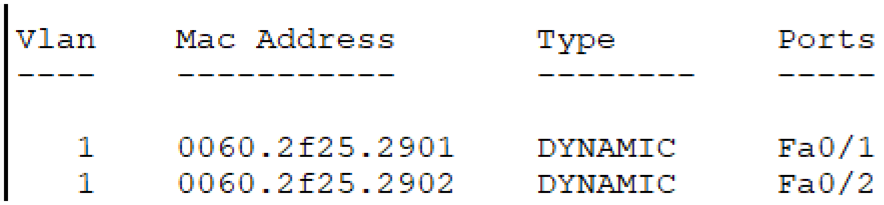
```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.428a.ede5    DYNAMIC     Fa0/2
   1    0002.1631.3c24    DYNAMIC     Fa0/2
   1    000a.f3ed.4d76    DYNAMIC     Fa0/2
   1    0010.11dd.9b4d    DYNAMIC     Fa0/2
   1    0060.2f25.2901    DYNAMIC     Fa0/1
   1    0060.2f25.2902    DYNAMIC     Fa0/2
```

9. Switch 2 Mac-address table after broadcast storm

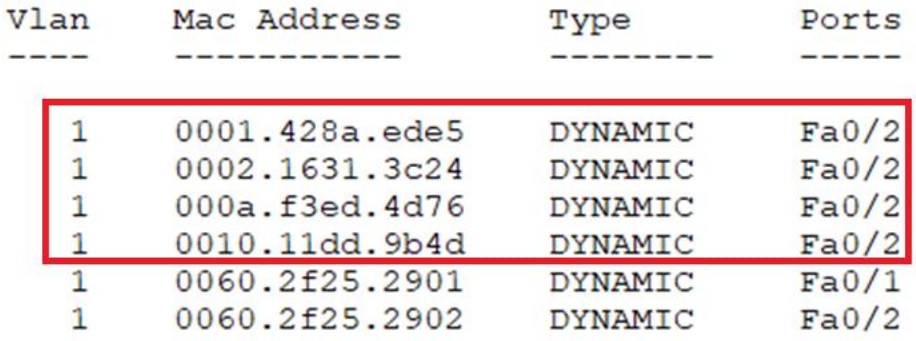


```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.428a.ede5    DYNAMIC     Fa0/1
   1    0002.1631.3c24    DYNAMIC     Fa0/1
   1    000a.f3ed.4d76    DYNAMIC     Fa0/1
   1    0010.11dd.9b4d    DYNAMIC     Fa0/2
   1    0060.472c.4c01    DYNAMIC     Fa0/1
   1    0060.472c.4c02    DYNAMIC     Fa0/2
```

10. Comparison of Switch 1 Mac-address tables before/after broadcast storm

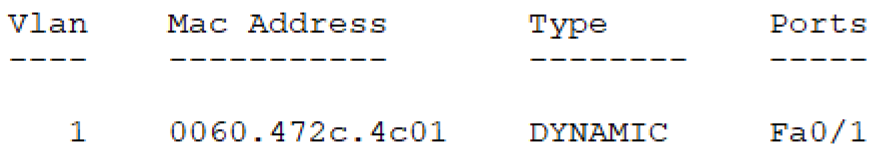


```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2f25.2901    DYNAMIC     Fa0/1
   1    0060.2f25.2902    DYNAMIC     Fa0/2
```

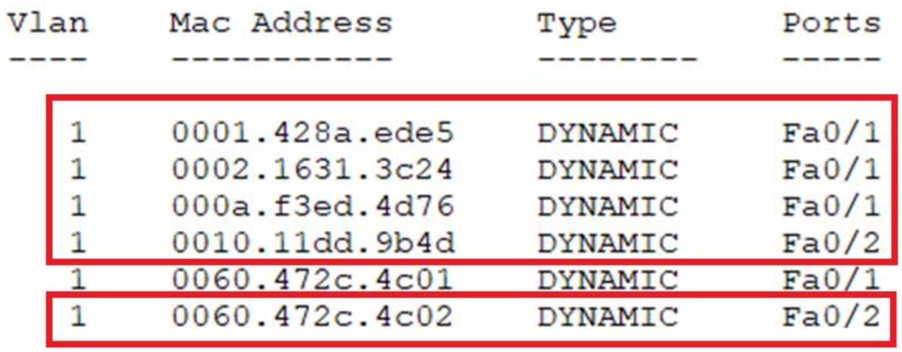


```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.428a.ede5    DYNAMIC     Fa0/2
   1    0002.1631.3c24    DYNAMIC     Fa0/2
   1    000a.f3ed.4d76    DYNAMIC     Fa0/2
   1    0010.11dd.9b4d    DYNAMIC     Fa0/2
   1    0060.2f25.2901    DYNAMIC     Fa0/1
   1    0060.2f25.2902    DYNAMIC     Fa0/2
```

11. Comparison of Switch 2 Mac-address tables before/after broadcast storm



```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.472c.4c01    DYNAMIC     Fa0/1
```



```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  1     0001.428a.ede5    DYNAMIC     Fa0/1
  1     0002.1631.3c24    DYNAMIC     Fa0/1
  1     000a.f3ed.4d76    DYNAMIC     Fa0/1
  1     0010.11dd.9b4d    DYNAMIC     Fa0/2
  1     0060.472c.4c01    DYNAMIC     Fa0/1
  1     0060.472c.4c02    DYNAMIC     Fa0/2
```

12. How to stop or eliminate the current broadcast storm?

Identify the Source: Use network monitoring tools to identify the source or sources of the broadcast storm. Look for devices or ports that are generating an unusually high amount of broadcast traffic.

Isolate the Affected Segment: Once you've identified the source of the broadcast storm, isolate the affected segment by shutting down or disconnecting the port or device causing the storm. This will prevent the broadcast traffic from spreading further across the network.

Implement Broadcast Storm Control: If your switches support it, configure broadcast storm control to automatically detect and mitigate excessive broadcast traffic. This feature can help prevent broadcast storms from occurring in the first place and limit their impact if they do occur.

Review and Optimize Network Design: After mitigating the immediate threat, review your network design to identify any underlying issues that may have contributed to the broadcast storm. Optimize your network design to minimize the risk of future broadcast storms, such as by implementing hierarchical design, optimizing spanning tree protocol (STP), and segmenting VLANs.

Regularly Monitor and Maintain the Network: Implement proactive network monitoring and maintenance practices to detect and prevent broadcast storms and other network issues before they escalate. Regularly audit network configurations, monitor network traffic, and conduct periodic security assessments to ensure the ongoing stability and reliability of your network.

13. What are the technical solutions to reduce or prevent such loops caused by configuration errors?

Spanning Tree Protocol (STP): Implement STP to prevent loops by blocking redundant paths in the network topology.

Port Security: Configure port security to restrict the number of MAC addresses allowed on a port, preventing unauthorized devices from causing loops.

VLAN Segmentation: Segment the network into VLANs to limit the scope of broadcast traffic and reduce the likelihood of loops affecting the entire network.

Loop Prevention Mechanisms: Use loop prevention mechanisms such as BPDU guard, loop guard, and root guard to detect and prevent loops in the network.

Optimized Network Design: Design the network with redundancy and resilience in mind, avoiding configurations that can lead to loops and ensuring proper VLAN and STP configurations.

Regular Audits and Monitoring: Regularly audit network configurations and monitor network traffic to identify and correct any misconfigurations or errors that could lead to loops.