Lab1: Connect to the ESXi Server

OBJECTIVES

This lab is designed to demonstrate how to connect the ESXi server via SSH tunneling using Putty in order to establish your virtual laboratory environment from workstations in our classroom, your notebook computer, and also from your home computer. Campus network has a lot of firewall rules to protect many workstations and servers. In order to connect your ESXi server, we will use SSH tunneling on campus and use VPN and SSH tunneling to connect from off campus.

VMWare provides the vSphere client for ESXi 5.5 for MS Windows only. A lot of people use MS Windows operating system for their workstations in their work environment. ESX will provide the web-based client for ESXi 6.0 or above.

In this lab, we will be creating a Linux systems administration environment for students and they will be able write scripts in Linux systems administration environment so that student can automate tasks.

PROCEDURE I

How-To: Connect to the ESXi system via Putty tunneling

Port overview:

Port	Purpose	Traffic Type
443 (Default)	HTTPS access vSphere Client access to vCenter Server vSphere Client access to ESXi hosts vSphere Client access to vSphere Update Manager	Incoming TCP
902 (Default)	vSphere Client access to virtual machine consoles	Incoming and outgoing TCP, outgoing UDP

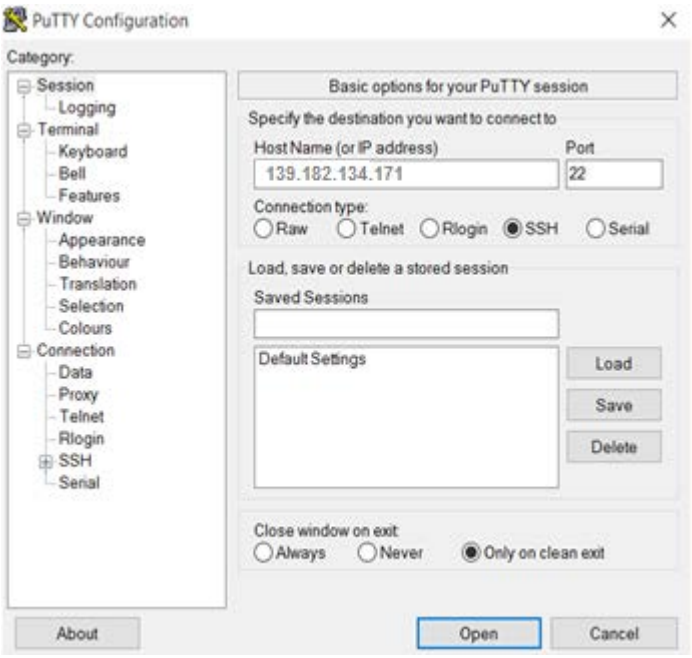
Coyote Wall Password Change:

You must change your temporary password given to you with your own password.
This password is used to log into Coyote Wall for access to the Repository and ESXi Servers.

Step 1:

Open Putty and add these parameters:

Hostname (or IP address): 139.182.134.171
Port: 22



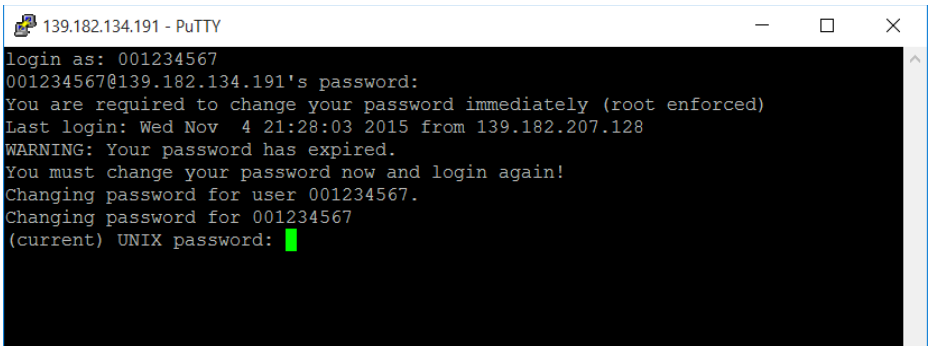
Click **Open.**

Step 2:

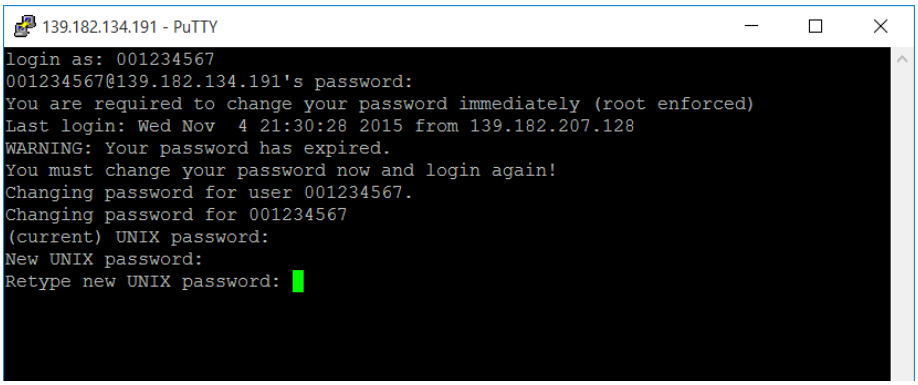
Type in your Coyote ID as the username and your supplied password to log into Coyote Wall.

Once you login to Coyote Wall, you are forced to change your supplied password with your own.

NOTE: Type your given password first where it says (current) as shown below. The window will close if you type in your given password wrong. That means re-logging into Wall and trying again.



After you type in your given password, type in your new password as shown below. The window will close once you change your password.



Only open Coyote Wall when connecting to the Coyote Repository or your ESXi Server as shown in the next tutorials.

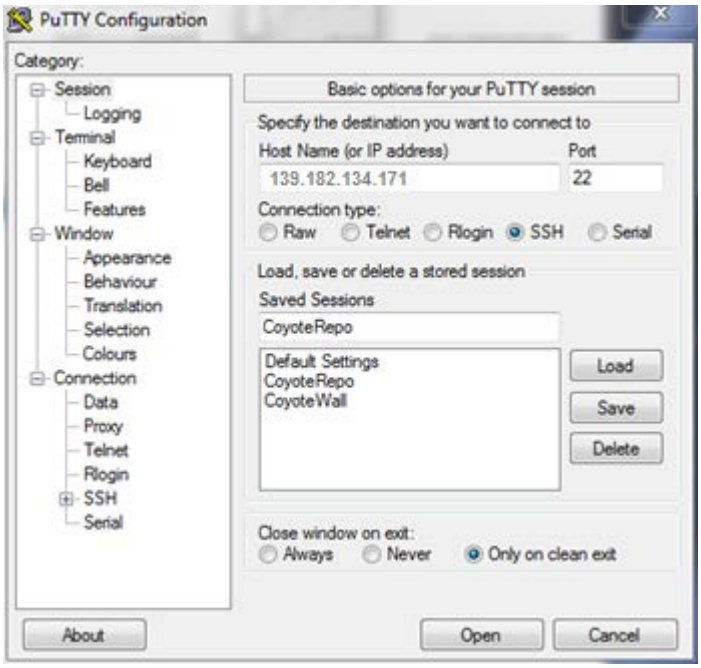
Connect to Coyote Repository for ISO's:

Step 1:

Open Putty and create a new session named CoyoteRepo.

Hostname (or IP address): 139.182.134.171
Port: 22

Click **Save** on right side.



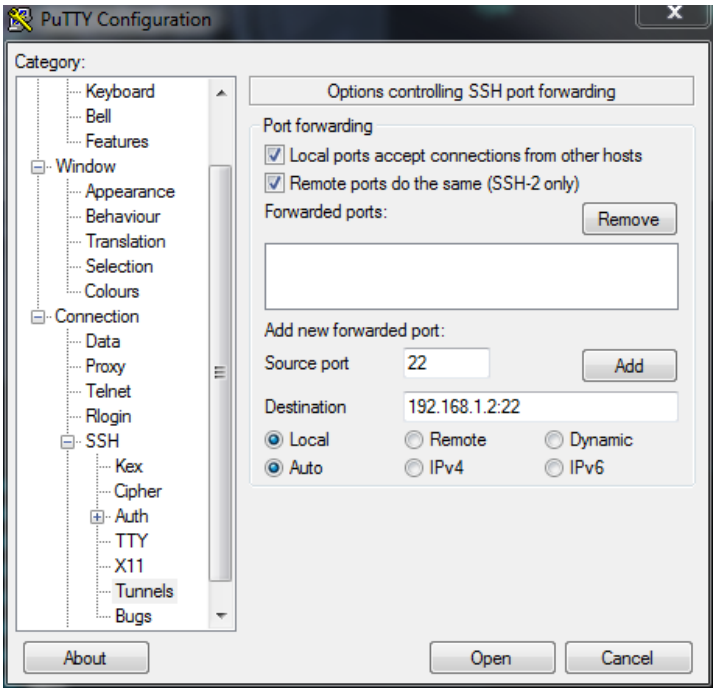
Step 2:

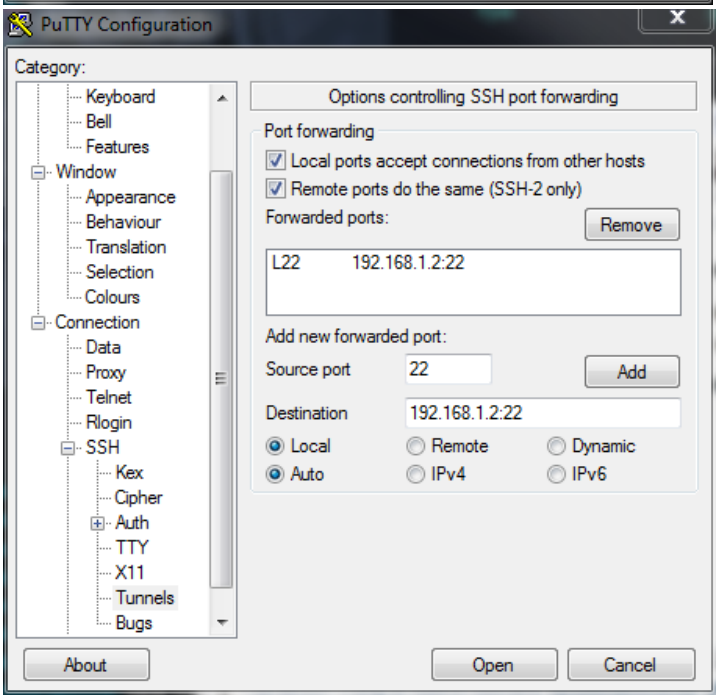
Under **Category** on left side, navigate to:

Connection → SSH → Tunnels

Forward ports: 192.168.1.2

1. **Check Both Checkboxes**
2. **Under Source port:** 22
3. **Under Destination:** 192.168.1.2:22





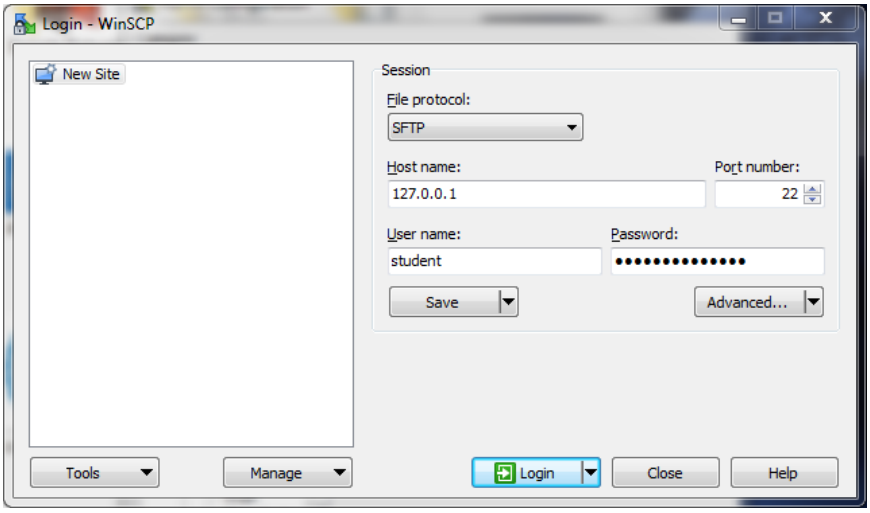
When the port is listed, go back to **Session** under **Category** on left side and click **Save.**

Click **Open.**

Step 3:

1. Now once logged into Coyote Wall with your new password, do not close putty.
2. Open a separate program called **WinSCP** with:

   File Protocol: SFTP
   IP/Hostname: 127.0.0.1
   Username: student
   Port Number: 22
   Password: *Sy$adm1nstudent*



3. Open **images** folder.
4. Drag and drop the images you need for the class to your computer.

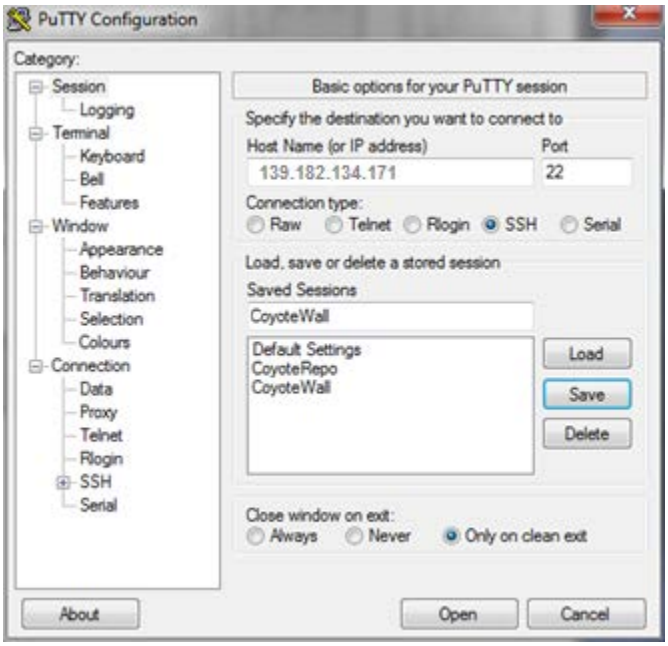
NOTE: Keep Putty tunnel open and logged into CoyoteWall while using **WinSCP**. Close Putty when done transferring images.

Connect to ESXi Host:

Step 1:

a. Close all open Putty sessions.
b. Open Putty and create a new session named **CoyoteWall**.

Hostname (or IP address): 139.182.134.171
Port: 22
Click **Save** on right side.



Step 2:

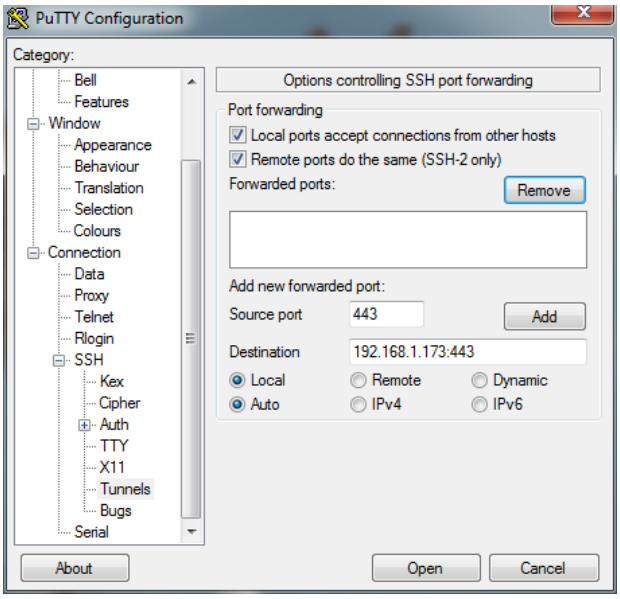
Under **Category** on left side, navigate to:

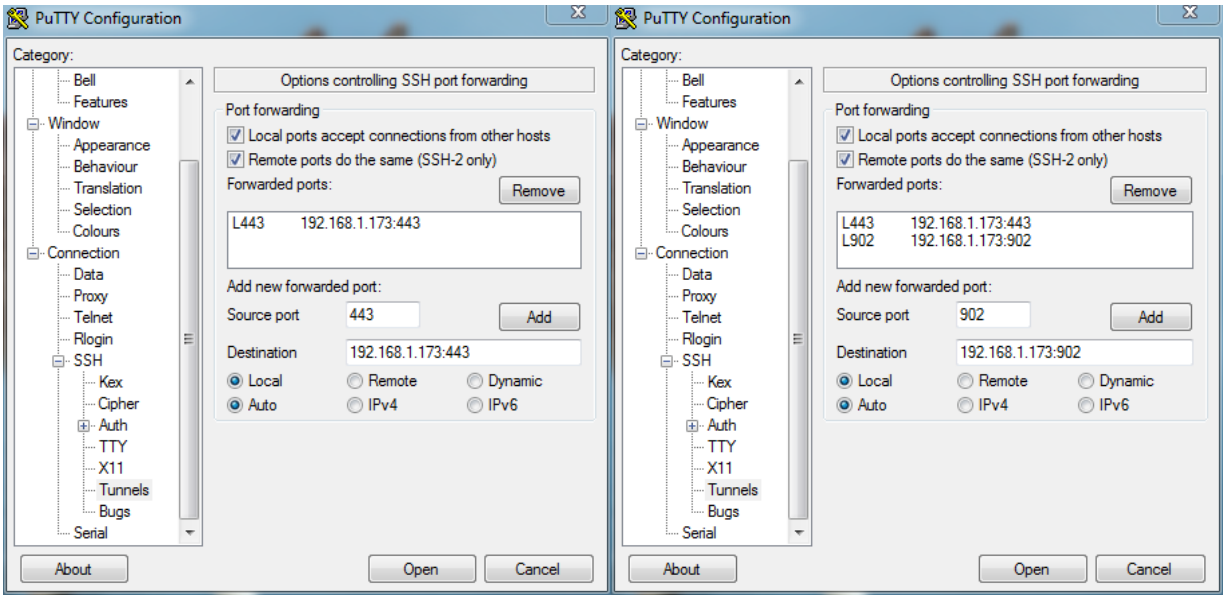
Connection → SSH → Tunnels

Forward ports for tunneling into ESXi host

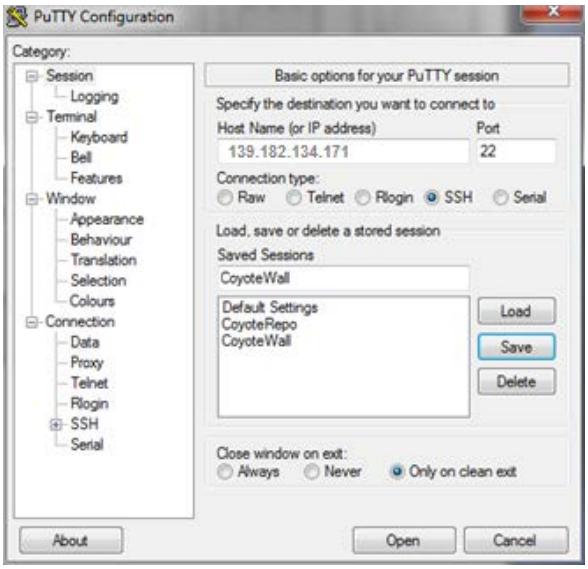
NOTE: 192.168.1.**173** is used as an example, use your own server ip!

Under **Source** port: 443
Under **Destination**: 192.168.1.173:443
Click **Add** and do the same for port 902
Steps shown in Putty below:





When both are listed, go back to **Session** under **Category** on left side and click **Save.**



Click **Open.**

Step 3:

Login to Coyote Wall using your Coyote ID and your password.
A tunnel has been created from your local computer and into the public side of the system. Now you must use this tunnel to login to your vSphere Client using 127.0.0.1.

IP address/Name: 127.0.0.1
Username: sysadmin# (your given number here)
Password: (Given to you)

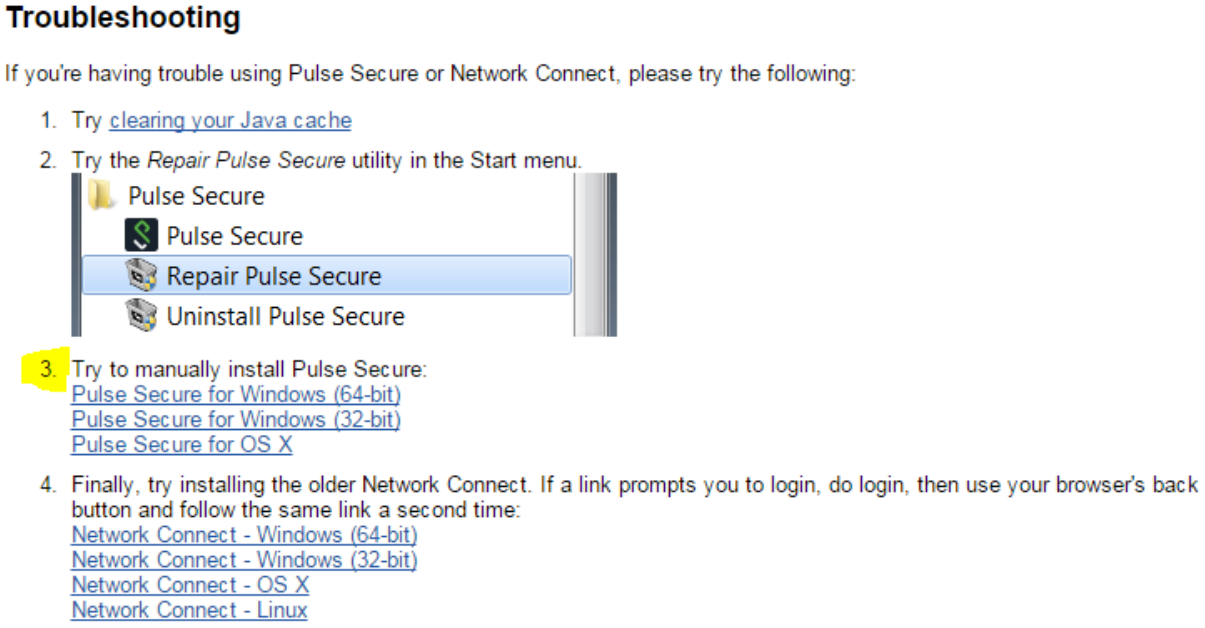
PROCEDURE II

Connect to ESXi Host via CSUSB VPN:

Step 1:

a. Download CSUSB's VPN software to run on your computer:
http://iso.csusb.edu/download/vpn

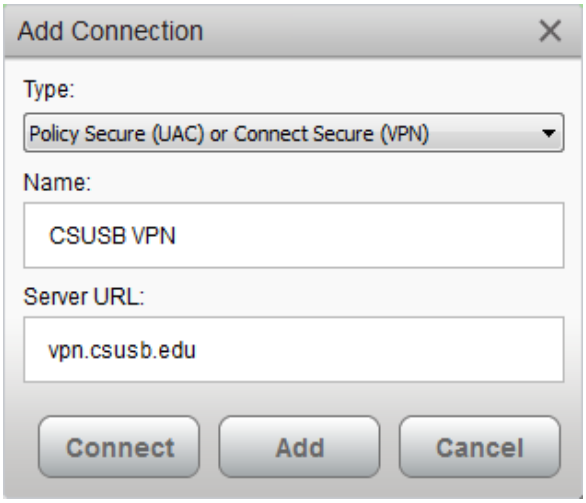
It is found near the **bottom** of the page under Troubleshooting, number 3. Select the appropriate version for your operating system.



b. When you start Pulse Secure, create a CSUSB connection:

1. To the right of **Connections**, click the plus sign.

2. Under **Add Connection** keep type **Policy Secure (UAC) or Connect Secure (VPN).**
3. Name your connection something like **CSUSB VPN**.
4. Type the VPN server URL: **vpn.csusb.edu**
5. Click **Connect.**



6. U**ser Name:** Coyote ID
   Password: MyCoyote Password

7. Click **Connect.**

Note: It will say connection complete in the taskbar at the bottom right.

Bug: When connecting, the program may also create a second CSUSB connection, in which there is no difference.

Step 2:

c. Download VMWare's vSphere Client to run on your computer:

1. Log into CoyoteRepo as shown on Page 4 of this document.
2. Download and run **VMware-viclient-all-5.5.0-3024345.exe** to your computer to install VMWare vSphere Client.
3. You will use this software to access your ESXi server.

LAB REPORT

NAME: _____

QUESTION:

1. Why we use Windows workstation for ESXi Server administration?
2. Why we use SSH tunneling in this lab?
3. How SSH tunneling works?
4. What is VPN?
5. Why we use VPN in this lab?
6. Why we do above lab tasks for script programming class?

UNIX COMMANDS:

List UNIX commands you know.

TROUBLESHOOTING

From this lab what troubles did you have? How did you resolve the problems?

Identify the problem:
Problem 1:

How did you solve the problem?
Solution 1:

.

.

Identify the problem:
Problem n:

How did you solve the problem?
Solution n: