

IP Address and Communication Mechanism

- Mechanism to identify devices from all over the world.
- Routing technology for acquiring destination routes.
(The role of subnet mask and default gateway)
- The role of MAC addresses in Ethernet.

Table of contents

1. IP address overview

2. IP address type and allocation

3. How routing works

4. Ethernet and MAC address

1. IP address overview

1-1. What are RFCs?

1-2. What is TCP/IP?

1-3. Protocol stack

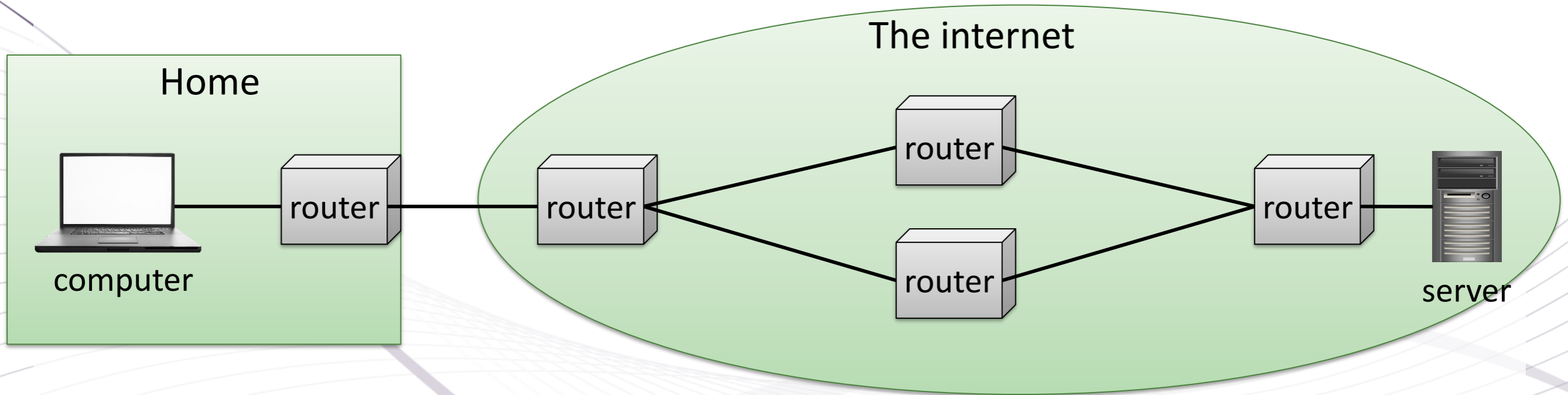
1-4. Packet data (capture)

1-5. "IPv4" and "IPv6"

1-6. IP address data format

1-1. What are RFCs?

All devices involved in Internet communication must handle data using a predetermined technology. Therefore, standardization (arrangement) of Internet technology is being carried out. This standardization is called RFC.

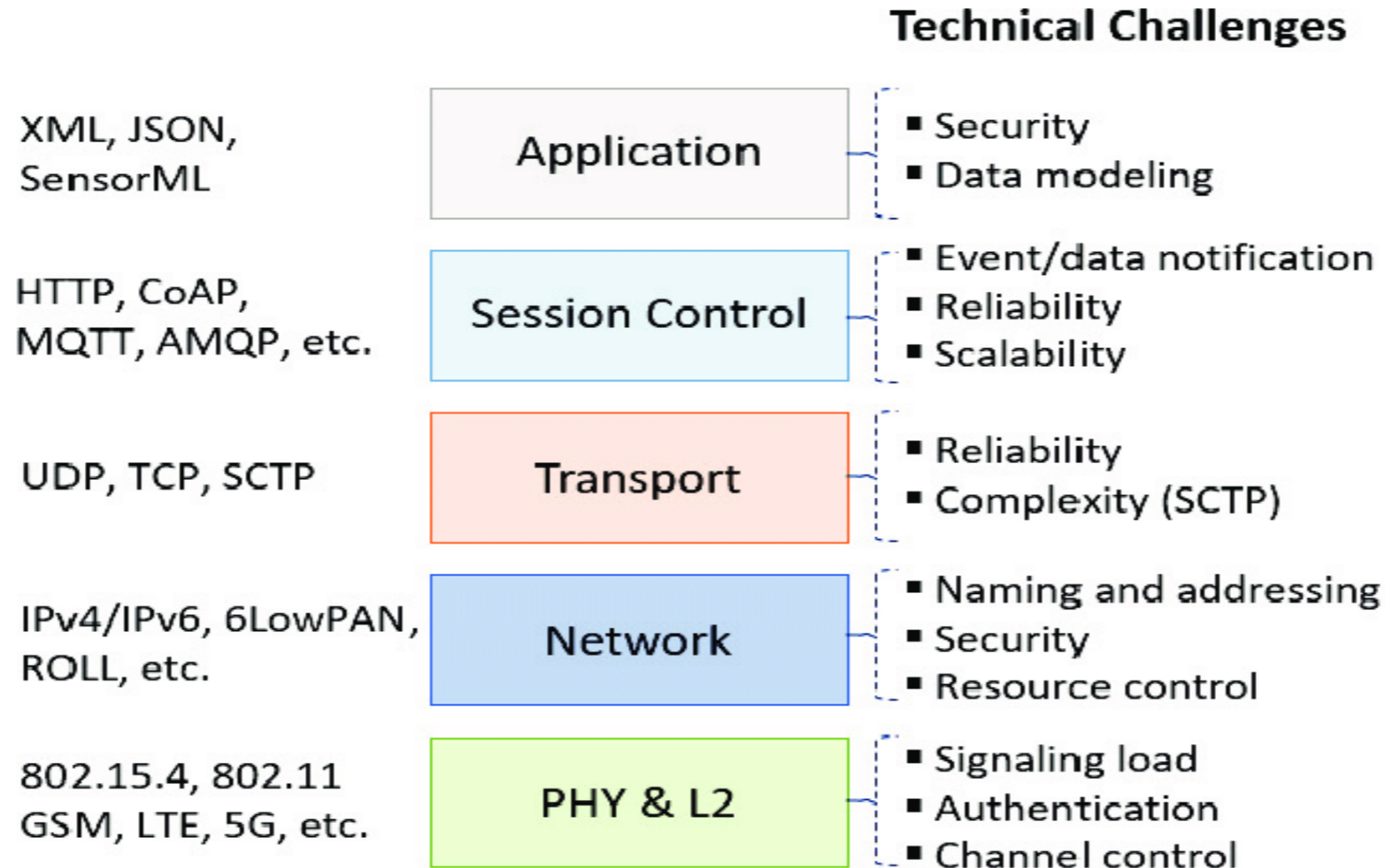


- Standardization organization: IETF (Internet Engineering Task Force)
 - Standardized regulations: RFC (Request for Comments)
- 1) IP: RFC791 (IPv4), RFC8200 (IPv6)
 - 2) TCP: RFC9293

1-2. What is TCP/IP?

- **TCP/IP** Regulations for communication on the Internet.
 - ① **IP** : The role of representing addresses on the Internet.
 - ② **TCP** : The role of delivering data efficiently and reliably according to the state of the communication path.
- **UDP/IP**
 - ③ **UDP** : It does not perform communication control just to deliver.

1-3. Protocol stack



https://www.researchgate.net/figure/Protocol-Stack-and-Technical-Challenges_fig1_320453832

- Match the rules used by each layer at the transmitting and receiving terminals.
- There is no dependency between layers.
Determine the rules to be used for each layer.

1-4. Packet capture (Wireshark)

The image shows a Wireshark packet capture window titled 'http_cap.pcapng'. The main pane displays a list of 12 network packets. Packet 5 is highlighted with a red box and is an HTTP GET request from 192.168.1.7 to 157.7.107.210. Below the packet list, the packet details pane shows the structure of packet 5: Ethernet II (14 bytes), Internet Protocol Version 4 (20 bytes), Transmission Control Protocol (20 bytes), and Hypertext Transfer Protocol. The raw packet bytes pane shows the hexadecimal and ASCII representation of the packet, with red boxes highlighting the Ethernet II header, IP header, and TCP header. Annotations with arrows point to these sections: 'Ethernet: 14Byte' points to the Ethernet II header, 'IP: 20Byte' points to the IP header, and 'TCP: 20Byte' points to the TCP header.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.7	157.7.107.210	TCP	66	53275 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000364	192.168.1.7	157.7.107.210	TCP	66	59662 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.015081	157.7.107.210	192.168.1.7	TCP	66	80 → 53275 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1414 SACK_PERM=1 WS=128
4	0.015193	192.168.1.7	157.7.107.210	TCP	54	53275 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5	0.016168	192.168.1.7	157.7.107.210	HTTP	614	GET / HTTP/1.1
6	0.016390	157.7.107.210	192.168.1.7	TCP	66	80 → 59662 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1414 SACK_PERM=1 WS=128
7	0.016462	192.168.1.7	157.7.107.210	TCP	54	59662 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
8	0.031443	157.7.107.210	192.168.1.7	TCP	60	80 → 53275 [ACK] Seq=1 Ack=561 Win=30336 Len=0
9	0.542488	157.7.107.210	192.168.1.7	TCP	392	80 → 53275 [PSH, ACK] Seq=1 Ack=561 Win=30336 Len=338 [TCP segment of a reassembled PDU]
10	0.543525	157.7.107.210	192.168.1.7	TCP	2882	80 → 53275 [ACK] Seq=339 Ack=561 Win=30336 Len=2828 [TCP segment of a reassembled PDU]
11	0.543622	192.168.1.7	157.7.107.210	TCP	54	53275 → 80 [ACK] Seq=561 Ack=3167 Win=131328 Len=0
12	0.544684	157.7.107.210	192.168.1.7	TCP	8538	80 → 53275 [ACK] Seq=3167 Ack=561 Win=30336 Len=8484 [TCP segment of a reassembled PDU]

Packet 5 details:

- Ethernet II, Src: Tp-LinkT 09:d6:7d (28:ee:52:09:d6:7d), Dst: Mitsubis 86:d6:65 (10:4b:46:86:d6:65)
- Internet Protocol Version 4, Src: 192.168.1.7, Dst: 157.7.107.210
- Transmission Control Protocol, Src Port: 53275, Dst Port: 80, Seq: 1, Ack: 1, Len: 560
- Hypertext Transfer Protocol

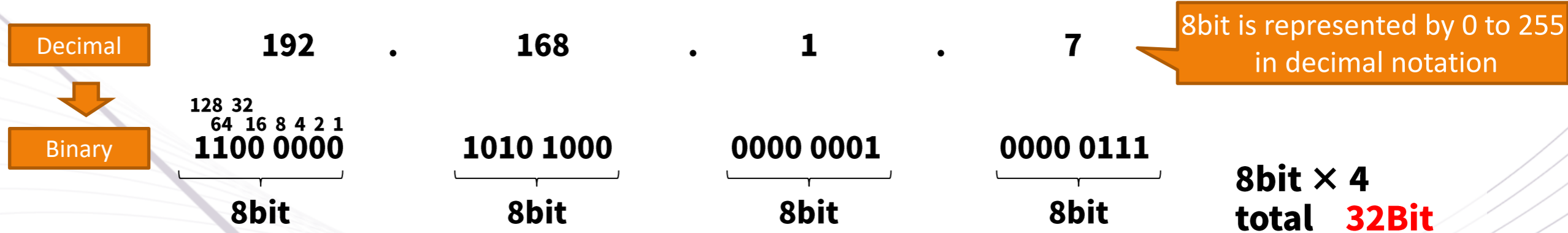
Raw packet bytes (hex and ASCII):

```
0000 10 4b 46 86 d6 65 28 ee 52 09 d6 7d 08 00 45 00  .KF..e(. R..}..E.  
0010 02 58 15 30 40 00 80 06 18 e7 c0 a8 01 07 9d 07  .X.0@... ..  
0020 6b 42 d0 1b 00 50 38 57 b9 9e 16 b5 52 a1 50 18  k...P8W....R.P.  
0030 02 01 e5 e0 00 00 47 45 54 20 2f 20 48 54 54 50  .....GE T / HTTP  
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6d 61 6e 61  /1.1..Ho st: mana  
0050 6b 61 6e 2e 6e 65 74 0d 0a 43 6f 6e 6e 65 63 74  kan.net..Connect  
0060 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d  ion: kee p-alive.  
0070 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72  .Upgrade -Insecur  
0080 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55  e-Request: 1..U  
0090 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c  ser-Agen t: Mozil
```

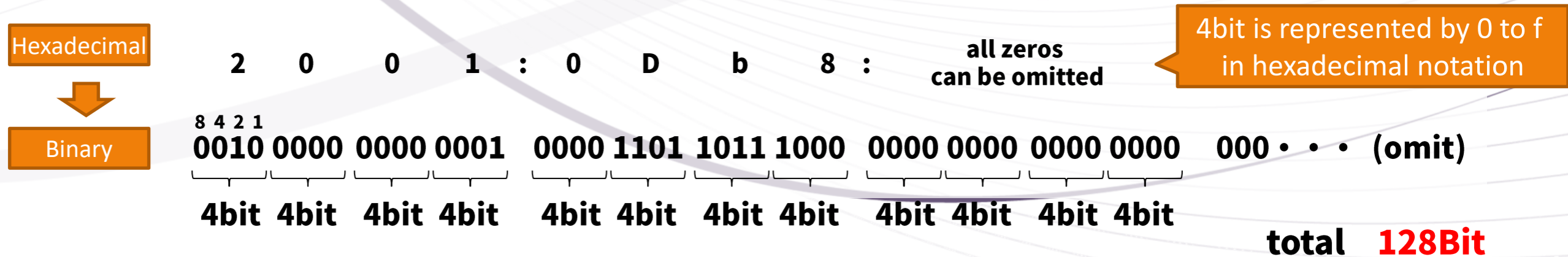
1-5. "IPv4" and "IPv6"

Difference in number of bits used for address

- **IPv4 Identify with 32bit.** ➔ 2 to the 32nd power, so "4,294,967,296 (about 430 million)"

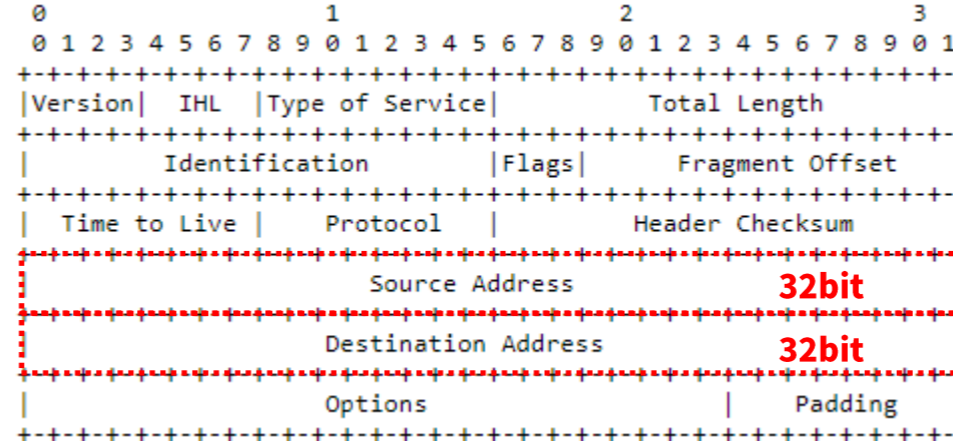


- **IPv6 Identify with 128bit.** ➔ 2 to the 128th power, so "3.4 x 10 to the 32nd power"



1-6. IP data format (Excerpt from the prescribed RFC)

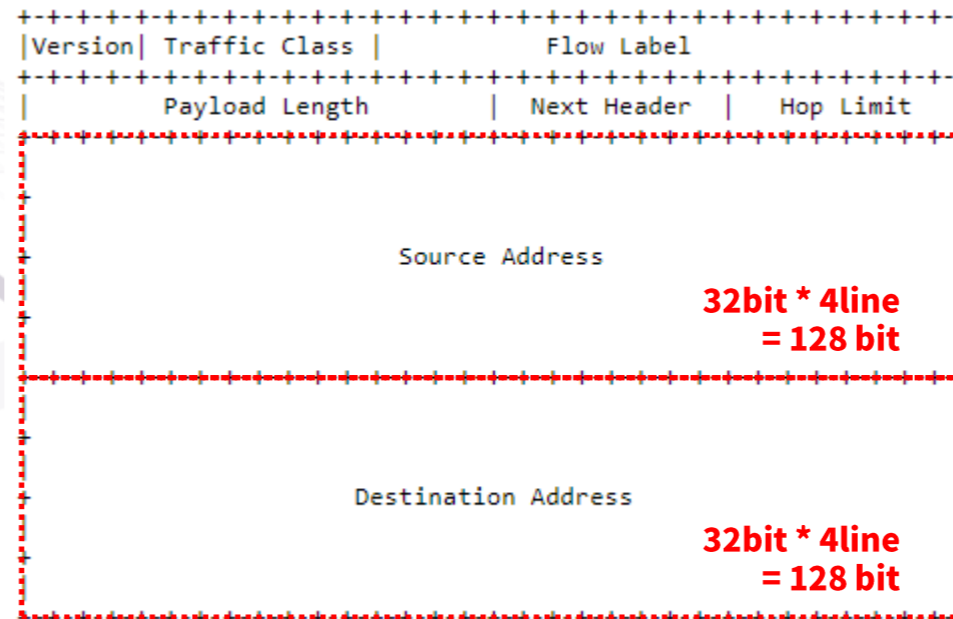
- **IPv4 RFC791**



The basic size is **20 bytes**
(1 line is 32bit, so 4 bytes)

[Optional]
variable in size depending on
the required options.

- **IPv6 RFC8200**



The basic size is **40 bytes**
(1 line is 32bit, so 4 bytes)

32bit * 4line
= 128 bit

32bit * 4line
= 128 bit

2. Types and allocation of IP addresses

2-1. Classes and CIDR

2-2. IP address management organization and allocation

2-3. Global and private

2-4. Internet communication with a private IP address

2-1. Classes and CIDR



- **Class:** As shown in the table below, build a network in units of a predetermined size → **more waste**

Class	address range	Network part	number of terminals
Class A	0.0.0.0 ~ 127.255.255.255	8 Bit	about 16 million
Class B	128.0.0.0 ~ 191.255.255.255	16 Bit	about 65000
Class C	192.0.0.0 ~ 233.255.255.255	24 Bit	254
Class D/E	224.0.0.0 ~ 255.255.255.255	(for multicast and reservation)	-

- **CIDR (Classless Inter-Domain Routing) :** Free use regardless of class

This is commonly used

Set a subnet mask to clearly separate the network part and the host part.

example) 1.0.16.0 / 20
 192.168.10.0 / 23

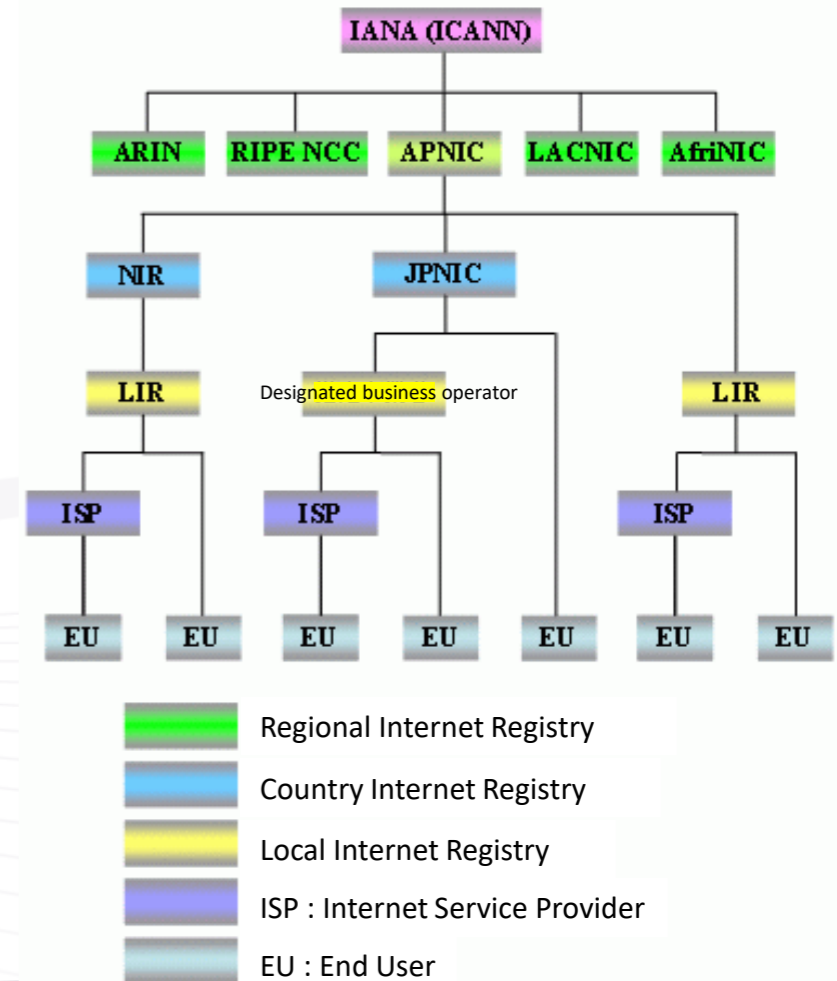
2-2. IP address management organization and allocation

- Strictly manage IP addresses so that they do not overlap around the world
- In Japan, they are distributed and managed in the following order, so that the location can be specified.
IANA → APNIC → JPNIC → ISP → End user

IP address management organization

Region	Management organization	Note
world	IANA (Internet Assigned Numbers Authority)	Managed on a global level
Asia	APNIC (Asia-Pacific Network Information Centre)	Dividing world into 5 regions
Japan	JPNIC (Japan Network Information Center)	Managed at country level

Management organization structure



Assignment to Japan

<https://ipv4.fetus.jp/jp>

CIDR	IPアドレス	割り振り日	レジストリ
1.0.16.0/20	1.0.16.0 - 1.0.31.255	2011/04/12	APNIC
1.0.64.0/18	1.0.64.0 - 1.0.127.255	2011/04/12	APNIC
1.1.64.0/18	1.1.64.0 - 1.1.127.255	2011/04/12	APNIC
1.5.0.0/16	1.5.0.0 - 1.5.255.255	2011/04/01	APNIC
1.21.0.0/18	1.21.0.0 - 1.21.63.255	2010/06/16	APNIC
1.21.64.0/19	1.21.64.0 - 1.21.95.255	2010/06/16	APNIC
1.21.96.0/20	1.21.96.0 - 1.21.111.255	2010/06/16	APNIC
1.21.112.0/20	1.21.112.0 - 1.21.127.255	2010/06/16	APNIC
1.21.128.0/20	1.21.128.0 - 1.21.143.255	2010/06/16	APNIC

Japan: 190,438,656

- 4.43% of total address space
- 5.14% excluding reservations

<https://www.nic.ad.jp/ja/ip/admin.html>

2-3. Global and private IP addresses

● Global IP address

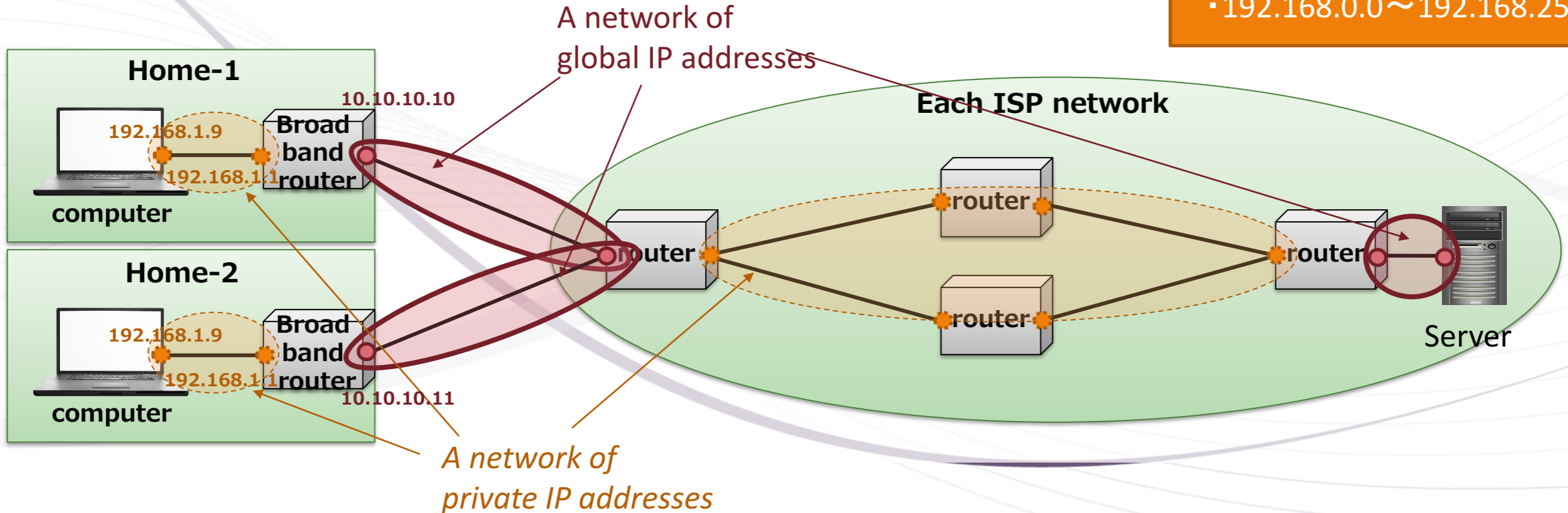
Unique address in the world
(can be identified from all over the world, so it is used for internet communication)

● Private IP address

An address that is used repeatedly in a network in each home or company.
(It cannot be specified from all over the world, but it is unique within the network without duplication))

【Private IP address Range】

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255



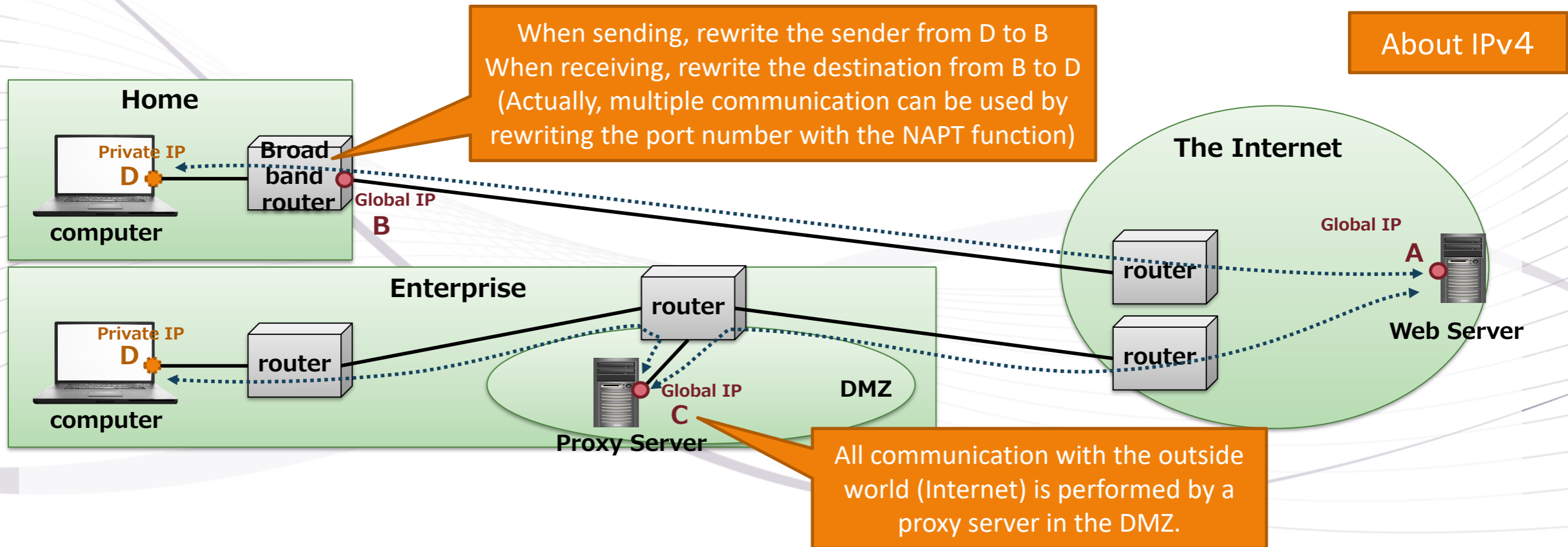
2-4. Internet use with private IP address

- Use of private IP at each home

Communication by replacing the global IP address with the private IP address on the broadband router.

- Use of private IP by each company

The proxy server in the DMZ relays and communicates with the outside.



3. Mechanism of routing

3-1. What is routing?

3-2. Subnet mask and Default Gateway

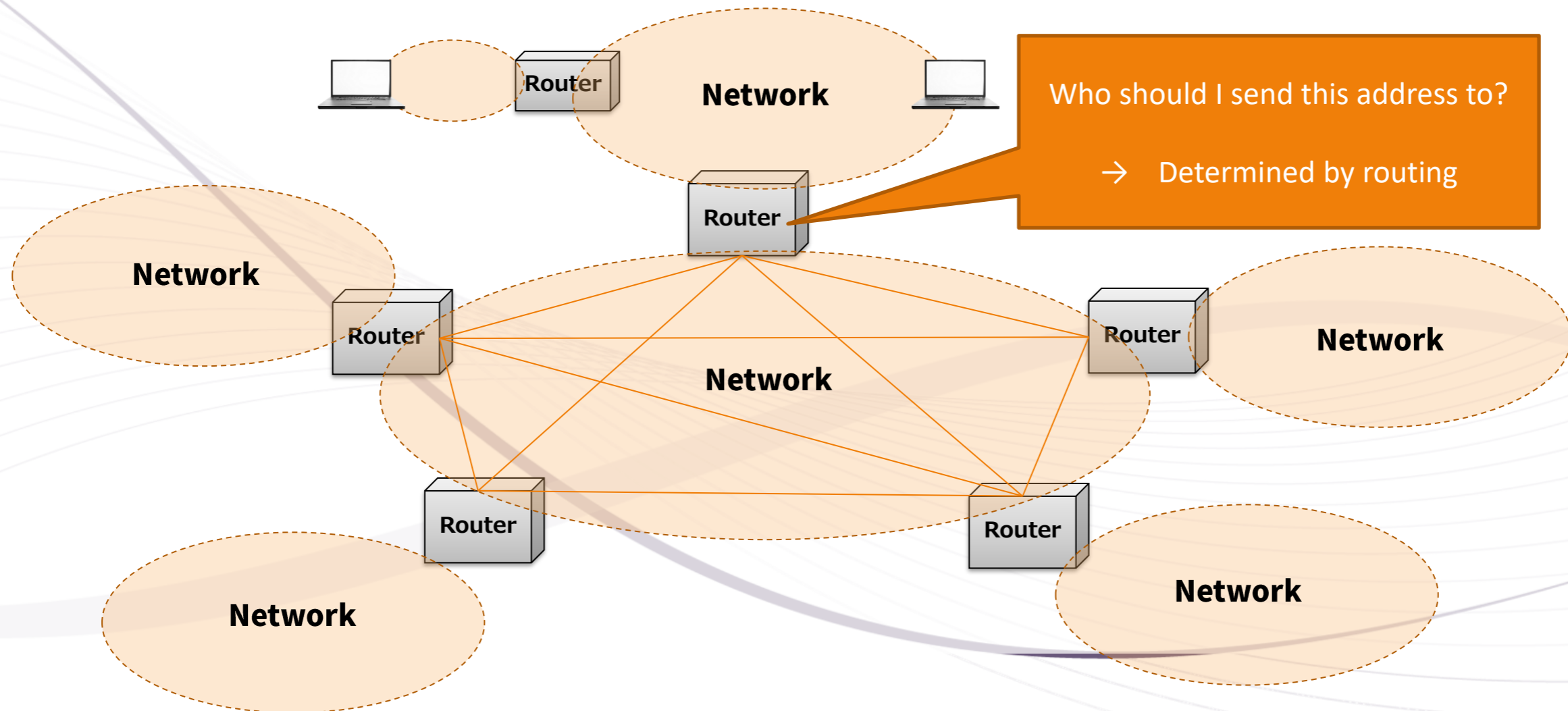
3-3. Decision by routing table

3-4. Priority of routing decisions

3-5. Internet routing

3-1. What is routing?

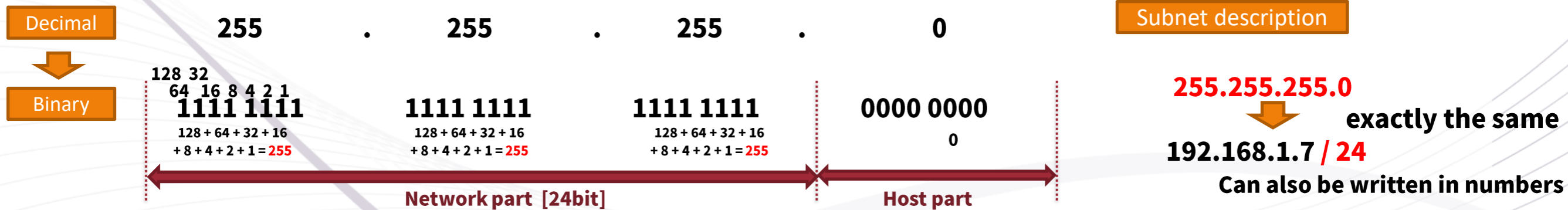
The destination address determines to whom in the connected network to send.



3-2. Subnet mask and Default Gateway

- The subnet mask represents the length of the network part (represents the size of the network)
 ⇒ The same network is determined by whether the network part has the same bit string
- The network part of the default gateway is set to zero, so "all addresses are applicable"

If the subnet mask is "255.255.255.0", Network part is 24bit.



When the destination IP address is "192.168.1.7"

● Network is 「192.168.1.0/24」

Dest : 1100 0000 1010 1000 0000 0001 0000 0111

NW : 1100 0000 1010 1000 0000 0001 0000 0000

"Same network" because the network part is the same bit strings

● Network is 「10.10.10.0/24」

Dest : 1100 0000 1010 1000 0000 0001 0000 0111

NW : 0000 1010 0000 1010 0000 1010 0000 0000

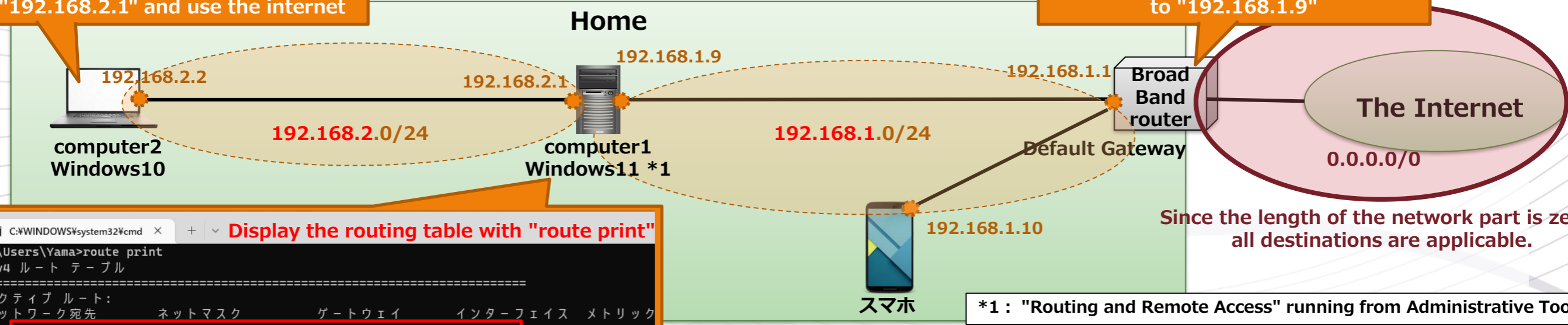
"Not the same" because the bit strings in the network part are different

3-3. Decision by routing table

- Terminals such as personal computers and routers have routing tables for resolving destinations.
- For the destination address, find the destination with the same network address from the routing table.
- Send the packet to the destination (Next-Hop) of the relevant network address.

Set the default gateway to PC 1 "192.168.2.1" and use the internet

Add route for "192.168.2.0/24" to "192.168.1.9"



```

C:\Users\Yama>route print
IPv4 ルート テーブル
=====
アクティブ ルート:
ネットワーク宛先    ネットマスク    ゲートウェイ    インターフェイス    メトリック
-----
0.0.0.0            0.0.0.0        192.168.1.1    192.168.1.9        331
127.0.0.0          255.0.0.0      リンク上       127.0.0.1          331
127.0.0.1          255.255.255.255 リンク上       127.0.0.1          331
127.255.255.255    255.255.255.255 リンク上       127.0.0.1          331
192.168.1.0        255.255.255.0   リンク上       192.168.1.9        291
192.168.1.9        255.255.255.255 リンク上       192.168.1.9        291
192.168.1.255     255.255.255.255 リンク上       192.168.1.9        291
192.168.2.0        255.255.255.0   リンク上       192.168.2.1        291
192.168.2.1        255.255.255.255 リンク上       192.168.2.1        291
192.168.2.255     255.255.255.255 リンク上       192.168.2.1        291
224.0.0.0          240.0.0.0      リンク上       127.0.0.1          331
224.0.0.0          240.0.0.0      リンク上       192.168.2.1        291
224.0.0.0          240.0.0.0      リンク上       192.168.1.9        291
255.255.255.255    255.255.255.255 リンク上       192.168.2.1        291
255.255.255.255    255.255.255.255 リンク上       192.168.2.1        291
255.255.255.255    255.255.255.255 リンク上       192.168.1.9        291
=====
  
```

Default Gateway

connection network

connection network

The red frame is the route that is mainly selected

*1: "Routing and Remote Access" running from Administrative Tools

- The destination is sent to a destination that matches the bit string of the length of the network part indicated by the subnet mask.
- Since the length of the network part of the default gateway is 0, all destinations are applicable destinations, so all addresses for the Internet are selected.
- Because the length of the network part of the connected link is 24, it is selected with priority over the default gateway.

3-3. Priority of routing decisions

- Routing is determined by multiple factors, but there is a priority.
- Priority is as follows

Priority 1: Longest Match

The length of the network part (the length of the subnet mask) has the highest priority.

Example) When there are 1 and 2 in the routing table

The destination "192.168.1.1" corresponds to both of the following, but length 24 ① is selected

	Network Address	Next-Hop
①	192.168.1.0/24	192.168.1.1
②	192.168.0.0/16	192.168.1.11

← This route with a longer network part is selected

Priority 2: Administrative distance

It is decided which route type to prioritize

- **Static route**
Route manually set by the operator
- **Dynamic routing**
Automatically update route information using a routing protocol
Dynamically update route information by notifying your route to the other party

《 Standard setting 》 (Excerpt)

Route information source		Administrative distance value
Direct connection (same network)		0
Static route (manual setting)		1
Dynamic Routing	BGP (external)	20
	OSPF	110
	RIP	120
	BGP (internal)	200

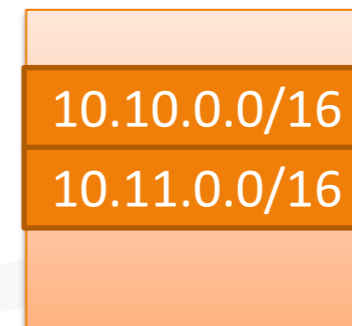
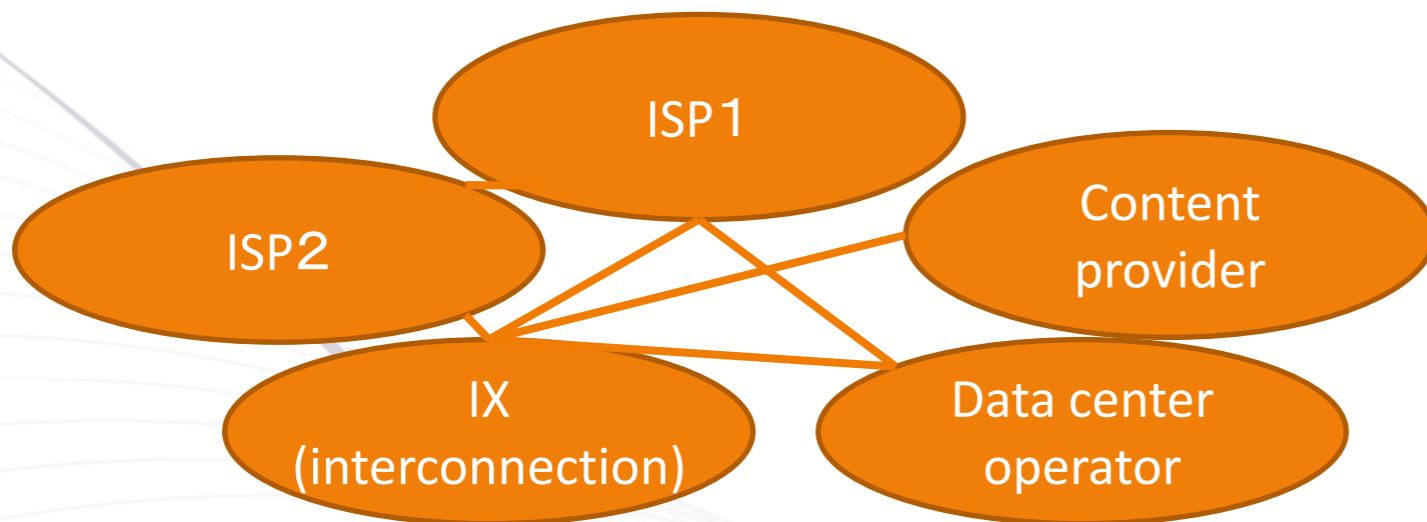
Priority 3: Metric

Used when manually setting the priority or operating the priority of the route based on the number of hops or cost.

3-4. Internet routing

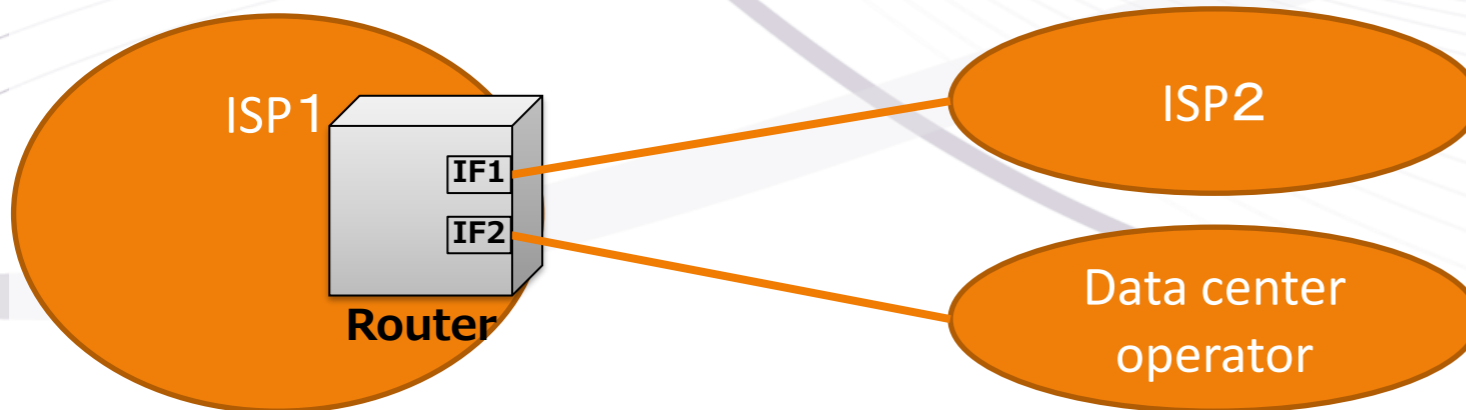
- Construct routing by exchanging network addresses in use between operators

Each operator notifies each other of the network address used by itself to the connection destination. (Automatically notify each other using a protocol called BGP)



10.10.0.0/15

The network addresses to be notified are sent together as much as possible.



Basically, the network address notified by the other party is used by the business operator, so it becomes the destination.

4. Ethernet and MAC address

4-1. What is Ethernet?

4-2. Sending to Nex-Hop and Mac address

4-3. MAC address resolution mechanism "ARP"

**4-4. Summary of transmission processing on
Ethernet terminals**

4-1. What is Ethernet?

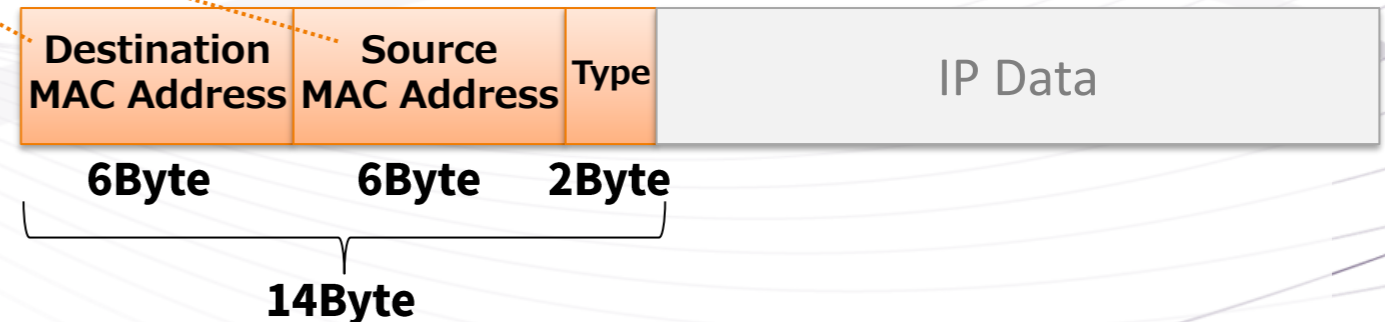
- Ethernet is a communication technology of IEEE, layer 2 data link layer technology
- Ethernet uses MAC addresses for terminal identification.



- **Ethernet standard**
 - **Wired: LAN cable, coaxial, optical cable**
Standardization IEEE802.3
 - **Wireless: Wi-Fi**
Standardization IEEE802.11 ac/a/n/g/b

- **Positioning of the protocol stack**
 - **Equivalent to the physical to data link layers of the OSI reference model (the layer below the IP address)**

- **Ethernet Data Format**



- **What is a MAC address?**
 - **A 6-byte address assigned to the interface. Given by the manufacturer.**

```
Wi-Fi 2
ip.addr == 23.59.13.91
No. Time Source Destination Protocol Length Info
48 1.868905 192.168.1.9 23.59.13.91 ICMP 74 Echo (ping) request id=0x0001, seq=11/2816,
49 1.878472 23.59.13.91 192.168.1.9 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816,
81 2.877676 192.168.1.9 23.59.13.91 ICMP 74 Echo (ping) request id=0x0001, seq=12/3072,
82 2.887161 23.59.13.91 192.168.1.9 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072,

> Frame 48: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{EE298557-9F26-440F-...}
Ethernet II, Src: Tp-LinkT_09:d6:7d (28:ee:52:09:d6:7d), Dst: Mitsubis_86:d6:65 (10:4b:46:86:d6:65)
  Destination: Mitsubis_86:d6:65 (10:4b:46:86:d6:65) Dest Mac Address
  Source: Tp-LinkT_09:d6:7d (28:ee:52:09:d6:7d) Src Mac Address
  Type: IPv4 (0x0800) Ethernet Header
Internet Protocol Version 4, Src: 192.168.1.9, Dst: 23.59.13.91
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x8933 (35123)
  > Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: ICMP (1)
  Header Checksum: 0xcb46 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.9 Src IP Address
  Destination Address: 23.59.13.91 Dest IP Address
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d50 [correct] Ethernet 14Byte

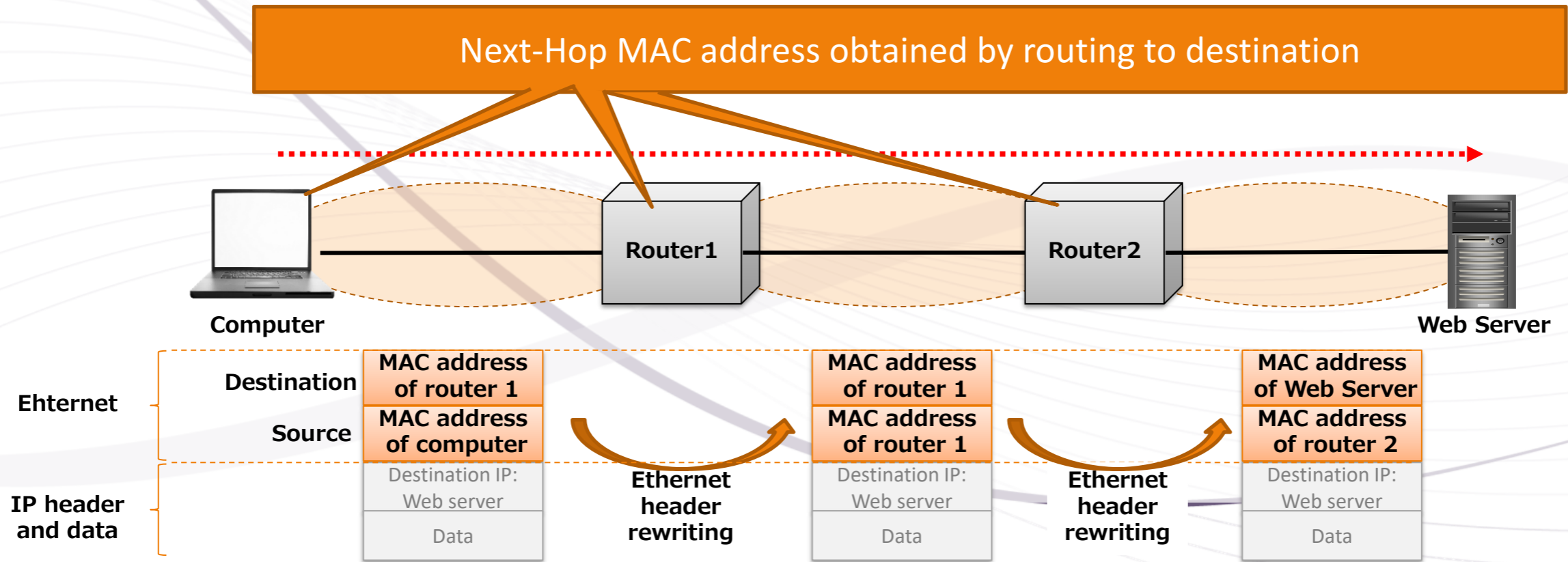
0000 10 4b 46 86 d6 65 28 ee 52 09 d6 7d 08 00 45 00 .KF..d(.R..)-E-
0010 00 3c 89 33 00 00 80 01 cb 46 c0 a8 01 09 17 3b <<-3....F.....;
0020 0d 5b 08 00 4d 50 00 01 ..MP...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 67 68 69 6a 6b 6c 6d 6e jklmnopqrstuv
0040 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f .....cdefghij
```

4-2. Sending to Nex-Hop and Mac address

- Send to the MAC address of the next-hop destination terminal acquired by routing.

● Communication from personal computer to web server

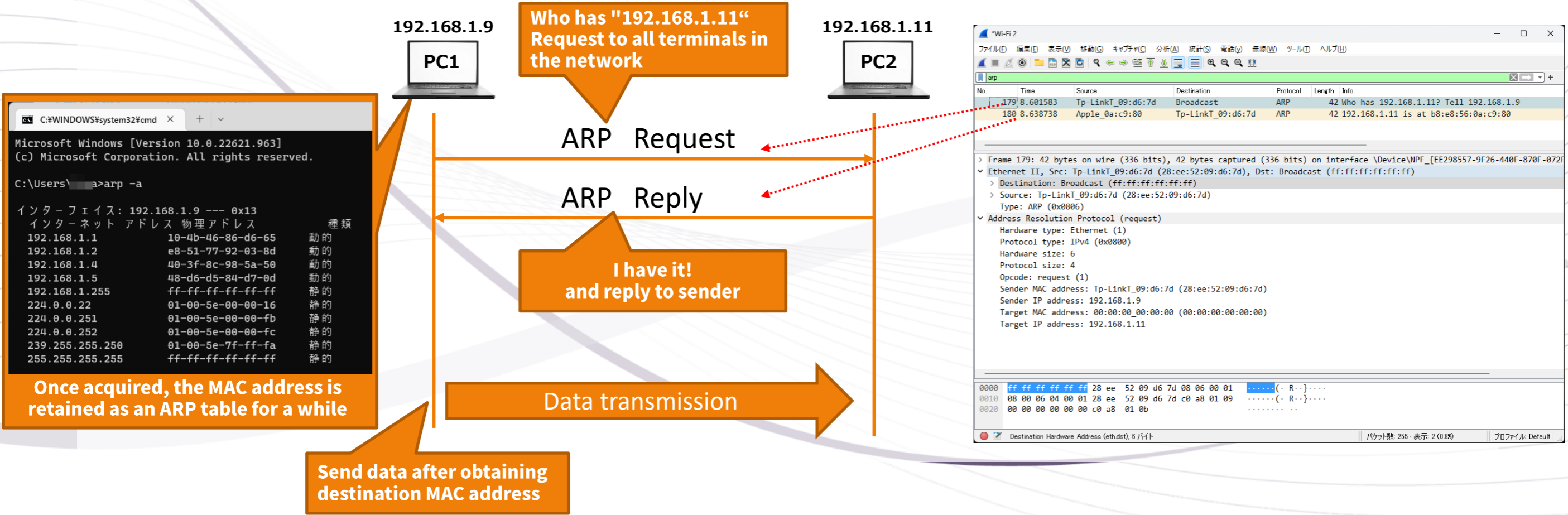
Terminals and routers create and send Ethernet headers to the Next-Hop MAC addresses obtained by routing. Therefore, every time it goes through a router, the Ethernet header is rewritten and communicated.



4-3. MAC address resolution mechanism "ARP"

- Since IP addresses are obtained in routing, a mechanism to obtain MAC addresses is required.
- The destination MAC address is obtained using ARP from the IP address obtained by routing.

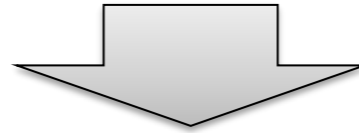
● When PC 1 communicates with PC 2



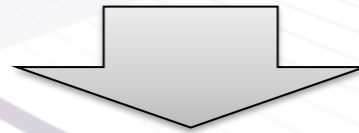
4-4. Summary of transmission processing on Ethernet terminals

Processing from determination of destination to data transmission.

Determine the destination (Next-Hop) from the routing table.



Acquire the MAC address of the destination (Next-Hop) by ARP.



Add Ethernet header, construct data and send.