Switch Loop (Broadcast Storm) Problem

Problem Description

Switch loop is an uncontrolled data flow problem that occurs when two or more switches in a network topology are interconnected by multiple physical links (cables). This structure causes Ethernet frames to continuously traverse the network and Layer 2 broadcast traffic to grow cyclically. Since the switches forward broadcast packets to all ports to learn their MAC addresses, these packets endlessly re-circulate when the loop occurs. Although this is not a physical error, the effect is extremely destructive because:

-Broadcast storm occurs: The same broadcast packet repeats continuously within the network.

-Switches cannot fill MAC address tables, they constantly delete and rewrite addresses.

-CPU and memory resources are overused, the switch becomes unmanageable.

Basic protocols such as CMP, DHCP do not work, devices cannot receive IP and cannot reach each other.

-Network traffic is locked: No pinging, file sharing stops, VoIP calls are interrupted.

Main cause: If Spanning Tree Protocol (STP) is not active on the network or is not configured properly, this loop will not break on its own. Switches cannot block loops naturally, because the Ethernet protocol does not carry a TTL (Time To Live) value to detect loops. This indicates a problem at Layer 2, not Layer 3.

As stated in my interview with an expert, "All devices connected to the switch froze, they could not receive IP, the lights were flashing but there was no internet" is a classic broadcast storm symptom. Even if the physical connection is active, functional network communication has not been achieved because data traffic is looped.

Switch loop is not a cyber attack, it is usually caused by network configuration error or unconscious physical connections, not a direct malicious action.

It is especially common in the following cases:

-If multiple switches in the network are physically connected to each other with multiple cables,

-If Spanning Tree Protocol (STP) is not enabled or is configured incorrectly,

-If users unconsciously combine switch ports with cross cabling,

This inevitably leads to a loop. This leads to non-stop looping of Layer 2 broadcast traffic and ultimately to the network becoming unusable.

OSI Layer: Layer 2

Signs of Detection (Symptoms)

-All port LEDs on the switch blink synchronously and rapidly: This indicates that a broadcast packet is being transmitted continuously over all ports of the switch. Broadcast storm has occurred.

-Ping commands remain unanswered (Request timed out): Packets cannot reach the destination or replies cannot be returned due to the loop. In-network ICMP packets enter an infinite loop.

-No IP can be received from the DHCP server: DHCPDISCOVER packets are lost in the loop, cannot reach the server, or responses cannot return to the client.

-Switch and router interfaces become inaccessible: Management traffic (e.g. telnet/SSH/HTTP) is overwhelmed by broadcast traffic. The switch or router cannot respond.

-All clients on the network lose connection or become very slow: Heavy traffic at Layer 2 paralyses data exchange. Upper layer services (DNS, web access, file sharing) become inoperable.

-If STP (Spanning Tree Protocol) is not activated, the loop is permanent: Only protocols such as STP can detect and break the loop. If disabled, the loop will not terminate without manual intervention.

Cause of Problem

The main reasons are the following:

-STP (Spanning Tree Protocol) is disabled or not configured at all: Switches cannot close alternate paths if the STP protocol, the loop prevention mechanism, is not active. In this case, the same MAC address starts to appear on more than one port and a loop occurs.

-Wrong cabling has been done: Multiple cables were pulled between the same two switches, but these connections were not filtered at Layer 2 level.

-Unconsciously combining trunk or access ports**:** Physically connecting two access ports without trunk configuration can also cause a switch loop. Unconscious connections made by end users pose a danger.

-The STP feature of the switch is turned off by default (some models): Some Layer 2 switch models may have STP disabled by default. In this case, manual activation is required.

-Incorrect VLAN configuration (VLAN STP instance separation) even if STP is configured: If STP is disabled on different VLANs over the same physical link, each VLAN can have its own loop.

Admin Guide - Solution and Precautionary Steps

Step 1: STP (Spanning Tree Protocol) feature should be activated. STP determines the most appropriate path by analysing redundant connections between switches to prevent loop formation and automatically closes connections that can create loops.

```
Switch(config)# spanning-tree vlan 1
```

Note: If STP is to be enabled for all VLANs, global configuration must be done.

Step 2: With PortFast, the STP time on end device ports should be shortened. It is used to disable unnecessary STP calculation on ports connected to end devices (e.g. computer, printer).

```
Switch(config)# interface fa0/1
```

```
Switch(config-if)# spanning-tree portfast
```

Warning: **PortFast should not be used** on ports used between two switches, because it makes them open to looping.

Step3 : Detect physical connections with loop and disconnect temporarily. Very fast flashing of LEDs on the switch or simultaneous data movement on all ports indicates the possibility of loop. In this case:

-Physical cable connections must be visually checked.

-If there is an unnecessary double connection, the cable must be removed.

At least one connection must be cancelled until -STP is activated.

Step 4: Enable Broadcast Storm control. It is used to prevent broadcast traffic from exceeding a certain threshold value. Broadcasts above the specified rate are blocked even in the loop state:

```
Switch(config)# interface range fa0/1 - 24
Switch(config-if-range)# storm-control broadcast level 5.00
```

Step 5: Review the VLAN-based STP configuration. If there are multiple VLANs, the STP instance for each VLAN may be separate. In this case, it is not enough to apply STP only to VLAN 1. It can be done as follows:

```
Switch(config)# spanning-tree vlan 10
Switch(config)# spanning-tree vlan 20
```

Result: Thanks to these steps, physical loops are automatically detected and interrupted. Network-wide broadcast storm is prevented, CPU overload and connection interruptions are prevented.

Technical Note:

STP is not turned on by default in the Cisco Packet Tracer environment. However, it can be activated manually. A double connection can be made between two switches to create a loop.

Simulation

Simulation: Loop demonstration will be performed without activating STP by establishing a double connection between two switches.

Necessary Devices:

2 pcs switch (2950-24)

2 computers (PC0 and PC1)

Cabling Process (Loop will be created)

Switch - Switch Connection (2 lines for LOOP)

Switch0 - FastEthernet0/1 → Switch1 - FastEthernet0/1

Switch0 - FastEthernet0/2 → Switch1 - FastEthernet0/2

This double connection will form the Switch Loop.

Computer - Switch Connections

PC0 - FastEthernet0 → Switch0 - FastEthernet0/3

PC1 - FastEthernet0 → Switch1 - FastEthernet0/3

Make the following settings for PC0 and PC1:

PC0

IP: 192.168.1.10

Subnet Mask: 255.255.255.0

PC1

IP: 192.168.1.11

Subnet Mask: 255.255.255.0

Purpose of Simulation:

To observe the broadcast storm and network collapse caused by the physical loop occurring at Layer 2 (Data Link Layer).

Switch Loop Simulation Report

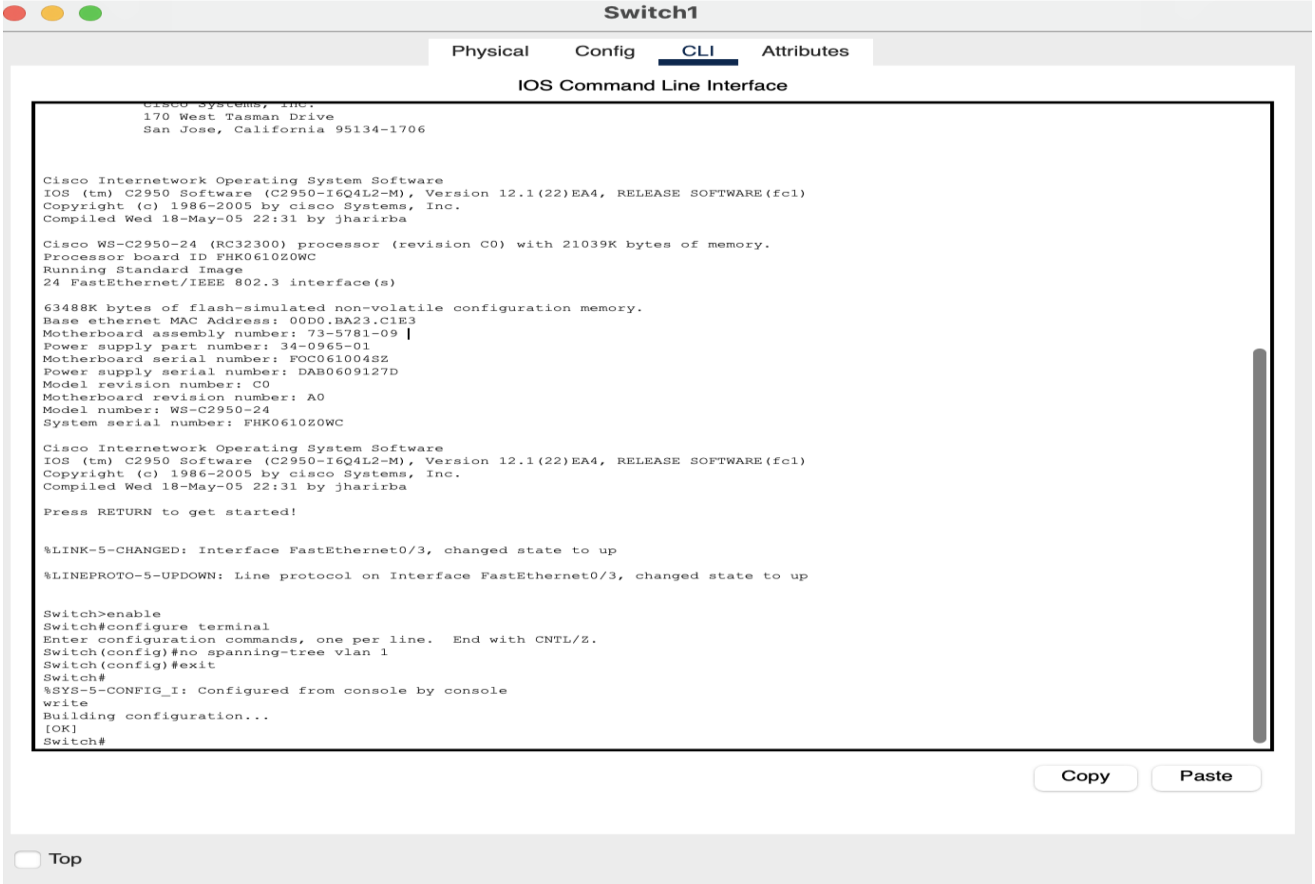
Physical Structure

In the simulation, 2 Cisco 2950-24 Switches (Switch0 and Switch1) and 2 PCs (PC0 and PC1) were used.

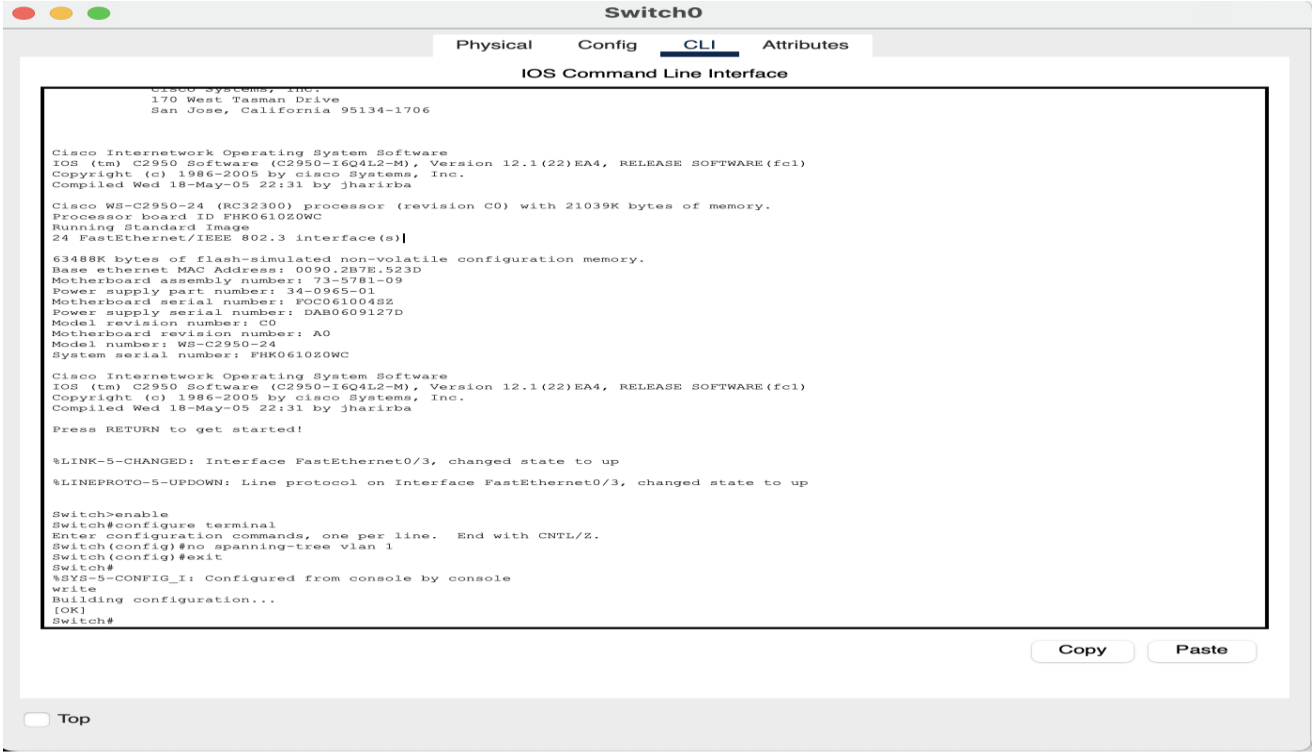
Two redundant connections are made between the switches. This structure creates a physical loop at Layer 2.

Initially all connections appear green; STP (Spanning Tree Protocol) has not yet been disabled.

Disabling STP - Occurrence of Error Source



```
            Cisco Systems, Inc.
            170 West Tasman Drive
            San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00D0.BA23.C1E3
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no spanning-tree vlan 1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
Switch#
```



```
            Cisco Systems, Inc.
            170 West Tasman Drive
            San Jose, California 95134-1706


Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0090.2B7E.523D
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no spanning-tree vlan 1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
Switch#
```

STP protocol is disabled on both switches:

Switch> enable

Switch# configure terminal

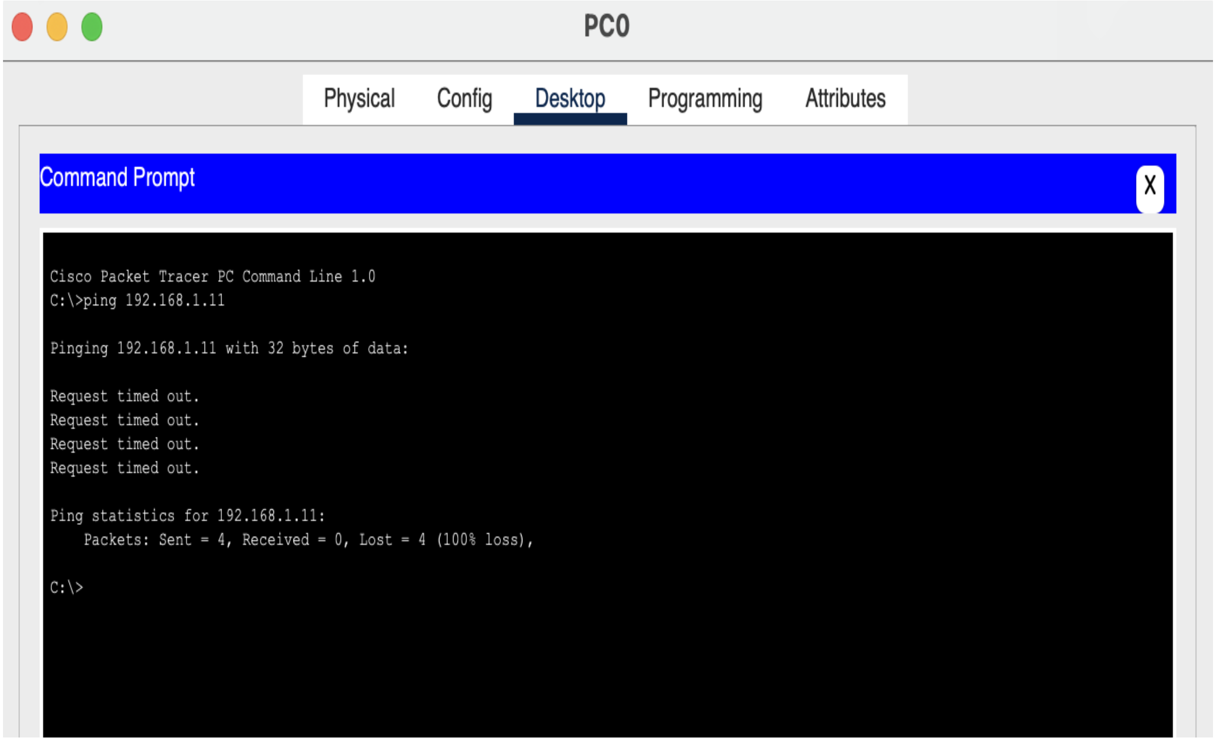
Switch(config)# no spanning-tree vlan 1

Switch(config)# exit

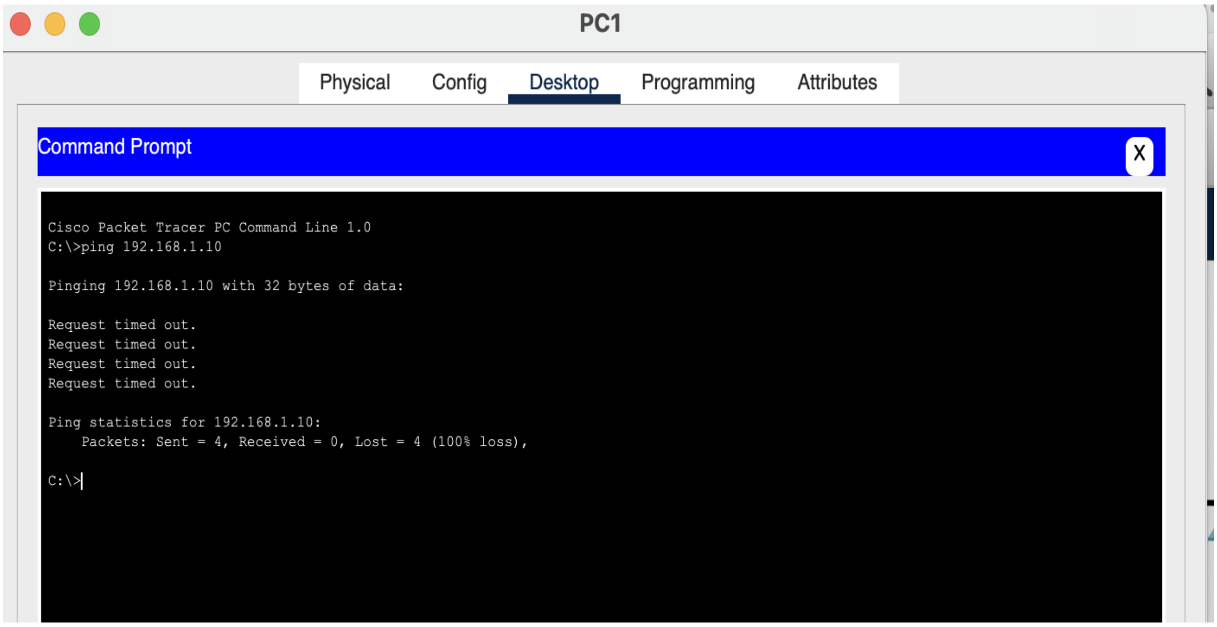
Switch# write

When STP is switched off, switches become unable to detect and block the loop.

Ping Failure - Unable to Establish Connection



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

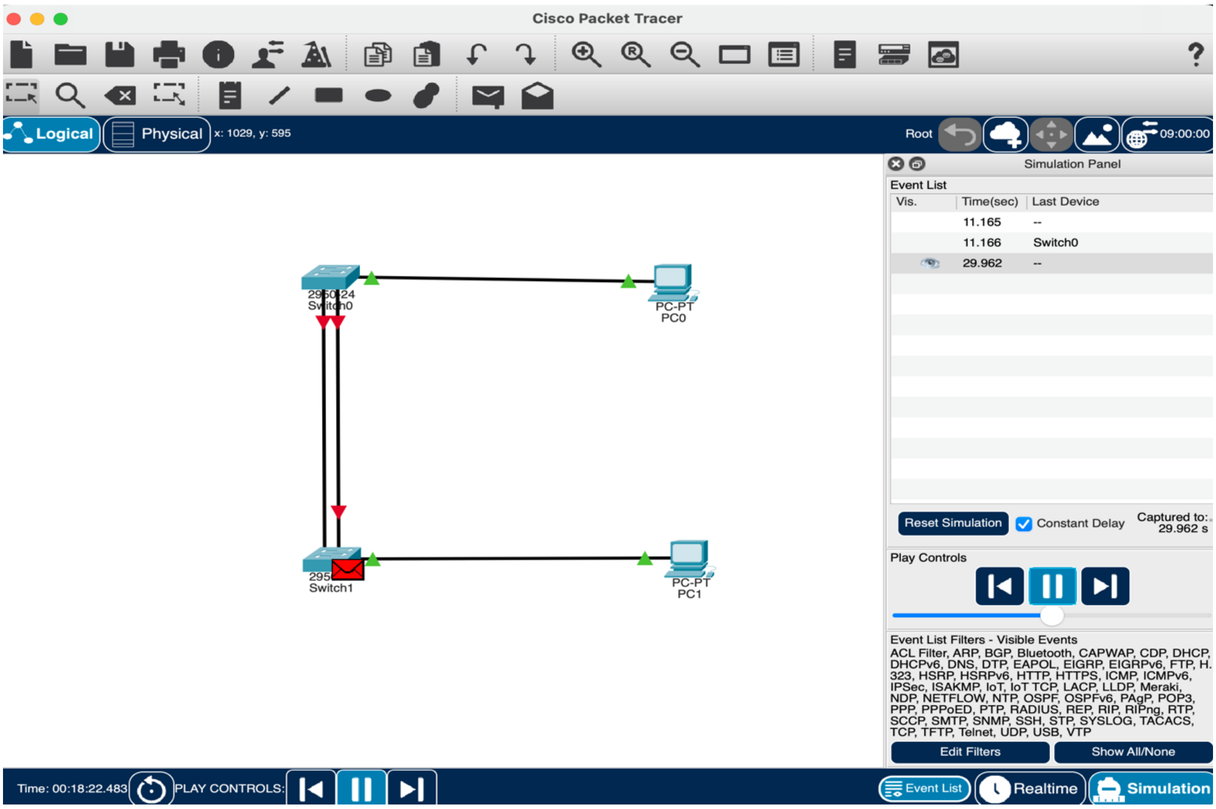


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

When PC0 and PC1 tried to ping each other, 100% packet loss occurred.

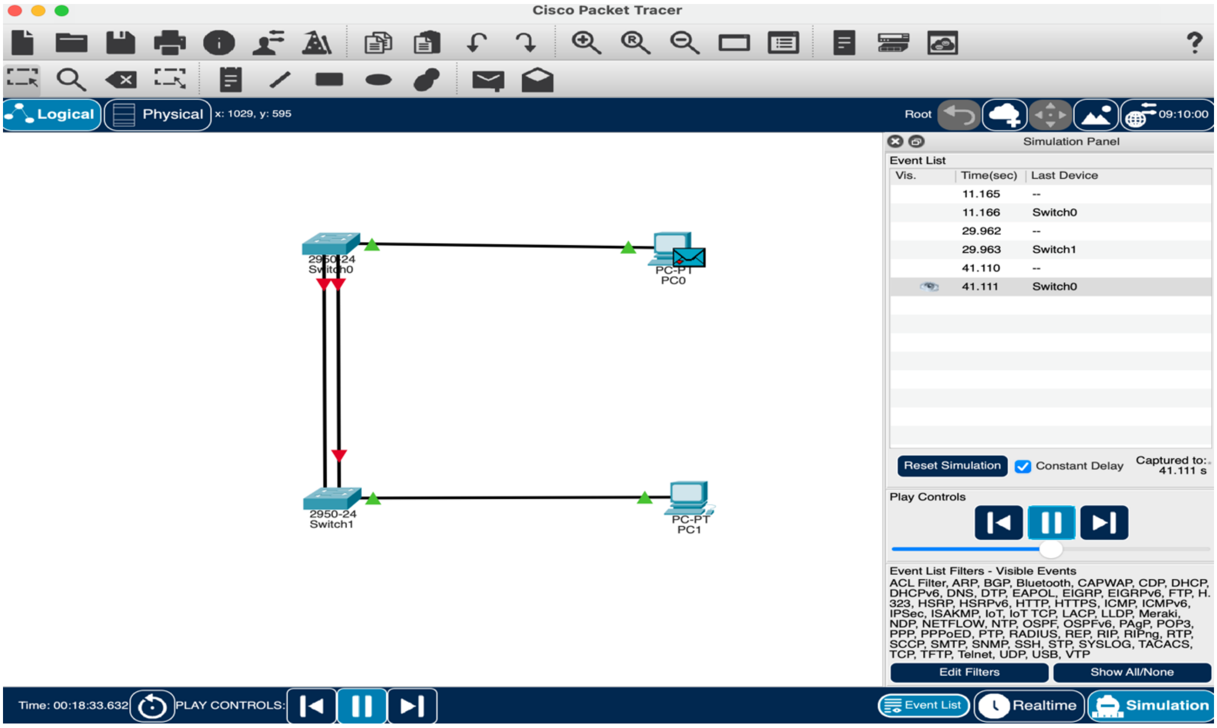
This indicates that ICMP packets cannot reach the network due to the loop and the broadcast is continuously rotating.

Broadcast Storm - Visual Signs of Loop:



Vis.	Time(sec)	Last Device
	11.165	--
	11.166	Switch0
	29.962	--

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

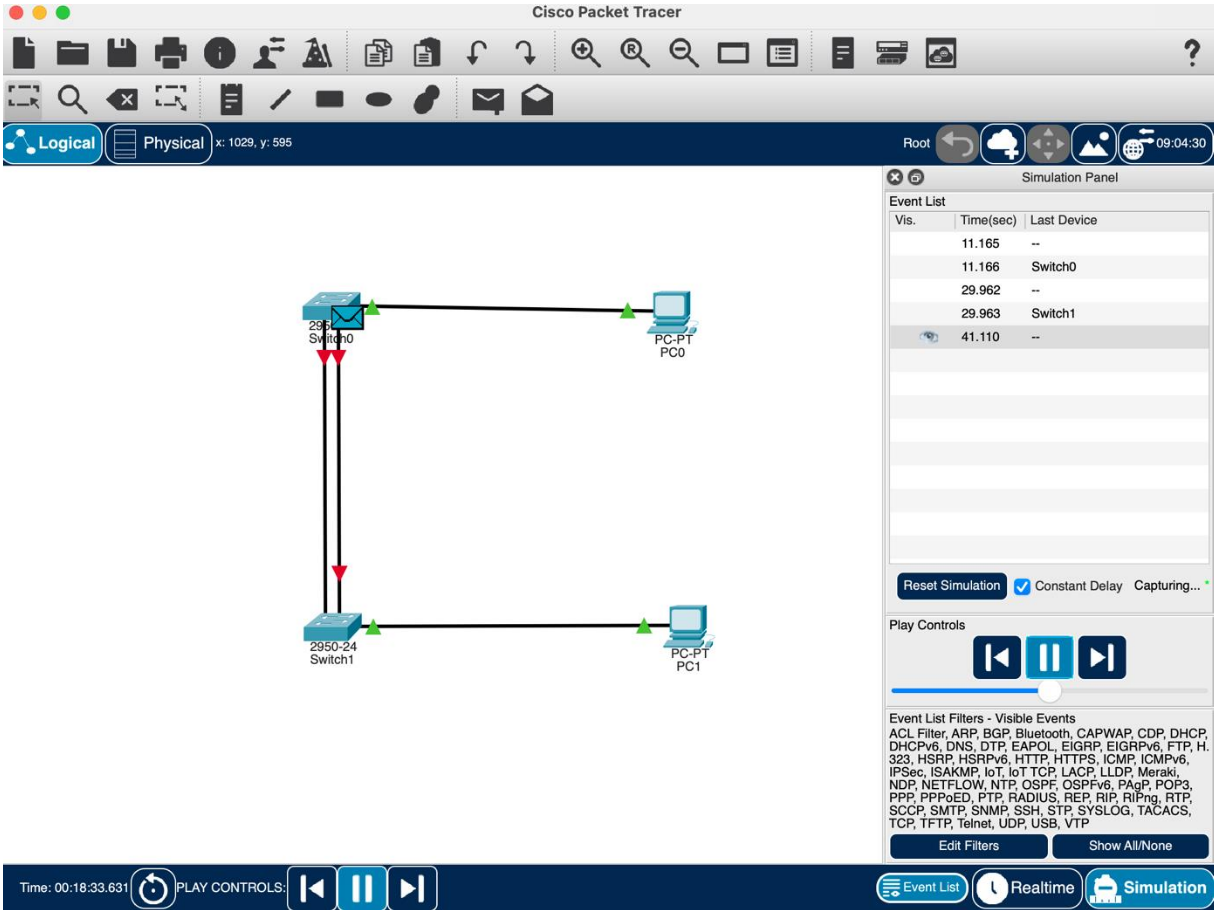


Event List

Vis.	Time(sec)	Last Device
	11.165	--
	11.166	Switch0
	29.962	--
	29.963	Switch1
	41.110	--
👁	41.111	Switch0

☑ Constant Delay Captured to: 41.111 s

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP



Event List

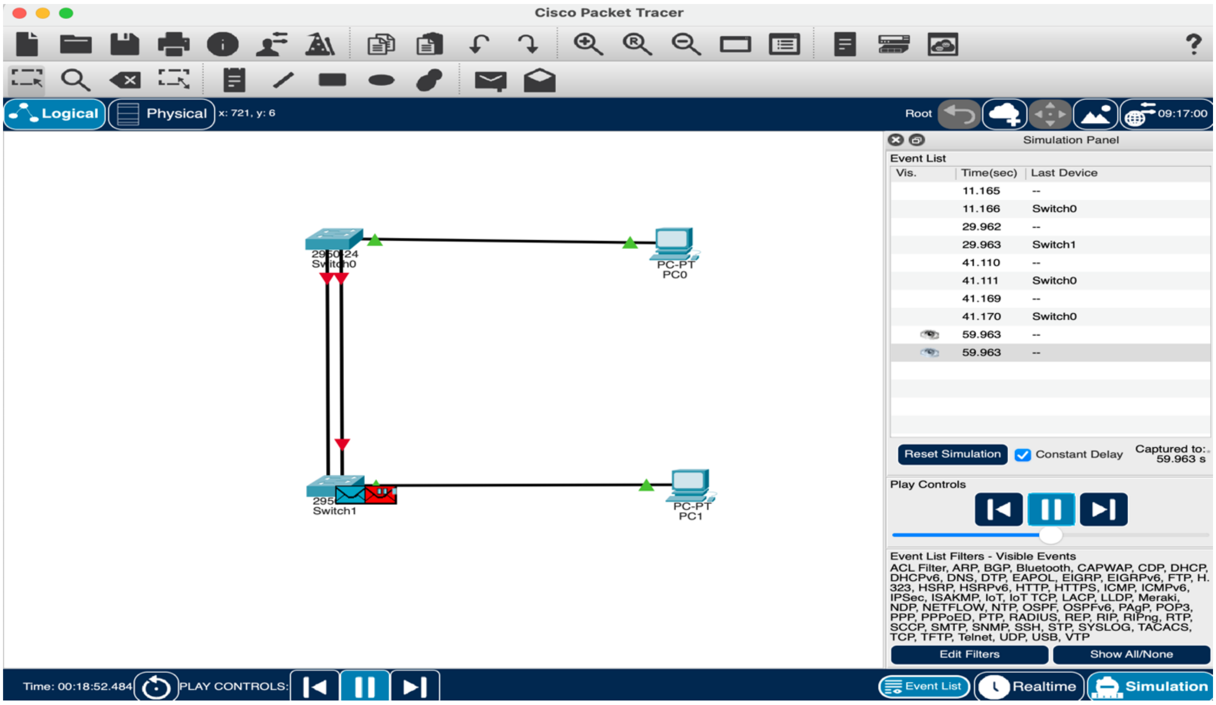
Vis.	Time(sec)	Last Device
	11.165	--
	11.166	Switch0
	29.962	--
	29.963	Switch1
👁	41.110	--

☑ Constant Delay Capturing...

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Repeated packets trigger a broadcast storm. In the Simulation Panel, it is seen that many broadcasts with the same timestamp are repeated.

Full Congestion - Network Crashes



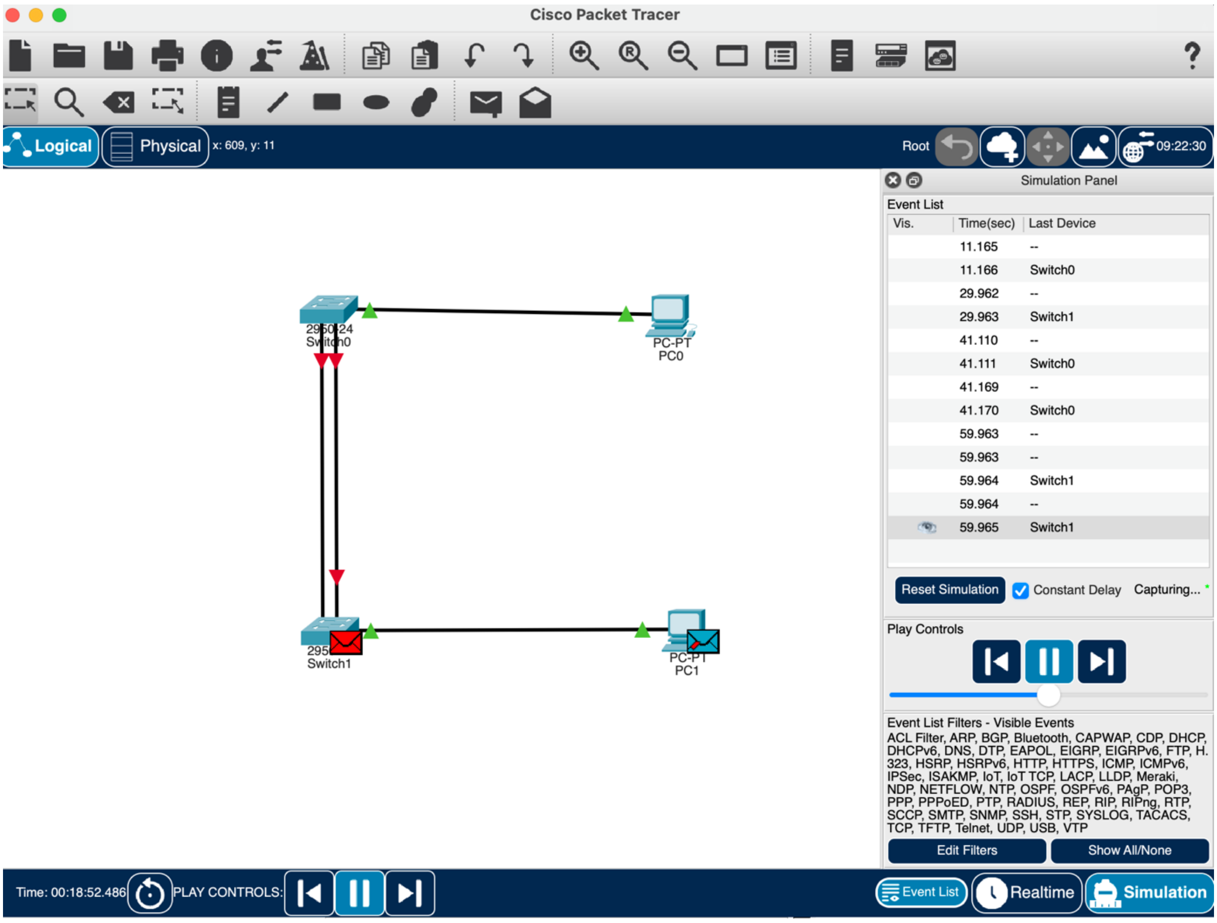
Event List

Vis.	Time(sec)	Last Device
	11.165	--
	11.166	Switch0
	29.962	--
	29.963	Switch1
	41.110	--
	41.111	Switch0
	41.169	--
	41.170	Switch0
👁	59.963	--
👁	59.963	--

☑ Constant Delay Captured to: 59.963 s

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Time: 00:18:52.484



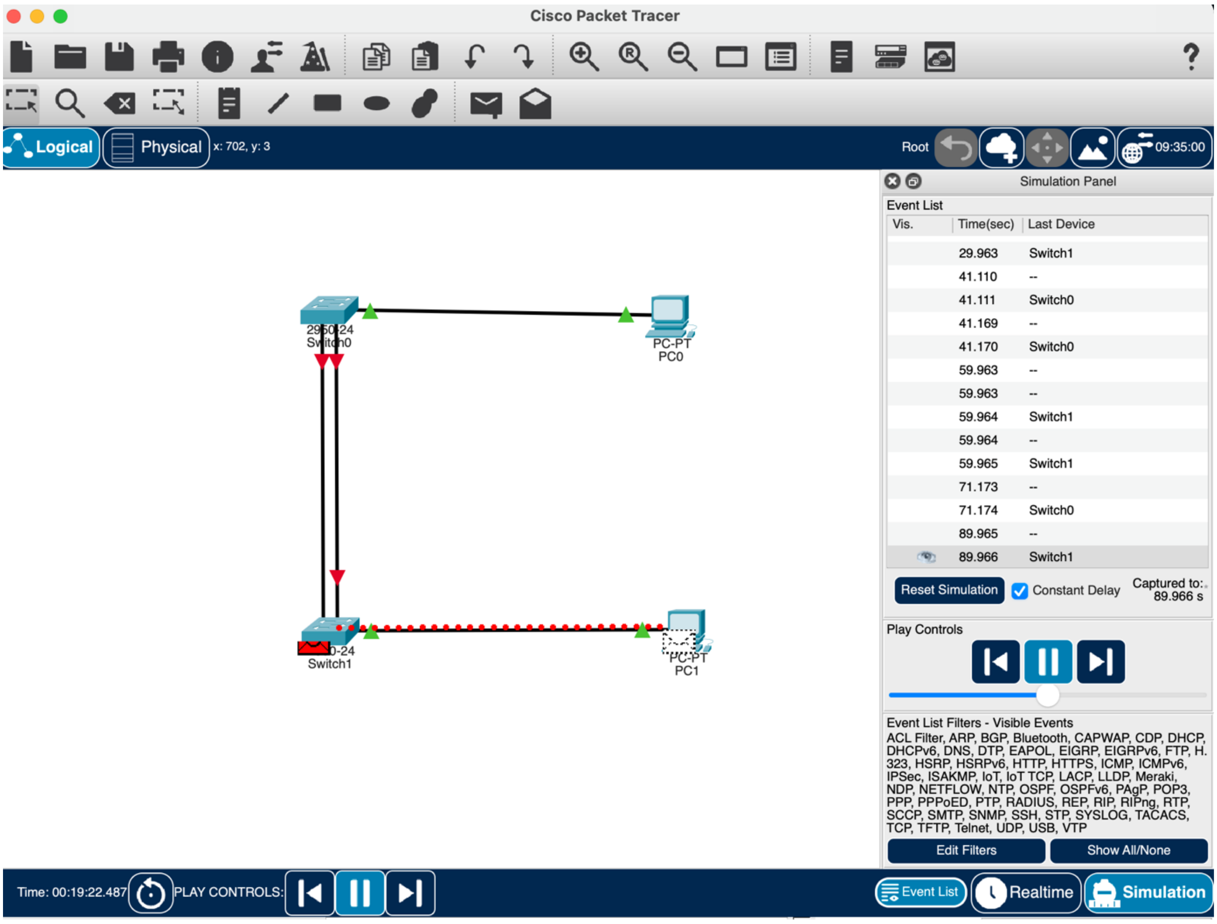
Event List

Vis.	Time(sec)	Last Device
	11.165	--
	11.166	Switch0
	29.962	--
	29.963	Switch1
	41.110	--
	41.111	Switch0
	41.169	--
	41.170	Switch0
	59.963	--
	59.963	--
	59.964	Switch1
	59.964	--
👁	59.965	Switch1

☑ Constant Delay Capturing...

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Time: 00:18:52.486



Event List

Vis.	Time(sec)	Last Device
	29.963	Switch1
	41.110	--
	41.111	Switch0
	41.169	--
	41.170	Switch0
	59.963	--
	59.963	--
	59.964	Switch1
	59.964	--
	59.965	Switch1
	71.173	--
	71.174	Switch0
	89.965	--
👁	89.966	Switch1

☑ Constant Delay

Captured to: 89.966 s

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Time: 00:19:22.487

The broadcast traffic in the network is continuously rotating in an infinite loop.

Now not only ping, but all data traffic is locked.

Since the CPUs of the switches cannot process this traffic, systemic collapse occurs.

Simulation File Name: P3_210316084_BinnurSöztutar_Switch_Loop.pkt

Conclusion:

It was successfully observed that when STP is disabled in the physical loop created with Cisco 2950-24 switches, the broadcast enters an infinite loop.

Communication between the PCs is completely cut off.

Red indicators on switch ports and 100% ping losses showed the serious consequences of a configuration error at the Layer 2 level.