Sniffer Wireless
Providing complete network and application management

Wireless LAN for the Enterprise
A growing demand for mobility is the inevitable evolution of today’s networked enterprise environment. According to Phillips Group InfoTech, the Wireless LAN market is projected to grow from $350 million in 1999 to $2 billion in 2003. For CIOs and network managers, this trend raises important questions:

• How can they architect a cost-effective Wireless LAN?
• How can they maximize application performance and minimize network downtime while managing this “network in the air”?
• What security risks are associated with Wireless LANs?
• How can they quickly identify the causes of slow response time in Wireless LAN environments?

Sniffer Wireless, the industry-first Wireless LAN management tool, spots security risks in real-time, identifies network problems quickly and efficiently, and reduces network operating costs.

Features and Benefits
Sniffer Wireless was designed in accordance with the IEEE 802.11b interoperability standard. It includes network monitoring, capturing, decoding, and filtering—all the standard award-winning Sniffer Pro features you already know and appreciate. Sniffer Wireless also provides the most comprehensive 802.11b solution to the unique aspects of wireless networks.

New features include:
• Automatic channel surfing or easy channel selection for a comprehensive view of the total wireless configuration
• Real-time Wired Equivalent Privacy (WEP) decryption when the keys are specified
• Dashboard tab with counters for different Wireless LAN statistics
• Monitor Host Table tab with entries for all detected wireless stations
• Each station is listed with several Wireless LAN-specific counters, including minimum, maximum, and current signal strength
• Decode display for clear understanding of Wireless LAN traffic layers
• Real-time expert analysis to help identify throughput problems, as they occur, and pinpoint which stations are involved, leading to quicker resolution

Wireless LAN for Network Equipment Developers
Developers of wireless network equipment will be pleased to learn that Sniffer Wireless is also an effective quality assurance tool. Sniffer Wireless can proactively analyze and test new products. This improves time to market and keeps your company ahead of the competition.

Automatic Channel Surfing
The Automatic Channel Surfing feature provides a quick overview of traffic and hosts on any of the possible 14 channels, enabling network managers to quickly identify all wireless traffic in their environments. Channel surfing statistics deliver information about all channels in a single consolidated view. To the left is an example of a Sniffer Wireless screen displaying channel traffic statistics.
Wired Equivalent Policy

If the network to be monitored uses Wired Equivalent Policy (WEP) encryption, WEP decryption options can be used to specify the keys in use. When the WEP function is enabled, Sniffer Wireless can decrypt and decode WEP-encrypted packets.

Dashboards

The HTML-based dashboard displays statistical counts for all monitored 802.11b data. It also shows how many packets are sent and at what speed—1Mbps, 2Mbps, 5.5Mbps, or 11Mbps. The Sniffer Wireless screenshot below shows data management and control statistics in a Wireless LAN environment. This information makes it possible to verify the performance of the 802.11b network.

Monitor’s Host Table

The 802.11b-specific host table shows details on every station Sniffer Wireless monitors, including transmission at each speed (1Mbps, 2Mbps, 5.5Mbps, or 11Mbps).

Host Table

Sniffer Wireless shows the extended service set ID (ESSID) per access point. Signal strength is also displayed per station, based on minimum, maximum, and current values.

Decode Display

The decode display provides all 802.11b protocol information needed to understand wireless communication status and identify possible network problems. For example, a network manager can easily determine the origin of a packet or whether a packet has been resent.

Expert System

The Expert system analyzes the 802.11b frames all the way from the physical layer to the application layer. This Expert analysis provides greater visibility into network anomalies and facilitates automatic problem solving. The Expert system includes:

• Automatic Analysis and Alarms—Sniffer Wireless automatically detects and pinpoints problems. The Expert system offers an explanation and probable causes, and tracks event details with an extensive line of protocol decodes
• Automatic Problem Solving—Bottlenecks, protocol violations, even problems like duplicate network addresses and misconfigured routers are identified automatically, before they can impact network performance and end users

Specifications

• A laptop with Microsoft Windows NT 4.0 or Microsoft Windows 2000 is required
  The laptop must have a PCMCIA slot available for a Wireless LAN adapter.

Driver Support and Integration

Currently Sniffer Wireless integrates from two leading manufacturers:

• Symbol Technologies Spectrum24 Model 4121 Wireless LAN adapter cards
• Cisco Systems Aironet 340 client adapter cards

The Cisco Aironet 340 drivers can only run in Sniffer mode (promiscuous 802.11b) or standard Microsoft® Windows mode one at a time. The Symbol Spectrum24 driver can only run in Sniffer mode using the Sniffer driver. For standard Windows use, please refer to Symbol’s standard NDIS driver.

About the Wireless Ethernet Compatibility Alliance and Sniffer Technologies

Sniffer Technologies joined the Wireless Ethernet Compatibility Alliance (WECA) in December 2000. WECA is a non-profit organization formed in 1999 to certify interoperability of Wi-Fi (IEEE 802.11b) products and to promote Wi-Fi as the global, wireless LAN standard across all market segments.

For more information on products, worldwide services, and support, contact your authorized Sniffer Technologies sales representative or visit us at:
3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337
Fax (888) 203-9258
www.sniffer.com