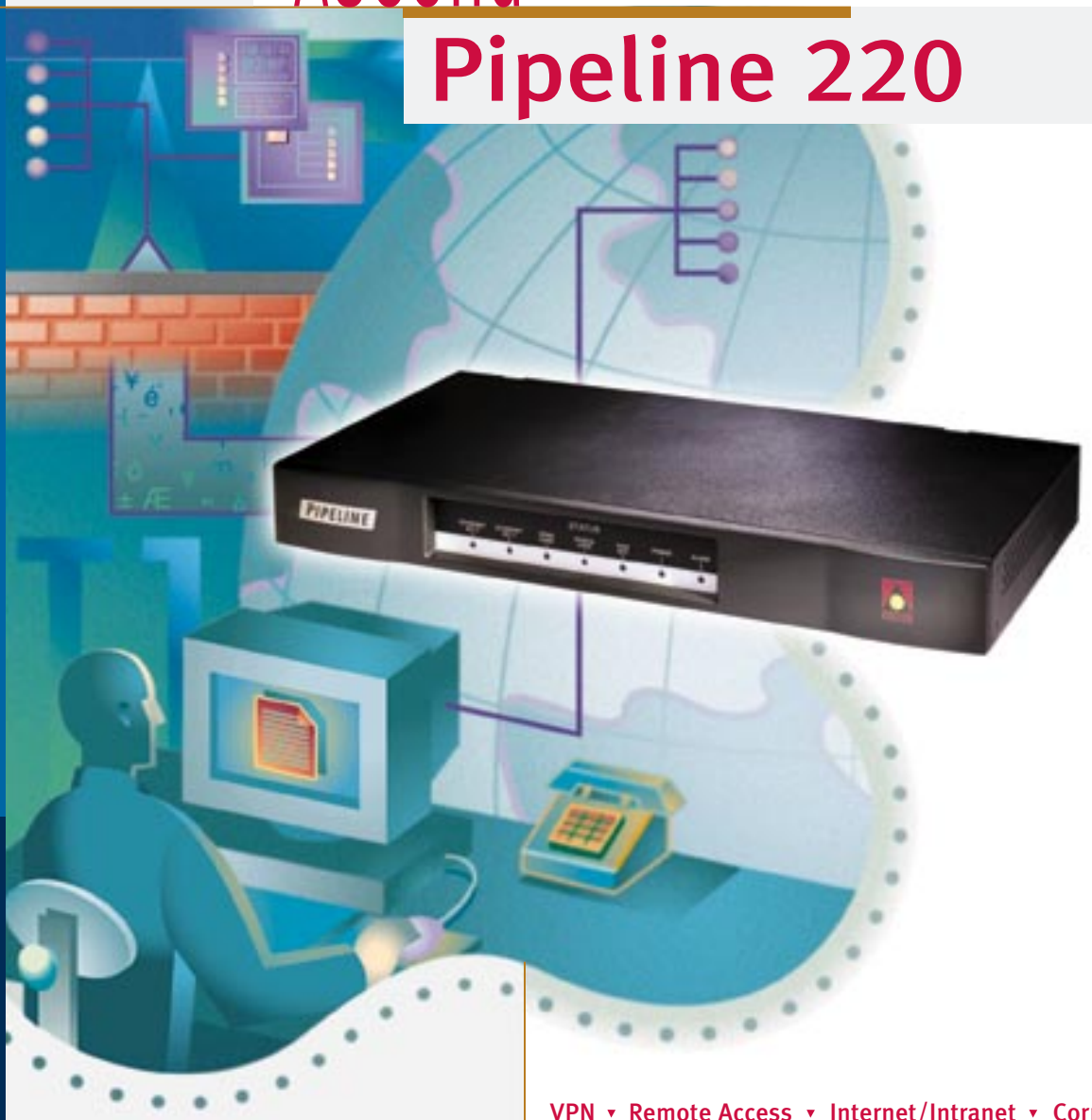
PRODUCT INFORMATION

Ascend Pipeline 220



VPN ▾ Remote Access ▾ Internet/Intranet ▾ Corporate LAN

Convenience, connectivity, and encrypted protection meet in the Pipeline 220 – an economical router for security-conscious businesses.

The Pipeline® 220 remote access router offers open WAN-to-LAN access and comprehensive security features in a single unit. It is ideal for organizations that need to maintain a tightly protected LAN for internal data transactions while permitting the outside world free access to Web servers, FTP sites, and other "public" resources.

The Pipeline 220 connects a Frame Relay or point-to-point WAN to dual independent Ethernet LANs. It uses the Ascend integrated SecureConnect™ Firewall and 40-bit IPSec encryption standard to safeguard all network connections. The formidable combination of LAN autonomy, dynamic firewall, and data encryption creates a "demilitarized zone" that effectively shields your intranet, virtual private network, or other private network from public access. The Pipeline 220 also saves you money by eliminating the need for separate routers and stand-alone security software. Now you can have the connectivity, high-performance, and security you need in one affordable easy-to-manage unit.

ASCEND

Remote Networking/VPN Solution for SOHOs and Remote Offices

Choice of configurations accommodates your WAN interface needs

With the Pipeline 220, remote offices and Internet users can connect to inexpensive Frame Relay services at speeds up to 2 Mbps (as determined by the clock speed from the link). Connections to the Frame Relay network are made either through a V.35 (RS-449) serial interface or an unchannelized T1/FT1 (or E1) interface, depending on the user-defined configuration.

- Choice of V.35 (RS-449) serial port (DB44 connector), T1/FT1 or E1 port (RJ48C connector)
- RFC 1490 Frame Relay encapsulation
- Annex D Link Management
- T1/FT1 interface includes integrated CSU/DSU
- Frame Relay or Point-to-Point transmission services
- PCMCIA card slot holds up to 32 MB of flash memory
- DRAM card slot holds up to 32 MB of additional DRAM

Tunneling protocol support enables virtual private networking

The Pipeline 220 supports popular VPN tunneling protocols, including PPTP, ATMP, and L2TP. These protocols encapsulate non-IP traffic so that it can be sent over the Internet, thereby creating a virtual private network (VPN). The combination of VPN tunneling with IPSec encryption ensures that mission-critical, proprietary, and sensitive data reaches its destination undisturbed and safely through the public Internet.

Concurrent routing and bridging simplify LAN and WAN connectivity

Concurrent routing and bridging eliminates the need for separate devices by providing a single configurable solution for LAN and WAN access.

- IP routing
- IPX and AppleTalk Routing
- BCP standard multiprotocol bridging

Point-and-click configurator makes setting parameters fast and easy

The Java-based Pipeline configurator is a graphical user interface (GUI) that lets users set, save, and restore parameters from any computer running Windows 95 or Windows NT 4.0. It allows network administrators to set or modify all but the firewall parameters via Ethernet.

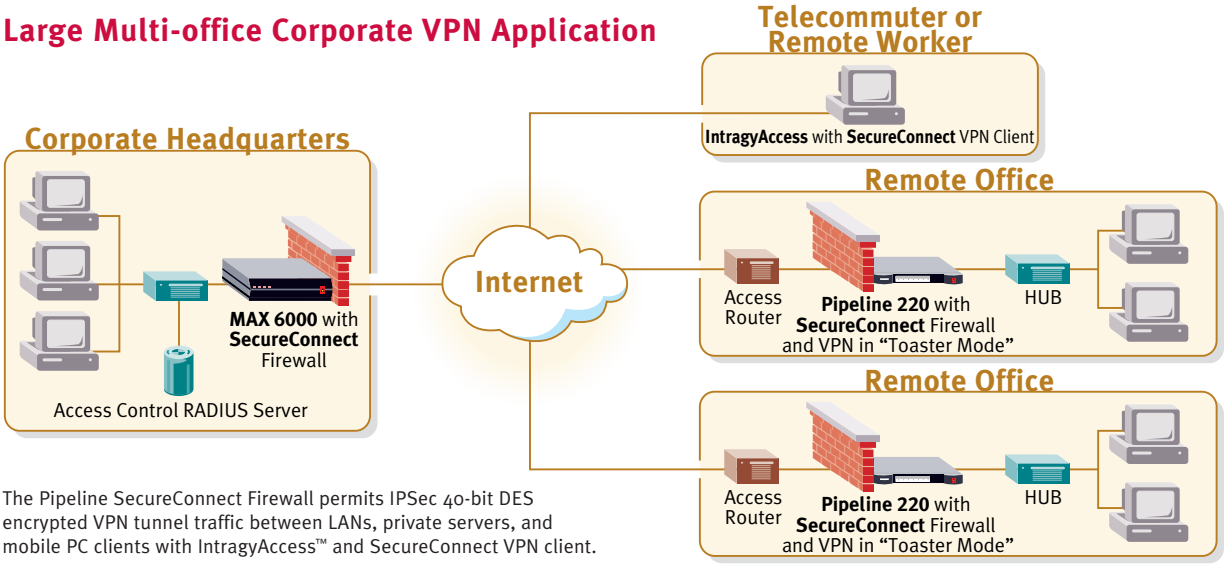
Included in the configurator is a QuickStart utility, which makes first-time setup fast and easy. This tool walks users through the application and features complete HTML-based, online help.

Remote and local management simplifies setup and administration

The Pipeline 220 can be managed locally over one of the Ethernets or remotely over the WAN. Remote management reduces the cost of installation and ongoing support by allowing network managers to monitor and troubleshoot remote user problems directly from the central site.

- Ascend comprehensive, multivendor network management support
- WAN loopback
- SNMP (MIB II) support
- Telnet remote management
- Syslog
- Ascend remote management protocol
- Battery-protected memory for configuration profiles
- Power loss alarm relay

Large Multi-office Corporate VPN Application



The Pipeline SecureConnect Firewall permits IPSec 40-bit DES encrypted VPN tunnel traffic between LANs, private servers, and mobile PC clients with IntragyAccess™ and SecureConnect VPN client.

Comprehensive Security

Protecting corporate assets and ensuring privacy requires comprehensive security – the kind that the Ascend SecureConnect suite of security features delivers. SecureConnect includes the Ascend SecureConnect Firewall and 40-bit IPSec encryption, which are integrated in the Pipeline 220. Completely transparent to valid users, SecureConnect offers one of the highest levels of security available for all devices on the protected LAN.

SecureConnect Firewall provides iron-clad security

The Ascend ICSA-certified SecureConnect Firewall safeguards information at the corporate LAN, remote offices, and telecommuter's home office. It can be activated on the Pipeline 220 WAN port and on one or both of its Ethernet ports. The firewall allows authorized Internet transmissions to securely tunnel through to the appropriate LAN, but soundly excludes unauthorized access attempts. Security statistics from the SecureConnect Firewall keep system administrators informed of any illicit access attempts. Visit the Ascend Web site for more information on SecureConnect.

- Stateful Packet Inspection
- Controlled access of all IP application level protocols
- User definable custom protocols
- Pass/Block control of DEC LAT, IBM LLC2 and all other ethertypes
- Anti-probing and anti-spoofing
- Tailorable Syslog for reporting security alerts
- Configured using SecureConnect Manager
- Remote control of firewall

IPSec encryption shields sensitive intellectual property

The SecureConnect suite of features for the Pipeline 220 includes the Ascend integrated SecureConnect Firewall with IETF-standard 40-bit IPSec encryption capability (56-bit and 3DES available as options). The encryptor encodes and authenticates each and every packet, making the encrypted information virtually impossible for an unauthorized user to interpret. Because the encryptor is integrated with the firewall, encryption becomes available anywhere firewall protection is available.

- Supports RFC 1825, 1826, 1827, 1828
- Supports IPSec tunneling and transport modes
- Authenticates and encrypts all router management transactions
- Supports Authenticated Headers (AH) and/or Encapsulating Security Protocol (ESP)

Network Address Translation conceals host identities

The Pipeline 220 can be configured to apply Network Address Translation (NAT) when routing data to and from the Internet over the WAN. This technique allows the registered IP address of the Pipeline 220 to be substituted for the unregistered IP addresses of the devices on the LANs. Because only one registered IP address needs to be purchased, NAT is a money saving technique. But NAT is also an excellent security technique, because the Pipeline 220 alone "knows" the identities of the devices on its logical ports, and there is no way of predicting which port will be assigned to which device. Moreover, the address of the Pipeline 220 itself is concealed. This makes NAT highly effective for concealing host identities.

The Security of Independent Ethernet LANs

Ethernet is the most popular interface for local area networks (LANs) because it allows heterogeneous devices such as PCs, UNIX workstations, and Macintoshes to share the same network. To keep their Ethernet LANs safe from hackers and other unauthorized users, some network managers install firewall software on every computer. Although this is an effective solution, it can be expensive, places an extra burden on each processor, and makes network management more difficult.

A better way to protect each device on a LAN would be to use a single, very sophisticated firewall and encryptor at the LAN's router. With the Pipeline 220, you can have this kind of independent protection without having to buy and manage extra routing, firewall, and encryption hardware/software.

The Pipeline 220 features two physically separate 10Base-T Ethernet interfaces. These can access the WAN or function in an Ethernet-only configuration. Users will typically dedicate one Ethernet as a "public" LAN while activating the firewall/encryption option on the other Ethernet for security. This combination of an open network with a protected one allows outside users access to an organization's Web site, FTP site, and other admissible resources while providing ironclad safeguards on restricted areas.

Navis network and service management provides advanced network control

The Ascend Navis™ suite of powerful network and service management applications lets service providers deliver new networking services to business and enterprise customers more quickly and profitably. In turn, this gives enterprise managers access to public networks with services that meet their needs. Navis software provides service providers and enterprise managers with extensive wide area network (WAN) and service management:

- Integrated solution for complete control across the WAN
- A robust solution that drives down service provider operating costs by protecting data, ensuring network uptime, and reducing ongoing maintenance costs
- Superior network management across the access, edge, and core layers of the WAN

Managed by Navis™

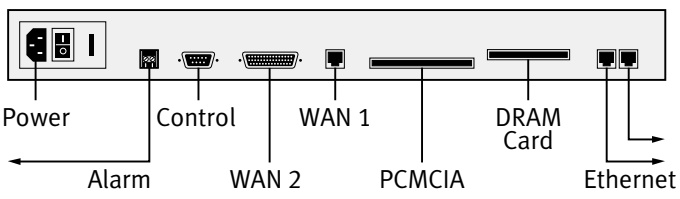
Hardware Specifications

Model No.	P22-T1-V35 P22-E1-V35
Dimensions	17.63 in x 2.0 in x 8.25 in [44.8 cm x 5.1 cm x 21.0 cm]
Weight	7.25 lbs [3.3 kg]
LAN Interface	Dual 10 Mbps Ethernet interfaces
WAN Interface	V.35/RS-449 or Unchannelized T1/FT1 (software configurable)
Software Upgrade	Via built-in flash RAM
Power Requirements	100-265 VAC, 47-63 Hz, 12-45 W
Operating Requirements	Temperature: 50-104˚F [10-40˚ C] Altitude: 0-12,000 feet [0-3,650 meters] Relative Humidity: 5-95% (non-condensing) EMI/RF FCC Part 68, FCC Part 15

Software Specifications

Routed Protocols Supported	Concurrent TCP/IP, IPX, AppleTalk, BCP standard bridging of all protocols
VPN Tunneling Protocols Supported	PPTP, ATMP, L2TP, (Model No. P22-SO-VPN or Model No. P22-SWOP-VPN)
WAN Protocols Supported	PPP, RFC 1490 Frame Relay, V.35
Management	Serial cable connection, Ascend remote management protocol, Telnet, SNMP, Java-based configurator, Navis™ network management
Security	SecureConnect Firewall, 40-bit IPSec encryption standard (56-bit and 3DES optional), VPN tunneling (L2TP, ATMP, PPTP)

Pipeline 220 Back Panel



Ascend Communications, Inc.

Worldwide and North American Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2300
Email: info@ascend.com
Toll Free: 800.621.9578
Fax Server: 650.688.4343
Web Site: http://www.ascend.com

European Headquarters
Rudolf-Diesel-Strasse 16
D-64331 Weiterstadt
Germany
Tel: +49.6150.1094.10
Fax: +49.6150.1094.98

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Asia-Pacific Headquarters
Suite 1908, Bank of America Tower
12 Harcourt Road
Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
Tel: 510.769.6001
Fax: 510.747.2669

Ascend Communications, Inc. is a leading provider of wide area network and intelligent networking technologies for the next-generation public network, a packet-based infrastructure that integrates data, fax, video, and voice communications.

Ascend markets the Ascend SS7 Gateway, B-STDX, CBX, GRF, GX, Intragy, IP Navigator, MAX, Multiband, MultiDSL, Navis, Pipeline, SA, and SecureConnect families of products. Ascend products are available in more than 40 countries worldwide. For more information about Ascend and its products, please visit the Ascend Web site at http://www.ascend.com, or email info@ascend.com.

Ascend and the Ascend logo are registered trademarks and all Ascend product names are trademarks of Ascend Communications, Inc. Other brand and product names are trademarks of their respective holders.

Specifications are subject to change without notice.

© Copyright 1999 Ascend Communications, Inc.

01-51a
03/99

ASCEND Where Network Solutions Never End™

ISO 9001 REGISTERED