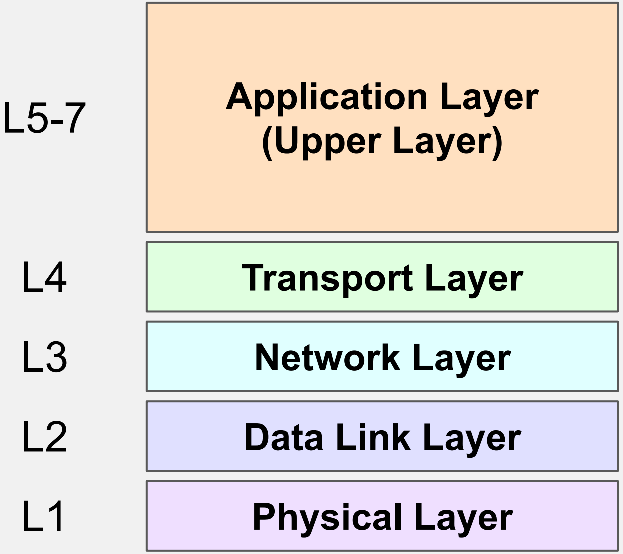
Network Security

IP Shortage? NAT on my watch

Gwendal Patat
Univ Rennes, CNRS, IRISA
2025/2026

Recall TCP/IP Model



L5-7 Application Layer (Upper Layer)

L4 Transport Layer

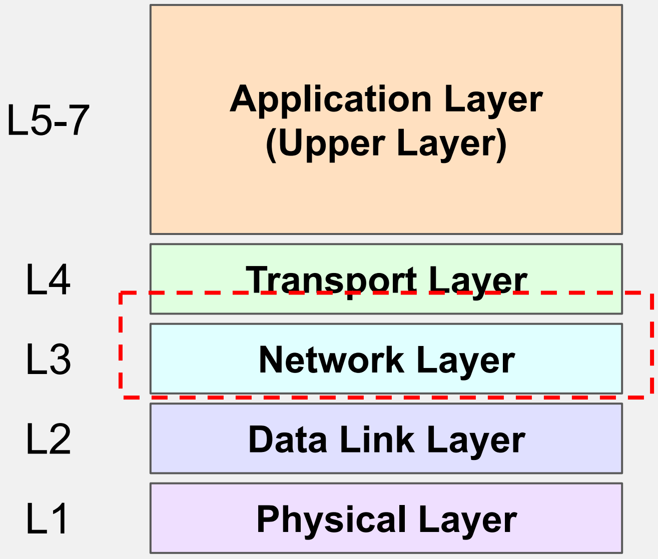
L3 Network Layer

L2 Data Link Layer

L1 Physical Layer

TCP/IP Model

Today’s Topic: Layer 3 with a bit of 4



TCP/IP Model

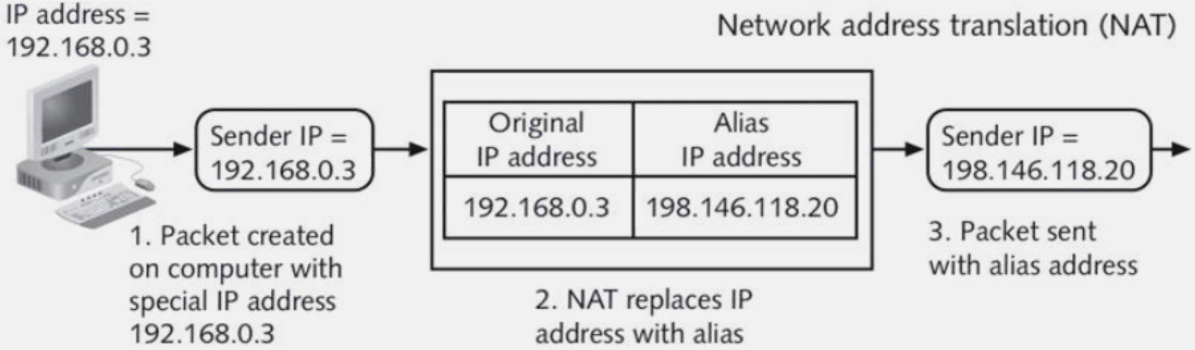
Private Addressing

- Public vs Private IPs
  - **Public**: unique address over the Internet.
  - **Private**: unique within the LAN.
- The private IP ranges have been defined by the IANA and cannot be advertised over the internet:

CIDR	**Range**
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

Network Address Translation (NAT)

- The NAT protocol allows hosts with private IP addresses to access the Internet.
- NAT is run on device (e.g., router) that connect private networks to public ones.
- NAT will translate IP addresses during transit.
  - NAT modifies the IP header of the packet.



Original IP address	Alias IP address
192.168.0.3	198.146.118.20

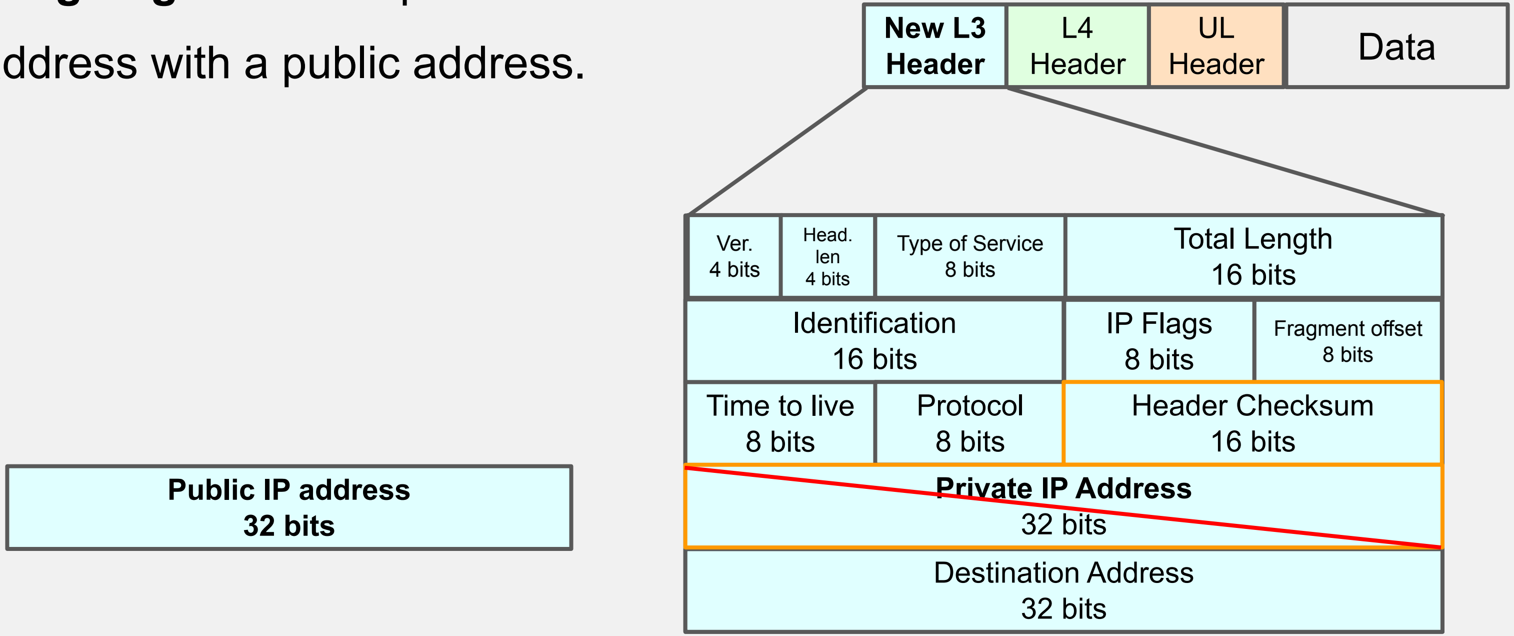
1. Packet created on computer with special IP address 192.168.0.3

2. NAT replaces IP address with alias

3. Packet sent with alias address

NAT: Outgoing Traffic

- **Outgoing traffic**: Replace the src address with a public address.



New L3 Header | L4 Header | UL Header | Data

Ver. 4 bits | Head. len 4 bits | Type of Service 8 bits | Total Length 16 bits

Identification 16 bits | IP Flags 8 bits | Fragment offset 8 bits

Time to live 8 bits | Protocol 8 bits | Header Checksum 16 bits

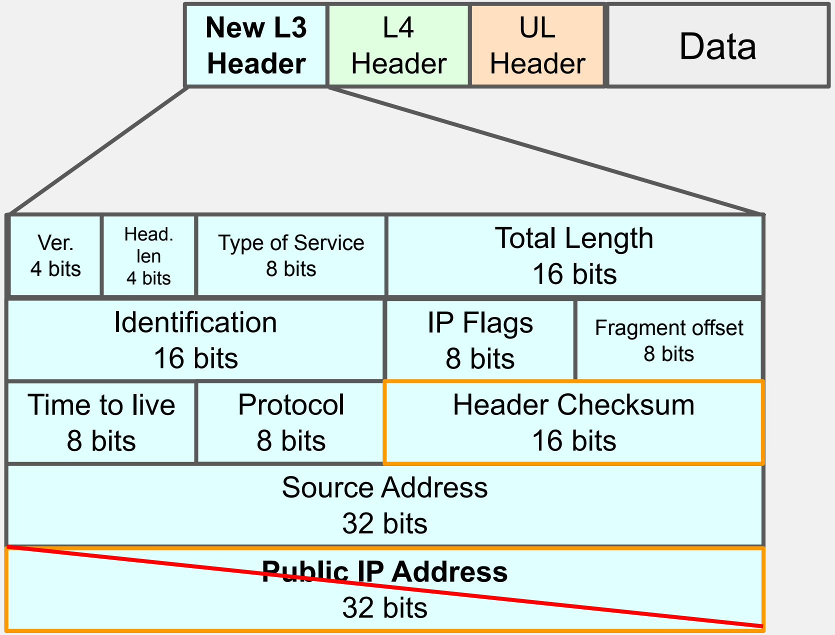
~~**Private IP Address** 32 bits~~

Destination Address 32 bits

Public IP address
32 bits

NAT: Incoming Traffic

□ **Incoming traffic**: Replace the dst address with a private address.



New L3 Header | L4 Header | UL Header | Data

Ver. 4 bits | Head. len 4 bits | Type of Service 8 bits | Total Length 16 bits

Identification 16 bits | IP Flags 8 bits | Fragment offset 8 bits

Time to live 8 bits | Protocol 8 bits | Header Checksum 16 bits

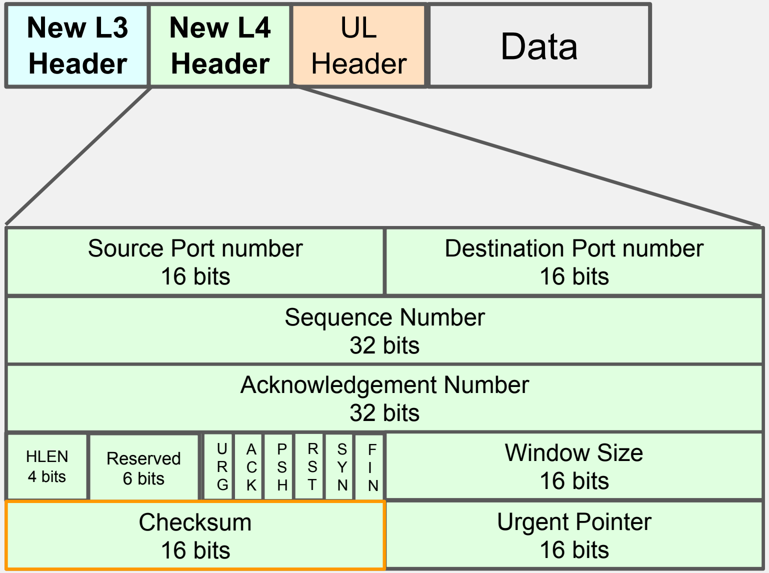
Source Address 32 bits

~~**Public IP Address**~~ ~~32 bits~~

Private IP address
32 bits

Layer 4 Checksum Trick

- In TCP/UDP implementations, checksums are **impacted by IP addresses.**



New L3 Header | **New L4 Header** | UL Header | Data

Source Port number
16 bits | Destination Port number
16 bits

Sequence Number
32 bits

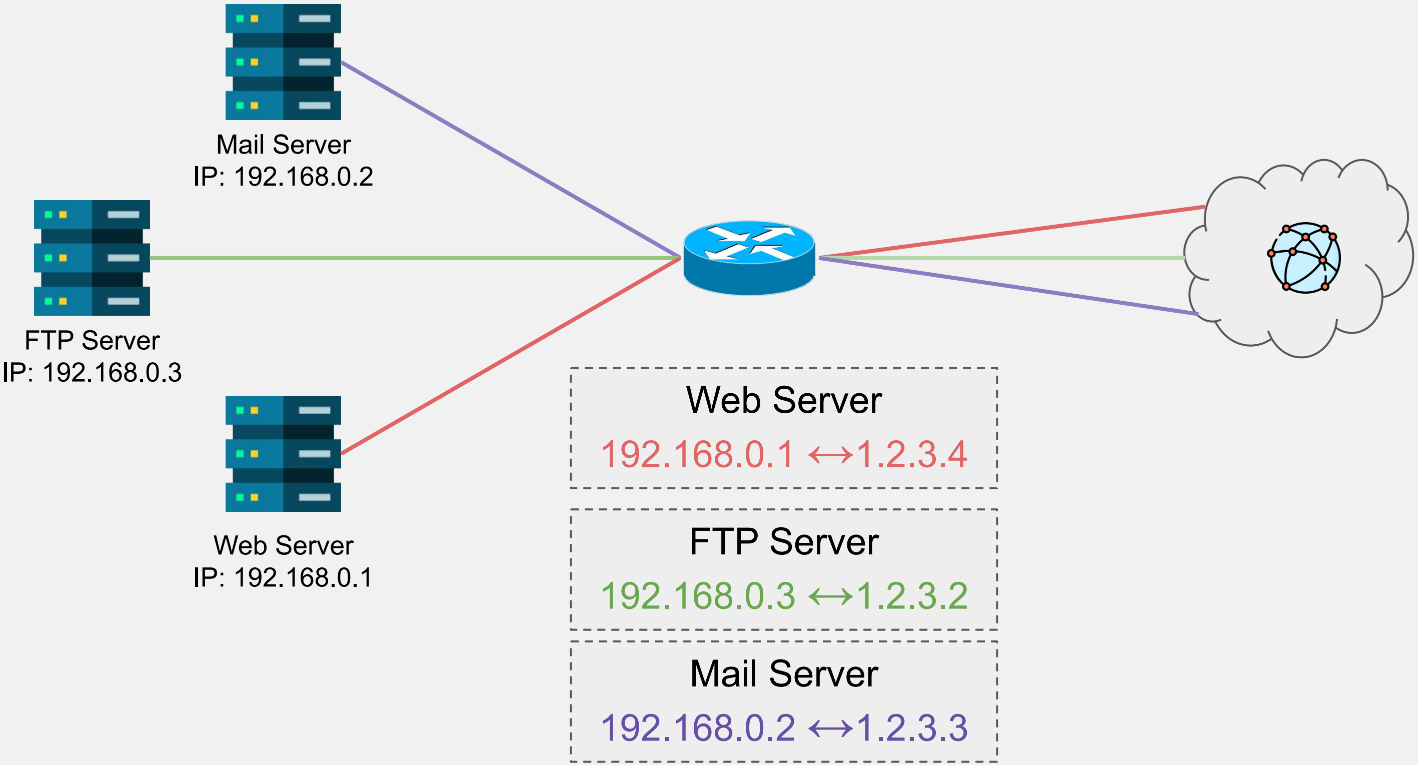
Acknowledgement Number
32 bits

HLEN
4 bits | Reserved
6 bits | URG | ACK | PSH | RST | SYN | FIN | Window Size
16 bits

Checksum
16 bits | Urgent Pointer
16 bits

Types of NAT

Static NAT



Mail Server
IP: 192.168.0.2

FTP Server
IP: 192.168.0.3

Web Server
IP: 192.168.0.1

Web Server
192.168.0.1 ↔1.2.3.4

FTP Server
192.168.0.3 ↔1.2.3.2

Mail Server
192.168.0.2 ↔1.2.3.3

Static NAT

Static NAT: A private IP is linked to one static public IP.

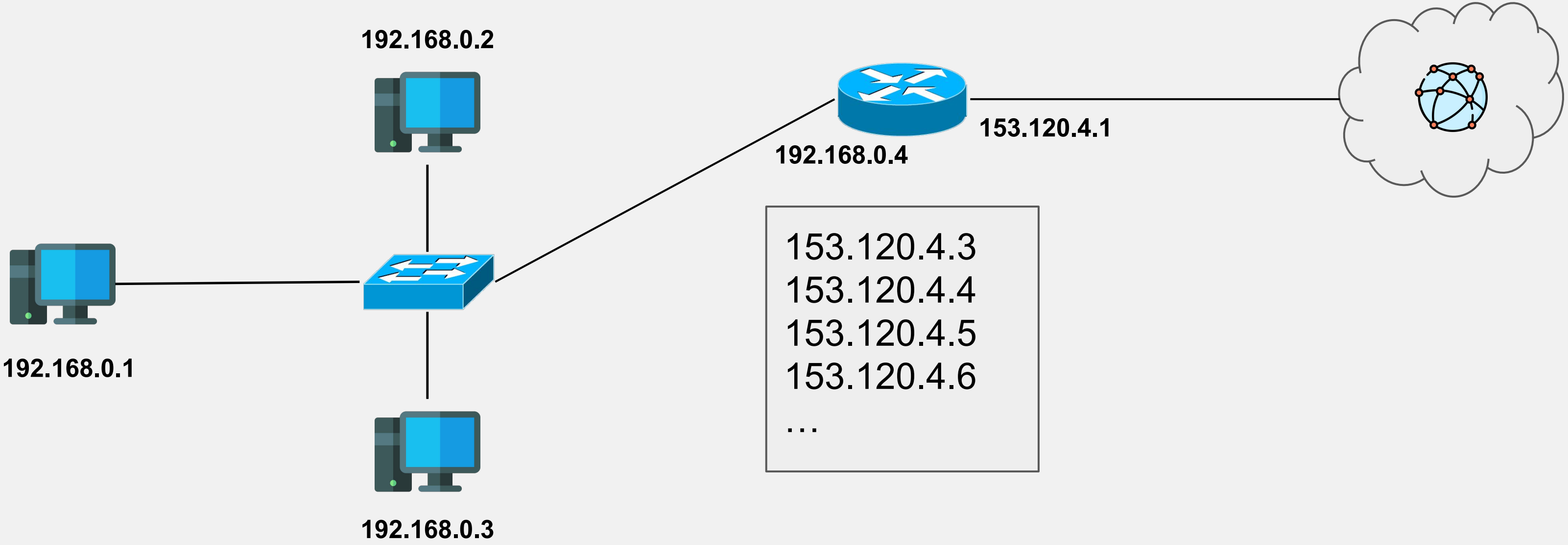
Advantages:

- Straight forward configuration.
- Internal servers can be exposed with static IP to the outside.

Disadvantage:

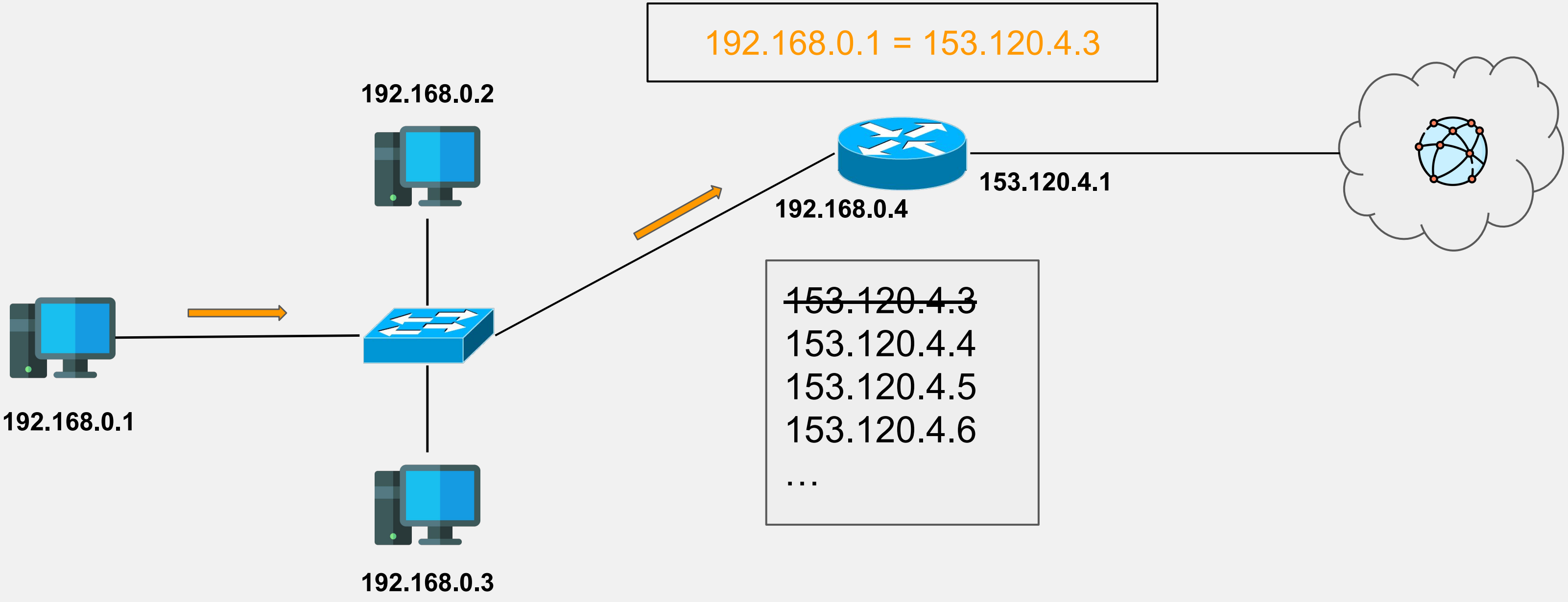
- one private IP = one public IP.
  - Do not resolve the IPv4 shortage problem.

Dynamic NAT



153.120.4.3
153.120.4.4
153.120.4.5
153.120.4.6
…

Dynamic NAT



192.168.0.1 = 153.120.4.3

192.168.0.2

192.168.0.1

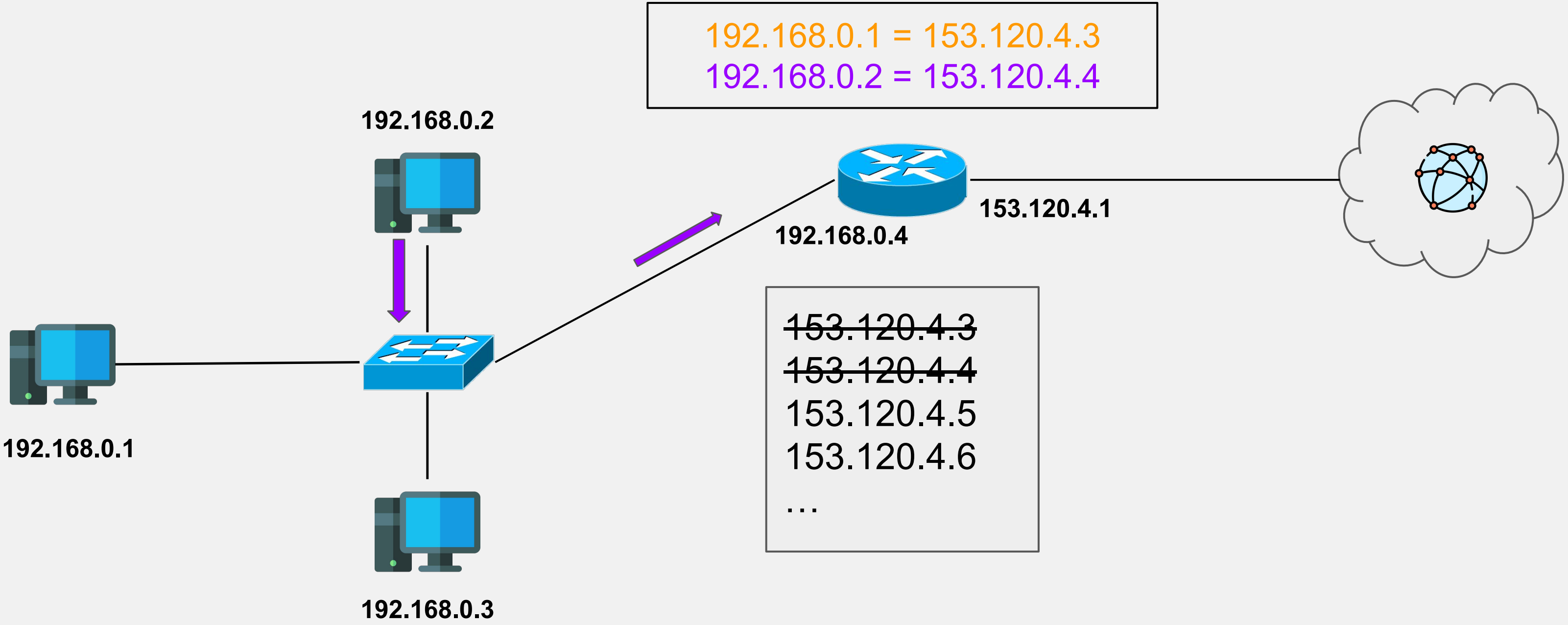
192.168.0.3

192.168.0.4

153.120.4.1

~~153.120.4.3~~
153.120.4.4
153.120.4.5
153.120.4.6
…

Dynamic NAT



192.168.0.1 = 153.120.4.3
192.168.0.2 = 153.120.4.4

~~153.120.4.3~~
~~153.120.4.4~~
153.120.4.5
153.120.4.6
…

Dynamic NAT

Dynamic NAT: A private IP is dynamically linked to the next available public IP in the pool.

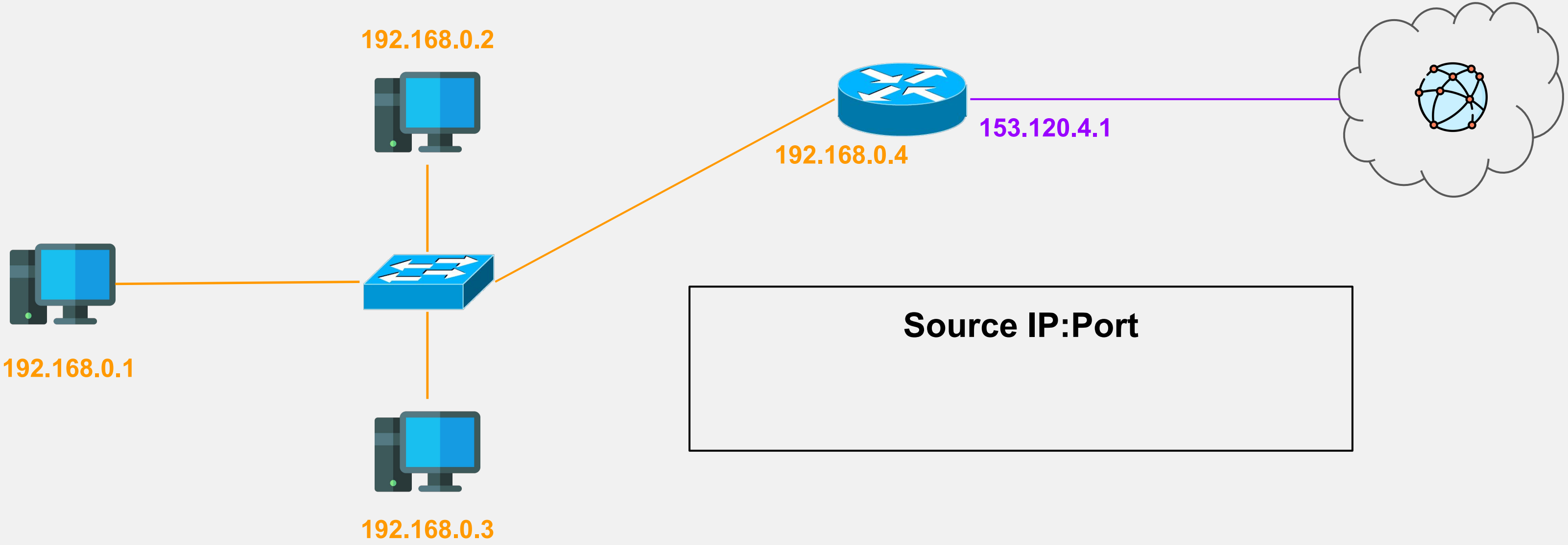
Advantage:

- Less wasteful then Static NAT
  - Many to many static/public IPs.
  - No per host mapping.

Disadvantage:

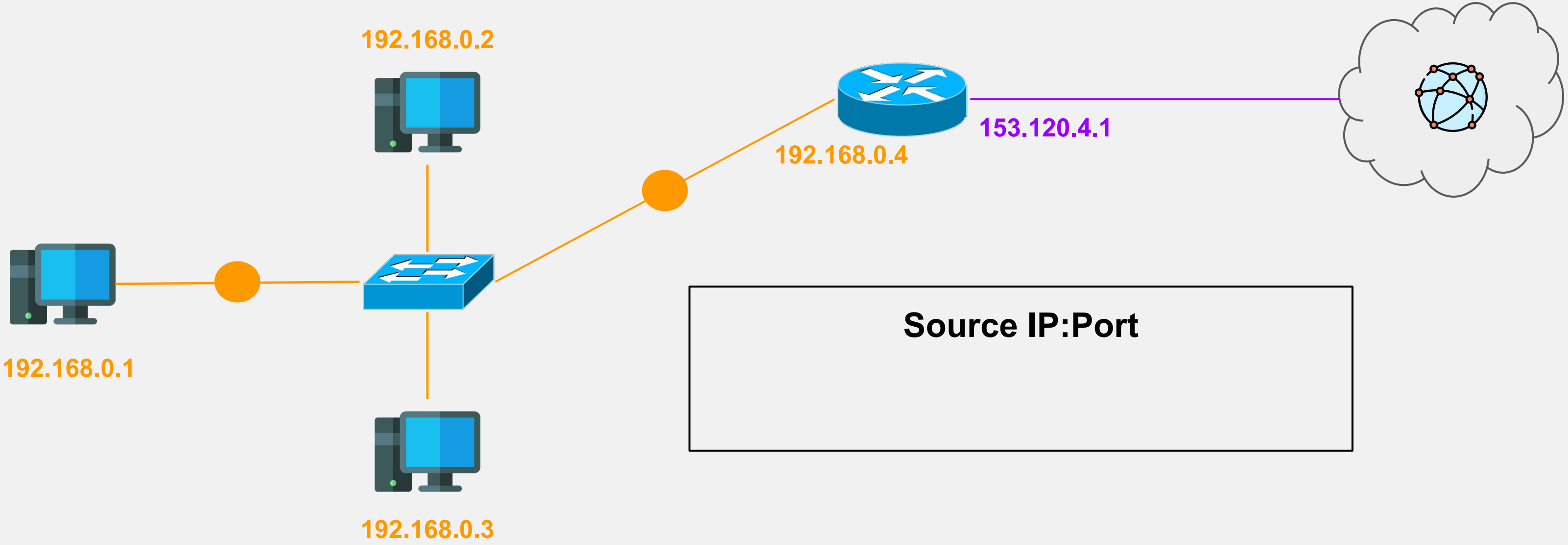
- Rolling IPs for internal servers.
  - Not stable for services.

Port Address Translation (PAT)



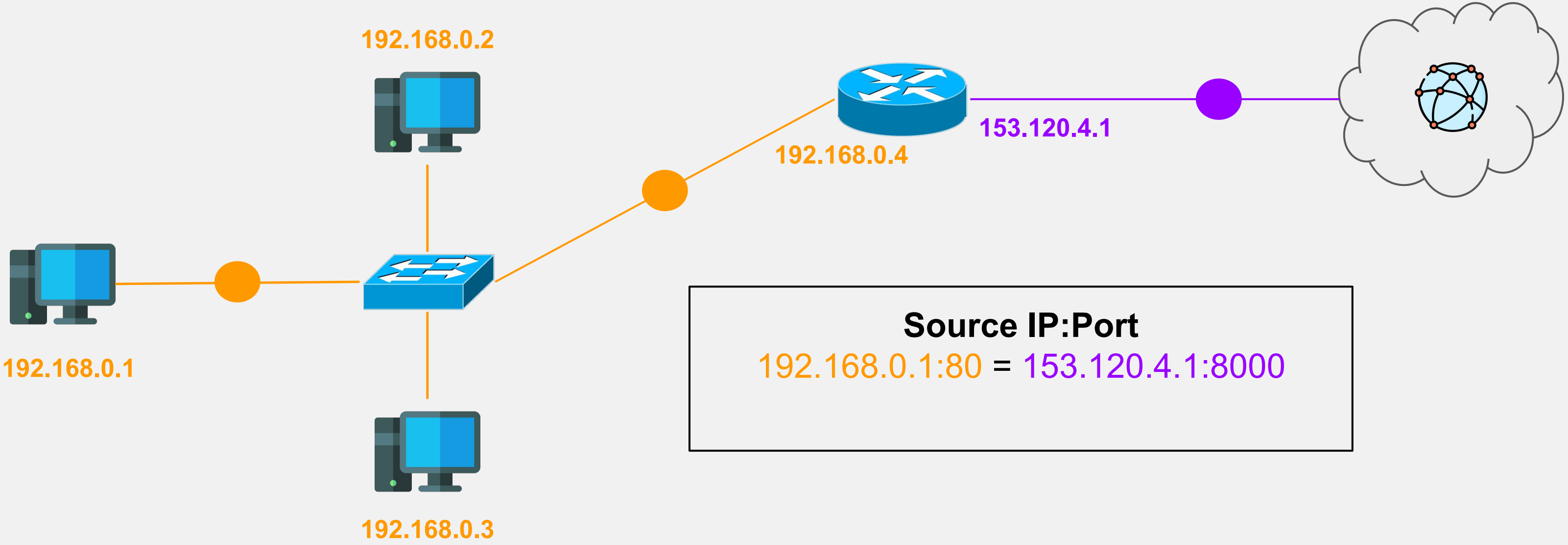
Source IP:Port

Port Address Translation (PAT)



Source IP:Port

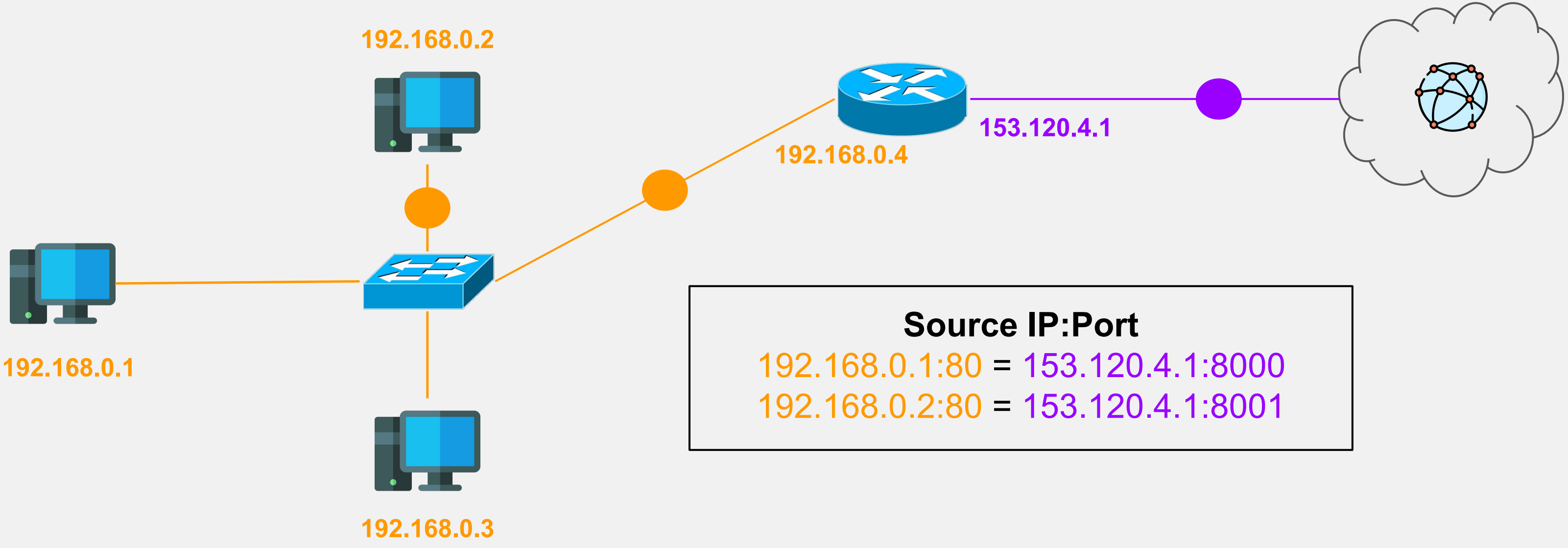
Port Address Translation (PAT)



Source IP:Port

192.168.0.1:80 = 153.120.4.1:8000

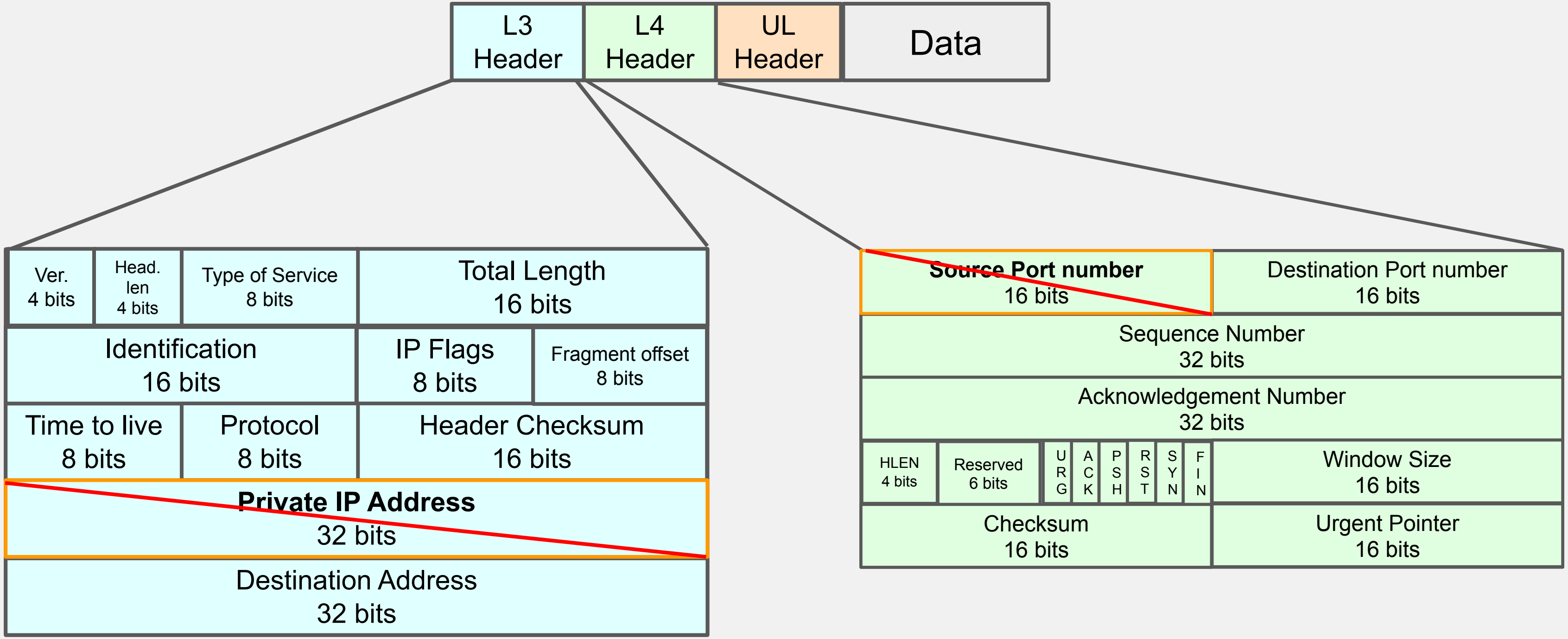
Port Address Translation (PAT)



Source IP:Port

192.168.0.1:80 = 153.120.4.1:8000
192.168.0.2:80 = 153.120.4.1:8001

PAT: Outgoing Traffic 1/2

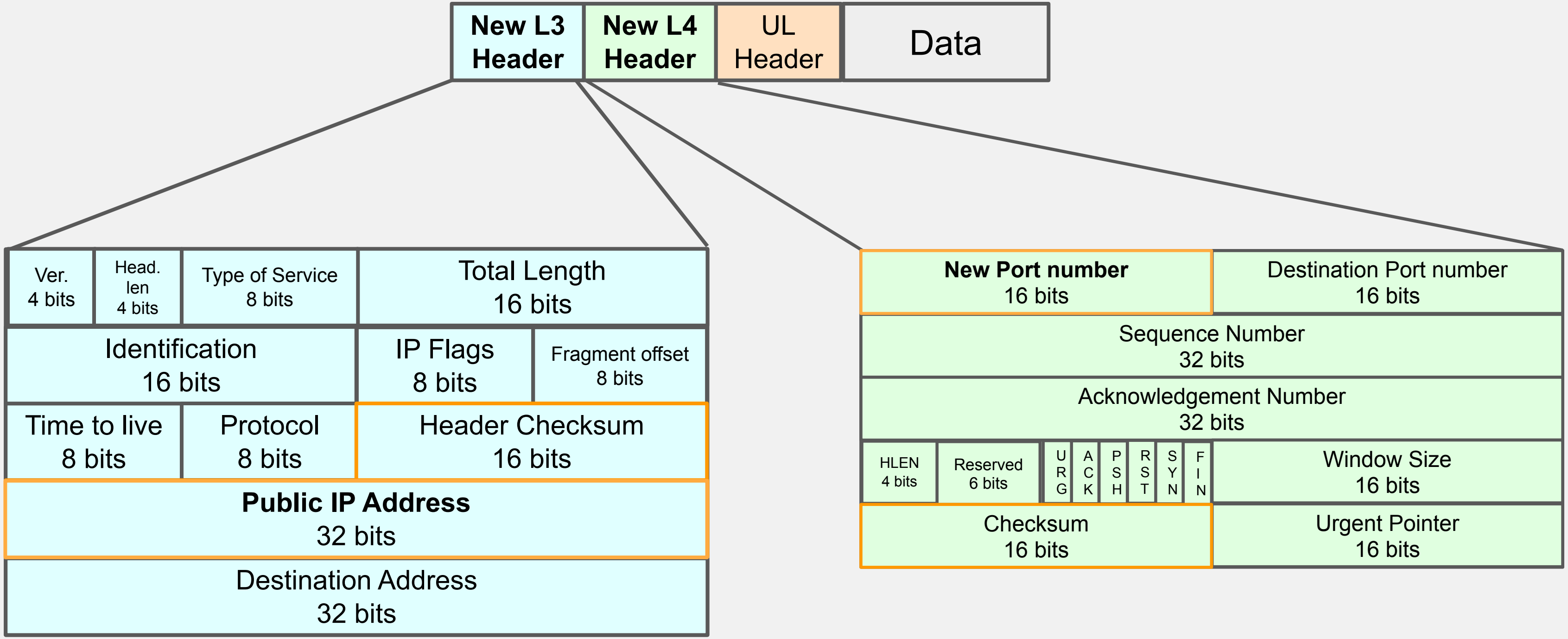


L3 Header	L4 Header	UL Header	Data

Ver. 4 bits	Head. len 4 bits	Type of Service 8 bits	Total Length 16 bits
Identification 16 bits		IP Flags 8 bits	Fragment offset 8 bits
Time to live 8 bits	Protocol 8 bits	Header Checksum 16 bits	
~~**Private IP Address**~~ ~~32 bits~~			
Destination Address 32 bits			

~~**Source Port number**~~ ~~16 bits~~								Destination Port number 16 bits
Sequence Number 32 bits								
Acknowledgement Number 32 bits								
HLEN 4 bits	Reserved 6 bits	URG	ACK	PSH	RST	SYN	FIN	Window Size 16 bits
Checksum 16 bits								Urgent Pointer 16 bits

PAT: Outgoing Traffic 2/2



New L3 Header | **New L4 Header** | UL Header | Data

Ver.
4 bits | Head. len
4 bits | Type of Service
8 bits | Total Length
16 bits

Identification
16 bits | IP Flags
8 bits | Fragment offset
8 bits

Time to live
8 bits | Protocol
8 bits | Header Checksum
16 bits

Public IP Address
32 bits

Destination Address
32 bits

New Port number
16 bits | Destination Port number
16 bits

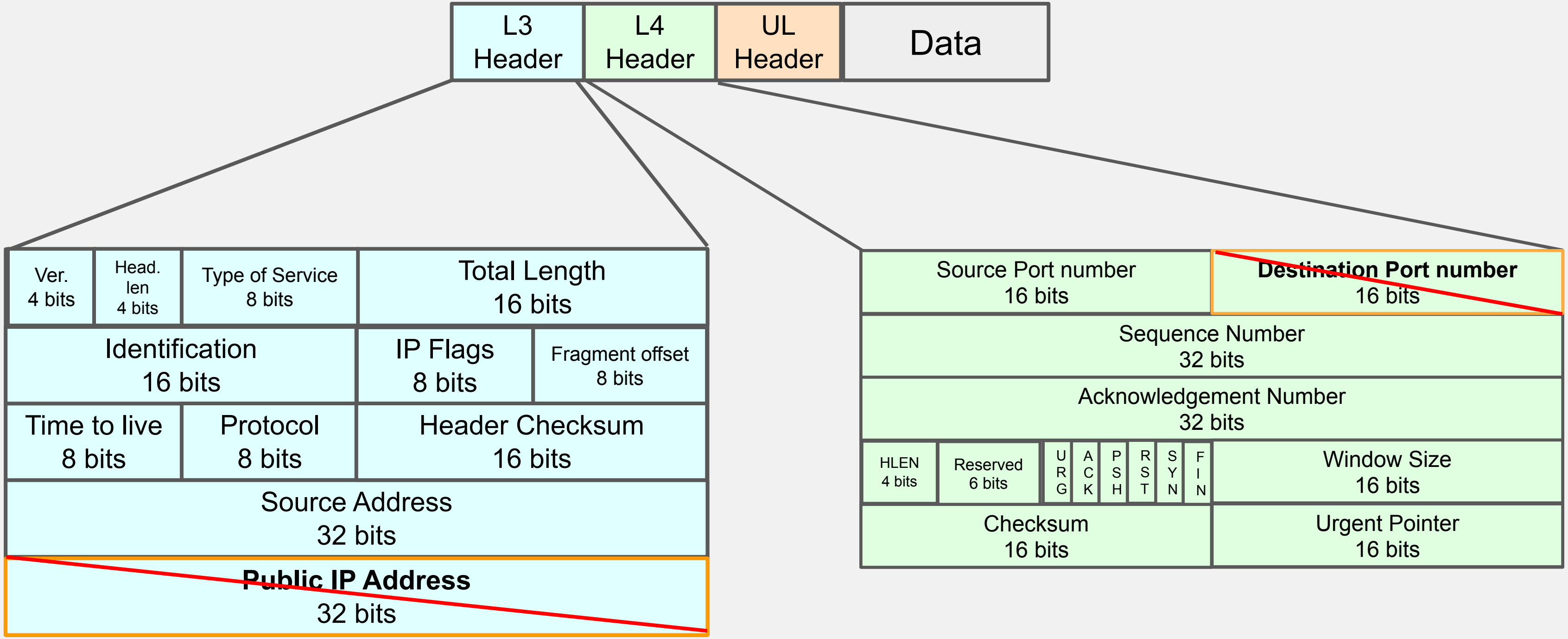
Sequence Number
32 bits

Acknowledgement Number
32 bits

HLEN
4 bits | Reserved
6 bits | URG | ACK | PSH | RST | SYN | FIN | Window Size
16 bits

Checksum
16 bits | Urgent Pointer
16 bits

PAT: Incoming Traffic 1/2



L3 Header | L4 Header | UL Header | Data

Ver. 4 bits | Head. len 4 bits | Type of Service 8 bits | Total Length 16 bits

Identification 16 bits | IP Flags 8 bits | Fragment offset 8 bits

Time to live 8 bits | Protocol 8 bits | Header Checksum 16 bits

Source Address 32 bits

~~**Public IP Address** 32 bits~~

Source Port number 16 bits | ~~**Destination Port number** 16 bits~~

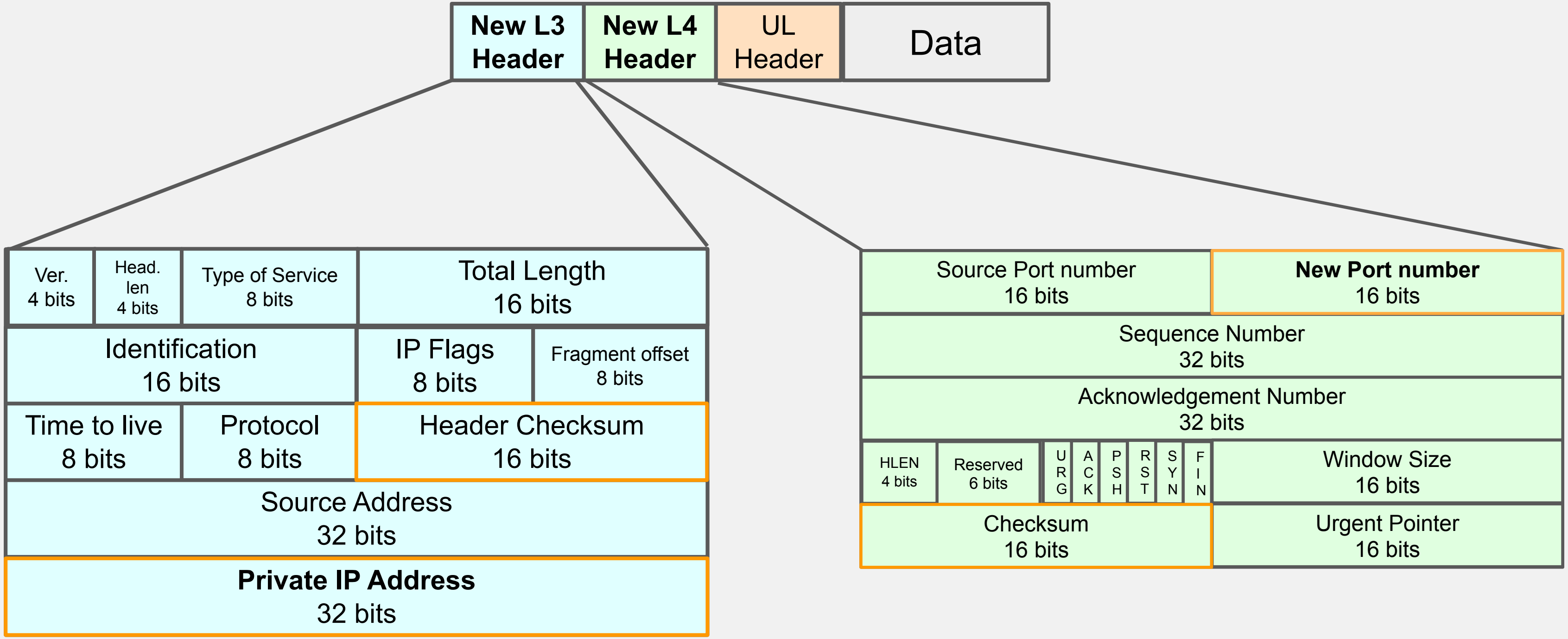
Sequence Number 32 bits

Acknowledgement Number 32 bits

HLEN 4 bits | Reserved 6 bits | URG | ACK | PSH | RST | SYN | FIN | Window Size 16 bits

Checksum 16 bits | Urgent Pointer 16 bits

PAT: Incoming Traffic 2/2



New L3 Header	**New L4 Header**	UL Header	Data

Ver. 4 bits	Head. len 4 bits	Type of Service 8 bits	Total Length 16 bits
Identification 16 bits		IP Flags 8 bits	Fragment offset 8 bits
Time to live 8 bits	Protocol 8 bits	Header Checksum 16 bits	
Source Address 32 bits			
Private IP Address 32 bits			

Source Port number 16 bits								**New Port number** 16 bits
Sequence Number 32 bits								
Acknowledgement Number 32 bits								
HLEN 4 bits	Reserved 6 bits	URG	ACK	PSH	RST	SYN	FIN	Window Size 16 bits
Checksum 16 bits								Urgent Pointer 16 bits

Port Address Translation (PAT)

PAT: Multiple private IPs can be linked to one public IP using port discrimination.

- Also known as **NAT Overload**.
- Most common NAT in the wild.

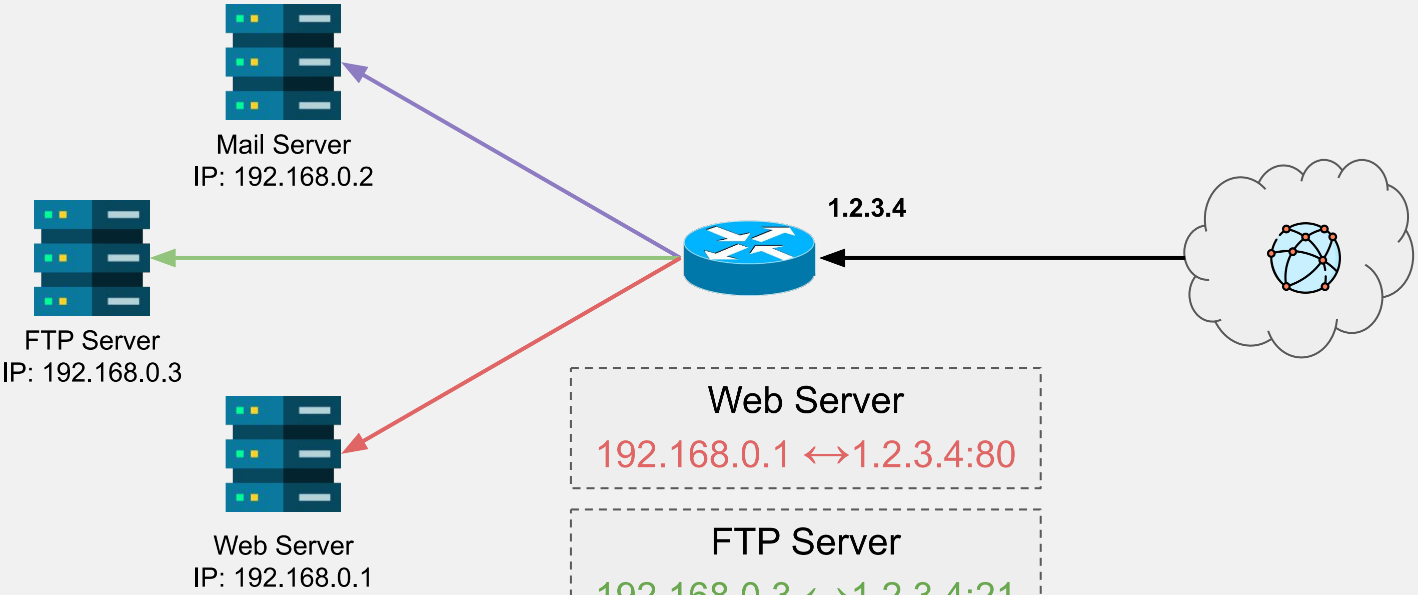
Advantages:

- Minimum public IP usage.

Disadvantage:

- Port numbers limited for a single public IP: maximum of 65535 connections.
- No unsolicited traffic from outside the network.
  - Problem for hosting servers.

Port Forwarding



Web Server

192.168.0.1 ↔1.2.3.4:80

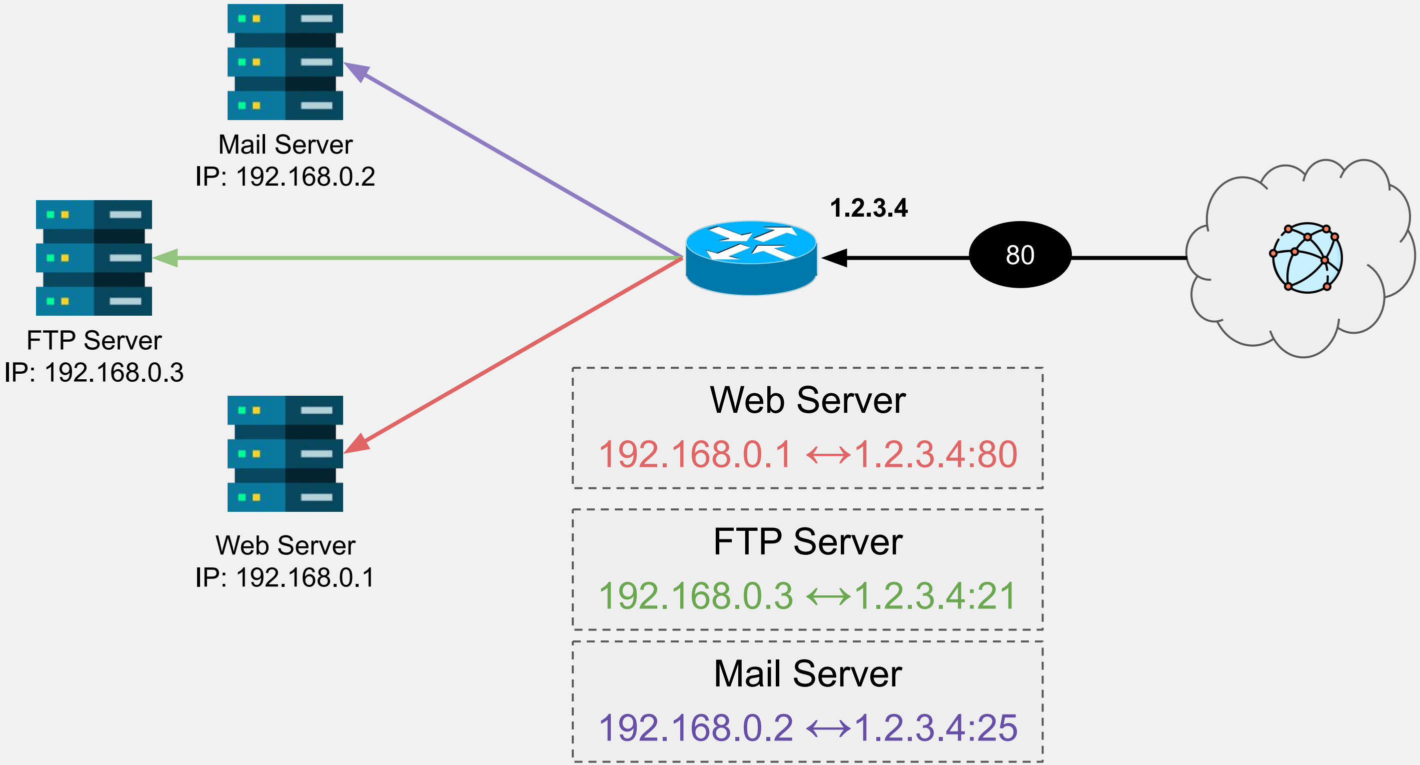
FTP Server

192.168.0.3 ↔1.2.3.4:21

Mail Server

192.168.0.2 ↔1.2.3.4:25

Port Forwarding



Mail Server
IP: 192.168.0.2

FTP Server
IP: 192.168.0.3

Web Server
IP: 192.168.0.1

1.2.3.4

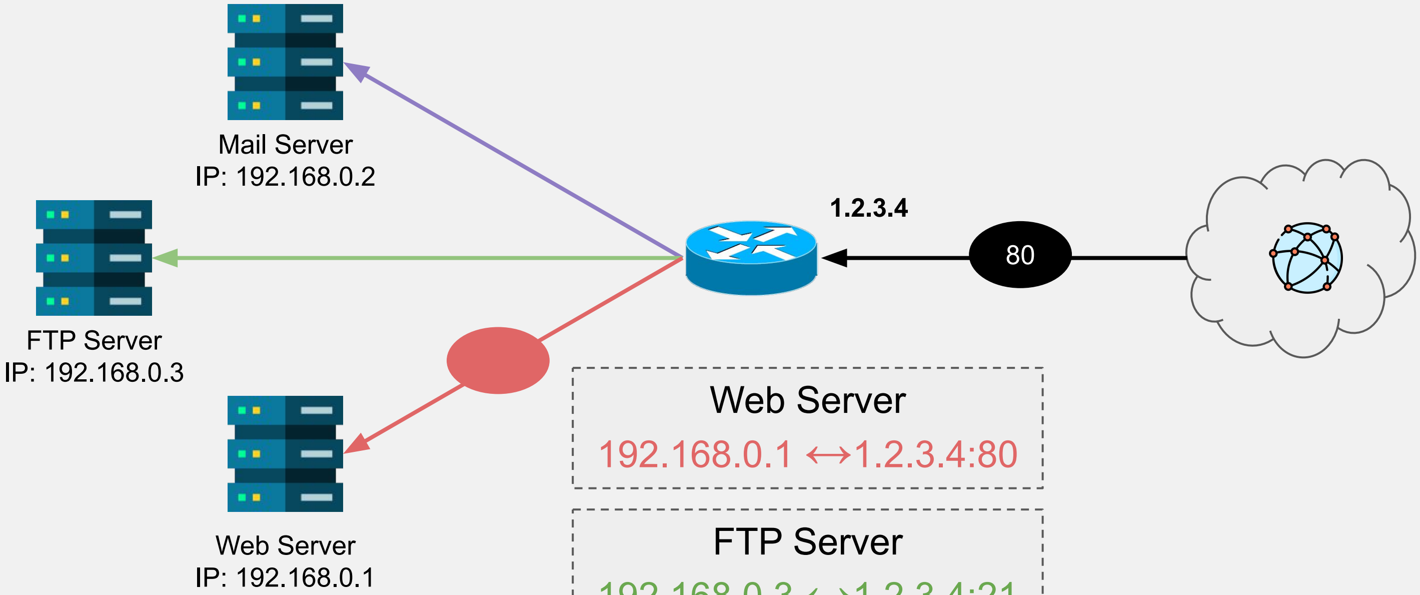
80

Web Server
192.168.0.1 ↔1.2.3.4:80

FTP Server
192.168.0.3 ↔1.2.3.4:21

Mail Server
192.168.0.2 ↔1.2.3.4:25

Port Forwarding



Mail Server
IP: 192.168.0.2

FTP Server
IP: 192.168.0.3

Web Server
IP: 192.168.0.1

1.2.3.4

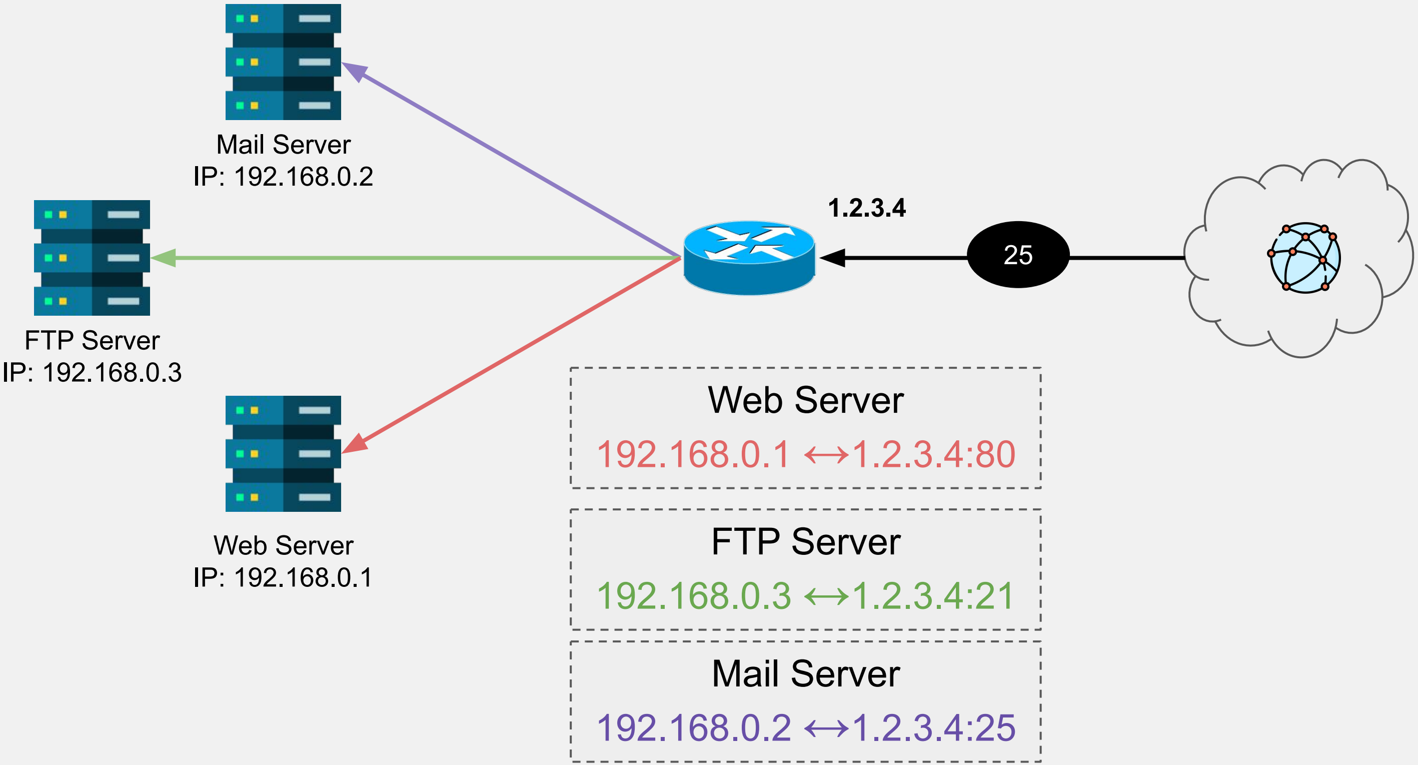
80

Web Server
192.168.0.1 ↔1.2.3.4:80

FTP Server
192.168.0.3 ↔1.2.3.4:21

Mail Server
192.168.0.2 ↔1.2.3.4:25

Port Forwarding



Web Server

192.168.0.1 ↔1.2.3.4:80

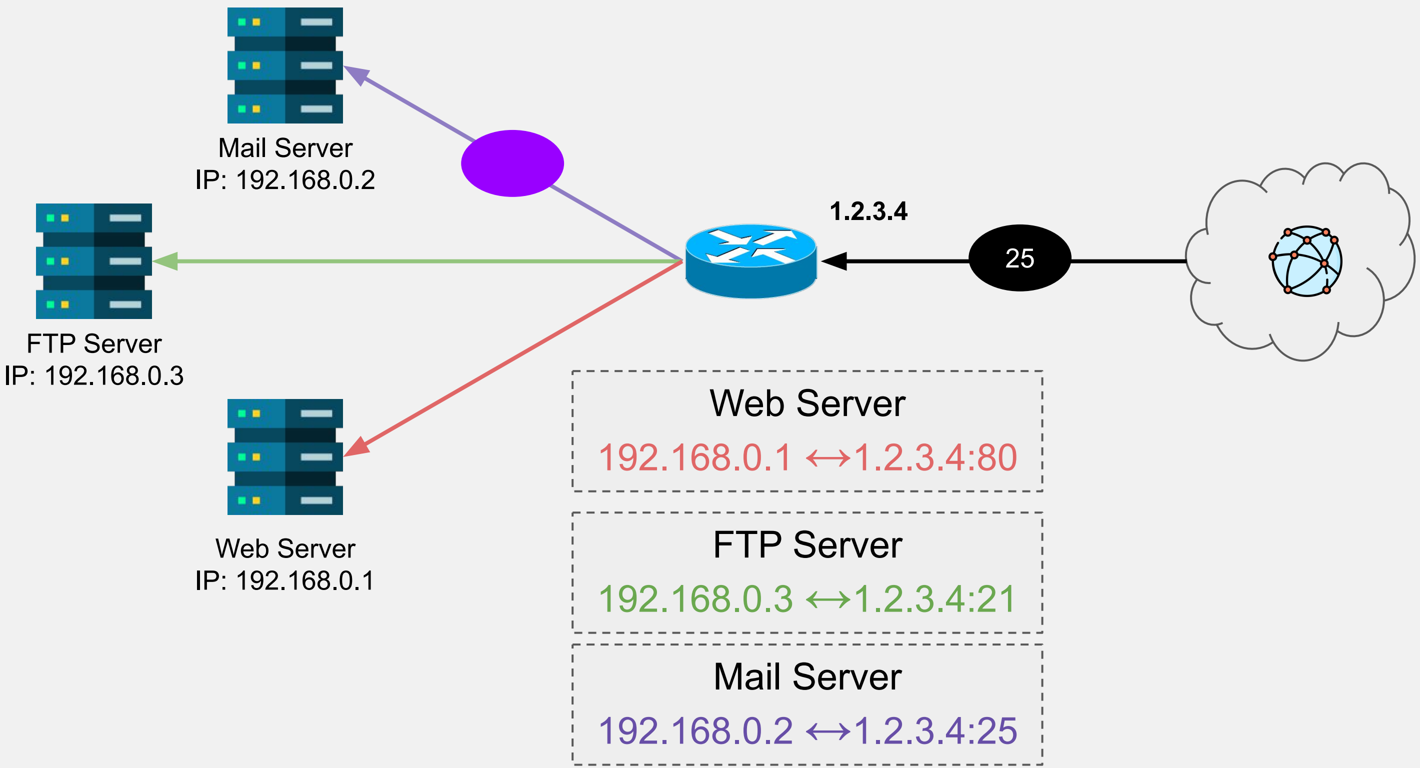
FTP Server

192.168.0.3 ↔1.2.3.4:21

Mail Server

192.168.0.2 ↔1.2.3.4:25

Port Forwarding



Web Server

192.168.0.1 ↔1.2.3.4:80

FTP Server

192.168.0.3 ↔1.2.3.4:21

Mail Server

192.168.0.2 ↔1.2.3.4:25

Port Forwarding

Port Forwarding: Single address - multiple ports dispatch to devices.

Advantage:

- Allows outbound connection to internal hosts.
  - Used for incoming traffic
- Controlled exposure (port not configured are blocked by default).

Disadvantage:

- A port can only be assigned to a single host.
  - E.g. two web servers on port 80 cannot be exposed using the same port.

A word on Acronyms

Online or inside documentations, you might come across *SNAT* and *DNAT*.

- They **do not** stand for Static and Dynamic!

SNAT: Source NAT

  - Includes every NAT that update the source address (outgoing traffic).

DNAT: Destination NAT

  - Includes every NAT that update the destination address (incoming traffic).

What NAT is not meant to be

If you ask internet or LLMs:

□ NAT is often mentioned as a security mechanism to isolate your private network…

IT IS NOT.

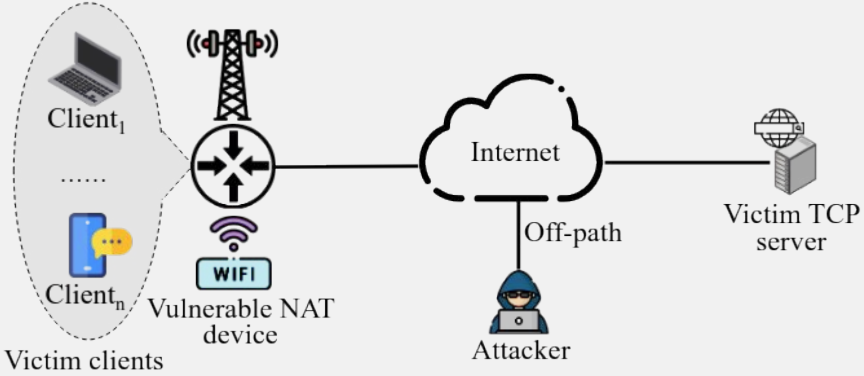
NAT was never designed to be used for security. The cloak over internal devices is a side effect, not a goal.

In security, there is no such thing as happy coincidences: if something has not been tested or designed for it, it will be flawed.

NAT Attacks

ReDAN: Remote DoS Attack against NAT (2025)

- **Objective:** Terminate a TCP connection between a NATed client and a server.
- **How:**
  - Send a TCP RST packet to a vulnerable NAT.
  - Spoof the NAT's IP to receive TCP packets from the server.
  - Send a RST to the server with the correct seq #.



Feng, Xuewei, et al. "ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks." NDSS 2025.

Some Out-of-Scope reading if you want

- NAT Slipstreaming (2020, 2021 for v2) by Samy Kamkar, Ben Seri, and Gregory Vishnipolsky.

Internet Protocol version 6 (IPv6)

IPv6

Here to solve the IPv4 IP exhaustion problem for good.

- IPv6:
  - **Address length:** 128 bits (16 bytes)
  - **Meaning:** 2^{128} addresses.

IPv6

2^{128}

IPv6

$$2^{128}$$

$$\Downarrow$$

340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6

$$2^{128}$$

⇩

340,282,366,920,938,463,463,374,607,431,768,211,456

In comparison, IPv4 with 2^{32}:

4,294,967,296

You can guess that some people still have PTSD from dealing with NAT…

IPv6 Address Notation

From RFC 5952:

- 8 words of 16 bits separated by ":"
- Each word represented as hexadecimal numbers.
- Consecutive words with null value can be abbreviated by "::"

2001:0db8:0000:009f:0000:0000:0000:000a

⇩

2001:0db8:0000:009f::000a

IPv6 Canonical Form

Also from RFC 5952, the canonical form involves:

- Representation in lowercase.
- To remove insignificant leading 0 of each word.
- "::" should no be used to shorten just one word.
- To avoid confusion, substitute only one sequence of zeros by ::
  - The longest run of 0 fields is shortened.

2001:0db8:0000:009f:0000:0000:0000:000a

⇩

2001:db8:0:9f::a

IPv6 Prefix

Like in IPv4, networks are identified using CIDR.

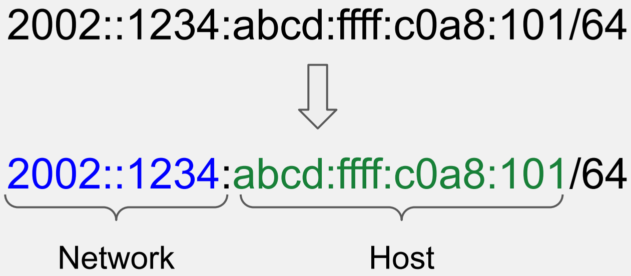
For instance:

2002::1234:abcd:ffff:c0a8:101/64

IPv6 Prefix

Like in IPv4, networks are identified using CIDR.

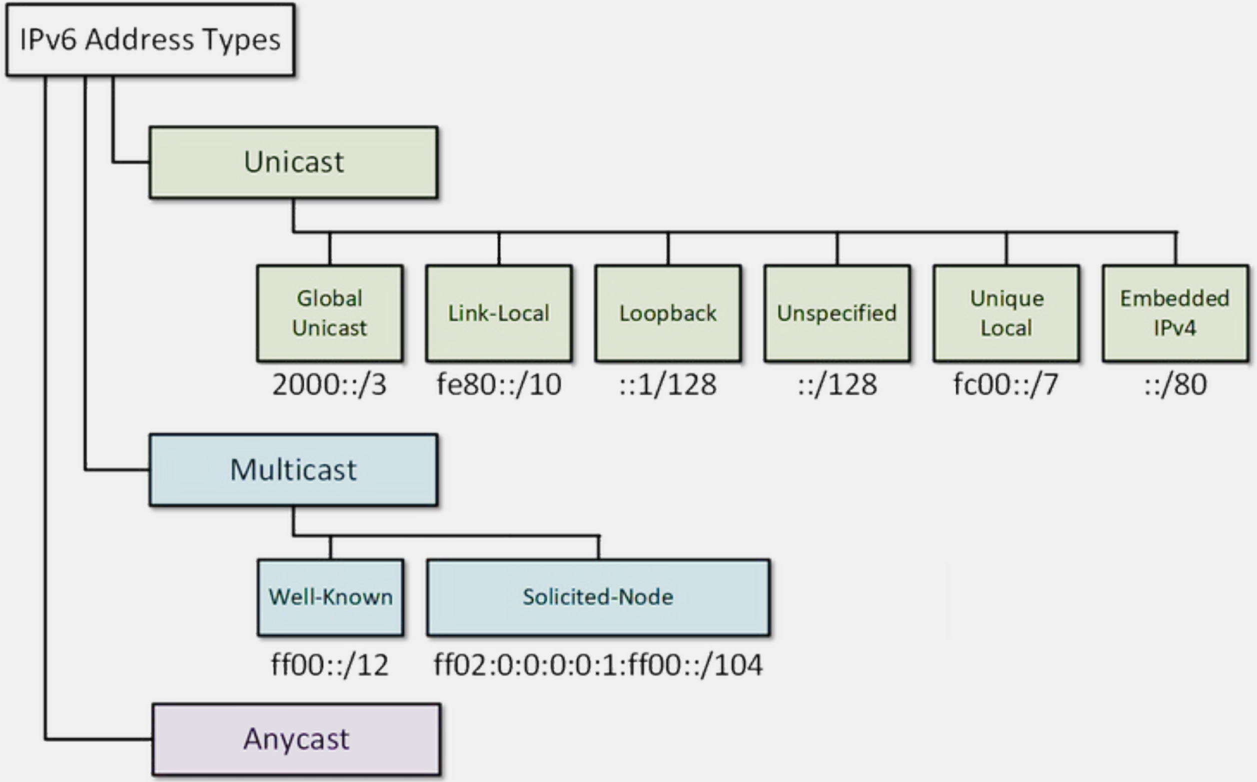
For instance:



2002::1234:abcd:ffff:c0a8:101/64

2002::1234:abcd:ffff:c0a8:101/64

IPv6 Addresses



IPv6 Address Types

Unicast

Global Unicast 2000::/3

Link-Local fe80::/10

Loopback ::1/128

Unspecified ::/128

Unique Local fc00::/7

Embedded IPv4 ::/80

Multicast

Well-Known ff00::/12

Solicited-Node ff02:0:0:0:0:1:ff00::/104

Anycast

IPv6 Unicast

Unicast: Packets sent to a unicast address are delivered to the interface configured with this specific IPv6 address.

- **one-to-one** communication.

IPv6 Unicast: Loopback

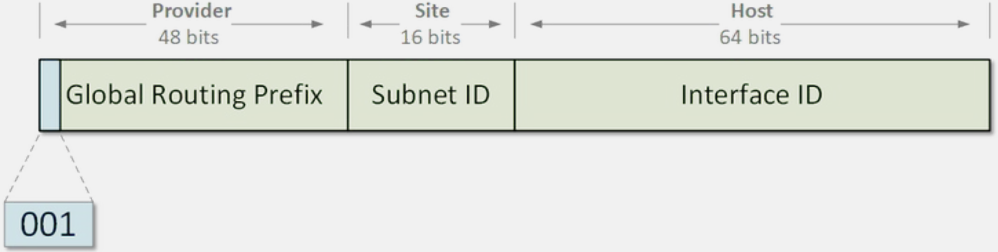
- **Address:** ::1/128
- Correspond to the localhost network, 127.0.0.0/8 in IPv4
  - remember : localhost is 127.0.0.1 in IPv4

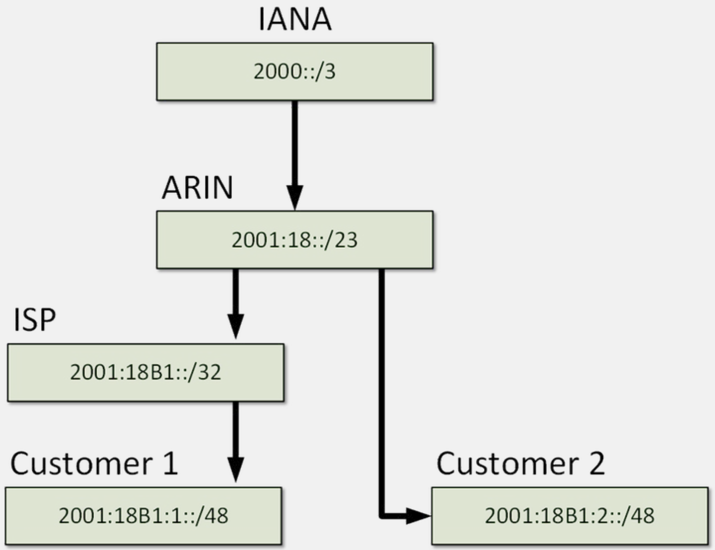
IPv6 Unicast: Link-Local

- **Prefix:** fe80::/10
- Correspond to 169.254.0.0/16 in IPv4
  - Used for Automatic Private IP Addressing.
  - In IPv4, this network is specific for devices without IP that cannot contact a DHCP server and do not have manual configuration.
  - In IPv6, a device with an IP also has a link-local address for LAN protocol (DHCPv6, NDP).
- Not forwarded by router, only used in the local network.

IPv6 Unicast: Global Unicast

- **Prefix:** 2000::/3
- Public addresses distributed by the IANA.





IPv6 Unicast: Unspecified

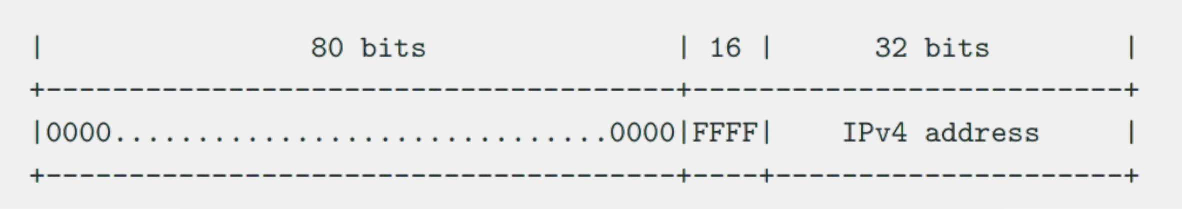
- **Address:** ::/128
- Like 0.0.0.0 in IPv4
- Means **“no address”**: Cannot be assigned to an interface or used as destination.
- Correspond to the device source when no unique address has been assigned yet.
  - Used within the LAN to define a unique address.
- In routing or sniffing context: means the default route/any interface like 0.0.0.0/0 in IPv4.

IPv6 Unicast: Unique Local

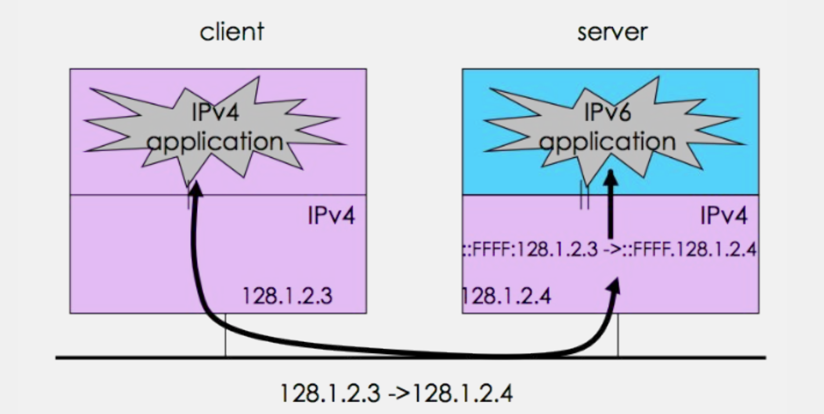
- **Prefix:** fc00::/7
- Used inside a private site/organization.
- Can be compared to private addresses.
- Routable only within private networks.
    - Unlike link local addresses that cannot be routed outside the link scope.

IPv6 Unicast: embedded IPv4

- IPv4 can be represented in IPv6.
- Here for applications compatibility without the need to rewrite the app itself.



```
|                80 bits               | 16 |      32 bits        |
+--------------------------------------+--------------------------+
|0000..............................0000|FFFF|    IPv4 address     |
+--------------------------------------+----+---------------------+
```



IPv6 Multicast

Multicast: Packets sent to a multicast address are delivered to all interfaces identified by that address.

- **one-to-many** communication.
- Not a broadcast.
  - IPv4 only devices will not understand it.
  - Device specific.

IPv6 Multicast: Well-Known 1/2

- **Prefix:** ff00::/12
    - First byte will always start with ff0.
- Not a broadcast
    - All devices will not received packets, only the concerned ones.

IPv6 Multicast: Well-Known 2/2

- **ff02::1** All Nodes Address (link-local scope)
- **ff02::2** All Routers Address
- **ff02::5** OSPFIGP
- **ff02::6** OSPFIGP Designated Routers
- **ff02::9** RIP Routers
- **ff02::fb** mDNSv6
- **ff02::1:2** All-dhcp-agents
- **ff02::1:ffxx:xxxx** Solicited-Node Address
- **ff05::1:3** All-dhcp-servers (site-local scope)

IPv6 Anycast

Anycast: Packets sent to an anycast address are delivered to the "closest" interface identified by that address. "Closest" typically means the one with the best routing metric.

- **one-to-closest** communication.

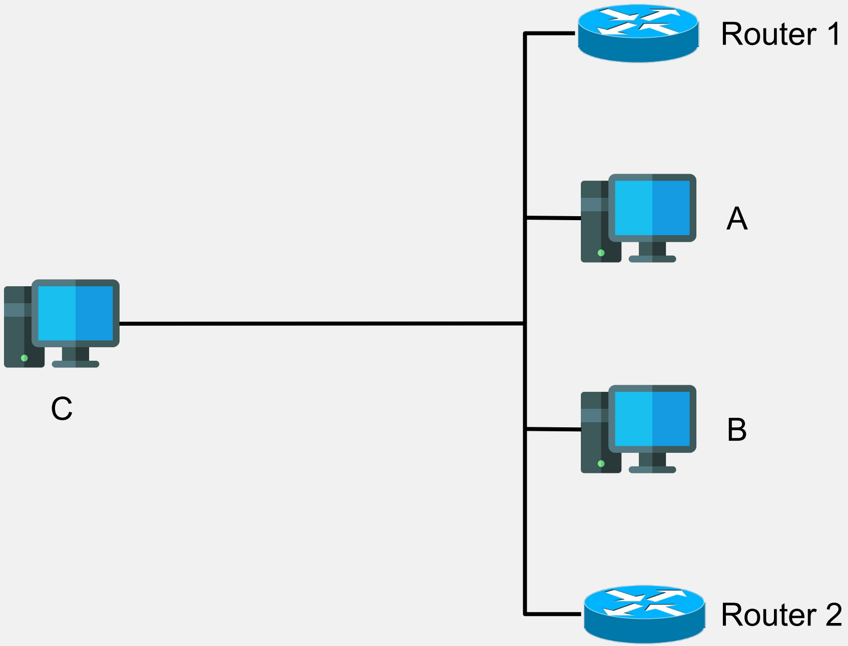
Some IPv6 protocols:
NDP and DAD

Neighbor Discovery Protocol (NDP) 1/3

- Layer 3 protocol used by IPv6 for:
  - MAC address discovery (like ARP in IPv4).
  - Router discovery and redirection.
  - Prefix/Parameter Discovery & Address Autoconfiguration.
- Uses ICMPv6 messages:
  - Router Solicitation (RS)
  - Router Advertisement (RA)
  - Neighbor Solicitation (NS)
  - Neighbor Advertisement (NA)
  - Redirect

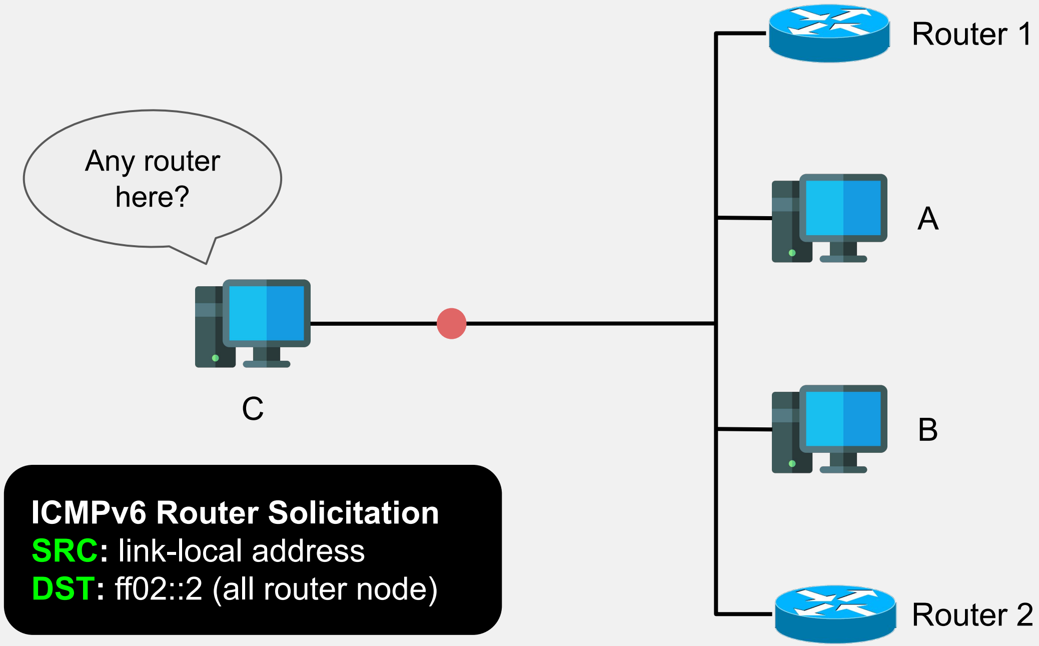
Neighbor Discovery Protocol (NDP) 2/3

Router Discovery



Neighbor Discovery Protocol (NDP) 2/3

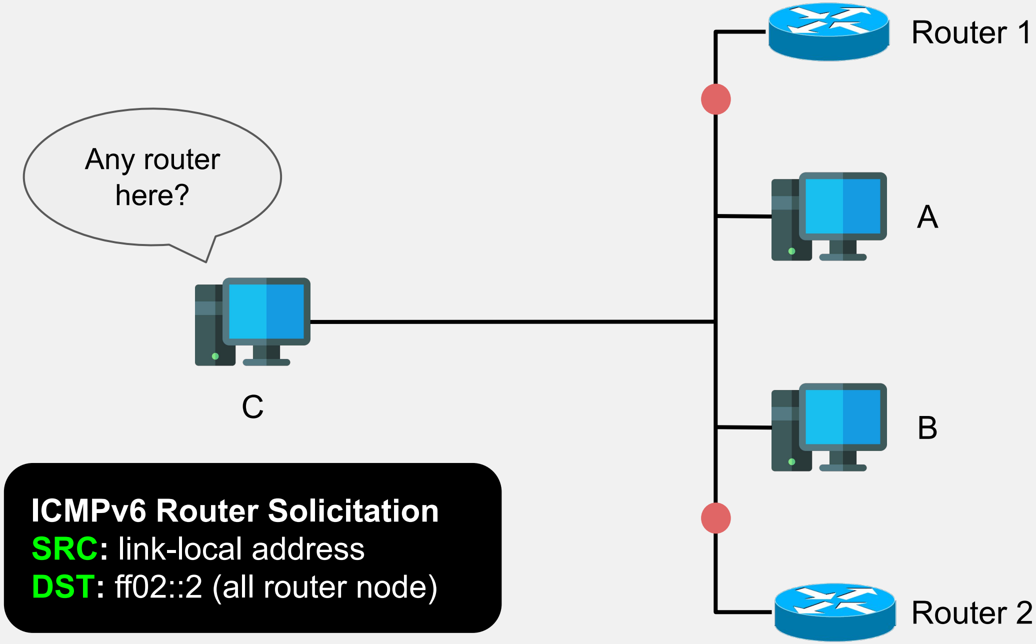
Router Discovery



ICMPv6 Router Solicitation
SRC: link-local address
DST: ff02::2 (all router node)

Neighbor Discovery Protocol (NDP) 2/3

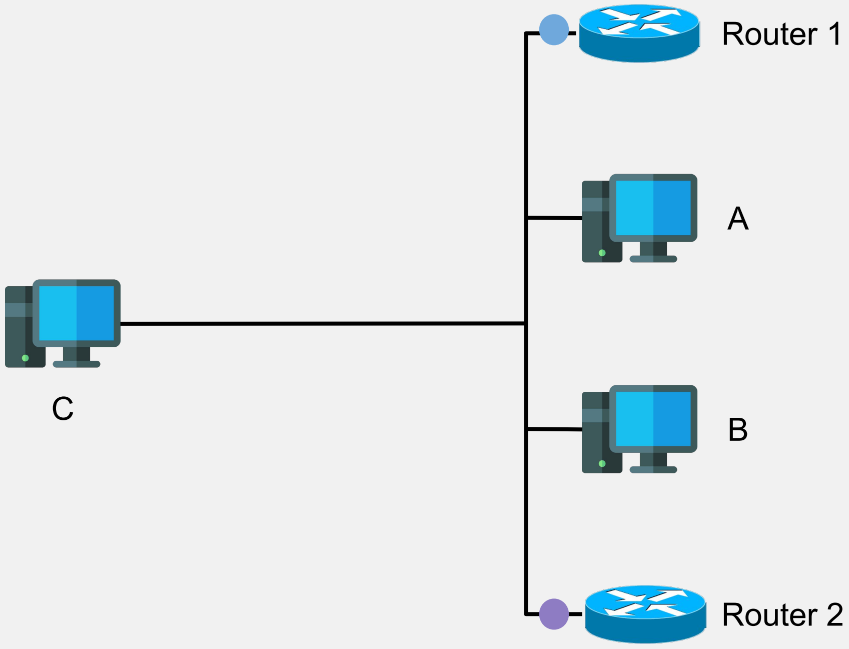
Router Discovery



ICMPv6 Router Solicitation
SRC: link-local address
DST: ff02::2 (all router node)

Neighbor Discovery Protocol (NDP) 2/3

Router Discovery



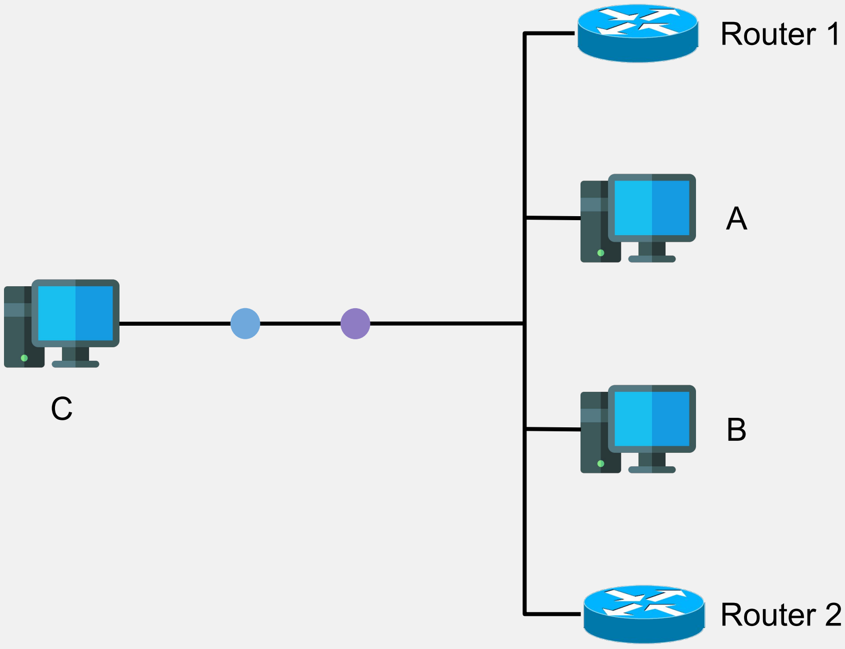
ICMPv6 Router Advertisement
SRC: router link-local address
DST: C's link-local

ICMPv6 Router Advertisement
SRC: router link-local address
DST: C's link-local

Neighbor Discovery Protocol (NDP) 2/3

Router Discovery

Content:
- IPv6 Prefix
- Address configuration info
- Default gateway info
- Hop limit, MTU

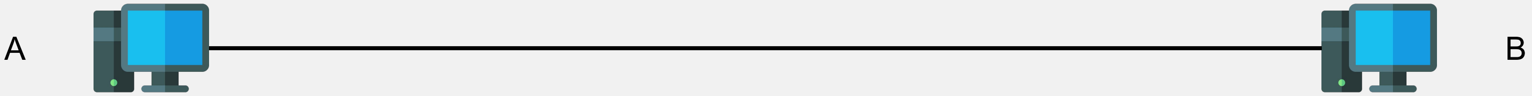


ICMPv6 Router Advertisement
SRC: router link-local address
DST: C's link-local

ICMPv6 Router Advertisement
SRC: router link-local address
DST: C's link-local

Neighbor Discovery Protocol (NDP) 3/3

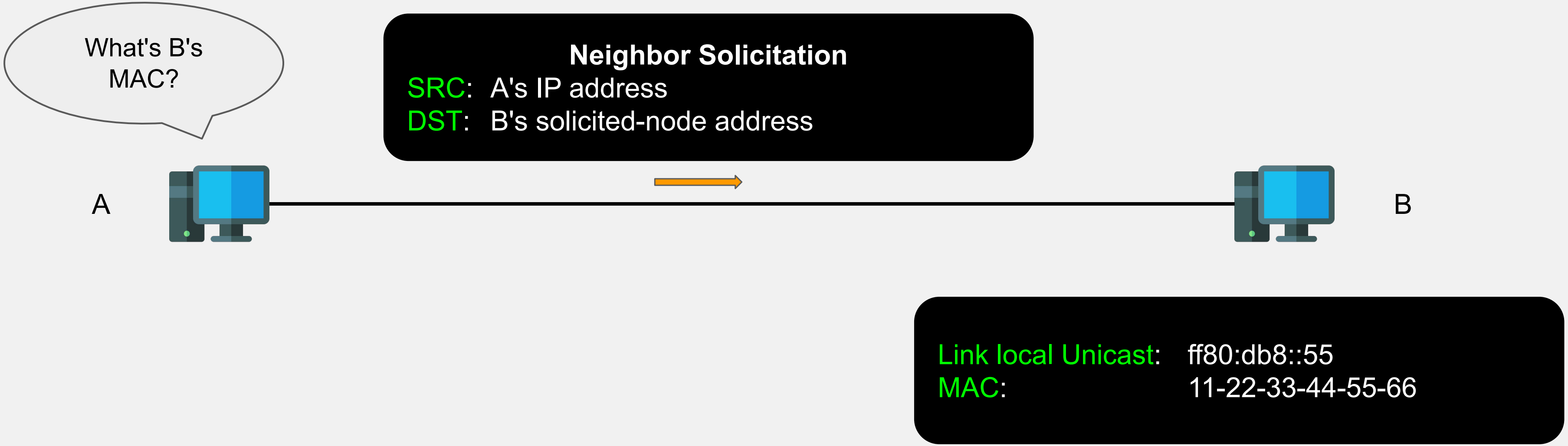
Neighbor Discovery



Link local Unicast: ff80:db8::55
MAC: 11-22-33-44-55-66

Neighbor Discovery Protocol (NDP) 3/3

Neighbor Discovery



Neighbor Solicitation

SRC: A's IP address
DST: B's solicited-node address

Link local Unicast: ff80:db8::55
MAC: 11-22-33-44-55-66

IPv6 Multicast: Solicited-Node 1/2

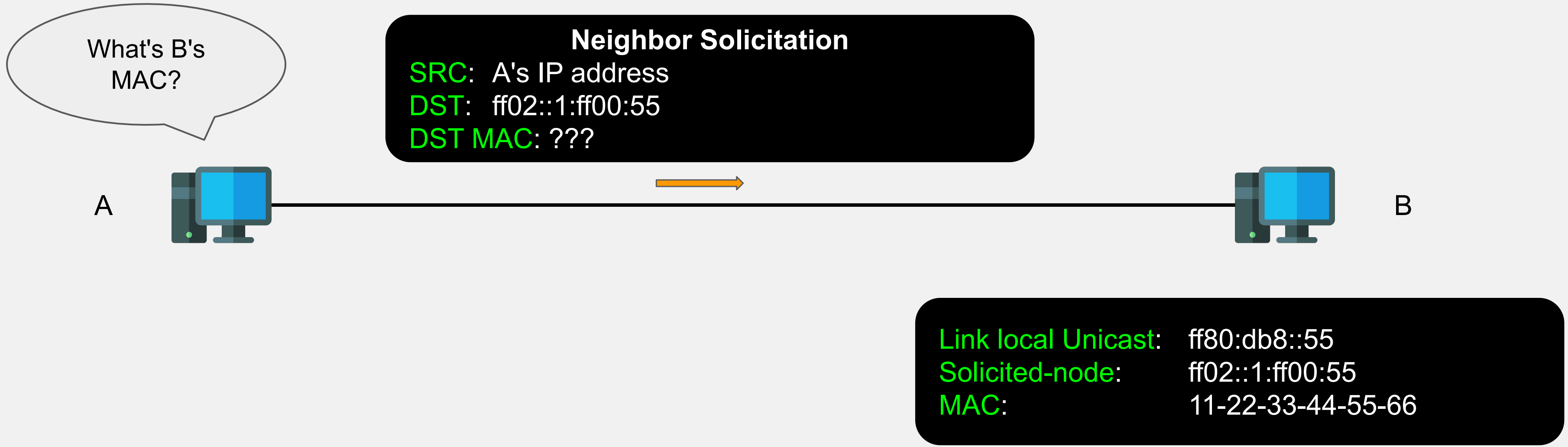
- **Prefix:** ff02::1:ff00:0/104
- Forged from the unicast address by keeping the **least significant 24 bits**.
- Here for efficient packet on the fly triage.

IPv6 Multicast: Solicited-Node 2/2

- **Prefix:** ff02::1:ff00:0/104
- In our exemple:
  - B's unicast: ff80:db8::55
- By keeping the least-significant 24 bits of the unicast address and adding the prefix we get:
  - ff02::1:ff00:55 as our solicited-node address.

Neighbor Discovery Protocol (NDP) 3/3

Neighbor Discovery

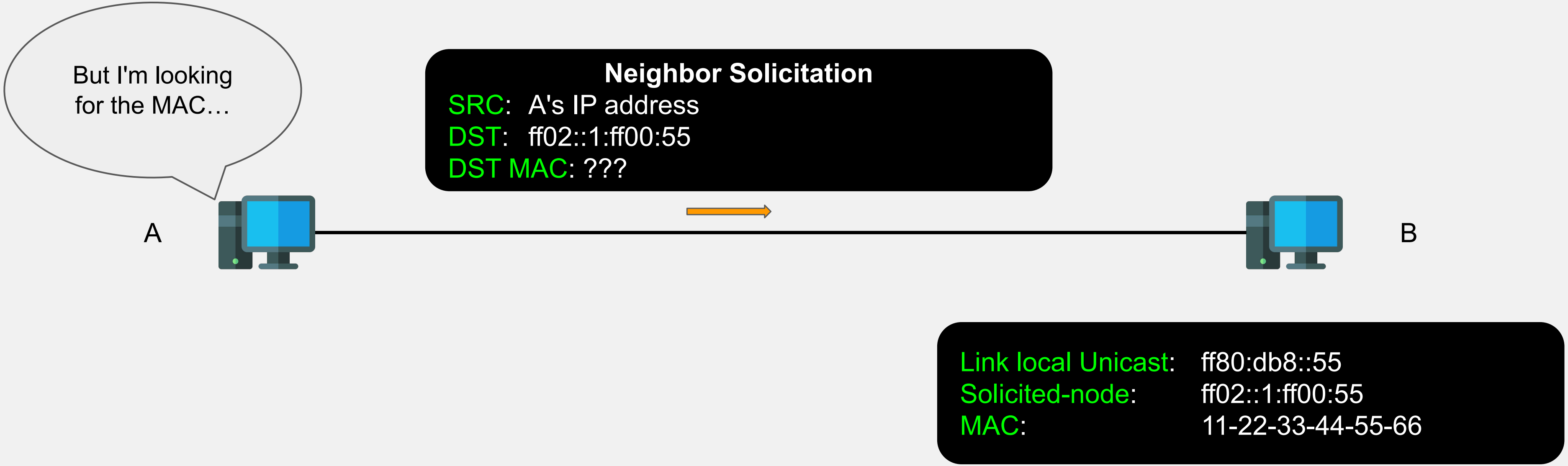


Neighbor Solicitation
SRC: A's IP address
DST: ff02::1:ff00:55
DST MAC: ???

Link local Unicast: ff80:db8::55
Solicited-node: ff02::1:ff00:55
MAC: 11-22-33-44-55-66

Neighbor Discovery Protocol (NDP) 3/3

Neighbor Discovery



But I'm looking for the MAC…

Neighbor Solicitation
SRC: A's IP address
DST: ff02::1:ff00:55
DST MAC: ???

Link local Unicast:	ff80:db8::55
Solicited-node:	ff02::1:ff00:55
MAC:	11-22-33-44-55-66

Solicited-Node MAC address 1/2

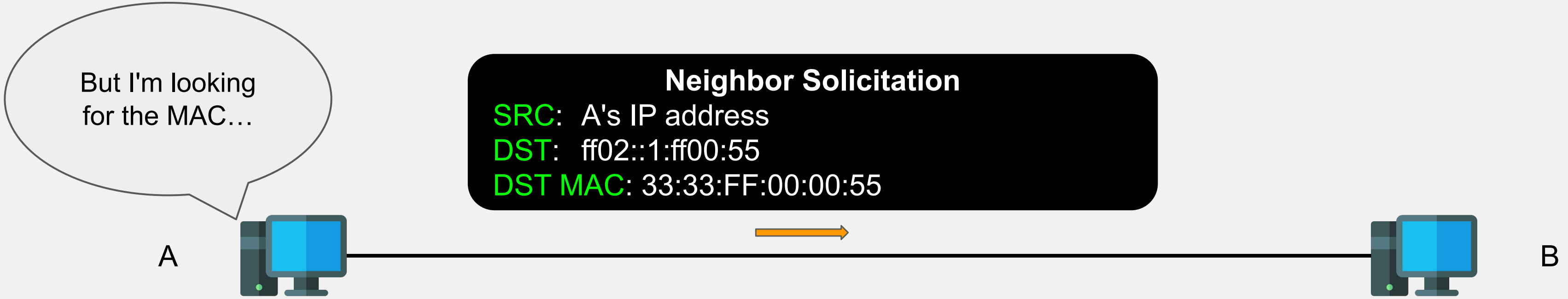
- We take the Solicited-Node Multicast address' **last 24 bits**.
  - And we prefix them with 33:33:FF:
- Efficient filter using the Network Interface Controller (NIC) by directly looking at the MAC address without sending the packet to the upper layers for fast discard.

Solicited-Node MAC address 2/2

- In our example, the solicited-node address is: ff02::1:ff00:55
- The resulting solicited-node MAC address is:
    - 33:33:FF:00:00:55

Neighbor Discovery Protocol (NDP) 3/3

Neighbor Discovery

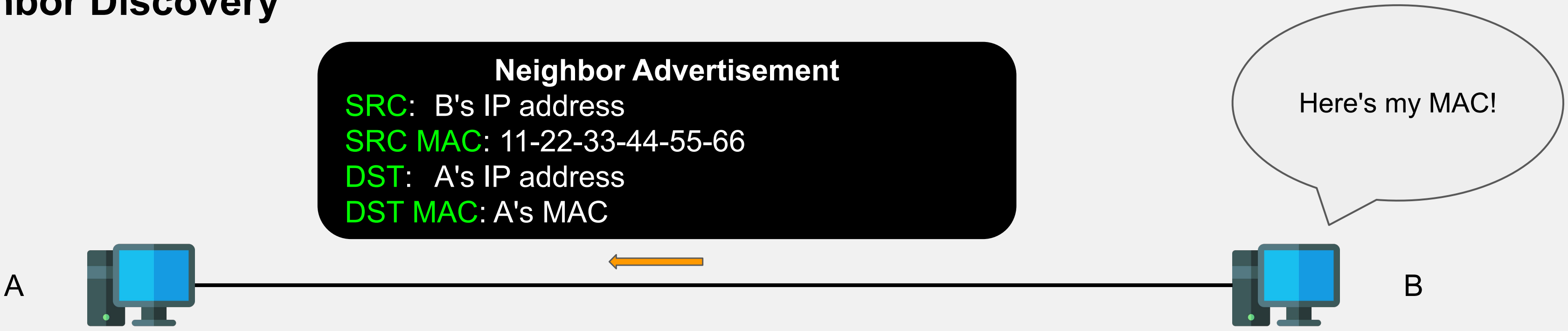


Neighbor Solicitation
SRC: A's IP address
DST: ff02::1:ff00:55
DST MAC: 33:33:FF:00:00:55

Link local Unicast:	ff80:db8::55
Solicited-node:	ff02::1:ff00:55
MAC:	11-22-33-44-55-66

Neighbor Discovery Protocol (NDP) 3/3

Neighbor Discovery



Neighbor Advertisement

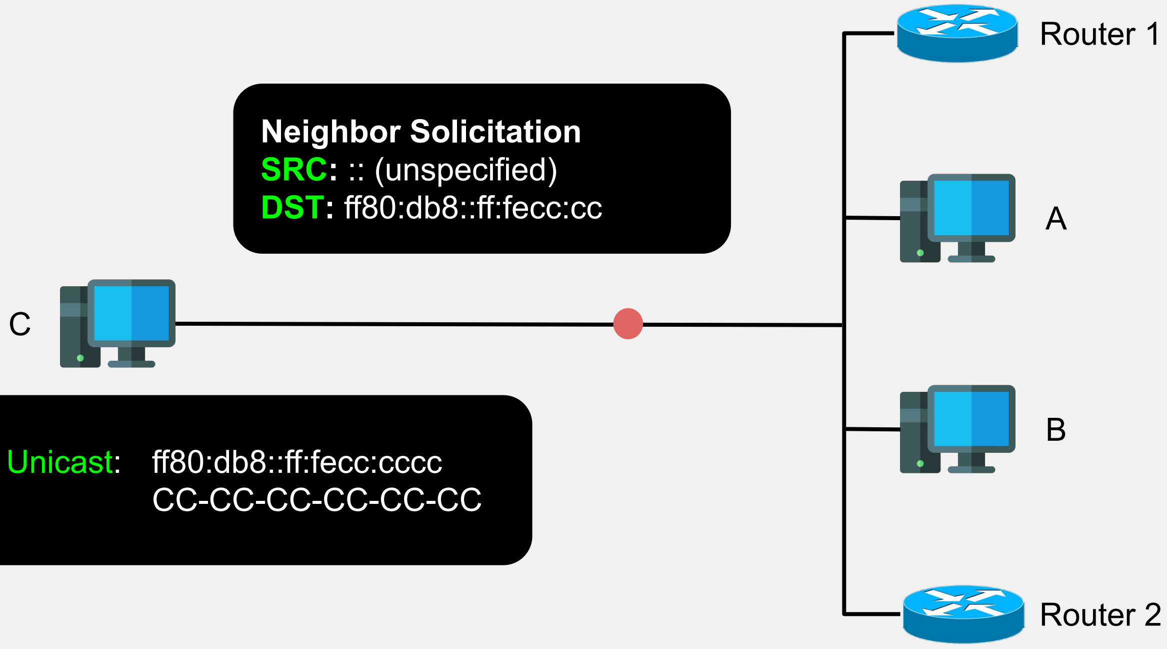
SRC: B's IP address
SRC MAC: 11-22-33-44-55-66
DST: A's IP address
DST MAC: A's MAC

Link local Unicast:	ff80:db8::55
Solicited-node:	ff02::1:ff00:55
MAC:	11-22-33-44-55-66

Duplicate Address Detection (DAD)

- Protocol used to assure that a local link address is unique in the local scope.
  - Need to be perform before using your link local address.
- Uses the Neighbor Solicitation and Advertisement messages.
- When a device when to join a local network, it generates a link local address based on its MAC address and the link-local prefix.

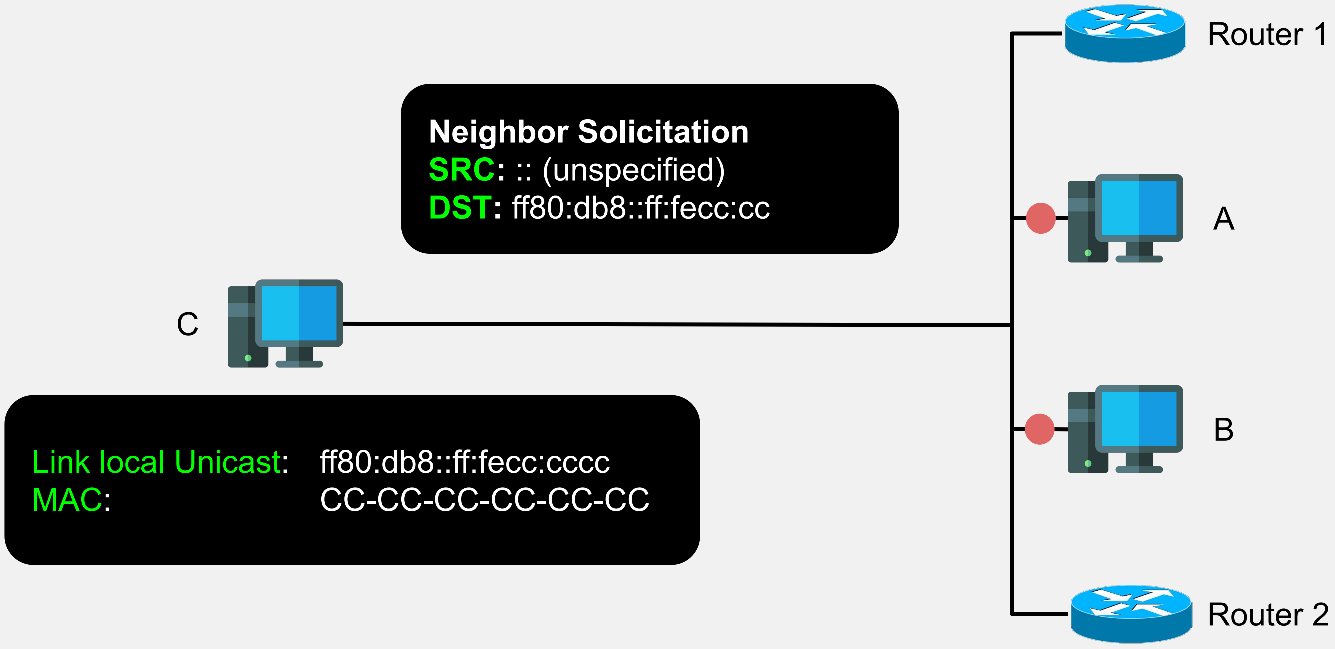
Duplicate Address Detection (DAD)



Neighbor Solicitation
SRC: :: (unspecified)
DST: ff80:db8::ff:fecc:cc

Link local Unicast: ff80:db8::ff:fecc:cccc
MAC: CC-CC-CC-CC-CC-CC

Duplicate Address Detection (DAD)

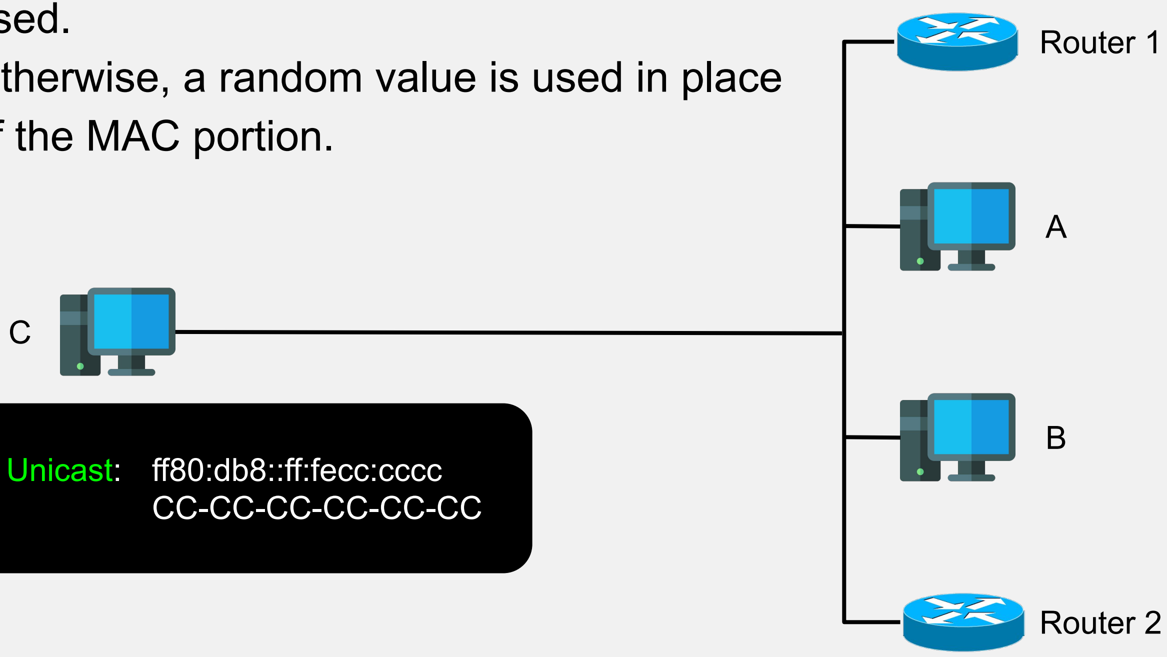


Neighbor Solicitation
SRC: :: (unspecified)
DST: ff80:db8::ff:fecc:cc

Link local Unicast: ff80:db8::ff:fecc:cccc
MAC: CC-CC-CC-CC-CC-CC

Duplicate Address Detection (DAD)

- If no one replies, the link-local address if used.
- Otherwise, a random value is used in place of the MAC portion.



Link local Unicast:	ff80:db8::ff:fecc:cccc
MAC:	CC-CC-CC-CC-CC-CC

Security in IPv6

- Remote attacks are difficult:
  - Large number of address to scan.
  - No broadcast address.
- On local network:
  - Neighbor Discovery is not secure (that is why SEND, Secure Neighbor Discovery, exists).
  - And what about DAD? -> DoS attacks.
  - Router advertisement? -> MitM.

Security in IPv6

- Remote attacks are difficult:
  - Large number of address to scan.
  - No broadcast address.
- On local network:
  - Neighbor Discovery is not secure (that is why SEND, Secure Neighbor Discovery, exists).
    - MitM
  - And what about DAD?
    - DoS
  - Router advertisement?
    - MitM

More IPv6 compatible protocols

- DHCPv6
- ICMPv6
- DNS64
- SLAAC (stateless address autoconfiguration)
- And much more…

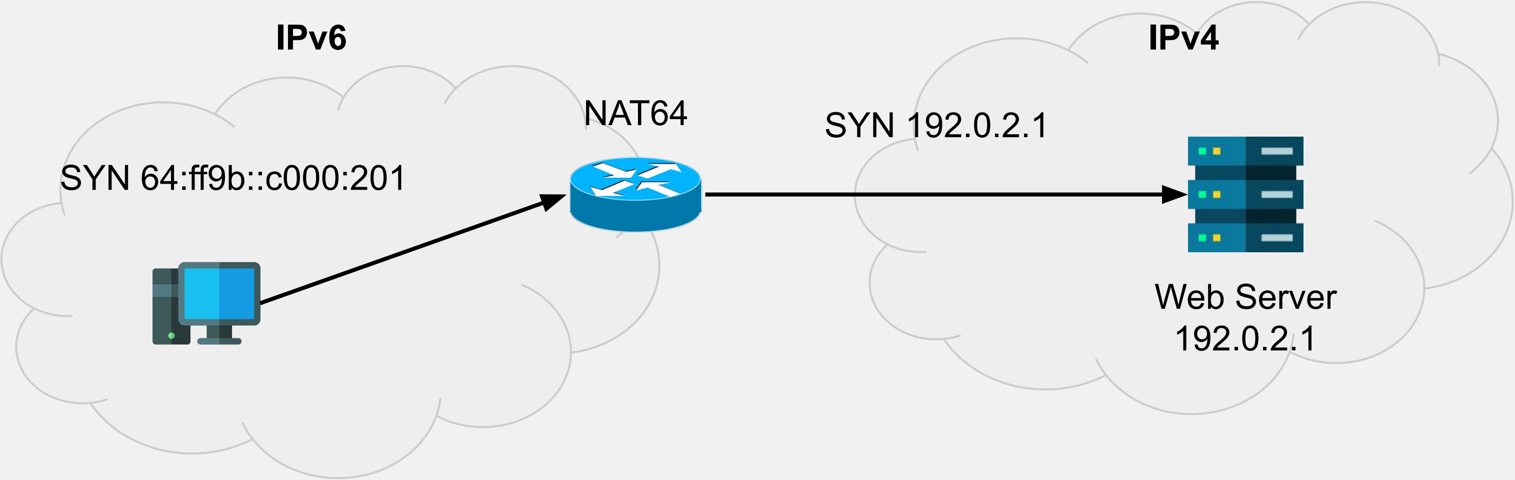
More IPv6 compatible protocols

- DHCPv6
- ICMPv6
- DNS64
- SLAAC (stateless address autoconfiguration)
- And much more…
  - Such as **NAT64!** *(there is no escape)*

Bonus: NAT64

NAT64

- Here to use IPv6 with IPv4 only devices.
  - Embedded IPv4 only work if the device knows IPv6 (App abstraction not Network)



IPv6

IPv4

NAT64

SYN 192.0.2.1

SYN 64:ff9b::c000:201

Web Server
192.0.2.1

Resources and Acknowledgements

- *Computer Networking: A Top-down Approach* by James F. Kurose, Keith W. Ross
- Previous material from Mathieu Goessens.