

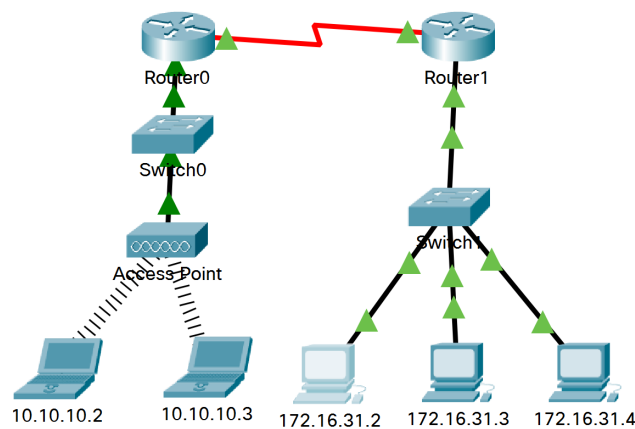
Lab 3: ARP, DHCP and DNS Protocols

Agenda

- Part1 Examine ARP
- Part2 Configure DHCP server at Router
- Part3 Examine DNS

Part 1: Examine ARP

Open the file **Examine_ARP_Table.pka**.



Addressing Table

Device	Interface	MAC Address	Switch Interface
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	N/A	N/A
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	N/A	N/A
10.10.10.2	Wireless	0060.2F84.4AB6	F0/2
10.10.10.3	Wireless	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Step 1: Generate ARP requests by pinging 172.16.31.3 from 172.16.31.2.

- Enter **Simulation** mode and set to filter only ICMP and ARP protocols.

ARP table of Router 1

ARP Table for Router1			
IP Address	Hardware Address	Interface	
172.16.31.1	00E0.F7B1.8901	GigabitEthernet0/0	

- d. Click **Capture/Forward** once. The ARP PDU moves to **Switch1** while the ICMP PDU disappears, waiting for the ARP reply. Open the PDU and record the destination MAC address.

1.2 What is the destination MAC address? Is this address listed in the table above?

Layer 2: Ethernet II Header 000C.85CC.
1DA7 >> FFFF.FFFF.FFFF ARP Packet Src.
IP: 172.16.31.2, Dest. IP: 172.16.31.3

DEST ADDR: FFFF.FFFF.FFFF

- e. Click **Capture/Forward** once to move the PDU to the next device.

1.3 How many copies of the PDU did Switch1 make?

3 copies

1.4 What is the IP address of the device that accepted the PDU?

172.16.31.3

- f. Open the PDU at the destination device and examine Layer 2.

1.5 What happened to the source and destination MAC addresses?

DEST ADDR: 000C.85CC.1D SRC ADDR: 0060
A7 | .7036.2849

- g. Click **Capture/Forward** until the PDU returns to **172.16.31.2**.

1.6 How many copies of the PDU did the switch make during the ARP reply?**1 copy****Step 2: Examine the ARP table.**

- a. Note that the ICMP packet reappears. Open the PDU and examine the MAC addresses.

2.1 What are the source and destination MAC addresses? Do the MAC addresses of the source and destination align with their IP addresses?

Layer 2: Ethernet II Header 000C.85CC.
1DA7 >> 0060.7036.2849

172.16.31.3 to 172.16.31.3**2.2 Fill in ARP table of 172.16.31.2, 172.16.31.3 and Router 1****ARP table of 172.16.31.2**

ARP Table for 172.16.31.2

IP Address	Hardware Address	Interface
172.16.31.3	0060.7036.2849	FastEthernet0

ARP table of 172.16.31.3

ARP Table for 172.16.31.3

IP Address	Hardware Address	Interface
172.16.31.2	000C.85CC.1DA7	FastEthernet0

ARP table of Router 1

ARP Table for Router1

IP Address	Hardware Address	Interface
172.16.31.1	00E0.F7B1.8901	GigabitEthernet0/0

Step 3: Examine the ARP Process in Remote Communications. Generate traffic to produce ARP traffic.

- a. Enter **Simulation** mode and set to filter only ICMP and ARP protocols.
- b. Use Inspect tool to open the ARP table at **172.16.31.2, Router 1** and **Router 0**.
- c. Use PDU to **ping 10.10.10.2 from 172.16.31.2**.

3.1 Fill in ARP table of Router 0.**ARP table of Router 0**

ARP Table for Router0			
IP Address	Hardware Address	Interface	
10.10.10.1	0001.6458.2501	GigabitEthernet0/0	

3.2 How many PDUs appear? What protocol(s) do(es) the PDU(s) belong?**2, ICMP and ARP**

- f. Click **Capture/Forward** until the packet arrives Router 0.

3.3 What happens with the packets at the Router 0?**One of the packet drop at Router 0.**

- g. Click **Capture/Forward** further until the end.

3.4 Can we ping 10.10.10.2 from 172.16.31.2. successfully? Why?**Failed, they not know each other.****3.5 Fill in ARP table of 172.16.31.2, Router 1 and Router 0.****ARP table of 172.16.31.2**

ARP Table for 172.16.31.2

IP Address	Hardware Address	Interface
172.16.31.1	00E0.F7B1.8901	FastEthernet0
172.16.31.3	0060.7036.2849	FastEthernet0

ARP table of Router 1

ARP Table for Router1

IP Address	Hardware Address	Interface
172.16.31.1	00E0.F7B1.8901	GigabitEthernet0/0
172.16.31.2	000C.85CC.1DA7	GigabitEthernet0/0

ARP table of Router 0

ARP Table for Router0

IP Address	Hardware Address	Interface
10.10.10.1	0001.6458.2501	GigabitEthernet0/0
10.10.10.2	0060.2F84.4AB6	GigabitEthernet0/0

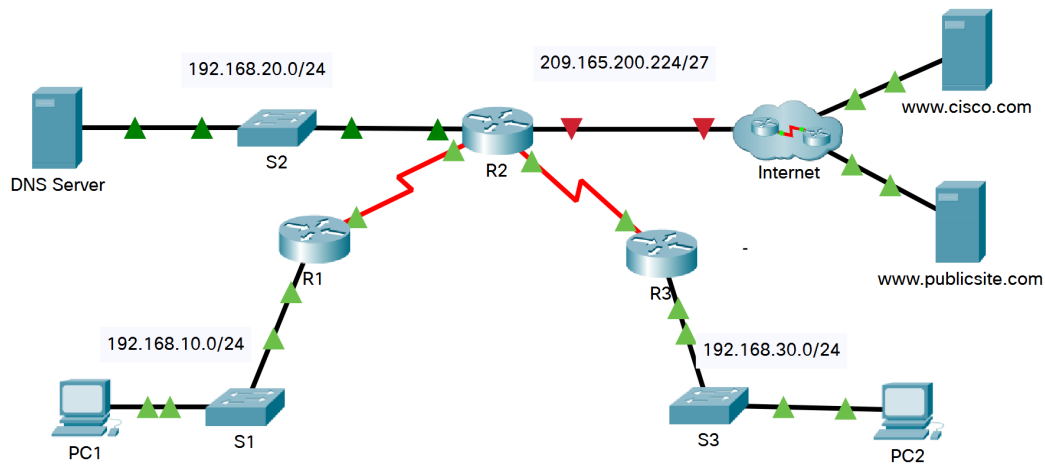
h. ping from the 172.16.31.2 to 10.10.10.2 again in simulation mode.

3.6 Can we ping 10.10.10.2 from 172.16.31.2. successfully? Why?

Success, they 172.16.31.2 and 10.10.10.2 already know another MAC address

Part 2: Configure DHCP server at Router

Open the file Implement_DHCPv4_DNS.pka.



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	DHCP Assigned	DHCP Assigned	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.0	N/A
PC1	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
PC2	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
DNS Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Configure a Router as a DHCP Server

Step 1: Configure the excluded IPv4 addresses.

Addresses that have been statically assigned to devices in the networks that will use DHCP must be excluded from the DHCP pools. This avoids errors associated with duplicate IP addresses. In this case the IP addresses of the R1 and R3 LAN interfaces must be excluded

from DHCP. In addition, nine other addresses are excluded for static assignment to other devices such servers and device management interfaces.

- a. Configure **R2** to exclude the first 10 addresses from the R1 LAN and to exclude the first 10 addresses from R3 LAN.

```
R2(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.10
```

Step 2: Create a DHCP pool on R2 for the R1 LAN.

- a. Create a DHCP pool named **R1-LAN** (case-sensitive).

```
R2(config)# ip dhcp pool R1-LAN
```

- b. Configure the DHCP pool to include the network address, the default gateway, and the IP address of the DNS server.

```
R2(dhcp-config)# network 192.168.10.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.10.1
R2(dhcp-config)# dns-server 192.168.20.254
```

Step 3: Create a DHCP pool on R2 for the R3 LAN.

- a. Create a DHCP pool named **R3-LAN** (case-sensitive).

```
R2(config)# ip dhcp pool R3-LAN
```

- b. Configure the DHCP pool to include the network address, the default gateway, and the IP address of the DNS server.

```
R2(dhcp-config)# network 192.168.30.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.30.1
R2(dhcp-config)# dns-server 192.168.20.254
```

Configure DHCP Relay

Step 4: Configure R1 and R3 as a DHCP relay agent.

For DHCP clients to obtain an address from a server on a different LAN segment, the interface that the clients are attached to must include a **helper address** pointing to the DHCP server. In this case, the hosts on the LANs that are attached to R1 and R3 will access the DHCP server that is configured on R2. The IP addresses of the R2 serial interfaces that are attached to R1 and R3 are used as the helper addresses. DHCP traffic from the hosts on the R1 and R3 LANs will be forwarded to these addresses and processed by the DHCP server that is configured on R2.

- a. Configure the helper address for the LAN interface on R1.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 10.1.1.2
```

- c. Configure the helper address for the LAN interface on R3.

```
R3(config)# interface g0/0
R3(config-if)# ip helper-address 10.2.2.2
```


Step 5: Configure hosts to receive IP addressing information from DHCP.

a. Configure hosts PC1 and PC2 to receive their IP addresses from a DHCP server.

- Click the PC1 -> IP Configuration -> click DHCP
- Click the PC2 -> IP Configuration -> click DHCP

5.1 Write down the IP addresses that the PC1 and PC2 get. Are these IP addresses from the correct DHCP pools?

The image shows two screenshots of a network configuration interface for two PCs, PC1 and PC2. Both windows have tabs for Physical, Config, Desktop, and Programming. The 'Desktop' tab is selected, and the 'IP Configuration' section is highlighted in blue. Under 'Interface', 'FastEthernet0' is selected. In the 'IP Configuration' section, the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the following values:

Field	PC1 Value	PC2 Value
IPv4 Address	192.168.10.11	192.168.30.11
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.30.1
DNS Server	192.168.20.254	192.168.20.254

b. Observe the DHCP packets. Choose simulation mode then filter to see only DHCP.

- Click PC1 -> IP Configuration -> click Static -> click DHCP

5.2 Fill in the following information from the packet at PC1.

Type of DHCP message: Discover CLIENT ADDRESS: 0.0.0.0
"YOUR" CLIENT ADDRESS: 0.0.0.0 SERVER ADDRESS: 0.0.0.0
Source IP Address: 0.0.0.0 Destination IP Address: 255.255.255.255
Source Port: 68 Destination Port: 67

5.3 What is the transport layer protocol that DHCP message use?

UDP

c. Click **Capture/Forward** two times (until the packet arrives **R1**). Observe the DHCP packet.

5.4 What are the source and destination IP addresses of the inbound and outbound PDUs?

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0	4	8	16	20	24	Bits
VER:4	IHL:5	DSCP:0x00	TL:62			
ID:0x0003			FLA GS:0	FRAG OFFSET:0x000		
TTL:128		PRO:0x11	CHKSUM			
SRC IP:192.168.10.1						
DST IP:10.1.1.2						

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

0		4		8		Bytes	
PREAMBLE: 101010..10				DEST ADDR:FFFF.FFFF.FF FF			
SRC ADDR:000 2.4AA5.1470		TYP E:0x		DATA (VARIABLE LENGTH)		FCS:0x00000000	

IP

0		4		8		16		20		24		Bits	
VER:4		IHL:5		DSCP:0x00		TL:62							
ID:0x0003						FLA GS:0		FRAG OFFSET:0x000					
TTL:128				PRO:0x11				CHKSUM					
SRC IP:0.0.0.0													
DST IP:255.255.255.255													

- d. Click **Capture/Forward** further until the DHCP packet is sent back to PC1. Observe the DHCP packet.

5.5 At inbound PDU, fill in the following information.

Type of DHCP message: Offer CLIENT ADDRESS: 0.0.0.0
 "YOUR" CLIENT ADDRESS: 192.168.10.11 SERVER ADDRESS: 10.1.1.2
 Source IP Address: 192.168.10.1 Destination IP Address: 255.255.255.255
 Source Port: 67 Destination Port: 68

5.6 What is the IP address that the DHCP server offers to the PC1?

192.168.10.11

5.7 At outbound PDU, fill in the following information.

Type of DHCP message: Request CLIENT ADDRESS: 0.0.0.0
 "YOUR" CLIENT ADDRESS: 192.168.10.11 SERVER ADDRESS: 10.1.1.2
 Source IP Address: 0.0.0.0 Destination IP Address: 255.255.255.255
 Source Port: 68_ Destination Port: 67

- e. Click **Capture/Forward** further until the end.

5.8 Fill in the following information.

Type of DHCP message: Request	CLIENT ADDRESS: 0.0.0.0
"YOUR" CLIENT ADDRESS: 192.168.10.11	SERVER ADDRESS: 10.1.1.2
Source IP Address: 192.168.10.1	Destination IP Address: 255.255.255.255
Source Port: 67	Destination Port: 68

Verify DHCP and Connectivity

Step 6: Verify DHCP bindings.

R2# show ip dhcp binding

IP address Client-ID/ Lease expiration Type

Hardware address

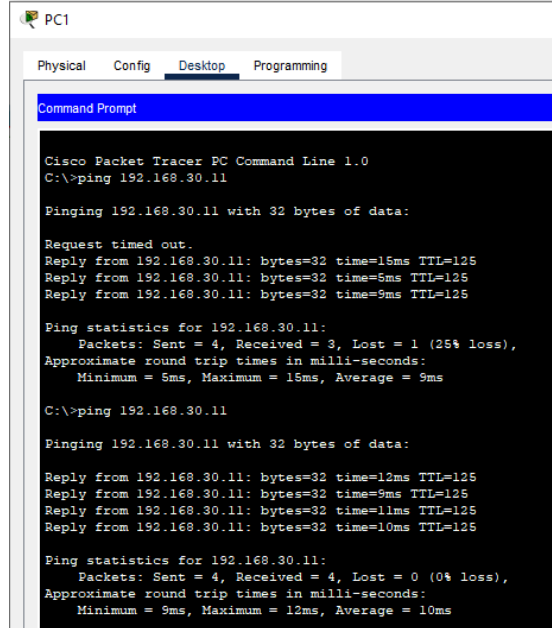
192.168.10.11 0002.4AA5.1470 -- Automatic

192.168.30.11 0004.9A97.2535 -- Automatic

Step 7: Verify configurations.

7.1 Can we ping from PC1 to PC2 successfully?

Successfully



```
PC1
Physical Config Desktop Programming
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.11: bytes=32 time=15ms TTL=125
Reply from 192.168.30.11: bytes=32 time=5ms TTL=125
Reply from 192.168.30.11: bytes=32 time=9ms TTL=125

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 15ms, Average = 9ms

C:\>ping 192.168.30.11

Pinging 192.168.30.11 with 32 bytes of data:

Reply from 192.168.30.11: bytes=32 time=12ms TTL=125
Reply from 192.168.30.11: bytes=32 time=9ms TTL=125
Reply from 192.168.30.11: bytes=32 time=11ms TTL=125
Reply from 192.168.30.11: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.30.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 12ms, Average = 10ms
```

Part 3: Examine DNS

Step 1: Configure the Gigabit Ethernet 0/1 interface on R2 to receive IP addressing from DHCP and activate the interface.

```
R2(config)# interface g0/1
R2(config-if)# ip address dhcp
R2(config-if)# no shutdown
```

1.1 What is the IP address that interface g0/1 of the R2 obtain?

209.165.200.254/27

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	192.168.20.1/24	<not set>	00D0.BCDA.3901
GigabitEthernet0/1	Up	--	209.165.200.254/27	<not set>	00D0.BCDA.3902

Step 2: Try to access www.cisco.com.

- a. Click PC1 -> click Web Browser -> type www.cisco.com

2.1 Can we access the www.cisco.com? Why?

No, we haven't configure DNS yet

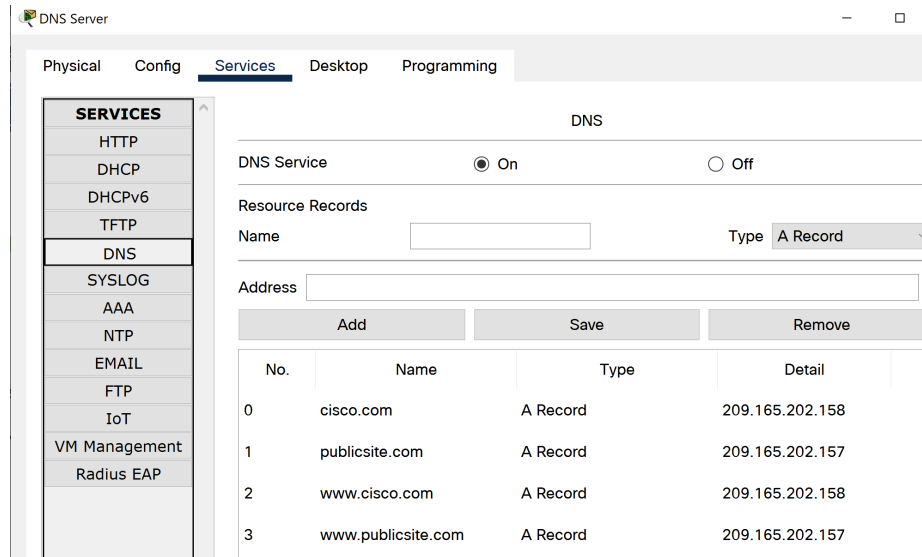
- b. Try using 209.165.202.158 at the Web Browser.

2.2 Can we access the website now? Why?

Yes, we know the IP and website is running

Step 3: Configure DNS service.

- a. Click on DNS Server → Services → DNS



- b. DNS or Domain Name System service provides a translation from **domain names** → **IP address**
- Turn on DNS service by clicking on **On** button
 - Name: cisco.com
 - Type: A Record
 - Address: 209.165.202.158
 - Click **Add**. This creates a mapping from cisco.com to 209.165.202.158
- c. Do the same to add following:
- Name: www.cisco.com, Type: A Record, Address: 209.165.202.158
 - Name: www.publicsite.com, Type: A Record, Address: 209.165.202.157
 - Name: publicsite.com, Type: A Record, Address: 209.165.202.157

Step 4: Examine DNS message.

- In simulation mode, filter to see only the DNS and HTTP.
- Click PC1 -> click Web Browser -> type www.cisco.com
- observe the DNS message at the PC1.

4.1 Fill in the following information of DNS query message at PC1.

Source IP Address: 192.168.10.11	Destination IP Address: 192.168.20.254
Source Port: 1027	Destination Port: 53
NAME: www.cisco.com	

4.2 What is the transport layer protocol that DNS use?

UDP

- d. Click **Capture/Forward** further until the DNS response arrives at PC1.

4.3 Fill in the following information of DNS message at PC1.

Source IP Address: 192.168.20.254	Destination IP Address: 192.168.10.11
Source Port: 53	Destination Port: 1028

4.4 What is the answer that the DNS response?

209.165.202.158

- e. Click **Capture/Forward** further once.

4.5 What is the type of message created?

HTTP request

Save your work as SecX-ID-Firstname-XXX.pka