实验 - 映射互联网

目标

第 1 部分：确定与目标主机的网络连接

第 2 部分：使用 Tracert 跟踪远程服务器的路由

背景/场景

路由跟踪计算机软件列出了数据从用户的原始终端设备到达远程目标设备遍历的网络。

此类网络工具通常在命令行的执行方式如下：

tracert <目标网络名称或目标终端设备地址>

（Microsoft Windows 系统）

或

traceroute <目标网络名称或目标终端设备地址>

（UNIX、Linux 系统和思科设备，如交换机和路由器）

tracert 和 **traceroute** 确定整个 IP 网络中数据包所采用的路由。

tracert（或 **traceroute**）工具通常用于网络故障排除。通过显示遍历的路由器列表，用户可识别到达网络中或网际网络中特定目标所采用的路径。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。路由器数等于数据从源流向目标经过的跳数。

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。执行下载数据等任务时，该列表也非常有用。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。

基于命令行的路由跟踪工具通常嵌入终端设备的操作系统中。本练习应在能够访问互联网和命令行的计算机上执行。

所需资源

接入互联网的 PC

第 1 部分：确定目标主机的网络连接

要跟踪到远程网络的路由，使用的 PC 必须有效地连接到互联网。使用 **ping** 命令测试是否可访问主机。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。

a 在命令行提示符后，键入 **ping www.cisco.com** 以确定其是否可达。

```
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
```

b 现在，对位于世界不同地方的区域互联网注册 (RIR) 网站中的一个网站执行 ping 命令，以确定是否可访问该网站：

非洲： **www.afrinic.net**

澳大利亚： **www.apnic.net**

南美： **www.lacnic.net**

北美： **www.arin.net**

注：撰写本文时，欧洲 RIR www.ripe.net 并不答复 ICMP 回应请求。

选定的网站将在第 2 部分中与 **tracert** 命令结合使用。

第 2 部分：使用 Tracert 跟踪通往远程服务器的路由

在您使用 **ping** 确定是否可访问选定的网站后，应使用 **tracert** 来确定访问远程服务器的路径。仔细查看所经过的每个网段会有所帮助。

tracert 结果中的每一跳显示数据包流向最终目标时采用的路径。PC 会向远程主机发送三个 ICMP 回应请求数据包。路径中的每个路由器在将生存时间 (TTL) 值传递给下一个系统之前会将其减小 1。当减小的 TTL 值达到 0 时，路由器会将 ICMP 超时消息及其 IP 地址和当前时间发回至源。当到达最终目标时，系统将向源主机发送一条 ICMP 回应答复。

例如，源主机向第一跳 (192.168.1.1) 发送三个 TTL 值为 1 的 ICMP 回应请求数据包。当路由器 192.168.1.1 接收到回应请求数据包时，会将 TTL 值减小到 0。路由器会将 ICMP 超时消息发回至源。此过程会持续，直到源主机发送最后三个 TTL 值为 8（以下输出中的第 8 跳，即最终目标）的 ICMP 回应请求数据包。ICMP 回应请求数据包到达最终目标后，路由器会以 ICMP 回应答复响应源。

对于第 2 跳和第 3 跳，这些 IP 地址为专用地址。这些路由器为 ISP 入网点 (POP) 的典型设置。POP 设备将用户连接到 ISP 网络。

在 http://whois.domaintools.com/ 上可以找到基于 Web 的 whois 工具。它用于确定从源到目标所遍历的域。

a 在命令行提示符下，跟踪 www.cisco.com 的路由。将 **tracert** 输出保存到一个文本文件中。另外，您可以使用 **>** 或 **>>** 将输出重定向到一个文本文件。

```
C:\Users\User1> tracert www.cisco.com
```

或

```
C:\Users\User1> tracert www.cisco.com > tracert-cisco.txt
```

```
Tracing route to e144.dscb.akamaiedge.net [23.67.208.170]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    14 ms     7 ms     7 ms  10.39.0.1
  3    10 ms     8 ms     7 ms  172.21.0.118
  4    11 ms    11 ms    11 ms  70.169.73.196
  5    10 ms     9 ms    11 ms  70.169.75.157
  6    60 ms    49 ms     *     68.1.2.109
  7    43 ms    39 ms    38 ms  Equinix-DFW2.netarch.akamai.com [206.223.118.102]
  8    33 ms    35 ms    33 ms  a23-67-208-170.deploy.akamaitechnologies.com
[23.67.208.170]

Trace complete.
```

b http://whois.domaintools.com/ 中基于 Web 的工具可用于确定 tracert 工具输出中显示的最终 IP 地址和域名的所有者。现在向第 1 部分中的一个 RIR 网站执行 **tracert** 并保存结果。

非洲： **www.afrinic.net**

澳大利亚： **www.apnic.net**

欧洲： **www.ripe.net**

南美： **www.lacnic.net**

北美： **www.arin.net**

使用基于 Web 的 whois 工具，列出 tracert 结果中的以下域名。

_____

_____

c 比较到达最终目标所经过的域列表。

思考

哪些因素会影响 **tracert** 结果？

_____

_____