



GNS3 实验1

1. 在 GNS3 中创建你的第一个拓扑

现在是时候在 GNS3 中创建你的第一个拓扑了。由于本实验需要使用 Alpine Linux，因此请根据实验0第2.4节提供的指南，在你的 GNS3 中安装 Alpine Linux 设备。此外，请确保在使用 GNS3 图形界面之前，已运行 GNS3 虚拟机（使用 VMware Workstation Player 或 VMware Fusion）。

首先，从文件菜单中创建一个“空白项目”，然后通过将三个元素拖放到项目中来构建图1所示的拓扑。这三个元素分别是 2 台 Alpine Linux 主机、1 个以太网交换机和 1 个 NAT 云。

要连接构成该拓扑的各个元素，可以通过图1中 **红色圆圈** 标出的部分添加链路。然后，你需要启动拓扑中的活动元素。为此，请单击工具栏上的 **启动/恢复所有节点** 按钮（图1中用 **绿色箭头** 标出）。几秒钟后，两台 Alpine Linux 主机将启动，你可以通过控制台访问它们。要打开这些控制台，请单击图1中用 **蓝色方框** 标出的部分。这将为你打开两个控制台，用于管理 **AlpineLinux-1** 和 **AlpineLinux-2** 主机。你也可以通过右键单击每台 Alpine Linux 主机并选择“> 控制台”选项来完成相同操作。图2显示了已打开的控制台以及创建的拓扑。

在构建此网络拓扑时，另一个重要点是：每当您从侧边栏将新元素（例如以太网交换机或NAT）拖放到拓扑中时，应选择GNS虚拟机作为服务器。这一关键点如图3所示，它能确保GNS3虚拟机作为这些元素的服务器，为准确模拟以太网交换机和NAT设备在GNS3拓扑中的行为提供必要的资源和功能。

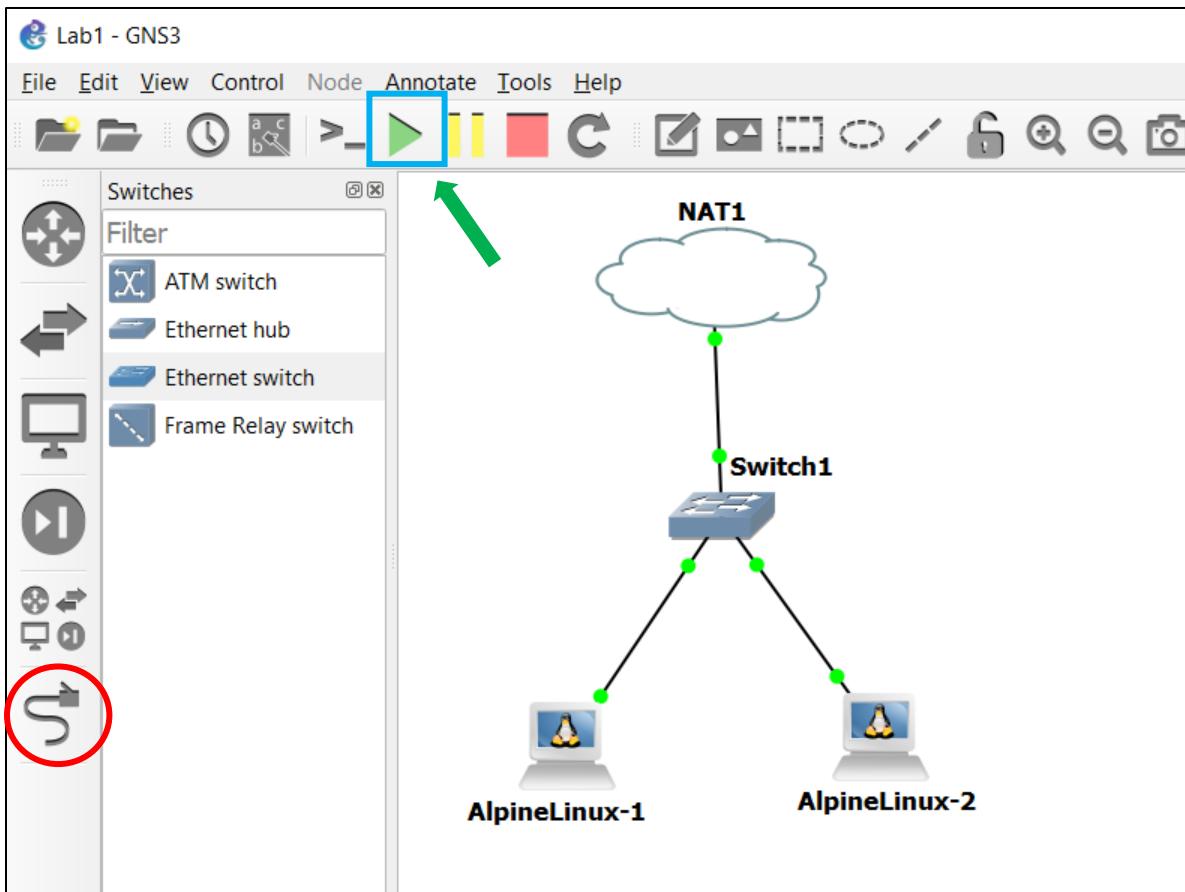


图1. 第一个GNS3项目的拓扑结构。

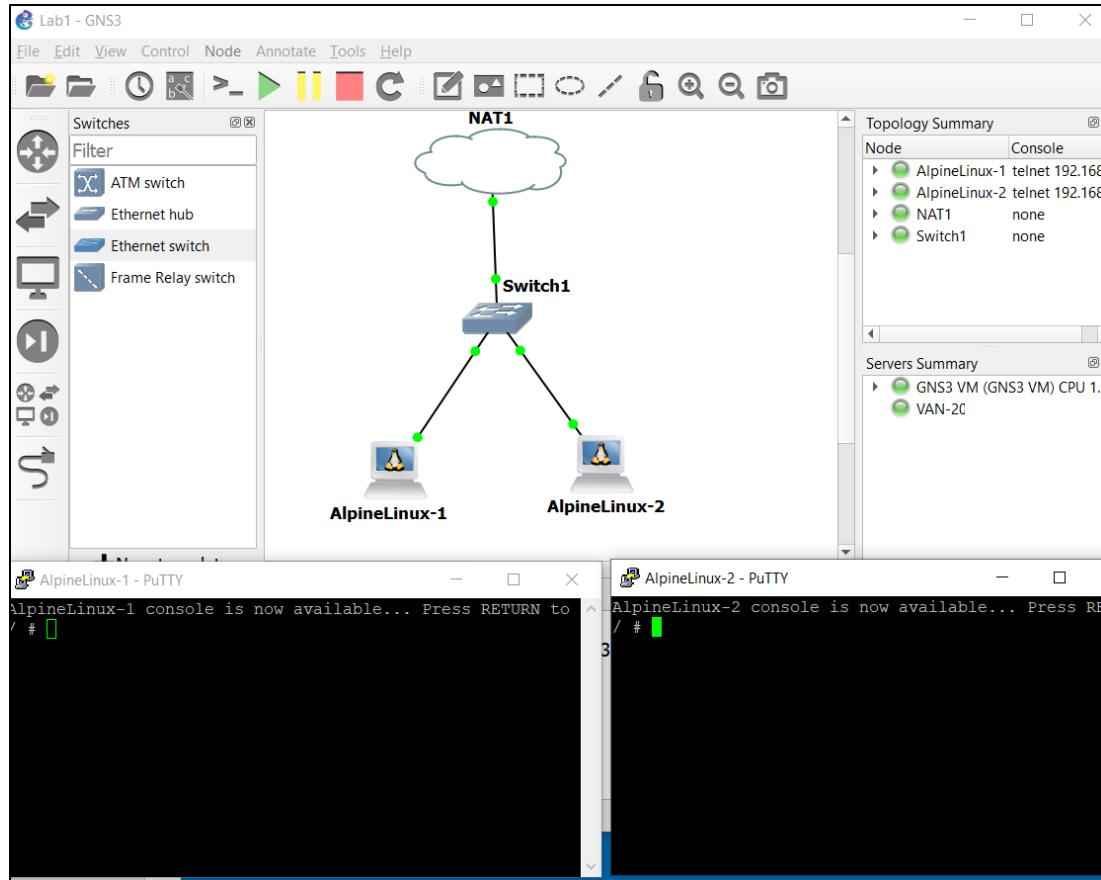


图 2. 用于访问 Alpine Linux 主机的两个控制台。

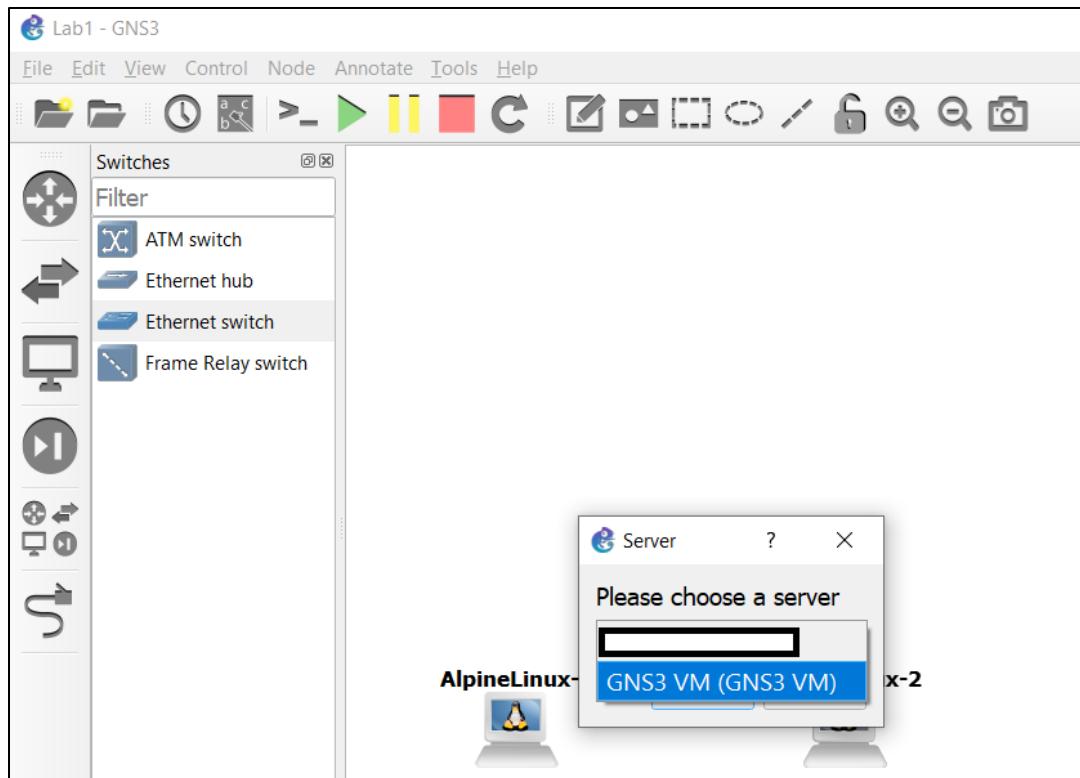


图3。将以太网交换机添加到拓扑时，选择GNS3 VM作为服务器。

1.1. 在GNS3拓扑中生成网络流量

现在，你需要在 Alpine Linux 主机的网络接口上配置 IP 地址，以实现与互联网以及其他拓扑中的主机进行通信。为此，首先在每个 Alpine Linux 主机上运行 ‘ifconfig’ 命令，查看 Alpine Linux 中可用的网络接口。默认情况下，每个 Alpine Linux 拥有一个 eth0（以太网 0）和一个 lo（回环）接口。第一个接口（eth0）是可用于发送/接收流量的接口。在生成任何流量之前，你必须为此接口分配一个 IP 地址，这可以通过运行 ‘udhcpc -i eth0’ 命令来完成。如果 Alpine Linux 成功从 DHCP 服务器（你的网络中）获取了 IP 地址，你将在 ‘udhcpc’ 以及 ‘ifconfig’ 命令的输出中看到新的 IP 地址，如图 4 所示。

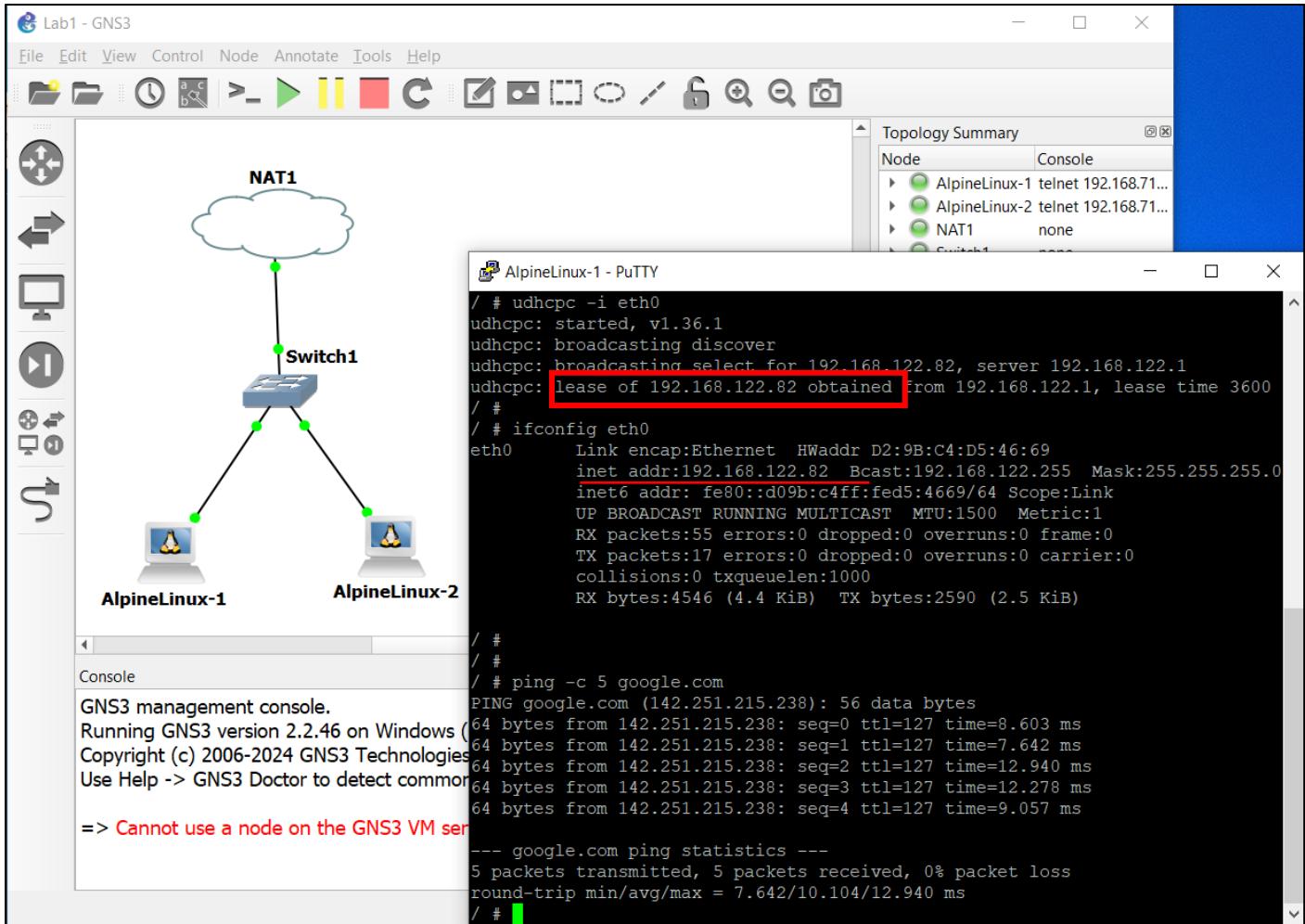


图4. 使用`DHCP客户端为Alpine Linux主机分配IP地址。

完成上述步骤后，请回答以下问题：

- 1) 每个Alpine Linux主机使用‘dhcpc’命令获取的IP地址是什么？你可以运行‘ifconfig’命令查看分配给每个主机的IP地址。
- 2) 运行‘ping’命令，如图4所示，从Alpine Linux 1访问google.com。根据ping命令的输出，往返时间(RTT)的平均值为多少毫秒(ms)？
- 3) 在获取分配给Alpine Linux2的IP地址后，在Alpine Linux1上打开一个控制台，并对Alpine Linux2的IP地址运行‘ping’命令，即‘ping -c 5 <Alpine Linux2 IP>’。然后，从ping命令的输出中记录平均RTT值。
- 4) 最后两个问题的答案之间的时间差是多少？为什么？
- 5) 运行‘apk update’，然后运行‘apk add tcpdump’命令，在Alpine Linux1主机上安装‘tcpdump’，这是Linux中一个知名的网络数据包捕获工具。

分发。然后，运行 ‘tcpdump -h’ 命令以检查数据包是否安装成功。从上一条命令的输出中，你刚刚安装的 ‘tcpdump’ 软件包的版本是什么？

6) 现在，在 Alpine Linux1 上运行 ‘tcpdump -i eth0 -w capture_lab1.pcap’ 命令。该命令将在此主机的 eth0 接口上启用数据包捕获，并将捕获的流量存储在一个名为 capture_lab1.pcap 的文件中（注意：此文件名与下面示例图中的名称不同）。当 tcpdump 命令在 Alpine Linux1 上运行时，请在 Alpine Linux2 上打开一个控制台，并从该主机 ping Alpine Linux1。为此，可运行 ‘ping -c 5 <Alpine Linux1 IP>’ 命令。在 Alpine Linux2 上完成 ping 命令执行后，按下 Ctrl + C 键以停止 Alpine Linux1 控制台上的 tcpdump 命令。要检查 Alpine Linux1 上存储的文件，请在控制台运行 ‘ls -l’ 命令，该命令会显示 ‘capture_lab1.pcap’，如图 5 所示。根据 ‘ls -l’ 命令的输出，确定该文件的大小是多少？

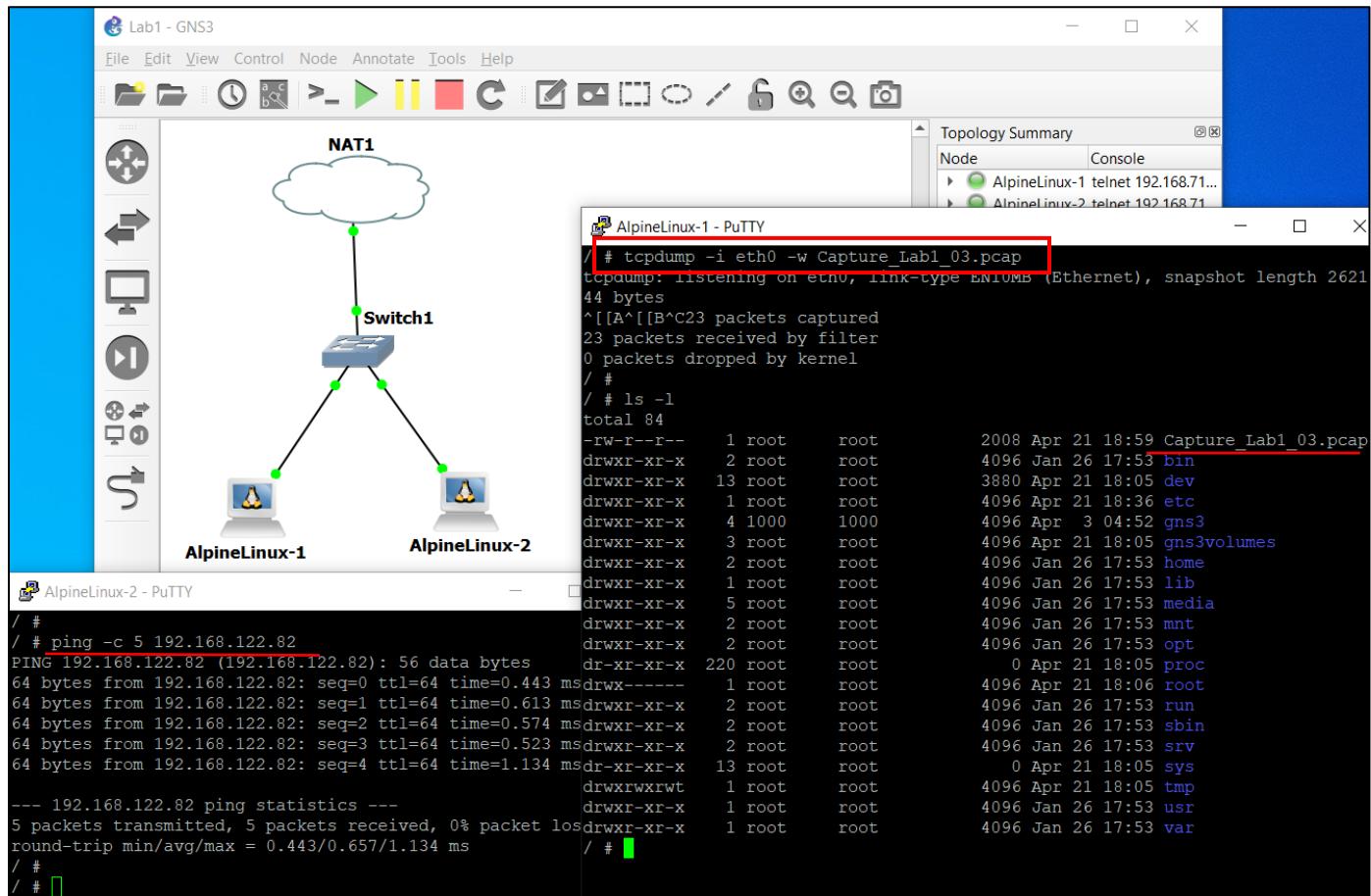


图5。示例：在Alpine Linux2上使用tcpdump捕获生成的ICMP流量。

1.2 从GNS3向您的计算机传输文件

我们已将通过接口 eth0 捕获的流量写入 capture_lab1.pcap 文件中。现在的问题是，如何将该文件从 GNS3 中的虚拟化环境（即 Alpine 虚拟机）传输到你计算机上安装的操作系统中。有多种方法可以实现此操作，但最简单的方法之一是使用 SSH（安全外壳）服务。第一步是在你的 Microsoft Windows 10 或 macOS 上启用 SSH 服务。

在Windows系统中，默认情况下未安装SSH服务，但可以通过执行以下步骤完成。首先，您需要通过点击任务栏上的“**设置**”图标并输入“设置”来进入Windows的“**系统**”，然后选择“可选功能”。接着，通过选择“添加功能”并搜索“OpenSSH 服务器”，即可在Windows上安装该服务。成功安装后，您应能在“已安装的功能”部分搜索并看到 OpenSSH 服务器，如图6所示。此处也展示了在 Windows 10 中安装 SSH 服务所需步骤的顺序。

设置 → 系统 → 可选功能 → 添加功能 → OpenSSH 服务器

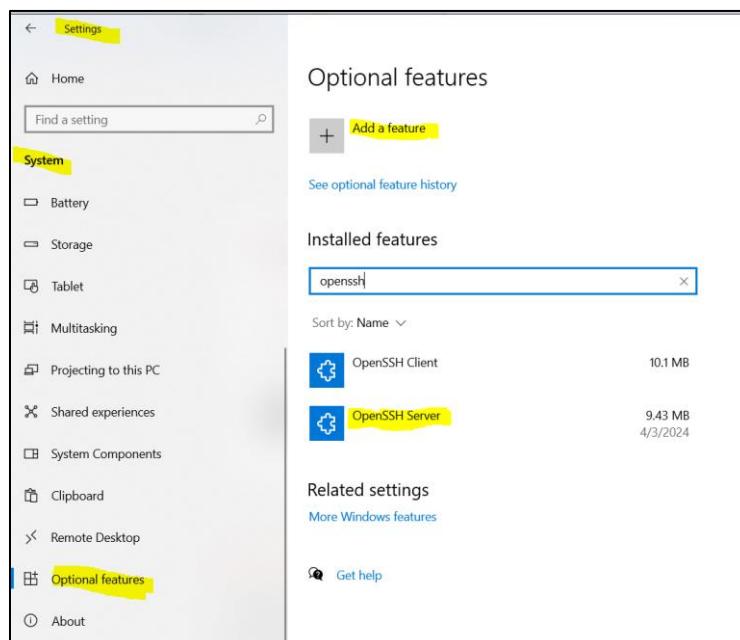


图6. 在Windows 10中安装OpenSSH服务。

安装 OpenSSH 服务后，您必须通过运行 ‘**services.msc**’ 命令，然后右键单击 ‘**OpenSSH Server**’ 并选择 ‘启动’ 选项来启动它。如果服务成功启动，服务状态将变为‘正在运行’，如图7所示。

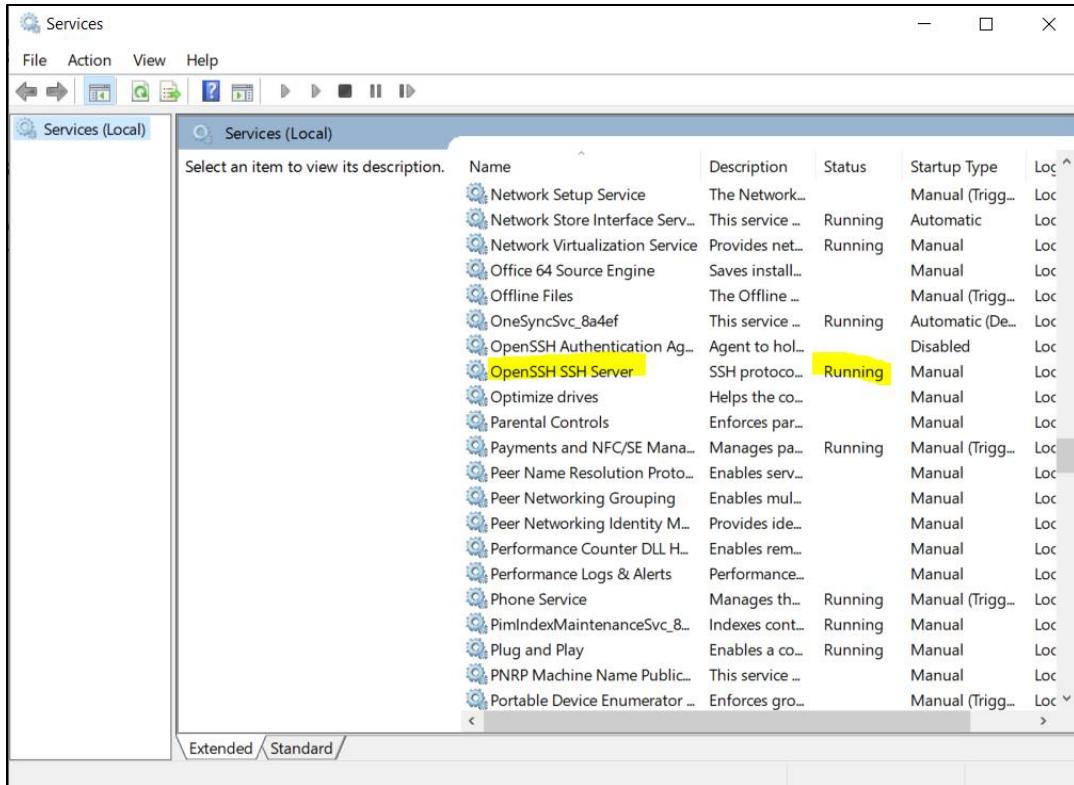


图7. 在Windows 10中启用OpenSSH服务。

在尝试测试 OpenSSH 服务之前，最后一步是在您的 Windows 系统中创建一个本地用户账户。如果您已经有一个活动的本地用户账户（而不是域用户），则可以跳过此步骤。现在，您可以使用 ‘scp’ 或安全复制命令，将文件从 Alpine Linux 复制到命令中指定的 `username` 用户的 Windows 主目录下。默认情况下，Alpine Linux 上未安装 ‘scp’ 命令，可通过在终端中运行 ‘apk update’ 和 ‘apk add openssh’ 命令进行安装。然后，您需要按照以下示例所示运行 ‘scp’ 命令。如果文件传输成功完成，您可以在 `C:\Users\username` 文件夹下找到 `capture_lab1.pcap` 文件，并可通过 Wireshark 应用程序打开它。

```
# scp capture_lab1.pcap <username>@<Windows IP>:~
```

如果您的用户名是 `bob`，且 Windows 的 IP 地址为 `192.168.1.10`，则 ‘`scp`’ 命令将如下所示：

```
# scp capture01.pcap bob@192.168.1.10:~
```

要获取 Windows 的 IP 地址，您可以在命令行 (cmd) 中运行 ‘`ipconfig`’。如果在 ‘`ipconfig`’ 的输出中看到多个 IP 地址，请使用分配给无线接口的那个（如果通过 Wi-Fi 连接互联网）。

在 macOS 中，要启用 SSH 服务，您需要进入 “**系统设置**” 并选择 “通用” 选项。然后，选择 “共享”，并启用 “远程登录”，如图 8 所示。

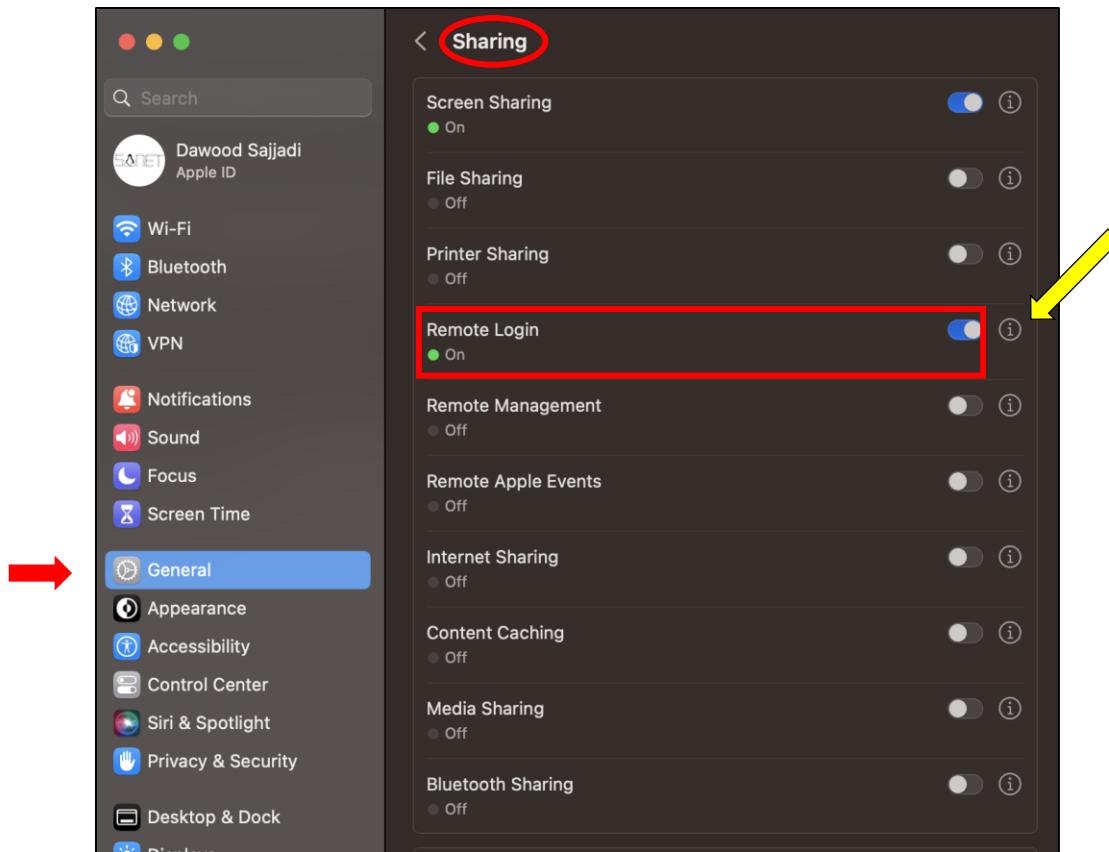


图8。在macOS中启用远程登录（SSH）

此外，您还必须允许希望经由 SSH 服务登录到您的 macOS 的用户进行访问。为此，您需要单击图 26 中黄色箭头所标注的圆形图标。单击该图标后，将弹出一个类似于图 26 所示的窗口，您可以使用 +/- 符号向现有列表中添加或删除用户。要确认 macOS 上 SSH 服务的状态，您可以在终端中运行以下命令。如果该命令有输出结果，则表示 SSH 服务器正在运行，您可以使用“scp”来复制文件。

```
# netstat -na | grep LISTEN | grep .22
```

在macOs上，该命令应在Alpine linux 1上输入，其操作方式与Windows平台相同

：~ 是文件存储位置。

```
scp capture_lab1.pcap username@ip: ~
```

然后，你可以输入ls -l来查看当前目录中列出的捕获文件，并确认文件传输已成功。

您可以在以下位置找到有关 scp 的更多信息：

<https://linux.die.net/man/1/scp>

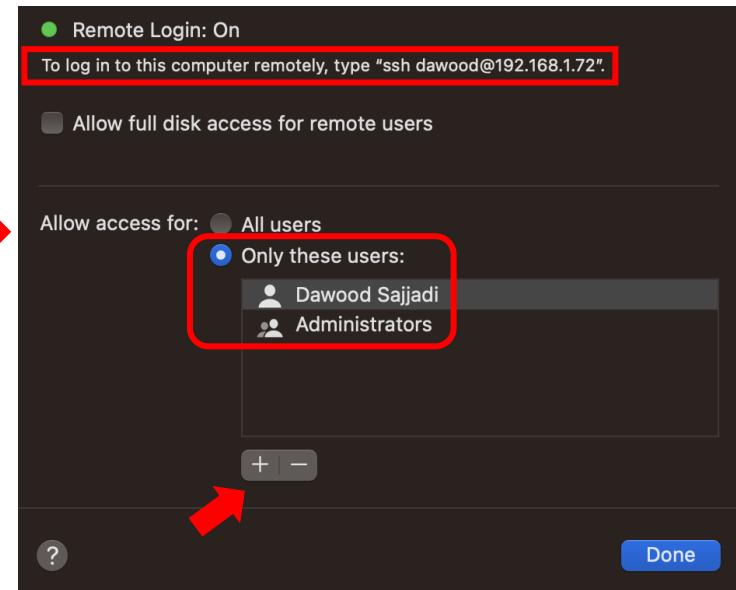


图26. 允许选定用户进行远程登录（SSH）访问。

在下一个实验中，我们将使用 Wireshark 打开捕获的文件，并分析该文件中的数据包。

作者：

Dawood Sajjadi

Maryam Tanha