Purpose

This application note will help you capture data packets on a switched Ethernet network.

Introduction

The complex nature of a communications network can make troubleshooting problems somewhat elusive. One useful procedure to find an elusive application problem is to capture and analyze the actual raw data that is traversing a network. This captured data is called a “data packet” or “packet trace.” Also, software developers occasionally request a packet trace to analyze application performance/operation of equipment on customer premises.

Generally, you capture packet traces with a laptop (as we show in the examples). Because of the mobility of a laptop, you can capture a packet trace from any point on a network—although most desktop personal computers can also do this. A packet capture application (usually called a “sniffer”) is also necessary for this procedure; in this application note we use Wireshark (http://www.wireshark.org/).

Note: We will use several applications in this note but will not give the installation procedures. These applications have standard installation procedures and our use here will not deviate from those norms.

Before we give procedures to attach and configure the laptop and software, there is a problem that is necessary for you to know—and to know how to solve—as described in the subsequent two sections:

Problem: The Network will not Naturally Forward Certain Packets to the Laptop

Because Ethernet switches only forward packets to the destination address contained in the packet header, there is a problem when you are plugged into one port of a switch while attempting to capture:

- Packets that are destined for a machine plugged into a different port or
- The data packets on a backbone port—for example, a fiber port as shown here.

If the network is operating correctly, the laptop cannot capture all data packets that are destined for the signal controller (ASC/3) or traversing the network backbone link (fiber). The laptop can only detect broadcast packets, unicast packets destined for the laptop itself and, in some network configurations, multicast traffic.
Two Possible Solutions to the Problem

1. **Connect to a Hub** – If it is necessary to capture packets destined for the signal controller, you can temporarily install a hub as shown here—but you cannot capture packets on backbone links with this solution.

   A hub is a network repeater that forwards all packets out of all ports at all times. Thus the laptop would detect and be able to capture packets destined to go to or from the signal controller.

   Hubs are inefficient and can be difficult to find.

2. **Enable Port Mirroring** – You can enable your Ethernet switch to mirror (copy) data packets on one switch port to a second switch port. Different manufacturers refer to this function in different terms. RuggedCom refers to this as Port Mirroring and we use its switch in our example. Cisco refers to this as Switched Port Analyzer (SPAN) port and other manufacturers refer to this as Roving Analysis.

**Notes**

Necessary information before you start the procedure that follows on the subsequent pages:

- For this procedure, your laptop must have a serial port and most laptops do not have a serial port. The easiest way to configure your laptop with a serial port is to buy and install a USB to DB-9 (serial port) adapter. The steps to do this depend on the manufacturer of that device and are outside of the scope of this application note.

- If you use an Ethernet switch manufacturer other than RuggedCom, its procedure will be different.

- If you use a terminal application other than Tera Term, its procedure will be different.
Procedure to Enable Port Mirroring

1. As shown here, connect an RS-232 serial cable from the laptop serial port to the console port of the switch.

2. Obtain a terminal application to enable the port monitoring feature in the switch. In our example, we use Tera Term. Currently, this is free open-source software that you can download from: http://en.sourceforge.jp/projects/ttssh2/

3. Launch the Tera Term terminal application.

4. You should see the configuration window shown here.

5. As shown, select the serial port to which you are connected.

6. Click OK.

   **Note:** Switch settings are usually silkscreened on the RuggedCom units as shown below.

7. From the setup menu, select “Serial Port.”

8. You should see the port setup window shown here.

9. Configure your serial port to match the settings of the switch.

10. Click OK.
11. Press **Enter**.

12. The login screen comes into view.

13. Enter your username and password. Factory default is:
   - Username: admin
   - Password: admin

14. From the “Main Menu” select **Ethernet Ports > Configure Port Mirroring**.
Now we will enable port mirroring and indicate:

- Where the laptop/sniffer is connected (that will be our “Target Port”) and
- The device to capture data to/from—in our example an ASC/3.

15. Refer back to the illustration on Page 1.
16. Note that the ASC/3 is connected to Port 6 and the laptop is connected to Port 2.

17. For our example, the configuration will look like this (although your setup is probably different).

If you try to capture data packets from a backbone port, then the source ports will be that port. The fiber port in our example would be Port 7.

**Note:** There are two entries for our source port labeled “Egr” and “Ingr”:
- Egr = Egress (departure point)
- Ingr = Ingress (entrance point)

Usually, your interest will be one physical Ethernet port at a time and the number of these entries will be the same. Occasionally, you might desire to trace entry packets from one interface and departure packets from another interface. You can also configure this for these rare applications.
Taking a Trace

Wireshark is a very powerful tool that has many different configuration parameters for a number of different applications. We will focus on what we consider to be the three most common uses:

- **Standard Packet Trace**
- **Filtered Packet Trace**
- **Snapshots**

**Standard Packet Trace** – Use this to take a quick look at network traffic for purposes of general discovery and/or verification.

**Filtered Packet Trace** – You filter out (remove from view) all packets except those you want to see.

**Snapshots** – Packet traces saved to disk on an interval, usually a set amount of time.

**Standard Packet Trace**

We will now start the sniffer application. If you are using Wireshark, you will see a screen similar to this.

Note several things from this initial screen (the areas circled in red):

**Interface List** – This list should show the Ethernet port on your laptop with which you will capture data packets.

**How to Capture** – Make sure you have internet access before you select this. This link will take you to a website with much more detailed information on how to set up Wireshark and packet capture options.

**User’s Guide**
Switched Ethernet Networks

AN2138: How to Capture a Data Packet Trace with Wireshark

1. From the “Interface List,” select your Network Interface Card.

   **Note:** For help to know which interface listed relates to your physical Ethernet port, refer to the Appendix at the end of this application note.

2. Now you will see packets streaming down a screen similar to what you see on this screen. This will capture any and all data packets entering or departing the particular Ethernet port to which you are attached. The amount of data packet traffic you see will probably be overwhelming. Thus, you might wish to narrow down your packet trace to a set of criteria—for example, one IP address.

![Packet Trace Screen](image)

The next section tells you how to filter out all packets except those you want to see.
Filtering with Wireshark

In most cases, you will want a filtered packet trace that shows packets from one particular device. For example, you can filter by IP address and capture/display only packets that are destined for or originate from that particular address.

1. As shown at the top of this screen, from the “Capture” menu select “Capture Filters.”

2. You will see a screen similar to this.

3. Enter the “Filter name” in the box at the bottom of the screen.

   Notice that there are many examples of predefined filters from which you can select. But the “Filter name” is a variable. That is, you can name a filter anything you like.

4. Enter the “Filter string” in the next box. As you would imagine, the “Filter string” values must follow a very strict yet simple set of rules. For one host IP address (as in the example here), you enter:
   - host
   - one space
   - the IP address

   Make sure there are no extra characters such as a space after the IP address.

5. When you are satisfied with your filter string, click [OK].
6. After you are satisfied that you have defined your capture filter correctly, you can start your packet trace.

Notice that the packets shown are destined for or originate from the IP address defined in our capture filter.

In this example, you can see data flowing between a Centracs server and an ASC/3.
Taking Snapshots

Often, network issues are time/event based and/or triggered. That is, issues that are happening infrequently but are not necessarily predictable can be difficult to catch. It can be advantageous in these instances to take periodic snapshots of packet data. When the event occurs, you can inspect the related packet trace.

We will demonstrate here how you would configure Wireshark to capture packet traces in 5-minute intervals.

1. As shown at the top of this screen, from the “Capture” menu select “Options.”

2. You should see the screen shown here. In the three highlighted sections of this screen (the areas circled in red)—from top to bottom:
   - Make sure you select the correct Ethernet interface; refer to the Appendix.
   - You can define a capture filter from this screen if you want (we will not use one in this example).
   - In “Capture File(s)” we will configure Wireshark to take snapshots.

3. To select the directory into which Wireshark will save snapshot files, click Browse….
Before you continue to the details of this process, you should create an empty folder in which to store your sniffer trace files. Anywhere that makes sense to you is fine. We recommend you keep all trace files in a common location, for example:

```
C:\Sniffer\CityName\n```

4. Browse to the directory you created previously and enter a file name in the available field titled “Name”.

Make sure you enter the extension pcap on the file name as shown here.

Notice [Create Folder] on the right side of the screen. You can also use this button to create your directory.

5. Select [OK] and return to the “Capture Options” screen.
Switched Ethernet Networks

AN2138: How to Capture a Data Packet Trace with Wireshark

6. Notice that the path and file name in the file entry window match our last selection.

7. To complete the configuration of this screen and start the process, click to check these boxes and enter numbers as shown:
   - Use multiple files
   - Next file every—5 minute(s)
   - Ring buffer with 72 files

Use multiple files – This is rather self-explanatory; it enables us to save more than one packet capture file.

Next file every—minute(s) – Our goal is to have snapshots of network traffic every 5 minutes, which is defined here.

Ring buffer with 72 files – This defines the maximum number of files that will be kept.

In our example, we can keep a maximum of 6 hours of snapshots. These calculations show you how 72 files store 6 hours:

1 file every 5 minutes X 72 = 360 minutes

= 6 hours

Verify Function

To verify function:

1. Allow some time to pass.

2. Inspect the directory you created. It should show files stacking up as shown here.

Note: The file names start and end with the naming convention you defined. The portion of the file name that Wireshark inserted is an index number and date/time stamp.
Appendix

The purpose of this appendix is to help you know which device to select from the “Interface list.”

Even though your laptop might only have one Ethernet port, it is likely to have a number of devices listed here.

The easiest way to know which one of these entries represents your physical Ethernet port is to check your “Network Connections” screen shown here.

In most cases it will be the connection labeled “Local Area Connection”. Also, it will not be grayed out as most of the other interfaces. Notice that the model number of this interface matches the initial entry from the “Interface List” in the initial Wireshark screen. This is your physical Ethernet port.
Another procedure to know which one of these entries represents your physical Ethernet port:

1. Select “Interfaces” from the “Capture” menu.

2. A menu similar to this comes up.
   Information given in this menu:
   - Your IP addresses are listed here which might clarify things for you.
   - You will see the packet counters increasing, which should indicate which Ethernet interface is plugged in and receiving data.

**Note:** From this screen, to start a packet trace, click the **Start** of its Interface.