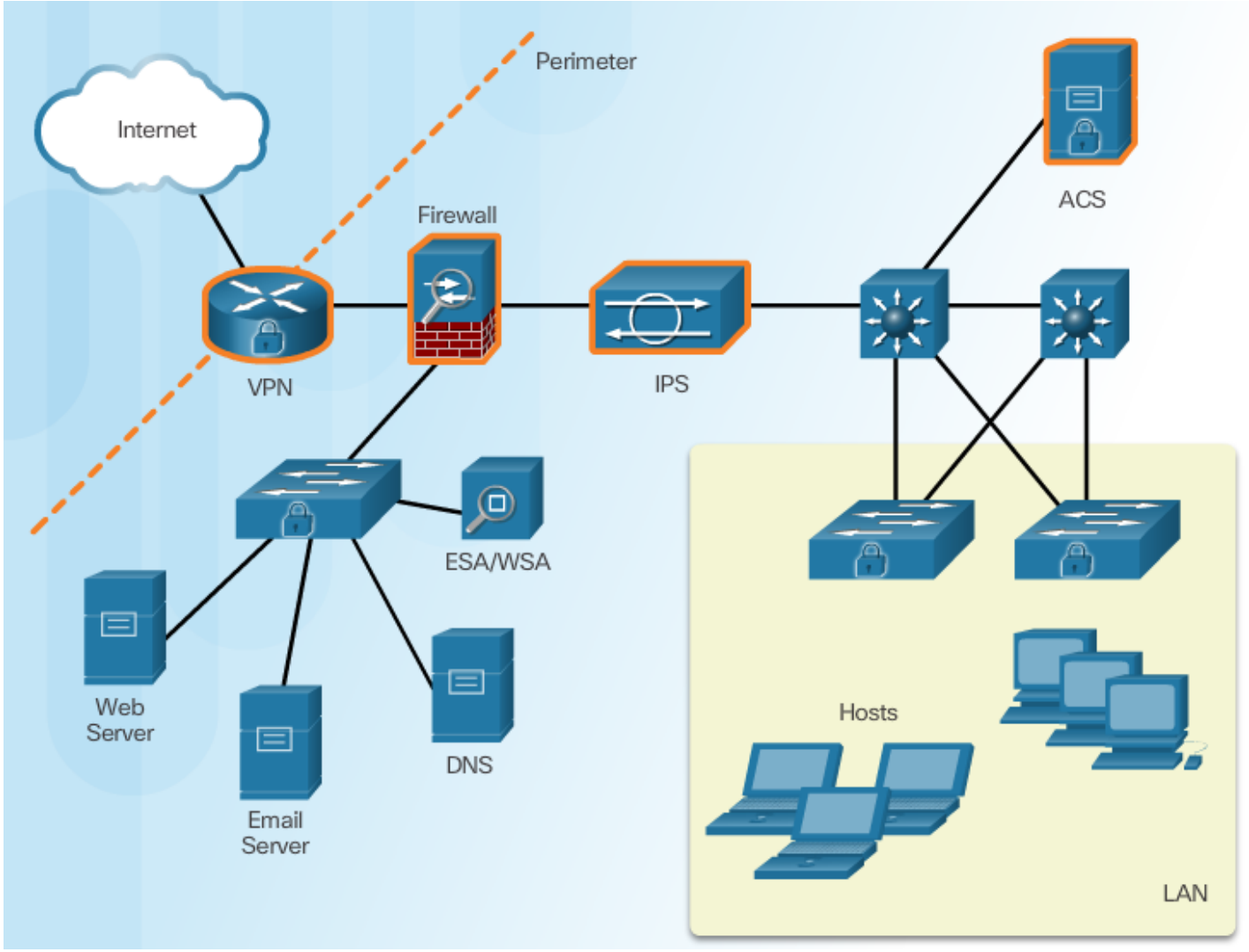
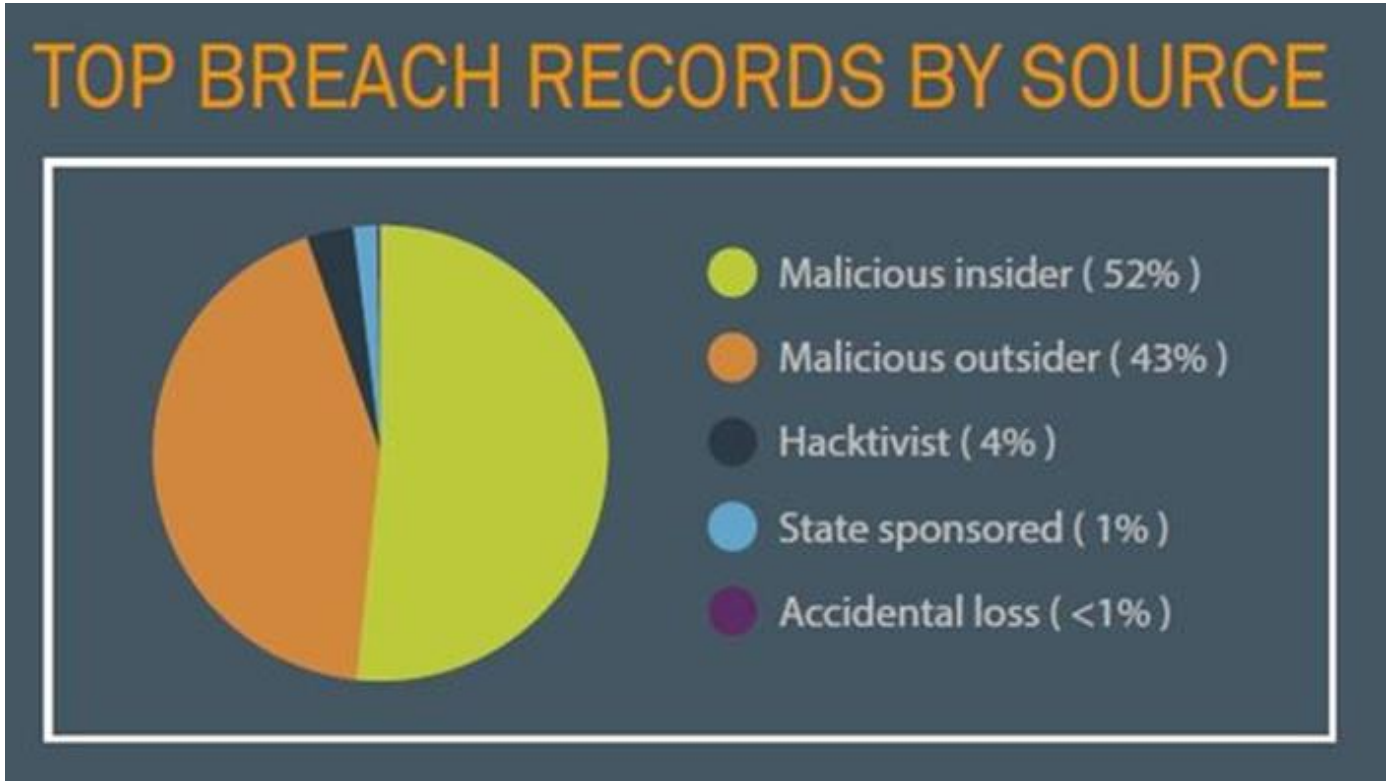
Layer 2 Security Threats

Creating attacks on Routers and Switches using Packet Tracer as a tool

Securing LAN Elements



Attacks



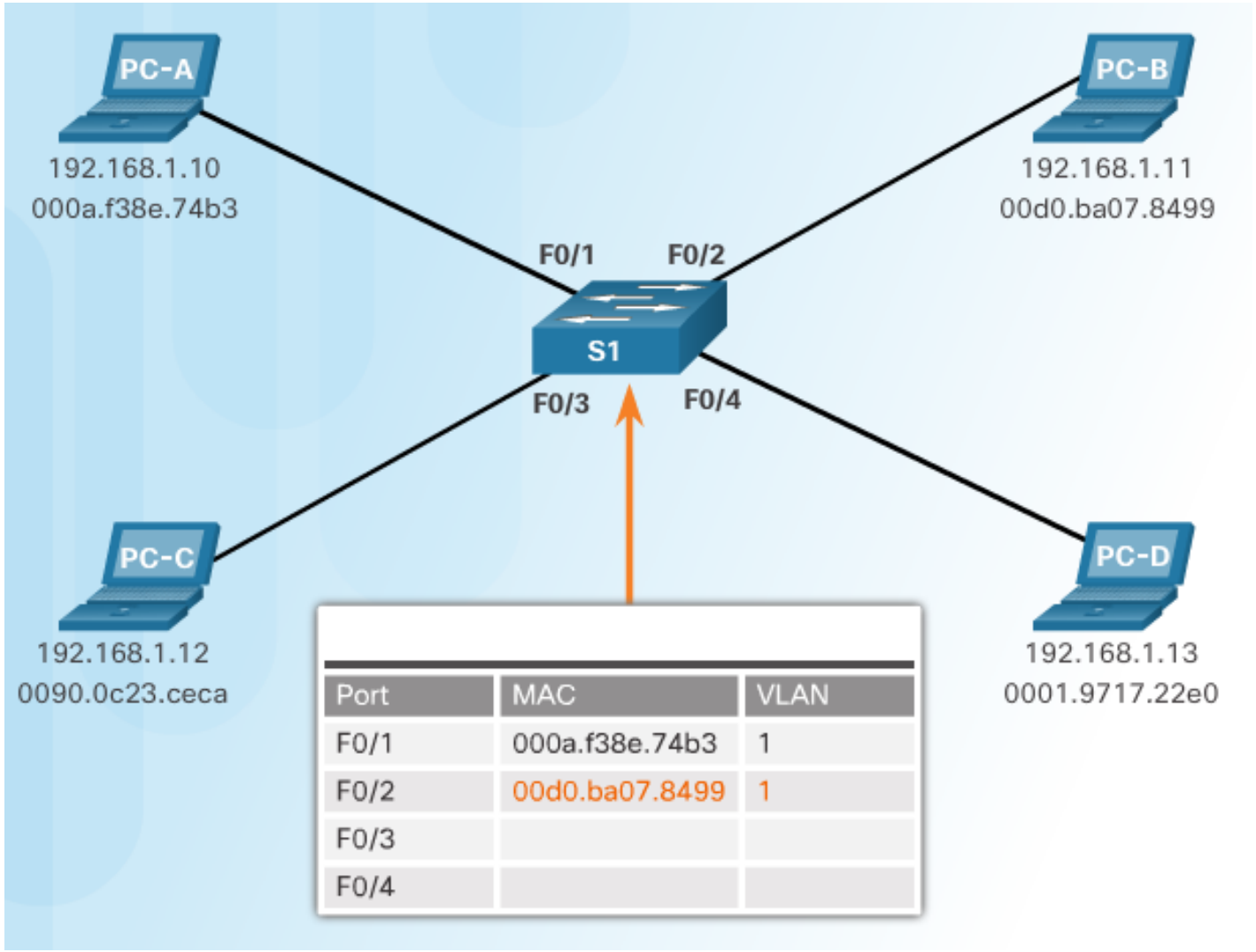
Switch Attack Categories

Topic 6.2.2:
CAM Table Attacks

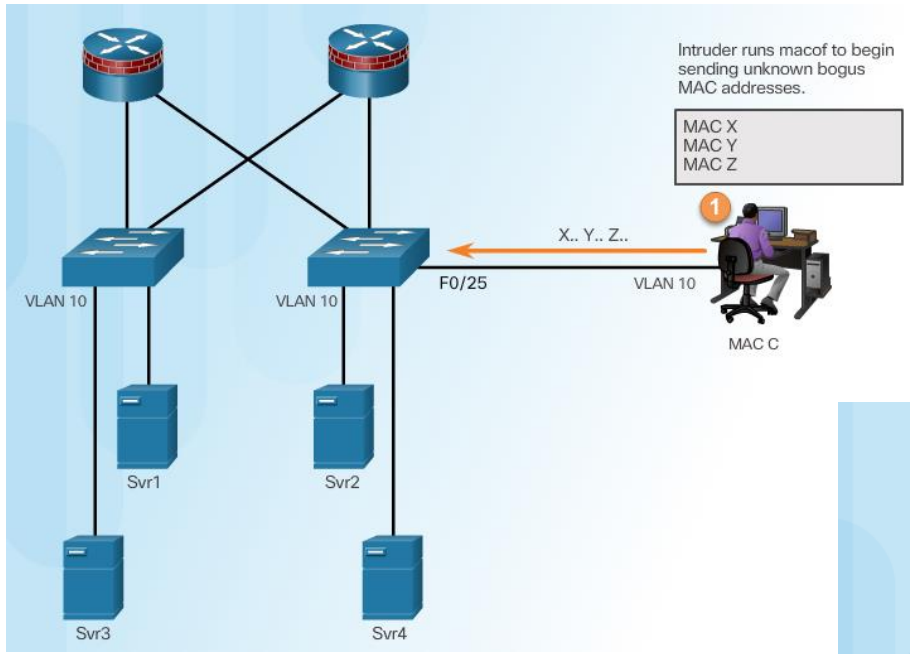
Basic Switch Operation

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

CAM Table Operation Example

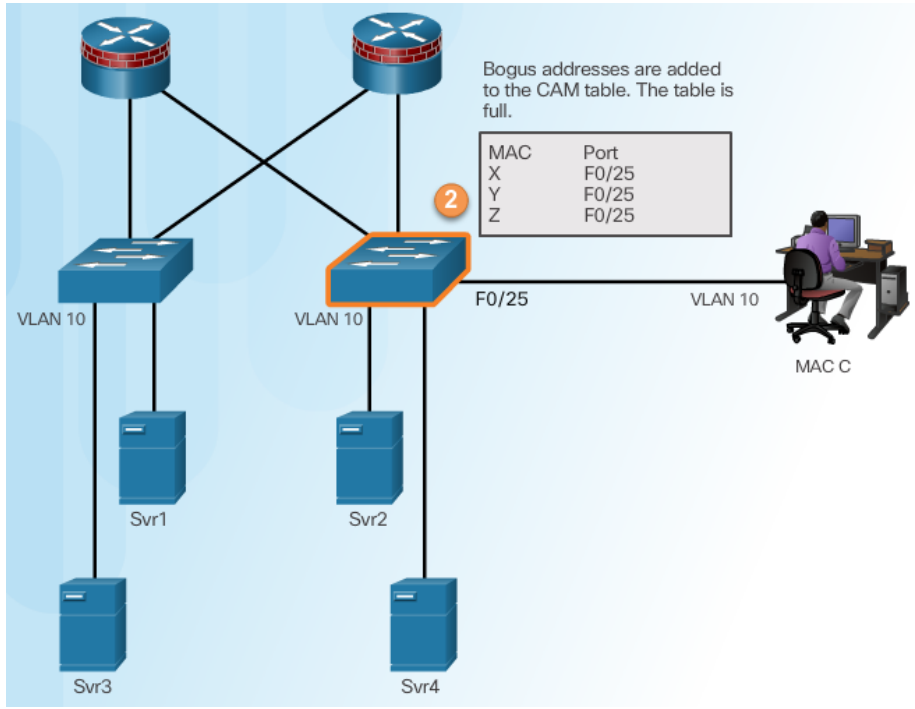


CAM Table Attack

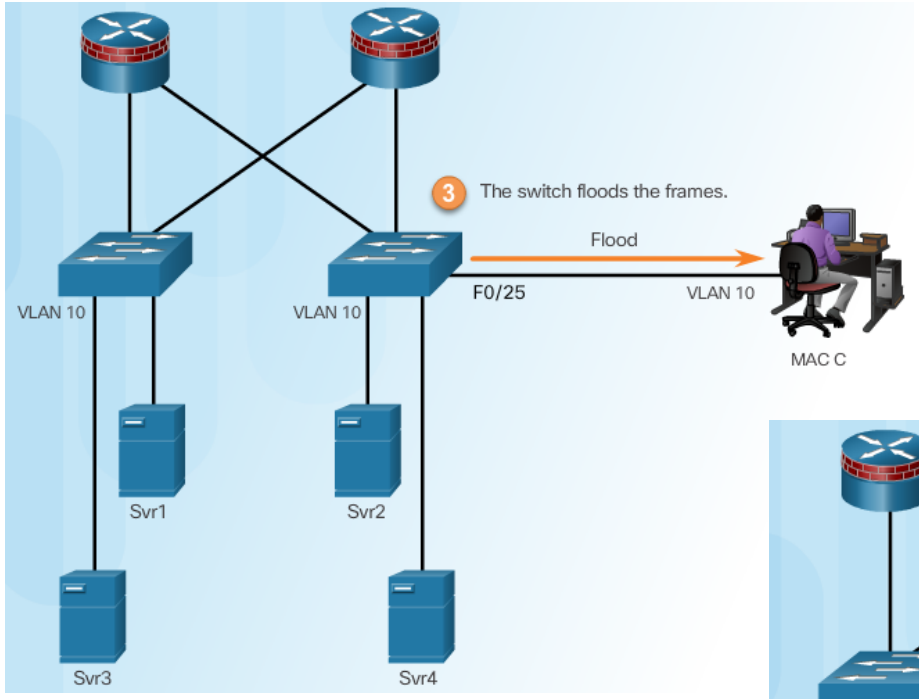


Intruder Runs Attack Tool

Fill CAM Table

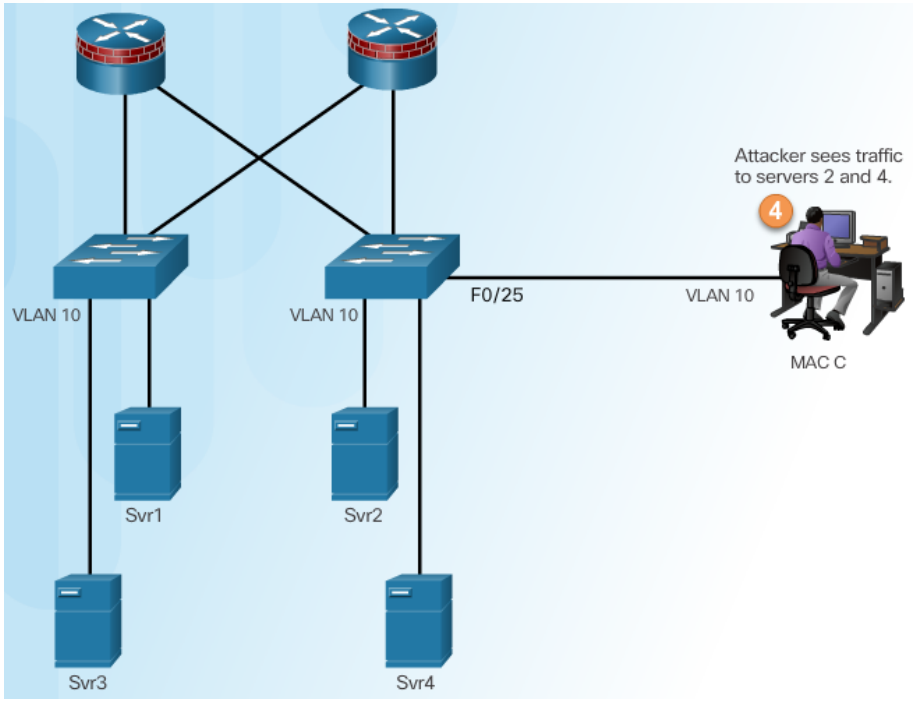


CAM Table Attack



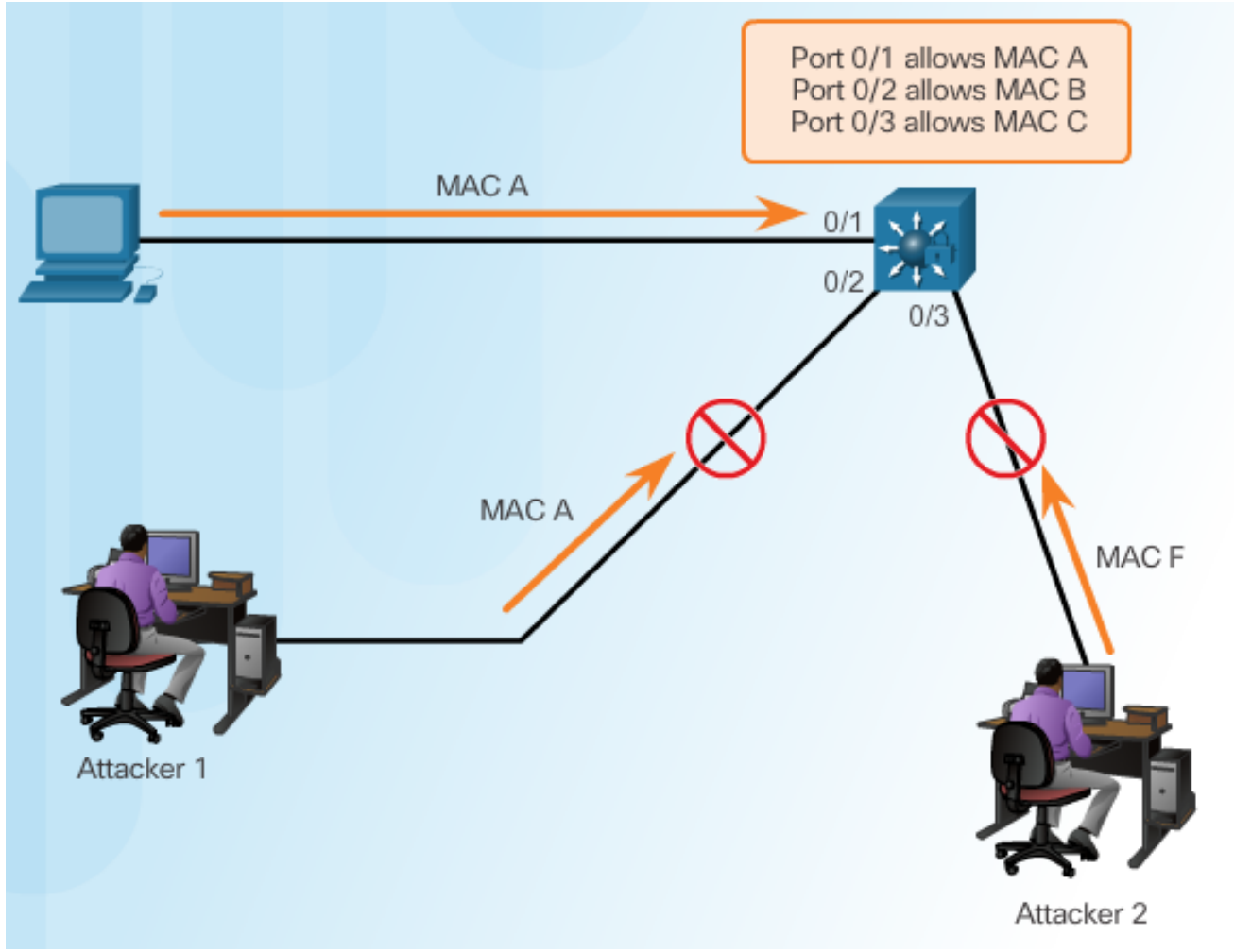
Switch Floods All Traffic

Attacker Captures Traffic



Topic 6.2.3:
Mitigating CAM Table Attacks

Countermeasure for CAM Table Attacks



Port Security

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Enabling Port Security

Verifying Port Security

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Port Security Options

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

S1(config-if)# switchport port-security
```

Enabling Port Security Options

Setting the Maximum Number of Mac Addresses

```
Switch(config-if)
switchport port-security maximum value
```

Manually Configuring Mac Addresses

```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Learning Connected Mac Addresses Dynamically

```
Switch(config-if)
switchport port-security mac-address sticky
```

Port Security Violations

Security Violation Modes:

- Protect
- Restrict
- Shutdown

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Port Security Aging

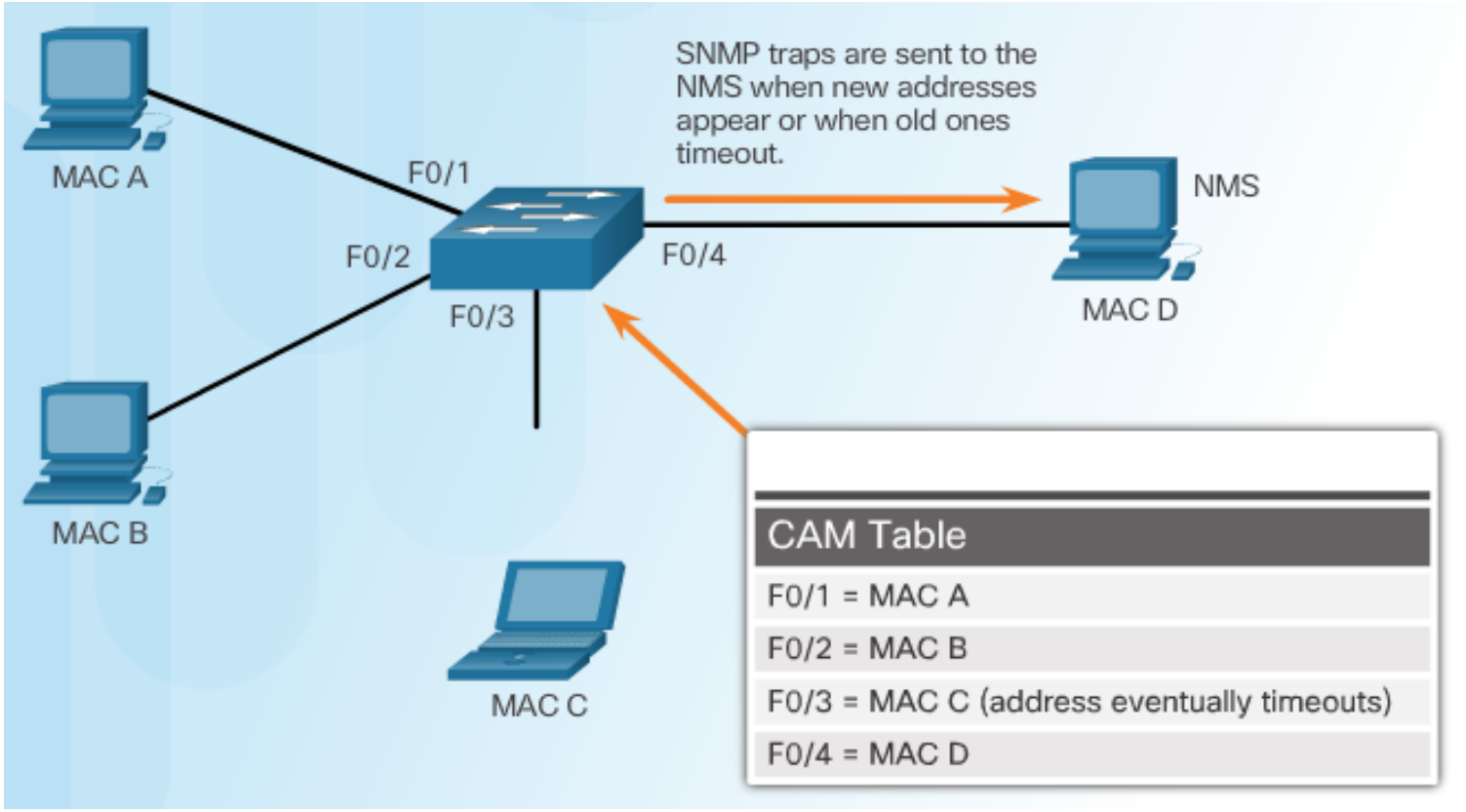
```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
time time	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
type absolute	• Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	• Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Port Security with IP Phones


```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

SNMP MAC Address Notification



Agenda

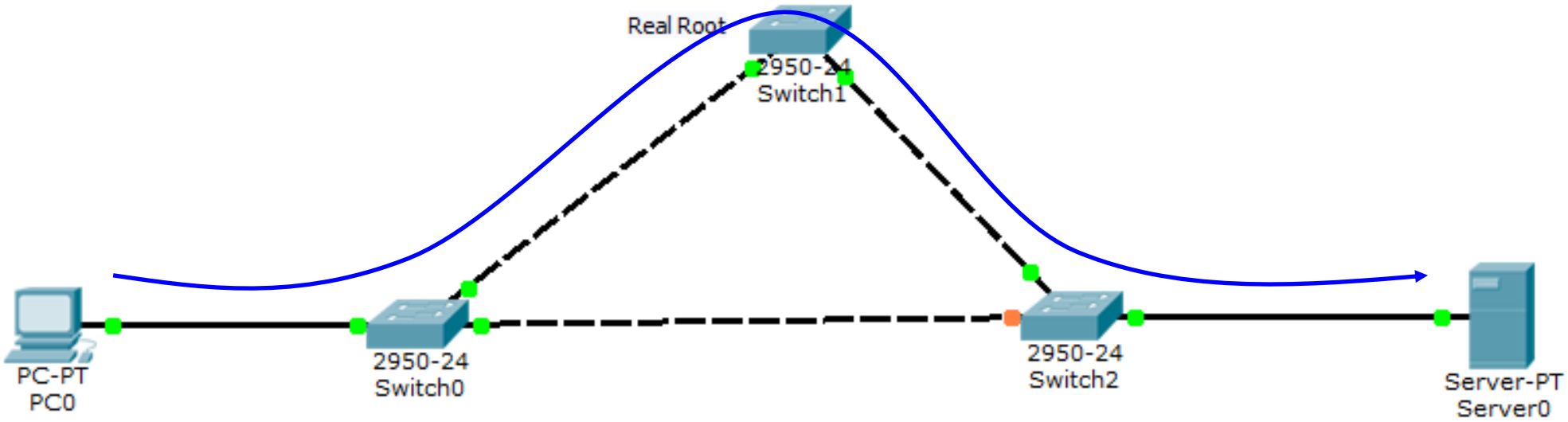
1. Attack the Root
2. DTP SMURF
3. DHCP 1 – starvation
4. DHCP 2 – spoofing
5. Attack Routing Protocol

INSTRUCTIONS for the ATTACKS

- It is foremost important for these attacks, that you only configure those features that is listed in the instructions!
- Carry out all the five attacks that are listed .
- At first create a new topology for each attack and save it as #.start where # is the sequence number of the attack.
- If the before topology is working correctly then please carry out the attack as it is described using the instructions.
- Then try to configure the countermeasure for that attack and save it as #.secured.neptuncode, where neptuncode is your code.
- I would like to receive these files form you, and I will try to carry out the attacks on these topologies.

ATTACK 1 - Attack the Root

- Attack the Root



Instructions for the 1. ATTACK

Configure IP addresses for PC0 and Server-PT from the same subnet range.

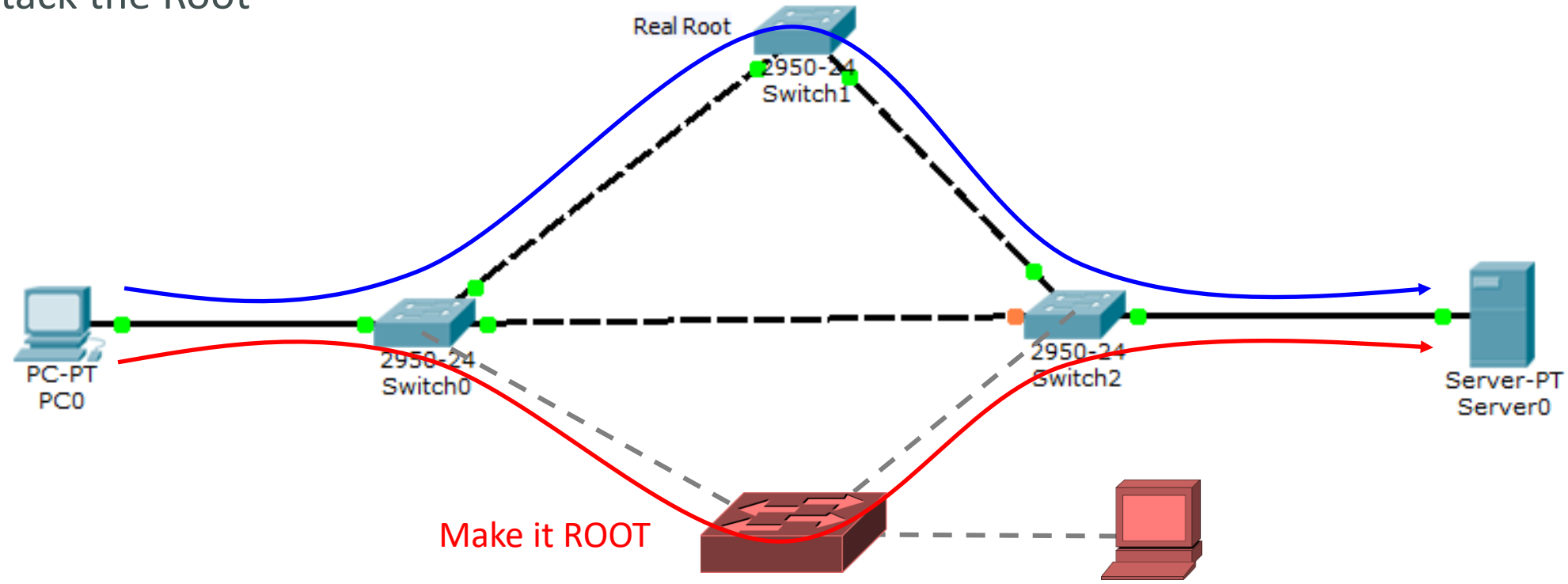
Configure trunk links between the switches and configure spanning-tree with default settings

Configure spanning-tree priority to 24576 on Switch1 (with the Spanning-tree priority command in VLAN 1

You managed to do it, when one of the leds is red on the link between Switch0 and Switch2! Check the path that packets take between PC0 and Server-PT in simulation mode. The blue line shows the paths that packets should take.

ATTACK 1 - Attack the Root

- Attack the Root



To carry out the 1st ATTACK:
Add a new switch to the topology, it is going to be the attacker,
Configure spanning-tree priority to become the root on this attacker switch. You have two choices:
Configure spanning tree priority on this switch to a lower value 24576, or configure spanning-tree root primary which ensures this situation.
Test again the paths that packets take from PC0 to Server. They should cross the Attacker switch.

The main problem with this attack

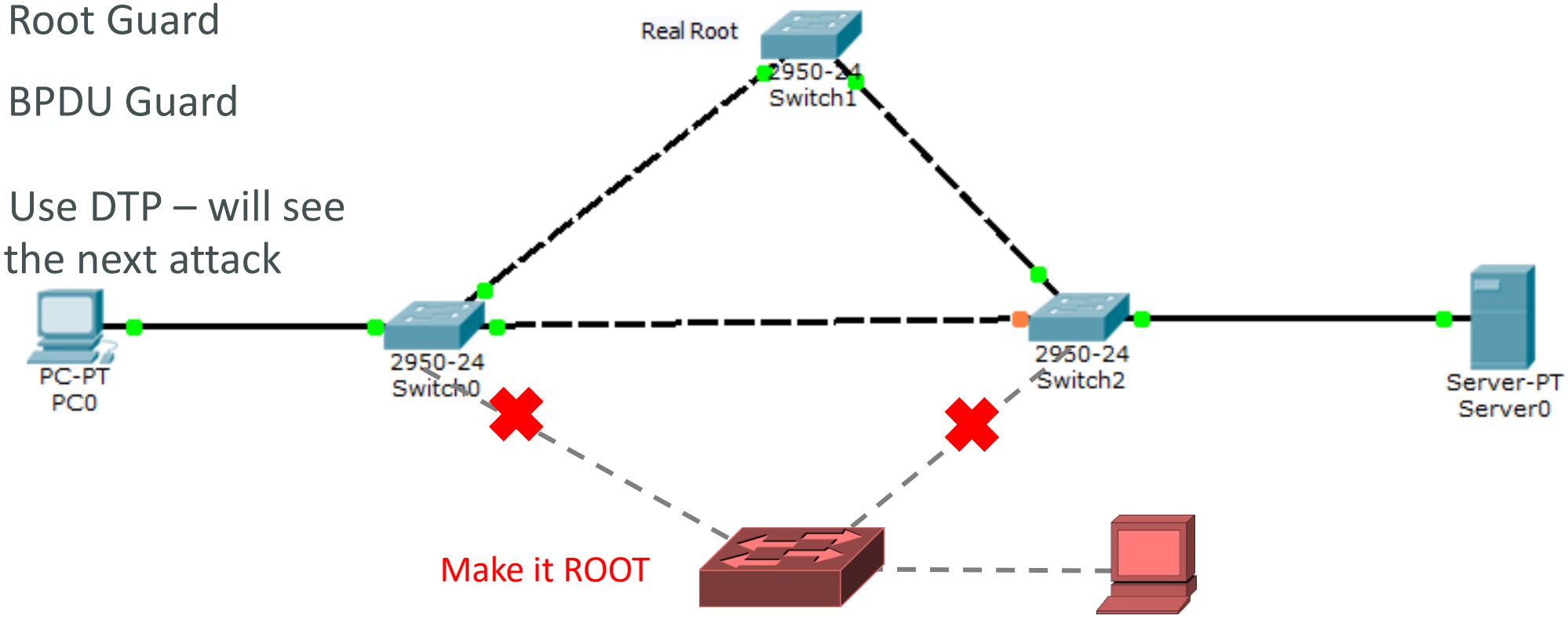
- The problem with this attack is that root switch has a special role in the netork, since most of the traffic is going to traverse the root switch!
- Therefore the root switch should be defended!
- An attacker that is connected to this switch with a packet sniffer can see most of the traffic.

Defense Mechanisms

Enable Root Guard

Enable BPDU Guard

Do not Use DTP – will see why in the next attack



As a defense mechanism configure root guard and bpdu guard where it is needed and disable DTP! For revision please look at the next two slides!

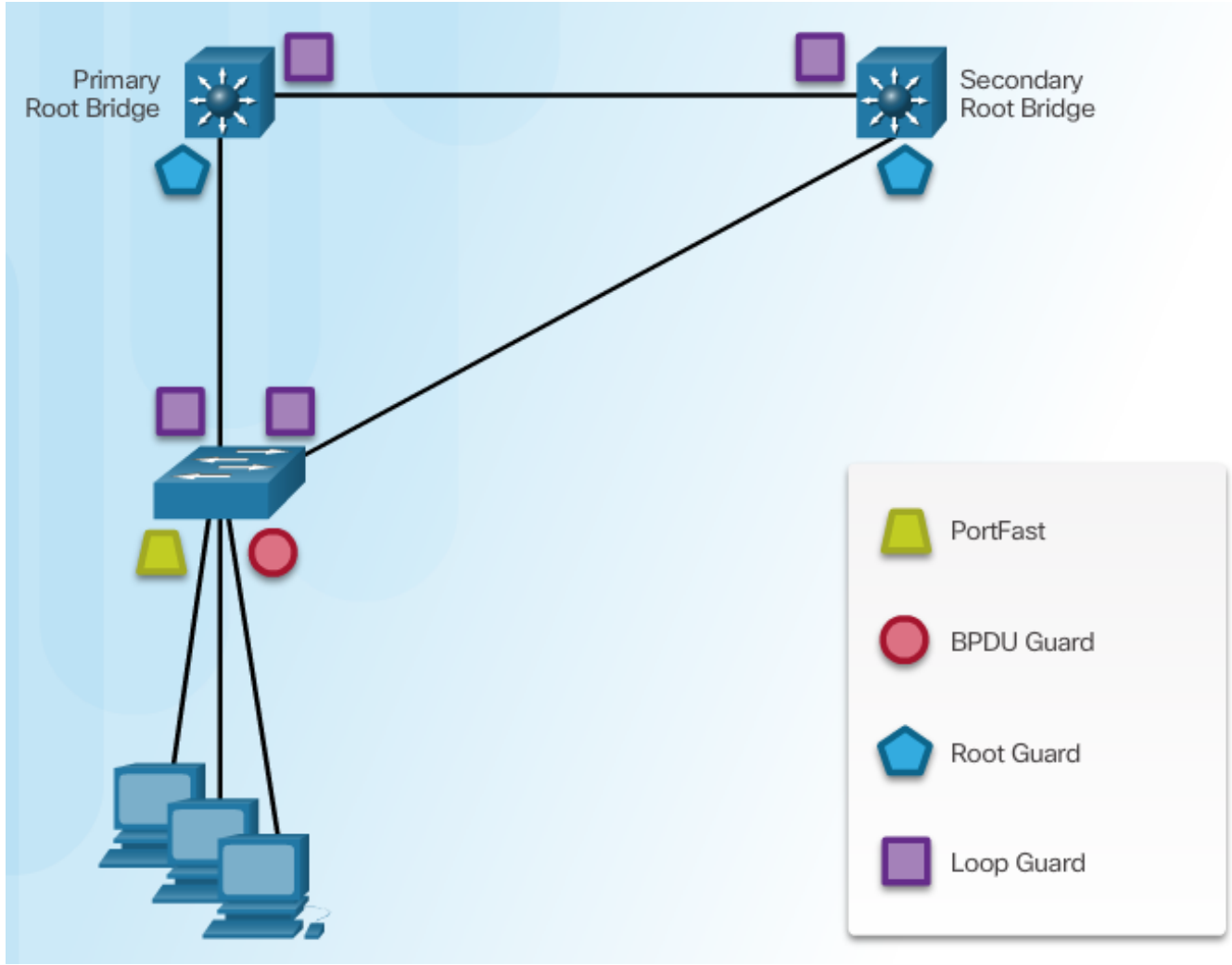
Mitigating STP Attacks

- **BPDU Guard** protects the integrity of ports that are PortFast-enabled. Also protects against additional switches added to the topology
  - Configure on all portfast enabled port (If PortFast is not configured, then BPDU Guard is not activated.)
  - Apply to all end-user ports.
- **Root Guard** is best deployed toward ports that connect to switches that should not be the root bridge. If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a root-inconsistent state (≈listening state)

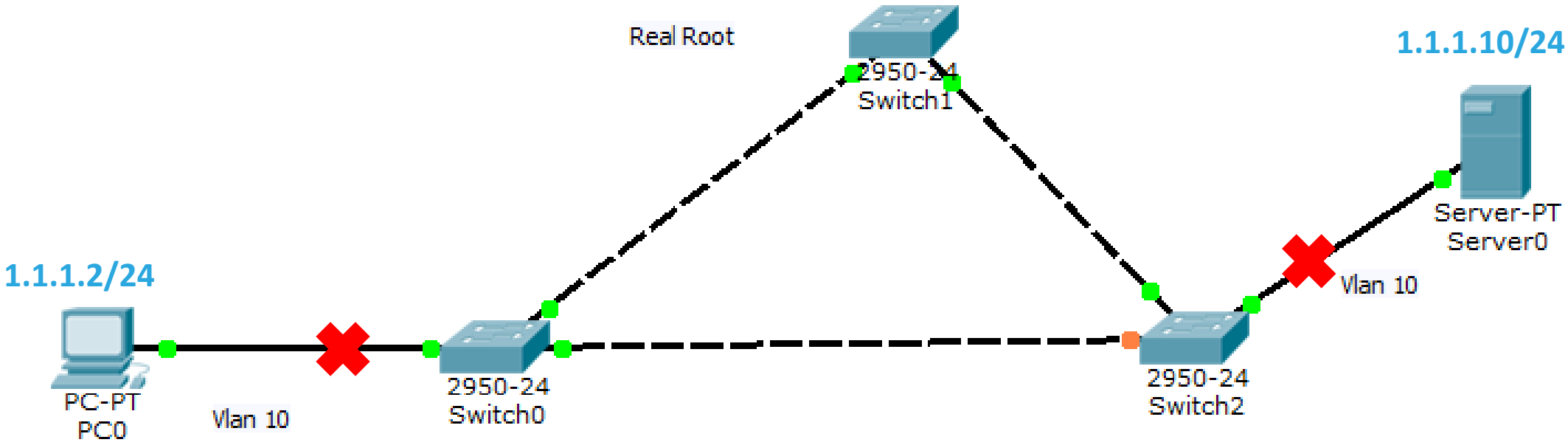
  Apply to all ports which should not become root ports.
- **Loop Guard** feature provides additional protection against Layer 2 loops. If BPDUs are not received on a non-designated Loop Guard-enabled port, the port transitions to a loop-inconsistent blocking state, instead of the listening / learning / forwarding state.

  Apply to all ports that are or can become non-designated.

Mitigating STP Attacks



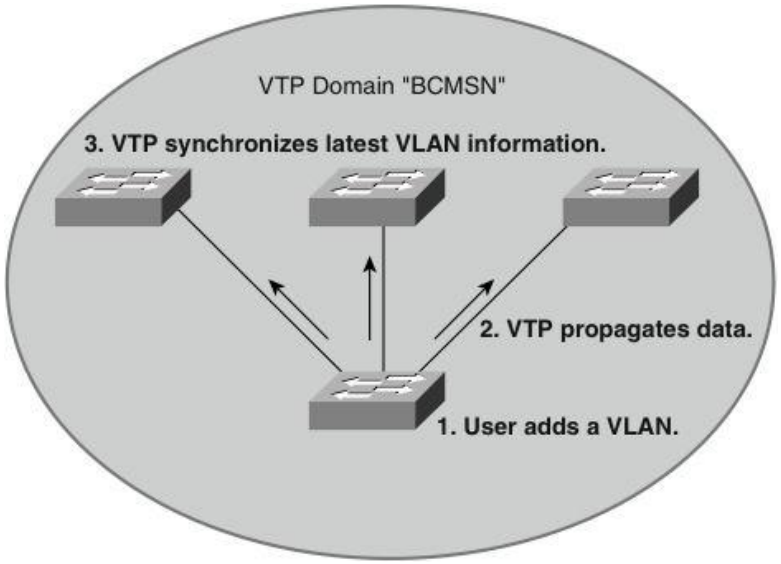
ATTACK 2 – DTP and VTP attack



For the starting topology, please

- Create this topology,
- Configure trunk links with the switchport mode trunk command between the switches.
- Configure vlan 10 on all 3 switches
- On Switch0 and Switch2 configure the appropriate portnumbers as access ports in VLAN 10
- Configure IP addresses on PC0 and Sever0 as shown in the topology
- Test your network! Ping from PC0 to Server0! It should be successful!
- The next 16 slides give revision about the VTP – VLAN Trunking Protocol. Please read it thoughtfully!

VLAN Trunking Protocol (VTP)

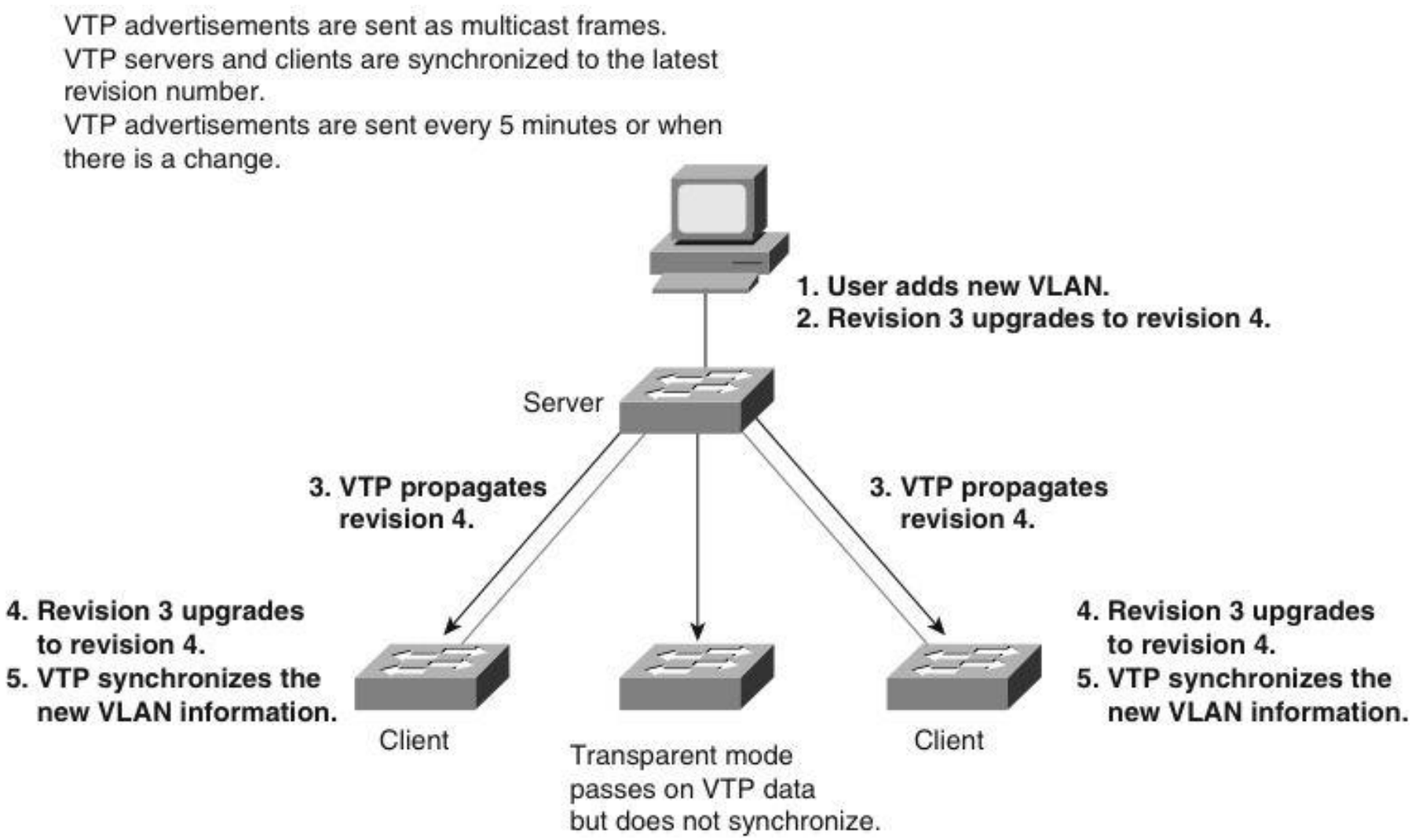


- VTP is a Cisco-proprietary protocol that automates the propagation of VLAN information between switches via trunk links. This minimizes misconfigurations and configuration inconsistencies.
- VTP does not configure switch ports for VLAN membership.
- Three types of VTP messages are sent via Layer 2 multicast on VLAN 1.
- VTP *domains* define sets of interconnected switches sharing the same VTP configuration.

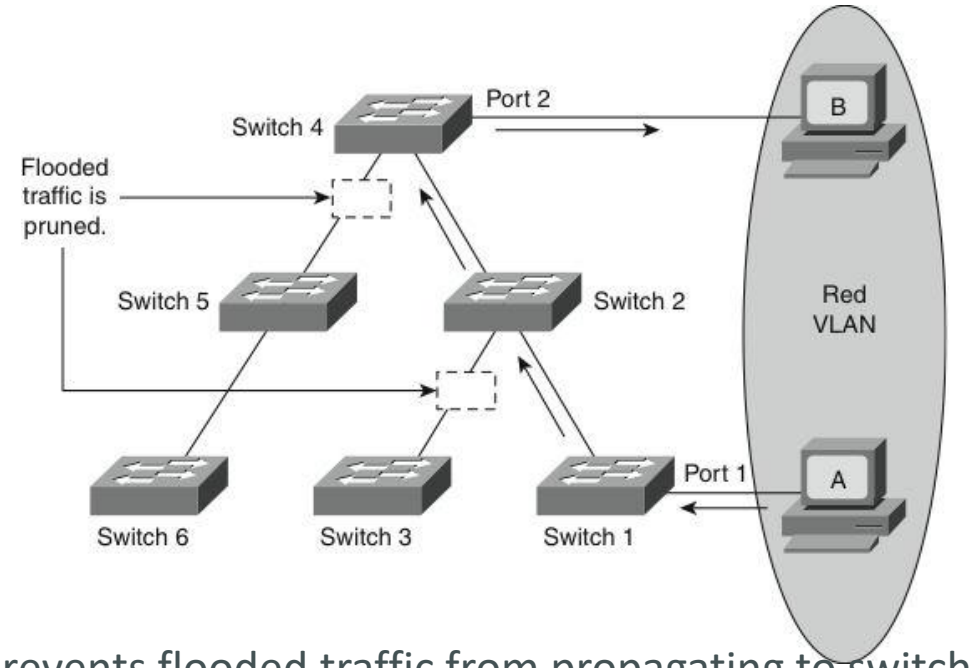
VTP Modes

Mode	Description
Client	• Cannot create, change, or delete VLANs on command-line interface (CLI). • Forwards advertisements to other switches. • Synchronizes VLAN configuration with latest information received from other switches in the management domain. • Does not save VLAN configuration in nonvolatile RAM (NVRAM).
Server	• Can create, modify, and delete VLANs. • Sends and forwards advertisements to other switches. • Synchronizes VLAN configuration with latest information received from other switches in the management domain. • Saves VLAN configuration in NVRAM.
Transparent	• Can create, modify, and delete VLANs only on the local switch. • Forwards VTP advertisements received from other switches in the same management domain. • Does not synchronize its VLAN configuration with information received from other switches in the management domain. • Saves VLAN configuration in NVRAM.

VTP Operation



VTP Pruning



- VTP pruning prevents flooded traffic from propagating to switches that do not have members in specific VLANs.
- VTP pruning uses VLAN advertisements to determine when a trunk connection is flooding traffic needlessly. Switches 1 and 4 in the figure support ports statically configured in the Red VLAN.
- The broadcast traffic from Station A is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated on Switches 2 and 4.

VTP

- Three VTP versions: V1, V2, V3.
- Versions are not interoperable (e.g., V2 supports token ring VLANs but V1 does not).
- V1 transparent switches inspect VTP messages for the domain name and version and forward a message only if the version and domain name match.
- V2 transparent switches forward VTP messages in transparent mode without checking versions.
- V3
- Support for extended VLANs (1025 to 4094)
  - Support for the creation and advertising of Private VLANs
  - Improved server authentication
  - Enhancements to a mechanism for protection from the “wrong” database accidentally being inserted into a VTP domain
  - Interaction with VTP versions 1 and 2
  - Configurable on a per-port basis

VTP Message Types

- Summary Advertisements
- Subset Advertisements
- Advertisement Requests

VTP Summary Advertisements

- By default, Catalyst switches issue summary advertisements in 5-minute increments. Summary advertisements inform adjacent switches of the current VTP domain name and the configuration revision number.
- When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent.

VTP Subset Advertisements

- When you add, delete, or change a VLAN, the VTP server where the changes are made increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement.
- A subset advertisement contains a list of VLAN information. If there are several VLANs, more than one subset advertisement can be required to advertise all the VLANs.

VTP Advertisement Requests

- A switch issues a VTP advertisement request in these situations:

  The switch has been reset.

  The VTP domain name has been changed.

  The switch has received a VTP summary advertisement with a higher configuration revision than its own.

- Upon receipt of an advertisement request, a VTP device sends a summary advertisement.
- One or more subset advertisements follow the summary advertisement.

Advertisement Request			
Version	Code	Rvsd	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start Value			

VTP Authentication

- VTP domains can be secured by using the VTP password feature. It is important to make sure that all the switches in the VTP domain have the same password and domain name; otherwise, a switch will not become a member of the VTP domain. Cisco switches use MD5 to encode passwords in 16-byte words. These passwords propagate inside VTP summary advertisements. In VTP, passwords are case-sensitive and can be 8 to 64 characters in length. The use of VTP authentication is a recommended practice.
- By default, a Catalyst switch does not have a VTP password. The switch does not automatically set the password parameter, unlike other parameters that are set automatically when a VTP advertisement is received.

Configuring VTP

- **Step 1.** Enter global configuration mode:

```
Switch# configure terminal
```

- **Step 2.** Configure the VTP mode as server:

```
Switch(config)# vtp mode server
```

- **Step 3.** Configure the domain name:

```
Switch(config)# vtp domain domain_name
```

- **Step 4.** (Optional.) Enable VTP version 2:

```
Switch(config)# vtp version 2
```

- **Step 5.** (Optional.) Specify a VTP password:

```
Switch(config)# vtp password password_string
```

- **Step 6.** (Optional.) Enable VTP pruning in the management domain:

```
Switch(config)# vtp pruning
```


VTP Configuration Example

- This example creates a VTP server with domain name `Modular_Form`, password `genus`, and pruning enabled.

```
Switch# configure terminal
Switch(config)# vtp mode server
Setting device to VTP SERVER mode.
Switch(config)# vtp domain Modular_Form
Switch(config)# vtp password genus
Switch(config)# vtp pruning
Switch(config)# end
```

Verifying VTP Configuration (1)

- The most useful command for verifying VTP configuration is the **`show vtp status`** command. The output displayed includes the VTP version, the VTP configuration revision number, the number of VLANs supported locally, the VTP operating mode, the VTP domain name, and the VTP pruning mode.

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode : Server
VTP Domain Name : Modular_Form
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:4
```

Verifying VTP Configuration (2)

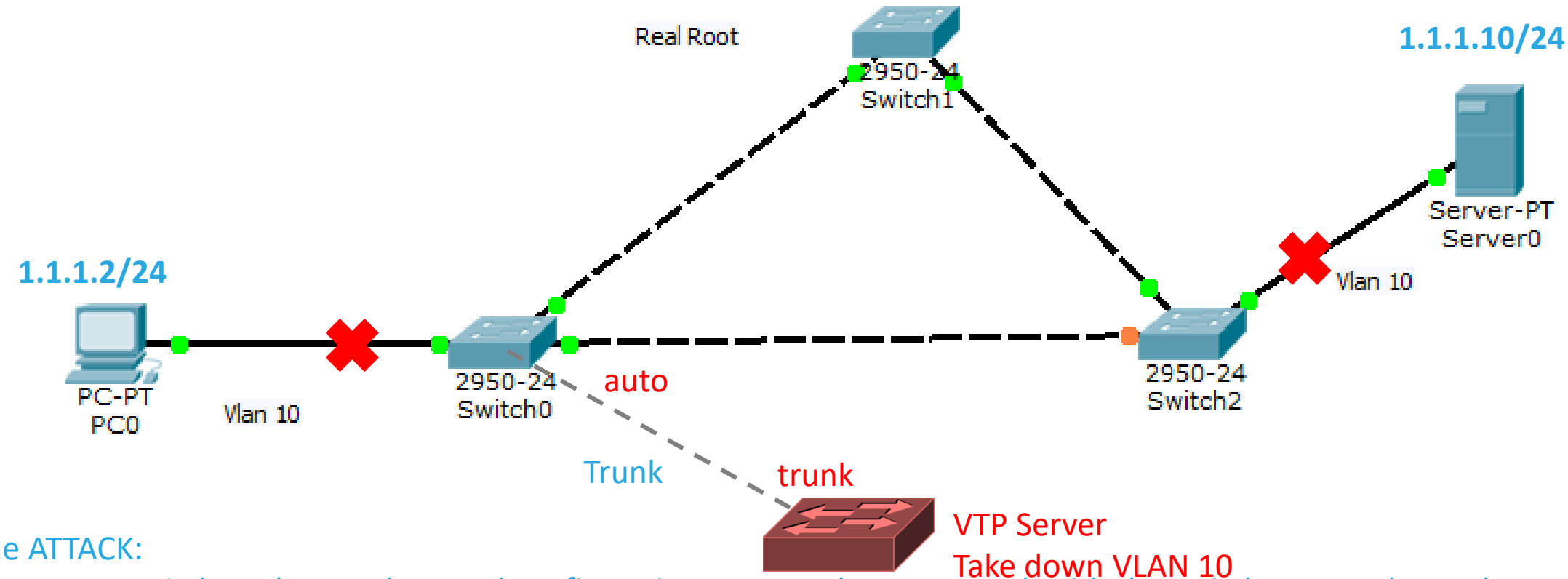
- Use the **`show vtp counters`** command to display statistics about VTP operation. If there are any problems regarding the VTP operation, this command helps look for VTP message type updates.

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received : 7
Subset advertisements received : 5
Request advertisements received : 0
Summary advertisements transmitted : 997
Subset advertisements transmitted : 13
Request advertisements transmitted : 3
Number of config revision errors : 0
Number of config digest errors : 0
Number of V1 summary errors : 0

VTP pruning statistics:

Trunk  Join Transmitted  Join Received  Summary advts received from non-pruning-capable
device
------ ----------------  -------------  -----------------
Fa5/8     43071               42766              5
```

VTP Troubleshooting

- Check that switches are interconnected by active trunk links.
- Check that the trunking protocol matches on opposite ends of a trunk link.
- Check VTP domain name (case-sensitive) and password.
- Check the VTP mode of the switches.
- Check the VTP versions of the switches.

ATTACK 2 – DTP, VTP



For the ATTACK:

- Give a new switch to the topology and configure its connected port as trunk with the switchport mode trunk command
- Do not configue anything else on Switch0, Switch1, Switch2, you only have to configure the attacker switch
- With the vtp domain name command give a name to the domain, e.g.: vtp domain name attacked
- Add a new vlan e.g.: vlan 20 on the attacker switch
- Check the other switches that they received this information and synchronized their vlan database with show vlan brief command
- Delete vlan 10 on attacker switch with no vlan 10 command. Test the results!

About the ATTACK 2.

- The point of this attack is that connecting with an attacker switch shown in the topology, beacuse of the by default enabled DTP on all ports, an attacker can form the new connection to trunk, and on trunk connection the VTP protocol can be used to propagate VLAN information. If the default settings remained on all 3 switches for VTP, then a newly connected switch can take down the connection between PC0 and Server0, because it can change VLAN infromation, for example it can delete the VLAN 10 from all switches.
- Why is it possible? It is possible only in that case when no vtp domain were configured before on the switches.
- If the attacker sets a domain name on it’s switch then this domain name will be propagated through the trunk links to all switches. All other switches will have the same domain name, and from that point they are in the same domain, they are all servers, so they will propagate changes and synchronize their databases.

Defense Mechanisms

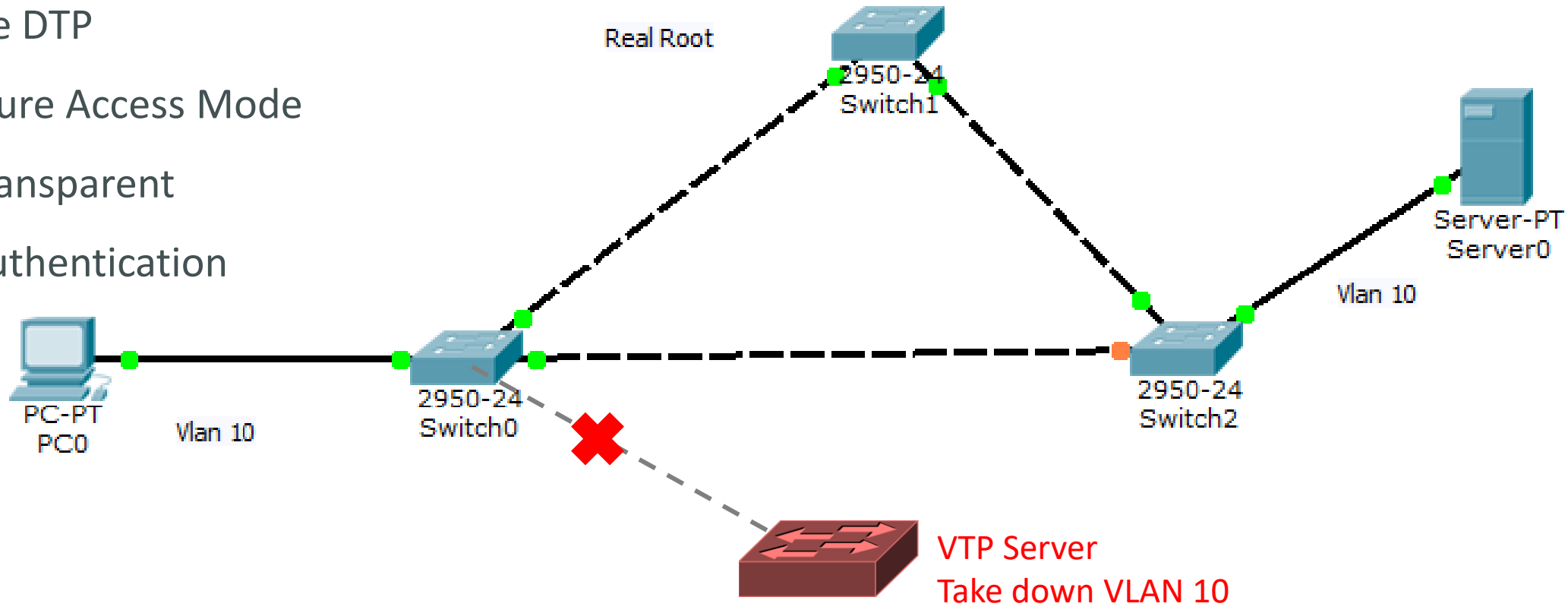
Shutdown unused port, Dot1x, PortSec

Disable DTP

Configure Access Mode

VTP Transparent

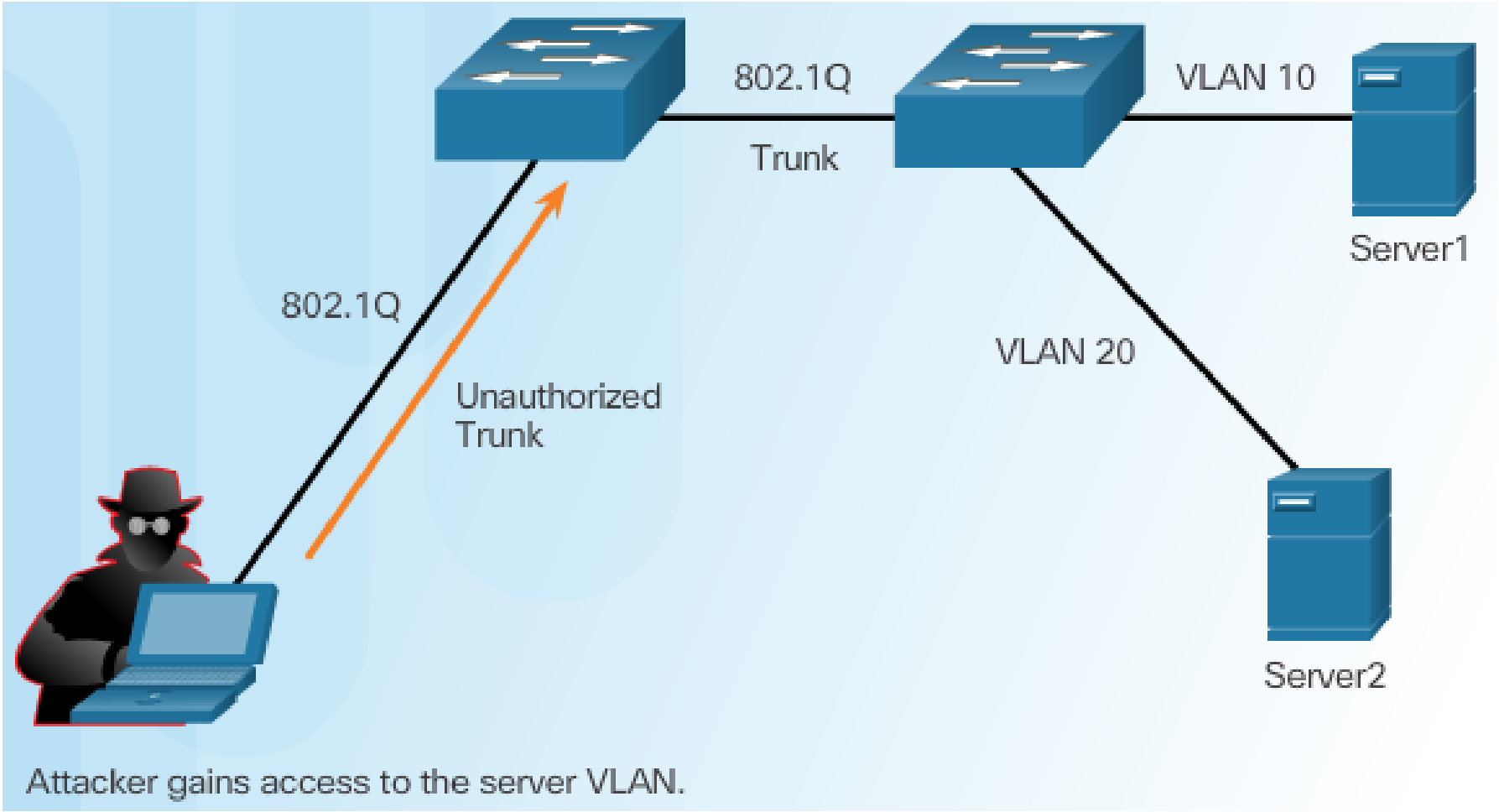
VTP Authentication



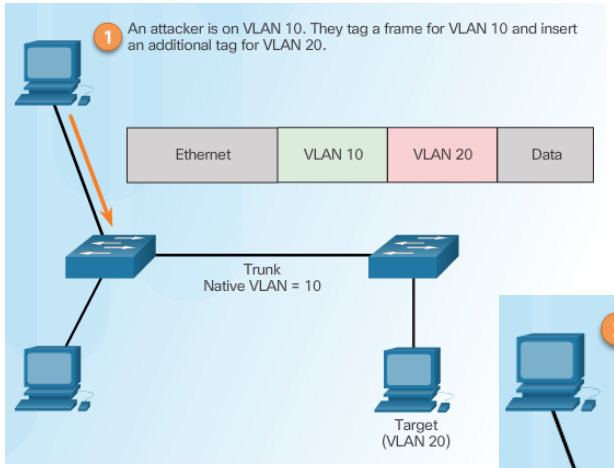
As a defense method configure vtp mode as transparent on all 3 switches, or configure VTP authentication! And disable DTP with the switchport nonegotiate command!

Topic 6.2.4:
Mitigating VLAN Attacks

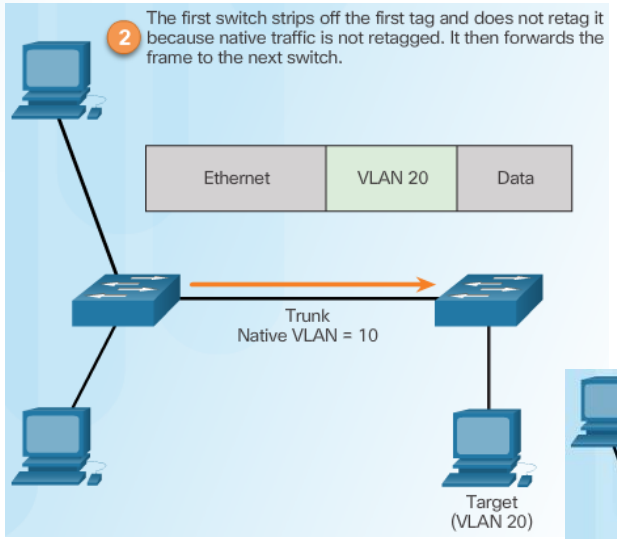
VLAN Hopping Attacks



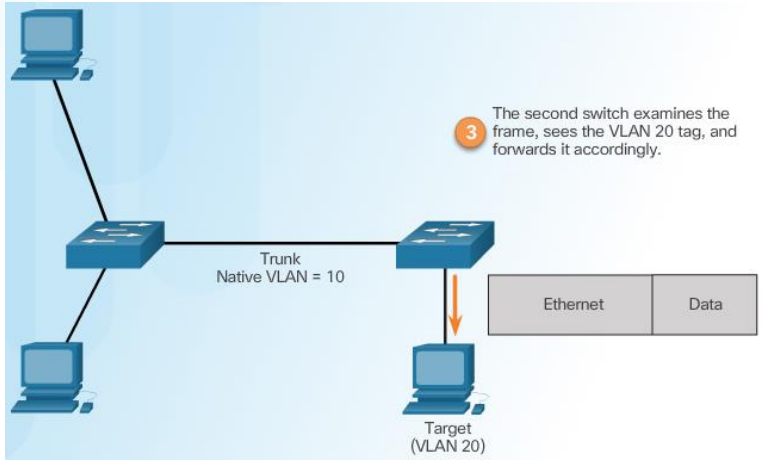
VLAN Double-Tagging Attack



Step 1 – Double Tagging Attack

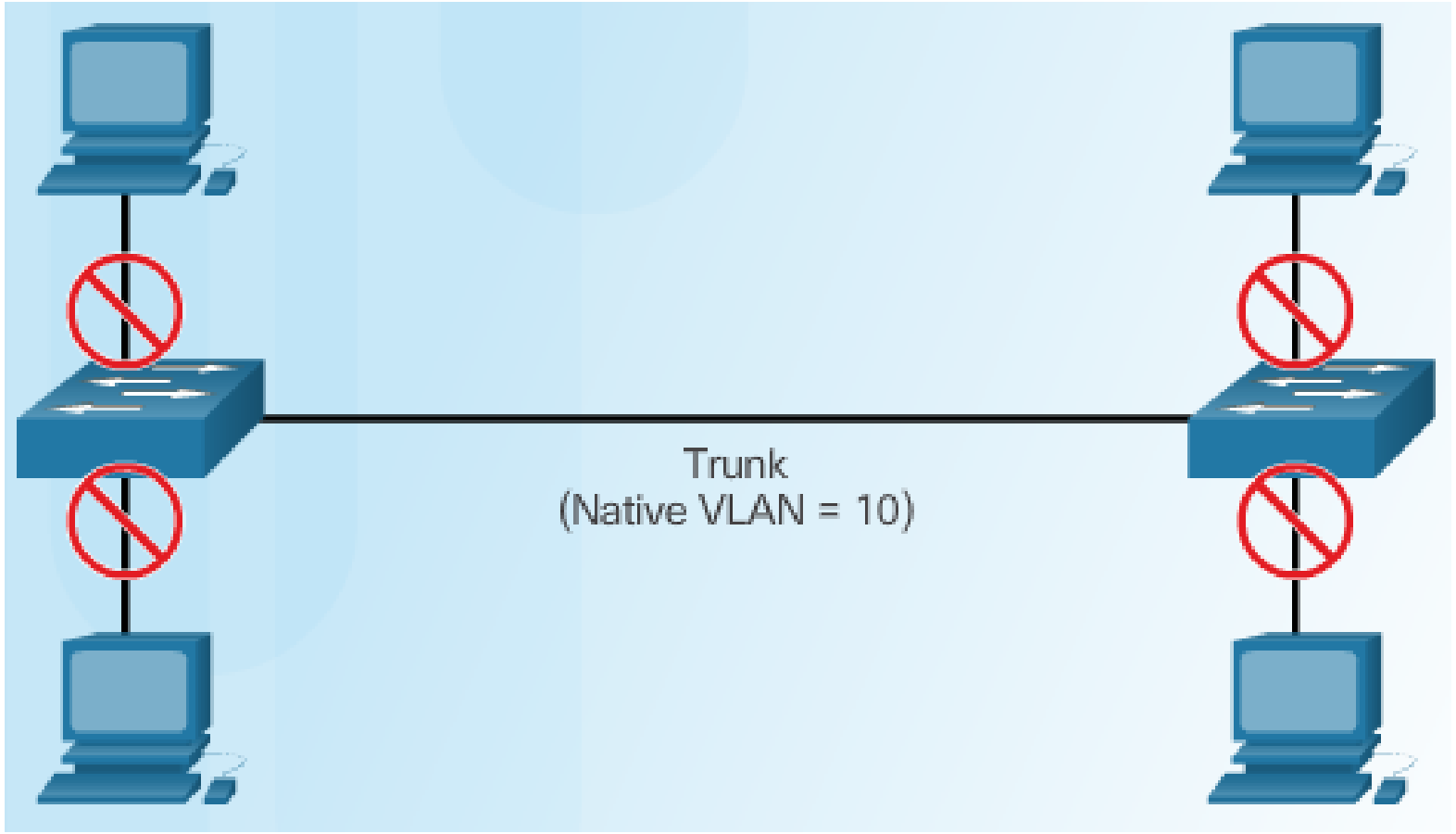


Step 2 – Double Tagging Attack



Step 3 – Double Tagging Attack

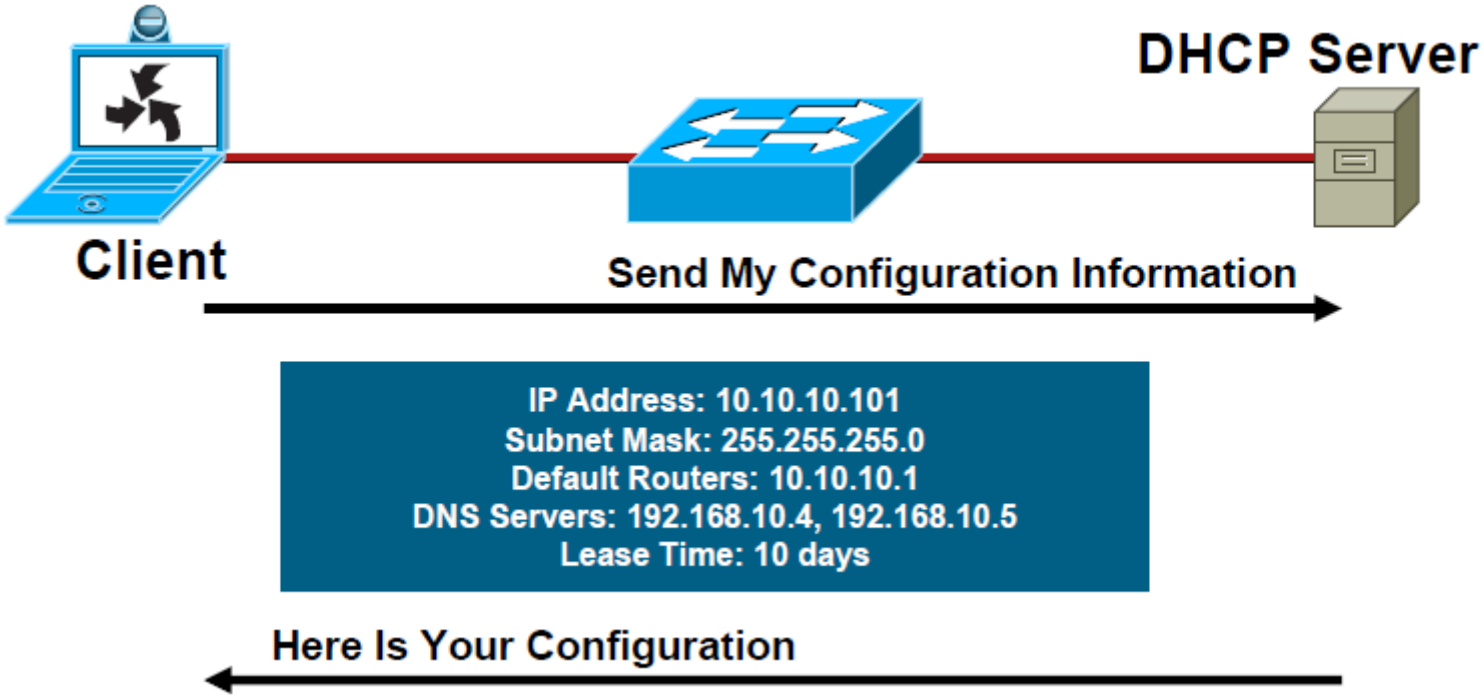
Mitigating VLAN Hopping Attacks



Mitigating VLAN Hopping Attacks

- Disable DTP (auto trunking) negotiations on non-trunking ports by using the **switchport mode access** interface configuration command.
- Manually enable the trunk link on a trunking port using the **switchport mode trunk** interface configuration command.
- Disable DTP (auto trunking) negotiations on trunking ports using the **switchport non-negotiate** interface configuration command.
- Set the native VLAN to be something other than VLAN 1 and to be set on an unused VLAN using the **switchport trunk native vlan** *vlan_number* interface configuration mode command.
- Disable unused ports and put them in an unused VLAN.

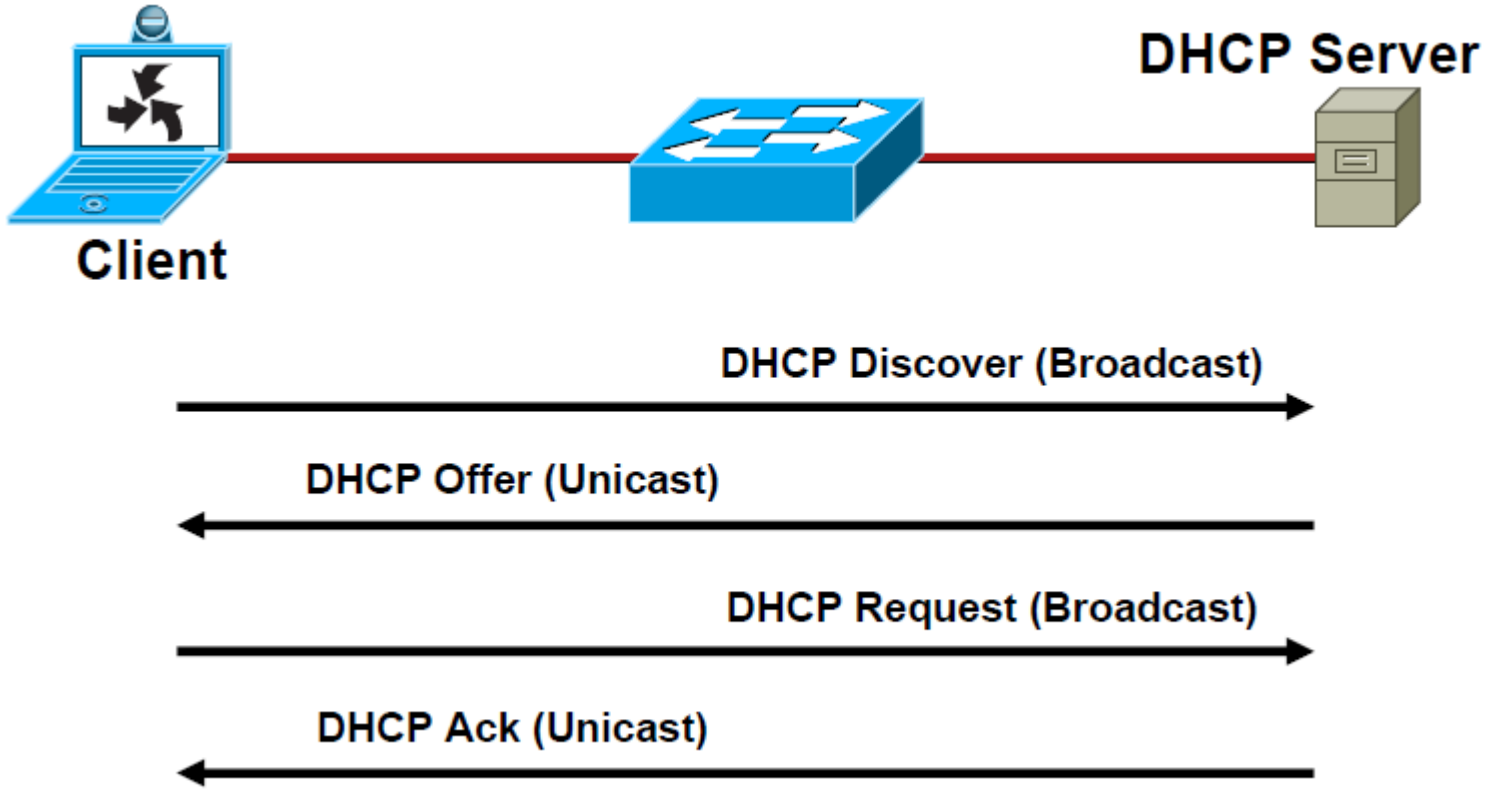
DHCP Function High Level



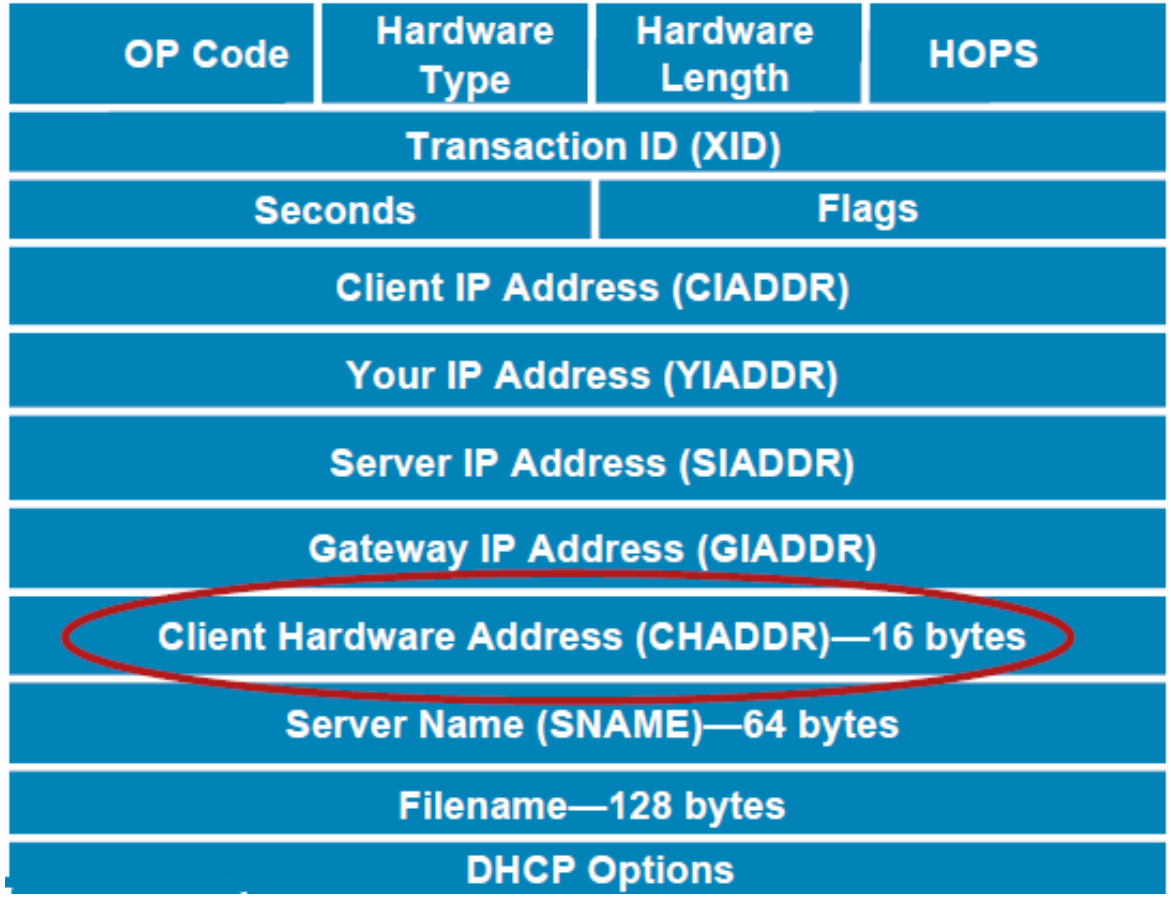
Server dynamically assigns IP address on demand
Administrator creates pools of addresses available for assignment
Address is assigned with lease time
DHCP delivers other configuration information in options

DHCP Function Low Level

- RFC 2131



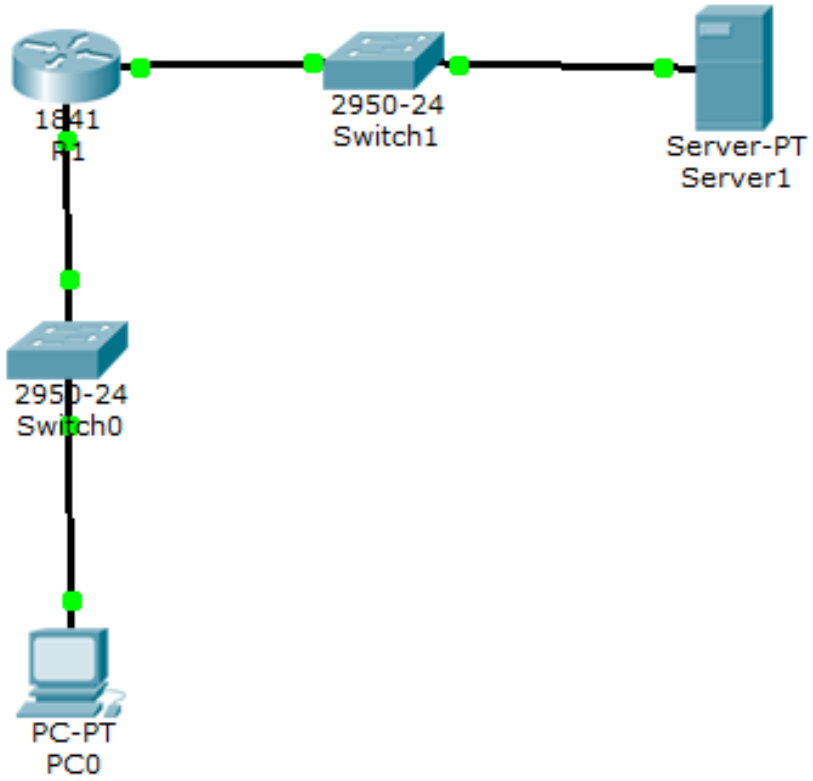
DHCP Function Low Level



DHCP Messages

Message	Use
DHCPDISCOVER	Client Broadcast to Locate Available Servers
DHCPOFFER	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPREQUEST	Client Message to Servers Either (a) Requesting Offered Parameters from One Server and Implicitly Declining Offers from All Others, (b) Confirming Correctness of Previously Allocated Address After, e.g., System Reboot, or (c) Extending the Lease on a Particular Network Address
DHCPACK	Server to Client with Configuration Parameters, Including Committed Network Address
DHCPNAK	Server to Client Indicating Client's Notion of Network Address Is Incorrect (e.g., Client Has Moved to New Subnet) or Client's Lease As Expired
DHCPDECLINE	Client to Server Indicating Network Address Is Already in Use
DHCPRELEASE	Client to Server Relinquishing Network Address and Canceling Remaining Lease
DHCPINFORM	Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address.

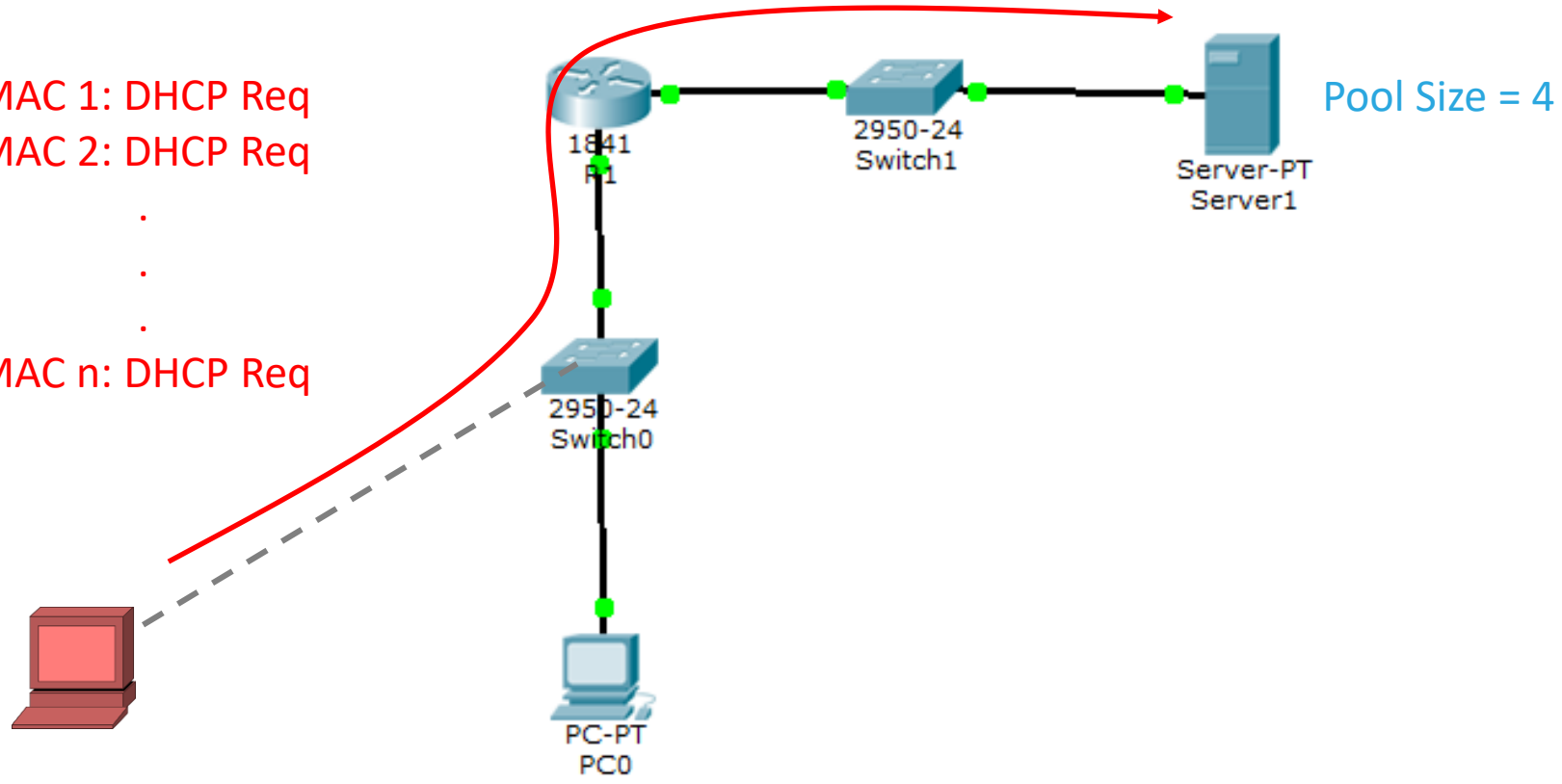
ATTACK 3 - DHCP STARVATION



Pool Size = 4

ATTACK 3 - DHCP - You do not have to configure this attack!

MAC 1: DHCP Req
MAC 2: DHCP Req
.
.
.
MAC n: DHCP Req



Pool Size = 4

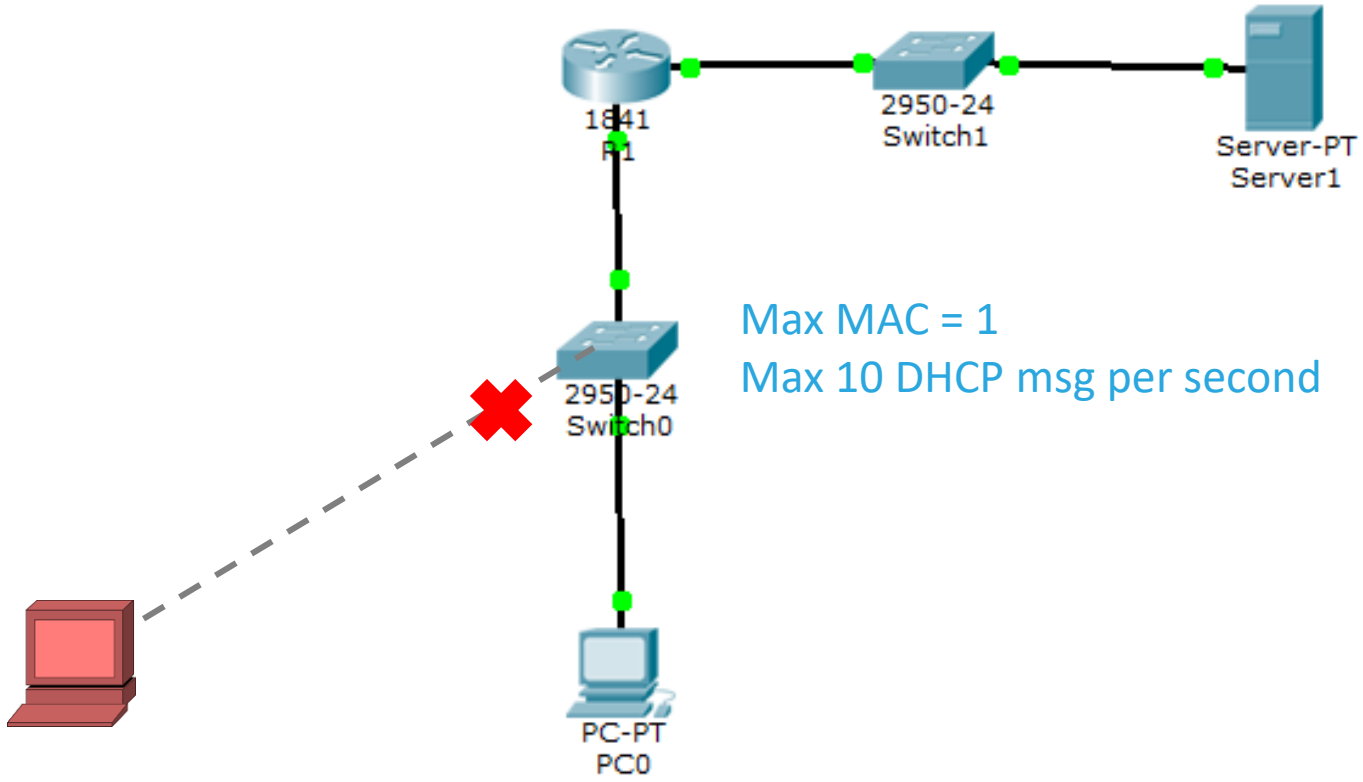
MAC Spoofing
Consume all IP addresses

Defense Mechanisms

Use Port Security

Use Dot1x Authentication

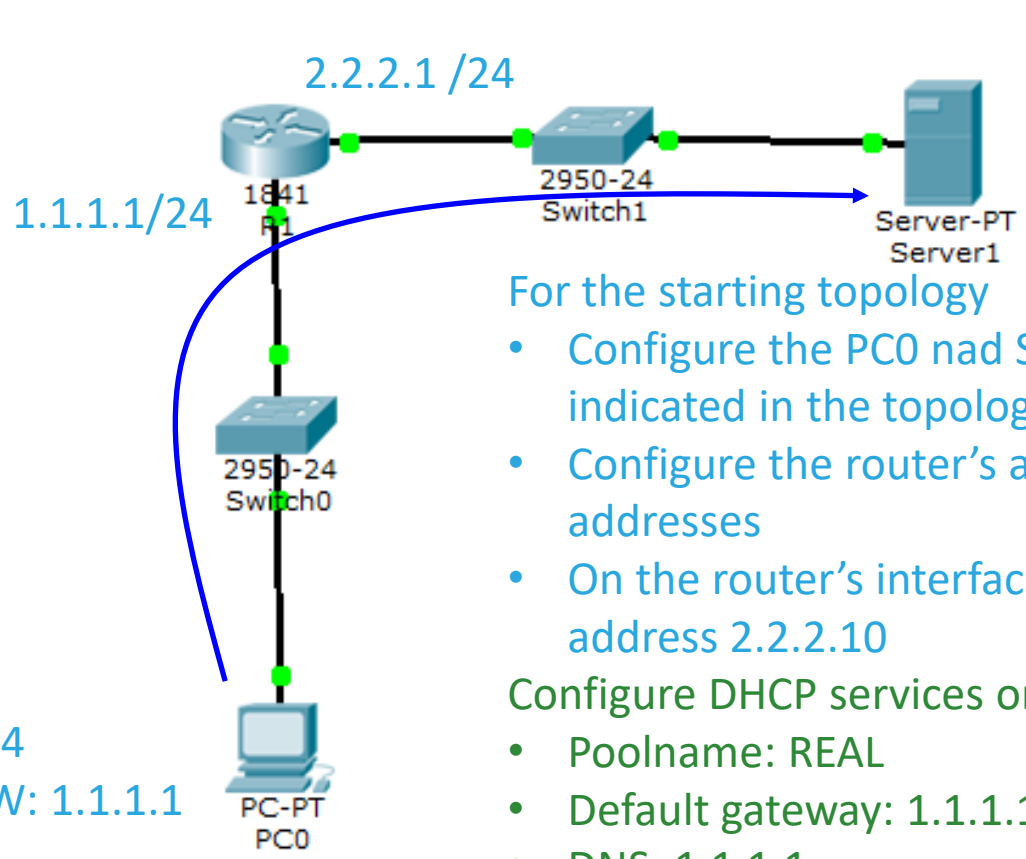
DHCP snooping rate limit



Max MAC = 1
Max 10 DHCP msg per second

Enable dhcp snooping
Enable dhcp snooping for vlan 1
Define interface as trust
Configure limit rate for an interface

ATTACK 4 - DHCP spoofing



For the starting topology

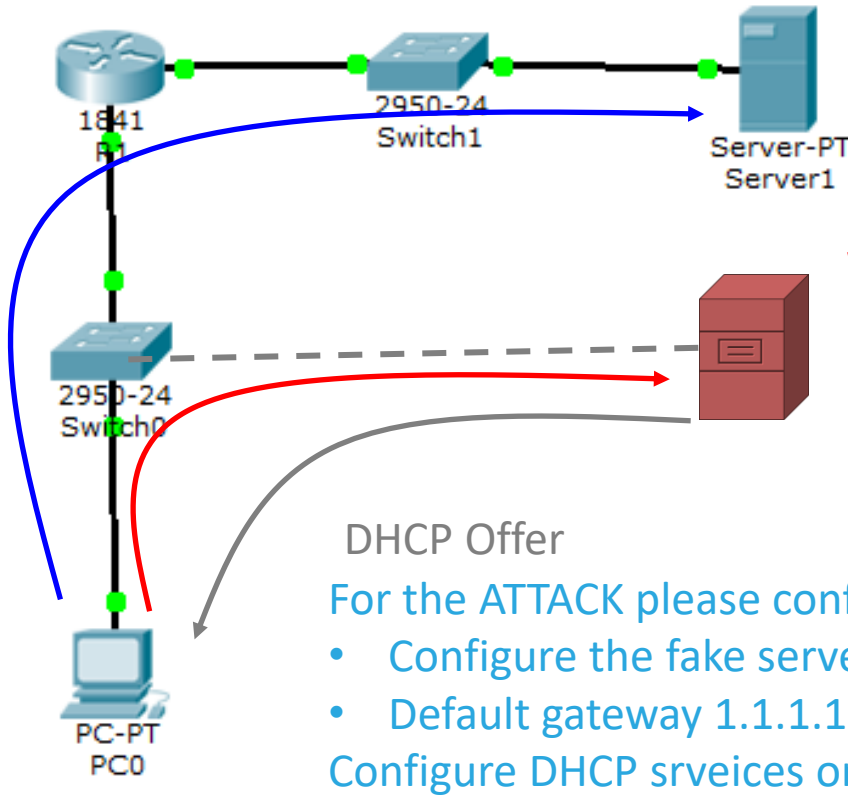
- Configure the PC0 nad Server1 IP addresss and default gateway address as indicated in the topology
- Configure the router's appropriate interfaces with the provided IP addresses
- On the router's interface facing towards PC0 please configure IP-helper address 2.2.2.10

Configure DHCP services on Server-1 with he following parameters:

- Poolname: REAL
- Default gateway: 1.1.1.1
- DNS: 1.1.1.1
- Start IP 1.1.1.11
- Subnet mask: 255.255.255.0 Then click add!

Test the operation, set the IP address settings to dynamic on Pc0!

ATTACK 4 - DHCP SPOOFING



www.real.com

Webserver www.real.com (fake)
DNS Server
DHCP Server

DHCP Offer

For the ATTACK please configure a FAKE DHCP server connected to Switch0

- Configure the fake server with IP address: 1.1.1.2/24
- Default gateway 1.1.1.1

Configure DHCP srveices on this fake server with the following settings:

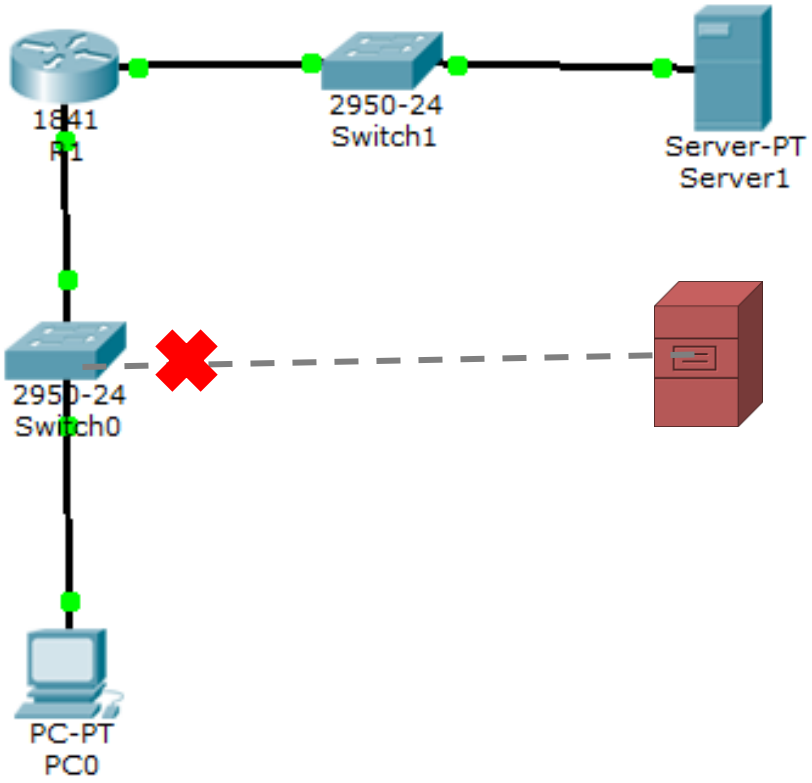
- Poolname: FAKE
- Default gateway 1.1.1.1
- DNS: 1.1.1.2
- Start IP : 1.1.1.21
- Subnet mask: 255.255.255.0, then click add!

The background of this attack

- This attack can be carried out, because the first DHCP packet originating on PC0 is a broadcast message, that means that each DHCP server is going to receive it!
- Both DHCP server will respond!
- PC0 will accept the first configuration parameters!
- Because the FAKE server is much closer than the real one, it will accept the fake's offer.
- You can test it with setting IP address on PC0 as dynamic.
- Check the obtained IP address!

Defense Mechanisms

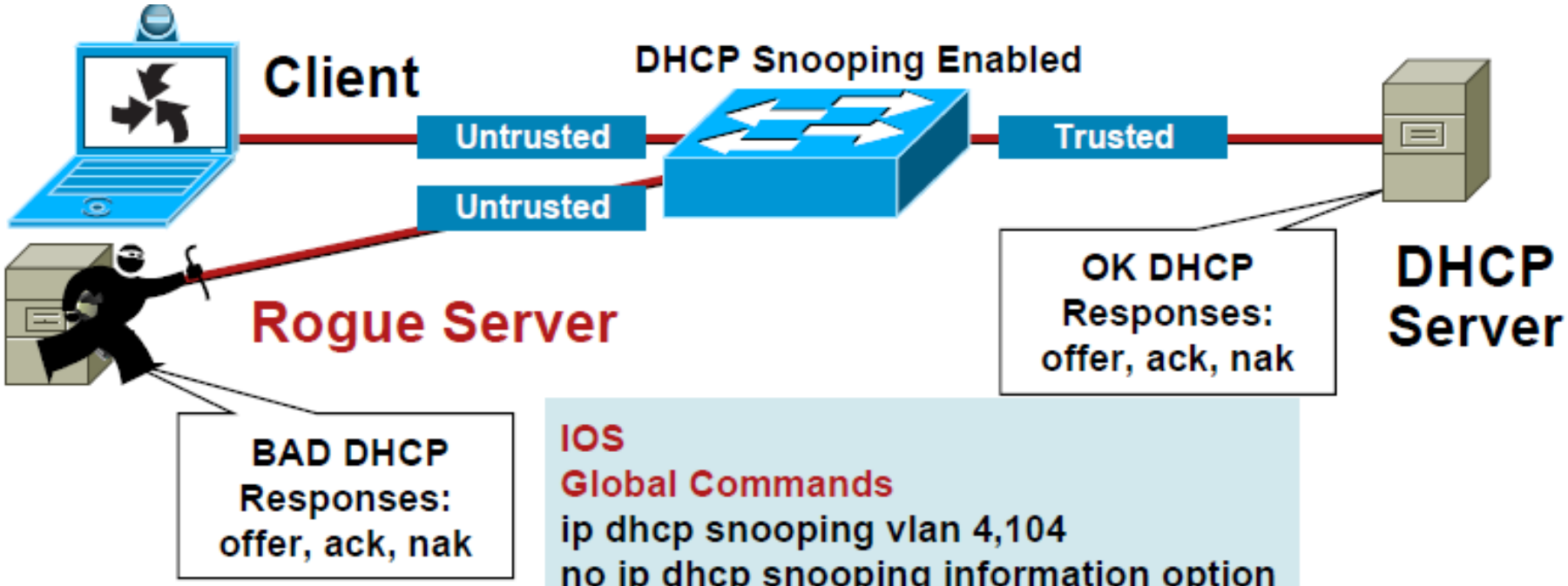
- DHCP SNOOPING trust port
- DOT1x Authentication
- Port Security
- Shutdown unused ports



Please configure DHCP snooping as a defense mechanism, and test whether the attack can be carried out or not.
The next two slides tells a bit about dhcp, and it is also covered in the curriculum, check it!
Configure appropriates ports as Trusted (untrusted is the default)!

Issue the show dhcp snooping binding to see what kinf of information is stored in the table!

DHCP snooping



IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping

DHCP Snooping Untrusted Client

Interface Commands
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)

DHCP Snooping Trusted Server or Uplink

Interface Commands
ip dhcp snooping trust

DHCP snooping

DHCP Snooping Binding Table

sh ip dhcp snooping binding

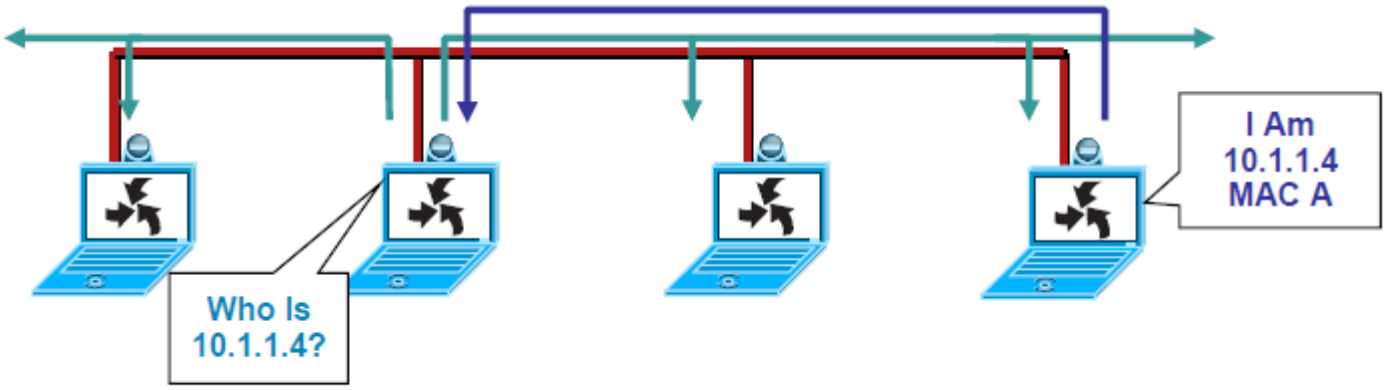
MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:03:47:B5:9F:AD	10.120.4.10	193185	dhcp-snooping	4	FastEthernet3/18

- Table is built by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires
- In the event of switch failure, the DHCP Snooping Binding Table can be written to bootflash, ftp, tftp, ….
- To provide more information about the actual client that generated the DHCP request, enable DHCP option 82 with the **ip dhcp snooping information option** global configuration command. This adds the switch port identifier into the DHCP request.

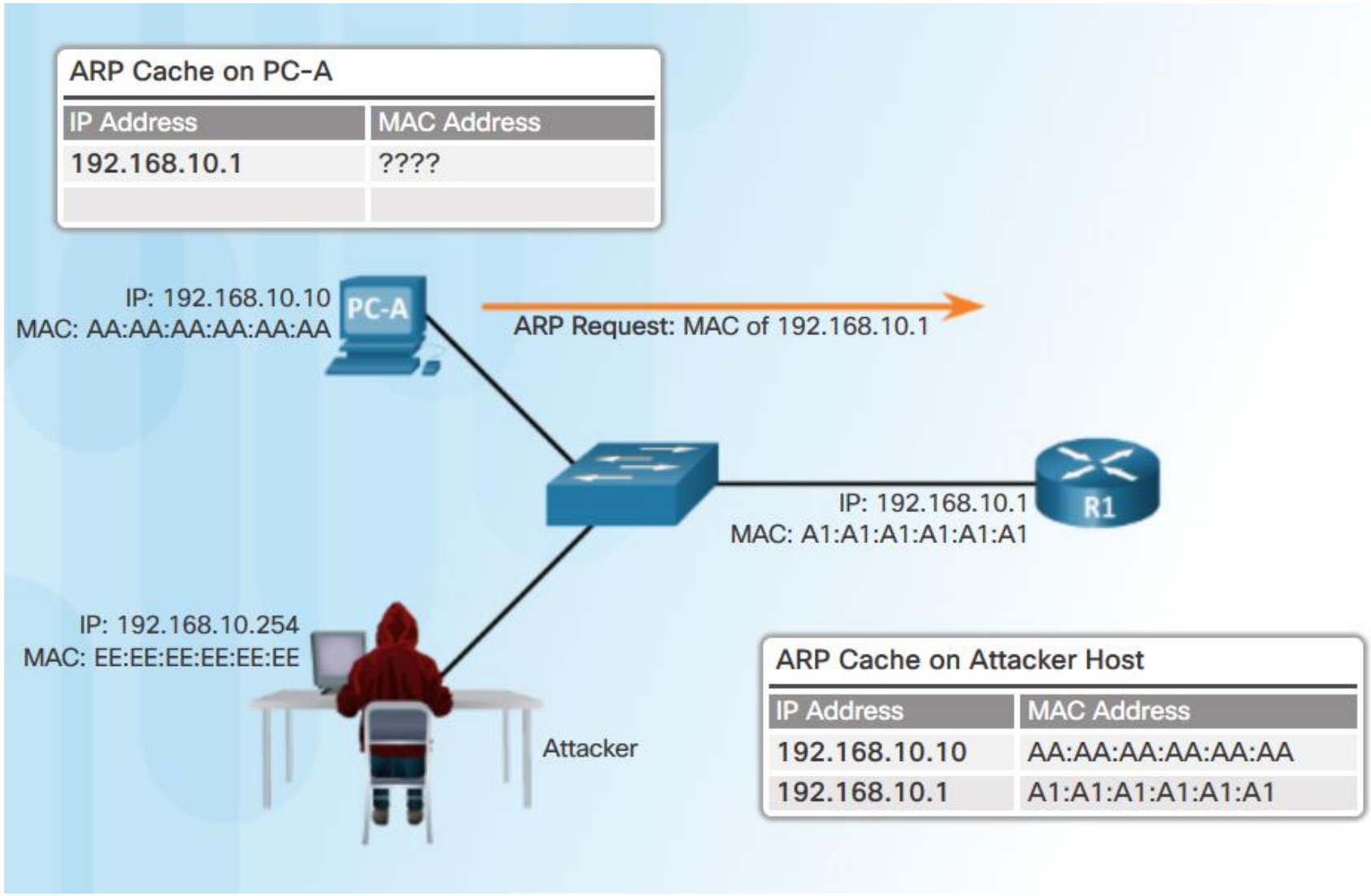
ip dhcp snooping database tftp://172.26.168.10/tftpboot/tulledge/ngcs-4500-1-dhcpdb
ip dhcp snooping database write-delay 60

ARP review

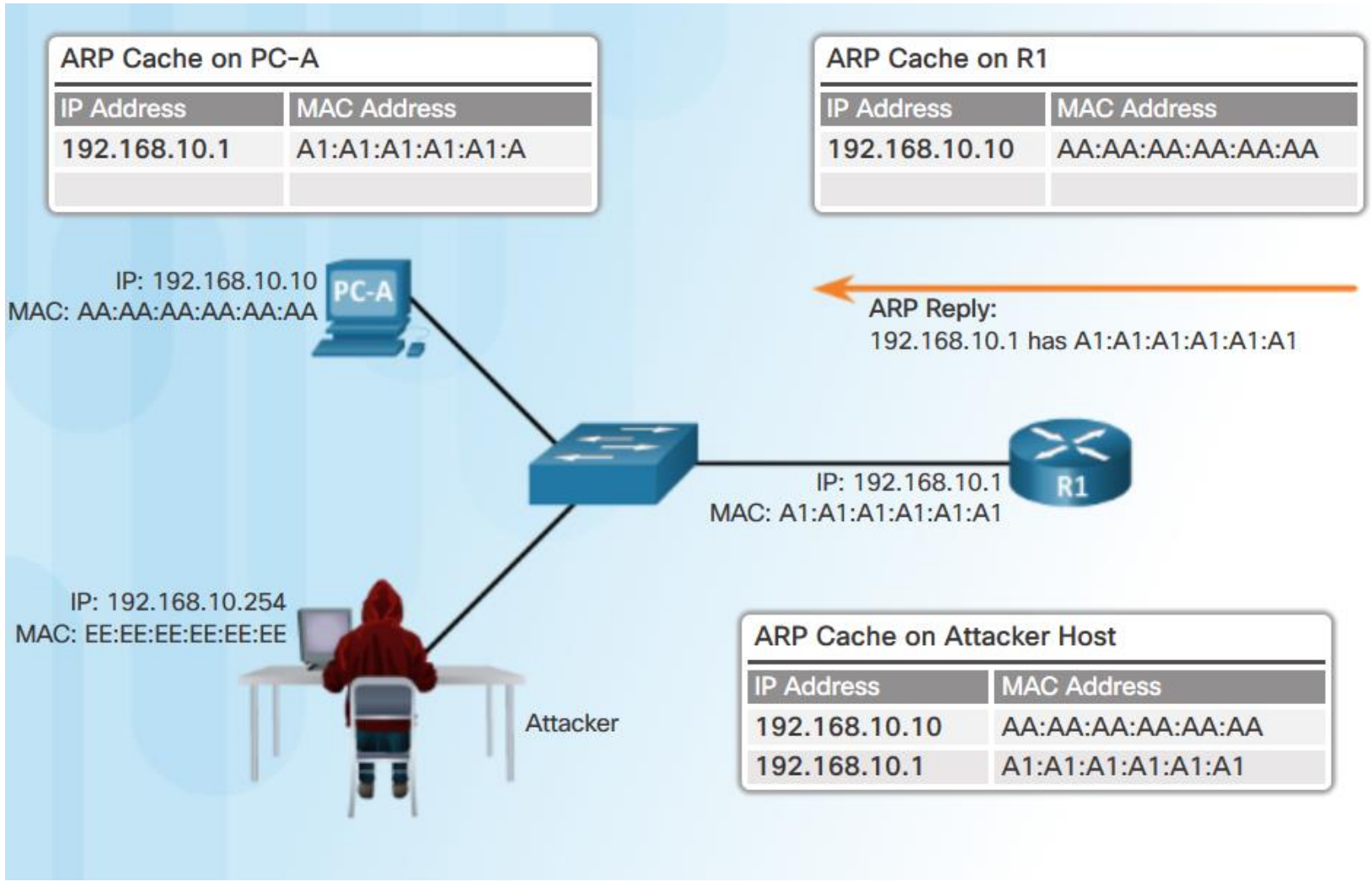
- Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address
- This ARP request is broadcast using protocol 0806
- All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply



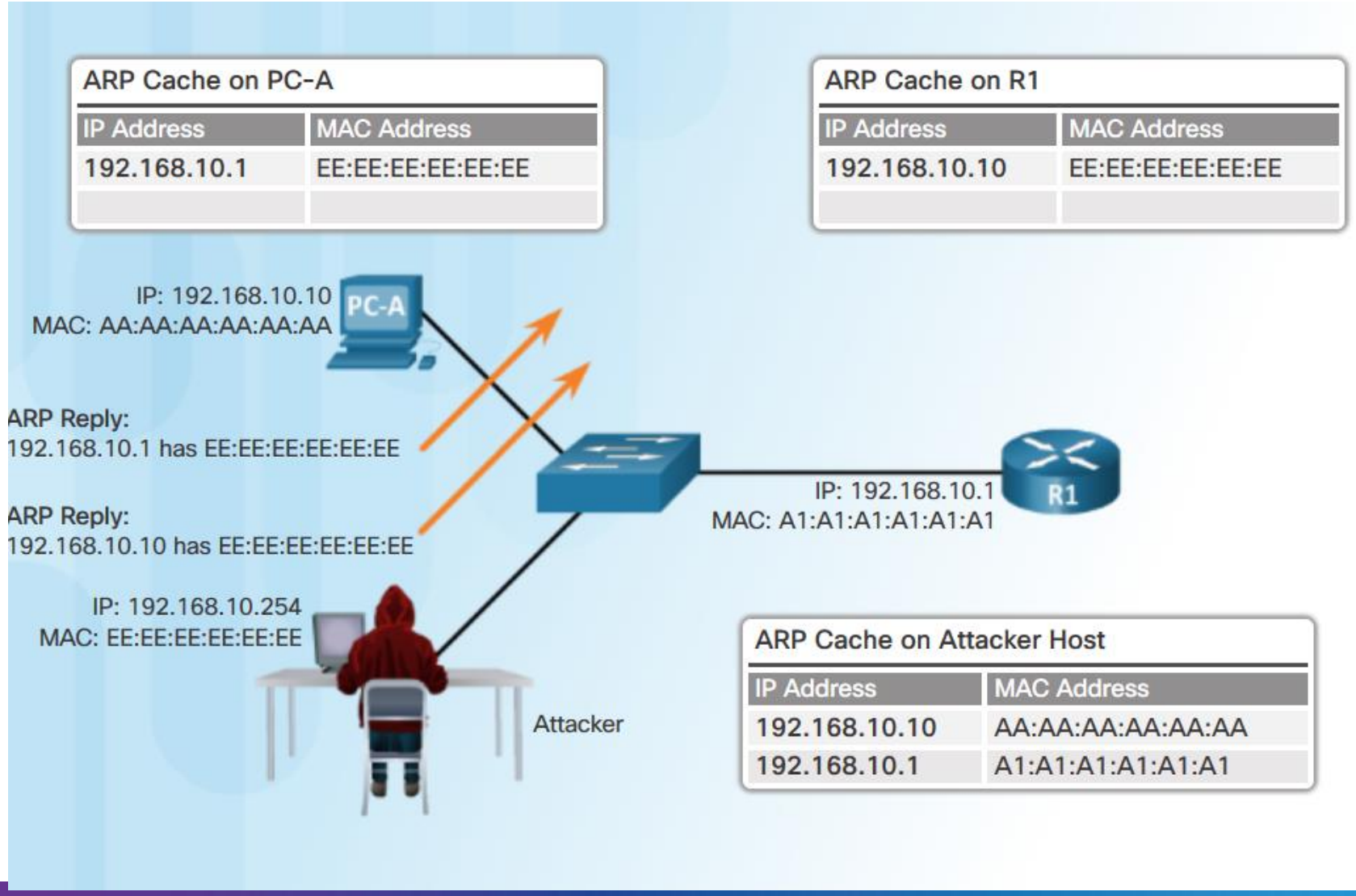
ARP Attack in Action



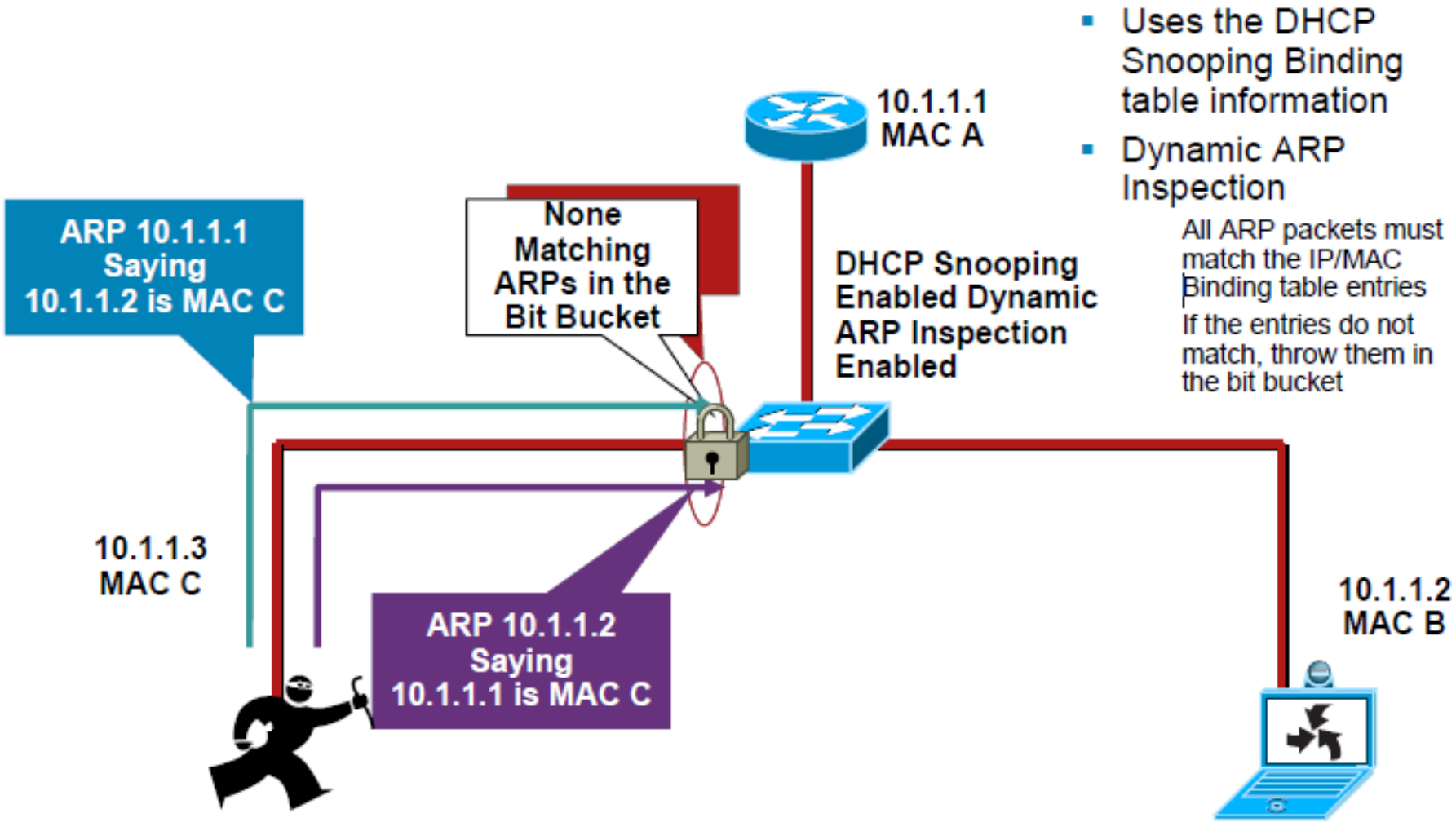
ARP Attack in Action



ARP Attack in Action



Countermeasures to ARP Attacks: Dynamic ARP Inspection



- Uses the DHCP Snooping Binding table information
- Dynamic ARP Inspection
  - All ARP packets must match the IP/MAC Binding table entries
  - If the entries do not match, throw them in the bit bucket

Countermeasures to ARP Attacks: Dynamic ARP Inspection

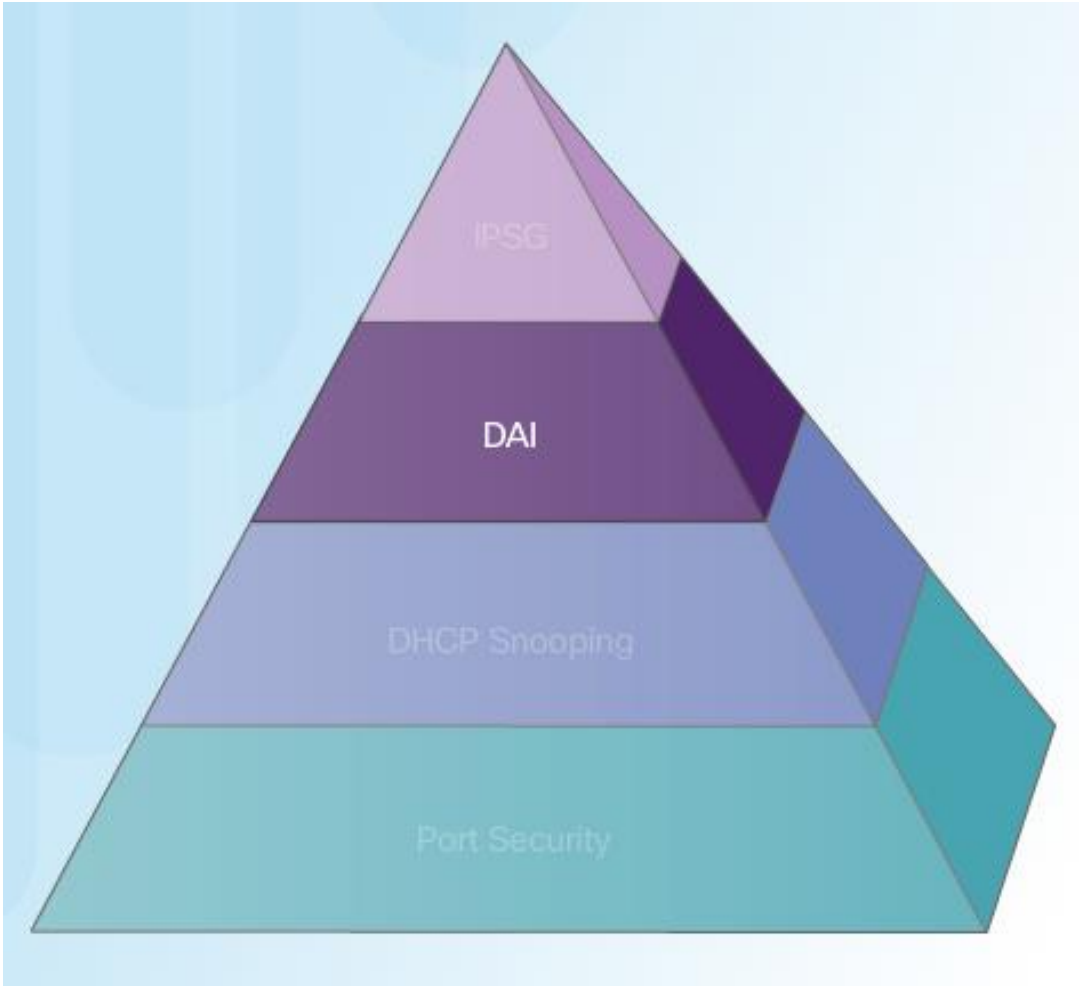
- Dynamic ARP Inspection prevents ARP attacks by intercepting all ARP requests and responses
- Uses the information from the DHCP Snooping Binding table. The DHCP Snooping table is built from the DHCP request, but you can put in static entries

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
------------------  --------------  ----------  --------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185      dhcp-snooping   4     FastEthernet3/18
```

- Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, if not, traffic is blocked
- DHCP Snooping had to be configured so the binding table is built
- DAI is configured by VLAN
- You can trust an interface like DHCP Snooping

Building the Layers

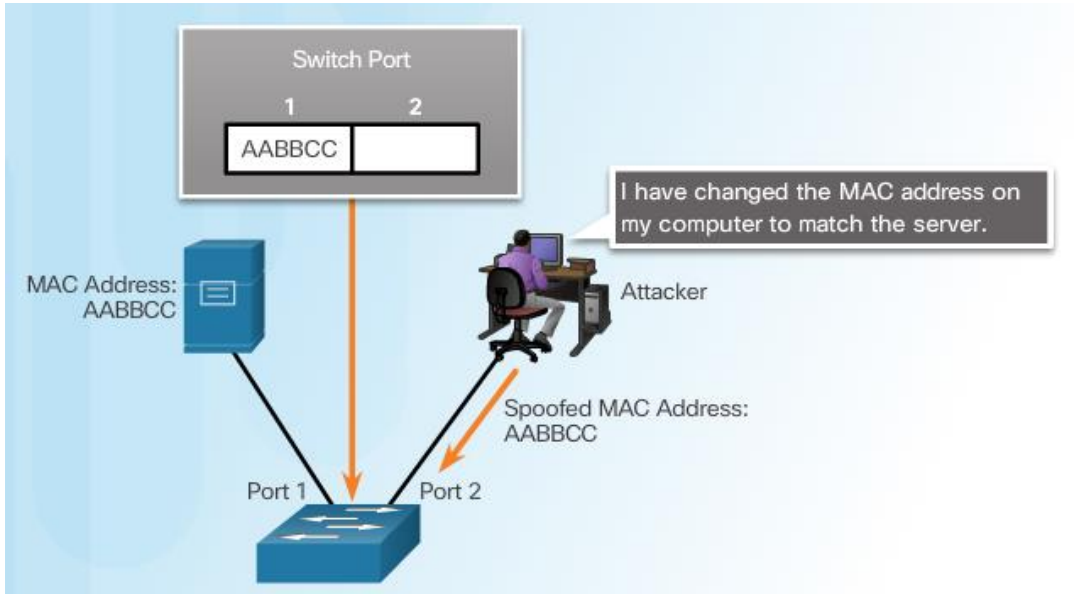
- Port security prevents CAM attacks and DHCP Starvation attacks
- DHCP snooping prevents rogue DHCP server attacks
- Dynamic ARP inspection prevents current ARP attacks

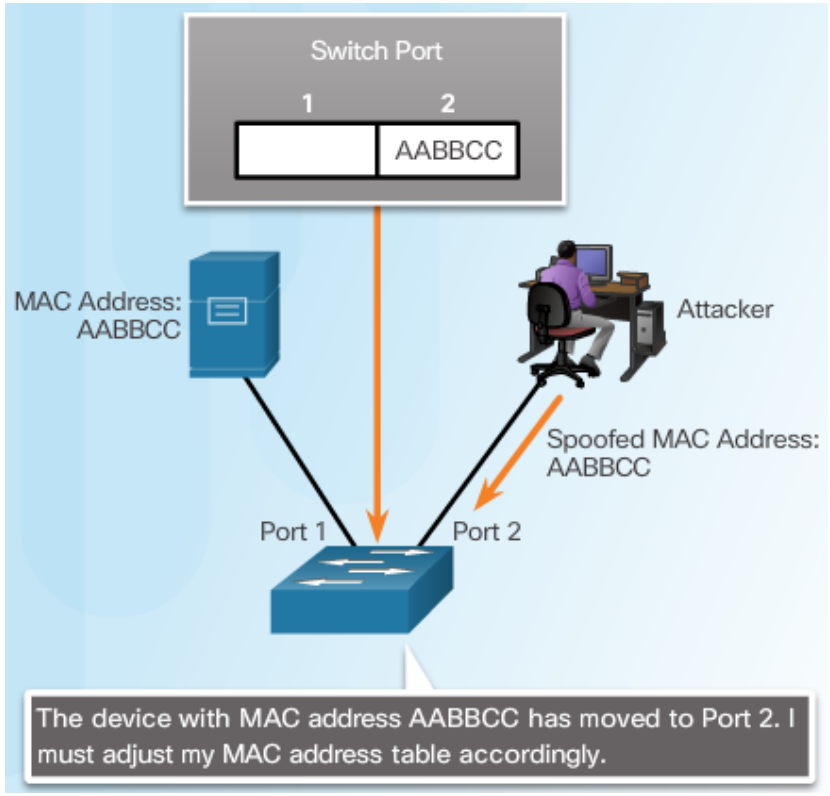


Address Spoofing Attacks

MAC address spoofing

- There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.





Mitigating Address Spoofing Attacks

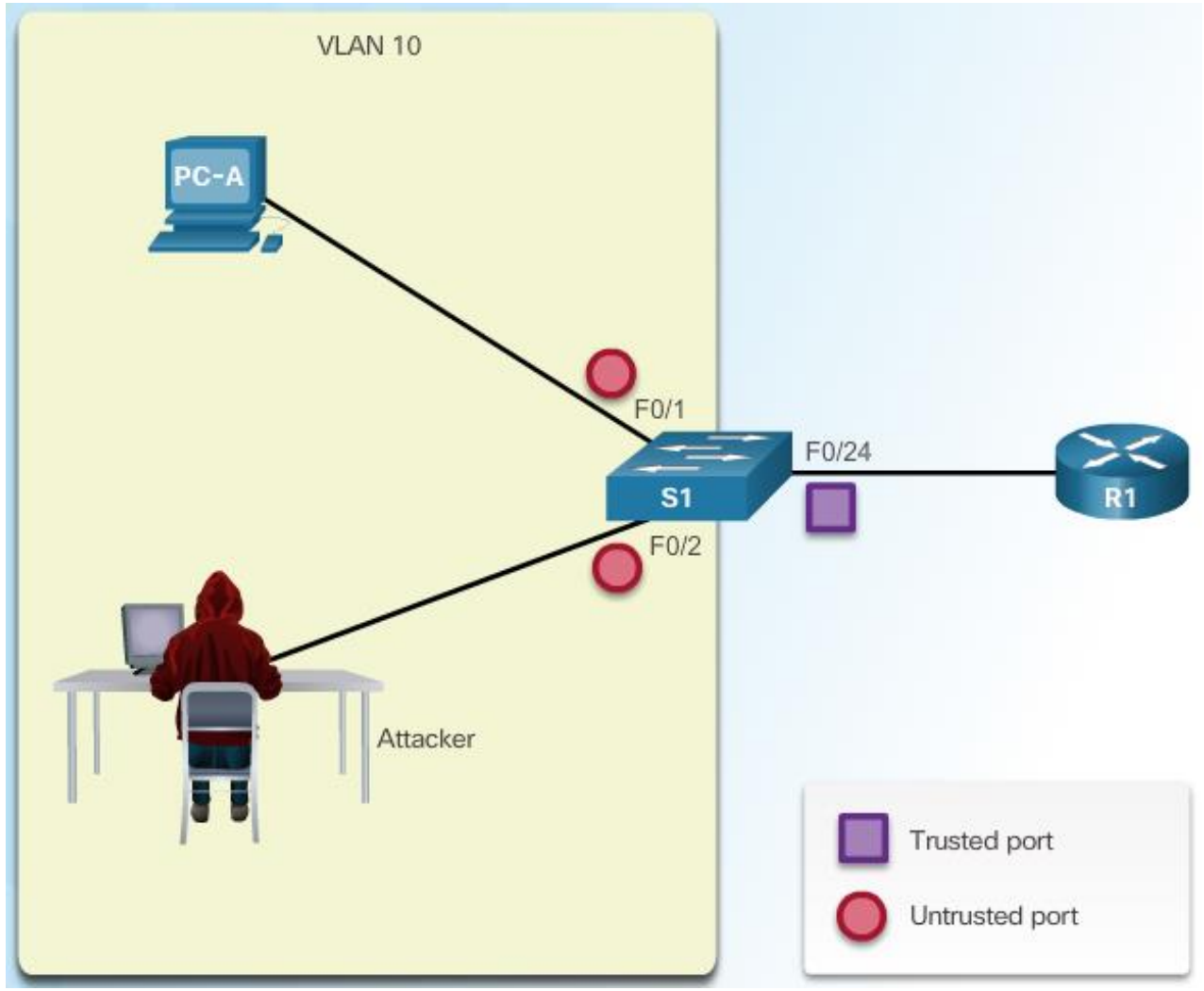
IP Source Guard (IPSG) security feature

- Uses the DHCP Snooping Binding Table Information and manually configured IP source bindings
- IP Source Guard Operates just like Dynamic ARP Inspection, but looks at every packet, not just ARP Packet

- Uses the information from the DHCP Snooping Binding table

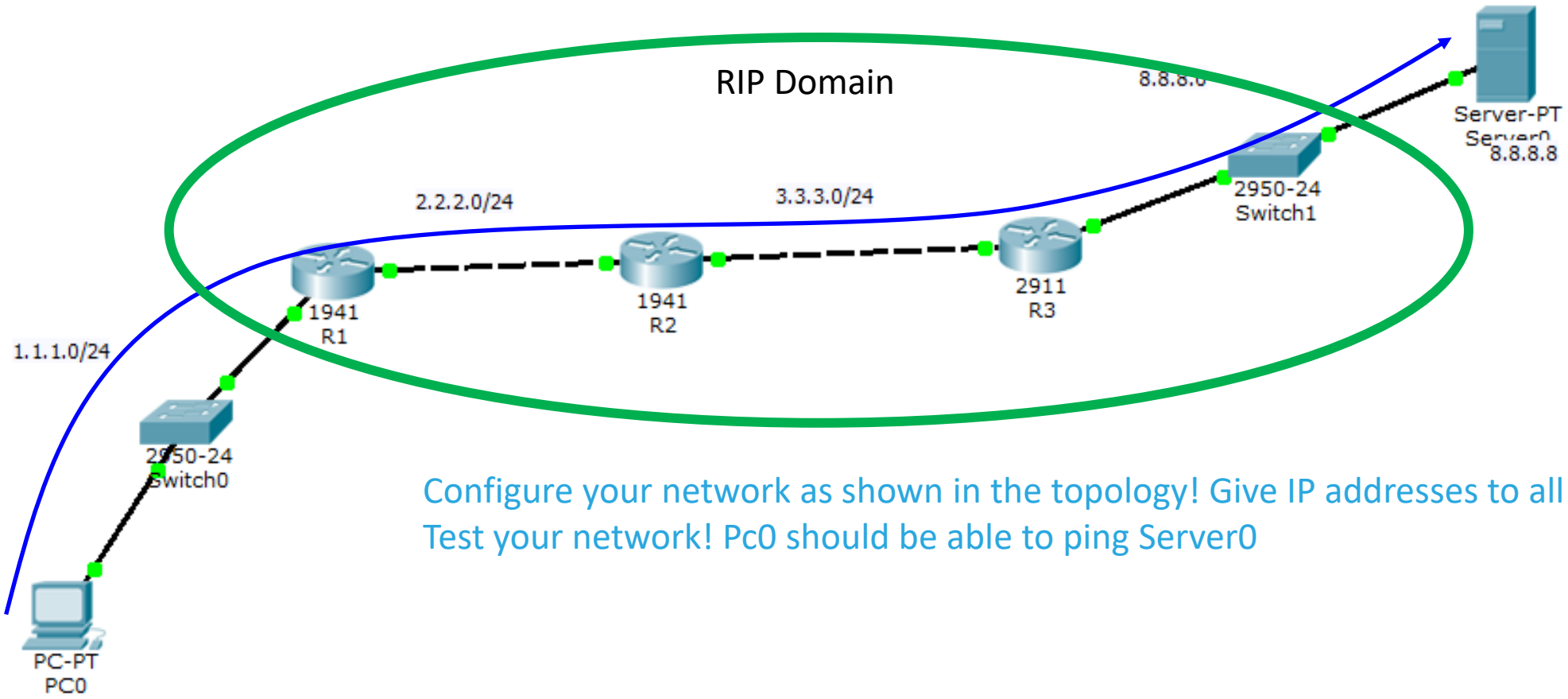
- Looks at the MacAddress and IpAddress fields to see if the traffic from the interface is in the binding table, if not, traffic is blocked.
- IPSG is deployed on untrusted Layer 2 access and trunk ports. IPSG dynamically maintains per-port VLAN ACLs (PVACL) based on IP-to-MAC-to-switch-port bindings.

Configuring Dynamic Arp Inspection



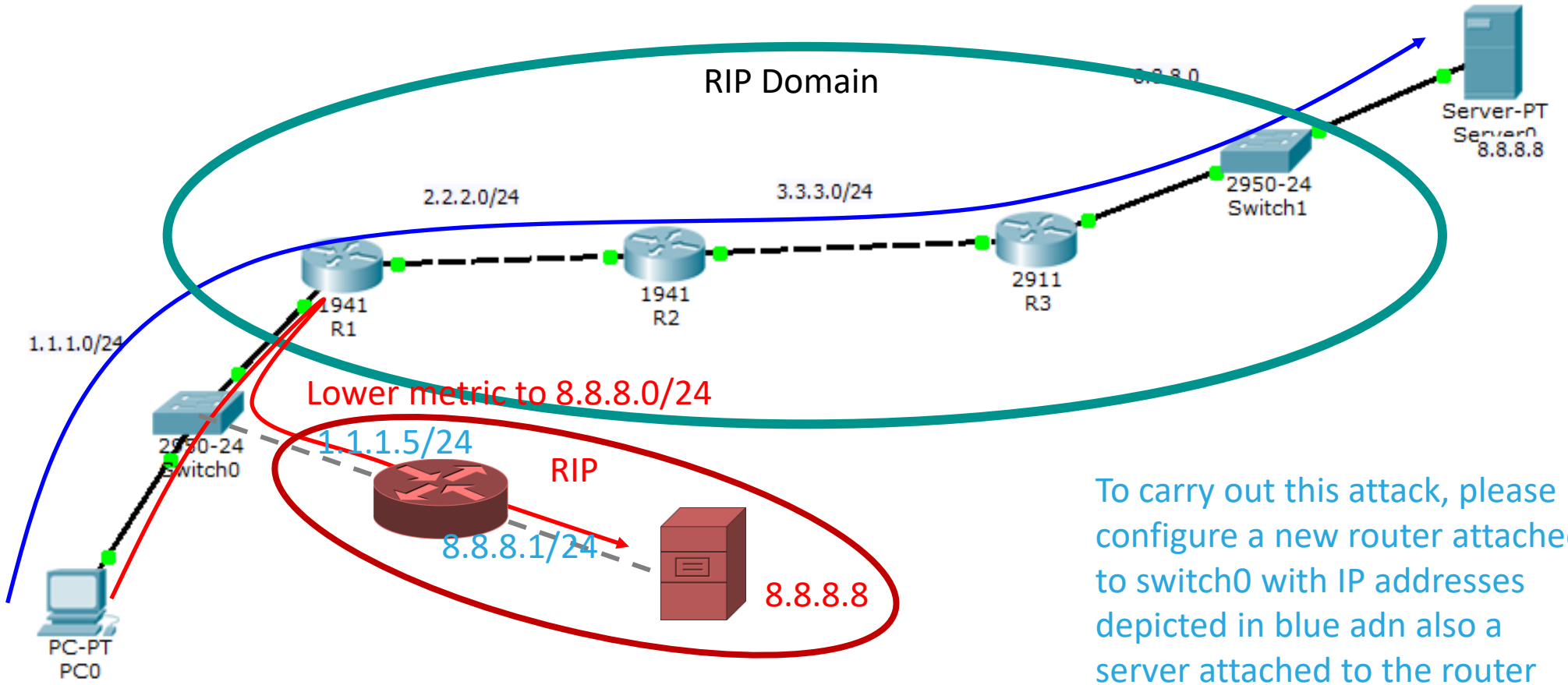

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)#
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection  trust
S1(config-if)#
```

ATTACK 5 - ROUTING



Configure your network as shown in the topology! Give IP addresses to all devices!
Test your network! Pc0 should be able to ping Server0

ATTACK 5 - ROUTING



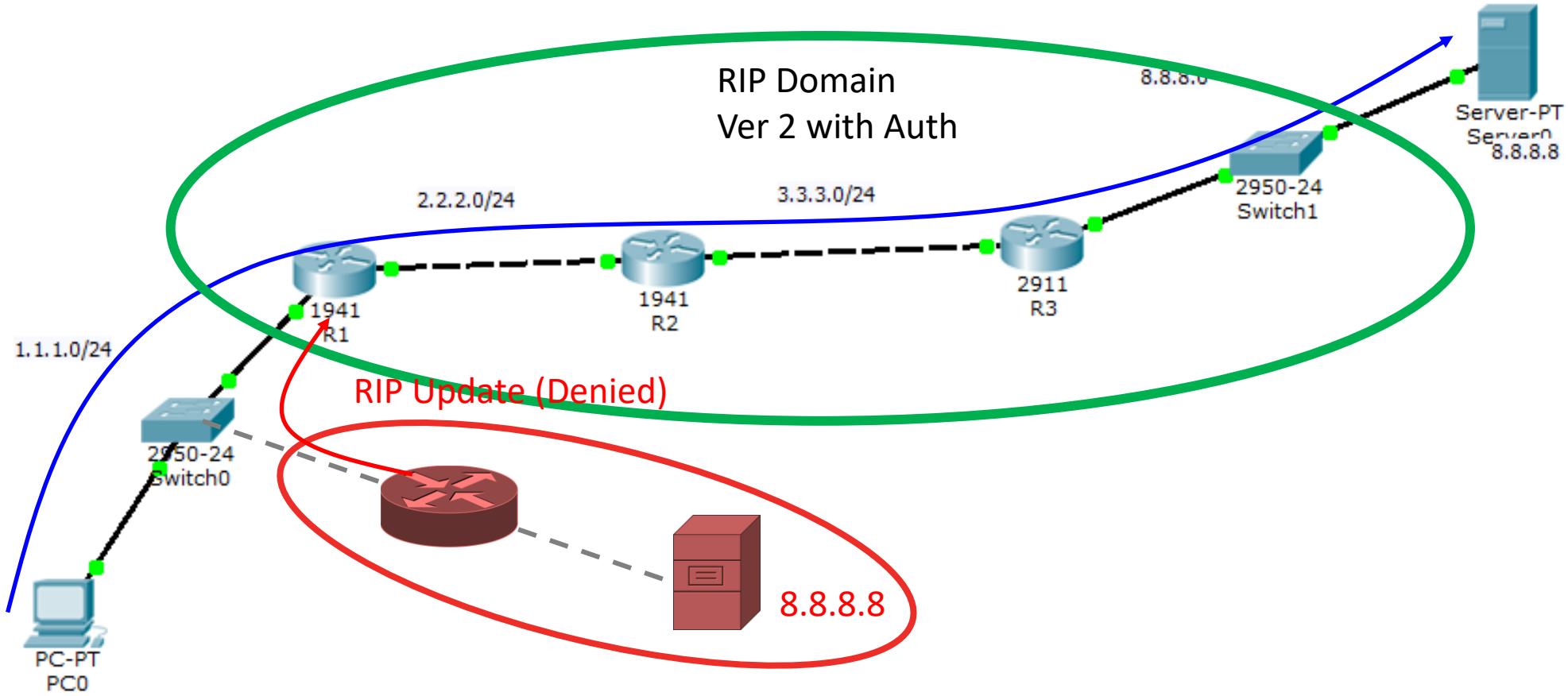
To carry out this attack, please configure a new router attached to switch0 with IP addresses depicted in blue adn also a server attached to the router with the given IP address.

Background of ATTACK 5

- If you configure RIPv2 on all routers, they will share routing information with each other.
- If you have done it correctly, R1 will have two known routes to 8.8.8.0.
- Because the attacker network has a lower metric because on R1 it is only 1 hop away, than it will forward all packets destined to 8.8.8.8 to the attacker server!
- Please test it with simulation mode: ping from Pc1 to 8.8.8.8 and see where the packets are sent!

Defense Mechanisms

- Routing Protocol Authentication



Routing Protocol Authentication

- RIPv1 does not support authentication
- RIPv2 supports authentication with plaintext (default) password or with md5 hash

  Define keychain

  Define the key or keys in the keychain

  Enable authentication on interface – (config-if)#ip rip authentication mode text

  (config-if)#ip rip authentication keychain KEYCHAIN

As a defense mechanism, try to configure RIPv2 authentication on the legitimate routers!

Summary

- **First line of defence (restrict access)**

  Shutdown unused port

  Port Security

  Dot1X authentication

  DHCP Snooping

- **Second line of defence (protocol security)**

  VTP Security

  HSRP Security

  Disable DTP

  Routing Protocol Authentication

  ACL