IPv6
Are we there yet?

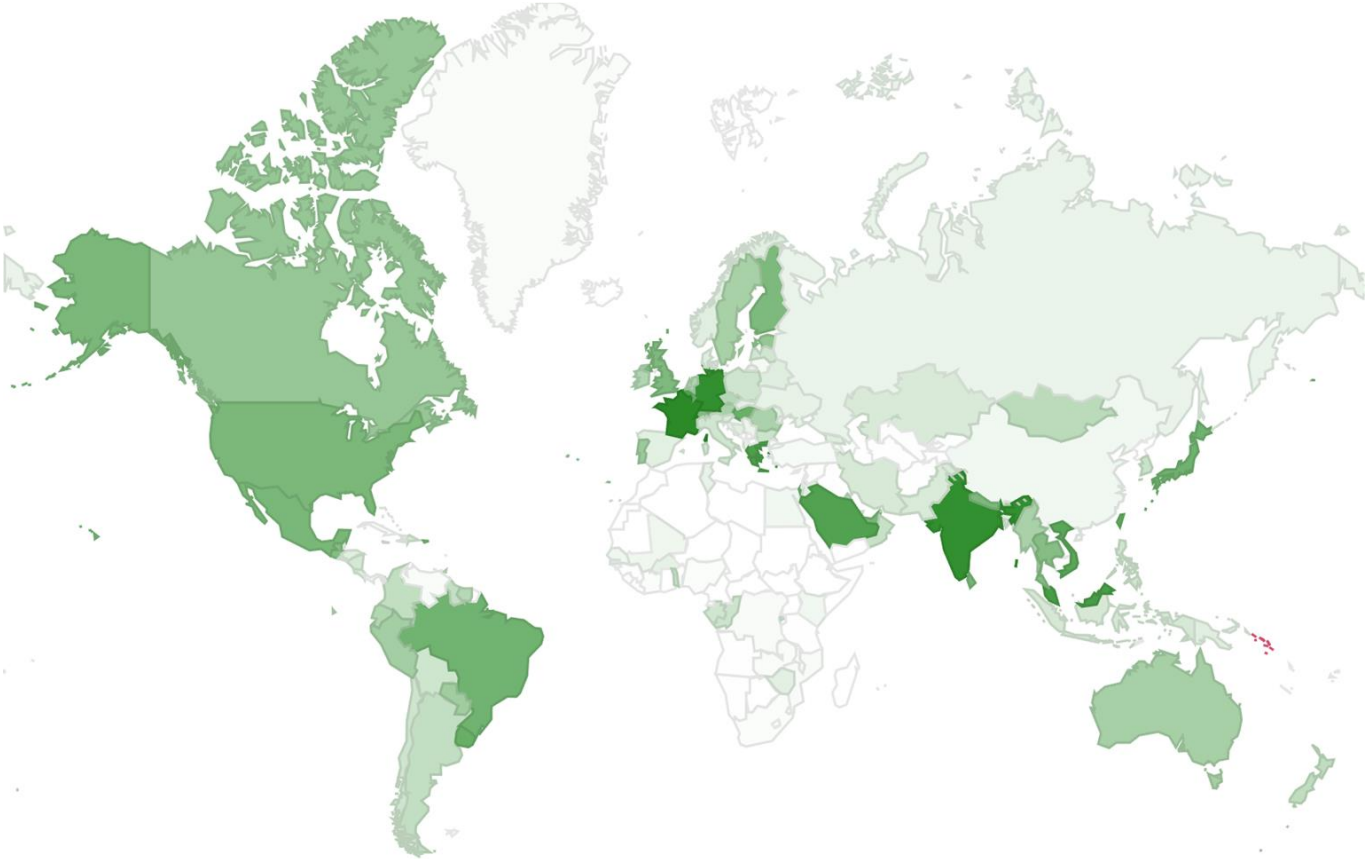
CERN iCSC
Vlad-Iulius Năstase

What is this lecture about?

- Introduction to IPv6
- (What I consider to be) interesting facts
- Rants about IPv6
- Personal opinions

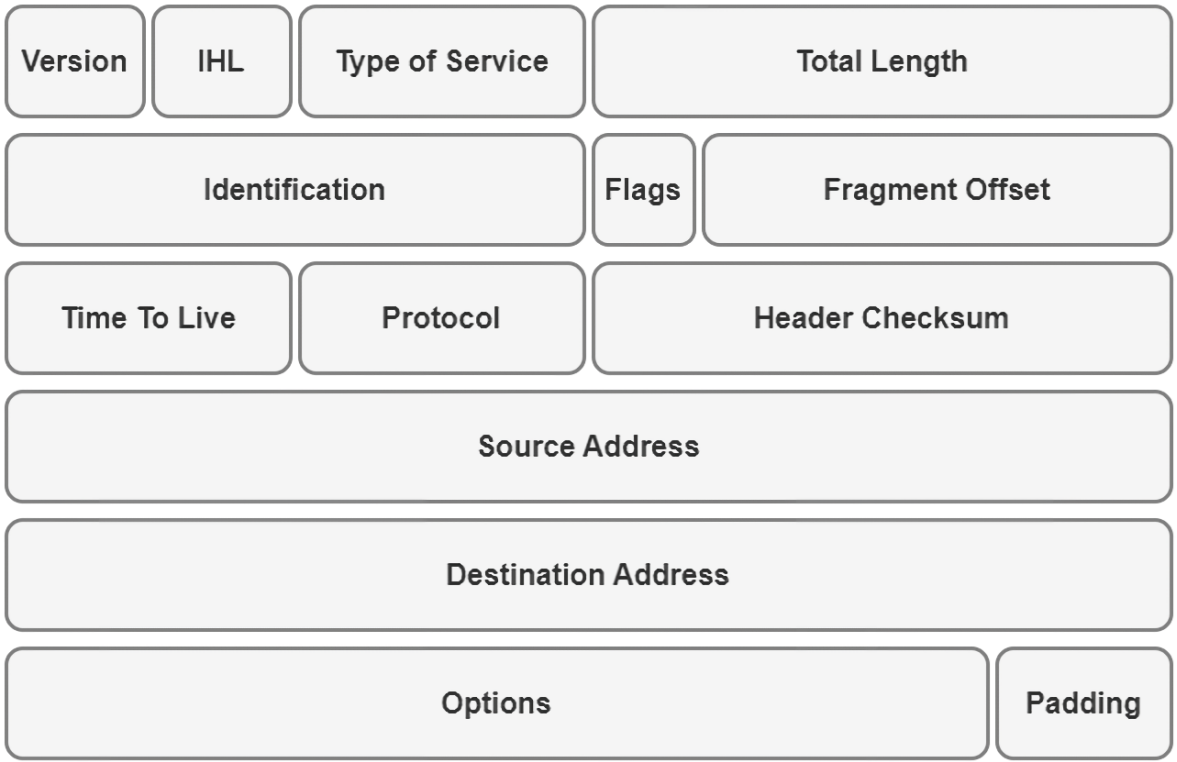

Are we there yet?

No.



Per country IPv6 adoption as of 2024/02/16; © Google;
https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

IPv4 refresher (IPv4 Header)



IPv4 refresher (IPv4 addresses)

10.42.0.1

IPv4 refresher (IPv4 addresses)

10.42.0.1

00001010.00101010.00000000.00000001

IPv4 refresher (IPv4 addresses)

10.42.0.1

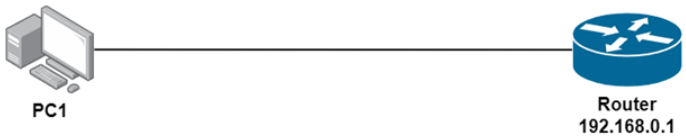
00001010.00101010.00000000.00000001

10.42.1

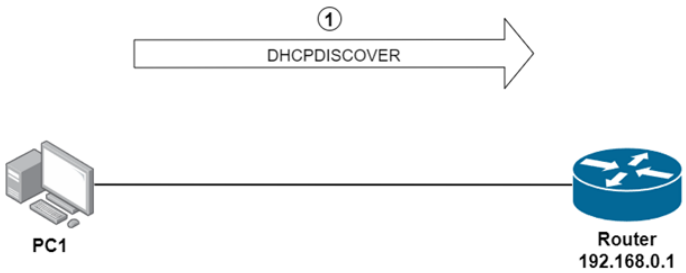
Supporting protocols for IPv4

- DHCP
- ARP
- ICMP
- DNS
- NAT (not a protocol)

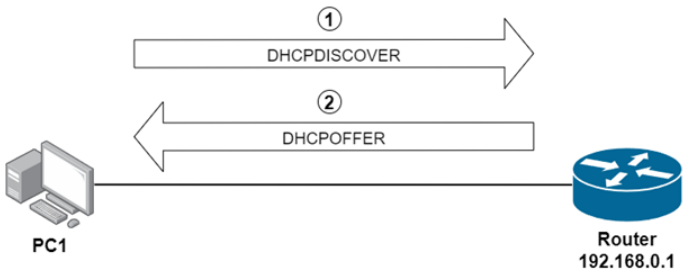
Supporting protocols for IPv4 (DHCP)



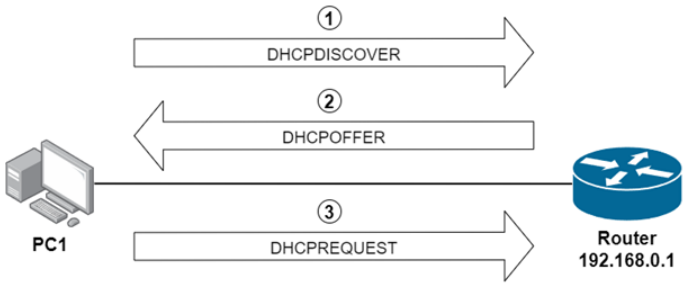
Supporting protocols for IPv4 (DHCP)



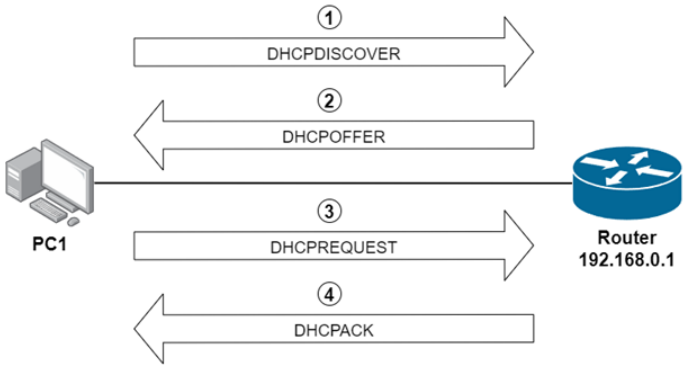
Supporting protocols for IPv4 (DHCP)



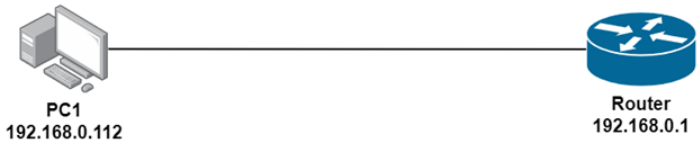
Supporting protocols for IPv4 (DHCP)



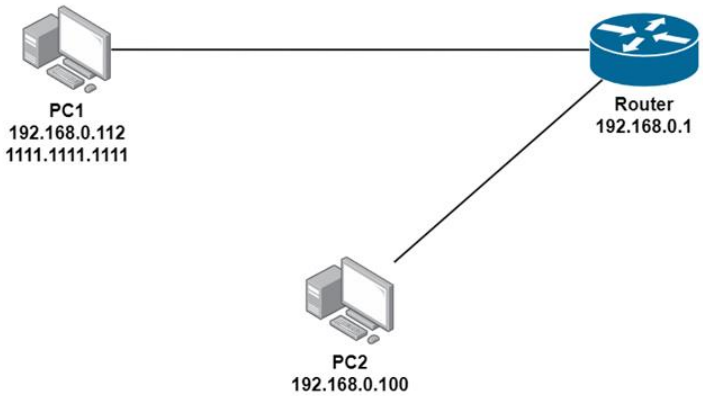
Supporting protocols for IPv4 (DHCP)



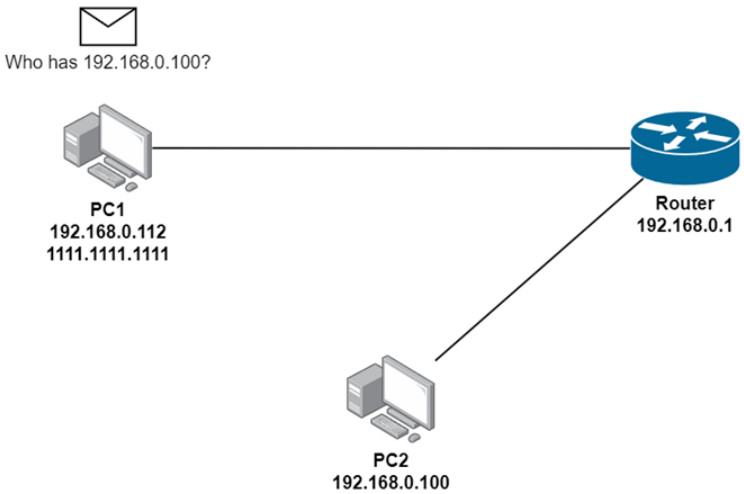
Supporting protocols for IPv4 (DHCP)



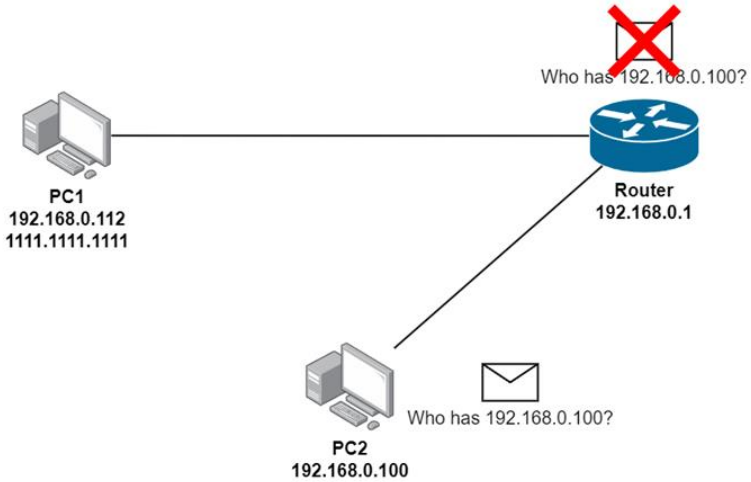
Supporting protocols for IPv4 (ARP)



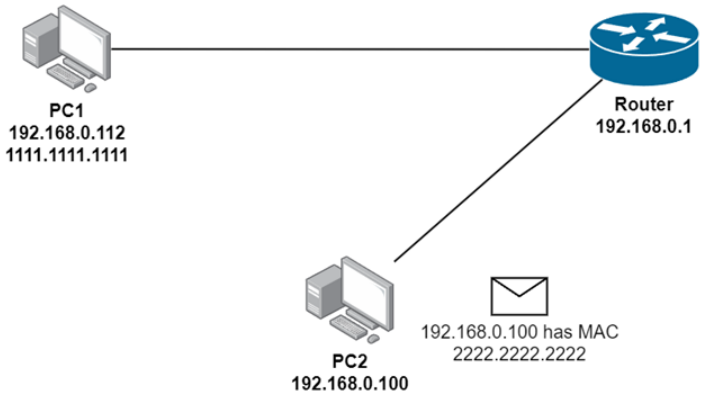
Supporting protocols for IPv4 (ARP)



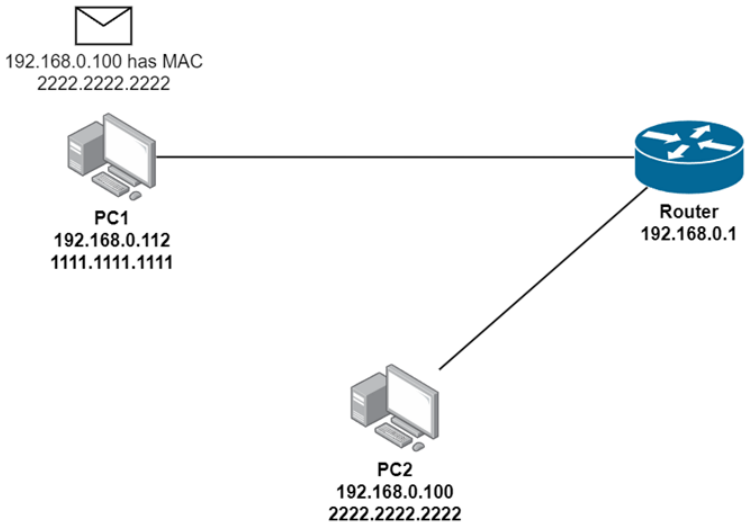
Supporting protocols for IPv4 (ARP)



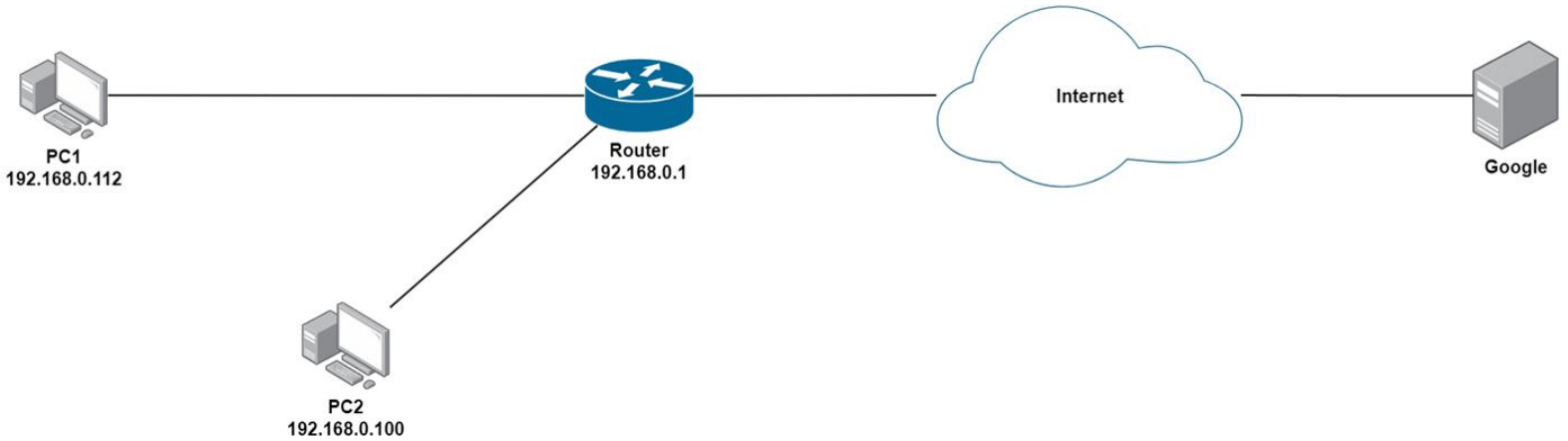
Supporting protocols for IPv4 (ARP)



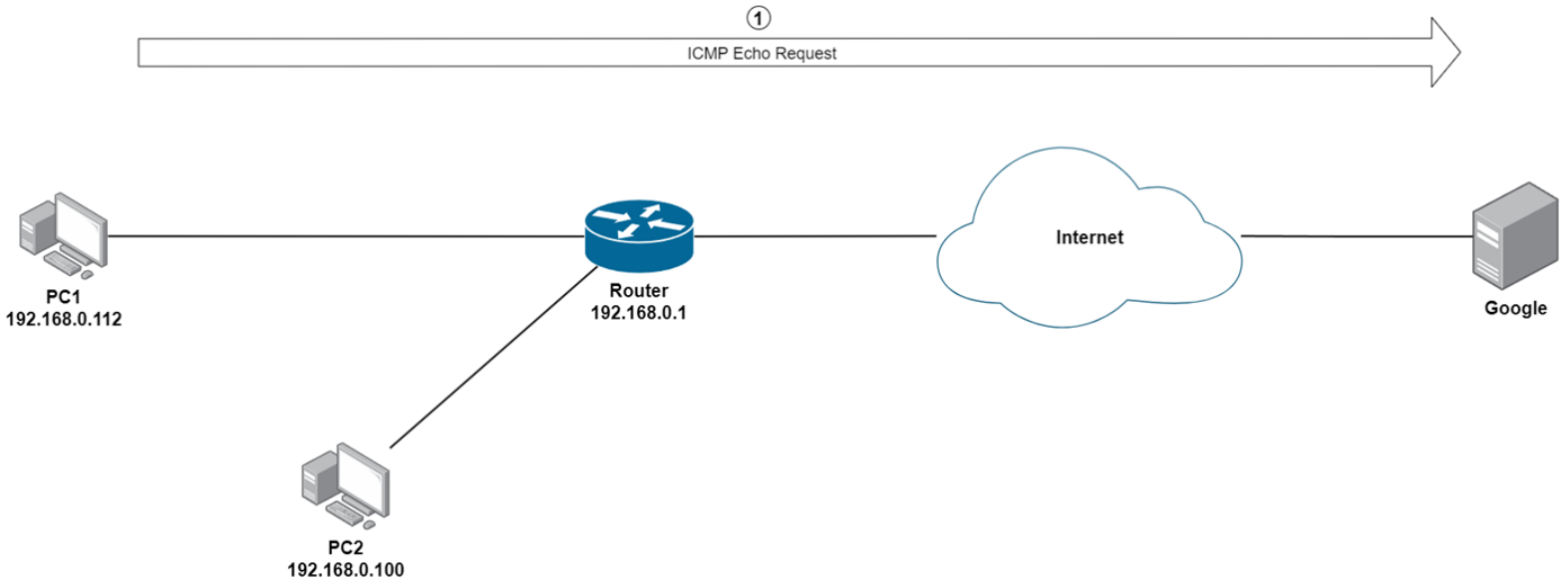
Supporting protocols for IPv4 (ARP)



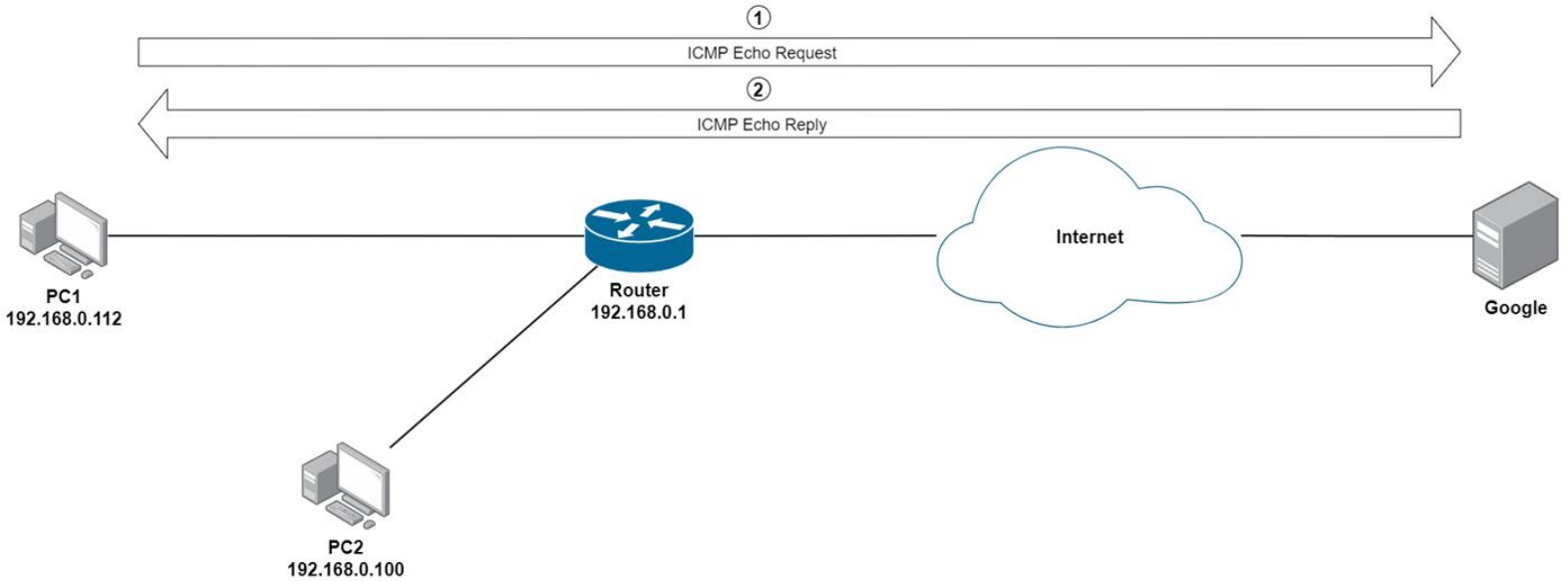
Supporting protocols for IPv4 (ICMP)



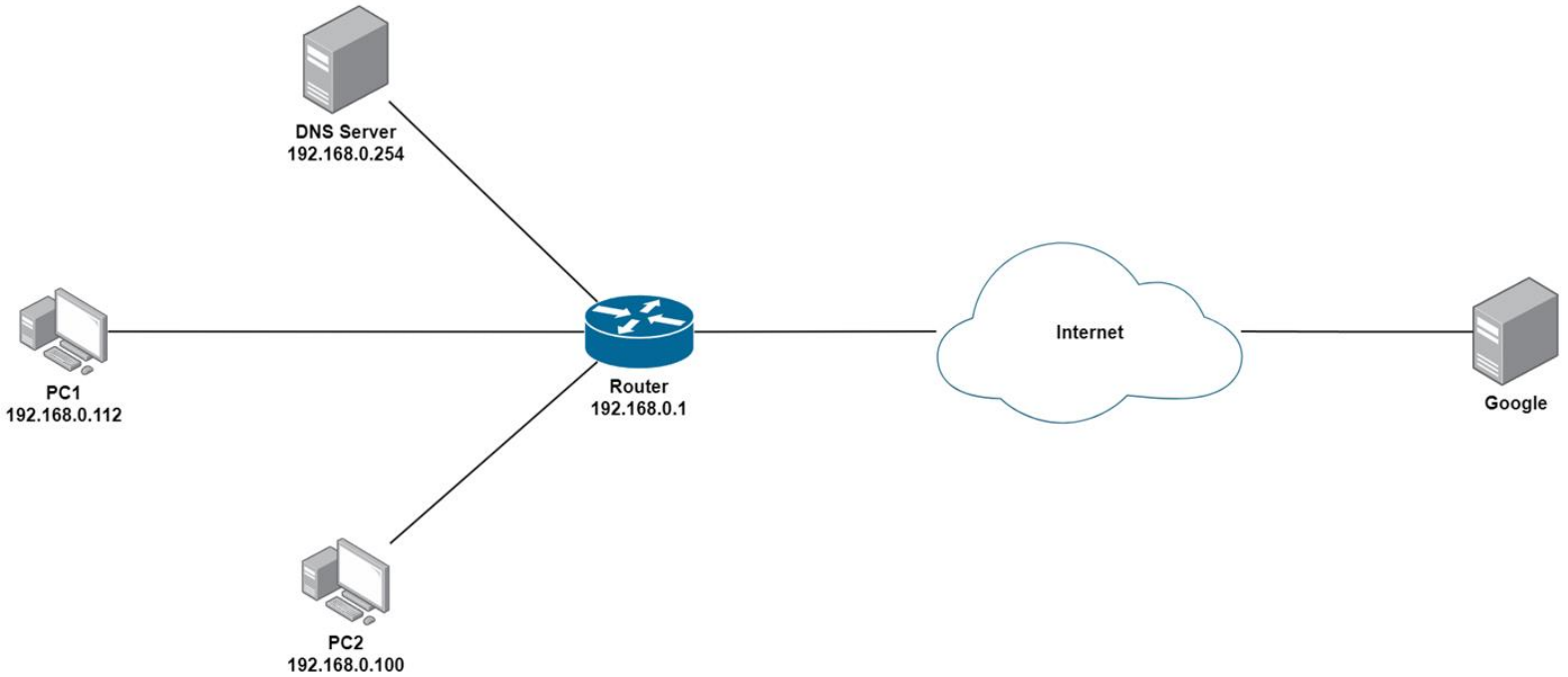
Supporting protocols for IPv4 (ICMP)



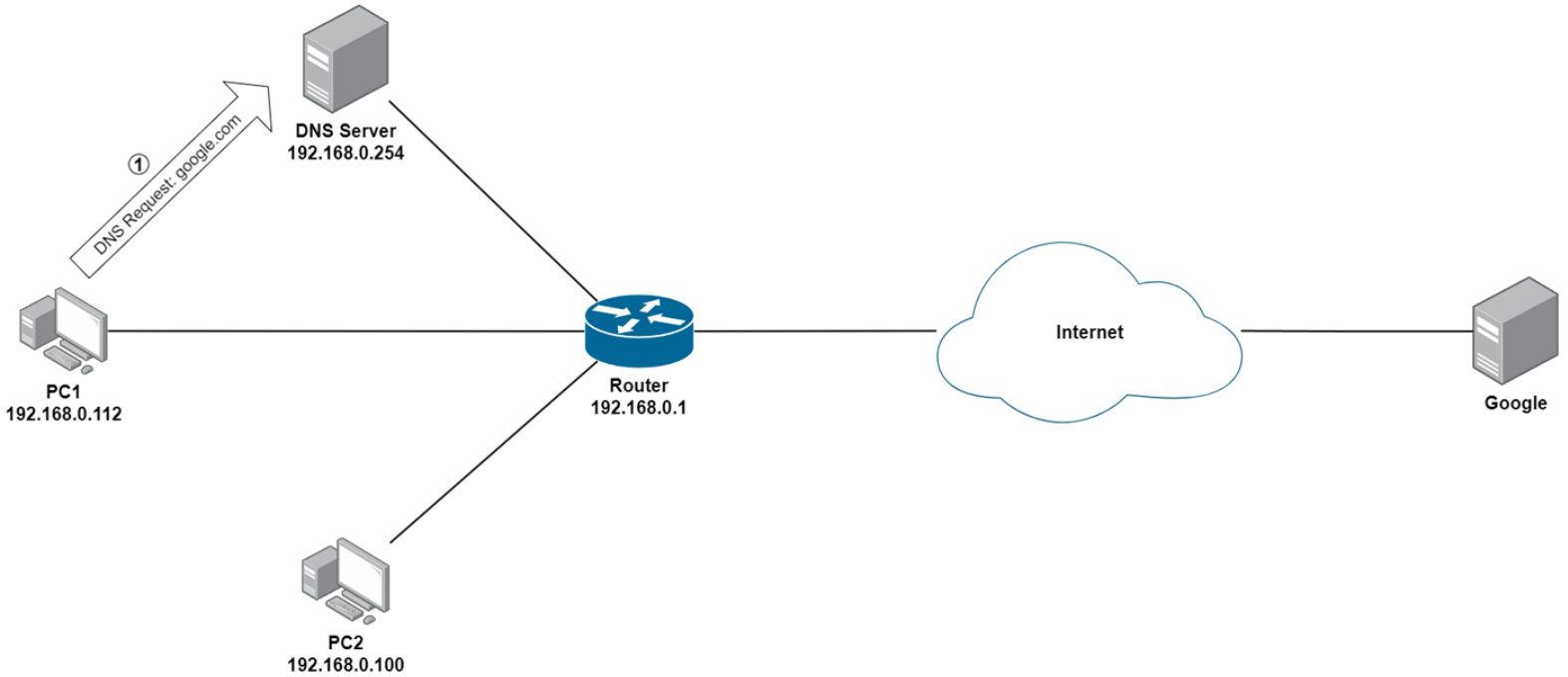
Supporting protocols for IPv4 (ICMP)



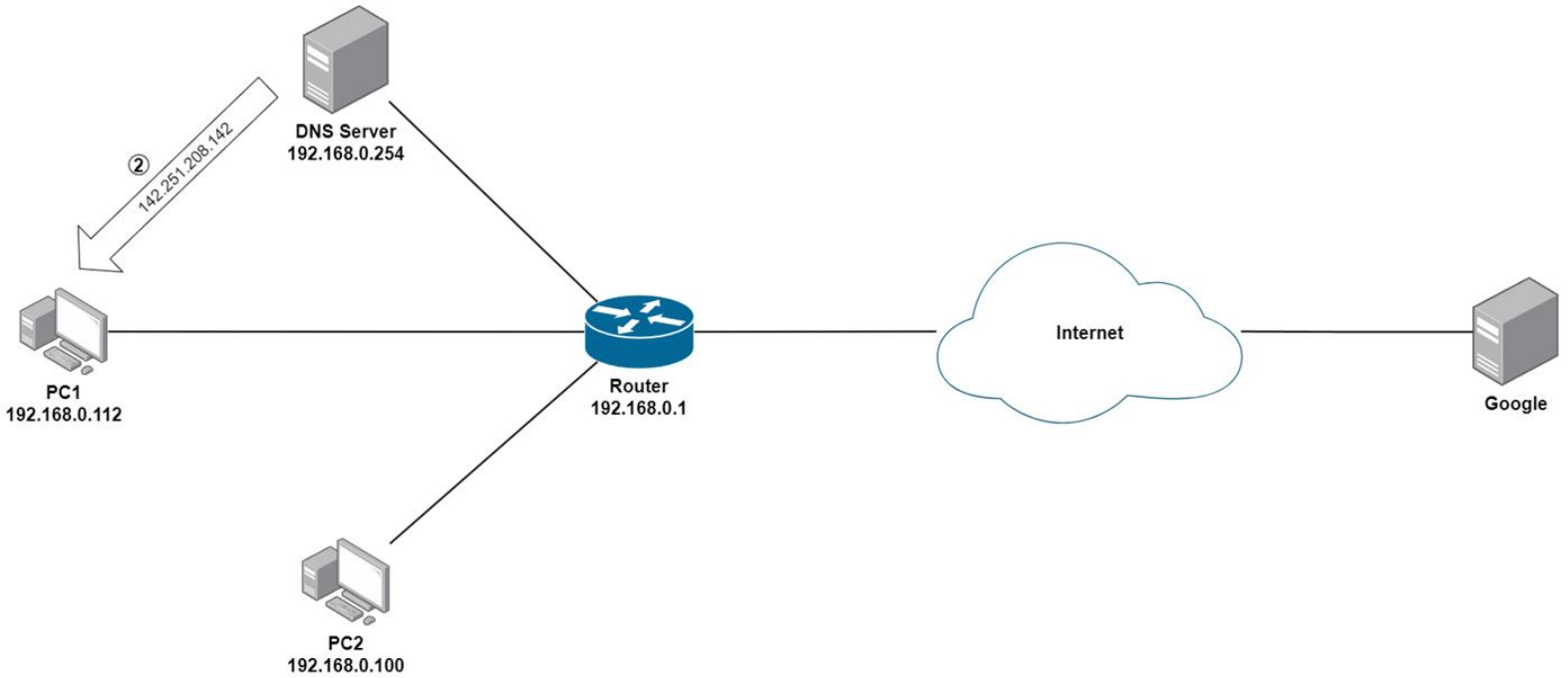
Supporting protocols for IPv4 (DNS)



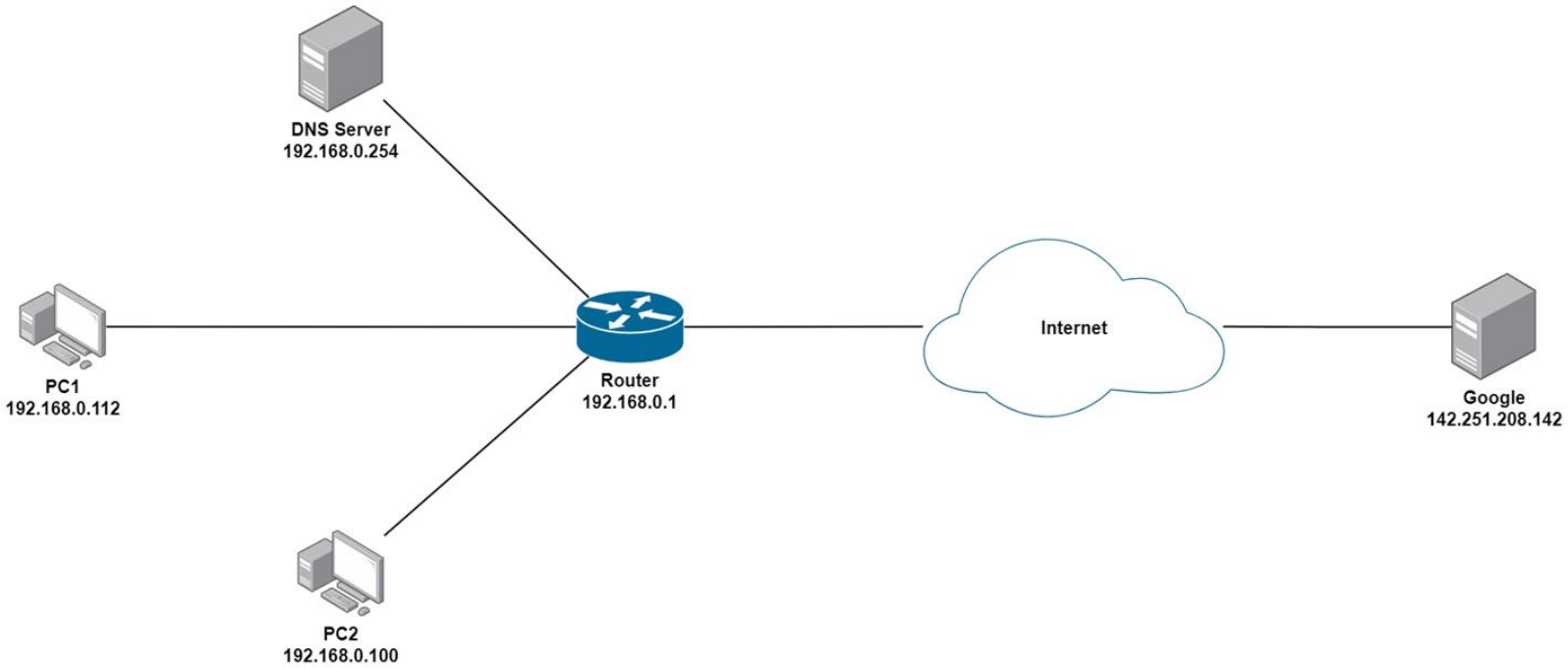
Supporting protocols for IPv4 (DNS)



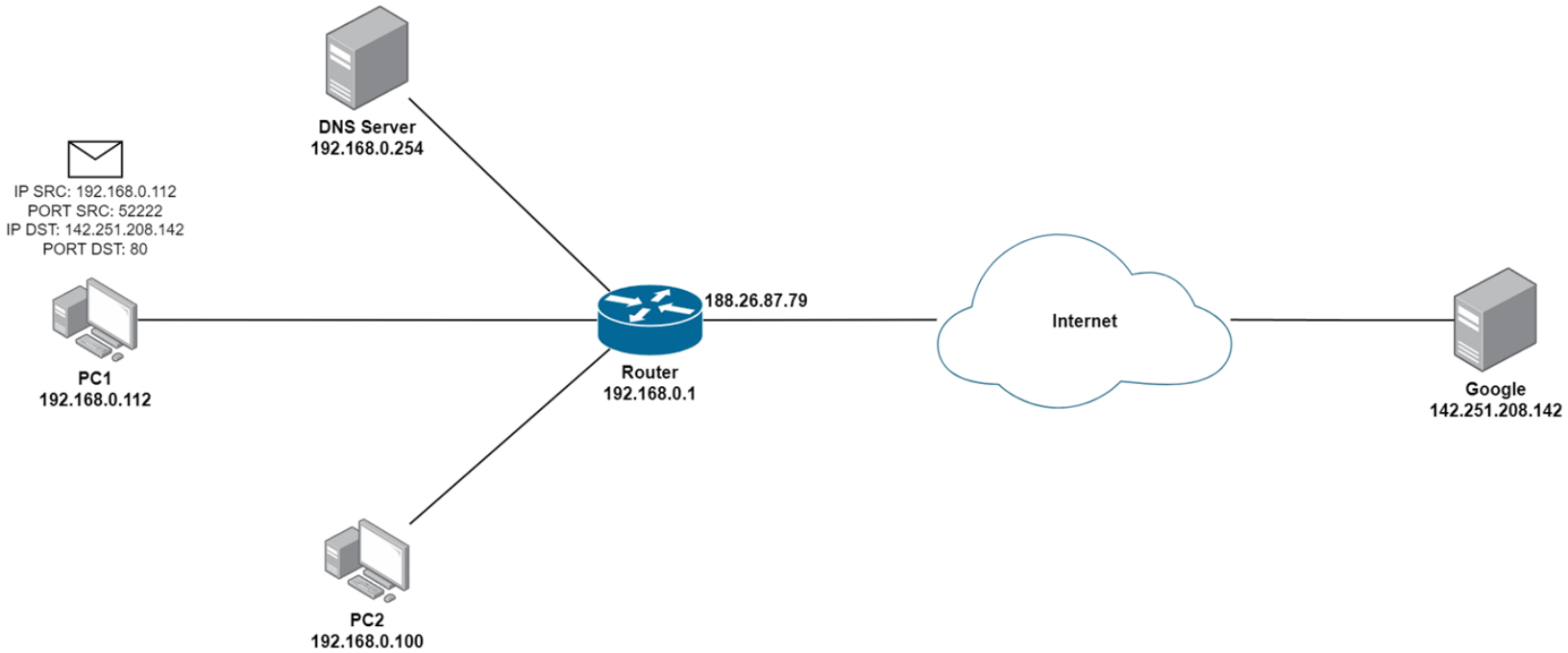
Supporting protocols for IPv4 (DNS)



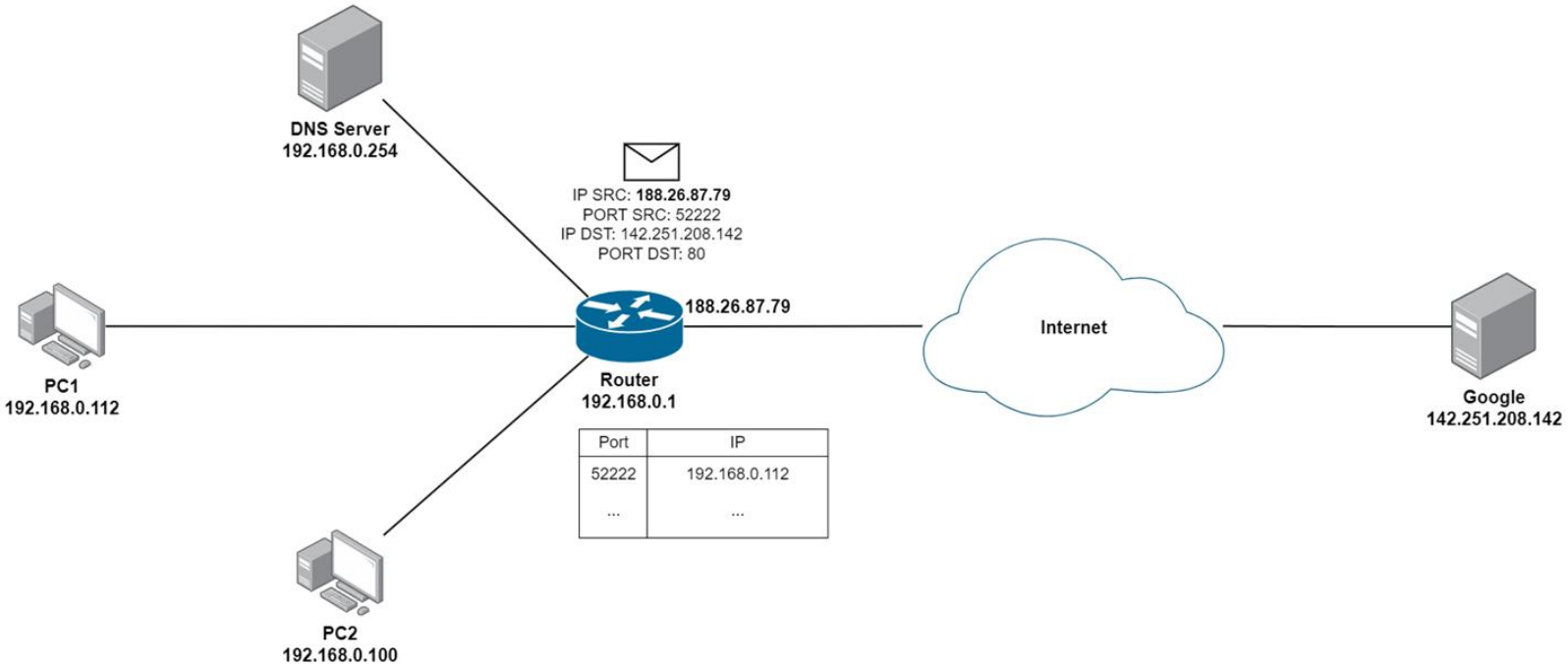
Supporting protocols for IPv4 (DNS)



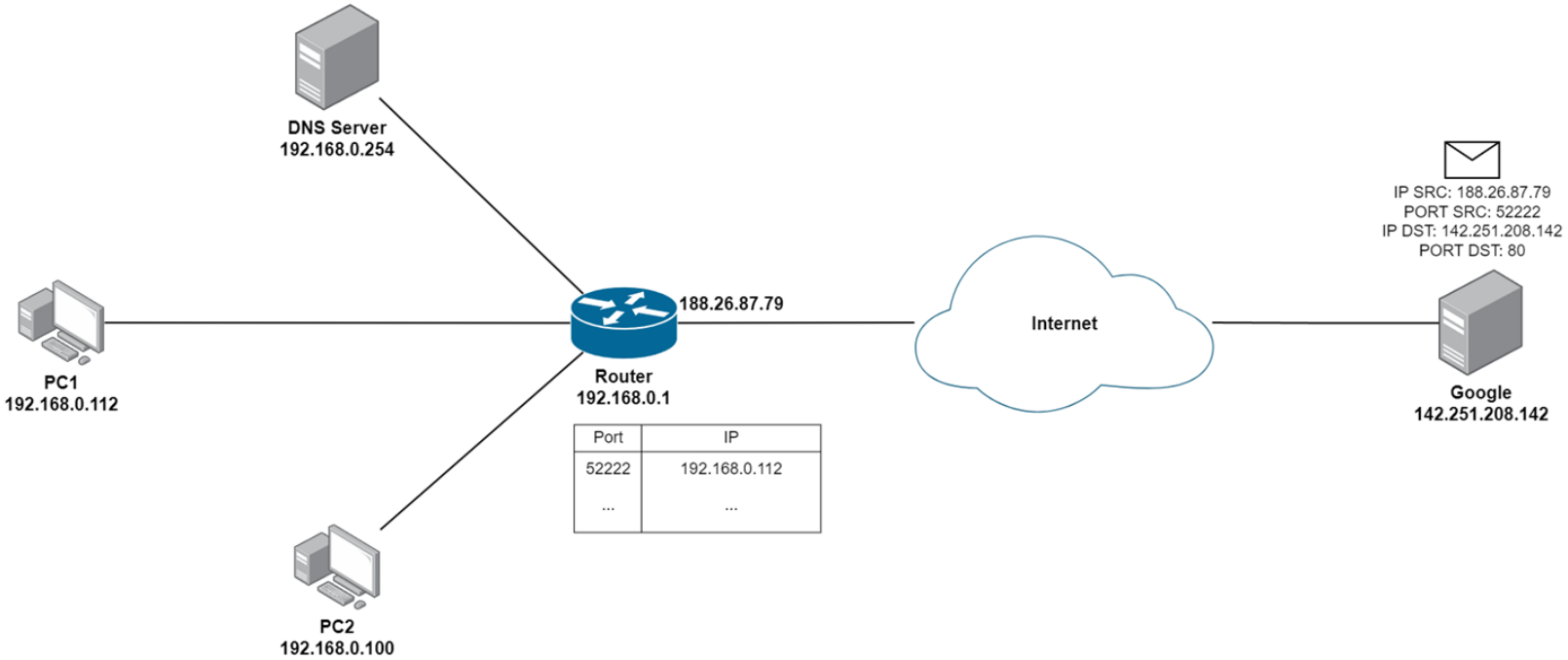
Supporting protocols for IPv4 (NAT)



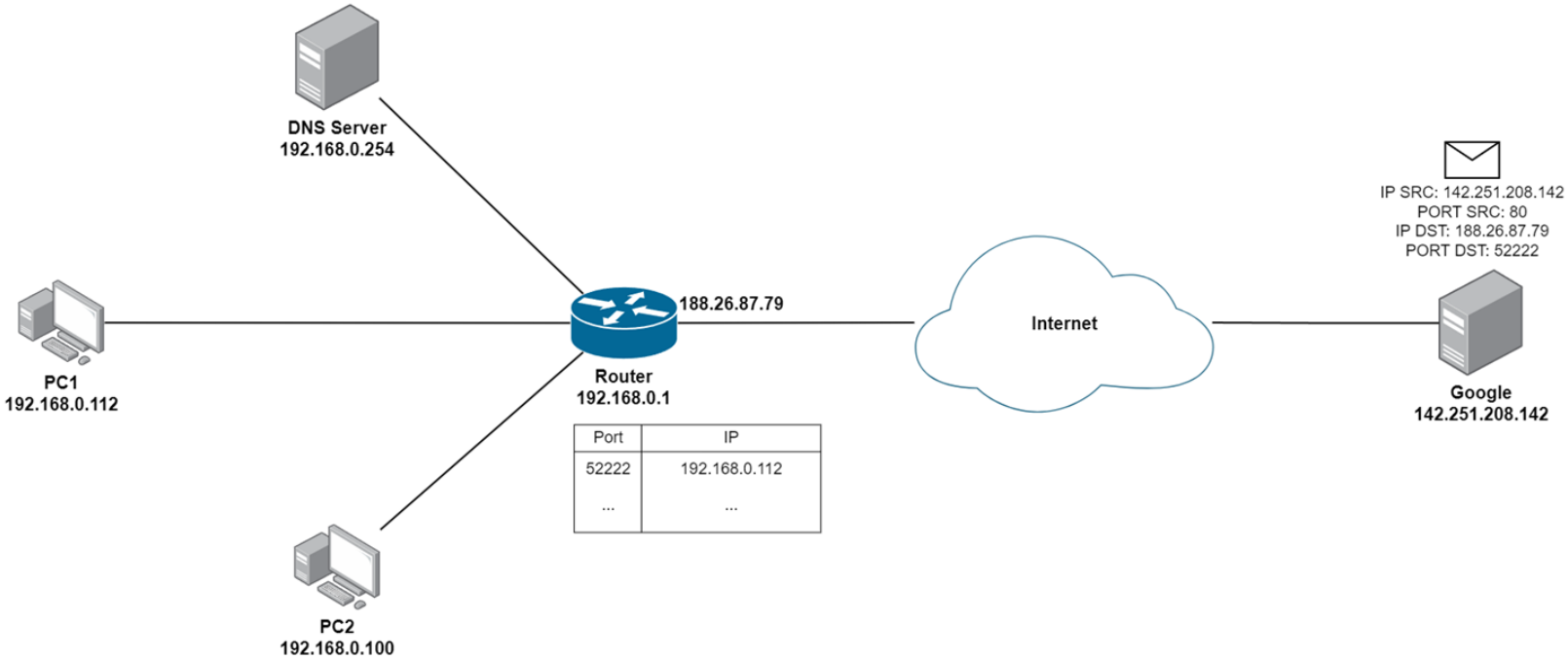
Supporting protocols for IPv4 (NAT)



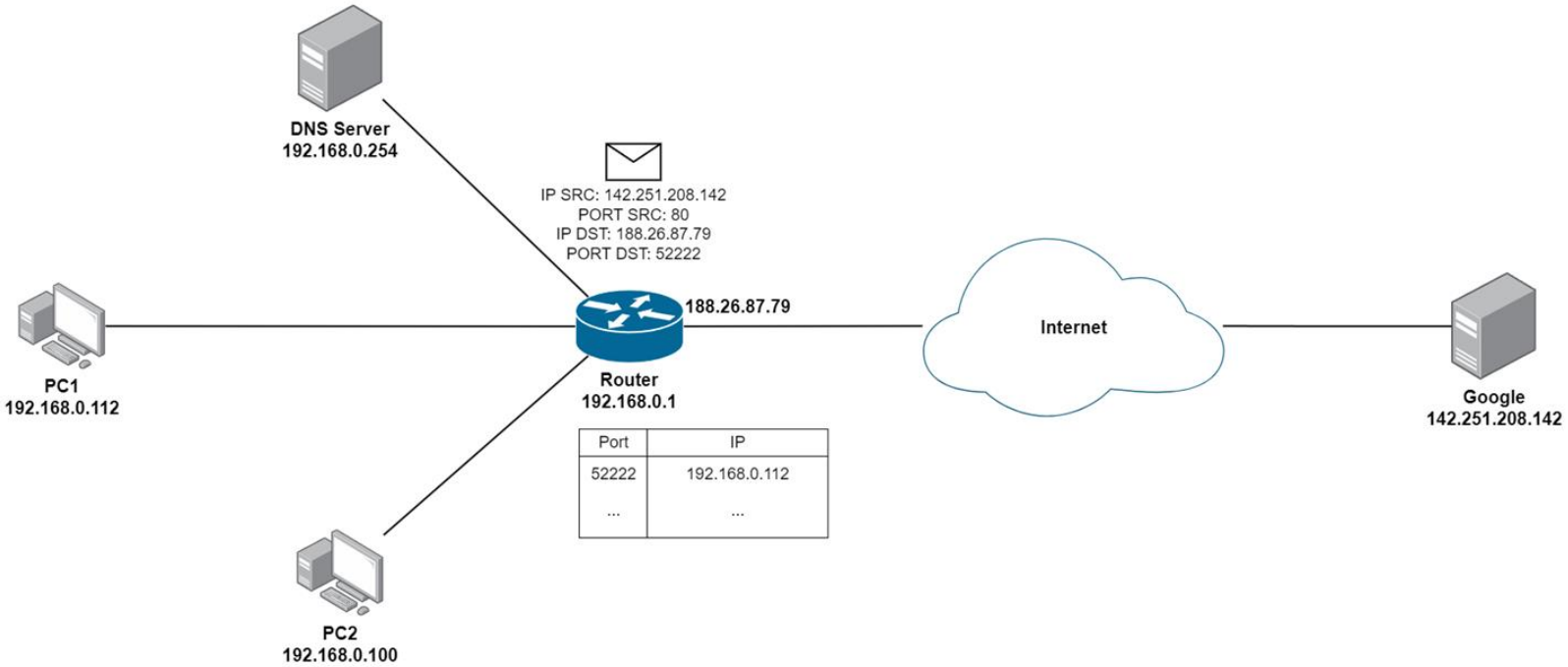
Supporting protocols for IPv4 (NAT)



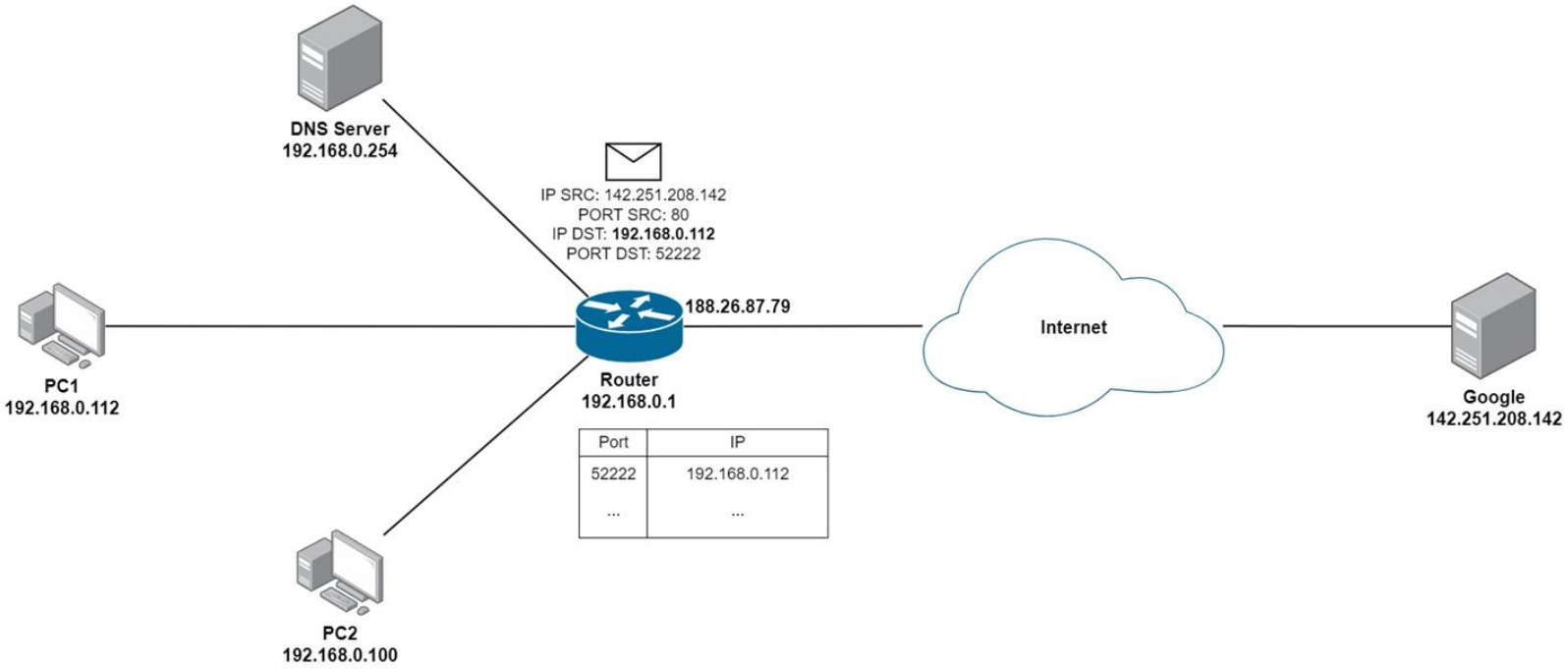
Supporting protocols for IPv4 (NAT)



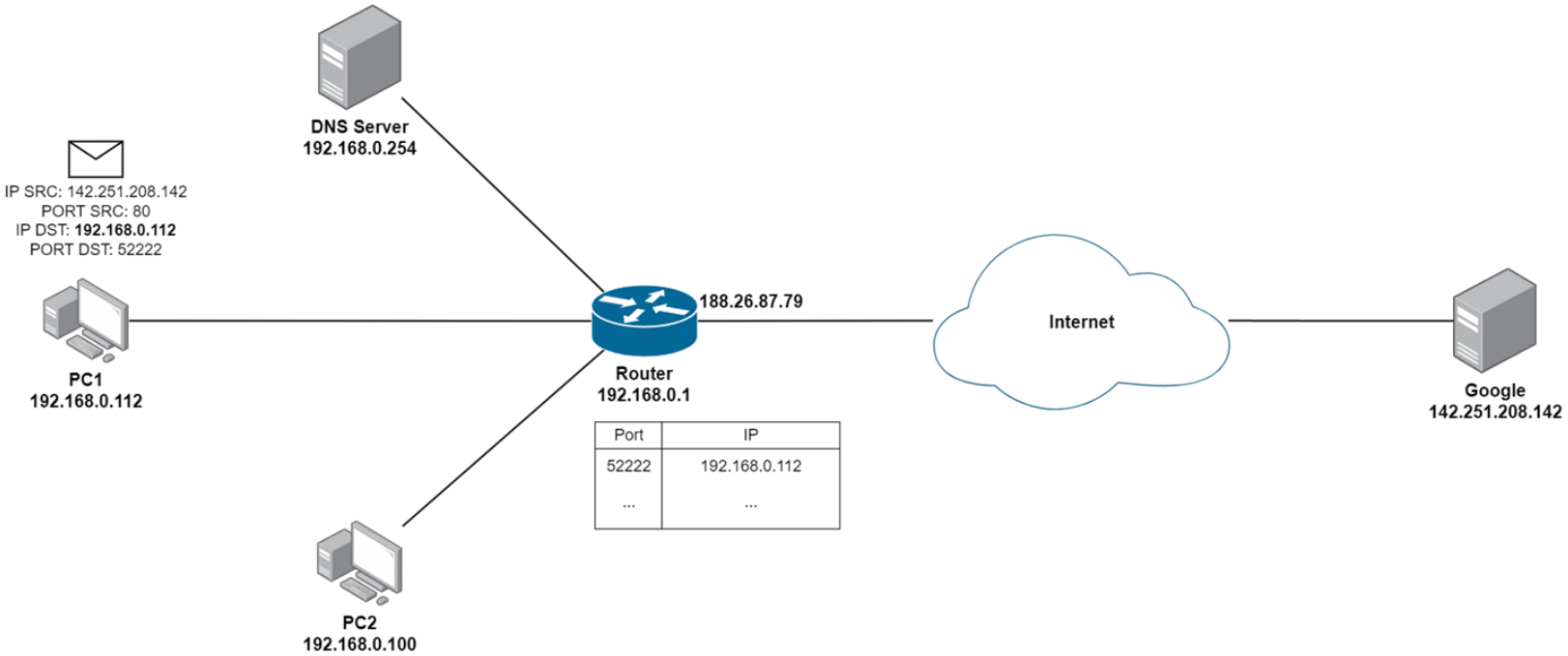
Supporting protocols for IPv4 (NAT)



Supporting protocols for IPv4 (NAT)



Supporting protocols for IPv4 (NAT)



IPv6

IPv6

- Motivation
  - Not enough public IPv4 addresses
  - Auto configuration of addresses
    - Link-local addresses
    - Stateless Address Autoconfiguration - SLAAC
  - Simpler header
    - Or is it?

IPv6 Header


Version
Traffic class
Flow label
Payload length
Next header
Hop limit
Source address
Destination address

IPv6 Extension Headers

- Hop-by-Hop Options
- Fragment
- Destination Options
- Routing
- Authentication
- Encapsulating Security Payload (ESP)

IPv6 Extension Headers

- Hop-by-Hop Options
- Fragment
- Destination Options
- Routing
- Authentication
- Encapsulating Security Payload (ESP)

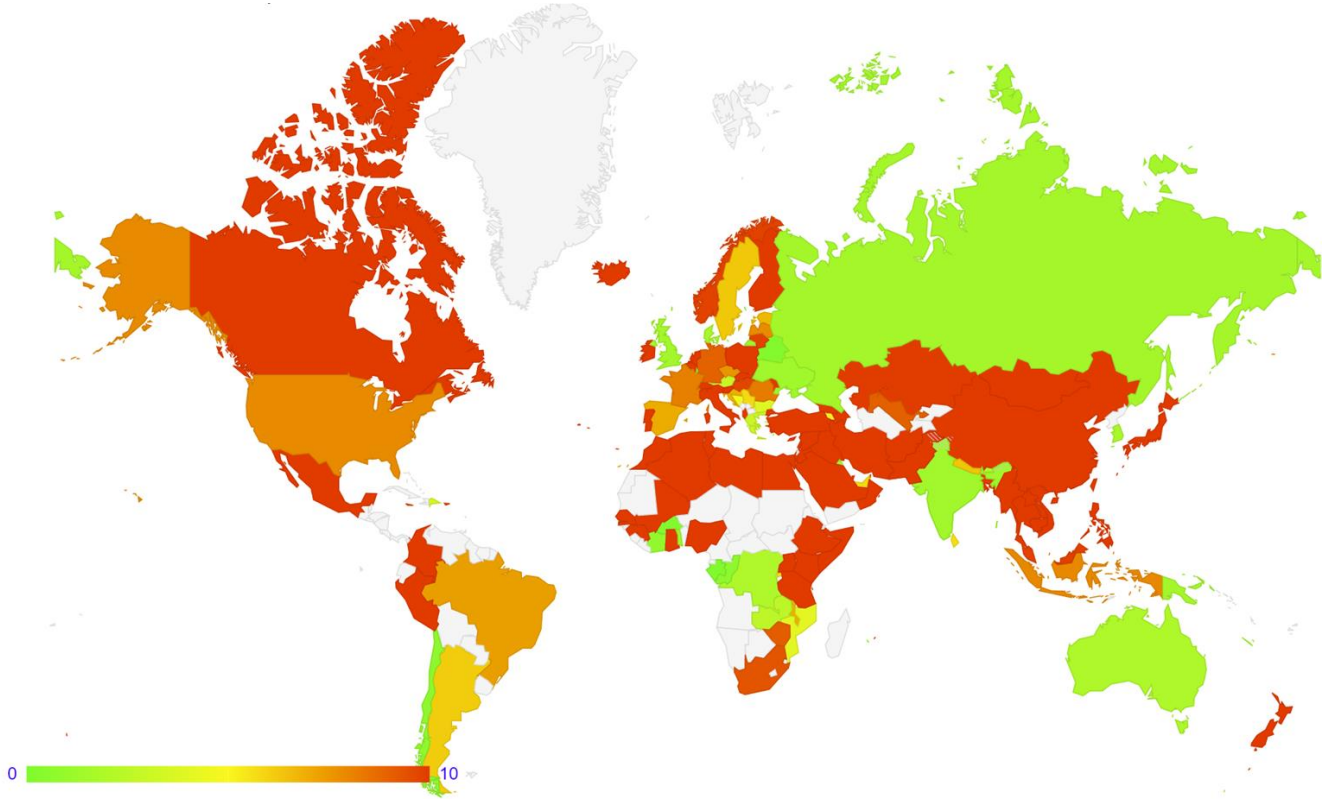
- Hop-by-Hop Options
- Destination Options
- Routing
- Fragment
- Authentication
- ESP
- Destination Options

IPv6 Extension Headers

- Hop-by-Hop Options
- Fragment
- Destination Options
- Routing
- Authentication
- Encapsulating Security Payload (ESP)

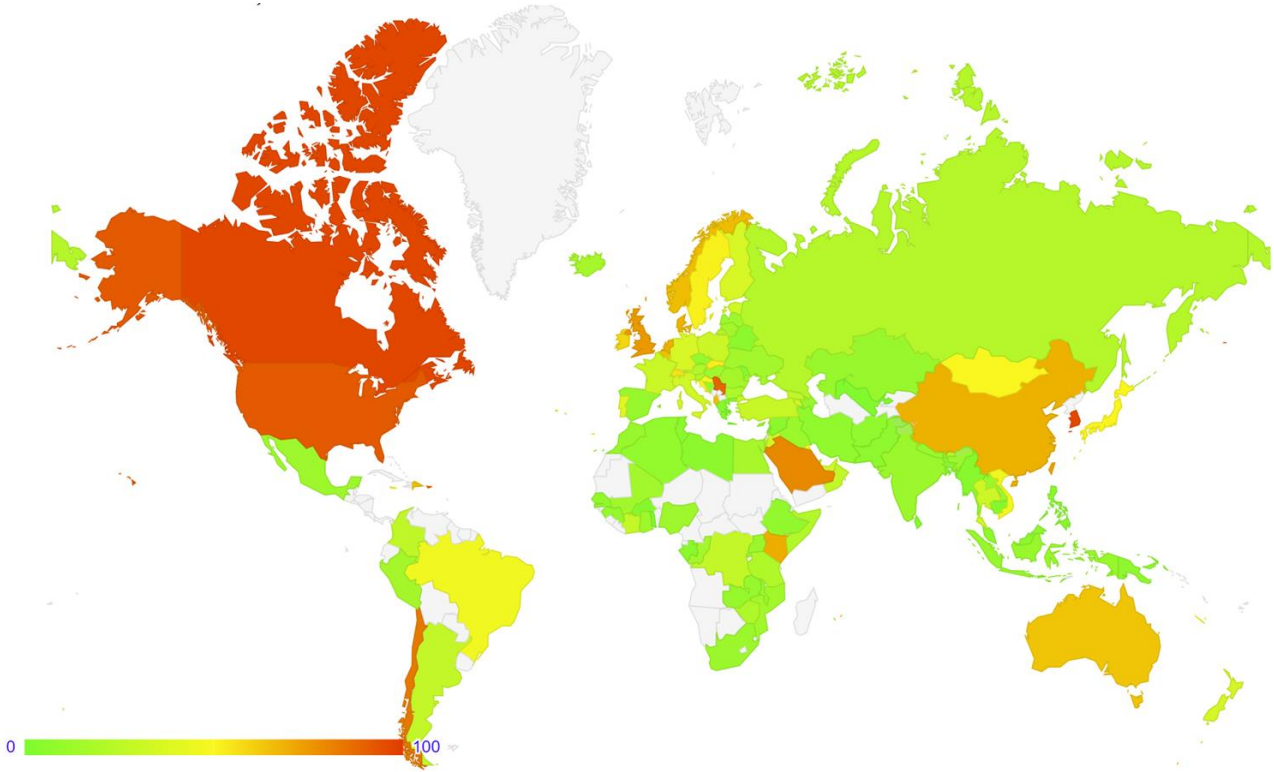
- Hop-by-Hop Options
- **Destination Options**
- Routing
- Fragment
- Authentication
- ESP
- **Destination Options**

IPv6 Fragmentation Header



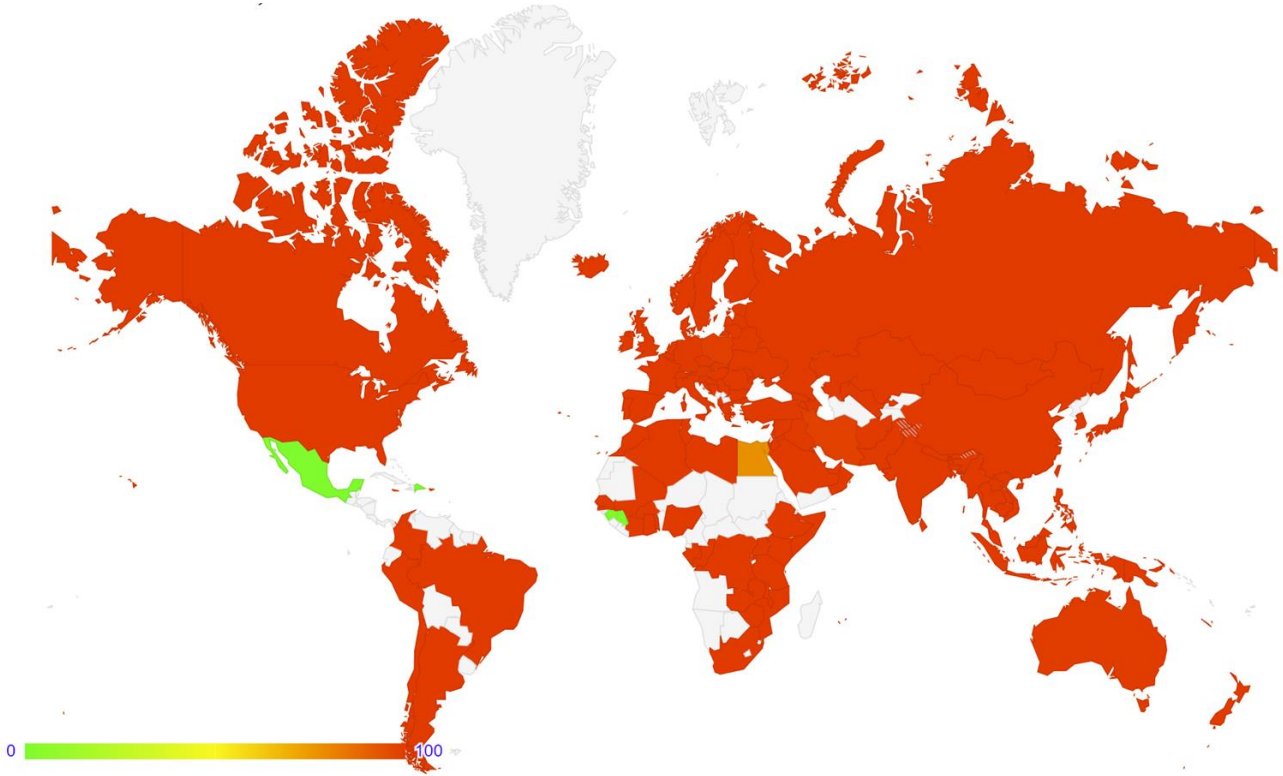
IPv6 Fragmentation Header drop rate as of 2024/02/20; © APNIC; https://stats.labs.apnic.net/v6frag

IPv6 Hop-by-Hop Options Header



IPv6 Hop-by-Hop Options Header drop rate as of 2024/02/20; © APNIC; https://stats.labs.apnic.net/cgi-bin/v6frag_worldmap?w=7&d=h

IPv6 Destination Options Header



IPv6 Destination Options Header drop rate as of 2024/02/20; © APNIC; https://stats.labs.apnic.net/cgi-bin/v6frag_worldmap?w=7&d=d

IPv6 Extension Headers

- RFC 8200 recommendations
  - Nodes should skip unrecognized Headers
  - Hop-by-Hop Options can be ***ignored***
  - Path MTU Discovery ***strongly recommended***
    - Makes Fragmentation Header useless

IPv6 Address Format

2001:0db8:85a3:0000:0000:8a2e:0000:7334

IPv6 Address Format

2001:0db8:85a3:0000:0000:8a2e:0000:7334

2001:db8:85a3:**0**:**0**:8a2e:**0**:7334

IPv6 Address Format

2001:0db8:85a3:0000:0000:8a2e:0000:7334

2001:db8:85a3:**0**:**0**:8a2e:**0**:7334

2001:0db8:85a3**::**8a2e:**0**:7334

IPv6 Addresses

- Link-local
  - fe80::/10
- Multicast
  - ff00::/8
  - ff01::1 - all nodes
  - ff01::2 - all routers
- Example
  - 2001:2b8::/32

Supporting protocols for IPv6

- IPv4
  - ICMP
  - ARP
  - DHCP
  - DNS
- IPv6
  - ICMPv6
  - ICMPv6
  - ICMPv6
  - DNS

Supporting protocols for IPv6

- IPv4
  - ICMP
  - ARP
  - DHCP
  - DNS
- IPv6
  - ICMPv6
  - ICMPv6 **(IPv6 ND)**
  - **DHCPv6**
  - DNS

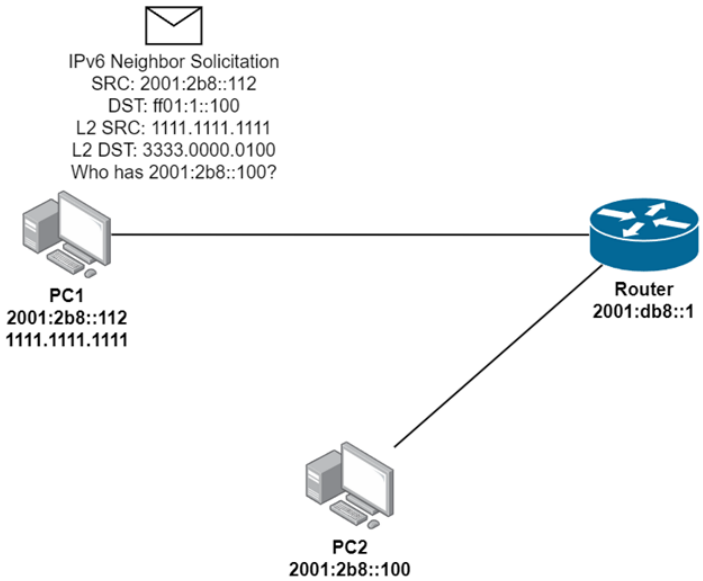
Supporting protocols for IPv6 (ICMPv6)

- Similar to ICMP
- Messages
  - Destination Unreachable
  - Packet Too Big
    - Essential for Path MTU Discovery
  - Time Exceeded
  - Parameter Problem
  - Echo Request & Echo Reply

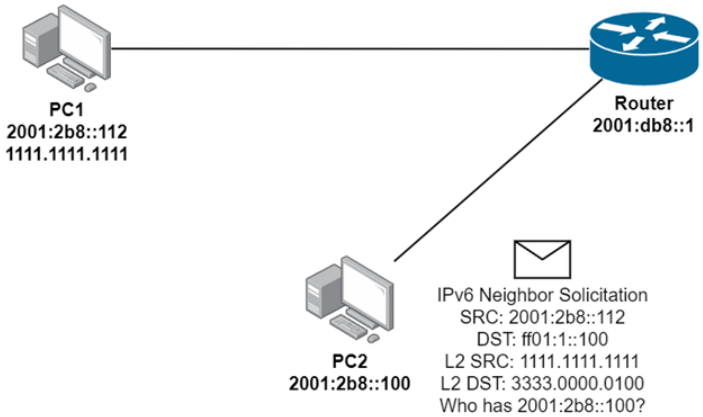
Supporting protocols for IPv6 (IPv6 ND)

- ARP replacement (and much more)
- Used together with SLAAC for IP address configuration
- RFC 4861
  - ~90 pages

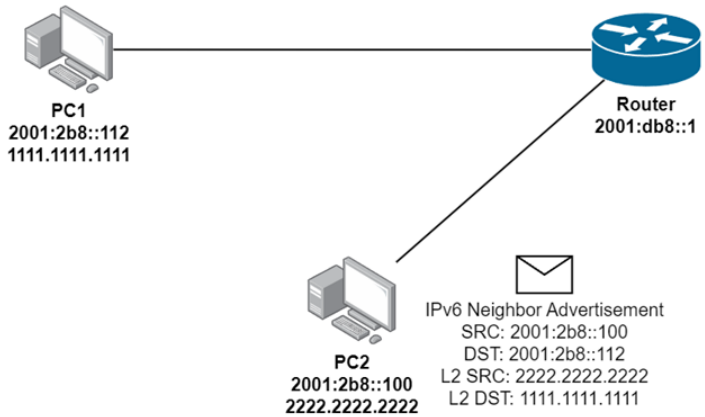
Supporting protocols for IPv6 (IPv6 ND)



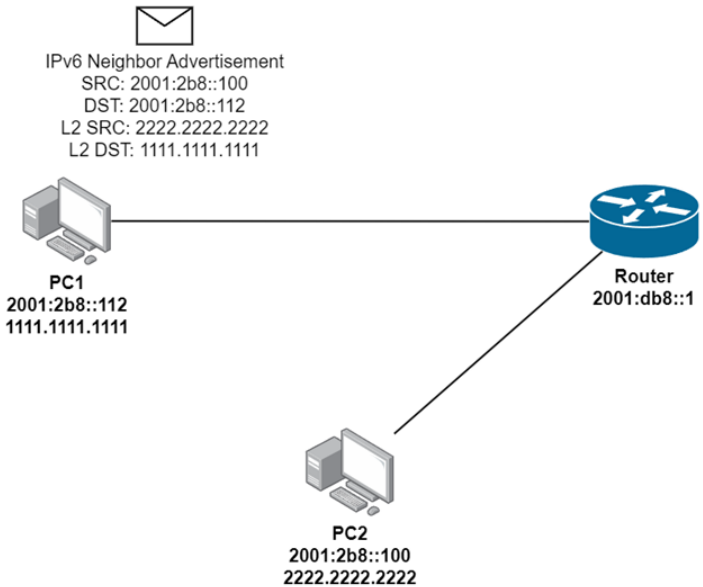
Supporting protocols for IPv6 (IPv6 ND)



Supporting protocols for IPv6 (IPv6 ND)



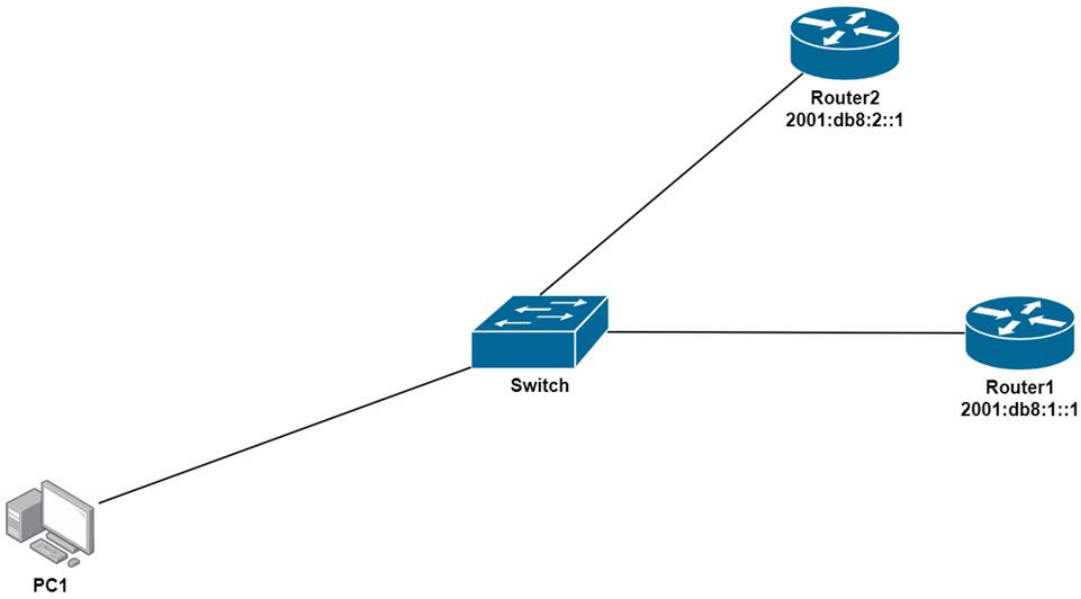
Supporting protocols for IPv6 (IPv6 ND)



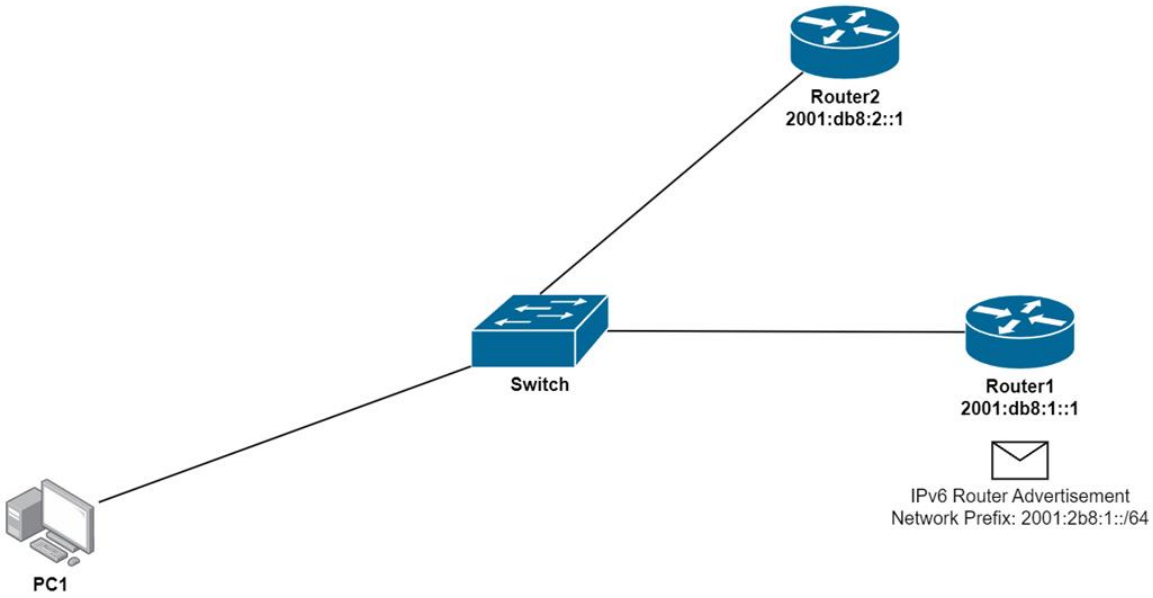
Supporting protocols for IPv6 (IPv6 ND)

- Essential part of SLAAC
  - Router Solicitation
  - Router Advertisements
    - Gateway
    - Address prefix
    - DNS Servers

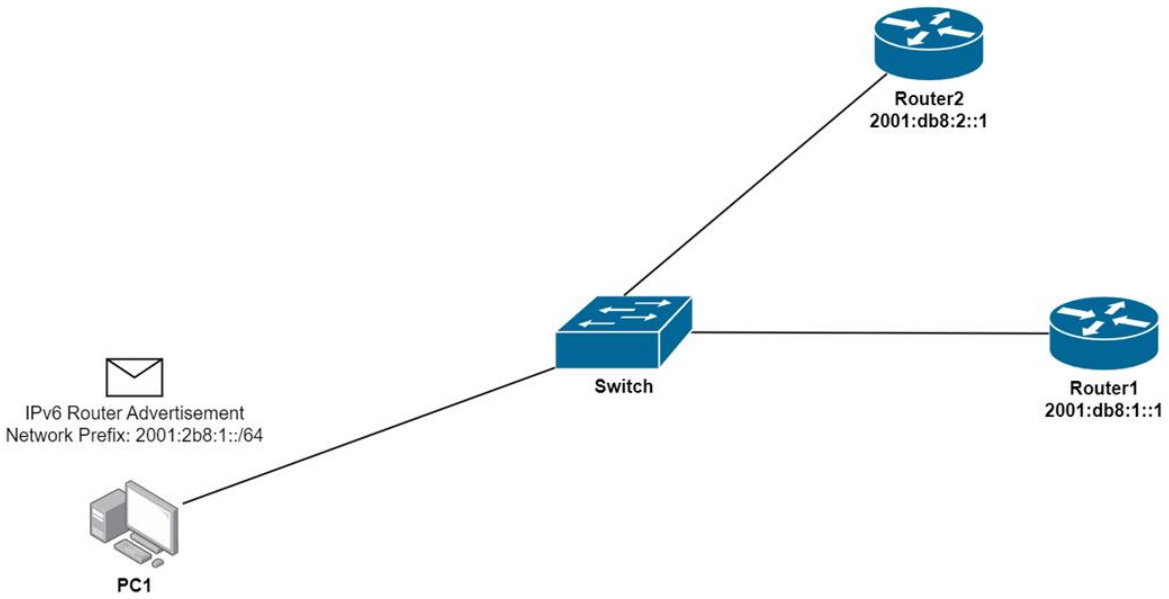
Supporting protocols for IPv6 (IPv6 ND)



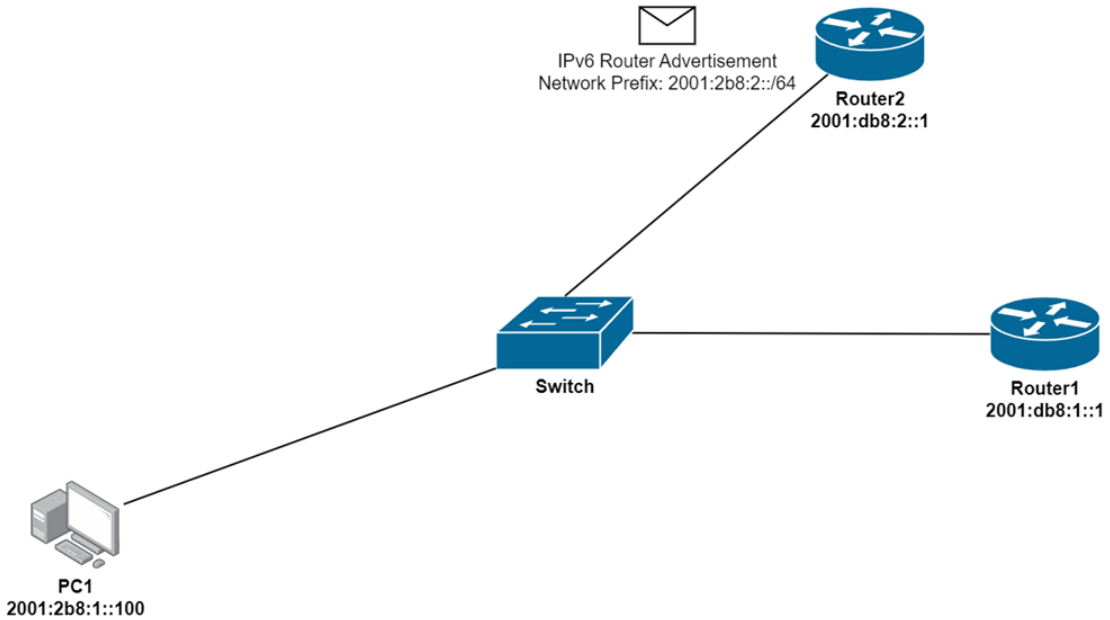
Supporting protocols for IPv6 (IPv6 ND)



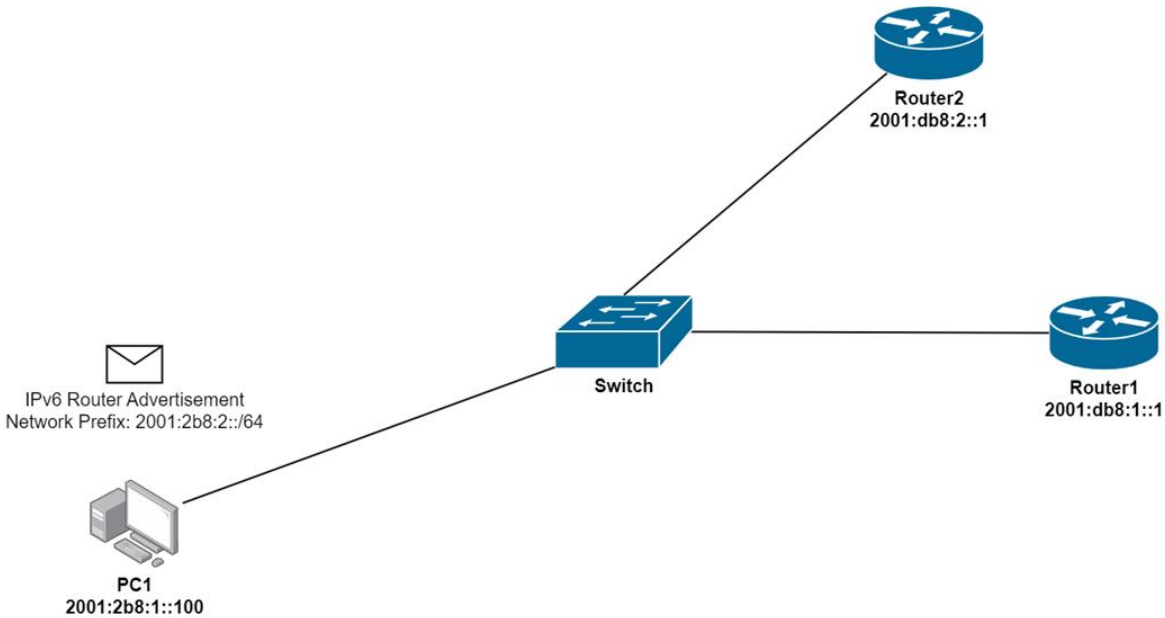
Supporting protocols for IPv6 (IPv6 ND)



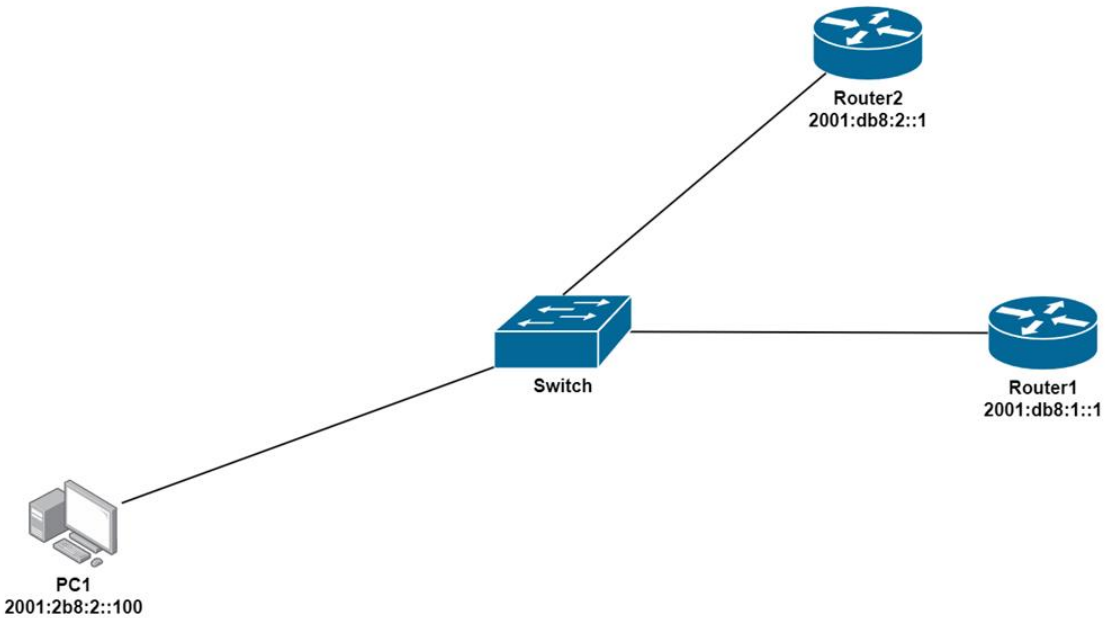
Supporting protocols for IPv6 (IPv6 ND)



Supporting protocols for IPv6 (IPv6 ND)



Supporting protocols for IPv6 (IPv6 ND)



Supporting protocols for IPv6 (IPv6 ND)

- Other things that Neighbor Discovery does
  - Neighbor Unreachability Detection
  - Duplicate Address Detection
  - Redirecting hosts to use another router

Supporting protocols for IPv6 (DHCPv6)

- RFC 8415
  - ~150 pages
- Can be used like DHCP
- Usually used for prefix delegation

Supporting protocols for IPv6 (DHCPv6)

- ISP Edge Router
  - DHCP Server
  - Use /48 network to send /56 prefixes
- Client Edge Router
  - DHCP Client
  - Receives /56 network prefix
  - Creates a /64 pool of addresses on a given interface
  - Sends Router Advertisements

Supporting protocols for IPv6 (DNS)

- It’s the same
  - AAAA Records

IPv6 address configuration

- Static assignment
- Link-local addresses

Link-local addresses

fe80::/10

Link-local addresses

fe80::/10

fe80::bde0:66c4:f4c6:7f35

IPv6 address configuration

- Static assignment
- Link-local addresses
- SLAAC
- EUI64

EUI64

1111.1111.1111

EUI64

1111.1111.1111

1111.11 11.1111

EUI64

1111.1111.1111

1111.11 11.1111

1111.11FF.FE11.1111

EUI64

1111.1111.1111

1111.11 11.1111

1111.11FF.FE11.1111

1311.11FF.FE11.1111

EUI64

1111.1111.1111

1111.11 11.1111

1111.11FF.FE11.1111

1311.11FF.FE11.1111

2001:2b8::***1311:11FF:FE11:1111***

IPv6 address configuration

- Static assignment
- Link-local addresses
- SLAAC
- EUI64
- Privacy Extensions for SLAAC

Privacy Extensions for SLAAC

2001:2b8:1111:1111:1111:1111

Privacy Extensions for SLAAC

2001:2b8::5555:5555:5555:5555

Privacy Extensions for SLAAC

2001:2b8::4444:4444:4444:4444

Privacy Extensions for SLAAC

2001:2b8::3333:3333:3333:3333

Privacy Extensions for SLAAC

2001:2b8::2222:2222:2222:2222

IPv6 address configuration

- Static assignment
- Link-local addresses
- SLAAC
- EUI64
- Privacy Extensions for SLAAC
- Privacy Stable SLAAC
- DHCPv6

Is this really easier?

CVE-2023-28231: RCE IN THE MICROSOFT WINDOWS DHCPV6 SERVICE

May 02, 2023 | Trend Micro Research Team

< BACK TO THE BLOG

In this excerpt of a Trend Micro Vulnerability Research Service vulnerability report, Guy Lederfein and Lucas Miller of the Trend Micro Research Team detail a recently patched remote code execution vulnerability in the Microsoft Windows DHCPv6 Service. This bug was originally discovered by YanZiShuang@BigCJTeam of cyberkl. The vulnerability results from the improper processing of DHCPv6 Relay-forward messages. A network-adjacent attacker can leverage this vulnerability to execute code in the context of the DHCP service. The following is a portion of their write-up covering CVE-2023-28231, with a few minimal modifications.

A heap-based buffer overflow has been reported in Microsoft DHCPv6 Server. The vulnerability is due to improper processing of DHCPv6 Relay-forward messages. A remote attacker can exploit this vulnerability by sending crafted DHCPv6 Relay-forward messages to the target server. Successful exploitation could result in the execution of arbitrary code with administrative privileges.

Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Relay and Server Denial of Service Vulnerability

High

Advisory ID:	cisco-sa-ios-dhcpv6-dos-44cMvdDK	CVE-2023-20080	Download CSAF
First Published:	2023 March 22 16:00 GMT	CWE-129	Email
Version 1.0:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvw60355		
CVSS Score:	Base 8.6		

Summary

A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition.

This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK

This advisory is part of the March 2023 release of the Cisco IOS and IOS XE Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: March 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Related to This Advisory

Cisco Event Response: March 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication

IPv6 vulnerabilities (2023)

- https://github.com/CVEProject/cvelistV5
- IPv6
  - 43 reported
  - 22 related to protocol implementation
- IPv4
  - 14 reported
  - 3 related to protocol implementation
- 9 common vulnerabilities (IPv4 and IPv6)

Personal opinions

- IPv6 is just different
- Common pro arguments
  - SLAAC
  - Everything is public; globally routable addresses
- Lots of vulnerabilities
  - Growing pains?
  - Complexity?

Personal opinions

- Endless cycle
  - IPv4 is the standard
  - Not enough people learn about IPv6
  - Not enough people to push adoption
  - IPv4 is still the standard
- I don’t think IPv4 will be fully out of use

Keywords

- IPv6
- ICMPv6
- Neighbor Discovery
- DHCPv6
- SLAAC
- EUI64
- Extension Headers
- IPv4
- DHCP
- ICMP
- ARP
- DNS