

《无线网络应用》第五次课之三

模块17 构建小型网络 (1/2) (17.1~17.5)

模块13 ICMP (ping和traceroute命令均基于ICMP协议)

网络简介 v7.02



17.1~17.3节：

从小型网络到大型网络（较简单，请自学）

学习完本节内容后，您将能够：

- 确定小型网络中使用的设备。
- 解释小型网络如何充当大型网络的基础。

17.1 小型网络中的设备



小型网络拓扑

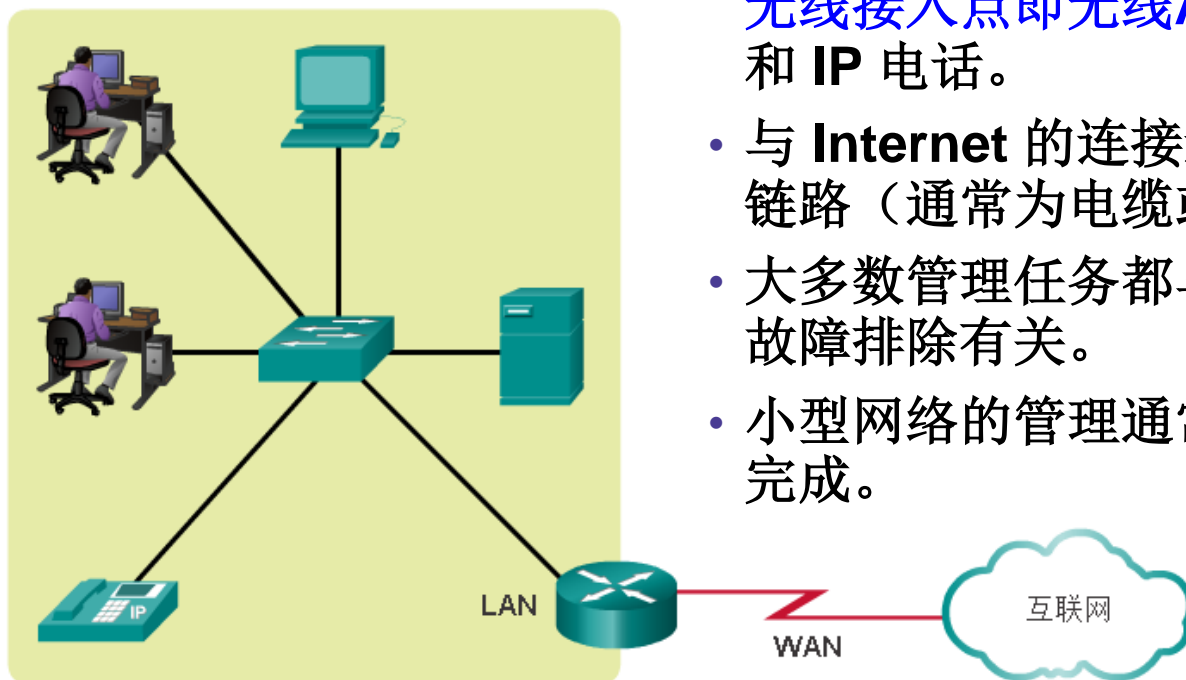
图中显示一个典型的小型企业网络。

- 小型网络的设计很简单。

- 只需少量的网络设备。

小型网络通常由一台路由器、几台交换机和用户 **PC** 组成。小型网络也可能有：
无线接入点即无线**AP**（或无线路由器）
和 **IP** 电话。

- 与 **Internet** 的连接通过单个**WAN**即广域网链路（通常为电缆或 **DSL**）来实现。
- 大多数管理任务都与现有设备的维护和故障排除有关。
- 小型网络的管理通常由第三方公司的员工完成。



小型网络的设备选择

为了满足用户需求，小型网络也要求**规划**和**设计**。

如图所示，在选择**中间设备**类型时，需要考虑诸多因素。



成本



端口



速度



可扩展/模块化



可管理

小型网络的 IP 编址

在实施小型网络时，需要规划 IP 编址空间：

- 与网络连接的所有设备都必须有地址。
- 地址方案必须进行规划、记录和维护。

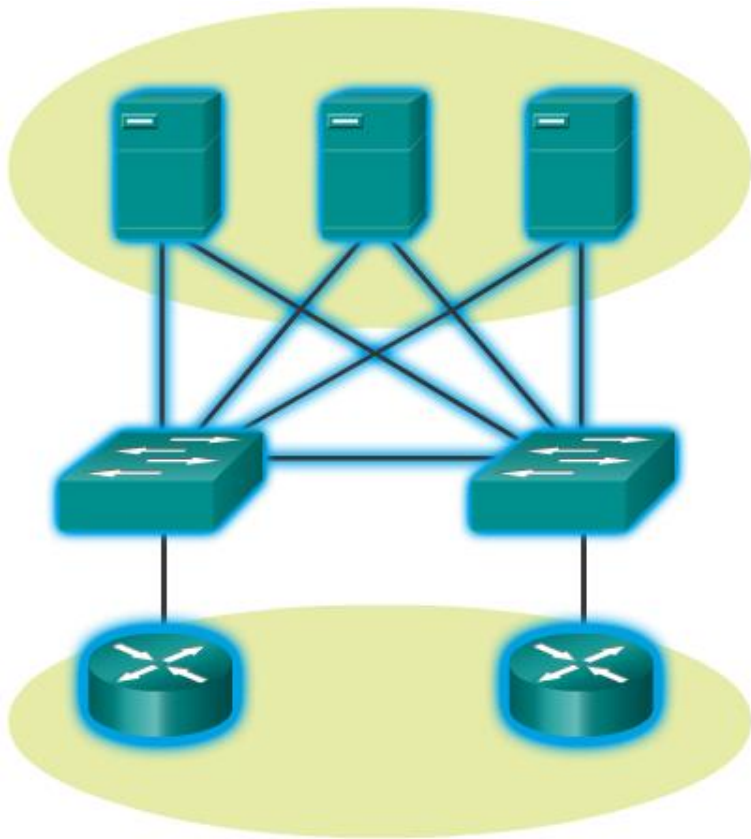
地址文档对故障排除非常有用。在控制资源访问时同样也很重要。



小型网络中的冗余

网络设计的另一个重要部分是**可靠性**（**第1章：容错能力；备用/备份**）：

- 冗余可以避免**单点故障**，从而可提高可靠性。
- 网络冗余可通过复制网络设备和链接来实现。

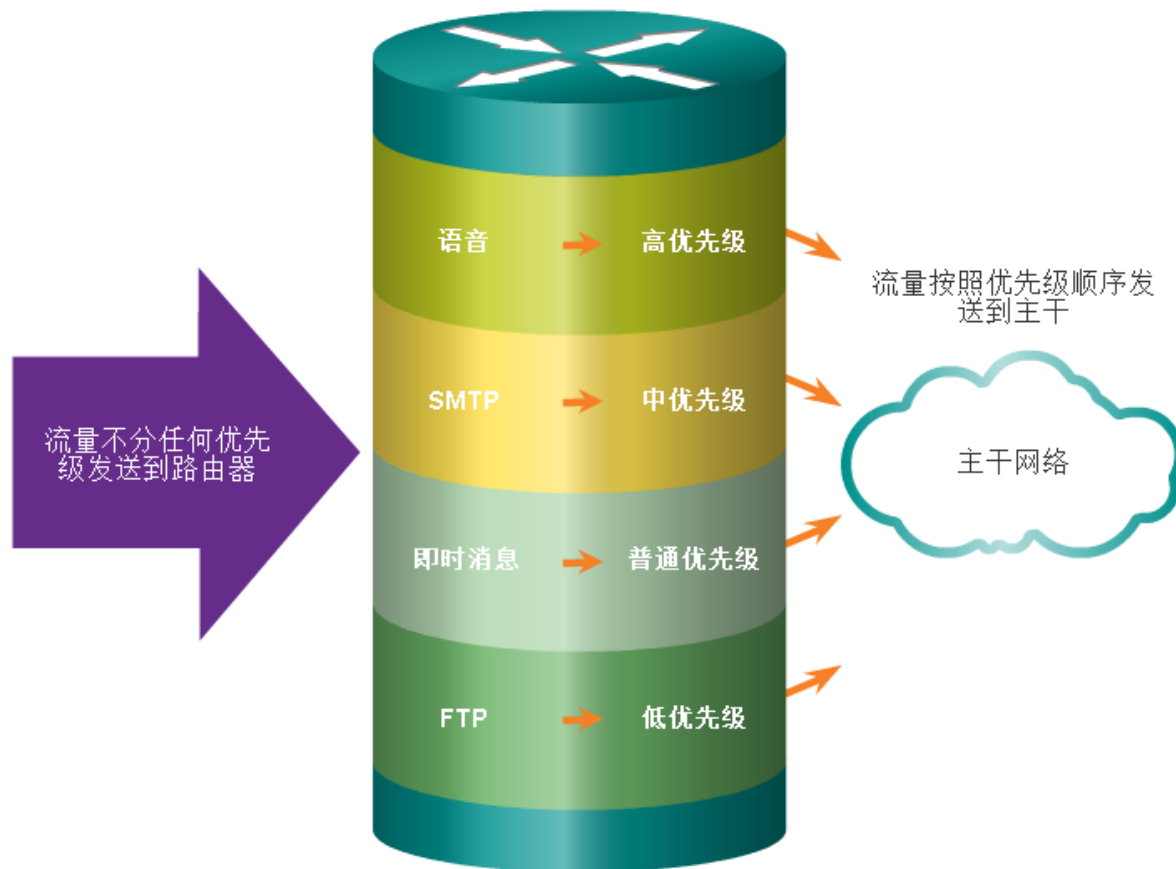


如果一台服务器发生故障，
另一台可随时处理客户请求。

如果通往一台交换机的链路发生故障，
通往第二台交换机的链路仍然可用。
部署冗余交换机可避免交换故障。

小型网络中的流量管理

- 设计网络时还需考虑流量类型及其处理。（第1章：服务质量QoS）
- 好的网络设计会根据**优先级**对流量进行分类。一般语音视频优先级最高。



17.3 扩展为大型网络



小型网络增长



不断扩展是许多小型企业必经的过程，而其网络也必须相应扩展。

要扩展网络，要求以下几个要素：

- **网络文档** - 物理和逻辑拓扑
- **设备清单** - 使用或构成网络的设备列表
- **预算** - 逐项记录的 IT 预算，包括财年设备的采购预算
- **流量分析** - 应当记录协议、应用程序和服务以及它们各自的流量要求

这些要素可用于为有关小型网络扩展的决策提供信息。

17.4~17.5节 基础网络性能

网络性能基线Baseline：是指网络在正常情况下的各种性能参数，是诊断排除网络问题的利器，同时也是网络的健康快照，是网络中不可或缺指标。

学习完本节内容后，您将能够：

- 了解 **ping/trace** 命令所使用的 ICMP 消息 (模块13)。
- 使用 **ping/trace** 命令的输出建立相关网络性能基线。
- 使用 **show** 命令检验网络设备的配置和状态。
- 使用 **Windows 主机命令**获取网络设备的相关信息。

模块13 ICMP消息

ICMPv4和ICMPv6消息

(*Internet Control Message Protocol*)

- **Internet 控制消息协议 (ICMP)** 提供了在一定条件下处理IP数据包的相关问题的反馈。
- **ICMPv4 是 IPv4 的消息协议。ICMPv6 是 IPv6 的消息协议，并包括额外的功能。**
- **ICMPv4 和 ICMPv6 通用的 ICMP 消息包括：**
 - ✓ **主机连通性**
 - ✓ **目的或服务不可达**
 - ✓ **超时**

模块13 ICMP消息

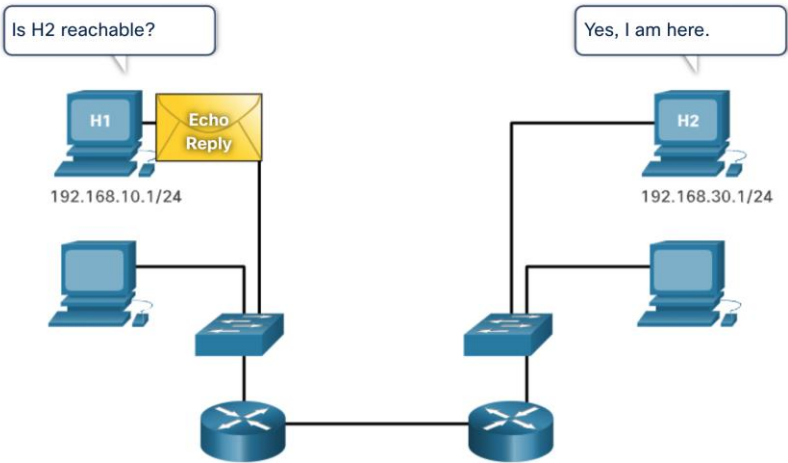
主机连通性

ICMP Echo消息 (Ping/Traceroute命令)

可用于测试 IP 网络上主机的连通性。

在示例中：

- 本地主机向一台主机发送 **ICMP 回应请求 (Echo Request)**。
- 如果主机可用，目的主机会回应以 **ICMP 回应应答 (Echo Reply)**。



目的或服务不可达

- ICMP目的不可达消息（Ping/Traceroute命令）
可用于通知源，说明某个目的或服务不可到达。
- 在ICMP目的不可达消息中，包括指示数据包为何无法传送的代码：

ICMPv4 的目的不可达代码：

- 0 - 网络不可达
- 1 - 主机不可达
- 2 - 协议不可达
- 3 - 端口不可达

ICMPv6 的目的不可达代码：

- 0 - 没有通往目的的路由
- 1 - 管理上禁止与目的通信（例如防火墙）
- 2 - 超出源地址的范围
- 3 - 地址无法访问
- 4 - 端口不可达

模块13 ICMP消息

超时

Time-To-Live (Ping/Traceroute命令)

- 当 IPv4 数据包中的生存时间 (TTL) 字段递减为 0 时，将向源主机发送 ICMPv4 超时消息。

(Ping/Traceroute命令)

- ICMPv6 也会发送 ICMPv6 超时消息。
ICMPv6 使用 IPv6 跳数限制字段来确定数据包是否已过期，而不是用 IPv4 TTL 字段。

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
正在 Ping 4.4.4.4 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

4.4.4.4 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```


模块13 ICMP消息

- 注意：ICMP消息有时并不是必需的，
而且在网络中可能 **出于安全原因而被禁止**。
- 这样，因为Ping和Traceroute命令都基于ICMP消息工作，
所以，有时Ping不通，或者Traceroute超时，
可能只是由于 **防火墙等安全原因阻挡ICMP消息** 所致。
- 也就是说，这时可能并非目的主机没有联网、无法被访问，
可能还是可以正常访问目的主机的 **应用层服务** 如Web或FTP站点的。

注：ICMP属于网络层即第三层协议，
而Web和FTP等服务属于应用层即第七层协议。
- ✓ 因此，这时如果 **关掉防火墙**，可能即可**Ping通**或**Traceroute通**。

模块13 ICMP消息

ICMPv6消息

ICMPv6具有ICMPv4中没有的新特性和改进功能，
包括作为邻居发现协议(ND或NDP)一部分的四个新协议。
Neighbor Discovery Protocol

IPv6路由器和IPv6设备之间的消息传递，包括：

- 路由器请求 (RS) 消息
(Router Solicitation)
- 路由器通告 (RA) 消息
(Router Advertisement)

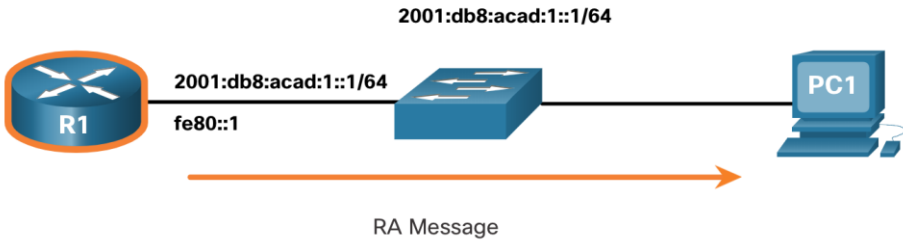
IPv6设备之间的消息传递，包括：

- 邻居请求 (NS) 消息
(Neighbor Solicitation)
- 邻居通告 (NA) 消息
(Neighbor Advertisement)

模块13 ICMP消息

ICMPv6消息： 路由器通告RA消息

- 启用 IPv6 的路由器每200秒发送 RA 消息，向启用 IPv6 的主机提供编址信息（即动态地址分配）。
- RA 消息中可以包含主机的编址信息，例如前缀、前缀长度、DNS 地址和域名。



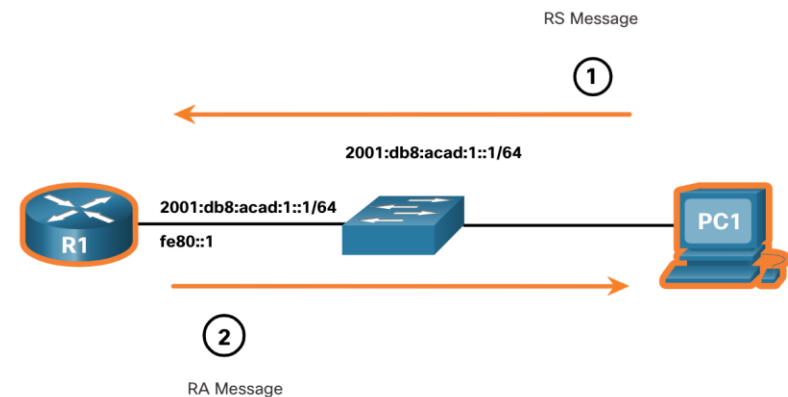
IPv6路由器向IPv6主机定期发送RA消息，给IPv6主机提供IPv6地址信息。

模块13 ICMP消息

ICMPv6消息： 路由器请求RS消息、 路由器通告RA消息

- 启用IPv6的路由器还会发送 **RA 消息** 以响应 PC 的 **RS 消息**。
- 在图中，PC1 发送 **RS 消息** 以确定如何动态接收 IPv6 地址信息（即**动态地址分配**，类似于**DHCPv6**）。然后，R1 用 **RA 消息** 回复 **RS 消息**。
 - PC1 发送一条 **RS 消息**说：“嗨，我刚刚启动。网络上是否有 IPv6 路由器？我需要知道如何动态获取我的 IPv6 地址信息？”。
 - R1 用 **RA 消息**回复：“嗨，所有IPv6 设备大家好。我是 R1，您可以使用 SLAAC 创建 IPv6 全局单播地址。前缀是2001:db8:acad:1::/64。顺便说一下，使用我的**本地链路地址fe80::1**作为你的默认网关”。

(SLAAC: Stateless Address Autoconfiguration 无状态地址自动配置)

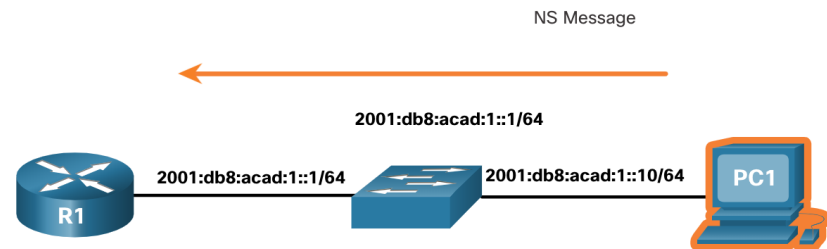


IPv6主机向IPv6路由器发送**RS消息**，
请求获得IPv6地址信息；
IPv6路由器向IPv6主机发回**RA消息**，
给IPv6主机提供IPv6地址信息。

模块13 ICMP消息

ICMPv6消息：邻居请求NS消息、邻居通告NA消息

- 设备分配有全局单播地址或本地链路单播地址，则会对地址执行 DAD (Duplicate Address Detection, **重复地址检测**) 来确保其唯一性。
- 要检查地址的唯一性，设备将发送 **NS 消息**，其中使用自身 IPv6 地址作为目标 IPv6 地址。
- 如果网络中的其他某设备A具有该地址，则设备A会使用 **NA 消息**进行响应，通知发送设备该地址正在使用中。



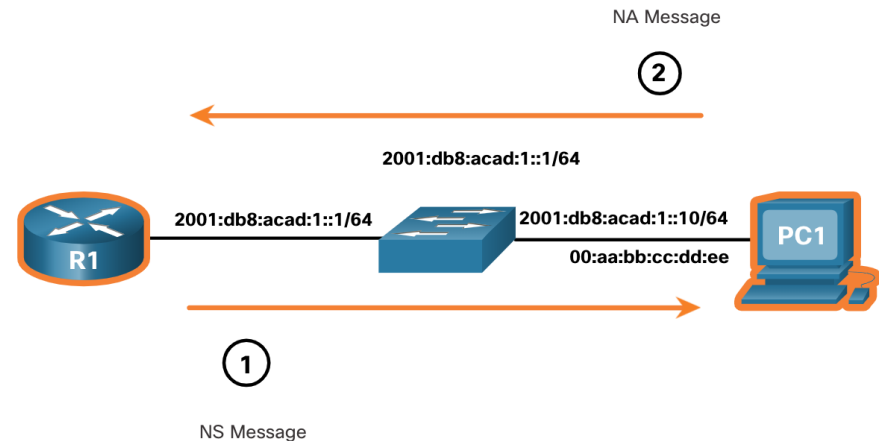
IPv6主机B发出NS消息检测地址重复；
与其地址重复的IPv6主机A发回NA消息，
通知源主机B“你的IPv6地址有重复”。

模块13 ICMP消息

ICMPv6消息：邻居请求NS消息、邻居通告NA消息

- 要确定目的设备的 MAC 地址，源设备会将 **NS 消息** 发送到目的设备。
- 该消息包括已知的目的设备的 IPv6 地址。具有该 IPv6 地址的目的设备会使用包含其 MAC 地址的 **NA 消息** 进行回应。

✓ 如图所示，R1 向 PC1 (2001:db8:acad:1::10) 发送一条 **NS 消息**，询问它的 MAC 地址。然后 PC1 将其 MAC 地址以 **NA 消息** 发回 R1。



- **这在 IPv6 中就相当于 IPv4 的 ARP 地址解析协议 (IP→MAC)。** 所以，在 IPv6 中没有 ARP，而是利用 **NS/NA** 消息相结合来代替 ARP。

IPv6设备B（如R1或其他主机）发出NS消息，检测询问具有某IPv6地址的主机的MAC地址；具有该IPv6地址的主机A（如PC1）发回NA消息，把A自己的MAC地址告诉给源设备B。

17.4.1~17.4.2节： ping 命令



Ping - 测试连通性 (Ping的工作基于ICMP消息)

- **ping**命令是一个IPv4和IPv6测试实用程序，它使用**ICMP Echo请求**和**Echo应答消息**来测试主机之间的连接，并提供一个包括成功率和到目的地的平均往返时间的总结。
- 如果在超时前没有收到应答，ping 会提供一条消息，表示未收到响应。

```
S1#ping 192.168.20.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

解读 Ping 结果

IOS Ping 指示符:

从 IOS 发出的 **ping** 命令将为发送的每个 **ICMP Echo Request** 请求消息生成一个指示符。

- **!** - 表示收到 **ICMP Echo Reply** 应答消息 (**ping 通了**)。
- **.** - 表示等待 **ICMP Echo Reply** 应答消息时超时 (**没有 ping 通**)。
- **U** - 表示收到了 **ICMP Unreachable** 无法到达消息 (**也没有 ping 通**)。

```
R1# ping 209.165.200.226
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout  
is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max =  
3/3/4 ms
```

```
R1#
```

ping一个地址是**标准ping命令** (>、#)

单独一个ping则是**扩展ping命令**，有很多选项 (#)

Windows主机上的ping命令也有很多选项，可用ping /?查看，比如：
-S srcaddr选项表示ping时使用的源地址，即可选择自本机的不同网卡发出。

解读 Ping 结果（续）

- “.”（句点）可能表示路径中某处可能发生连接问题。
很多原因会导致这个指示符的出现：
 - 路径沿途的某个路由器没有通往目的地的路由，而且也没有发回 **ICMP** 目的无法到达的消息。
 - 设备安全阻止了 **ping**。
 - **ping** 在收到另一个协议的回应前超时（比如 **ARP: IP→MAC**）。
- “U” 表示路径沿途的某个路由器发回了 **ICMP** 目的无法到达的消息。
路由器没有通往目的地址的路由，或 **ping** 请求被阻止。

17.4.3~17.4.4节： traceroute 命令



Traceroute - 测试路径 (Traceroute的工作也基于ICMP消息)

- Traceroute (**tracert**)是一个实用程序，用于测试两个主机之间的路径，并提供沿着该路径成功到达的每一跳的列表。
- Traceroute 可提供沿路径每一跳的往返时间并指示是否有某一跳未响应。
星号 (*) 表示丢失的或无应答的数据包。
- 此信息可用于在路径中定位有问题的路由器，或表示**路由器配置为不应答** (比如出于安全原因)。

```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2
```

1	192.168.10.2	1 msec	0 msec	0 msec
2	192.168.20.2	2 msec	1 msec	0 msec
3	192.168.30.2	1 msec	0 msec	0 msec
4	192.168.40.2	0 msec	0 msec	0 msec

通过最多 30 个跃点跟踪到 10.10.0.21 的路由

1	3 ms	5 ms	2 ms	10.185.127.254
2	9 ms	4 ms	4 ms	10.3.7.178
3	3 ms	3 ms	2 ms	10.3.7.229
4	*	*	*	请求超时。
5	*	*	*	请求超时。
6	5 ms	13 ms	8 ms	10.10.0.21

跟踪完成。

注意：Traceroute 使用第 3 层报头中的 IPv4 TTL 字段功能、IPv6 跳数限制字段功能、以及 **ICMP 超时消息**。

解读 Trace 消息

- **Trace**可用于返回数据包在网络中传输时沿途经过的每跳（即每个路由器）列表。
- 该命令的形式取决于平台：
tracert 命令用于 **Windows** 系统，
traceroute 命令用于 **Cisco IOS** 和 **Linux** 等系统。

如右图所示：

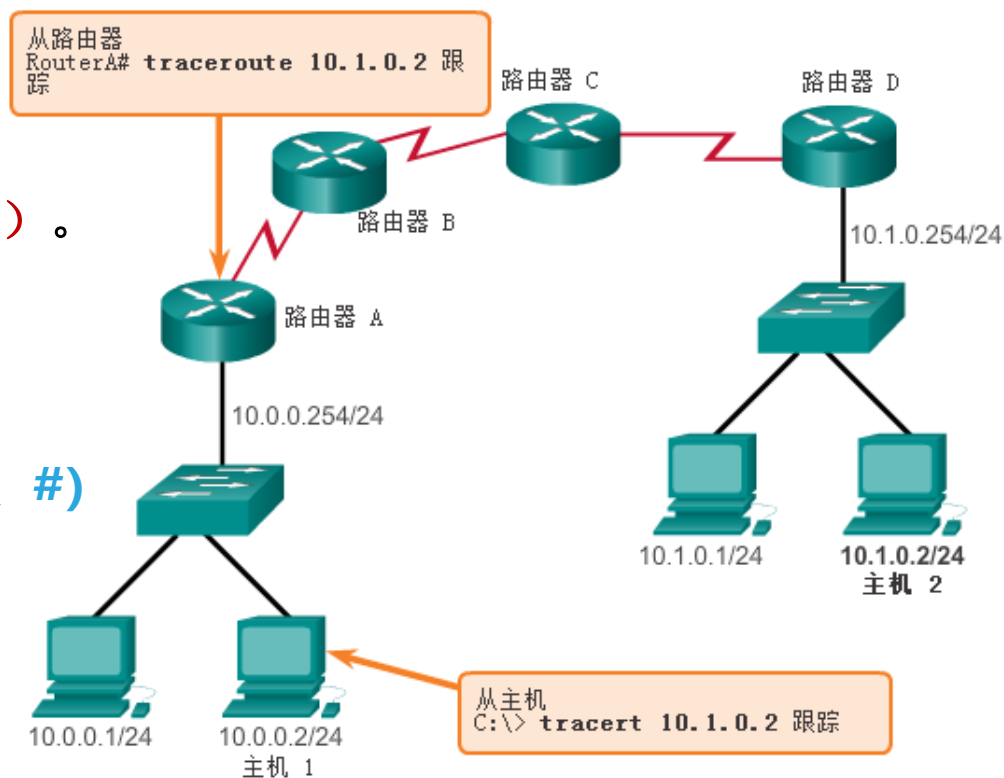
若从路由器 **CLI** 上执行追踪，
请使用 **traceroute**（可缩写为 **trace**）。

若从 **Windows** 计算机上执行追踪，
请使用 **tracert**。

在**IOS**中：

trace一个地址是**标准trace命令**（>、#）
单独一个**trace**则是**扩展trace命令**，
有很多选项（#）

Windows主机上的**tracert**命令也有
很多选项，可用**tracert /?**查看。



17.5节： 主机和 IOS 的命令



常用 IOS show 命令（参见7.02版模块2、10）

- Cisco IOS CLI **show** 命令是强大的故障排除工具。
- **show** 命令可用于查看配置文件、检查设备接口和进程的状态、以及检验设备的运行状态。
- 几乎路由器的每个进程或功能的状态都可使用 **show** 命令显示出来。
- 比较常用的 **show** 命令有：

sh run ○ **show running-config**（查看运行配置文件）

sh start ○ **show startup-config**（查看启动配置文件）

sh int ○ **show interfaces**（查看设备接口信息）或 **show ip interface brief**

○ **show arp**（查看设备的ARP表/ARP缓存）

○ **show ip route**（查看路由表）

○ **show protocols**（查看设备上配置的协议）

○ **show version**（查看设备系统硬件软件等版本信息）

✓ 注：**show** 命令总是在 用户 EXEC 或 特权 EXEC 模式下运行！

主机的 ipconfig 命令

- **ipconfig** 命令可用于显示基于 **Windows** 的计算机的 **IP** 信息。
- **ipconfig** 命令可显示主机及其默认网关的 **IP** 地址。
- 使用 **ipconfig /all** 命令可查看更详细的主机 **IP** 配置，包括**MAC**地址、默认网关和**DNS**服务器**IP**地址等。

ipconfig




```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

图例

-  此主机计算机的 IP 地址
-  本地网络子网掩码
-  此主机计算机的默认网关地址

ipconfig /all

```
C:\>ipconfig /all

Ethernet adapter Network Connection:

    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                                2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                                2007 6:57:11 AM

C:\>
```

- **ipconfig /displaydns** 命令显示基于Windows计算机系统中的所有DNS缓存条目 (不再查hosts文件或问DNS服务器)
- **ipconfig /flushdns** 命令清除所有DNS缓存条目 (以便重新从本机hosts文件或DNS服务器获取域名对应的最新IP地址信息——
一般用在修改了 hosts文件 或 DNS服务器地址 以后)

```
C:\> ipconfig /displaydns
```

```
Windows IP Configuration
```

```
cisco-tags.cisco.com
```

```
-----  
Record Name . . . . . : cisco-tags.cisco.com
```

```
Record Type . . . . . : 1
```

```
Time To Live . . . . . : 44024
```

```
Data Length . . . . . : 4
```

```
Section . . . . . : Answer
```

```
A (Host) Record . . . : 72.163.10.10
```

```
<省略部分输出>
```

DNS缓存：以前曾经 查本机hosts文件 或 问DNS服务器 获得的域名与IP地址对应关系，保存在本机本地DNS缓存中以便下次快速查询。

Windows下的本机hosts文件位于：
c:\Windows\System32\drivers\etc\hosts

For example:

# 102.54.94.97	rhino.acme.com	# source server
# 38.25.63.10	x.acme.com	# x client host

主机的 arp 命令

- **arp -a** 命令可列出主机的 ARP缓存（即ARP表） 中所有的当前设备。
- 包括每台设备的 **IPv4地址**、物理地址即 **MAC地址** 和 **ARP条目类型**（静态/动态）。
- 可使用 **arp -d** 命令清除所有 ARP缓存（即ARP表）
（以便重新发起 ARP进程 去查询 IPv4地址 对应的 MAC地址）

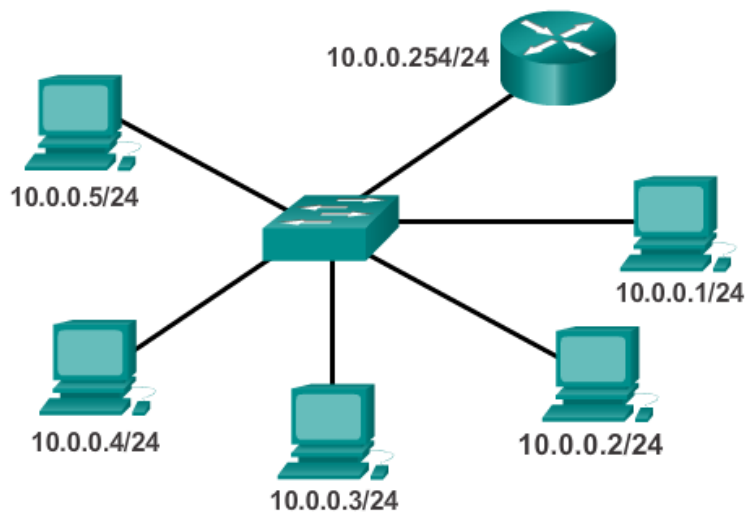
IPv6用NS/NA消息或者说NDP
(邻居发现协议) 替代IPv4的ARP。

Windows查看IPv6 IP-MAC对的命令:

netsh interface ipv6 show neighbors

Windows清除IPv6 IP-MAC对的命令:

netsh interface ipv6 delete neighbors



```
c:\>arp -a
Internet Address Physical Address Type
10.0.0.2          00-08-a3-b6-ce-04 dynamic
10.0.0.3          00-0d-56-09-fb-d1 dynamic
10.0.0.4          00-12-3f-d4-6d-1b dynamic
10.0.0.254       00-10-7b-e7-fa-ef dynamic
```

IP - MAC 地址对

谢谢。



Cisco Networking Academy
Mind Wide Open