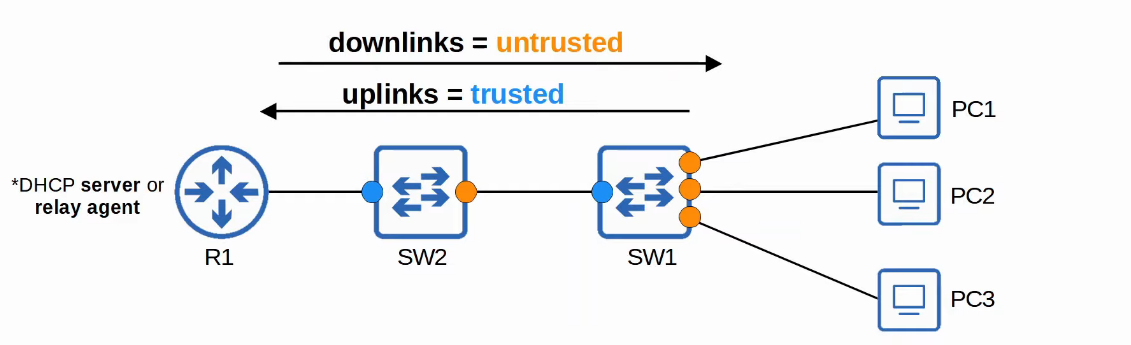
# **50. DHCP Snooping (Layer 2)**

## **What is DHCP Snooping?**

* **DHCP Snooping** is a security feature of switches used to filter DHCP messages received on untrusted ports.
* It only filters **DHCP messages** and does not affect non-DHCP messages.
* **By default, all ports are untrusted**.
  + Typically, **uplink ports** are configured as **trusted**, while **downlink ports** remain **untrusted**.



## **Attacks on DHCP**

### **DHCP Starvation**

* A type of DHCP-based attack known as a **DHCP Starvation Attack**.
* The attacker **spoofs MAC addresses** to flood DHCP Discover messages.
* This causes the **target DHCP server’s pool to become full**, resulting in a **Denial of Service (DoS)** to other devices.

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

* Similar to **ARP Poisoning**, **DHCP Poisoning** enables **Man-in-the-Middle (MitM) attacks**.
* A **spurious DHCP server** responds to clients’ DHCP Discover messages, assigning them **fake IP addresses**.
* The **clients unknowingly use the attacker’s server as their default gateway**.
  + Clients typically **accept the first DHCP Offer message they receive**.
* This allows the attacker to **intercept, examine, or modify traffic** before forwarding it to the legitimate gateway.

## **DHCP Messages**

DHCP Snooping differentiates between messages sent by **DHCP servers** and **DHCP clients**:

### **Messages Sent by DHCP Servers:**

* **OFFER**
* **ACK**
* **NAK** (Opposite of ACK; used to decline a client’s request)

### **Messages Sent by DHCP Clients:**

* **DISCOVER**
* **REQUEST**
* **RELEASE** (Notifies the server that the client no longer needs the assigned IP address)
* **DECLINE** (Client declines the IP address offered by a DHCP server)

## **How Does DHCP Snooping Work?**

1. **Trusted Ports**:  
   * If a **DHCP message** is received on a **trusted port**, it is **forwarded as normal** without inspection.
2. **Untrusted Ports**:  
   * If a **DHCP message** is received on an **untrusted port**, it is **inspected and processed** as follows:
     + If it is a **DHCP server message**, it is **discarded**.
     + If it is a **DHCP client message**, additional checks are performed:
       - **DISCOVER / REQUEST Messages**:
         * Check if the **frame’s source MAC address** matches the **DHCP message’s CHADDR field**.
         * **Match → Forward**
         * **Mismatch → Discard**
       - **RELEASE / DECLINE Messages**:
         * Check if the **packet’s source IP address** matches the entry in the **DHCP Snooping Binding Table**.
         * **Match → Forward**
         * **Mismatch → Discard**
3. **DHCP Snooping Binding Table**:  
   * When a **client successfully leases an IP address**, an entry is created in the **DHCP Snooping Binding Table**.

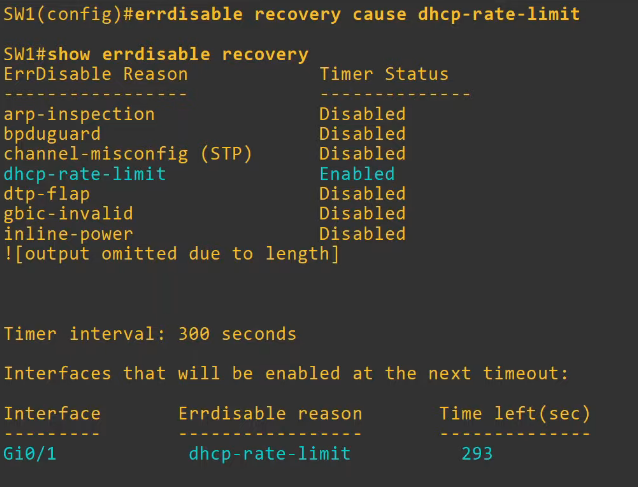
## **DHCP Snooping Configuration**

### **DHCP Snooping Rate-Limiting**

* DHCP Snooping can **limit the rate** of DHCP messages entering an interface.
* If the **rate exceeds the limit**, the interface is **err-disabled**.

The interface can be **manually or automatically re-enabled** using:  
SW1(config)# errdisable recovery cause dhcp-rate-limit

* Setting the limit too low (e.g., 1) may **immediately disable the port**.



## **DHCP Option 82 (Information Option)**

* Also known as **DHCP Relay Agent Information Option**.
* Provides additional information about **which DHCP relay agent** received the client’s message (e.g., interface, VLAN, etc.).
* DHCP relay agents can **add Option 82** before forwarding messages to a remote DHCP server.
* **Cisco switches add Option 82 by default**, even if they are **not acting as a DHCP relay agent**.
* **By default, Cisco switches drop DHCP messages with Option 82 received on untrusted ports**.

### **Enabling Option 82 on Both Switches**

* Ensures **PC1’s DHCP Discover message** passes through **SW1 and SW2** to **R1**.
* **R1 responds with a DHCP Offer message as normal**.

## 

## 

## **Command Summary**

| **Command** | **Description** |
| --- | --- |
| ip dhcp snooping | Enables DHCP Snooping globally |
| ip dhcp snooping vlan <VLAN\_ID> | Enables DHCP Snooping for a specific VLAN |
| interface <INTERFACE> | Enters interface configuration mode |
| ip dhcp snooping trust | Configures an interface as **trusted** |
| ip dhcp snooping limit rate <RATE> | Limits the rate of DHCP messages per second |
| show ip dhcp snooping | Displays the DHCP Snooping configuration and statistics |
| show ip dhcp snooping binding | Displays the DHCP Snooping binding table |