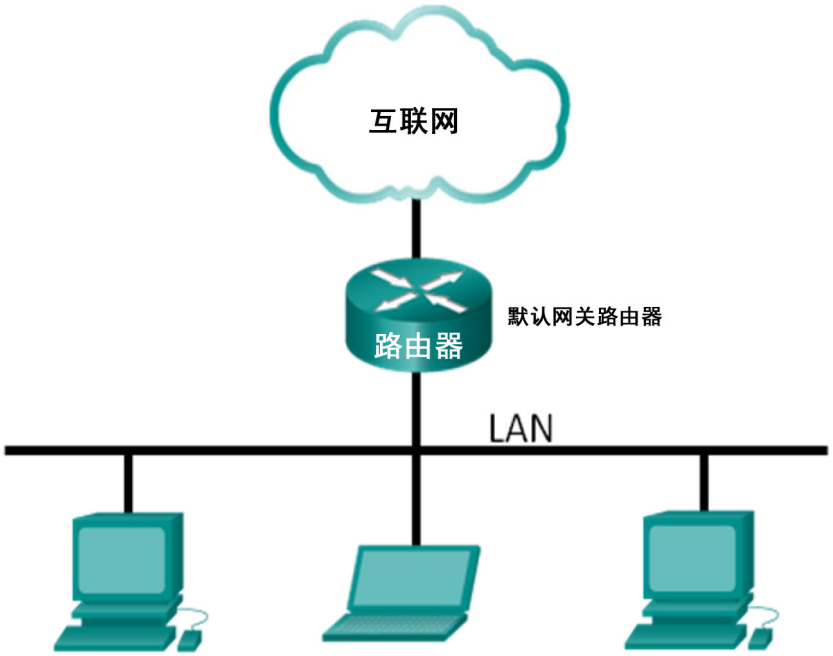
实验 - 使用 Wireshark 查看网络流量

拓扑



目标

第 1 部分：在 Wireshark 中捕获和分析本地 ICMP 数据

第 2 部分：在 Wireshark 中捕获和分析远程 ICMP 数据

背景/场景

Wireshark 是一种协议分析器软件，即“数据包嗅探器”应用程序，适用于网络故障排除、分析、软件和协议开发以及教学。当数据流通过网络来回传输时，嗅探器可以“捕获”每个协议数据单元 (PDU)，并根据适当的 RFC 或其他规范对其内容进行解码和分析。

对于任何从事网络工作的人而言，Wireshark 都是一款实用工具，而且可以在 CCNA 课程的大部分实验中用于数据分析和故障排除。在本实验中，您将使用 Wireshark 捕获 ICMP 数据包的 IP 地址和以太网帧的 MAC 地址。

所需资源

- 1 台 PC（采用 Windows 7 或 Windows 8 且可访问互联网）
- 局域网上的其他 PC，将用于响应 ping 请求。

第 1 部分：在 Wireshark 中捕获和分析本地 ICMP 数据

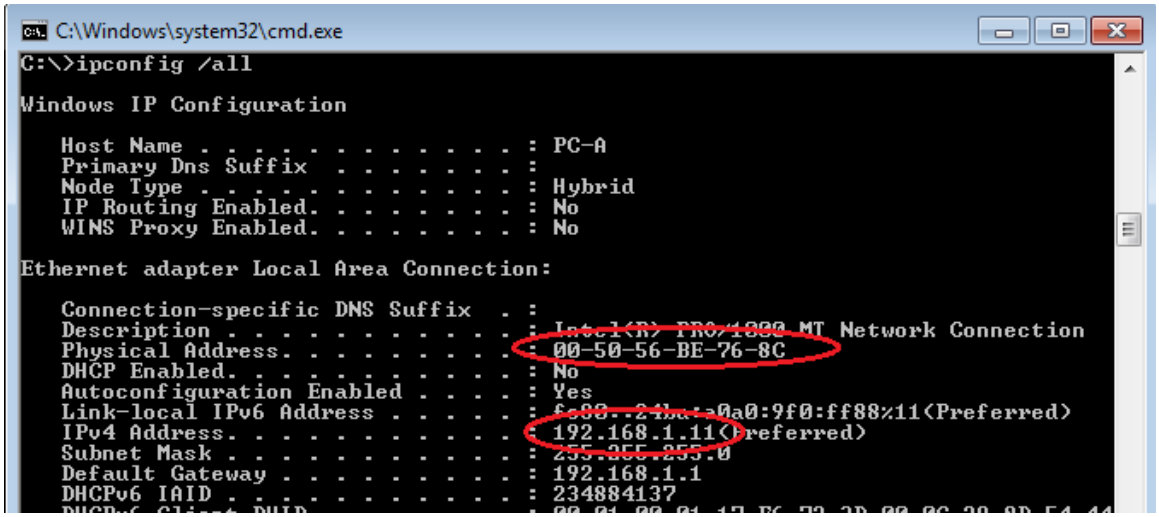
在本实验第 1 部分，您将对 LAN 上的另一 PC 执行 ping 操作，并在 Wireshark 中捕获 ICMP 请求和响应。您还将查看已捕获的帧的内部是否存在特定信息。这种分析应有助于阐明数据包报头如何用于将数据传输到其目的地。

第 1 步： 检索 PC 的接口地址。

对于本实验，您将需要检索 PC 的 IP 地址及其网络接口卡 (NIC) 物理地址（也称为 MAC 地址）。

a. 打开命令窗口，键入 **ipconfig /all**，然后按 Enter 键。

b. 注意您的 PC 接口的 IP 地址和 MAC（物理）地址。

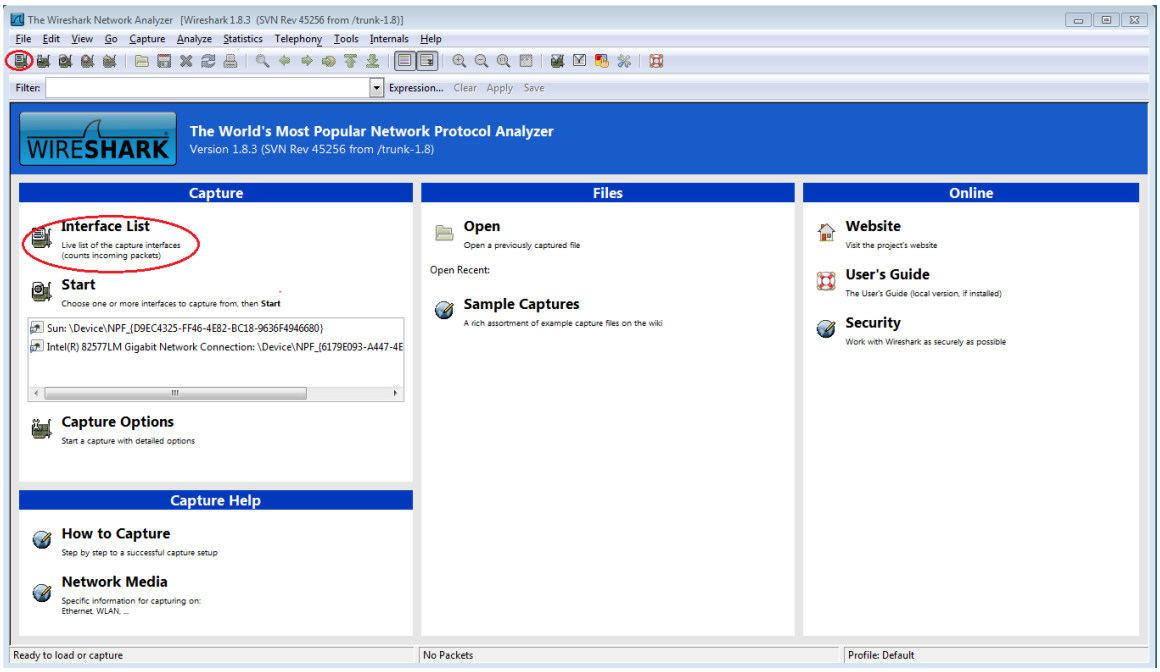


c. 向团队成员询问其 PC 的 IP 地址，并向其提供您的 PC 的 IP 地址。此时不要向其提供您的 MAC 地址。

第 2 步： 启动 Wireshark 并开始捕获数据。

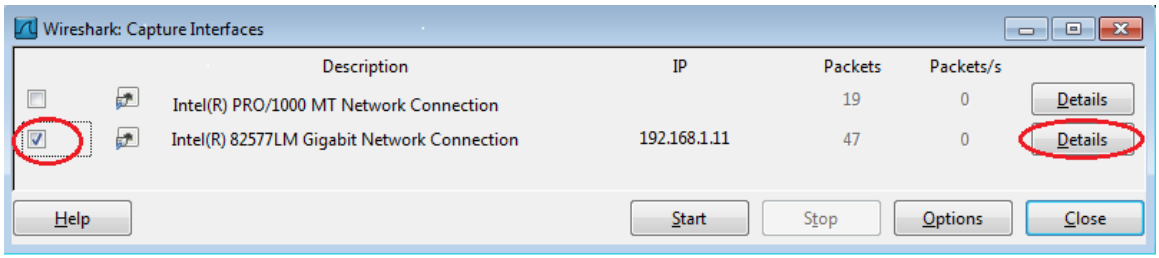
a. 在您的 PC 上，单击 Windows “**开始**”按钮，查看列为弹出菜单中的一个程序的 Wireshark。双击 “**Wireshark**”。

b. 在 Wireshark 启动之后，单击“**接口列表**”。

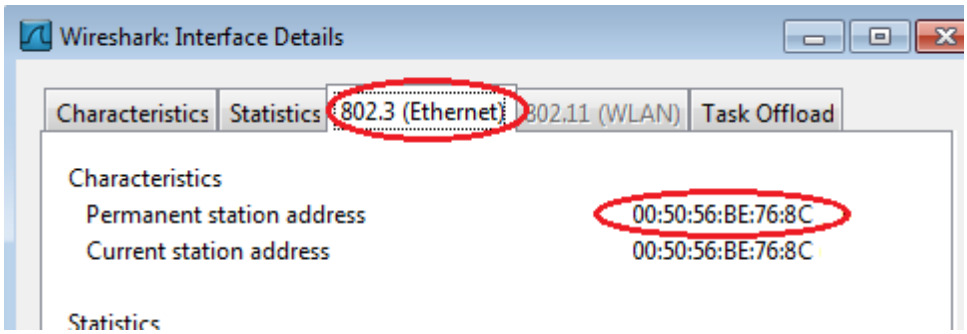


注意：单击图标行中的第一个接口图标也可以打开“接口列表”。

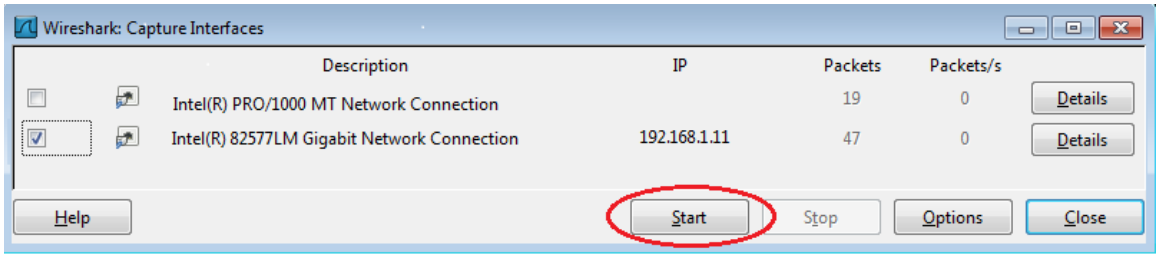
c. 在“Wireshark：捕获接口”窗口，单击与您的 LAN 连接的接口旁的复选框。



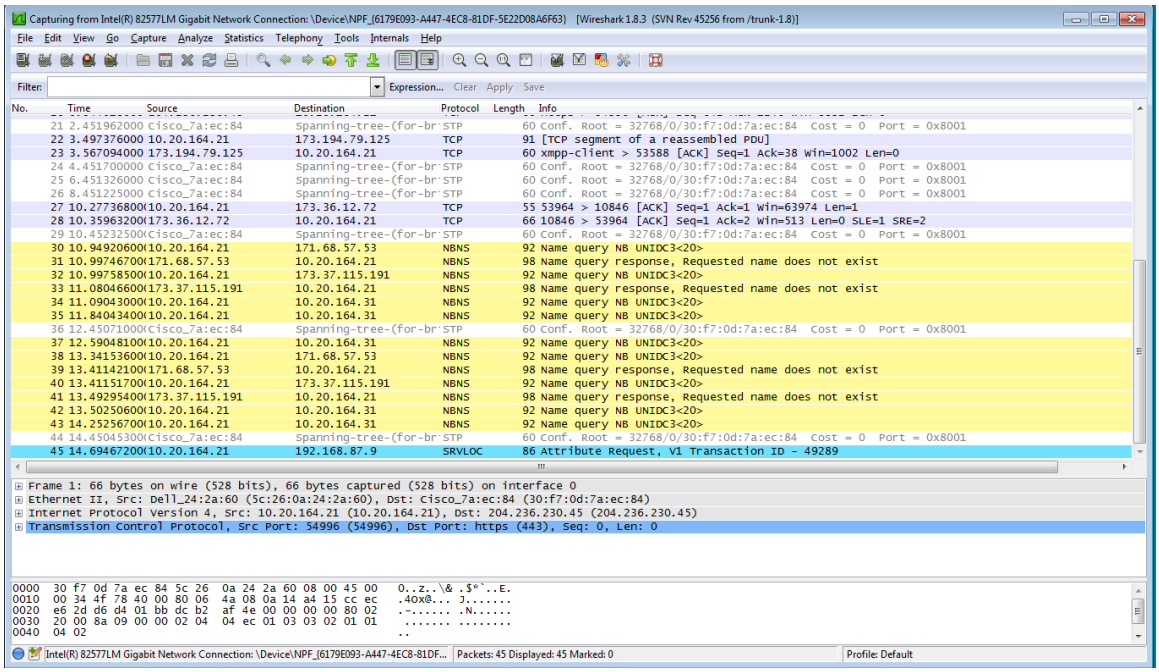
注意：如果列出了多个接口，而您不能确定要检查哪个接口，请单击“**详细信息**”按钮，然后单击“**802.3 (以太网)**”选项卡。检验 MAC 地址是否与您在第 1b 步中看到的匹配。确认接口正确后，关闭“接口详细信息”窗口。



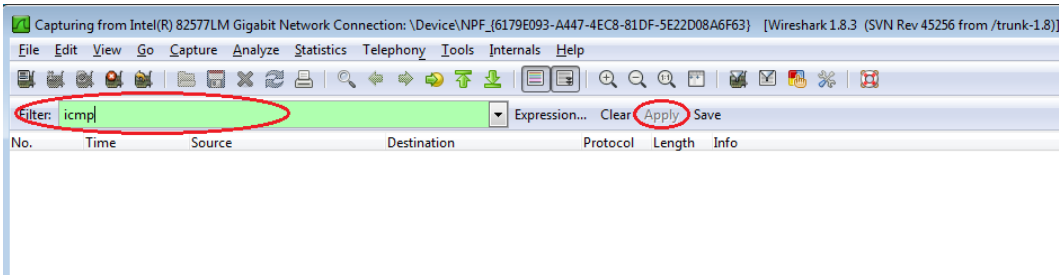
d. 检查了接口正确后，单击“**开始**”开始数据捕获。



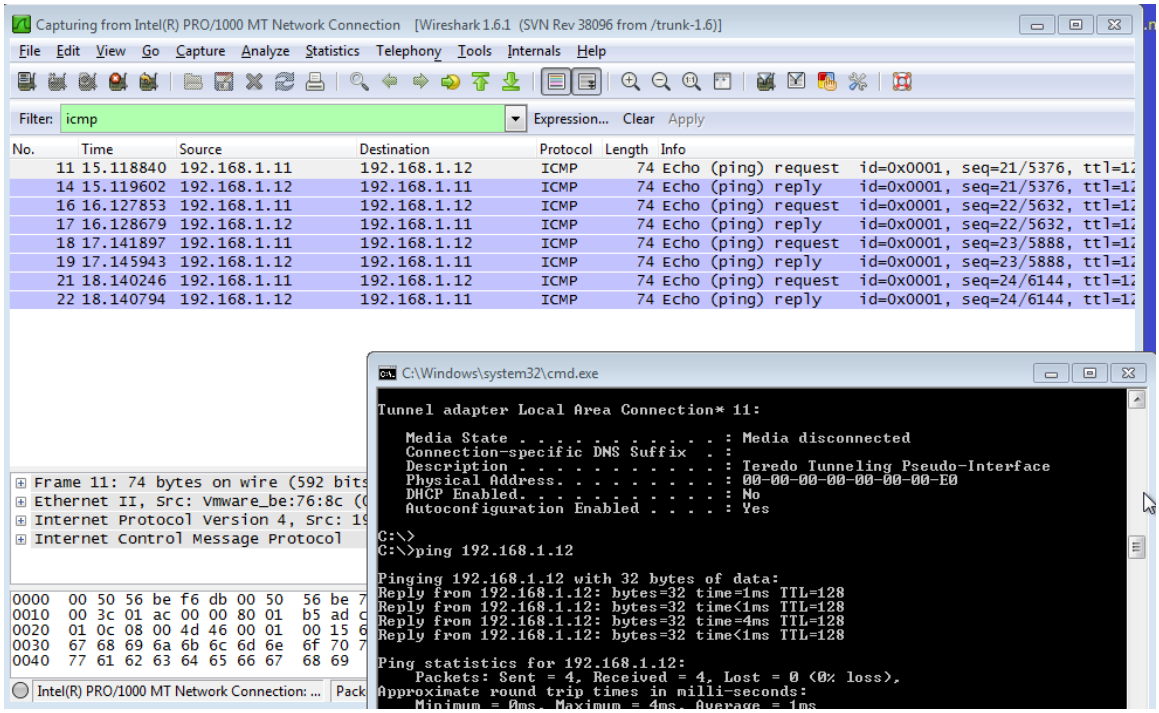
信息将开始从 Wireshark 中的顶部部分向下滚动。根据协议，数据行将以不同的颜色显示。



e. 该信息可能会滚动得非常快，具体取决于您的 PC 和 LAN 之间进行的是什么通信。我们可以应用一个过滤器，以便更轻松地查看和使用通过 Wireshark 捕获的数据。对于本实验，我们只关注显示 ICMP (ping) PDU。在 Wireshark 顶部的“过滤器”框中键入 **icmp**，然后按 Enter 键或单击“**应用**”按钮以仅查看 ICMP (ping) PDU。

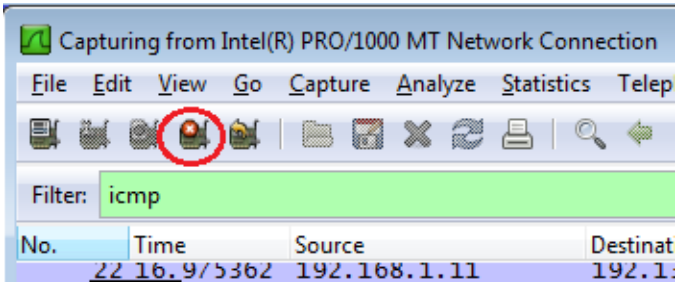


f. 此过滤器将会使顶部窗口中的所有数据全部消失，但您仍在捕获接口上的流量。打开您之前打开过的命令提示符窗口，对您从团队成员那里获得的 IP 地址执行 ping 操作。注意，您会开始看到数据再次显示在 Wireshark 的顶部窗口中。



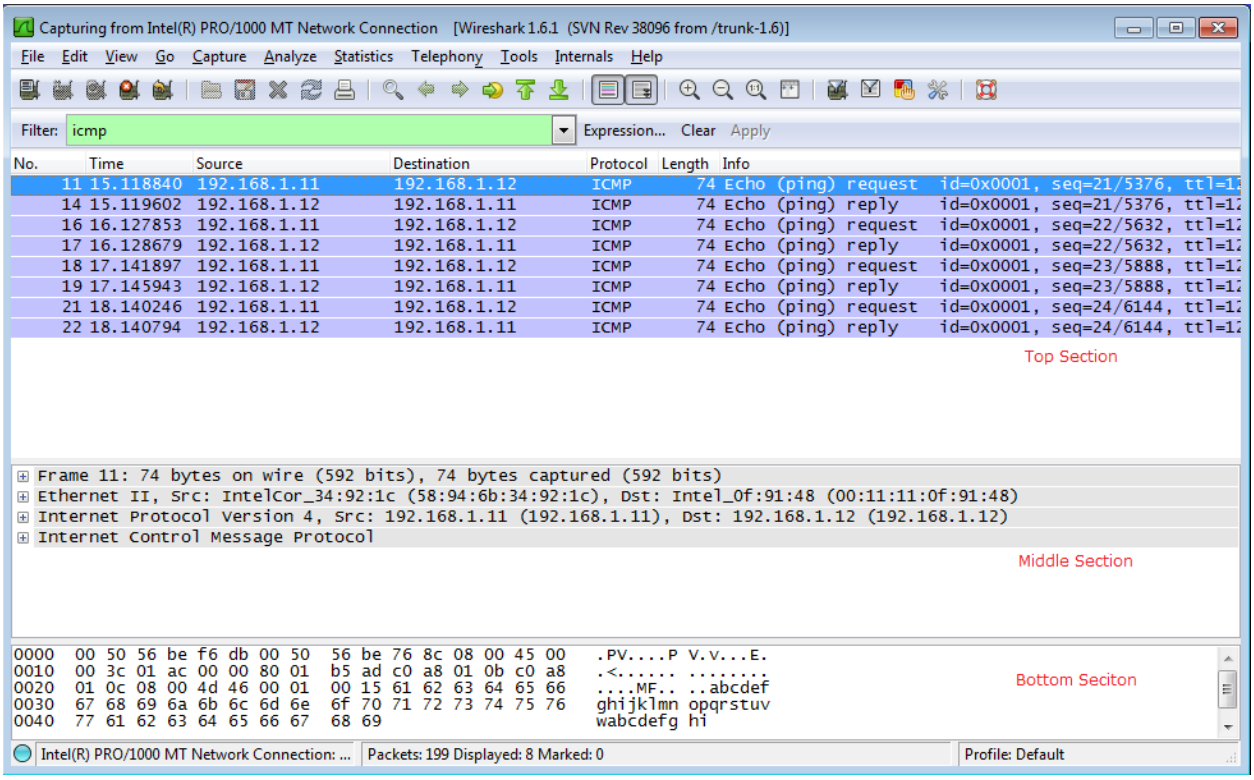
注意：如果您的团队成员的 PC 没有对您的 ping 操作做出响应，这可能是因为他们的 PC 防火墙拦截了这些请求。请参阅 Appendix A: Allowing ICMP Traffic Through a Firewall，了解如何允许 ICMP 流量通过使用 Windows 7 系统的防火墙。

g. 单击**停止捕获**图标停止捕获数据。

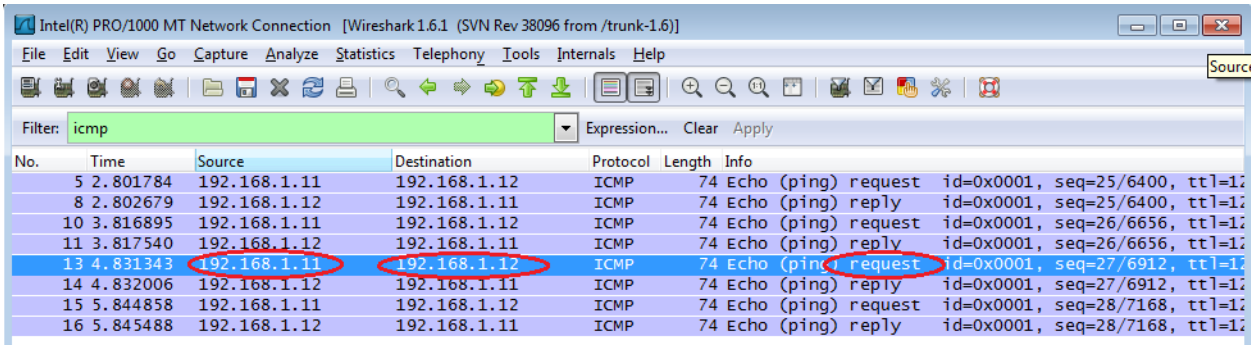


第 3 步： 研究捕获的数据。

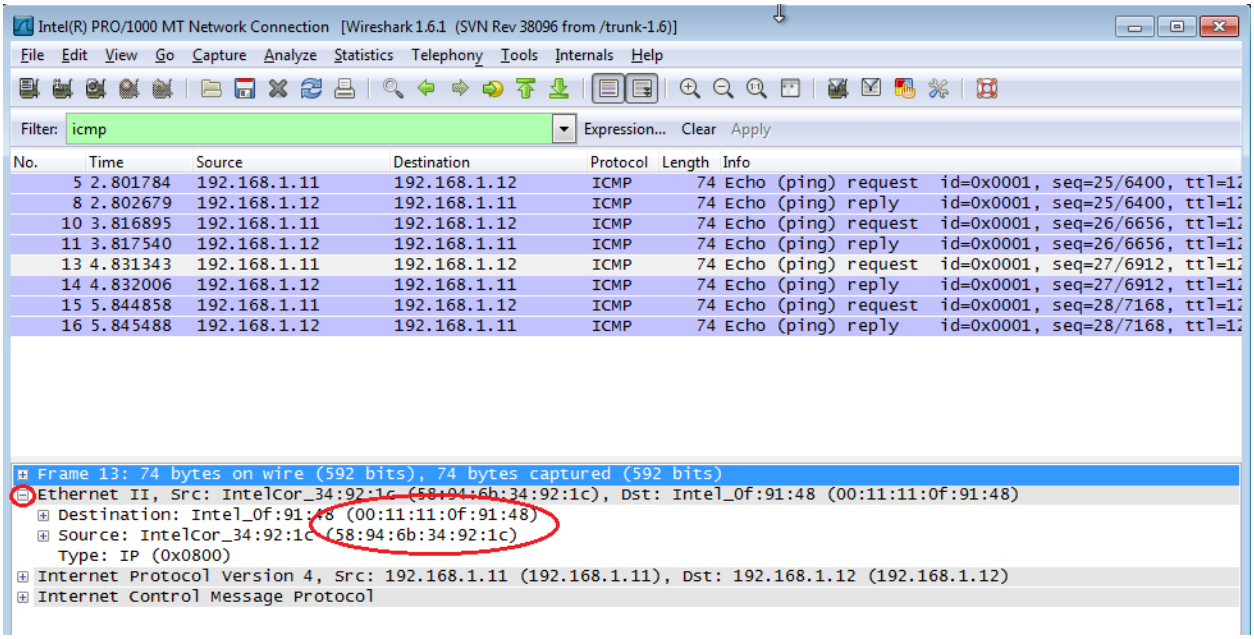
在第 3 步中，研究由您的团队成员的 PC 的 ping 请求生成的数据。Wireshark 数据分三个部分显示：1) 顶部部分显示捕获的 PDU 帧列表，其中列出 IP 数据包信息总结，2) 中间部分列出屏幕顶部部分中所选帧的 PDU 信息，并根据协议层分隔捕获的 PDU 帧，以及 3) 底部部分显示每层的原始数据。原始数据同时以十六进制和十进制形式显示。



a. 单击 Wireshark 顶部部分的第一个 ICMP 请求 PDU 帧。注意“源”列中有您的 PC 的 IP 地址，而“目的地”列包含您对其进行了 ping 操作的团队成员 PC 的 IP 地址。



b. 仍然在顶部部分选中此 PDU 帧，导航至中间部分。单击“以太网 II”行左侧的加号，查看目的 MAC 地址和源 MAC 地址。



源 MAC 地址是否与您的 PC 的接口匹配？

Wireshark 中的目的 MAC 地址是否与您的团队成员的 MAC 地址匹配？

您的 PC 如何获得对其执行了 ping 操作的 PC 的 MAC 地址？

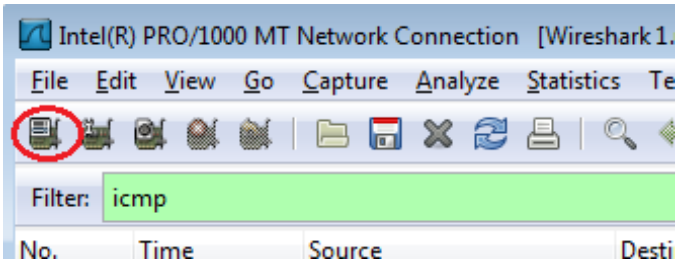
注意：在之前的已捕获 ICMP 请求示例中，ICMP 数据封装在 IPv4 数据包 PDU（IPv4 报头）内，然后该 PDU 会被封装到以太网 II 帧的 PDU（以太网 II 报头）中，以便在 LAN 上传输。

第 2 部分：在 Wireshark 中捕获和分析远程 ICMP 数据

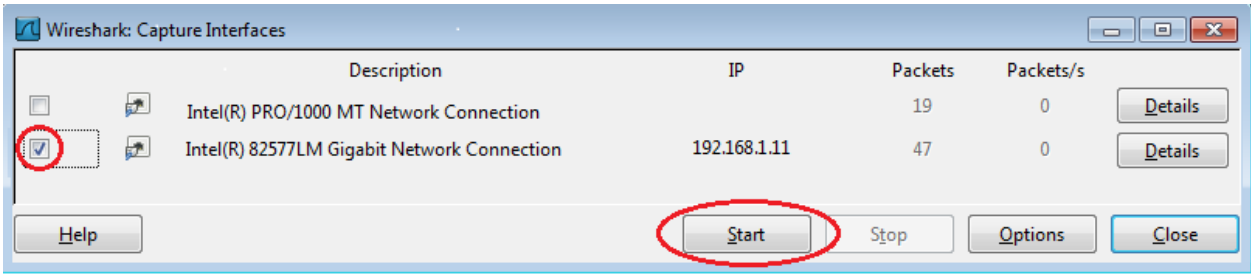
在本实验第 2 部分，您将对远程主机（不在 LAN 中的主机）执行 ping 操作，并研究从这些 ping 操作生成的数据。然后您将确定该数据与第 1 部分中研究的数据有何不同。

第 1 步：开始捕获接口上的数据。

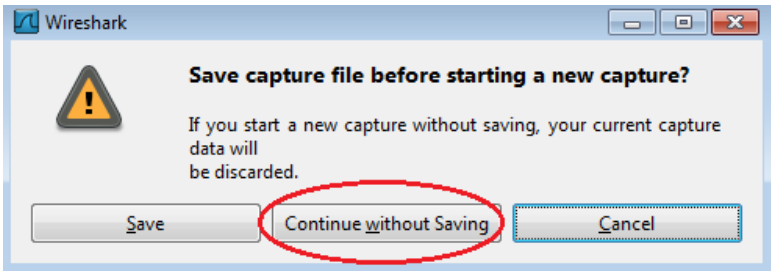
a. 单击**接口列表**图标，再次打开 PC 接口列表。



b. 确保选中 LAN 接口旁的复选框，然后单击“**开始**”。

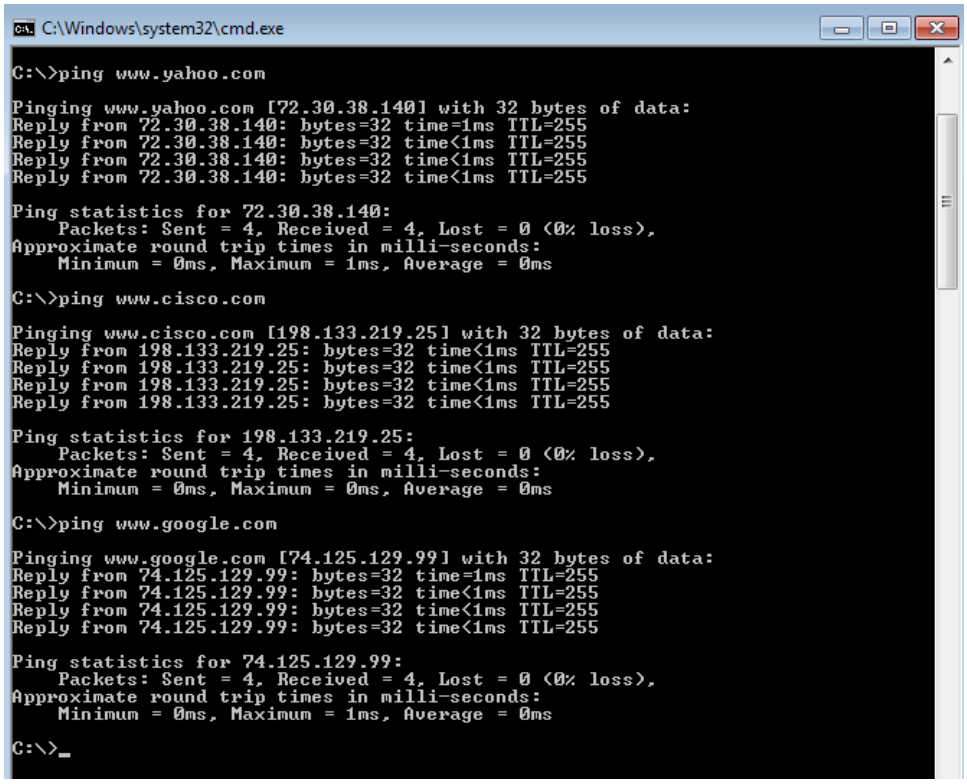


c. 此时会出现一个窗口提示在开始另一捕获之前先保存之前捕获的数据。无需保存此数据。单击“**继续但不保存**”。



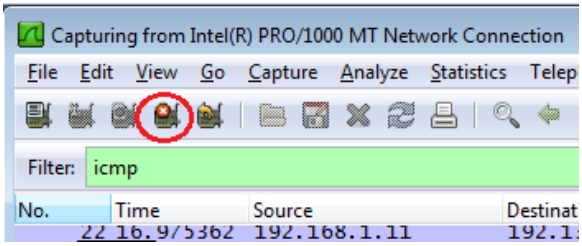
d. 在捕获处于活动状态时，对以下三个网站 URL 执行 ping 操作：

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



注意：当您对所列 URL 执行 ping 操作时，注意一下，域名服务器 (DNS) 会将 URL 转换为 IP 地址。注意每个 URL 收到的 IP 地址。

e. 您可以单击**停止捕获**图标停止捕获数据。



第 2 步： 检查并分析来自远程主机的数据。

a. 查看 Wireshark 中捕获的数据，检查您执行了 ping 操作的三个位置的 IP 和 MAC 地址。在所提供的空格中列出所有三个位置的目的 IP 和 MAC 地址。

第 1 个位置： IP： . . . MAC： : : : : :

第 2 个位置： IP： . . . MAC： : : : : :

第 3 个位置： IP： . . . MAC： : : : : :

b. 此信息有何意义？

c. 该信息与您在第 1 部分收到的本地 ping 信息有何不同？

思考

为什么 Wireshark 显示本地主机的实际 MAC 地址，但不显示远程主机的实际 MAC 地址？

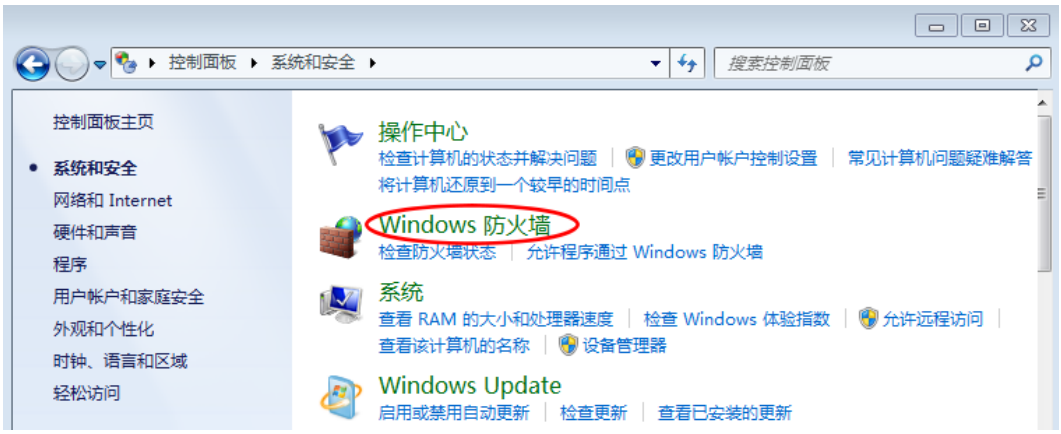
附录 A：允许 ICMP 流量通过防火墙

如果您的团队成员无法对您的 PC 执行 ping 操作，可能是防火墙拦截了这些请求。该附录描述了如何在防火墙中创建规则以允许 ping 请求。其中还描述了在您完成实验后如何禁用该新 ICMP 规则。

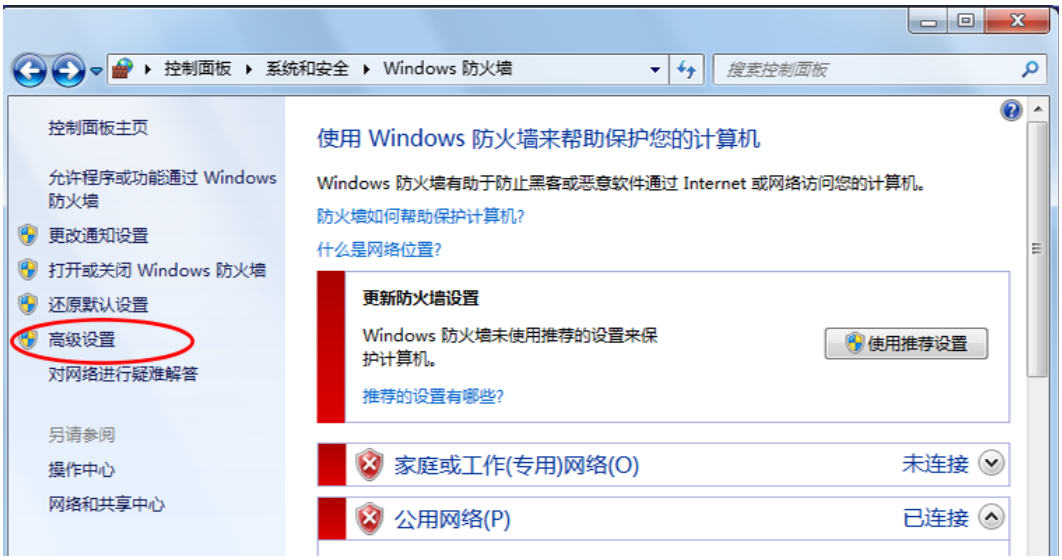
第 1 步： 创建一个新的入站规则，以允许 ICMP 流量通过防火墙。

a. 从“控制面板”中，单击“**系统和安全**”选项。

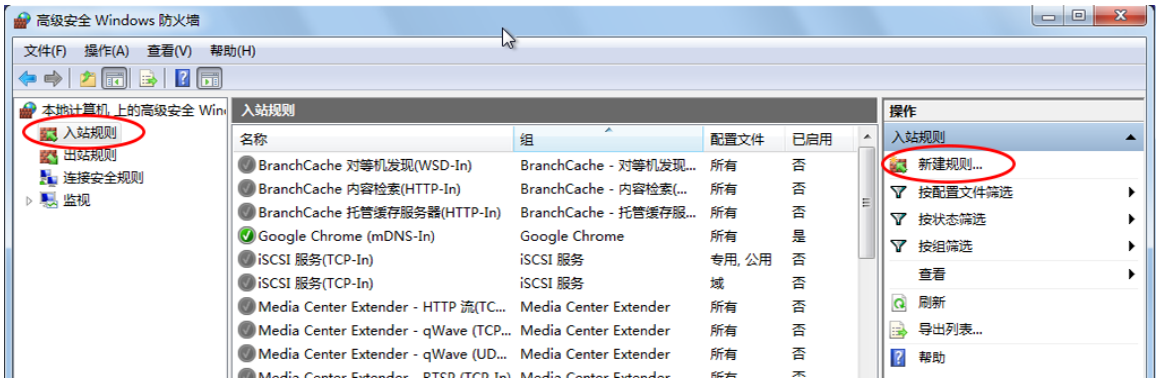
b. 在“系统和安全”窗口，单击“**Windows 防火墙**”。



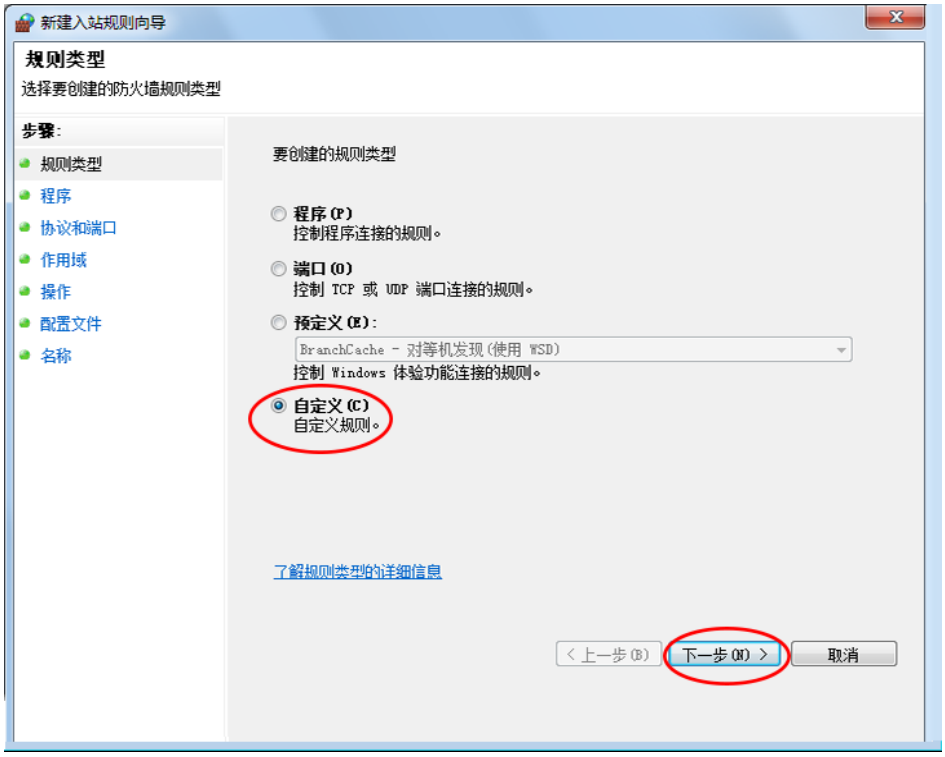
c. 在“Windows 防火墙”窗口的左窗格中，单击“**高级设置**”。



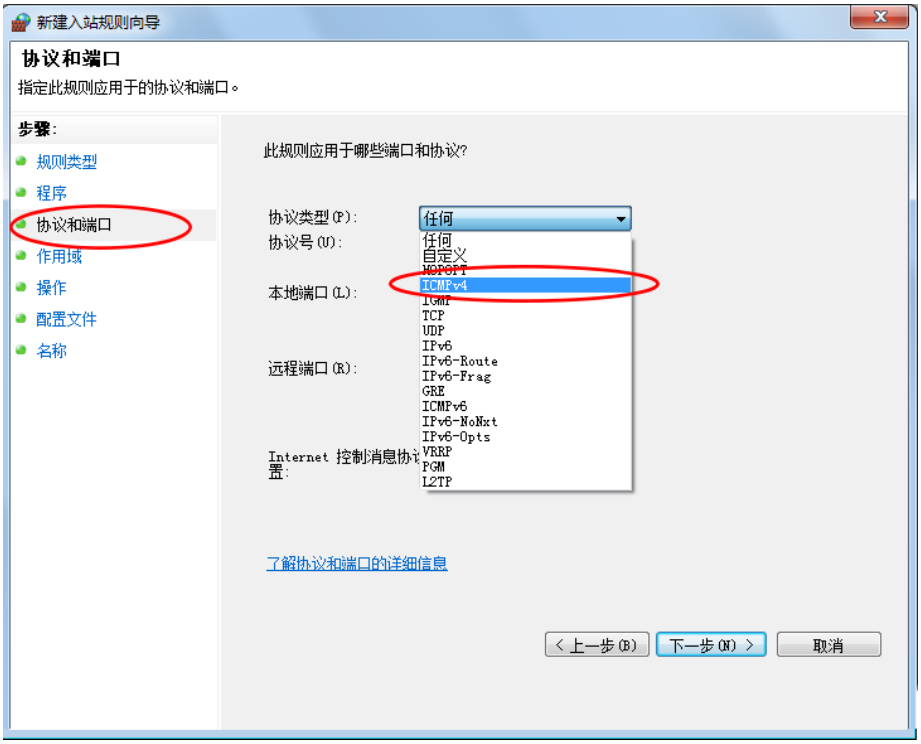
d. 在“高级安全”窗口，选择左侧栏中的“**入站规则**”选项，然后在右侧栏中单击“**新建规则…**”。



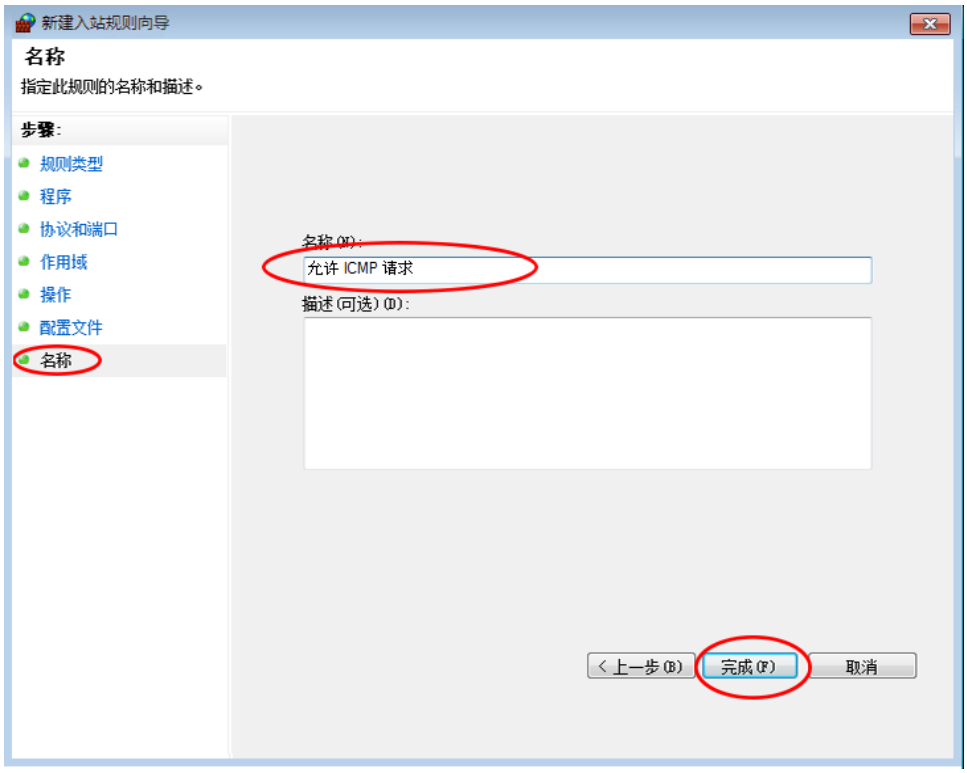
e. 这将启动新建入站规则向导。在“规则类型”屏幕上，单击“**自定义**”单选按钮，然后单击“**下一步**”。



f. 在左窗格中，单击“**协议和端口**”选项，并使用“协议类型”下拉菜单，选择“**ICMPv4**”，然后单击“**下一步**”。



g. 在左窗格中，单击“**名称**”选项，在“名称”字段中键入“**允许 ICMP 请求**”。单击“**完成**”。

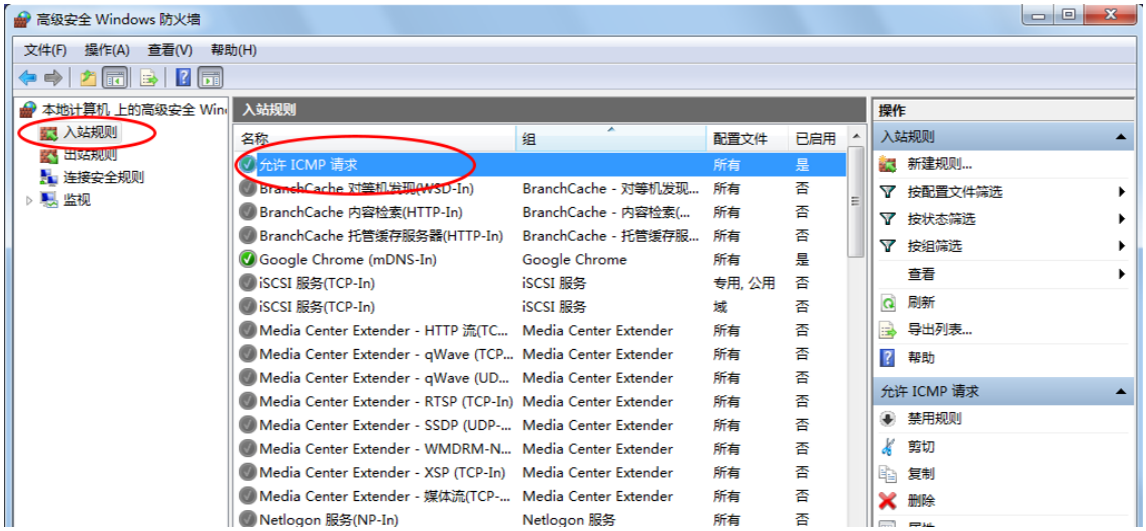


此新规则应该会允许您的团队成员收到来自您的 PC 的 ping 响应。

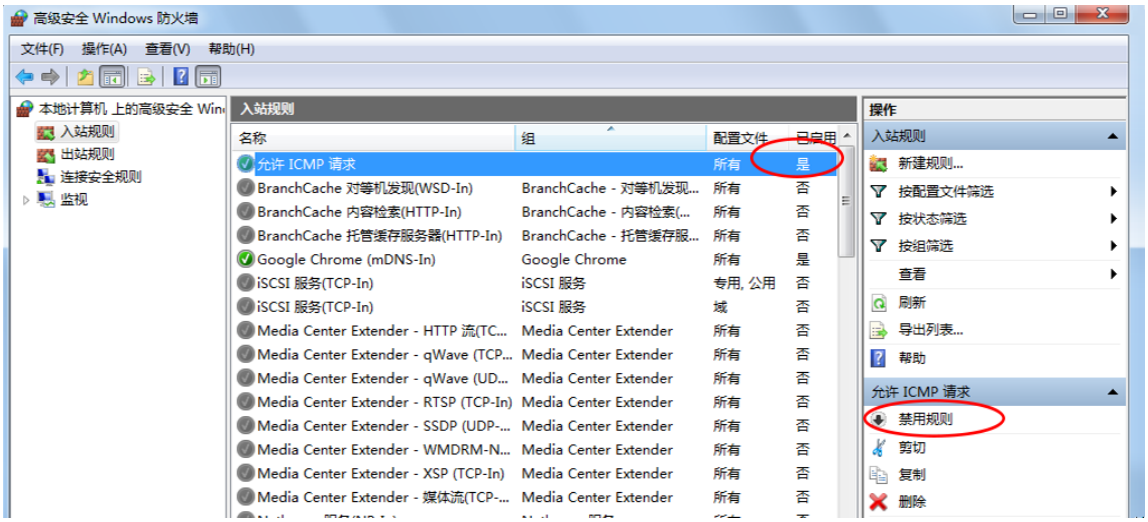
第 2 步： 禁用或删除此新 ICMP 规则。

实验完成后，您可能希望禁用，或者删除您在第 1 步中创建的新规则。以后您可以使用“**禁用规则**”选项再次启用该规则。删除该规则，则会将其从“入站规则”列表中永久删除。

a. 在“高级安全”窗口中，单击左窗格中的“**入站规则**”，然后找到您在第 1 步中创建的规则。



b. 要禁用此规则，请单击“**禁用规则**”选项。选择此选项后，您将会看到该选项变为“**启用规则**”。您可以在“禁用规则”和“启用规则”之间来回切换；规则的状态还会在“入站规则”列表的“已启用”列中显示。



c. 要永久删除此 ICMP 规则，请单击“**删除**”。如果选择此选项，您将必须重新创建规则来允许 ICMP 响应。