



AppDancer/FA™

Network Flow Analyzer

- » Three Products in One – Monitors Network Applications, Network Devices, and Network Data
 - » Quickly Identifies Unauthorized or Illegal Applications On Your Network
 - » Actively Monitors Service Level Agreements for All Major Servers
 - » Identifies Potential Network Brown Outs
 - » Advanced Intuitive GUI
 - » Sophisticated, Yet Easy to Use
 - » Viewable From Any Standard Web Browser
 - » Made in the USA
 - » Affordable and Available Now!

It's no secret that today's networks are difficult to monitor and manage. There always seems to be some new application, or some new user requirement, or some new piece of hardware that complicates the lives of network managers and network engineers. Even in the best planned and managed networks, the expectations of corporate management often go unfulfilled.

Requirements continue to change, seemingly on a daily basis. New protocols and applications proliferate, often consuming large chunks of available bandwidth. Any degradation of service - network outages or just slow response time - is perceived as a "network problem", even when the real problem turns out to be a poorly written application, a renegade server, or a user error. Sometimes the problem may be a network problem. But who can tell?

One proposed "solution" has been to move to the ASP/MSP (Application Service Provider/Managed Service Provider) model, outsourcing whole applications to independent third parties. This really just moves the problems elsewhere; it doesn't solve them. And, of course, someone still has to measure the performance of the ASP/MSP.

To make matters worse, many network managers are trying to cope with all these problems using monitoring tools that are not well matched to today's requirements. Many tools were developed in the early or mid 90's, before the full impact of the Internet was understood, before streaming audio and video, before the dominance of the web browser on the desktop, before the emergence of the ASP/MSP model.

Existing tools often are focused on the network/data link layer, while many of today's network problems reside elsewhere. What is needed is an application centric analysis tool, focused where today's network managers really need help - the application layer.

So, with these requirements in mind, allow us to introduce you to **AppDancer/FA™**, the world's first Network Flow Analyzer.

AppDancer/FA provides a unique blend of features, benefits, and value to assist today's network managers in resolving today's real network problems. But don't take our word for it; arrange for a no cost evaluation of **AppDancer/FA** today!



AppDancer/FA consists of a number of processing modules, each designed to help you monitor and manage a different part of your network. Let's take a look at what each module does and how they all work together to assist the network manager every day...

Health Module: The AppDancer/FA Health Module lets you see your IP layer data as you've never seen it before. Real time gauges and graphs quickly inform you as to which applications, protocols, nodes, conversations, and **IP Flows** are using critical levels of your network resources. With just a few clicks, you can quickly identify your true "high demand" users and applications. Often, network problems originate from unauthorized applications running on your network; AppDancer/FA quickly shows you many types of unauthorized traffic, including AOL Instant Messaging™, Microsoft Messenger™, Yahoo Messenger™, Media Player™, Quicktime™, Real Player™, Napster™, and similar high bandwidth applications. AppDancer/FA points you directly to the offending user(s) so that corrective action may be taken. But that's not all – legitimate applications, such as HTTP, SMTP, POP, XWindows, FTP, RIP, and many more, are also identified and categorized regarding each application's impact on available bandwidth. Potential problems are quickly identified for investigation. In total, AppDancer/FA identifies and tracks over 40 different applications and protocols running on your network.

Application Monitoring Module: The AppDancer/FA Application Monitoring Module contains some of the most advanced technology in our entire system. We have focused on seven key network applications for extensive application analysis - HTTP (web), DNS (domain name resolution), POP (incoming mail) SMTP (outgoing mail), FTP (file transfer), H.323 (multimedia/voice), and SIP (Voice over IP). AppDancer/FA presents many views of these applications - beginning with summary gauges that record parameters appropriate for each application, such as emails sent/received, files downloaded, calls made, web sites/pages visited, domain names resolved, etc. - as well as any application level errors encountered. Extensive statistics, appropriate and specific for each application, are easily accessible in table form (a complete list of available statistics may be found in the AppDancer/FA User Manual). AppDancer/FA provides a complete listing of each server it encounters running each application (for example, it might see 2-3 DNS servers, 1-2 FTP servers, 15-20 web servers, and 1-3 mail servers). Each server is identified by IP address and domain name, if applicable. Extensive statistics are again available, listed by server and with errors sorted by server.

AppDancer/FA's most important and powerful analysis feature may be its unique ability to display **Application Flows** for each application. An Application Flow is a set of frames (about 5-200 frames per Flow) that perform a defined function, such as accessing a web server, sending or receiving an email message, resolving a domain name, or making a phone call. For each Application Flow, AppDancer/FA rebuilds and displays the data and logic between sending and receiving network nodes, as well as its associated delta timing and absolute timing. For some Application Flows, such as email messages, FTP commands, and web hits, AppDancer/FA goes even further, rebuilding and displaying the **Content Flow**, the transaction as the end user sees it. This unique feature, unavailable in competitive products, greatly assists the network manager in determining unauthorized application access, abnormal data patterns, and application level errors.

Another important AppDancer/FA feature is its ability to generate **Synthetic Transactions**, allowing the user to actively and periodically monitor the performance levels of applications and servers. AppDancer/FA currently monitors Service Level Agreements (SLAs) for DNS servers, HTTP servers (web sites), SMTP servers, POP servers, and FTP servers. The acceptable level of service (i.e., the expected maximum response time and expected percentage this response time must be met) and the frequency of the tests (i.e., the time interval between individual transactions) are determined by the user. AppDancer/FA then executes the transactions as directed and sets an alarm whenever these thresholds are exceeded.

What about other types of servers? No problem with AppDancer/FA. Define your own servers & traffic types. Traffic to and from these servers will be identified and monitored both in the Health Module and the Application Monitoring Module. AppDancer/FA automatically recognizes many server types including Telnet, Gopher, HTTPS, NNTP, IMAP, LDAP, Radius, Oracle, Microsoft SQL Server, and Sybase. To configure, simply identify a known IP address or hostname as one of these server types and AppDancer/FA does the rest! Or, for unique servers, simply define each one by host name, IP address, and port number; AppDancer/FA will immediately begin identifying and monitoring all traffic to and from these servers. We even support SLA monitoring for the TCP layer connection for all configured servers, even those special ones you define from scratch - what could be more flexible!

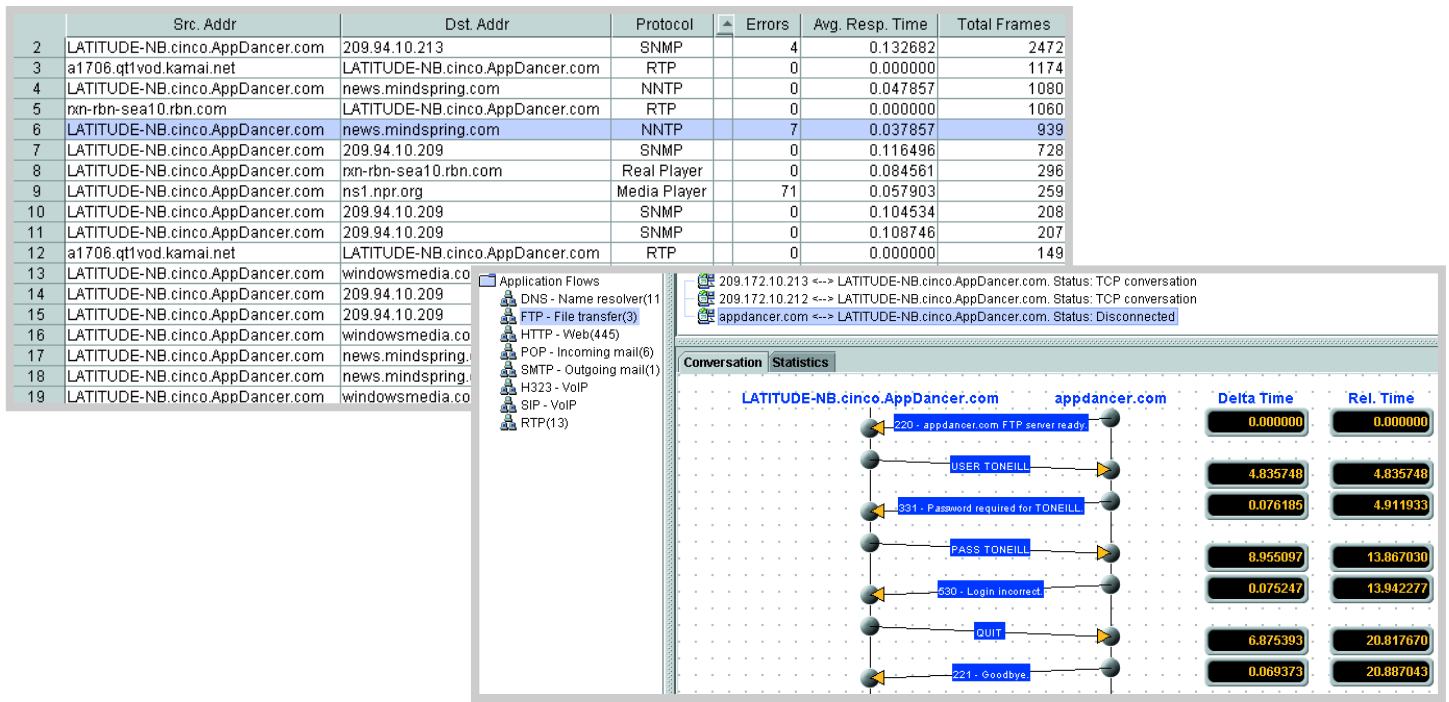


Figure 1. IP Flow View (upper left)

Application Flow View (lower right)

IP Flow View shown above identifies SNMP, NNTP, Real Player, Media Player, and RTP traffic, source and destination addresses, errors, average response times, and total frames.

Application Flow View shows detailed FTP log on/log off logic and associated Delta and Absolute Timing.

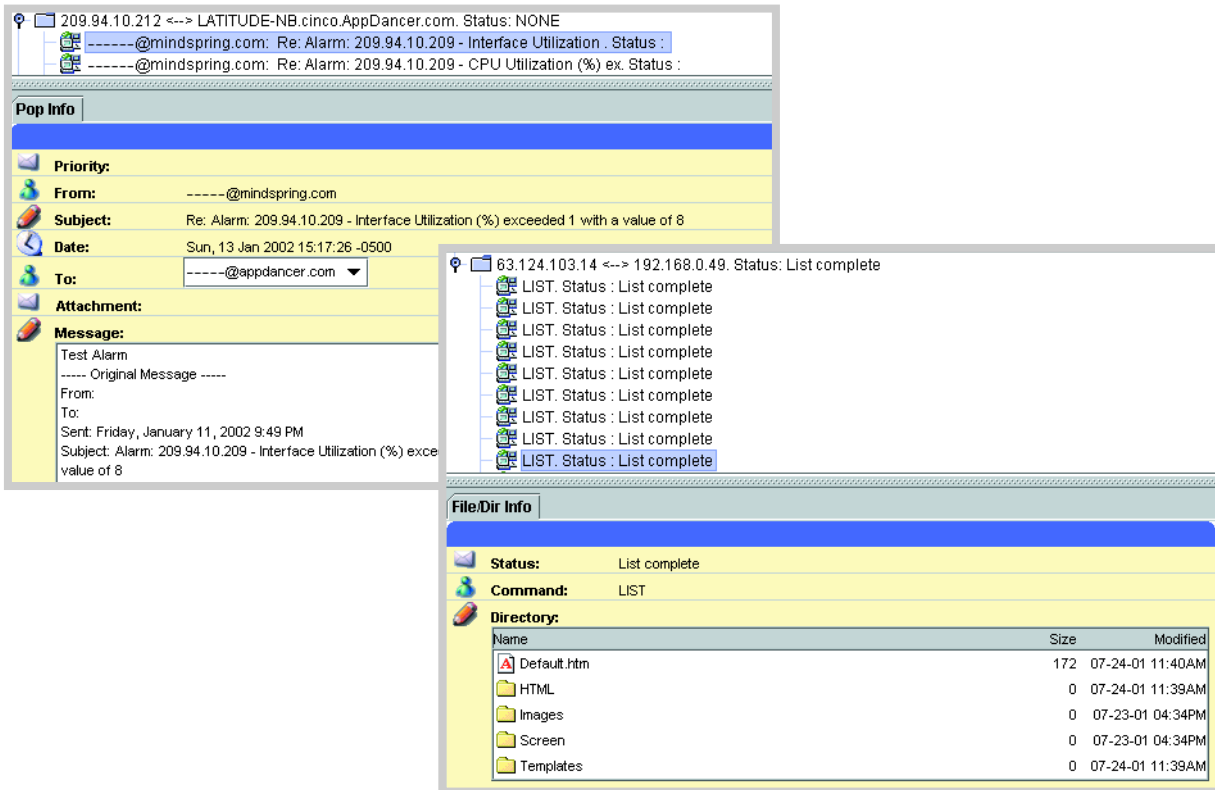


Figure 2. Content Flow Views

Contents Flows recreate end user views of email transactions (upper left) and FTP transactions (lower right).
 NOTE: For privacy, email addresses have been deleted from samples above.

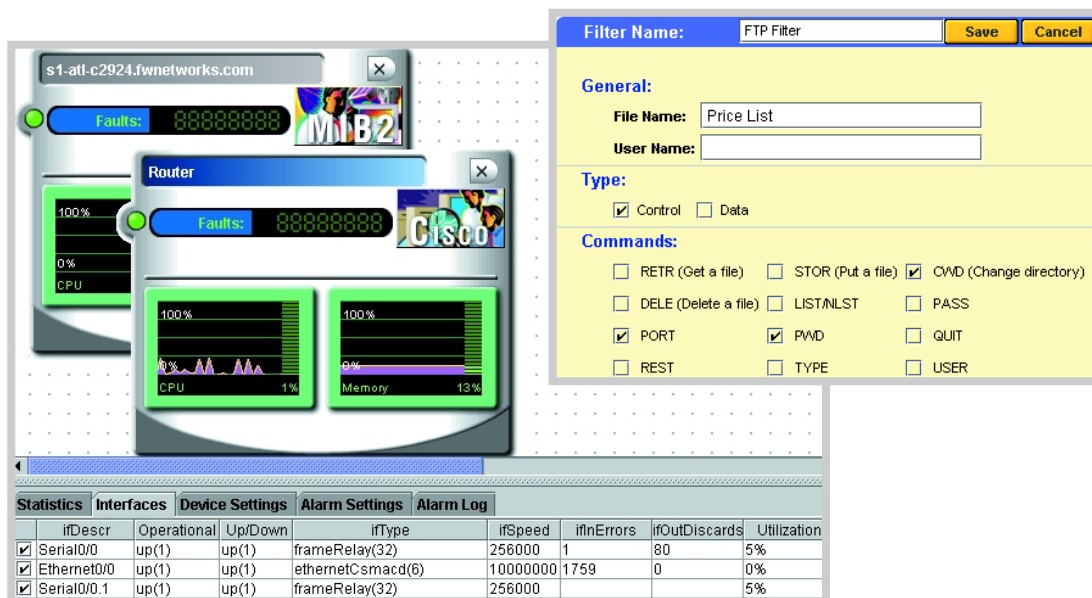


Figure 3. Network Devices Summary View (left)

Network Devices View shows real time status of routers, switches, actual and virtual interfaces, and other network equipment.

Device Monitoring Module: The AppDancer/FA Device Monitoring Module lets you monitor key network devices present in your network, including switches, routers, hubs, gateways, and other addressable devices. AppDancer/FA gathers status information from devices via SNMP commands, but unlike competitors, we don't stop there! AppDancer/FA also uses additional techniques, including Cisco IOS™ commands and CLI (command line interface) emulation, to monitor network devices absolutely invisible to SNMP-only packages! All status data collected for a given device is displayed in a common table or graph – regardless of the source of the data. All MIB1 and MIB2 compatible devices are fully supported. The user may easily add support for other MIBs, including private and unpublished MIBs, by developing custom Java Scripts; modification of the core software is unnecessary. Only AppDancer/FA provides this level of flexibility in monitoring network devices.

Analysis Module: AppDancer/FA also supports traditional protocol analysis features, but with a very important difference – the analysis is **Application Centric** rather than network centric – think of a protocol analyzer turned upside down. Once data has been captured into a local buffer, the application layer is analyzed first, and application errors are identified without requiring the user to plow through the buffer packet by packet (like a traditional protocol analyzer does). Thus, application errors may be identified more quickly, often by lower level support staff.

Capturing data is easy: select a stored filter (optional), and start the capture. Capture buffers of up to 48 Meg are supported, and if the buffer is filled, the user can choose to stop capture or wrap the buffer. Whole frames or only frame headers may be captured. After capture, a buffer may be saved to a file using industry standard formats.

Typical Filter View (upper right)

Filter view illustrates how a filter is created based upon FTP file name, data type, and specific commands.

The complete feature set of Health Module and Application Monitoring Module may be equally applied to the capture buffer, including all summary views, nodes views, and statistics views. AppDancer/FA's unique Flow Views are also supported, including IP Flows, Application Flows, and Content Flows. Advanced filters, available only in post analysis mode, also may be defined to further analyze the buffer data.

And in rare cases, when all else fails to identify and resolve a problem, the user may fall back on the classic three panel decode window, the place where traditional protocol analyzers have always started their "bottom up" analysis. That is, AppDancer/FA can provide all the details of current generation analyzers any time a problem merits such a detailed view. AppDancer/FA's advanced high level views and analysis, however, will often render this type of analysis obsolete and unnecessary.

Configuration Module: The Configuration Module allows users to customize the AppDancer/FA software specifically for their environment. Among the many parameters which may be specified are real time filters, advanced data buffer filters, address book, SLA (service level agreement) thresholds, global sampling intervals, display options, and home page options.

Sophisticated & Elegant Filtering: AppDancer/FA allows the user to create sophisticated, context sensitive data filters by simply clicking boxes appropriate to a specific application, flow, or protocol. For example, one may easily create a filter for a specific web address, web server type, browser type, to/from email address, DNS resolution, VoIP phone number, IP precedence, and much more.

In comparison, creating similar filters in competing products often requires that the user enter exact data patterns, buffer offsets, and hexadecimal data. AppDancer/FA completely avoids the use of these frustrating techniques.

Web Accessible by Design: As a 21st century application, AppDancer/FA is web accessible by design, viewable from any standard web browser “out of the box”. Of course, security functions are included to insure unauthorized third parties cannot view *your* data from *their* browsers. Suppliers of older applications are now attempting to “bolt on” web viewing to their original Wintel applications, with varying degrees of success. AppDancer/FA’s native mode accessibility is a far superior approach.

Customized Home Page View: AppDancer/FA allows users to customize their internal Home Page View in a manner similar to that of major web sites. A personalized single page view may be built where the user can see all important applications, servers, devices, and/or monitoring tasks at a glance. Competing products support only one function, or at best, support multiple functions via disparate page views with no ability to see everything together. Only AppDancer/FA provides a multi-function single page view of all important routers, switches, servers, applications, and data.

Advanced GUI: AppDancer/FA is easy to use. Users traverse from screen to screen in an intuitive fashion; early adopters report a minimal learning curve, especially when compared to competitive products.

Support for Today’s Converging Networks: The old idea of separate networks for voice and data traffic is giving way to new realities. Today’s blended networks must support voice and video, plus traditional data. AppDancer/FA includes extensive monitoring of H.323 & SIP applications (multi-media/VoIP) and also recognizes all popular streaming video/audio traffic on your network, including Real Player, Media Player, and Quicktime. Get ready for the multimedia future with AppDancer/FA!

Powerful, Flexible Alarm Management: AppDancer/FA includes an extremely powerful and flexible alarm manager to inform the network manager of any resource outage or abnormal network condition. Alarms may be based on poorly performing network equipment (router down, high memory utilization, etc.), customized for each major application (slow response time, unauthorized access, illegal data, etc.), linked to suspected network intrusions (broadcast storm, ping storm, syn storm, etc.), and much more. Alarms may be classified as informational, warning, minor, major, and critical. In addition, each alarm may be linked to one or more specific actions, including sending a specific email, sending a page, sending SMS (short message service) text to a cellular phone, sending a SNMP trap, or running a Java Script. The Java Script, of course, may perform any other action required by the user, such as notifying the network SYSLOG.

Reports Galore: Each AppDancer/FA module includes appropriate reports, such as SLA Active Monitor Reports; IP Layer Reports by Flows, Conversations, and Hosts; Network Traffic Reports by Application and Server; VoIP Jitter Analysis; Network Device Status Reports; and more. In the future, an enhanced Reporting Module will be added, providing even more detailed and flexible reports.

Standard Hardware & Software Platforms: AppDancer/FA is a software-only product, requiring no special hardware platform or adapters. Currently, AppDancer/FA runs on Windows 2000 Professional and Windows NT Workstation 4.0. Future versions will support alternative platforms, such as Sun Solaris, Windows 2000 Server, Windows NT Server, Linux, and UNIX.

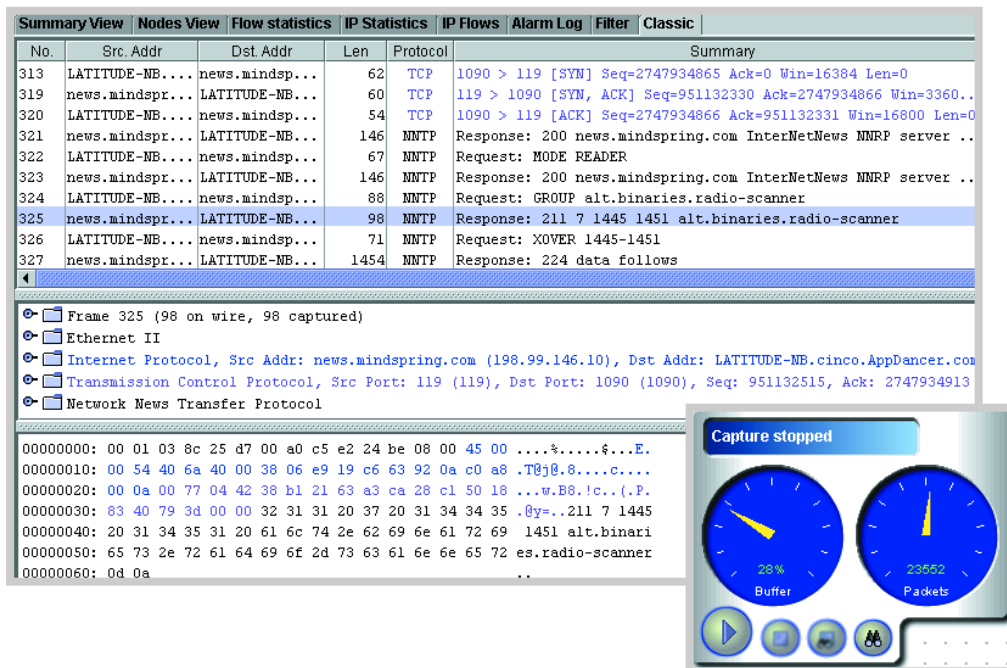


Figure 4. Classic 3 Panel Decode View (left)

Classic three panel decode view shows frame by frame summary, decode, and hex data. The decode view above is filtered based on NNTP protocol.

Capture Gauge (lower right)

Capture Gauge is active during actual capture of data. The number of packets captured and the percent of the buffer filled are shown in real time.

TECHNICAL SPECIFICATIONS

System Requirements:

Industry Standard (Intel or equivalent) computer system, laptop or desktop

Processor: Pentium III or higher (or equivalent); 800 MHz or higher

Monitor: 800x600, 16 color minimum; 1024x768 recommended

Windows 2000 Professional or Windows NT Workstation 4.0 SP6+ Operating Software

Minimum 256Mbyte RAM

Minimum Disk Space: 200Mbyte during installation; thereafter 80Mbyte plus capture files, up to 48Mbyte each

Network Connection with NDIS compliant network device driver

Standard CD drive required for installation from CD; no CD required for Internet download installation

Internal software languages: HTML and Java

Remote Browser Viewing available using Microsoft IE 5.0+, Netscape 6.2+, or equivalent browsers

Product Extensions Available Via Java Scripts:

Custom displays of specific MIB variables and device SHOW commands from CLI (command line interface)

Specific action(s) to be executed as a result of an alarm condition

Support for import/export of various data types

Protocol Decodes Supported (at time of publication):

AARP, AFS, AH, AIM, ARP, ASCEND, ATM, AUTO_RP, BACAPP, BACNET, BACP, BAP, BEEP, BGP, BOOTP, BOOTPARAMS, BROWSER, BVLC, CBCP, CCP, CDP, CGMP, CHAP, CHDLC, CLNP, CLTP, COMP_DATA, CONV, COPS, COTP, CUPS, DATA, DCERPC, DDP, DDTP, DEC_STP, DFS, DIAMETER, DNS, DSI, DVMRP, EAP, EAPOL, EIGRP, EPM, ESIS, ESP, ETH, FDDI, FR, FRAME, FTP, FTP-DATA, GIOP, GMRP, GNUTELLA, GRE, GTPV0, GTPV1, GVRP, H1, H261, HCLNFS, HSRP, HTTP, ICAP, ICMP, ICMPV6, ICP, ICQ, IGMP, IGRP, ILM1, IMAP, IP, IPCOMP, IPCP, IPP, IPV6, IPX, IPXMSG, IPXRIP, IPXSAP, IRC, ISAKMP, ISCSI, ISIS, ISL, ISUP, IUA, KERBEROS, KLM, L2TP, LANE, LANMAN, LAPB, LAPBETHER, LAPD, LCP, LDAP, LDP, LLAP, LLC, LMI, LPD, LSA, M2PA, M2TP, M3UA, MAILSLLOT, MALFORMED, MAPI, MBTCP, MGMT, MIP, MMSE, MOUNT, MP, MPEG1, MPLS, MRDISC, MSDP, MSNIP, MSPROXY, MTP2, MTP3, NBDGM, NBIPX, NBNS, NBP, NBSS, NCP, NDMP, NETBIOS, NETLOGON, NFS, NISPLUS, NISPLUSCB, NLM, NMPI, NNTP, NTP, NULL, OSPF, OXID, PAP, PCNFSD, PGM, PIM, PIPE, POP, PORTMAP, PPP, PPOED, PPOES, PPTP, PRISM, Q2931, Q931, QLLC, QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RADIUS, RANAP, REG, REMACT, RIP, RIPNG, RLOGIN, RPC, RPC_NETLOGON, RQUOTA, RSH, RSVP, RTCP, RTMP, RTP, RTSP, RWALL, RX, SAMR, SAP, SCTP, SDP, SHORT, SIP, SKINNY, SLARP, SLL, SMB, SMPP, SMTP, SMUX, SNA, SNMP, SOCKS, SPOOLSS, SPRAY, SPX, SRVLOC, SRVSVC, SSCOP, SSL, STAT, STATNOTIFY, STP, SUA, SYSLOG, TACACS, TACPLUS, TCP, TELNET, TFTP, TIME, TNS, TPKT, TR, TRMAC, UCP, UDP, V120, VINES, VINES_FRP, VINES_SPP, VJ, VLAN, VRRP, VTP, WAP-WSP, WAP-WSP-WTP, WAP-WTLS, WCCP, WCP, WHO, WKSSVC, WLAN, WLAN_MGT, X.25, X11, XOT, YHOO, YPBIND, YPPASSWD, YPSERV, YPXFR, ZEBRA

Note: New decodes are being added constantly. Please contact AppDancer Networks if your network requires a proprietary, custom or critical decode not listed above; these decodes may now be available.

Order Information:

Order No.	Description
2101-00	AppDancer/FA base software (includes user manual on CD)
2101-10	AppDancer/FA VoIP Module
2104-00	AppDancer/FA Annual Support
2101-90	Hard Copy User Manual

AppDancer Networks, Inc.

1000 Holcomb Woods Parkway
Suite 426
Roswell, GA 30076-2585 USA
Phone 770.643.6800 USA
Toll Free 800.825.7563
Fax 770.643.8888
email info@appdancer.com
web www.appdancer.com



AppDancer and the AppDancer logo are trademarks of AppDancer Networks, Inc. All Rights Reserved.

All software specifications apply to release 1.0. Some versions of AppDancer/FA may not support all features described herein.

All third party trade names used are trademarks or registered trademarks of their respect owners.

Copyright ©2002 AppDancer Networks, Inc.
All Rights Reserved.

Doc version 1.0.1, produced February 2002

For more information contact: