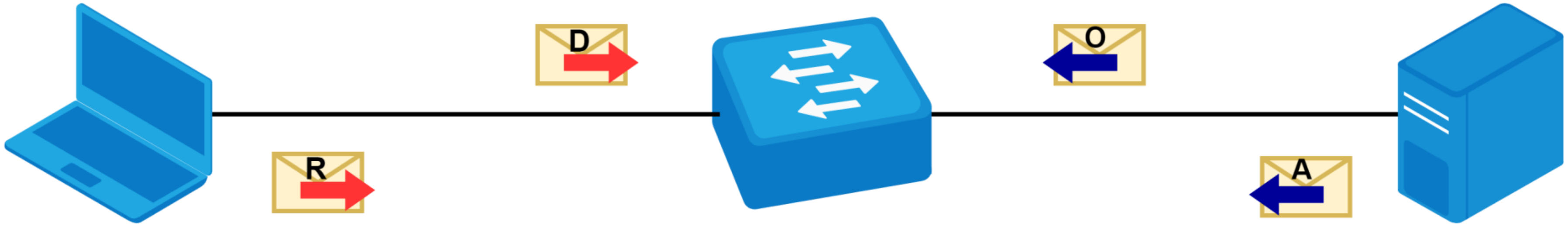
Securing Client’s Ports

DHCP Protocol Transactions



IP: ?
MAC: AA:BB:CC:DD:EE:11

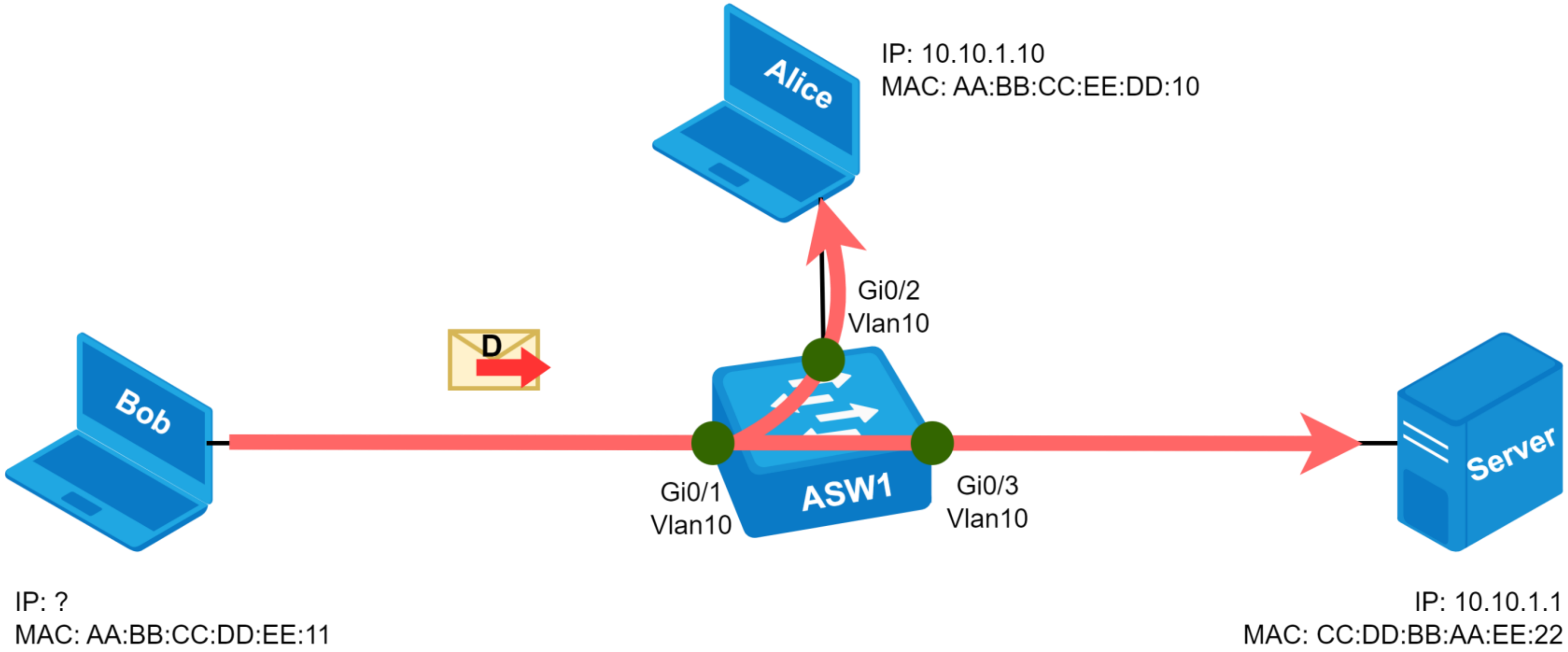
IP: 10.10.1.1
MAC: CC:DD:BB:AA:EE:22

	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
D →	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
O ←	AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: OFFER YIADDR: 10.10.1.15
R →	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: REQUEST YIADDR: 10.10.1.15
A ←	AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: ACK YIADDR: 10.10.1.15

DHCP Spoofing Attack

Consider the network where Bob is trying to obtain an IP address from DCHP server, and Alice being a malignant actor.

Bob broadcasts a DHCP Discover message, which becomes readily available to all the hosts withing the network, including the Server, but also Alice

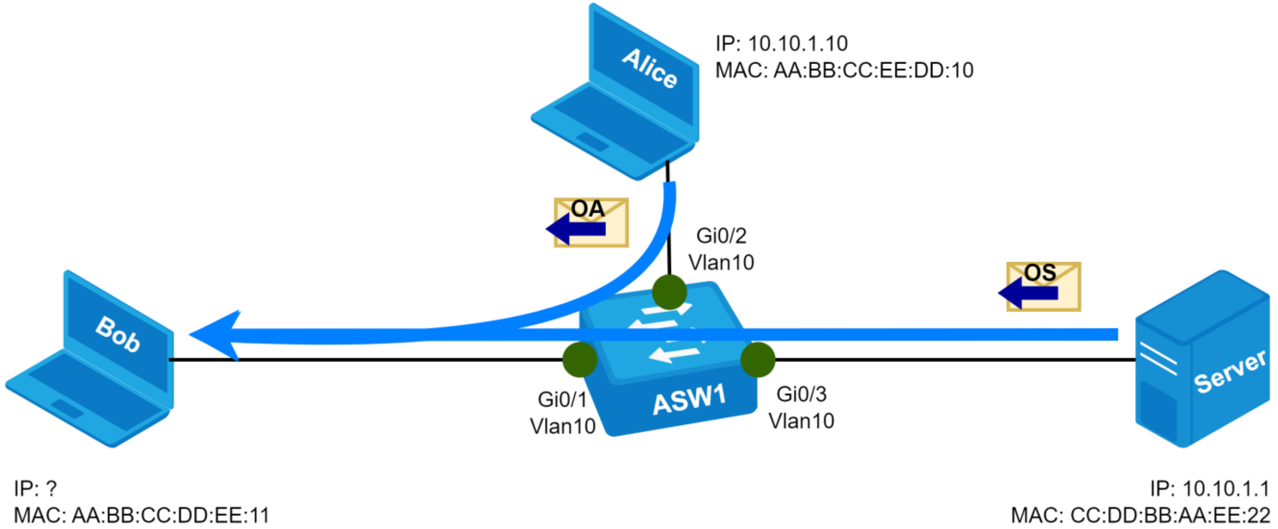


	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
D	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER

DHCP Spoofing Attack

On the second stage the Server replies with the DHCP Offer message (OS), but so does Alice (OA), who disguises as legitimate DHCP server. In practice, she has a good chance of success, as Bob accepts the first offer.

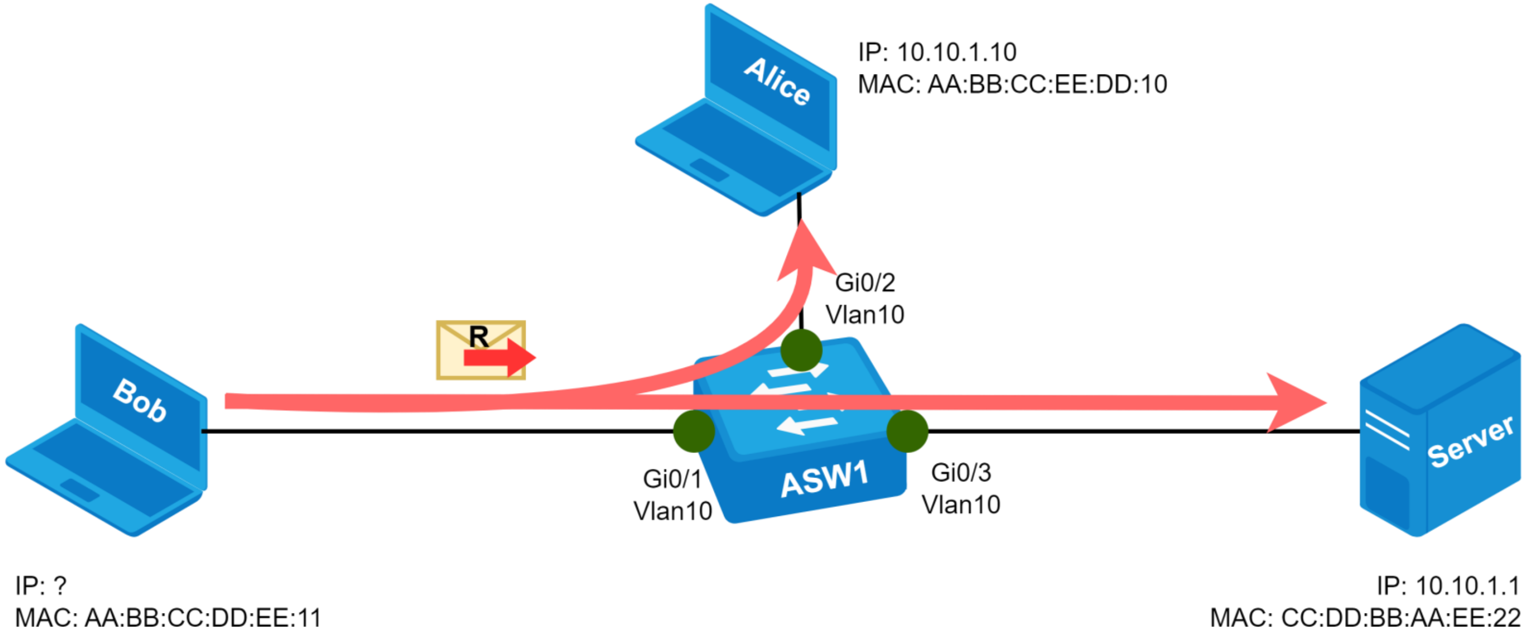
With the DHCP Offer Alice is also trying to become a DNS server and Default Gateway for Bob (options 3 and 6)



	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
OA	AA:BB:CC:DD:EE:11	AA:BB:CC:EE:DD:10	0800	10.10.1.10	0.0.0.0	67	68	MsgType: OFFER YIADDR: 10.10.1.200 SIADDR: 10.10.1.10 Router (Opt 3): 10.10.1.10 DNS (Opt 6): 10.10.1.10
OS	AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: OFFER YIADDR: 10.10.1.15 SIADDR: 10.10.1.1 Router (Opt 3): 10.10.1.1 DNS (Opt 6): 10.10.1.1

DHCP Spoofing Attack

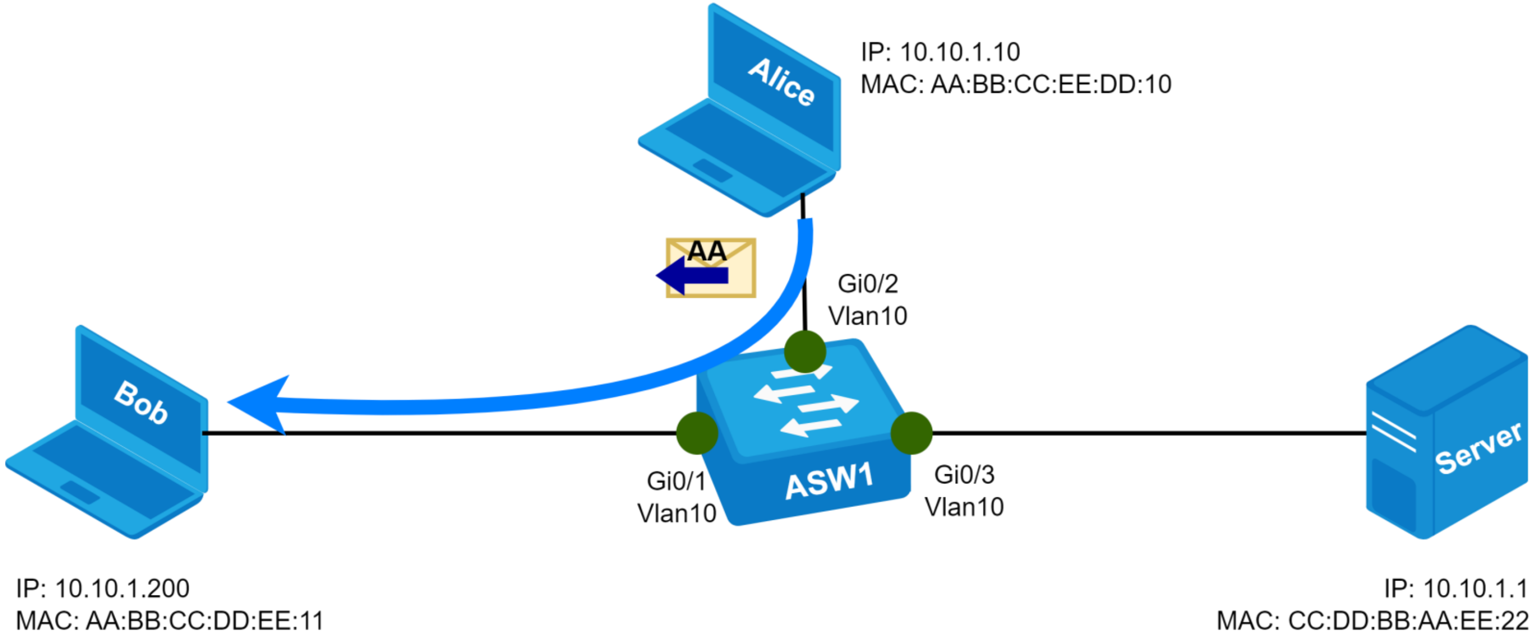
At the third stage, Bob broadcasts the DHCP Request message confirming the choice of Alice and Bob's DHCP server



	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
R	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: REQUEST YIADDR: 0.0.0.0 SIADDR: 10.10.1.10

DHCP Spoofing Attack

Finally Alice confirms the association with DHCP Ack message thus becoming the point of interception for Bob’s traffic, which is from now on susceptible to various malignant activities



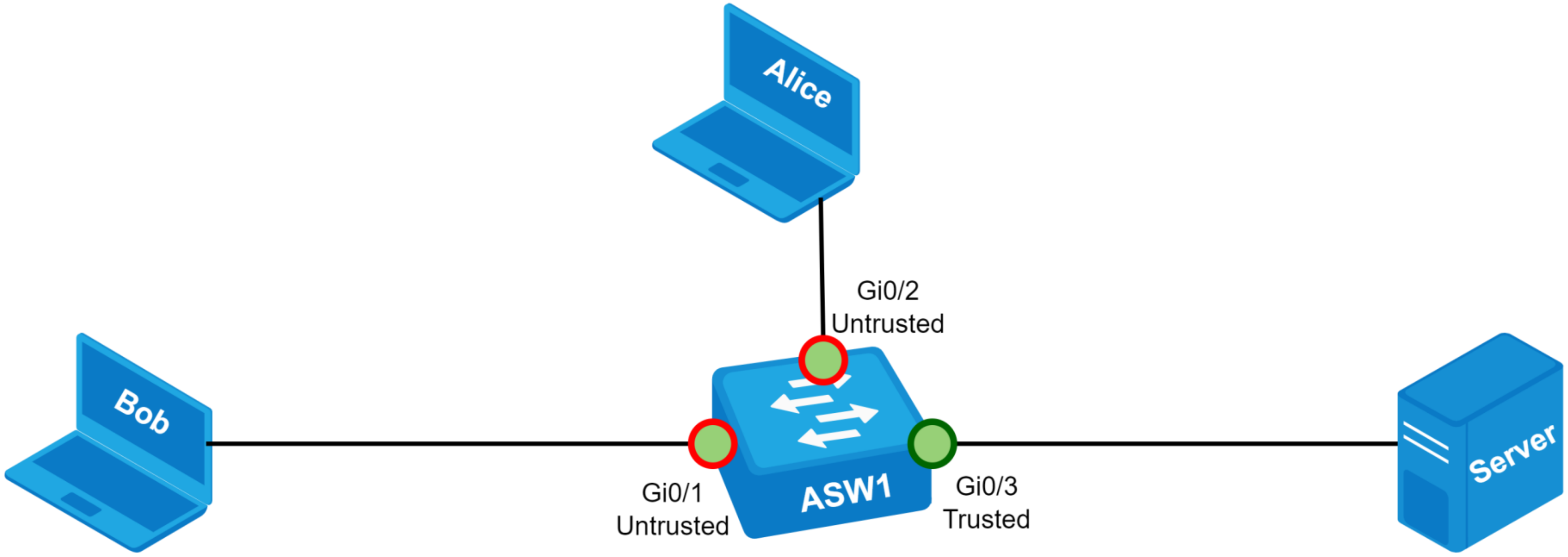
Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
AA:BB:CC:DD:EE:11	AA:BB:CC:EE:DD:10	0800	10.10.1.10	10.10.1.200	67	68	MsgType: ACK YIADDR: 10.10.1.200 SIADDR: 10.10.1.10 Router (Opt 3): 10.10.1.10 DNS (Opt 6): 10.10.1.10

DHCP Snooping

DHCP Snooping is a countermeasure to DHCP Spoofing attacks implemented at L2 or L3 access switches.

First, the ports of the switch are divided into two categories: trusted and untrusted ones.

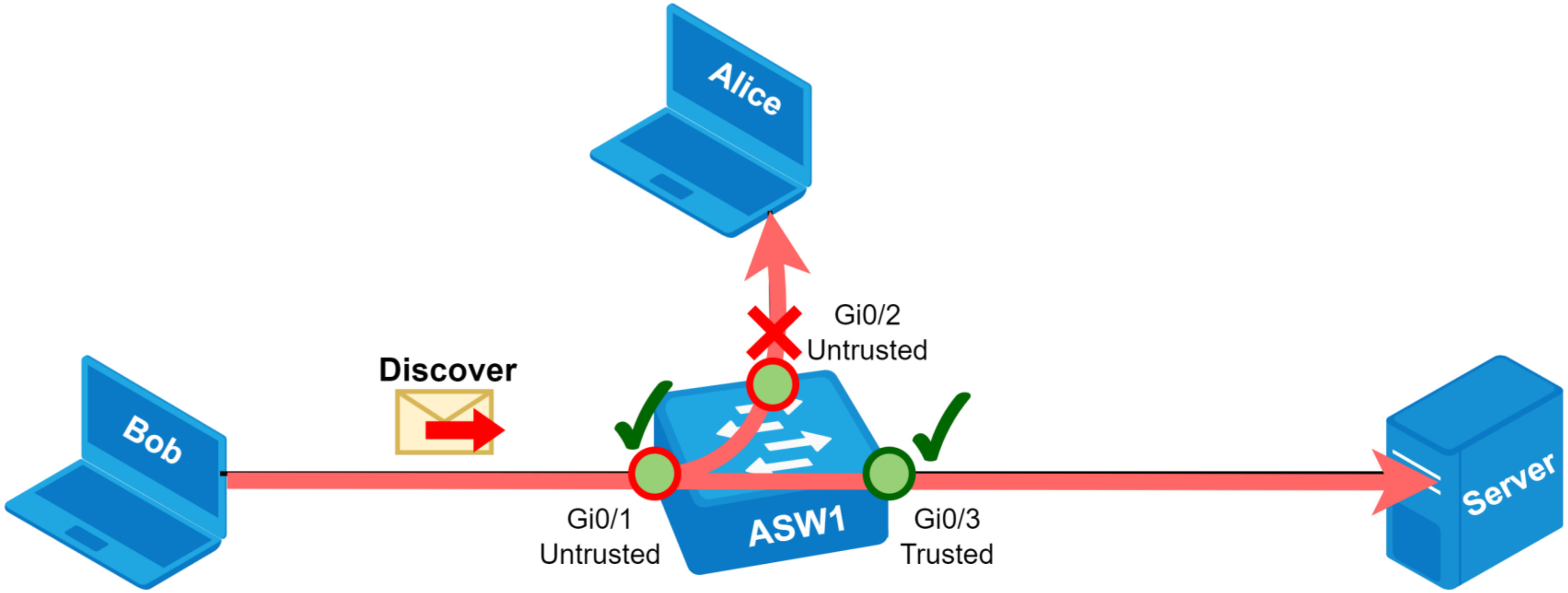
The Trusted ports allow all DHCP messages without filtering. The Trusted ports allow only the DHCP clients' message on the ingress and only DHCP server's messages on the egress



DHCP Snooping

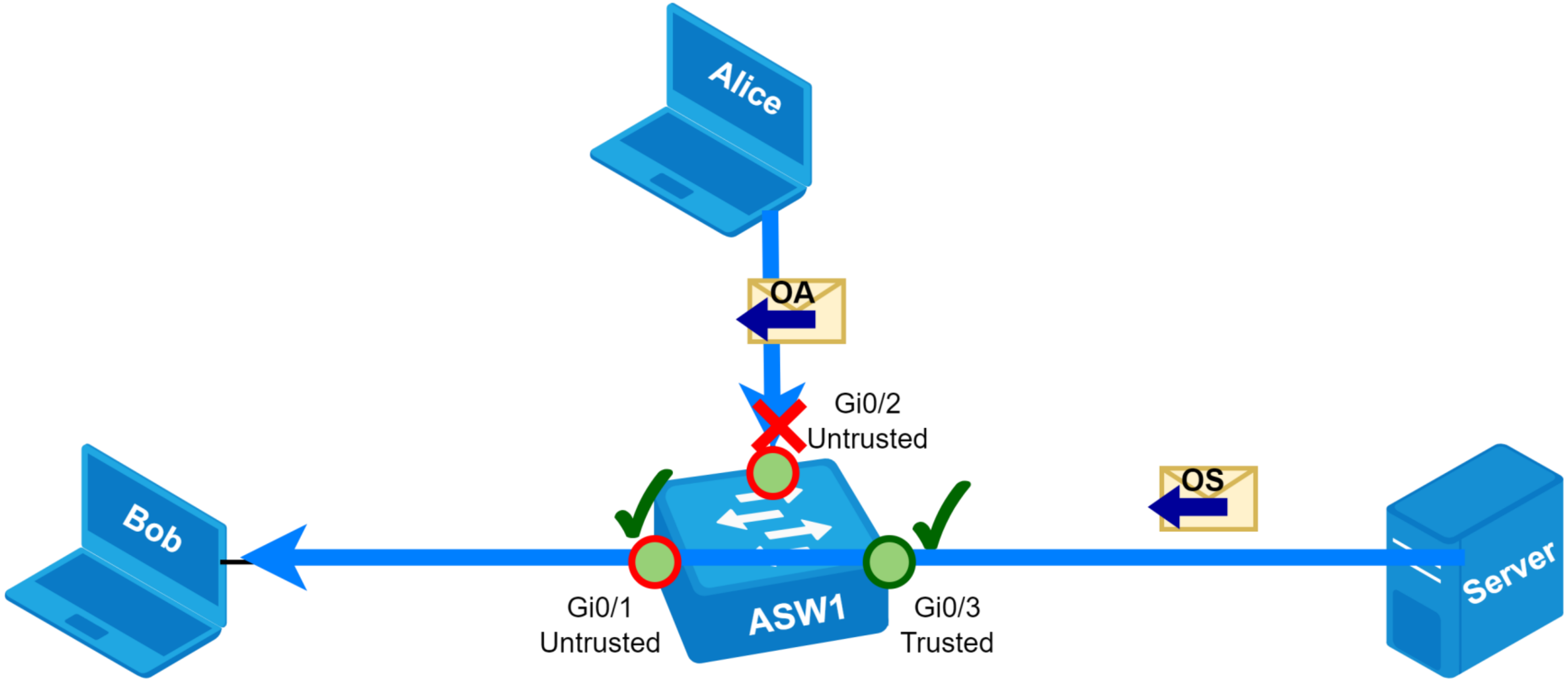
Now that Bob broadcasts the DCHP Discover message, it is allowed at Gi0/1 untrusted port on the ingress, but gets rejected on the egress of Gi0/2 untrusted port.

Thus the adversaries like Alice do not receive the Discovers from network host and have little chance to perpetrate a Spoofing attack



DHCP Snooping

Even if Alice tries to issue some random DHCP Offer, the respective frame will be blocked on the ingress of the untrusted port

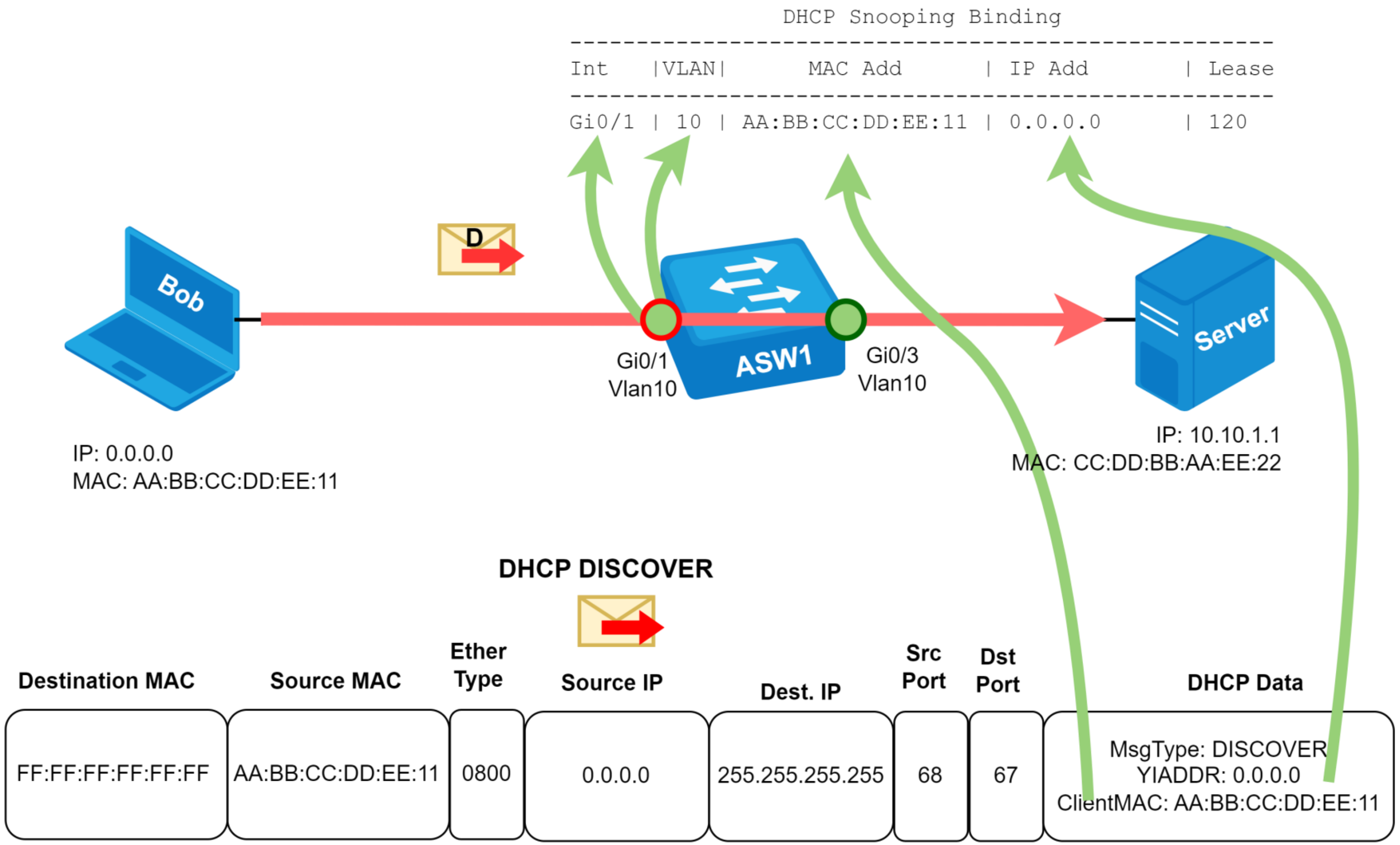


DHCP Snooping

When the Discover message arrives at the untrusted port, the switch parses the Client’s IP address and Client’s MAC address data from the respective fields of the DHCP packet (YIADDR and ClientMAC), and binds them to the port ID and VLAN ID in the DHCP Snooping Binding table.

As the Clients has no IP address at this stage of DHCP interaction, the respective field of the table fills in with all zeroes (IP 0.0.0.0).

The Lease field by default is assigned a value of 120 seconds.



```
                DHCP Snooping Binding
-----------------------------------------------------------
Int    |VLAN|      MAC Add       | IP Add         | Lease
-----------------------------------------------------------
Gi0/1  | 10  | AA:BB:CC:DD:EE:11 | 0.0.0.0        | 120
```

DHCP DISCOVER

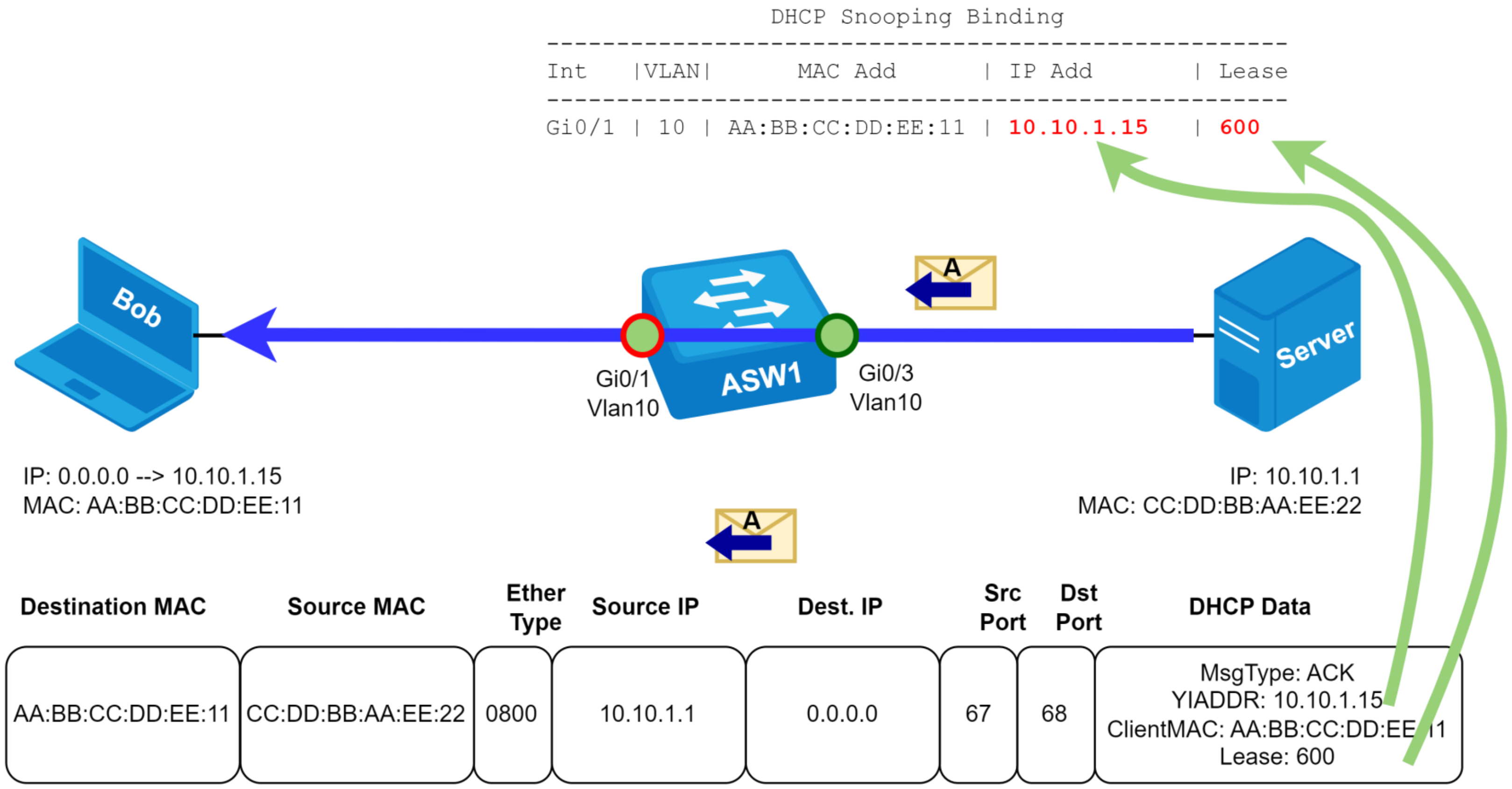
Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER YIADDR: 0.0.0.0 ClientMAC: AA:BB:CC:DD:EE:11

DHCP Snooping

Upon the receipt of the Ack message from DHCP Server, the switch extracts the values of YIADDR and LEASE fields and binds them into the respective row of the DHCP Snooping table.

Now the process of binding the Port, VLAN, Client’s MAC and Client’s IP address together is complete and the respective record may be used for frame filtering purposes.

DHCP Snooping table is a useful tool int countering DHCP Spoofing, ARP Spoofing and Man-in-the-Middle attacks.



```
                 DHCP Snooping Binding
----------------------------------------------------------
Int    |VLAN|      MAC Add        | IP Add        | Lease
----------------------------------------------------------
Gi0/1 | 10 | AA:BB:CC:DD:EE:11 | 10.10.1.15    | 600
```

Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
AA:BB:CC:DD:EE:11	CC:DD:BB:AA:EE:22	0800	10.10.1.1	0.0.0.0	67	68	MsgType: ACK YIADDR: 10.10.1.15 ClientMAC: AA:BB:CC:DD:EE:11 Lease: 600

DHCP Snooping @ MES23xx/33xx/35xx/5324

To configure the DHCP Snooping feature at MES 23xx/33xx/35xx/5324 switches according to our example, use the following commands:

```
MES2308P(config)# interface range gigabitEthernet 0/1-2
MES2308P(config-if-range)# switchport mode access
MES2308P(config-if-range)# switchport access vlan 10
MES2308P(config-if-range)# interface gigabitEthernet 0/3
MES2308P(config-if)# ip dhcp snooping trust
MES2308P(config-if)# exit
MES2308P(config)# ip dhcp snooping
MES2308P(config)# ip dhcp snooping vlan 10
```

DHCP Snooping @ MES23xx/33xx/35xx/5324

To view the DHCP Snooping table of particular MES23xx/33xx/35xx/5324 switch, use the following command:

```
MES2308P# show ip dhcp snooping binding
Total number of binding: 2

   MAC Address       IP Address    Lease (sec)     Type    VLAN Interface
------------------ --------------- ------------ ---------- ---- ----------
AA:BB:CC:DD:EE:11   10.10.1.15     499          learned    10   gi1/0/1
AA:BB:CC:DD:EE:10   10.10.1.10     520          learned    10   gi1/0/2
```

DHCP Snooping @ MES14xx/24xx

To configure a DHCP Snooping feature at MES 14xx/24xx switches, the following commands are applied:

Create VLAN 10, activate it and initiate DHCP Snooping for the VLAN

```
MES1428(config)# vlan 10
MES1428(config-vlan)# vlan active
MES1428(config-vlan)# ip dhcp snooping
MES1428(config-vlan)# exit
```

Configure untrusted ports:

```
MES1428(config)# interface range gi0/1-2
MES1428(config-if-range)# switchport mode access
MES1428(config-if-range)# switchport access vlan 10
```

continued on the next slide
↓ ↓

DHCP Snooping @ MES14xx/24xx

Configure trusted port:

```
MES1428(config-if-range)# interface gi0/3
MES1428(config-if)# switchport mode access
MES1428(config-if)# switchport access vlan 10
MES1428(config-if)# port-security-state trusted
MES1428(config-if)# set port uplink
```

To view the DHCP Snooping Binding table, use the following command:

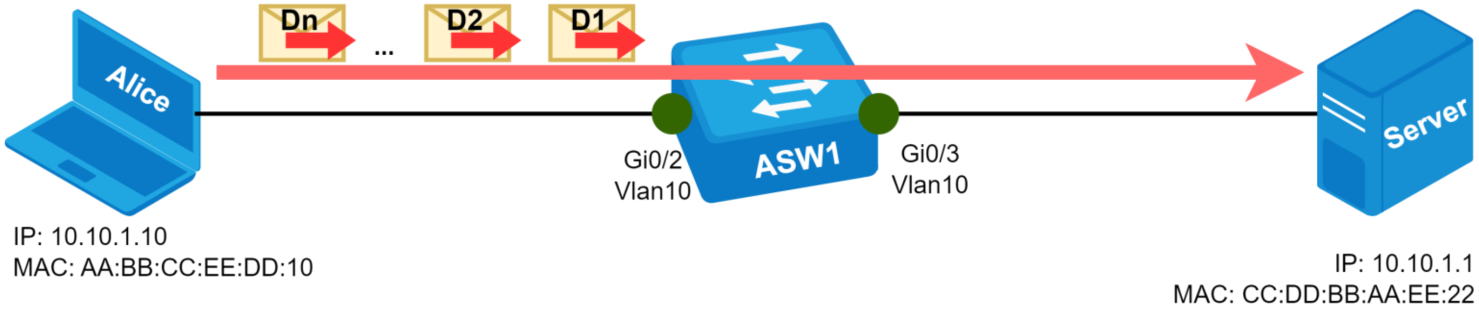
```
MES1428# show ip binding
VLAN      HostMac           HostIP       Port    GatewayIP    Type   Lease Duration
----  ------------------ -----------   --------  -----------  -----  -------------
10    AA:BB:CC:DD:EE:11   10.10.1.15    gi 0/1   10.10.1.1     dhcp    513
10    AA:BB:CC:DD:EE:10   10.10.1.10    gi 0/2   10.10.1.1     dhcp    513
```

DHCP Starvation Attack

The DHCP Starvation attack exploits one of the natural flaws of DHCP: when DHCP server receives a DHCP Discover message from a client, it books and IP address from a pool of addresses and keeps it available for issue for a certain period of time or till it receives a Request message from the client.

If an adversary can generate the random Discover messages fast enough, the DHCP server ends up with no IP addresses available in the pool. Such a condition is called ‘DHCP starvation’.

```
#    |        MAC        |    IP
-----|-------------------|----------
1    | AA:BB:CC:DD:EE:11 |10.10.1.11
2    | AA:BB:CC:DD:EE:12 |10.10.1.12
...
244  | AA:BB:CC:DD:EE:FE |10.10.2.254
```



	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
D1	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
D2	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:12	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
	...							
Dn	FF:FF:FF:FF:FF:FF	AA:BB:CC:FF:EF:FF	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER

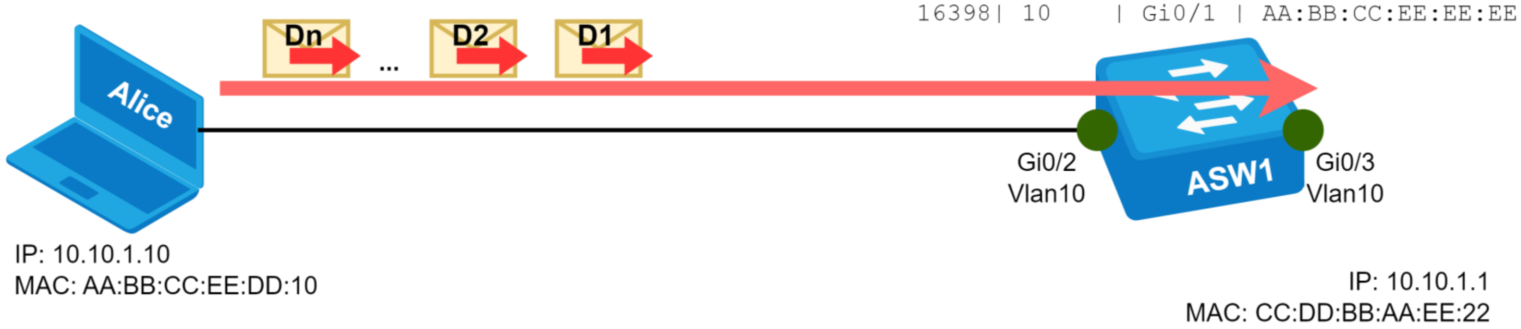
MAC Poisoning Attack

Another vector of mass-broadcast of forged Discover packets is the overfill of MAC address table of a switch.
As we know, a switch is learning the Source MAC addresses of ingress frames on its interface.

However, the MAC address table has its limits. Thus, provided the frames are generated by the adversary quick enough, the MAC address table may become overfilled and, when the last MAC is learned and there is no more spare entries to learn the MACs, the switch starts flooding the ingress frames from all available ports, creating a broadcast or unknown unicast storms.

Port Security feature helps mitigate the MAC poisoning attack by reducing the rate the MACs are learned on a particular port.

```
                MAC Address Table
 #    | VLAN  | Port  |        MAC
------|-------|-------|-----------------
1     | 10    | Gi0/1 | AA:BB:CC:DD:EE:11
2     | 10    | Gi0/1 | AA:BB:CC:DD:EE:12
                  ...
16398| 10     | Gi0/1 | AA:BB:CC:EE:EE:EE
```



	Destination MAC	Source MAC	Ether Type	Source IP	Dest. IP	Src Port	Dst Port	DHCP Data
D1	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:11	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
D2	FF:FF:FF:FF:FF:FF	AA:BB:CC:DD:EE:12	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER
	...							
Dn	FF:FF:FF:FF:FF:FF	AA:BB:CC:FF:EF:FF	0800	0.0.0.0	255.255.255.255	68	67	MsgType: DISCOVER

Port security @ MES23xx/33xx/35xx/5324

To leverage the PortSecurity feature, you are expected to configure the following:

Maximum possible number of MACs to be learned on the particular switch port

1

The way the MAC addresses will be learned at the switch port

2

The way the learned MAC addresses will be stored withing the switch

3

The way the unlearned MAC addresses will be treated by the switch

4

Port security @ MES23xx/33xx/35xx/5324

Configure the maximum possible number of learned MAC addresses:

```
MES2308P(config)# interface gi1/0/1
MES2308P(config-if)# port security max num
```

num – maximum number of learned MAC addresses

Port security @ MES23xx/33xx/35xx/5324

Configure the MAC addresses learning mode:

```
MES2308P(config-if)# port security mode learningmode
```

The learningmode variable may have the following values:

`Max-addresses` – deletes the already-learned MACs and allows the learning up to the number indicated by port security max command. Aging and re-learning of MACs are ***allowed***

`Secure` – deletes the learned MACs and allows the learning up to the number indicated by port security max command. Aging and re-learning of MACs are ***forbidden***

`Lock` – saves the already-learned MACs. Aging and re-learning of MACs are ***forbidden***

The aging of the addresses in MAC address table may be fine-tuned by the following command:

```
MES2308P(config)#mac address-table aging-time <10-1000000 sec>
```

Port security @ MES23xx/33xx/35xx/5324

If you use the `secure` learning mode, you may choose from two options of storing the MAC addresses learned at the port:

```
MES2308P(config-if)# port security mode secure storemode
```

The *storemode* variable accepts the following values:

`permanent` – the learned MAC-addresses are stored at startup-config and persist after reload

`delete-on-reset` – the learned MACs are deleted after reload

Port security @ MES23xx/33xx/35xx/5324

Configure what the switch will do with frames with unlearned Source MAC addresses”

```
MES2308P(config-if)# port security discardmode
```

The possible options are as follows:

`Discard` – (default mode). The frames with unlearned MAC-addresses are discarded, the MACs are not to be learned.

`discard-shutdown` – The frames with unlearned MAC-addresses are discarded, the MACs are not to be learned, the port goes into Errdisable status.

`Discard-shutdown-vlan` – The frames with unlearned MACs are discarded, the port is assigned to VLAN 4095.

Port security @ MES23xx/33xx/35xx/5324

Configuration example: limit the number of MACs to be learned to 2 maximum, store the learned MACs permanently, even if the switch will be re-loaded, discard all other frames without shutting the port down:

```
MES2308P(config)# interface gi1/0/5
MES2308P(config-if)#port security max 2
MES2308P(config-if)#port security mode secure permanent
MES2308P(config-if)#port security discard
```

Port security @ MES23xx/33xx/35xx/5324

```
MES2308P#show ports security status
Port        Status      Action       Current      Blocked VLAN list
---------  ----------  ------------  -----------  -------------------
gi1/0/1    Disabled    -             -            -
gi1/0/2    Disabled    -             -            -
gi1/0/3    Disabled    -             -            -
gi1/0/4    Disabled    -             -            -
gi1/0/5    Enabled     Discard       0            -
gi1/0/6    Disabled    -             -            -
gi1/0/7    Disabled    -             -            -
gi1/0/8    Disabled    -             -            -
gi1/0/9    Disabled    -             -            -
gi1/0/10   Disabled    -             -            -
gi1/0/11   Disabled    -             -            -
gi1/0/12   Disabled    -             -            -
```

We are always ready to discuss, develop and customize products for your needs!

630020, Russia, Novosibirsk, Okruzhnaya street, 29V
9:00 AM – 6:00 PM (GMT+7)
Monday – Friday

+7 (383) 274-10-01, 274-48-48
eltex@eltex-co.ru; eltex-co.com

ELTEX Enterprise Ltd. | Russian developer and manufacturer of communication equipment