D-Link®
Building Networks for People

Product Highlights

Comprehensive Management Solution

Advanced features such as WAN failover, load balancing and integrated firewall make this a reliable, secure and flexible way to manage your network

Complete VPN Features

With fully featured VPN as well as IPSec hub-and-spoke technology, secure communications between mobile employees and offices can be configured easily

Web Authentication Capabilities

Captive Portal allows employees and guest users to be easily authenticated and authorised by accessing customised landing pages

DSR Series
Unified Services VPN Routers

Features

High-Performance VPN
- Protocols
  - IPSec, PPTP/L2TP, GRE, SSL, OpenVPN
- VPN Tunnels
  - DES, 3DES, AES, Blowfish, Twofish, CAST128
  - Hub and Spoke

Enhanced Network Service
- IPv6
- IEEE 802.11q VLAN
- Multiple SSIDs
- Port Monitoring/Bandwidth Control
- IGMP Proxy, IGMP Snooping
- Web Authentication Capabilities
- Application Control
- Web Content Filtering

Wireless Access and Security (DSR-1000AC only)
- IEEE 802.11 a/b/g/n/ac
- IEEE 802.1x RADIUS Authentication with EAP-TLS, EAP-TLLS, EAP-PEAP
- WPS, WEP, WPA-PSK, WPA-EAP, WPA2-PSK, WPA2-EAP

Fault Tolerance
- WAN Traffic Failover & Outbound Load Balancing

The DSR Series Unified Services VPN Routers provide secure, high-performance networking solutions to address the growing needs of small and medium businesses. With integrated high-speed wireless technology, the DSR-1000AC offer comparable performance to wired networks but with fewer limitations. 802.11ac offers wider radio frequency band support on the 5 GHz band, allowing devices to connect at wireless speeds of up to 1300 Mbps[1].

Comprehensive Management Capabilities

The DSR series include dual WAN Gigabit Ethernet ports to provide high availability for your WAN or Internet connections. Traffic can be load-balanced across the links with Outbound Load Balancing, increasing the performance and availability of business applications. The secondary WAN port can also be used to create a DMZ, isolating servers from your LAN. The DSR series supports mobile broadband networks via an extendable USB modem[2], such as 3G/4G dongles. Traffic load balancing can be performed on mobile data connections, providing an additional layer of redundancy for critical or backup applications.

Web Authentication Capabilities

Captive Portal allows employees and guest users to authenticate and authorise easily by accessing a customised landing page. A local database, RADIUS, LDAP, Microsoft Windows Active Directory, NT Domain and POP3 server can authenticate users. A maximum of four servers can be configured at any one time.

Application Control

Application control enhances security by only allowing certain types of network traffic for predefined applications. The DSR Series uses application control to help accurately shape network traffic by either giving priority or applying control policies to effectively manage network utilisation. Using packet inspection and a database of application signatures based on the application's network usage patterns, the DSR Series gives complete control over the content that is delivered to end users.

Web Content Filtering

The DSR-250V2 also provides a web content filtering feature to help administrators monitor, manage and control employees' Internet usage. Static web content filtering helps to remove malicious objects such as Java applets, ActiveX, and cookies or to block URLs by keyword. Dynamic web content filtering, which requires a license subscription, allows administrators to filter content from a list of categories. Multiple global index servers, with millions of URLs and real-time website data, enhance performance and maximise service availability.
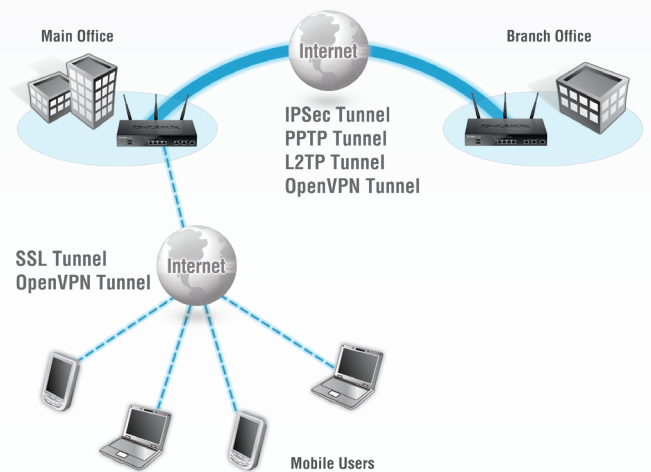
Complete and Robust VPN Features

A fully featured virtual private network (VPN) provides your mobile workers and branch offices with a secure link to your network. The DSR series routers are capable of Secure Sockets Layer (SSL) VPN tunnels, as well as Generic Routing Encapsulation (GRE) tunnels, empowering your mobile users by providing remote access to a central corporate database. Site-to-site VPN tunnels use IP Security (IPSec) Protocol, Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunneling Protocol (L2TP) to facilitate branch office connectivity through encrypted virtual links. OpenVPN allows mobile users to connect to the intranet via encrypted links with their PC, laptops or mobile devices.
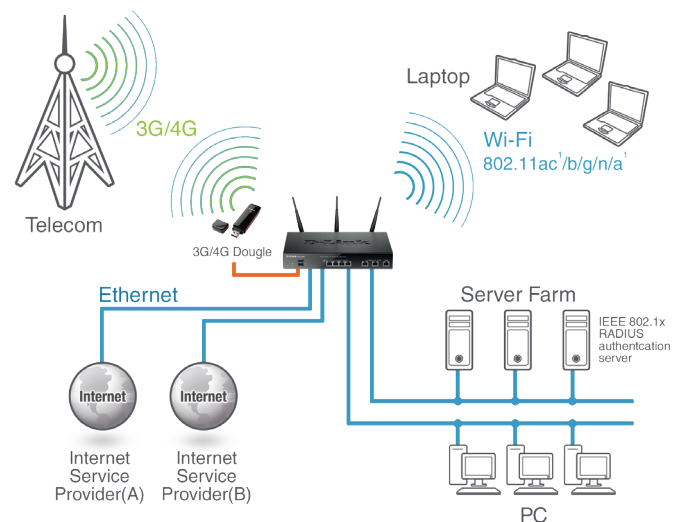
Web Content Filtering

Application Control

Secure VPN Network Implementation

Main Office

Internet

Branch Office

IPSec Tunnel
PPTP Tunnel
L2TP Tunnel
OpenVPN Tunnel

SSL Tunnel
OpenVPN Tunnel

Internet

Mobile Users

Dual WAN for Redundant Internet

Laptop

3G/4G

Wi-Fi
802.11ac[1]/b/g/n/a[1]

Telecom

3G/4G Dougle

Ethernet

Server Farm

IEEE 802.1x
RADIUS
authentcation
server

Internet

Internet

Internet
Service
Provider(A)

Internet
Service
Provider(B)

PC

Technical Speci cations

General	DSR-250V2	DSR-1000AC
Hardware Version	B1	A1
Ethernet Interface	1 x 10/100/1000 Mbps WAN port 3 x 10/100/1000 Mbps LAN ports 1 x 10/100/1000 Mbps configurable port	2 10/100/1000 Mbps WAN Ports 4 10/100/1000 Mbps LAN Ports
Wireless Interface	-	802.11 ac/a/b/g/n (Concurrent dual band) 3 Detachable 2 dBi Omni-Directional Antennas
Maximum Wireless Speeds[1]	-	450 Mbps - 2.4 GHz 1300 Mbps - 5 GHz
USBPort	1 x USB 3.0	2 x USB 2.0
Console Port	RJ-45	
Performance[4]		
Firewall Throughput[3]	950 Mbps	950 Mbps
VPN Throughput (3DES)[5]	200 Mbps	250 Mbps
Concurrent Sessions	50,000	100,000
New Sessions (per second)	2,000	1,000
Firewall Policies	300	600
Internet Connection Type		
Static/Dynamic IP	✓	
PPPoE/L2TP/PPTP	✓	
Multiple PPPoE	✓	
Firewall System		
Static Route	✓	
Dynamic Route	RIP v1/v2, OSPF, OSPFv3	
Dynamic DNS	✓	
Inter-VLAN Route	✓	
NAT, PAT	✓	
Web Content Filtering	Static URL, Keywords, Dynamic WCF (License is required)	
Intrusion Prevention System (IPS)	Signature Package Included in Firmware	
Authentication	Internal User Database, Radius, POP3, LDAP, AD, NT Domain	
Application Control	✓	

Technical Speci cations

Networking	DSR-250N	DSR-1000AC
DHCP Server/Client	1024 client	
DHCP Relay	✓	
IEEE 802.11q VLAN	✓	
Number of VLANs (port-based)	16	
IP Multicast	IGMP Proxy, IGMP Snooping	
IPv6	✓	
Route Failover	✓	
Outbound Load Balancing	✓	
3G/4G Redundancy	✓	
Wireless		
Multiple Service Set Identifier (SSID)	-	✓
Service Set Identifier (SSID) to VLAN Mapping	-	✓
Standard	-	802.11 ac/a/b/g/n
Wireless Security	-	Wired Equivalent Privacy (WEP) Wi-Fi Protect Setup (WPS) Wi-Fi Protected Access – Personal (WPA-PSK) Wi-Fi Protected Access – Enterprise (WPA-EAP) Wi-Fi Protected Access version 2 – Personal (WPA-PSK) Wi-Fi Protected Access version 2 – Enterprise (WPA-EAP)
Virtual Private Network (VPN)		
VPN Tunnels	75	195
IPSec Tunnels	50	70
PPTP/L2TP Tunnels	30	50
GRE	20	25
OpenVPN Tunnels	20	25
Encryption Methods	DES, 3DES, AES, Twofish, Blowfish, CAST-128, NULL	
SSL Encryption Methods	RC4-128, 3DES, AES	
IPSec/PPTP/L2TP/OpenVPN Server	✓	
IPSec NAT Traversal	✓	
Dead Peer Detection	✓	
IP Encapsulating Security Payload (ESP)	✓	
IP Authentication Header (AH)	✓	
VPN Tunnel Keep Alive	✓	
Hub and Spoke	✓	

Technical Speci cations		
Bandwidth Management	**DSR-250N**	**DSR-1000AC**
Maximum Bandwidth Control	Classes Minimum/maximum bandwidth control rate	
Priority Bandwidth Control	Low/Medium/High	
System Management		
Web-based User Interface	✓	
Command Line	✓	
SNMP	v1, v2c, v3	
Physical & Environment		
Power Supply	External Power Supply Unit DC 12 V/1.5 A	External Power Supply Unit DC 12 V/3 A
Max. Power Consumption	14.4 W	23.1 W
Dimensions (L x W x H)	190 x 120 x 38 mm	280 x 180 x 44 mm
Operation Temperature	0 to 40 ℃	
Storage Temperature	-20 to 70 ℃	
Operation Humidity	5% to 95% non-condensing	
EMI/EMC	FCC Class B, CE Class B, RCM, IC, VCCI	
Safety	LVD (EN62368)	
MTBF	1,230,157.85 hours	360,000 hours

[1] Maximum wireless signal rate derived from IEEE standard 802.11 and 802.11ac speci cations. Actual data throughput will vary. Network conditions and environmental factors, including volume of network tra c, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors may adversely a ect wireless signal range.
[2] The following portable modem are supported: DWM-152 A1, DWM-156 A1/A3/A5/A6/A7/A8, DWM-157 A1/B1/C1/D1, DWM-158 D1/E1 and DWP-156 B1 and DWP-157 B1, DWM-221/222, HUAWEI: E1550, E173, EC306 and E303.
[3] Firewall throughput is measured using UDP tra c with a 1,518 bytes packet size, adhering to RFC2544.
[4] Actual performance may vary depending on network conditions and activated services.
[5] VPN throughput is measured using UDP tra c with the packet size 1420 bytes and encryption method 3DES plus SHA-1, adhering to PFC2544.

For more information: eu.dlink.com

D-Link®
Building Networks for People