



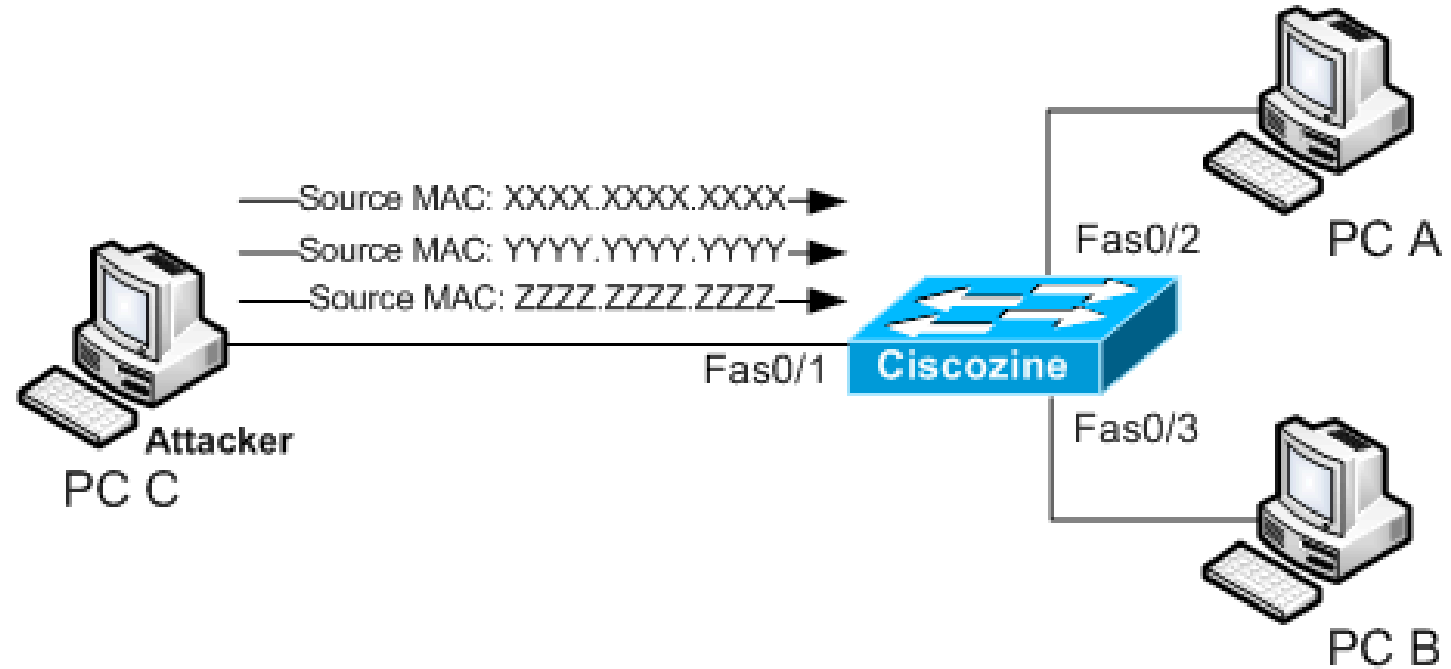
حملات به شبکه های محلی و راه های مقابله

کوشا اسماعیل پور

[Koosha.id.ir](http://Koosha.id.ir)

[Koosha.es@gmail.com](mailto:Koosha.es@gmail.com)

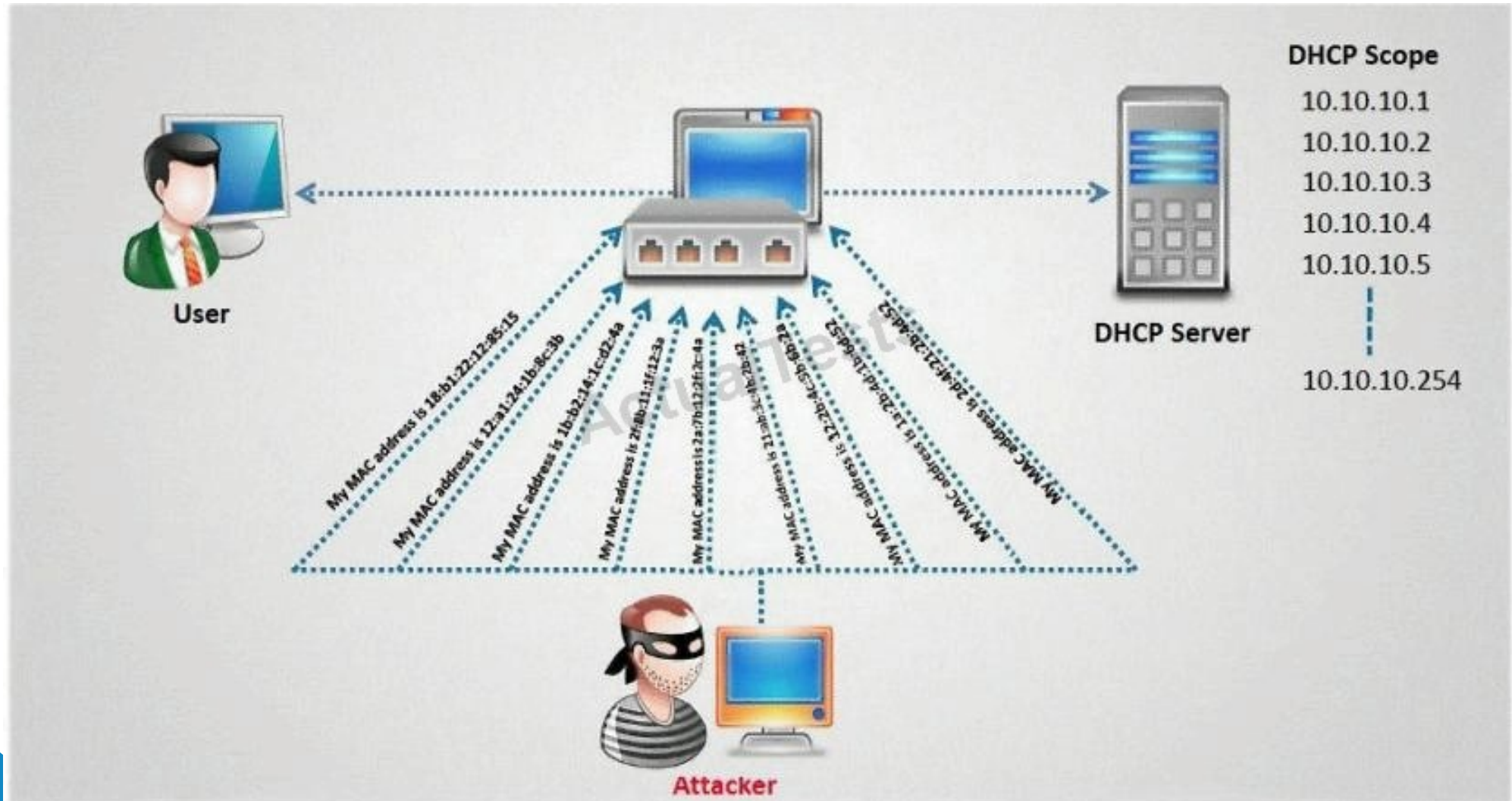
# MAC Flood



# macof

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# macof
4f:a1:99:3b:6d:fa b9:b1:e2:2:cd:20 0.0.0.0.48913 > 0.0.0.0.28324: S 338224536:33
8224536(0) win 512
c:d7:b7:52:bd:83 de:9c:41:4f:8d:86 0.0.0.0.2136 > 0.0.0.0.40073: S 1147012463:11
47012463(0) win 512
d1:3e:9e:27:bb:0 9c:2c:74:77:e3:58 0.0.0.0.43099 > 0.0.0.0.7663: S 1456266181:14
56266181(0) win 512
39:39:5d:57:7a:8f 5f:fe:7b:6b:32:45 0.0.0.0.48972 > 0.0.0.0.28506: S 1593632709:
1593632709(0) win 512
77:7a:a7:a:85:f0 47:99:84:23:3e:71 0.0.0.0.40702 > 0.0.0.0.65387: S 298375442:29
8375442(0) win 512
8b:b7:34:61:4a:51 d2:fd:b3:6b:d0:3c 0.0.0.0.61466 > 0.0.0.0.53896: S 612749537:6
12749537(0) win 512
7a:f2:7c:4f:fe:85 7c:41:ab:70:d2:2b 0.0.0.0.33775 > 0.0.0.0.35452: S 1158909109:
1158909109(0) win 512
90:e4:fa:5e:e7:56 88:20:b0:1a:56:80 0.0.0.0.20136 > 0.0.0.0.26404: S 828244057:8
28244057(0) win 512
42:91:ae:3e:77:ca 85:2:49:8:76:b9 0.0.0.0.37103 > 0.0.0.0.63330: S 1586735345:15
86735345(0) win 512
17:49:f8:50:7b:c9 ce:38:86:53:36:cc 0.0.0.0.11942 > 0.0.0.0.31038: S 975415262:9
75415262(0) win 512
ec:67:3:5c:8c:a5 40:a7:16:30:27:ff 0.0.0.0.45427 > 0.0.0.0.29835: S 1807031020:1
807031020(0) win 512
76:6:99:27:91:d6 8a:50:18:5d:dd:38 0.0.0.0.28120 > 0.0.0.0.41208: S 990343494:99
0343494(0) win 512
```

# DHCP starvation



# Sending DISCOVER packet

The screenshot shows a network security tool interface with a 'Choose attack' dialog box open. The main window has a menu bar (File, Protocols, Actions, Options, Help) and a toolbar with icons for 'Launch attack', 'Edit interfaces', 'Load default', and 'List attacks'. A table lists protocols and their packet counts:

| Protocols | Packets |
|-----------|---------|
| CDP       | 0       |
| DHCP      | 0       |
| 802.1Q    | 0       |
| 802.1X    | 0       |
| DTP       | 0       |
| HSRP      | 0       |
| ISL       | 0       |
| STP       | 0       |

The 'Choose attack' dialog box has tabs for CDP, DHCP, 802.1Q, 802.1X, DTP, HSRP, ISL, STP, and VTP. The 'DHCP' tab is selected. The dialog contains the following options:

- Choose attack: \_\_\_\_\_
- Description: \_\_\_\_\_
- DoS: \_\_\_\_\_
- sending RAW packet
- sending DISCOVER packet
- creating DHCP rogue server
- sending RELEASE packet

Buttons for 'Cancel' and 'OK' are at the bottom of the dialog. Below the dialog, the 'Dynamic Host Configuration Protocol' configuration fields are visible:

Source MAC: 02:48:33:66:02:51    Destination MAC: FF:FF:FF:FF:FF:FF  
SIP: 0.0.0.0    DIP: 255.255.255.255    SPort: 68    DPort: \_\_\_\_\_  
Op: 01    Htype: 01    HLEN: 06    Hops: 00    Xid: 00009869    S: \_\_\_\_\_  
CI: 0.0.0.0    YI: 0.0.0.0    SI: 0.0.0.0    C: \_\_\_\_\_

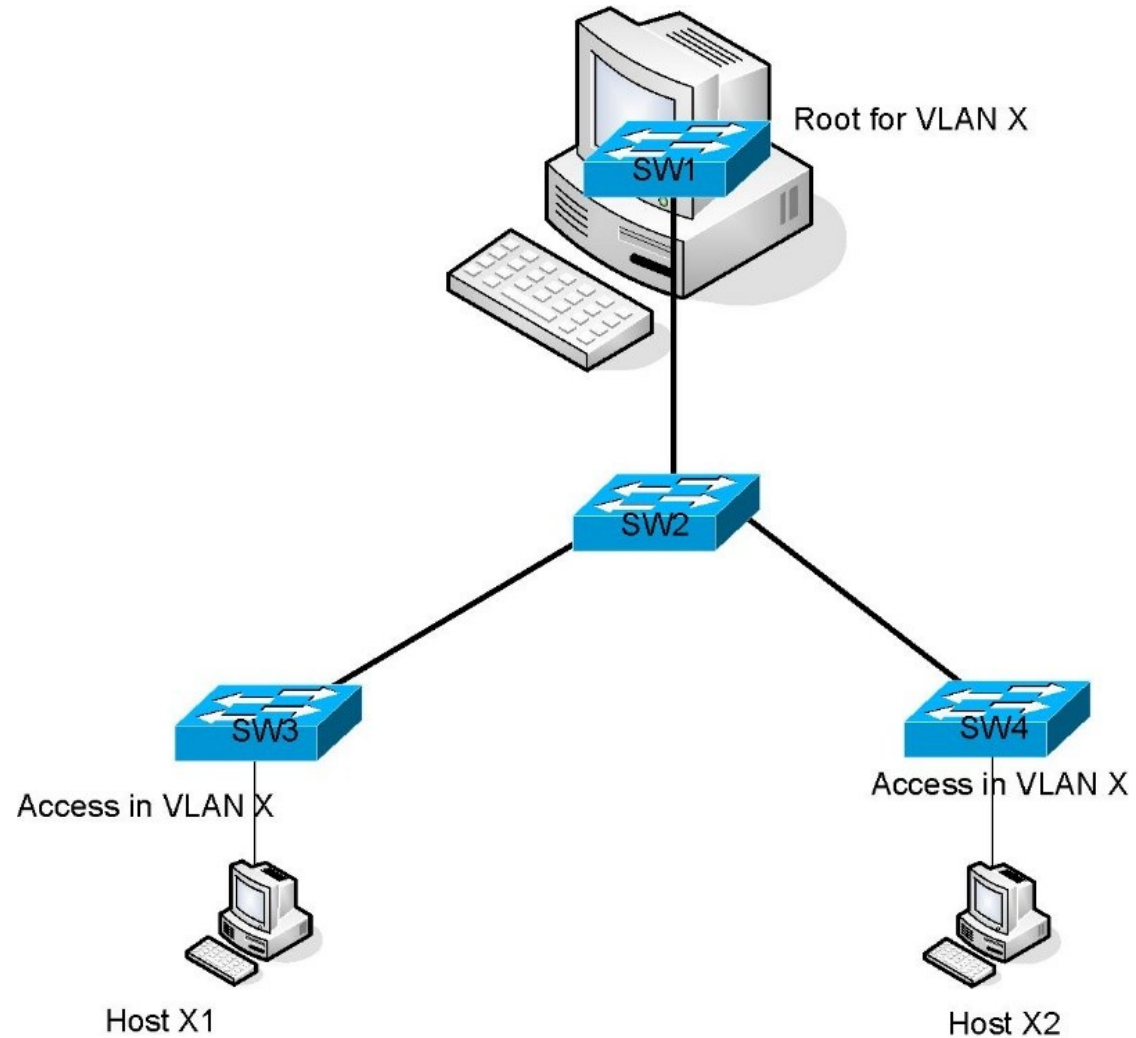
# Port Security

- Switch(config)# interface interface\_id
- Switch(config-if)# switchport mode access
- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security maximum value
- Switch(config-if)# switchport port-security violation {protect | restrict | shutdown }

# VLAN hopping

- 1-Switch spoofing
- 2-Double tagging

# 1-Switch spoofing





# Enabling trunking

The screenshot shows a network attack tool interface. The main window has a menu bar (File, Protocols, Actions, Options, Help) and a toolbar with icons for Launch attack, Edit interfaces, Load default, and List attacks. Below the toolbar is a table of protocols and their packet counts:

| Protocols | Packets |
|-----------|---------|
| CDP       | 0       |
| DHCP      | 0       |
| 802.1Q    | 0       |
| 802.1X    | 0       |
| DTP       | 0       |
| HSRP      | 0       |
| ISL       | 0       |
| STP       | 0       |

Below the table is a 'Field Value Description' section. The 'Dynamic Trunking Protocol' section is visible, showing fields for Source MAC (0C:7C:E8:46:D5:95), Destination MAC (01:00:0C:CC:CC:CC), Version (01), Neighbor-ID (0C7CE846D595), Status (03), and Type (A5).

A 'Choose attack' dialog box is open, showing a list of attack types: CDP, DHCP, 802.1Q, 802.1X, DTP, HSRP, ISL, STP, and VTP. The 'DTP' tab is selected. The dialog box contains a 'Choose attack' section with two radio button options: 'sending DTP packet' (unchecked) and 'enabling trunking' (checked). There are also 'Cancel' and 'OK' buttons at the bottom of the dialog box.



1. Ensure that ports are not set to negotiate trunks automatically :

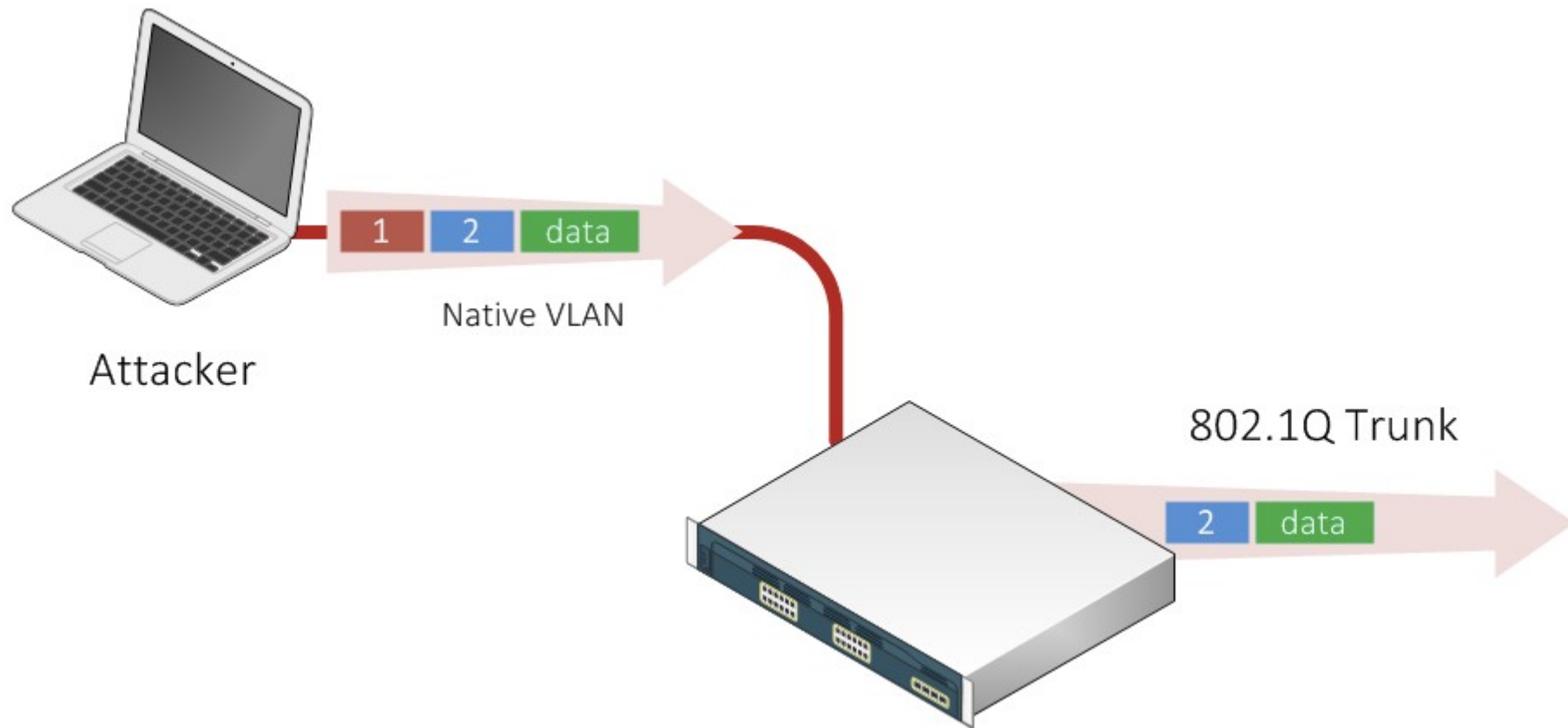
- Switch(config-if)# switchport nonegotiate

OR

2. Ensure that ports that are not meant to be trunks are explicitly configured as access ports

- Switch(config-if)# switchport mode access

# Double tagging



# Sending .1Q double encapsulation

The screenshot shows the Yersinia 0.7.1 application interface. The main window has a menu bar (File, Protocols, Actions, Options, Help) and a toolbar with icons for Launch attack, Edit interfaces, Load default, and List attacks. A table on the left lists protocols and their packet counts:

| Protocols | Packets |
|-----------|---------|
| CDP       | 0       |
| DHCP      | 0       |
| 802.1Q    | 0       |
| 802.1X    | 0       |
| DTP       | 0       |
| HSRP      | 0       |
| ISL       | 0       |
| STP       | 0       |

A 'Choose attack' dialog box is open, showing the following options:

- CDP
- DHCP
- 802.1Q (selected)
- 802.1X
- DTP
- HSRP
- ISL
- STP
- VTP

The 'Choose attack' dialog box contains the following options:

- Choose attack
- Description
- DoS
- sending 802.1Q packet
- sending 802.1Q double enc. packet
- sending 802.1Q arp poisoning

The 'IEEE 802.1Q' configuration section shows the following fields:

- Source MAC: 0E:5C:49:19:32:BF
- Destination MAC: FF:FF:FF:FF:FF:FF
- VLAN: 1
- Priority: 7
- CFI: 00
- L2Proto1: 0800
- VLAN2: [ ]
- L2Proto2: 0800
- Src IP: 10.0.0.1
- Dst IP: 255.255.255.255



Simply do not put any hosts on VLAN 1

- Switch(config-if)# switchport access vlan 2

OR

Change the native VLAN on all trunk ports to an unused VLAN ID.

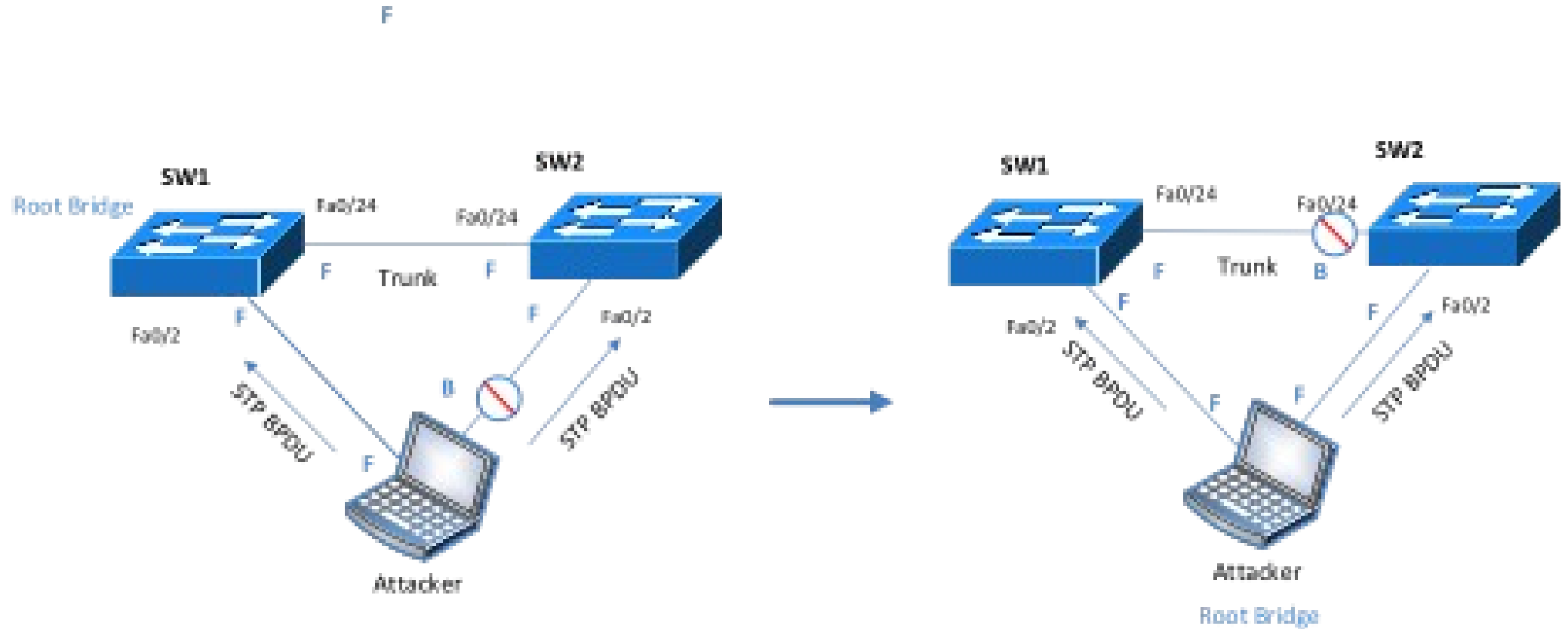
- Switch(config-if)# switchport trunk native vlan 999

OR

Explicit tagging of the native VLAN on all trunk ports.

- switch(config)# vlan dot1q tag native

# STP Attack



# Claiming Root Role

The screenshot displays a network attack tool interface with a 'Choose attack' dialog box open. The main window shows a menu bar (File, Protocols, Actions, Options, Help) and a toolbar with icons for launching attacks, editing interfaces, loading defaults, and listing attacks. A table lists protocols and their packet counts:

| Protocols | Packets |
|-----------|---------|
| CDP       | 0       |
| DHCP      | 0       |
| 802.1Q    | 0       |
| 802.1X    | 0       |
| DTP       | 0       |
| HSRP      | 0       |
| ISL       | 0       |
| STP       | 0       |

The 'Choose attack' dialog box has tabs for CDP, DHCP, 802.1Q, 802.1X, DTP, HSRP, ISL, STP, and VTP. The STP tab is selected. The dialog contains the following options:

- sending conf BPDU  DoS
- sending tcn BPDU  DoS
- sending conf BPDUs  DoS
- sending tcn BPDUs  DoS
- Claiming Root Role**  DoS
- Claiming Other Role  DoS
- Claiming Root Role with MiTM  DoS

Buttons for 'Cancel' and 'OK' are at the bottom of the dialog. Below the dialog, the 'Spanning Tree Protocol' configuration is visible:

Source MAC: 04:08:20:12:A9:75    Destination MAC: 01:80:C2:00:00:00  
Id: 0000    Ver: 00    Type: 00    Flags: 00    RootId: AC58.E7CD90  
BridgId: 8423.1B231602FF08    Port: 8002    Age: 0000    Max: 0014

# BPDU guard OR Root guard

- SW1(config)#interface interface\_id
- SW1(config-if)#spanning-tree bpduguard enable

OR

- SW1(config)#interface interface\_id
- SW1(config-if)#spanning-tree guard root



# CDP Flood

The screenshot shows the Yersinia 0.7.3 interface. The main window has a menu bar (File, Protocols, Actions, Options, Help) and a toolbar with icons for Launch attack, Edit interfaces, Load default, List attacks, Clear stats, Capture, and Edit mode. A table on the left lists protocols and their packet counts:

| Protocols | Packets |
|-----------|---------|
| CDP       | 0       |
| DHCP      | 0       |
| 802.1Q    | 0       |
| 802.1X    | 0       |
| DTP       | 0       |
| HSRP      | 0       |
| ISL       | 0       |
| MPLS      | 0       |

The 'Choose attack' dialog box is open, showing the 'CDP' tab selected. The 'Choose attack' section has three radio button options:

- sending CDP packet
- flooding CDP table
- Setting up a virtual device

The 'DoS' column has checkboxes for each option, with the 'flooding CDP table' checkbox checked. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Below the dialog, the 'Cisco Discovery Protocol' configuration is visible, showing:

Source MAC: 06:45:8B:6B:41:56    Destination MAC: 01:00:0C:CC:CC:CC    Extra

# Disable or Turn Off CDP on Cisco Switches & Routers

- Router(config)# no cdp run

OR

- Router(config)# int interface\_id
- Router(config-if)# no cdp enable

سال نو مبارک



مبارک سال نو

مبارک سال نو

مبارک سال نو