AiroPeek™
AiroPeek NX™

Version 2.0.1 Technical Specifications

Supported Wireless Standards

AiroPeek analyzes traffic on networks conforming to three of the more recent revisions of the IEEE 802.11 WLAN standard: 802.11a, 802.11b, and 802.11g. 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) technology in the 5.0 GHz band to achieve data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. 802.11b uses Direct Sequence Spread Spectrum (DSSS) technology in the 2.4 GHz band to achieve data rates of 1, 2, 5.5, and 11 Mbps. 802.11g is somewhat of a hybrid of the two previous standards as it uses Orthogonal Frequency Division Multiplexing (OFDM) technology in the 2.4 GHz band to achieve data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps at the same time that it is backward compatible with 802.11b DSSS networks and data rates. Although 802.11g also optionally supports Texas Instruments' Packet Binary Convolutional Code (PBCC) coding scheme, AiroPeek does not currently support any cards with this feature. The original specification for 802.11 included another technology, Frequency-Hopping Spread Spectrum (FHSS) which is not widely implemented and is not supported in AiroPeek.

Note: 802.11a WLAN cards based on the Atheros chipset may support a proprietary mode called Turbo Mode (specific card vendors may use other names). Turbo Mode doubles the standard data rates and uses twice the RF spectrum specified for a normal channel in the 802.11a WLAN standard. For more information, please visit the support pages of our website, at: www.wildpackets.com/support.

Support for WEP

WEP (Wired Equivalent Privacy) is a data encryption technique supported as an option in the 802.11 WLAN protocols. The technique uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. The 802.11 WLAN network headers themselves are not encrypted.

AiroPeek Version 2.0.1 Supported Standards

Standard	Spectrum Spreading	RF Band	Data Rates
802.11a	Orthogonal Frequency Division Multiplexing (OFDM)	5 GHz	6, 9, 12, 18, 24, 36, 48, and 54 Mbps
802.11b	Direct Sequence Spread Spectrum (DSSS)	2.4 GHz	1, 2, 5.5, and 11 Mbps
802.11g	DSSS OFDM	2.4 GHz 2.4 GHz	1, 2, 5.5, and 11 Mbps 6, 9, 12, 18, 24, 36, 48, and 54 Mbps

AiroPeek supports the decryption of WEP traffic at various key lengths. Additionally, by allowing the user to input a network's WEP key, AiroPeek can decrypt "on-the-fly" using multiple named key sets. Using a convenient command line utility, AiroPeek can also decode whole packet files that were captured in an encrypted state.

Support for WPA

WPA (Wi-Fi Protected Access) is an encryption and authentication technique that improves the security protection available to wireless networks as compared to the more vulnerable WEP. Wi-Fi Protected Access is derived from and will be forward compatible with the upcoming IEEE 802.11i standard. To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (EIV) with sequencing rules, and a re-keying mechanism. To strengthen user authentication, Wi-Fi Protected Access implements the 802.1x Extensible Authentication Protocol (EAP). Together, these implementations provide a framework for strong user authentication. This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs "mutual authentication" so that the wireless user doesn't accidentally join a rogue network that might steal its network credentials.

AiroPeek supports the decoding and troubleshooting of all of the unencrypted traffic associated with WPA, including the important set-up and key exchange. AiroPeek is therefore able to provide valuable troubleshooting capabilities to the configuration and setup of WPA.
As WPA maintains a secure and ever changing encryption scheme, decryption is not possible and therefore not supported.

System Requirements

AiroPeek requires a computer running Windows 2000, Windows XP, or Windows XP Tablet PC Edition with one of the wireless PC Cards or built-in mini PCI adapters mentioned below. The recommended configuration is a 600 MHz processor with 256 MB RAM or better.

Distributed Analysis with RFGrabber™

AiroPeek's wireless analysis can be distributed throughout an Enterprise or to a geographically remote location with the use of RFGrabber, WildPacket's distributed WLAN analysis probe. For more information about distributed wireless analysis, please visit http://www.wildpackets.com/products/rfgrabber.

Hardware Support

Wireless adapter support is augmented on a regular basis. Check www.wildpackets.com/support for recent additions.

AiroPeek supports the following multi-mode IEEE 802.11a and 802.11g adapters:

- NETGEAR WAG511 802.11a/b/g Dual Band Wireless PC Card
- Linksys WPC55AG Dual-Band Wireless A+G Notebook Adapter
- D-Link AirXpert DWL-AG650 Wireless Cardbus Adapter
- SMC EZ Connect Universal 2.4GHz/5GHz Wireless Cardbus Adapter SMC2336W-AG

AiroPeek supports the following multi-mode IEEE 802.11a and 802.11b adapters:

- D-Link AirPro DWL-AB650 Multimode Wireless Cardbus Adapter
- Linksys Dual Band Wireless A+B Notebook CardBus Adapter
- Linksys Dual Band Wireless A+B Notebook MiniPCI Adapter
- NetGear WAB501 Dual Band Wireless Adapter
- ORiNOCO 8460 Gold 802.11a/b ComboCard
- SMC EZ Connect 2.4Ghz/5Ghz Universal Wireless Cardbus Adapter (2335W)

AiroPeek supports the following 802.11a wireless adapters

- Cisco Systems AIR-CB20A Wireless LAN PC Card
- D-Link AirPro DWL-A650 Wireless Cardbus Adapter
- D-Link AirPro DWL-A650 rev.B Wireless Cardbus Adapter
- Intel(R) PRO/Wireless 5000 LAN Cardbus Adapter
- Intel(R) PRO/Wireless 5000 LAN 3A Mini PCI Adapter
- LinkSys Instant Wireless PC Card (WPC54A)
- NetGear HA501 Wireless Adapter
- Proxim Harmony 802.11a Network Adapter (Model 8450)
- Proxim Skyline 802.11a Network Adapter (Model 4030)
- SMC EZ Connect 802.11a Wireless Cardbus Adapter (2735W)
- Sony 802.11a Wireless LAN Adapter (PCWA-C500)

AiroPeek supports the following 802.11b wireless adapters:

- 2Wire Wireless PC Card
- 3Com 3CRWE737 AirConnect Wireless LAN PC Card
- Avaya Wireless PC Card
- Agere/Lucent ORiNOCO Wireless LAN PC Card
- Agere/Lucent ORiNOCO Wireless LAN Mini PCI
- Buffalo WLI-PCM-L11/GP Wireless LAN Adapter
- Buffalo WLI-PCM-L11G Wireless LAN Adapter
- Cisco Systems 340 or 350 Series Wireless LAN PC Card (WildPackets resells this card, for more information please contact our sales department via email at sales@wildpackets.com or phone at (925)937-3211.)
- Cisco Systems MPI350 Wireless Mini PCI Card
- Compaq WL110 PC Card
- Dell TrueMobile 1150 Series Mini PCI Card
- Dell TrueMobile 1150 Series PC Card
- D-Link Air DWL-660 Wireless PC Card
- ELSA AirLancer MC-11
- ELSA Vianect WLAN MC-11
- Ericsson DSSS Wireless LAN PC Card
- Fujitsu connect2Air WLAN E-1100 PC-Card
- I-Gate 11M PC Card
- Intel(R) PRO/Wireless 2011 LAN PC Card
- Joynet WLAN PC Card
- LANCOM Systems AirLancer MC-11
- NCR WaveLAN/IEEE PC Card
- NEC Corporation Wireless PC Card
- Nortel Networks e-mobility 802.11 Wireless LAN PC Card
- Onair PC Card (INT)
- Onair PC Card (EMB)
- RoamAbout 802.11 DS (Enterasys)
- Samsung SEW-2001p Card
- Samsung SEW-2001m Card
- Skyward PC Card
- Sony PCWA-C100 Wireless PC Card
- Sony PCWA-C150 Wireless PC Card
- SPEED TOUCH PC Card
- Symbol Spectrum24 11 Mbps DS Wireless LAN PC Card
- Toshiba Wireless LAN Mini PCI Card
- Toshiba Wireless LAN PC Card
- WARPSTAR WL11C (PC-WL/1C)
- Westell 802.11b PC Card
- Xircom Wireless Ethernet Adapter

AiroPeek supports the following 802.11g wireless adapters:

- D-Link AirPlus Xtreme G DWL-G650 Adapter (rev A1 not supported)
- D-Link AirPlus Xtreme G DWL-G520 Adapter

Important: Because AiroPeek puts the card in a "listen-only" mode, simultaneous network services are not supported when running AiroPeek. You may receive "Network cable unplugged" or other messages - this is normal. After quitting the program, network services should be restored. If you are using 3Com, Nortel, Symbol, or 802.11b Intel drivers, it may be necessary to switch to the original vendor-supplied drivers for normal network operation.

802.11a Channels

The 802.11a WLAN standard uses OFDM in the 5.0 GHz band. The standard defines channels 1-199, starting at 5.005 GHz, with their center frequencies spaced 5 MHz apart. The FCC in the United States has allocated bandwidth in three parts of the spectrum, low band (5150 MHz to 5250 MHz), medium band (5250 MHz to 5350 MHz), and high band (for outdoor use - 5725 MHz to 5825 MHz). The ETSI and ERM in Europe, MKK in Japan, and other regulatory agencies in other jurisdictions have made their own allocations within this band.

Note: AiroPeek, in conjunction with cards based on the Atheros AR5000 or AR5001 chipsets, will support only channels 36-64 and 149-161.

802.11b Channels

The 802.11b WLAN standard uses DSSS in the 2.4 GHz band. Taking 2412 MHz as the center frequency of the first channel, the standard described 14 channels, 5 MHz apart, numbered 1 to 14. In the United States, the FCC allocated bandwidth to support the first 11 channels. Regulatory bodies in other jurisdictions made different allocations from within this same band.

Note: Adapters purchased in North America operate and capture on channels 1- 11. If you are using AiroPeek outside of North America and need to analyze traffic on channels 12-14 in addition to 1-11, you must purchase a WildPackets-supported card which operates on the correct channels for your location.

802.11g Channels

802.11g functions on the same channels in the same frequency band as 801.11b with the exception that at the higher data rates, it will use OFDM modulation. 802.11g also functions optionally using PBCC, however this is not supported by AiroPeek.

Protocols

AiroPeek decodes over 1,000 protocols and sub-protocols. Below is a list of the higher-level protocols the program decodes. Protocol decodes can be customized or added using the SDK that ships with the AiroPeek software.

Apple	AURP, AARP, ABP, ADSP Header, AEP, AFP, ASP, ATP Header, DDP Header, MACIP, NBP, PAP, RTMP, ZIP
Banyan	ARP, RTP, ICP, EP, IP, IPC, SPP, VINES
Cisco	CDP, HSRP, SCCP
DEC	DNA, DNS, DTS, LAT, MOP, MOP, NSP, SCP, Diagnostic Protocol, DNA Level 1 Routing, DNA Level 2 Routing, Phase IV Routing
IBM	SMB, SNA, FID, NetBEUI, NetBIOS
IEEE	802.1d, 802.1q, 802.11w, 802.1x, 802.2, 802.11, TKIP
IETF	AFP, AH, ARP, ATIP, BGP, BOOTP, CCP, CHAP, DHCP, DNS, DRARP, DVMRP, EAP, ECHO, EIGRP, EGP, ESP, Finger, FTP, GARP/GVRP/GMRP, GRE, GTP/GPRS, HSRP, HTTP, ICMP, IGAP, IGMP, IGRP, IMAP, IPSec, IP, IPv6, IP Mobility, IP NetBIOS Datagram Service, IRC, ISAKMP, iSCSI, KERBEROS, L2F, L2TP, LCP, LDAP, LPD/LPR, MGCP, MPLS, NCP, NNTP, NTP, OSPF, PAP, PIM, PEAP, POP, POP3, PPP, PPPoE, PPTP, RADIUS, RARP, RIP, RSH/RCMD, RSTP, RSVP, RTP, RTCP, RTSP, SAP, SDP, SIP, SLP, SMTP, SNMP, SSDP, SSH, SSL, RMON, SNTP, TALI, TCP, TDS, TLS, TELNET, TFTP, TNS, UDP, VRRP, Multicast DNS
ISO/OSI	CLNP, COTS, ES-IS, IS-IS, OSI, TARP
ITU (VoIP)	ASN.1, H.225, H.245, H.261, H.323, G.711, G.723, G.728, G.729, Q.850, Q.931, Q.932, Q.952, Q.953, Q.955, Q.956, Q.957, SAP, SIP, SSDP
Microsoft	CIFS, SMB, MAPI, MSN Instant Messenger, MSRPC, MSRAP, WINS
Novell	IPX, NetBIOS, NCP, NDS, NLSP, RIP, SAP, SPX
Sun	NFS, RPC, RPC Port Mapper Procedures, RPC NFS Procedures, RPC Mount Procedures
Xerox	ECHO, ERROR, PEP, RIP, SPP, XNS
Others	AOL Instant Messenger, BACnet, DCE RPC, Gnutella, Napster, Yahoo Instant Messenger, WPA/SSN, WAP, WSP, WTP

WildPackets

1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
main (925)937-3200
fax (925)937-3211

www.wildpackets.com

APNX2.0.1, AP2.0.1 -20030626