



Network

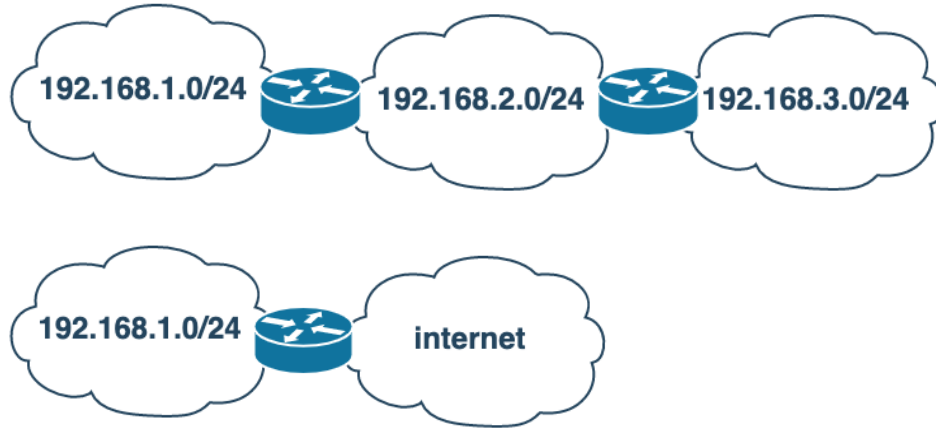
Network basic configuration IPv4

IP addressing

Okay. We have addressing on Ethernet, why we need another protocol with addressing?
We need IP for Routing,

Routing = ability to determine the path to travel across multiple networks.
Fragmenting = ability to split to smaller packets

Why we need routing?



Get IP address

```
[stepan@sun /]$ ifconfig
enp0s13f0u1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.78 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::71b7:eae0:bd4e:d798 prefixlen 64 scopeid 0x20<link>
    ether 94:05:bb:14:45:7e txqueuelen 1000 (Ethernet)
    RX packets 17138 bytes 12518717 (11.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9570 bytes 1020083 (996.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
[stepan@sun /]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlp0s20f3: <BROADCAST,MULTICAST> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 42:43:33:ba:57:18 brd ff:ff:ff:ff:ff:ff permaddr 90:cc:df:1e:31:38
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:94:63:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
4: enp0s13f0u1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 94:05:bb:14:45:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s13f0u1
        valid_lft 74875sec preferred_lft 74875sec
    inet6 fe80::71b7:eae0:bd4e:d798/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

How to get RIB

```
[stepan@sun /]$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.1     0.0.0.0          UG      100    0      0 enp0s13f0u1
192.168.1.0      0.0.0.0         255.255.255.0    U       100    0      0 enp0s13f0u1
192.168.122.0    0.0.0.0         255.255.255.0    U       0      0      0 virbr0
[stepan@sun /]$
```

```
[stepan@sun /]$ ip route
default via 192.168.1.1 dev enp0s13f0u1 proto dhcp metric 100
192.168.1.0/24 dev enp0s13f0u1 proto kernel scope link src 192.168.1.78 metric 100
192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1 linkdown
```

Default route = Default gateway = 0.0.0.0/0

Wireshark: IP address

Wireshark packet capture showing an HTTP GET request. The packet list shows four packets: a SYN, an ACK, another ACK, and a GET request. The packet details pane shows the structure of the GET request, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw hex and ASCII data of the request.

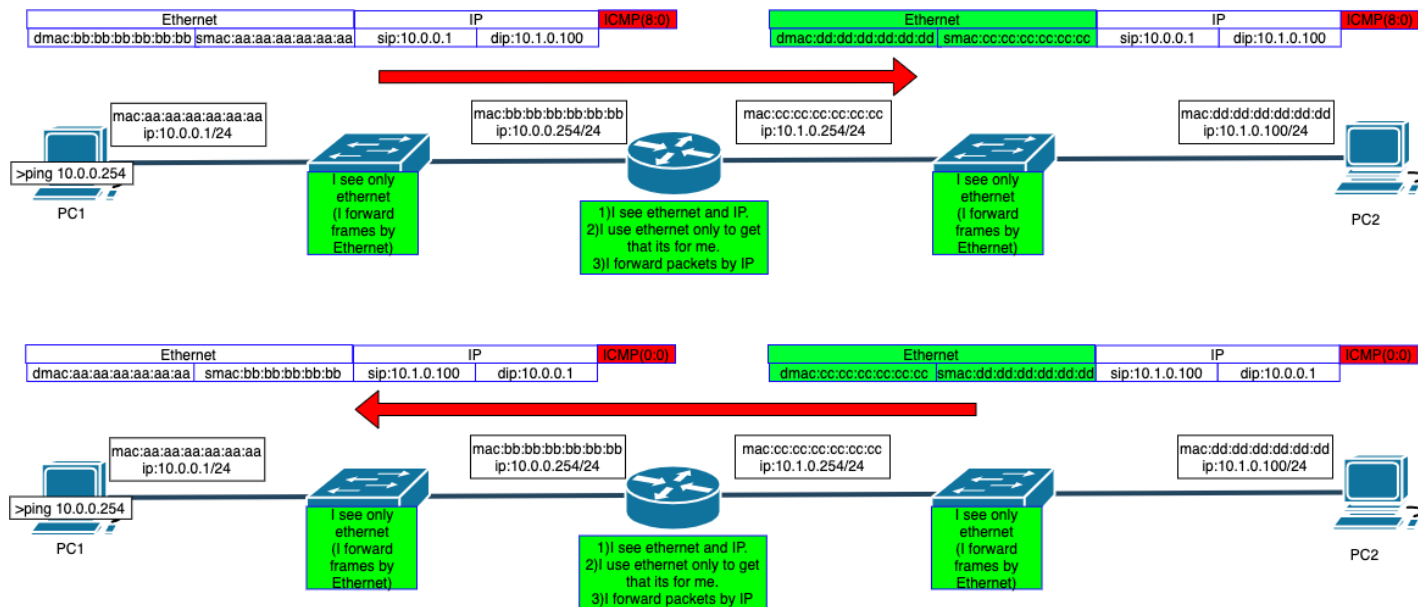
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 519
Identification: 0x0f45 (3909)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x9010 [validation disabled]
[Header checksum status: Unverified]
Source Address: 145.254.160.237
Destination Address: 65.208.228.223
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol

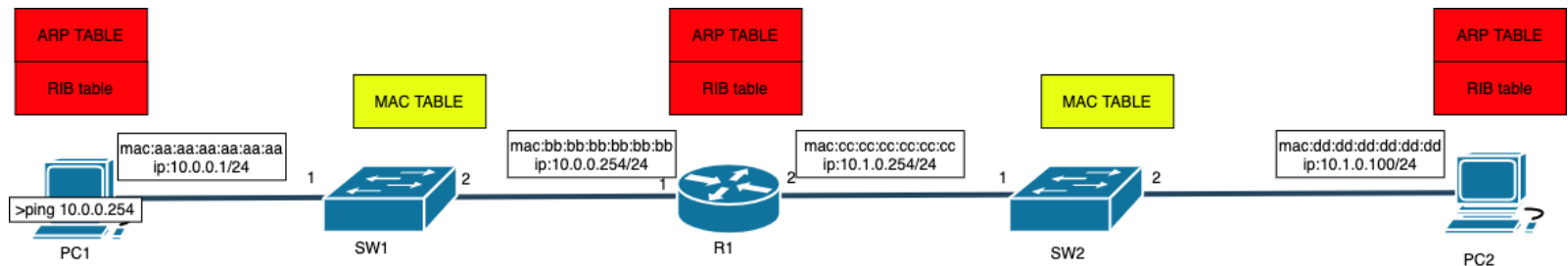
0010 02 07 0f 45 40 00 80 06 90 10 91 fe a0 ed 41 d0 ...E@... ..A.
0020 e4 df 0d 2c 00 50 38 af fe 14 11 4c 61 8c 50 18 ...P8...LaP
0030 25 bc ad 58 00 00 47 45 54 20 2f 64 6f 77 6e 6c %X·GE T/downl
0040 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e oad.html HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68 1·Host: www.eth
0060 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 d ereal.co m·User-
0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5
0080 2e 30 20 28 57 69 6a 64 6f 77 73 3b 20 55 3b 20 ·0 (Windw; U;
0090 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 Wndows NT 5.1;
00a0 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47 en-US; r v:1.6) G
00b0 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41 ecko/200 40113·A
00c0 63 63 65 74 3a 20 74 65 78 74 2f 78 6d 6c 2c ccept: t ext/xml,
00d0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c applicat ion/xml,
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm
00f0 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b l+xml,te xt/html;
0100 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e q=0.9,te xt/plain
0110 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67 ;q=0.8,i mage/png
0120 2c 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 ,image/j peg,imag
0130 65 2f 67 69 6b 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b e/gif;q= 0.2,w/;
0140 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.1·A ccept-La
0150 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e nguage: en-us,en
0160 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5· Accept-E
0170 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 ncoding: gzip,de
0180 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 flate·A ccept-Ch
0190 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d arset: I 50-8859-

What a router sees?

Network	sip, dip, routing table
	arp table
Data Link	smac, dmac
Physical	electricity/light, up/down



Lets talk about the tables. Again.



PC1:
ARP:
10.0.0.254-bb:bb:bb:bb:bb:bb

RIB:
0.0.0.0/0 via 10.0.0.254
OR
10.1.0.100/32 via 10.0.0.254
OR
10.1.0.0/24 via 10.0.0.254
OR
10.0.0.0/8 via 10.0.0.254
Etc...

SW1:
MACtable:
Aa:aa:aa:aa:aa:aa port 1
Bb:bb:bb:bb:bb:bb port 2

R1:
ARP:
10.0.0.10-aa:aa:aa:aa:aa:aa
10.1.0.100-dd:dd:dd:dd:dd:dd

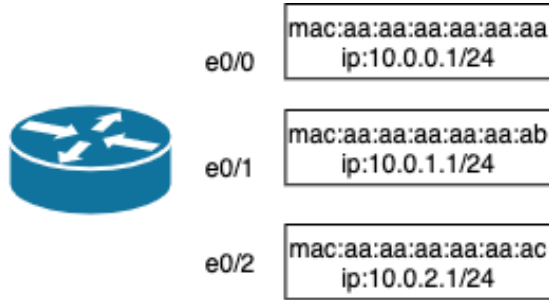
RIB:
10.0.0.0/24 via connected port 1
10.1.0.0/24 via connected port 2

SW2
MACtable
Cc:cc:cc:cc:cc:cc port 1
Dd:dd:dd:dd:dd:dd port 2

PC2
ARP
10.1.0.254 - cc:cc:cc:cc:cc:cc

RIB:
0.0.0.0/0 via cc:cc:cc:cc:cc:cc
OR
10.0.0.1/24 via 10.1.0.254
Etc...

Connected vs Static Routing



No static routes, but

RIB:

10.0.0.0/24 connected via e0/0

10.0.1.0/24 connected via e0/1

10.0.2.0/24 connected via e0/2

Added static route

8.8.8.8/32 via 10.0.0.1

RIB:

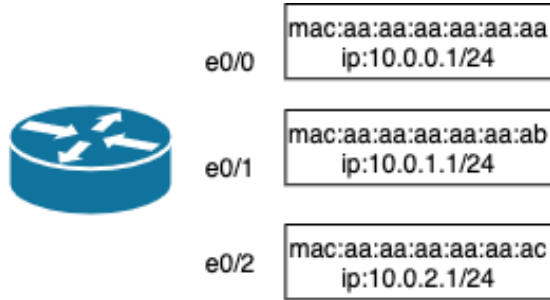
10.0.0.0/24 connected via e0/0

10.0.1.0/24 connected via e0/1

10.0.2.0/24 connected via e0/2

8.8.8.8/32 via e0/0 (static)

Connected vs Static Routing



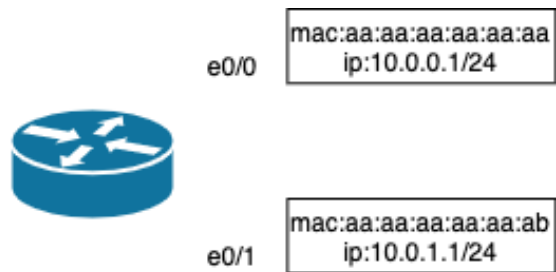
If e0/0 is down

RIB:

10.0.1.0/24 connected via e0/1

10.0.2.0/24 connected via e0/2

Connected vs Static Routing



Static route
10.0.0.0/24 via e0/1

RIB:
10.0.0.0/24 connected via e0/0
10.0.0.0/24 via e0/1
10.0.1.0/24 connected via e0/1

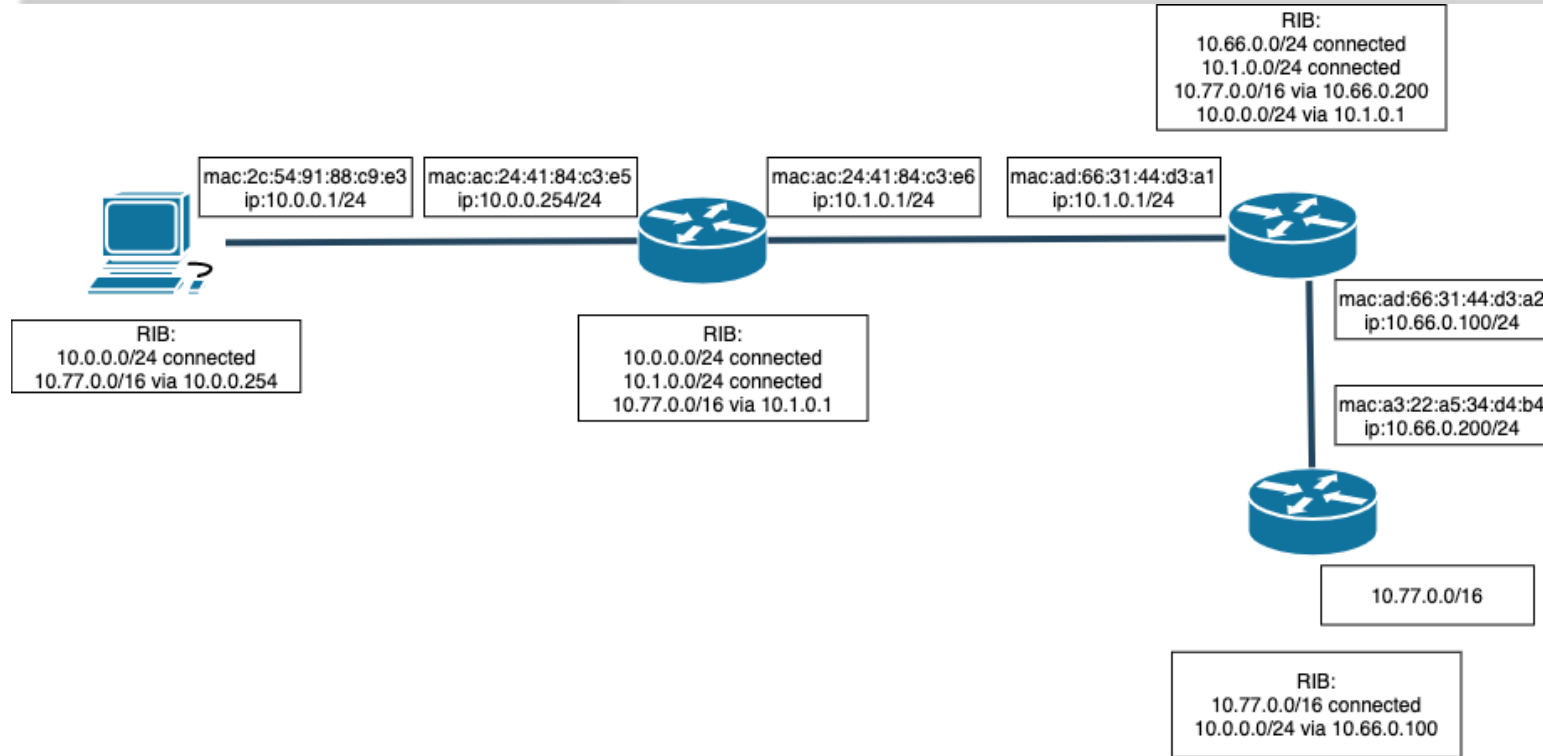
Connected > static (always)

Routing configuration

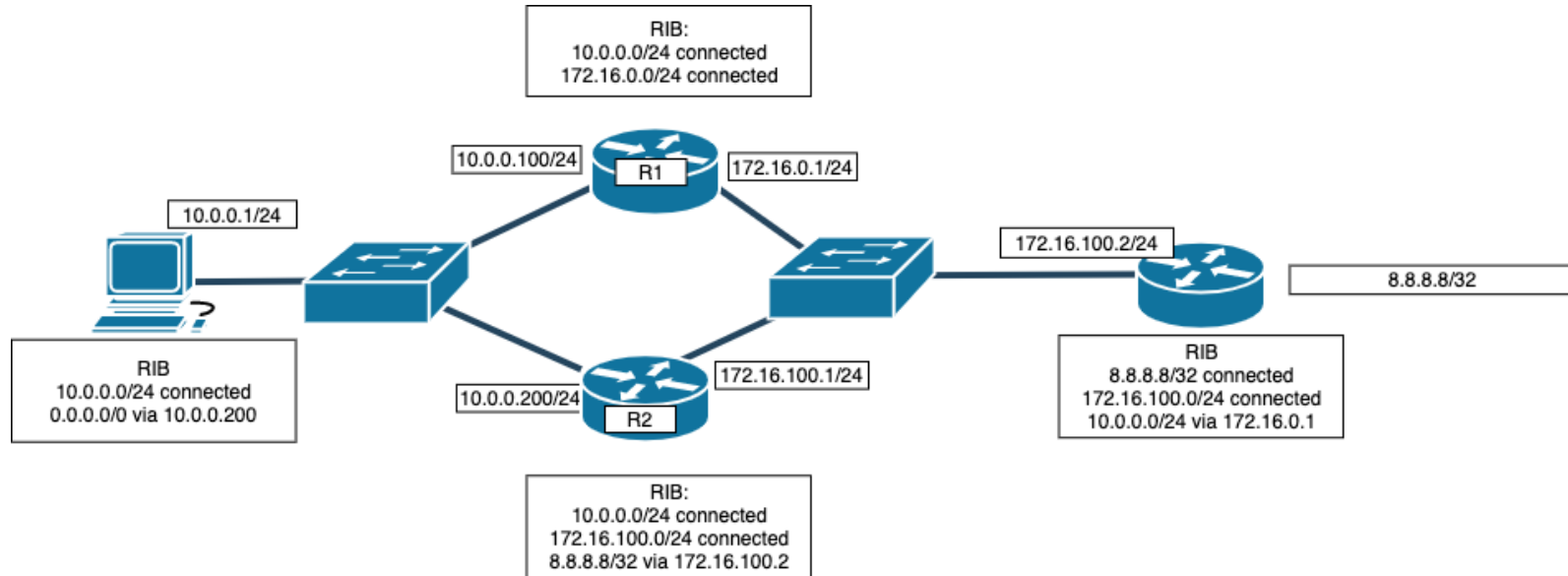
```
ip route add {NETWORK/MASK} via {GATEWAYIP}  
ip route add {NETWORK/MASK} dev {DEVICE}  
ip route add default {NETWORK/MASK} dev {DEVICE}  
ip route add default {NETWORK/MASK} via {GATEWAYIP}
```

```
ip route add 10.0.0.0/24 via 10.0.0.100
```

Many static routes



Indirect routing, manipulations

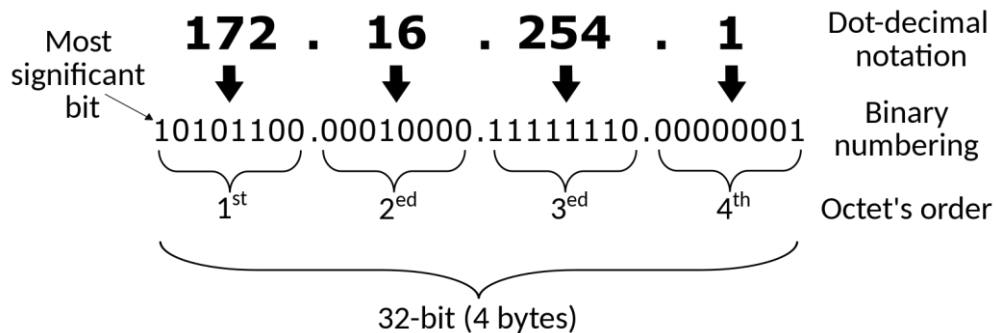


Routing

Routing = lookup in the RIB (what is the my interface to get that IP?)
Encapsulations to Ethernet

```
[stepan@sun /]$ ping 1111  
PING 1111 (0.0.43.103) 56(84) bytes of data.
```

```
[stepan@sun /]$ ping 87263458  
PING 87263458 (5.51.136.226) 56(84) bytes of data.
```



Routing

RIB

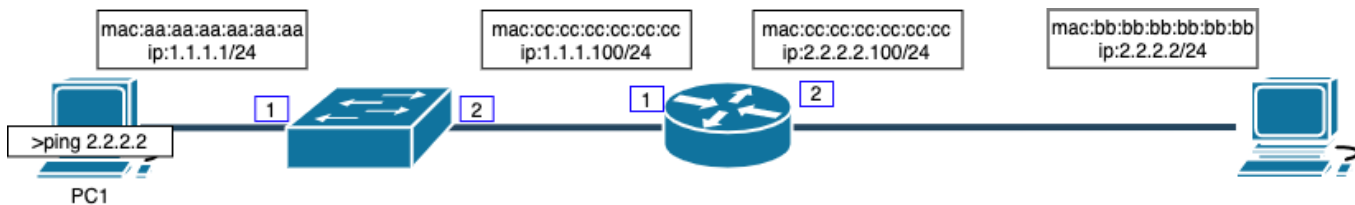
- 1) 8.8.8.0/24 via 192.168.1.254
- 2) 0.0.0.0/0 via 192.168.1.254
- 3) 8.8.8.8/32 via 192.168.1.254

If ping <> which route will use:

- 1) 8.8.8.8
- 2) 8.8.8.7
- 3) 1.1.1.1

Hometask1

Ethernet		IP		ICMP
dmac	smac	sip	dip	



Hometask2

ipconfig/ifconfig

Get ip address, mac address

Start wireshark

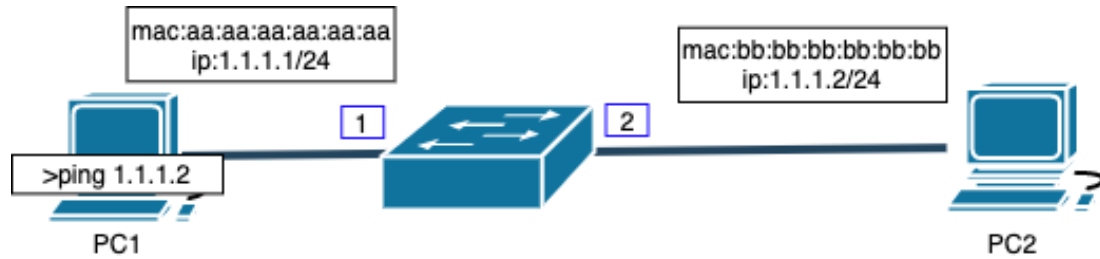
Ping 8.8.8.8

Do you see ARP, IP, Ethernet?

Try open youtube/google or something HTTP

Do you see ARP, IP, Ethernet, TCP, HTTP?

Hometask3



THANK YOU