**Experiment- 1**

**Aim Of the Experiment:** Study Various methods for 'Taping into the wire'.

**Learning Objective/Theory**

At the end of the experiment we will be able to

* + - Become familiar with how and when to capture the data packet appropriately.
		- The aim is to help you develop and understanding of packet-sniffer placement.
		- You will come to know the different guidelines for Packet Sniffing in networking and inter- networking environment.

## Theory

## Introduction to Tapping into the Wire.

A key decision for effective packet analysis is where to position a packet sniffer to appropriately capture the data. This is most often referred to by packet analysts as sniffing the wire, tapping the network, or tapping into the wire. Simply put, this is the process of placing a packet sniffer on a network in the correct physical location.

Unfortunately, sniffing packets is not as simple as plugging a laptop into a network port and capturing traffic. In fact, it is sometimes more difficult to place a packet sniffer on a network’s cabling system than it is to actually analyze the packets.

The challenge with sniffer placement is that a large variety of networking hardware is used to connect devices. Figure illustrates a typical situation. Because the three main devices on a modern network (hubs, switches, and routers) each handles traffic differently, you must be very aware of the physical setup of the network you are analyzing.

The goal of this manual is to help you develop an understanding of packet-sniffer placement in a variety of different network topologies. But first, let’s look at how we’re actually able to see all the packets that cross the wire we’re tapping into.

## D:\Practical\Sir\Screenshots\Screenshot (337).pngSniffing in a Switched Environment

Switches are the most common type of connection device used in modern network environments. They provide an efficient way to transport data via broadcast, unicast, and multicast traffic. As a bonus, switches allow full-duplex

communication, meaning that machines can send and receive data simultaneously. Unfortunately for packet analysts, switches add a whole new level of complexity. When you connect a sniffer to a port on a switch, you can see only broadcast traffic and the traffic transmitted and received by your machine, as shown in Figure

There are four primary ways to capture traffic from a target device on a switched network: port mirroring, hubbing out, using a tap, and ARP cache poisoning.

1. **Port Mirroring**

Port mirroring, or port spanning, is perhaps the easiest way to capture the traffic from a target device on a switched network. In this type of setup, you must have access to the command-line or web- management interface of the switch on which the target computer is located. Also, the switch must support port mirroring and have an empty port into which you can plug your sniffer.

To enable port mirroring,

1. we issue a command that forces the switch to copy all traffic on one port to another port. (For instance, to capture the traffic from a device on port 3 of a switch, you could simply plug your analyzer into port 4 and mirror port 3 to port 4, allowing you to see all traffic transmitted and received by your target device. Figure illustrates port mirroring.
2. The way that you set up port mirroring depends on the manufacturer of your switch. For most switches, you’ll need to log in to a command line interface and enter the port mirroring command. You’ll find a list of common port-mirroring commands in Table

Table: Commands Used to Enable Port Mirroring

## Hubbing Out

Another way to capture the traffic through a target device on a switched network is by hubbing out. This is a technique by which you segment the target device and your analyzer system on the same network segment by plugging them directly into a hub. Many people think of hubbing out as cheating, but it’s really a perfect solution in situations where you can’t perform port mirroring but still have physical access to the switch the target device is plugged into. To hub out, all you need is a hub and a few network cables. Once you have your hardware, connect it as follows:

* + - 1. Go to the switch the target device resides on and unplug the target from the network.
			2. Plug the target’s network cable into your hub.
			3. Plug in another cable that connects your analyzer to the hub.
			4. Plug in a network cable from your hub to the network switch to connect the hub to the network.
1. **Using a Tap**

A network tap is a hardware device that you can place between two points on your cabling system in order to capture the packets between those two points. As with hubbing out, you place a piece of hardware on the network that allows you to capture the packets you need. The difference is that rather than using a hub, you use a specialized piece of hardware designed for network analysis.

There are two primary types of network taps: aggregated and non- aggregated. Both types of taps sit in between two devices in order to sniff the communications. The primary difference between an aggregated tap and a non-aggregated tap is that the non-aggregated tap has four ports, as shown in Figure, and the aggregated tap only has three ports. Taps also typically require a power connection, although some include batteries for brief stints of packet sniffing without the need to plug into a power receptacle.

1. **Aggregated Taps**

The aggregated tap is the simplest to use. It has only one physical monitor port for sniffing bidirectional traffic. To capture all traffic to and from a single computer plugged into a switch using an aggregated tap, follow these steps:

* + - * 1. Unplug the computer from the switch.
				2. Plug one end of a network cable into the computer, and plug the other end into the tap’s “in” port.
				3. Plug one end of another network cable into the tap’s “out” port, and plug the other end into the network switch.
				4. Plug one end of a final cable into the tap’s “monitor” port, and plug the other end into the computer that is acting as your sniffer.

## Non-aggregated Taps

It allows a bit more flexibility when capturing traffic. Instead of a single monitor port that can be used to listen to bidirectional communication, the non-aggregated type has two monitor ports. One monitor port is used for sniffing traffic in one direction (from the computer connected to the tap), and the other monitor port is used for sniffing traffic in the other direction (to the computer connected to the tap). To capture all traffic to and from a single computer plugged into a switch, follow these steps:

* + - * 1. Unplug the computer from the switch.
				2. Plug one end of a network cable into the computer, and plug the other end into the tap’s “in” port.
				3. Plug one end of another network cable into the tap’s “out” port, and plug the other end into the network switch.
				4. Plug one end of a third network cable into the tap’s “monitor A” port, and plug the other end into one NIC on the computer that is acting as your sniffer.
				5. Plug one end of a final cable into the tap’s “monitor B” port, and plug the other end into a second NIC on the computer that is acting as your sniffer. The non-aggregated tap should be connected.

## ARP Cache Poisoning

One of good techniques for tapping into the wire is ARP cache poisoning. ARP cache poisoning, sometimes called ARP spoofing, is the process of sending ARP messages to an Ethernet switch or router with fake MAC (layer 2) addresses in order to intercept the traffic of another computer. Figure illustrates this setup.

ARP cache poisoning is an advanced form of tapping into the wire on a switched network. It is commonly used by attackers to send falsely addressed packets to client systems in order to intercept certain traffic or cause denial-of-service (DoS) attacks on a target. However, it can also be a legitimate way to capture the packets of a target machine on a switched network.



**Conclusion:**

Wehave successfully studied various methods for 'Taping into the wire'.