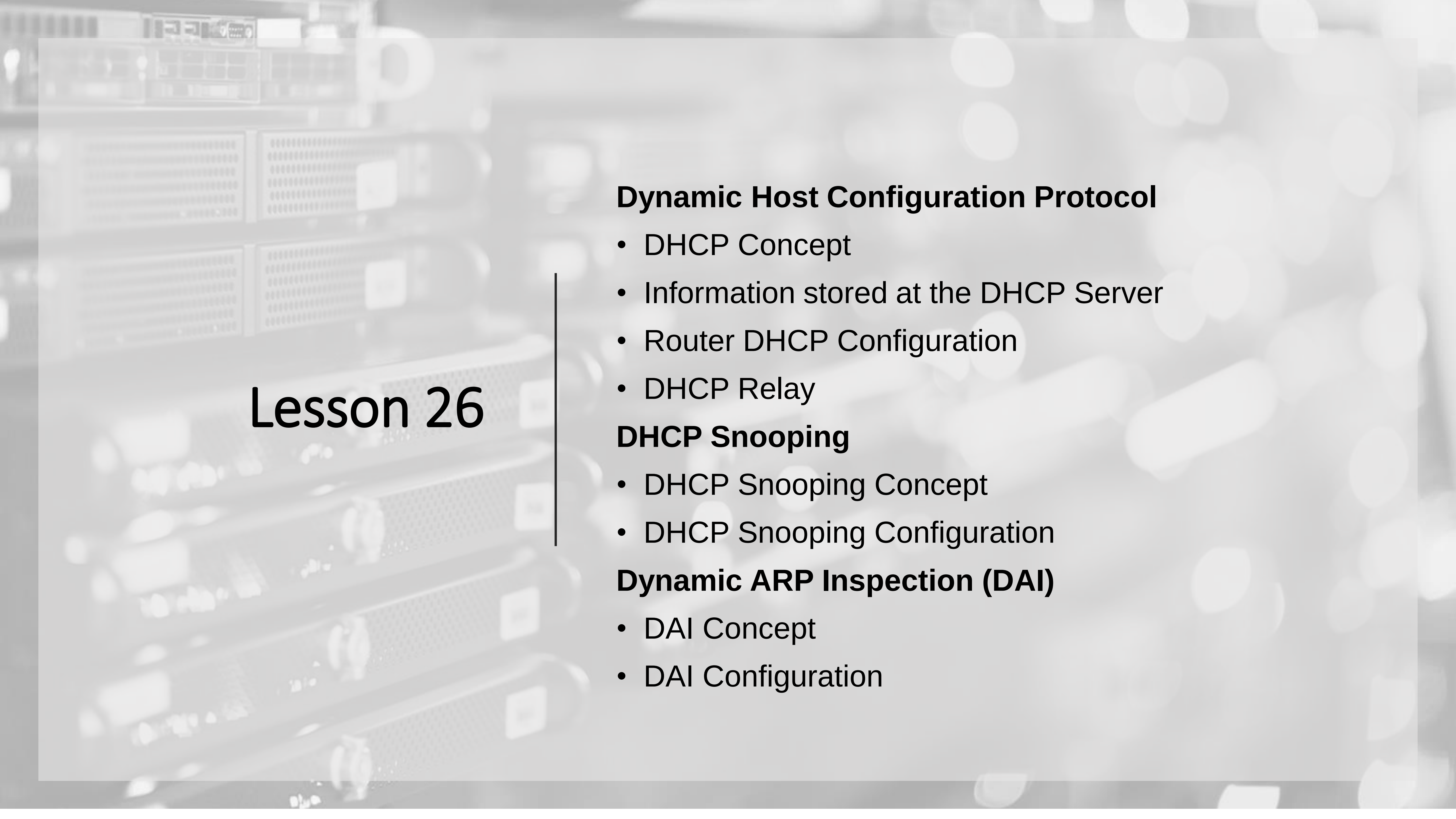
CCNA 200-301

CISCO™



Lesson 26

Dynamic Host Configuration Protocol

- DHCP Concept
- Information stored at the DHCP Server
- Router DHCP Configuration
- DHCP Relay

DHCP Snooping

- DHCP Snooping Concept
- DHCP Snooping Configuration

Dynamic ARP Inspection (DAI)

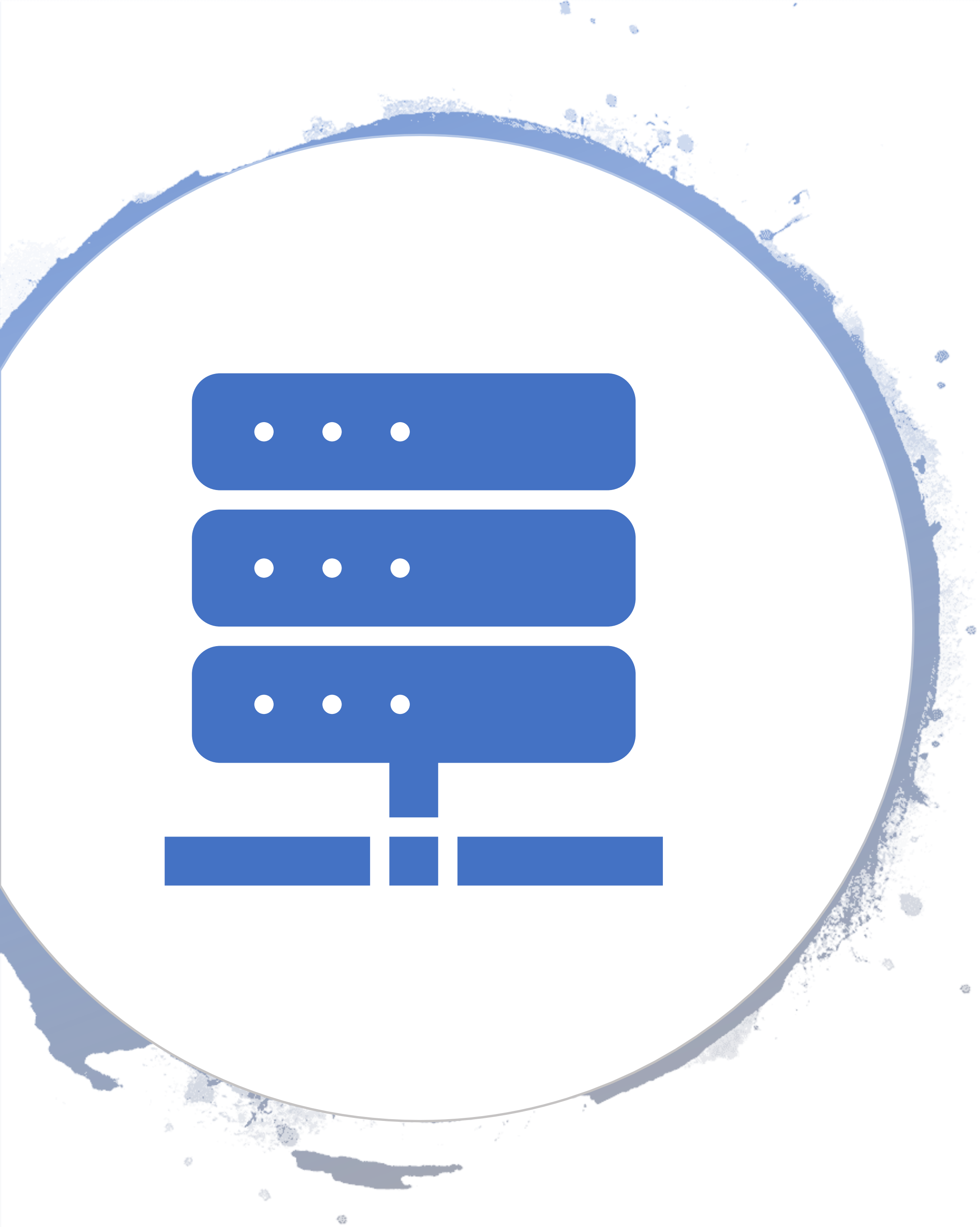
- DAI Concept
- DAI Configuration

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) provides one of the most commonly used services in a TCP/IP network. The vast majority of hosts in a TCP/IP network are user devices, and the vast majority of user devices learn their IPv4 settings using DHCP.

Using DHCP has several advantages over the other option of manually configuring IPv4 settings. The configuration of host IP settings sits in a DHCP server, with each client learning these settings using DHCP messages. As a result, the host IP configuration is controlled by the IT staff, rather than on local configuration on each host, resulting in fewer user errors. DHCP allows both the permanent assignment of host addresses, but more commonly, DHCP assigns a temporary lease of IP addresses. With these leases, the DHCP server can reclaim IP addresses when a device is removed from the network, making better use of the available addresses.

DHCP also enables mobility. For example, every time a user moves to a new location with a tablet computer—to a coffee shop, a client location, or back at the office—the user's device can connect to another wireless LAN, use DHCP to lease a new IP address in that LAN, and begin working on the new network. Without DHCP, the user would have to ask for information about the local network and configure settings manually, with more than a few users making mistakes.



DHCP Concepts

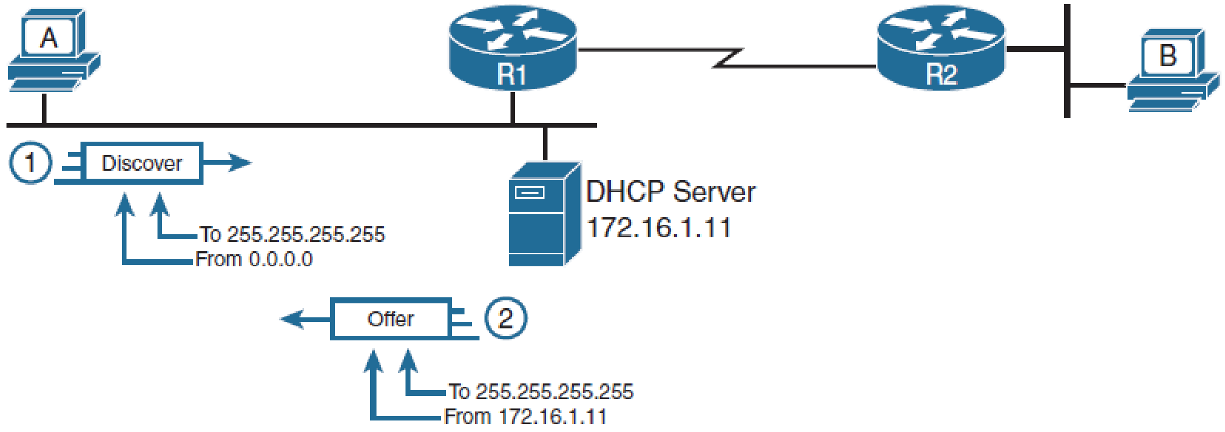
DHCP uses the following four messages between the client and server. (Also, as a way to help remember the messages, note that the first letters spell DORA):

- **Discover:** Sent by the DHCP client to find a willing DHCP server
- **Offer:** Sent by a DHCP server to offer to lease to that client a specific IP address (and inform the client of its other parameters)
- **Request:** Sent by the DHCP client to ask the server to lease the IPv4 address listed in the Offer message
- **Acknowledgment:** Sent by the DHCP server to assign the address and to list the mask, default router, and DNS server IP addresses

DHCP Concepts cont.

DHCP clients, however, have a somewhat unique problem: they do not have an IP address yet, but they need to send these DHCP messages inside IP packets. To make that work, DHCP messages make use of two special IPv4 addresses that allow a host that has no IP address to still be able to send and receive messages on the local subnet :

- **0.0.0.0:** An address reserved for use as a source IPv4 address for hosts that do not yet have an IP address.
- **255.255.255.255:** The local broadcast IP address. Packets sent to this destination address are broadcast on the local data link, but routers do not forward them.



Information Stored at the DHCP Server

The following list shows the types of settings the DHCP server needs to know to support DHCP clients:

- **Subnet ID and mask:** The DHCP server can use this information to know all addresses in the subnet. (The DHCP server knows to not lease the subnet ID or subnet broadcast address.)
- **Reserved (excluded) addresses:** The server needs to know which addresses in the subnet to *not* lease. This list allows the engineer to reserve addresses to be used as static IP addresses. For example, most router and switch IP addresses, server addresses, and addresses of most anything other than user devices use a statically assigned IP address. Most of the time, engineers use the same convention for all subnets, either reserving the lowest IP addresses in all subnets or reserving the highest IP addresses in all subnets.
- **Default router(s):** This is the IP address of the router on that subnet.
- **DNS IP address(es):** This is a list of DNS server IP addresses.

Configuring Router as a DHCP Server

```
ip dhcp pool {pool_name}
  network {networ_id subnet_mask}
  default-router {default_router_IP}
  dns-server {dns_server_IP}
ip dhcp excluded-address {reserved_addresses}
```

DHCP Relay

Network engineers have a major design choice to make with DHCP: Do they put a DHCP server in every LAN subnet or locate a DHCP server in a central site? The question is legitimate. Cisco routers can act as the DHCP server, so a distributed design could use the router at each site as the DHCP server. With a DHCP server in every subnet, the protocol flows stay local to each LAN.

However, a centralized DHCP server approach has advantages as well. In fact, some Cisco design documents suggest a centralized design as a best practice, in part because it allows for centralized control and configuration of all the IPv4 addresses assigned throughout the enterprise.

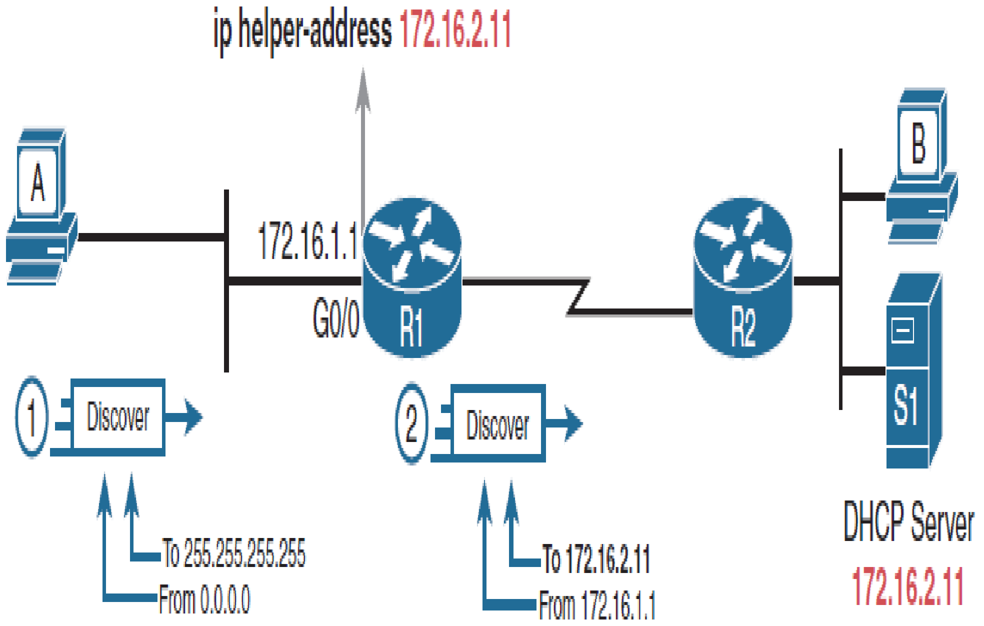
The **ip helper-address** *server-ip* subcommand tells the router to do the following for the messages coming in an interface, from a DHCP client:

1. Watch for incoming DHCP messages, with destination IP address 255.255.255.255.

2. Change that packet's source IP address to the router's incoming interface IP address.

3. Change that packet's destination IP address to the address of the DHCP server (as configured in the **ip helper-address** command).

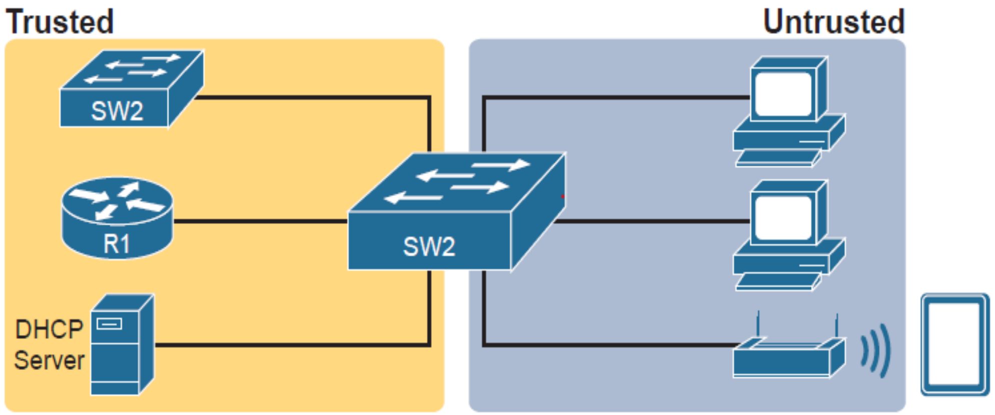
4. Route the packet to the DHCP server.



DHCP Snooping Concept

DHCP Snooping on a switch acts like a firewall or an ACL in many ways. It analyzes incoming messages on the specified subset of ports in a VLAN. DHCP Snooping never filters non-DHCP messages, but it may choose to filter DHCP messages, applying logic to make a choice—allow the incoming DHCP message or discard the message.

While DHCP itself provides a Layer 3 service, DHCP Snooping operates on LAN switches and is commonly used on Layer 2 LAN switches and enabled on Layer 2 ports. The reason to put DHCP Snooping on the switch is that the function needs to be performed between a typical end-user device—the type of device that acts as a DHCP client—and DHCP servers or DHCP relay agents.

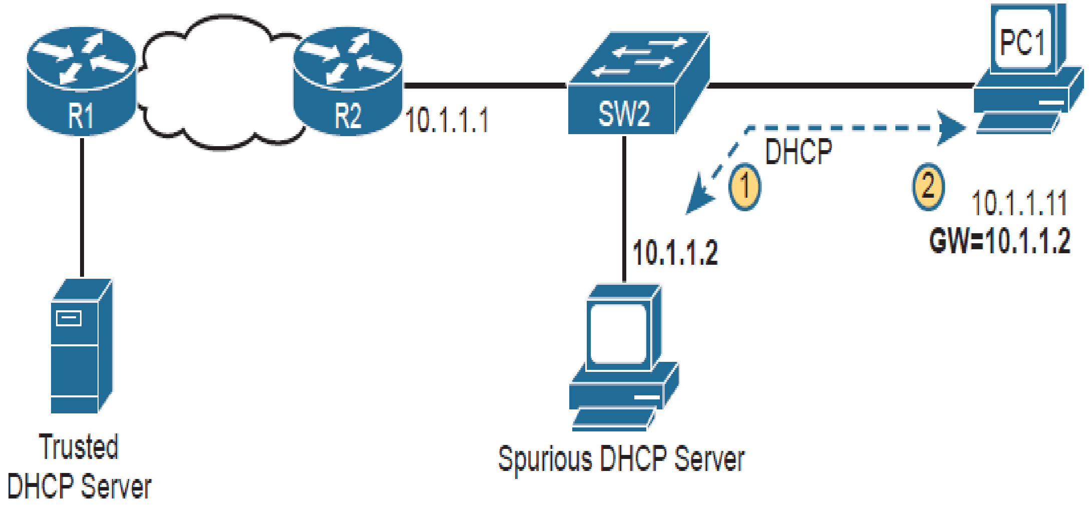


A Sample Attack: A Spurious DHCP Server

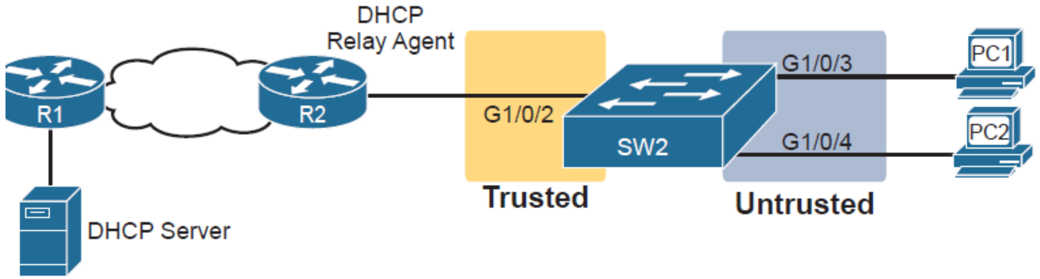
To give you some perspective, Figure shows a legitimate user's PC on the far right and the legitimate DHCP server on the far left. However, an attacker has connected his laptop to the LAN and started his DHCP attack by acting like a DHCP server. Following the steps in the figure, assume PC1 is attempting to lease an IP address while the attacker is making his attack:

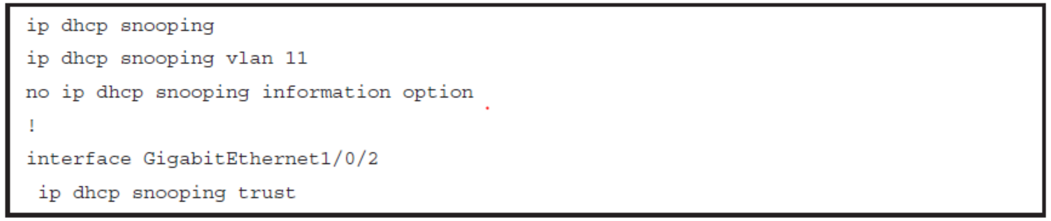
1. PC1 sends a LAN broadcast with PC1's first DHCP message (DHCPDISCOVER).

2. The attacker's PC—acting as a spurious DHCP server—replies to the DHCPDISCOVER with a DHCPOFFER.



Configuring DHCP Snooping on a Layer 2 Switch





```
ip dhcp snooping
ip dhcp snooping vlan 11
no ip dhcp snooping information option
!
interface GigabitEthernet1/0/2
 ip dhcp snooping trust
```

Limiting DHCP Message Rates

- **Step 1. (Optional):** Configure DHCP Snooping rate limits and err-disabled recovery:

A. (Optional): Configure the **ip dhcp snooping limit rate** *number* interface subcommand to set a limit of DHCP messages per second.

B. (Optional): Configure the **no ip dhcp snooping limit rate** *number* interface subcommand to remove an existing limit and reset the interface to use the default of no rate limit.

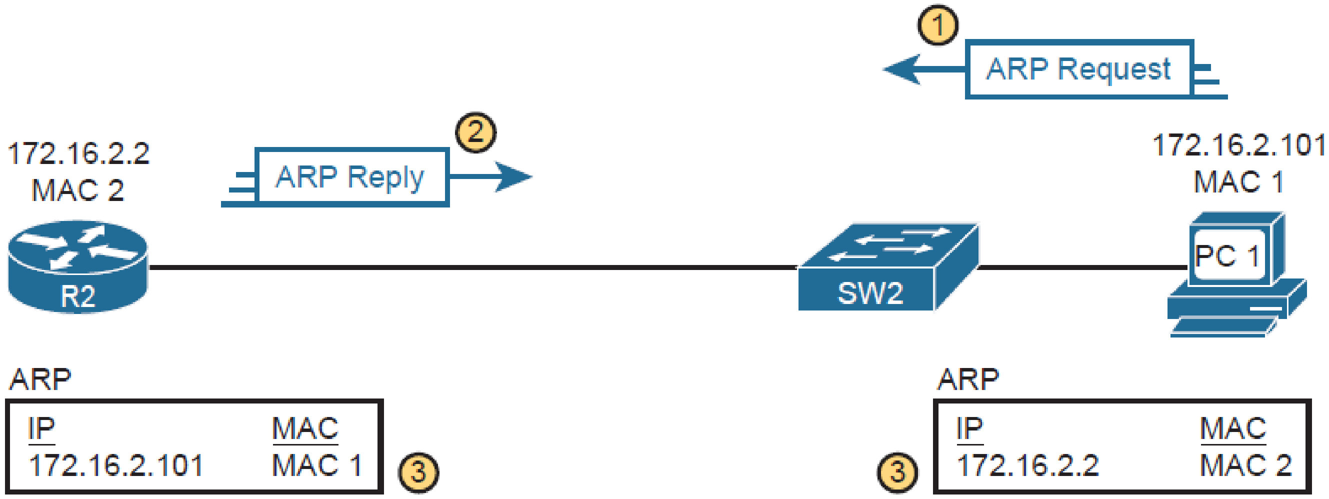
C. (Optional): Configure the **errdisable recovery cause dhcp-rate-limit** global command to enable the feature of automatic recovery from err-disabled mode, assuming the switch placed the port in err-disabled state because of exceeding DHCP Snooping rate limits.

D. (Optional): Configure the **errdisable recovery interval** *seconds* global commands to set the time to wait before recovering from an interface err-disabled state (regardless of the cause of the err-disabled state) .

DAI

The Dynamic ARP Inspection (DAI) feature on a switch examines incoming ARP messages on untrusted ports to filter those it believes to be part of an attack. DAI's core feature compares incoming ARP messages with two sources of data: **the DHCP Snooping binding table and any configured ARP ACLs.** If the incoming ARP message does not match the tables in the switch, the switch discards the ARP message.

Normal IP ARP.



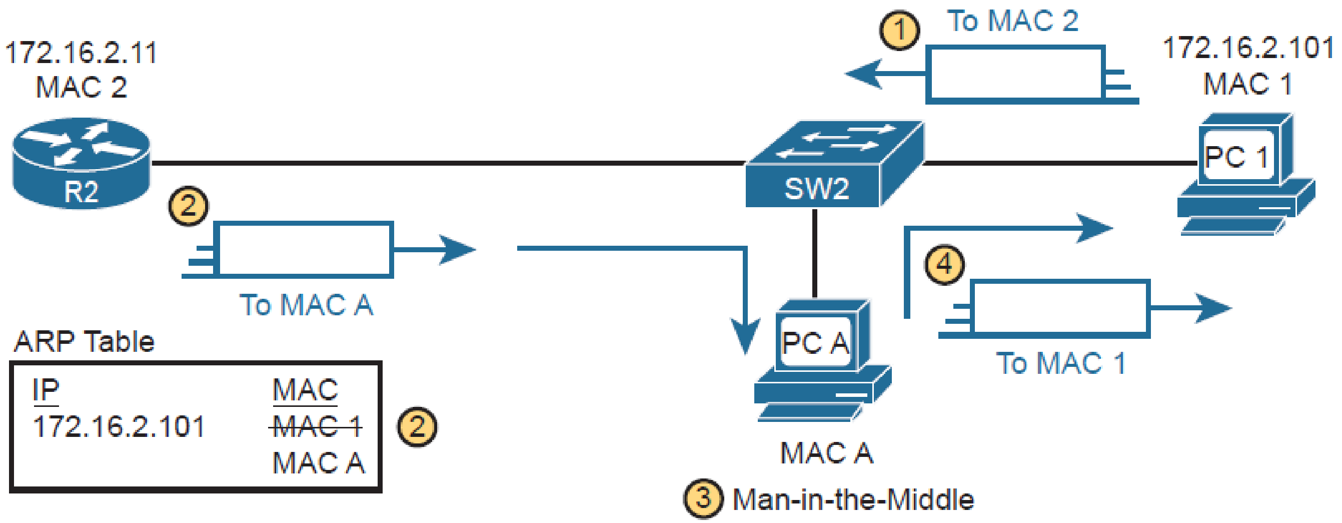
Gratuitous IP ARP

1. PC1 sends messages to some server on the left side of router R2.

2. The server replies to PC1’s IP address, but R2 forwards that packet to PC A’s MAC address, rather than to PC1.

3. PC A copies the packet for later processing.

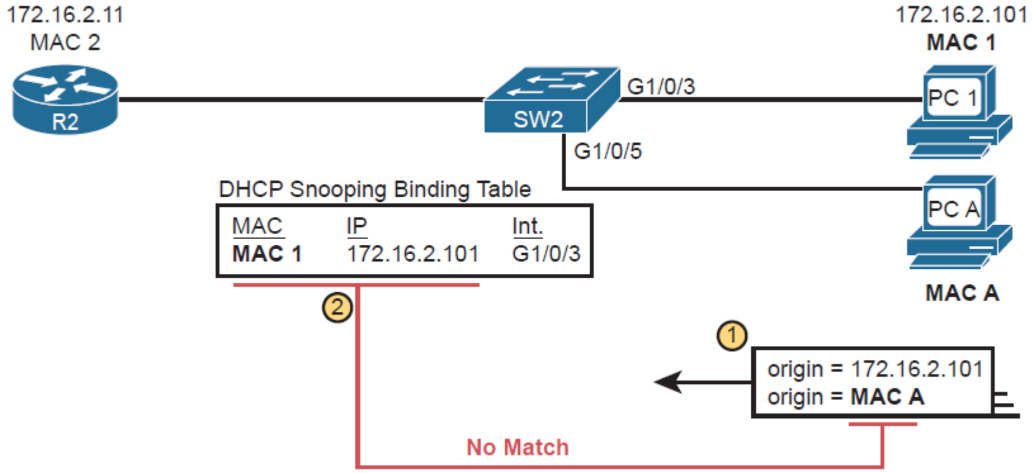
4. PC A forwards the packet inside a new frame to PC1 so that PC1 still works.



ARP Table

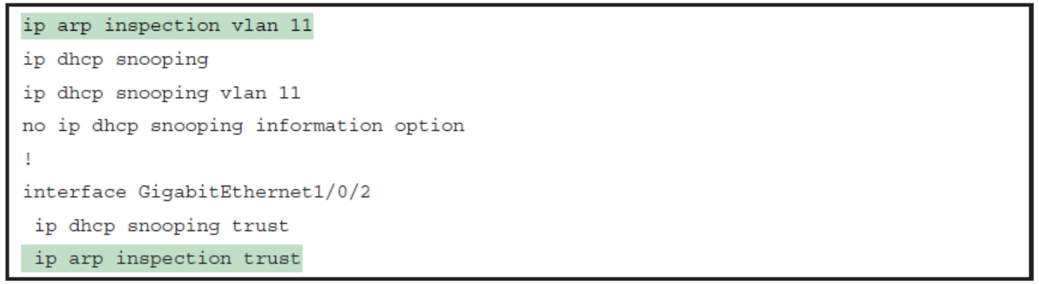
IP	MAC
172.16.2.101	~~MAC 1~~ MAC A

DAI Configuration



DHCP Snooping Binding Table

MAC	IP	Int.
MAC 1	172.16.2.101	G1/0/3



```
ip arp inspection vlan 11
ip dhcp snooping
ip dhcp snooping vlan 11
no ip dhcp snooping information option
!
interface GigabitEthernet1/0/2
 ip dhcp snooping trust
 ip arp inspection trust
```

IP ARP Inspection Configuration Summary

Step 1. Use the **ip arp inspection vlan** *vlan-list* global command to enable Dynamic ARP Inspection (DAI) on the switch for the specified VLANs.

Step 2. Separate from the DAI configuration, also configure DHCP Snooping and/or ARP ACLs for use by DAI.

Step 3. Configure the **ip arp inspection trust** interface subcommand to override the default setting of not trusted.

Step 4. (Optional): Configure DAI rate limits and err-disabled recovery:

Step A. (Optional): Configure the **ip arp inspection limit rate** *number* [**burst interval** *seconds*] interface subcommand to set a limit of ARP messages per second, or ARP messages for each configured interval.

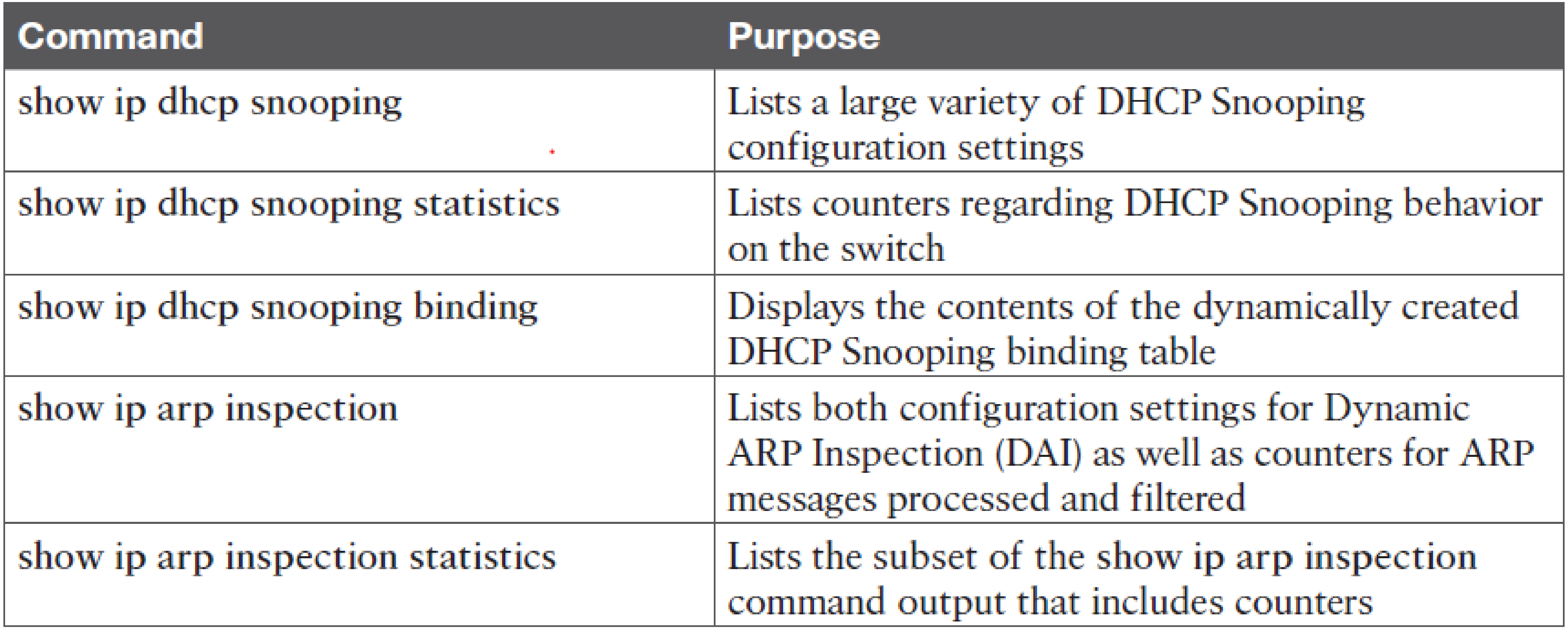
Step B. (Optional): Configure the **ip arp inspection limit rate none** interface subcommand to disable rate limits.

Step C. (Optional): Configure the **errdisable recovery cause arp-inspection** global command to enable the feature of automatic recovery from err-disabled mode, assuming the switch placed the port in err-disabled state because of exceeding DAI rate limits.

Step D. (Optional): Configure the **errdisable recovery interval** *seconds* global commands to set the time to wait before recovering from an interface err-disabled state (regardless of the cause of the err-disabled state).

Step 5. (Optional): Configure the **ip arp inspection validate** {[**dst-mac**] [**src-mac**] [**ip**]} global command to add DAI validation steps .

DHCP Snooping and DAI verification commands



Command	Purpose
show ip dhcp snooping	Lists a large variety of DHCP Snooping configuration settings
show ip dhcp snooping statistics	Lists counters regarding DHCP Snooping behavior on the switch
show ip dhcp snooping binding	Displays the contents of the dynamically created DHCP Snooping binding table
show ip arp inspection	Lists both configuration settings for Dynamic ARP Inspection (DAI) as well as counters for ARP messages processed and filtered
show ip arp inspection statistics	Lists the subset of the show ip arp inspection command output that includes counters

That is all for Lesson 26

The key is :

Learn

Repeat

Practice

You will be able to reach your goals.

GOOD LUCK !!!!!...