Promiscuous Monitoring in Ethernet and Wi-Fi Networks

Executive Summary

This white paper examines the problems related to the deployment and usage of software-based network monitoring solutions in wired and wireless Ethernet Local Area Networks (LANs). It demonstrates the methods of achieving network traffic visibility in various network configurations, explains important network monitoring concepts, and describes solutions to the typical problems encountered by network administrators in setting up network monitoring software.

Contents

What Is Promiscuous Monitoring

In the realm of computer networking, *promiscuous mode* refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

In a wider sense, promiscuous mode also refers to network visibility from a single observation point, which doesn't necessarily have to be ensured by putting network adapters in promiscuous mode. Modern hardware and software provide other monitoring methods that lead to the same result. In this white paper, we'll discuss the techniques that are commonly used to ensure network visibility in different network environments, both wired and wireless, equipped with different kinds of hardware.

Practical Applications

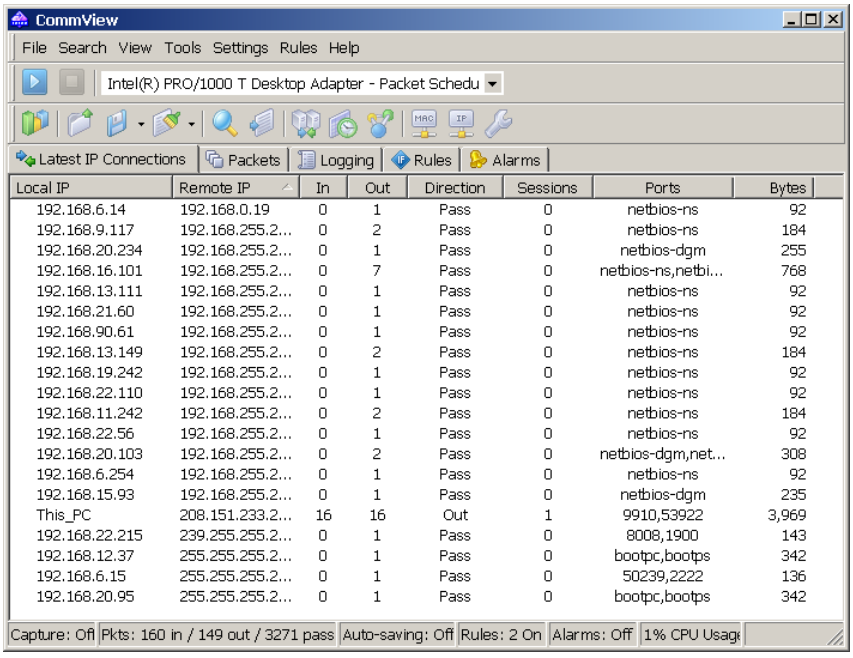
So why would we need to monitor anything other than our own computer? Simply put, in a situation where your network consists of three computers, A, B, and C, and the network analyzer is running on computer A, you should be able to see not only the data being sent from/to computer A, but also the data being sent from B to C. This is practical if you use network analyzers, traffic accounting systems, content monitoring systems, and similar applications. In theory, you could run a monitoring application on each computer, but it's inconvenient, as you wouldn't have the complete picture in front of you.

This white paper was written to address frequently asked questions by the users of TamoSoft products CommView and CommView for WiFi, network analyzers for wired and wireless networks, CommTraffic, a traffic accounting system, and NetResident, a content monitoring system. However, the monitoring principles and network topologies discussed here are universally used, so this information, by large, is applicable to any other Ethernet and Wi-Fi monitoring and analysis software, regardless of the vendor and operating system.

Ethernet Networks, Hubs and Switches

In Ethernet networks, hubs and switches are central connection points for the networking of multiple computers or other network devices. Together, these computers form a network segment. On this segment, all computers can "talk" directly to each other. Hubs are less intelligent devices than switches: They simply receive incoming packets on one port and broadcast them to all other ports. This feature makes them ideal for promiscuous network monitoring.

Unlike hubs, switches inspect packets as they are received to check the source and destination MAC addresses and forward them to the correct port. In a switched network environment, a packet analyzer is limited to capturing broadcast and multicast packets and the traffic sent or received by the PC on which it is running. The screen shot below illustrates a typical snapshot of the network activities in a switched network environment:

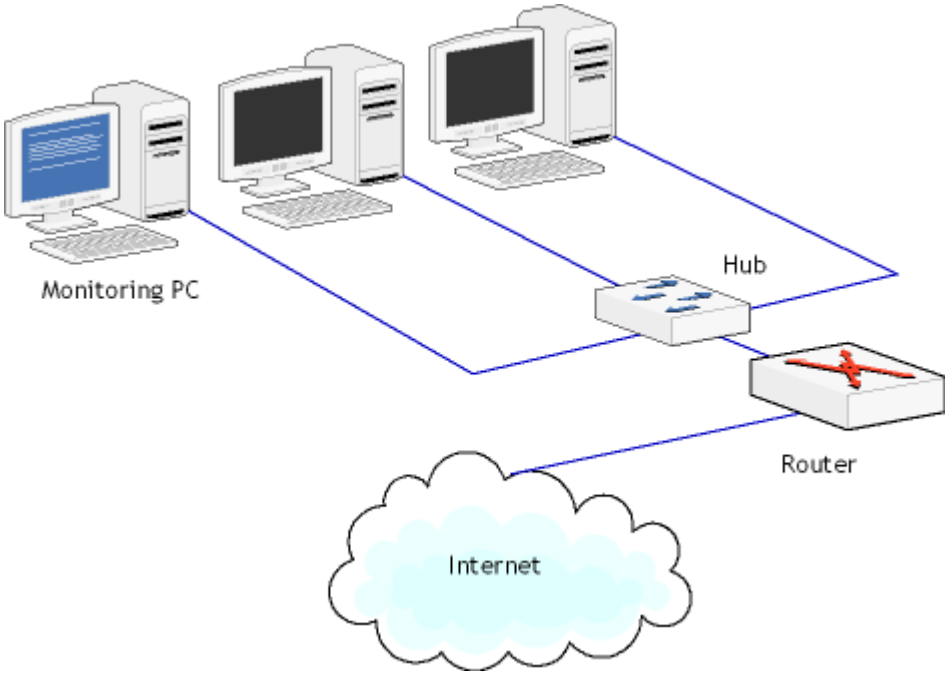


You can see many broadcast packets being sent from the hosts in your LAN segment to the broadcast IP addresses, but you can't see normal, unicast traffic between these hosts or between these hosts and the Internet. Despite the fact that most switches prevent promiscuous monitoring, a lot of switches can be configured to forward packets to a special monitoring port. We'll discuss the usage of hubs and switches for monitoring purposes below.

Monitoring Using Hubs

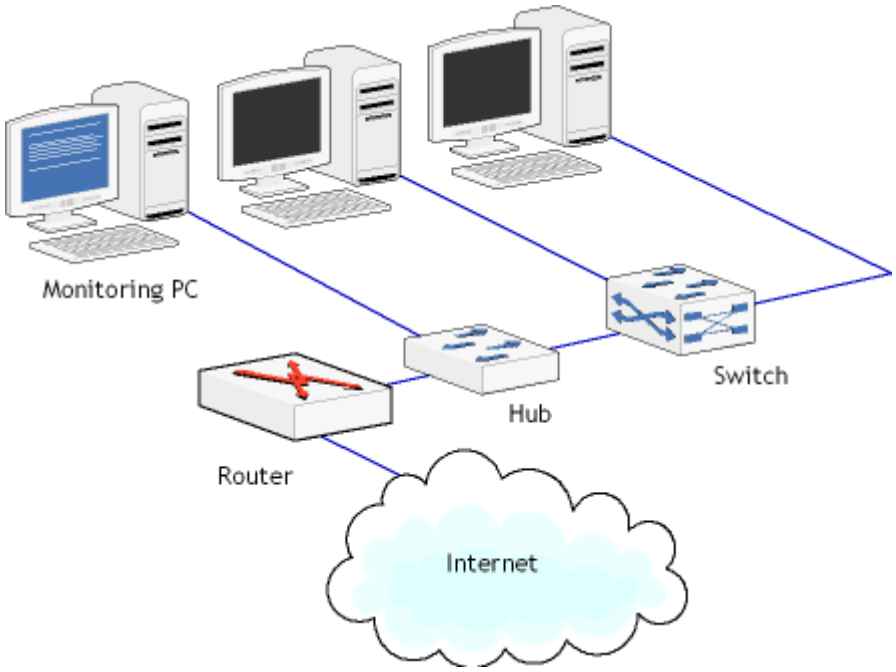
Hubs are still popular devices for small networks because of their low cost, but attention should be paid to potential problems with using hubs for network monitoring. First, hubs are open to unauthorized monitoring from within the LAN segment, as any port can be used for promiscuous mode monitoring. Second, "auto-sensing", "dual-speed", "switching", or "intelligent" hubs may prevent you from monitoring the entire LAN segment. This problem will be discussed in the next chapter; meanwhile, we'll show a few alternative network layouts that use hubs for monitoring purposes.

Layout 1



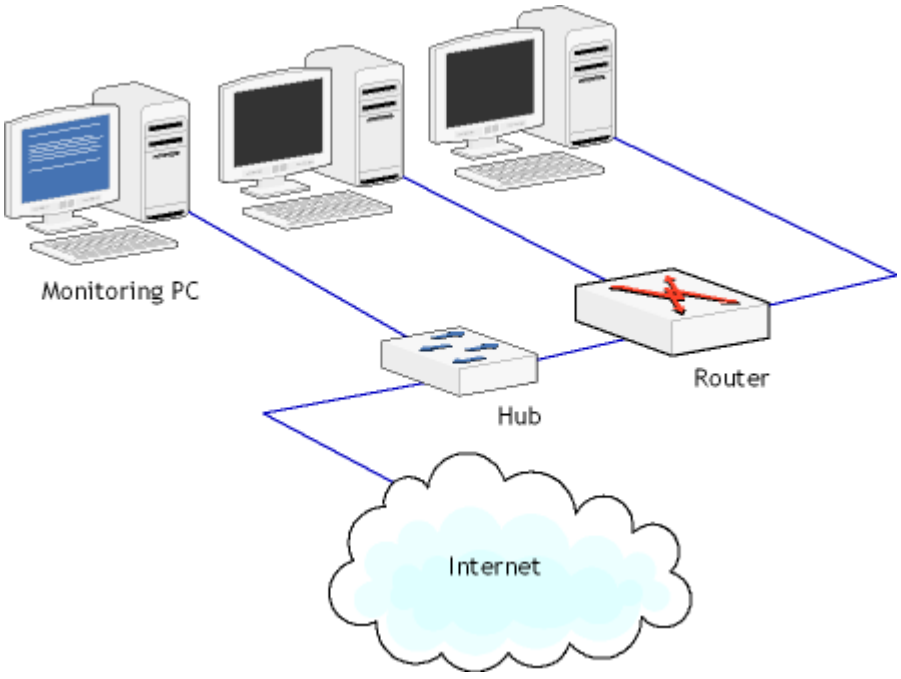
This is probably the simplest and most obvious layout. Here, any computer connected to the hub can be a monitoring computer, as the hub replicates the data received/sent to/from the router to all ports. Additionally, data exchange between the local workstations can be monitored.

Layout 2



In this layout, the hub is inserted between the router and the switch. This layout allows you to monitor the data being sent to/from the Internet, but not the data being exchanged by the local workstations.

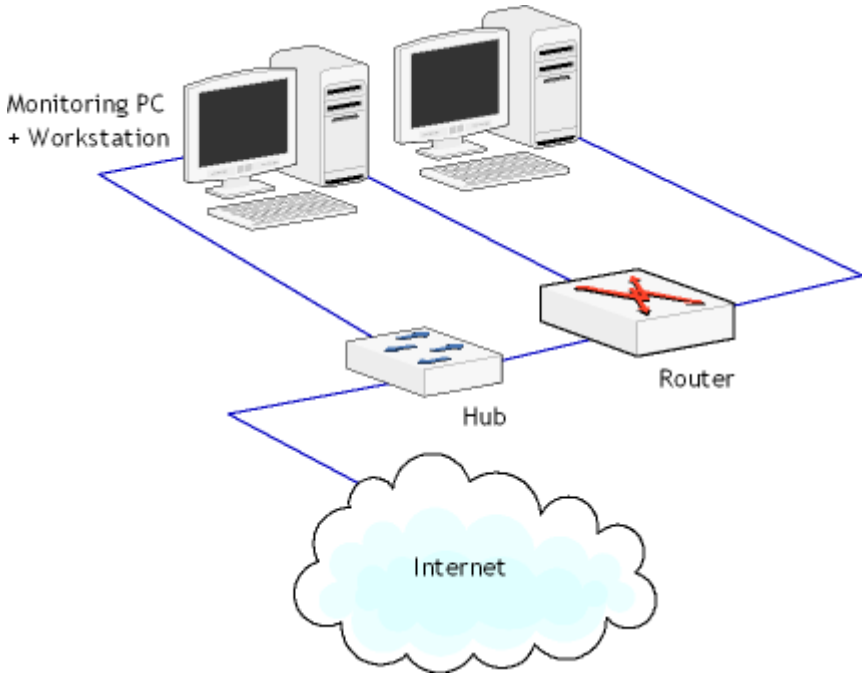
Layout 3



This layout illustrates how you can monitor a small LAN that doesn't use a switch. This is a typical layout for a home or small office network, where the router is combined with a switch to which a few workstations are connected. To monitor the data being sent to/from the Internet, you can insert a hub between the Internet and your router. It should be noted that the monitoring software would not be able to distinguish between traffic originating from different workstations, unless the workstations behind the router have routable IP addresses. If they don't have routable IP addresses, all packets will have the same IP address, i.e. the public IP address of your network.

The monitoring computer located outside your LAN should be totally passive, i.e. the network interface should be used for data capturing only. This can be achieved by assigning a non-routable IP address to the NIC, e.g. 10.0.0.1, or unbinding TCP/IP from the NIC altogether. To achieve complete passiveness, a read-only cable can be used; this method will be discussed below.

Layout 4



This layout is a variation of Layout 3, but here the monitoring functions are performed by one of the workstations that is equipped with two NICs: One NIC is used for normal connectivity inside the LAN, while the second NIC is used for monitoring. As with Layout 3, steps should be taken to make the second NIC passive. This layout should be considered as a budget solution only.

Hubs: Potential Problems

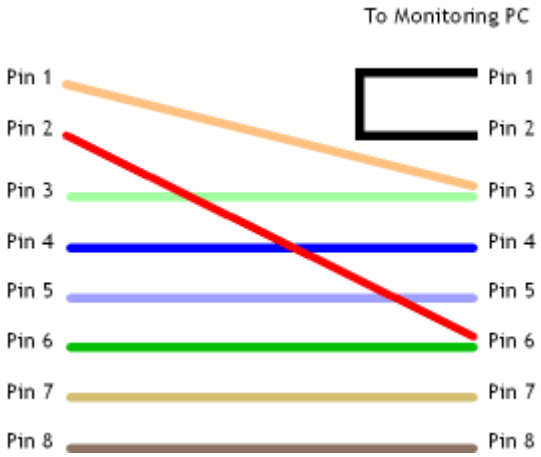
Aside from the fact that hubs have lower performance than switches, you can encounter two other problems when using a hub for promiscuous monitoring.

The first problem is related to dual-speed (a.k.a. auto-sensing) hubs that support both 10 Mbps and 100 Mbps hardware. Such hubs don't replicate the data received from the port(s) operating at 10 Mbps to the ports operating at 100 Mbps, and vice versa. This problem can be addressed by configuring all your hardware to run at the same speed. Most multi-speed NICs allow you to "force" a specific speed.

The second problem stems from the fact that some hubs are only labeled as hubs, but inside are switches (some vendors like Linksys do that). These hubs are frequently referred to as "intelligent" or "switching" hubs by the vendor, but this is not always the case. Even without any indication in the documentation, a hub may turn out to be a switch. The only way to find out would be to try. Typically, old and cheap hubs have a greater chance of being "real" hubs. Also, a good indication that the device in front of you is a "real" hub is the Collision LED. Collisions are not possible in a switched environment, so a switch won't have the Collision LED.

Read-Only Cables

As we mentioned above, using a network layout with a hub and monitoring computer outside of the router may pose a security problem unless the computer works in receive-only mode. The ultimate solution to this problem suggested by some people would be a read-only Ethernet cable that can be made with CAT5 cable, two RJ-45 connectors, and a crimping tool. The diagram below illustrates the wiring scheme.



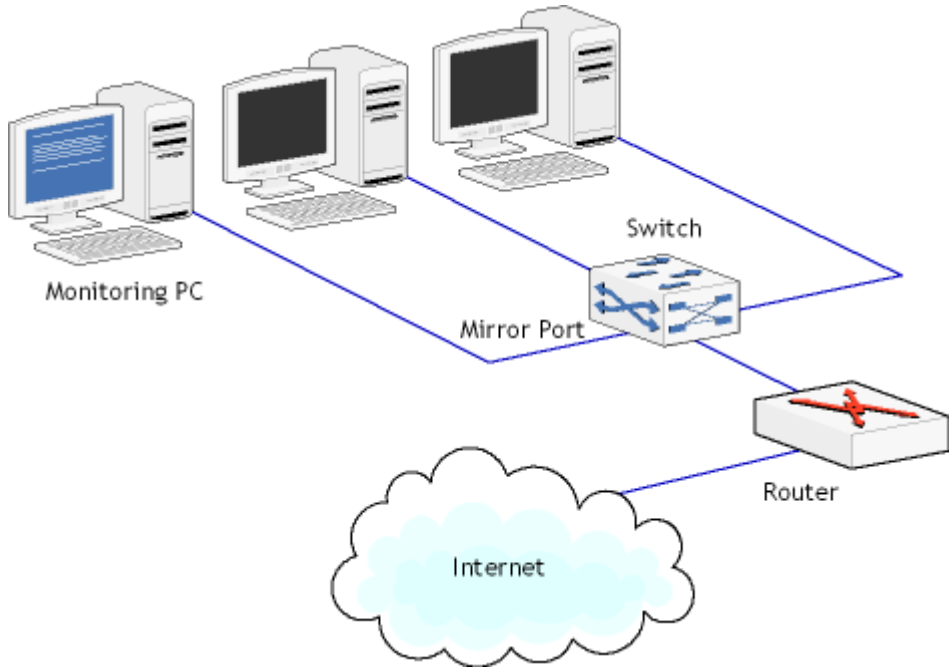
If you would like detailed instructions on making a read-only cable, you will easily find them on the Internet.

Monitoring Using Switches

A managed switch that supports port mirroring, a feature that allows you to configure the switch to redirect the traffic that occurs on some or all ports to a designated monitoring port on the switch, is an ideal device for network monitoring purposes. The way port mirroring is configured depends on the specific model and vendor (there are dozens of different models that have this functionality, ranging in price from $100 to a few thousand dollars.)

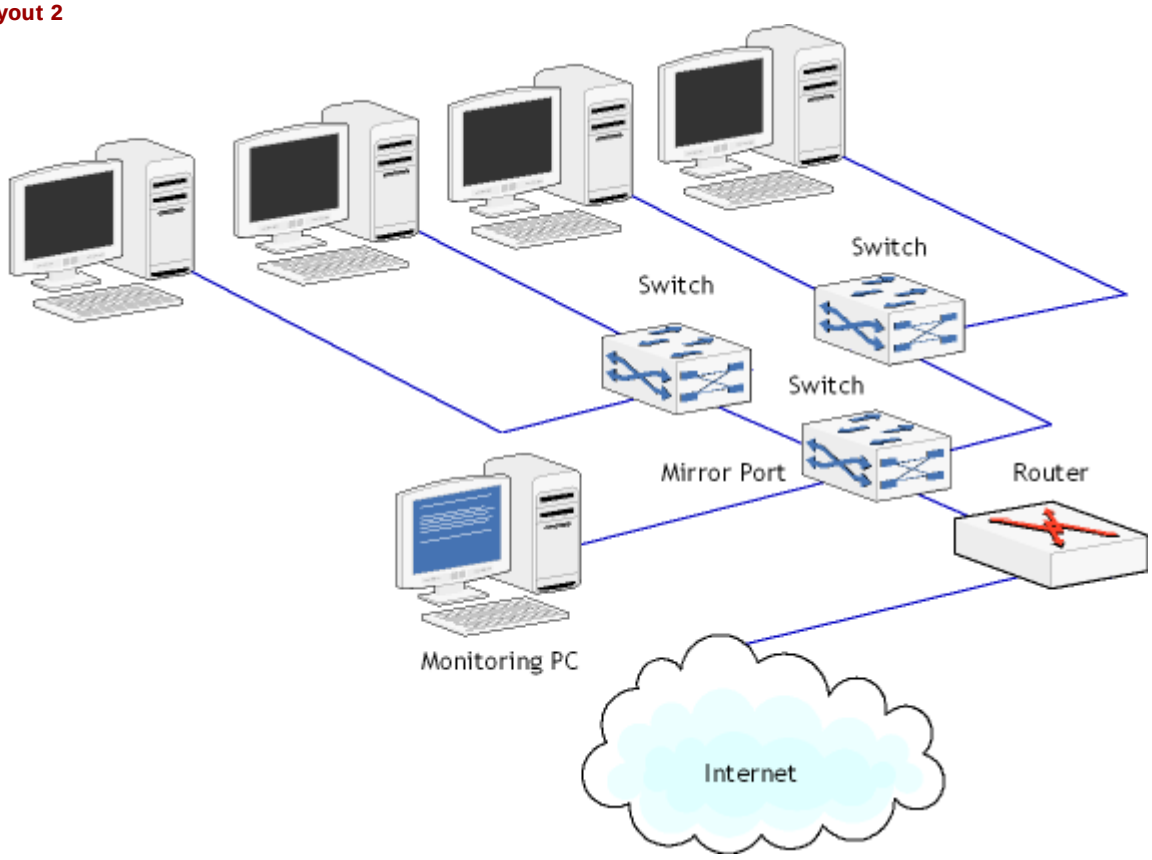
Two typical network layouts using port mirroring are shown below.

Layout 1



In this layout the primary switch supports port mirroring. A monitoring computer is connected to the mirror port, to which all traffic between the local workstations and the router is replicated. The switch can be configured to replicate data from one or several ports, depending on your purposes.

Layout 2

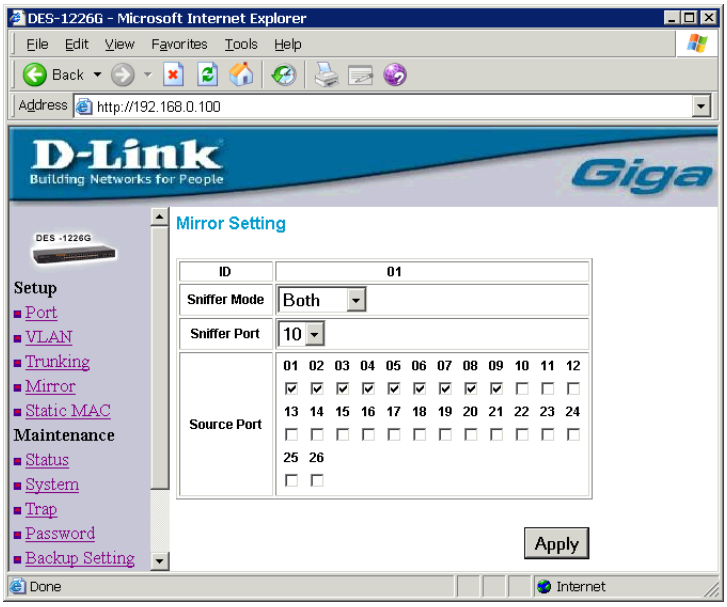


If your LAN segment is built on unmanaged switches that don't support port mirroring, you can add a managed switch to your network. By routing the Internet traffic via the switch that supports port mirroring, you make it possible to connect the monitoring computer to the mirror port and be able to capture traffic that goes from the local workstations to the router and back. However, this layout doesn't let you monitor the traffic between the local workstation, as it is routed via the unmanaged switches and doesn't reach the monitoring switch.

As a side note, we should mention that some switches that don't support port mirroring could be exploited for promiscuous mode monitoring. Network attacks, like "ARP Flood" or "ARP Spoofing", may be mounted against the network and cause a switch to send packets to all ports. These are, by no means, recommended monitoring methods.

Port Mirroring Configuration

As was mentioned above, there are many switches on the market that support port mirroring. Please bear in mind that networking hardware manufacturers use different names for the same feature: It can be called "Port mirroring", "Switched Port Analyzer" (SPAN), or "Roving analysis port" (RAP). To configure port mirroring in your switch, please refer to the documentation that comes with it. Typically, the configuration process is quick and easy. The screen shot below illustrates port-mirroring configuration in DES-1226G by D-Link, an affordable and easy-to-configure managed switch.



After selecting "Mirror" on the left pane of the Web management console, you select the **Sniffer Mode** option (Tx, Rx, or Both), **Sniffer Port**, i.e. the port to which packets will be replicated, and select **Source Ports** from which packets should be mirrored.

Best Practices

While all of the network layouts described above can be used for network monitoring, not all of them are equally good in terms of network performance and security. We recommend considering the following when selecting your network layout:

- Use a dedicated computer for monitoring. Monitoring a busy network is a CPU-intensive task that should not be performed on a computer running other CPU-intensive processes, especially on an application server, such as Web or FTP server. Doing so may seriously degrade server performance. Use a computer with a fast CPU and at least 512 Megabytes of RAM.
- Use managed switches rather than hubs whenever possible. Switches provide better performance and replicate packets to a single port only, thus diminishing risks of promiscuous mode monitoring from unauthorized workstations.

Monitoring Across WAN

There are situations where monitoring network traffic beyond one's own LAN segment is extremely helpful. For example, a software engineer may need to troubleshoot a network-related software installation in another building, or even a different part of the world. Being able to watch the actual packets flowing through the remote computer may be tremendously helpful. This can be achieved by two methods.

The first method is rather obvious and straightforward: Considering the vast proliferation of remote access software, including the native Microsoft tools such as Remote Desktop Connection and Terminal Services available to the users of the latest Windows versions, one can simply have a network analyzer installed on a remote system and then gain full access to it by means of Remote Desktop Connection.

The second method is based on the usage of remote network probes, i.e. software agents installed on a remote system. By connecting to one or several remote agents from one central location, the administrator can have the actual network traffic sent back to his monitoring software for real-time analysis. This approach offers a number of benefits, such as simultaneous connection to any number of probes and the ability to analyze and log data on your own computer, but requires a good communication link between the probes and the analyzer, as well as the thoughtful use of traffic filters.

A good example of this remote monitoring technology would be CommView Remote Agent that was first product of this kind on the market and remains a leader in this field. Aside from intrinsic advantages offered by remote monitoring technology, this product features data compression and strong encryption.

Wi-Fi (802.11) Networks

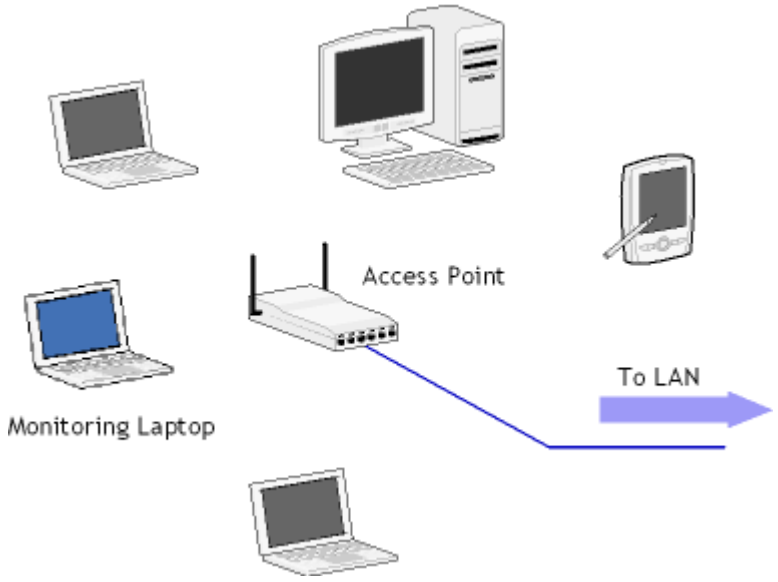
Promiscuous monitoring of Wi-Fi networks has often been a source of confusion, especially among users not professionally involved in wireless software development. It appears logical that if any Ethernet adapter can be used for promiscuous mode

monitoring in a wired Ethernet network, then any Wireless Ethernet adapter is equally good for doing the same in a 802.11 a, b, or g network. Theoretically, this is true, but in practice, this is very far from reality.

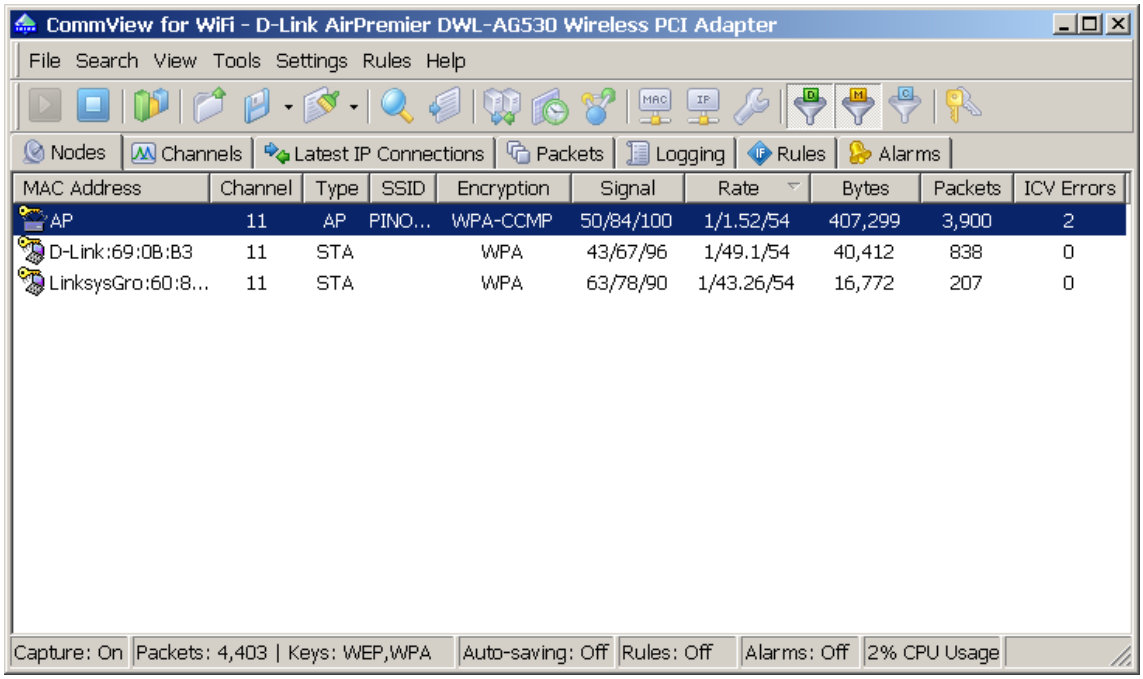
The truth is that the standard drivers for wireless NICs simply don't support promiscuous mode (or, rather, "RF Monitoring", as this feature is called in the wireless world) functionality. While the adapter can receive radio signals on a given frequency regardless of the destination MAC address in the packet, the packets that are not addressed to this adapter are discarded by the driver, and there is no way to make the standard driver pass them to the network monitoring software.

The good news is a number of network monitoring software vendors make special RF monitoring drivers for a limited number of supported wireless adapters. Having obtained a supported wireless adapter, the user has to install the wireless monitoring program, replace the original driver by the special RF monitoring driver, and only after that can he monitor the WLAN. Therefore, the frequently asked question, "Does my Wi-Fi card support promiscuous mode?" is, unfortunately, meaningless. This is an issue of driver availability. The correct version of this question would be "Is there a RF monitoring driver for my Wi-Fi card and operating system?"

When your wireless network analyzer is up and running, the only thing required for monitoring a WLAN is being within the signal range. Then the software can intercept and display wireless packets, show nodes and access points, signal strength, and other important statistics and indicators.

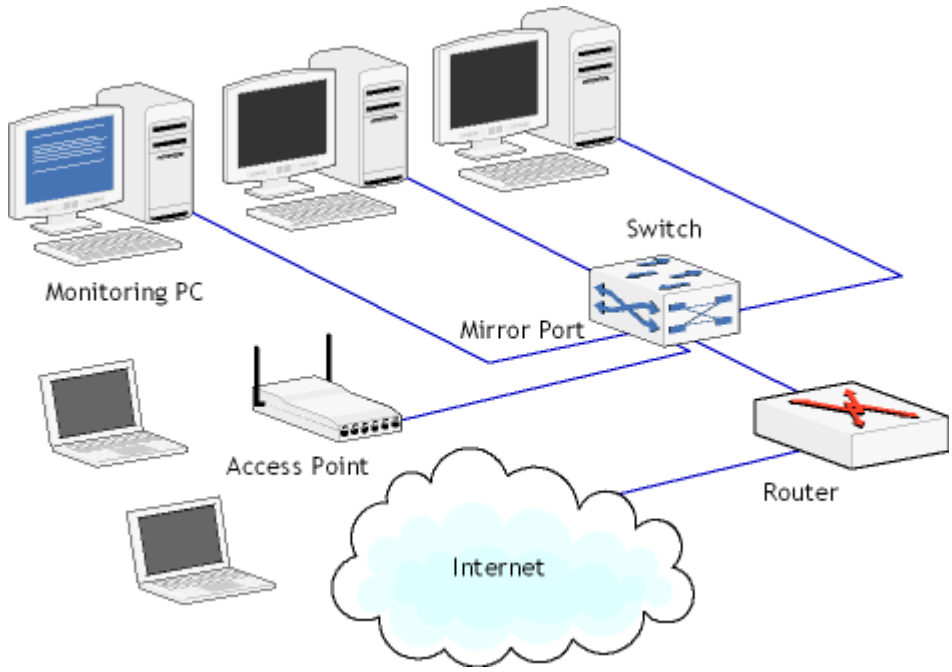


A typical wireless monitoring layout is simple: Just a number of computers and access points and a computer running a network analyzer in the vicinity. Your network analyzer would display your WLAN nodes in a way similar to the one shown in the screen shot below:



Aside from the problems related to NIC drivers, wireless traffic is sometimes encrypted using WEP (an older standard) or WPA. A good WLAN analyzer must be capable of decrypting encrypted network traffic on the fly utilizing a user-provided WEP or WPA-PSK key.

A WLAN analyzer may not be required if all you need to monitor is the traffic between the wireless stations and the Internet. Using a standard, non-wireless monitor on a mirror port would make it possible to capture the packets being sent and received through the access point. A network layout illustrating this method is shown below.



Naturally, this setup can't be used to see the traffic between the wireless stations or gain access to wireless-specific indicators and data, such as signal strength, data transfer rate, or intrusion incidents.

Conclusion

In the today's networking world, the number of network configurations and layouts is unlimited. Yet, understanding the monitoring principles and concepts provides the user with the ability to find a solution that can ensure traffic visibility in virtually

any situation. Naturally, the network visibility is not the final purpose. Rather, it's a base required for the correct usage of network monitoring and analysis software.

TamoSoft recommends its array of cutting-edge network monitoring solutions for LAN and WLAN administrators, security professionals, forensic experts, and application developers. Visit us today to download our free trial versions.

About TamoSoft

TamoSoft develops cutting-edge security and network monitoring software for the Internet and Local Area Networks, providing clients with the ability and confidence to meet the challenges of tomorrow's technology. Keeping pace with industry trends, we offer professional tools that support the latest standards, protocols, software and hardware in both wired and wireless networks.

With a portfolio including such companies as Motorola, Siemens, Ericsson, Nokia, Cisco, Lucent Technologies, Nortel Networks, Unisys, UBS, Dresdner Bank AG, Olympus and General Electric, TamoSoft is one of the fastest growing IT application development firms in the marketplace today. TamoSoft products are available through this Web site as well as through a network of distributors and resellers.

Founded in 1998 as the software division of a Cyprus-based business consulting company, TamoSoft is a privately held company based in Christchurch, New Zealand. TamoSoft employs an international team dedicated to the creation of high quality software that customers from over 100 countries rely on and partners with industry leaders in technology and services, such as Zone Labs, Visualware, and The CWNP Program.

TamoSoft
PO Box 1385
Christchurch 8015
New Zealand
www.tamos.com