CSCI 466: Networks

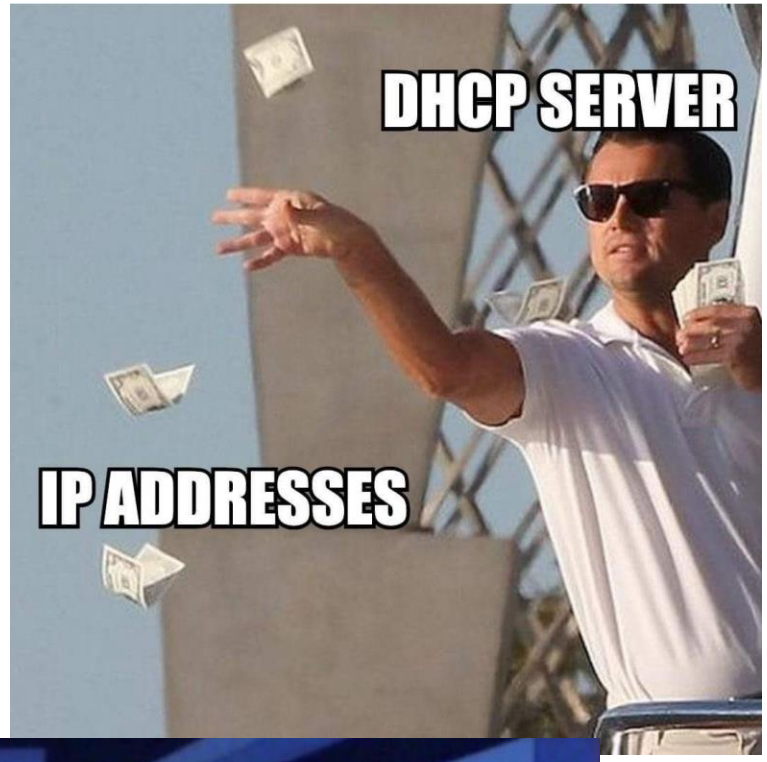
More on IP Addressing, NAT, Subnets + Routing

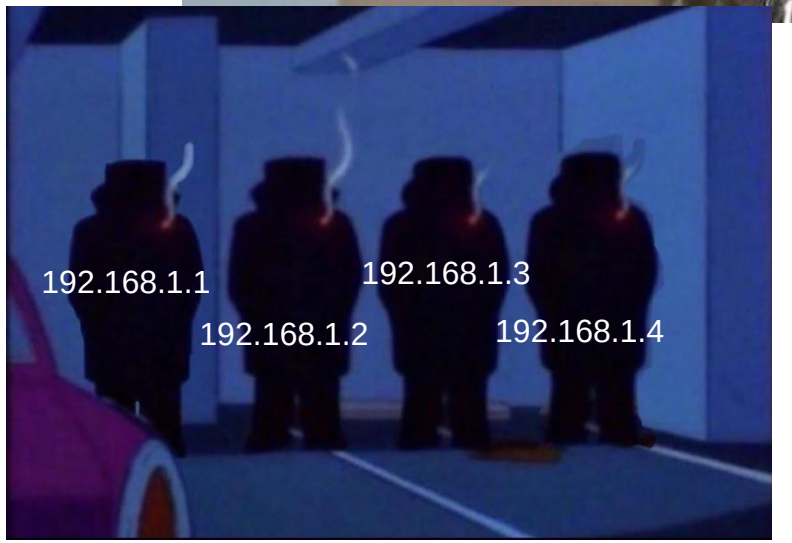
Reese Pearsall

Fall 2024

Announcements

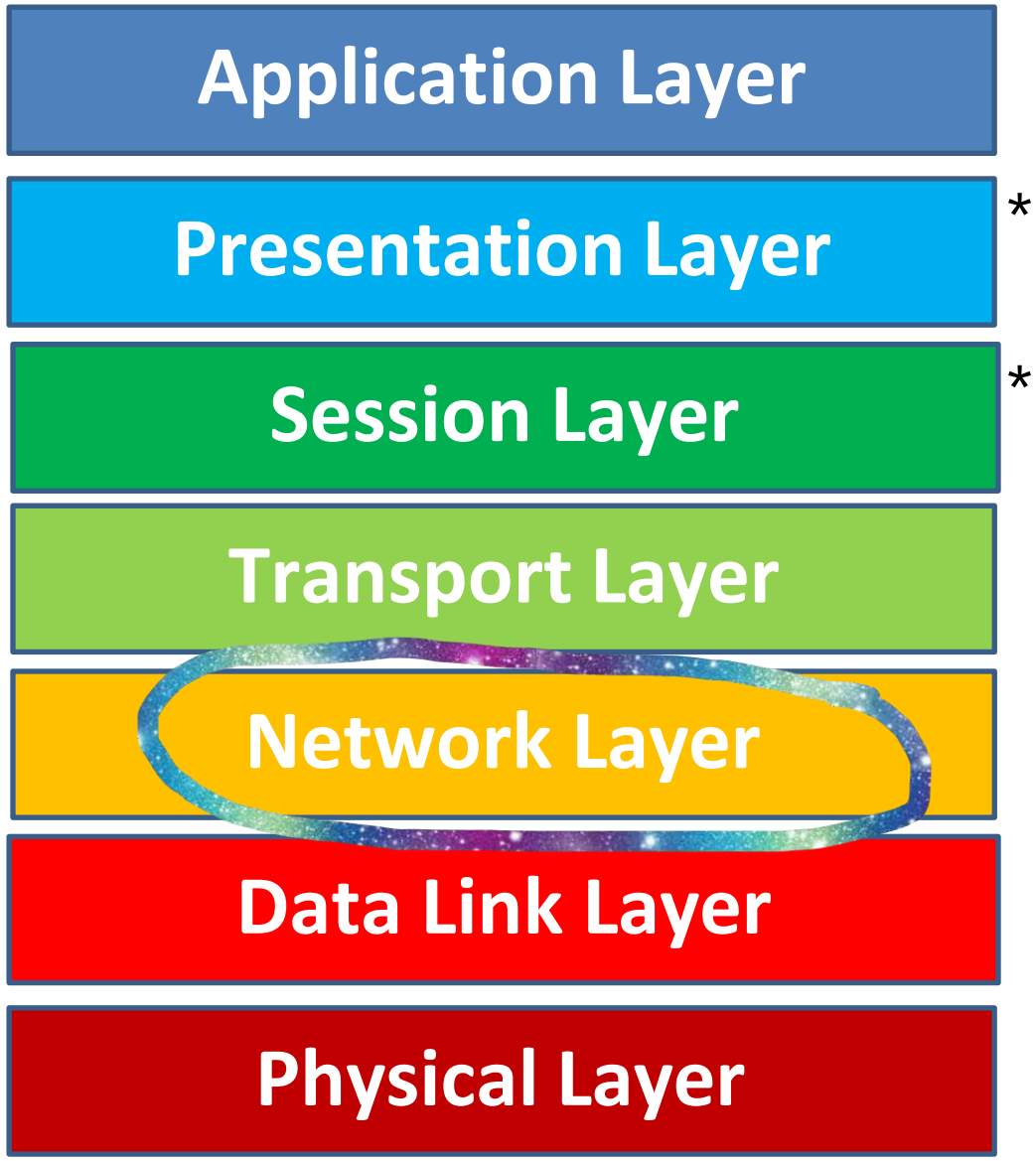
PA2 due on Sunday (10/13)





MSU Video Game Development club has their first meeting **tonight** at 5PM in SUB 235

OSI Model



Application Layer

Messages from Network Applications

Physical Layer

Bits being transmitted over a medium

**In the textbook, they condense it to a 5-layer model, but 7 layers is what is most used*

IP Address: 32 bit (4 byte) **dotted decimal** number assigned to interfaces on hosts and routers

IP addresses are heavily used in the routing process and ensuring packets get sent to the correct location

193.32.216.9

An IP address has two parts: the **network bits** and **host bits**

(area code) *(phone number)*

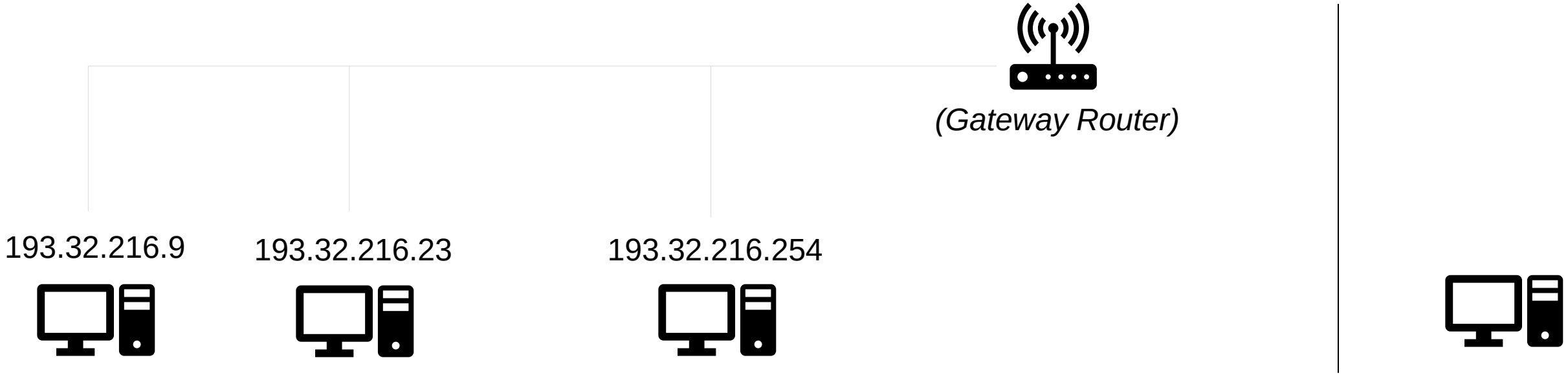
IP Address: 32 bit (4 byte) **dotted decimal** number assigned to interfaces on hosts and routers

IP addresses are heavily used in the routing process and ensuring packets get sent to the correct location

193.32.216.9

An IP address has two parts: the **network bits** and **host bits**

(area code) *(phone number)*



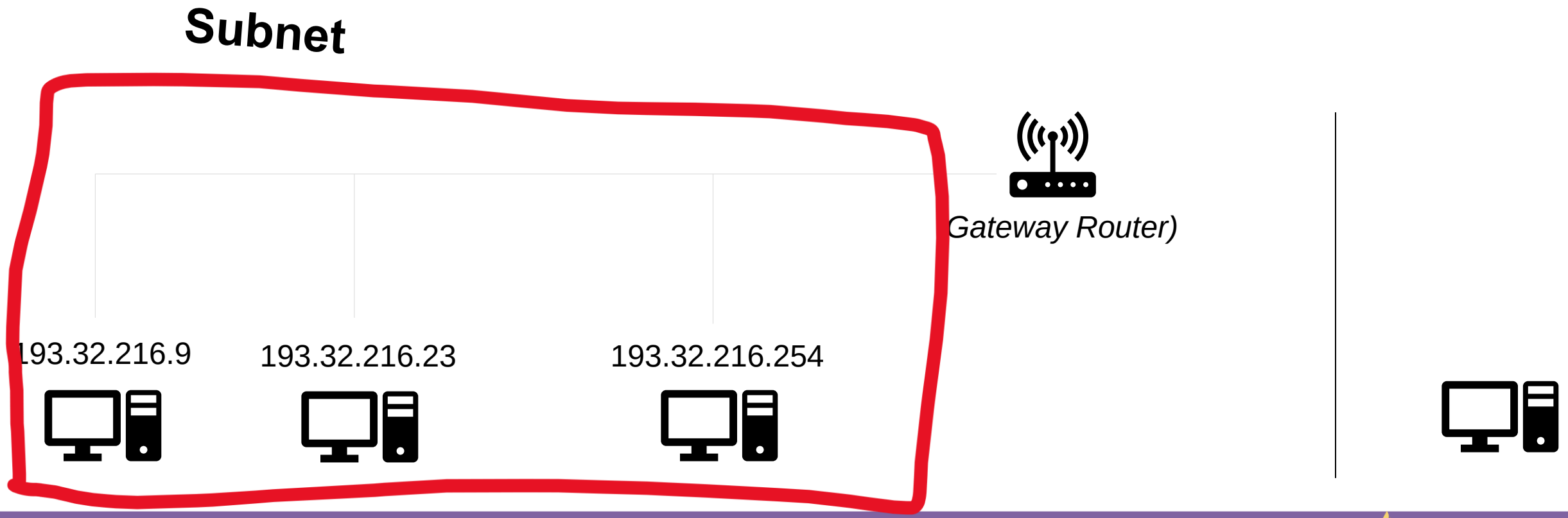
IP Address: 32 bit (4 byte) **dotted decimal** number assigned to interfaces on hosts and routers

IP addresses are heavily used in the routing process and ensuring packets get sent to the correct location

193.32.216.9

An IP address has two parts: the **network bits** and **host bits**

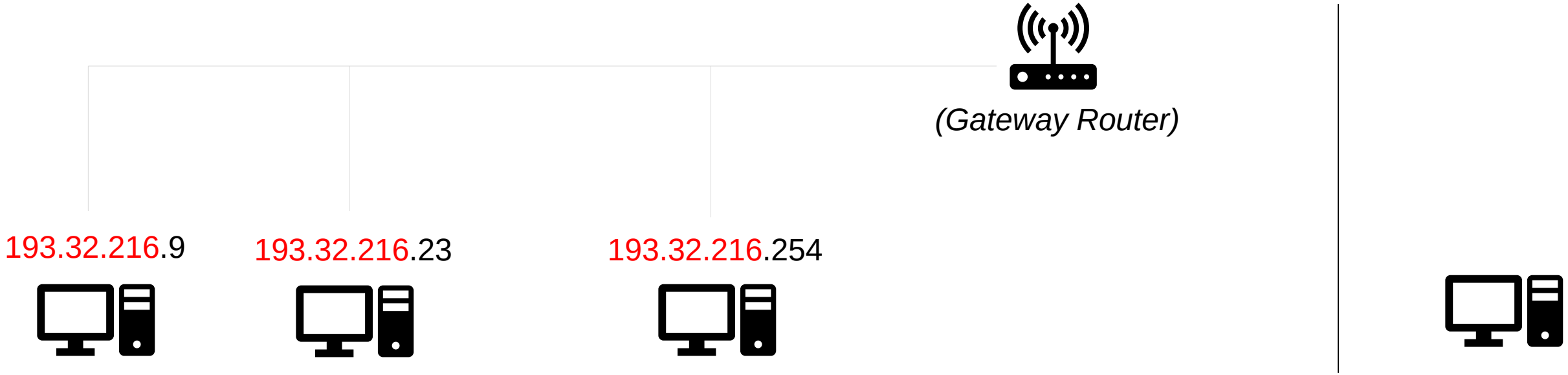
(area code) *(phone number)*



IP Address: 32 bit (4 byte) **dotted decimal** number assigned to interfaces on hosts and routers

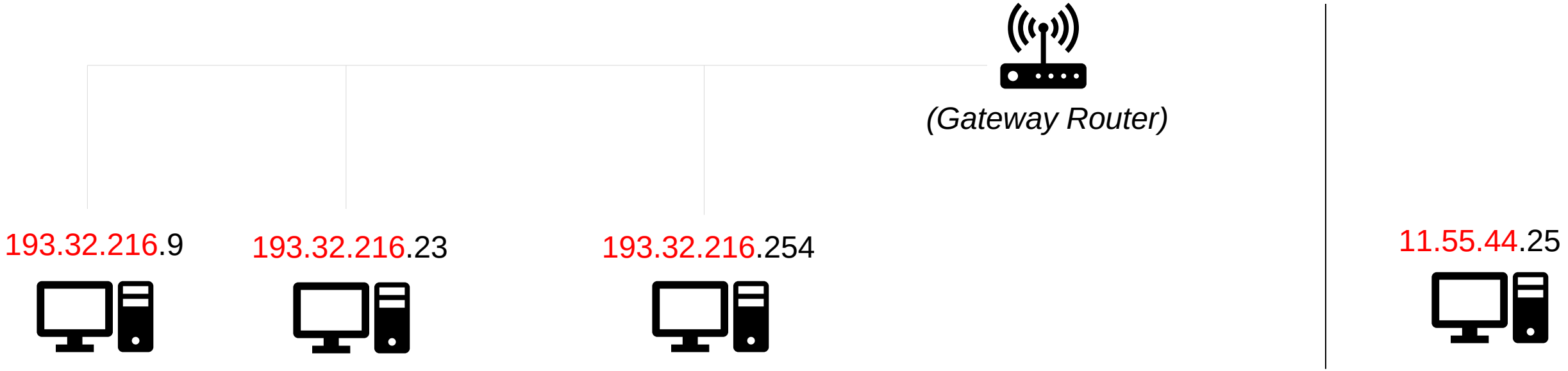
An IP address has two parts: the **network bits** and **host bits**

Devices on the same subnet will have the same **network bits** for their IP address



Devices on the same subnet will have the same **network bits** for their IP address

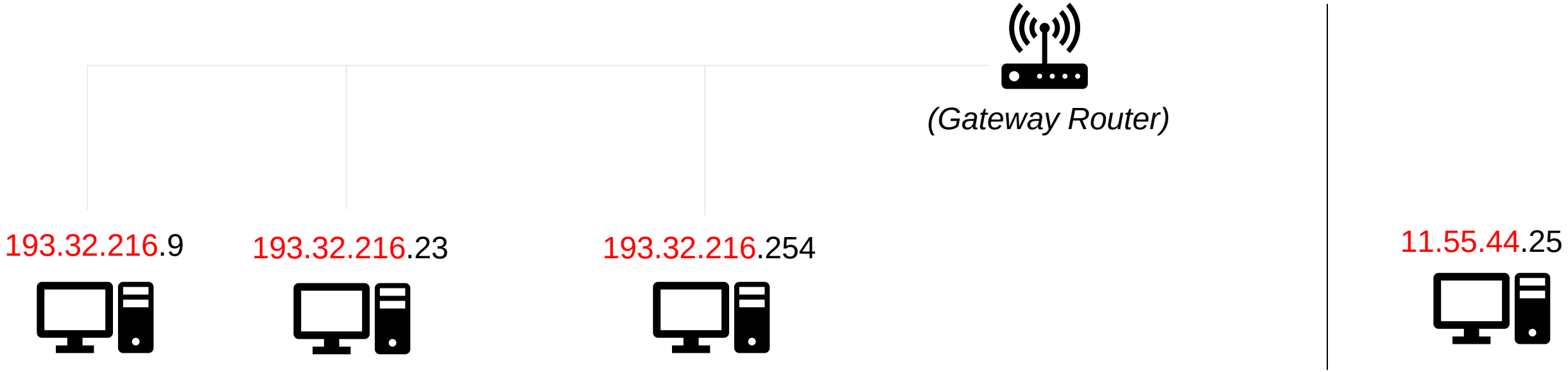
Each device has the **subnet mask** for their network



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

193.32.216.9 The first 24 bits (3 octets) are the network bits



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

193.32.216.9 The first 24 bits (3 octets) are the network bits

193.32.216.0 /24

Subnet Mask

11111111 1111111 1111111 0000000

(Gateway Router)

193.32.216.9

193.32.216.23

193.32.216.254

11.55.44.25

Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

193.32.216.9 The first 24 bits (3 octets) are the network bits

193.32.216.0 /24

Subnet Mask

11111111 1111111 1111111 0000000

Network bits

Host bits

(Gateway Router)

193.32.216.9

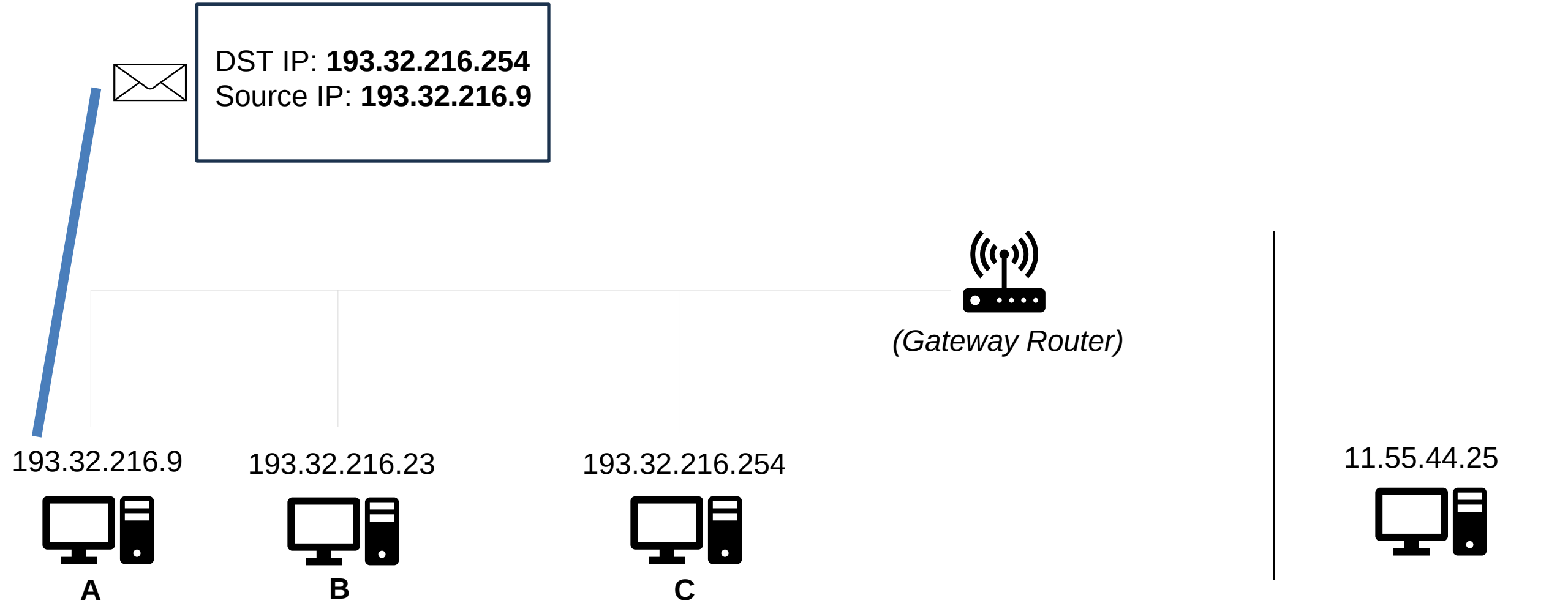
193.32.216.23

193.32.216.**254**

11.55.44.25

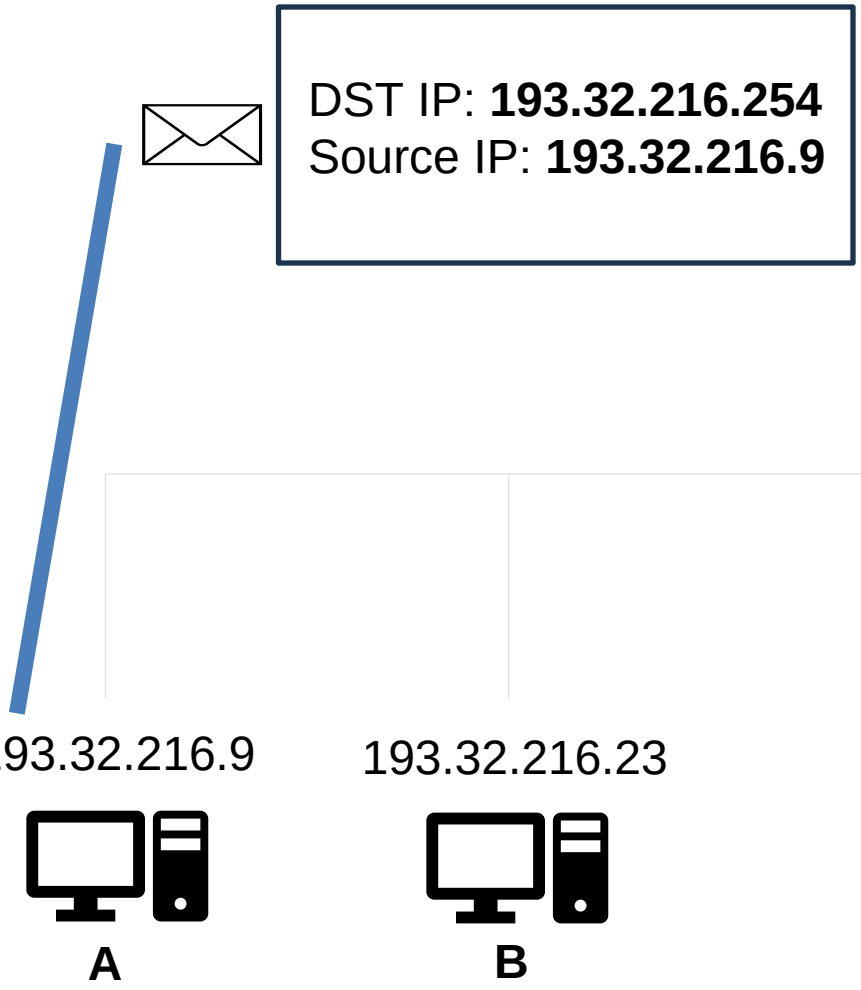
Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network



First question asked when routing:

- Is this packet going to somewhere on my network ?

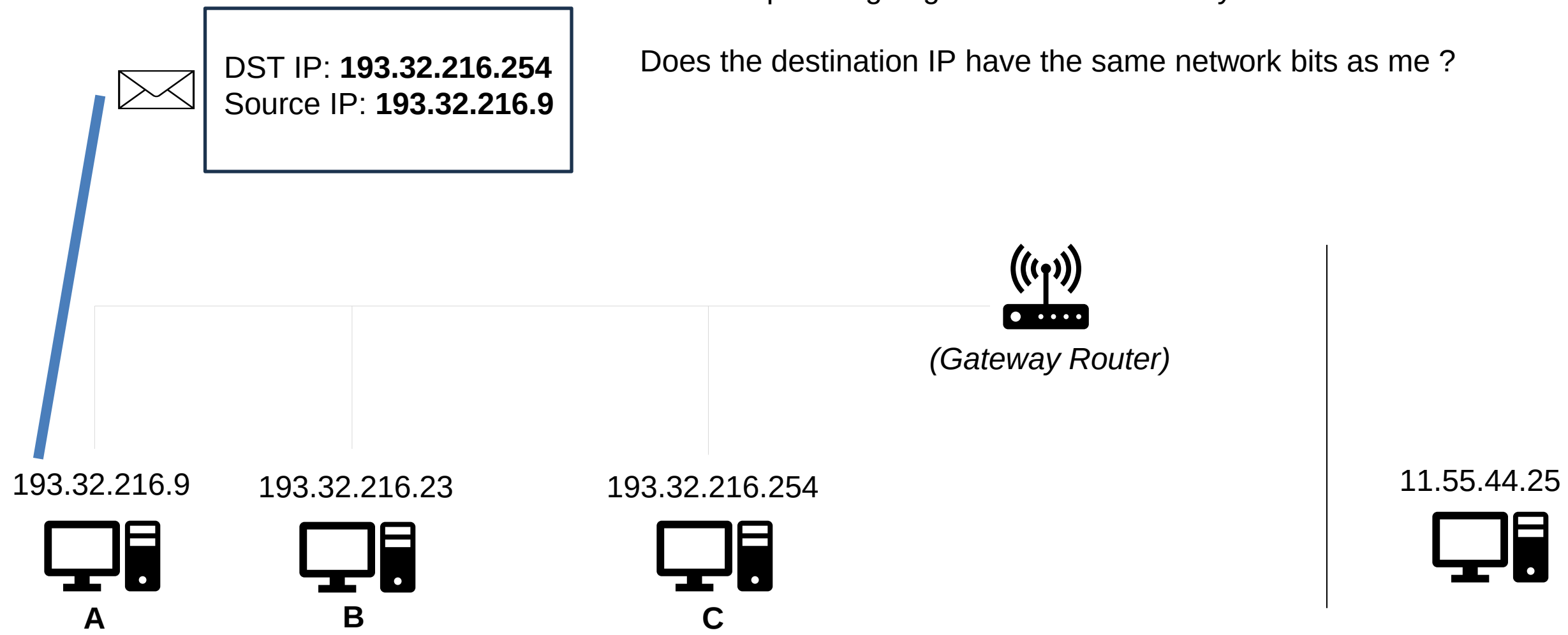
Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

First question asked when routing:

- Is this packet going to somewhere on my network ?

Does the destination IP have the same network bits as me ?



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

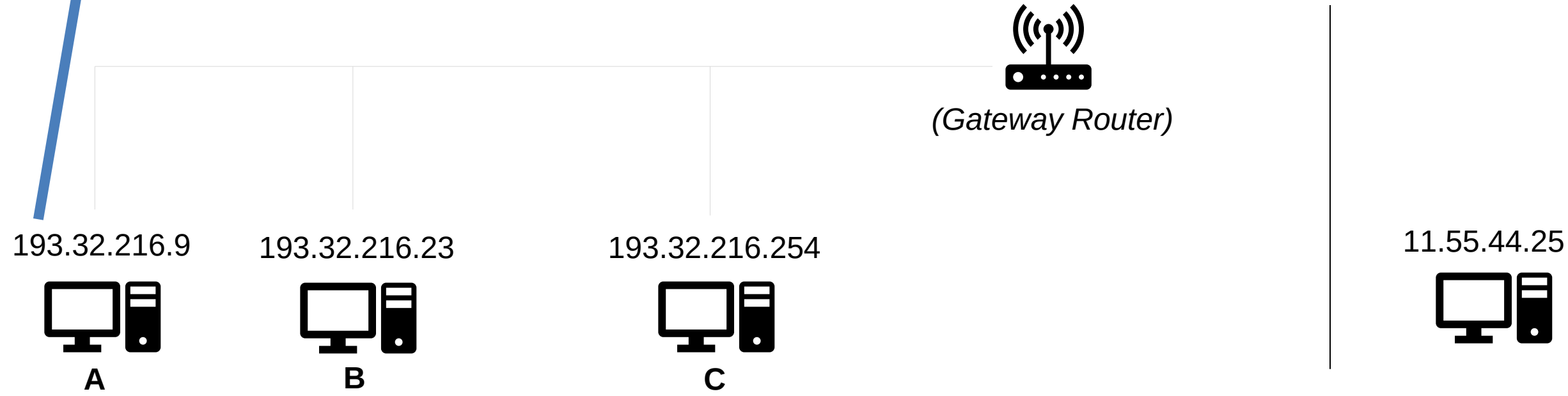
A subnet mask tells a device which bits of an IP address are the host bits and network bits

DST IP: **193.32.216.254**

11000001 00100000 11011000 11111110

11111111 11111111 11111111 00000000 Subnet mask of A

DST IP: **193.32.216.254**
Source IP: **193.32.216.9**



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

A subnet mask tells a device which bits of an IP address are the host bits and network bits

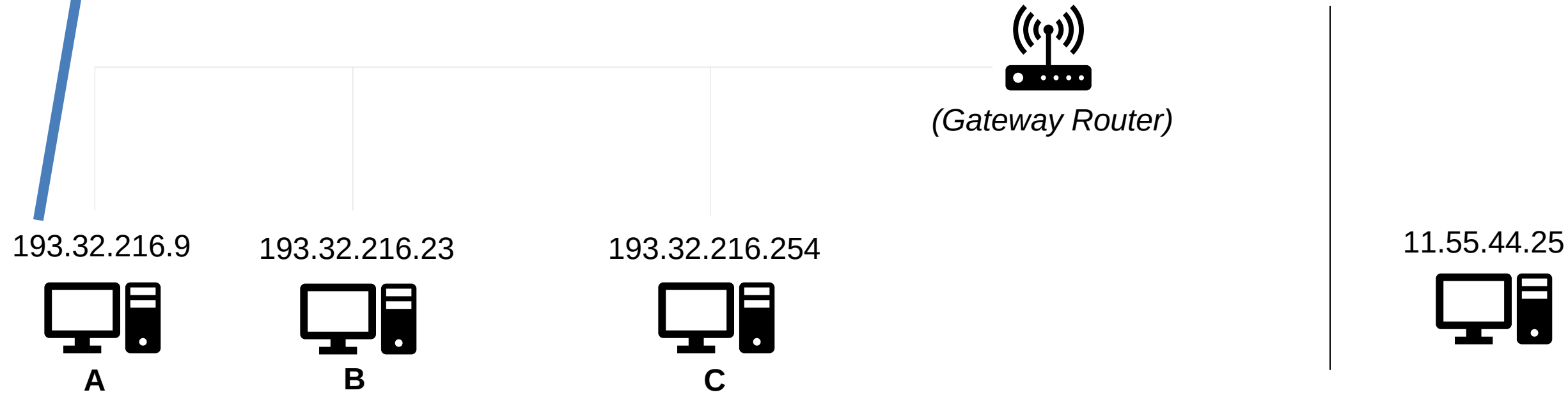
DST IP: **193.32.216.254**

11000001 00100000 11011000 11111110 DST IP

11111111 11111111 11111111 00000000 Subnet mask of A

11000001 00100000 11011000 00011001 Source IP

DST IP: **193.32.216.254**
Source IP: **193.32.216.9**



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

A subnet mask tells a device which bits of an IP address are the host bits and network bits

DST IP: **193.32.216.254**

11000001 00100000 11011000 11111110	DST IP
11111111 11111111 11111111 00000000	Subnet mask of A
11000001 00100000 11011000 00011001	Source IP

DST IP: **193.32.216.254**
Source IP: **193.32.216.9**

They have matching network bits, so this packet needs to be sent within the network!

(Gateway Router)

193.32.216.9

A

193.32.216.23

B

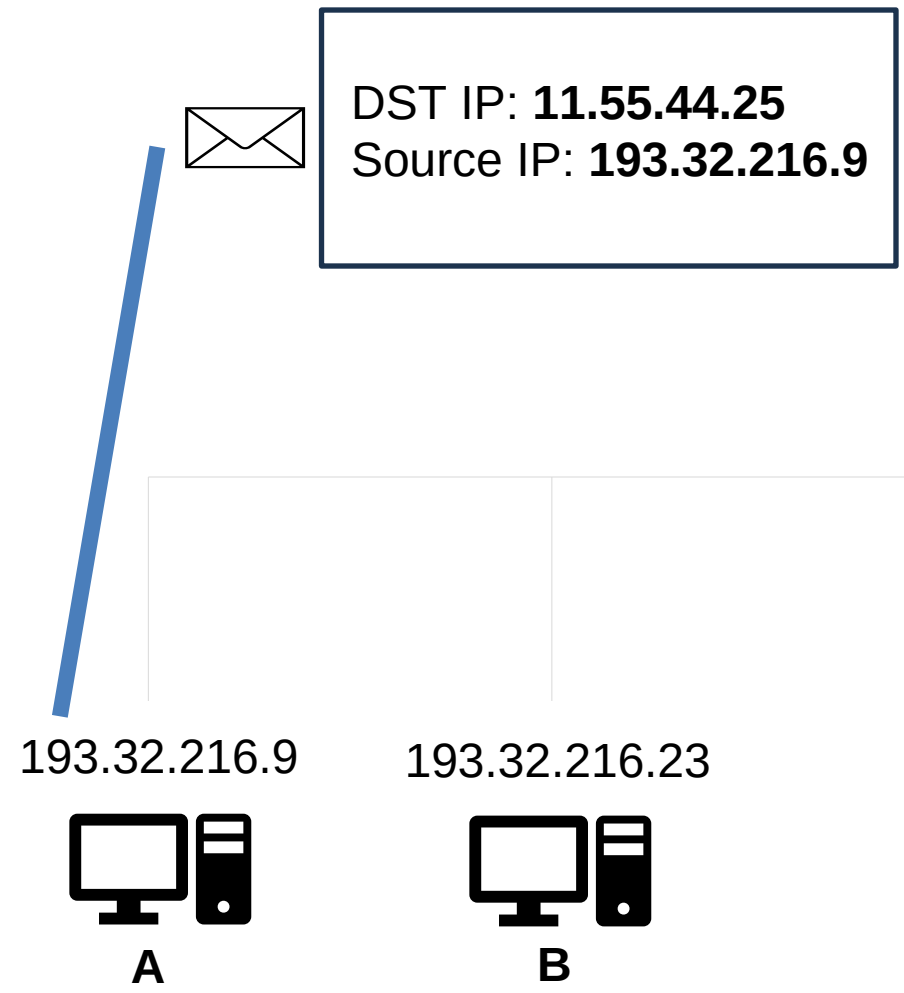
193.32.216.254

C

11.55.44.25

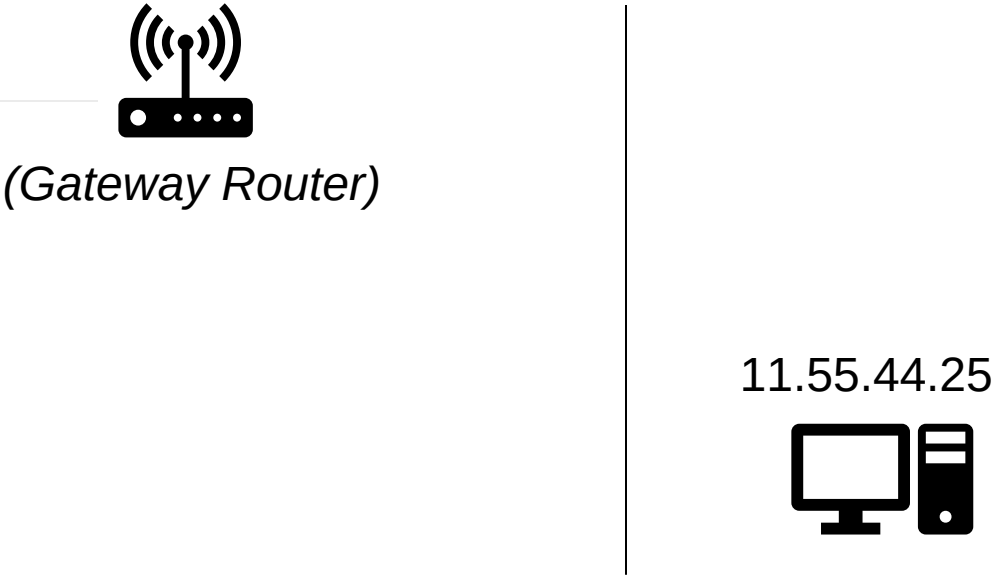
Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network



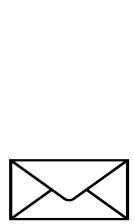
First question asked when routing:

- Is this packet going to somewhere on my network ?



Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network



DST IP: **11.55.44.25**
Source IP: **193.32.216.9**

00001011 00110111 00101100 00011001 DST IP

11111111 11111111 11111111 00000000 Subnet mask of A

11000001 00100000 11011000 00011001 Source IP

(Gateway Router)

193.32.216.9

A

193.32.216.23

B

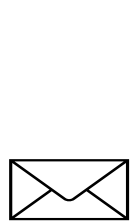
193.32.216.254

C

11.55.44.25

Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network



DST IP: **11.55.44.25**
Source IP: **193.32.216.9**

00001011 00110111 00101100 00011001 DST IP

11111111 11111111 11111111 00000000 Subnet mask of A

11000001 00100000 11011000 00011001 Source IP

(Gateway Router)

193.32.216.9

A

193.32.216.23

B

193.32.216.254

C

11.55.44.25

Devices on the same subnet will have the same **network bits** for their IP address

Each device has the **subnet mask** for their network

DST IP: **11.55.44.25**
Source IP: **193.32.216.9**

00001011 00110111 00101100 00011001 DST IP

11111111 11111111 11111111 00000000 Subnet mask of A

11000001 00100000 11011000 00011001 Source IP

They do not have matching network bits, so this packet needs to be sent to the **gateway router**

(Gateway Router)

193.32.216.9

A

193.32.216.23

B

193.32.216.254

C

11.55.44.25

64.201.33.0 /24

64.201.33.0 - 64.201.33.255

(256 usable IPs)

Classful networks:
Class A: /8
Class B: /16
Class C: /24

Now obsolete!

64.201.33.0 /20

64.201.32.0 - 64.201.47.255

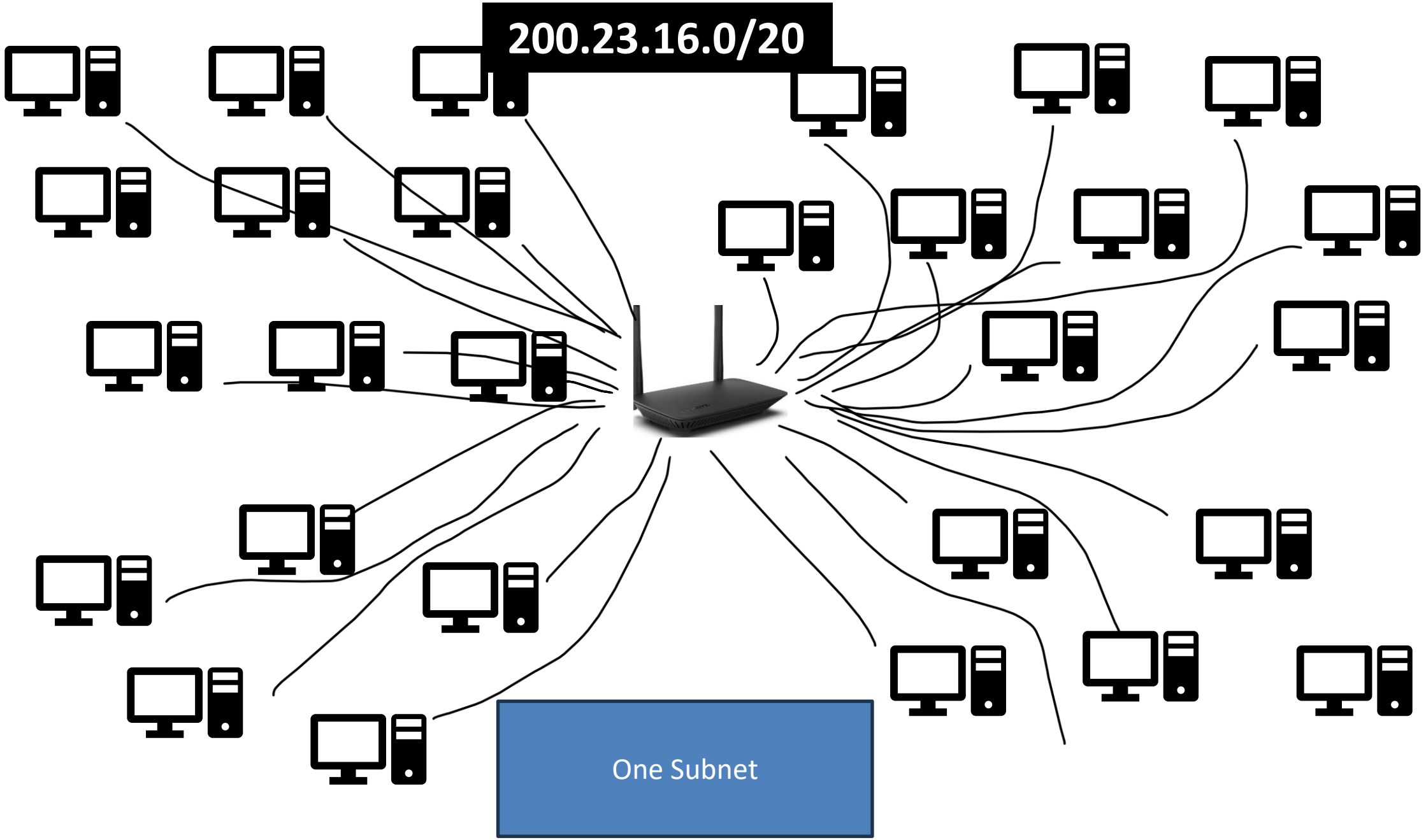
(4096 usable IPs)

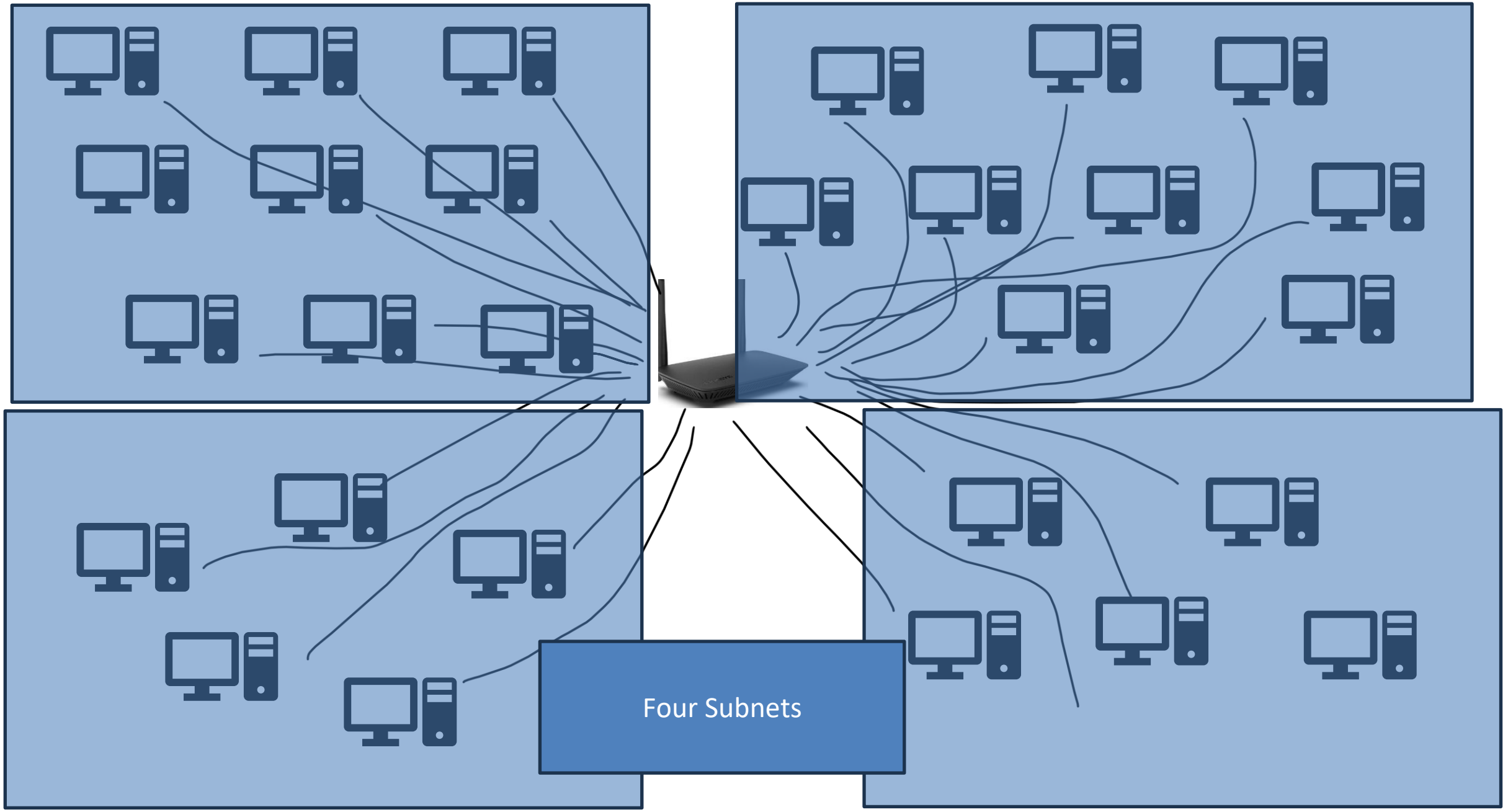
64.201.33.0 /9

64.128.0.0 - 64.255.255.255

(8,388,608 usable IPs)

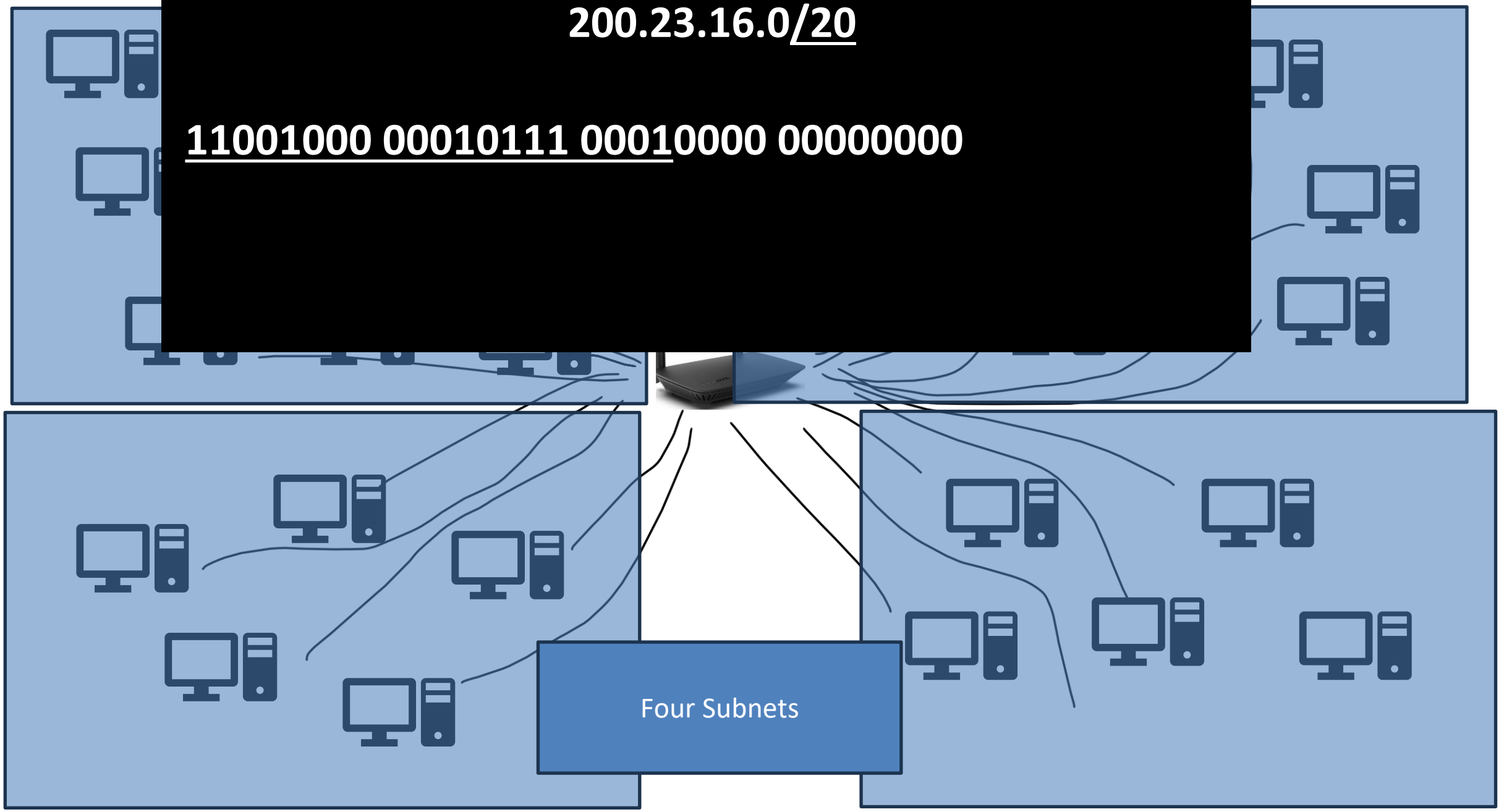
The more bits we allocate for **host bits,** the more IP addresses we can fit on a network!


200.23.16.0/20
One Subnet


Four Subnets

200.23.16.0/20

11001000 00010111 00010000 00000000

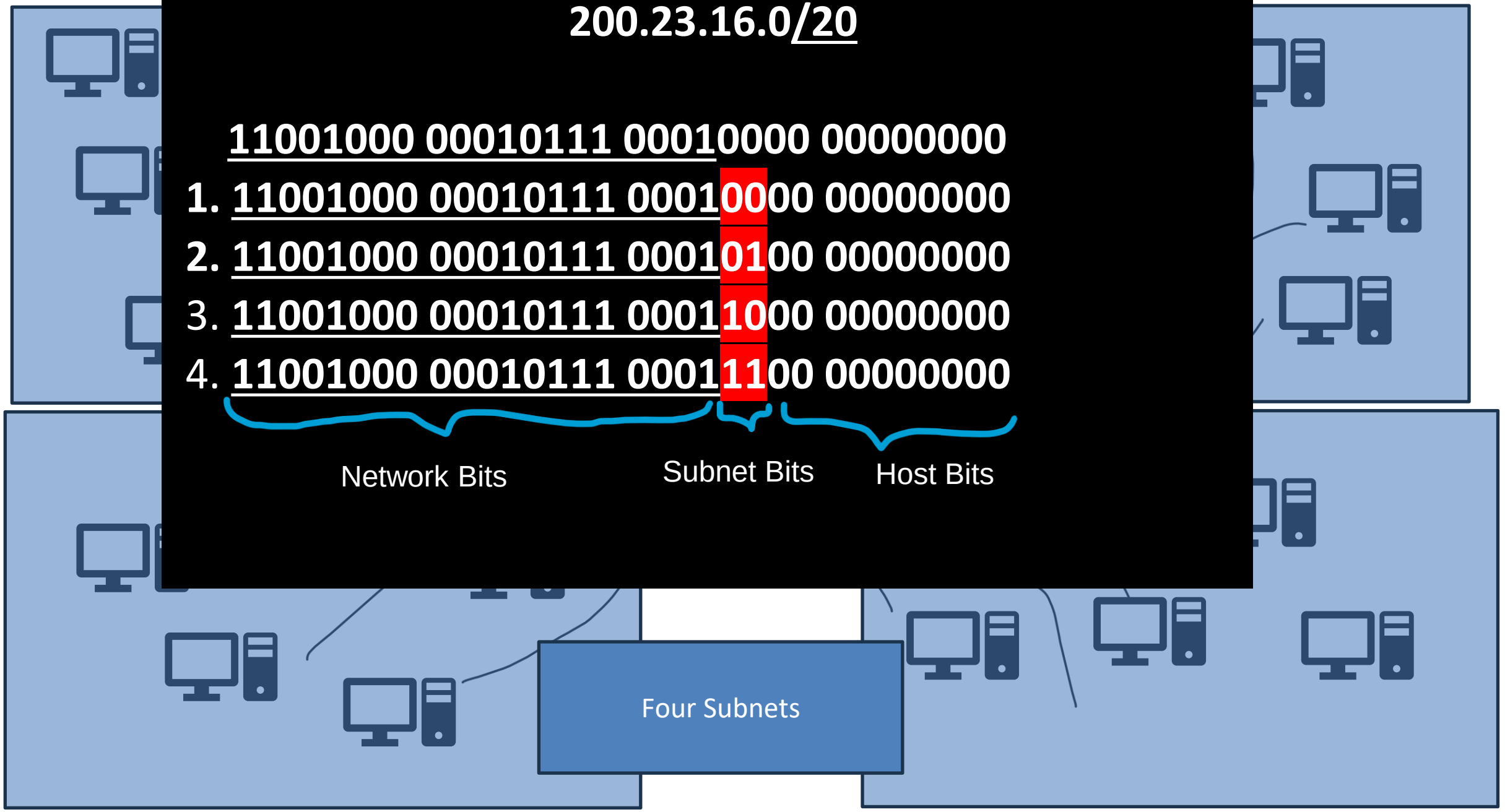


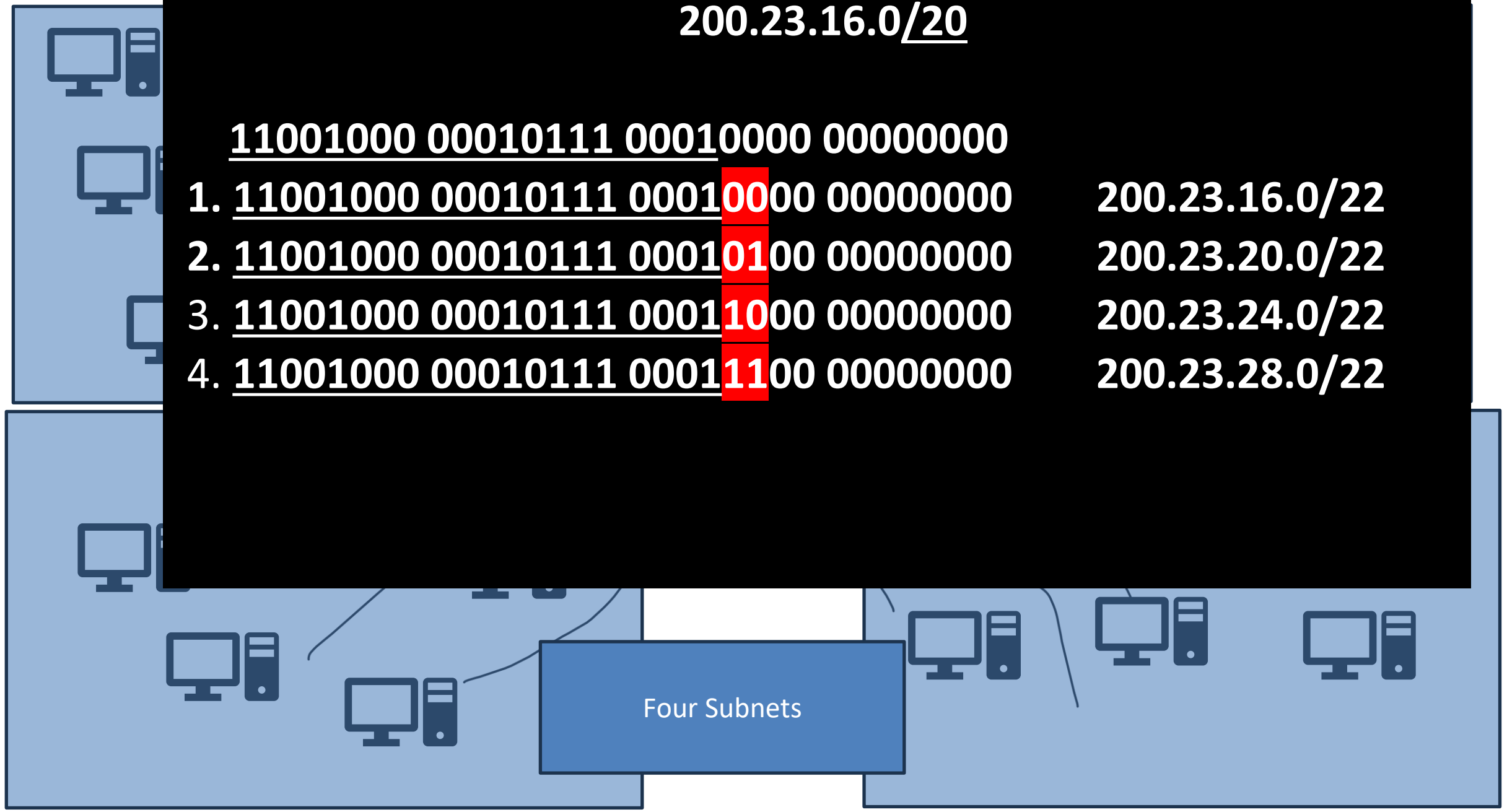
200.23.16.0/20

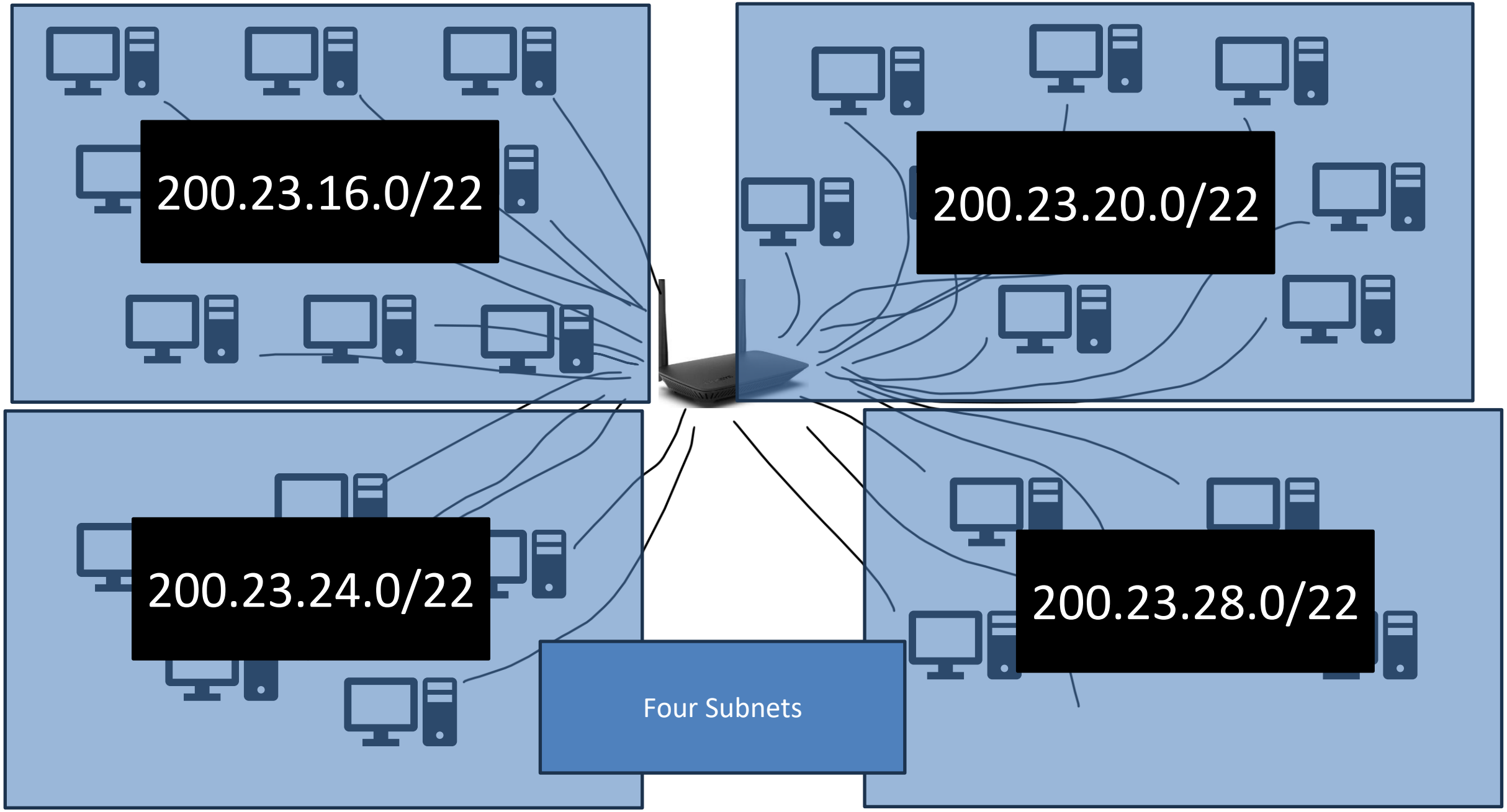
11001000 00010111 00010000 00000000

1. 11001000 00010111 00010000 00000000
2. 11001000 00010111 00010100 00000000
3. 11001000 00010111 00011000 00000000
4. 11001000 00010111 00011100 00000000

Network Bits | Subnet Bits | Host Bits



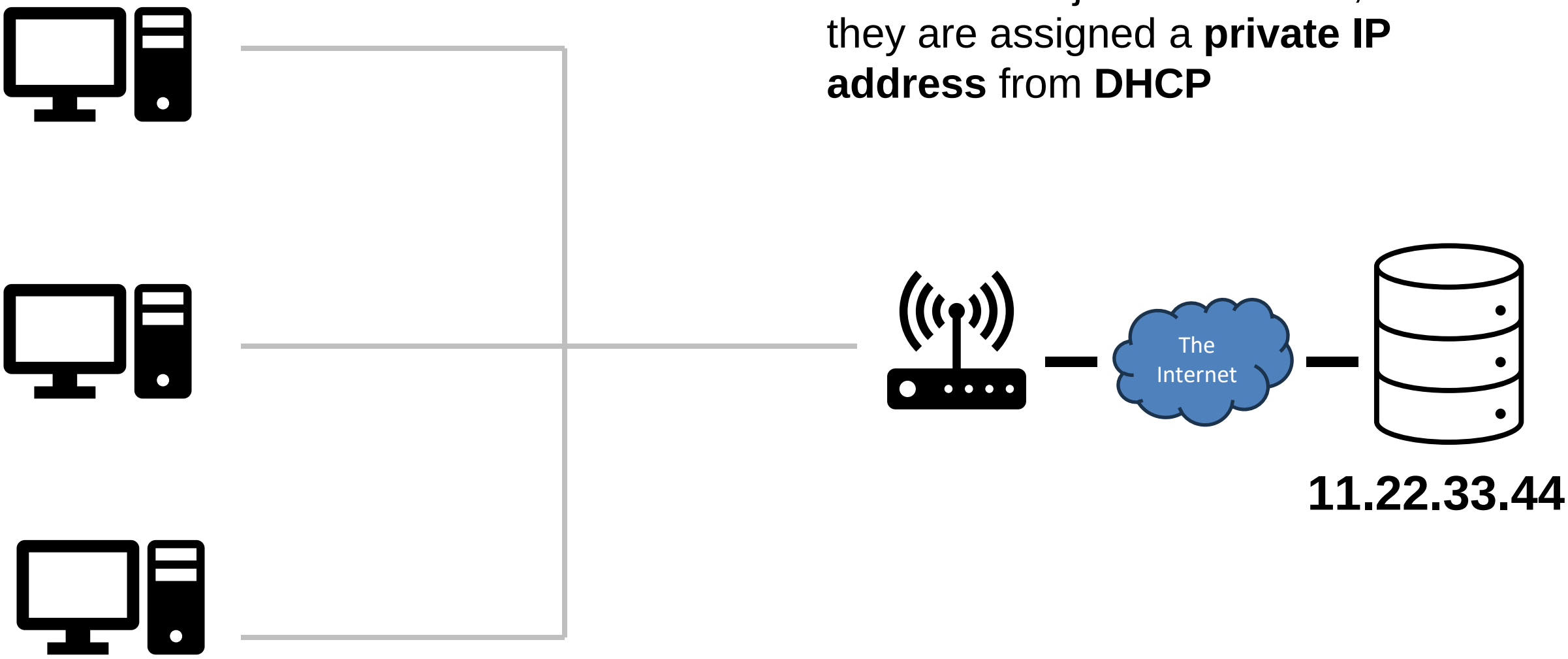

200.23.16.0/20
11001000 00010111 00010000 00000000
1. 11001000 00010111 00010000 00000000 200.23.16.0/22
2. 11001000 00010111 00010100 00000000 200.23.20.0/22
3. 11001000 00010111 00011000 00000000 200.23.24.0/22
4. 11001000 00010111 00011100 00000000 200.23.28.0/22
Four Subnets


200.23.16.0/22
200.23.20.0/22
200.23.24.0/22
200.23.28.0/22
Four Subnets

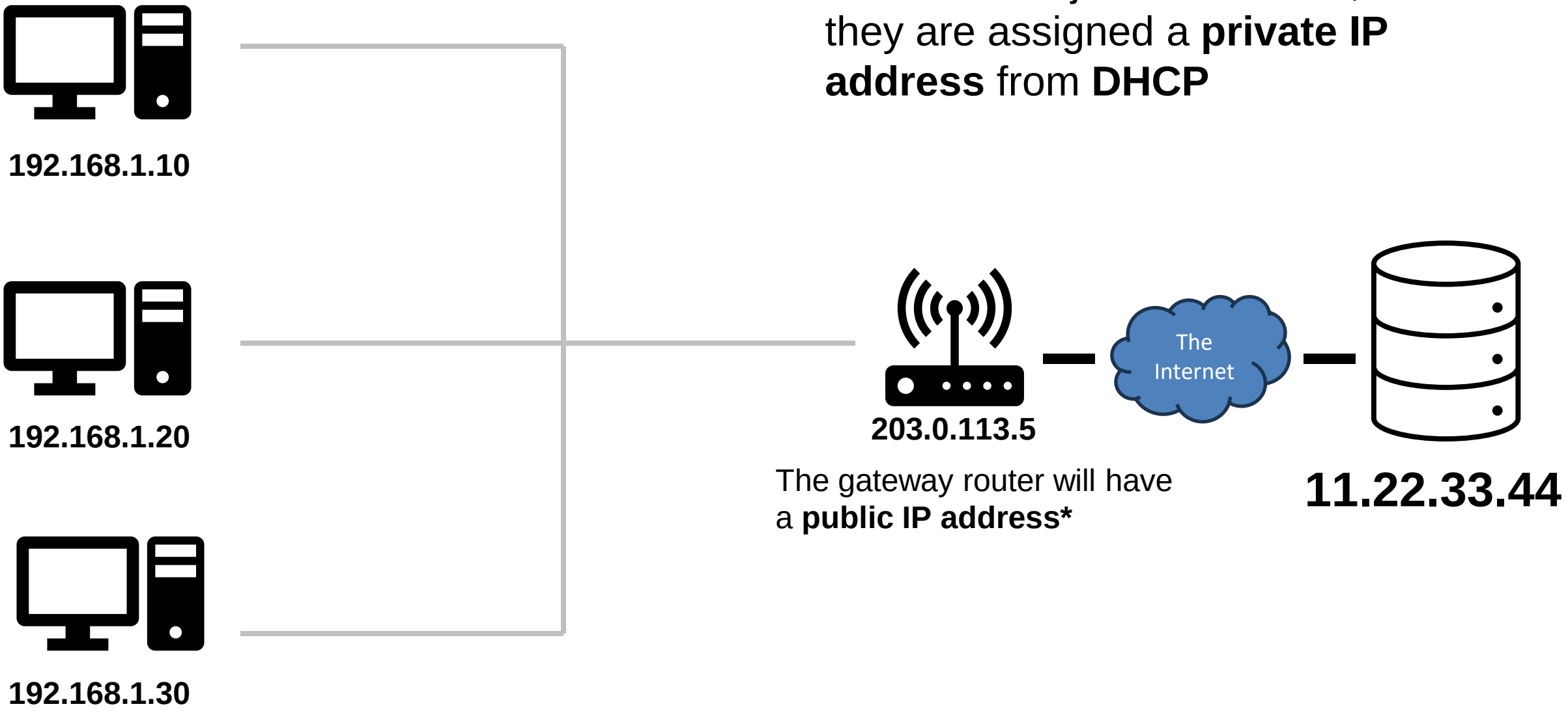
Subnetting for IPv6 networks exist, and function very similar

- No subnet mask (called “prefix length” in IPv6)

When a host joins a network, they are assigned a **private IP address** from **DHCP**

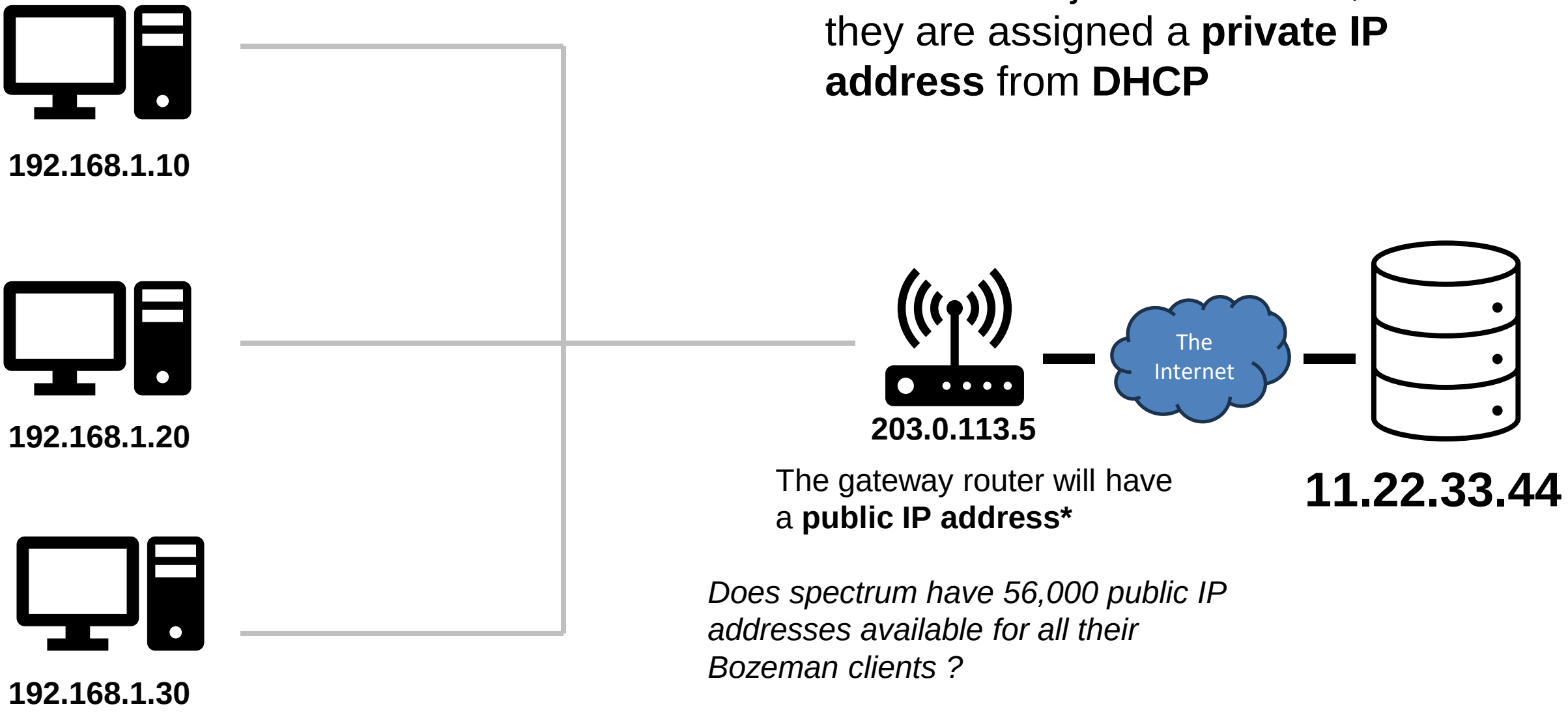


When a host joins a network, they are assigned a **private IP address** from **DHCP**



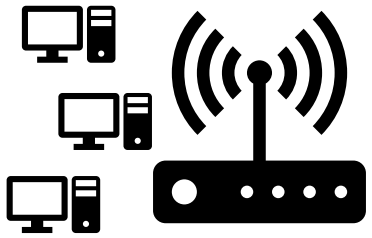
The gateway router will have a **public IP address***

When a host joins a network, they are assigned a **private IP address** from **DHCP**

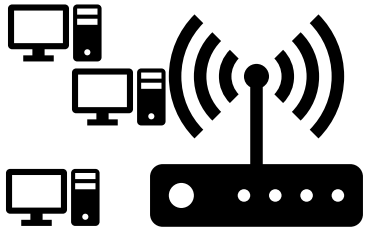


The gateway router will have a **public IP address***

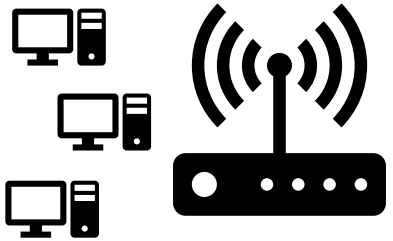
Does spectrum have 56,000 public IP addresses available for all their Bozeman clients ?



192.168.1.10



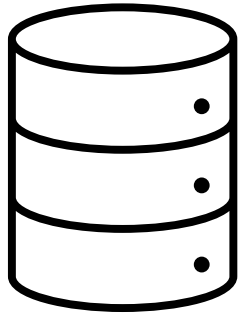
192.168.1.20



192.168.1.30

When a host joins a network, they are assigned a **private IP address** from **DHCP**

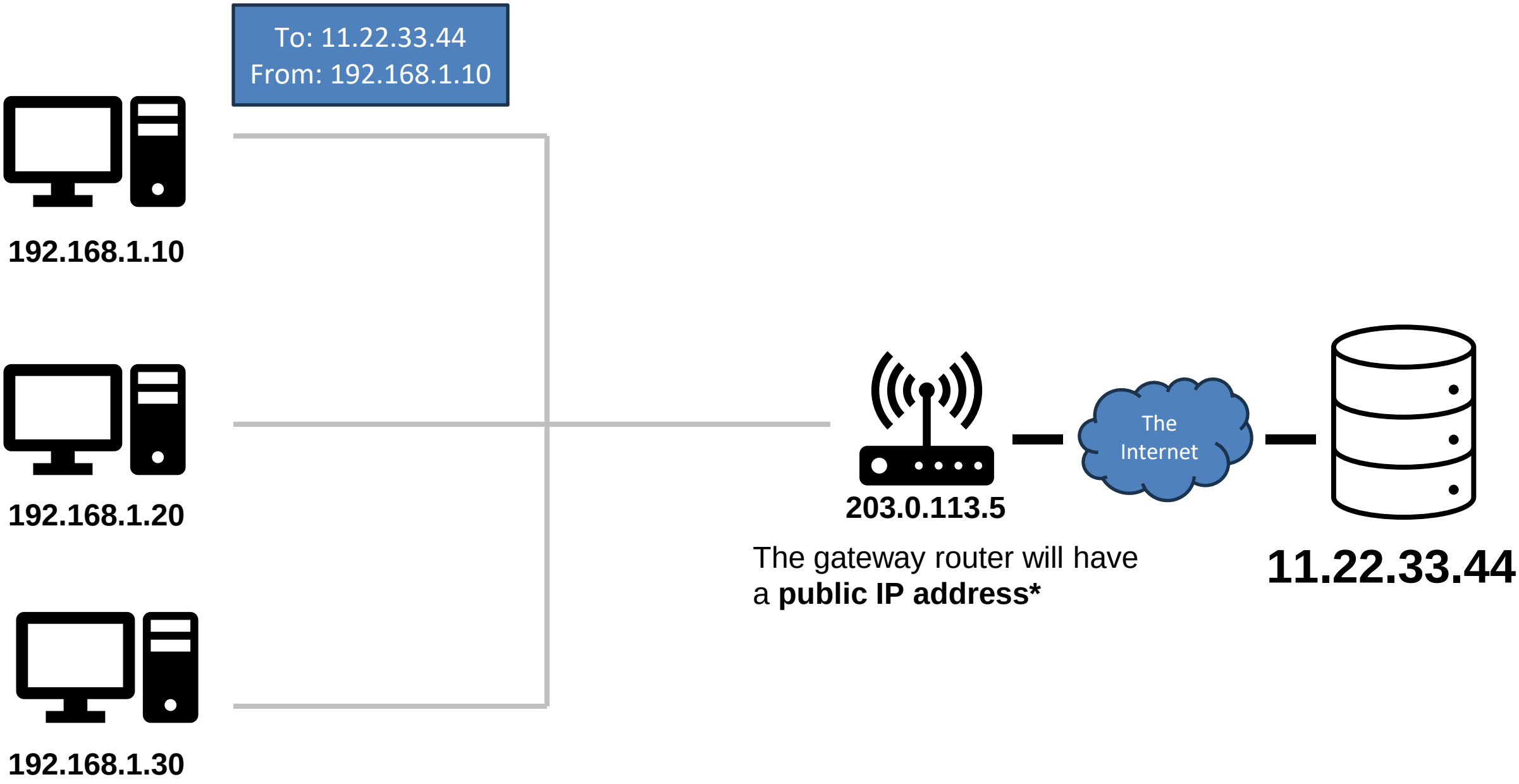
203.0.113.5



11.22.33.44

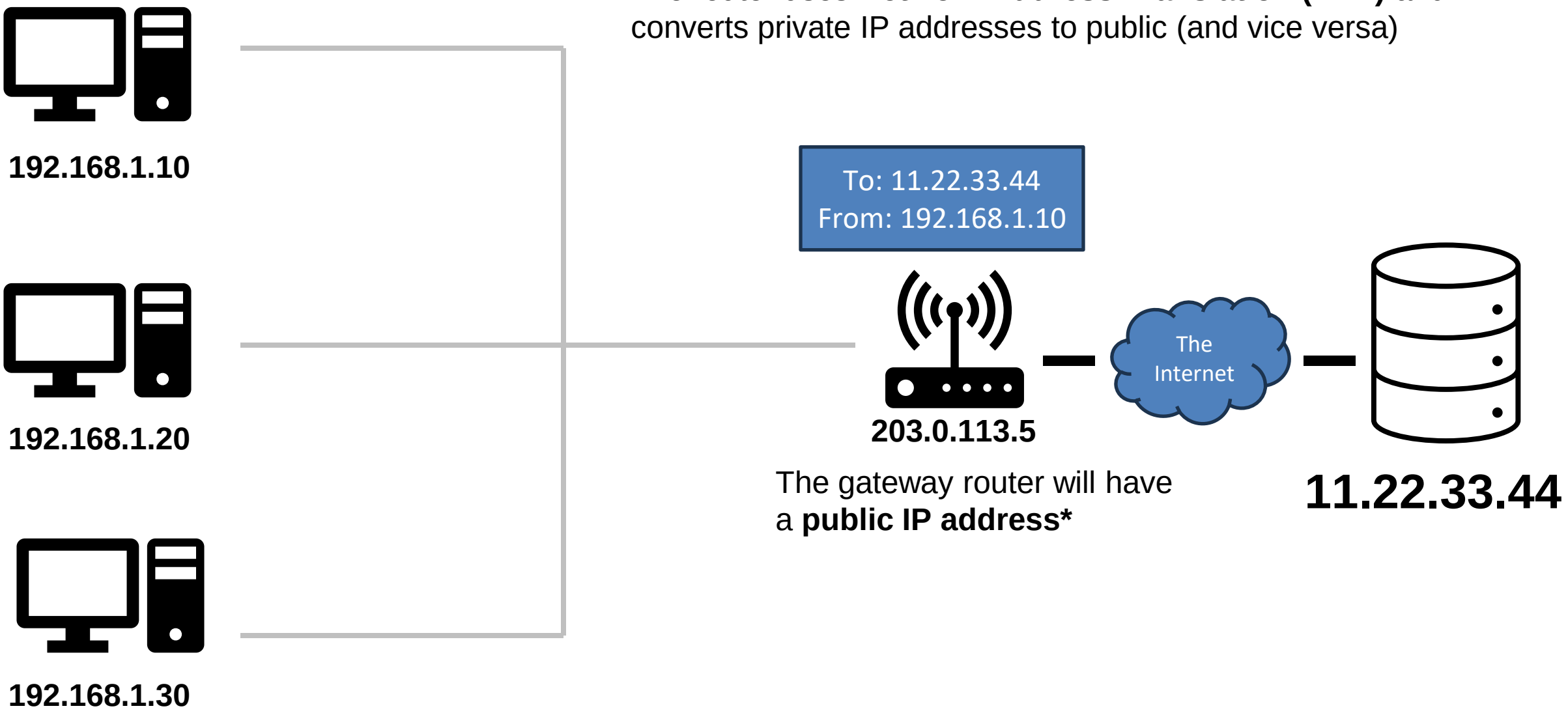
The gateway router will have a **public IP address***

Large ISPs will have their own NAT that translates private residential networks to public IPv4 addresses



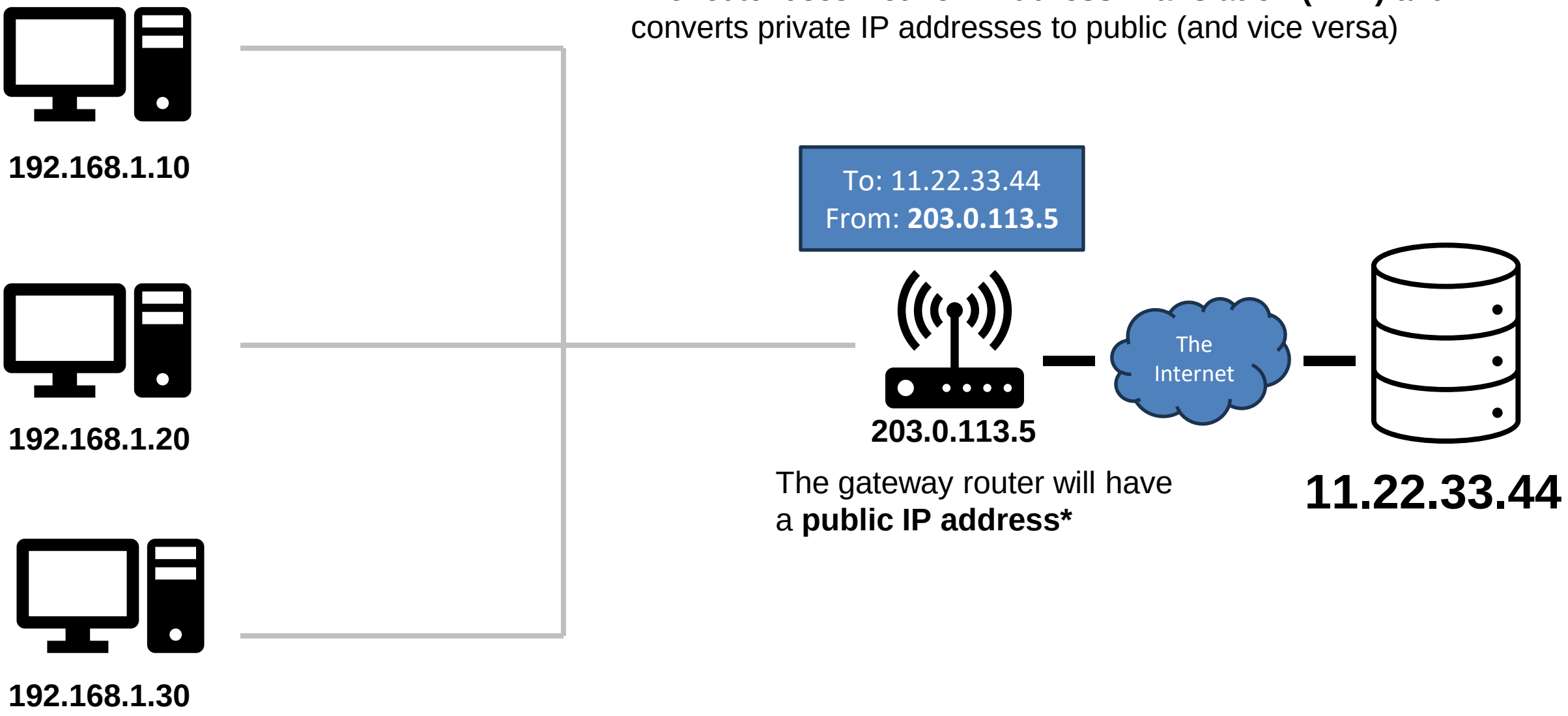
The gateway router will have a **public IP address***

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)



The gateway router will have a **public IP address***

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)



The gateway router will have a **public IP address***

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)

192.168.1.10

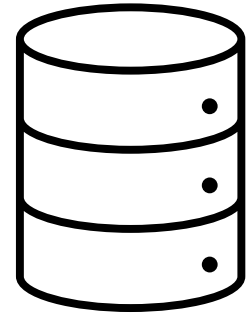
192.168.1.20

192.168.1.30

If we ever get something back from **11.22.33.44**, we know it needs to go to **192.168.1.10**

To: 11.22.33.44
From: **203.0.113.5**

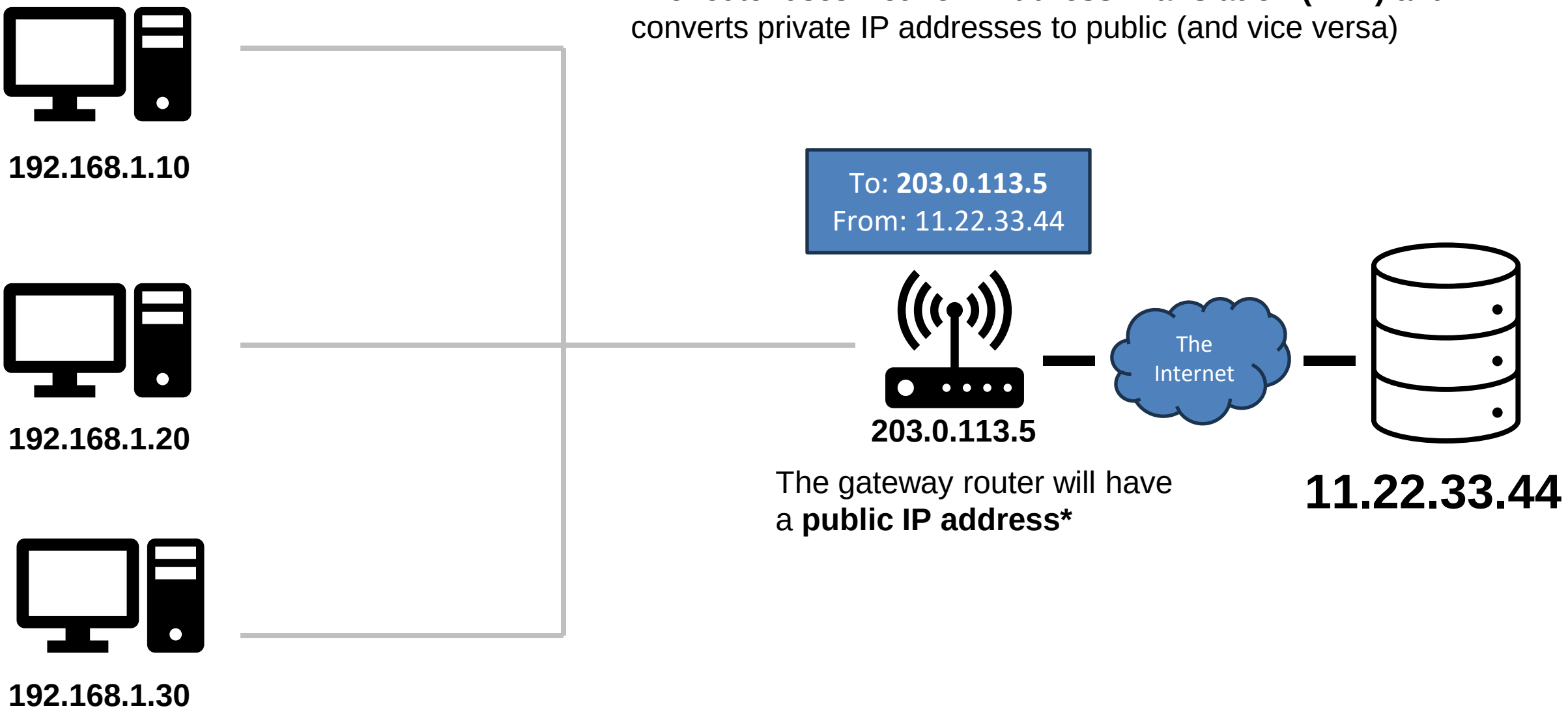
203.0.113.5



11.22.33.44

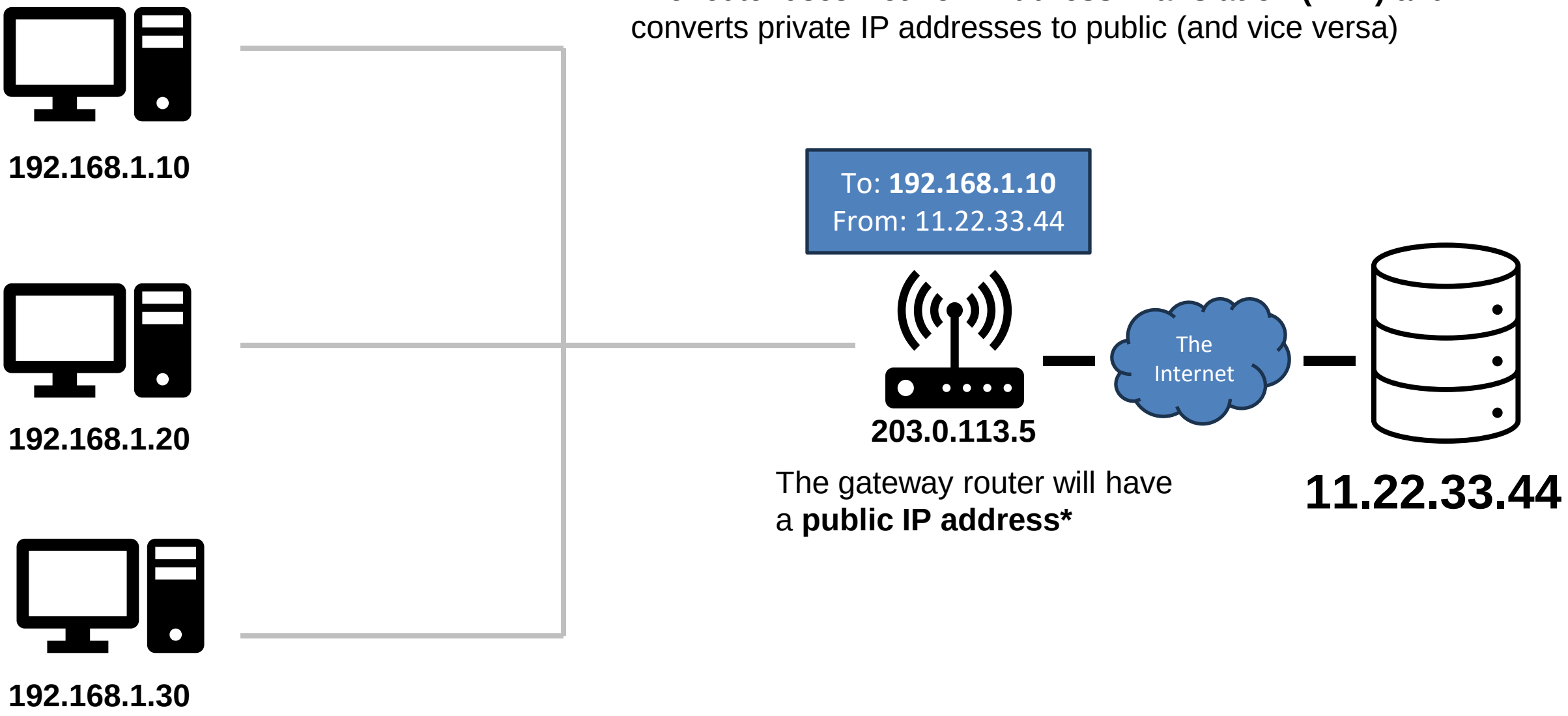
The gateway router will have a **public IP address***

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)



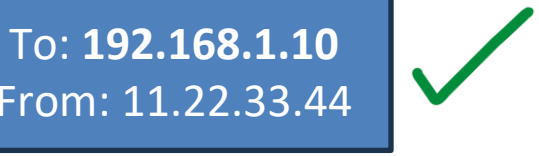
The gateway router will have a **public IP address***

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)



The gateway router will have a **public IP address***

To: **192.168.1.10**
From: 11.22.33.44



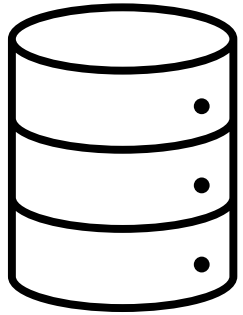
192.168.1.10

192.168.1.20

192.168.1.30

The router uses **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)

203.0.113.5



11.22.33.44

The gateway router will have a **public IP address***

Routers use **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)

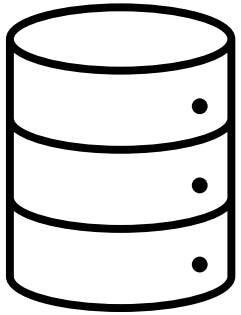
192.168.1.10

192.168.1.20

192.168.1.30

Any weird situations that could happen?

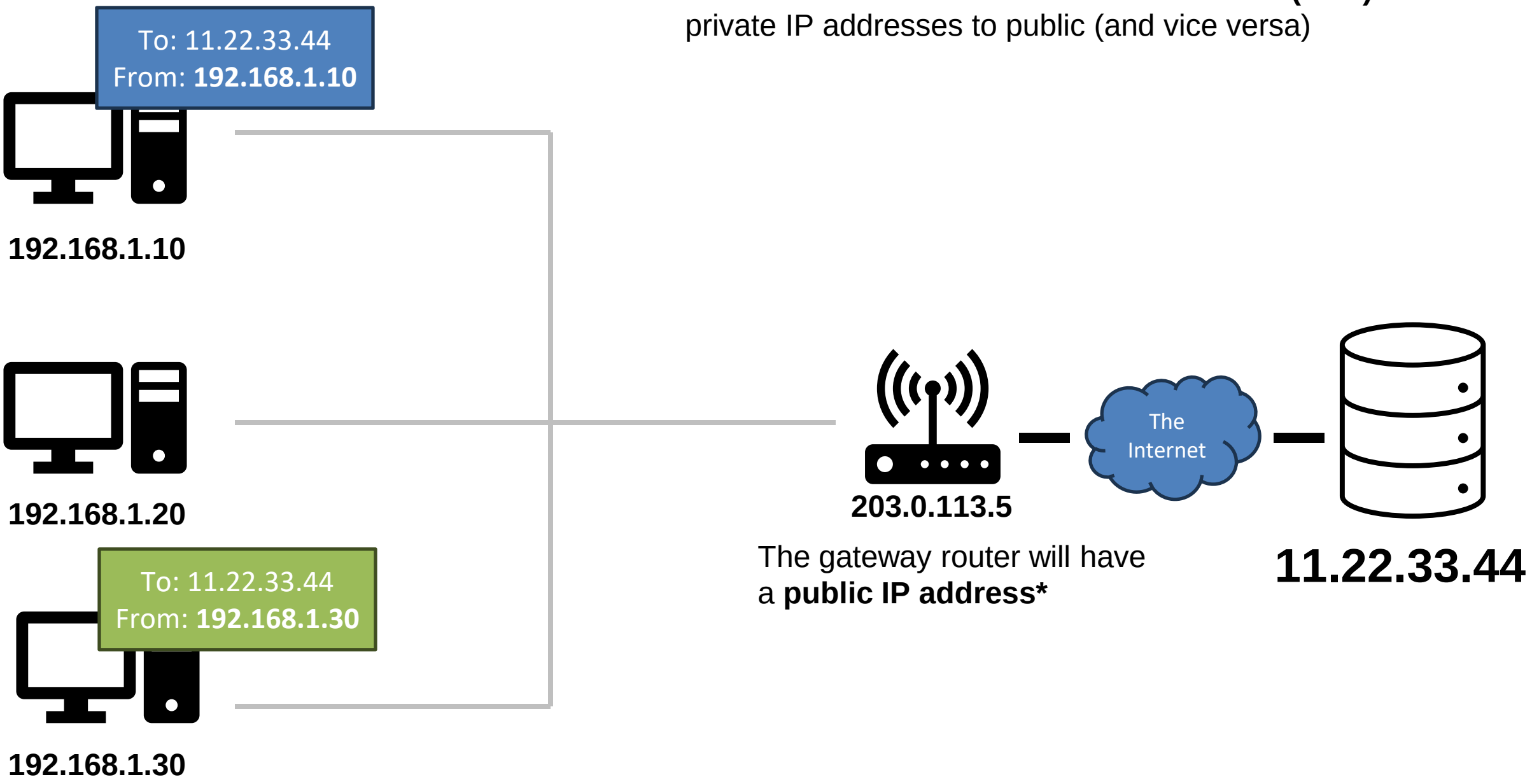
203.0.113.5



11.22.33.44

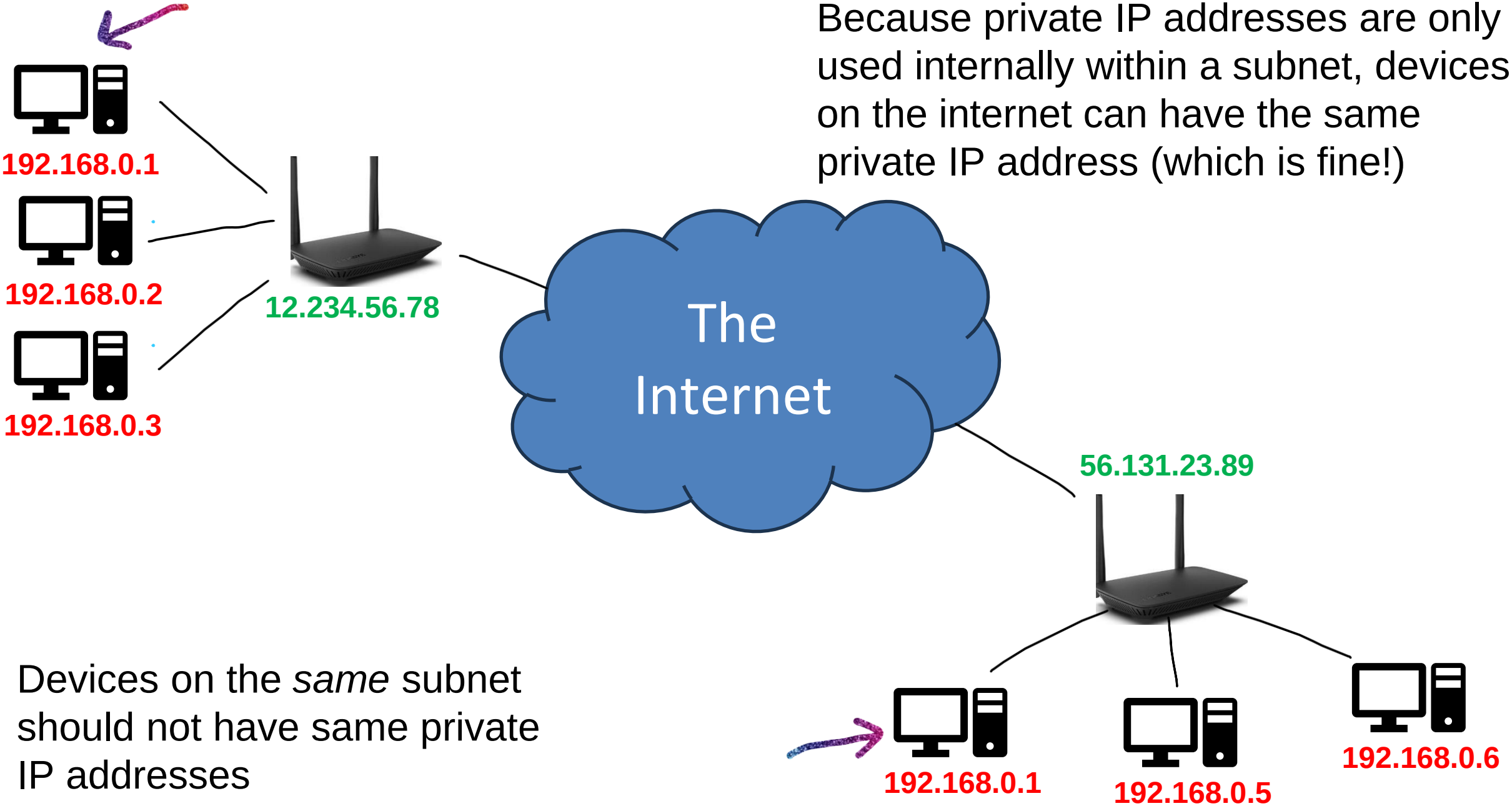
The gateway router will have a **public IP address***

Routers use **Network Address Translation (NAT)** and converts private IP addresses to public (and vice versa)



The gateway router will have a **public IP address***

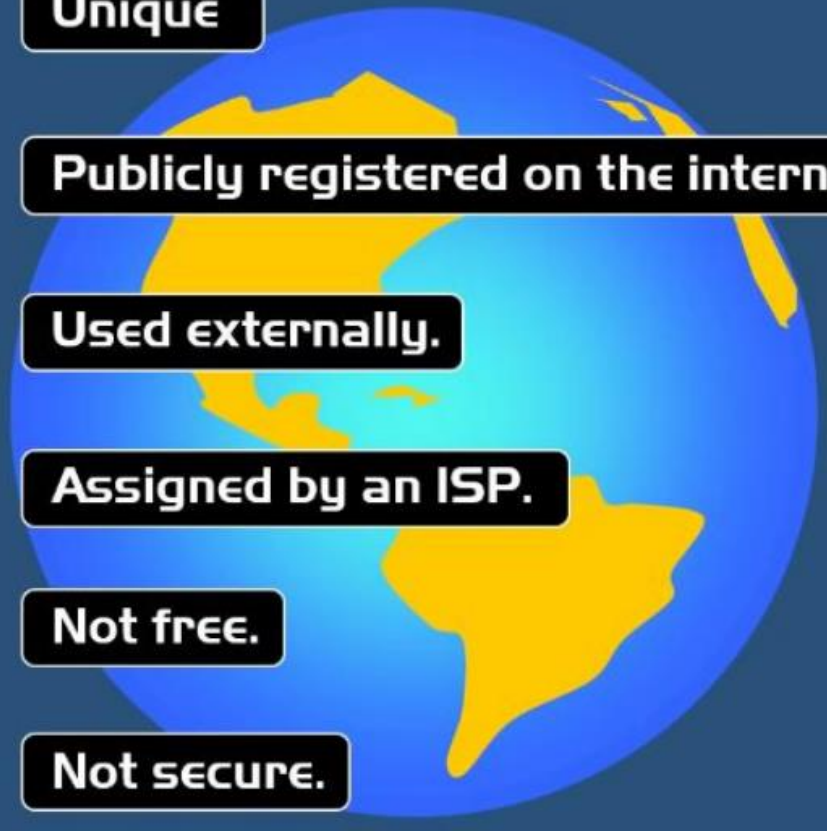
Because private IP addresses are only used internally within a subnet, devices on the internet can have the same private IP address (which is fine!)



Devices on the *same* subnet should not have same private IP addresses

Public IP

- Unique
- Publicly registered on the internet.
- Used externally.
- Assigned by an ISP.
- Not free.
- Not secure.



Private IP

- Non-unique. Can be used on other private networks.
- Not publicly registered.
- Used internally.
- Assigned by a router.
- Free.
- More secure.

How to see your public/private IP address

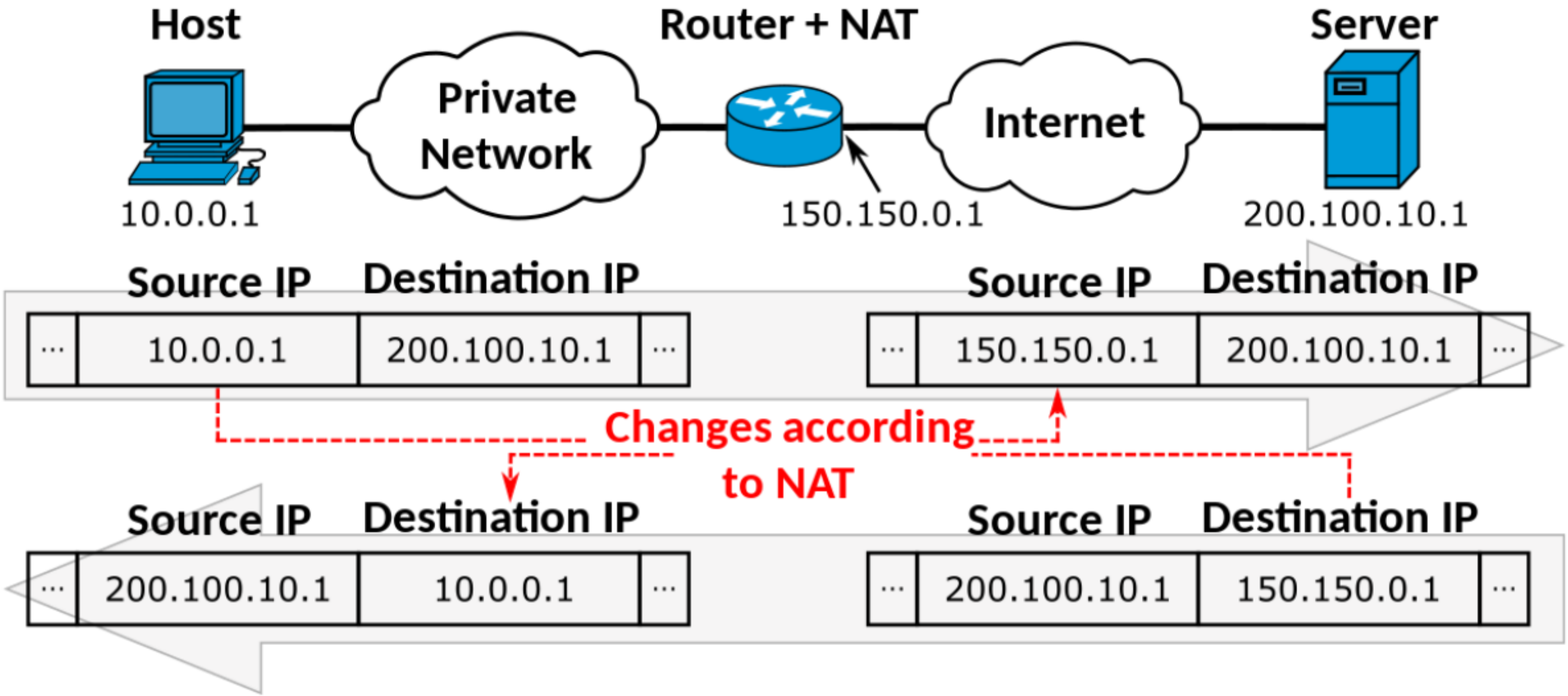
The three Rs of NAT

NAT Router MUST

- Outgoing Datagram: **Replace**
  (Source IP Address, Port #) → (NAT IP address, new port #)
  (private) (public)
- **Remember**
  In some kind of NAT table data structure
- Incoming Datagram: **Replace**
  (NAT IP Address, new Port #) → (Source IP Address, Port #)
  (public) (private)

"If you remember the three Rs of NAT, no amount of IP addresses on earth can fool you"

- *Patches O'Houlihan (probably)*


Host
Router + NAT
Server
Private Network
Internet
10.0.0.1
150.150.0.1
200.100.10.1
Source IP
Destination IP
10.0.0.1
200.100.10.1
Source IP
Destination IP
150.150.0.1
200.100.10.1
Changes according to NAT
Source IP
Destination IP
200.100.10.1
10.0.0.1
Source IP
Destination IP
200.100.10.1
150.150.0.1

The following IP ranges are reserved for private IP addressing

192.168.X.X (class c networks)

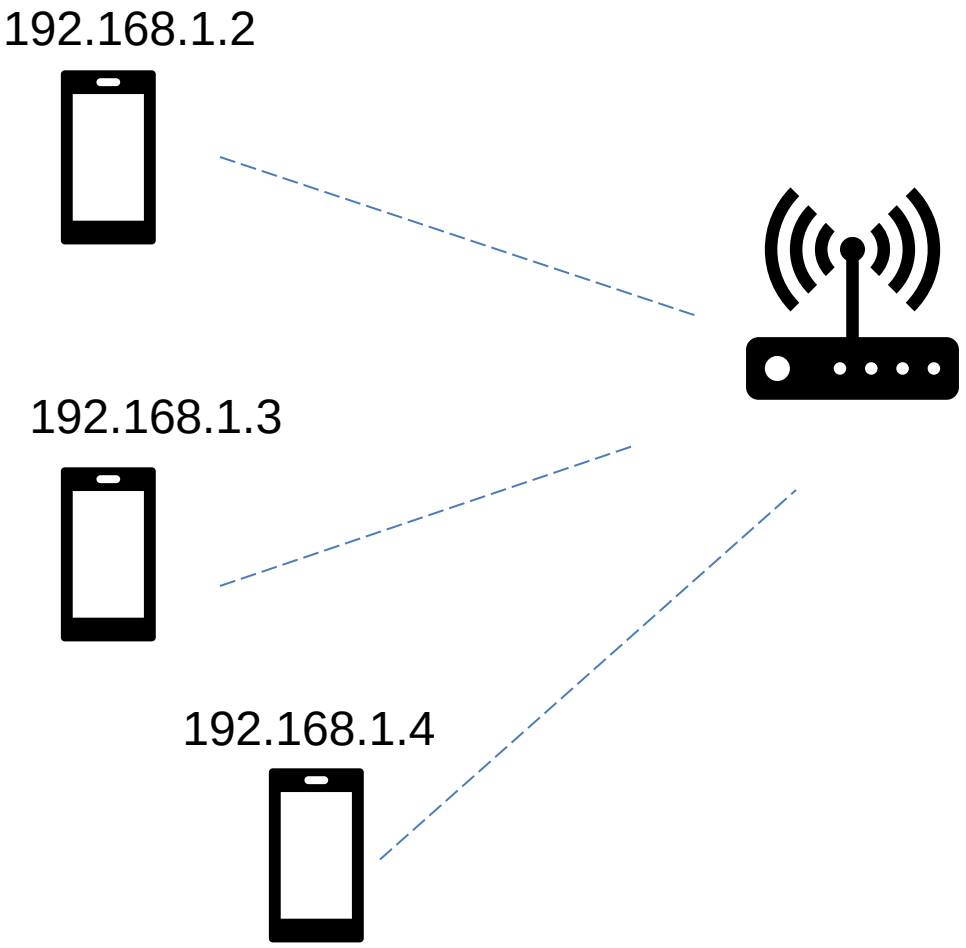
10.X.X.X (class a networks)

172.16.X.X (class b networks)

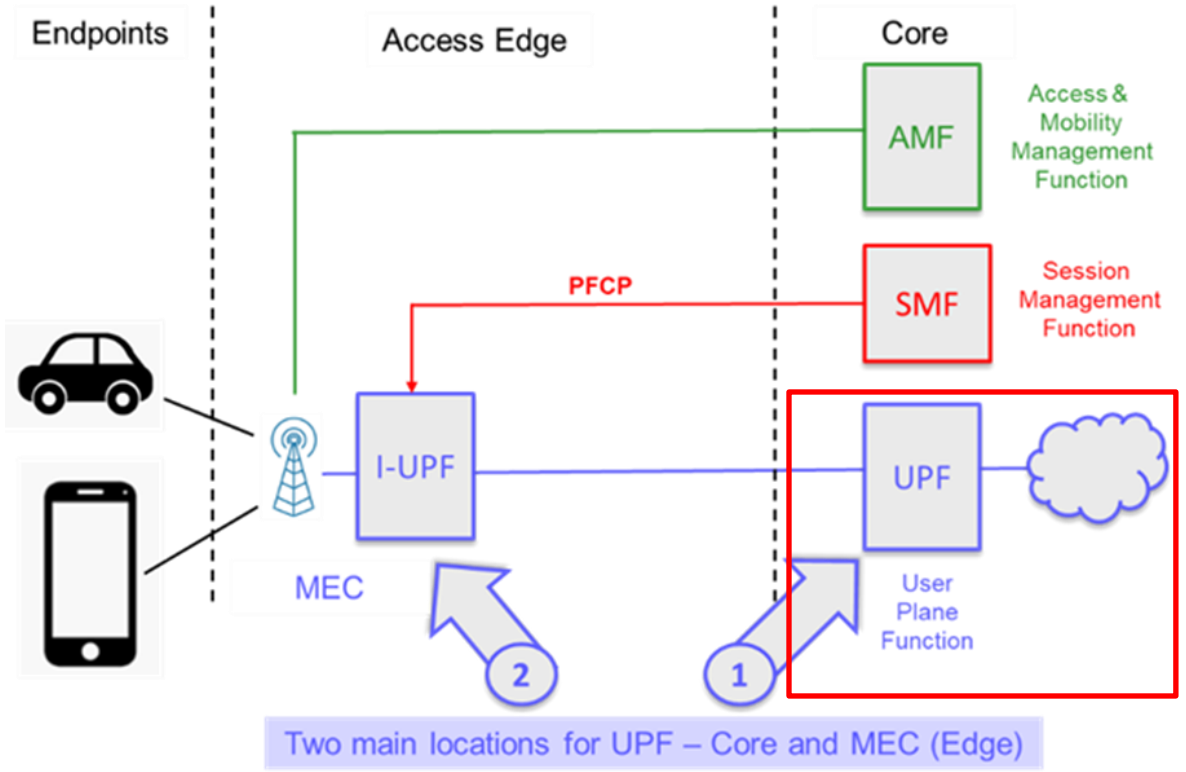
This means that you will never see a public IP address that begins with these prefixes

Smartphones get IP addresses just like normal hosts

Wi-Fi

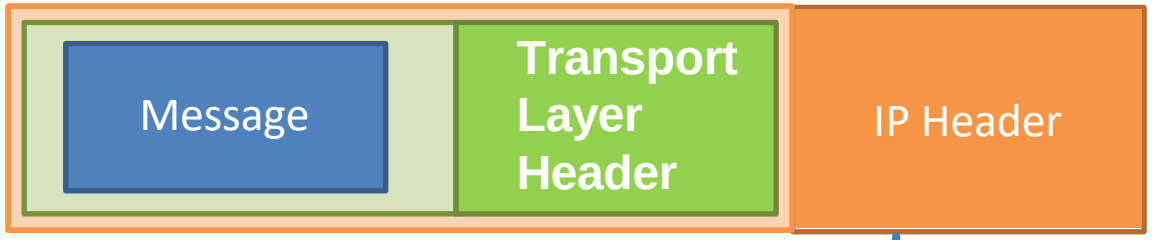


Cellular Network

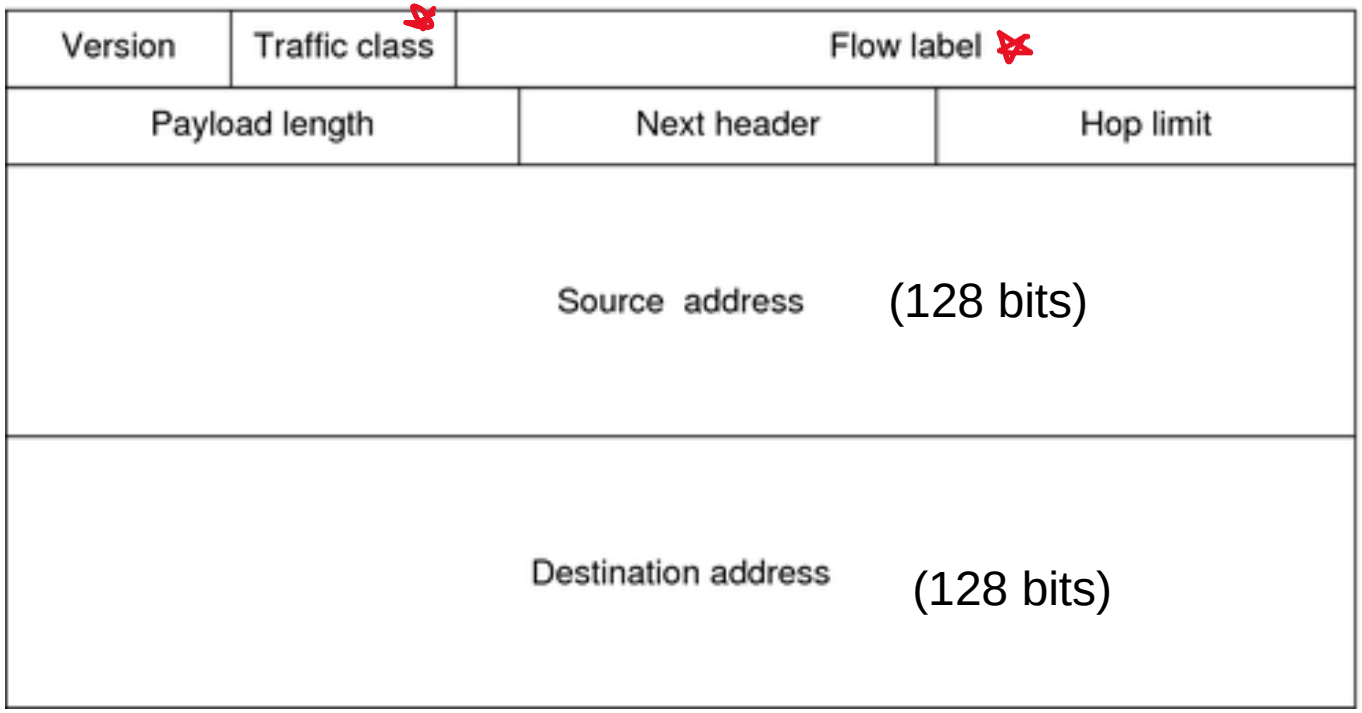


The **user plane function/packet gateway** handles things like NAT/DHCP for cellular networks

Packets traversing through the network layer are referred to as a **datagram**. Each packet gets an IPv4/IPv6 header



TCP header = 20 bytes
IP header = 20 bytes



IPv6 = **128 bits**

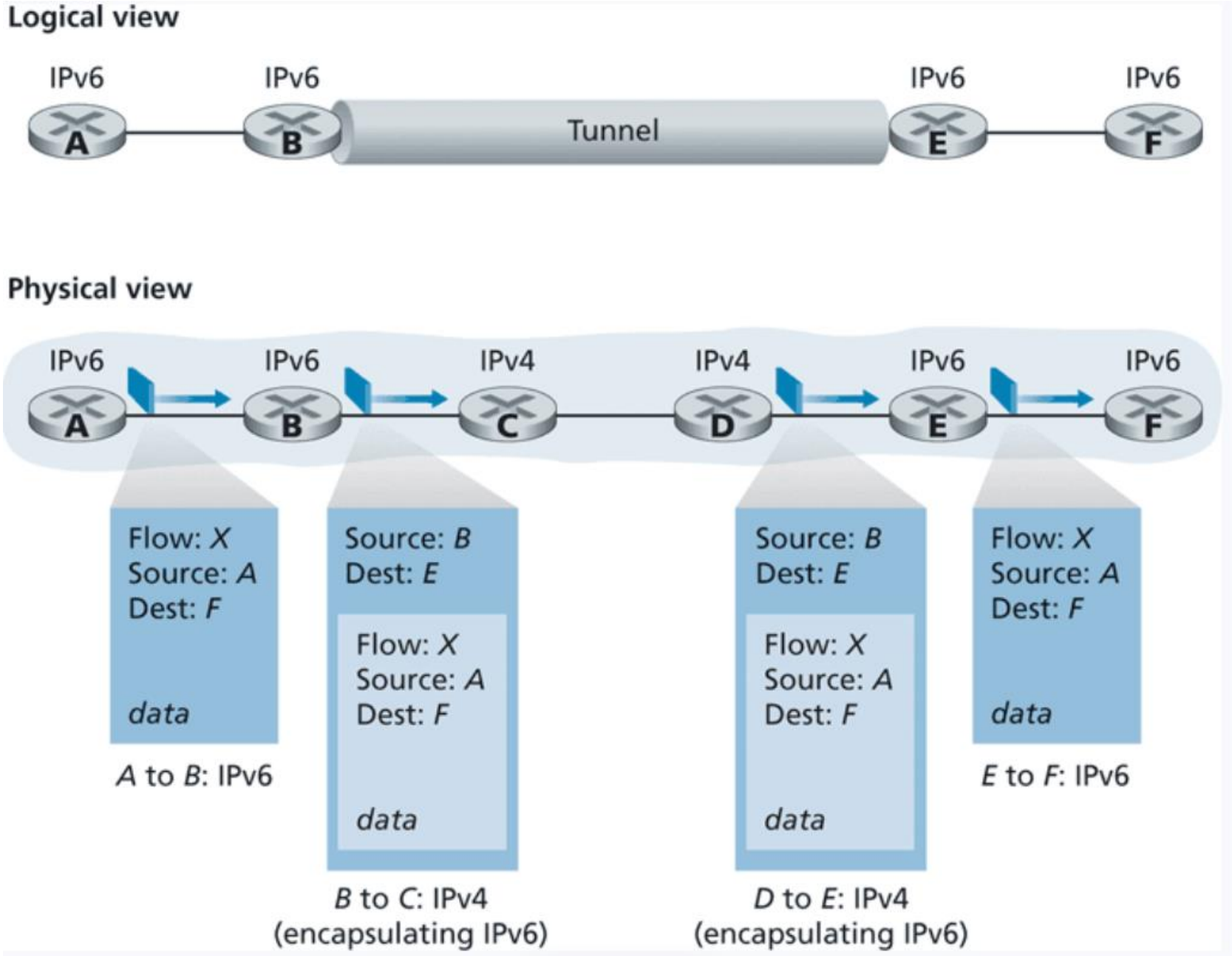
IPv6 Header

Issue: some routers use IPv4, some use IPv6, some use both. How do we get all networking equipment to coexist with each other?

Solution:

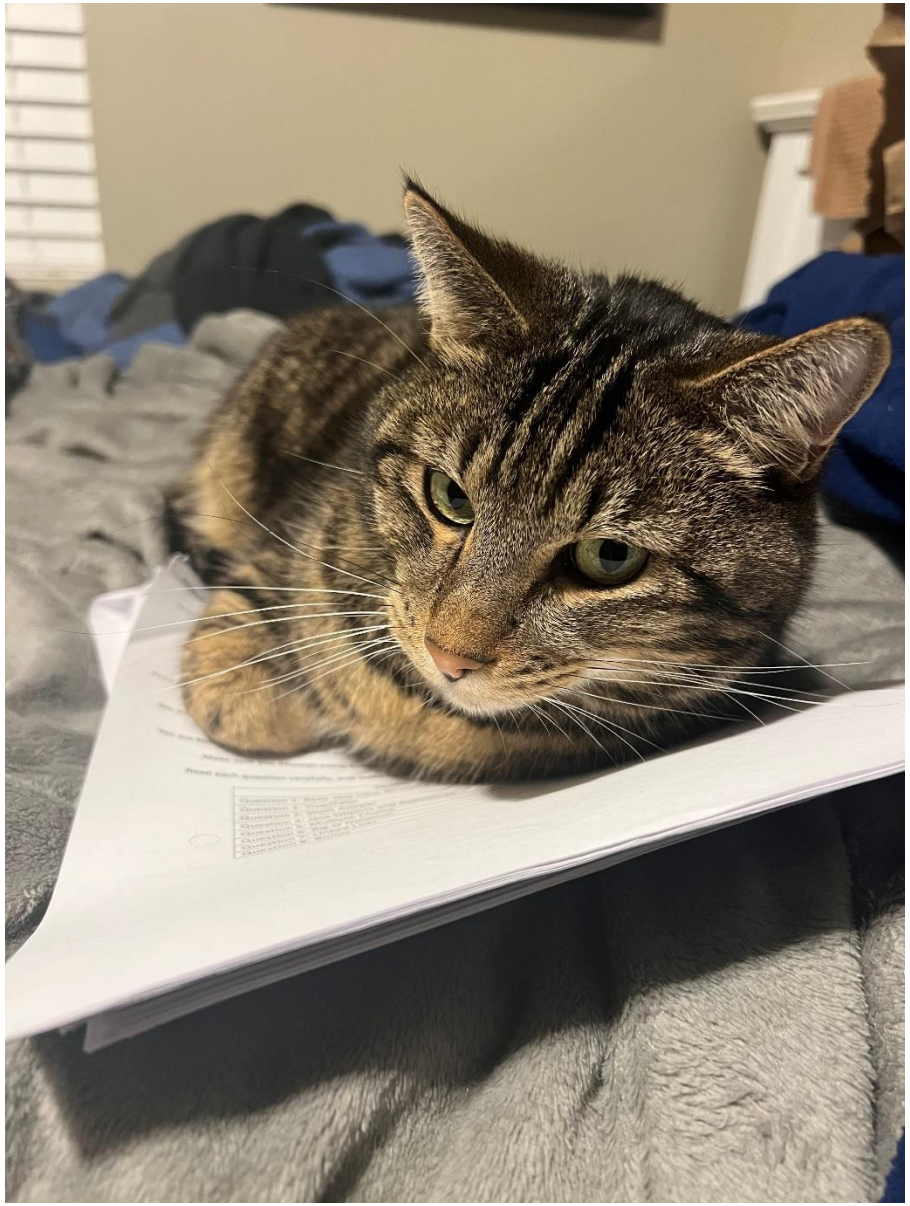
Issue: some routers use IPv4, some use IPv6, some use both. How do we get all networking equipment to coexist with each other?

Solution: **Tunneling**



tl:dr

We wrap our IPv6 datagram in an IPv4 header, and pass it to the IPv4 router!



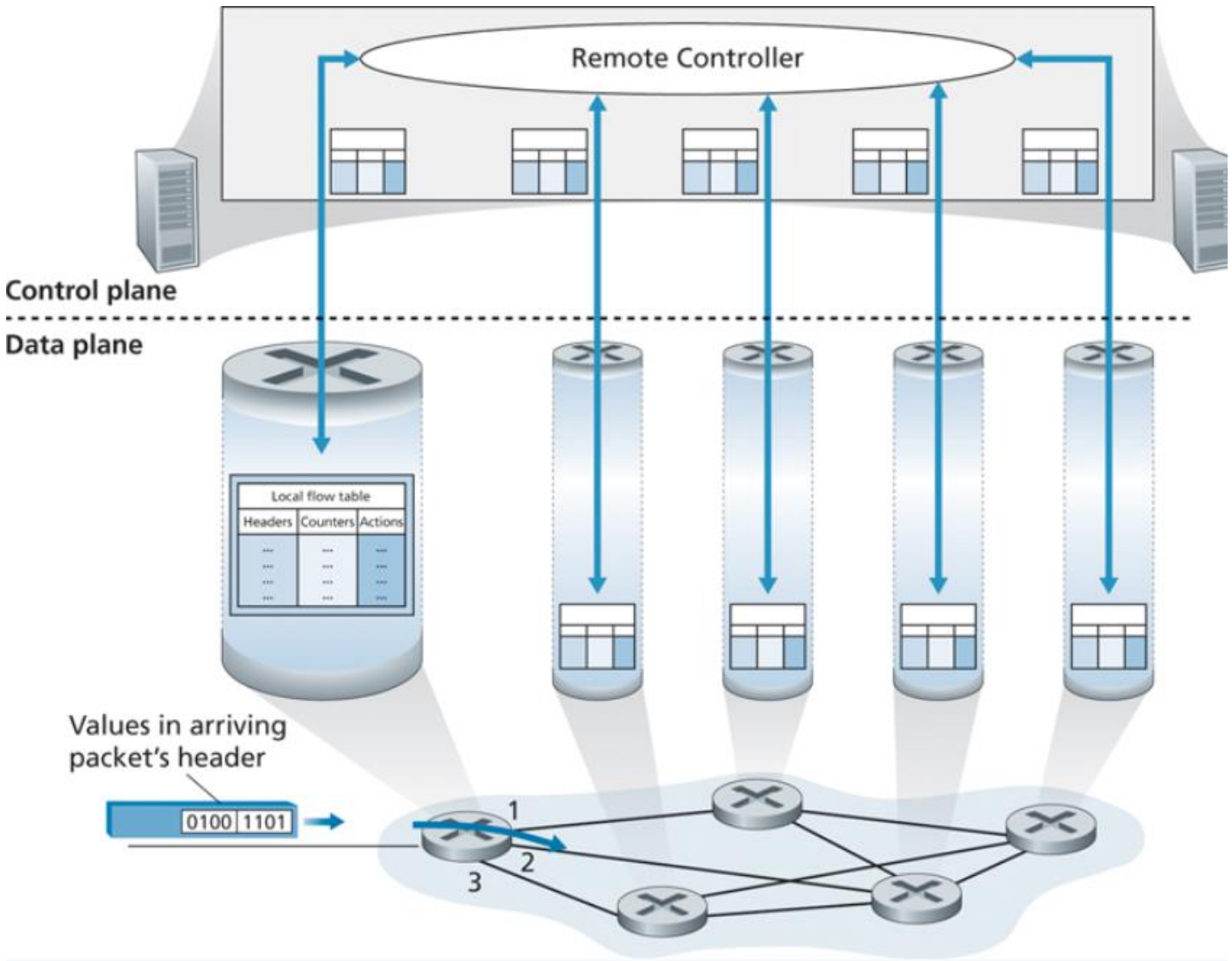
So far, a router takes input from input port, and then outputs on some output port

What else might a router need to do?

Forward, Drop stuff, Modify, Load balance

We need more flexibility and functionality with our forwarding!!

Generalized Forwarding and Software Defined Network (SDN)



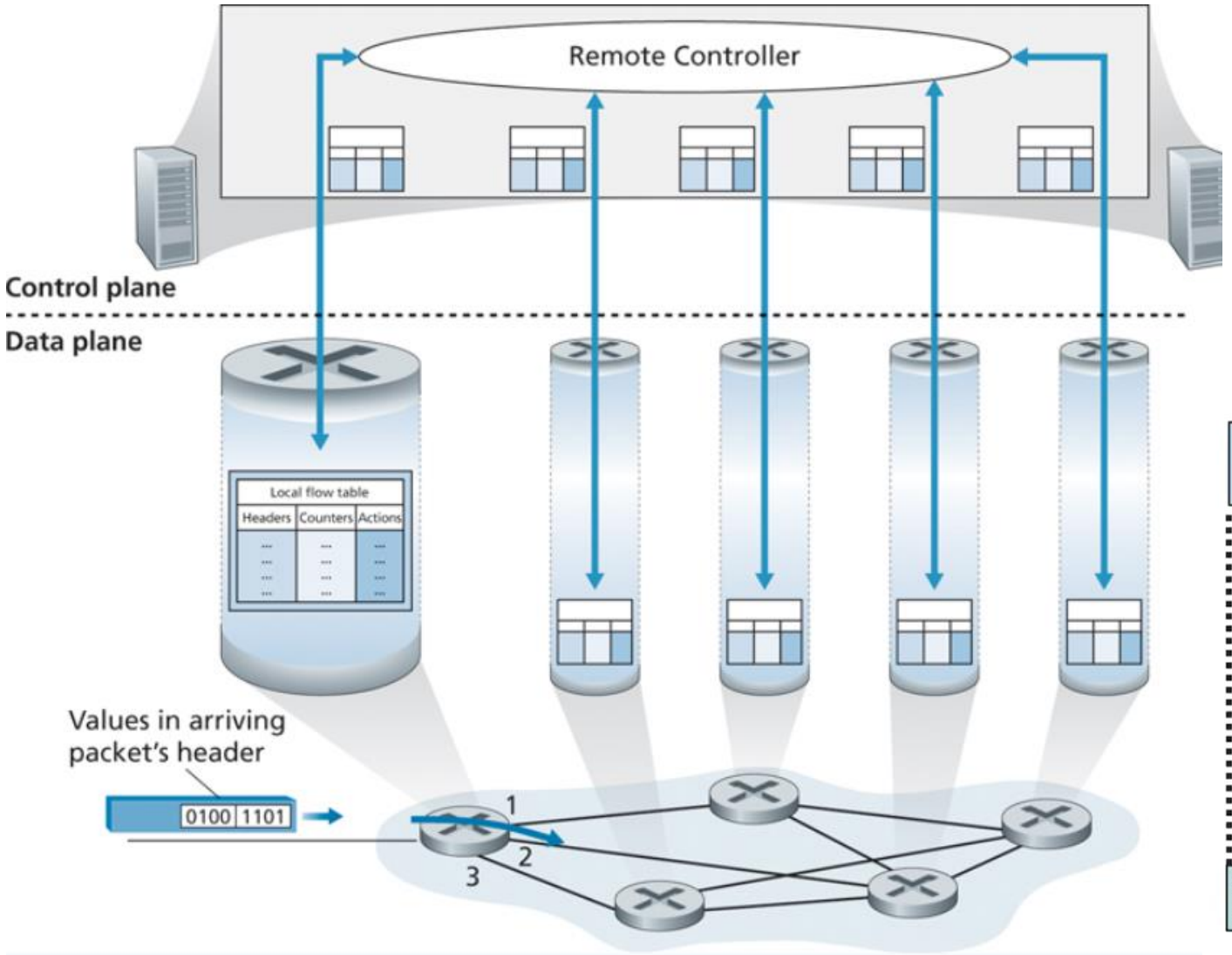
Uses **OpenFlow** standard

A remote controller fills the **flow tables** of each router

Flow tables are entries of match+action “rules”

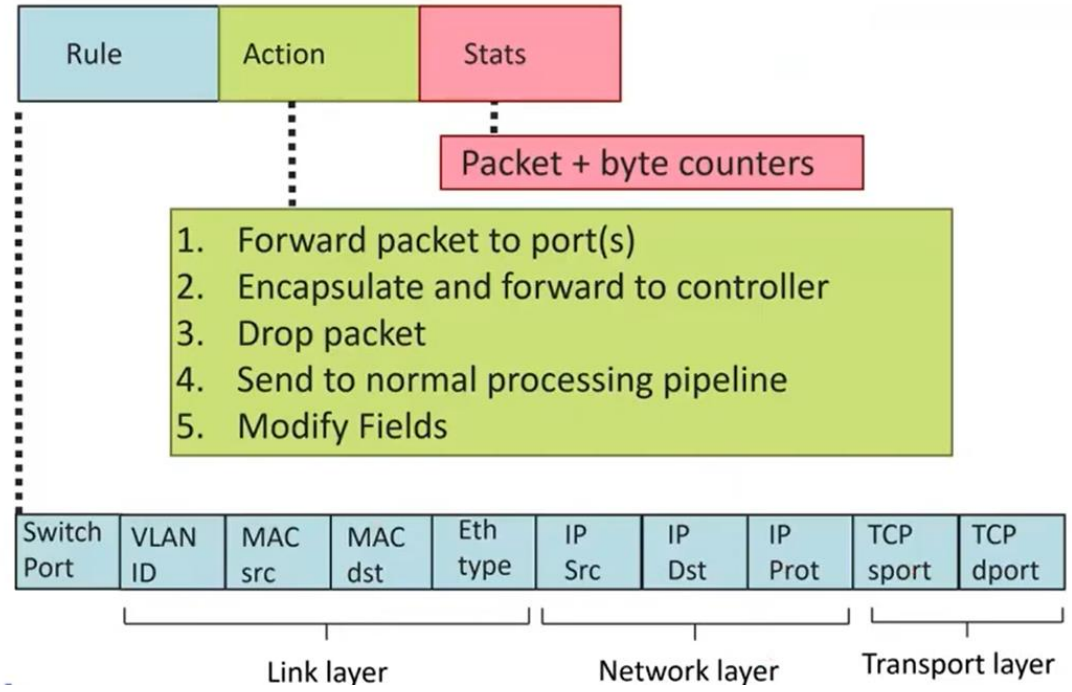
Generalized Forwarding and Software Defined Network (SDN)

Uses **OpenFlow** standard



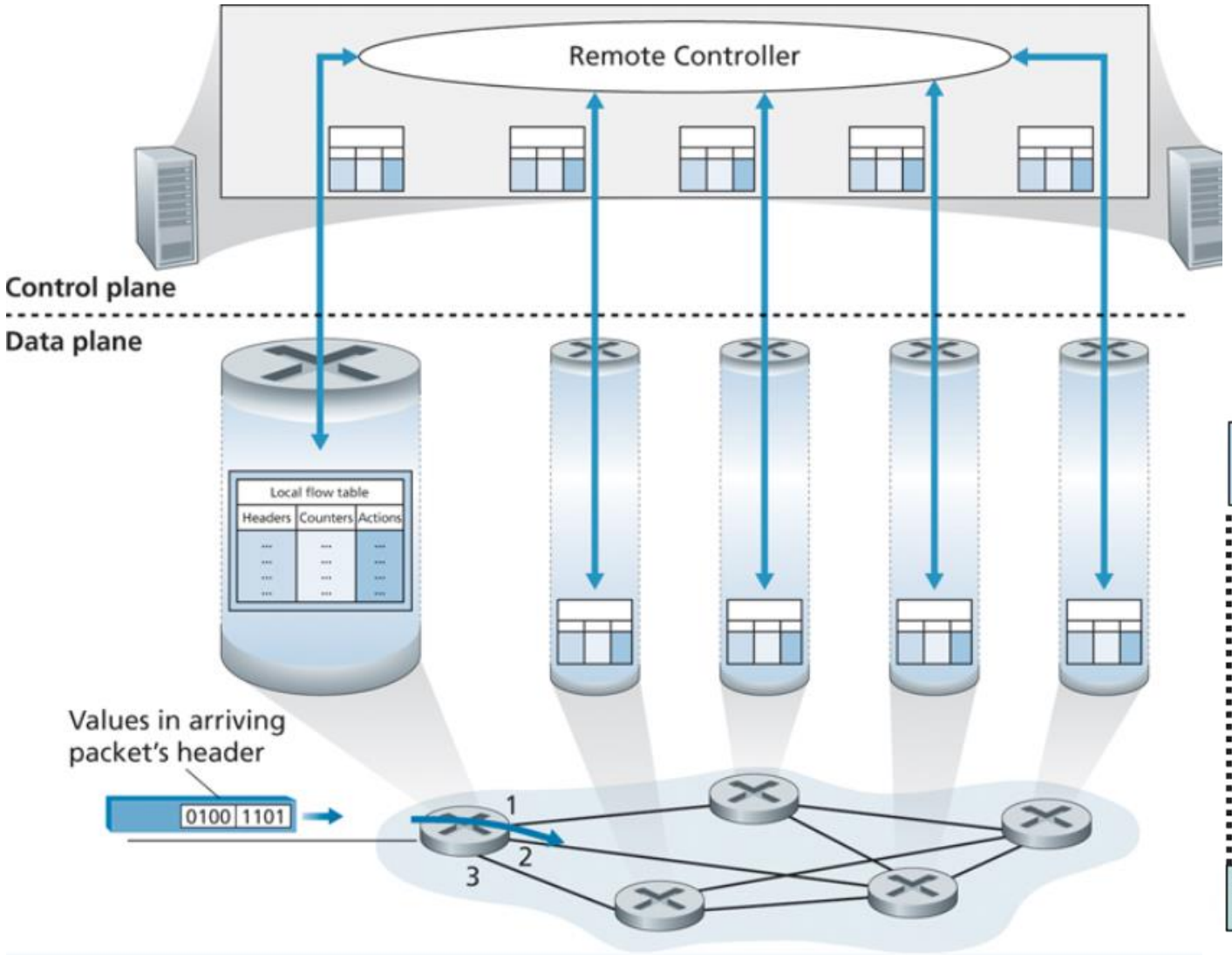
A remote controller fills the **flow tables** of each router

Flow tables are entries of match+action "rules"



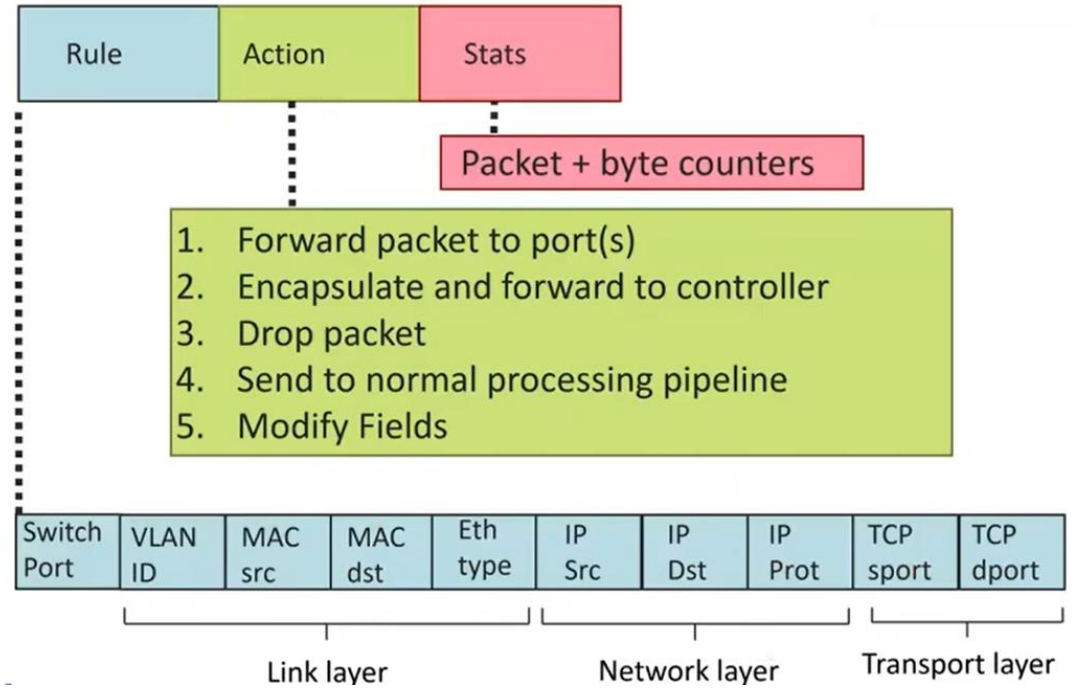
Generalized Forwarding and Software Defined Network (SDN)

Uses **OpenFlow** standard

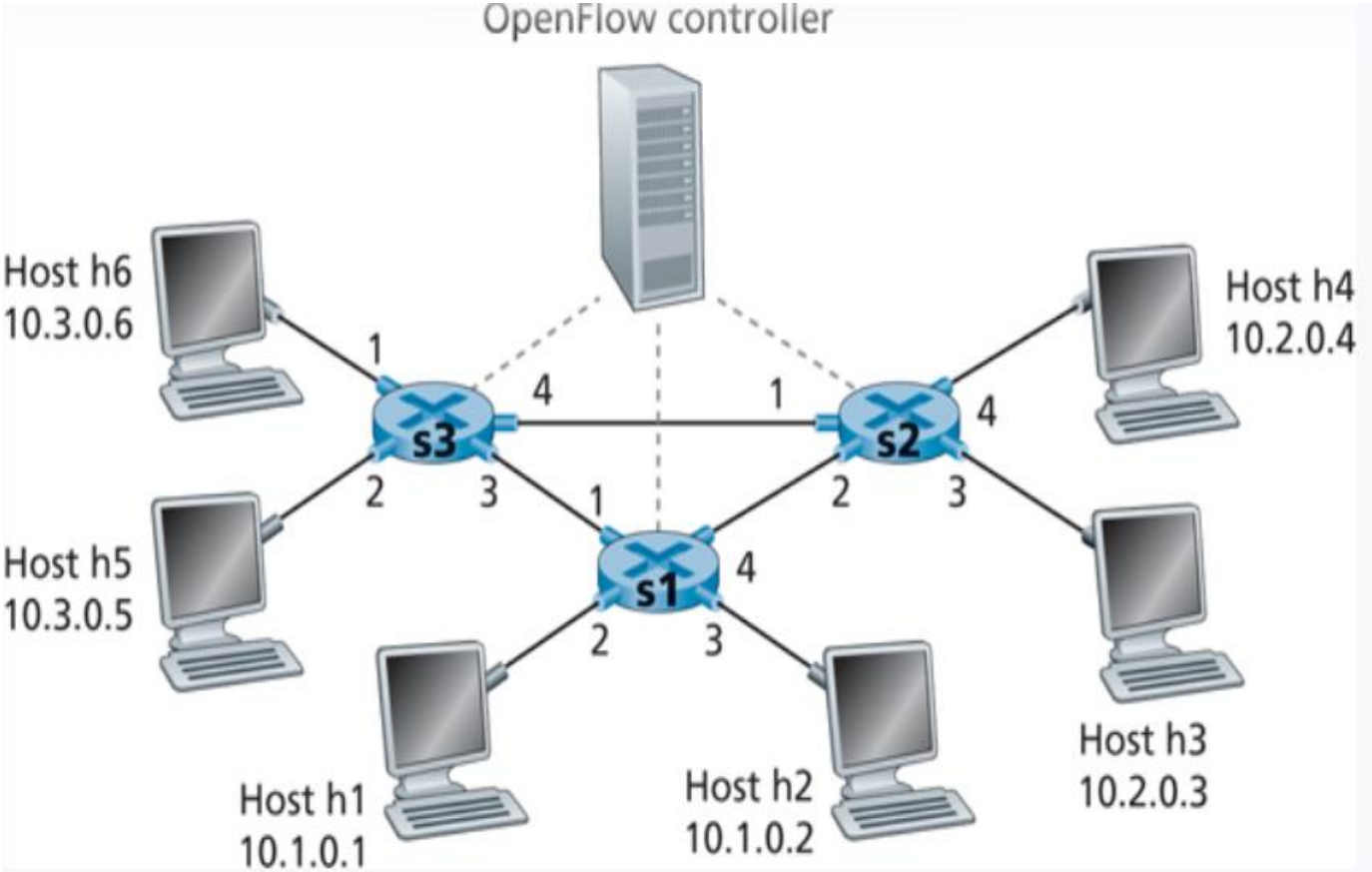


A remote controller fills the **flow tables** of each router

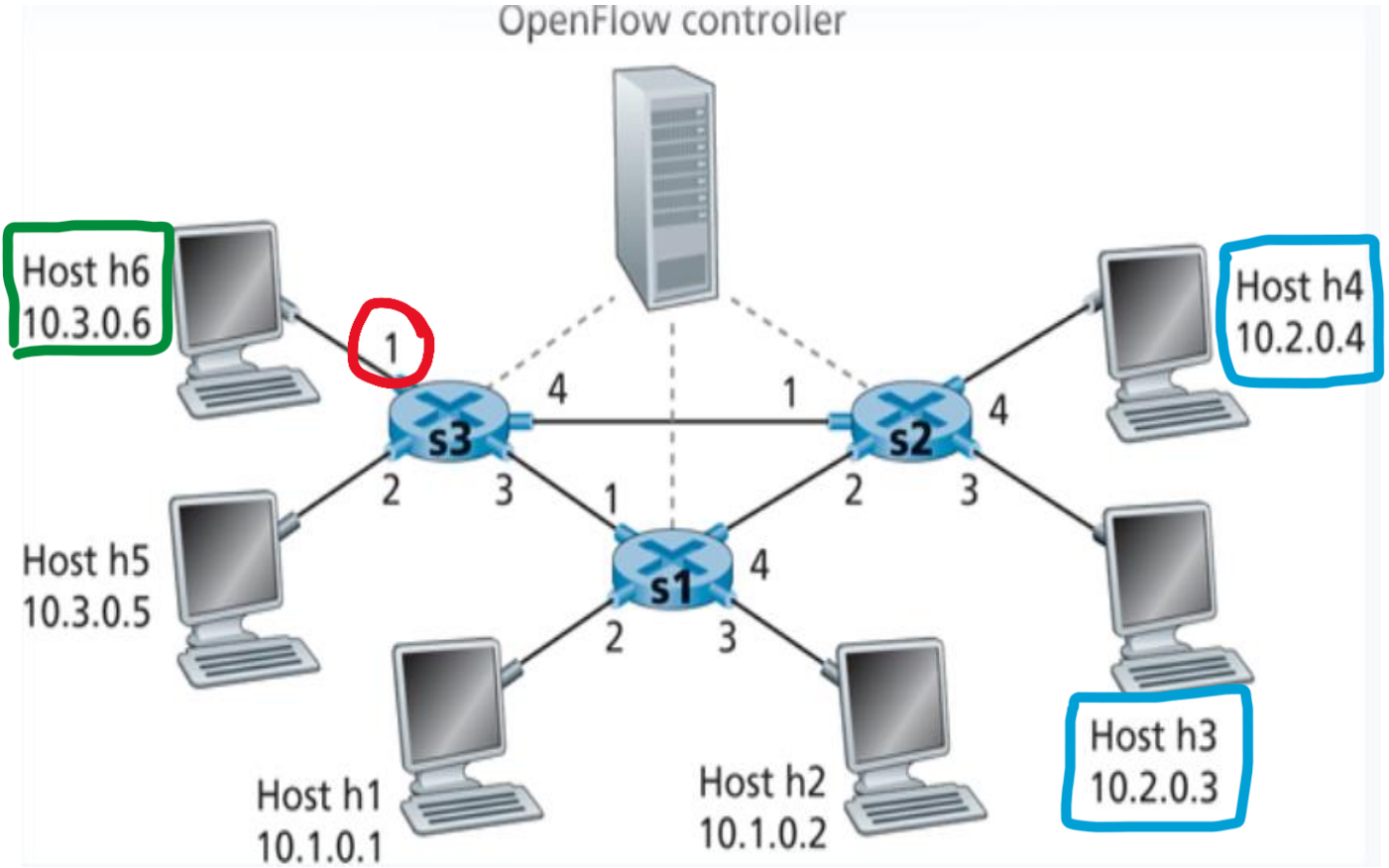
Flow tables are entries of match+action "rules"



Generalized Forwarding and Software Defined Network (SDN)

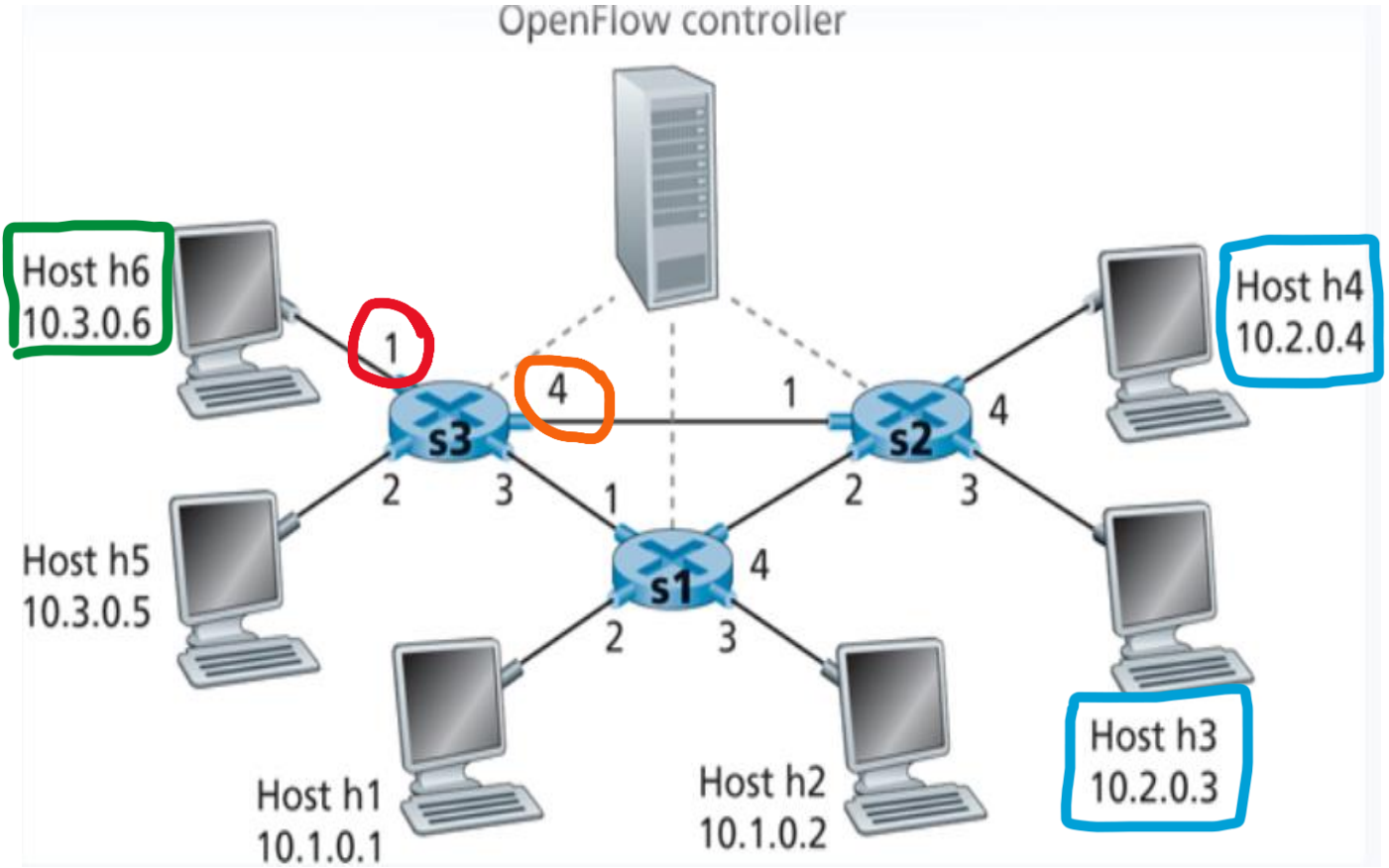


Generalized Forwarding and Software Defined Network (SDN)



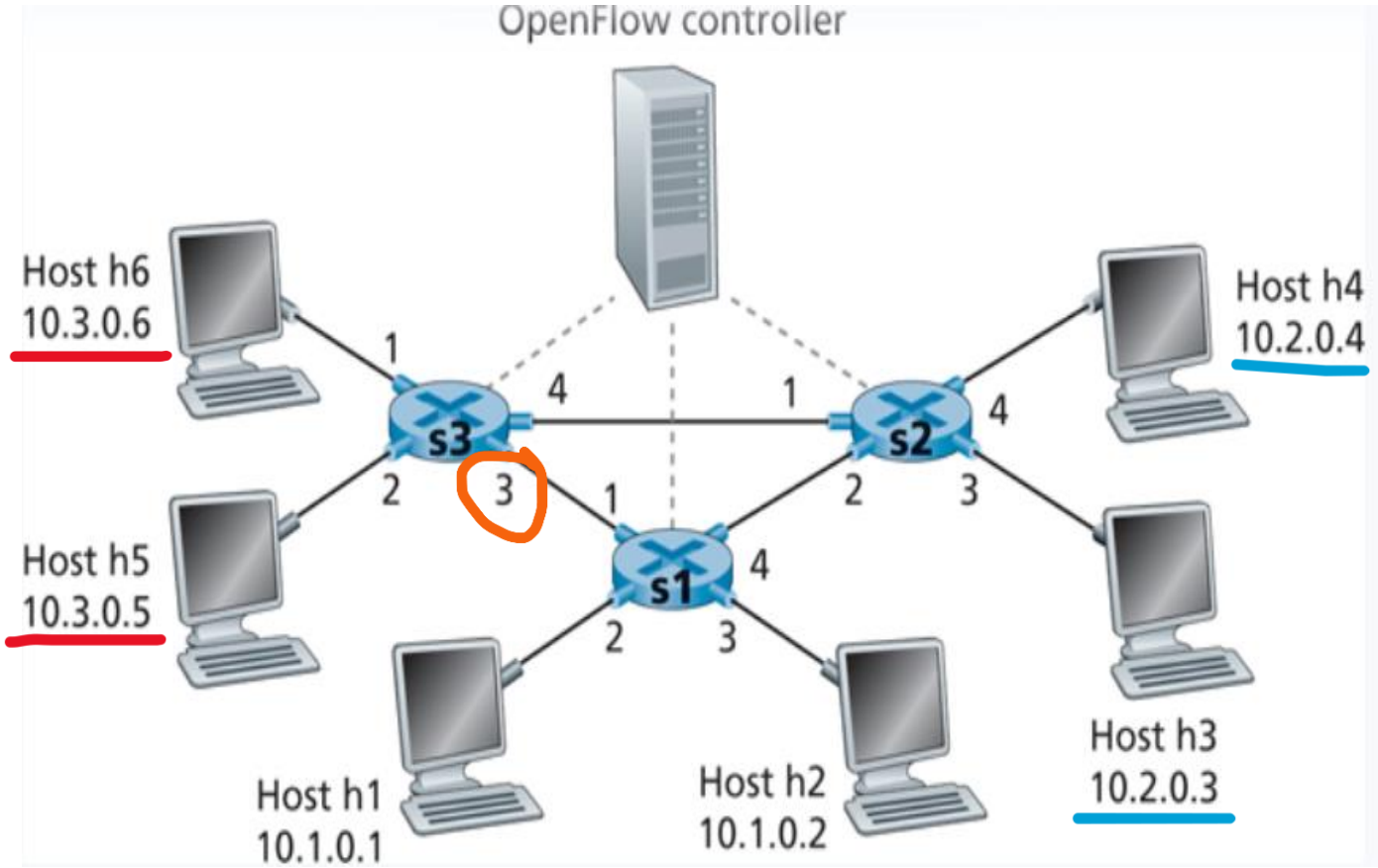
Match	Action
Ingress Port = 1 ; IP Src = 10.3.* .* ; IP Dst = 10.2.* .*	Forward(4)

Generalized Forwarding and Software Defined Network (SDN)



Match	Action
Ingress Port = 1 ; IP Src = 10.3.* .* ; IP Dst = 10.2.* .*	Forward(4)

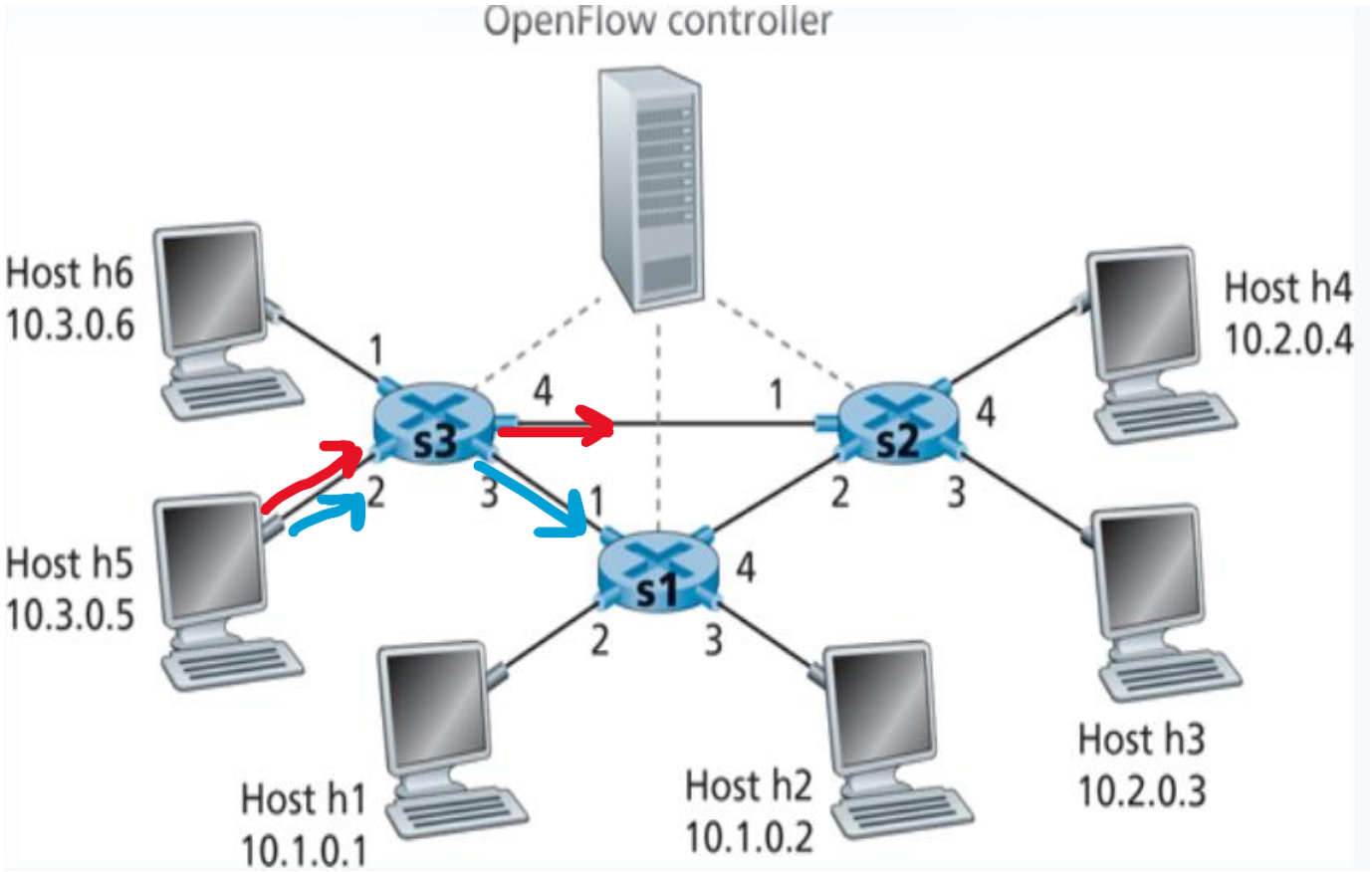
Generalized Forwarding and Software Defined Network (SDN)



Match	Action
Ingress Port = 1 ; IP Src = 10.3.*.* ; IP Dst = 10.2.*.*	Forward(4)

Match	Action
IP Src = 10.3.*.* ; IP Dst = 10.2.*.*	Forward(3)

Generalized Forwarding and Software Defined Network (SDN)



Match	Action
Ingress Port = 1 ; IP Src = 10.3.*.* ; IP Dst = 10.2.*.*	Forward(4)

Match	Action
IP Src = 10.3.*.* ; IP Dst = 10.2.*.*	Forward(3)

Match	Action
Ingress port = 2 ; IP Dst = 10.2.0.3	Forward(3)
Ingress port = 2 ; IP Dst = 10.2.0.4	Forward(4)

Load Balancing

Generalized Forwarding and Software Defined Network (SDN)

Destination-based forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
Pattern →	*	*	*	*	*	*	51.6.0.8	*	*	*	port6

← Action

IP datagrams destined to IP address 51.6.0.8 should be forwarded to router output port 6

Firewall:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Forward
*	*	*	*	*	*	*	*	*	22	drop

do not forward (block) all datagrams destined to TCP port 22

Destination-based layer 2 (switch) forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	22:A7:23:11:E1:02	*	*	*	*	*	*	*	*	port3

layer 2 frames from MAC address 22:A7:23:11:E1:02 should be forwarded to output port 6