Cable/DSL VPN Router With IPSec and 4-port Switch

The DI-804V is a high-performance broadband Internet Gateway Router with secure data transmission designed for branch office communication. Cost-effectively linking a small office to the outside world through the Internet, the DI-804V offers an alternative to the cost-prohibitive point-to-point dedicated connectivity of leased lines. This business-class router provides IPSec security for Virtual Private Network applications, enabling you to extend your branch network to remote networks, such as your corporate office or a trusted supplier, to act as if the two are a single LAN. In addition, the DI-804V also provides cost-saving Internet functions to let you share a single cable/DSL modem and ISP account among your office users, while providing them with physical connections through the built-in LAN switch ports.

Secure Transmission Over the Internet
The DI-804V prevents your confidential data from being accessed and tampered with when traveling along the public Internet to your destinations. Through VPN tunneling protocols, the DI-804V privatizes your communication channels. You can safely exchange mail and data with your head office over the Internet, without fear of observation, modification, or spoofing.

IPSec and Multi-Level VPN Services
With support for up to 8 IPSec tunnels, the DI-804V can provide flexible VPN implementation for data confidentiality, integrity and origin authentication to remote sites. Supported data encapsulation, encryption and authentication options include IP ESP, DES, 3DES, MD5 and SHA-1. This enables you to carry out applications such as virtual private networks, including Intranets, Extranets, and remote user access.

Powerful Routing Engine
The DI-804V is equipped with a powerful 32-bit RISC CPU and large RAM to perform its intensive security tasks. This allows the router to run without data throughput degradation while supporting DES/3DES encryption and other security features.

Business-class LAN Security
The DI-804V provides firewall security using Stateful Packet Inspection (SPI) and hacker attack logging for Denial of Service (DoS) attack protection, plus VPN pass-through for extra security. SPI inspects the contents of all incoming packet headers before deciding what packets are allowed to pass through. The DI-804V also blocks and re-directs certain ports to limit the services that outside users can access on your network. Virtual Server Mapping is used to re-task services to multiple servers. The DI-804V can be set to allow separate FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting your servers and workstations from hackers. To monitor hacker attacks, the DI-804V can log up to 32 event messages showing possible attacks.

DMZ Host to Open Public Domain
A DMZ setting can be applied to a single client (such as a Web server) behind the DI-804V to fully expose it to the Internet and ensure complete Internet application compatibility even if the specific port is not known. This allows you to set up web sites and e-commerce applications from your office while maintaining protection for the rest of your office LAN.

Simplified, Cost-saving Broadband Internet Connection
Of course, the basic benefit is to share the broadband line to the entire office, using a single cable or DSL modem. To let everybody logon, the DI-804V automatically creates and assigns an IP number for each computer, simplifying every one’s logon operation.

4 Switch Ports for Ready LAN Connection
With 4 built-in auto-sensing 10/100Mbps Fast Ethernet switch ports, the DI-804V provides ready connection for workstations and servers, saving you the cost and trouble of installing a separate LAN switch.

UPnP Enabled for Compatibility
The DI-804V is designed for easy and robust connectivity among heterogeneous standards-based network devices. Computers can communicate directly with the DI-804V for automatic opening and closing of UDP/TCP ports to take full advantage of security provided without sacrificing functionality of on-line applications such as video conferencing.

Features
- Broadband Internet Gateway (NAT router)/IP router with VPN
- 168-bit 3DES IPSec advanced VPN security
- 3DES with SHA-1 advanced secure configuration
- Up to 8 VPN tunnels to 8 remote sites
- Packet filtering firewall protection
- Broadband DSL or cable modem connection
- ISDN or 56Kbps analog modem backup
- Dial-on-Demand & idle timer auto-disconnection (for dial-up
- ISDN & analog connection)
- Virtual servers & DMZ support
- Web-based configuration setup
- Firmware upgradeable with future enhanced versions
- Universal Plug-n-Play (UPnP) enabled
DI-804V
Technical Specifications

Hardware
Number of Ports
- 1 RJ-45 10BASE-T port for DSL/Cable modem connection
- 1 DB-9 RS-232 port (460Kbps Baud) for ISDN TA/analogue modem connection (for WAN backup)
- 4 RJ-45 10BASE-T/100BASE-TX 10/100Mbps LAN switch ports

CPU
Arm7 32-bit RISC

Memory
- SDRAM: 16MB
- Flash: 1MB

Factory Reset
1 push button

WAN
Number of WAN Ports
- 1 RJ-45 10BASE-T port for DSL/Cable modem connection
- 1 DB-9 RS-232 port (460Kbps Baud) for ISDN TA/analogue modem connection (for WAN backup)

Broadband Support
- ADSL modem
- Cable modem
- PPP over Ethernet

Backup Link Support
- Dial-up ISDN TA
- Dial-up Analog modem
- PPP
- Dial-on-Demand with auto login to ISP
- Auto-disconnect with user-defined idle timer
- PAP/CHAP security

Routing
Routed Packet Type
IP packets

Routing Protocols & Methods
- RIP-1, RIP-2

Static Routing
- Dynamic Routing

Firewall Security
Stateful Packet Inspection (SPI) to prevent Denial of Service (DoS) attacks (Syn flood, ICMP flood, UDP flood, “ping of death”, IP spoofing, land attack, tear drop attack, IP address sweep attack, Win Nuke attack), Intrusion Detection Logging and LAN/WAN filtering.

VPN
Functionality
Eight (8) dedicated VPN tunnels, Manual key and IKE Security Association(SA) assignment, 56-bit (DES) or 168-bit (3DES) IPSec encryption algorithms, MD5 or SHA-1 authentication algorithm, pre-shared key, perfect forward secrecy (Diffie-Hellman AND Oakley client support), key life and IKE lifetime settings, prevent replay attack, remote access VPN (client-to-site), site-to-site, VPN pass-through.

VPN Layers
- Layer 2 pass-through
- Layer 3 with IPSec

VPN Layer 2 Protocols
- PPTP (Point-to-Point Tunneling Protocol)
- L2TP

Application Support
- IPSec pass-through
- PPTP
- NetMeeting

Layer 3 IPSec Security
Data Encryption Methods
- IP ESP (Encapsulating Security Payload) Confidentiality over IP payload
- Optional authentication of IP payload and ESP header
- Null encryption

Encryption Transforms
- DES (Data Encryption Standard)
- 3DES

Authentication Transforms (for ESP and AH)
- MD5
- SHA-1

Supported Key Management Protocol
Internet Security Association and Key Management Protocol (ISAKMP)

Connection Modes
- Site to Site
- Client to Site

Number of Tunnels
8 IPSec tunnels (max.)

Internet Gateway
Supported Functions
- Network Address Translation (NAT)
- DHCP server automatic IP assignment
- Virtual server

Packet Inspection
Stateful Packet Inspection (SPI)

Hacker Attack Logging 32 event messages (max.)

RFC Support
- PPTP client and server (RFC 2637)
- IPSec tunnel mode (RFC 2401)
- HMAC-MD5-96 (RFC 2403)
- HMAC-SHA1-96 (RFC 2404)
- Encapsulation Security Payload Protocol (RFC 2406)
- DHCP server (RFC 2131)
- DHCP client (RFC 2131)
- IP routing (RIP1, RIP2) (RFC 2453)
- NAT (many-to-one) (RFC 1631)
- IP control Protocol (RFC 1332)
- PPPoE (RFC 2516)

LAN
Standards
- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- ANSI/IEEE 802.3 NWay auto-negotiation
- IEEE 802.3x full-duplex flow control

LAN Protocol CSMA/CD
Topology
Star

Number of LAN Ports
4 RJ-45 10BASE-T/100BASE-TX auto-sensing switch ports

Data Transfer Rates
- Ethernet:
  - 10Mbps (half duplex)
  - 20Mbps (full duplex)
- Fast Ethernet:
  - 100Mbps (half duplex)
  - 200Mbps (full duplex)

Network Cables
- 10BASE-T:
  - UTP Cat. 3, 4, 5 (100 m max.)
  - EIA/TIA-586 100-ohm STP (100 m max.)
- 100BASE-TX:
  - UTP Cat. 5 (100 m max.)
  - EIA/TIA-568 100-ohm STP (100m max.)

Media Interface Exchange
MDI-II/MDI-X auto-sensing for all LAN ports

Packet Switching Method
Store-and-forward

MAC Address Filtering Table
1K entries per device

MAC Address Learning
Automatic update

Management & Configuration
IP Number Self-identification
- Through DHCP client

Local & Remote Management
Web-based utilities (via browser)

Firmware Upgrade
- Web-based (via browser)
DI-804V
Technical Specifications

**Physical & Environmental**

**Diagnostic LEDs**
- Link (WAN port and serial port)
- Act (WAN port and serial port)
- Link/Act (per LAN port)
- Power (per device)

**Power Supply**
- DC 5V 1.5A
- Through external AC power adapter

**Dimensions**
190 x 117 x 31 mm palm-sized

**Weight**
360 grams (approx.)

**Operating Temperature**
-5° - 45°C (23° - 113°F)

**Storage Temperature**
-20° - 70°C (-4° - 158°F)

**EMI Certification**
- FCC Class B
- CE Class B
- C-Tick Class B
- BSMI Class B

---

**Ordering Information**

Broadband Internet Gateway With VPN Security

**DI-804V**
1 RJ-45 10BASE-T port for ADSL/cable modem connection
1 RJ-45 10BASE-T hub port
4 RJ-45 10BASE-T/100BASE-TX switch ports

Please specify one of the following after the model number:

/A Includes an American standard AC power adapter
/E Includes an EU standard AC power adapter
/B Includes a UK standard AC power adapter
/N Includes an Australian standard AC power adapter

D-Link®

Specifications subject to change without notice.
D-Link is a registered trademark of D-Link Corporation or its subsidiaries. All other trademarks belong to their proprietors.

Rev. 01 (June 2002)
Printed in Taiwan
DI-804V
Applications

Cable/DSL VPN Router

LAN Security From Internet Attacks
The DI-804V provides firewall and other security protection against attacks from outsiders.

Virtual Private Network
The DI-804V provides up to 8 IPSec tunnels for VPN application.

Head Office
Database
Workstations
Remote Router
IPSec Security

Trust Supplier
Database
Workstations
Remote Router
IPSec Security

Branch Office
DSL/Cable Modem
Web Server
Internal Mail Server
DMZ Public Domain
Private Domain