Computer Network Architecture

计算机网络体系结构

沈航

南京工业大学

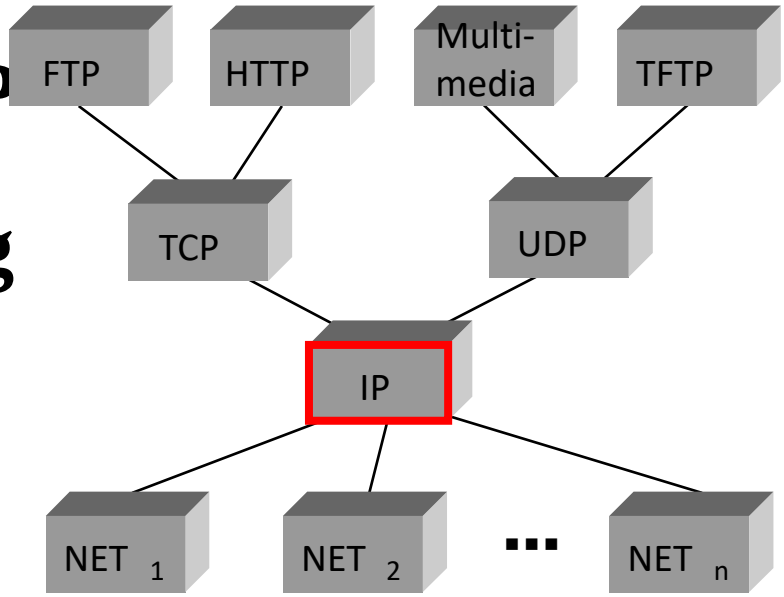

Email: hshen@njtech.edu.cn

The TCP/IP Architecture

(continued)

TCP/IP Architecture

- The TCP/IP Architecture defined by IETF
- Transparent Design
  - Everything over IP
  - IP over Everything
  - Best-effort



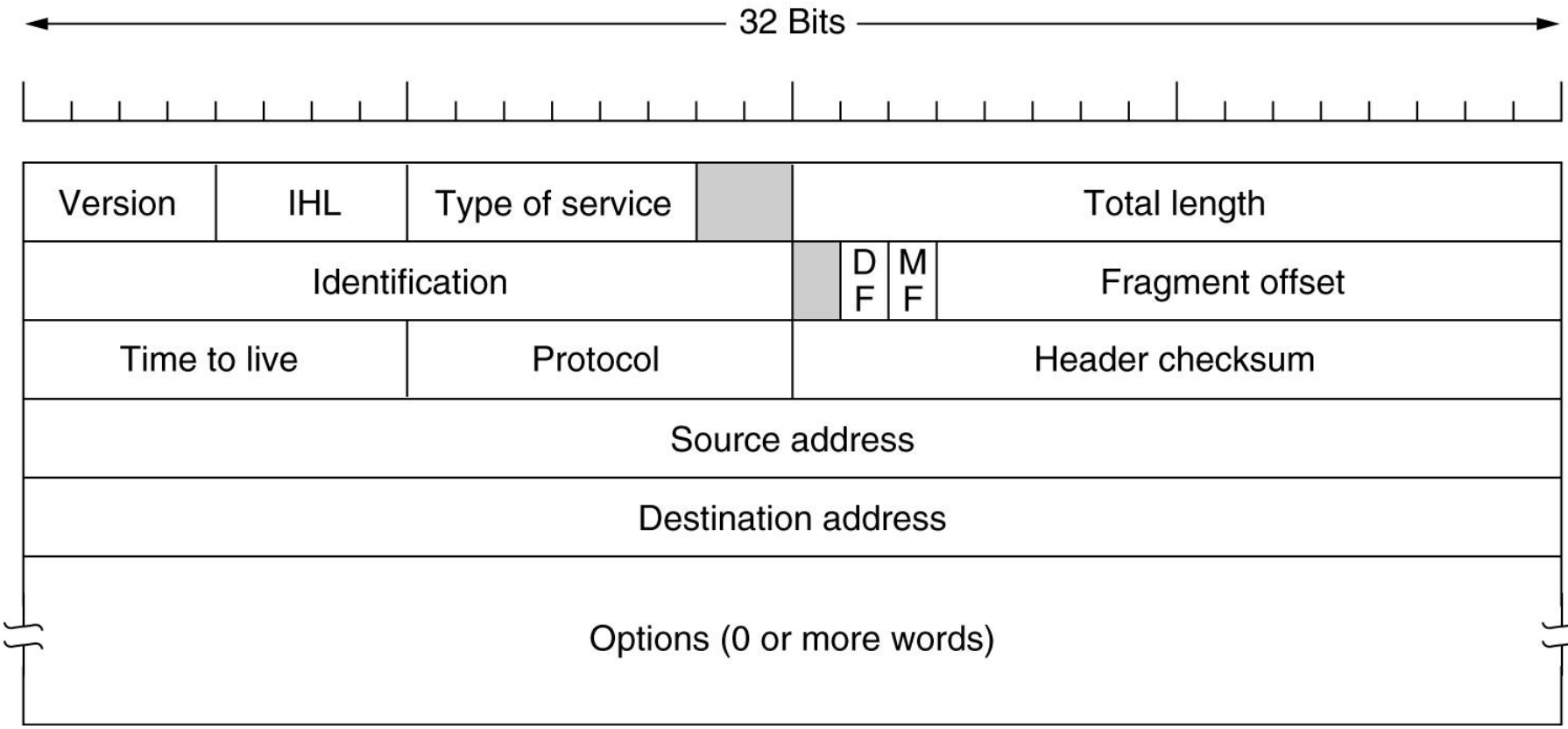
The IP Protocol协议

- connectionless protocol does not exchange control information to establish end-to-end connection before transmitting data
- defining the datagram数据报
- defining the internet addressing scheme寻址方案
- moving data between the Data Link Layer and the Transport Layer

The IP Protocol

- routing datagrams to remote hosts
- performing fragmentation and re-assembly of datagrams完成数据报的分段与重组
- relies on other protocols to establish connection if required
- best-efforts way, *i.e.*, not guaranteed

The IP datagram数据报



The IPv4 header.

IP Addresses

- **Every node on the Internet has an IP address, used to identify the network and the host on a given network**
- **Each IP address consists of *net-id* and *host-id*;**

IP Addresses

- **Each IP address is 32 bits long, *e.g.***

  10000000 00001011 00000011 00011111

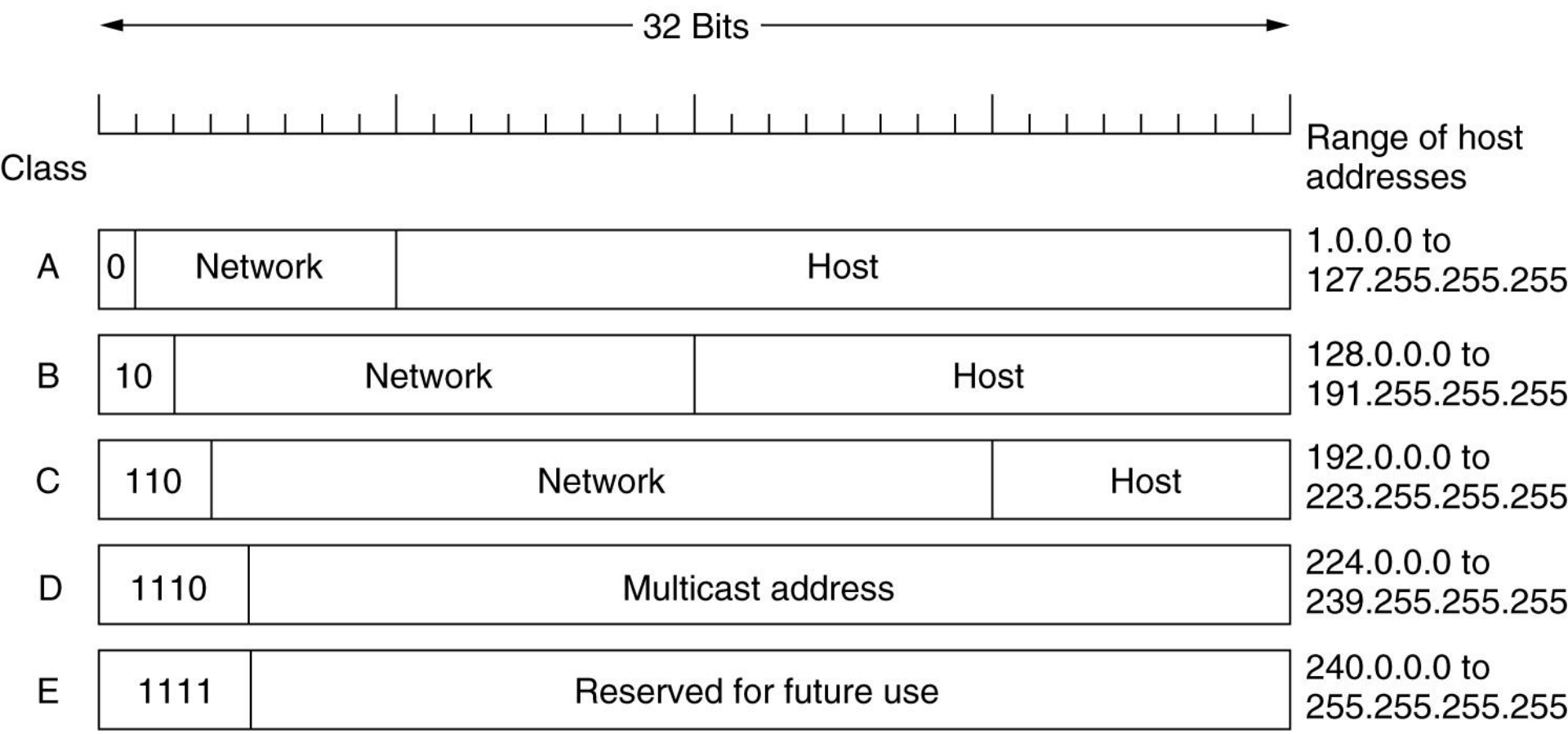
  it is usually written in dotted decimal notation(点分十进制记法)， *e.g.* 128.11.3.31

  just easy to read!

- **The IP address is divided into two parts:**

  IPaddr::={<net-id>, <host-id>}

Classes of IP Addresses IP地址分类



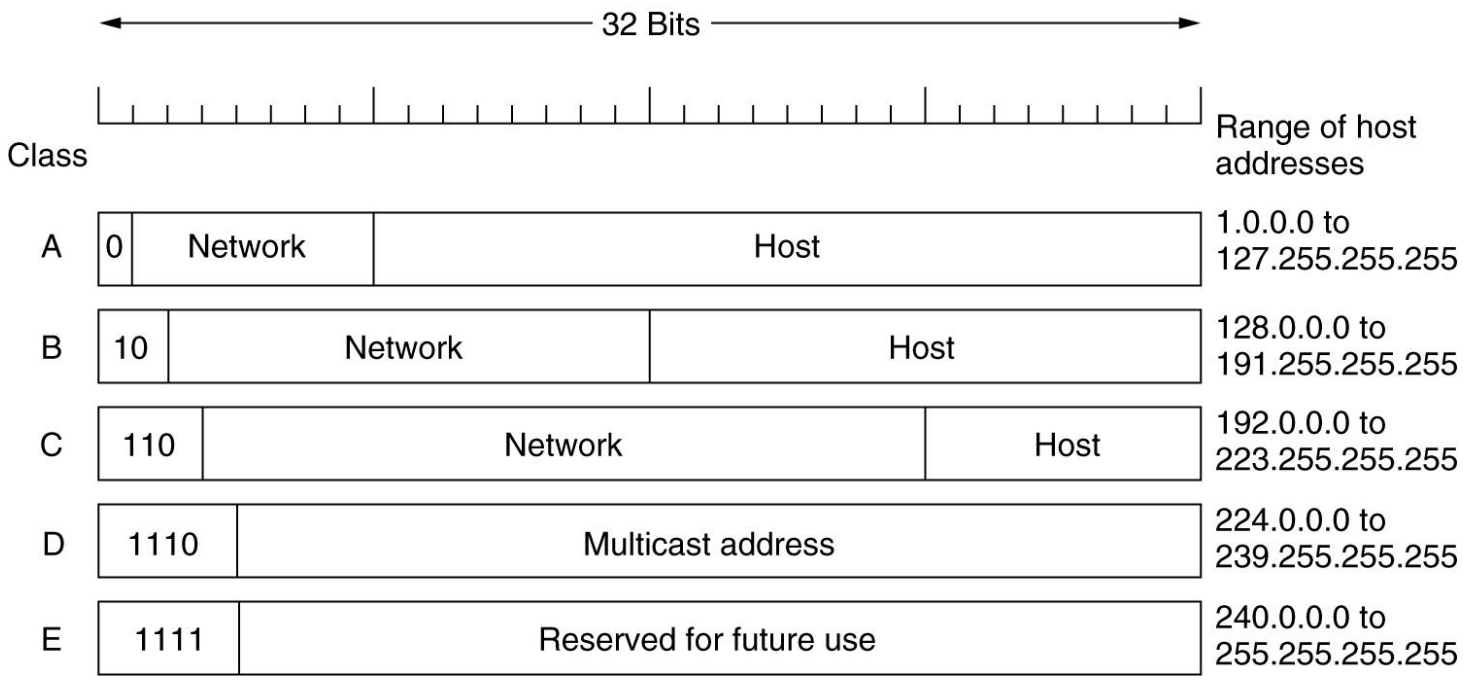
IP address formats.

Quiz

To which class do the following IP addresses belong ?

(1) 128.36.199.3 **(2) 21.12.240.17**

(3) 192.12.69.248 **(4) 183.194.76.253**

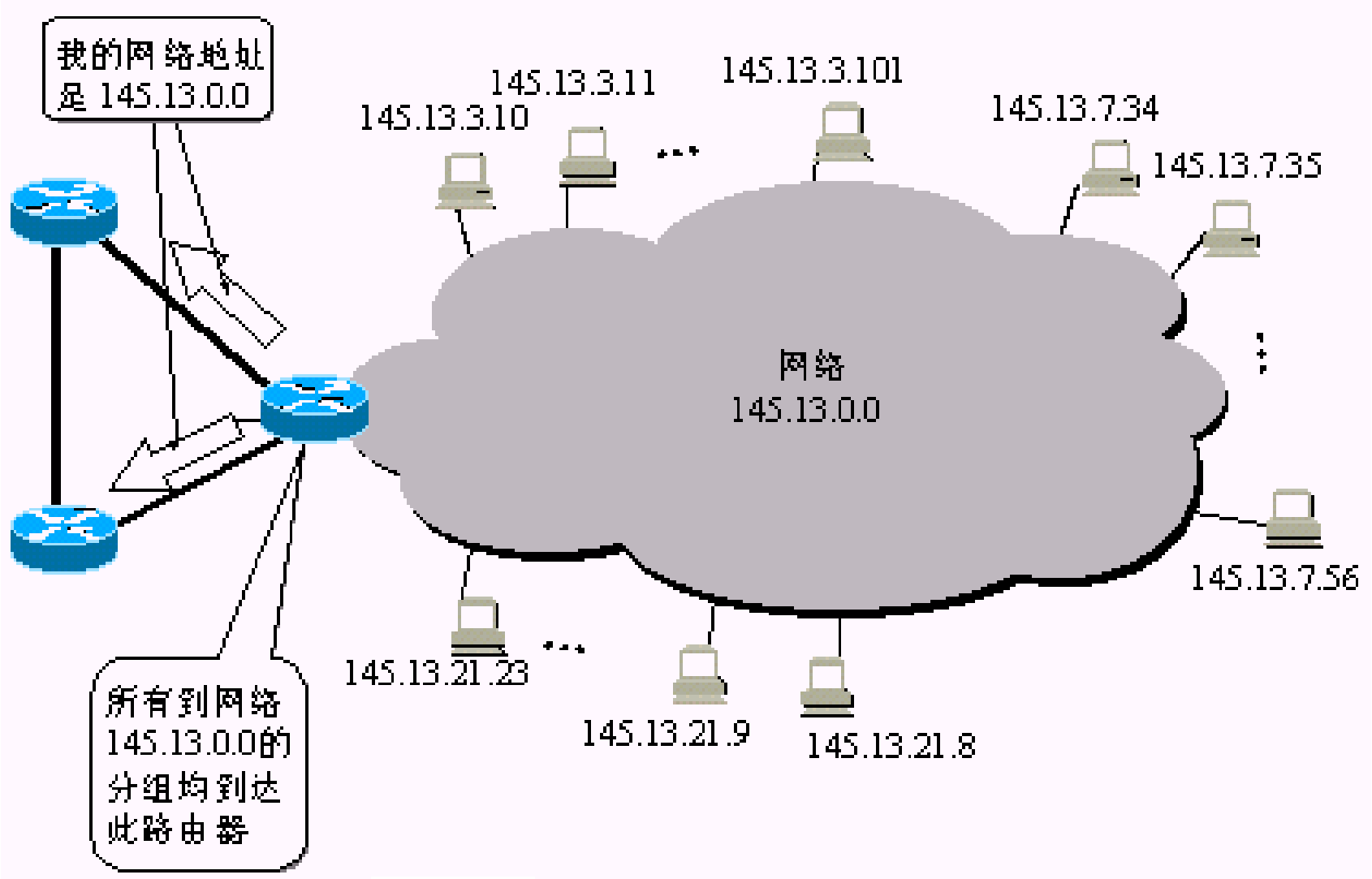


Classes of IP Addresses IP地址分类

The following IP addresses are not allowed in the public Internet:

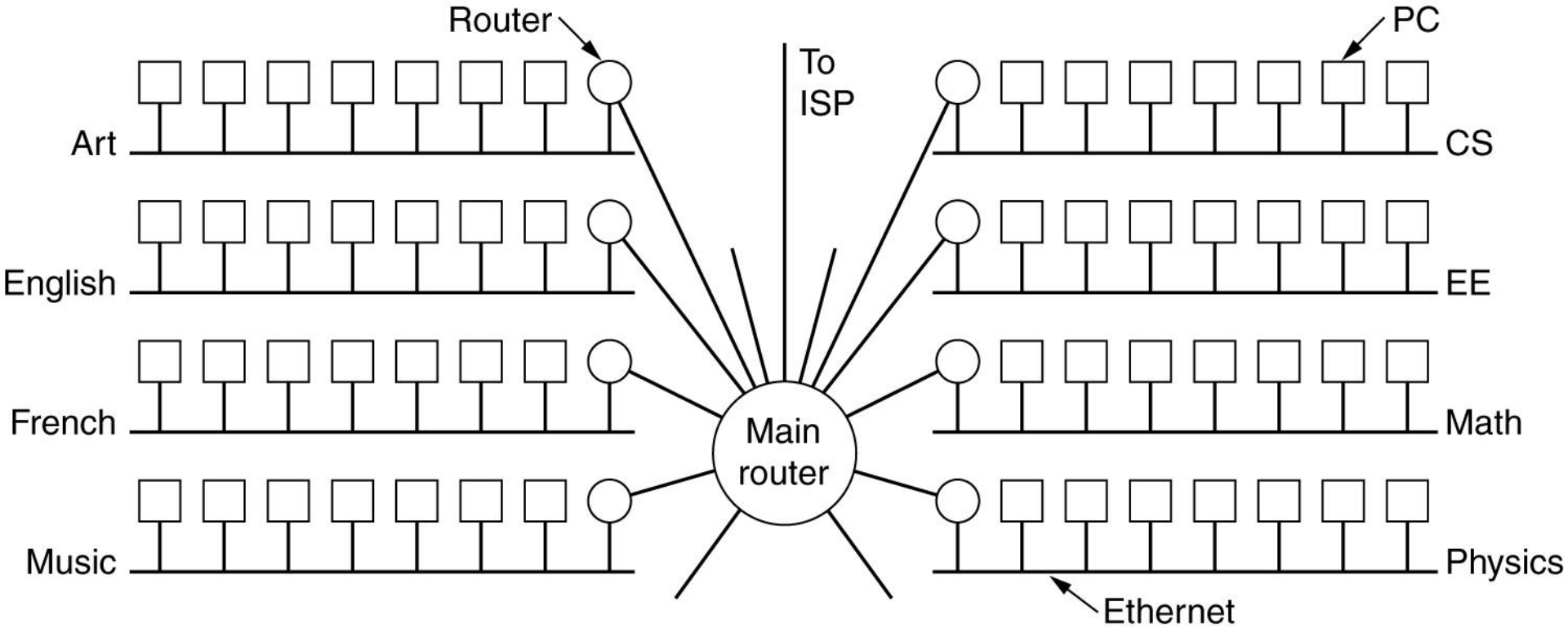
- **Class C： 192.168.X.X**
- **Class B： 172.X.X.X**
- **Class A： 10.X.X.X**

举例：一个单位拥有一个B类IP地址，网络地址是145.13.0.0 (net-id)。



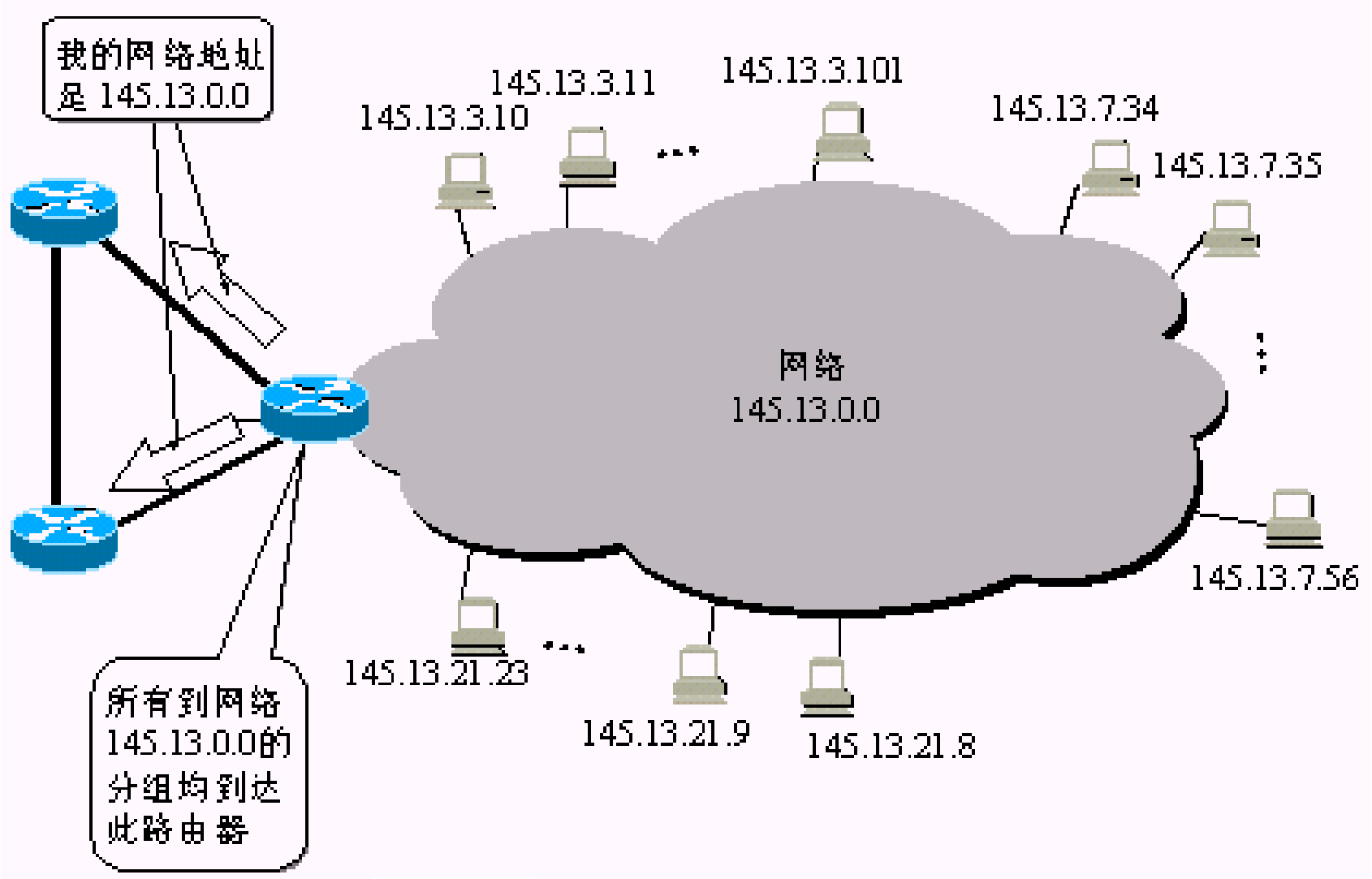
一个 B 类网络 145.13.0.0

Subnets



A campus network consisting of LANs for various departments.

举例：一个单位拥有一个B类IP地址，网络地址是145.13.0.0 (net-id)。



一个 B 类网络 145.13.0.0

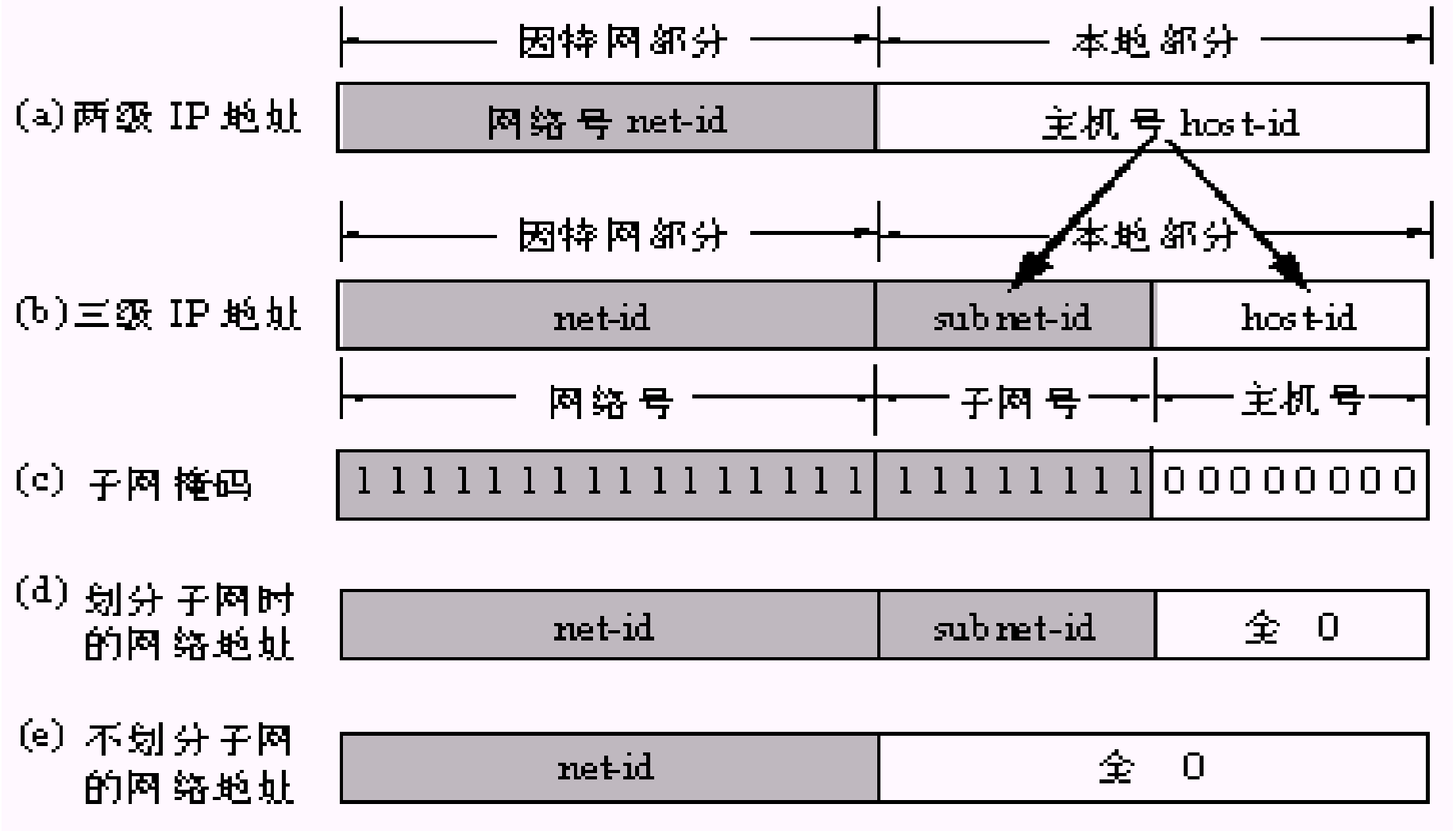
Subnetting划分子网

- **Proposed in *RFC950: (Request For Comments* 网络技术文件)**
- **Basic idea:**
  - **A organization with a large network can be divided to many smaller networks, i.e. subnets. Subnetting is an intramural matter.**
  - **take some bits from the host number part to create a “subnet” number.**

IPaddr ::= { <*net-id*>, <*host-id*>}

IPaddr ::= {<*net-id*>, <*subnet-id*>, <*host-id*>}

Subnets子网



IP 地址的各字段和子网掩码

Subnetting划分子网

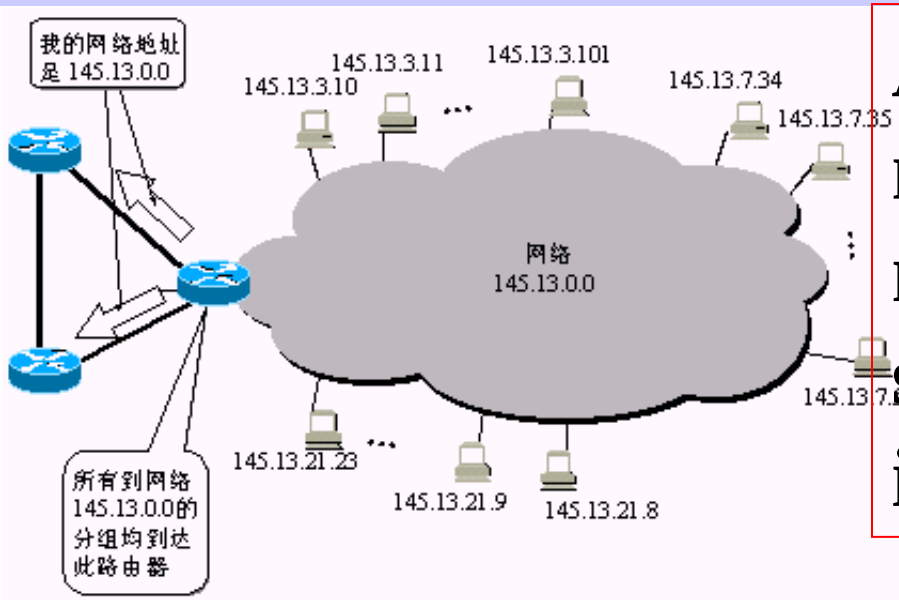


图 7-17　一个 B 类网络 145.13.0.0

A organization with a large network can be divided to many smaller networks, i.e. subnets. Subnetting is an intramural matter.

Subnetting:
take some bits from the host number part to create a "subnet" number.

IPaddr ::= {<net-id>, <subnet-id>, <host-id>}

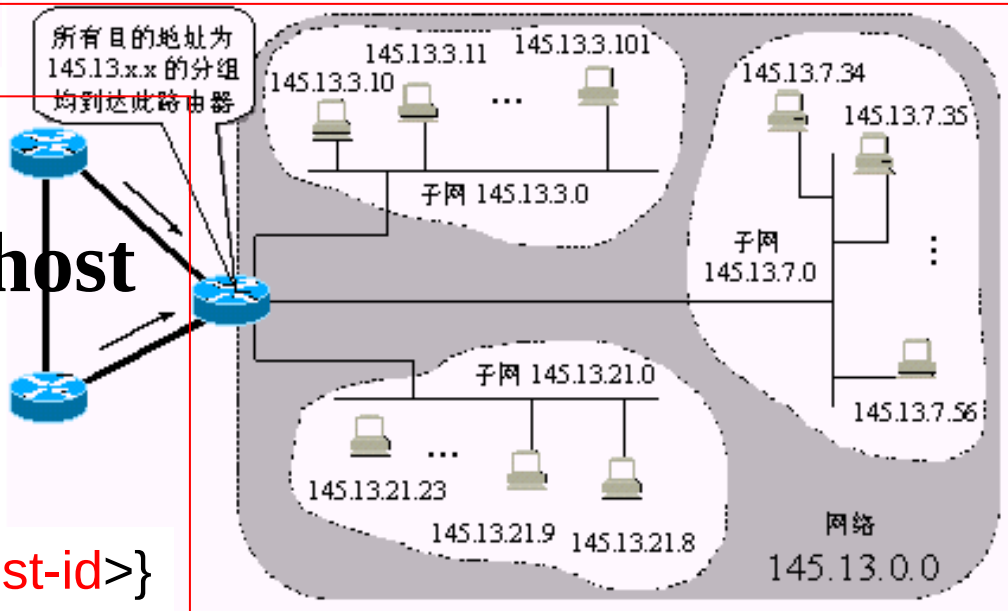


图 7-18　将图 7-17 的网络划分为三个子网，但对外仍是一个网络

Subnetting划分子网

- Packet routing from the source to the destination across the network:

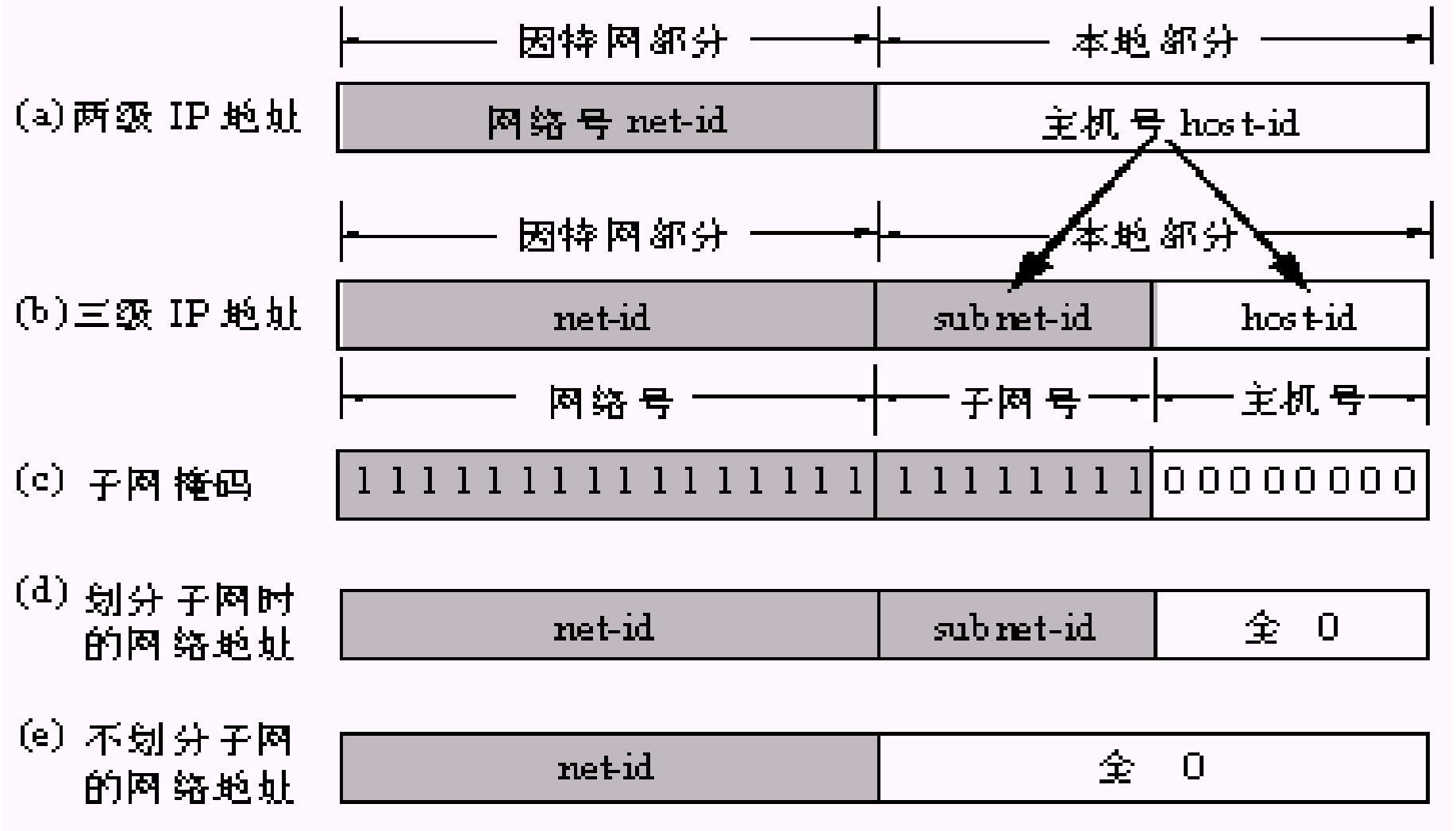
  → Destination Network

  → Destination Subnet

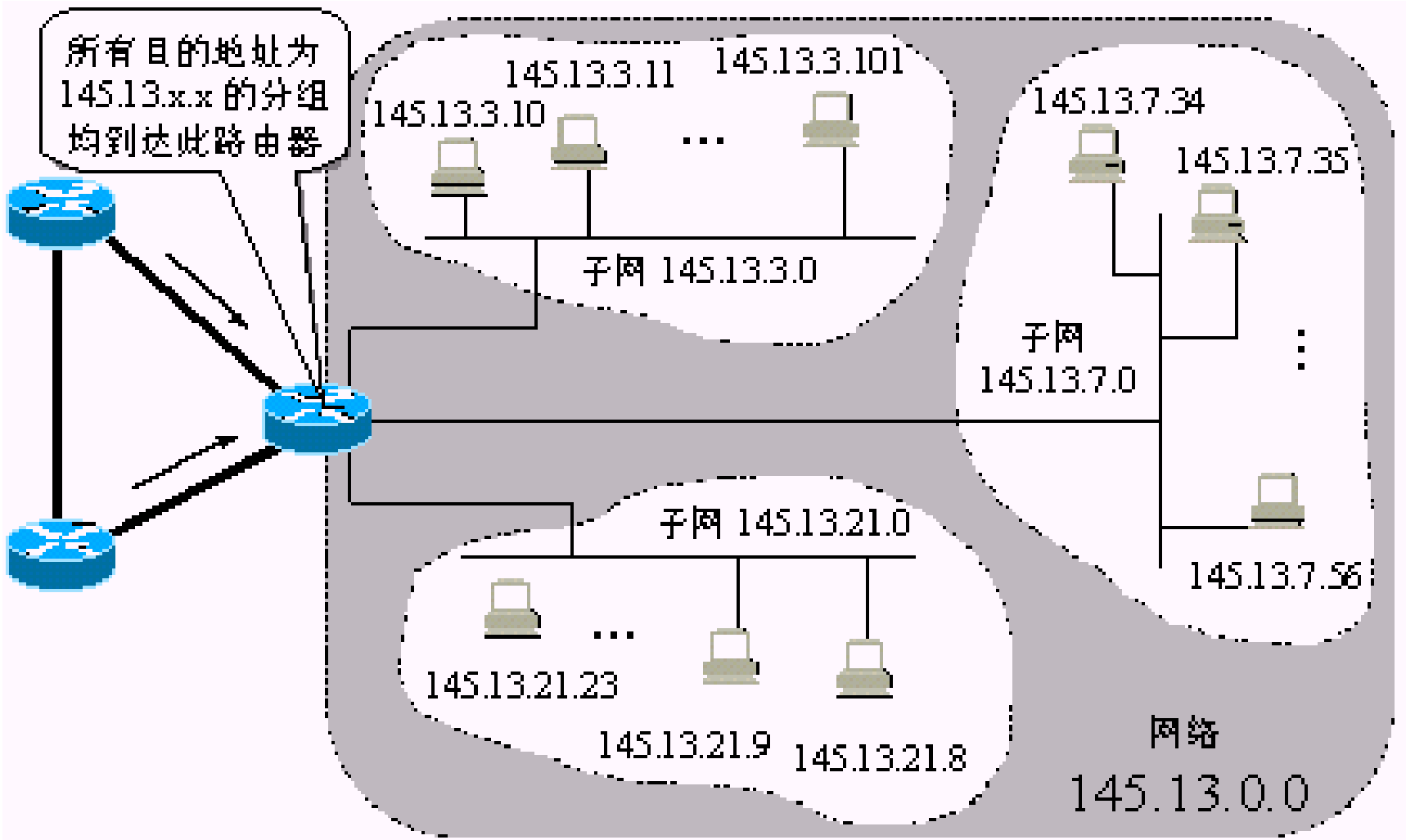
  →Destination Host

- Subnet masks子网掩码 indicates which part of a 32-bit IP address represents *net-id* and *subnet-id*

Subnets子网



IP 地址的各字段和子网掩码



网络划分为三个子网：145.13.3.0，145.13.7.0，145.13.21.0，但对外仍是一个网络

Quiz

Question: With a subnet mask of 255.255.0.0, do IP addresses 172.16.1.58 and 172.16.4.36 belong to the same network?

```
172.16.1.58   10101100 00010000 00000001 00111010
255.255.0.0   11111111 11111111 00000000 00000000
AND           10101100 00010000 00000000 00000000
-------------------------------------------------
172.16.4.36   10101100 00010000 00000100 00100100
255.255.0.0   11111111 11111111 00000000 00000000
AND           10101100 00010000 00000000 00000000
```

YES!

Subnet Example #1

- IP Address: **130.97.16.132**
- Subnet Mask: 255.255.255.192
  - Net-id=?
  - Host-id=?

Subnet Example #1

- IP Address: **130.97.16.132**
- Subnet Mask: 255.255.255.192

```
10000010 01100001 00010000 10000100
11111111 11111111 11111111 11000000
```

Net-id

```
10000010 01100001 00010000 10000000
```

→ 130.97.16.128

Host-id

```
00000000 00000000 00000000 00000100
```

→ 0.0.0.4

Subnet Example #2

- IP Address: **130.97.17.132**
- Subnet Mask: 255.255.254.0

Subnet Example #2

- IP Address: **130.97.17.132**
- Subnet Mask: 255.255.254.0

  10000010 01100001 00010001 10000100
  11111111 11111111 11111110 00000000

  - Net-id

    10000010 01100001 00010000 00000000

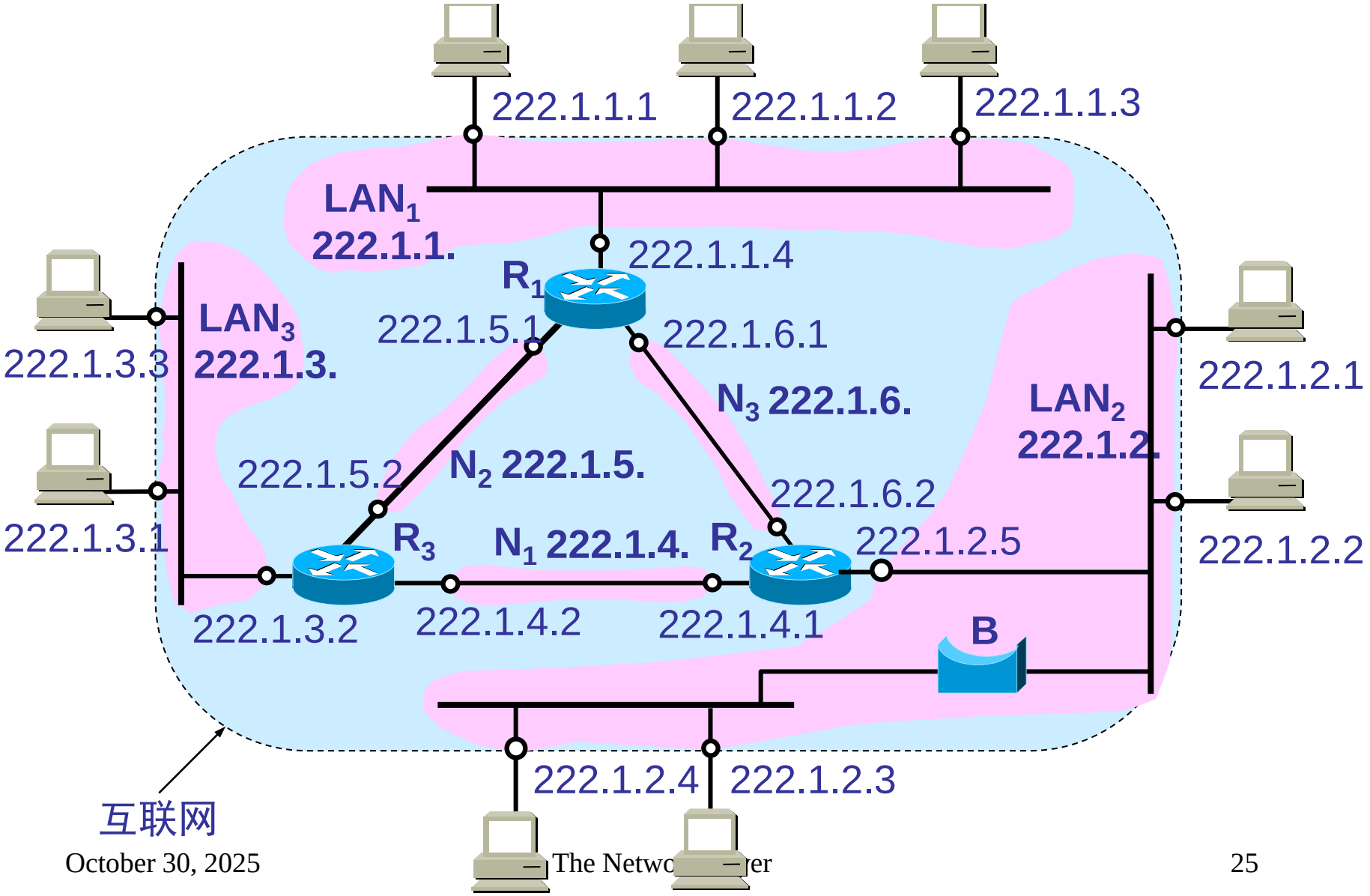
    → 130.97.16.0

  - Host-id

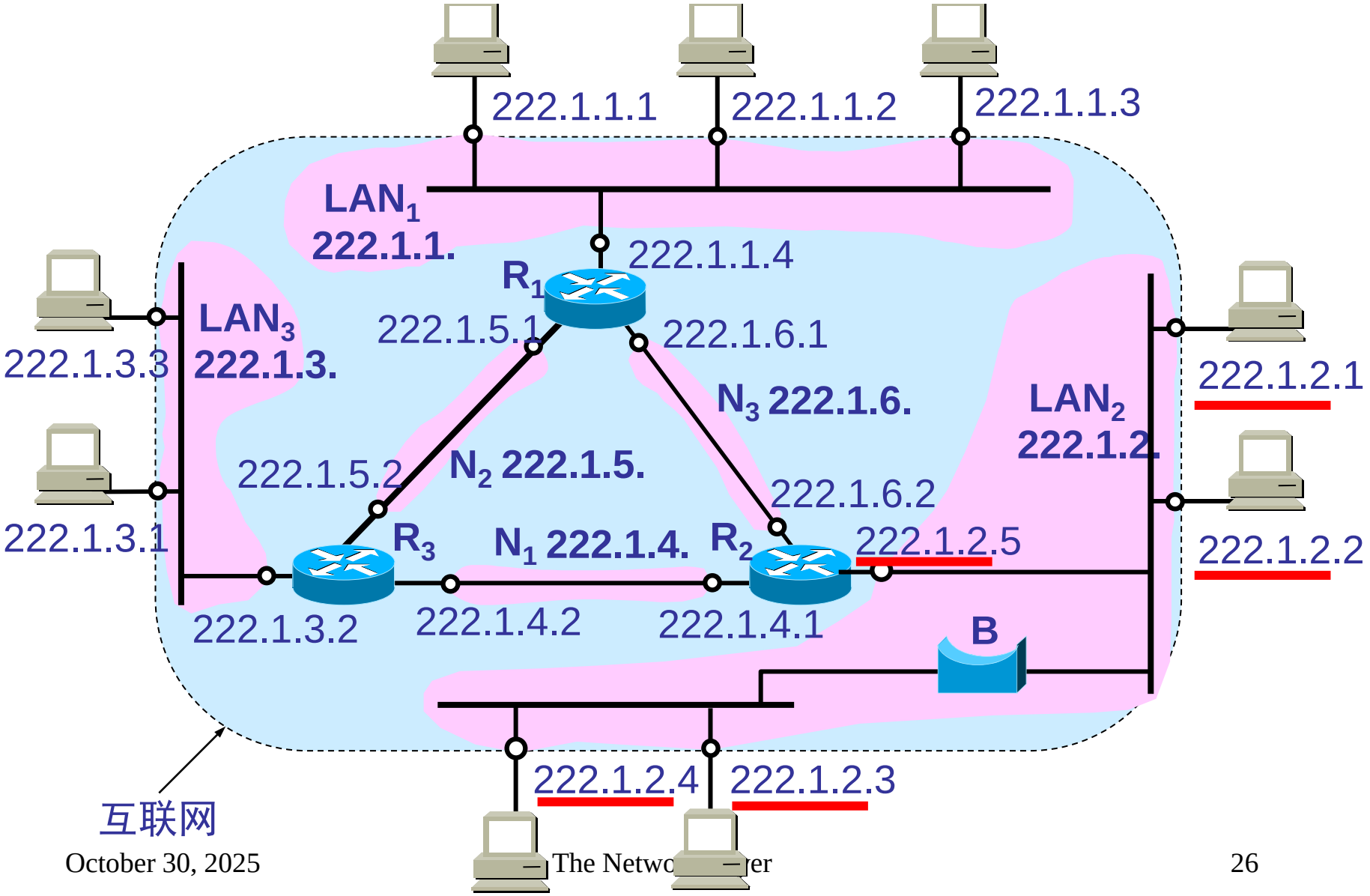
    00000000 00000000 00000001 10000100

    → 0.0.1.132

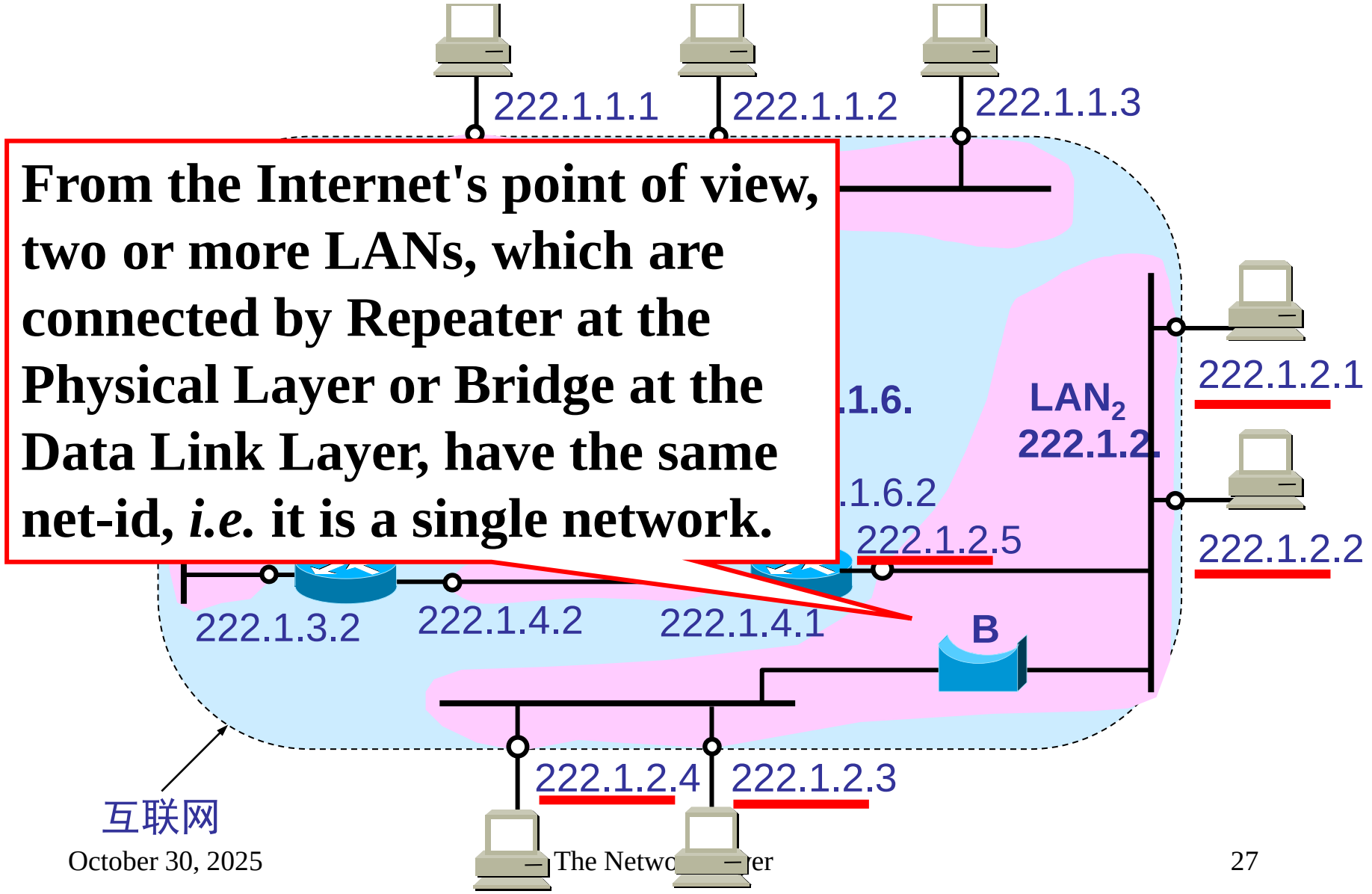
Example: LAN1, LAN2 and LAN3 are connected by three routers, *i.e.* R1, R2 and R3.



Example: LAN1, LAN2 and LAN3 are connected by three routers, *i.e.* R1, R2 and R3.



Example: LAN1, LAN2 and LAN3 are connected by three routers, *i.e.* R1, R2 and R3.



IP address space

- **IP addr is 32 bits long, *i.e.* 2^{32}=4,294,967,296! That means, more than 4.2 billion can be connected to the Internet!!**

IP address space

- **IP addr is 32 bits long, *i.e.* 2^{32}=4,294,967,296! That means, more than 4.2 billion can be connected to the Internet!!**
- **Exponential growth of the Internet in 1990~1999 → The IP address space will be exhausted soon!!!**

IP address space

- **The address space of IPv4 is extreme wasteful!**
- **The main problem is that too many class B addresses are being used. The max. number of networks: 2^{14} =16384**
- **At the same time, many of the 2 million class C addresses are idle because it is too small. The max. number of hosts is only 254**

IP address space

- **Routing table explosion: If half a million class C networks were in use, every router in the entire Internet would need a table with half a million entries.**

The TCP/IP Architecture

(continued)

IP address space

- **The address space of IPv4 is extreme wasteful! We must improve the utilization of the IP address space !**
  - **CIDR: Classless InterDomain Routing**
  - **NAT: Network Address Translation**
- **We need a new IP protocol!**
  - **IPv4→IPv6**

CIDR – Classless InterDomain Routing无类域间路由选择

- The basic idea behind CIDR is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.
- CIDR: Assign class C addresses in contiguous blocks of 256 addresses邻近的地址块.
- It is more complicated than class.

CIDR – Classless InterDomain Routing无类域间路由选择

- ***net-id*** **and** ***host-id*** **are replaced by** ***network-prefix网络前缀***

i.e. IPaddr ::= {<net-prefix>, <host-id>}.

e.g. 128.14.46.34/20

→ 10000000 00001110 00101110 00100010

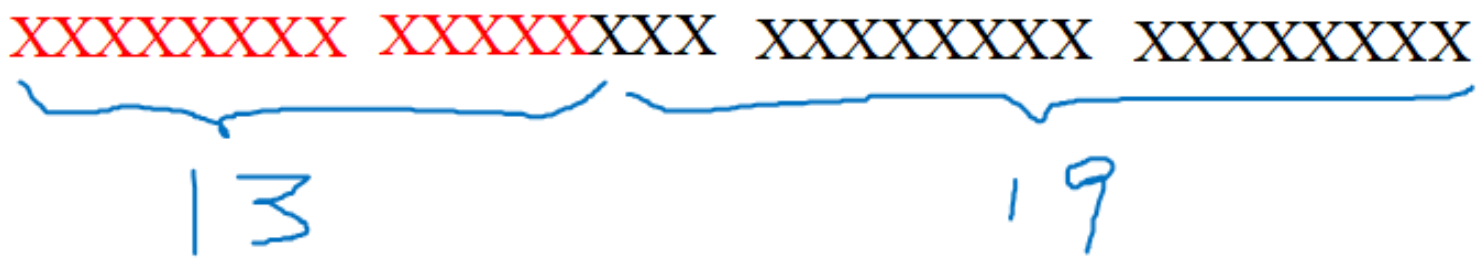
net-prefix **host-id**

常用的 CIDR 地址块

CIDR 前缀长度	点分十进制	包含的地址数	包含的分类的网络数
/13	255.248.0.0	512 K	8 个 B 类或 2048 个 C 类
/14	255.252.0.0	256 K	4 个 B 类或 1024 个 C 类
/15	255.254.0.0	128 K	2 个 B 类或 512 个 C 类
/16	255.255.0.0	64 K	1 个 B 类或 256 个 C 类
/17	255.255.128.0	32 K	128 个 C 类
/18	255.255.192.0	16 K	64 个 C 类
/19	255.255.224.0	8 K	32 个 C 类
/20	255.255.240.0	4 K	16 个 C 类
/21	255.255.248.0	2 K	8 个 C 类
/22	255.255.252.0	1 K	4 个 C 类
/23	255.255.254.0	512	2 个 C 类
/24	255.255.255.0	256	1 个 C 类
/25	255.255.255.128	128	1/2 个 C 类
/26	255.255.255.192	64	1/4 个 C 类
/27	255.255.255.224	32	1/8 个 C 类

常用的 CIDR 地址块

CIDR 前缀长度	点分十进制	包含的地址数	包含的分类的网络数
/13	255.248.0.0	512 K	8 个 B 类或 2048 个 C 类



/19	255.255.224.0	
/20	255.255.240.0	
/21	255.255.248.0	
/22	255.255.252.0	
/23	255.255.254.0	
/24	255.255.255.0	
/25	255.255.255.128	
/26	255.255.255.192	
/27	255.255.255.224	

常用的 CIDR 地址块

CIDR 前缀长度	点分十进制	包含的地址数	包含的分类的网络数
/13	255.248.0.0	512 K	8 个 B 类或 2048 个 C 类
/14	255.252.0.0	256 K	4 个 B 类或 1024 个 C 类
/15	255.254.0.0		
/16	255.255.0.0		
/17	255.255.128.0		
/18	255.255.192.0		
/19	255.255.224.0		
/20	255.255.240.0		
/21	255.255.248.0		
/22	255.255.252.0		
/23	255.255.254.0		
/24	255.255.255.0		
/25	255.255.255.128		
/26	255.255.255.192		
/27	255.255.255.224		

常用的 CIDR 地址块

CIDR 前缀长度	点分十进制	包含的地址数	包含的分类的网络数
/13	255.248.0.0	512 K	8 个 B 类或 2048 个 C 类
/14	255.252.0.0	256 K	4 个 B 类或 1024 个 C 类
/15	255.254.0.0	128 K	2 个 B 类或 512 个 C 类
/16	255.255.0.0	64 K	1 个 B 类或 256 个 C 类
/17	255.255.128.0	32 K	128 个 C 类
/18	255.255.192.0	16 K	64 个 C 类
/19	255.255.224.0	8 K	32 个 C 类
/20	255.255.240.0	4 K	16 个 C 类
/21	255.255.248.0	2 K	8 个 C 类
/22	255.255.252.0	1 K	4 个 C 类
/23	255.255.254.0	512	2 个 C 类
/24	255.255.255.0		
/25	255.255.255.128		
/26	255.255.255.192		
/27	255.255.255.224		

常用的 CIDR 地址块

CIDR 前缀长度	点分十进制	包含的地址数	包含的分类的网络数
/13	255.248.0.0	512 K	8 个 B 类或 2048 个 C 类
/14	255.252.0.0	256 K	4 个 B 类或 1024 个 C 类
/15	255.254.0.0	128 K	2 个 B 类或 512 个 C 类
/16	255.255.0.0	64 K	1 个 B 类或 256 个 C 类
/17	255.255.128.0	32 K	128 个 C 类
/18	255.255.192.0	16 K	64 个 C 类
/19	255.255.224.0	8 K	32 个 C 类
/20	255.255.240.0	4 K	16 个 C 类
/21	255.255.248.0	2 K	8 个 C 类
/22	255.255.252.0	1 K	4 个 C 类
/23	255.255.254.0	512	2 个 C 类
/24	255.255.255.0	256	1 个 C 类
/25	255.255.255.128	128	1/2 个 C 类
/26	255.255.255.192	64	1/4 个 C 类
/27	255.255.255.224	32	1/8 个 C 类

CIDR – Classless InterDomain Routing

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

A set of IP address assignments.

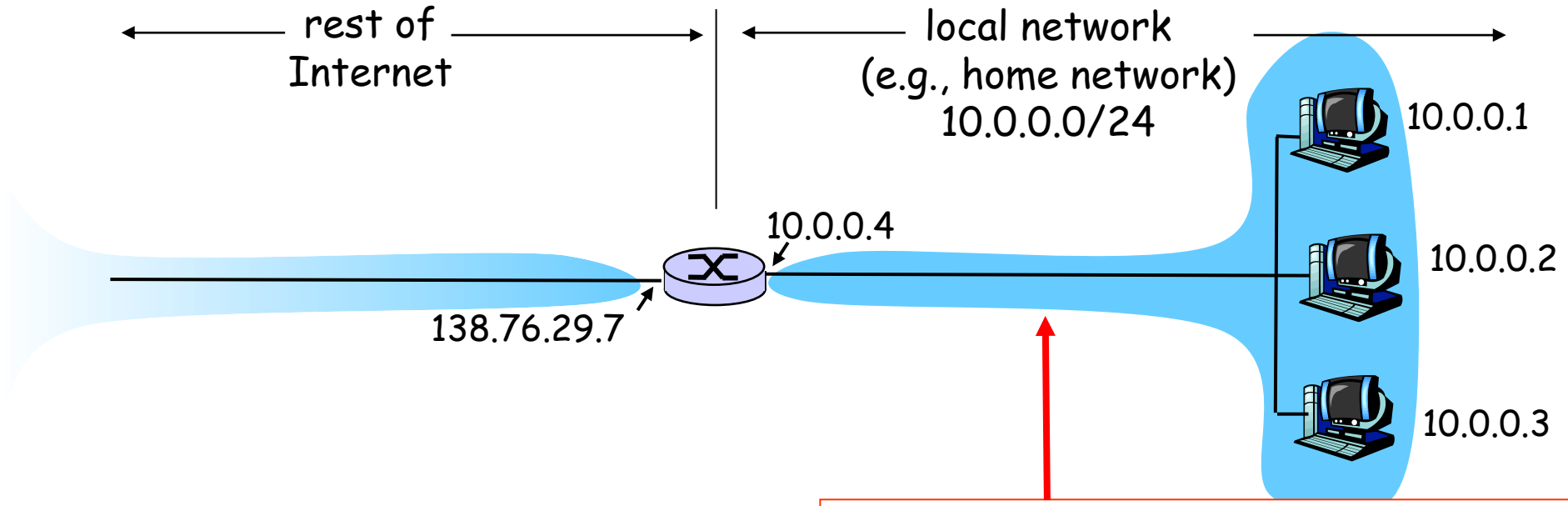
IP address space

- **The address space of IPv4 is extreme wasteful! We must improve the utilization of the IP address space !**
  - **CIDR: Classless InterDomain Routing**
  - **NAT: Network Address Translation**
- **We need a new IP protocol!**
  - **IPv4→IPv6**

NAT – Network Address Translation 网络地址转换

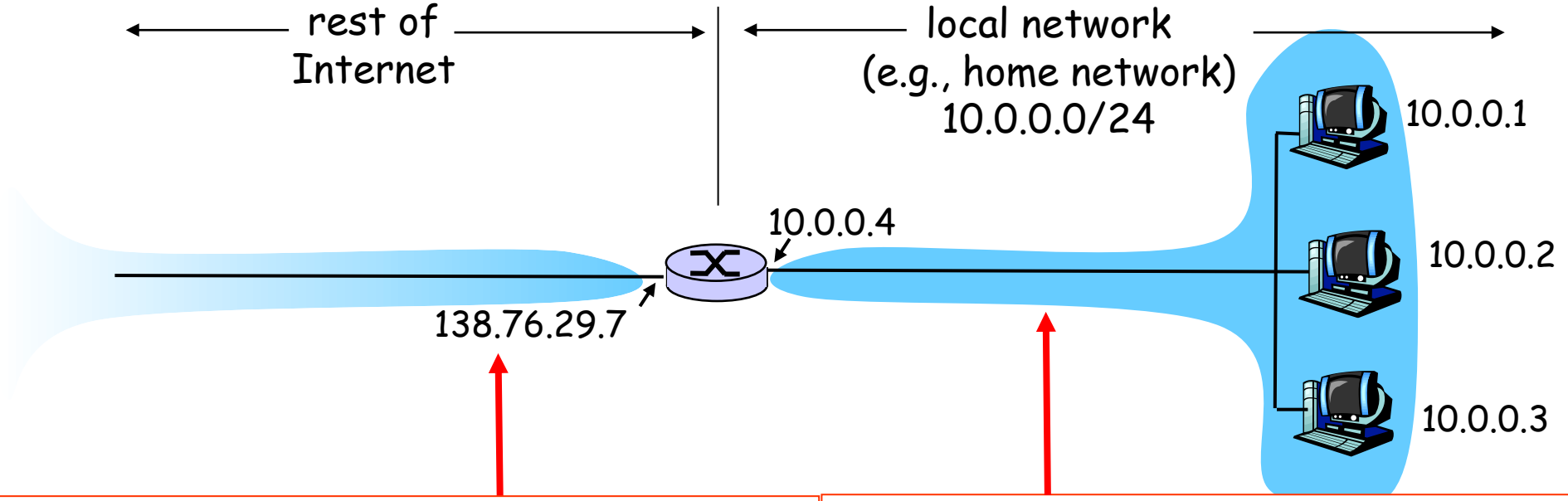
- The basic idea behind NAT is to assign each company a single IP address for Internet traffic.
- Within the company, every computer gets a unique IP address, which is used for routing intramural traffic(内部通信), such as, 10.X.X.X, 172.X.X.X, 192.168.X.X.
- However, when a packet exits the company, an address translation takes place, i.e. internal IP addr → company's true IP address

NAT – Network Address Translation



Datagrams with source or destination in this network have 10.0.0.0/24 address for source, destination (as usual)

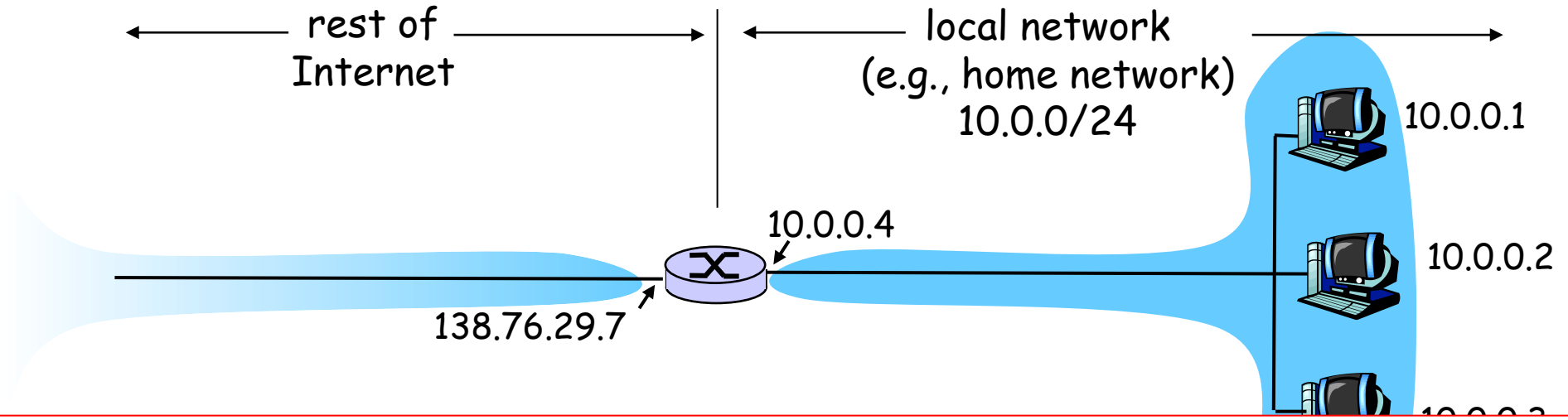
NAT – Network Address Translation



All **datagrams** ***leaving*** **local network have same single source NAT IP address: 138.76.29.7, with different source port numbers**

Datagrams with source or destination in this network have 10.0.0.0/24 address for source, destination (as usual)

NAT – Network Address Translation

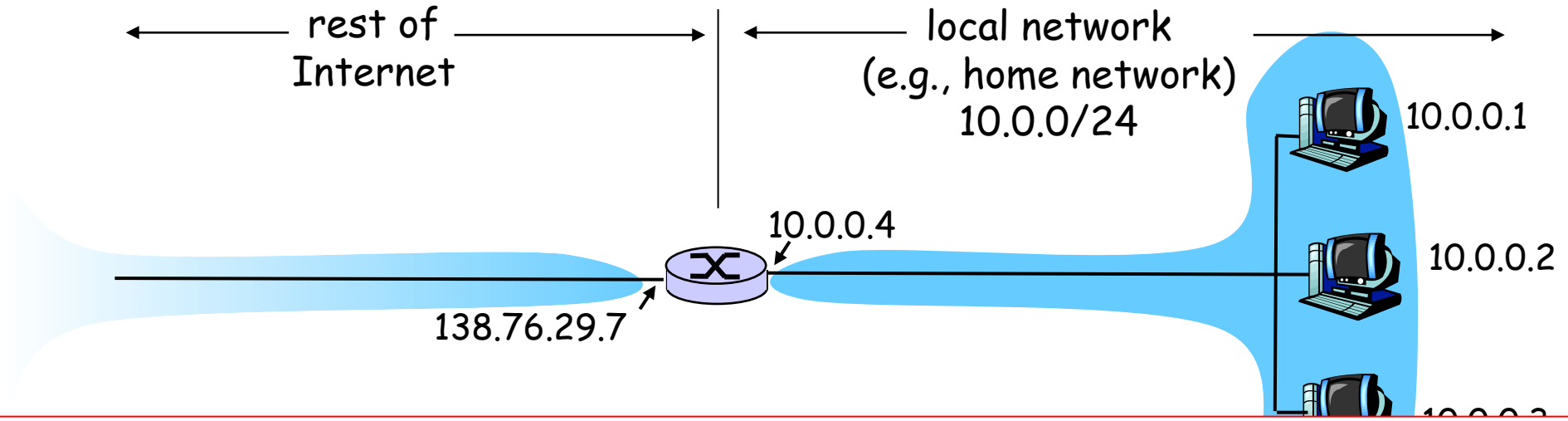


When the packet arrives from the Private Network to NAT router, NAT router will:

① **Insert |Source Address| Source Port| into a table**

② **Change Source address to NAT router address**

NAT – Network Address Translation

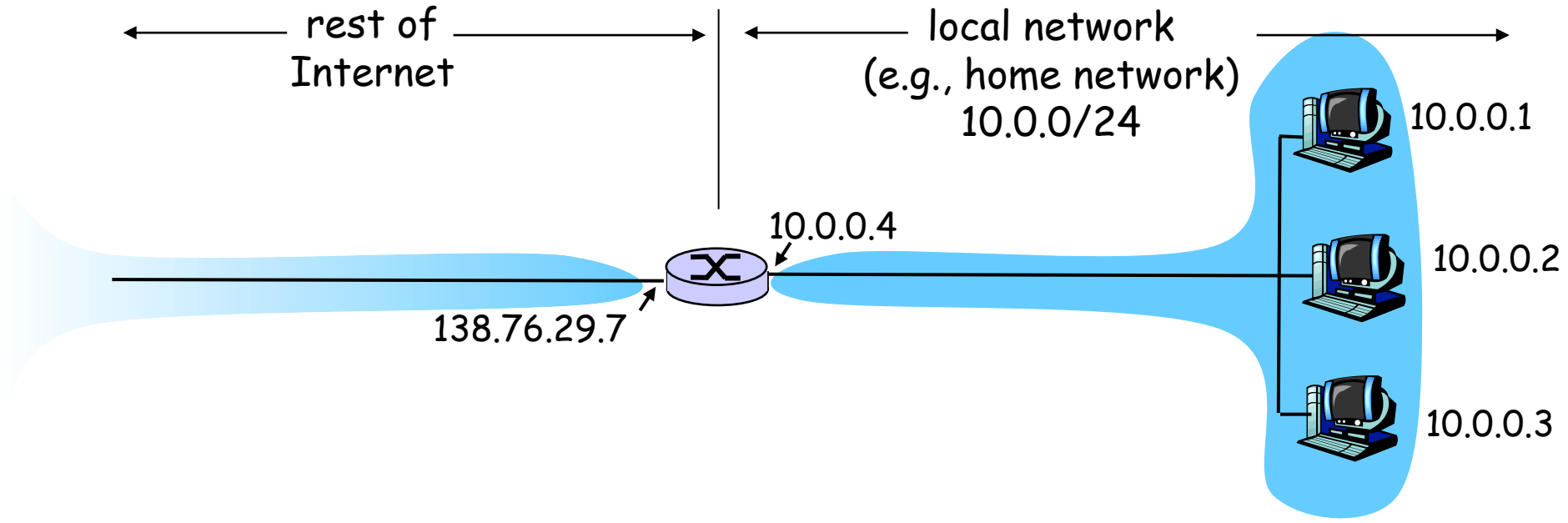


When the packet arrives from the Private Network to NAT router, NAT router will:

③ **Change Source Port to the table offset**

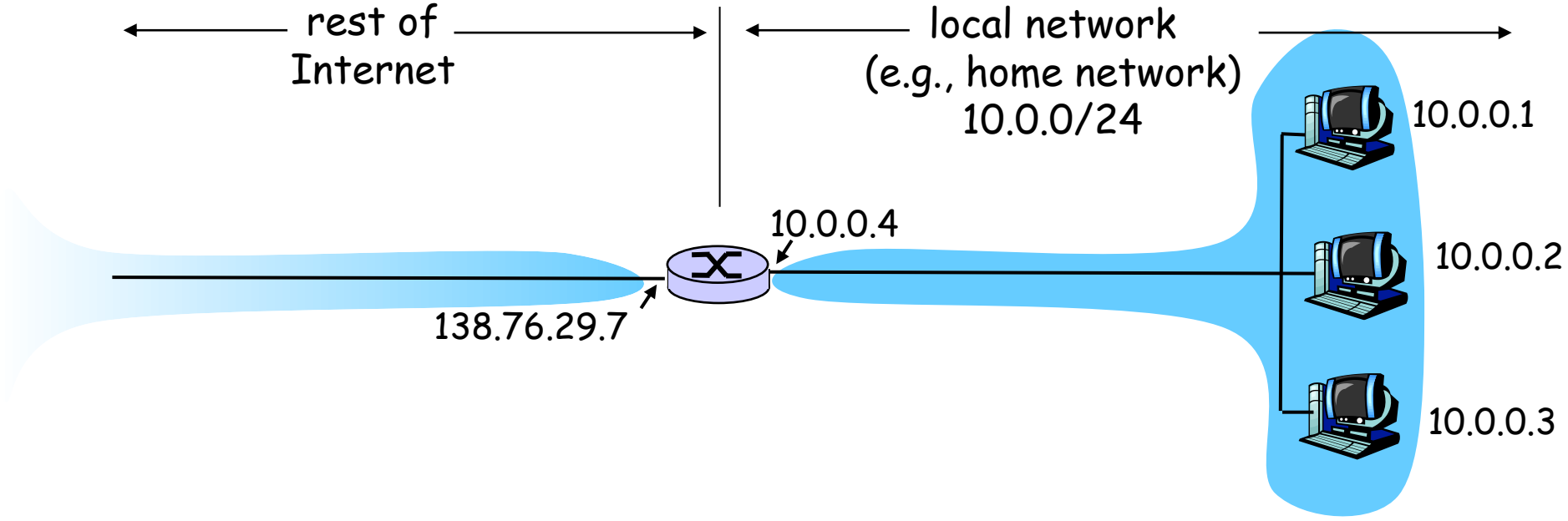
④ **Send the modified packet to the destination on the Internet**

NAT – Network Address Translation



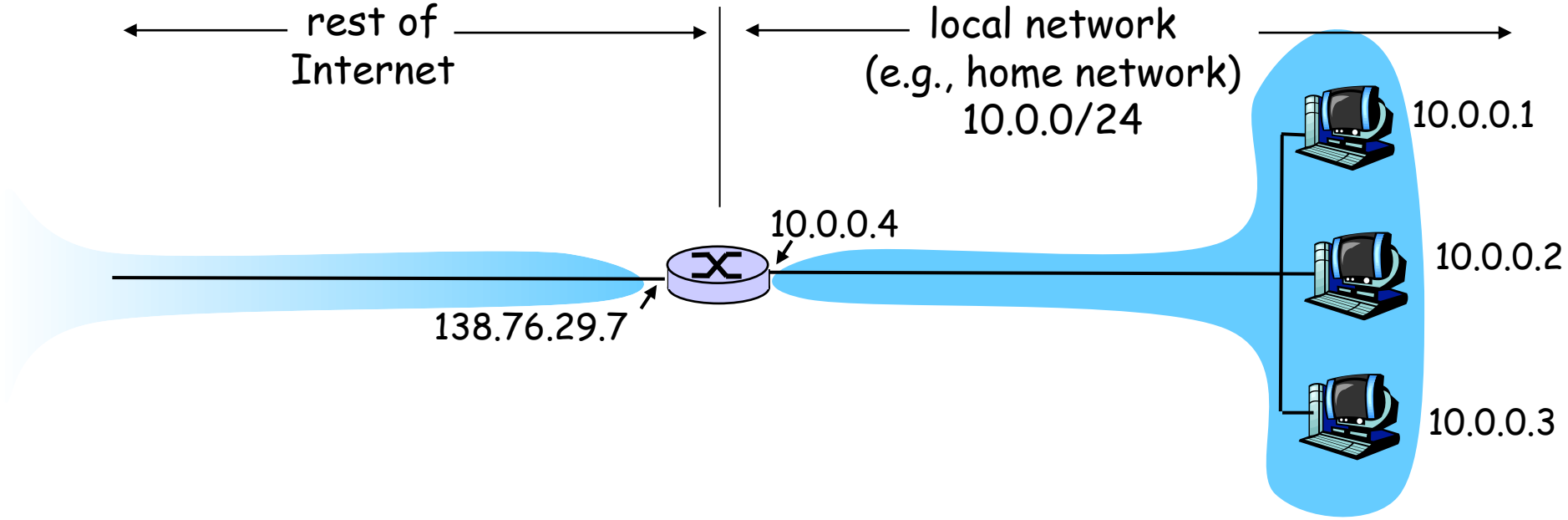
When the response comes back, NAT router replaces the modified Source info with the original source info and then sends it to the client.

NAT – Network Address Translation



Outside node cannot initiate the communication to any node within the private network

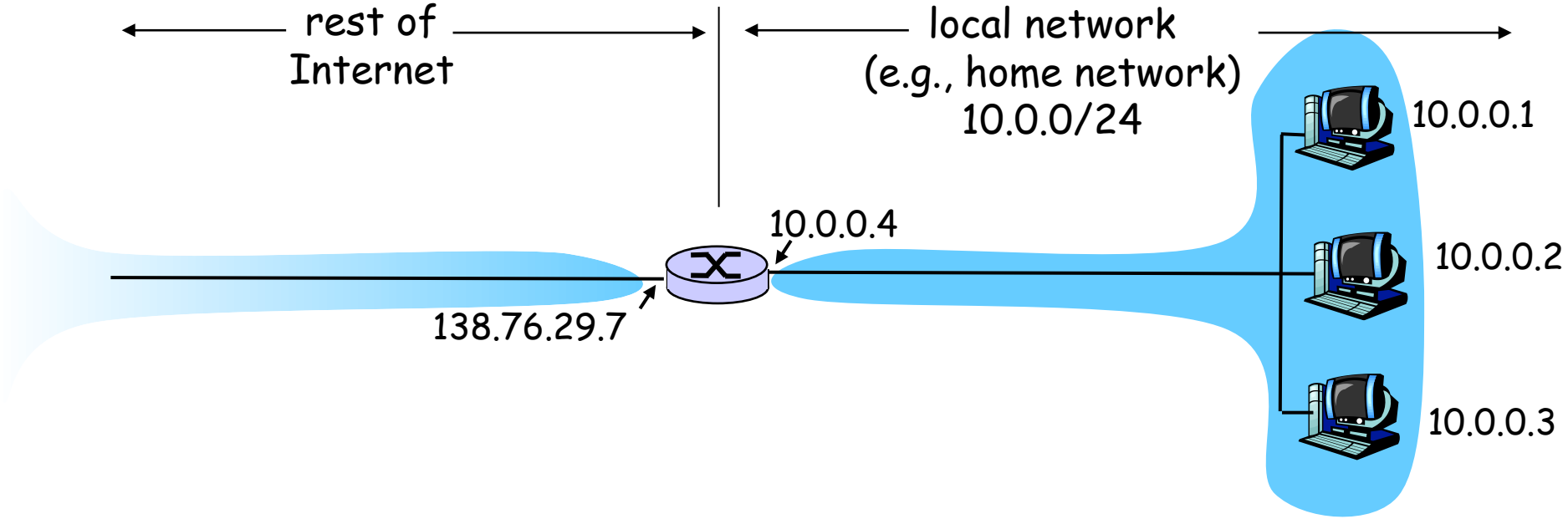
NAT – Network Address Translation



Benefits

can change addresses of devices in local network without notifying outside world

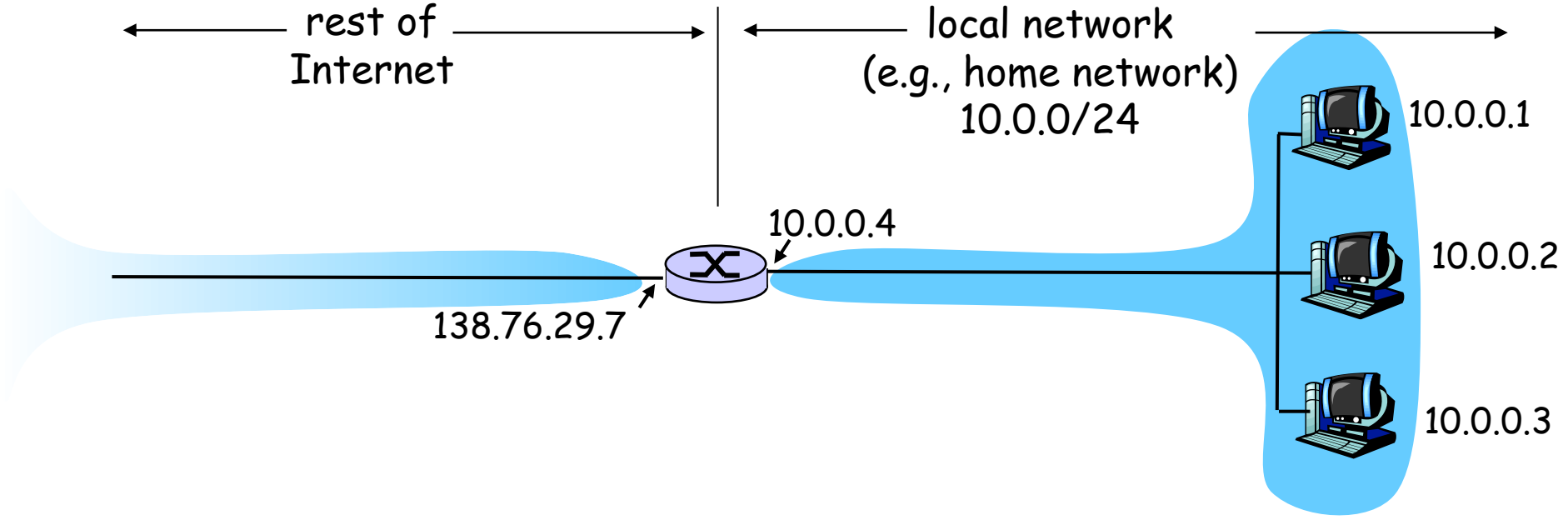
NAT – Network Address Translation



Benefits

no need to be allocated range of addresses from ISP: - just one IP address is used for all devices

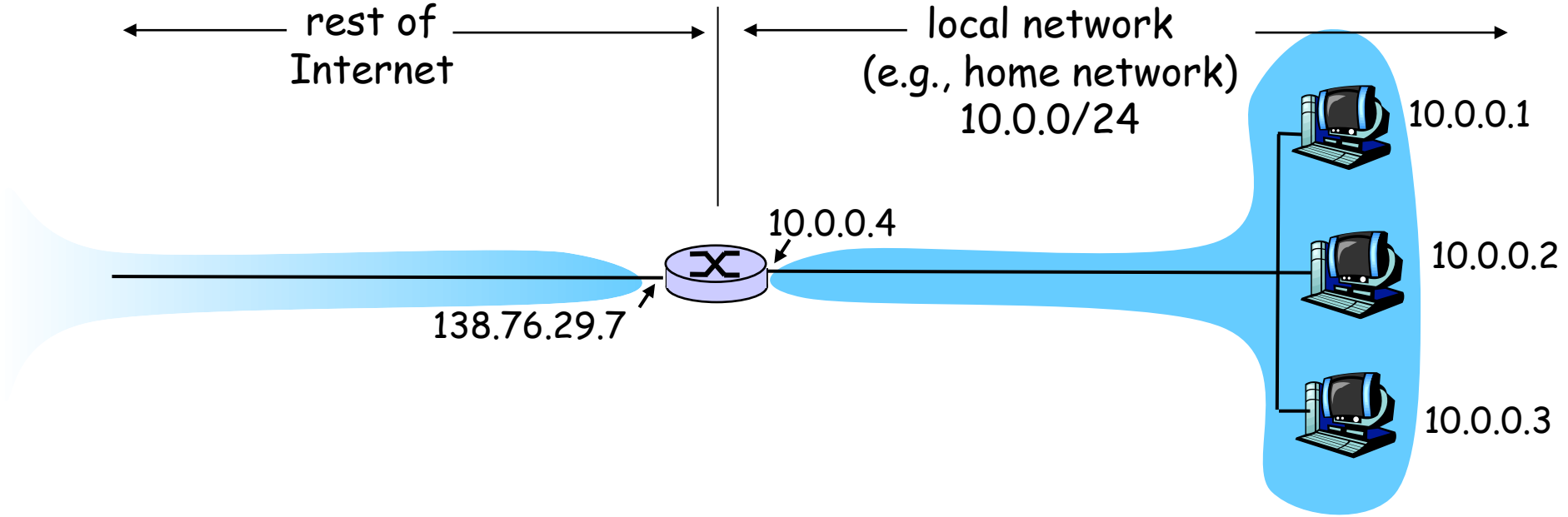
NAT – Network Address Translation



Benefits

can change ISP without changing addresses of devices in local network

NAT – Network Address Translation



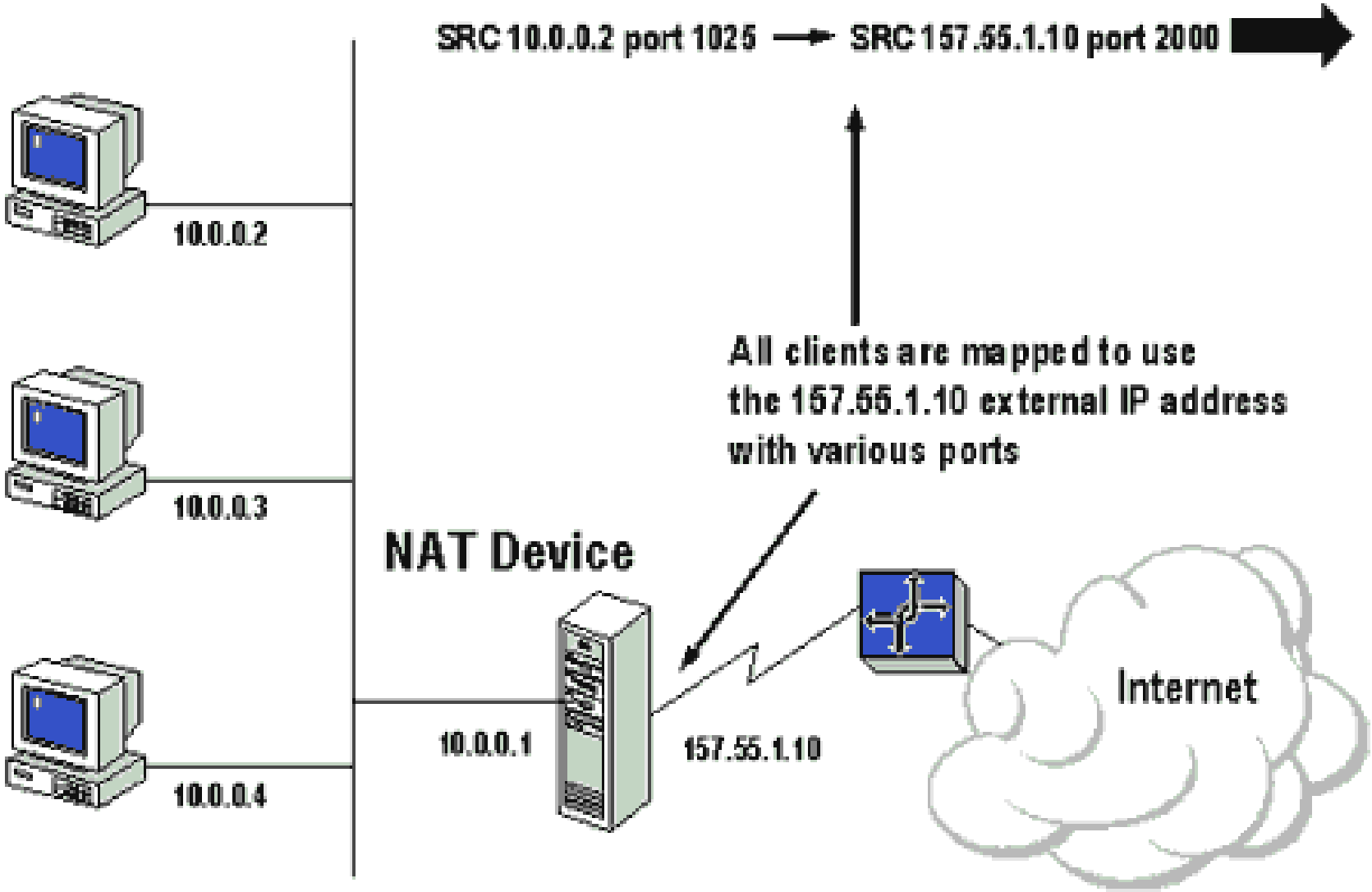
Benefits

devices inside local net not explicitly addressable, visible by outside world (a security plus).

问题：
QQ是怎么穿透NAT进入内网进行通信的？

IP: SUMMARY

NAT – Network Address Translation



NAT – Network Address Translation

- **PROBLEMS WITH NAT**
  - ☹ **If NAT box fails, all the connections are lost**
  - ☹ **It violates the OSI layers independency**

Layers and Services

- **Other services:**
  - **DNS:** translation between domain names and IP addresses
  - **ARP:** Translation between IP addresses and MAC addresses