实验 - 映射 Internet

目标

第 1 部分：使用 Ping 测试网络连接

第 2 部分：使用 Windows Tracert 跟踪通往远程服务器的路由

背景信息

路由跟踪计算机软件是一种实用程序，它列出了数据在从用户的始发终端设备传输到远程目的网络的过程中必经的网络。

此类网络工具通常在命令行的执行方式如下：

tracert <destination network name or end device address>

（Microsoft Windows 系统）

或

traceroute <destination network name or end device address>

（Unix 和类似系统）

用户可以使用路由跟踪实用程序来确定路径或路由以及 IP 网络中的延迟。现有多个工具可以执行此功能。

traceroute（或 **tracert**）工具通常用于排除网络故障。通过它显示的沿途路由器的列表，用户就可以确定到达网络中或网间特定目的地址所经过的路径。每个路由器都代表一个网络与其他网络的连接点，也是数据包的转发点。路由器数量也就是数据从源设备传送到目的设备所经过的“跳”数。

显示的列表可以帮助诊断尝试访问服务（如网站）时的数据流问题。也有助于执行下载数据之类的任务。如果有多个网站（镜像）可用于同一个数据文件，我们可以跟踪每个镜像，从而了解使用哪个镜像的速度最快。

同一个源和目的地之间相距一段时间执行的两次跟踪路由可能会产生不同的结果。这是因为构成 Internet 的各个互联网络具有“网状”性质，并且 Internet 协议能够选择不同的路径发送数据包。

基于命令行的路由跟踪工具通常内嵌于终端设备的操作系统。

场景

通过 Internet 连接，您将使用三种路由跟踪实用程序检查通往目的网络的 Internet 路径。本练习应在能够访问 Internet 和命令行的计算机上执行。首先，您将使用 Windows 内嵌的 tracert 实用程序。

所需资源

1 台 PC（采用 Windows 7 或 8 且可访问互联网）

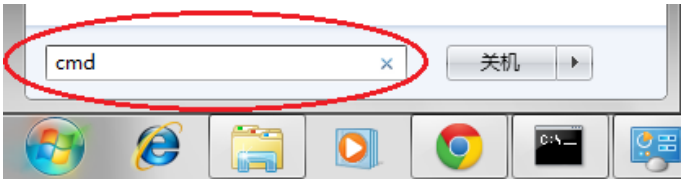
第 1 部分：使用 ping 测试网络连接

第 1 步：确定远程服务器是否可达。

要跟踪到远程网络的路由，使用的 PC 必须有效地连接到 Internet。

a. 我们使用的第一个工具是 ping。Ping 是一种用于测试主机是否可达的工具。它将向远程主机发送信息数据包，并指示其作出回复。您的本地 PC 会测量是否接收到了对每个数据包的响应，以及这些数据包通过网络所需要的时间。名称 ping 来自主动声纳技术，该技术是在水下发送一个声音脉冲，遇到地面或其他船只以后反弹回来。

b. 从 PC 上，单击“**Windows 开始**”图标，在“**搜索程序和文档**”框中输入 **cmd**，然后按 Enter 键。



c. 在命令行提示符后键入 **ping www.cisco.com**。

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

d. 第一行输出显示完全限定域名 (FQDN) e144.dscb.akamaiedge.net。它的后面是 IP 地址 23.1.48.170。思科在全球的不同服务器上托管相同的 Web 内容（称为镜像）。因此，根据您的地理位置不同，FQDN 和 IP 地址也会不同。

e. 根据这一部分输出：

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

发送了四个 ping，并且每个 ping 收到一个回复。由于每个 ping 都收到了回复，因此丢包率为 0%。平均来说，每个数据包通过网络需要 54 ms（54 毫秒）。一毫秒是一秒的千分之一。

当数据包丢失或网络连接速度较低时，视频流和在线游戏这两种应用程序会受到影响。要想确定更精确的 Internet 连接速率，可以发送 100 个 ping，而不是默认的 4 个。具体操作如下：

```
C:\>ping -n 100 www.cisco.com
```

该操作的输出如下：

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

f. 现在请对全球不同位置的地区性互联网注册机构 (RIR) 网站执行 ping 操作：

非洲：

C:\> **ping www.afrinic.net**

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

澳大利亚：

C:\> **ping www.apnic.net**

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

欧洲：

C:\> **ping www.ripe.net**

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

南美洲：

C:\> **ping www.lacnic.net**

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

所有这些 ping 都是从位于美国的一台计算机发出的。与数据从北美洲传输到不同大陆相比，当数据在同一个大陆（北美洲）内传输时，平均 ping 时间（毫秒）将会出现什么情况？

发送到欧洲网站的 ping 操作将会出现什么情况？

第 2 部分：使用 Tracert 跟踪通往远程服务器的路由

第 1 步：确定 Internet 流量使用哪条路由传输到远程服务器。

现在我们已经使用 ping 工具检验了基本的可达性，而深入了解所经过的每个网段也会很有帮助。为此，我们将使用 **tracert** 工具。

a. 在命令行提示符后键入 **tracert www.cisco.com**。

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

b. 按照下列步骤将 tracert 输出保存在文本文件中：

1) 右键单击命令提示符窗口的标题栏，然后选择**编辑 > 全选**。

2) 再次右键单击命令提示符窗口的标题栏，然后选择**编辑 > 复制**。

3) 打开“**Windows 记事本**”程序：**Windows 开始**图标>“**所有程序**”>“**附件**”>“**记事本**”。

4) 要将输出粘贴到记事本中，可选择**编辑 > 粘贴**。

5) 选择**文件 > 另存为**，将记事本文件命名为 tracert1.txt 并保存在桌面上。

c. 针对每个目的网站运行 **tracert**，然后将输出保存在按顺序编号的文件中。

```
C:\> tracert www.afrinic.net
C:\> tracert www.lacnic.net
```

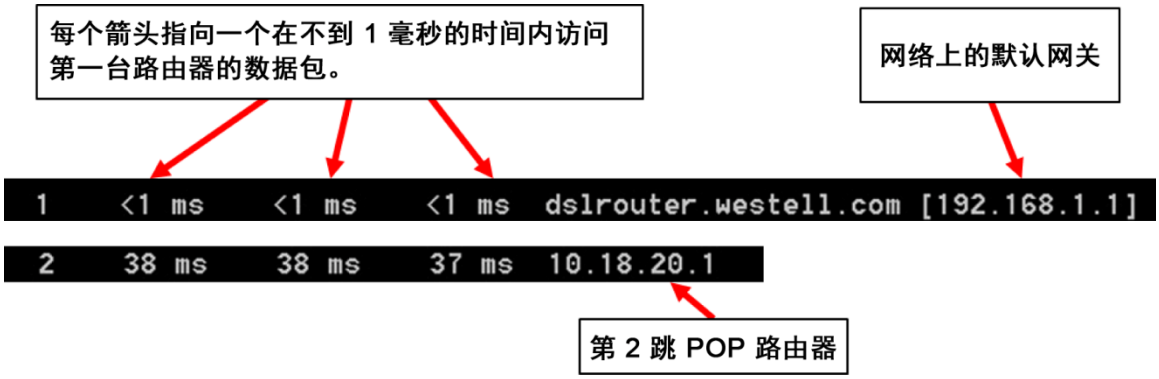
d. 解释 **tracert** 输出。

根据 ISP 的规模以及源主机和目的主机所在的位置，您跟踪到的路由可能途经了许多跳和多家不同的 Internet 服务提供商 (ISP)。每个“跳”代表一台路由器。路由器是用于在 Internet 中指引流量的一种特殊类型的计算机。假设您正通过许多公路在多个国家/地区之间开车旅行。在旅途的不同点，您会在道路上遇到一个分岔点，您可以从多条不同的公路中进行选择。现在进一步假设，道路上的每个分岔点都有一台设备，它可以指引您通过正确的公路到达您的最终目的地。路由器对网络中的数据包能够起到同样的作用。

由于计算机之间使用数字通信，而不使用字词，因此我们使用 IP 地址（采用 x.x.x.x 格式的数字）唯一识别路由器。**tracert** 工具可以为您显示信息数据包通过哪条网络路径到达其最终目的地。**tracert** 工具还可以为您显示流量在每个网段上的传输速度。已经向该路径中的每个路由器发送了三个数据包，并且返回时间以毫秒为单位进行测量。现在，请使用此信息分析对 www.cisco.com 执行 **tracert** 的结果。完整的 traceroute 如下：

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

分解如下：



在如上所示的示例输出中，tracert 数据包从源 PC 传输到本地路由器默认网关（第 1 跳：192.168.1.1），然后传输到 ISP 入网点 (POP) 路由器（第 2 跳：10.18.20.1）。每个 ISP 都拥有许多 POP 路由器。这些 POP 路由器位于 ISP 的网络边缘，也是客户连接到 Internet 的途径。数据包沿着 Verizon 网络传输两跳，然后跳到属于 alter.net 的路由器。这可能意味着数据包已传输到另一个 ISP。这将具有重大影响，因为有时在 ISP 之间传输时会造成丢包，或者有时一个 ISP 比另一个 ISP 慢。我们如何确定 alter.net 是另一个 ISP 还是同一个 ISP？

e. 有一个名为 whois 的 Internet 工具。使用 whois 工具可以确定域名的拥有者。在 http://whois.domaintools.com/ 上可以找到基于 Web 的 whois 工具。根据基于 Web 的 whois 工具，此域也属于 Verizon。

```
Registrant:
        Verizon Business Global LLC
        Verizon Business Global LLC
        One Verizon Way
         Basking Ridge NJ 07920
        US
         domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

    Domain Name: alter.net
```

简而言之，Internet 流量从家用 PC 开始，通过家用路由器传输（第 1 跳）。然后，它会连接到 ISP 并通过其网络传输（第 2 跳至第 7 跳），直至其到达远程服务器（第 8 跳）。这是一个相对不常见的示例，因为自始至终只涉及了一个 ISP。通常会涉及到两个或更多 ISP，如以下示例所示。

f. 现在请看通过多个 ISP 传输 Internet 流量的示例。以下是对 www.afrinic.net 执行的 tracert：

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

在第 7 跳发生了什么情况？level3.net 是与第 2 跳至第 6 跳相同的 ISP 还是不同的 ISP？请使用 whois 工具回答此问题。

_____

当数据包在华盛顿和巴黎之间传输时，与前面的 1 到 9 跳相比，在第 18 跳发生了什么情况?

.

在第 18 跳发生了什么情况？使用 whois 工具对 168.209.201.74 执行 whois 查找。该网络的拥有者是谁？

.

g. 键入 **tracert www.lacnic.net**。

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

在第 7 跳发生了什么情况？

思考

ping 命令和 tracert 命令之间有哪些功能差异？