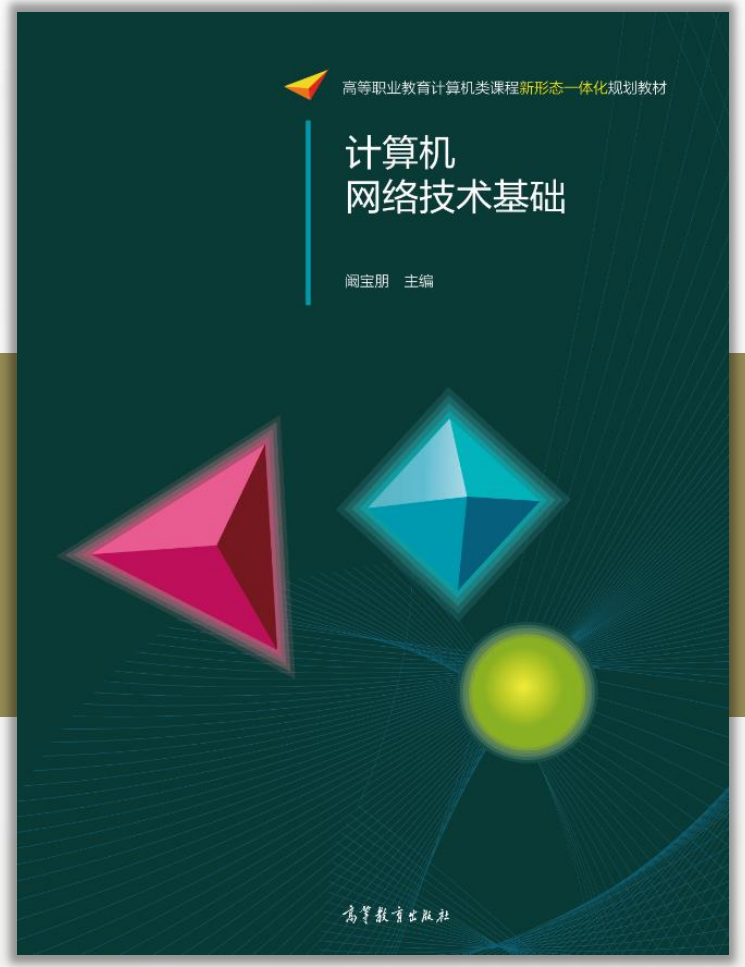


新形态一体化教材 配套MOOC课程

计算机网络技术基础

主编 阚宝朋

高等教育出版社
书号：978-7-04-043546-7

扫描教材上二维码 实现随扫随学

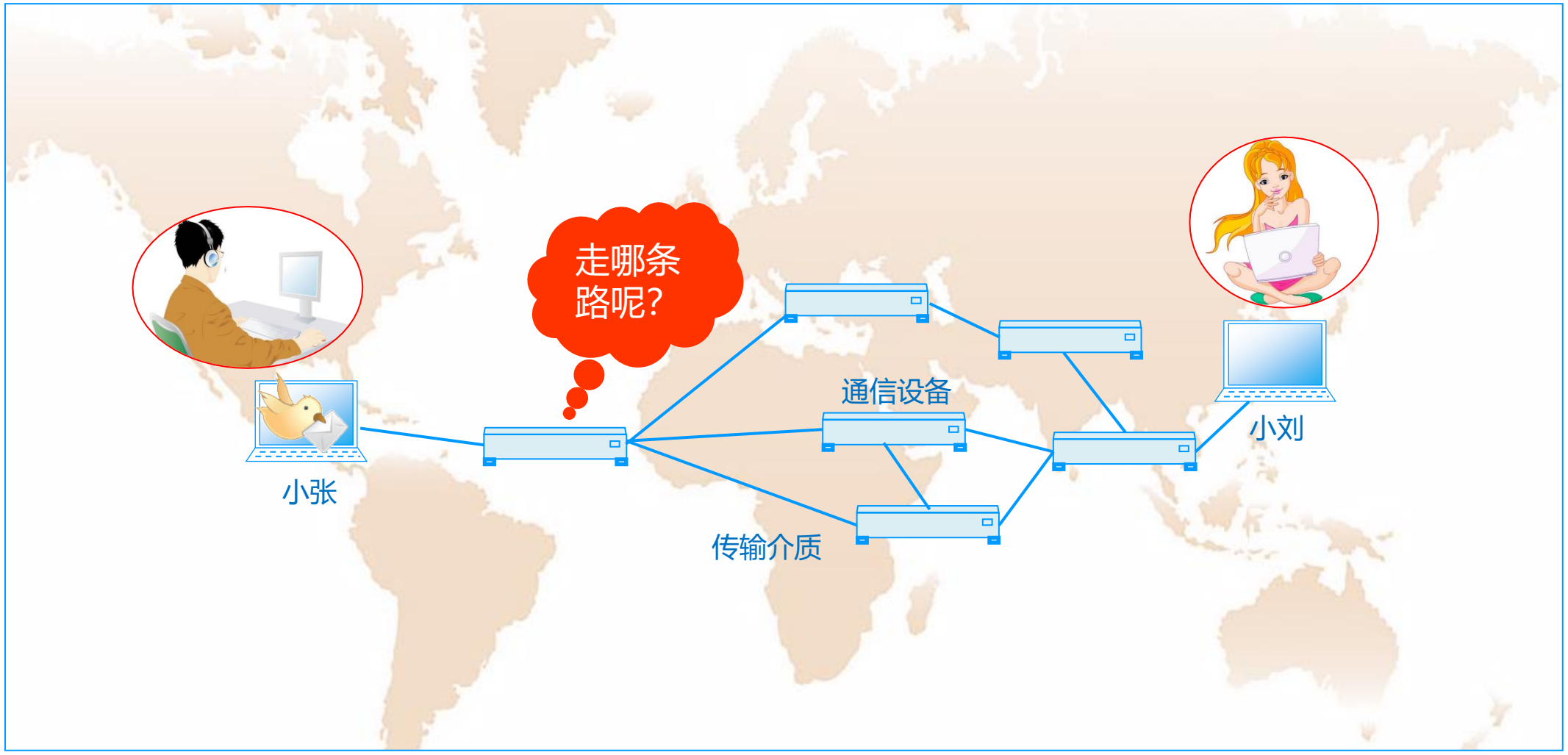
高等教育出版社
HIGHER EDUCATION PRESS

网络层的主要功能

网络基础

高等教育出版社
HIGHER EDUCATION PRESS

网络层的主要功能



网络层关注的是：如何将数据包从源端找到合适网络路径送达目标端。

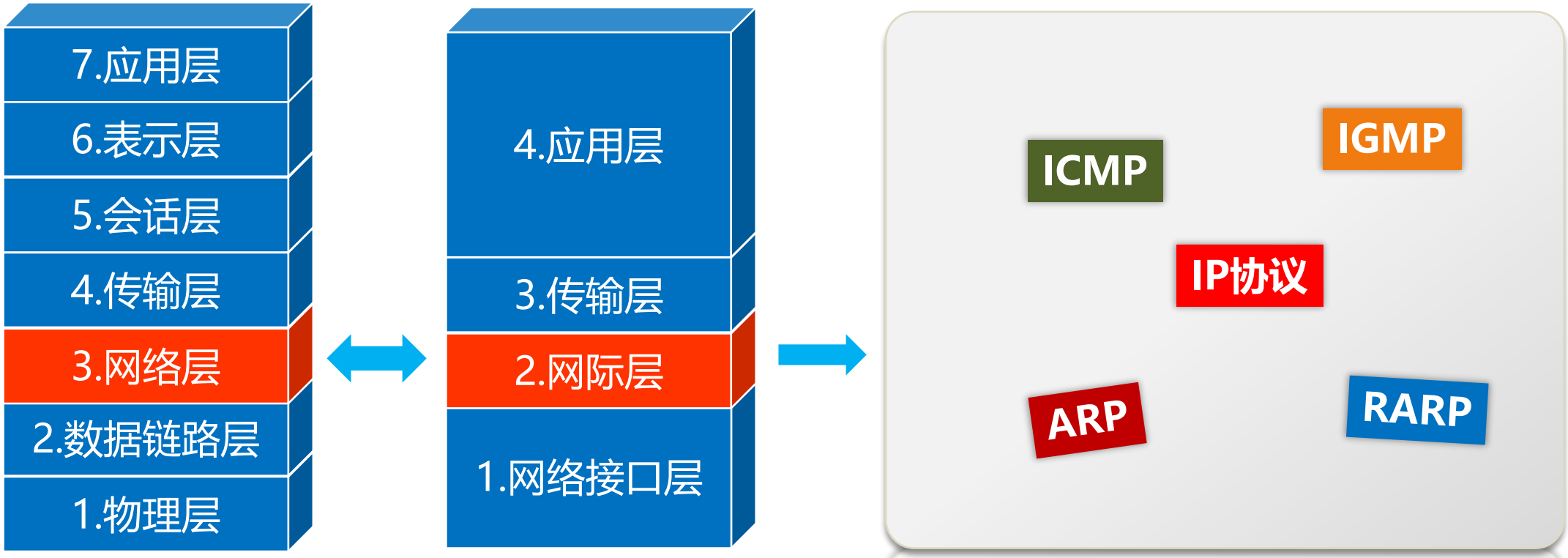
目录
Contents

学习目标

- 了解网络层协议
- 了解网络层的主要功能

高等教育出版社
HIGHER EDUCATION PRESS

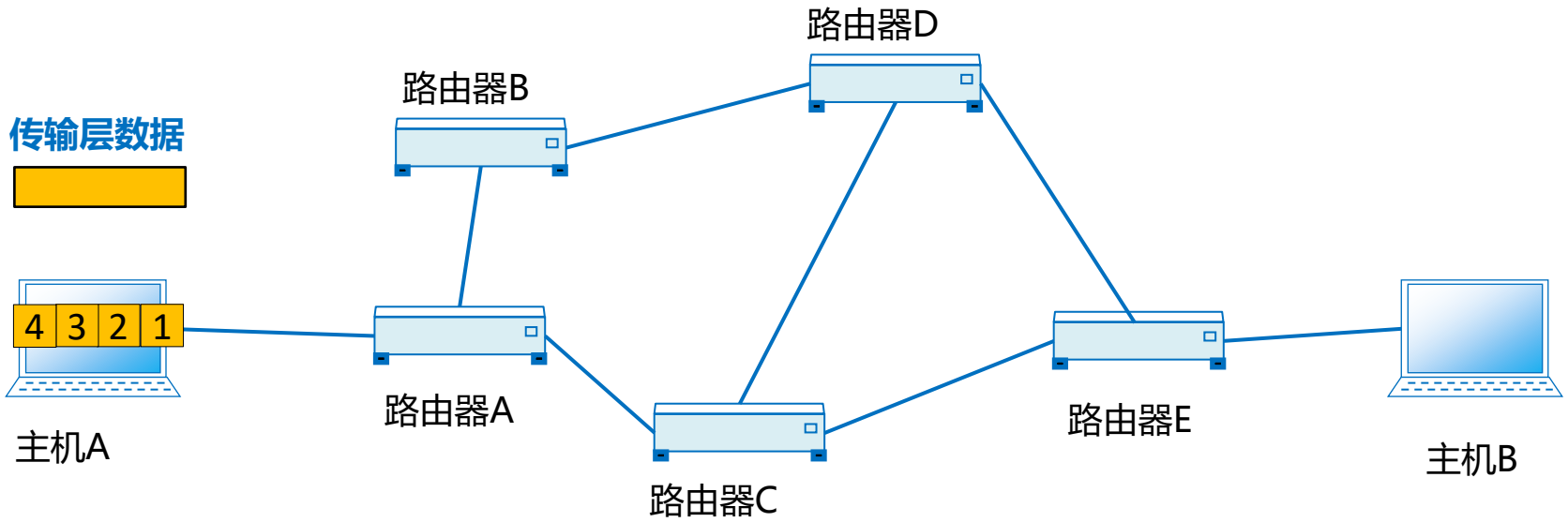
网络层的位置

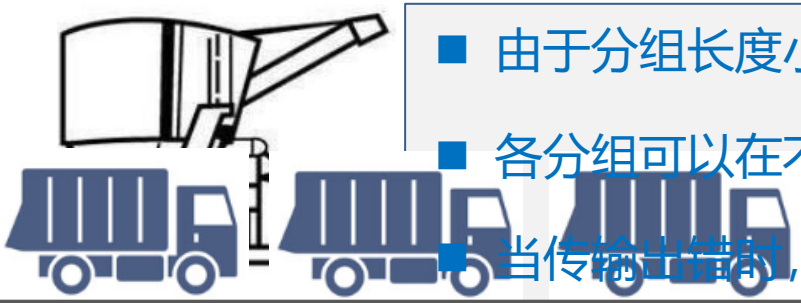


OSI参考模型　　TCP/IP协议栈　　网络层主要协议

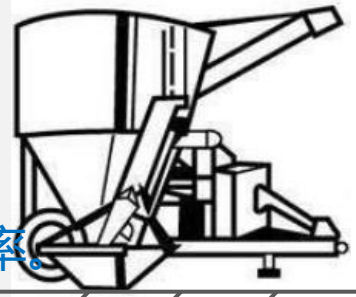
数据包分组与封装

分组交换是以分组为单位的存储转发的传输方式，将长的报文分割成若干短的分组进行多次传输。



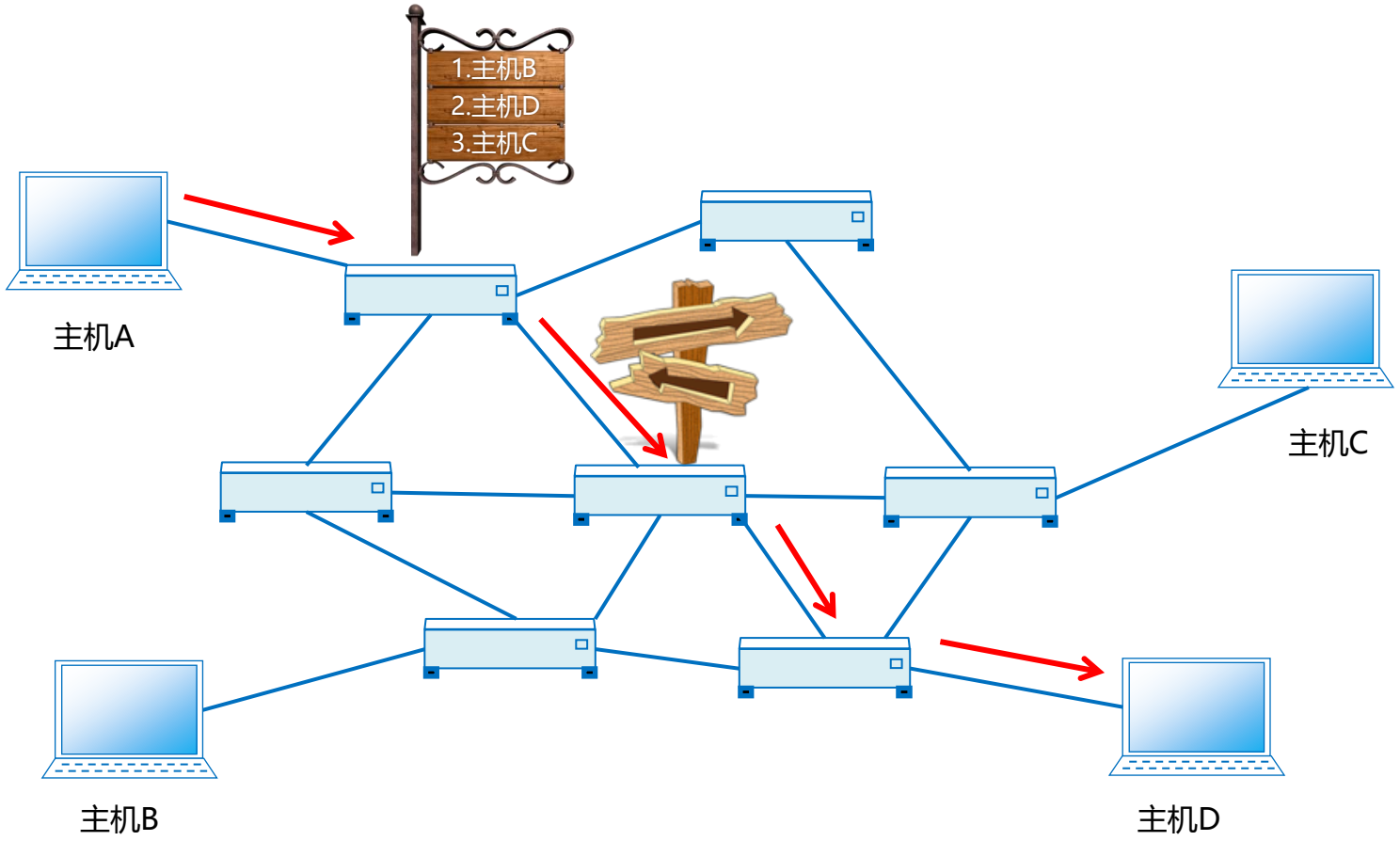


- 由于分组长度小，大大提高了转发速度；
- 各分组可以在不同传输路径上同时被发送，降低了总体的传输时间；
- 当传输出错时，只需重传出错的分组，而不必重传整个报文，提高了效率。



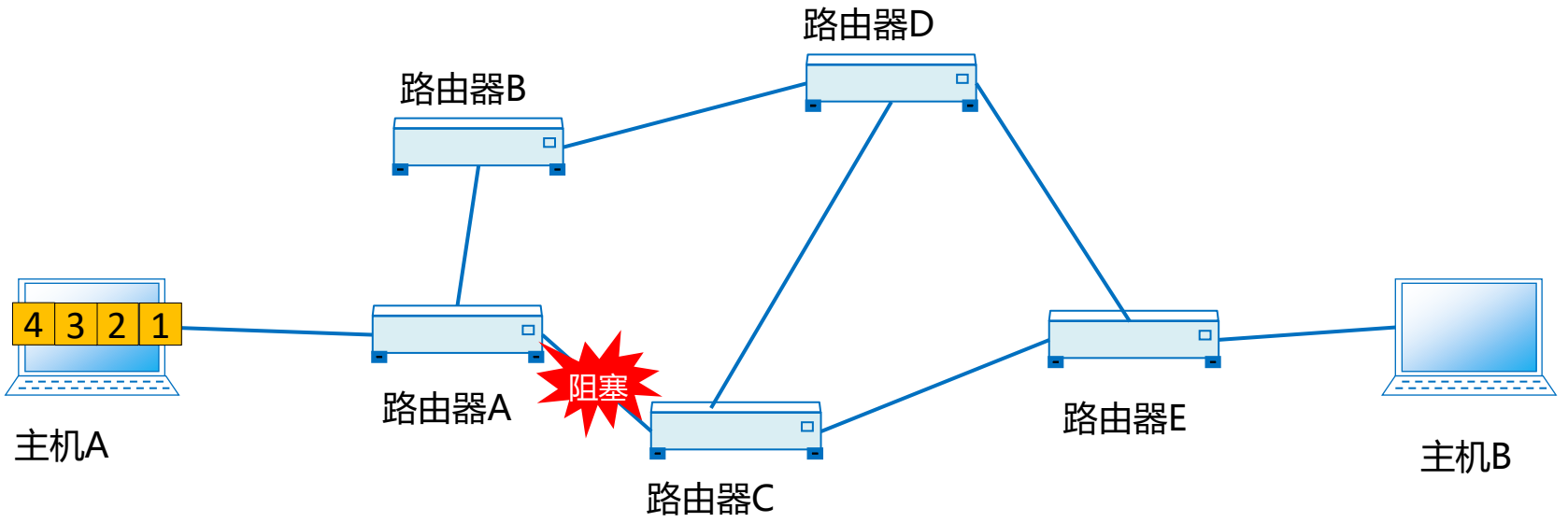
路由与转发

路由转发：源与目的主机之间可能存在多条相通的路径，网络层选择一条“最佳”路径完成数据转发。



拥塞控制

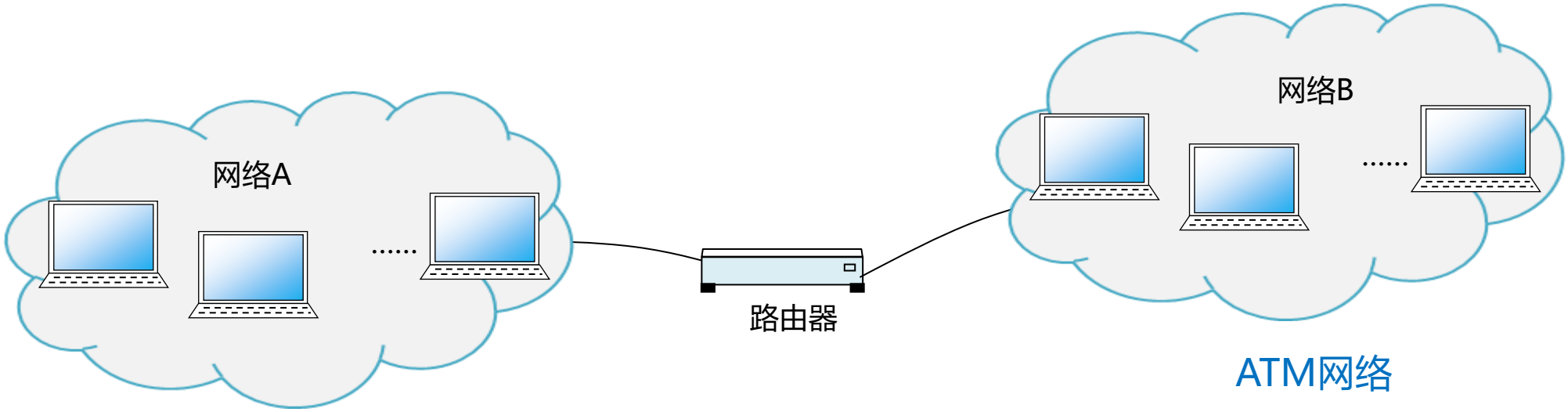
拥塞控制：合理分配数据包的转发路径，提高转发效率。



- 当产生网络拥塞时，及时更换传输路径；

异种网络的互连

异种网络的互连：当源主机和目标主机的网络不属于同一种网络类型时，为了解决不同网络在寻址、分组大小、协议等方面的差异，要求在不同种类网络交界处的路由器能够对分组进行处理，使得分组能够在不同网络上传输。



- 不同的网络类型对分组大小要求不一样，需要重新分组

网络层提供的服务类型

网络基础

目录
Contents

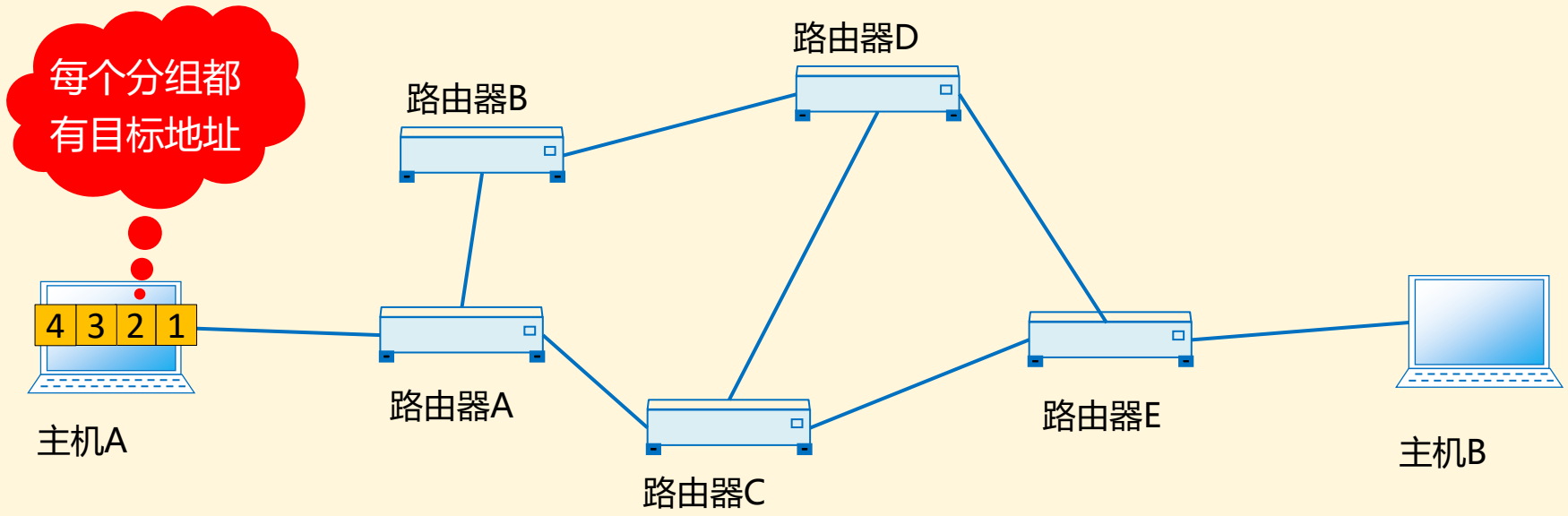
学习目标

- 了解网络层提供的服务类型
- 了解数据报与虚电路的区别

数据报方式

以Internet为代表的阵营认为：

网络中传送的每个分组需要携带完整的目标地址，分组的排序及流控制需要终端来解决

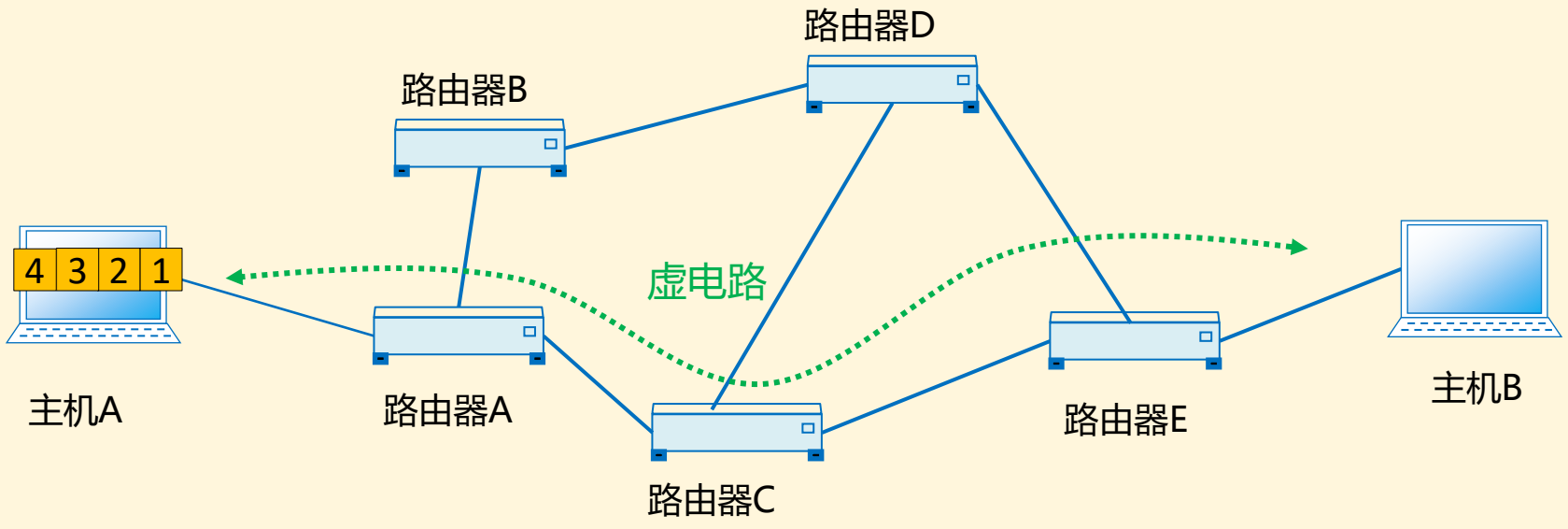


Internet网络层的IP数据报的转发

虚电路方式

以电话公司为代表的阵营认为:

通信子网应该提供可靠的、面向连接的服务。通信的两端需要建立一条逻辑链路（不是物理链路），以保证传输的质量。



ATM网络

数据包与虚电路比较

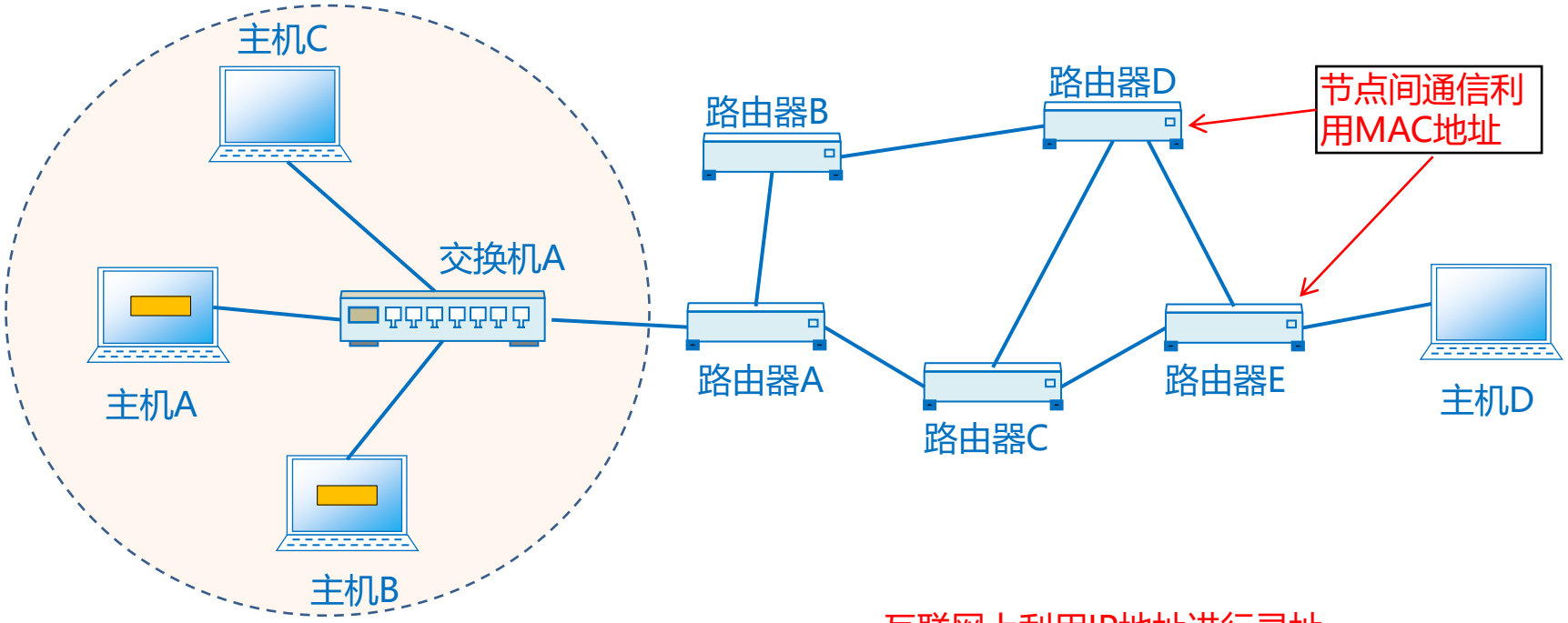
数据报	比较方面	虚电路
不需要建立逻辑链路	连接建立	需要建立逻辑链路
每个分组需要完整源和目的地址	目的站地址	每个分组包含相同的虚电路号
可根据网络状况选择不同路径传输	传输路径	每个分组包含相同的虚电路号
可能丢失分组，路由会发生变化	传输节点出现故障	整个虚电路不能工作
不保证按发送顺序到达目的主机	分组顺序	分组按照发送顺序到达目的主机
可根据网络流量改变传输路径	流量平衡	不能根据网络流量改变传输路径

网络层与数据链路层的关系

网络基础

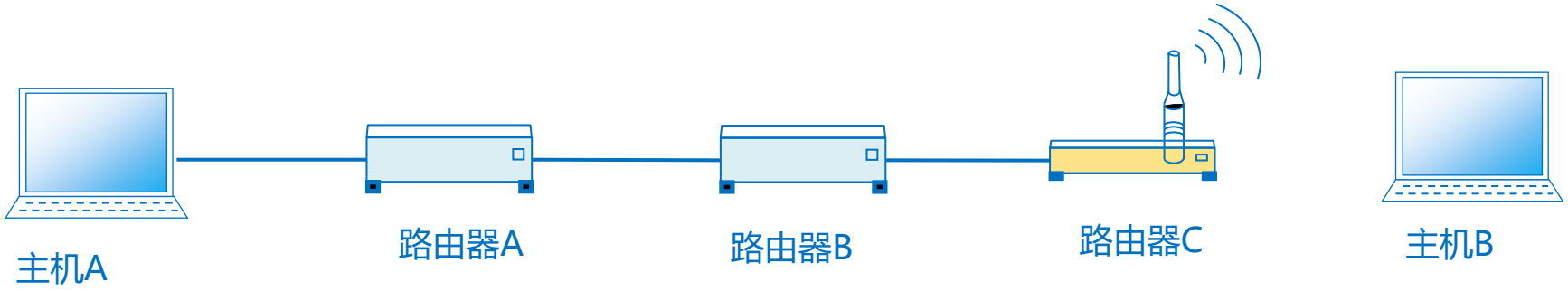
网络层与数据链路层的关系

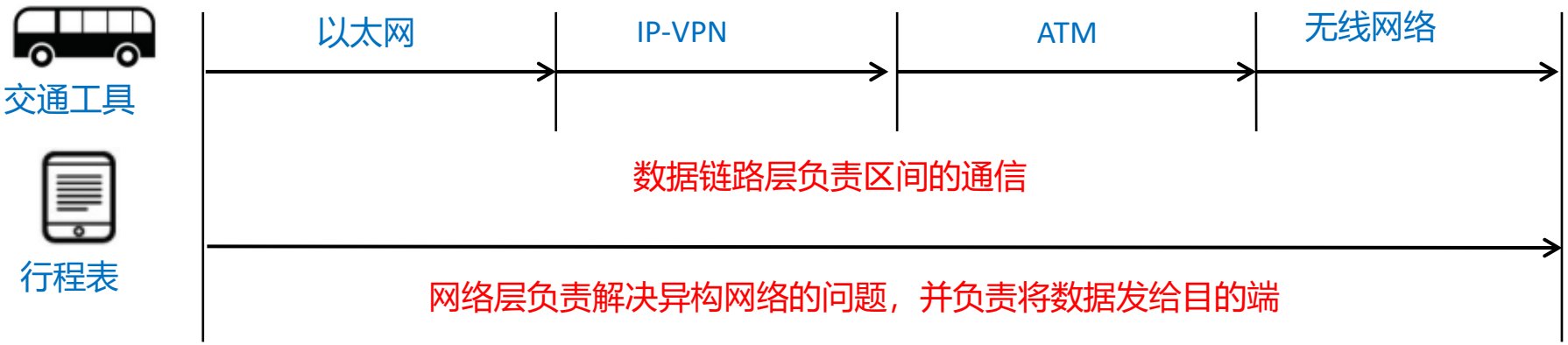
1.数据链路层实现同一局域网中利用MAC地址通信，网络层利用IP地址实现网络寻址。



网络层与数据链路层的关系

2. 网络层要解决异构网络互联的问题，按照不同网络协议的格式完成数据的重新封装，数据链路层实现的是保证两端链路的连通性，可以说数据链路层不能分辨异构的网络。



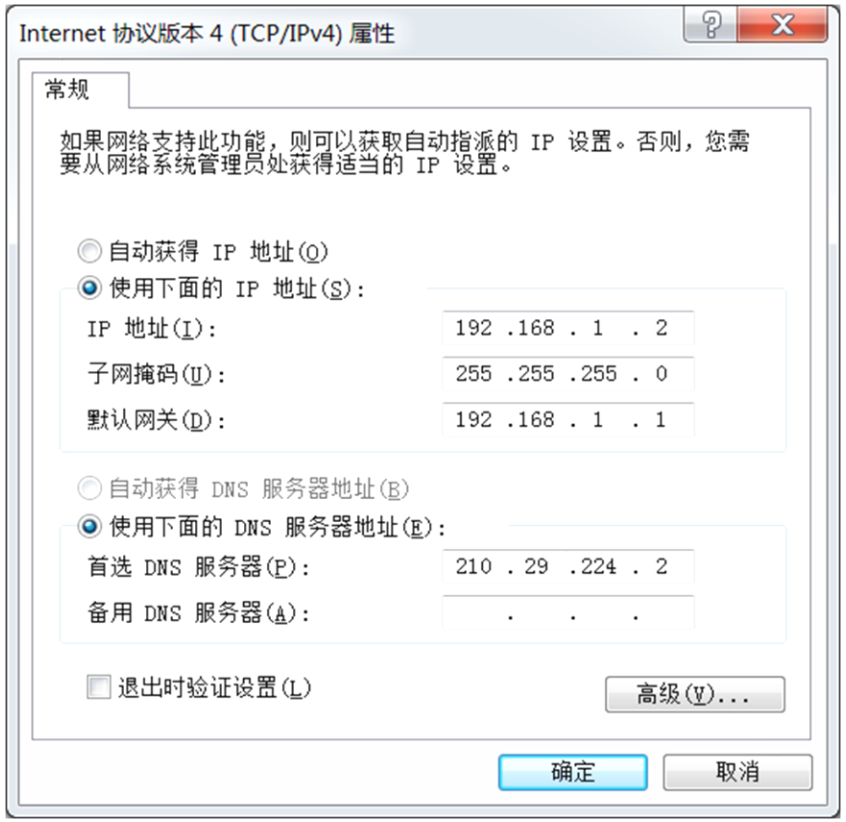


IP地址基础知识

网络基础

IP地址基础知识

网络层主要利用IP地址完成路由寻址功能。

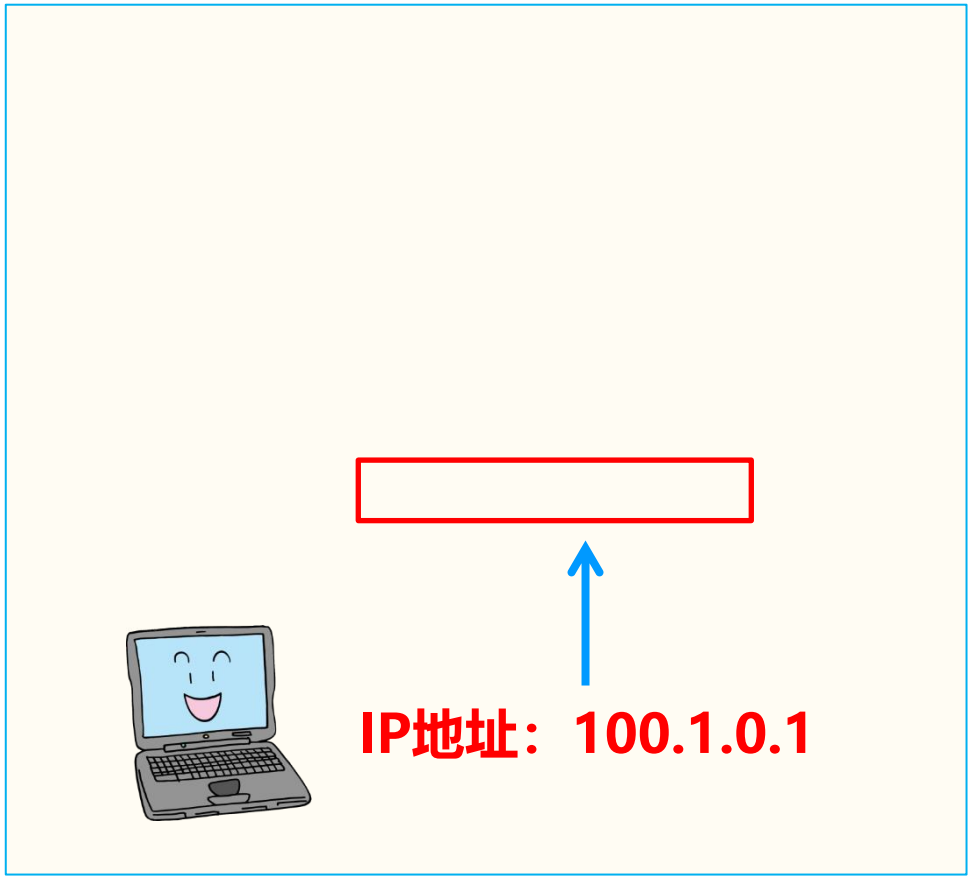


目录
Contents

学习目标

- 掌握IP地址的结构
- 掌握子网掩码的作用
- 掌握网关的作用

IP地址 是主机在Internet上的一个全世界范围内唯一32位标识符



点分十进制：用4个十进制数表示，中间用圆点隔开

100. 29 . 0 . 2

二进制： 01100100 00011101 00000000 00000010

8 + 8 + 8 + 8

32位

思考：计算机使用二进制，为什么用十进制表示IP地址呢？

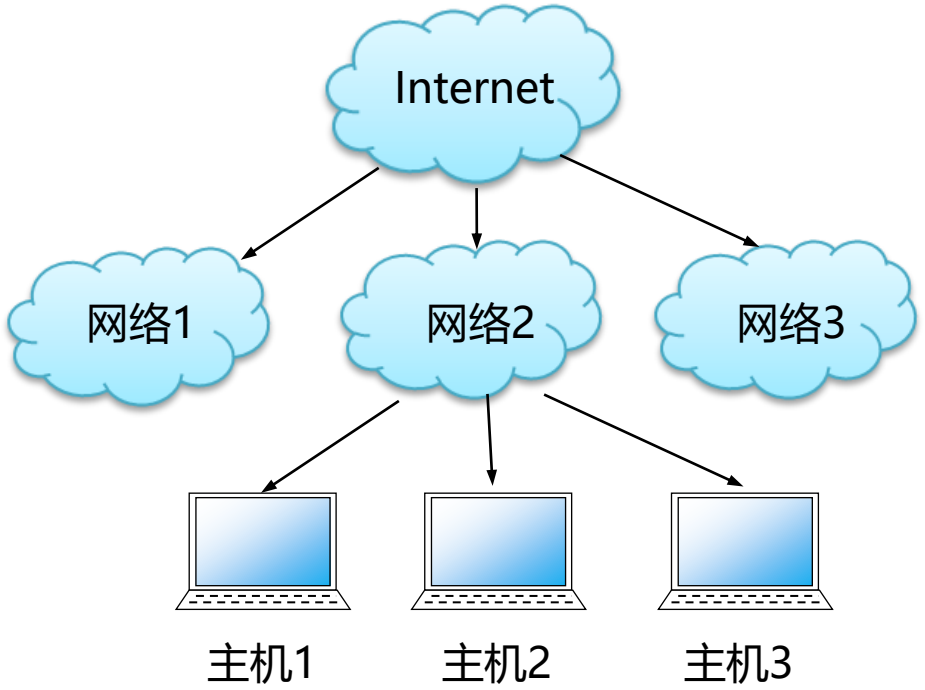
2.IP地址结构

100 . 29 . 0 . 2

网络号　　主机号

区号　　电话号

0517 – 83808237



互联网层次结构

思考：如何确定网络号呢

子网掩码
Netmask

通过将网络号所占二进制位置为1，主机号所占二进制位置为0，然后转换成十进制计算得来的。用来确定IP地址的网络号。

100 . 29 . 0 . 2

网络号　　主机号

01100100 00011101 00000000 00000010

↓

11111111 11111111 00000000 00000000

↓

255. 255 . 0 . 0

计算网络号方法：IP地址与子网掩码**与**运算

01100100 00011101 00000000 00000010

11111111 11111111 00000000 00000000

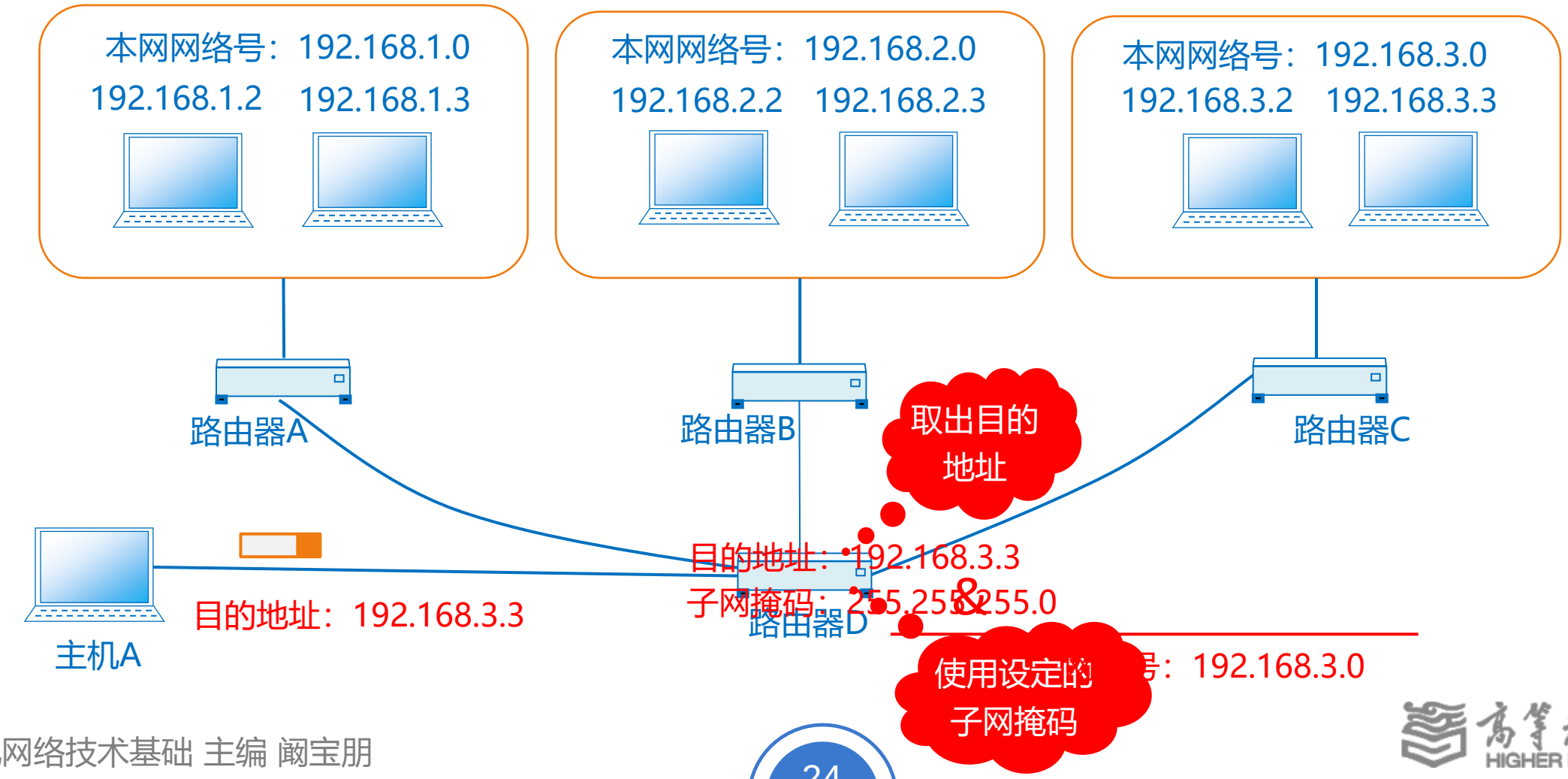
01100100 00011101 00000000 00000000

↓

100 . 29 . 0 . 0

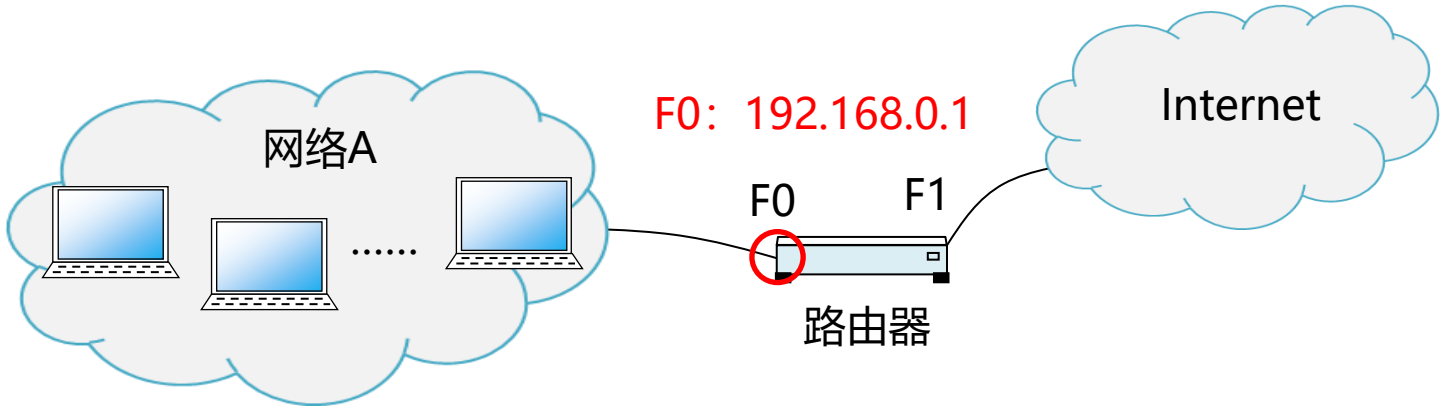
表示方法： 100.29.0.0 **/ 16**　　**前缀表示法**

应用举例：


本网网络号：192.168.1.0
192.168.1.2
192.168.1.3
本网网络号：192.168.2.0
192.168.2.2
192.168.2.3
本网网络号：192.168.3.0
192.168.3.2
192.168.3.3
路由器A
路由器B
路由器C
路由器D
主机A
目的地址：192.168.3.3
取出目的地址
目的地址：192.168.3.3
子网掩码：255.255.255.0
&
使用设定的子网掩码
号：192.168.3.0

网关
Gateway

一个网络的出口就称为网关。当一个主机要将数据发送给其他网络的主机时，通常首先将数据发往网关。



分类的IP地址

网络基础

目录
Contents

学习目标

- 掌握IP地址的分类
- 掌握每类的网络位数
- 掌握每类网络包含主机数量

1.具体分类方式

第一字节范围

0 00000000-01111111

128 10000000-10111111

192 11000000-11011111

224 11100000-11101111

240 11110000-11111111

A B C三类为常用地址

192.168.1.1 C类

D类为多播地址

保留为实验科研用

2.每类网络所包含主机数量

IP地址类别	网络地址长度	子网掩码	包含主机数量
A类	8位	255.0.0.0	$2^{24}-2=16777214$
B类	16位	255.255.0.0	$2^{16}-2=65534$
C类	24位	255.255.255.0	$2^{8}-2=254$

255 . 0 . 0 . 0

全局地址与私有地址

网络基础

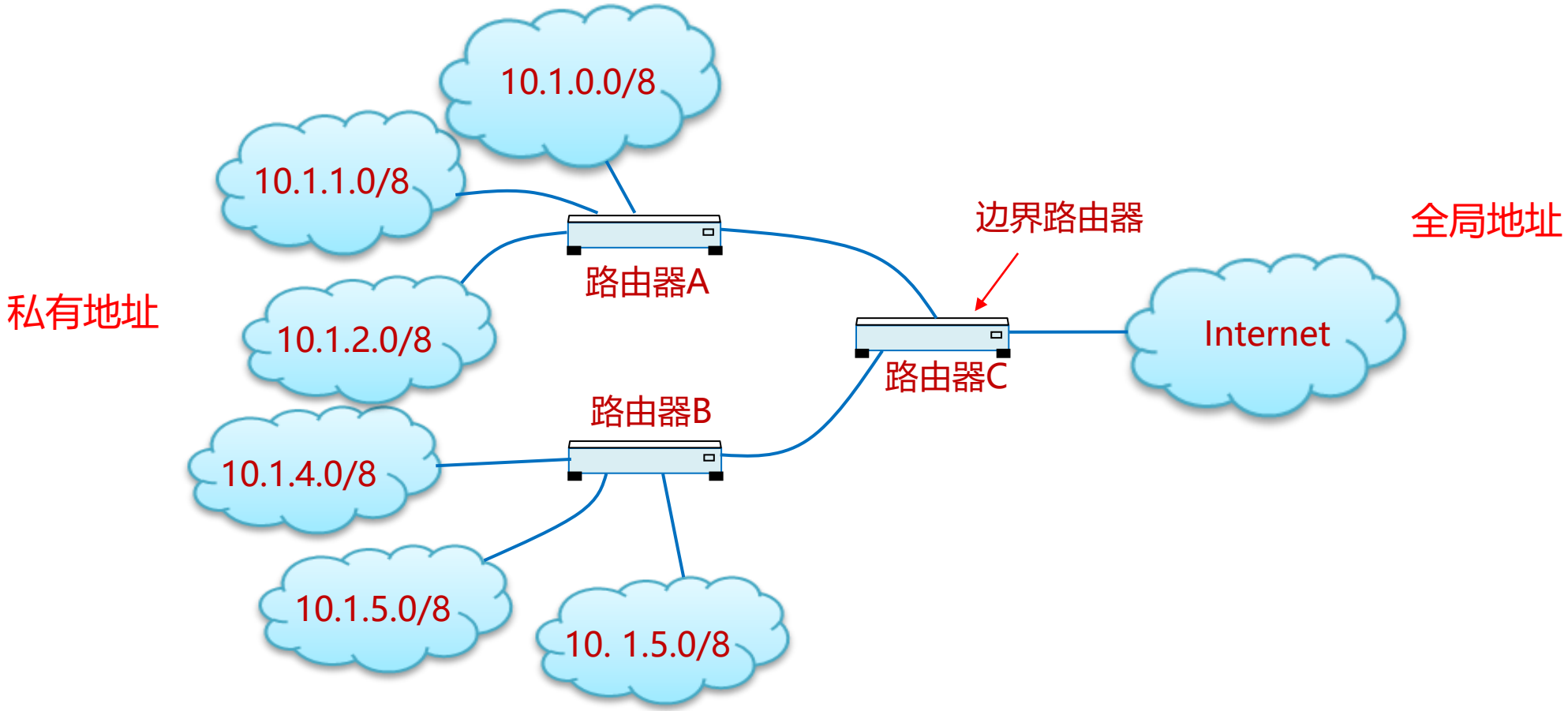
目录
Contents

学习目标

- 了解全局地址的含义
- 掌握私有地址的使用方式
- 掌握私有地址的范围

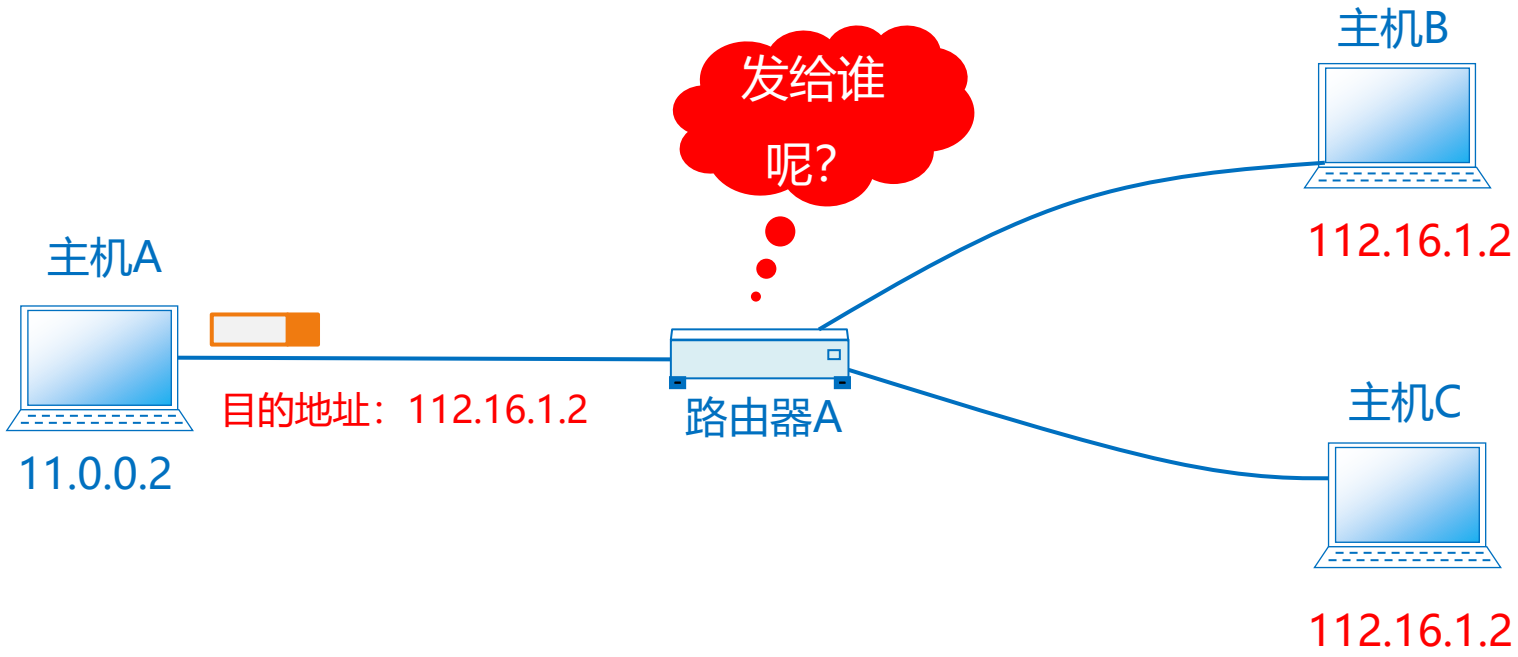
1.全局地址的使用

全局地址也就是可以在公网上（Internet）使用的地址，必须是唯一的。



1.全局地址的使用

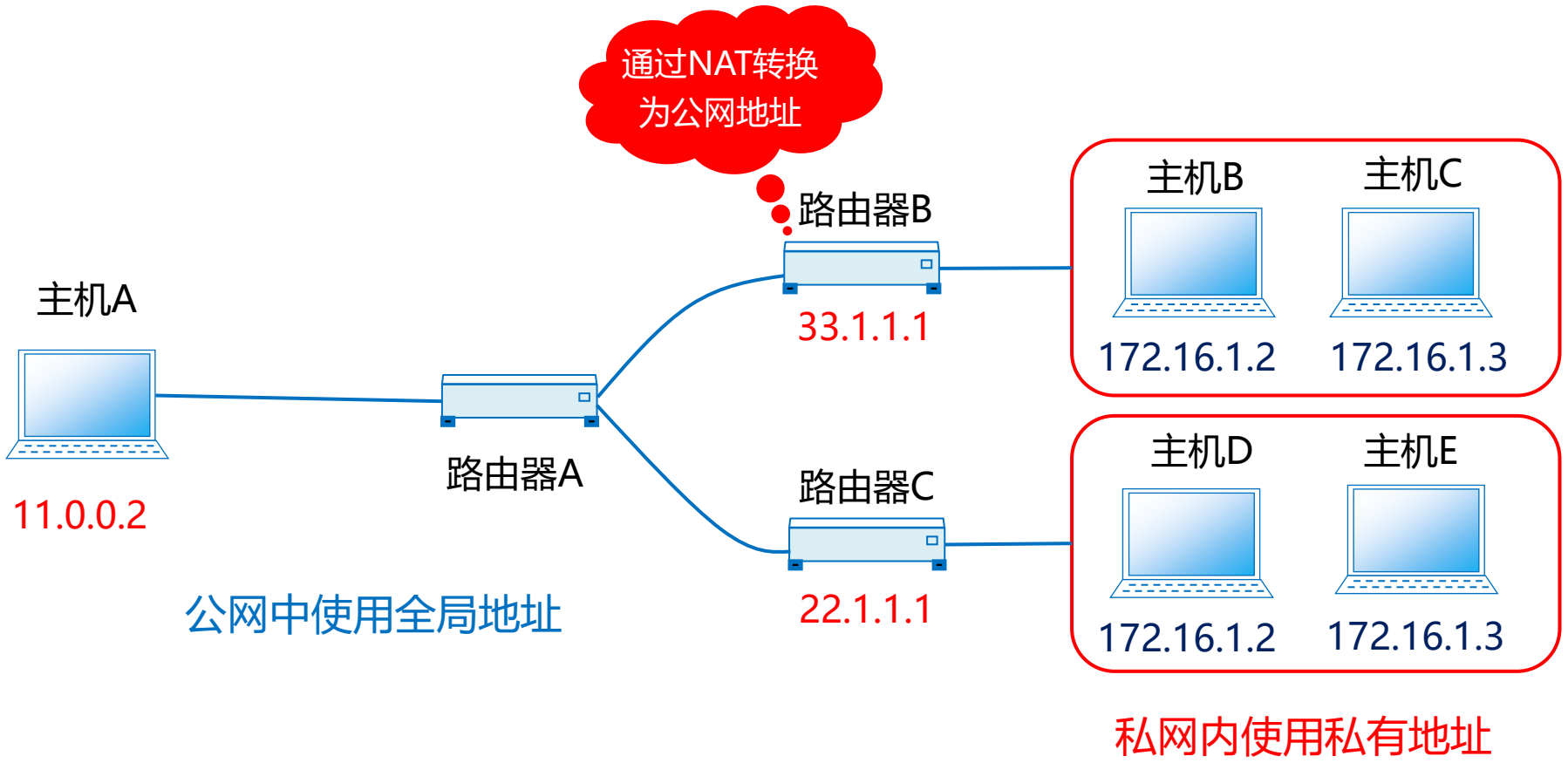
全局地址也就是可以在公网上（Internet）使用的地址，必须是唯一的。



随着互联网的迅速普及，IP地址不足的问题日趋显著。

2.私有地址的使用

私有地址暂时解决了地址短缺问题，它可以在不同的局域网中重复使用。



全局IP地址要在整个互联网内保持唯一性，但私有地址不需要，只要在同一个私网中保证唯一即可。

3.私有地址的范围

私有地址包含了A类、B类和C类三类地址空间中的3个小部分

IP地址类别	私有地址范围
A类	10.0.0.0～10.255.255.255
B类	172.16.0.0～172.31.255.255
C类	192.168.0.0～192.168.255.255

举例：以下哪些地址属于私有地址？

10.1.1.1　　172.32.1.2　　192.168.1.2　　192.168.100.1

特殊IP地址及应用

网络基础

目录
Contents

学习目标

- 理解特殊IP地址的应用

1.网络地址

网络地址包含了一个有效的网络号和一个全“0”的主机号。

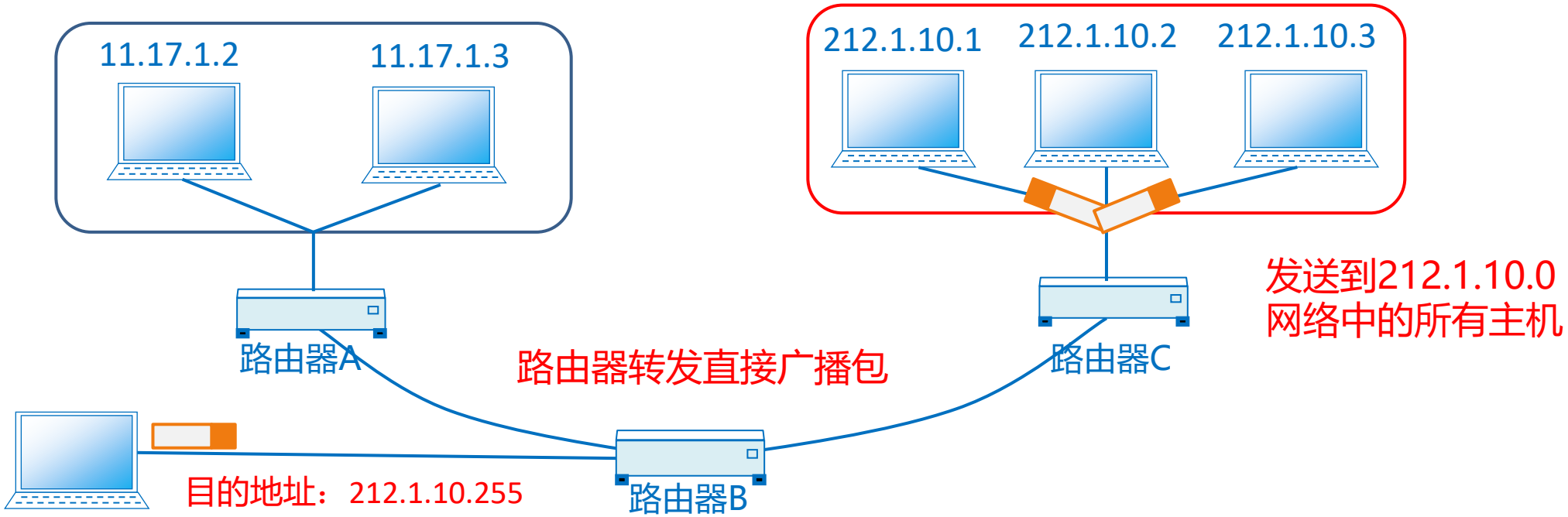
如：114.0.0.0/8

主机位全为0，为网络号，因此不能分配给主机使用。

2.广播地址

直接广播（Directed Broadcasting）

包含一个有效的网络号和一个全“1”的主机号，即将IP地址中的主机号部分全部设置为1，如192.168.1.255/24

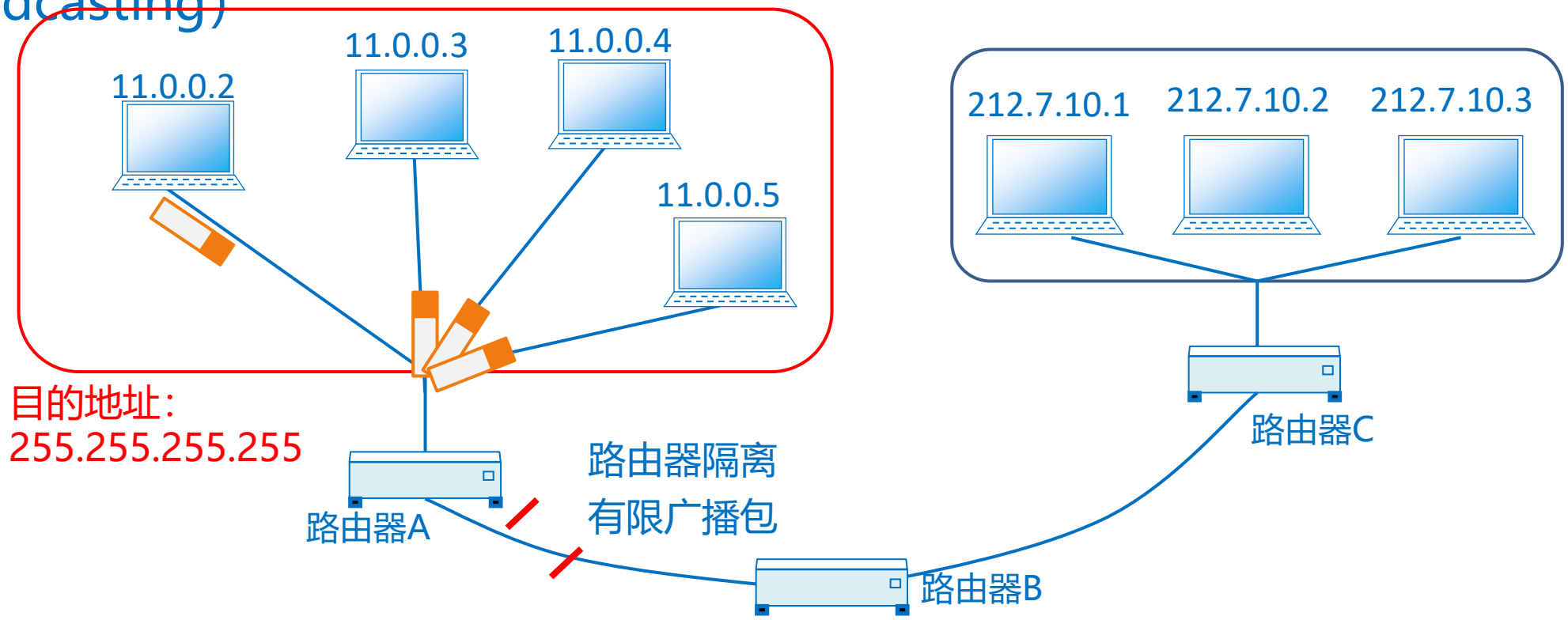


2.广播地址

有限广播（Limited Broadcasting）

也称受限广播地址，指32位全为“1”的IP地址，即255.255.255.255。

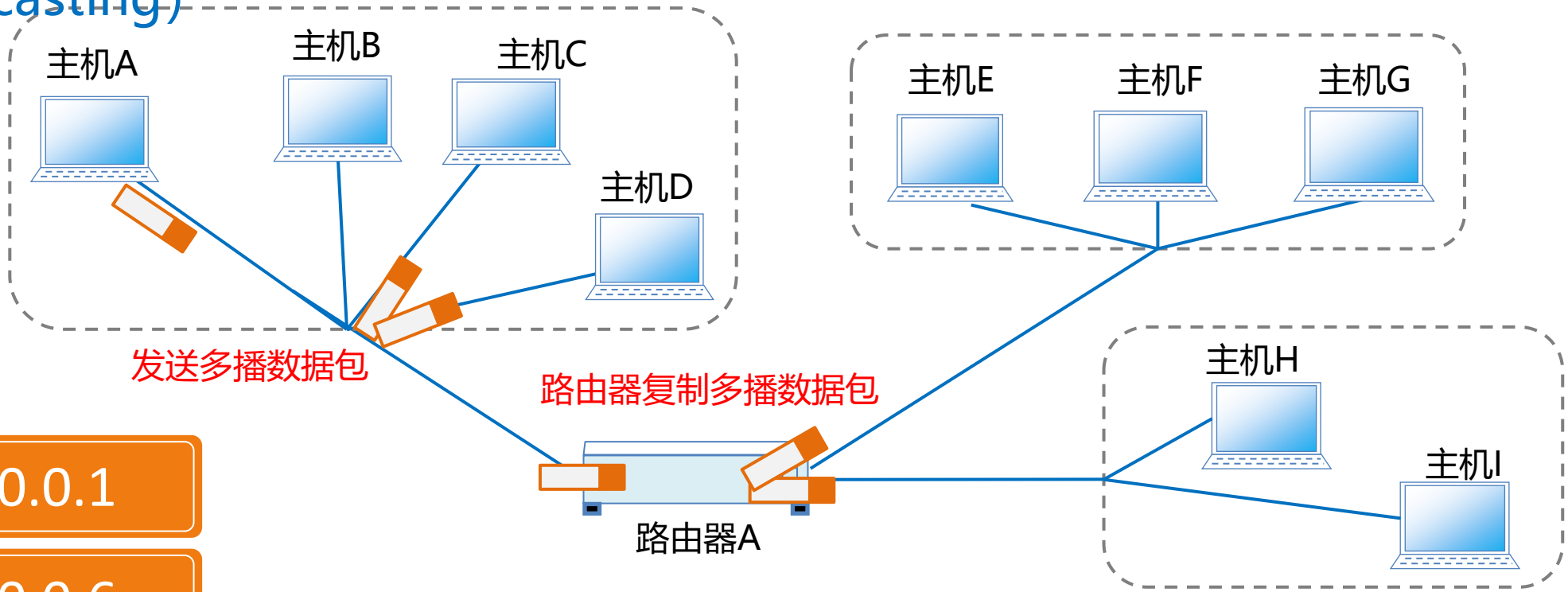
用于本网广播，即被限制在本网络之中。



3.多播地址

多播（Limited Broadcasting）

多播（Multicast）也称为组播，D类的IP地址就属于多播地址。



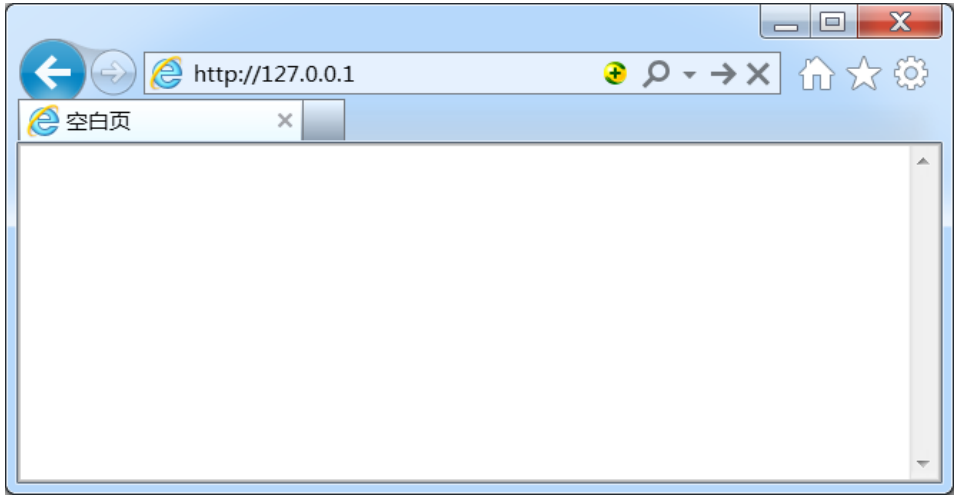
224.0.0.1

224.0.0.6

环回地址

在A类网络中，当网络号部分为127，主机号为任意值时的地址称为环回地址。它主要用于网络软件测试以及本地进程之间的通信。

本地主机



5.保留地址

0.0.0.0

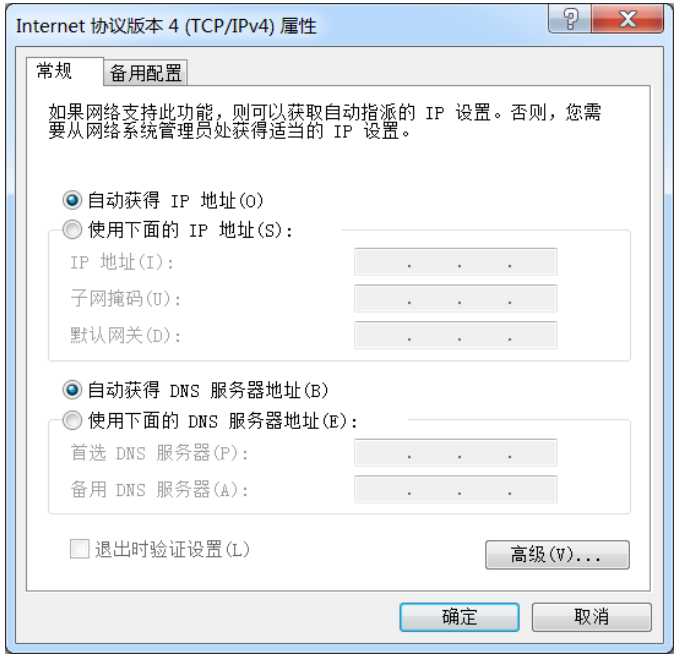
表示所有不清楚的主机和目的网络

```
C:\>route print
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    210.29.228.65    210.29.228.68      20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
      169.254.0.0      255.255.0.0    210.29.228.68    210.29.228.68      20

        224.0.0.0        240.0.0.0    210.29.228.68    210.29.228.68      20
  255.255.255.255  255.255.255.255    210.29.228.68    210.29.228.68       1
Default Gateway:      210.29.228.65
```

169.254.*.*

使用DHCP无法自动获取地址时，系统自动分配这个网段的地址



子网划分

网络基础

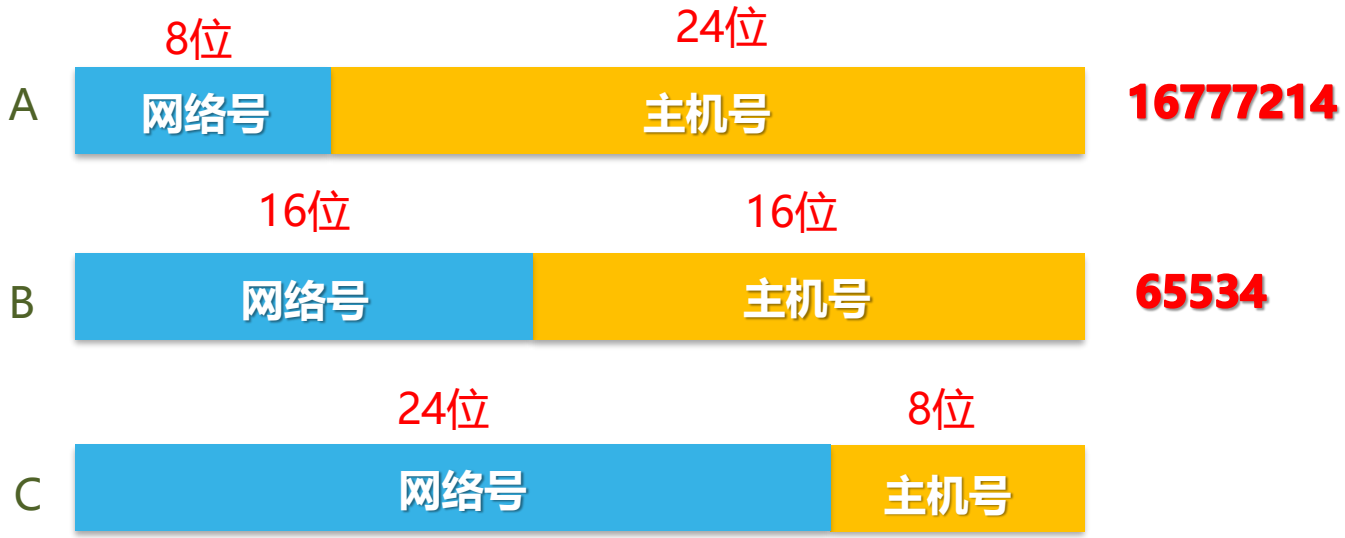
目录
Contents

学习目标

- 了解子网划分的原因
- 掌握子网划分的方法

1.为什么要划分子网

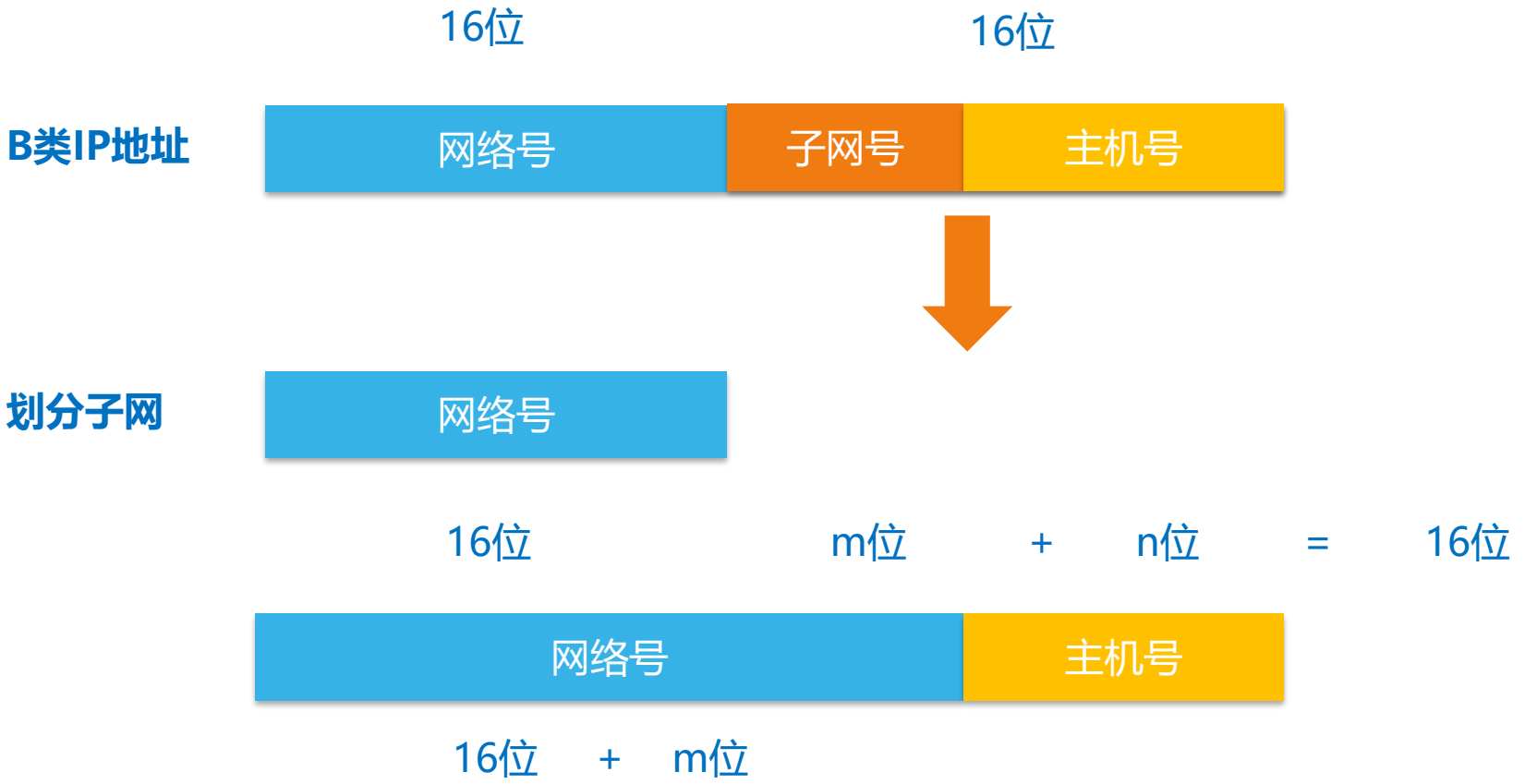
1 ABC三类网络中主机数



2 子网划分原因

2.子网划分的方法

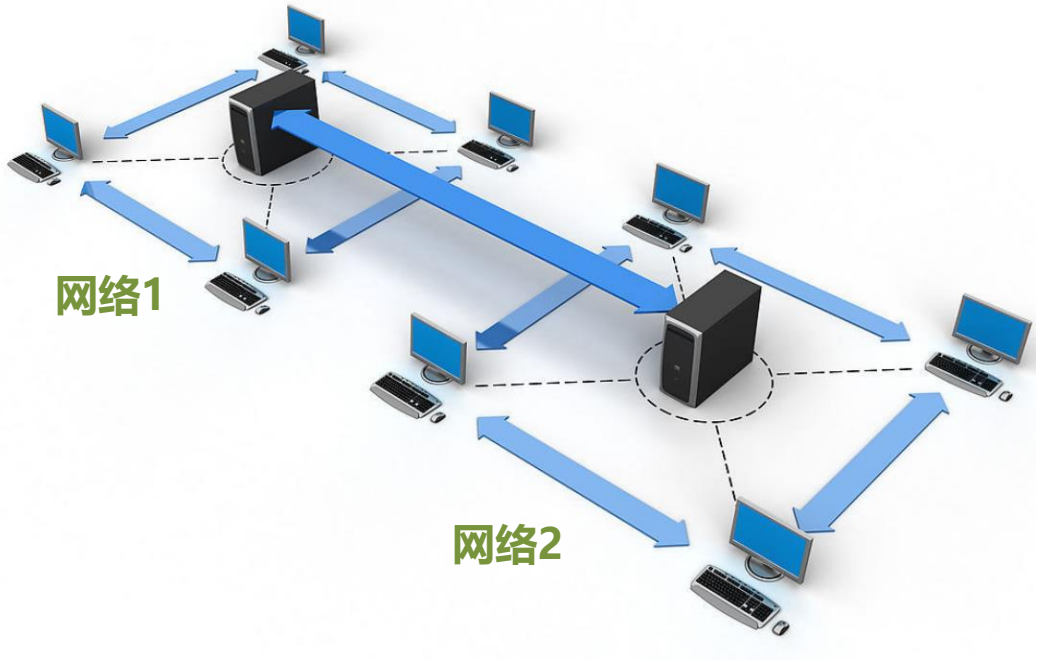
借位：从主机最高位开始借位变为新的子网位，剩余部分仍为主机位，使IP地址的格式变为：



2.子网划分的方法

1 按照网络数量划分

公式: $2^n \geq N$　　N代表网络数量　n代表子网位数



举例：原有网络号192.168.1.0/24，划分成2个网络

$2^n \geq 2$ ➡ n=1

11000000	10101000	00000001	00000000

192.168.1.	00000000

192.168.1.0/25

网络1

192.168.1.	10000000

192.168.1.128/25

网络2

2 按照主机数量划分

公式: $2^n-2\geq N$　　N代表主机数量　n代表主机所占位数　　-2是指减掉主机位全0和全1的两种情况

100台主机

举例：原有网络号192.168.1.0/24，其中一个网络包含100台主机

$2^n-2\geq 100$ ➡ n=7

11000000 10101000 00000001 00000000

192.168.1. 00000000

192.168.1.0/25

192.168.1. 10000000

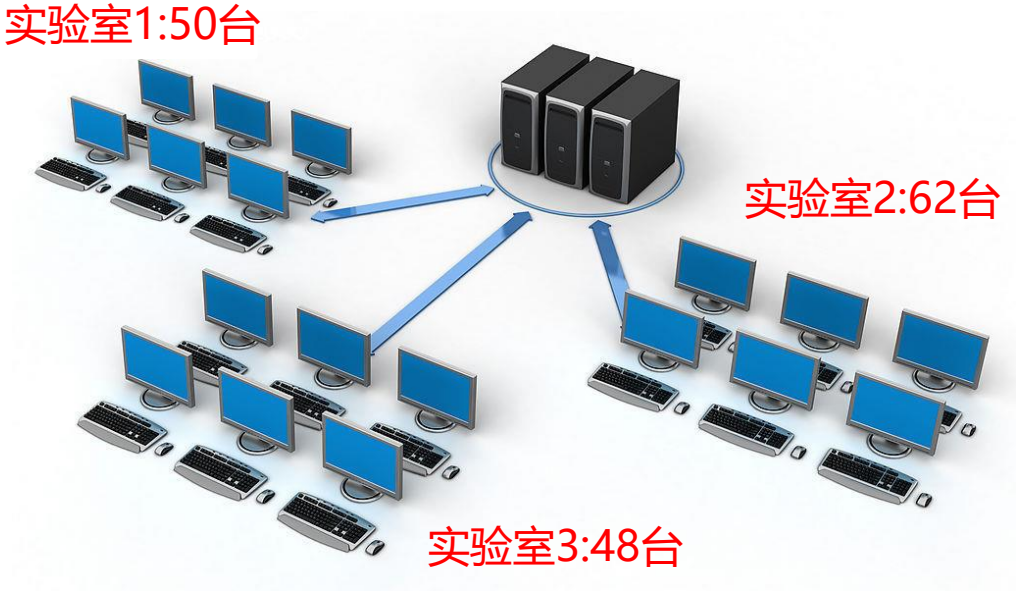
192.168.1.128/25

等长掩码子网划分举例

网络基础

等长掩码子网划分举例

举例：假设一个学校的计算机系，新建了三个实验室，主机数量分别是62台、48台、50台。现给一C类网络地址192.168.1.0/24，请将其进行子网划分，分配给这三个实验室使用



1 按照网络数量划分

$2^n \geq 3$ ➡ n=2

192.168.1.	00000000	192.168.1.0/26	实验室1
192.168.1.	01000000	192.168.1.64/26	实验室2
192.168.1.	10000000	192.168.1.128/26	实验室3
192.168.1.	11000000	192.168.1.192/26	

2 按照主机数量划分

$2^n-2 \geq 62$ ➡ n=6

192.168.1.	00000000

VLSM与CIDR的应用

网络基础

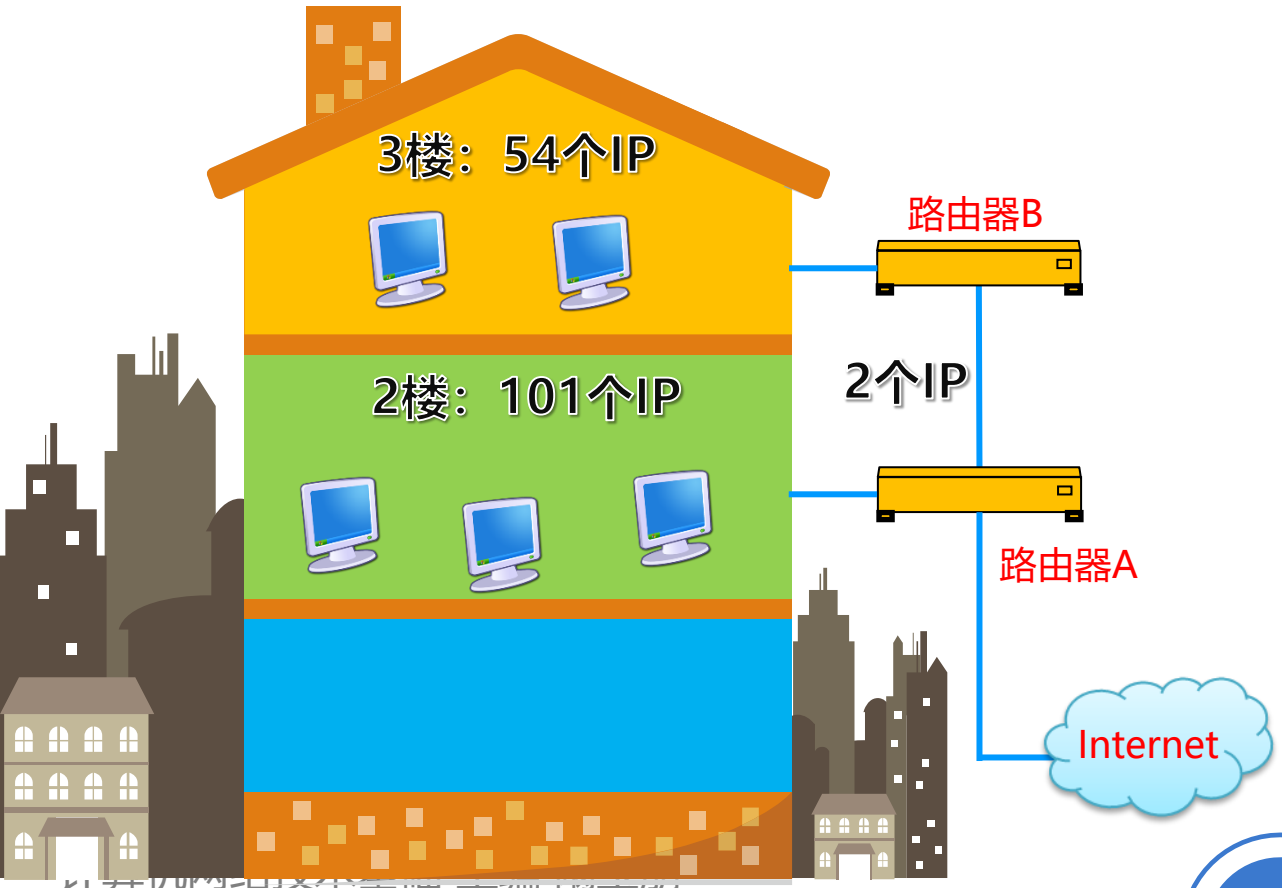
目录
Contents

学习目标

- 掌握VLSM子网划分方法
- 了解CIDR的计算方法

1. VLSM子网划分方法

可变长子网掩码（VLSM）：各子网主机规模不一致的情况，允许在同一网络范围内使用不同长度子网掩码。



例 192.168.1.0/24

1.按照2楼主机数划分

$2^n-2 \geq 101$ ➡ $n=7$ 2楼使用

192.168.1.	1000000	其他网络使用

2.按照3楼主机数划分

192.168.1.0/25

$2^n-2 \geq 54$ ➡ $n=6$ 3楼使用

192.168.1.128/25

192.168.1.	1100000	其他网络使用

3.为路由器之间网络划分

192.168.1.128/26

$2^n-2 \geq 2$ ➡ $n=2$ 路由器之间使用

192.168.1.192/26

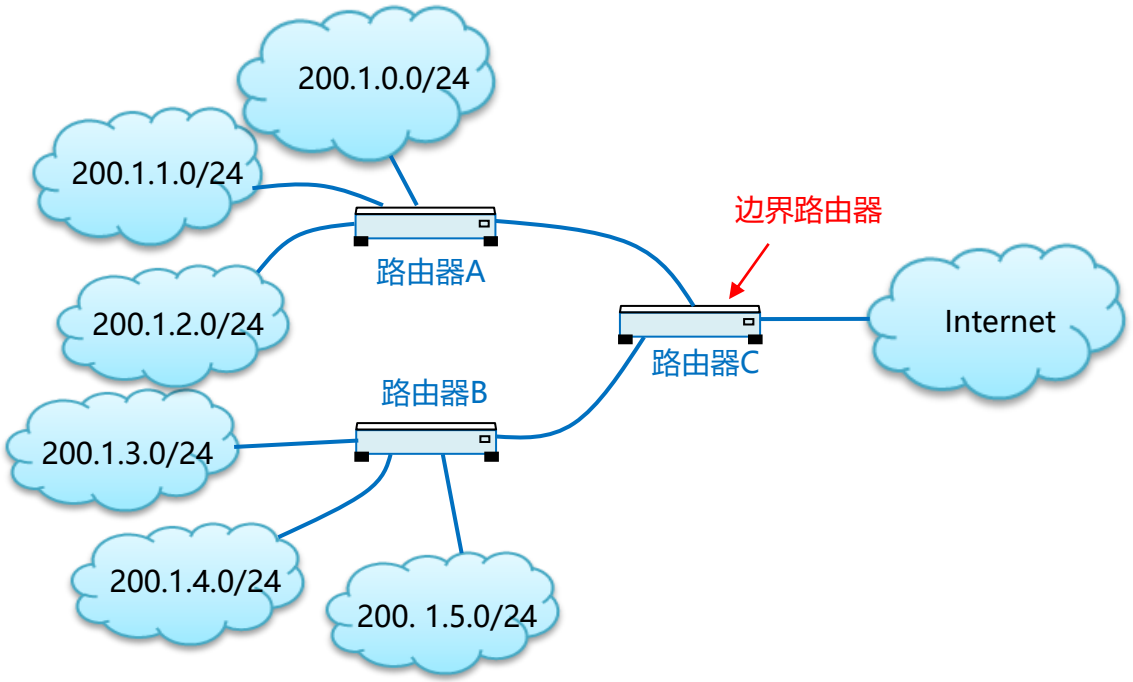
192.168.1.	11000000

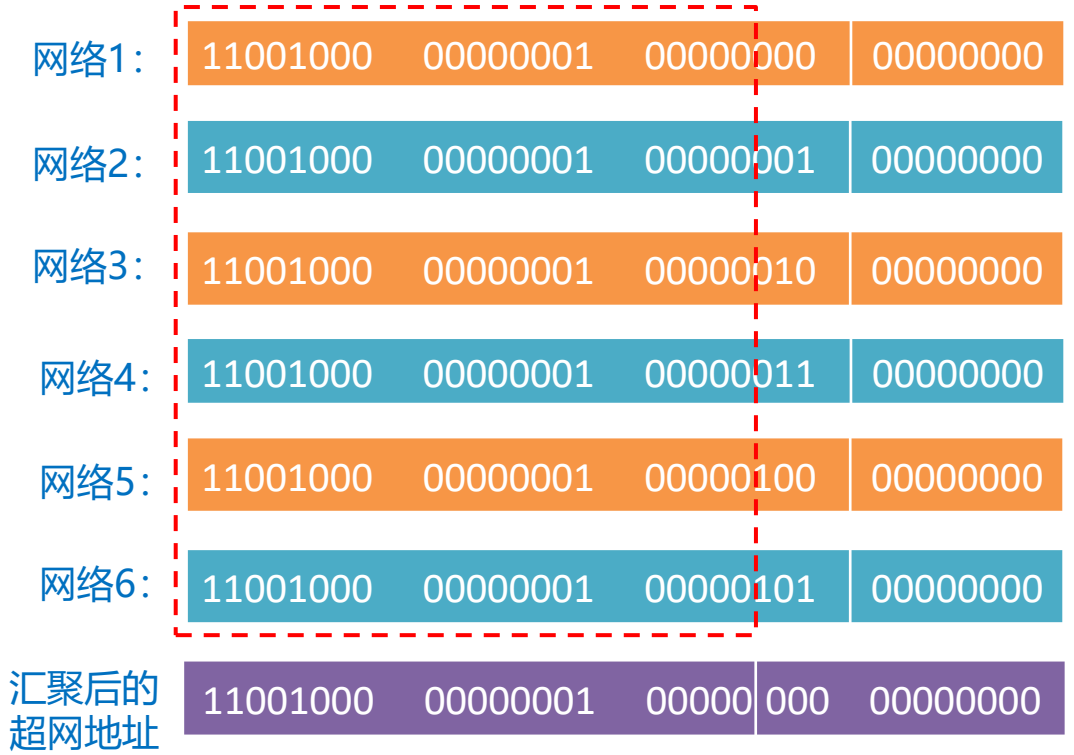
192.168.1.192/30

2. CIDR路由聚合方法

无类域间路由（CIDR）：

由于使用了VLSM无形中增加了路由条目，降低了通信效率，因此利用CIDR可以将若干个较小的网络合并成一个较大的网络





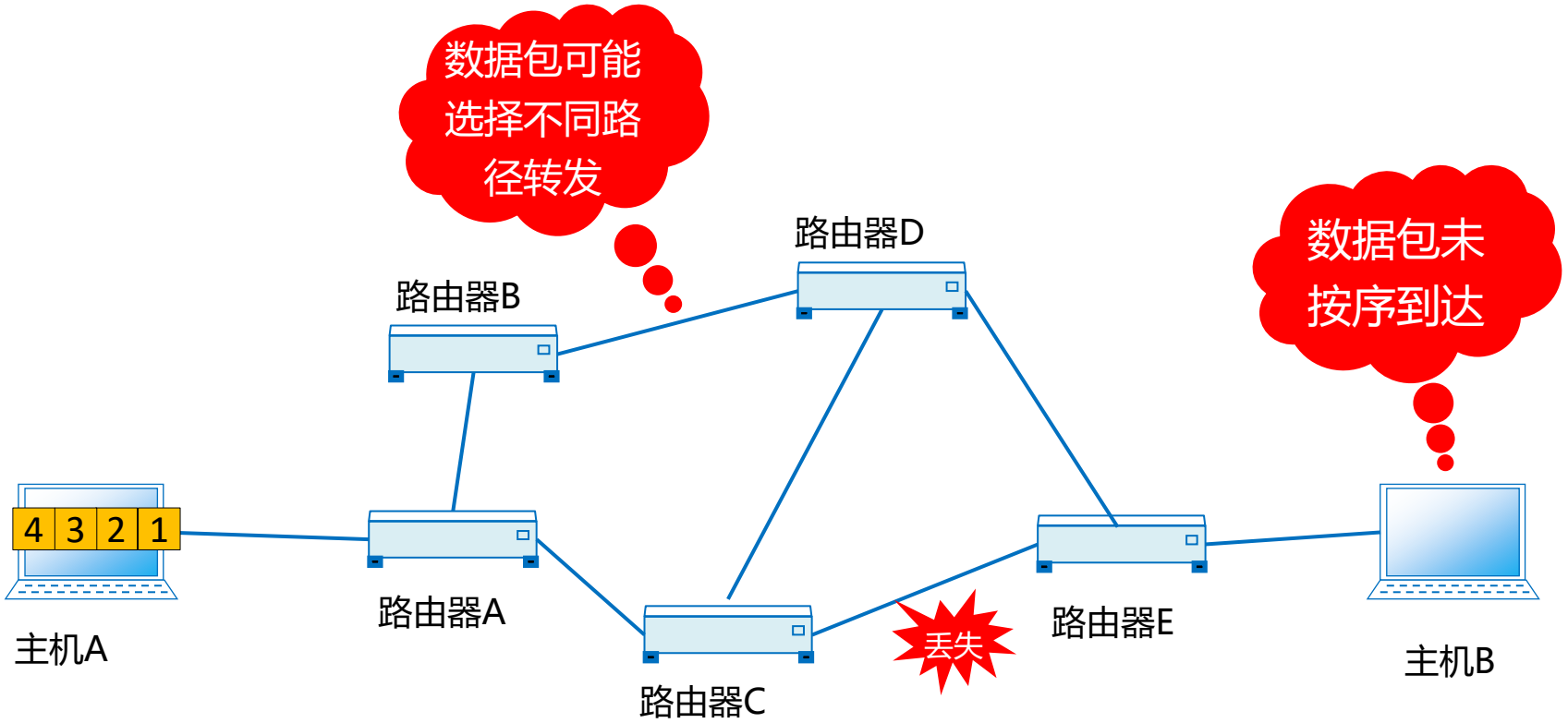
200.1.0.0/21

IP协议特点

网络基础

IP协议特点

IP协议是TCP / IP网际层的核心协议，也是整个TCP / IP模型中的核心协议之一。



1 面向无连接的传输服务

2 不可靠的数据投递服务

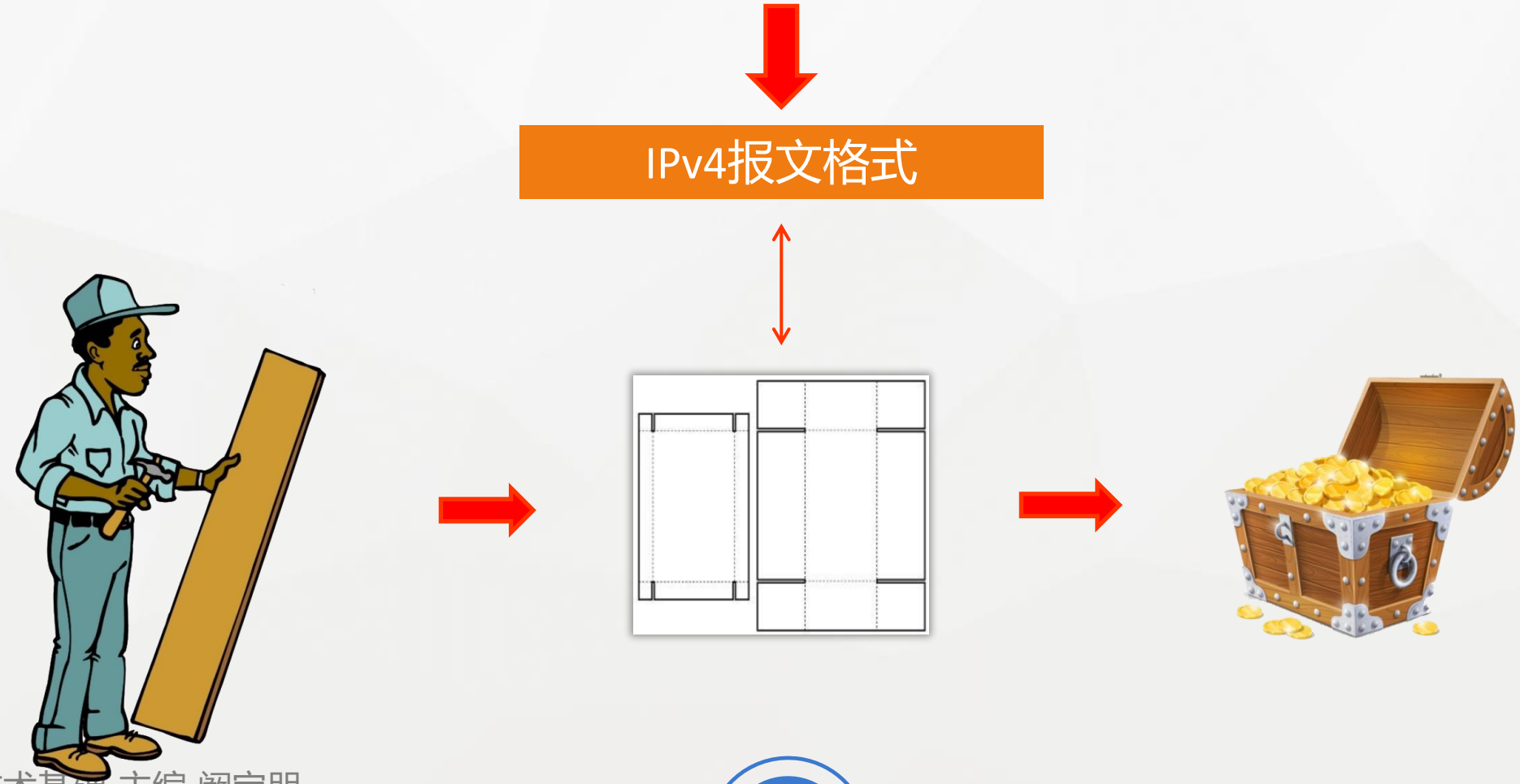
3 尽最大努力投递服务

IPv4报文格式

网络基础

IPv4报文格式

01000100010101010101001001001000110.....



目录
Contents

学习目标

- 理解IP报文格式
- 理解IP报文各字段含义

1. IPv4报文格式

IP报文格式

1. IPv4报文格式

IP报文格式

1 版本（version）

表示该数据报所使用的IP协议版本号

0100 ➡ IPv4

0110 ➡ IPv6

1. IPv4报文格式

IP报文格式

2 头长度（IHL）

指明“报头区”的长度

单位是32bits

如： 0111 → 7

报头区长度为：

7*32bits=224bits=28Bytes

1. IPv4报文格式

IP报文格式

3 服务类型（TOS）

区分不同的服务种类，对传输速度及可靠性等方面加以控制

- 优先级
- 可靠性
- 吞吐量
- 延迟

IP报文格式

4 总长度（Total Length）

定义了报文总长，包含首部和数据，单位为字节。

20~65,535

IP报文格式

5 标识符（Identification）

让目标主机确定一个新到达的分段属于哪一个数据报。

同一个数据报的所有分段包含相同的Identification值

1. IPv4报文格式

IP报文格式

6 标志位（Flags）

用于控制和识别分片。

0	DF	MF

DF =0 时才允许分片

MF为1 表示后面还有分片

MF为0 表示最后一个分片

1. IPv4报文格式

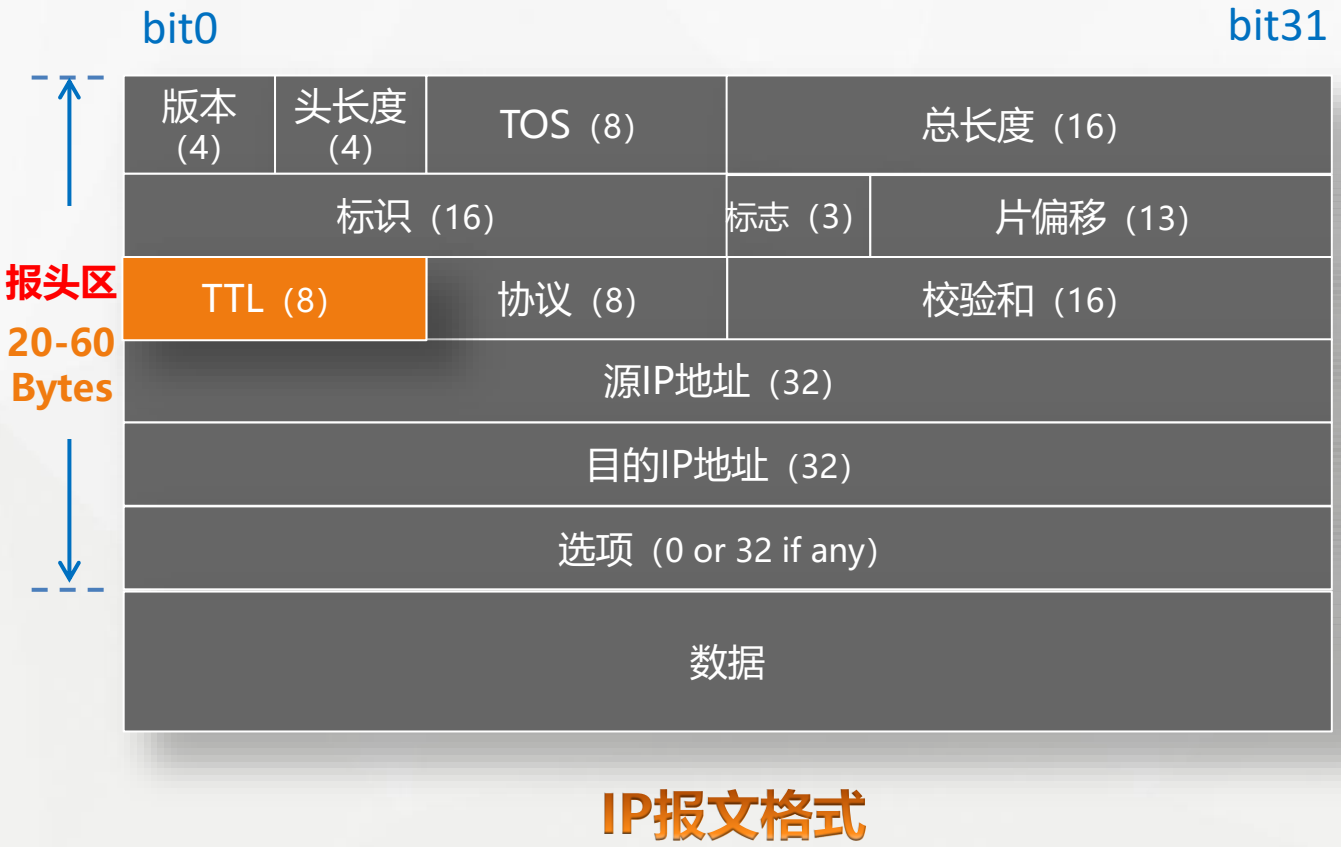
IP报文格式

7 片偏移（Fragment Offset）

指明了每个分片相对于原始报文开头的偏移量，以8字节作单位

分片1	分片2	分片3

1. IPv4报文格式

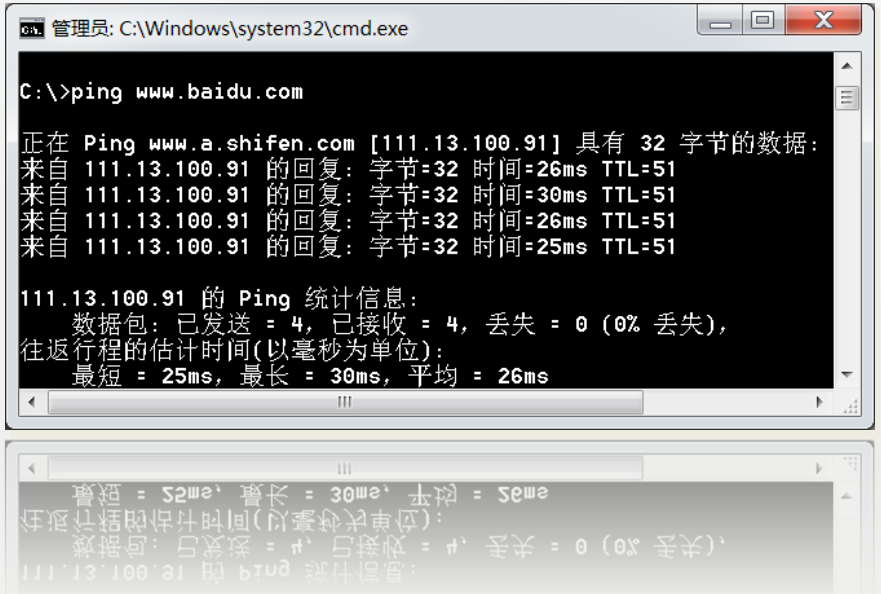


IP报文格式

8 存活时间（TTL）

避免报文在网络中永远存在。

最大的生存期为255秒



1. IPv4报文格式

IP报文格式

9 协议（Protocol）

定义了该报文数据区使用的协议

协议字段值	协议类型
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

1. IPv4报文格式

IP报文格式

10 校验和（Header Checksum）

只检验数据报的首部部分（报头区），不包括数据部分（数据区）

数据区的错误留待上层协议处理

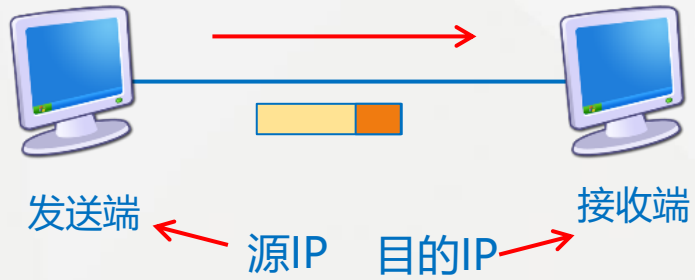
1. IPv4报文格式

IP报文格式

11 源、目的IP地址

源IP地址是报文的发送端的地址，

目的IP地址是报文接收端的地址。



1. IPv4报文格式

IP报文格式

12 源、目的IP地址

选项字段用来支持排错、测量以及安全等措施，内容很丰富。

1. IPv4报文格式

IP报文格式

13 数据（Data）

数据字段内容是上层所封装的完整数据。

3.IPv4报文应用方式

01000100010101010101001001001000110.....

4 4

IPv4 报头长度 4*8=32Byte

IPv4协议抓包体验

网络基础

体验过程
Operating Steps

1 IPv4抓包方法及过程

2 抓包结果分析

学习目标

- 掌握数据包抓包方法
- 掌握IP数据包分析方法

1.IPv4抓包方法及过程

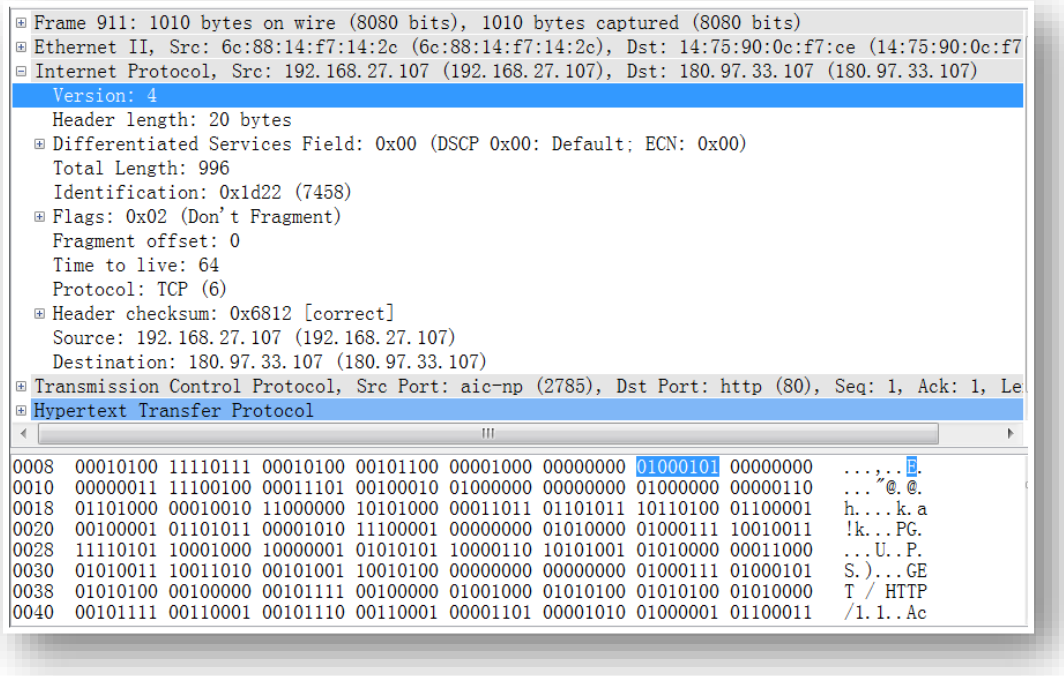
抓包操作过程：

1. 启动Wireshark抓包功能
2. 在浏览器中输入网址
3. 停止抓包
4. 对抓取的数据包进行过滤

2.抓包结果分析

抓包分析内容：

1. 版本、报头长度
2. 标志符、TTL
3. 源目的IP地址
4. 上层协议



什么是路由

网络基础

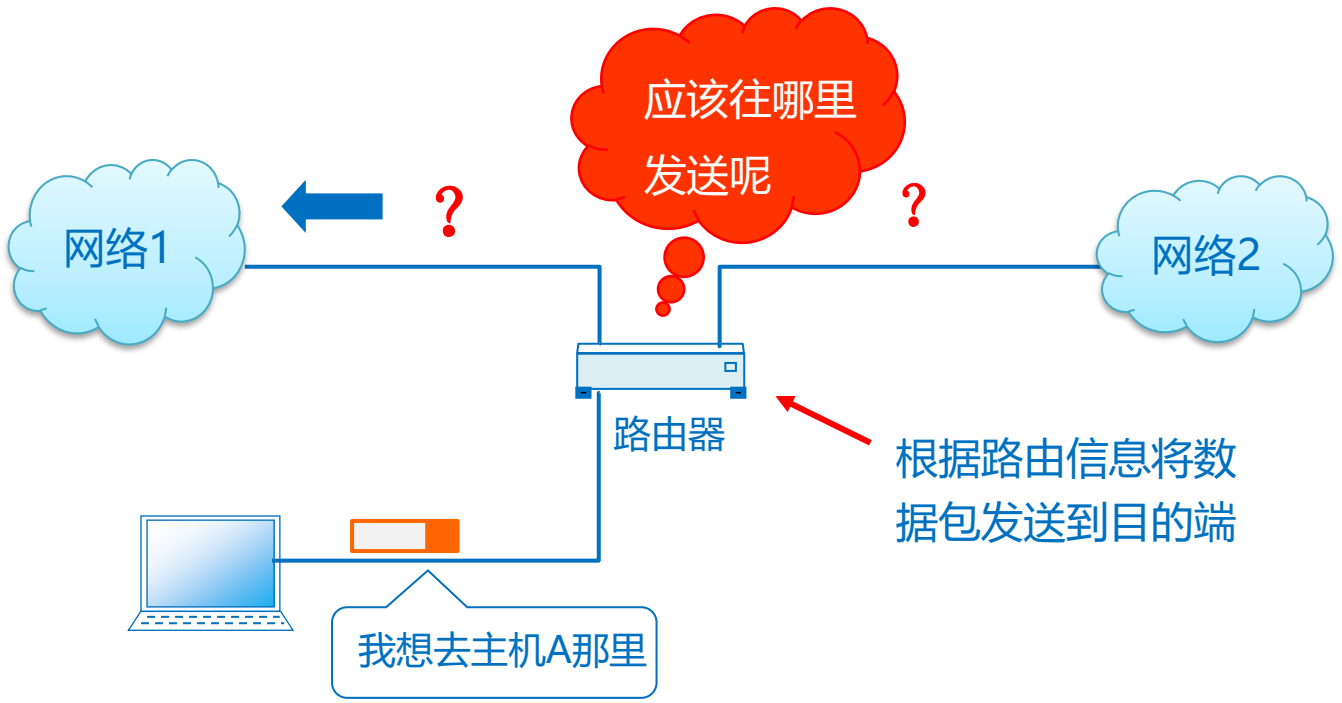
目录
Contents

学习目标

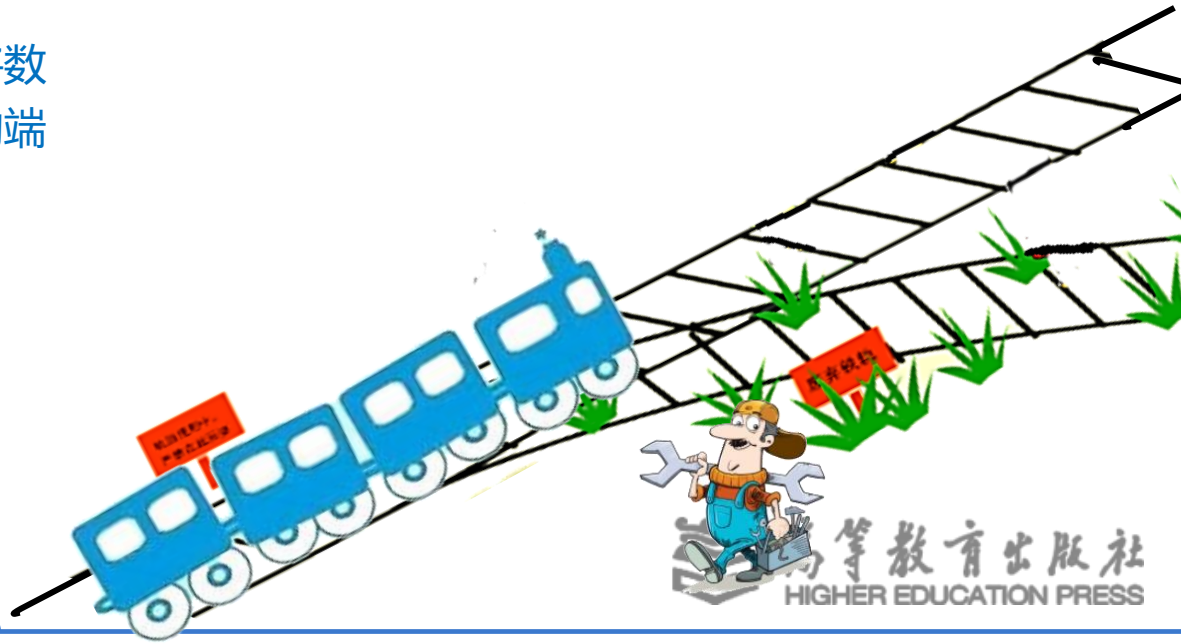
- 了解路由的作用
- 了解路由表中包含的信息
- 理解路由转发方式

1.路由的含义

路由是指数据包转发路径选择的过程。

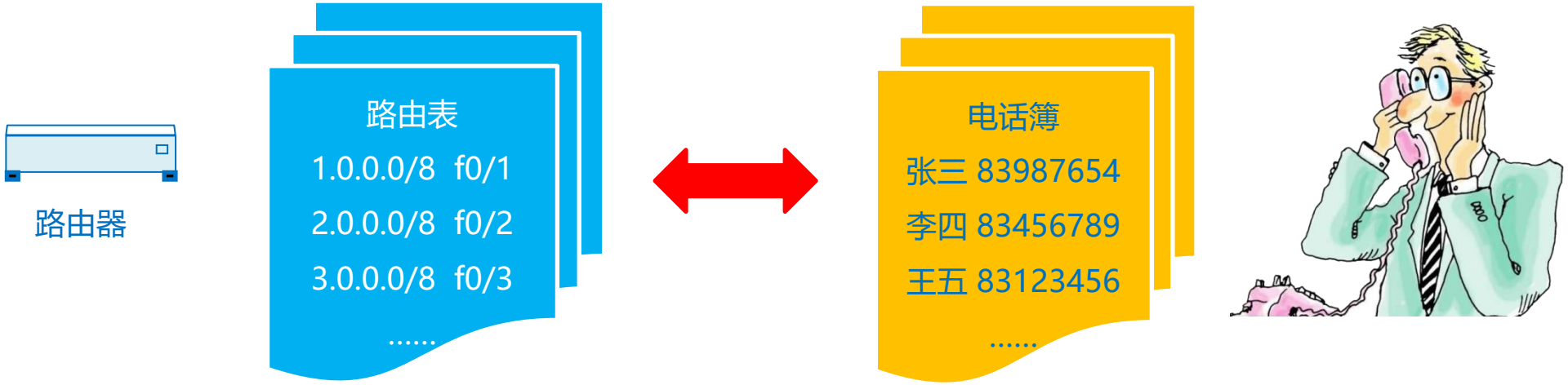


一个数据包之所以能够到达目标地址，全靠路由控制，它主要根据数据包中的目的IP地址进行寻址。



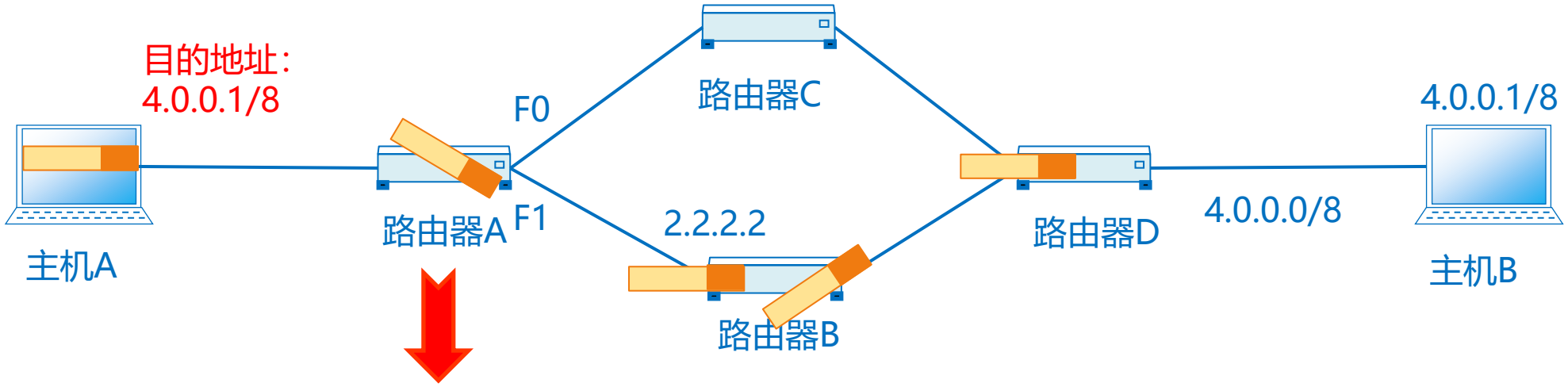
2.路由表的作用

路由表是指路由器将所有关于如何到达目标网络的最佳路径信息以数据库表的形式存储起来的表



R 4.0.0.0/8 [120/1] via 2.2.2.2, 00:00:16, F1

2.路由转发的过程



R 4.0.0.0/8 [120/1] via 2.2.2.2, 00:00:16, F1

表示路由的来源　目的网络号　表示管理距离和度量值　下一站要发往哪里　从哪个接口发出去

路由协议及分类

网络基础

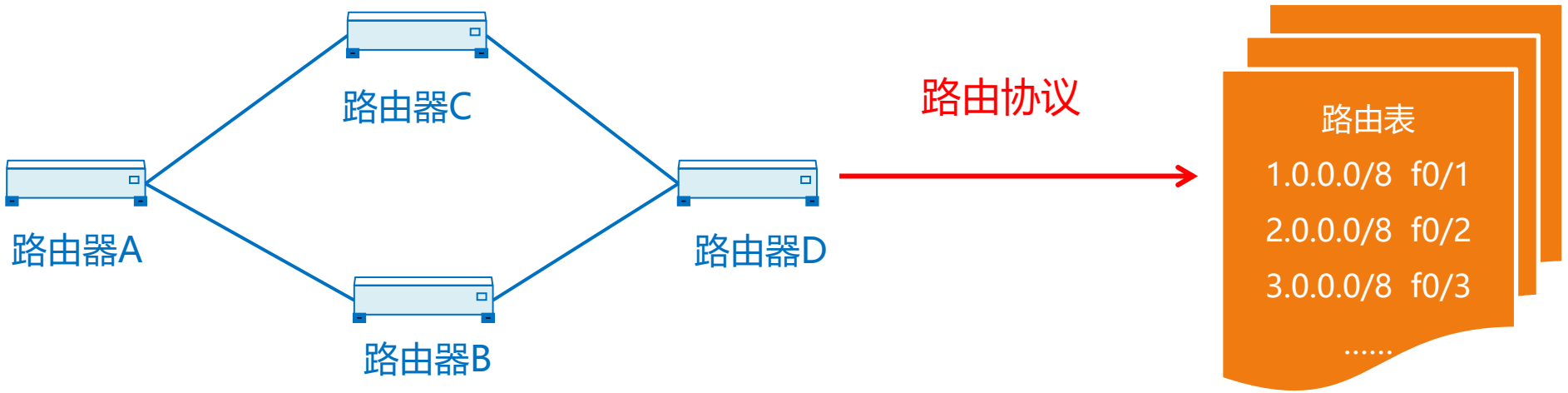
目录
Contents

学习目标

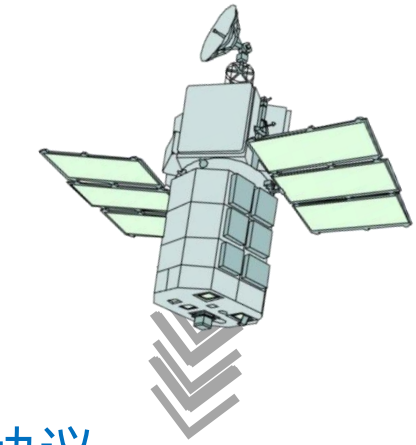
- 了解路由协议的作用
- 了解路由协议的分类
- 了解路由协议的工作方式

1.什么是路由协议

路由协议是在路由指导IP数据包发送过程中事先约定好的规定和标准。它通过在路由器之间共享路由信息来支持可路由协议创建了路由表，描述了网络拓扑结构。



2.路由协议分类



静态路由协议

手工添加到路由器上的，有多少个网络就需要添加多少路由信息条目。

动态路由协议

路由器之间通过交换路由信息，负责建立、维护动态路由表，并计算最佳路径的协议。

静态路由协议

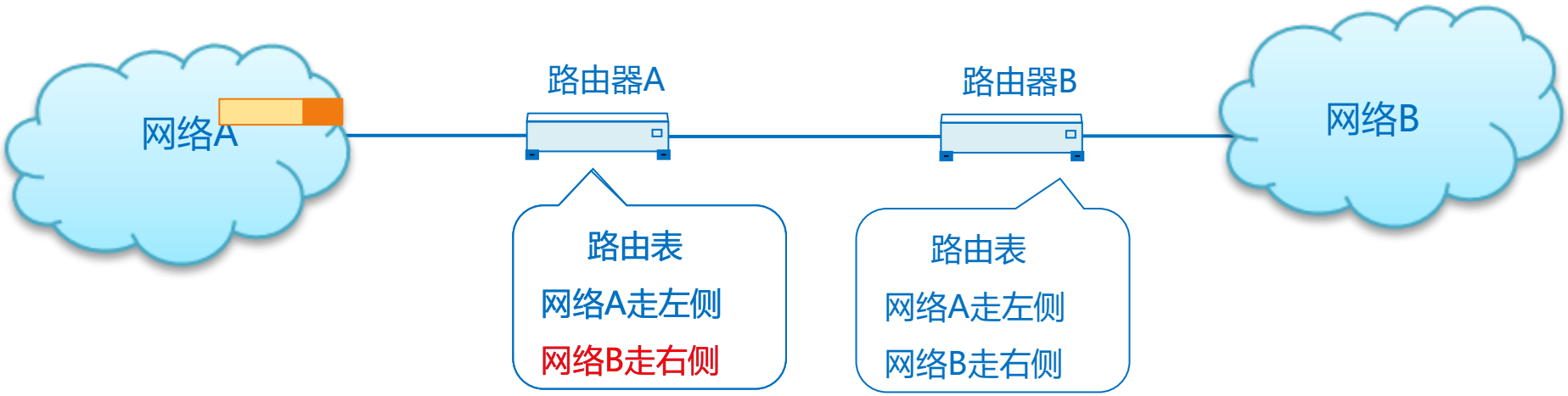
动态路由协议

2.路由协议分类

静态路由协议

手工添加到路由器上的，有多少个网络就需要添加多少路由信息条目。

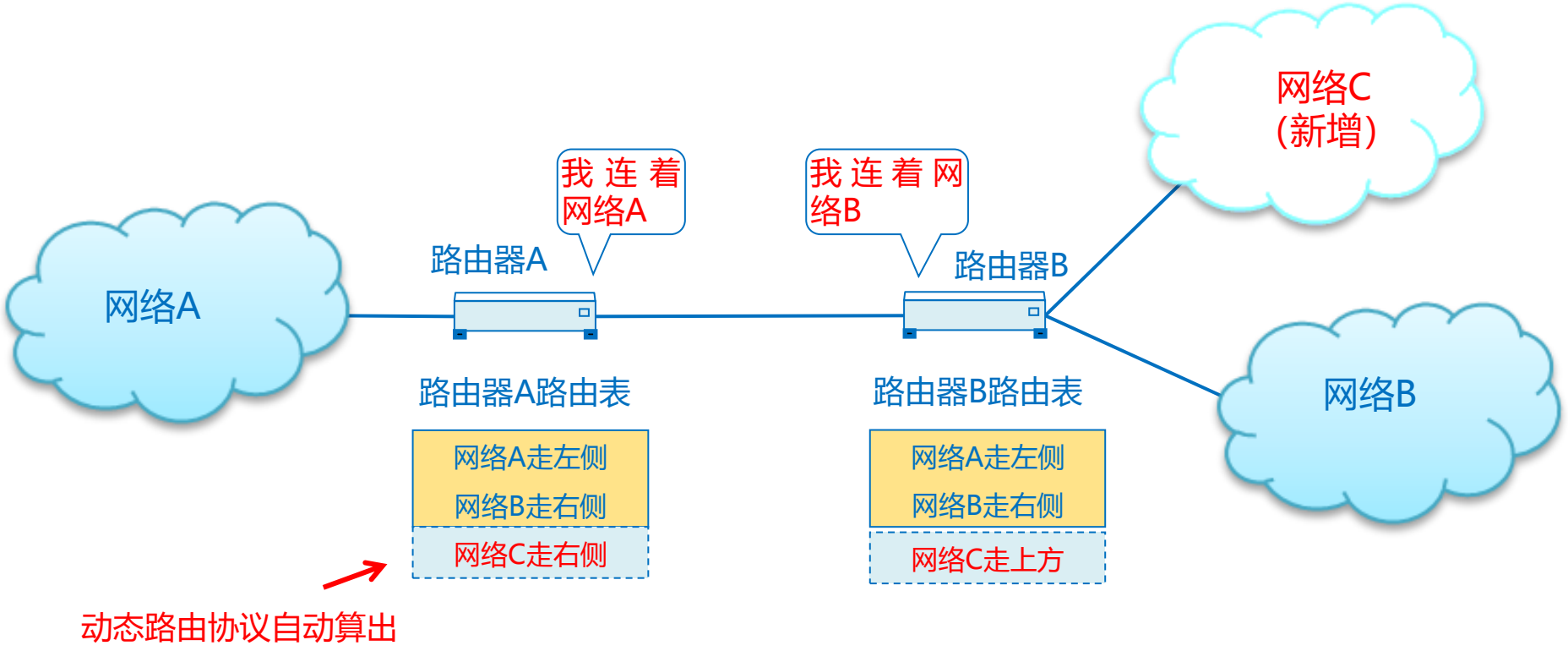
根据手动设定路由信息进行数据转发



2.路由协议分类

动态路由协议

路由器之间通过交换路由信息，负责建立、维护动态路由表，并计算最佳路径的协议。



3.动态路由协议的分类

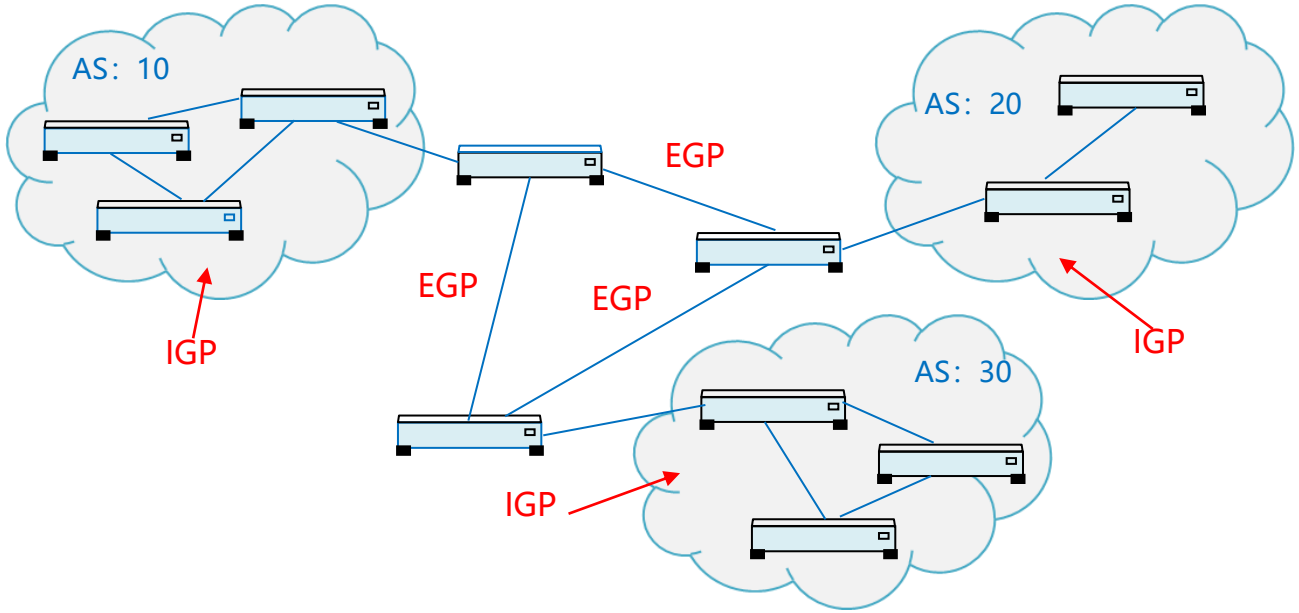
动态路由协议

路由器之间通过交换路由信息，负责建立、维护动态路由表，并计算最佳路径的协议。

应用的区域：

外部网关协议EGP

内部网关协议IGP



3.动态路由协议的分类

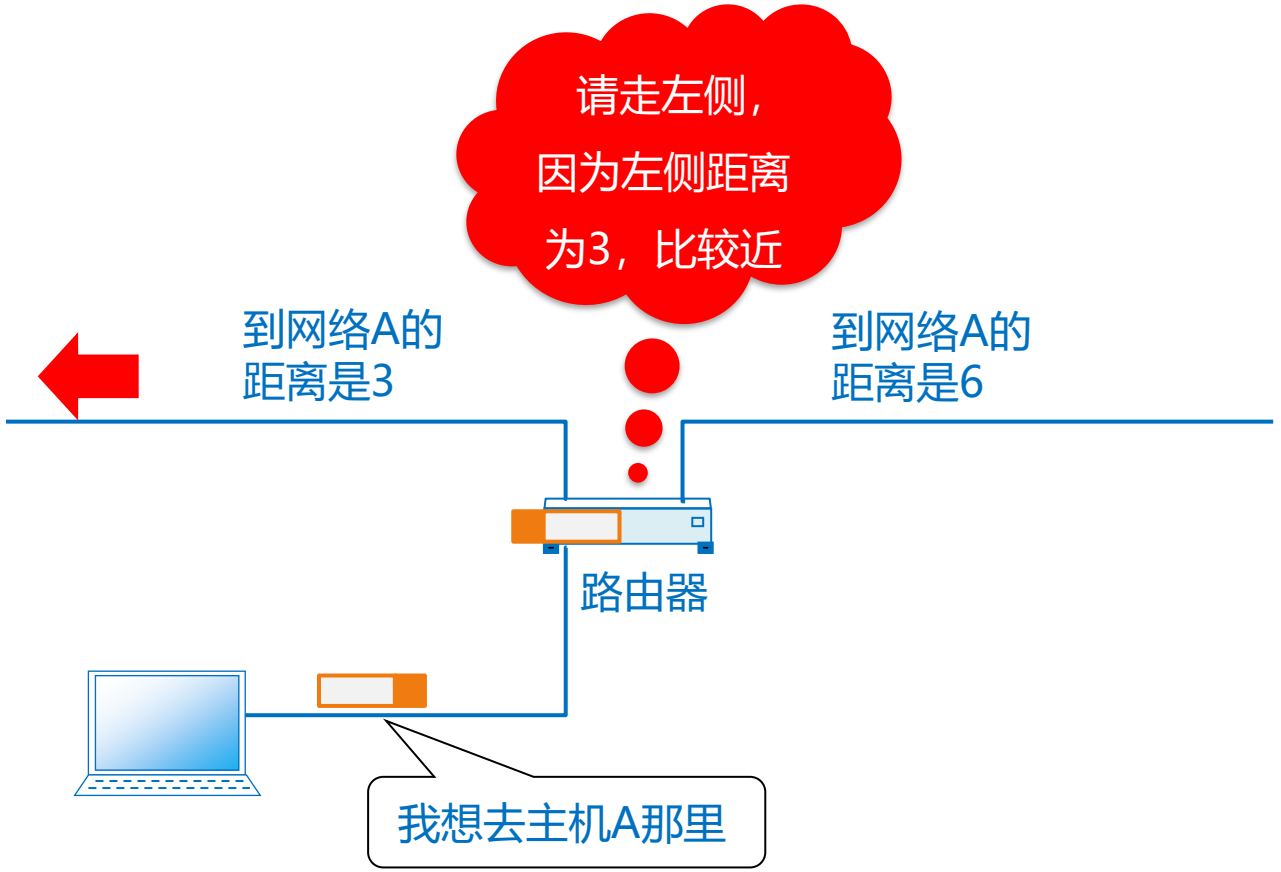
动态路由协议

路由器之间通过交换路由信息，负责建立、维护动态路由表，并计算最佳路径的协议。

按照使用的算法：

距离矢量路由协议

链路状态路由协议



3.动态路由协议的分类

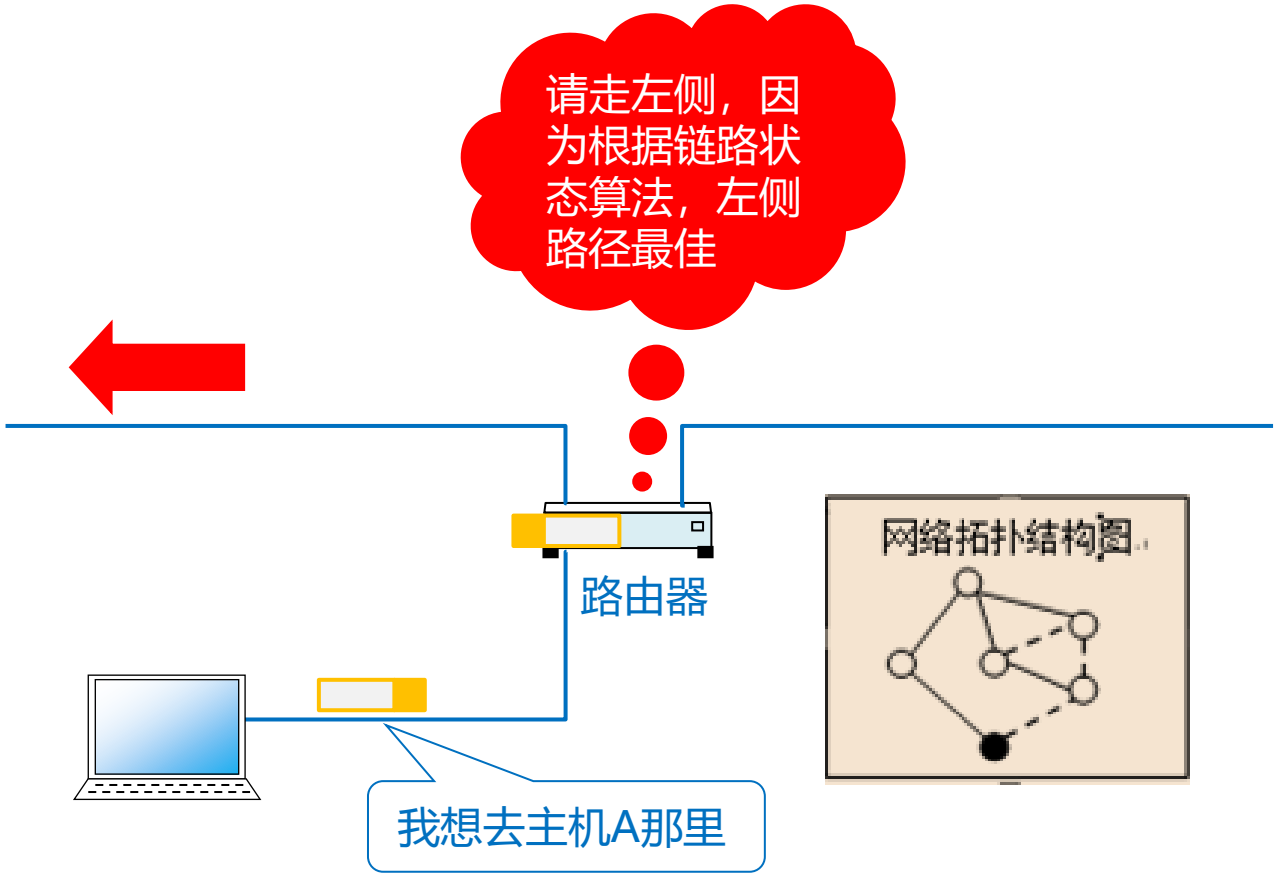
动态路由协议

路由器之间通过交换路由信息，负责建立、维护动态路由表，并计算最佳路径的协议。

按照使用的算法：

距离矢量路由协议

链路状态路由协议



3.路由协议分类

路由协议分很多种，每种都有自己的特点及适合使用的网络。

协议名称	使用的下层协议	类型	适用范围
RIP	UDP	距离矢量路由协议	域内
OSPF	IP	链路状态路由协议	域内
EIGRP	IP	综合了距离矢量和链路状态两种协议	域内
IS-IS	IP	链路状态协议	域内
EGP	IP	距离矢量	对外连接
BGP	TCP	路径矢量	对外连接

主机静态路由配置体验

网络基础

体验过程
Operating Steps

1 主机路由信息

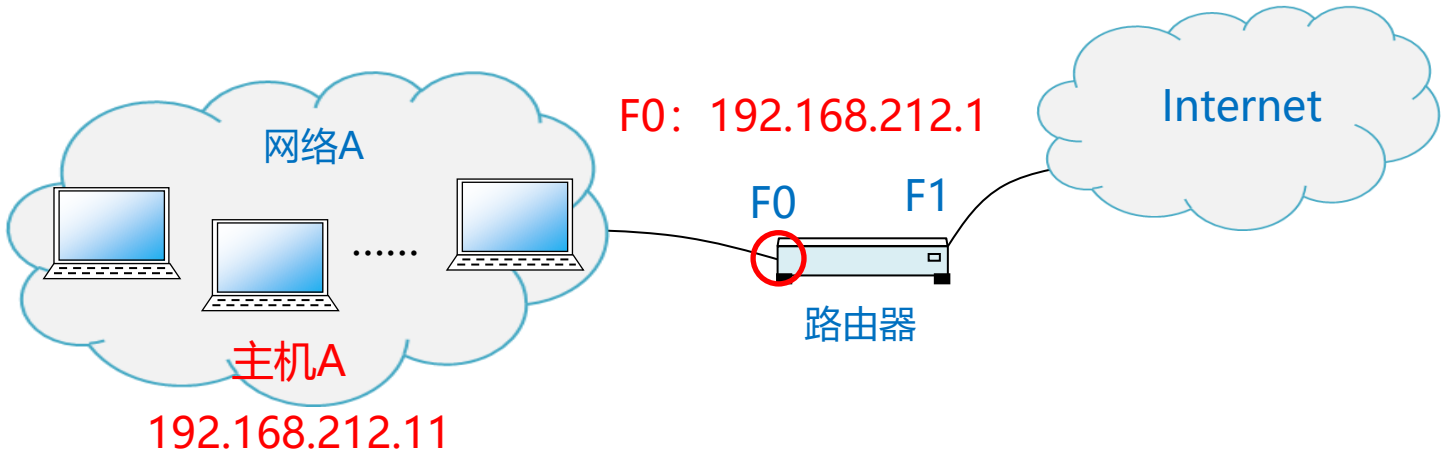
2 主机静态路由配置

学习目标

- 了解主机的路由信息
- 理解静态路由的作用
- 了解主机静态路由配置方法

1.主机路由信息

网关也称为网络的出口，网关的使用实际上是通过一条静态路由来（默认路由）体现的。



route print：

```
C:\>route print
IPv4 路由表
===========================================================================
活动路由:
          网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    192.168.212.1  192.168.212.11     20
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255         在链路上   192.168.212.11    276
===========================================================================
```

Route /?

查看主机静态路由

配置方法

2.主机静态路由配置

配置过程：

1. 删除原有默认路由（0.0.0.0）
2. 测试上网情况
3. 为确定网络添加一条静态路由
4. 添加一条默认路由实现完全联网

动态路由协议举例

网络基础

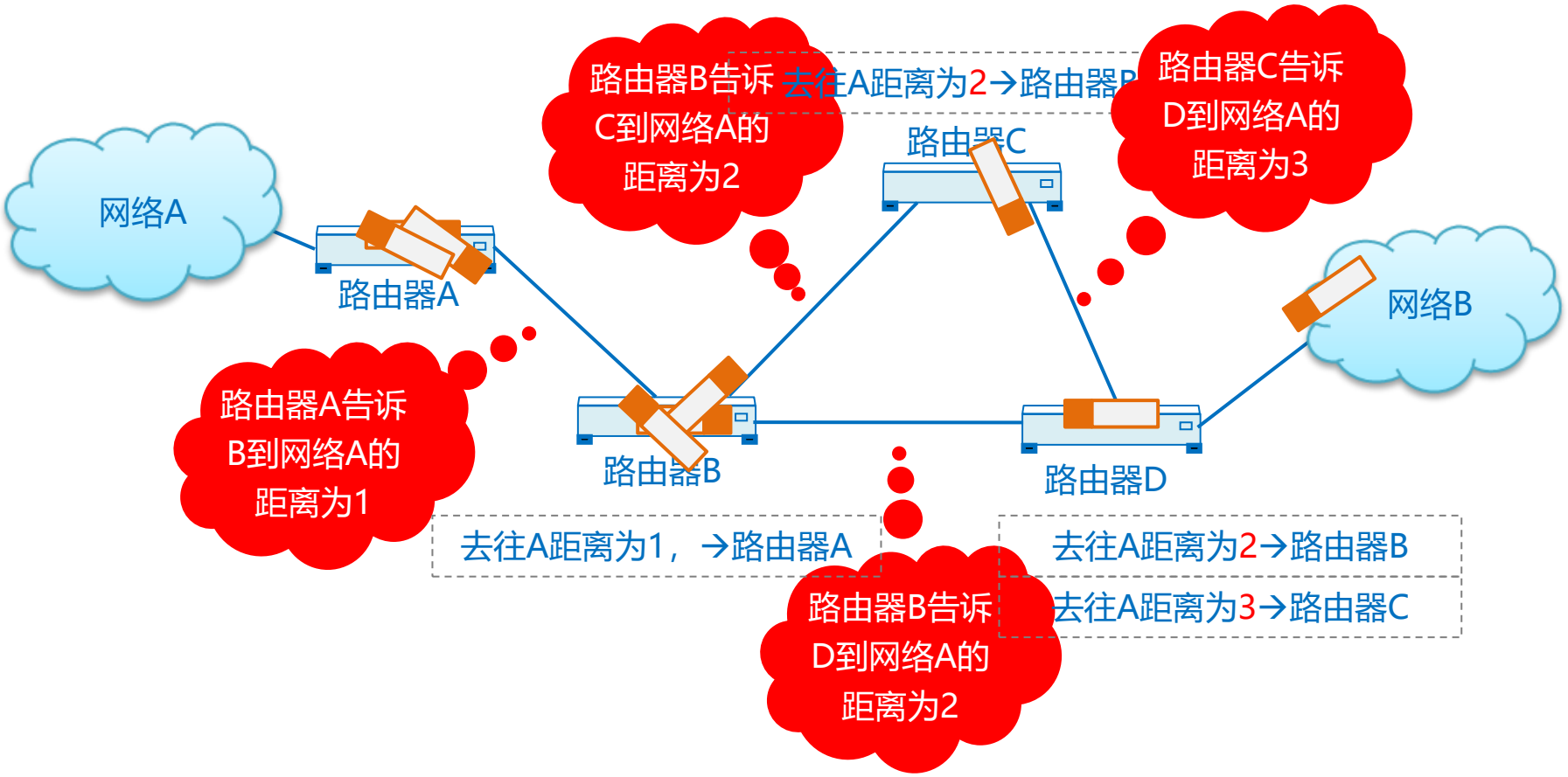
目录
Contents

学习目标

- 了解RIP路有协议工作方式
- 了解OSPF路由协议工作方式

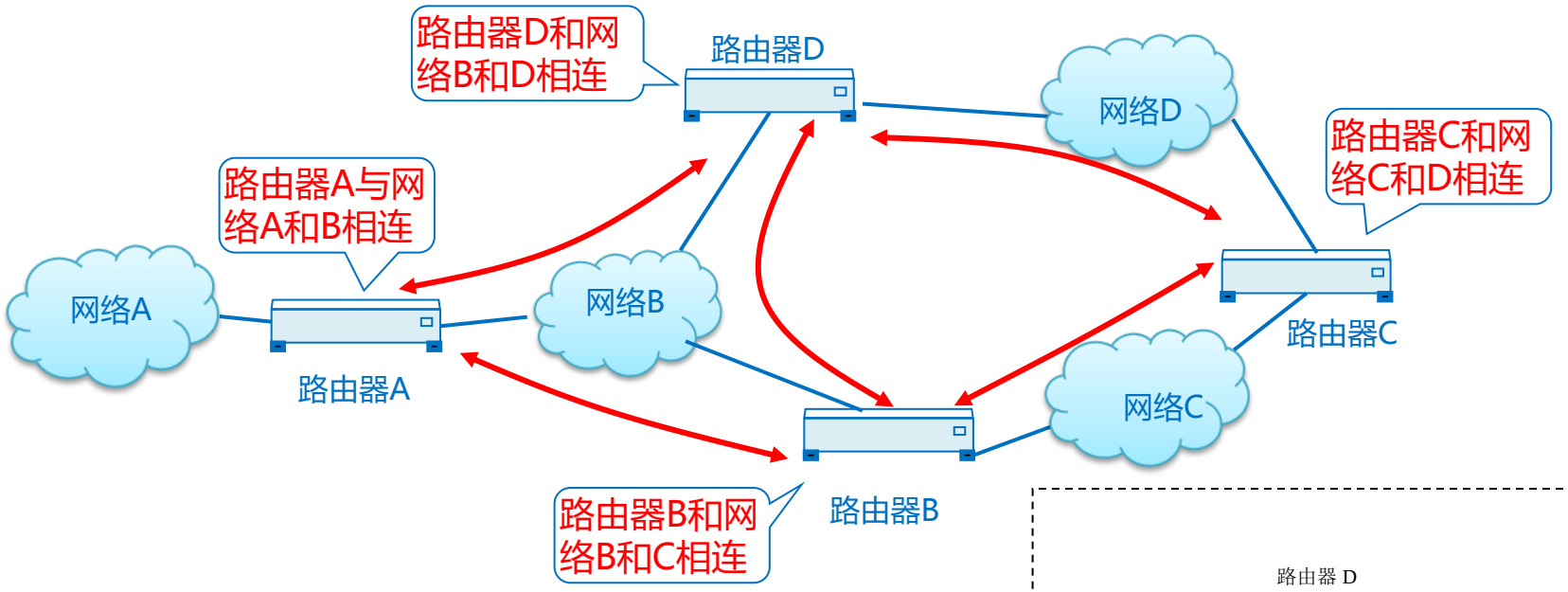
1. RIP路由协议工作方式

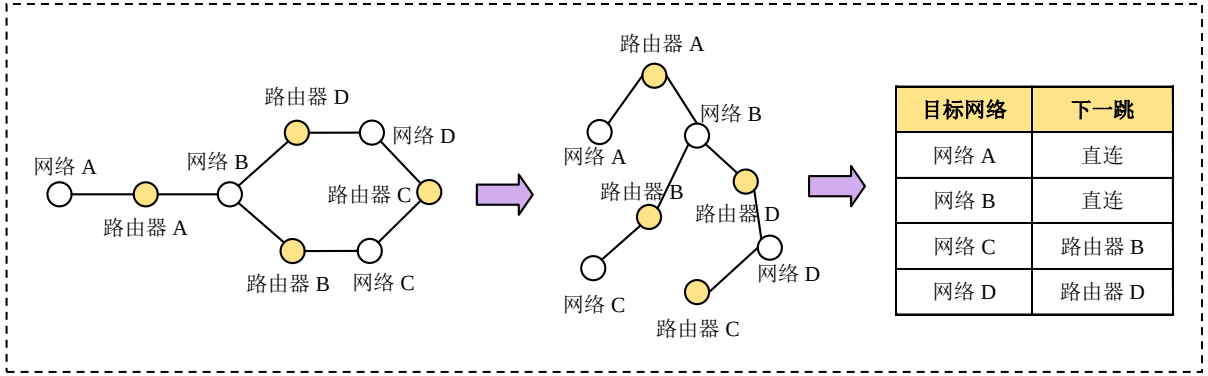
RIP是距离矢量路由协议的一种，它使用跳数作为路径选择的依据。



2. OSPF路由协议工作方式

OSPF是链路状态的路由协议，通过使用SPF算法对收集的链路状态计算出一条到目的网络的最佳路径





目标网络	下一跳
网络 A	直连
网络 B	直连
网络 C	路由器 B
网络 D	路由器 D

MPLS技术

网络基础

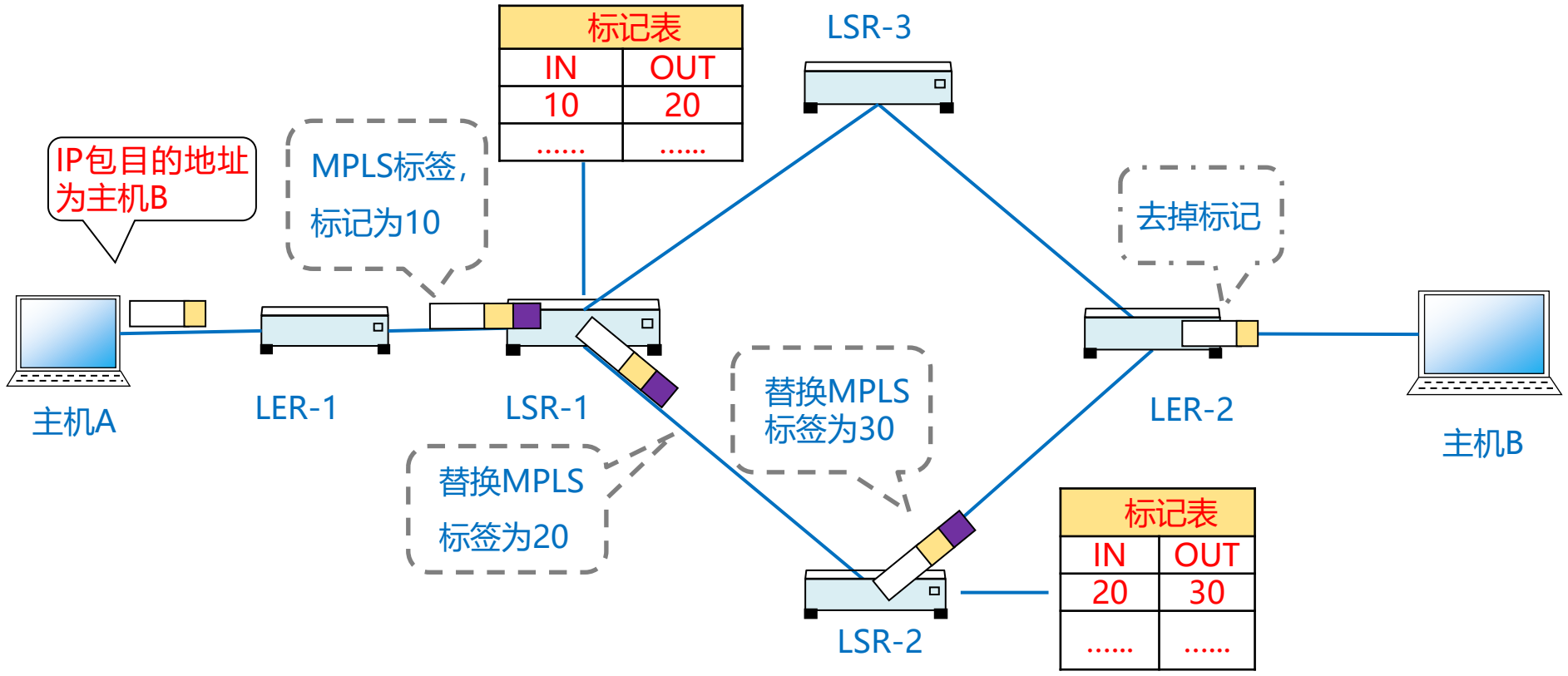
目录
Contents

学习目标

- 了解MPLS技术
- 了解MPLS优势

1.什么是路由协议

MPLS(多协议标记交换技术)是每个IP包都设定一个叫做“标记”的值，然后根据这个“标记”再进行转发。



转发速度快

- 使用固定长度的标记信息，使得处理更加简单，可以通过高速的硬件实现转发。
- MPLS只需要设置必要的几处信息即可，所要处理的数据量也大幅度减少。

标记生成虚拟的路径

- 利用标记生成虚拟的路径，并在它的上面实现IP等数据包的通信
- 提供基于MPLS的通信质量控制、带宽保证和VPN等功能

分片与重组

网络基础

目录
Contents

学习目标

- 了解不通网络MTU的值
- 了解分片的方式

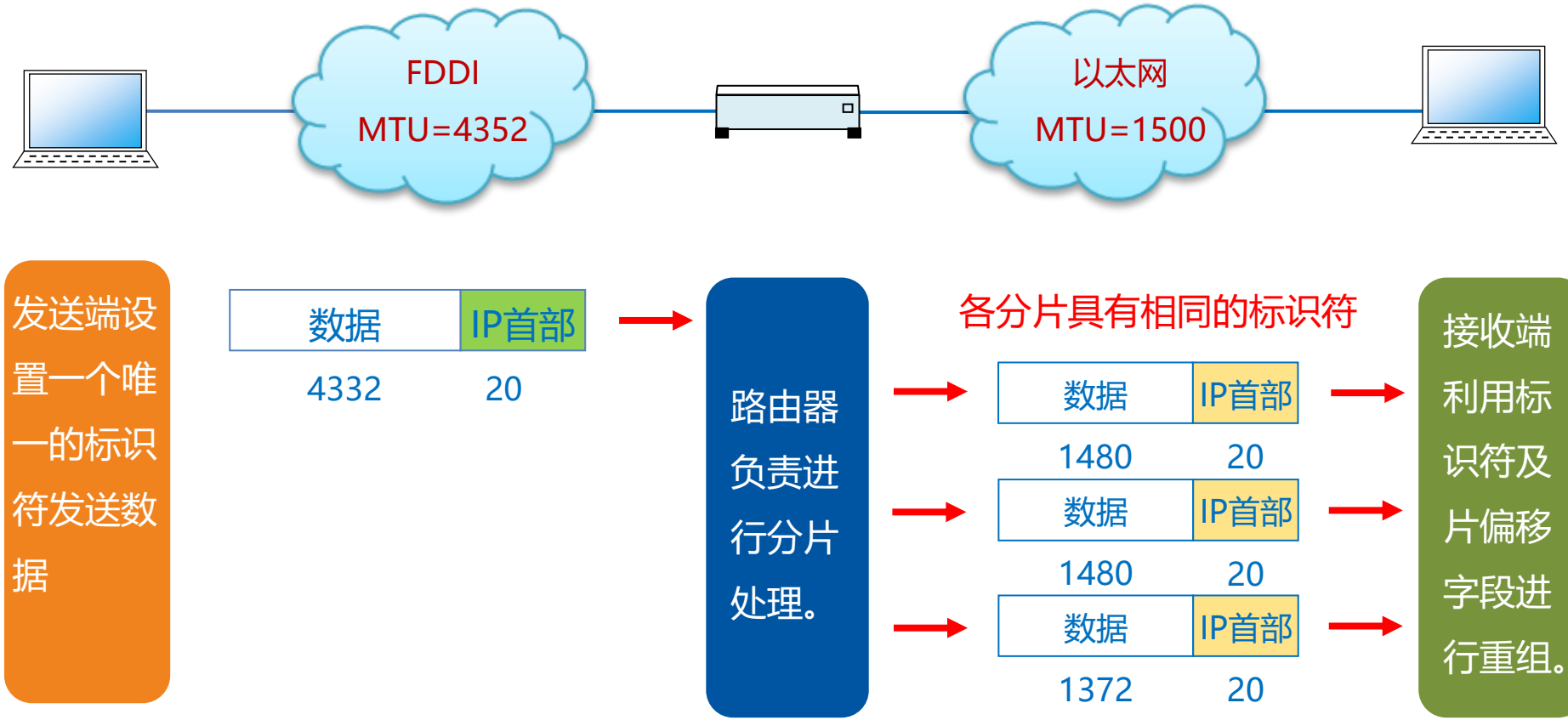
1.最大传输单元MTU

每种网络都规定了一个帧最多能够容纳的数据量，这一限制称为最大传输单元。数据报的总长度一定不能超过下层的数据链路层的MTU值，否则无法传输。

网络类型	MTU（字节）	总长度（字节，含FCS）
IP网络	65535	——
IP over ATM	9180	——
PPP（Default）	1500	——
以太网	1500	1518
IEEE802.4 Token Bus	8166	8191
IEEE802.5 Token Ring	4464	4508
PPPoE	1492	——
FDDI	4352	4500

2.分片方式

网络中不同网络的MTU各不相同，经过转发节点后需要进行分组。

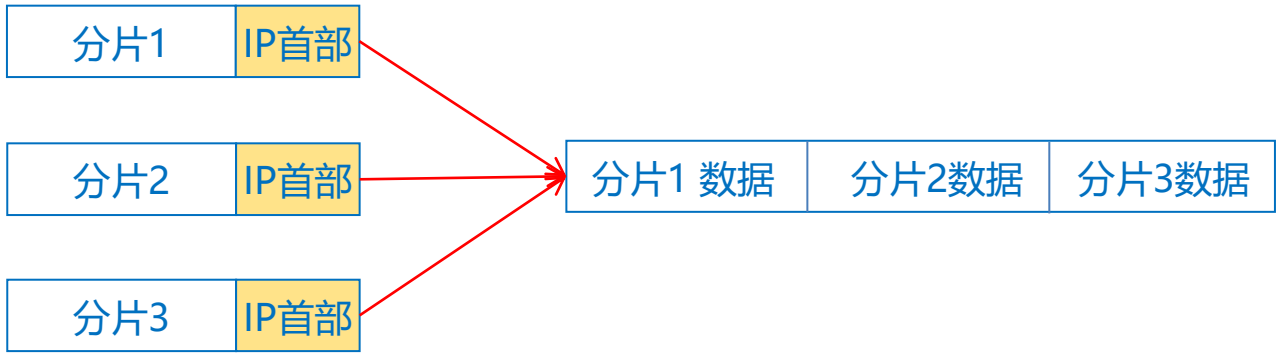


3.各分片重组方式

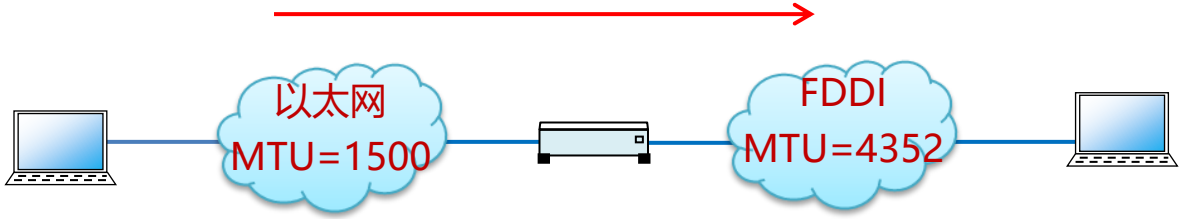
经过分片之后的IP数据报在被重组的时候，只能由目标主机进行，路由器虽然做分片但不会进行重组。

bit0 bit31

版本（4）	头长度（4）	TOS（8）	总长度（16）
标识（16）		标志（3）	片偏移（13）
TTL（8）	协议（8）	校验和（16）	
源IP地址（32）			
目的IP地址（32）			
选项（0 or 32 if any）			
数据			



思考



路径MTU发现技术

网络基础

目录
Contents

学习目标

- 了解不通网络MTU的值
- 了解路径MTU发现机制

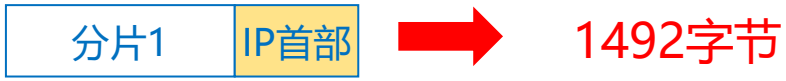
1.什么是路径MTU发现

路径MTU 是指从发送端主机到接收端主机之间不需要分片时最大MTU的大小，即路径中存在的所有数据链路中最小的MTU。

路径MTU出现原因：

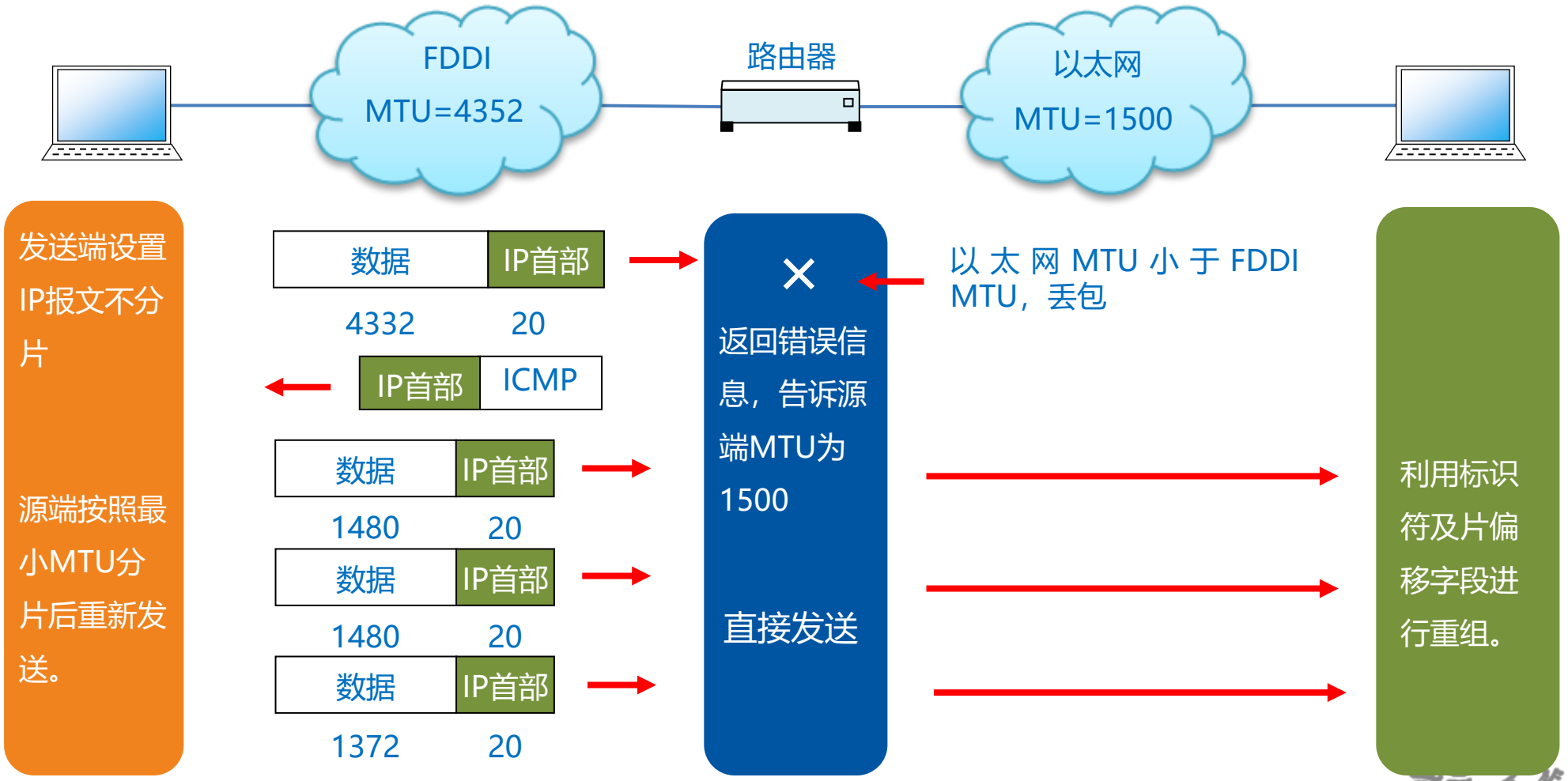
1. 路由器的处理负荷加重
2. 路由器需要处理的很多
3. 分片丢失造成整个IP数据报作废

路径MTU技术：



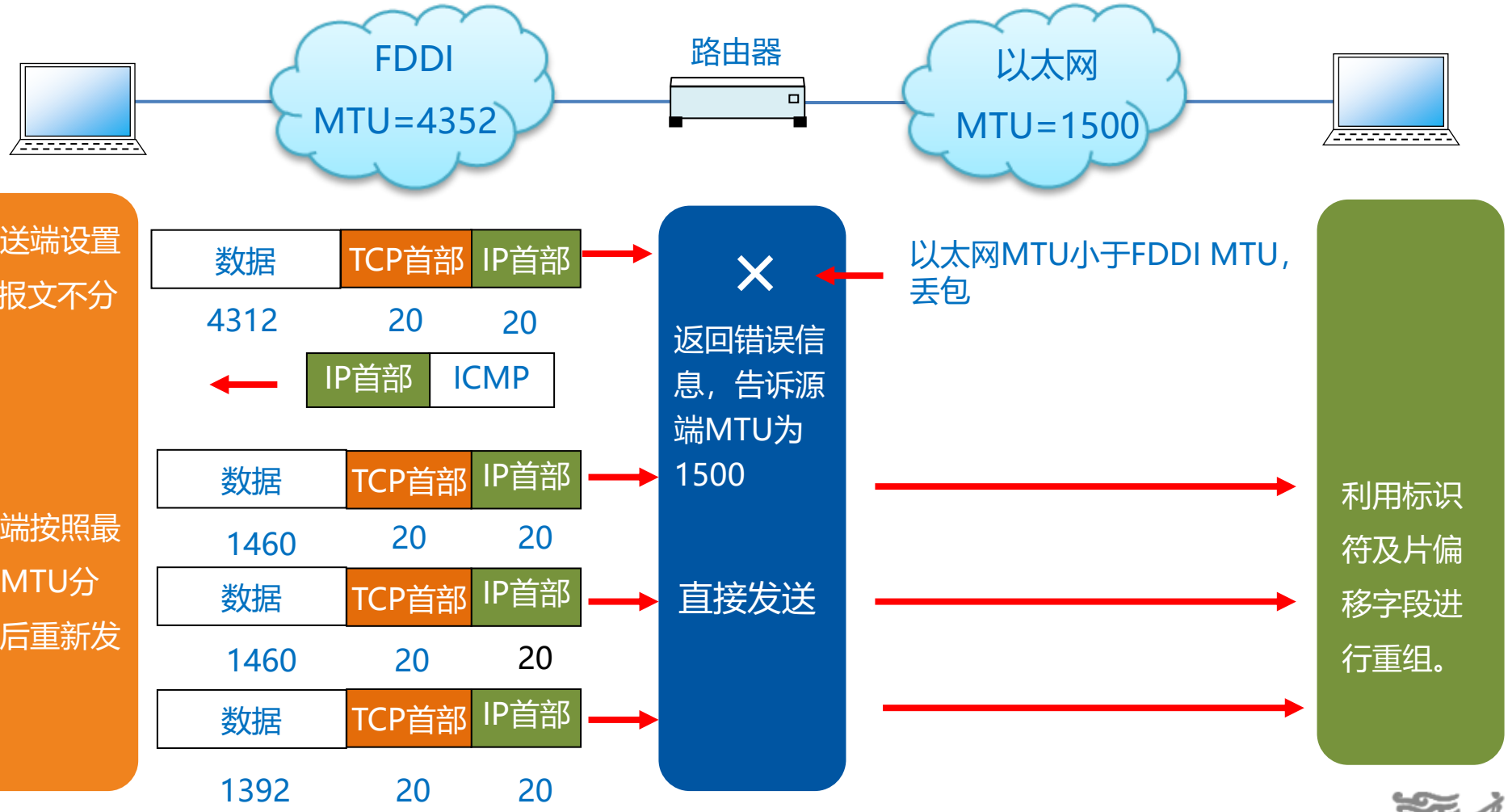
2.路径MTU发现机制

UDP是无连接的协议，对数据包的到达顺序以及是否正确到达不甚关心，所以一般UDP对分片没有特殊要求。



2.路径MTU发现机制

TCP是面向连接的协议，它非常在意数据包的到达顺序以及是否传输中有错误发生，有些TCP应用要求不能分片



地址解析协议ARP

网络基础

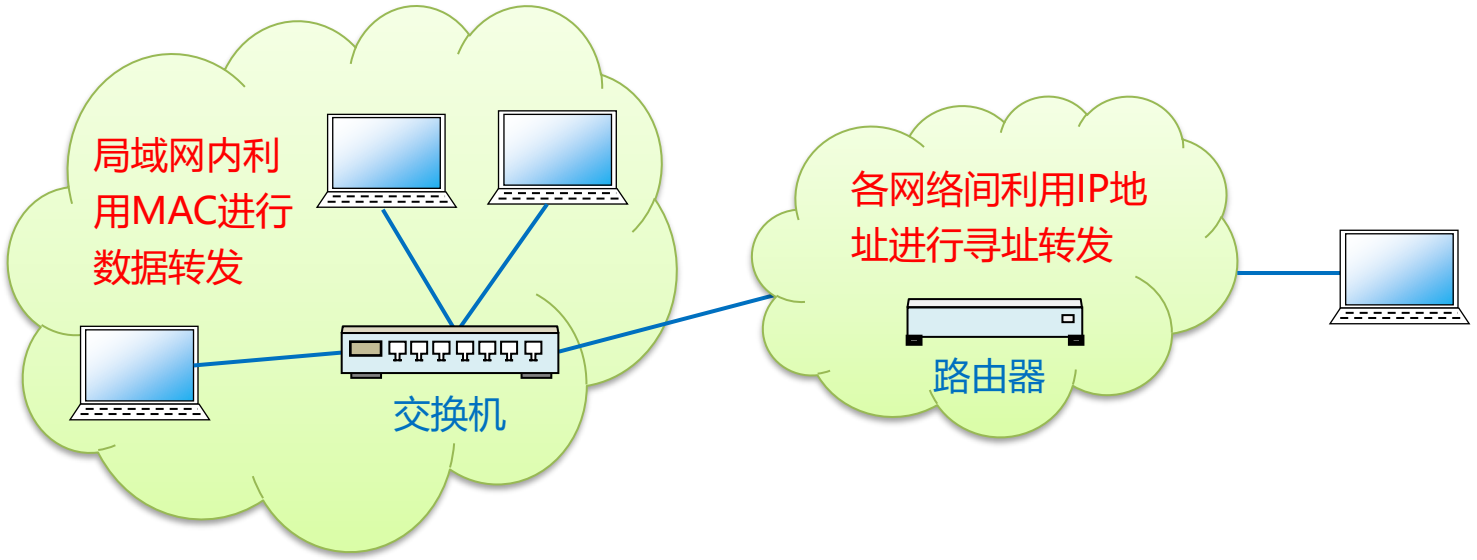
目录
Contents

学习目标

- 掌握ARP协议的作用
- 掌握ARP的工作原理
- 掌握ARP的应用方式

1. ARP协议的作用

ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。



利用ARP –a命令查看主机中MAC地址信息

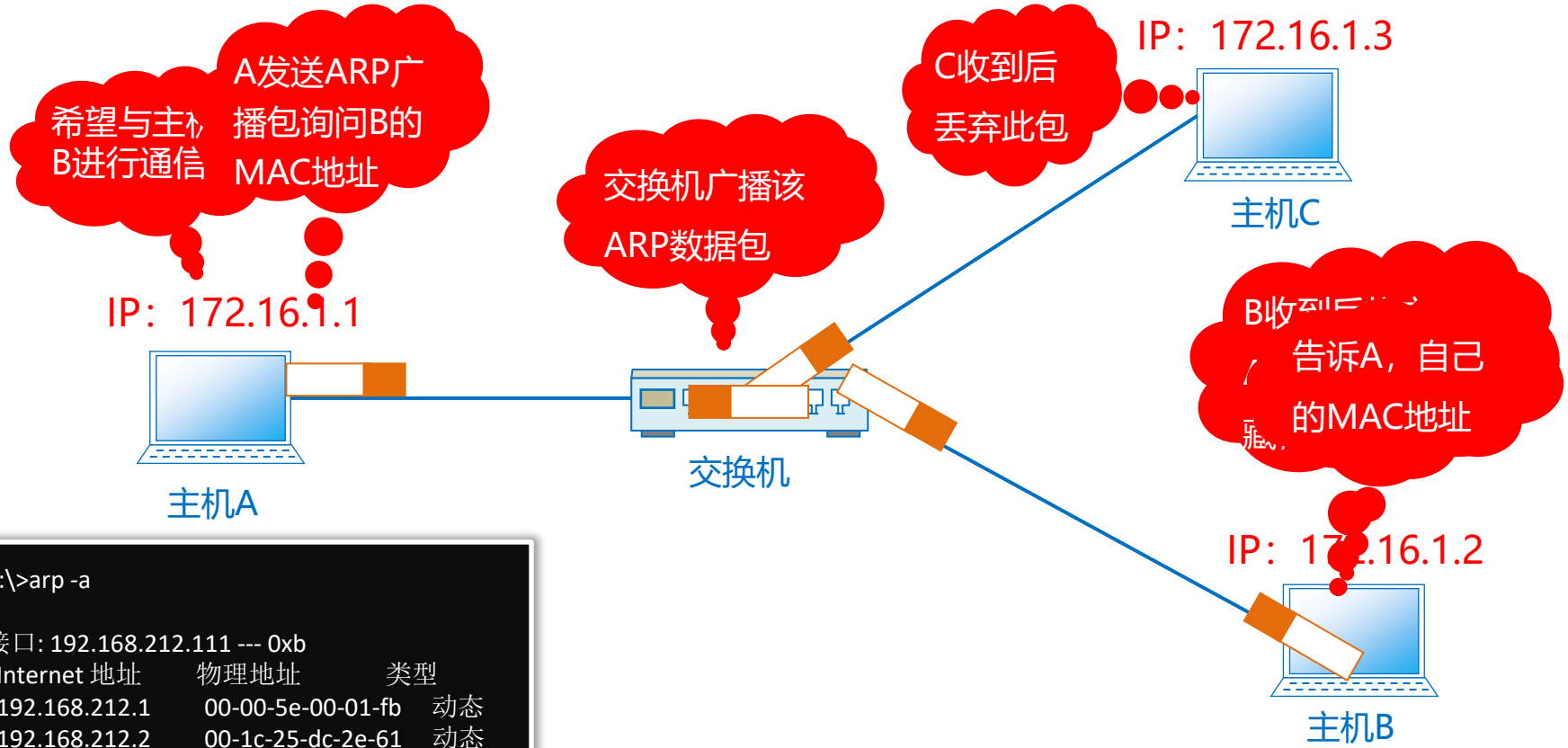
```
C:\>arp -a

接口: 192.168.212.111 --- 0xb
  Internet 地址         物理地址              类型
  192.168.212.1         00-00-5e-00-01-fb     动态
  192.168.212.2         00-1c-25-dc-2e-61     动态
  192.168.212.3         00-16-36-bc-8a-76     动态
  192.168.212.4         ec-a8-6b-8a-1c-ab     动态
  192.168.212.8         d4-3d-7e-d0-e6-63     动态
  192.168.212.9         00-21-97-c2-51-b9     动态
```

以太网中一个主机和另一个主机进行直接通信，必须要知道目标主机的MAC地址。

2. ARP工作原理

ARP是借助ARP请求与ARP响应两种类型的包确定MAC地址的

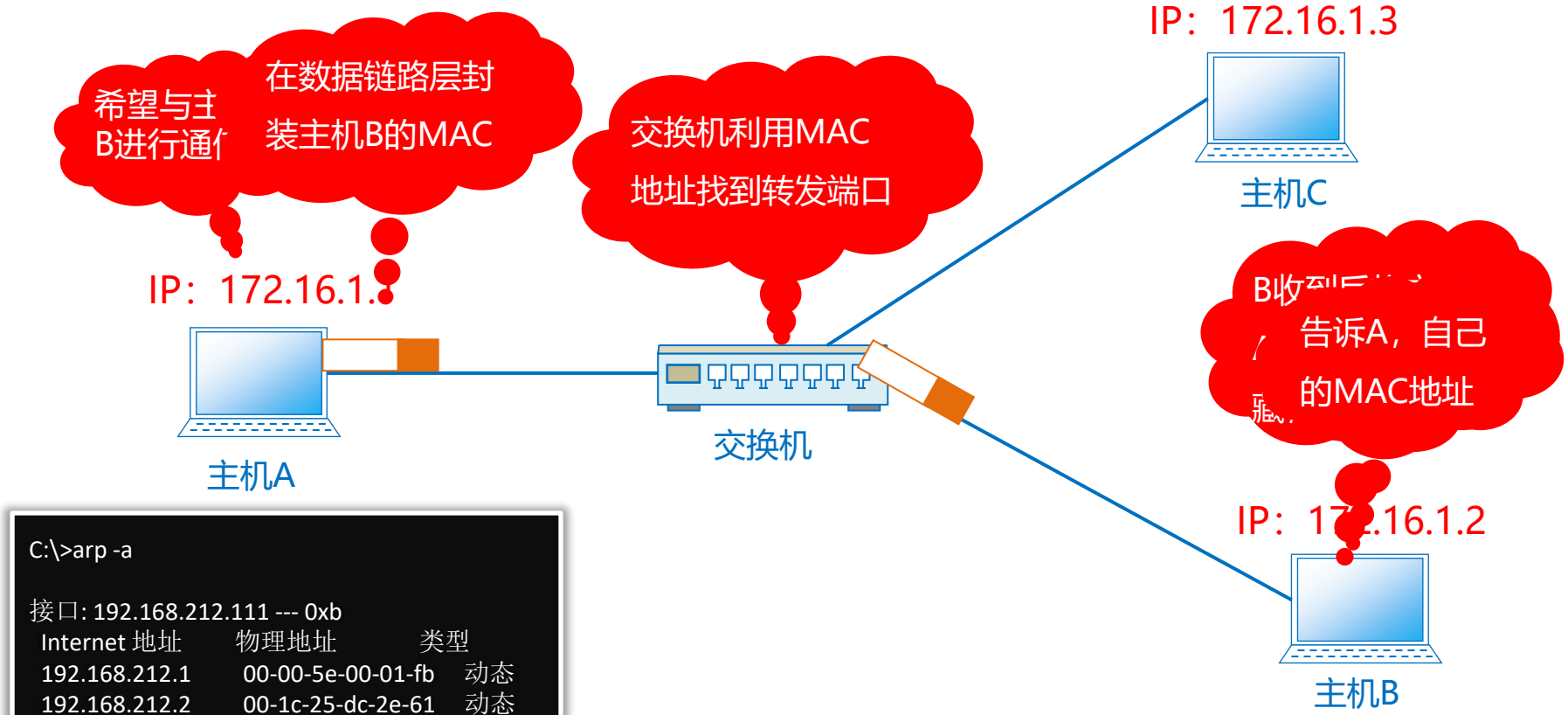



```
C:\>arp -a

接口: 192.168.212.111 --- 0xb
  Internet 地址         物理地址              类型
  192.168.212.1         00-00-5e-00-01-fb     动态
  192.168.212.2         00-1c-25-dc-2e-61     动态
  192.168.212.3         00-16-36-bc-8a-76     动态
  172.16.1.2            ec-a8-6b-8a-1c-ab     动态
```

3. ARP应用方式

ARP地址查询完成后，交换机将利用这一MAC地址进行转发




```
C:\>arp -a

接口: 192.168.212.111 --- 0xb
  Internet 地址         物理地址           类型
  192.168.212.1         00-00-5e-00-01-fb     动态
  192.168.212.2         00-1c-25-dc-2e-61     动态
  192.168.212.3         00-16-36-bc-8a-76     动态
  172.16.1.2            00-00-36-00-00-01     动态
```

ARP与跨网络通信

网络基础

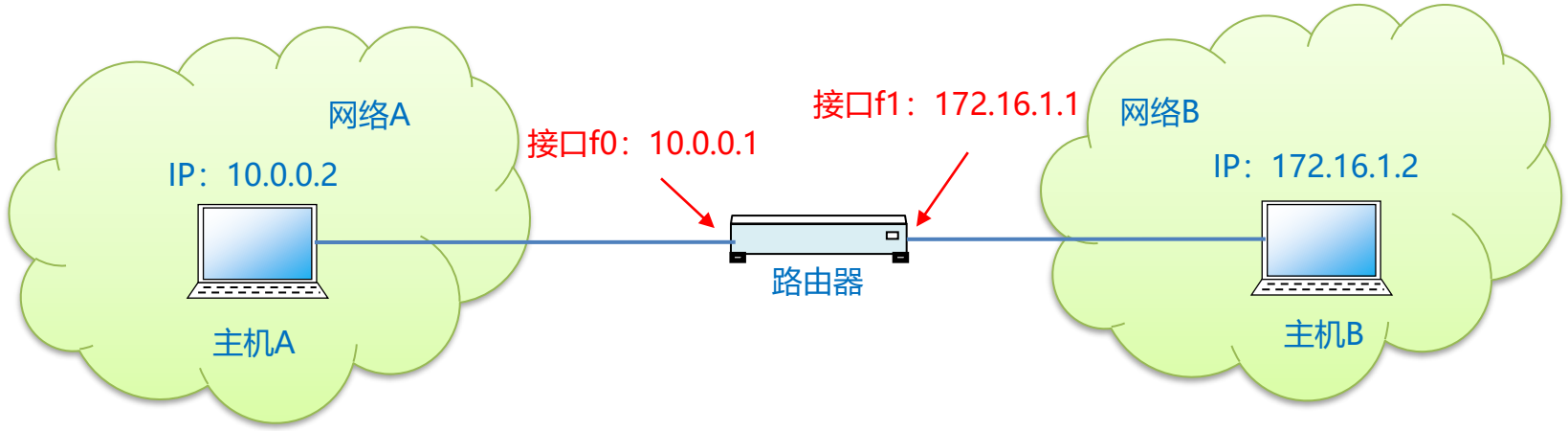
目录
Contents

学习目标

- 理解ARP为什么不能跨网通信
- 理解ARP代理工作方式

1. ARP与跨不同网络通信

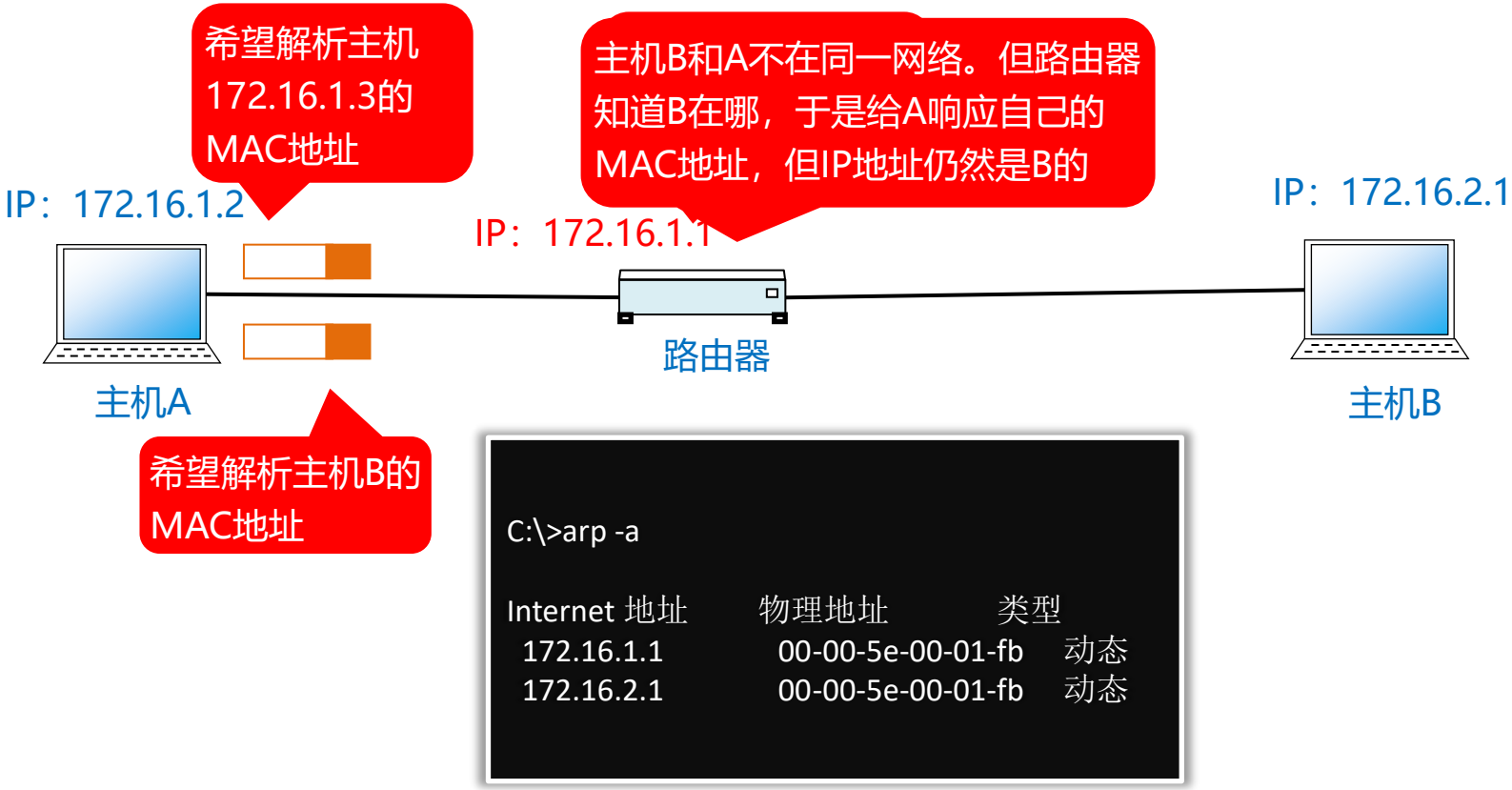
ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。



正常情况下，主机只能解析到与之同一网络的其它主机及网关的MAC地址，而不能跨网络进行地址解析。

2. ARP代理

采用代理ARP的路由器可将ARP请求转发给邻近的网段。两个以上网段的节点之间可以像在同一个网段中一样进行通信。

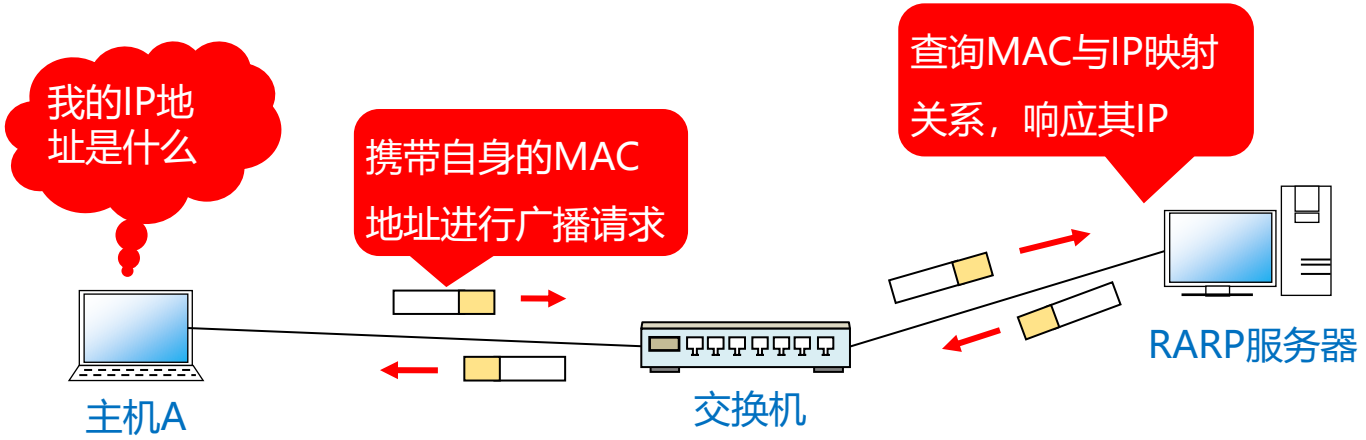


反向地址解析协议RARP

网络基础

1.反向地址解析协议RARP

利用MAC地址解析出相对亦的IP地址。例如将打印机服务器等小型嵌入式设备接入到网络时就经常会用到。



ICMP协议

网络基础

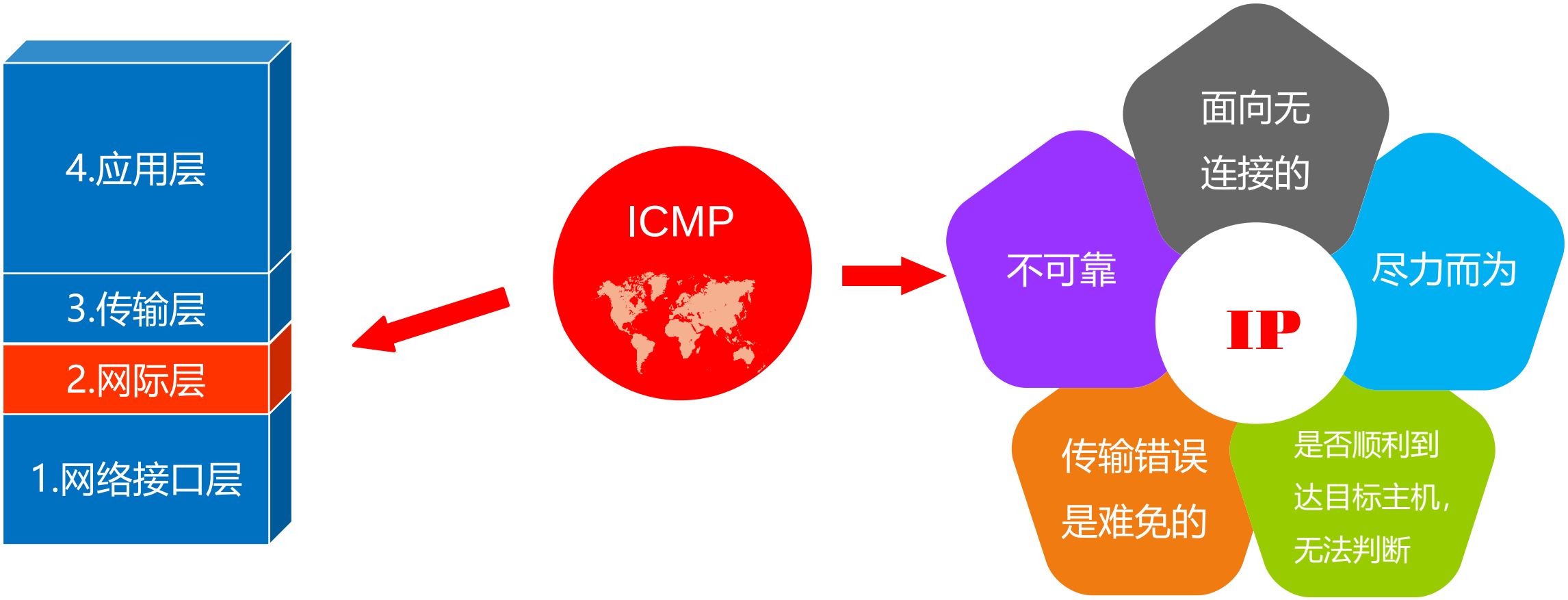
目录
Contents

学习目标

- 理解ICMP的作用
- 了解ICMP报文格式及含义

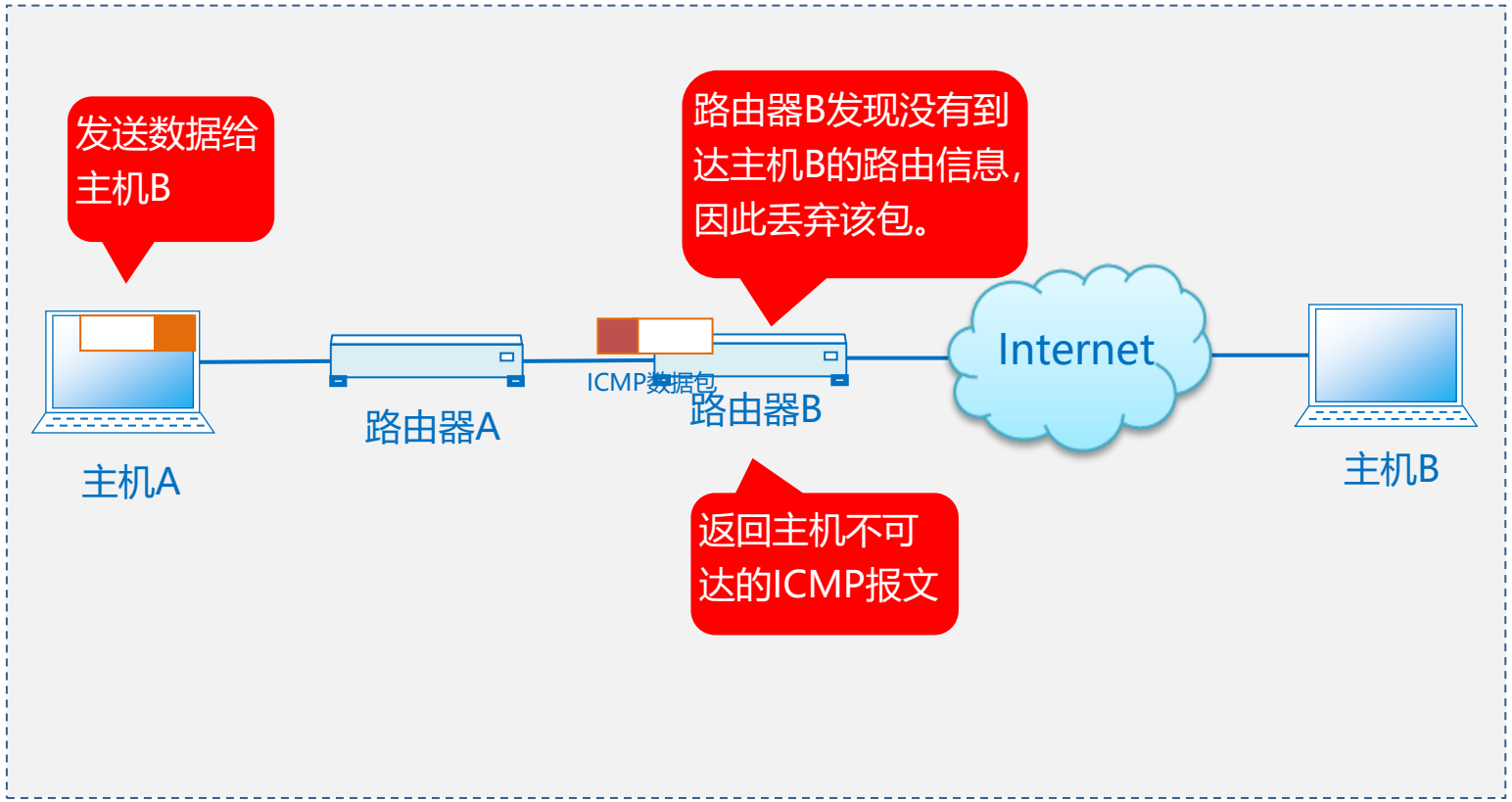
1.设计ICMP协议目的

ICMP用于在IP主机、路由器之间传递控制消息，控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。



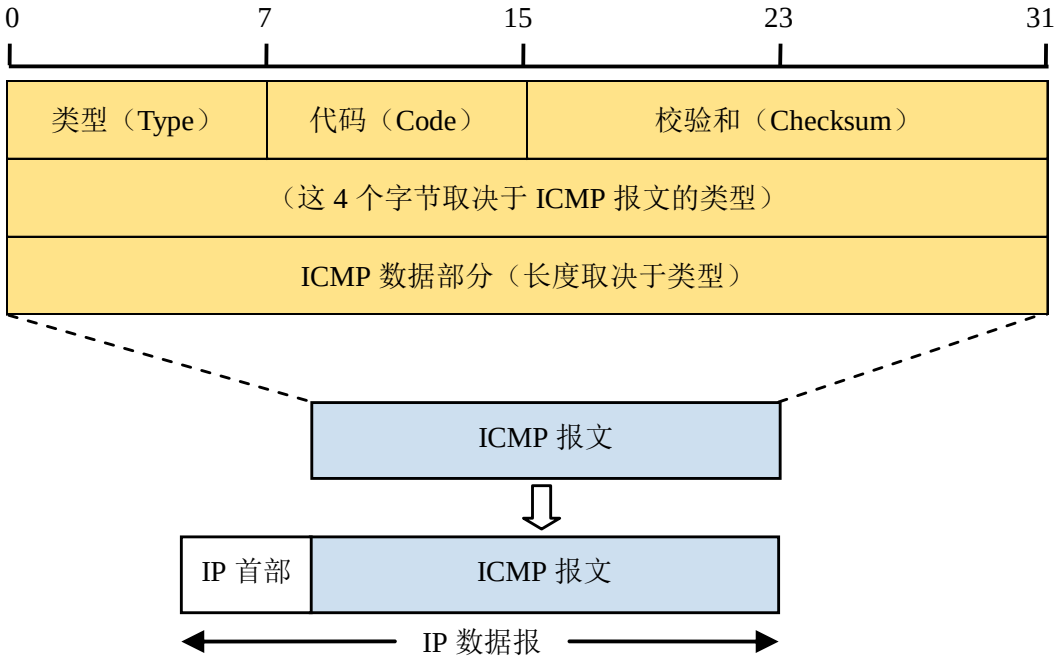
2. ICMP主要功能

可以获得网络是否正常、设置是否有误以及设备有何异常等信息，从而便于进行网络上的问题诊断。



3. ICMP协议报文格式

ICMP消息分为两类：一类是ICMP差错控制报文，即通知出错原因的错误消息，另一类是ICMP询问报文，即用于诊断的查询消息。



ICMP报文种类	类型	内 容
差错报告报文	3	目标不可达
	4	源点抑制
	5	重定向或改变路由
	9	路由器公告
	10	路由器请求
	11	超时

ICMP主要消息类型及现象分析

网络基础

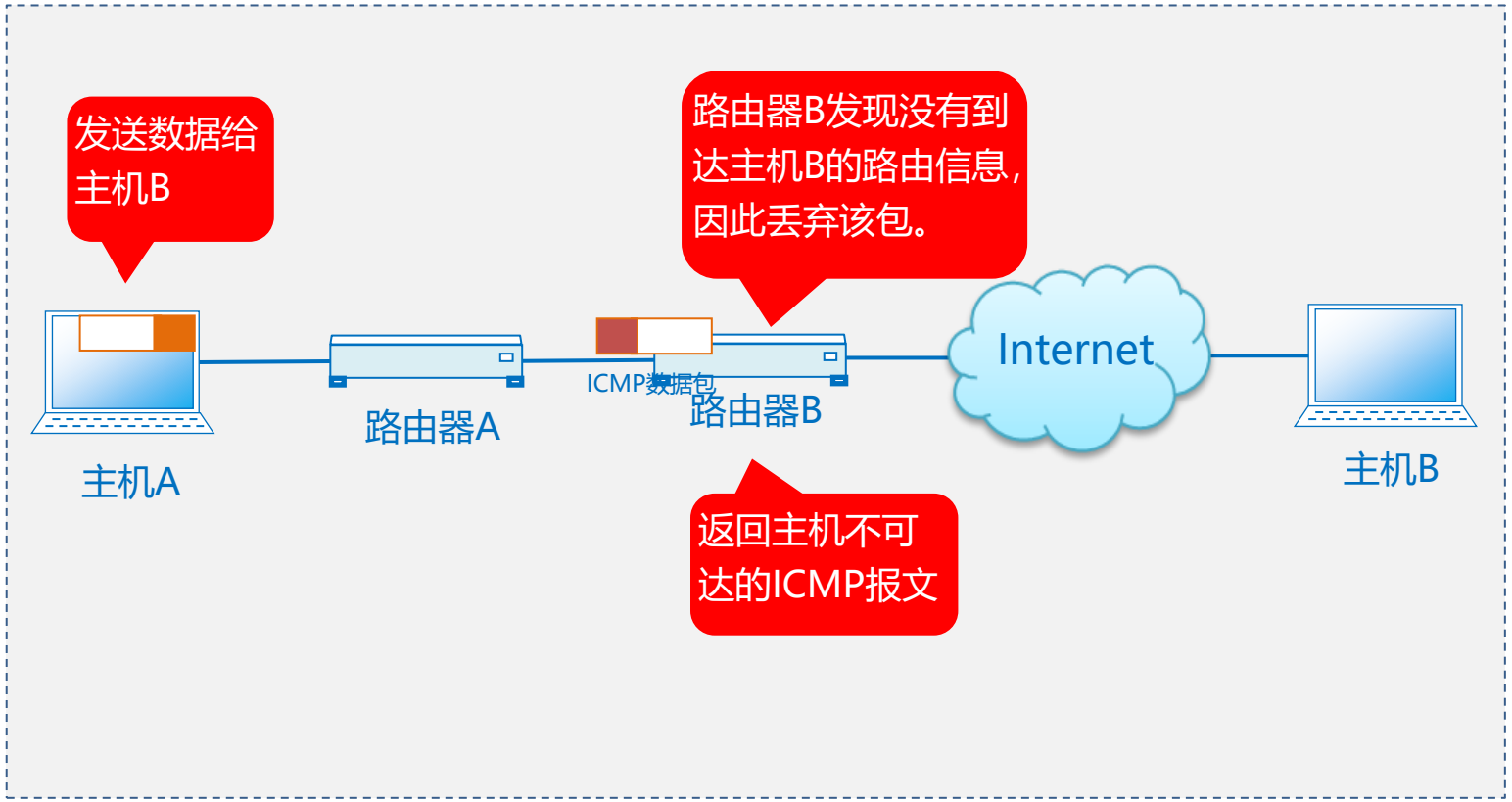
目录
Contents

学习目标

- 理解ICMP消息类型
- 了解ICMP消息应用场景

1.目标不可达

网络中，路由器无法将数据包发送给目的地址时，会给发送端返回目标不可达的消息，并在这个消息中显示具体原因。



错误号	ICMP不可达消息
0	目标网络不可达
1	目标主机不可达
2	目标协议不可达)
3	目标端口不可达
6	未知的目标网络
7	未知的目标主机

2.超时的消息

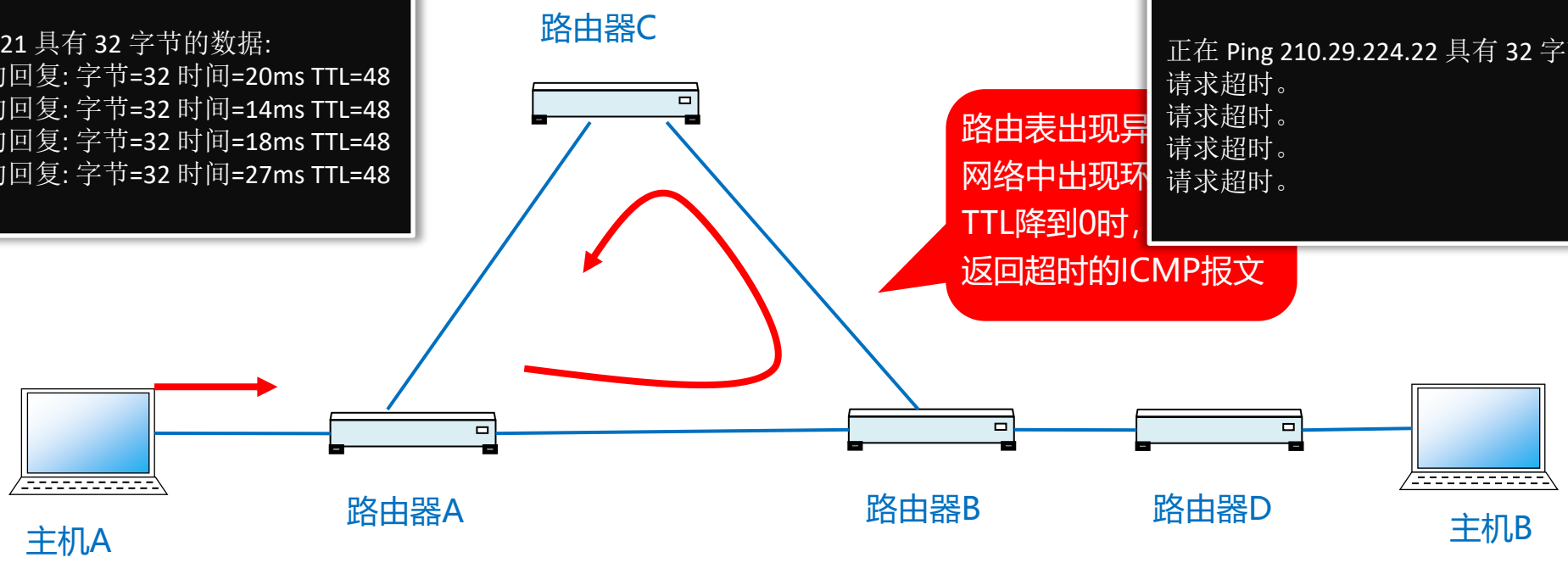
IP包中有一个字段叫做TTL，它的值随着每经过1s就会减1，直到减到0时该IP包会被丢弃。

```
C:\Users\jier>ping 210.29.224.21

正在 Ping 210.29.224.21 具有 32 字节的数据:
来自 210.29.224.21 的回复: 字节=32 时间=20ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=14ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=18ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=27ms TTL=48
```

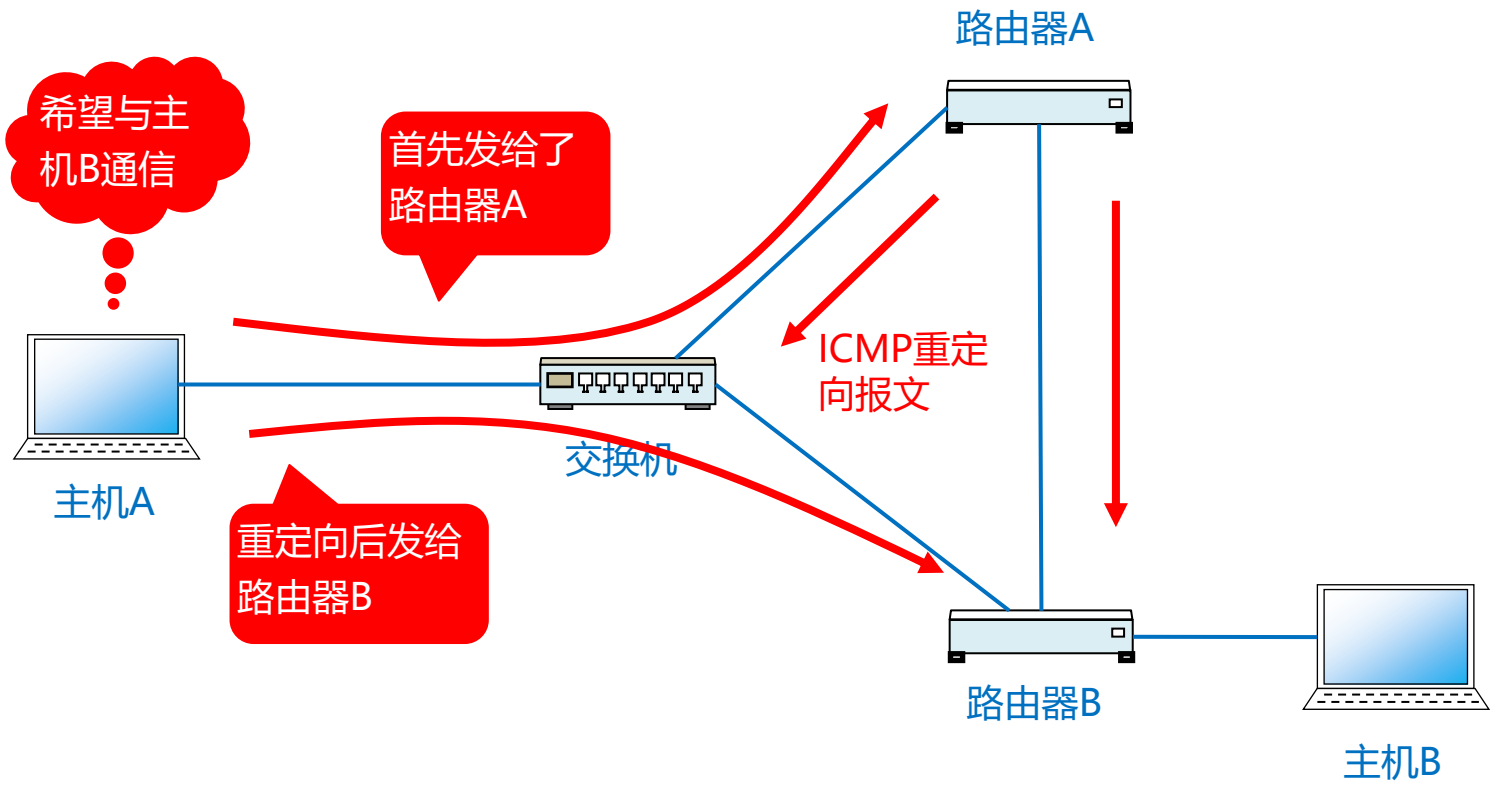
```
C:\Users\jier>ping 210.29.224.22

正在 Ping 210.29.224.22 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
```



3.重定向消息

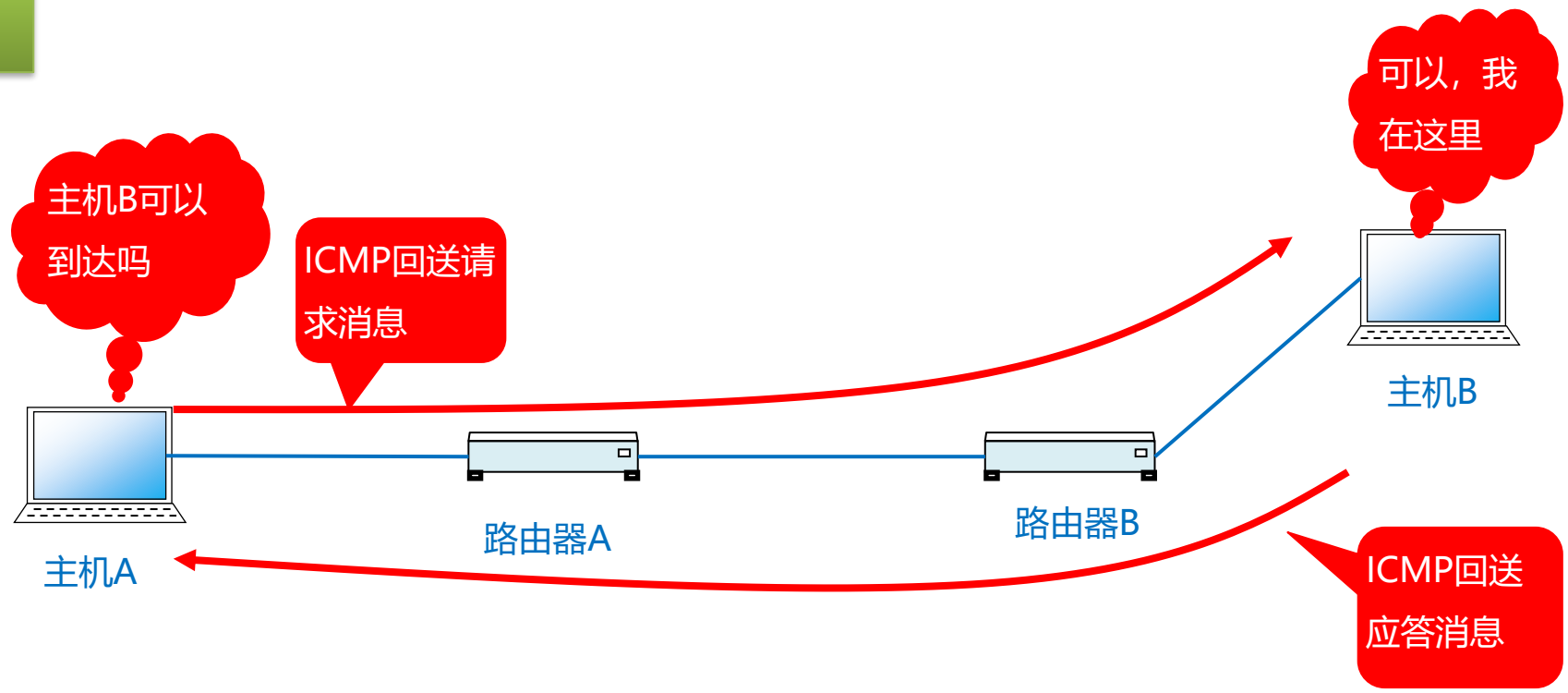
路由器一旦检测到某IP数据报经非优路径传输，将向主机发送一个路由重定向报文，通知主机去往目的主机的最优路径



4.回送消息

用于进行通信的主机或路由器之间，用于测试路由器和目的主机的可达性。

Ping



常用网络命令体验

网络基础

目录
Contents

学习目标

- 了解网络故障诊断时常用的命令
- 掌握常用故障排除命令使用方法

1. ipconfig命令

Ipconfig命令用于显示网络适配器的物理地址、IP地址、子网掩码以及默认网关等相关信息

IPConfig最常用的选项

- ipconfig的命令格式如下：

  ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

  - /?:　显示ipconfig的格式和参数的英文说明
  - /all:
  - /release
  - /renew

2. Ping命令

ping命令就是利用回应请求 / 应答ICMP报文来测试目的主机或路由器的可达性。

可检测的信息：

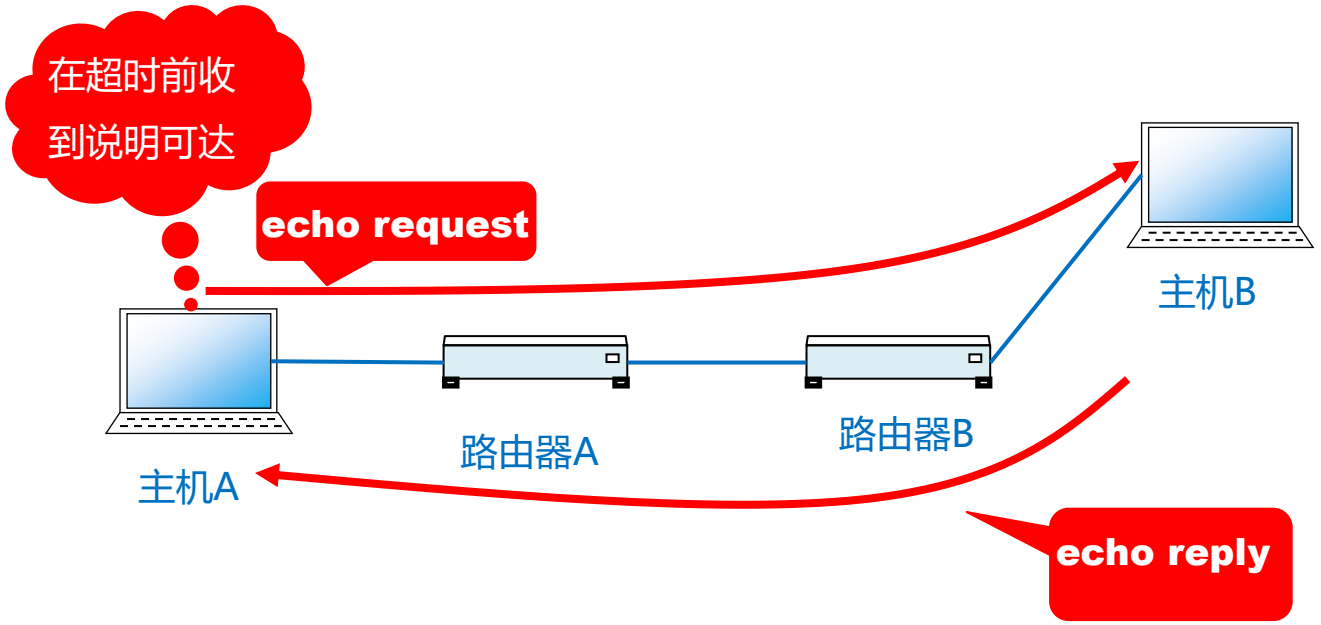

```
C:\Users\jier>ping 210.29.224.21

正在 Ping 210.29.224.21 具有 32 字节的数据:
来自 210.29.224.21 的回复: 字节=32 时间=20ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=14ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=18ms TTL=48
来自 210.29.224.21 的回复: 字节=32 时间=27ms TTL=48

Ping statistics for 192.168.224.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2. Ping命令

- ping 是如何工作的



➢Ping的命令格式如下：

ping [-t] [-a] [-n count] [-l length] {-j computer-list]} [-w timeout] target-name

选项	选项含义
-t	连续发送和接收回送请求和应答ICMP报文直到手动停止(CTR+Break：查看统计信息，CTR+C：停止ping命令)
-a	将IP地址解析为主机名
-n Count	发送回送请求ICMP报文的数量
-l Size	发送探测数据包的大小(默认值为32 Byte)
-f	不能分片(默认为允许分片)
-i TTL	指定生存周期
-w Timeout	指定等待每个回送应答的超时时间(以ms为单位，默认值为1 000)

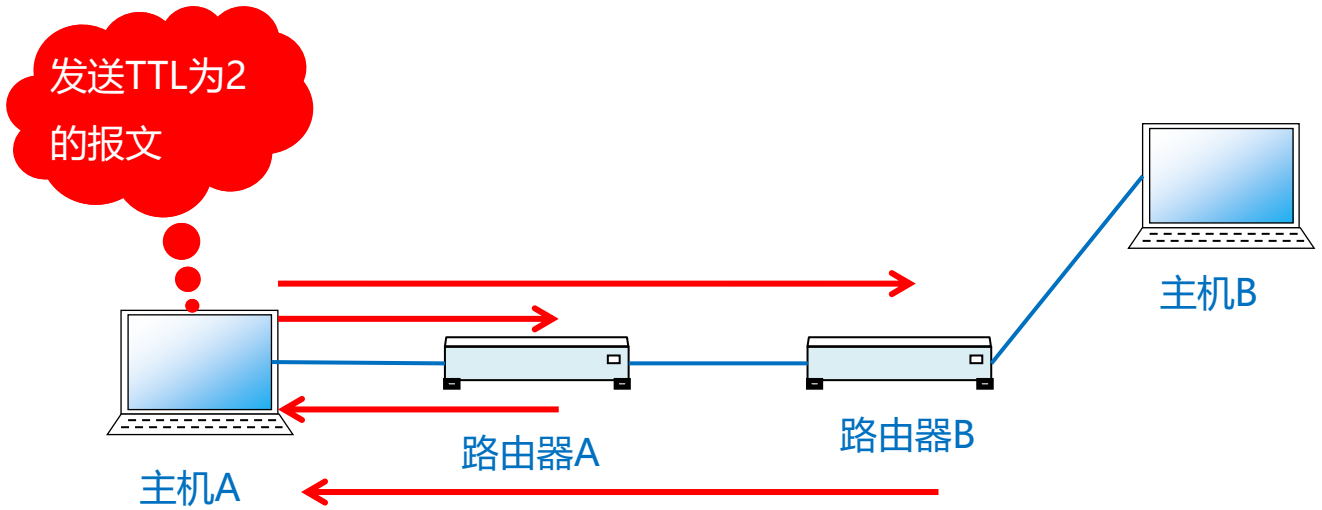
2. Ping命令

- ping命令测试返回的信息含义

返回信息	信息含义
!（叹号）	成功收到响应，网络可达
.（点）	等待响应超时（Request Timed Out）
U	目标不可达（destination unreachable）或接收到错误的 PDU
Q	目标地址过于繁忙（Source quench received）
M	不能分片
？（问号）	未知的数据包类型
&	生存期(TTL=0)超出
Bad IP address	可能没有连接到DNS服务器所以无法解析这个IP地址，也可能是IP地址不存在
Unknown host	

3. Tracert命令

- tracert可以显示出由执行程序的主机到达特定主机之前历经多少路由器，确定数据包为到达目的地所必须经过的有关路径，并指明哪个路由器在浪费时间。




```
C:\WINDOWS>tracert -d 172.16.2.65
Tracing route to  172.16.2.65
over a maximum of 30 hops:
 1   <10 ms   <10 ms   <10 ms 172.16.2.65
Trace complete.
```

4. nslookup命令

- nslookup命令主要用来诊断域名系统 (DNS) 基础结构的信息，是查询域名信息的一个非常有用的命令

```
C:\>nslookup www.baidu.com
服务器:  dns.hcit.edu.cn
Address:  210.29.224.21

非权威应答:
名称:    www.a.shifen.com
Addresses:  119.75.218.70
          119.75.217.109
Aliases:  www.baidu.com
```

```
C:\>nslookup
> set type=a
> www.baidu.com
服务器:  dns.hcit.edu.cn
Address:  210.29.224.21

非权威应答:
名称:    www.a.shifen.com
Addresses:  119.75.217.109
          119.75.218.70
Aliases:  www.baidu.com
```

5. Netstat命令

- netstat命令用于显示各种网络相关信息，如网络连接，路由表，接口状态，masquerade 连接，多播成员等

```
C:\>netstat -t
活动连接
  协议  本地地址          外部地址              状态           卸载状
态
  TCP    127.0.0.1:1082         PC-201310082321:1083   ESTABLISHED     InHost
  TCP    127.0.0.1:1083         PC-201310082321:1082   ESTABLISHED     InHost
  TCP    127.0.0.1:11941        PC-201310082321:11942  ESTABLISHED     InHost
  TCP    127.0.0.1:11951        PC-201310082321:11950  ESTABLISHED     InHost
  TCP    192.168.212.11:16551   220.181.90.74:http     ESTABLISHED     InHost
  TCP    192.168.212.11:16609   180.153.160.57:http    CLOSE_WAIT      InHost
  TCP    192.168.212.11:16676   220.181.89.69:http     ESTABLISHED     InHost
```

VPN虚拟专用网

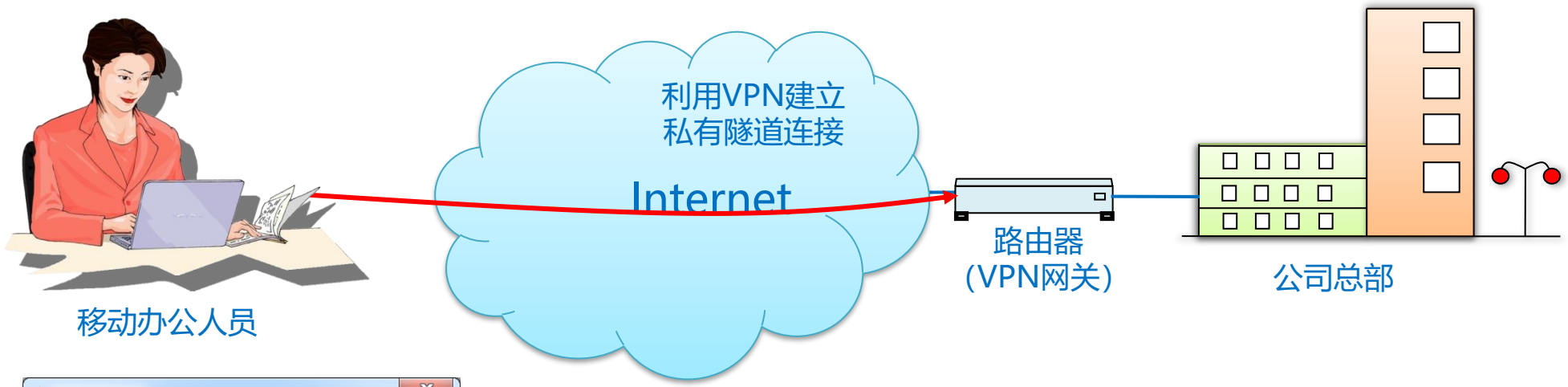
网络基础

目录
Contents

学习目标

- 了解VPN的应用方式
- 了解VPN的技术特点

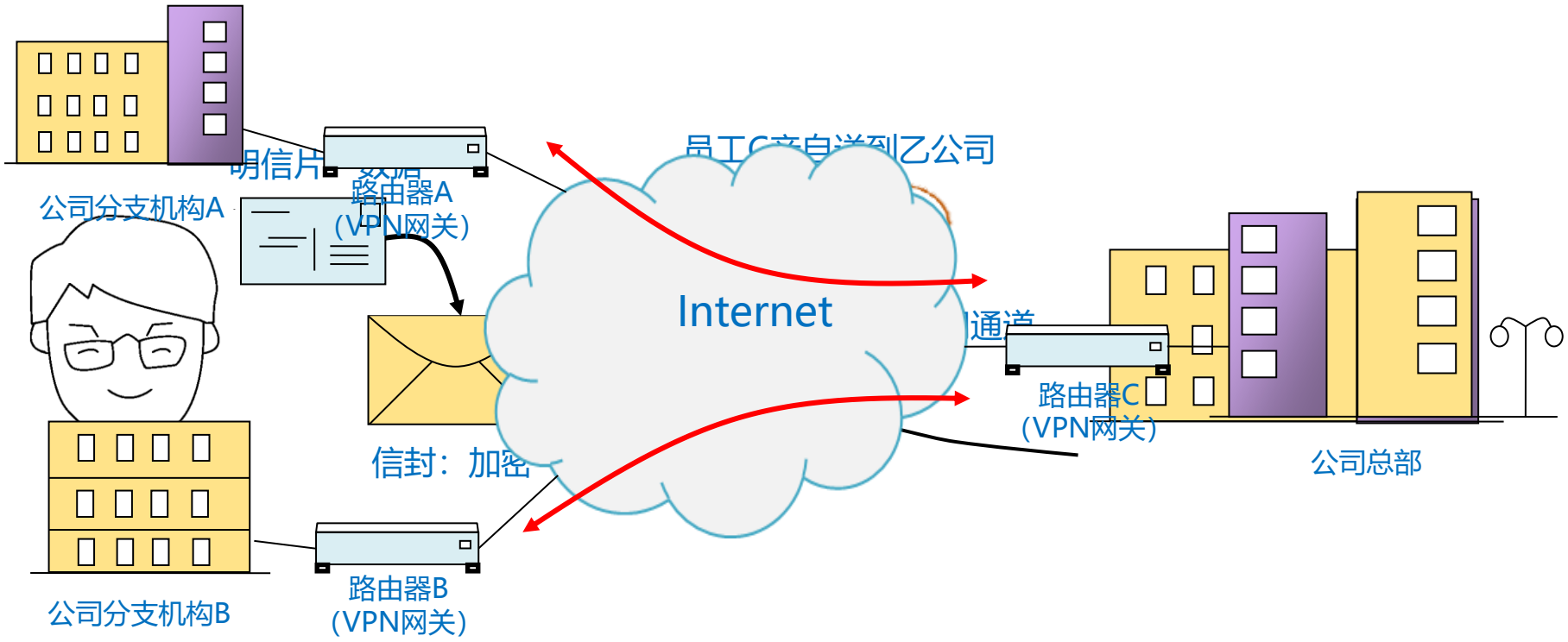
1. VPN概述


利用VPN建立
私有隧道连接
Internet
路由器
(VPN网关)
公司总部
移动办公人员


连接 VPN 连接
用户名(U):
密码(P):
域(M):
为下面用户保存用户名和密码(S):
只是我(N)
任何使用此计算机的人(A)
连接(C)
取消
属性(O)
帮助(H)

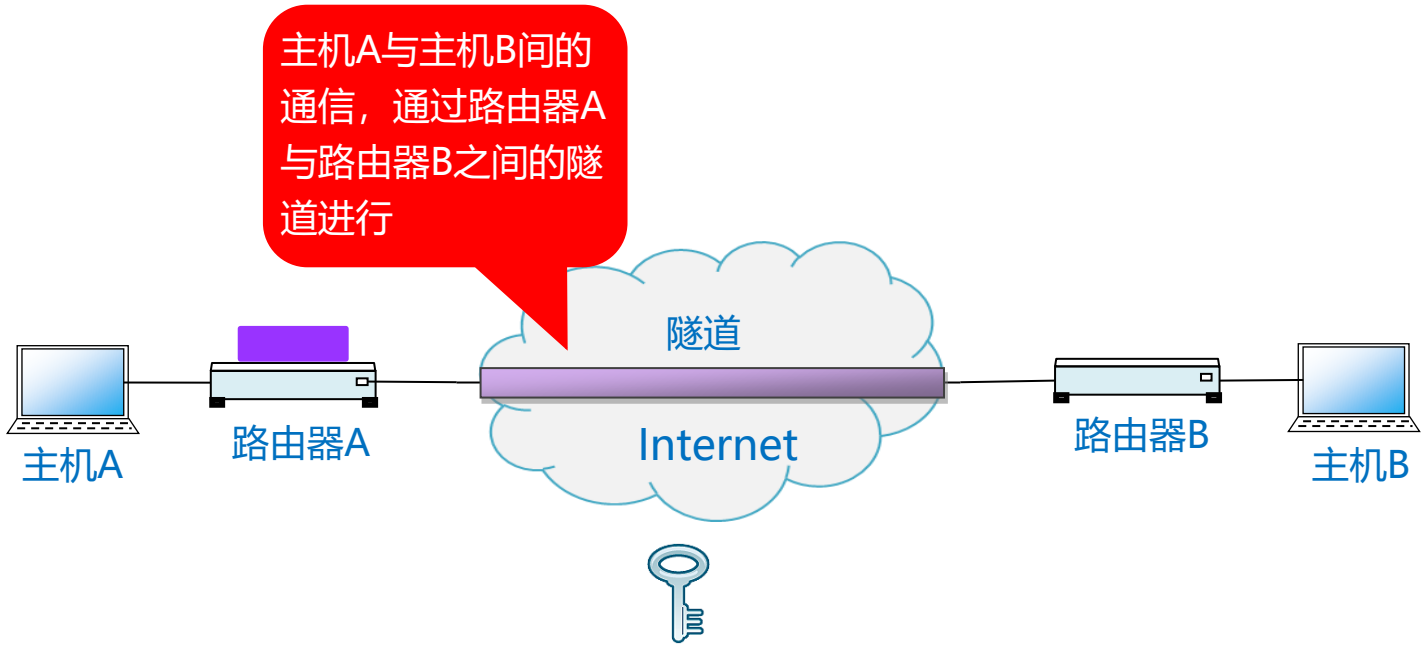
1. VPN概述

虚拟专用网，是一种常用于连接中、大型企业或团体与团体间的私人网络的通讯方法。



2. VPN中常用技术


隧道技术
加解密技术
密钥管理技术
数据认证和身份认证技术


主机A与主机B间的通信，通过路由器A与路由器B之间的隧道进行
隧道
主机A
路由器A
Internet
路由器B
主机B
用户名+密码

NAT地址转换

网络基础

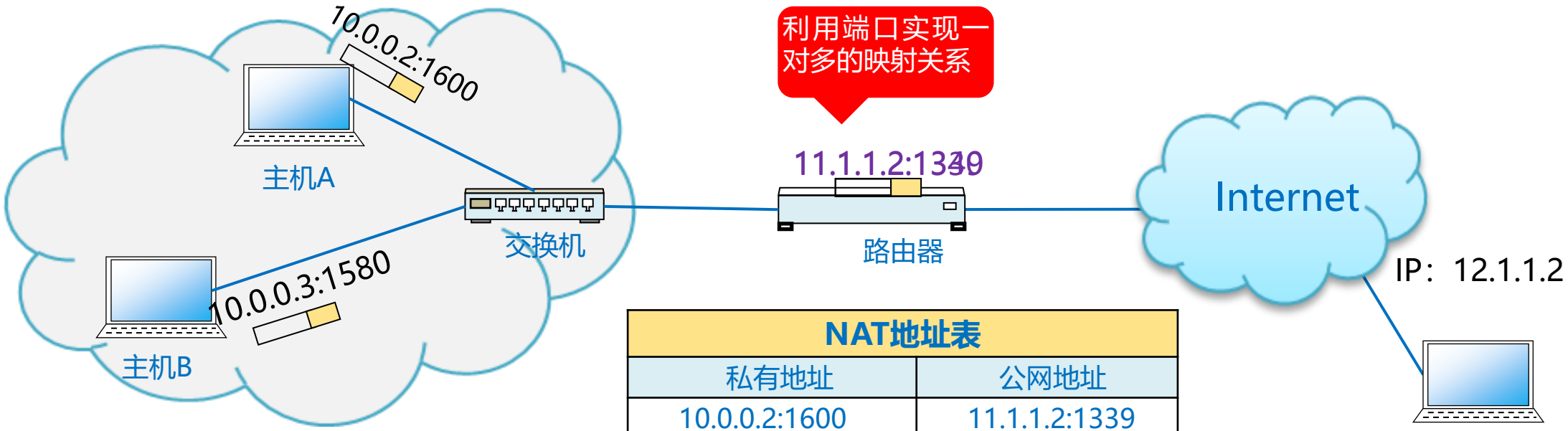
目录
Contents

学习目标

- 了解NAT地址转换的基本方式
- 掌握NAT地址转换的缺点

1. NAT地址转换的方式

NAT地址转换就是将私网地址转换为公网地址的过程



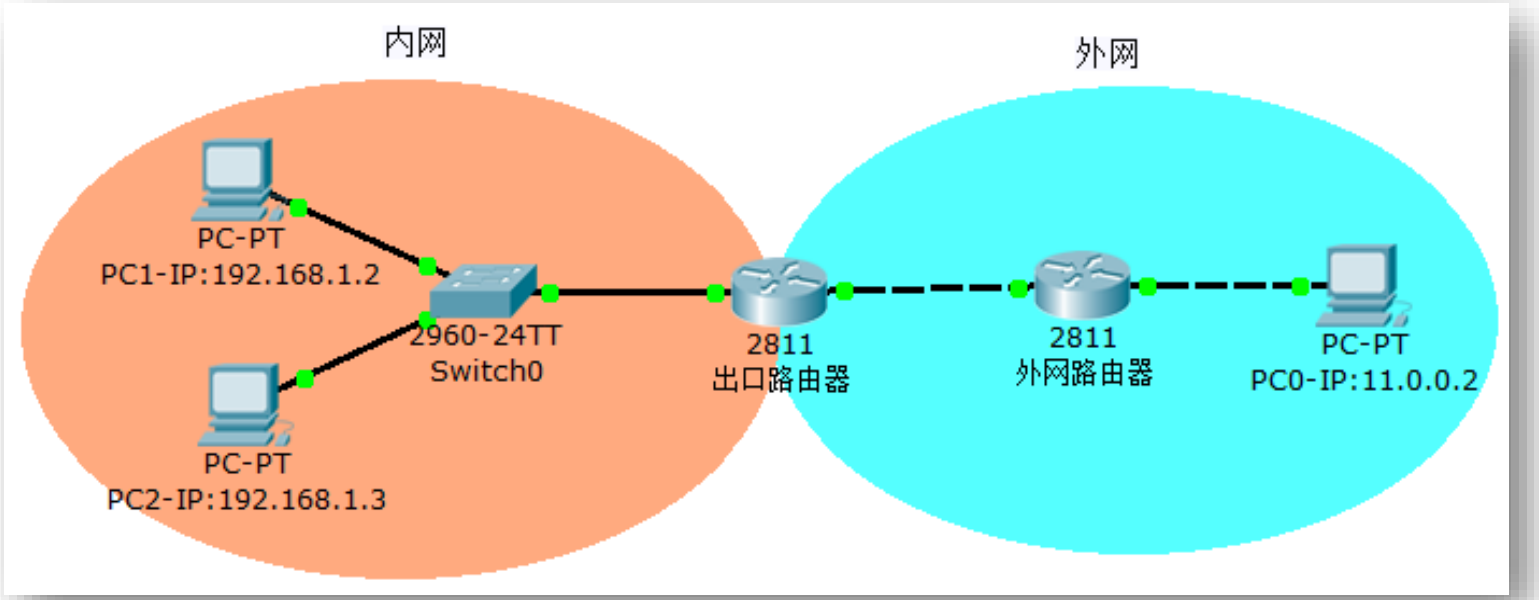
NAT地址表	
私有地址	公网地址
10.0.0.2:1600	11.1.1.2:1339
10.0.0.3:1580	11.1.1.2:1340

2. NAT地址转换优缺点

NAT地址转换过程体验

网络基础

NAT地址转换过程体验



IPv6协议

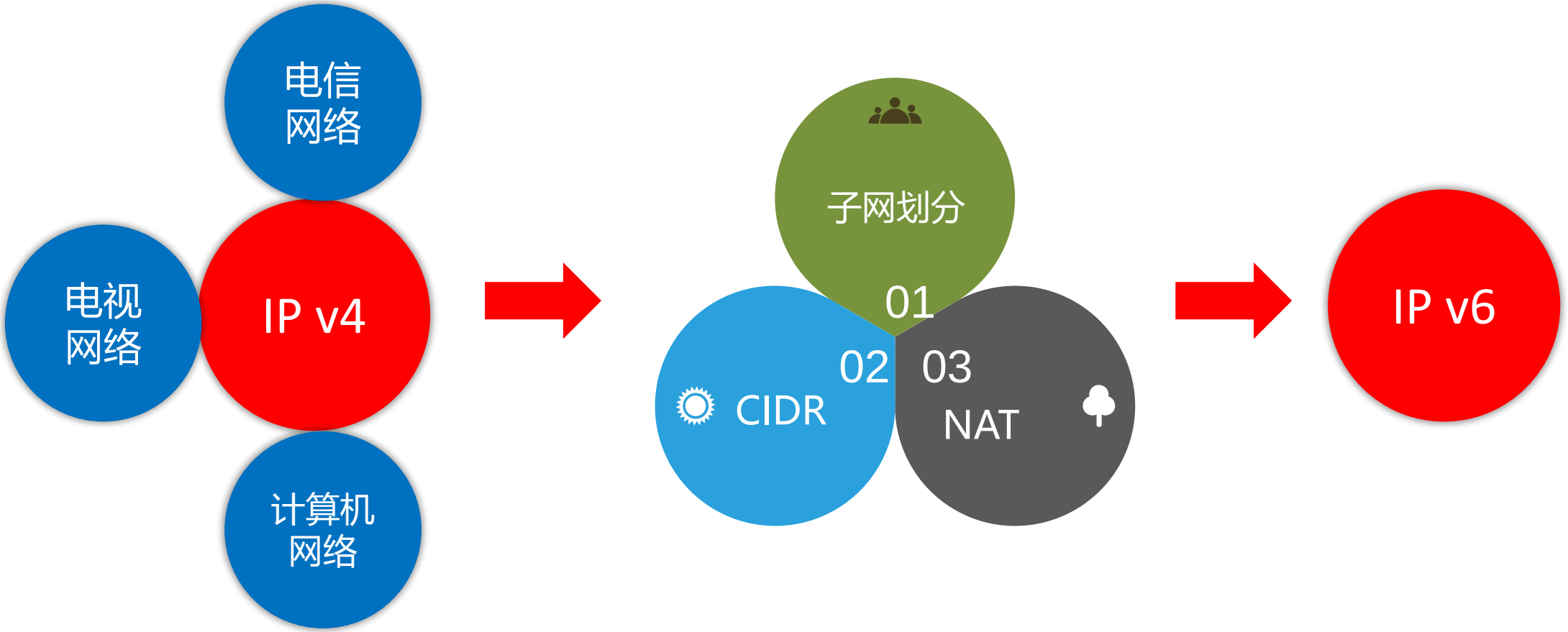
网络基础

目录
Contents

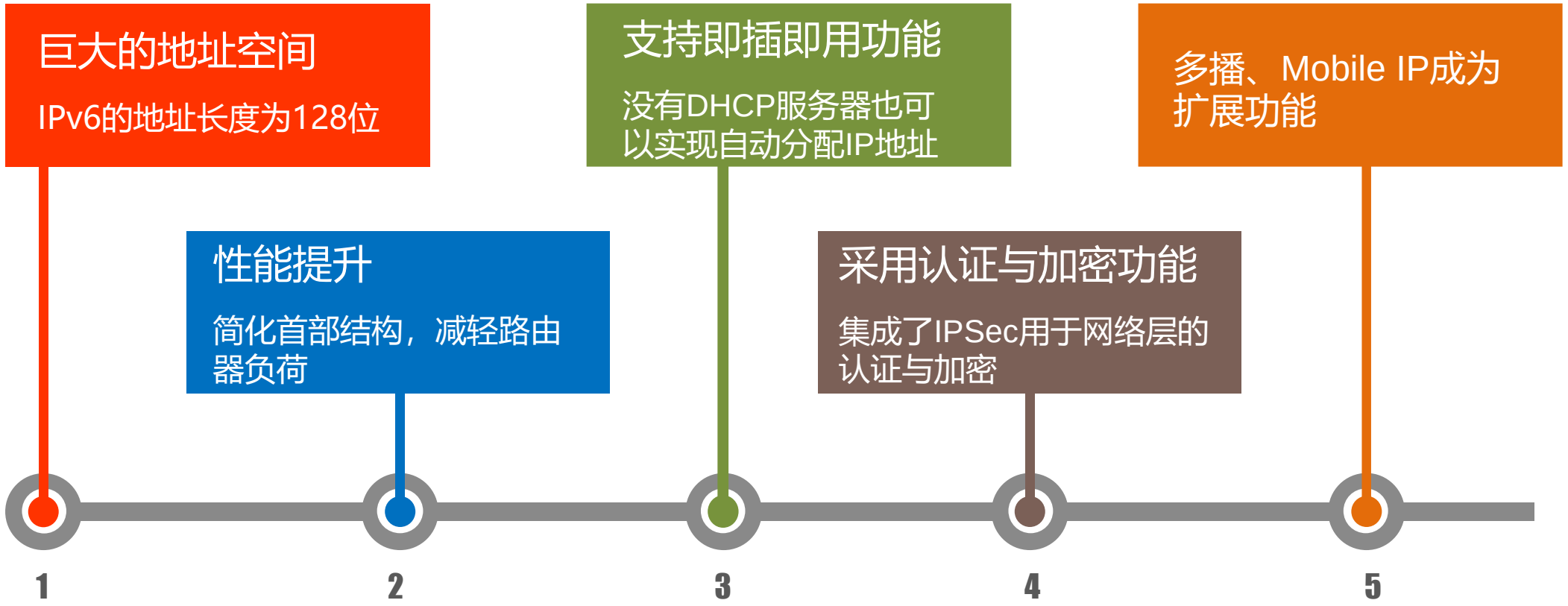
学习目标

- 了解IPv6出现背景
- 了解IPv6协议特点

IPv4地址出现短缺



2. IPv6的特点


巨大的地址空间
IPv6的地址长度为128位
性能提升
简化首部结构，减轻路由器负荷
支持即插即用功能
没有DHCP服务器也可以实现自动分配IP地址
采用认证与加密功能
集成了IPSec用于网络层的认证与加密
多播、Mobile IP成为扩展功能
1
2
3
4
5

IPv6协议报文格式

网络基础

目录
Contents

学习目标

- 理解IPv6报文格式
- 理解IPv6报文各字段含义

2. IPv6报文各字段含义

IPv6报文格式

2. IPv6报文各字段含义

IPv6报文格式

1 版本（version）

表示该数据报所使用的IP协议版本号

0110 ➡ IPv6

2. IPv6报文各字段含义

IPv6报文格式

2 流量类别

长度为8位

相当于IPv4中的TOS

主要用以标识IPv6分组的类别和优先级

2. IPv6报文各字段含义

IPv6报文格式

3 流标签

流：单播或组播分组

属于同一个流的数据分组都具有相同的流标签

2. IPv6报文各字段含义

IPv6报文格式

4 有效载荷长度

长度为16位，表示IPv6数据报除基本头部以外的字节数。

最大长度为65535字节的有效载荷，如果超过这个值，该字段会置零。

2. IPv6报文各字段含义

IPv6报文格式

5 下一个首部

相当于IPv4中的协议字段或可选字段

表示后面第一个扩展首部的协议类型

2. IPv6报文各字段含义

IPv6报文格式

6 跳数限制

相当于IPv4中的生存时间

分组每经过一个路由器，该字段值递减

1。当跳限制降为0时，分组将会被丢弃。

2. IPv6报文各字段含义

IPv6报文格式

7 源地址与目的地址

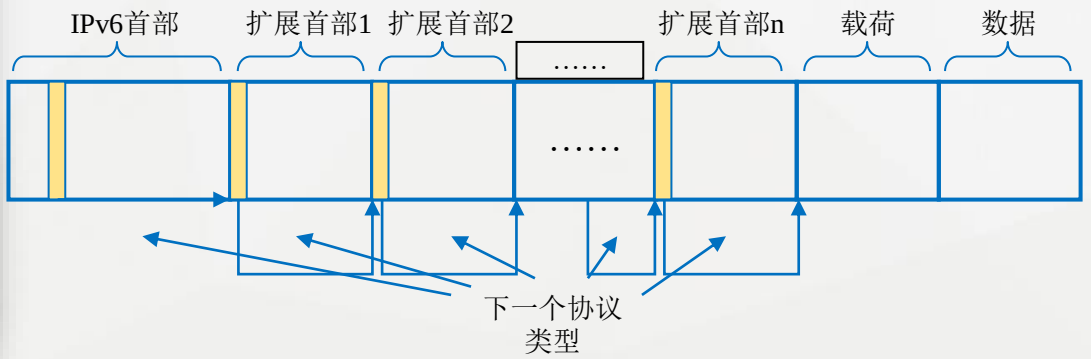
长度为128位，用以标识发送分组的源主机和接收分组的目标主机的IPv6地址。

2. IPv6报文各字段含义

IPv6报文格式

8 IPv6扩展首部

IPv6首部中没有标识以及标记字段，在需要对IP数据报进行分片时，就可以使用扩展首部



2. IPv6报文各字段含义

IPv6报文格式

9 IPv6上层首部与数据

数据字段内容是上层所封装的完整数据。

IPv6地址

网络基础

目录
Contents

学习目标

- 掌握IPv6地址表示方法
- 理解IPv6地址分类

1. IPV6地址表示方法

1.IPv6地址共128位

2.冒号分十六进制：

16位一组，用十六进制表示，中间用冒号隔开

108A:0:0:0:8:800:200C:417A

1 包含长串0位的地址

108A:0:0:0:8:800:200C:417A → 108A: :8:800:200C:417A

108A:0:0:8:0:0:0:417A → 108A: :8:0:0:0:417A √

108A:0:0:8: :417A √

108A: :8: :417A ×

2 IPv4和IPv6混合表示

x:x:x:x:x:x:D.D.D.D

0:0:0:0:0:0:123.1.68.3 → : :123.1.68.3

3 URL表示方法

::13.1.68.3

URL格式表示为：http://[::13.1.68.3]/index.html

2. IPV6地址分类

单播地址

01

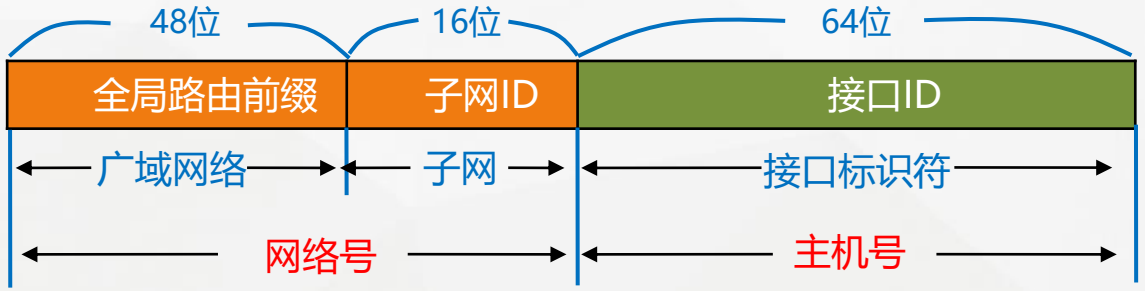
1 全局单播地址

2 唯一本地地址

3 链路本地地址

1 全局单播地址

它是互联网中唯一的一个地址，不需要正式分配IP地址。



接口ID可以由设备随机生成或手动配置。

2. IPV6地址分类

单播地址

01

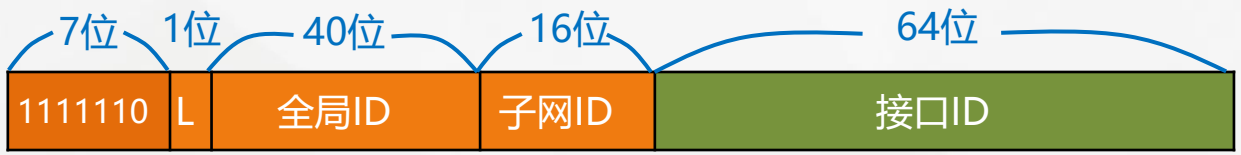
1 全局单播地址

2 唯一本地地址

3 链路本地地址

2 唯一本地地址

不与互联网直接接入的私有网络，可以使用区域唯一本地地址。



唯一本地地址固定前缀为FC00::/7，即前7位为"1111110"

L表示地址的范围，取值为1表示本地范围，0则保留

全局ID全球唯一前缀

子网ID在划分子网时使用

2. IPV6地址分类

单播地址

01

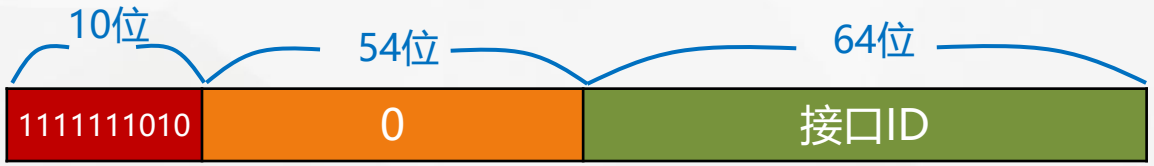
1 全局单播地址

2 唯一本地地址

3 链路本地地址

3 链路本地地址

在同一个以太网网段内进行通信时，可以使用链路本地地址。



链路本地地址使用特定的前缀FE80::/64，接口ID为地址的低64位

在IPv6邻居节点之间的通信协议中广泛使用了该地址，如邻居发现协议、动态路由协议等。

2. IPV6地址分类

单播地址

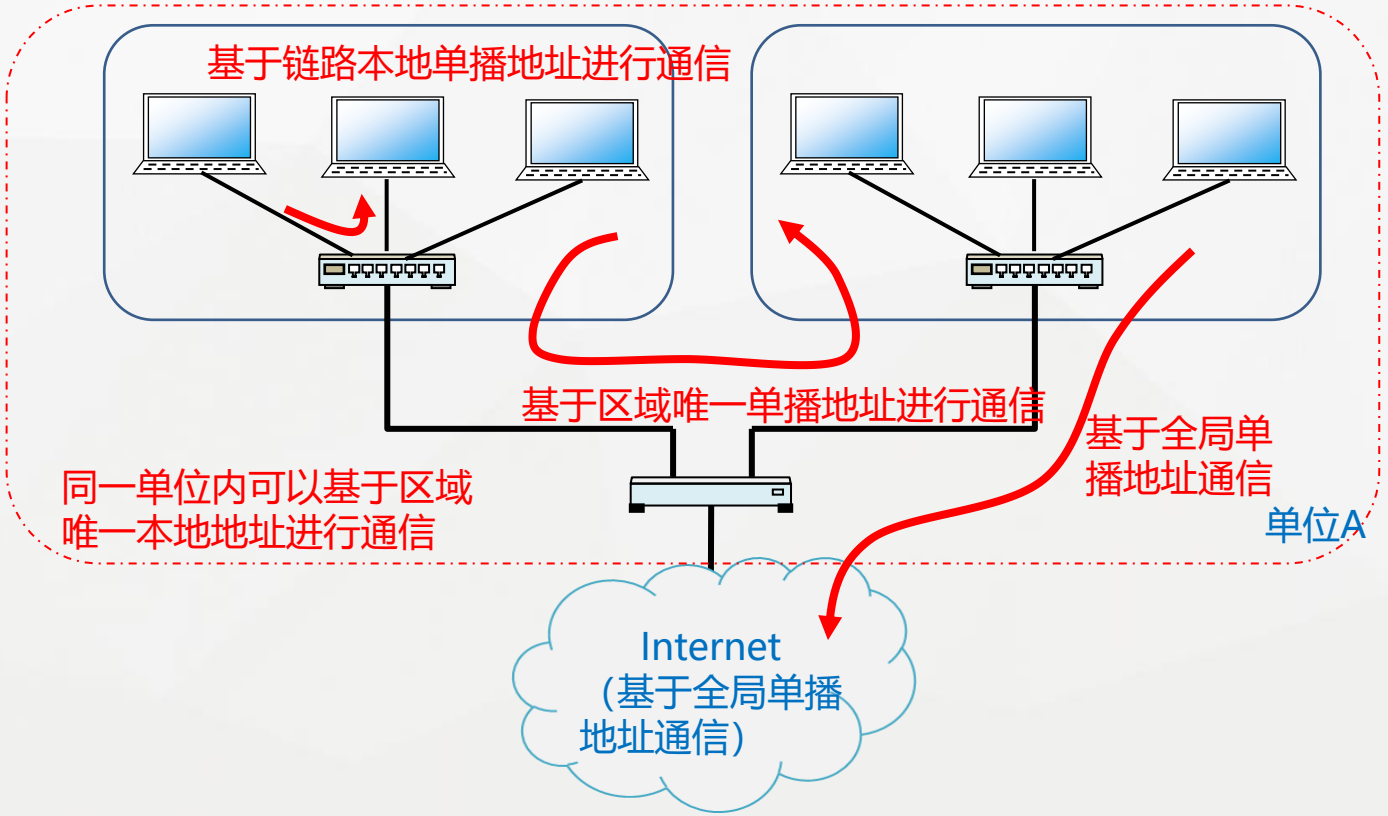
01

1 全局单播地址

2 唯一本地地址

3 链路本地地址

4 使用方式比较



1.用来标识一组接口（通常这组接口属于不同的节点），类似于IPv4的组播地址。

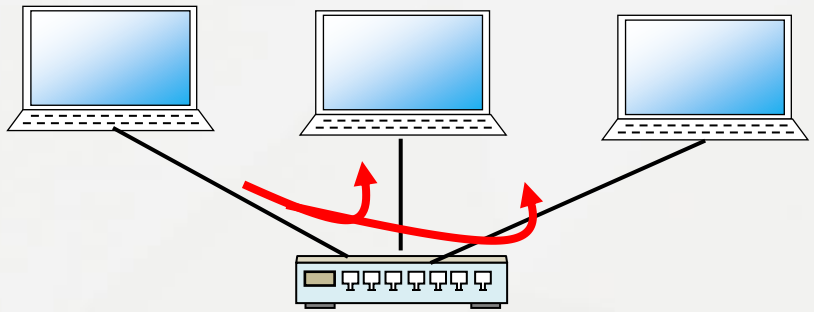
2.任播会有一组接收节点的地址栏表，只会发送给距离最近或发送成本最低的其中一个接收地址

多播地址

03

1.多播地址也称组播地址,用来标识一组接口

2. IPv6中没有广播地址，广播地址的功能通过组播地址来实现。



3. IPV6特殊地址

类型	二进制表示方式	十六进制表示方式
未定义	0000……0000(128位)	：：/128
环回地址	0000……0001(128位)	：：1/128
唯一本地地址	1111 110	FCOO：：/7
链路本地地址	1111 1110 10	FE80：：/10
多播地址	1111 1111	FFOO：：/8

IPv4到IPv6过渡技术

网络基础

目录
Contents

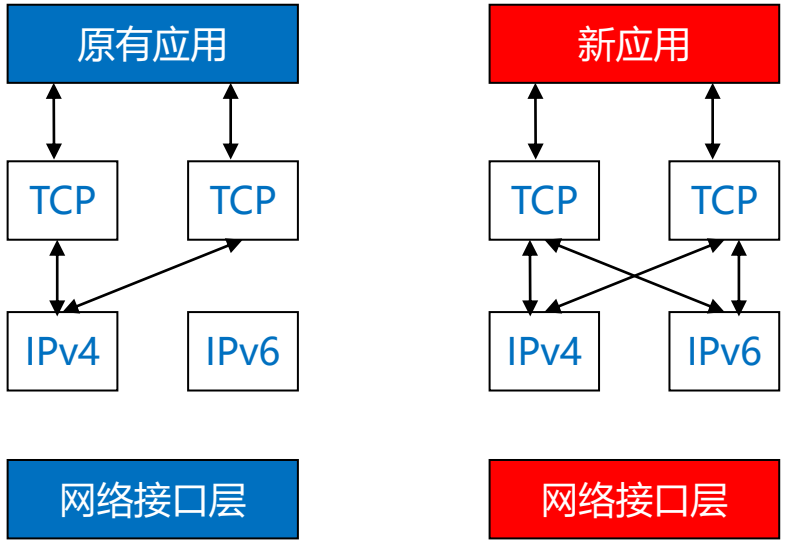
学习目标

- 了解IPv4到IPv6过渡技术

1.双协议栈

双协议栈是一种最直接的过渡机制。

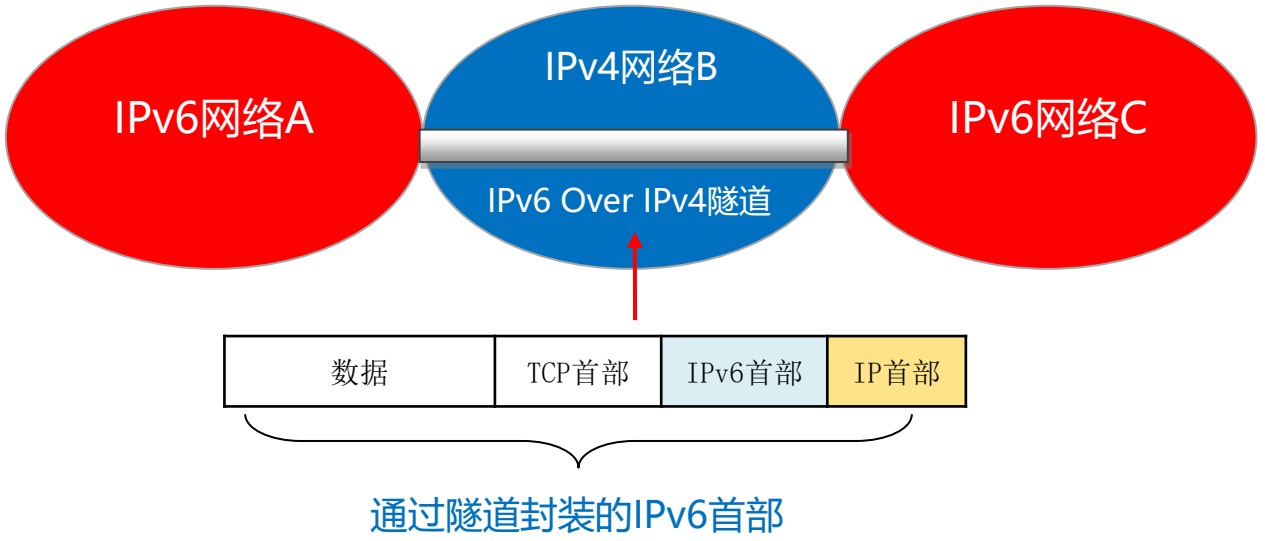
- 该机制在主机或路由器上同时实现IPv4和IPv6两种协议，由此在通过IPv4协议与现有的IPv4网络通信的同时，可以通过IPv6协议与新建的IPv6网络通信。



双协议栈由于需要同时支持IPv4和IPv6两种协议

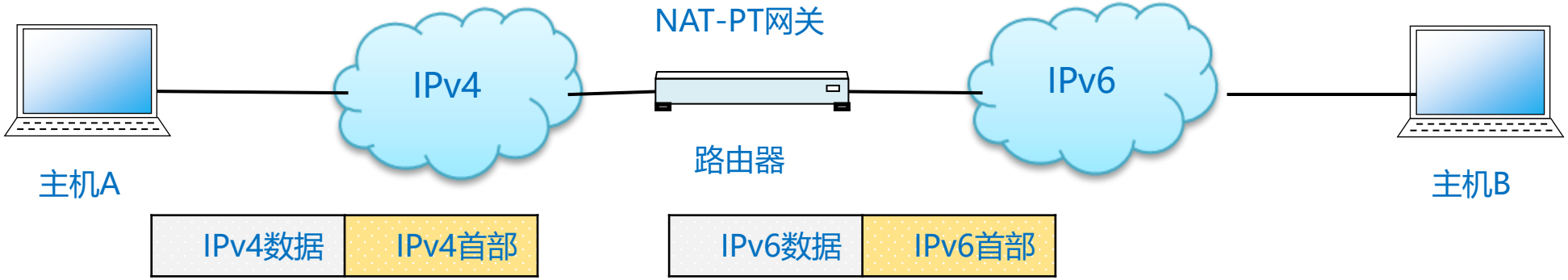
2.隧道技术

保证IPv6报文能够从一个IPv6网络出发，穿过IPv4互联网，到达目的端的IPv6网络



3.协议转换

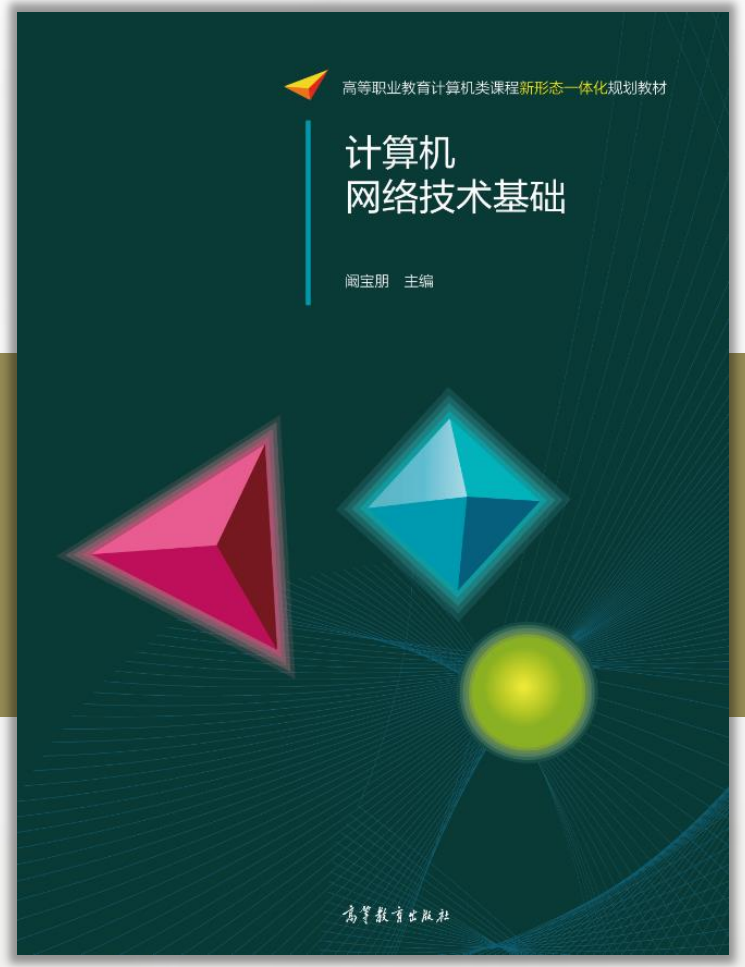
协议转换技术就是一种利用协议转换来实现纯IPv6网络和纯IPv4网络之间互通的方法。



阚宝朋 主编

高等教育出版社
书号：978-7-04-043546-7

高等教育出版社
HIGHER EDUCATION PRESS



新形态一体化教材 配套MOOC课程

计算机网络技术基础

主编 阚宝朋

高等教育出版社
书号：978-7-04-043546-7

扫描教材上二维码 实现随扫随学

高等教育出版社
HIGHER EDUCATION PRESS