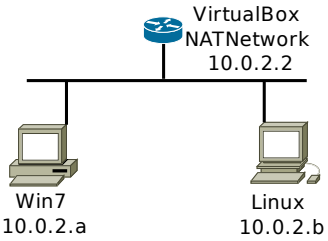
Networking
LLTD Worksheet

Use Microsoft's Link-Layer Topology Discovery (LLTD) protocol

In this worksheet you will install an LLTD responder service in your Ubuntu VM, so that it can respond when your Windows VM tries to map the LAN. The LLTD protocol can be observed in Wireshark, using Ethernet type 0x88d9.



Introduction

The Link Layer Topology Discovery (LLTD) protocol is a Microsoft protocol that allows a computer on a Local Area Network (LAN) to discover other devices on the LAN, and how they are connected to each other. Windows 7 and Vista run a mapper application that seeks other devices; if those are running a responder application then the mapper can identify their "location" and connectivity within the LAN.

In this exercise we are building a demonstration Microsoft responder application for Linux, so that the Windows VM can determine how it is connected. Our virtual network's topology is actually very simple; however, Wireshark captures of the LAN traffic involved reveal a protocol that operates at Layer 2, without involving higher-protocols such as IP or ARP

Modify your VM environment

1. Start Virtualbox.

   In the Oracle VM Virtualbox Manager window, click on:
   File → Preferences → Network

2. In the "NAT Networks" tab, click the "Plus" icon on the right.

   You should see a new named network, perhaps "NatNetwork". Whatever the name is, remember it.

3. Click on "OK".
4. Select on of your VMs, and click on **Settings → Network**.
5. Adapter 1 is (probably) currently attached to "NAT". Change it to be attached to "NAT network".

   Select the same name that was added to the "NAT Networks" earlier.

6. Click on "OK".
7. Repeat this setting for your other VM as well.

Now start your VMs. They should come up with different IP addresses, and you should be able to ping each one from the other one. You should also be able to ping 4.2.2.2 from either one. Can you ping "google.com"? (*Hint*: no.)

Set up the LLTD service in Ubuntu

1. If it's not already running, start Virtualbox.
2. Start your Ubuntu Linux VM. Open a shell (command terminal).
3. Run the command `sudo apt install build-essential`. This installs the gcc compiler and other tools on your VM.

4. Run the command `sudo apt install linux-headers-`uname -r``.

   Important: Notice that "uname -r" is in *backquotes*, which are on the key above the Tab key on the left side of the keyboard. (Try running the command `uname -r` by itself to see what you get.)

5. Enter these commands, one at a time:

```
wget --no-check-certificate https://montcs.bloomu.edu/VM-LAN/LLTD-software/LLTD-linux.zip
unzip LLTD-linux.zip
cd LLTD
```

   These commands obtain a copy of the LLTD source code.

6. Now build the LLTD service on Ubuntu:

```
cd "Sample Code/native-linux/"
make
sudo cp lld2d /usr/sbin/
cd ../..
```

7. Configure the service-startup script for your VM. First run "ifconfig" again, and verify your network interface's name. It should be something like "eth0", or "enp0s3"; it is the one that has an IP address of 10.2.0.⟨something⟩.

   If the interface name is "eth0", you're good to go — skip to the next step.

   If it *isn't* "eth0", then edit the file "lld2d" (you can do this with a command like `gedit lld2d`). Change line 16 from "INTFACE=eth0" — replace the "eth0" with whatever your VM's interface name is (such as "enp0s3"). Save the file.

8. Now set up the service-startup script, and start the service:

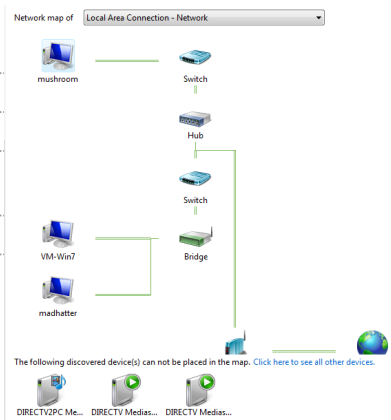
```
chmod 755 lld2d


sudo ./lld2d start
```

9. From your Ubuntu terminal, run the command `sudo wireshark`.
   1. Select the "eth0"/"enp0s3" interface.
   2. Click on "Start".
   3. Put in a display filter:
      `eth.type==0x88d9`.

      You won't see anything until you do the next step...

Try out the protocol in the Windows VM



1. Start your Windows VM.
2. Click the "Start" button, and open the "Control Panel".
3. Under the "Network and Internet" group, choose "View network status and tasks".
4. On the right-hand side, click on "See full map".
5. Windows should draw out a map showing your two VMs, connected through a switch. It may also show a connection through a gateway to the Internet.

   The instructor's home network is shown at right, for comparison. (Woo-hoo!)

6. Look at your Wireshark display (in the Linux VM). You should see a number of Ethernet frames, all carrying the LLTD protocol.

   Scan through the Ethernet headers and data areas of the frames. Can you find the frames that contain the hosts' responses to the LLTD mapper request?

Congratulations! You've mapped your Local-Area Network at the Data-Link layer.

Shut down both VMs. You're done with this lab.

File last modified *09/24/2016 05:46:02*