Elk Technologies
https://elktech.org
Scott Stephenson

Module 9: Address Resolution

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Module Objectives

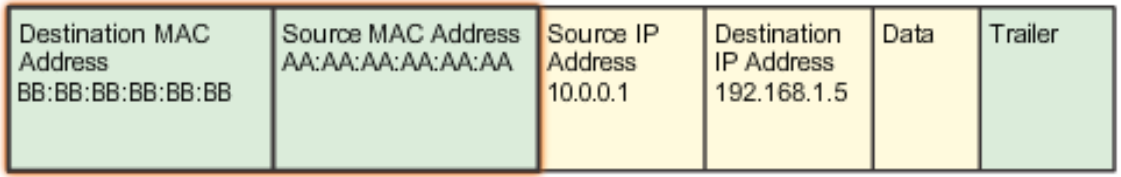
- Module Title: Address Resolution
- Module Objective: Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
9.1 MAC and IP	Compare the roles of the MAC address and the IP address.
9.2 ARP	Describe the purpose of ARP.
9.3 Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

9.1 MAC and IP

End-to-End Connectivity

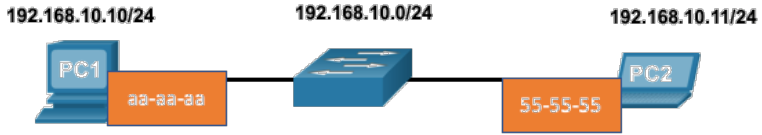
- The combination of MAC and IP facilitate the End-to-End communication
- Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another



- Destination and source IP addresses in a packet header remain constant along the entire path to a target host

Destination on Same Network

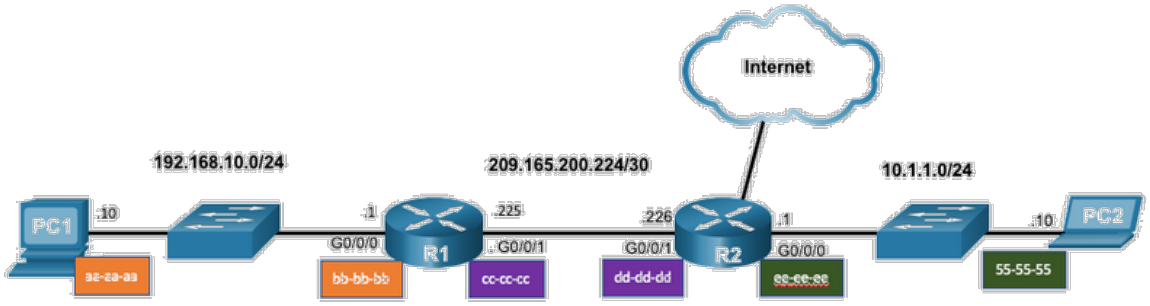
- There are two primary addresses assigned to a device on an Ethernet LAN:
  - **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
    - Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network.
  - **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.
    - If a destination IP address is on the same network, the destination MAC address will be that of the destination device.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Destination on Remote Network

- When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.
  - ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
  - ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.

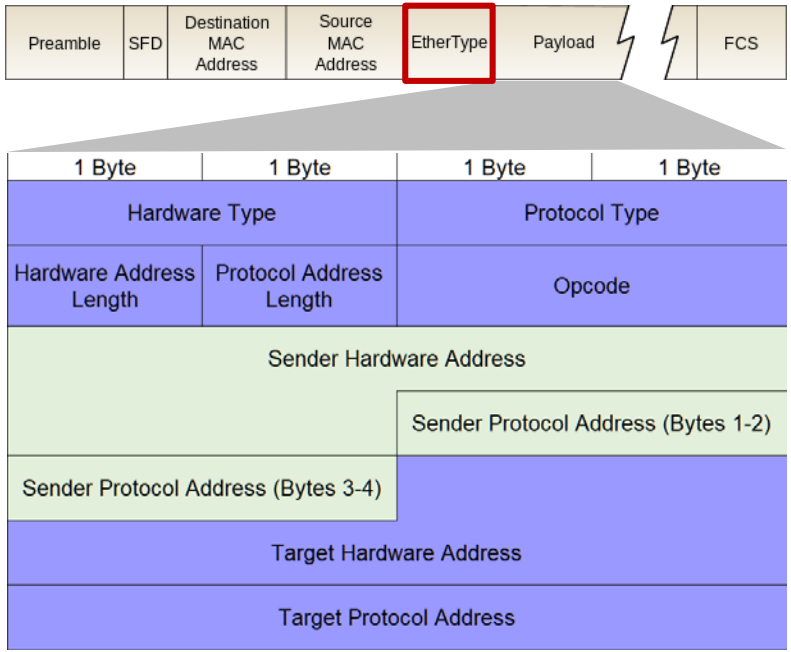


Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

9.2 ARP

EtherType Field

- An ARP message is 28 Bytes in length.
- An EtherType field of 0x0806 in the header of the Ethernet frame causes the NICs receiving an ARP request to pass the data portion of the Ethernet frame to the ARP process.
- Common EtherType Field values:
  - 0x0800 – IPv4
  - **0x0806 – ARP frame**
  - 0x8035 – Reverse ARP (RARP)
  - 0x8100 – 802.1Q (VLAN-tagged)
  - 0x86DD – IPv6
  - 0x9100 – VLAN double tagging



Ethernet: ARP Message Payload Format

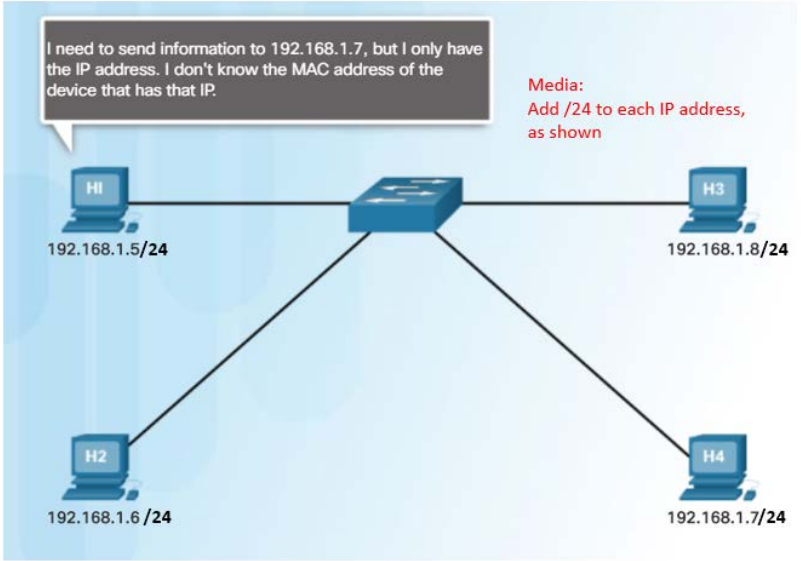
Function	Description
Hardware Type	This field specifies the type of hardware used for the local network transmitting the ARP message and the type of addressing (value: **6 – 802 networks**, 15 – Frame Relay, 17 – HDLC, 20 – Serial Line).
Protocol Type	This field is the complement of the *Hardware Type* field, specifying the type of layer three addresses used in the message. For IPv4 addresses, this value is **2048** (**0800 hex**), which corresponds to the EtherType code for the Internet Protocol. 34,525 (86DD hex) for IPv6.
Hardware Address Length	Specifies how long hardware addresses are in this message. For Ethernet or other networks using IEEE 802 MAC addresses, the value is **6** (bytes).
Protocol Address Length	The complement of the preceding field; specifies how long protocol (layer three) addresses are in this message. For IP(v4) addresses this value is of **4** (bytes).
Opcode	This field specifies the nature of the ARP message being sent (value: **1** – ARP Request, **2** – ARP Reply, 3 – RARP Request, 4 – RARP Reply).
Sender Hardware Address	MAC address of the source device.
Sender Protocol Address	The IP address of the source device.
Target Hardware Address	MAC address of the destination device.
Target Protocol Address	The IP address of the destination device.

ARP Functions/Operation

- **ARP Table**
  - Used to find the data link layer address that is mapped to the destination IPv4 address.
  - As a node receives frames from the media, the switch's ARP table records the source IP (Layer 3) and MAC (Layer 2) address as a mapping in the ARP table.
- **ARP Request**
  - Layer 2 broadcast (`FF-FF-FF-FF-FF-FF`) to all devices on the Ethernet LAN.
  - The node that matches the IP address in the broadcast will reply.
  - If no device responds to the ARP request, the packet is dropped because a frame cannot be created.
- Static map entries can be entered in an ARP table, but this is rarely done.

ARP Overview

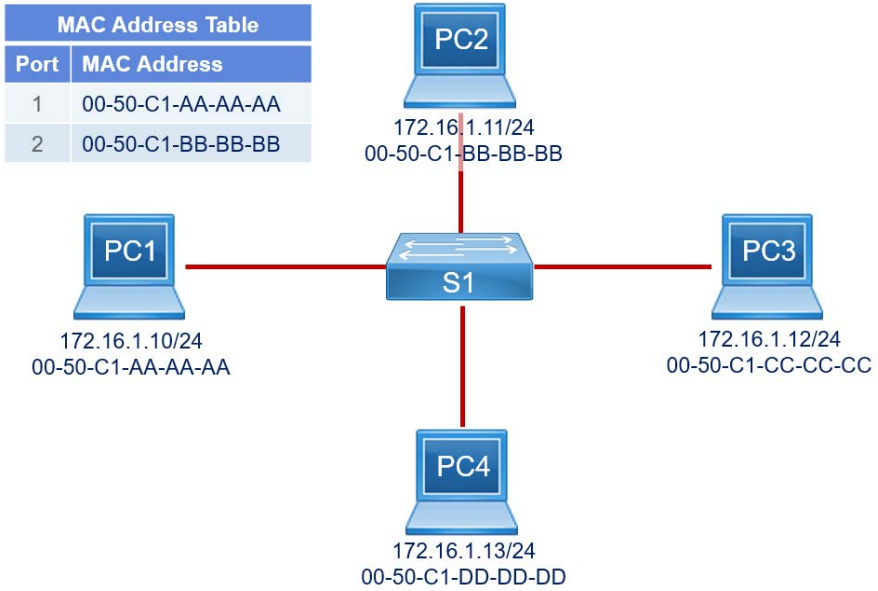
- ARP requests are received and processed by every device on the local network.
- A device uses ARP to determine the destination MAC address of a local network device when it knows its IPv4 address.
- The destination MAC address in frame headers are examined in order to forward frames.
- ARP provides two basic functions:
  - Resolving IPv4 addresses to MAC addresses.
  - Maintaining an ARP table of IPv4 to MAC address mappings.



ARP Functions

- To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.
  - If the packet's destination IPv4 address is on the same network, the device will search the ARP table for the destination IPv4 address.
  - If the destination IPv4 address is on a different network, the device will search the ARP table for the IPv4 address of the default gateway.
  - If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
  - If there is no ARP table entry is found, then the device sends an ARP request.
- ARP requests will send the destination MAC address as FFFF.FFFF.FFFF.

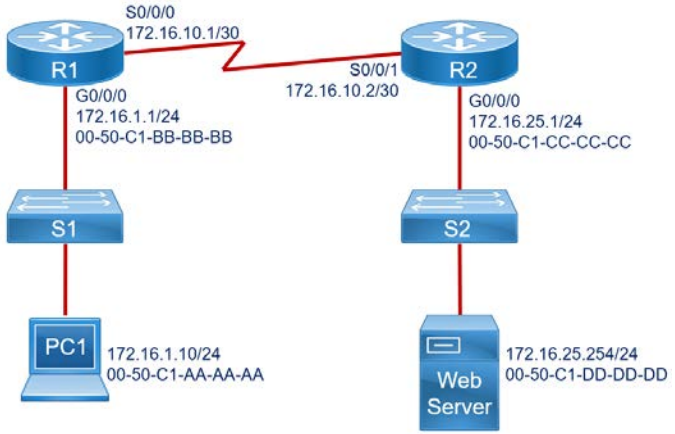
Local ARP Requests



- This switched network shows the contents of the MAC address table. PC1 has sent a frame addressed to PC3. What will the switch do with the frame?

The switch will forward the frame to all ports except port 1.

Remote ARP Requests



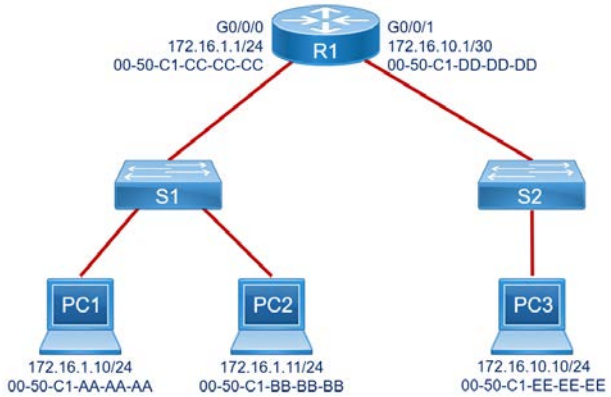
- PC1 attempts to connect to the Web Server and sends an ARP request to obtain a destination MAC address. Which MAC address will PC1 receive in the ARP reply?

  The MAC address of the G0/0/0 interface on R1 (Default Gateway)

ARP Operation

- PC1 issues an ARP request because it needs to send a packet to PC2. What will happen next?

  PC2 will send an ARP reply with its MAC address

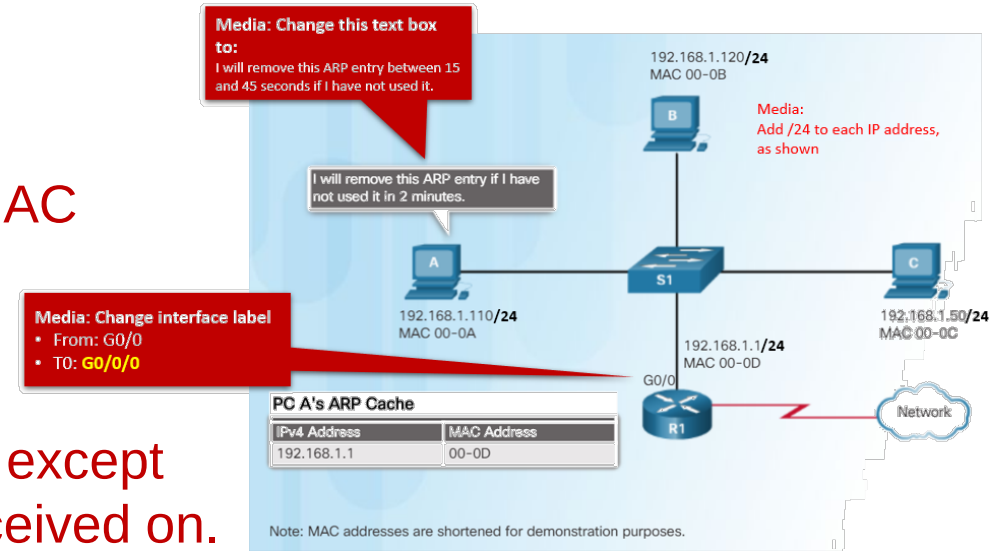


- PC1 needs to send an ARP to PC3. What will it do?

  It will send an ARP request for the MAC address of the default gateway

Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer expires after a specified period of time.
- The duration of the ARP cache timer differs depending on the operating system.
- ARP table entries can also be removed manually by the administrator.
- If a frame has the broadcast MAC address as the destination address or the destination address is unknown, a switch flood a frame out of every port except the port that the frame was received on.



ARP Tables on Networking Devices

- A **static** IP-to-MAC address entry can be entered manually into an ARP table.
- The **show ip arp** command displays the ARP table on a Cisco router.
- All host computers maintain layer 2 addresses in the ARP cache.
  - The **arp -a** command displays the ARP table on a Windows 10 PC.
  - The **arp -d** command clears the ARP table cache.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

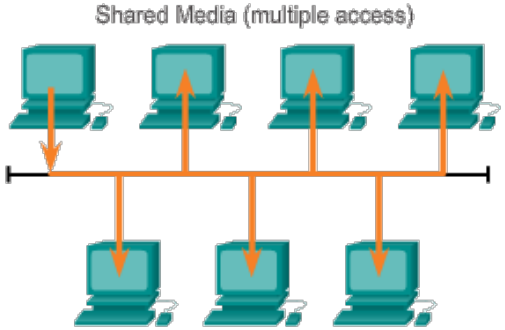
```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

ARP Broadcasting

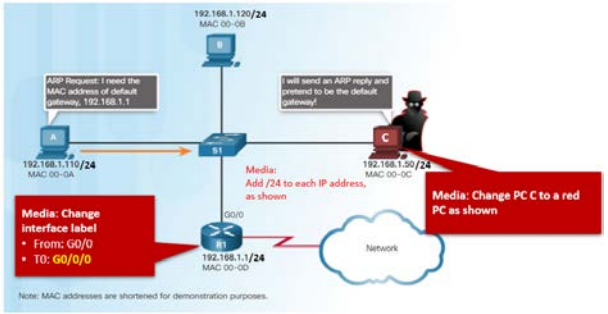
- On large networks with low bandwidth, multiple ARP broadcasts could cause data communication delays (overhead on the media).
- **ARP Broadcasts** – An ARP request is received and processed by every device on the local network.
  - ARP requests can flood the local segment if a large number of devices were to be powered up and all start accessing network services at the same time.
  - Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent of intercepting network traffic (security).

ARP broadcasts can flood the local media.



ARP Spoofing

- ARP requests are received and processed by every device on the local network.
- ARP replies can be spoofed by a threat actor to perform an ARP poisoning attack.
- **ARP Spoofing** – A technique that is used to send fake ARP messages to other hosts in the LAN to associate IP addresses with wrong MAC addresses.
  - Attackers can respond to requests and pretend to be providers of services.
  - One type of ARP spoofing attack used by attackers is to reply to an ARP request for the default gateway.
- In this example, host A requests the MAC address of the default gateway:
  - Host C replies to the ARP request.
  - Host A receives the reply and updates its ARP table.
  - It now sends packets destined to the default gateway to the attacker host C.
- Enterprise level switches include mitigation techniques known as **dynamic ARP inspection** (DAI).



Mac-Address-Table Configuration

- **mac-address-table aging-time seconds [10 – 1000000]** (default 300)
- **mac-address-table static *MAC* vlan # interface *ID***
- **clear mac-address-table**
- **show mac-address-table [static | dynamic | aging-time]**

ARP Tables on Networking Devices

- Router

```
Router#show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229    -    0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218    -    0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.168.11     -    0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254    9    0000.0c36.6965  ARPA   Ethernet0/0
```

- Switch

```
Router# show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000b.000c         Secure       1      FastEthernet0/1/8
000d.e105.cc70         Self         1      Vlan1
00aa.00bb.00cc         Static       1      FastEthernet0/1/0
```

- PC

```
C:\>arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254         64-0f-29-0d-36-91     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

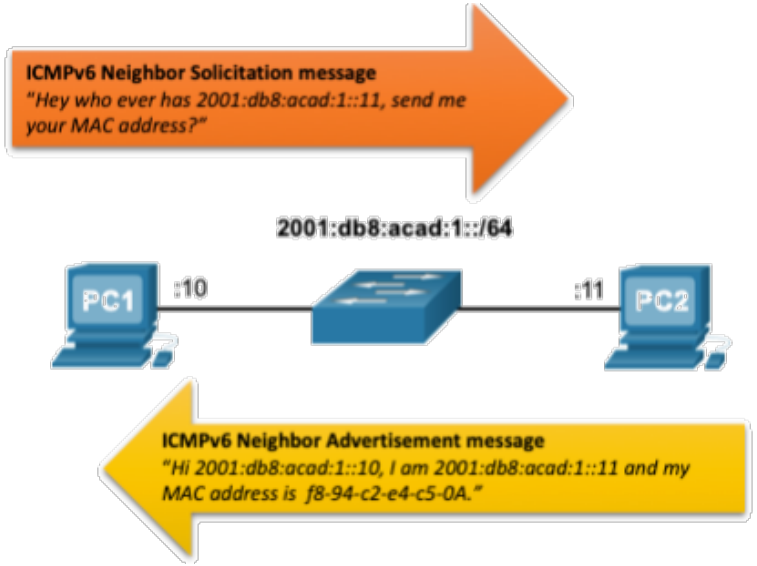
9.3 Neighbor Discovery

IPv6 Neighbor Discovery Messages

- IPv6 **Neighbor Discovery** (ND) protocol provides:
  - Address resolution
  - Router discovery
  - Redirection services
- ICMPv6 **Neighbor Solicitation** (NS) and **Neighbor Advertisement** (NA) messages are used for device-to-device messaging such as address resolution.
- ICMPv6 **Router Solicitation** (RS) and **Router Advertisement** (RA) messages are used for messaging between devices and routers for router discovery.
- ICMPv6 redirect messages are used by routers for better next-hop selection.

IPv6 Neighbor Discovery – Address Resolution

- IPv6 devices use ND to resolve the MAC address of a known IPv6 address.
- ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.



9.4 Module Practice and Quiz

What did I learn in this module?

- Layer 2 physical addresses (i.e., Ethernet MAC addresses) are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network.
- If the destination IP address is on the same network, the destination MAC address will be that of the destination device.
- When the destination IP address (IPv4 or IPv6) is on a remote network, the destination MAC address will be the address of the host default gateway (i.e., the router interface).
- An IPv4 device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

What did I learn in this module?

- ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.
- After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table.
- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.
- IPv6 does not use ARP, it uses the ND protocol to resolve MAC addresses.
- An IPv6 device uses ICMPv6 Neighbor Discovery to determine the destination MAC address of a local device when it knows its IPv6 address.

New Terms and Commands

- Address Resolution Protocol (ARP)
- ARP table
- show ip arp
- arpr -a
- ICMPv6 Neighbor Discovery protocol (ND)
- ICMPv6 Neighbor Solicitation (NS) message
- ICMPv6 Neighbor Advertisement (NA) message
- ICMPv6 Router Solicitation (RS) message
- ICMPv6 Router Advertisement (RA) message
- ICMPv6 Redirect Message


CISCO


Elk Technologies
https://elktech.org
Scott Stephenson