Switch security features

Lecture 5

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Table of Contents

Software University

1. Port security
2. DHCP snooping
3. Dynamic ARP inspection
4. Demonstration

Have a Question?

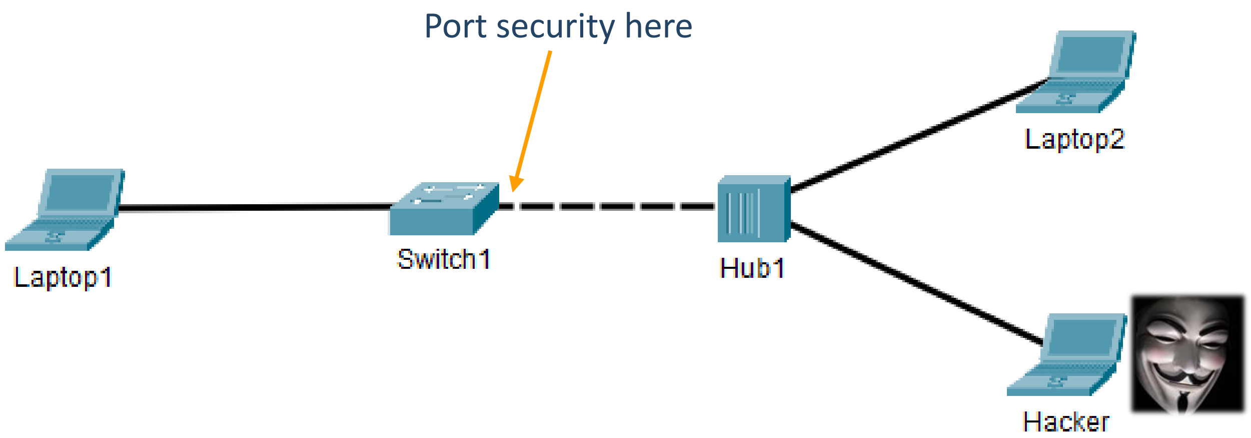
sli.do

#CNA

Port security

What is port security?

- Without port security, any device can connect to any port in the network
- With port security, the switch looks at the source MAC address of the received frames



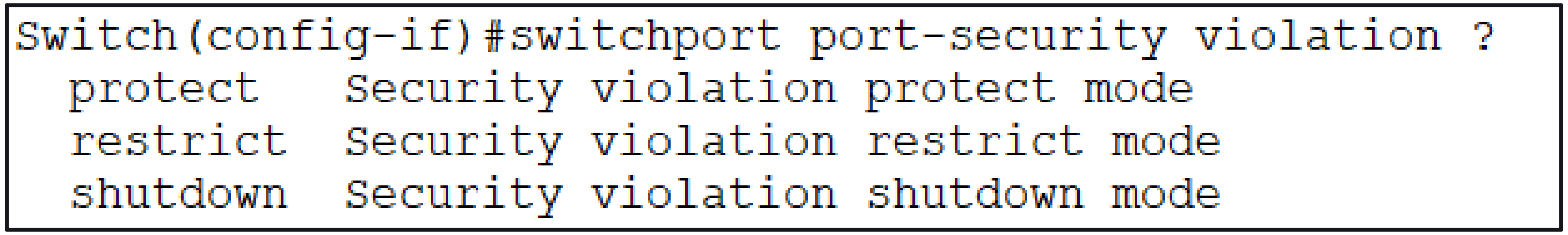
Note: This is not a user authentication (802.1X, discussed later in the course)

Configuration options

- Static
  - Manually configure the allowed MAC addresses on a port
  - Better control, but requires manual configuration
- Dynamic learning
  - Specify a number of allowed MAC address on a port (let’s say “n”)
  - Only the first “n” dynamically learned MAC addresses are allowed
  - When the switch is rebooted, the learning process starts over! (not in the config)
- Combination of static and dynamic learning
  - Specify a number of allowed MAC address on a port, let’s say 5
  - Manually configure only some of them, let’s say 2
  - The other 3 MAC addresses will be dynamically learned

Violation actions

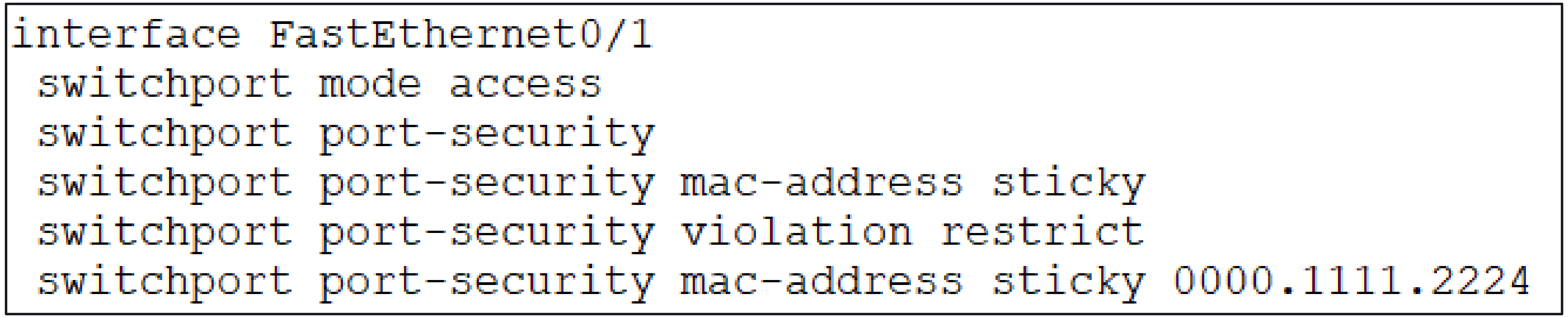
- What happens when a device with not allowed MAC address tries to access the switch port?
  - **Protect** - drops packets with unknown source MAC when the allowed maximum is reached
  - **Restrict** - same as Protect + logging (counters will increment)
  - **Shutdown** (default) - puts the port into Error disable mode and sends SNMP trap notification



```
Switch(config-if)#switchport port-security violation ?
  protect    Security violation protect mode
  restrict   Security violation restrict mode
  shutdown   Security violation shutdown mode
```

MAC address sticky

- The “static” option drawback - requires to manually enter MAC addresses
- The “dynamic learning” option drawback - the learned allowed MAC addresses are lost after device reboot
- The “sticky” option learns the allowed MAC addresses dynamically and then adds them to the running configuration



```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0000.1111.2224
```

Error disable and auto recovery

- Normally, the “shutdown” violation action requires manual intervention to re-enable it (shutdown + no shutdown)
- A switch port can be configured to auto recover after a period of time
- Example:
  - **errdisable recovery cause psecure-violation**
  - **errdisable recovery interval 30**
- Note that this functionality is not (currently) available in Cisco Packet Tracer

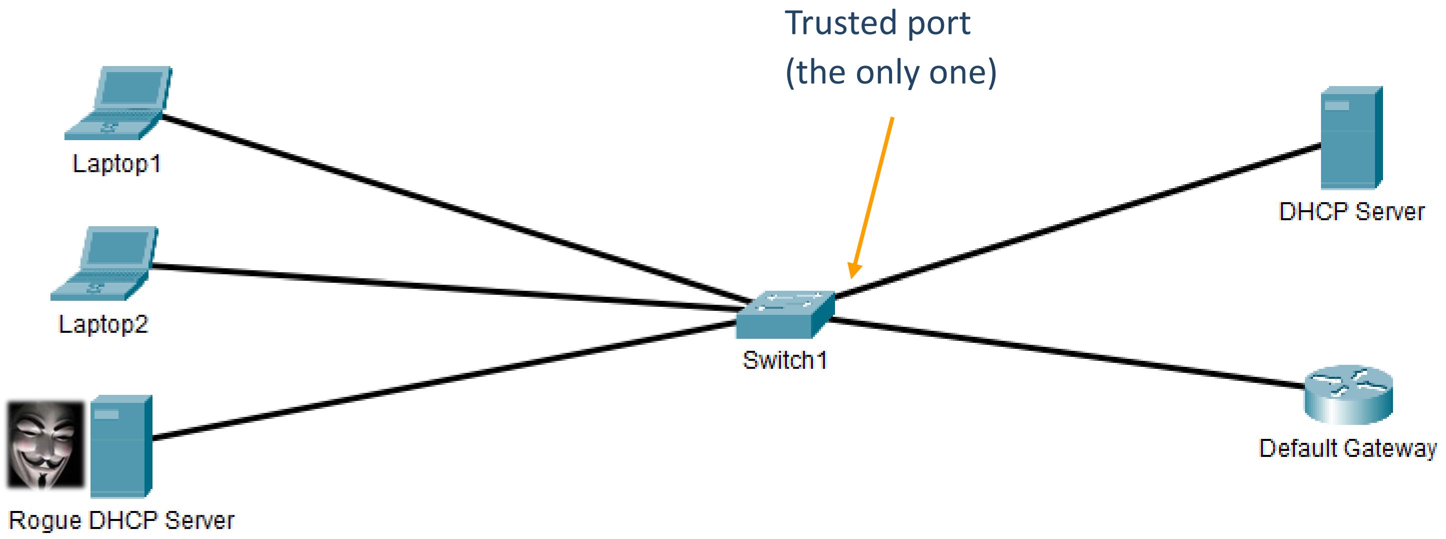
Port security configuration

- Minimum required configuration:
  - (config-if)# **switchport mode access** (not allowed on dynamic ports)
  - (config-if)# **switchport port-security** (enables port security with default settings)
- Optional configurations:
  - (config-if)# **switchport port-security violation** [**protect/restrict/shutdown**]
  - (config-if)# **switchport port-security maximum** [**1-132**]
  - (config-if)# **switchport port-security mac-address** ***MAC***
  - (config-if)# **switchport port-security mac-address sticky**
  - (config-if)# **switchport port-security aging time [1-1440]**

DHCP snooping

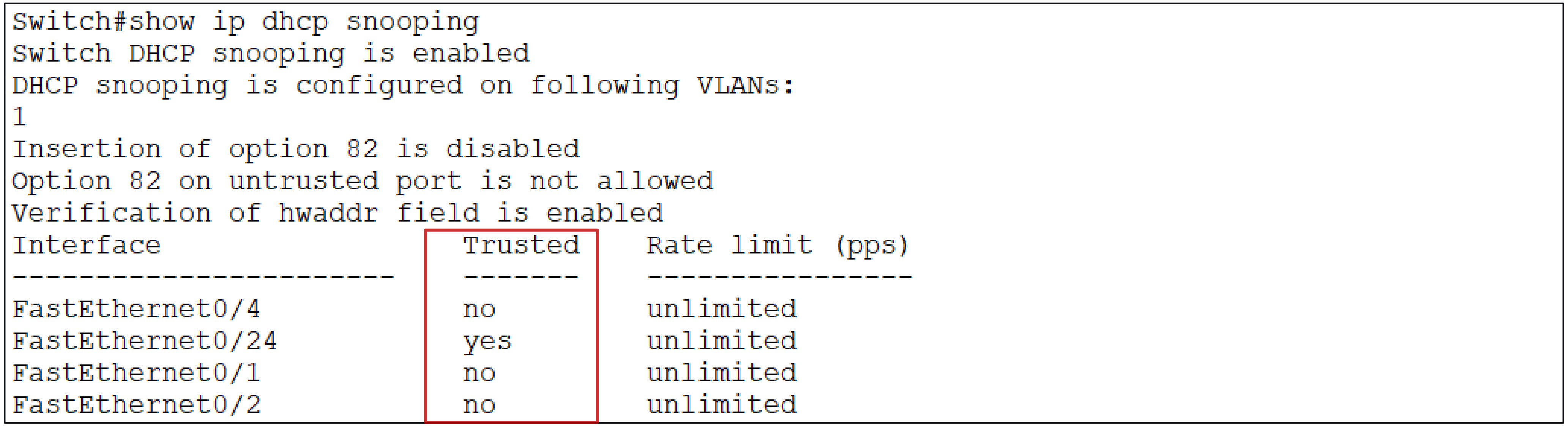
What is DHCP snooping?

- Without DHCP snooping, anyone can act as a DHCP server in the segment (VLAN), intentionally or not
- This can lead to security problems (point users to a wrong DNS or gateway, for example) or simply Denial Of Service
- DHCP snooping does not allow server messages on “untrusted” ports



Trusted and untrusted ports

- When DHCP snooping is enabled, all ports by default are “untrusted”
- DHCP “offer” and “acknowledge” messages are not allowed on untrusted ports
- The port going to the **real** DHCP server should be configured as trusted



```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/4            no         unlimited
FastEthernet0/24           yes        unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/2            no         unlimited
```

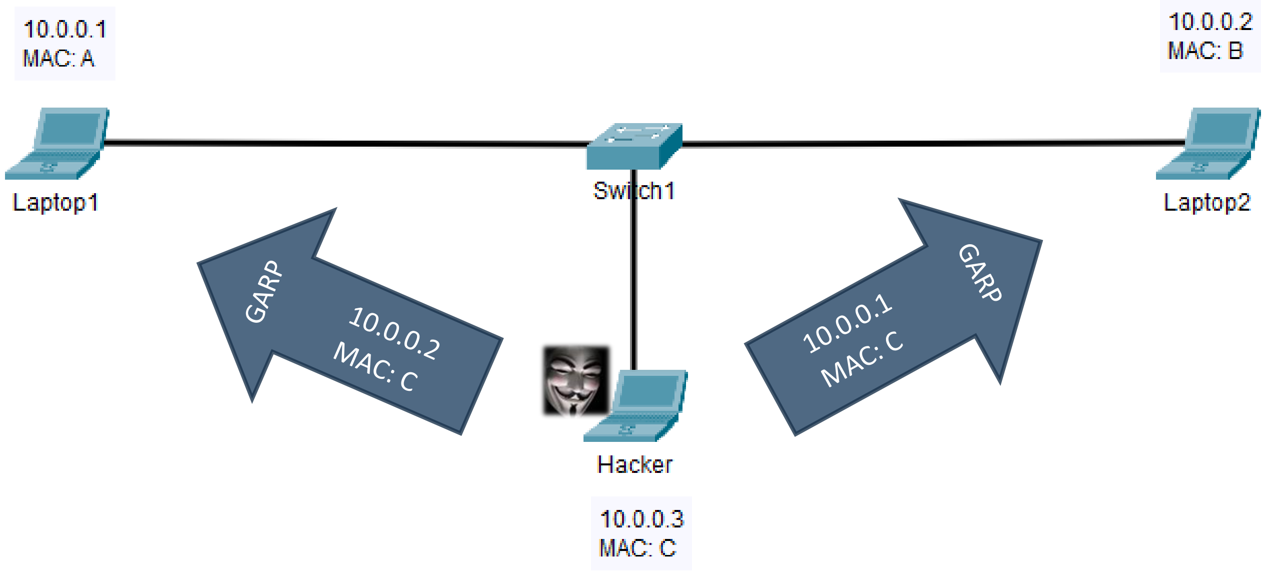
DHCP snooping configuration

- (config)# **ip dhcp snooping** - globally enables the feature
- (config)# **ip dhcp snooping vlan *n*** - enables the feature for VLAN *n*
- (config-if)# **ip dhcp snooping trust** - makes a port trusted (allows DHCP “offer” and “acknowledge” messages)
- (config-if)# **no ip dhcp snooping information option** - disables insertion of option 82

Dynamic ARP inspection

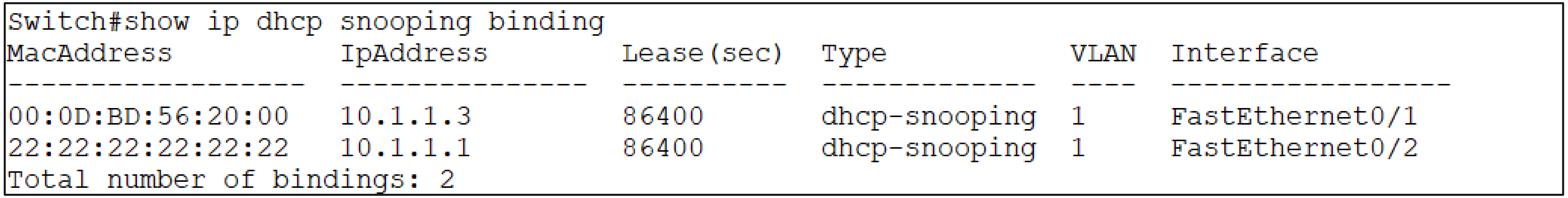
What is dynamic ARP inspection?

- Without dynamic ARP inspection (DAI), a malicious user can insert himself between the communicating devices and perform “man in the middle” attacks
- An attacker can poison the ARP cache tables of the hosts with gratuitous ARP
- The result: traffic between the laptops goes through the “Hacker” device



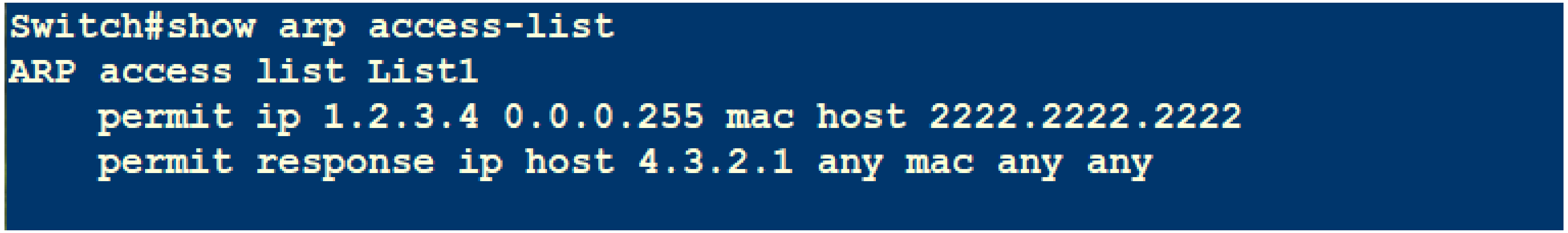
What is dynamic ARP inspection (2)?

- With dynamic ARP inspection (DAI), the switch will check the MAC-to-IP entries in the ARP messages and verify if they are correct
- How does the switch verifies these entries:
  - Via DHCP snooping (1)
  - Via manually created access list (2)



```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:0D:BD:56:20:00   10.1.1.3         86400       dhcp-snooping  1     FastEthernet0/1
22:22:22:22:22:22   10.1.1.1         86400       dhcp-snooping  1     FastEthernet0/2
Total number of bindings: 2
```

(1)

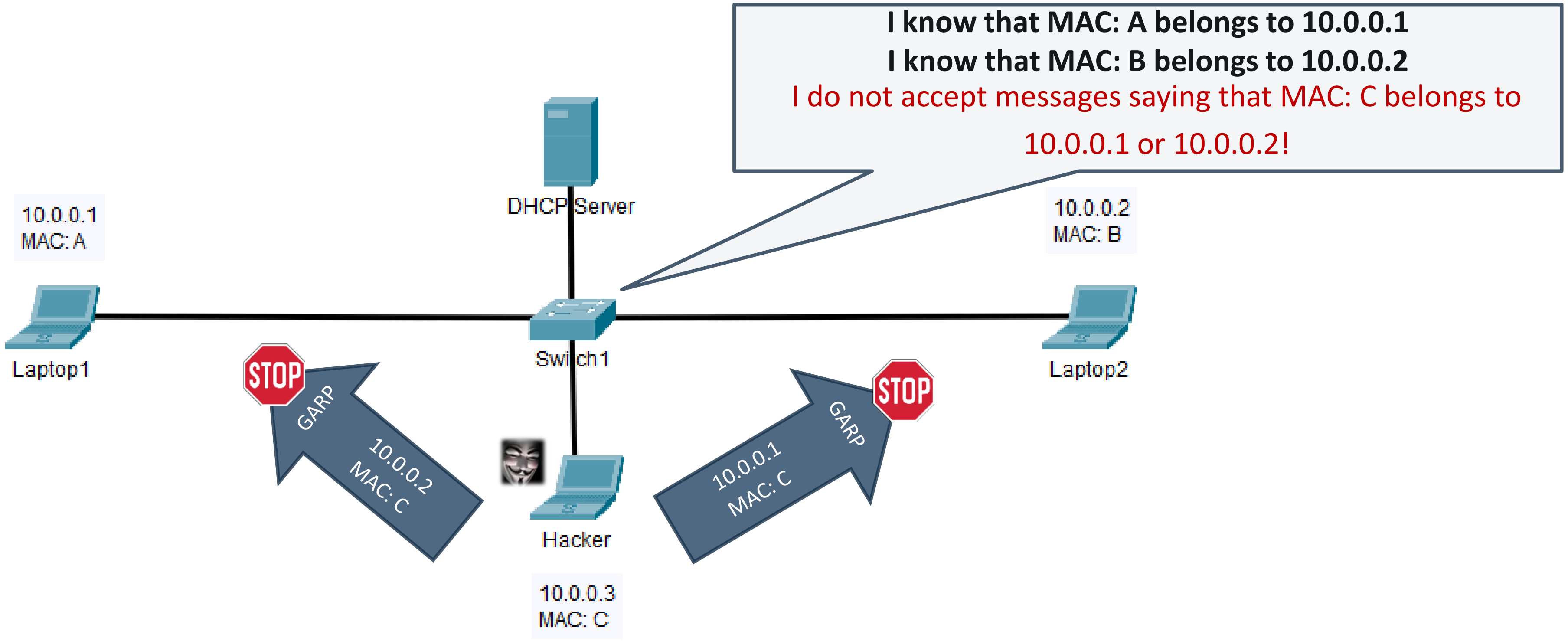


```
Switch#show arp access-list
ARP access list List1
    permit ip 1.2.3.4 0.0.0.255 mac host 2222.2222.2222
    permit response ip host 4.3.2.1 any mac any any
```

(2)

Dynamic ARP inspection

- Because the switch knows which are the correct mappings between MAC and IP addresses, it will discard any other information regarding this topic



I know that MAC: A belongs to 10.0.0.1

I know that MAC: B belongs to 10.0.0.2

I do not accept messages saying that MAC: C belongs to 10.0.0.1 or 10.0.0.2!

Dynamic ARP inspection configuration

- (config)# **ip arp inspection vlan *n***
- (config)# **ip arp inspection validate** [**dst-mac/ip/src-mac**]

- (config-if)# ip arp inspection trust - defines an interface as trusted, no inspection
- (config-if)# ip arp inspection limit rate [0-2048] - packets per second

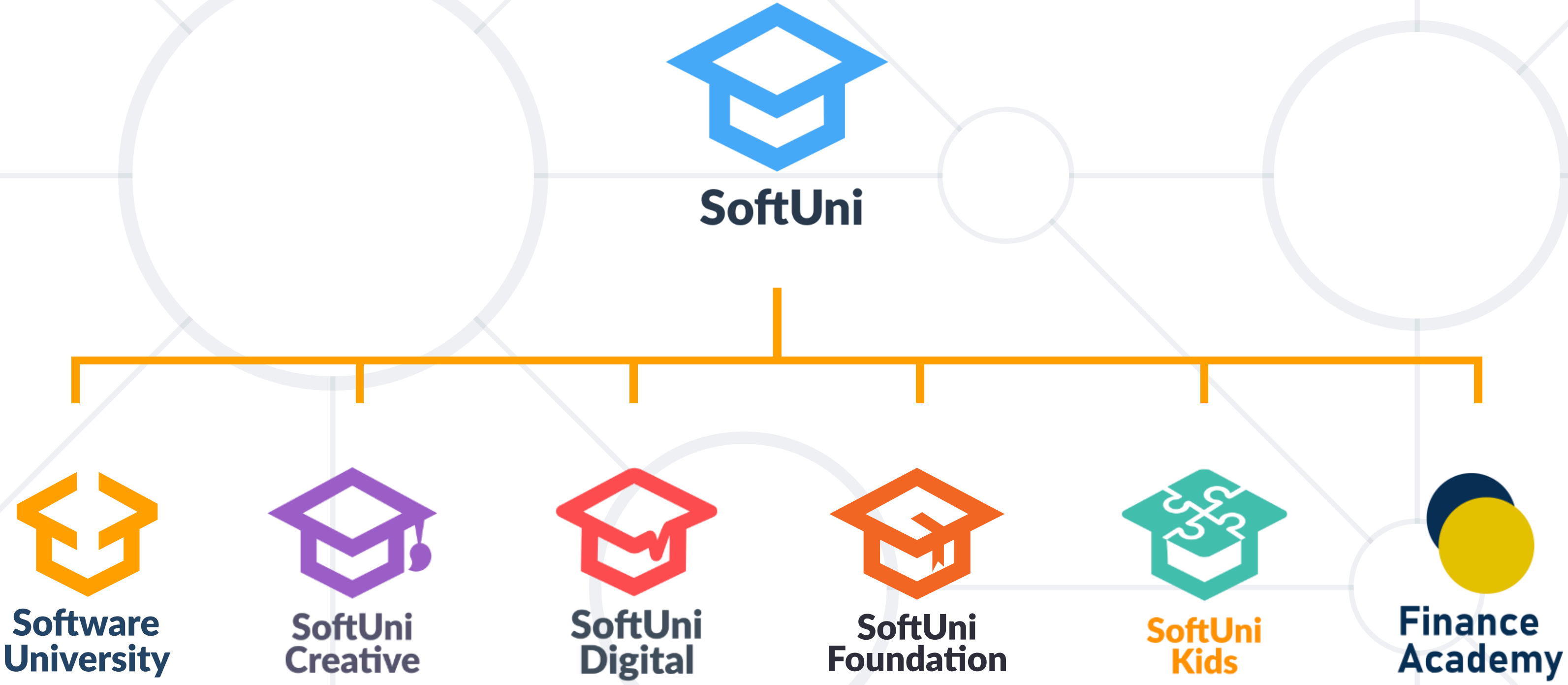
- (config)# **arp access-list *name***

Demonstration

Summary

1. Port security
2. DHCP snooping
3. Dynamic ARP inspection
4. Demonstration

Questions?



SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

Finance Academy

SoftUni Diamond Partners

SmartIT

Coca-Cola HBC Bulgaria

SOFTWARE GROUP

DXC TECHNOLOGY

createX

Postbank

Решения за твоето утре

SUPER HOSTING .BG

DRAFT KINGS

VIVACOM

INDEAVR

Serving the high achievers

AMBITIONED

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg