Introduction and Overview

- Welcome to **Jeremy's IT Lab**, a free, complete course for the **CCNA**.
- This video focuses on **DHCP snooping**.

What is DHCP Snooping?

- **DHCP snooping** is a security feature available on Cisco switches which helps to protect against attacks which take advantage of **DHCP**.

Exam Context

- **DHCP snooping** is covered in **exam topic 5.7**, which requires the ability to configure layer 2 security features, including:
  - **DHCP snooping**
  - **Dynamic ARP inspection**
  - **Port security**
- **Port security** was already covered in a previous lecture.
- **Dynamic ARP inspection** will be covered in the next lecture.

Lecture Structure

- This lecture is similar in structure to the previous video on port security.
- The following topics will be covered:
  - What **DHCP snooping** is
  - How it works
  - What attacks it prevents
  - How to configure it on Cisco switches

Bonus Content

- A bonus practice question from **Boson Software's ExSim for CCNA** is included at the end of the video.

Basics of DHCP Snooping

- **DHCP snooping** is a security feature of switches that is used to **filter DHCP messages** received on **untrusted ports**.
- **DHCP snooping** only filters **DHCP messages** — any other **non-DHCP messages** are not affected.

Trusted and Untrusted Ports

- **All ports are untrusted by default**.
- It is up to the network admin to configure which ports will be **trusted**.
- Usually, **uplink ports** are configured as **trusted ports**, and **downlink ports** remain **untrusted**.

Example: Network Diagram — R1, Switches, and End Hosts

- **R1** is either a **DHCP server** or a **DHCP relay agent**.
- The end hosts, the **PCs**, will use **DHCP** to receive an IP address from **R1**.
- **Downlink ports** on the switches (interfaces pointing toward the end hosts) should be **untrusted**:
  - The network admin does **not** have direct control over end user devices.
  - A malicious user could initiate a **DHCP-based attack** from one of their devices.
  - It is best to leave these ports in the default **untrusted** state.
- **Uplink ports** point toward the **network infrastructure**, the devices the network admin has control over:
  - We can be pretty sure that **R1** isn't going to initiate a **DHCP-based attack**.
  - These interfaces can be configured as **trusted ports**.
  - **DHCP snooping** will not inspect any messages on trusted ports — the switch will simply forward them as normal.

Example: PC1 Sends a DHCP Message (Forwarded Normally)

- **PC1** sends a DHCP message, for example a **DISCOVER** message.
- **SW1** receives the message on an **untrusted port**, so it inspects the message to see if it is okay.
- **SW1** determines the message is fine, so it forwards it as normal.
- **SW2** receives it, again on an **untrusted interface**.
- **SW2** checks the message, determines it is okay, and forwards it to **R1**.
- **R1** then sends the reply, and it goes straight back to **PC1** without being inspected by **SW2** or **SW1**.

Why don't the switches inspect the message from R1?

- The switches received the reply on their **trusted ports**, so they assume the message is okay — no need to check it.

Example: PC2 Sends a DHCP Message (Discarded by SW1)

- **PC2** sends a DHCP message.
- **SW1** receives it on an **untrusted port**, so it inspects the message.
- This time, **SW1** determines that the message is **not OK**, so it **discards** the message.
- Perhaps the user of **PC2** was trying to use a **DHCP exploit**, so **SW1** decided to drop the message.

> ***Note: The professor notes that the exact mechanism for how DHCP snooping determines if a message is OK or not will be covered later in the video.***
