

● 无分类域间选路 (CIDR)

- IPv4地址：网络前缀+主机号
- 路由聚合
- 最长网络前缀匹配

● IPv6

- 数据报格式
- 地址：前缀+接口标识
- 地址记法
- 地址类型

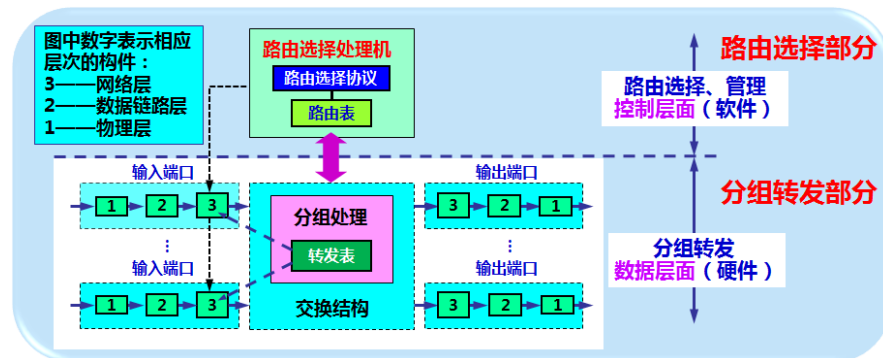
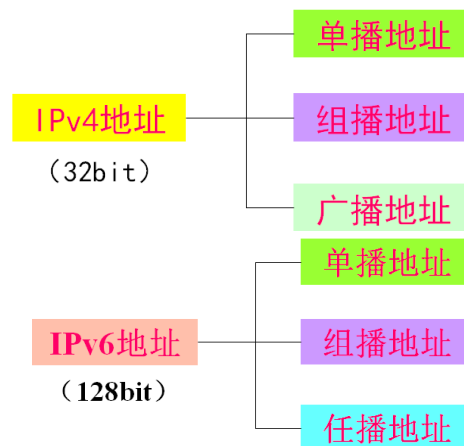
● IP选路

✓ 路由器的结构

- 路由选择处理机
- 分组处理与交换部分

注意：路由选择和转发的区别

✓ netstat命令



IP路由选择的顺序

路由表中的表项具有一定的优先级，按照怎样的顺序进行路由选择呢？



1

主机路由

搜索路由表，寻找能与目的IP地址完全匹配的表目（网络号和主机号都要匹配）。

2

网络路由

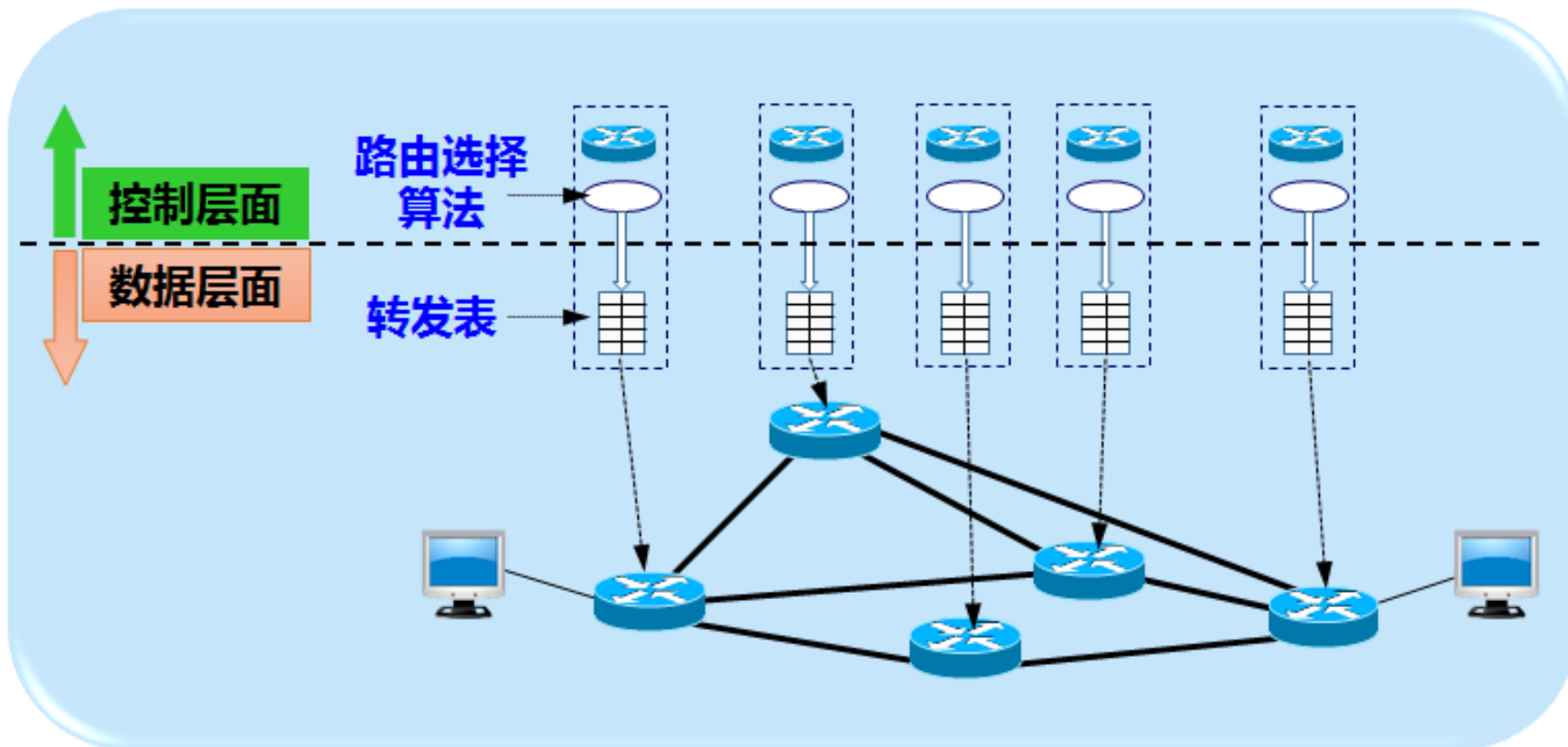
搜索路由表，寻找能与目的网络号相匹配的表目。

3

默认路由

搜索路由表，寻找标为“默认”的表目。

路由选择协议属于网络层控制层面的内容



理想的路由算法

- 路由选择协议的核心是**路由算法**，即需要何种算法来获得路由表中的各条目。



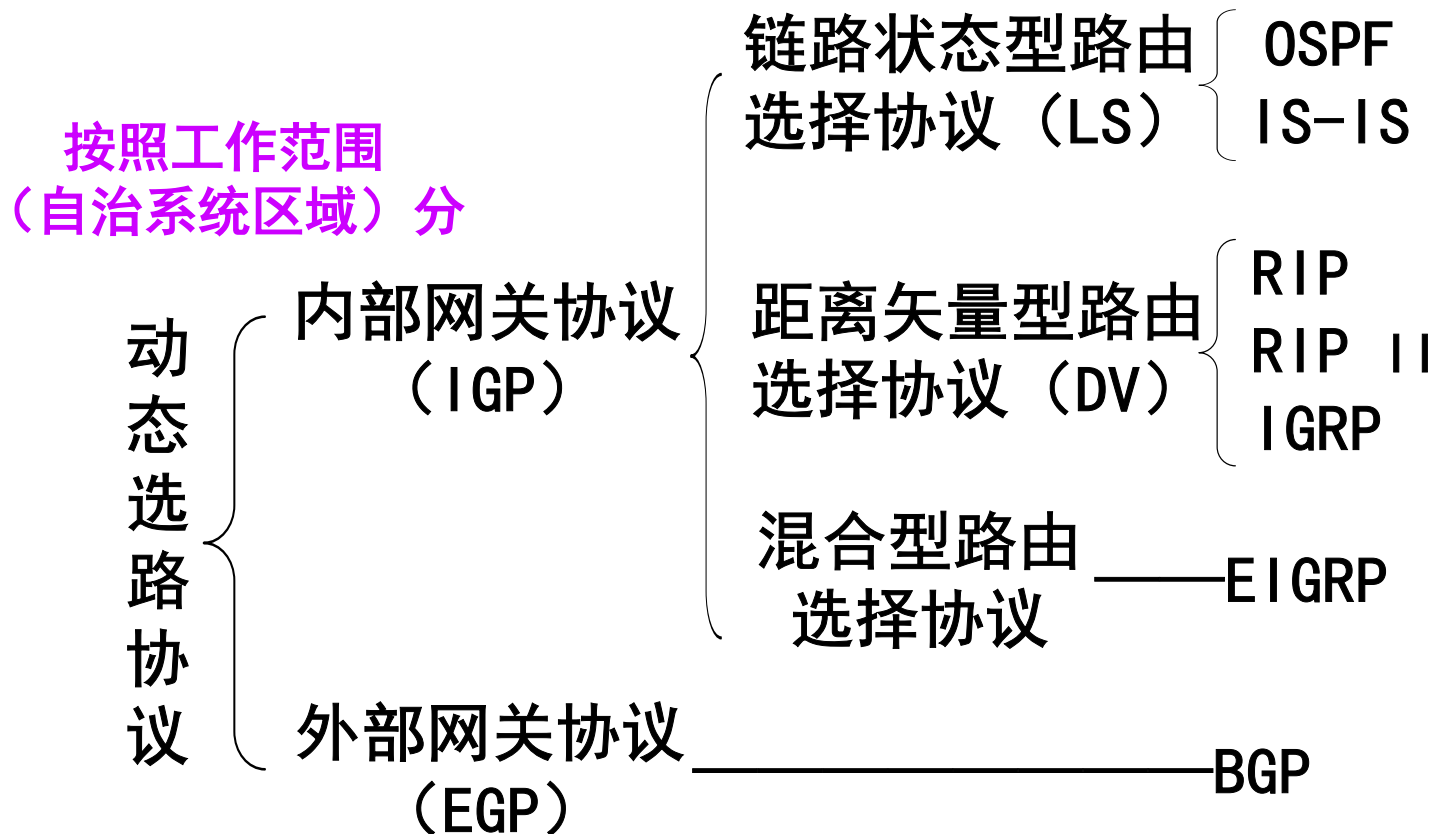
- 关于“最佳路由”
 - 不存在一种绝对的最佳路由算法。
 - 所谓“最佳”只能是相对于某一种特定要求下得出的**较为合理的选择**而已。
- 路由选择是个**非常复杂的问题**
 - 是网络中所有节点**共同协调工作**的结果。
 - 路由选择的**环境往往是不断变化的**，而这种变化有时无法事先知道。

路由算法分类（从自适应性和通信量考虑）

静态路由选择策略	动态路由选择策略
<ul style="list-style-type: none">◆ 非自适应路由选择；◆ 不能及时适应网络状态的变化；◆ 简单，开销较小；◆ 适用于简单的小网络。	<ul style="list-style-type: none">◆ 自适应路由选择；◆ 能较好地适应通信量和网络拓扑的变化；◆ 实现较为复杂，开销较大；◆ 适用于较复杂的网络。

- ⊙ 动态选路协议是动态选路的重要组成部分，用于**路由器之间、相邻路由器之间的通信**。
- ⊙ 路由器上一个名为**路由守护程序**的进程运行选路协议，并与其相邻的一些路由器进行通信，根据从相邻路由器接收到的信息来更新内核中的路由表。

动态选路协议



- **OSPF**(Open Shortest Path First, 开放式最短路径优先) 是对链路状态路由协议的一种实现。著名的迪杰斯特拉 (Dijkstra) 算法被用来计算最短路径树。OSPF支持负载均衡和基于服务类型的选路, 也支持多种路由形式, 如特定主机路由和子网路由等。
- **IS-IS** (Intermediate System-to-Intermediate System , 中间系统到中间系统) 路由协议最初是ISO为CLNP (Connection Less Network Protocol , 无连接网络协议) 设计的一种动态路由协议。
- **RIP** (Routing Information Protocol , 路由信息协议) 是基于距离矢量算法的路由协议, 利用跳数来作为计量标准。RIP2由RIP而来, 属于RIP协议的补充协议, 主要用于扩大 RIP 信息装载的有用信息的数量, 同时增加其安全性能。



- **IGRP** (Interior Gateway Routing Protocol , 内部网关路由协议), 又称为网关间选径协议, 是由Cisco公司发展而成的专利协议, 采用距离向量算法, 以自治系统的方式提供路由选择。其算法与路由信息协议 (RIP) 类似, 延时、带宽、可靠性及负载等均被用于路由选择。默认情况下, IGRP选用路由协议的链路延时和带宽作为度量值, 可靠性及负载只有在路由器上进行人工配置后才能被应用。
- **EIGRP** (Enhanced Interior Gateway Routing Protocol , 增强内部网关路由协议), 也称为加强型内部网关路由协议, 是Cisco公司的私有协议, 结合了链路状态和距离矢量型路由选择, 采用弥散修正算法(DUAL)来实现快速收敛, 可以不发送定期的路由更新信息以减少带宽的占用, 支持Appletalk、IP、Novell和NetWare等多种网络层协议。
- **BGP** (Border Gateway Protocol , 边界网关协议), 是唯一一个用来处理像因特网大小的网络的协议, 也是唯一能够妥善处理好不相关路由域间的多路连接的协议。

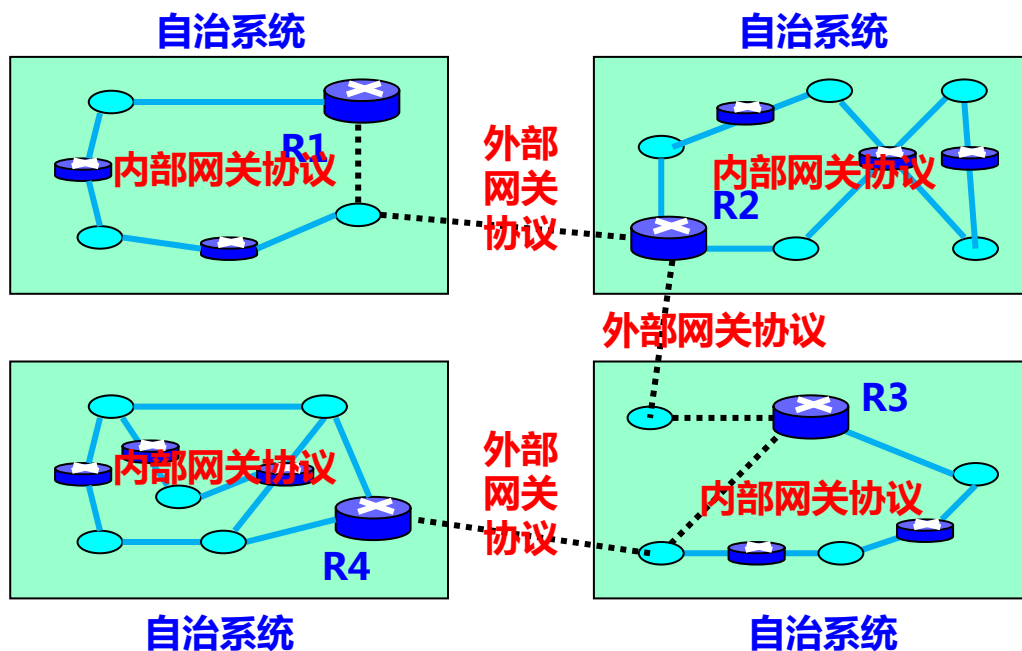


分层的路由选择协议

- 互联网采用自适应的（即动态的）、分布式路由选择协议。
 - 把整个互联网划分为许多较小的**自治系统AS**，采用分层的路由选择协议。
 - 分为 2 个层次：

◆ **域内路由选择**：自治系统内部的路由选择

◆ **域间路由选择**：自治系统之间的路由选择



自治系统 (AS)：处于一个管理机构控制下的路由器和网络群组，有时也称为**路由选择域**。注意：尽管一个 AS 使用了多种内部路由选择协议和度量，但重要的是一个 AS 对其他 AS 表现出的是一个单一的和一致的路由选择策略。

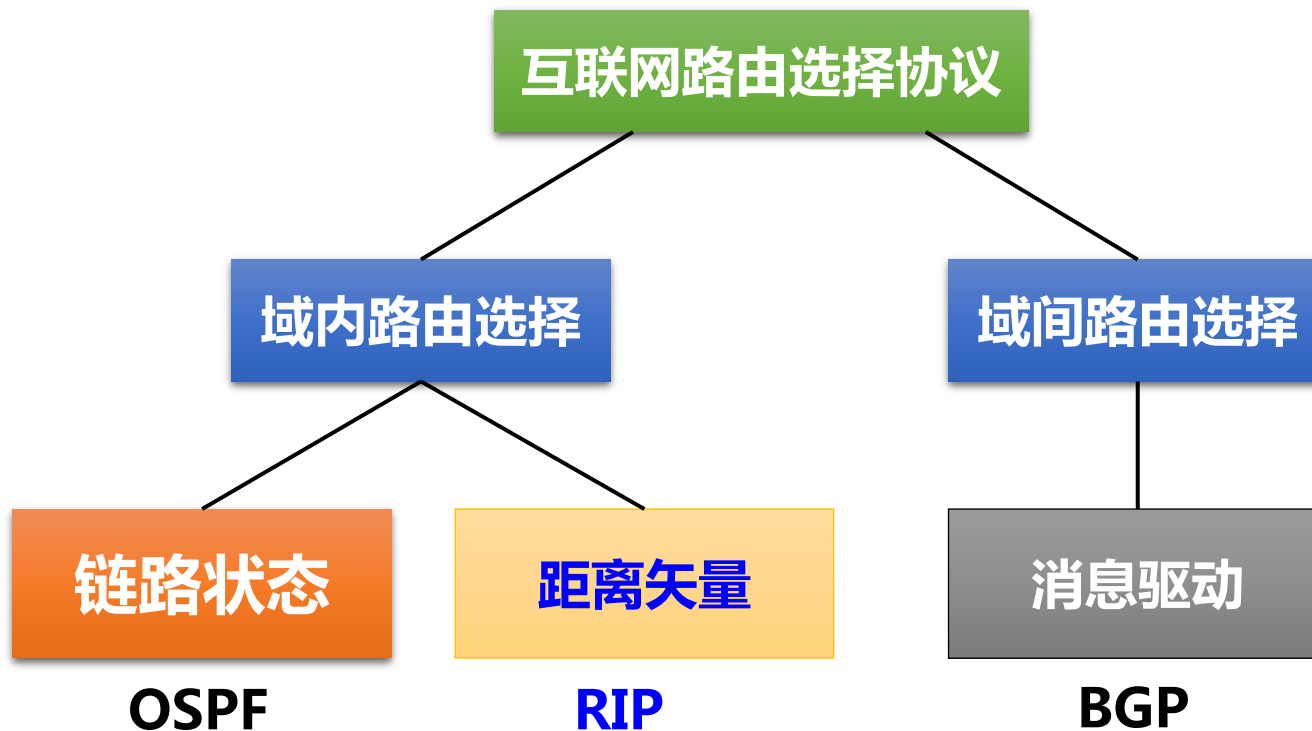
分层的路由选择协议

互联网为什么采用分层的路由选择协议？



- **互联网的规模非常大**。如果让所有的路由器知道所有的网络应该怎样到达，则会使**路由表非常大**，加大了处理时间，而所有这些路由器之间交换路由信息所需的带宽就会使互联网的**通信链路饱和**。
- 许多单位**不愿意外界了解自己单位网络**的布局细节和本部门所采用的路由选择协议（这属于本部门内部的事情），但同时还希望能连接到互联网上。

分层次的路由选择协议

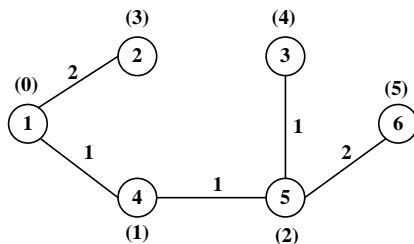
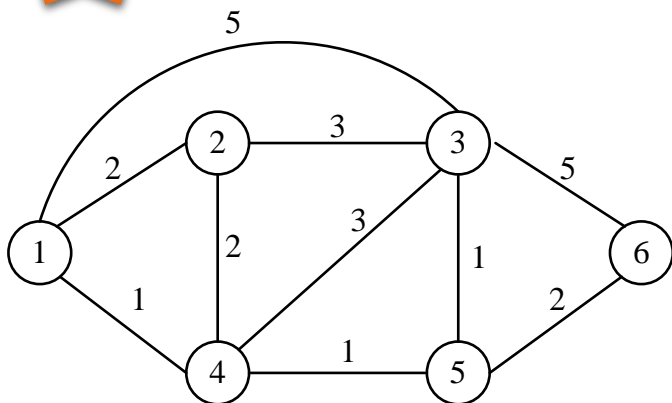


开放最短路径优先（OSPF）协议

- “**开放**”表明 OSPF 协议不是受某一家厂商控制，而是公开发表的。
- “**最短路径优先**”是因为使用了 Dijkstra 提出的最短路径算法 SPF。
- **分布式的链路状态协议** (link state protocol)。
- **注意**：OSPF 只是一个协议的名字，它并不表示其他的路由选择协议不是“最短路径优先”。

例

求源节点1到其他节点的最短路由以及节点1的路由表。



目的节点	下一跳节点
2	2
3	4
4	4
5	4
6	4

开放最短路径优先（OSPF）协议

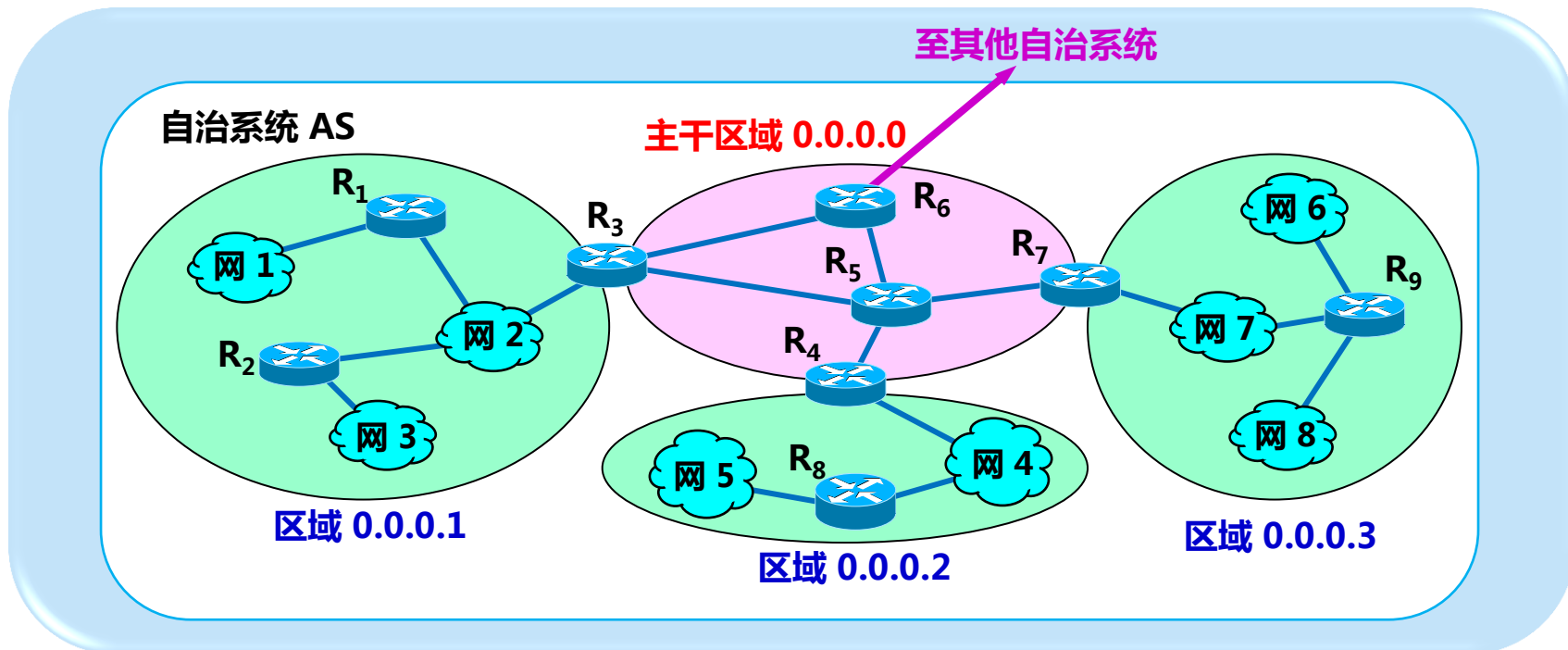
● 三个要点

- **和谁交换信息**：采用**洪泛法**（flooding）向本自治系统中所有路由器发送信息。
- **交换什么信息**：发送的信息是与本路由器**相邻**的所有路由器的**链路状态**，但这只是路由器所知道的**部分信息**。
“链路状态”就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”（费用、距离、时延、带宽等）。
- **何时交换信息**：只有当链路状态**发生变化**时，路由器才用洪泛法向所有路由器发送此信息。

WWW { Who?
What?
When?

开放最短路径优先 (OSPF) 协议 -- 相关概念

- **区域(area)**。为了使 OSPF 能够用于规模很大的网络，OSPF 将一个自治系统划分为两种不同的区域——**主干区域**和**非主干区域**，每一个区域都有一个 **32 位的区域标识符**（用点分十进制表示）。



主干区域标识符：0.0.0.0，**作用**：用来连通其他下层区域。

开放最短路径优先（OSPF）协议协议 -- 相关概念

划分区域的优缺点

优点

- ◆ 将利用洪泛法交换链路状态信息的范围局限于每个区域中，**减少了网络上的通信量**；
- ◆ 一个区域的路由器只保存该区域的链路状态，**减少了需要维护的状态数量**。

缺点

- ◆ 交换信息的种类增多了；
- ◆ 使 OSPF 协议更加复杂了。

开放最短路径优先（OSPF）协议 -- 相关概念

- 相邻路由器

指的是两台通过一条普通链路相连的、可以对话的路由器。

- 相邻关系

指的是两台相邻路由器的双向关系。

注意：是邻居不一定就有相邻关系。

- 链路状态数据库（LSDB）

由于各路由器之间频繁地交换链路状态信息，因此所有的路由器最终都能建立一个LSDB，它实际上是全网的拓扑结构图，在全网范围内是一致的（这称为链路状态数据库的同步）。

- 链路状态广播（LSA）

每台路由器根据自己周围的网络拓扑结构生成LSA，通过相互之间发送协议报文将LSA发送给网络中其他路由器，这样每台路由器都收到了其他路由器的LSA，所有的LSA放在一起便组成了LSDB。

OSPF 使用Dijkstra算法，根据自己的链路状态数据库构造到其他节点的最短路径。

开放最短路径优先（OSPF）协议 -- 报文类型

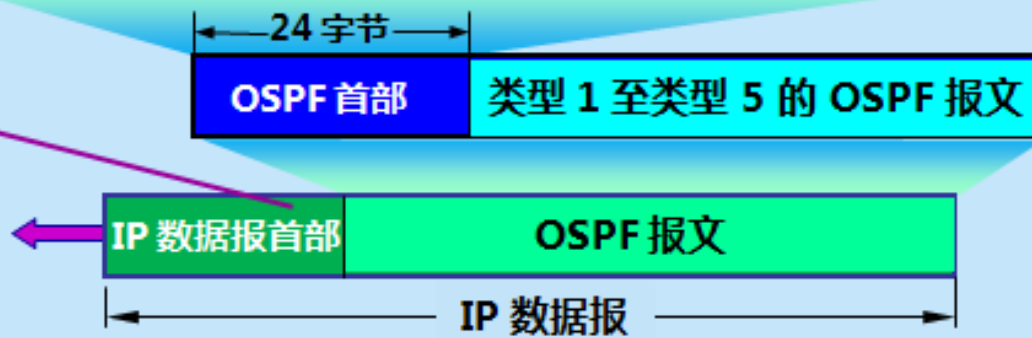
类型	含 义	作 用
1	问候报文 (HELLO)	发现邻居；设置参数：metric、area_id、router_id等；邻居保持
2	数据库描述报文 (DD报文)	向邻居发送链路状态摘要信息
3	链路状态请求报文 (LSR报文)	向邻居请求自己没有的链路状态信息
4	链路状态更新报文 (LSU报文)	用洪泛法对全网更新链路状态
5	链路状态应答报文 (LSAck报文)	向第1个发送更新的路由器发送确认

开放最短路径优先 (OSPF) 协议

- OSPF 协议**直接用IP数据报传送**，OSPF 构成的数据报很**短**，这样做可减少路由信息的通信量，也可以避免分片操作，防止丢失引起重传。

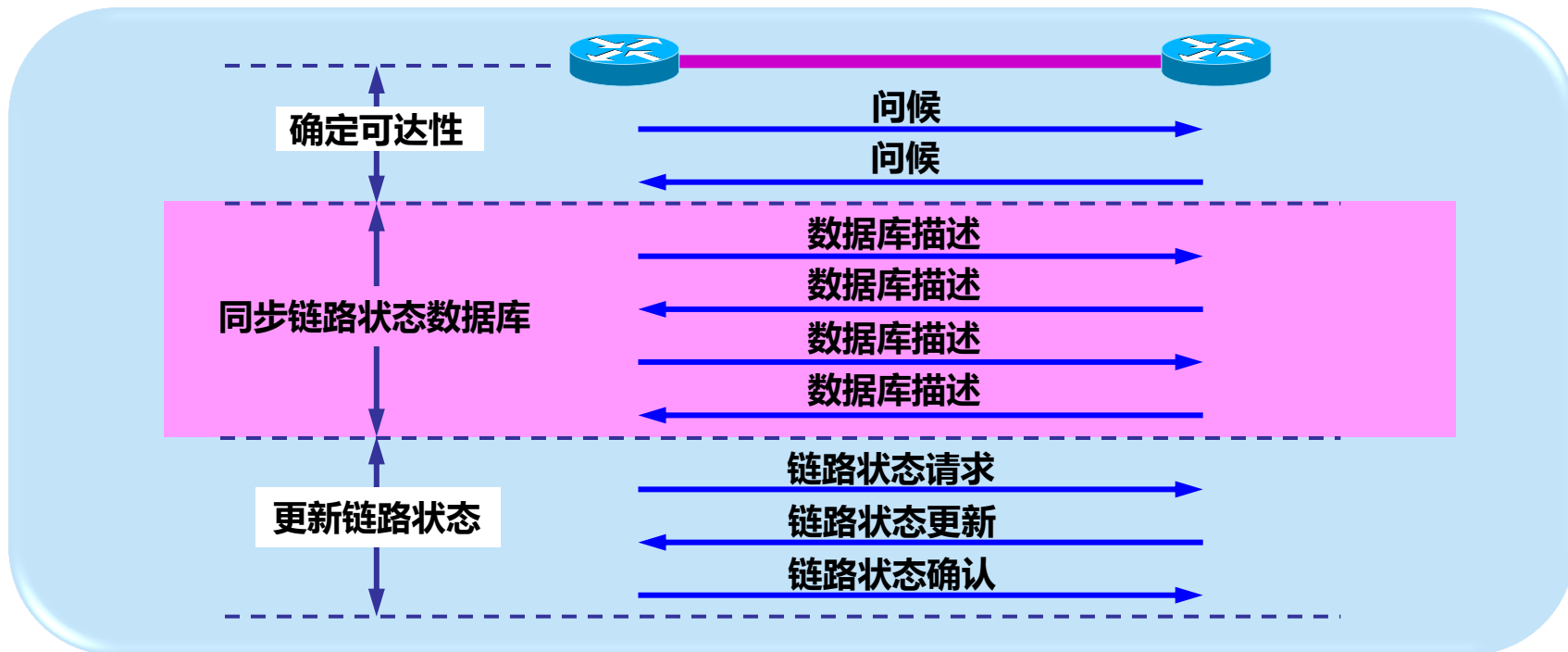


其 IP 数据报首部的协议字段值为 89



开放最短路径优先 (OSPF) 协议

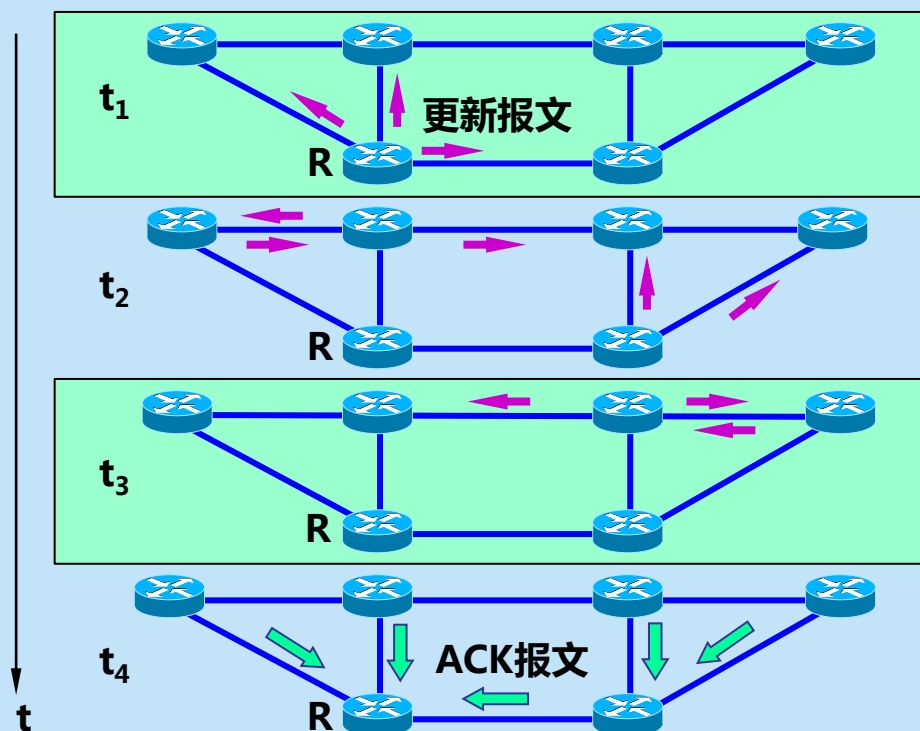
● 基本操作

**OSPF规定:**

- ◆两个相邻路由器每隔10s交换一次Hello报文，确认相邻路由器是“可达”的。
- ◆若40s没收到Hello报文，则认为该路由器不可达，立即修改LSDB，并重新计算路由表。
- ◆每隔一段时间（如30min），路由器刷新一次数据库中的链路状态。

开放最短路径优先 (OSPF) 协议

- OSPF使用**可靠的洪泛法**发送更新分组；
- 向最早向外发送LSA的路由器发送确认。



ICMP 设计的必要性

- **IP**提供**无连接、尽力而为**的数据报传送服务，**没有提供**检验或跟踪机制，**不能解决**网络低层的数据报丢失、重复、延迟或乱序等问题。
- **TCP**在IP基础上建立**面向连接服务**解决以上问题，但**不能解决**因网络故障或其他网络原因而无法传输数据报的问题。
- **ICMP**设计的**本意**就是希望在IP数据报无法进行传输时**提供报告**，这些差错报告能够帮助发送端了解数据报为什么无法传递，网络发生了什么问题，以确定应用程序后续的操作。



ICMP 的重要性

- **ICMP**是**TCP/IP**协议族的一个**子协议**，属于**网络层协议**，主要用于在主机与路由器之间传递**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**。这些控制消息虽然并不传输用户数据，但是对于用户**数据的传递**和**网络安全**具有极其重要的意义。

例

海信集团悬赏50万人民币测试防火墙。

攻击类型	攻击次数
ICMP攻击	334050
碎片攻击	25524
端口扫描	4365
WEB服务攻击	1227
UDP攻击	234

ICMP 的重要性

“Ping of Death” 攻击的原理

拒绝服务攻击 (DoS)

- 攻击者故意发送长度超过65535字节的ICMP数据包，导致内存溢出，这时主机就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。

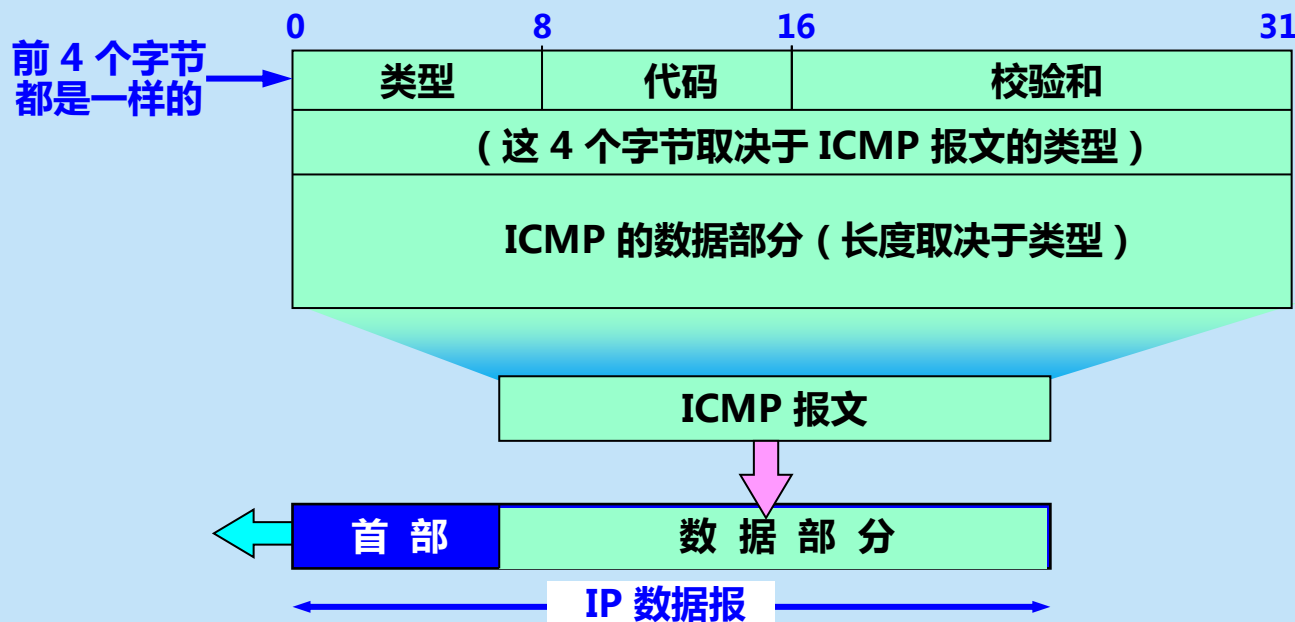
常见的ICMP网络攻击手段

- 利用ICMP echo 数据包进行 DoS(Denial of Service)攻击
- 利用ICMP重定向报文进行IP欺骗与窃听
- 利用ICMP隧道机制绕过防火墙进行信息获取和远程控制



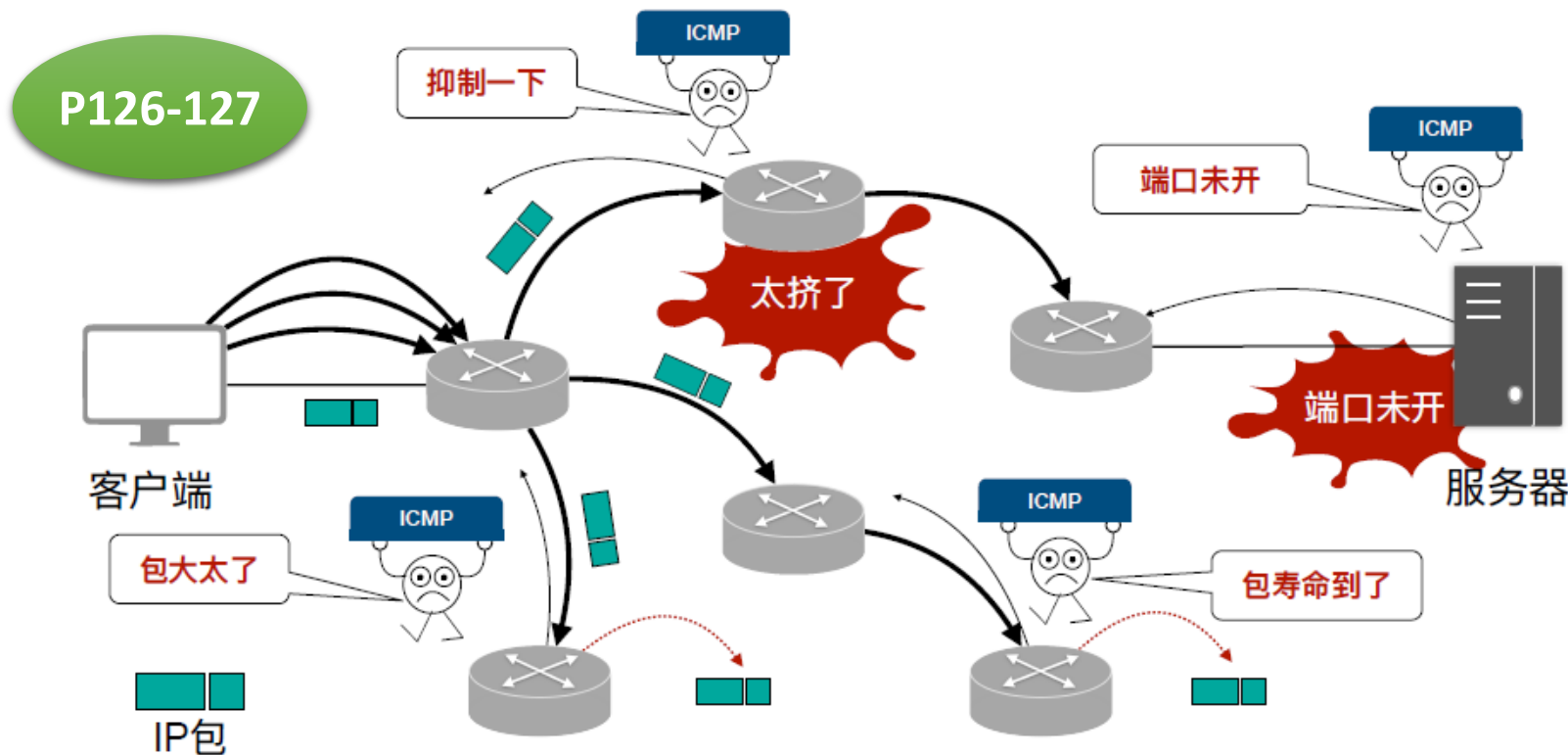
ICMP 报文格式

- ICMP 报文的前 4 个字节是**统一**的格式，共有三个字段：**类型**、**代码**和**校验和**。接着的 4 个字节的内容与 ICMP 的**类型**有关。



ICMP 报文类型

- **差错报文**：反馈路由器或目的主机处理IP数据报时遇到的问题，如目的不可达、源站抑制、超时、参数问题、重定向等。
- **查询报文**：帮助网络管理员从一个路由器或主机得到特定信息，如回显请求/应答报文，时间戳请求/应答报文，地址掩码请求/应答报文。



ICMP 报文类型

- ICMP差错报文弥补了IP协议的不可靠问题
 - 发现错误的设备**只向源主机报告差错**。
 - **只报告差错**，但不负责纠正错误，纠错工作留给高层协议去处理；
 - 差错报文作为一般数据传输，不享受特别的优先级和可靠性。
 - 产生ICMP差错报文的同时会丢弃出错的IP数据报。
- 不应发送ICMP差错报告报文的几种情况
 - ICMP差错报文本身不会再产生ICMP差错报文
 - 广播或组播地址的数据报不会产生ICMP差错报文
 - 分片的IP数据报的非第一个分片不会产生ICMP差错报文
 - 特殊地址0.0.0.0和127.0.0.1的报文不会产生ICMP差错报文

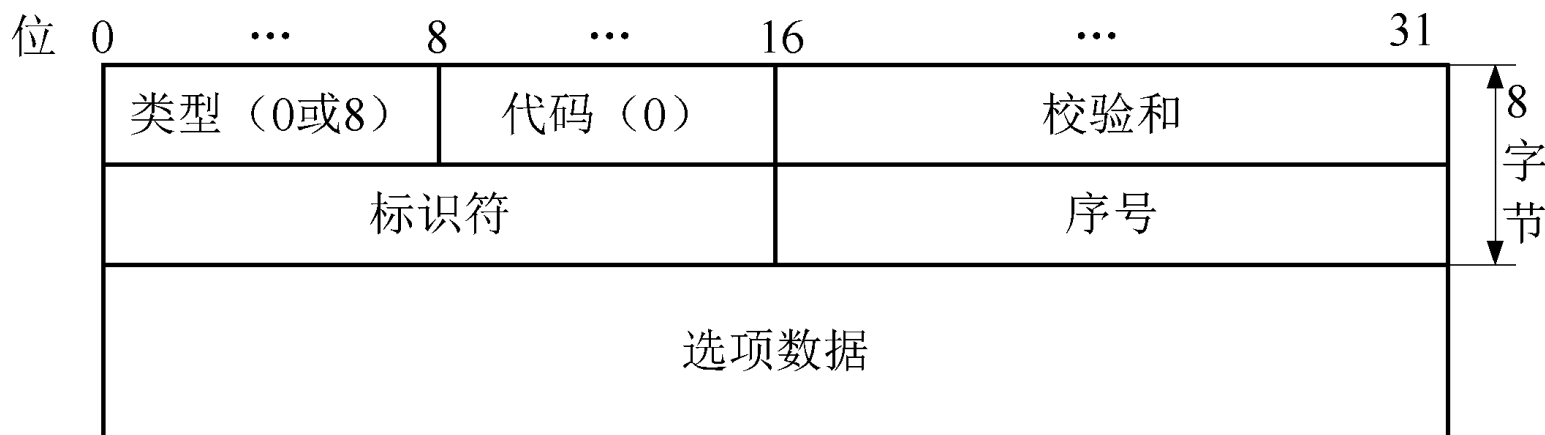


ICMP的两种典型应用

- Ping程序
- Traceroute (Tracert) 程序

Ping程序

- **作用**：侦测另一台主机是否可达。
- **原理**：使用 ICMP **回显请求/应答报文**。发送一个类型字段为 8 的 ICMP 回显请求报文给主机，收到请求的主机则返回类型字段为 0 的 ICMP 回显应答报文。
- Ping 是应用层直接使用网络层 ICMP 的例子，没有通过运输层的 TCP 或 UDP。



Ping命令

如何利用 *ping* 命令检查网络的连通状态呢？

网络故障的判断

- ❑ 网卡安装是否正确？
- ❑ TCP/IP协议配置是否正确？
- ❑ 是否与邻居计算机连接正常（线路）？
- ❑ 是否与路由器连接正常？
- ❑ 是否与DNS服务器连接正常？
- ❑ 网络是否堵塞？





Ping命令

- ping 127.0.0.1检查本地的TCP/IP协议是否运行正常



```
管理员: C:\Windows\system32\cmd.exe

C:\Users>wanglina>ping 127.0.0.1

正在 Ping 127.0.0.1 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64

127.0.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```



Ping命令

- ping本机IP地址，检查本机的IP地址设置和网卡安装配置是否有误。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\wanglina>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    IPv6 地址 . . . . . : 2001:da8:208:166:99c:d0f1:97b8:dec3
    临时 IPv6 地址 . . . . . : 2001:da8:208:166:d058:68bc:ae51:1d7b
    本地链接 IPv6 地址 . . . . . : fe80::99c:d0f1:97b8:dec3%11
    IPv4 地址 . . . . . : 202.204.54.43
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : fe80::223:89ff:fe27:73b9%11
                        202.204.54.1

隧道适配器 isatap.{5F3259F6-096F-4CFC-AF63-A895FF6D9C9F}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

    连接特定的 DNS 后缀 . . . . . :
```



Ping命令

- ping本机IP地址，检查本机的IP地址设置和网卡安装配置是否有误。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\wanglina>ping 202.204.54.43

正在 Ping 202.204.54.43 具有 32 字节的数据:
来自 202.204.54.43 的回复: 字节=32 时间<1ms TTL=64
来自 202.204.54.43 的回复: 字节=32 时间<1ms TTL=64
来自 202.204.54.43 的回复: 字节=32 时间<1ms TTL=64
来自 202.204.54.43 的回复: 字节=32 时间<1ms TTL=64

202.204.54.43 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```




Ping命令

- ping本网网关或本网IP地址，检查硬件设备是否有问题，也可以检查本机与本地网络连接是否正常。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users>wanglina>ping 202.204.54.1

正在 Ping 202.204.54.1 具有 32 字节的数据:
来自 202.204.54.1 的回复: 字节=32 时间=1ms TTL=255
来自 202.204.54.1 的回复: 字节=32 时间=1ms TTL=255
来自 202.204.54.1 的回复: 字节=32 时间=3ms TTL=255
来自 202.204.54.1 的回复: 字节=32 时间=1ms TTL=255

202.204.54.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```

Ping命令

- ping远程IP地址，检查本网或本机与外部的连接是否正常。

C:\Windows\system32\cmd.exe

C:\Users\dell>ping sina.com.cn

正在 Ping sina.com.cn [202.108.33.60] 具有 32 字节的数据:

来自 202.108.33.60 的回复: 字节=32 时间=8ms TTL=249

来自 202.108.33.60 的回复: 字节=32 时间=4ms TTL=249

来自 202.108.33.60 的回复: 字节=32 时间=4ms TTL=249

来自 202.108.33.60 的回复: 字节=32 时间=18ms TTL=249

202.108.33.60 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):

最短 = 4ms, 最长 = 18ms, 平均 = 8ms

Ping命令

- Ping的返回信息--Request Timed Out
 - Ping的返回信息--Destination Host Unreachable
- 如果所经过的路由器的路由表中具有到达目标主机的路由，而目标主机因为其他原因不可达，这时会出现“Request timed out”。
 - 对方已关机，或者网络上根本没有这个地址。
 - 对方与自己不在同一网段内，通过路由器也无法找到对方。
 - 对方确实存在，但设置了ICMP数据包过滤（如防火墙）。
 - 错误设置IP地址
 - 如果路由表中没有连到目标主机的路由，那么就会出现“Destination Host Unreachable”。
 - 对方与自己不在同一网段内，而自己又未设置默认路由。
 - 网线出了故障

Ping命令

```
C:\Users\dell>ping/?
```

```
用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

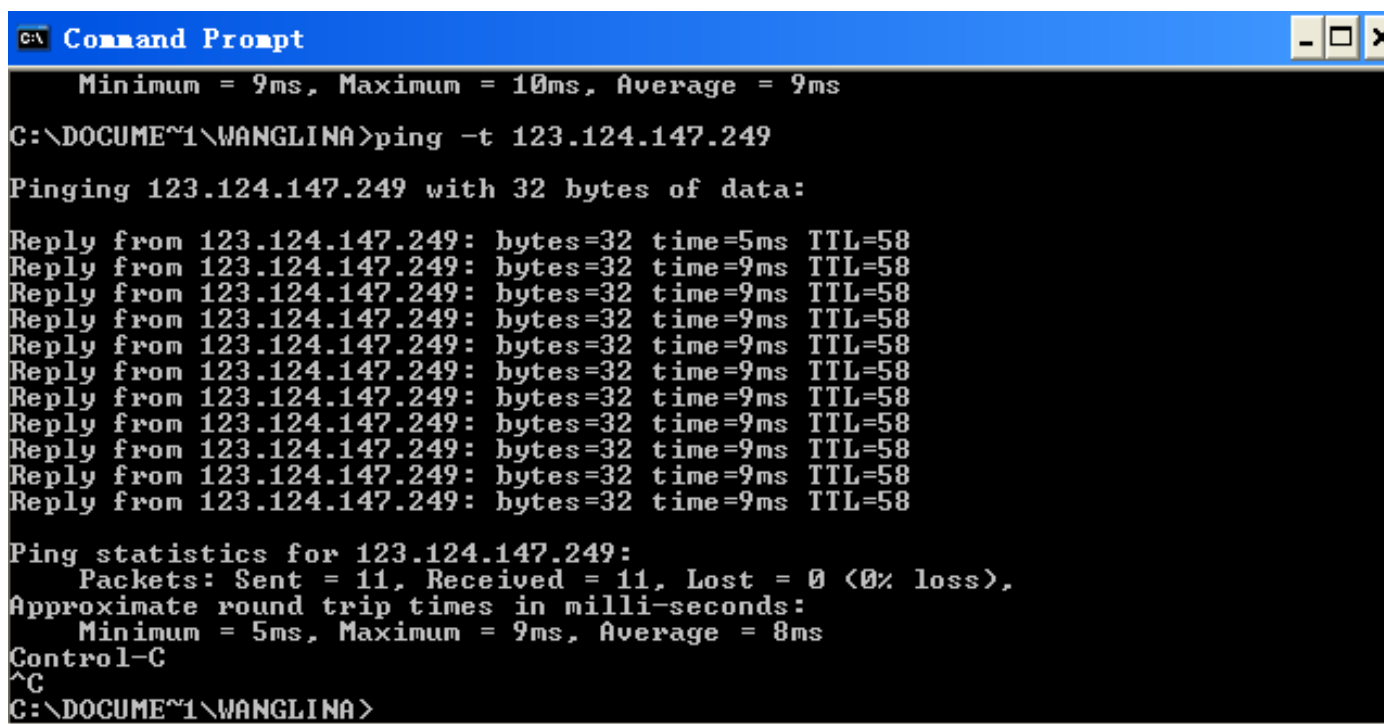
选项:

-t	Ping 指定的主机，直到停止。 若要查看统计信息并继续操作 - 请键入 Control-Break ; 若要停止 - 请键入 Control-C 。
-a	将地址解析成主机名。
-n count	要发送的回显请求数。
-l size	发送缓冲区大小。
-f	在数据包中设置“不分段”标志(仅适用于 IPv4)。
-i TTL	生存时间。
-v TOS	服务类型(仅适用于 IPv4。该设置已不赞成使用，且对 IP 标头中的服务字段类型没有任何影响)。
-r count	记录计数跃点的路由(仅适用于 IPv4)。
-s count	计数跃点的时间戳(仅适用于 IPv4)。
-j host-list	与主机列表一起的松散源路由(仅适用于 IPv4)。
-k host-list	与主机列表一起的严格源路由(仅适用于 IPv4)。
-w timeout	等待每次回复的超时时间(毫秒)。
-R	同样使用路由标头测试反向路由(仅适用于 IPv6)。
-S srcaddr	要使用的源地址。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

Ping命令

Ping命令参数

-t	不停地ping对方主机，直到你按下Ctrl-C。
----	--------------------------

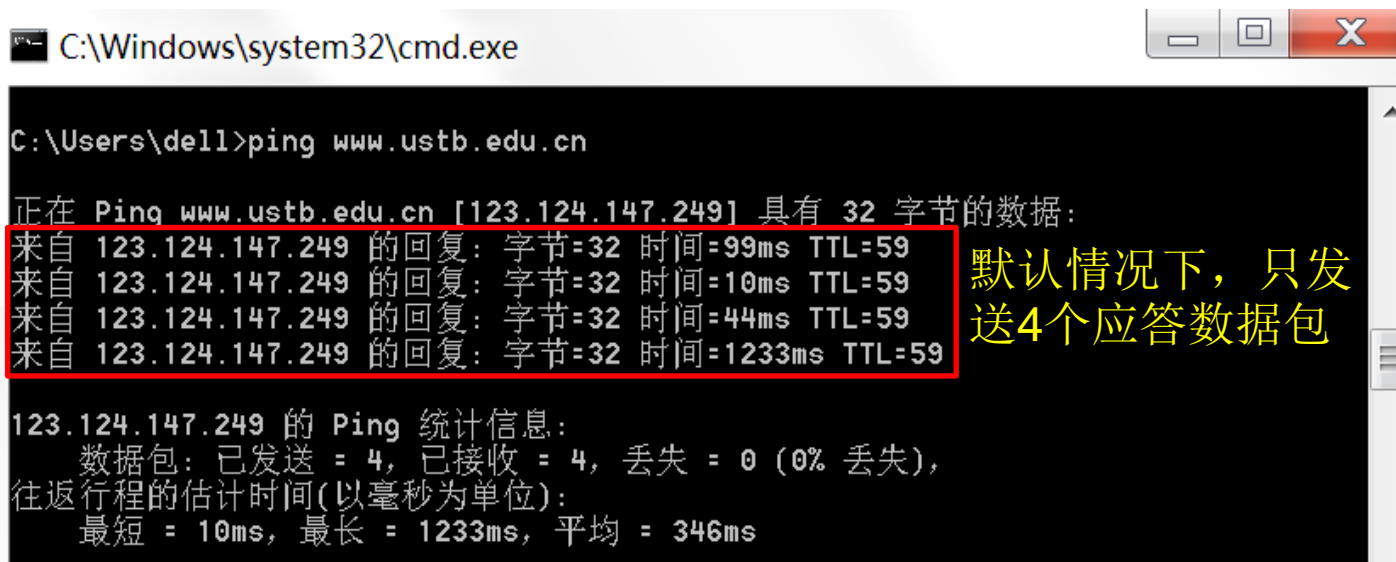


```
C:\ Command Prompt
Minimum = 9ms, Maximum = 10ms, Average = 9ms
C:\DOCUME~1\WANGLINA>ping -t 123.124.147.249
Pinging 123.124.147.249 with 32 bytes of data:
Reply from 123.124.147.249: bytes=32 time=5ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Ping statistics for 123.124.147.249:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 9ms, Average = 8ms
Control-C
^C
C:\DOCUME~1\WANGLINA>
```

Ping命令

Ping命令参数

-n count	发送count指定的Echo数据包数。
-----------------	---------------------



The screenshot shows a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The user has entered the command "ping www.ustb.edu.cn". The output shows four successful replies from 123.124.147.249, each with 32 bytes of data. A red box highlights these four lines of output. To the right of the red box, yellow text states: "默认情况下，只发送4个应答数据包". Below the ping output, the statistics for the ping are displayed: "123.124.147.249 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 10ms, 最长 = 1233ms, 平均 = 346ms".

```
C:\Windows\system32\cmd.exe

C:\Users\dell>ping www.ustb.edu.cn

正在 Ping www.ustb.edu.cn [123.124.147.249] 具有 32 字节的数据:
来自 123.124.147.249 的回复: 字节=32 时间=99ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=10ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=44ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=1233ms TTL=59

123.124.147.249 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 10ms, 最长 = 1233ms, 平均 = 346ms
```



Ping命令

- `ping -n 50 www.ustb.edu.cn`

```
C:\Windows\system32\cmd.exe

来自 123.124.147.249 的回复: 字节=32 时间=11ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=17ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=19ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=41ms TTL=59
请求超时。
来自 123.124.147.249 的回复: 字节=32 时间=23ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=14ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=9ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=8ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=7ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=9ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=14ms TTL=59
请求超时。
来自 123.124.147.249 的回复: 字节=32 时间=20ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=13ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=19ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=10ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=7ms TTL=59
来自 123.124.147.249 的回复: 字节=32 时间=6ms TTL=59

123.124.147.249 的 Ping 统计信息:
    数据包: 已发送 = 50, 已接收 = 44, 丢失 = 6 (12% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 6ms, 最长 = 141ms, 平均 = 15ms
```



Ping命令

- **ping -n 50 www.ustb.edu.cn**

```

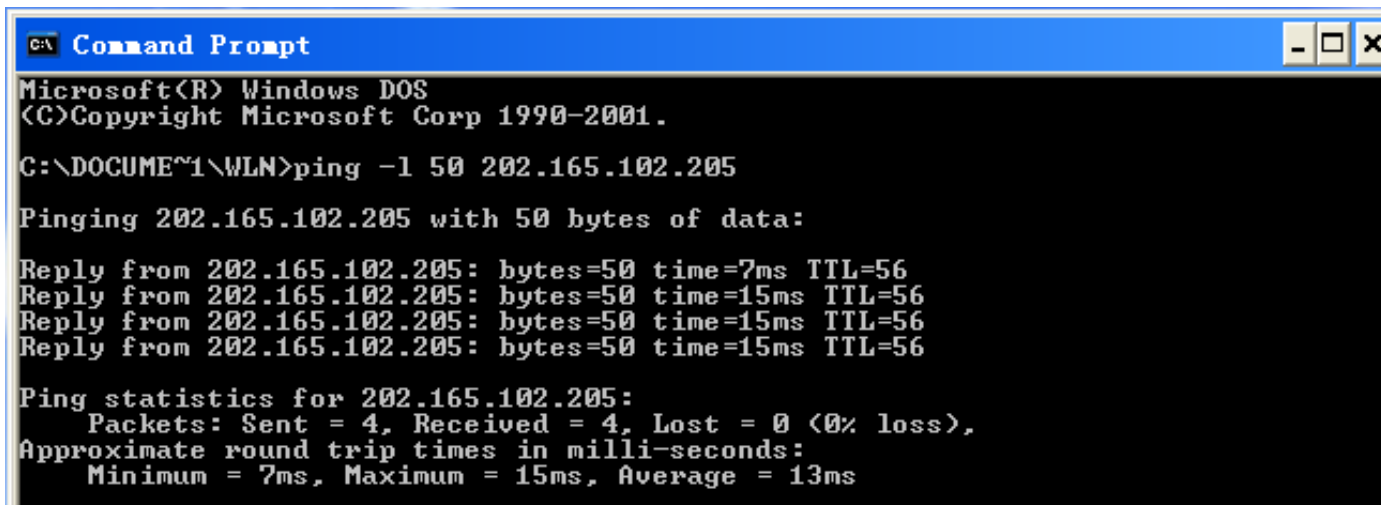
C:\ Command Prompt
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=11ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Reply from 123.124.147.249: bytes=32 time=9ms TTL=58
Ping statistics for 123.124.147.249:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 11ms, Average = 8ms
C:\DOCUMENT1\WANGLINA>

```


Ping命令

Ping命令参数

-l size	定义echo数据包大小
---------	-------------



```
C:\ Command Prompt
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUME~1\WLN>ping -l 50 202.165.102.205
Pinging 202.165.102.205 with 50 bytes of data:
Reply from 202.165.102.205: bytes=50 time=7ms TTL=56
Reply from 202.165.102.205: bytes=50 time=15ms TTL=56
Reply from 202.165.102.205: bytes=50 time=15ms TTL=56
Reply from 202.165.102.205: bytes=50 time=15ms TTL=56
Ping statistics for 202.165.102.205:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 15ms, Average = 13ms
```

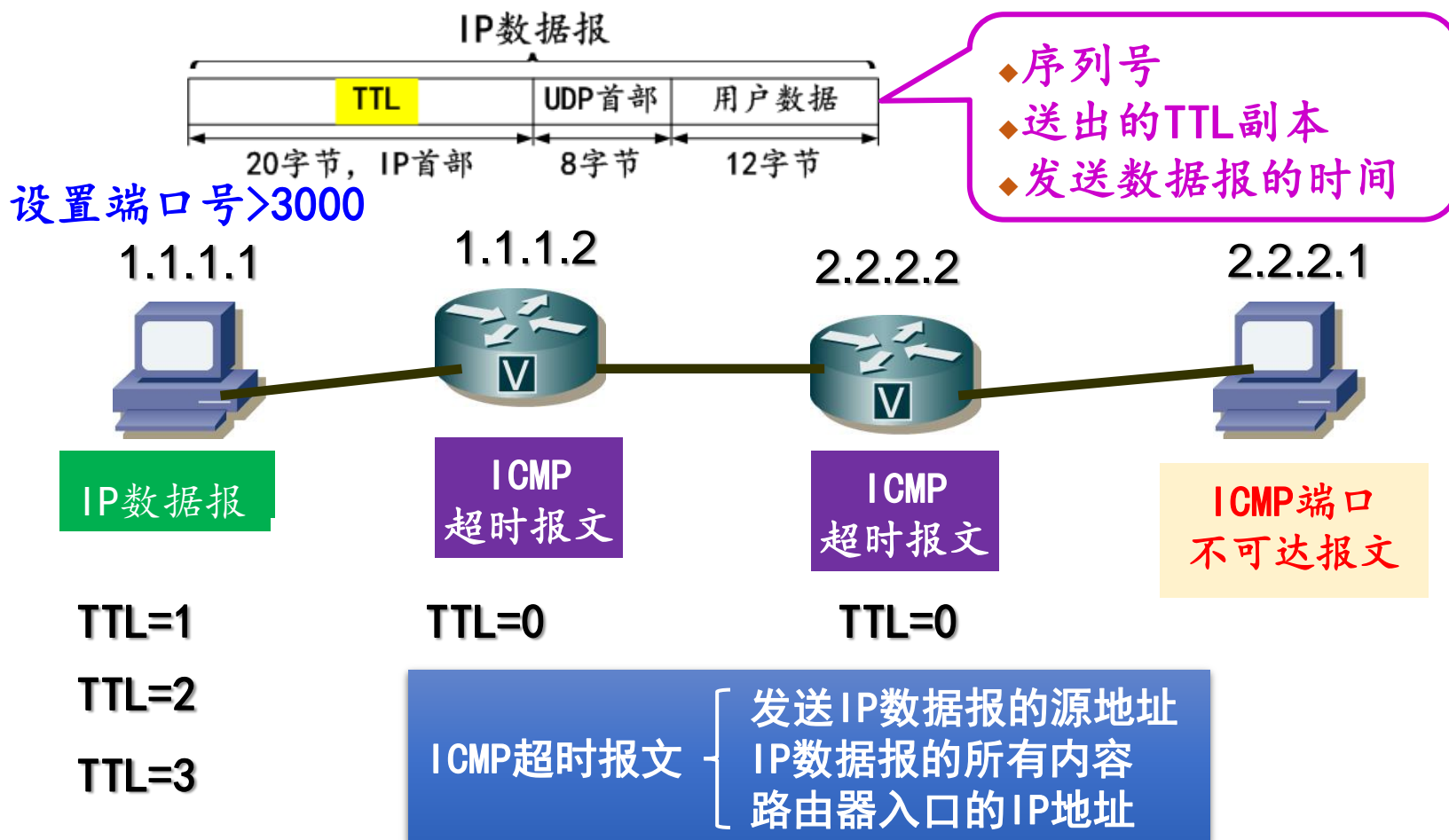
C:\>ping -l 65500 -t ip_address

traceroute (tracert) 程序

- UNIX系统 : **traceroute**
- Windows系统 : **tracert**
- 对路由信息进行**跟踪** , 显示IP数据报从本地主机到目的主机所经过的路径。

traceroute (tracert) 程序

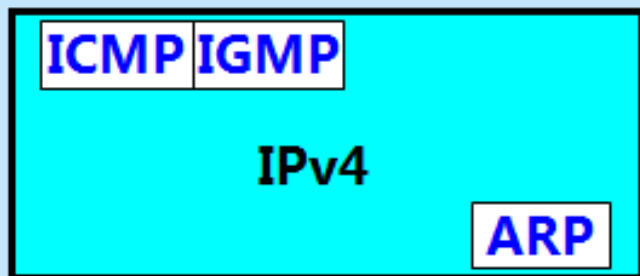
- **traceroute (tracert)** 命令用 IP 首部中的**生存时间 (TTL)** 字段和 **ICMP 差错报文** 来确定从一个主机到网络上其他主机所经过的路由。



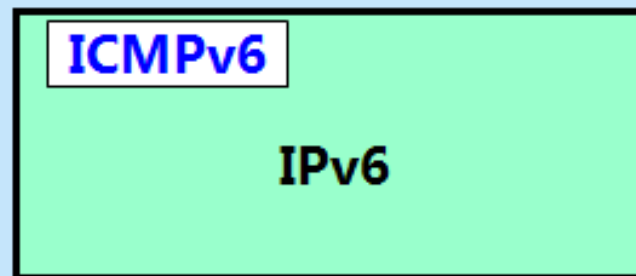
ICMPv6

- ICMPv6 是面向报文的协议，用来报告差错，获取信息，探测邻站或管理多播通信。
 - 比 ICMPv4 复杂；
 - ARP 和 IGMP 的功能合并到 ICMPv6 中；
 - 增加了对移动IPv6的支持。
- 报文类型：差错报文，信息报文。

P129-130



IPv4 的网络层



IPv6 的网络层

为什么有MPLS？

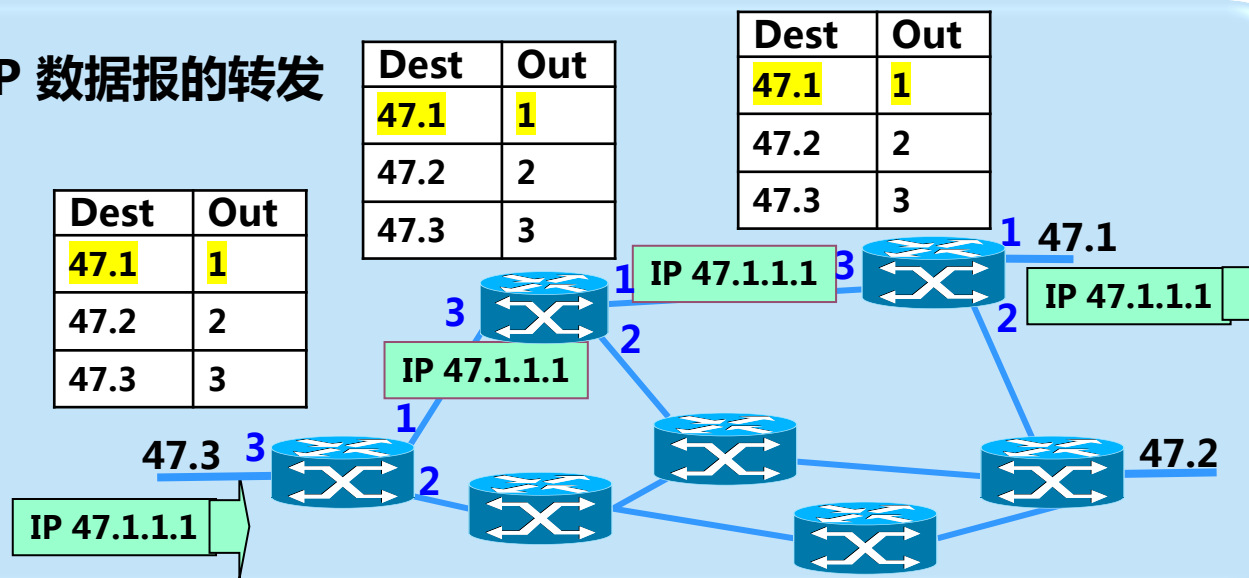
● 三层“转发” (forwarding)

- 需要解封，获取三层地址（软件实现，速度慢）；
- 当网络很大时，查找含有大量项目的路由表要花费很多的时间；
- 获取下一跳硬件地址，封装成帧后发送至下一跳（硬件实现，速度快）。

● 二层交换 (switch)

- **直接使用硬件转发（速度快）**

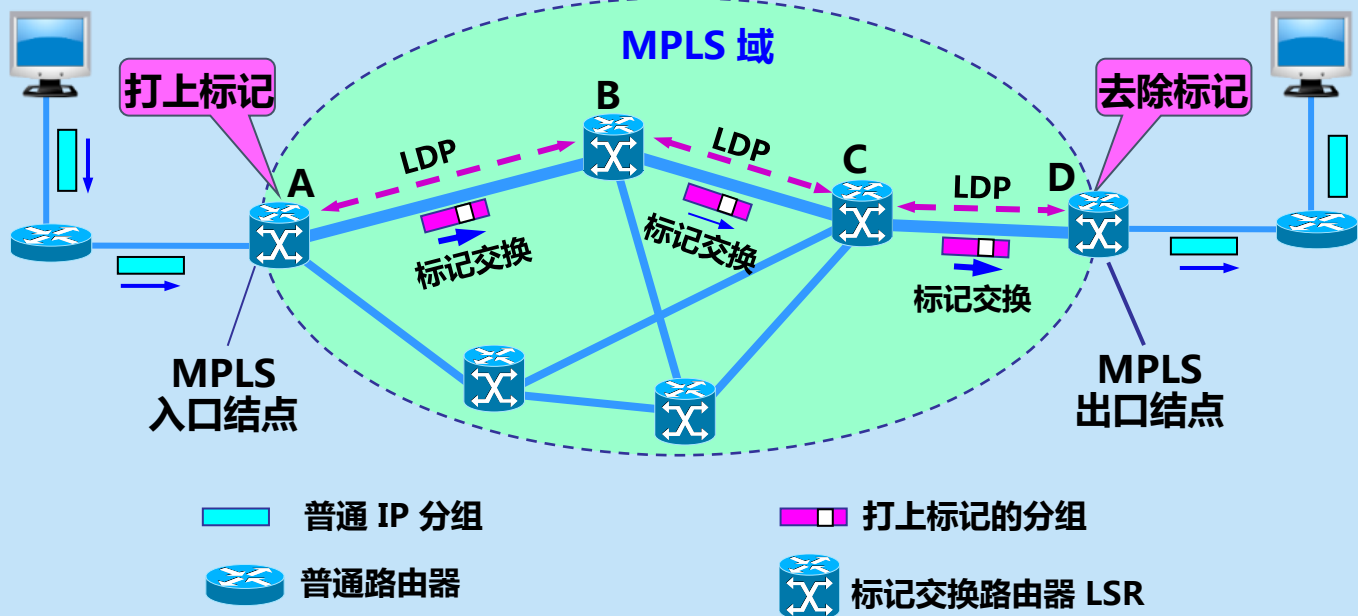
传统 IP 数据报的转发



MPLS

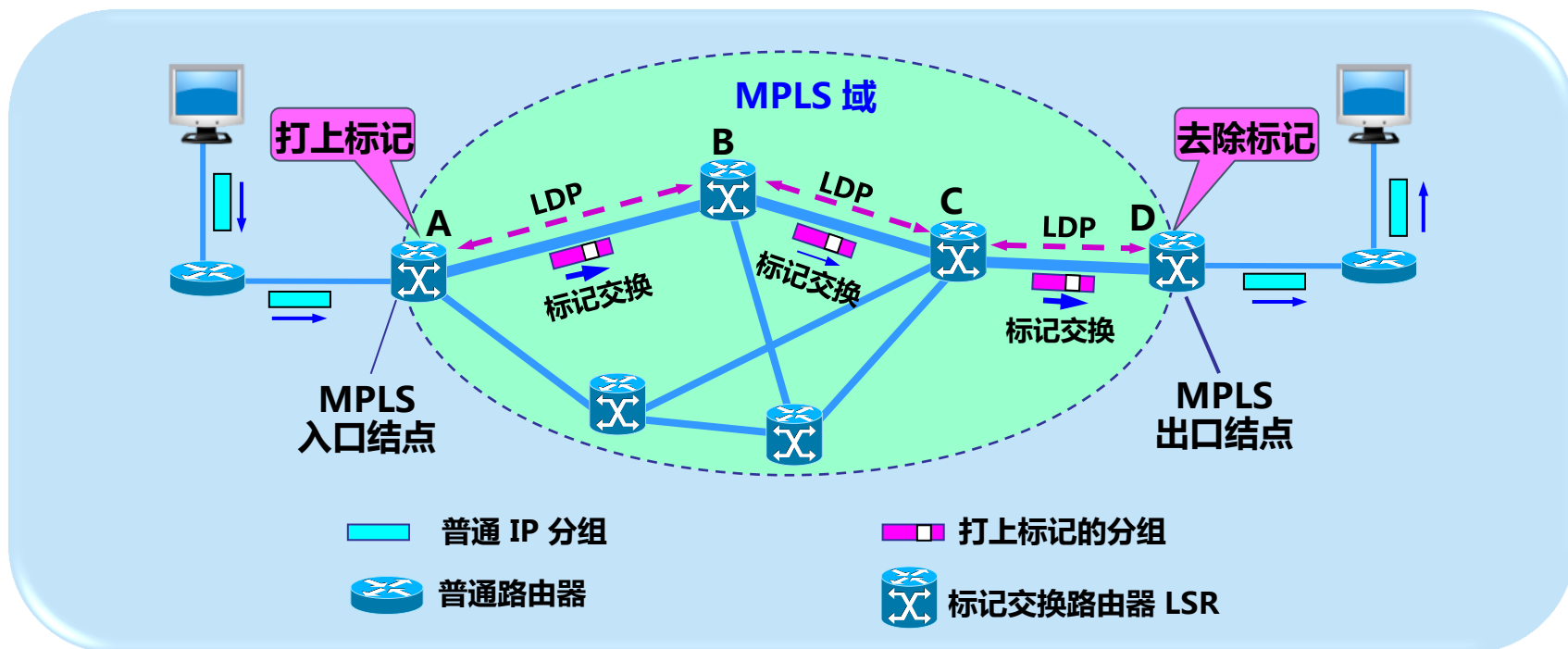
- **MPLS** (Multi Protocol Label Switching) : 互联网建议标准。
 - “**多协议**” : 表示在 MPLS 的上层可以支持多种协议 , 例如 IP、IPX ; 可以使用多种**数据链路层协议** , 例如PPP、以太网、ATM 等。
 - “**标记**” : 每个数据报被打上一个标记 (label) , 标记交换路由器根据**标记值**检索转发表 , 实现数据报的快速转发。
 - “**交换**” : 在转发时不再上升到第三层查找转发表 , 而是根据标记在第二层 (数据链路层) 用硬件进行转发。
- MPLS 并没有取代 IP , 而是作为一种 **IP 增强技术**被广泛地应用在互联网中。

基本原理



- **MPLS 域**中有许多彼此相邻的路由器，并且所有的路由器都是支持 MPLS 技术的**标记交换路由器 LSR**。
- LSR 同时具有标记交换和路由选择这两种功能，**标记交换功能是为了快速转发，但在这之前LSR 需要使用路由选择功能构造转发表。**

基本原理



- MPLS 域中的各 LSR 使用专门的**标记分配协议 LDP** 交换报文，并**找出和特定标记相对应的路径**，即**标记交换路径 LSP**。
- 在 MPLS 域的**入口**处，给每一个 IP 数据报打上**固定长度“标记”**，然后对打上标记的 IP 数据报按照转发表用**硬件进行转发**，即**标记交换**。



5.1	网络层概述
5.2	网际协议 (IPv4 和IPv6)
5.3	IP选路
5.4	路由选择协议
5.5	互联网控制报文协议
5.6	多协议标记交换