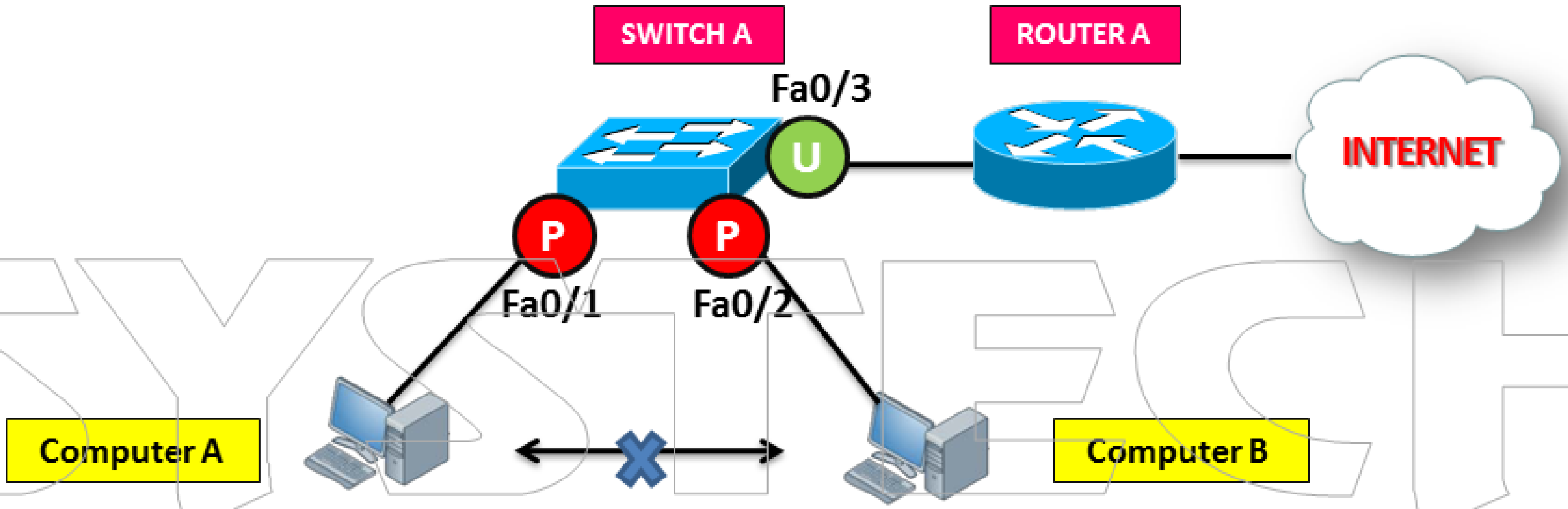
Switch Security

Protected & unprotected ports:

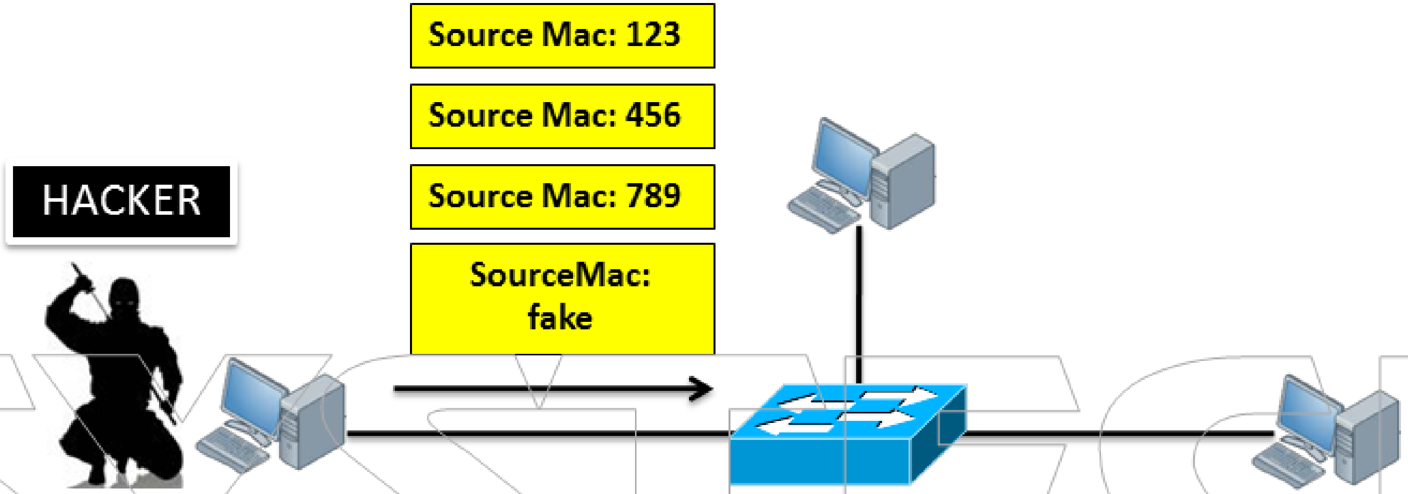


SWITCH A

```
# int fa0/1
#switchport protected
#Int fa0/2
#switchport protected
#show interface fa0/1 switchport
     Protected : true
#show interface fa0/1 switchport | include protected
     Protected : true
```

Protected Port	---	Unprotected Port	= working
Protected Port	---	Protected Port	= not working

MAC Flooding :



✓This attack will overflow the MAC address table of the switch.

✓There are tools that will generate Ethernet Frames with fake source MAC addresses and these will be sent to the interfaces

✓Switch has a limited capability to store MAC address.Once it's full it wont learn any new MAC addresses and as a result it will flood traffic

✓The attacker can run wireshark and try to capture some of the traffic flooded by switch

✓The solution for MAC flooding is port security

```
#int fa0/1
#switchport mode access
#switchport port-security
#switchport port-security maximum 1
```

```
#int fa0/1
#switchport port-security mac-address aaaa.bbbb.cccc
#switchport port-security violation shutdown
```

Ping any ip from the pc connected to fa0/1 and it goes to err-disable state

```
#show port-security interface fa0/1
```

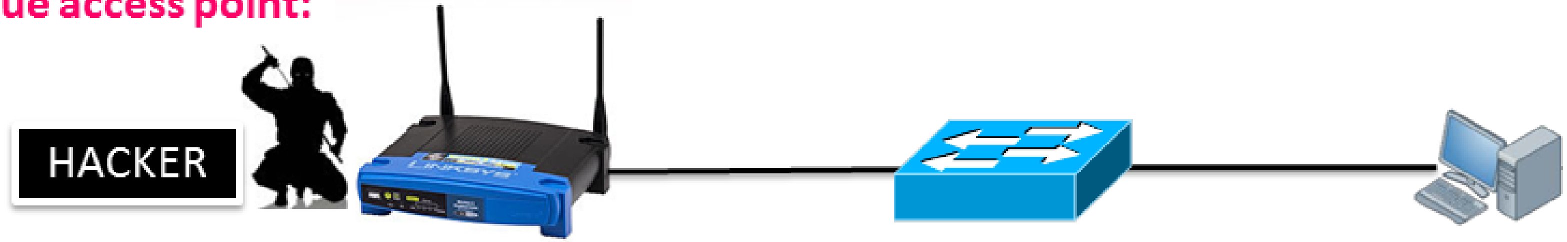
To enable fa0/1 back you have to shutdown & no shutdown it.

```
#errdisable recovery cause psecure-violation
#int fa0/1
#switchport port-security aging time 10
```

```
#switchport port-security mac-address sticky
#sh run int fa0/1
```

It will save MAC of the pc connected in fa0/1

Rogue access point:

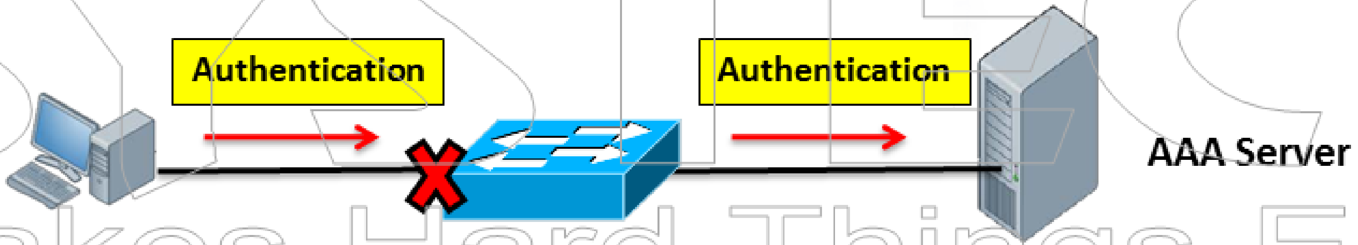


✓ MAC addresses are easy to spoof

✓ A hacker can connect his wireless router to the switch port

✓ It's hard to detect because on switch you will see only one MAC

✓ To overcome this we have to use **AAA** (Authentication,Authorization and Accounting)



✓User has to authenticate before getting access to the network.

✓ All the switch ports will be blocked

✓ If the credentials are OK then the ports will be unblocked

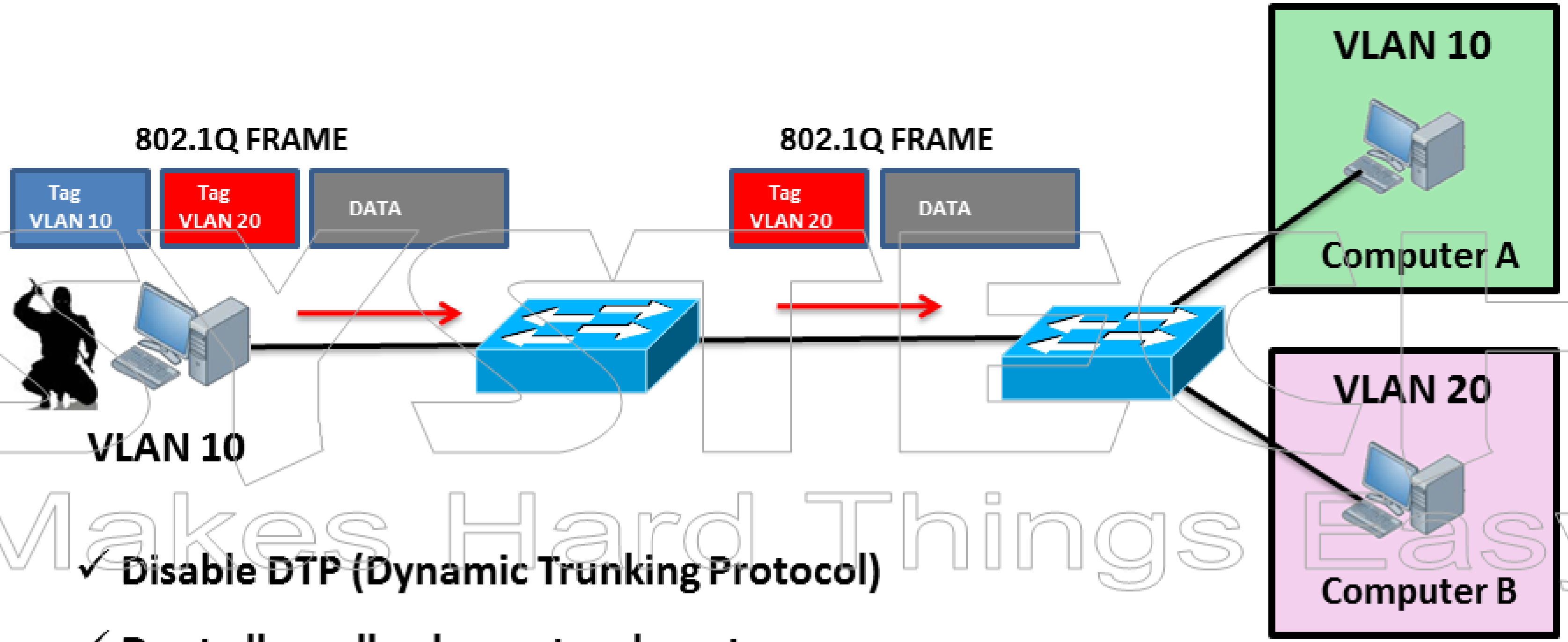
✓Authentication servers :

RADIUS: Remote Authentication Dial In User Service

TACACS+: Terminal Access Controller Access-Control System (cisco proprietary)

VLAN hopping:

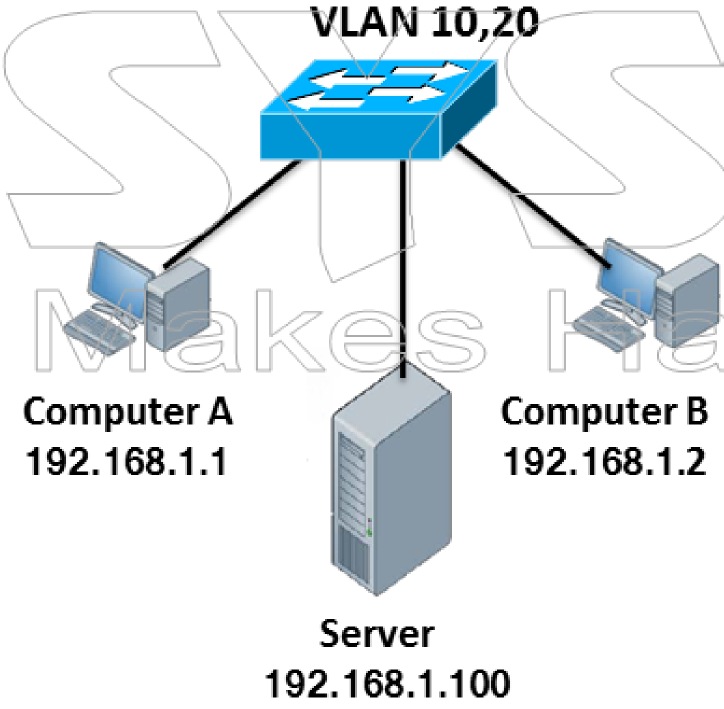
- ✓A attack where the attacker will send ethernet Frames with two 802.1q tags



- ✓ Disable DTP (Dynamic Trunking Protocol)
- ✓ Dont allow all valns on trunk port
- ✓ Shut down interfaces not in use
- ✓ Place unused interfaces in separate VLAN ,dont leave in VLAN 1

Security within VLAN:

- ✓ Three Kind of Access-lists
- ✓ Routed ACL: applies to layer 3 (router)
- ✓ Port ACL (PACL) applies to layer 2 switchport interface
- ✓ VLAN ACL (VACL): it will apply to all traffic within VLAN



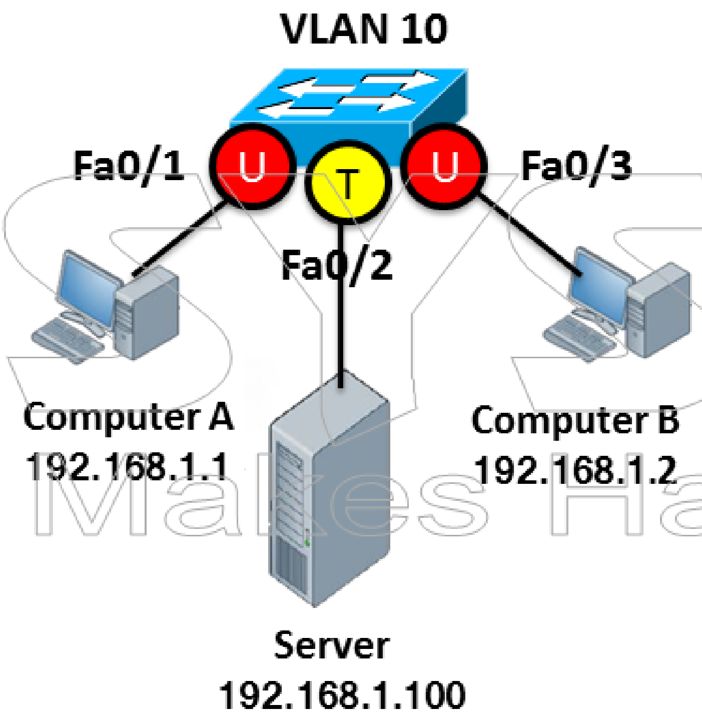
```
# access-list 100 permit ip any host 192.168.1.100
#vlan access-map systech 10
#match ip address 100
#action drop
#vlan access-map systech 20
#match ip address 100
#action forward

#vlan filter systech vlan-list 10
#vlan filter systech vlan-list 20
```

Now Computer A will not ping with server

DHCP spoofing:

- ✓The attacker will run his own DHCP server and will assign IP to other users



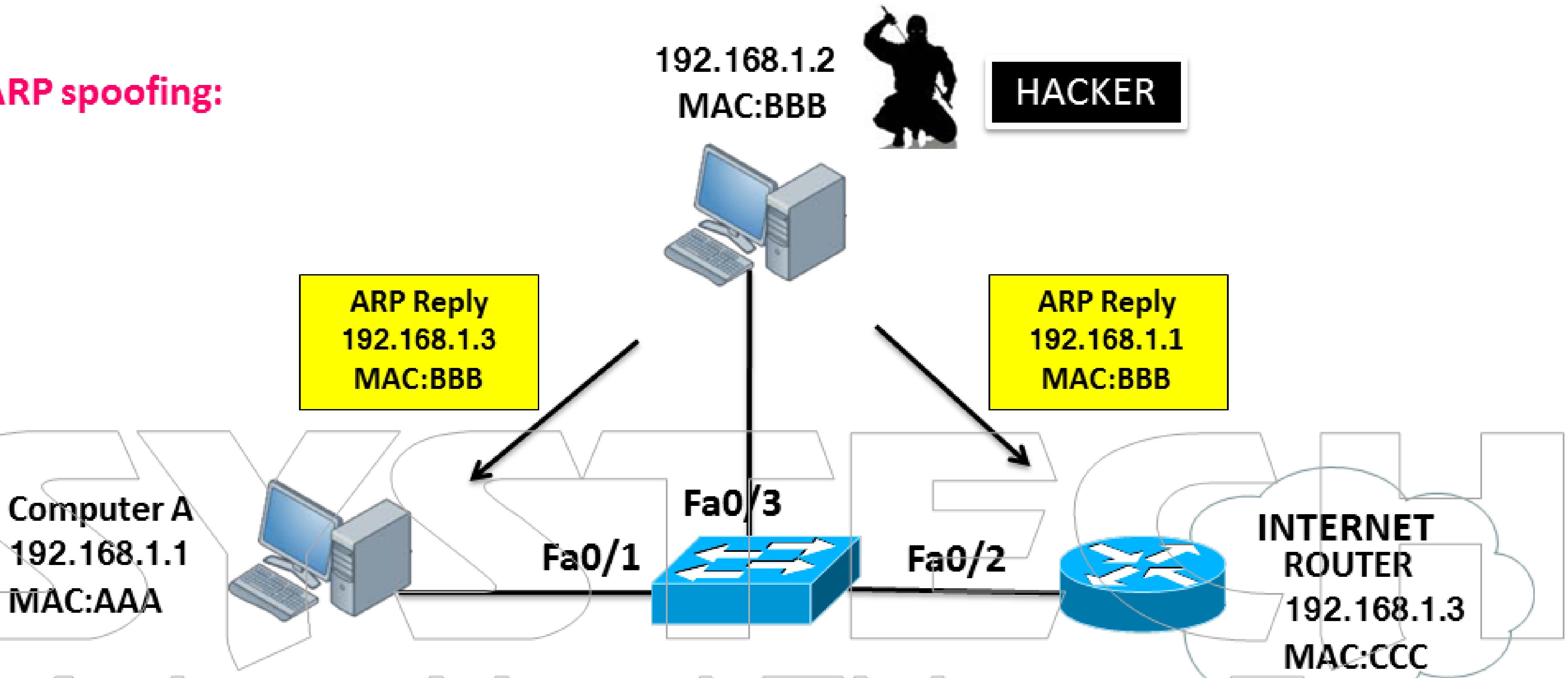
#ip dhcp snooping
now all ports will become untrusted

#no ip dhcp snooping information option

#ip dhcp snooping vlan 1
#int fa0/2
#ip dhcp snooping trust

show ip dhcp snooping

ARP spoofing:



192.168.1.2
MAC:BBB

HACKER

ARP Reply
192.168.1.3
MAC:BBB

ARP Reply
192.168.1.1
MAC:BBB

Computer A
192.168.1.1
MAC:AAA

Fa0/3

Fa0/1

Fa0/2

INTERNET
ROUTER
192.168.1.3
MAC:CCC

- ✓Man in the middle attack
- ✓Cain & able
- ✓Solution for this is DAI (Dynamic ARP Inspection)

```
#ip dhcp snooping
#ip dhcp snooping vlan 1
#IP arp inspection vlan 1
```