# **51. Dynamic ARP Inspection (DAI)**

## **What is Dynamic ARP Inspection (DAI)?**

### **ARP Review**

* ARP is used to learn the MAC address of another device with a known IP address.
  + For example, a PC will use ARP to learn the MAC address of its default gateway to communicate with external networks.
* Typically, it is a two-message exchange:
  + **ARP Request**
  + **ARP Reply**

### **Gratuitous ARP (GARP)**

* A **Gratuitous ARP (GARP) message** is an ARP reply that is sent without receiving an ARP request.
* It is sent to the broadcast MAC address.
* It allows other devices to learn the MAC address of the sending device without having to send ARP requests.
* Some devices automatically send GARP messages when:
  + An interface is enabled.
  + An IP address is changed.
  + A MAC address is changed.

## **Dynamic ARP Inspection (DAI)**

* DAI is a **security feature** of switches that filters ARP messages received on **untrusted ports**.
* DAI only filters **ARP messages**; non-ARP messages are not affected.
* By default, **all ports are untrusted**.
  + Typically, all ports connected to other network devices (switches, routers) should be configured as **trusted**.
  + Interfaces connected to end hosts should remain **untrusted**.

## **ARP Poisoning (Man-in-the-Middle Attack)**

* Similar to **DHCP poisoning**, ARP poisoning involves an attacker manipulating a target’s ARP tables so that traffic is sent to the attacker.
* The attacker can send **Gratuitous ARP messages** using another device’s IP address.
* Other devices in the network will receive the GARP and update their ARP tables, causing them to send traffic to the attacker instead of the legitimate destination.

## **Dynamic ARP Inspection Operations**

* DAI inspects the **Sender MAC** and **Sender IP** fields of ARP messages received on untrusted ports and checks for a matching entry in the **DHCP Snooping Binding Table**:
  + **If there is a match**, the ARP message is forwarded.
  + **If there is no match**, the ARP message is discarded.
* DAI does **not** inspect messages received on trusted ports; they are forwarded as normal.
* **ARP ACLs** can be manually configured to map IP addresses to MAC addresses for DAI verification.
  + Useful for hosts that **don’t use DHCP**.
* DAI can be configured for **additional checks**, though these are optional.
* **Rate-limiting** is supported to prevent attackers from overwhelming the switch with ARP messages.
  + Both **DHCP Snooping** and **DAI** require processing by the switch’s CPU.
  + Even if the attacker's messages are blocked, they can overload the switch CPU with ARP messages.

## **Dynamic ARP Inspection Configuration**

### **Basic Commands:**

**Verify configuration:** SW1#show ip arp inspection interfaces

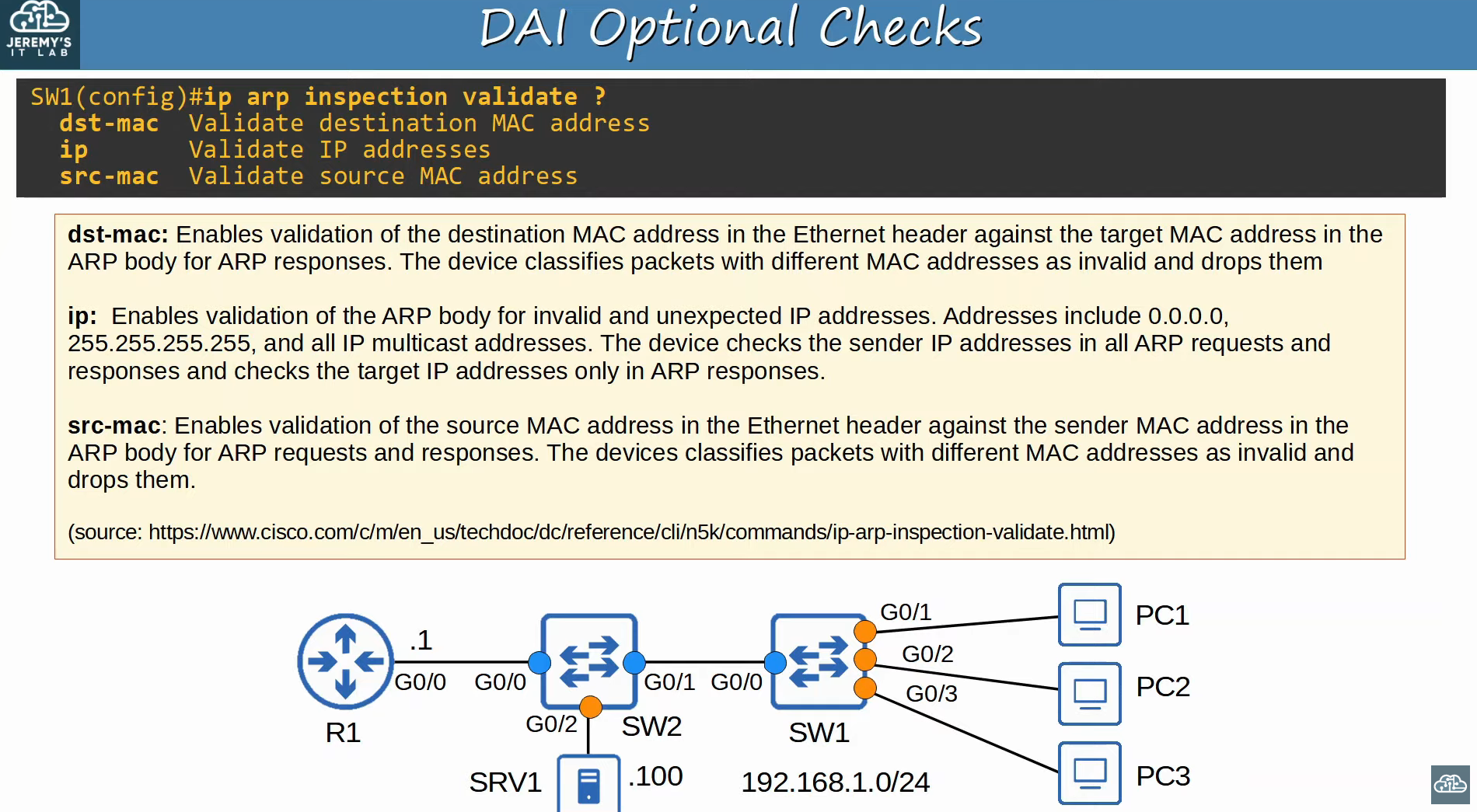
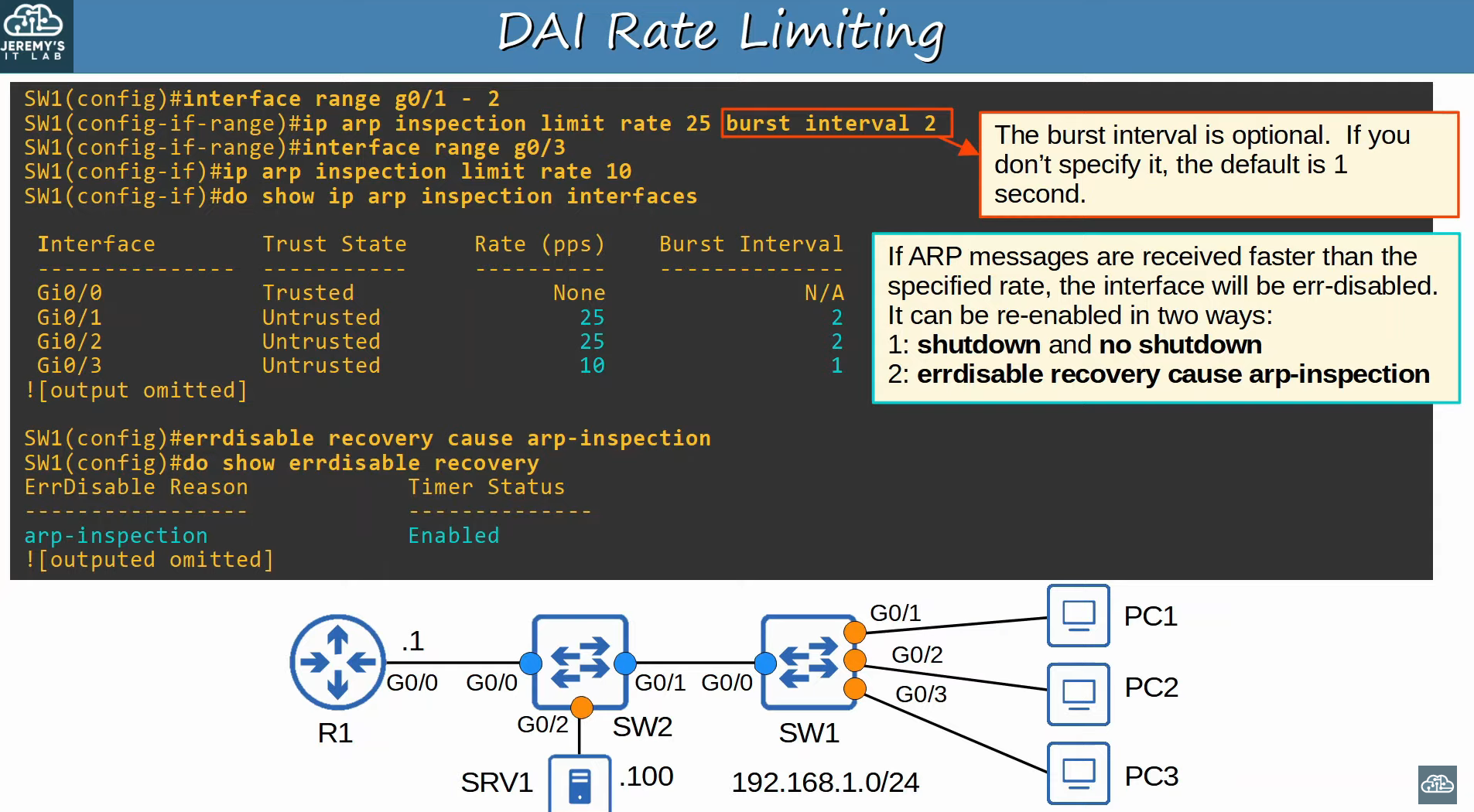
**Enable DAI on a VLAN:** SW2(config)# ip arp inspection vlan <VLAN\_ID>

**Set a trusted interface:** SW2(config)# interface <INTERFACE>

SW2(config)# ip arp inspection trust

**Configure rate-limiting:** SW1# ip arp inspection limit rate <RATE>

**Check DAI statistics:** SW1#show ip arp inspection



## **ARP ACLs (Beyond Scope of CCNA)**

* ARP ACLs can be used to define static mappings for IP and MAC addresses.

Example: **Creating an ARP ACL for SRV1** ip arp access-list <ACL\_NAME>

permit ip host <IP\_ADDRESS> mac host <MAC\_ADDRESS>

**Apply ACL to a switch:** ip arp inspection filter <ACL\_NAME> vlan <VLAN\_ID>

## **Command Review**

| **Command** | **Description** |
| --- | --- |
| show ip arp inspection | Displays a summary of DAI configuration and statistics |
| ip arp inspection vlan <VLAN\_ID> | Enables DAI on a specific VLAN |
| ip arp inspection trust | Configures an interface as trusted |
| ip arp inspection limit rate <RATE> | Limits the rate of ARP messages |
| show ip arp inspection interfaces | Displays per-interface DAI settings |