

CommView[®] Remote Agent for WiFi

Help Documentation

Copyright © 2001-2007, TamoSoft

Introduction

About CommView Remote Agent for WiFi

CommView Remote Agent for WiFi is an application for remote WLAN traffic monitoring. It allows CommView for WiFi users to capture network traffic on any computer where Remote Agent for WiFi is running, regardless of the computer's physical location. This application allows you to ensure better wireless network visibility within an office or building by collecting data from multiple locations and to provide a means of remote network monitoring and troubleshooting, eliminating the need to be physically present on site.

After the installation and simple configuration, CommView Remote Agent for WiFi is ready to accept connections from CommView for WiFi. Once the connection is established and the authentication is successful, CommView Remote Agent for WiFi is ready to capture packets and transmit them to CommView for WiFi. The transmitted packets are compressed to save bandwidth and encrypted to ensure safe transmission over insecure network channels.

CommView Remote Agent for WiFi is an indispensable tool for networking, software, and security professionals that offers a wide range of solutions, such as monitoring large WLANs or remote software and network troubleshooting.

This application requires a compatible wireless network adapter. For the list of supported adapters, please visit our [Web site](#).

What's New

Version 2.2

- Support for 802.11n.
- Support for cards based on the latest Atheros chipsets.

Version 2.1

- Windows Vista support.

Version 2.0

- The initial release.

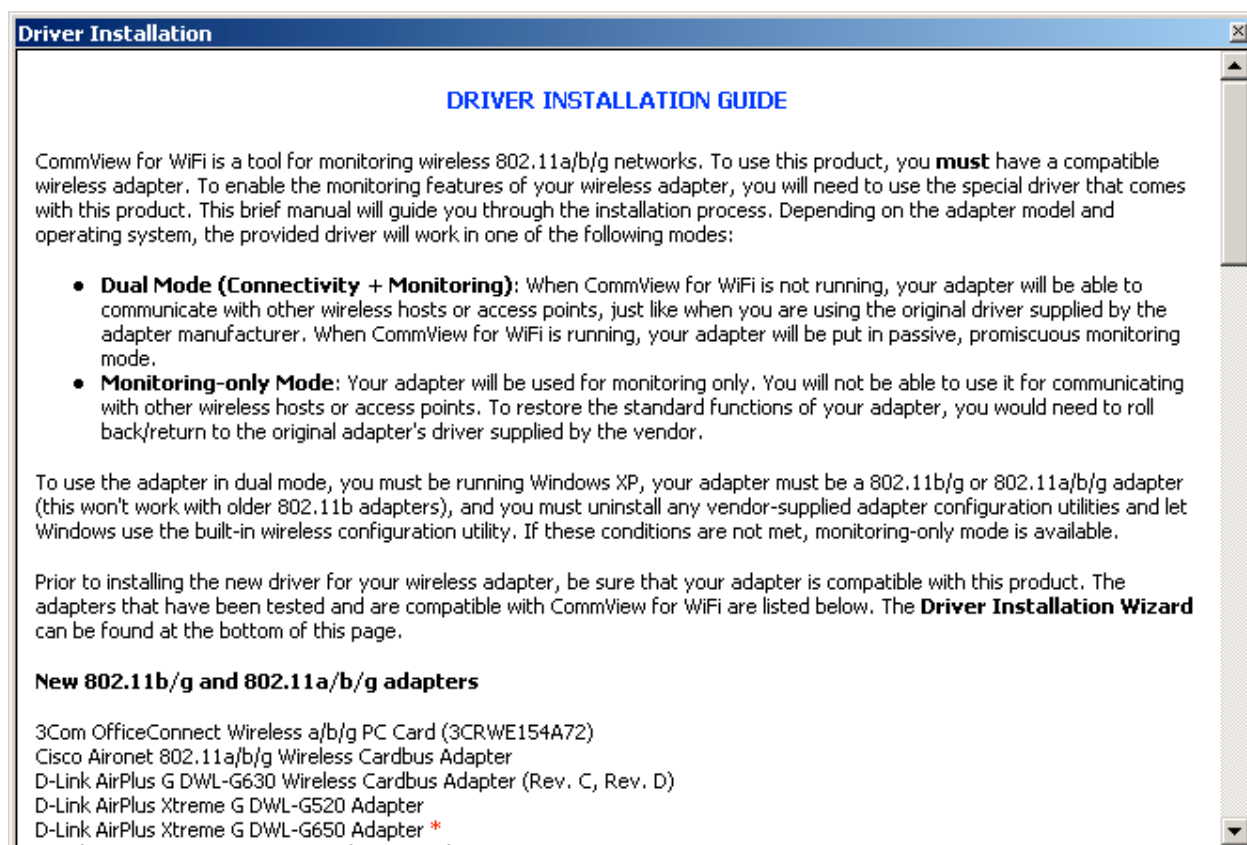
Using the Program

Installation and Configuration

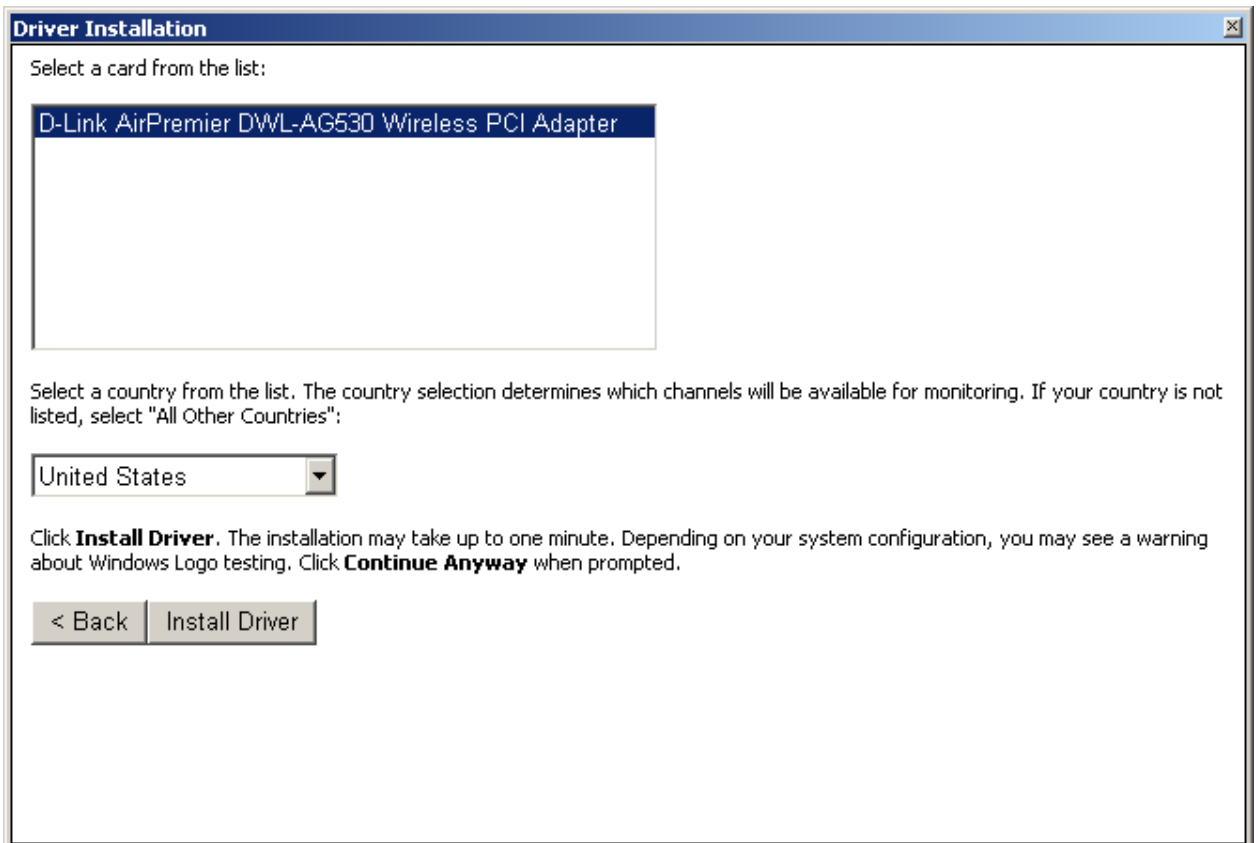
CommView Remote Agent for WiFi should be installed on a computer that has a compatible wireless adapter (to be used for monitoring) and Ethernet adapter (to be used for the connection between Remote Agent and CommView for WiFi). You must have administrative privileges to install the program, although such privileges are no longer required after the initial installation and configuration. You must NOT install both CommView for WiFi and CommView Remote Agent for WiFi on the same computer.

Installation

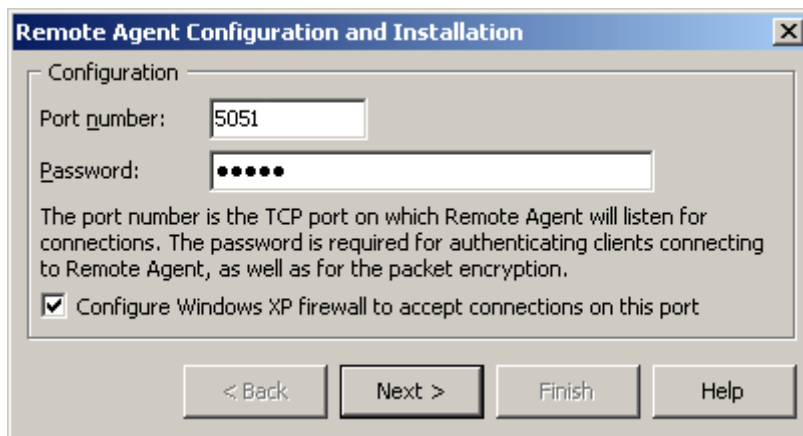
To install the program, run SETUP.EXE and follow the instructions on the screen. The first step is installing the special driver for your compatible wireless adapter. The Driver Installation Guide will guide you through the installation process; you will need to scroll down to the bottom of the page shown below and click **Next** to initiate the driver installation process. The driver can be installed automatically by the application (recommended) or manually, using Device Manager.



If a compatible wireless adapter is found on your system, the final screen will allow you to install the driver for it, as shown below:



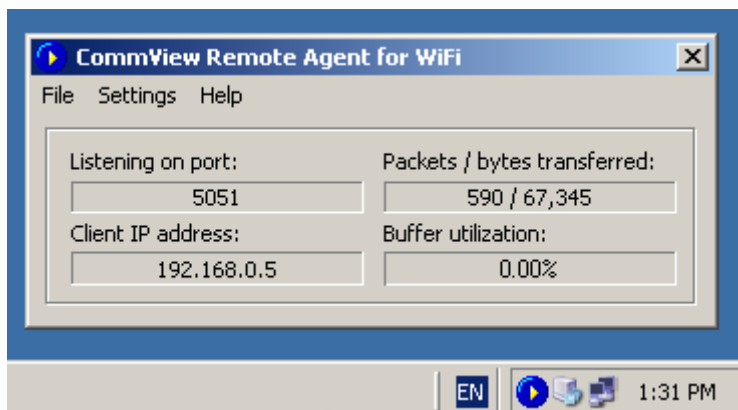
If driver installation has completed successfully, you will see an Installation and Configuration window that will prompt you to enter two initial settings. You should select a TCP port number and password. The TCP port number (5051 by default) will be used by the program to accept client connections from CommView for WiFi. The password is required for client authentication and subsequent packet encryption. Be sure to choose a long, hard-to-guess password, using alphanumeric upper and lower case characters; because if somebody guesses your password, he/she will be able to gain access to the network traffic captured by the computer on which you have installed CommView Remote Agent for WiFi.



Click **Next** to continue, and the program will install the remaining components and launch CommView Remote Agent for WiFi for the first time.

Interface

Once the installation and initial configuration have been completed, the program's icon should appear in the system tray as shown below. Clicking on the icon will bring up an application window that displays the program status – the port number that CommView Remote Agent for WiFi listens on, the IP address of a client that is currently connected to it, packet transmission statistics, and buffer utilization.



Main Menu

File

Start/Resume Service – starts or resumes the CommView Remote Agent for WiFi service if it has been stopped or paused.

Stop Service – stops the service.

Pause Service – pauses the service.

Exit – closes the CommView Remote Agent for WiFi console. Please note that the service continues to run and accept connections from CommView for WiFi.

Settings

Change Port – allows you to change the port number that the application listens on.

Change Password – allows you to change the connection password.

Language – allows you to change the interface language.

Help

Contents – opens the help documentation.

About – shows information about the program.

Note: CommView Remote Agent for WiFi can accept only one client connection at any given time.

Controlling The Program

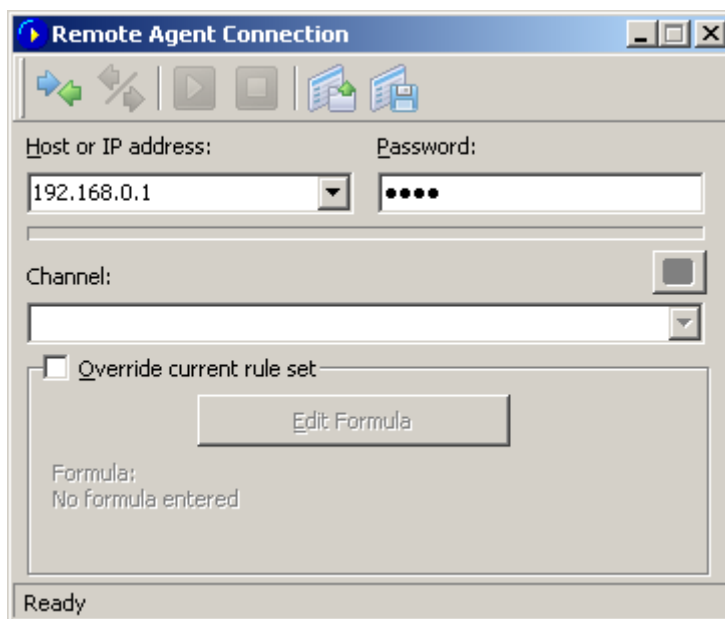
CommView Remote Agent for WiFi is a **service application**. This means that it starts automatically when the computer is booted up and runs even if no one is logged on to the system. The service can be controlled using the **File** menu described above. Additionally, as with any other service application, it can be controlled using Control Panel => Administrative Tools => Services. There you can also change the start-up mode (automatic/manual).

Monitoring Traffic

This chapter describes how to use CommView for WiFi to connect to CommView Remote Agent for WiFi and capture traffic remotely. To monitor wireless network traffic using remote computers, you need to have CommView Remote Agent for WiFi running on the remote host and CommView for WiFi running on your computer. It is assumed that Remote Agent is already installed and running (see the previous chapter for instructions) and that you are already familiar with CommView for WiFi and know how to use it. If you have no experience with CommView for WiFi, please [download](#) it and familiarize yourself with it prior to using CommView Remote Agent for WiFi.

Using CommView for WiFi to Connect to CommView Remote Agent for WiFi

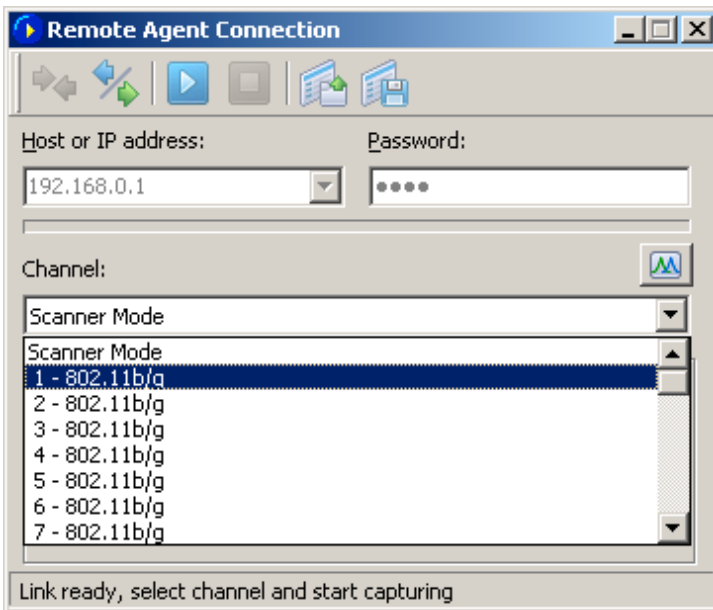
To switch to remote monitoring mode, click **File => Remote Monitoring Mode**. An additional toolbar will appear in the CommView for WiFi main window next to the main toolbar. If you are behind a firewall or proxy server, or using a non-standard Remote Agent port, you may need to click on the **Advanced Network Settings** button to change the port number and/or enter SOCKS5 proxy server settings. The **Advanced Network Settings** dialog also allows you to define whether Remote Agent will apply the filtering rules locally, or send all the captured traffic to CommView for WiFi; this will be discussed in detail later in this chapter.



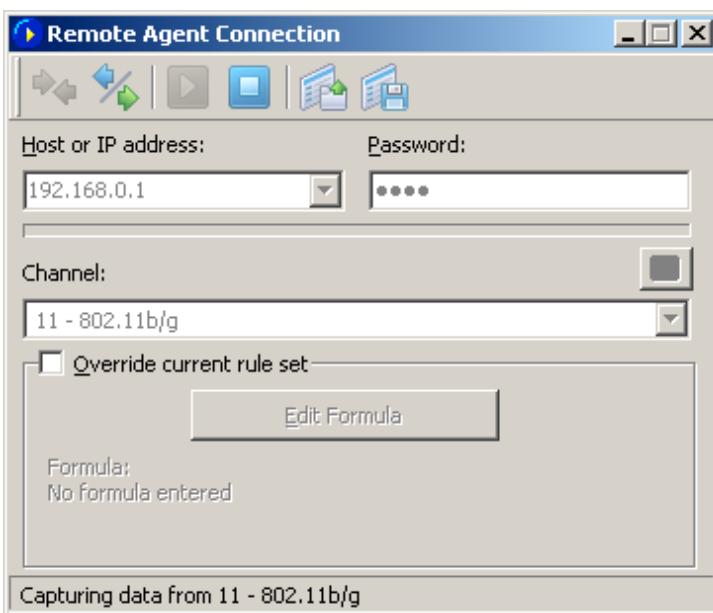
Click on the **New Remote Agent Connection** button to establish a new connection, or click on the **Load Remote Agent Profile** toolbar button to load a previously saved Remote Agent connection profile. A previously saved profile may also be loaded from the New Remote Agent Connection window.

A Remote Agent Connection window will appear. Enter the IP address of the computer running CommView Remote Agent for WiFi into the IP address input area, enter the connection password and click on the **Connect** button. If the password is correct, a connection will be established. You will then see the *Link Ready* message in the status bar and the channel selection box will list the channels supported by the wireless adapter installed on the remote computer. In addition to the channel list, a special **Scanner Mode** item will be added as the first item on the list.

If you select **Scanner Mode**, the remote wireless adapter will cycle through the available channels, capturing data from each of them for several seconds. The small button located on the right side of the window, just above the channel selection box, allows you to adjust the scanner settings. Click on this button to select the channels to be monitored in Scanner Mode and set the interval, i.e. the number of seconds per channel. Note that for Intel wireless adapters, the interval cannot be below 4 seconds due to technical limitations.



Now is the best time to configure the capturing rules using the **Rules** tab in the CommView for WiFi main window. You can also apply a custom set of capturing rules to this connection and override the current rules defined in CommView by checking the **Override current rule set** box, clicking on the **Edit Formula** button and entering the rules formula in the field below. The formula syntax is the same as the one used in Advanced Rules. Once you're ready to start monitoring, select the channel from the list and click the **Start Capture** toolbar button. CommView for WiFi allows you to save the Remote Agent Connection settings as a connection profile for quick and easy access in the future. Click on the **Save Remote Agent profile** toolbar button in the New Remote Agent Connection window and enter a name for the file.



CommView for WiFi will start to capture the remote adapter's traffic as if it's your local network traffic; there is virtually no difference between using CommView for WiFi locally or remotely. When you are done with remote monitoring, just click on the **Stop Capture** toolbar button. You can then change the channel or disconnect from Remote Agent by clicking the **Disconnect** toolbar button. To return to the standard mode, click **File => Remote Monitoring Mode**, and the additional toolbar will disappear.

Please note that CommView for WiFi can work with multiple Remote Agents simultaneously. You can open several remote connections, each having its own settings and an independent set of rules and collect the traffic from remote WLANs in one CommView for WiFi instance.

How to Use CommView Remote Agent for WiFi Efficiently

The key to efficient Remote Agent usage is ensuring that enough bandwidth is available to transfer the data collected by Remote Agent to CommView for WiFi. As mentioned before, Remote Agent should be installed on a computer that has a compatible wireless adapter (to be used for monitoring) and Ethernet adapter (to be used for the connection between Remote Agent and CommView for WiFi).

By default, Remote Agent sends all the collected packets back to CommView for WiFi, regardless of the capturing rules that may be configured in CommView for WiFi. This is done for providing correct statistical data and decryption, as well as the means for correct identification of wireless nodes. Since a fully loaded WiFi network has a bandwidth of 54 Mbit/s (or even 108 Mbit/s with some proprietary hardware), it's important that the wired link between Remote Agent and CommView for WiFi be capable of handling this bandwidth. In a modern office environment, where Gigabit networks are common, a single Gigabit adapter can easily receive data from a dozen Remote Agents.

There are situations where a fast connection is problematic. For example, a high bandwidth connection may not be available if you're monitoring a remote WLAN over the Internet. Even a T3 connection (4.5 Mbit/s) is insufficient to transfer all packets from a moderately loaded WLAN. In such situations, you can change the default setting and make Remote Agent filter the packets before they are transferred to CommView for WiFi. The **Advanced Network Settings** button on the additional remote monitoring toolbar in the main CommView for WiFi window allows you to enable the **Minimize bandwidth** option. When this option is enabled, the current CommView for WiFi rule set is periodically sent to Remote Agent. This rule set is then applied locally, so that only those packets that pass the rules are sent back to CommView for WiFi. In this mode, the **Nodes** may not display any nodes, and the **Channels** tab will not show full per-channel statistics, so use this mode only when you have limited bandwidth, but still need access to the packets from a remote WLAN.

For the same bandwidth reasons, it is highly recommended to NOT use a wireless connection for exchanging data between Remote Agent and CommView for WiFi. It's also a bad idea because the monitoring wireless adapter would pick up the packets sent by the wireless adapter being used for communicating with CommView for WiFi if they operate on the same or close channels. This will simply cause the snowball effect.

If CommView Remote Agent for WiFi captures more data than it can send to CommView for WiFi, it uses an internal buffer to store the packets that cannot be sent immediately. The buffer size is 5 Mbytes. The **Buffer utilization** indicator in the Remote Agent window shows the current status of the buffer. For example, if the program has buffered 2.5 Mbytes of data, the buffer utilization is 50%. If/when the buffer utilization reaches 100%, the program stops buffering data and discards captured packets until some buffer space is free.

Security

CommView Remote Agent for WiFi was made with security in mind. It can be accessed only by using a password that is never transmitted in plain text and that is ensured by using a challenge-response protocol with a secure hash function. If the authentication is successful, all transmitted traffic is compressed and then encrypted with the same password. Please take precautions to keep your password secret. Once it is revealed to an unauthorized person, that person will have broad capabilities to study your network and intercept network traffic on the remote computer.

Information

How to Purchase CommView Remote Agent for WiFi

This program is a 30-day evaluation version; please [visit our Web site](#) for pricing and ordering information.

As a registered user, you will receive:

- Fully functional, unrestricted copy of the software
- Free updates that will be released within 1 year from the date of purchase
- Information on updates and new products
- Free technical support

Please note that CommView Remote Agent for WiFi **is licensed per computer, not per user**. A single computer license grants you the right to install and use CommView Remote Agent for WiFi on one computer. If you need to install the program on multiple computers, you need to purchase a multi-computer license. You will also need at least one licensed copy of CommView for WiFi to connect to CommView Remote Agent for WiFi.

Contacting Us

Web

<http://www.tamos.com>

E-mail

sales@tamos.com (Sales-related questions)
support@tamos.com (All other questions)

Mail and Fax

Mailing address:

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Fax: +643 359 0392 (New Zealand)
Fax: +1 917 591-6567 (USA)

Other Products by TamoSoft

CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity, capable of capturing and analyzing network packets. It gathers information about data passing through your dial-up connection or Ethernet card and decodes the analyzed data. With CommView you can see the list of network connections and vital IP statistics and examine individual packets. IP packets are decoded down to the lowest layer with full analysis of the main IP protocols: TCP, UDP, and ICMP. Full access to raw data is also provided in real time. CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

[More information](#)

CommView for WiFi

CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry. CommView for WiFi captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for WiFi can help you view and examine packets, pinpoint network problems, perform site surveys, and troubleshoot software and hardware.

[More information](#)

NetResident

NetResident is an advanced network content monitoring program that captures, stores, analyzes, and reconstructs network events such as e-mail messages, Web pages, downloaded files and instant messages. NetResident uses advanced monitoring technology to capture the required data from the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format. While NetResident is similar to network analyzers in many respects, it focuses on high-level protocols that are used to transfer content over the Internet or LAN. With NetResident, you don't need a profound understanding of networking technologies, have to use complex packet capturing and analysis software, or dig through network packets in order to reconstruct the actual data; NetResident does all the work for you and presents only the Web pages, e-mails, instant messages, or downloaded files as requested. NetResident is used by network administrators to enforce IT policy, parents to monitor their children's communication on the Internet, and by forensic experts to gain crucial information.

[More information](#)

SmartWhois

SmartWhois is a handy utility for obtaining information about any IP address, hostname, or domain in the world. Unlike standard whois utilities, it automatically delivers information associated with an IP address or domain, no matter where it is registered geographically. In just a few seconds, you get all you want to know about a user: domain, network name, country, state or province, and city. Even if the IP address cannot be resolved to a hostname, SmartWhois won't fail!

[More information](#)

CountryWhois

CountryWhois is a utility for identifying the geographic location of an IP address. CountryWhois can be used to analyze server logs, check e-mail address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address.

[More information](#)

Essential NetTools

Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer's network connections. It's a Swiss Army knife for everyone interested in a set of powerful network tools for everyday use. The program includes a NetStat utility that shows your computer's network connections and open ports and maps them to the owning application. It also features a fast NetBIOS scanner, a NetBIOS Auditing Tool for checking LAN security, and a monitor of external connections to your computer's shared resources, as well as a process monitor that displays information about all the programs and services running on your computer. Other useful tools are included, such as Ping, TraceRoute, and NSLookup. Additional features include report generation in HTML, text, and comma delimited formats and a customizable interface. The program is an easy-to-use and powerful replacement for such Windows utilities as nbtstat, netstat, and NetWatcher. It incorporates many advanced features that standard Windows tools can't offer.

[More information](#)

DigiSecret

DigiSecret is an easy-to-use, secure, and powerful application for file encryption and sharing. It utilizes strong and time-proven encryption algorithms for creating encrypted archives, self-extracting EXE files, and sharing files with your associates and friends. DigiSecret also includes powerful and intelligent file compression; you no longer need .zip files when you can have encrypted and compressed DigiSecret files. The program is integrated with the Windows shell, and you can perform operations on files by right-clicking on them. It also fully supports drag-and-drop operations.

[More information](#)

CommTraffic

CommTraffic is a network utility for collecting, processing, and displaying traffic and network utilization statistics for network connections, including LAN and dial-up. It shows traffic and network utilization statistics for each computer in the segment. The software provides a very attractive and customizable interface, with an optional tray icon menu that displays general network statistics. You can also generate reports that reflect the network traffic volume and Internet connection expenses (if any). CommTraffic supports virtually any rate plan your ISP might use, such as the one based on connection time, traffic volume, time of the day, and other measures. You can set alarms that will inform you when certain criteria (e.g. amount of traffic, expenses) are reached. A configuration wizard will guide you through the setup and automatically detect your network or connection settings.

[More information](#)