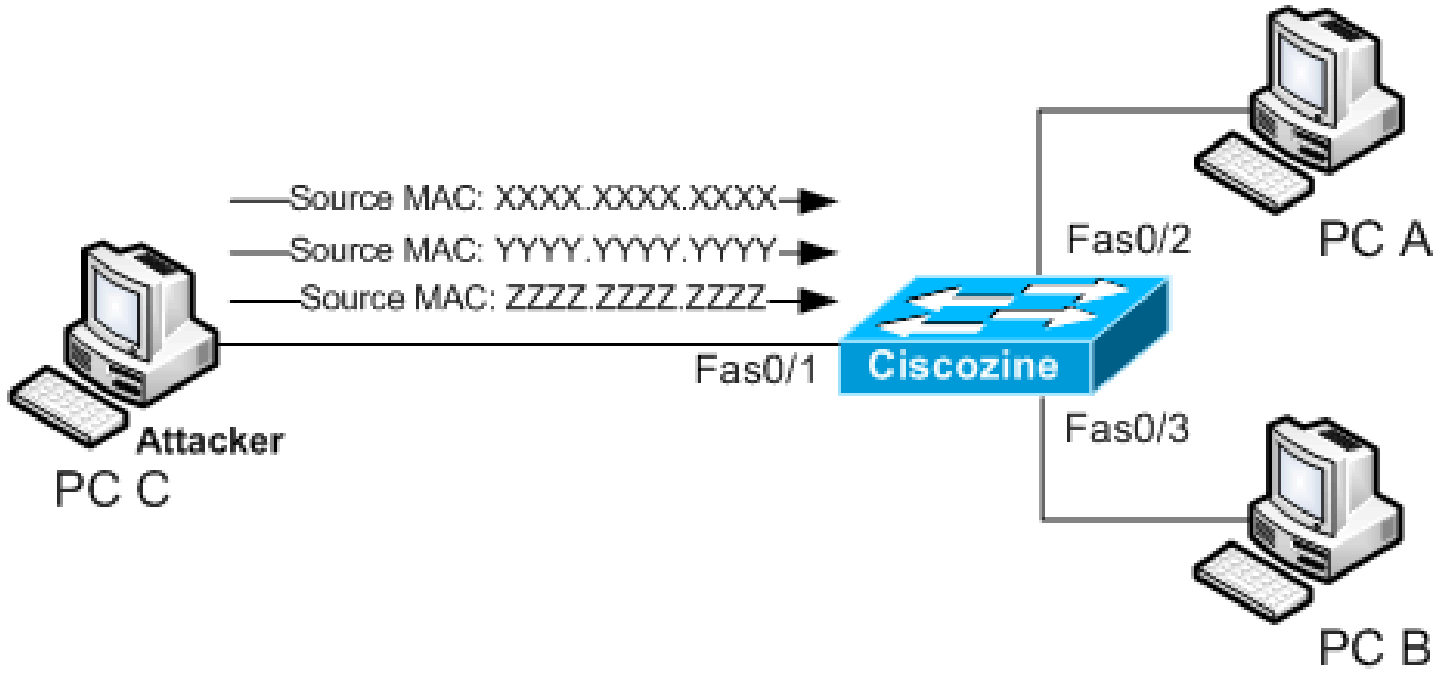
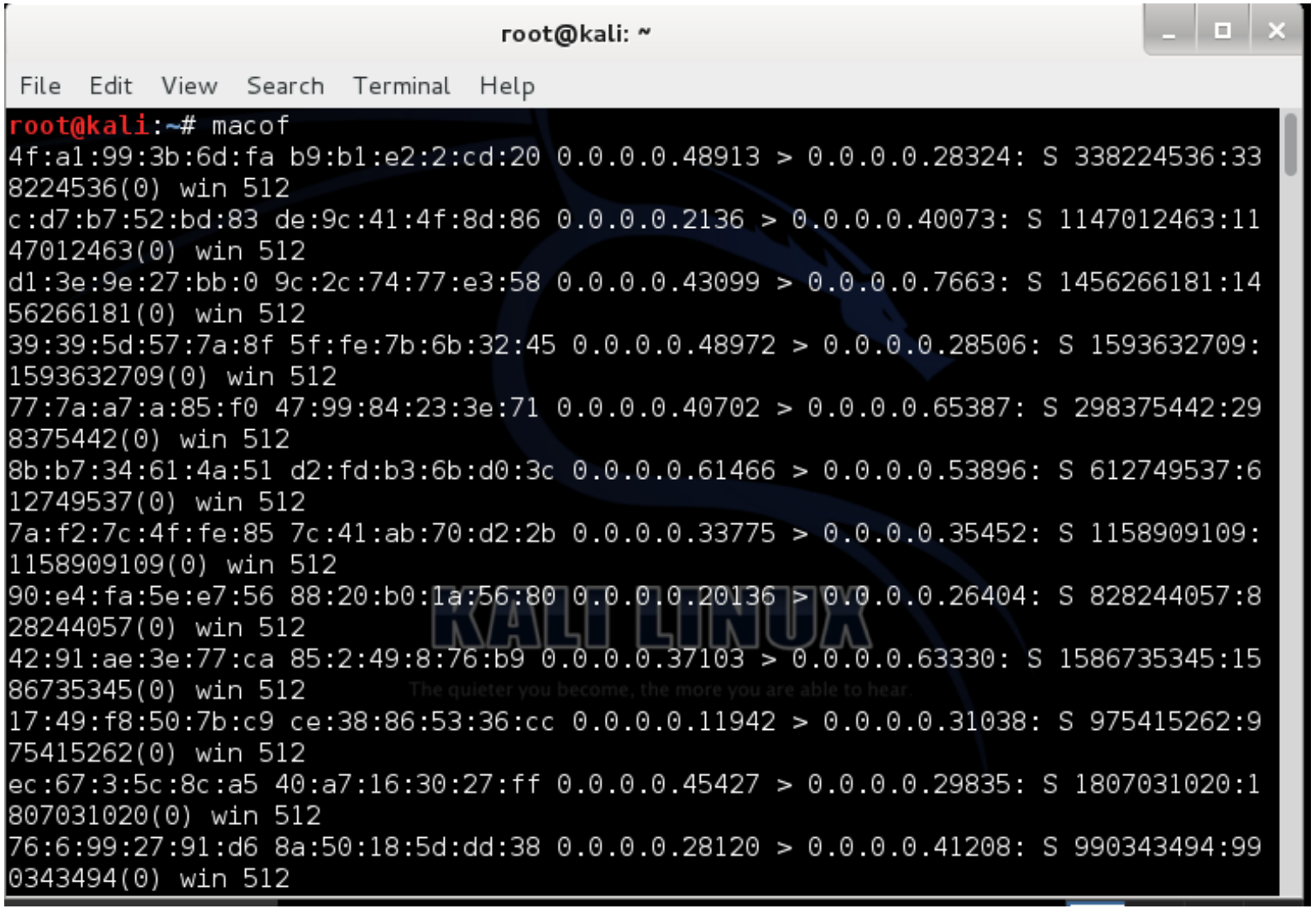
حملات به شبکه های محلی و راه های مقابله

کوشا اسماعیل پور
Koosha.id.ir
Koosha.es@gmail.com

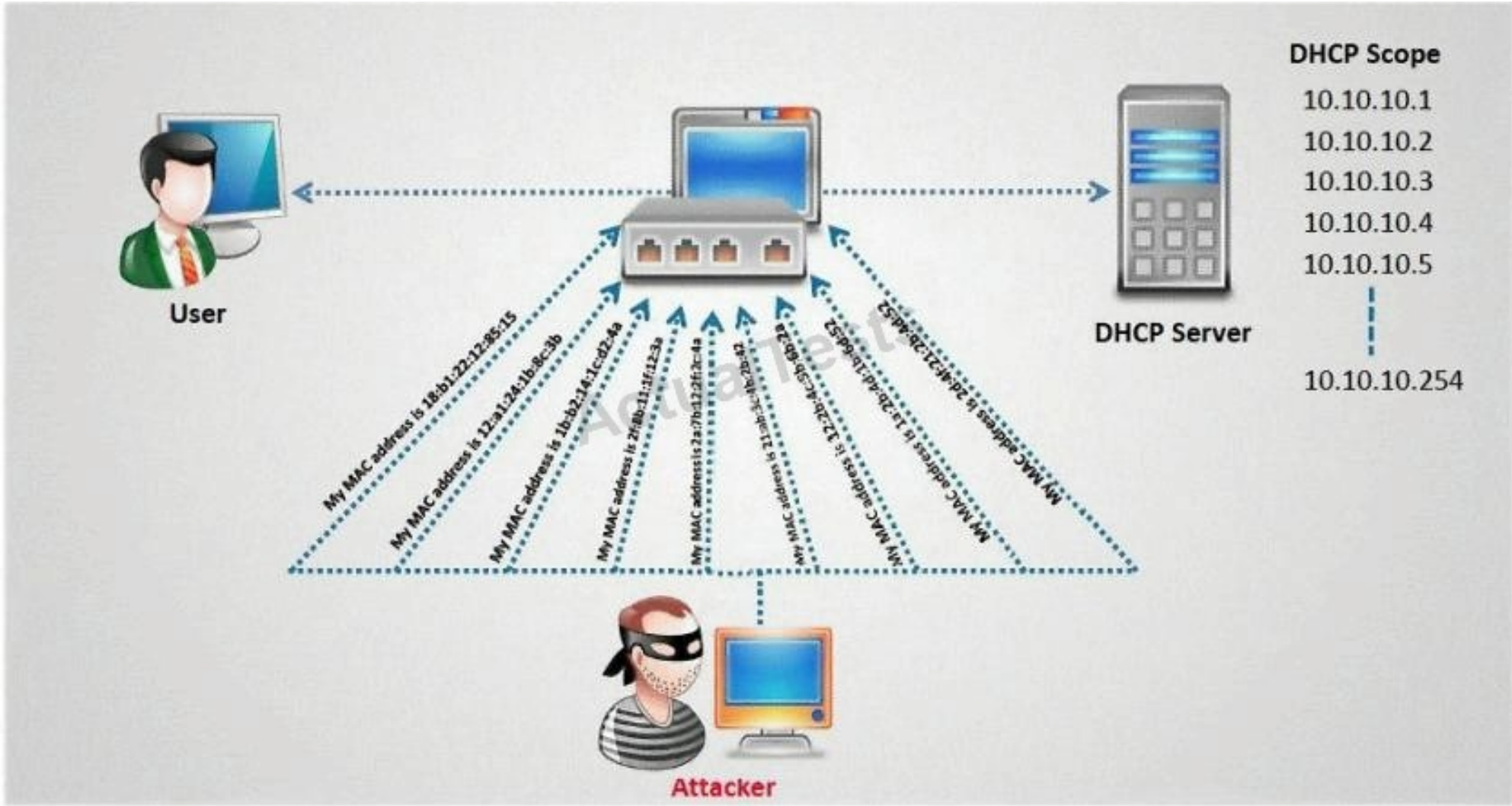
MAC Flood


Source MAC: XXXX.XXXX.XXXX
Source MAC: YYYY.YYYY.YYYY
Source MAC: ZZZZ.ZZZZ.ZZZZ
Fas0/1
Ciscozine
Fas0/2
PC A
Fas0/3
PC B
Attacker
PC C

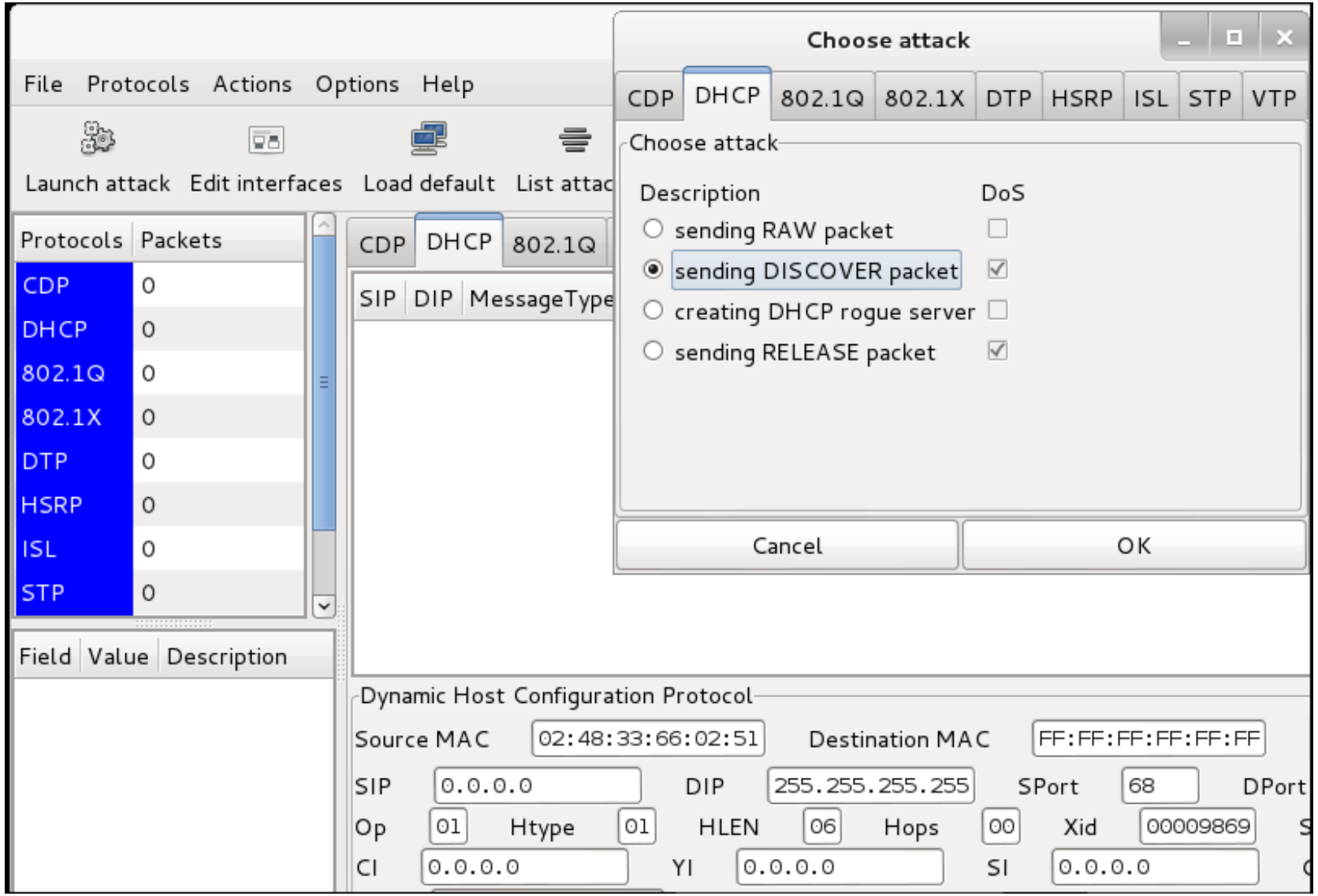
macof


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



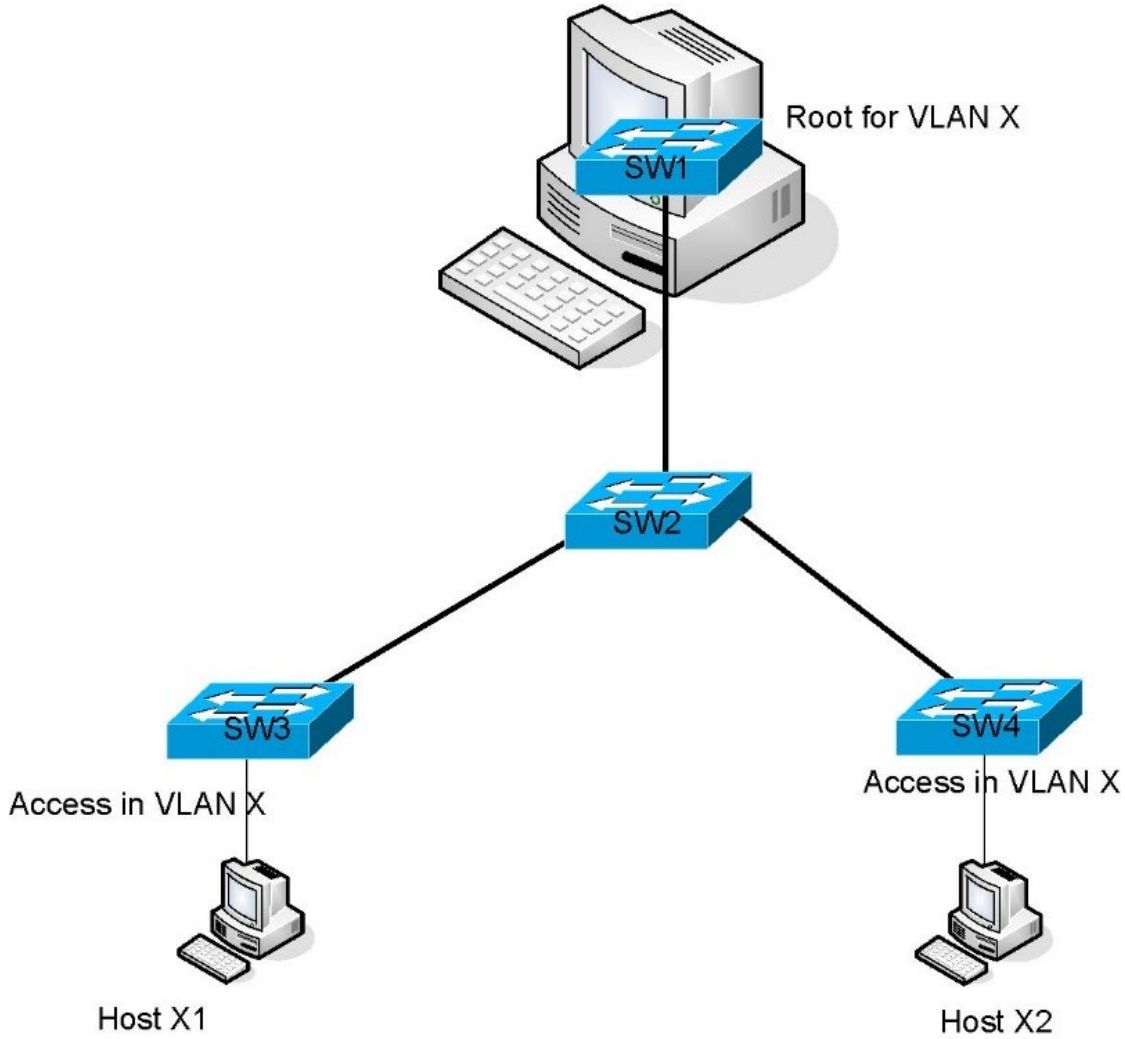
Port Security

- 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 }

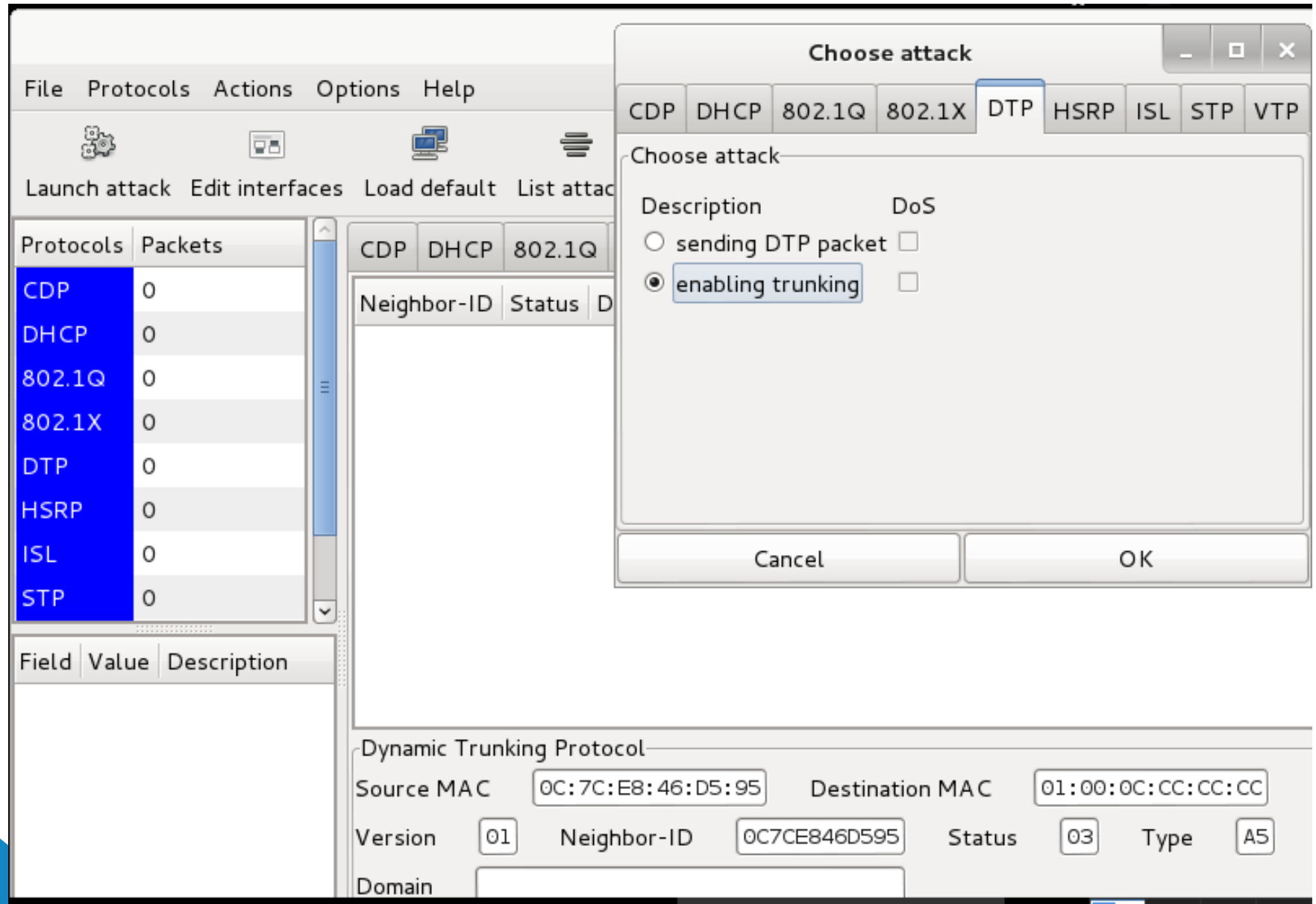
VLAN hopping

- 1-Switch spoofing
- 2-Double tagging

1-Switch spoofing



Enabling trunking



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

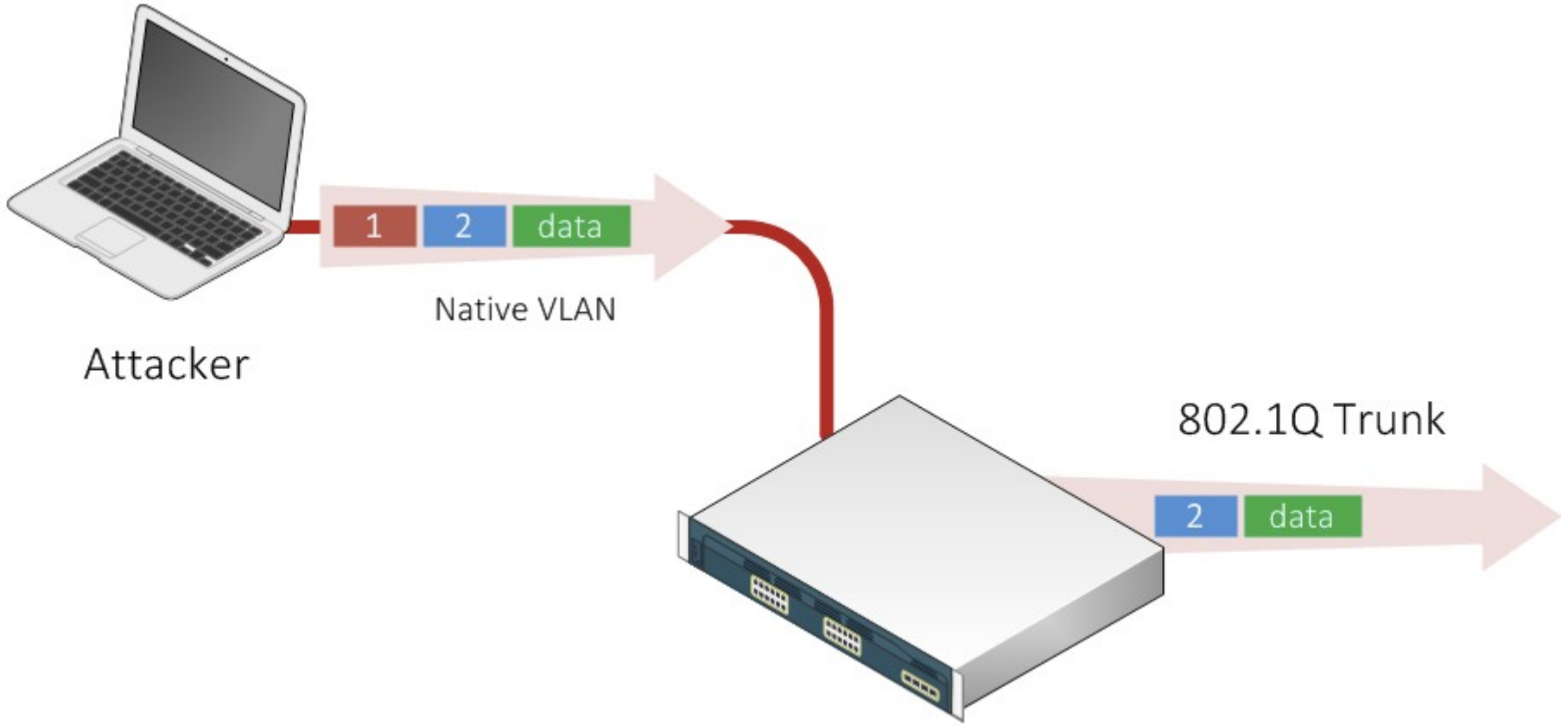
- Switch(config-if)# switchport nonegotiate

OR

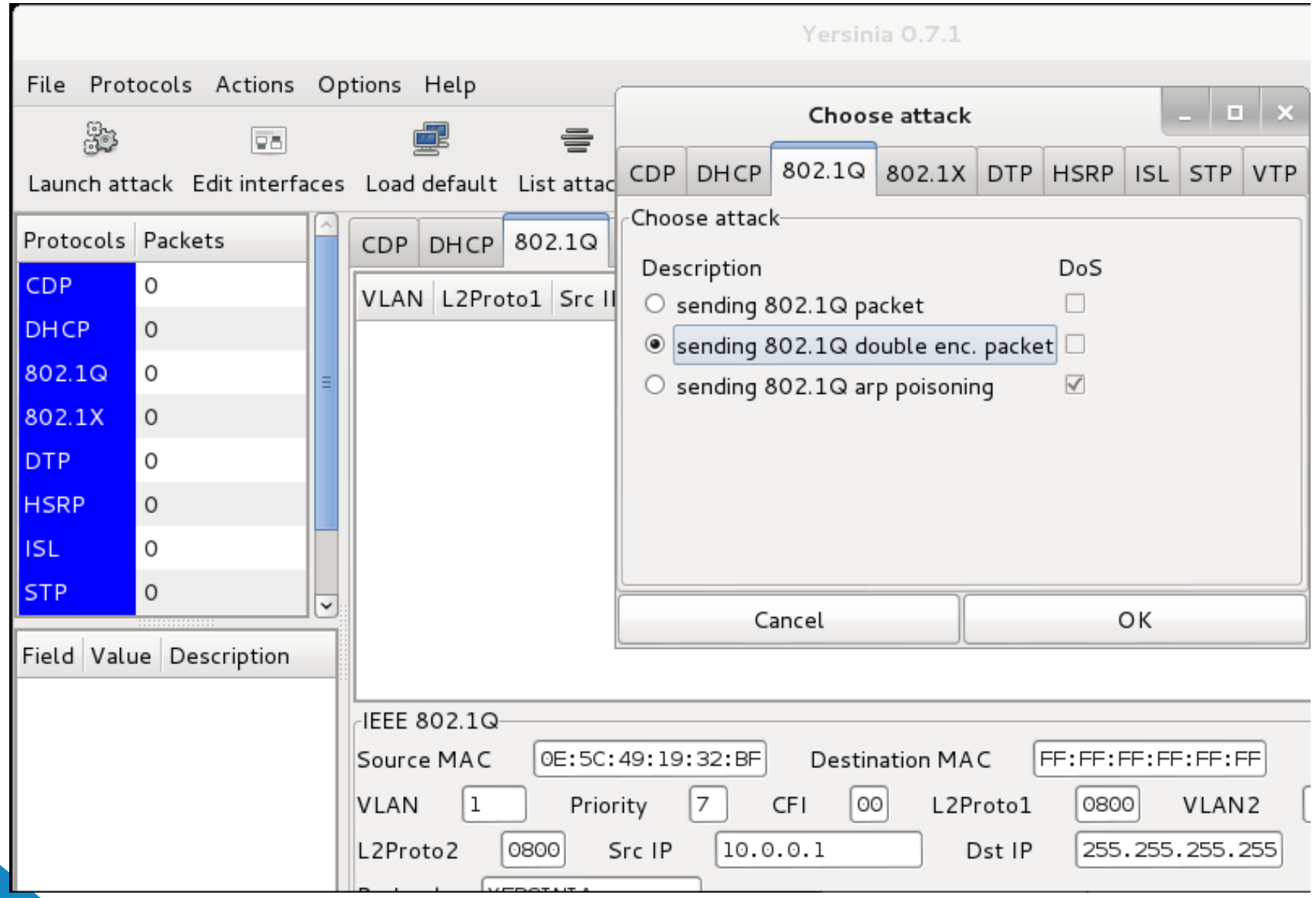
2. Ensure that ports that are not meant to be trunks are explicitly configured as access ports

- Switch(config-if)# switchport mode access

Double tagging



Sending .1Q double encapsulation



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.

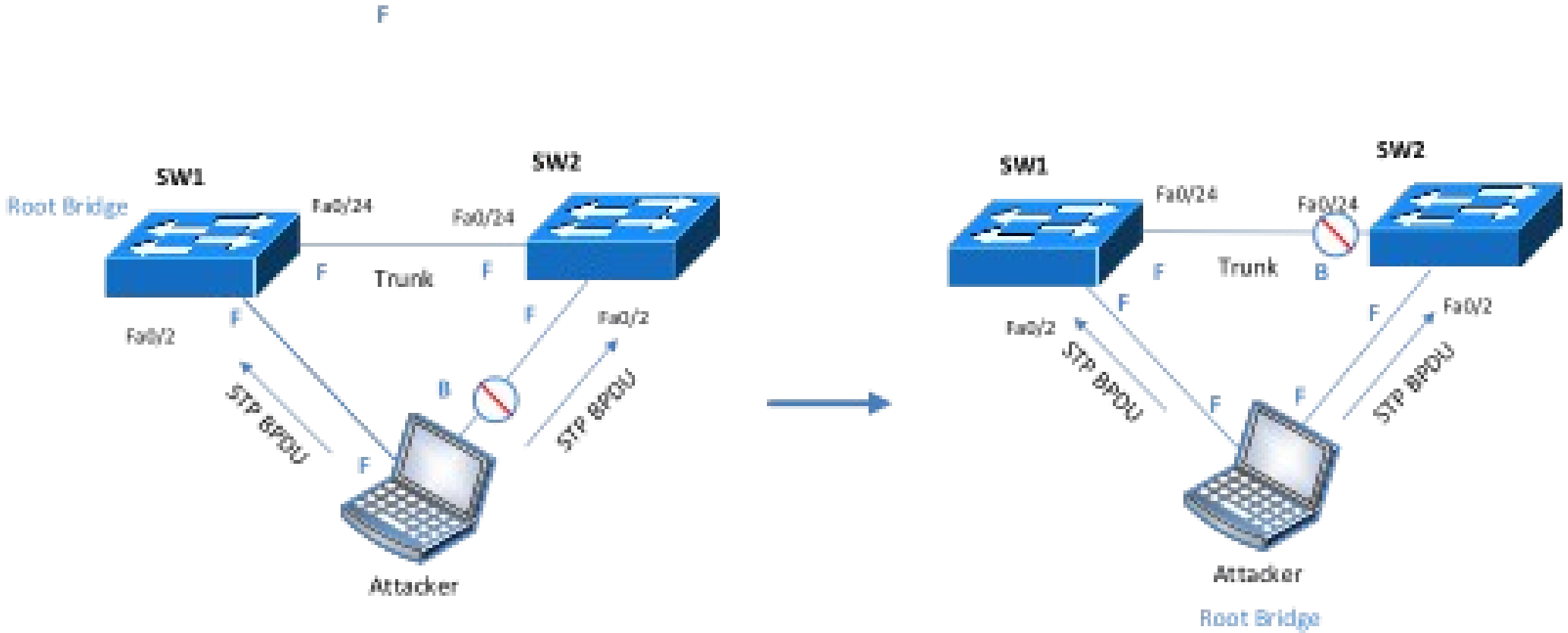
- Switch(config-if)# switchport trunk native vlan 999

OR

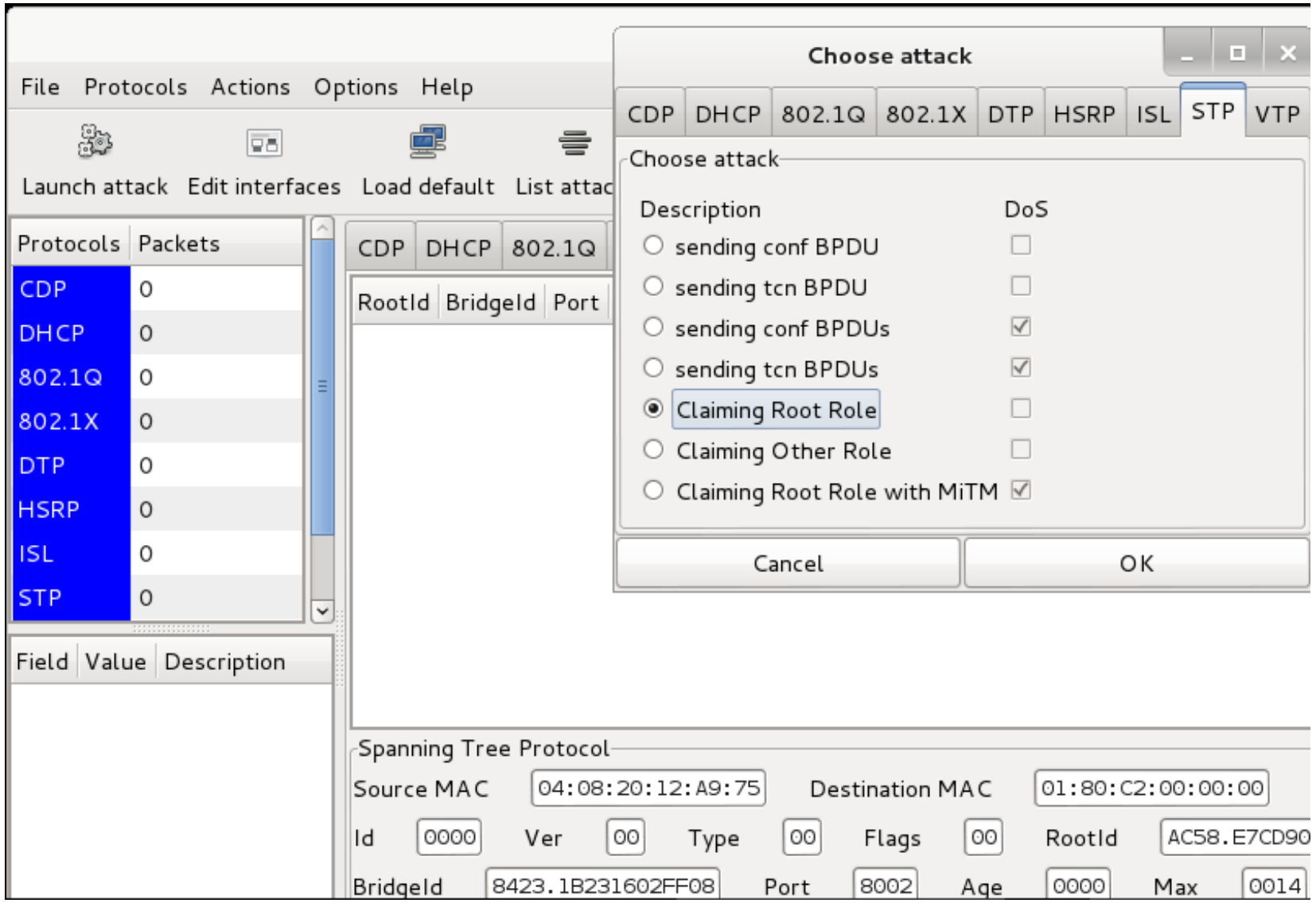
Explicit tagging of the native VLAN on all trunk ports.

- switch(config)# vlan dot1q tag native

STP Attack


F
SW1
SW2
Root Bridge
Fa0/24
Fa0/24
F
Trunk
F
F
Fa0/2
F
Fa0/2
B
STP BPDU
STP BPDU
F
Attacker
SW1
SW2
Fa0/24
Fa0/24
F
Trunk
B
F
F
Fa0/2
Fa0/2
STP BPDU
F
F
STP BPDU
Attacker
Root Bridge

Claiming Root Role



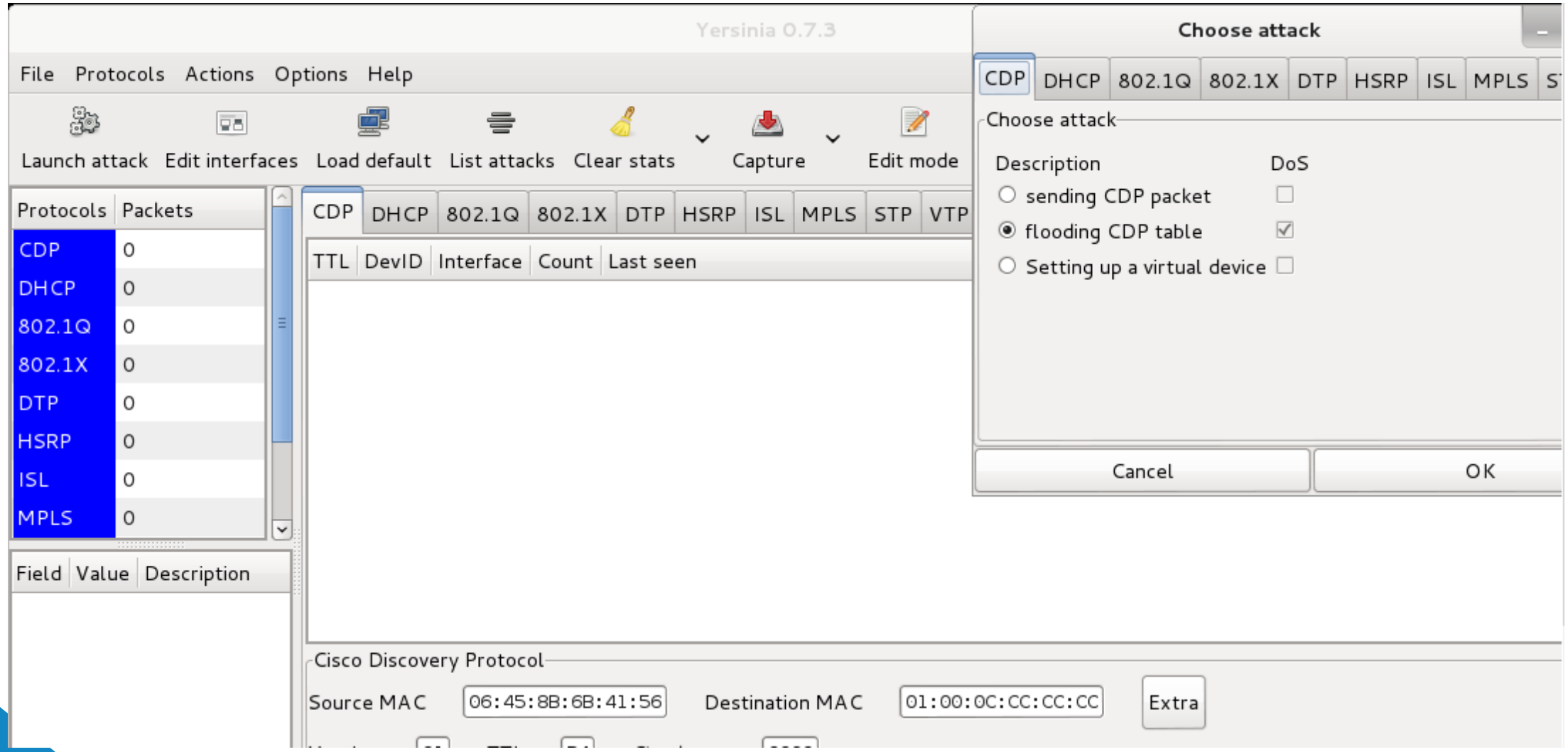
BPDU guard OR Root guard

- 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


Yersinia 0.7.3
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Protocols Packets
CDP 0
DHCP 0
802.1Q 0
802.1X 0
DTP 0
HSRP 0
ISL 0
MPLS 0
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP
TTL DevID Interface Count Last seen
Field Value Description
Cisco Discovery Protocol
Source MAC 06:45:8B:6B:41:56
Destination MAC 01:00:0C:CC:CC:CC
Extra
Choose attack
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS
Choose attack
Description DoS
sending CDP packet
flooding CDP table
Setting up a virtual device
Cancel
OK

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


یا مقلب القلوب والابصار
یا مقلب القلوب والابصار
یا مقلب القلوب والابصار