Vigor3900

Multi-WAN Security Appliance

DrayTek

www.draytek.com

- 500 simultaneous VPN connections
- Gigabit Ethernet LAN/WAN and active fiber interfaces with load-balancing
- High Availability and failover
- Robust Firewall and Bandwidth Management
- Ease of management

The Vigor3900 Central site VPN gateway is an enterprise-level VPN concentrator providing security and cost savings benefits for business through flexible, reliable, and high-performance LAN-to-LAN and remote-access solutions. Vigor3900 not only offers hundreds of VPN tunnels compatible with multiple VPN protocols, such as PPTP/L2TP/IPSec/L2TP over IPSec to satisfy LAN-to-LAN and remote secure communication needs, but also provide SSL VPN* connectivity to better facilitate remote users to access corporate database. With Gigabit Ethernet LAN/WAN and active fiber interfaces, Vigor3900 offers unprecedented data transmission speed for mission-critical applications and do load-balancing for WAN and VPN failover to enhance performance, redundancy and reliability of business operation.

Enterprise-level central site VPN gateway

By using VPNs to establish secure, end-to-end private network connections over a public networking infrastructure, business can reduce considerable communications/travels expenses and still remain seamless connectivity between central and remote sites including mobile workers, telecommuters, and extranet users by accessing corporate database any time in anywhere.

Vigor3900 with a dedicated VPN co-processor, the hardware encryption of AES/DES/3DES and hardware key hash of SHA-1/MD5 are seamlessly handled, thus maintaining maximum router performance. For remote sites and inter-office links, the Vigor3900 supports up to 500 simultaneous VPN tunnels (such as IPSec/PPTP/L2TP protocols).

Without the necessity of installing VPN client on individual PC, the Secure Socket Layer (SSL) virtual private network (VPN) facility lets remote workers connect to the office network at any time. SSL is supported by standard web browsers such as FireFox and IE. For users of small offices and tele-workers who need to access enterprises' internal applications, file server and file sharing.

In short, Vigor3900 gives a highly secure but flexible network for the multi-site business operation and retain corporate HQ's ultimate control of the system.

High performance gigabit and fiber interfaces

Vigor3900 with four Gigabit Ethernet-ports and one SFP active fiber port as WAN interfaces allows corporation to subscribe internet connection service from up-to five different ISPs. These five WAN interfaces can do load-balancing to facilitate bandwidth usage in the connection uptime and failover backup during downtime to prevent temporary service outage from subscribed ISP(s). In addition, Vigor3900 with two Gigabit Ethernet-ports and one SFP active fiber port as LAN interfaces facilitates large data and business applications exchange to reach corporate intranet client ends.

Vigor3900 is also the future proof procurement as considering tech refresh of your central site or major regional branches. From infrastructure viewpoint, Vigor3900 is not only working with current IPv4 network but also compliant with future IPv6 migration. From service viewpoint, corporation begins to turn to virtualization and cloud computing services when the speed of WAN connection is rising to reduce overhead of IT and enhance productivity.

Stable inline reliability

Vigor3900 offers High Availability by Common Address Redundancy Protocol (CARP) to remain reliable network for business operation even during system downturn. Network administrator can configure another Vigor3900 as the passive standby backup device in case of failure of main Vigor3900. Moreover, administrator can enable reciprocal backup functionality for multiple active Vigor3900 that includes load balancing configuration and user definable backup priorities.

The advance Load Balance and Failover features of Vigor3900 can balance traffic from your LAN to multiple internet connections (WANs). The easy-to-use web user interface allows administrator to configure comprehensive network settings in minutes to optimize bandwidth usage and establish a reliable network based on actual operation needs. Traffics from the LAN are shared out on a round robin basis across the available WANs. Vigor3900 can monitor each WAN connection, using an IP address you provide, and if Vigor3900 monitors fails, a failover configuration will take place and typically just feeds all traffic down the other connection(s). Especially, the pooling configuration concept allows administrator to select desire WAN ports as load-balancing pools with weight setting capability / failover pools and modify policy if necessary and then configure each WAN port with detail network information that helps administrator build a substantial network to facilitate daily operation with versatility, scalability and reliability.

IPv6 Ready | Multi-WAN | Giga LAN/WAN Gigabit LAN / WAN | VPN | Fiber | CSM | Bandwidth MGMT

Highly secure and efficient corporate application management

Vigor3900 with Certificate Management function including Root CA, Trusted CA and Local CA is a comprehensive Certificate Authority (CA) server. To prevent eavesdropping, Vigor3900 enforces advance encrypted mechanism implemented a pair of public and private keys as exchanging certificate between server and client instead of using pre-shared key which might be stolen by hackers during interchange. Vigor3900 offers flexible methods to grant certificate for any trusted applicant who may use it for the VPN connection. Administrator of Vigor3900 can choose to accept/sign client's CA certificate or generate a signed CA certificate through building root CA function for client's VPN connection needs in case some clients do not have CA certificate in hand. As a result, Certificate Management by Vigor3900 offers secure and flexible ways for business certification process.

The DoS/DDoS prevention and URL/Web content filter strengthen the security outside and inside the network. The enterprise-level CSM (Content Security Management) enables users to control and manage IM (Instant Messenger) and P2P (Peer-to-Peer) applications more efficiently. The CSM hence prevents inappropriate content from distracting employees and impeding productivity. Furthermore, the CSM can keep office networks threat-free and available.

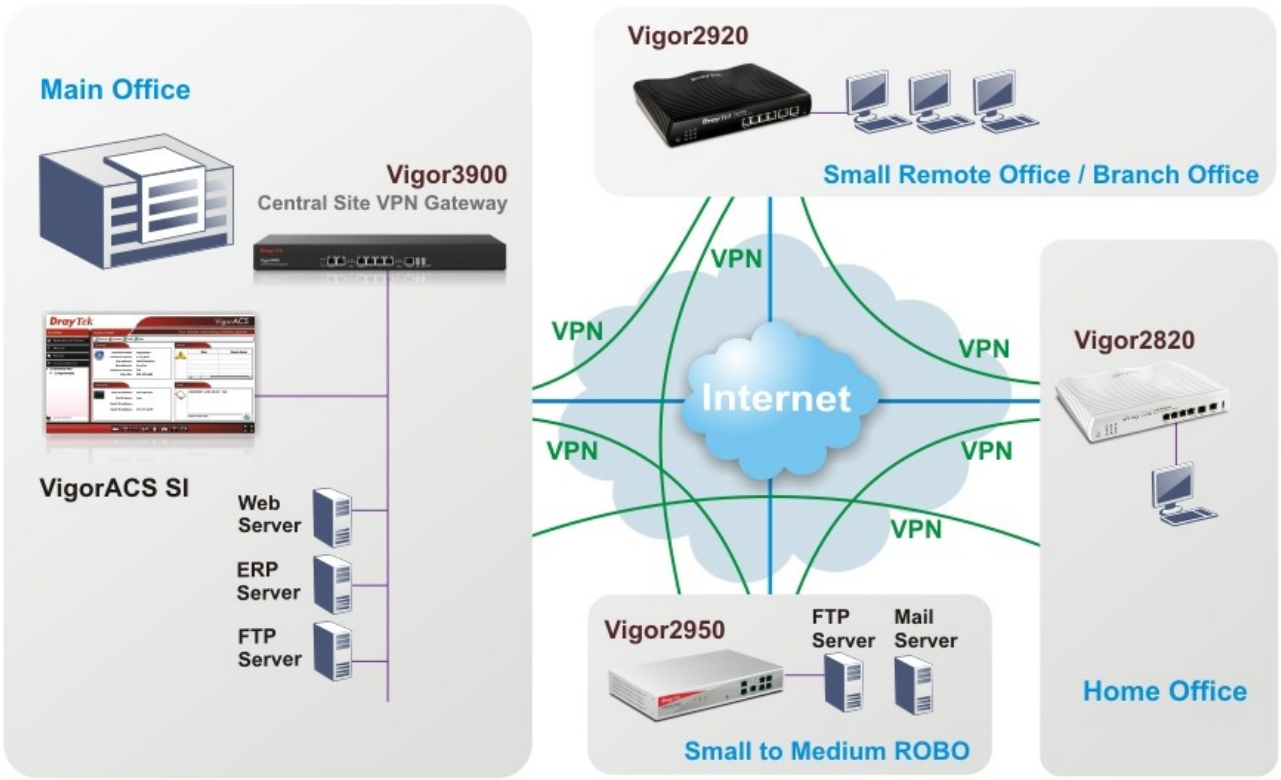
Quality of Service (QoS) function of Vigor3900 implemented Ingress and Egress Filter Rules monitoring LAN/WAN incoming and outgoing data packets. These rules can prevent unwanted data packets from outside to access corporate network as well as distribute corporate data to non-recognizable destinations. The subscribed bandwidth wouldn't be wasted on useless data packet exchange activities and may reduce the risk of damage corporate network or confidential information leakage. Moreover, Vigor3900 has eight classes of priority level settings which allow administrator to better prioritize the importance of bandwidth usage in detail. Administrator can use bandwidth limitation to grant different bandwidth to different workgroups based on their main job function which can be viewed as macro view of bandwidth allocation. In the micro view, administrator can define different sessions through session limitation to individual client device based on IP address in each workgroup. For instance, Sales Dept. in total might need the larger bandwidth than others for better serving customers. However, sales assistants could be granted minimum sessions because they don't need to interact with customers directly to facilitate their jobs.

Easy-to-use centralized management

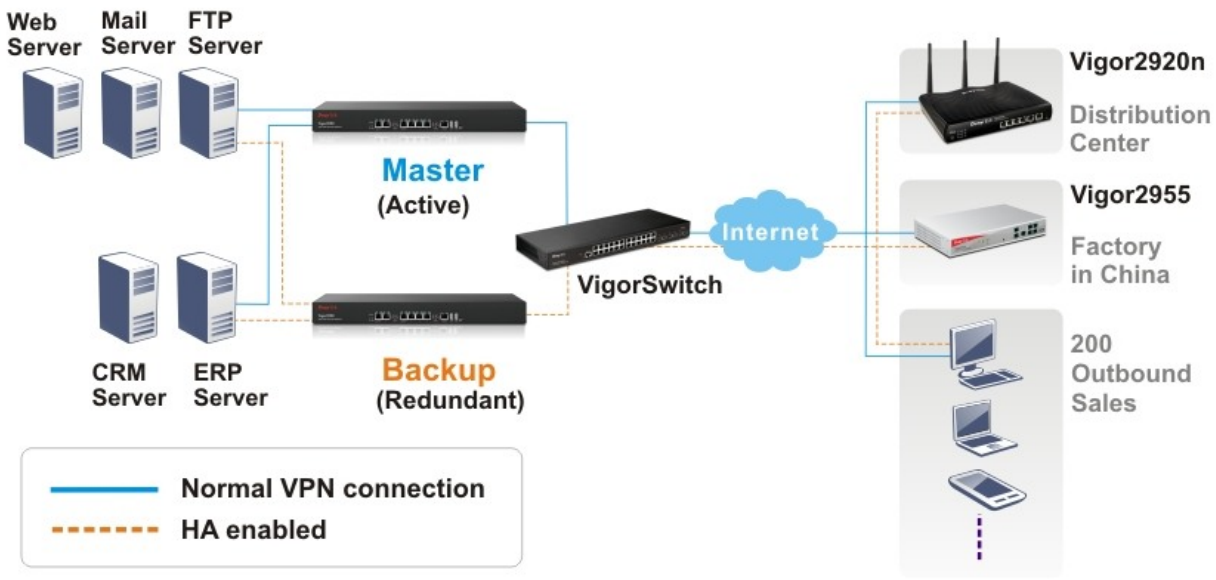
Vigor3900 embedded with an easy-to-use user interface shorten administrator's learning curve to adopt its management mechanism to control CO side network and hundreds VPN connections of remote sites. By the easy-to-use user interface, business doesn't need to allocate the highly experienced technician as the administrator and can save training cost/time for recruiting new hire. Besides, Vigor3900 compliant with TR-069 protocol can be managed by VigorACS SI centralized management system that makes you have the choice to outsource IT management to System Integrator who can provide both Internet access service (last mile license from ISP/Telco) and device remote management/diagnostic services to stay focused on business essentials.

* Firmware upgradeable

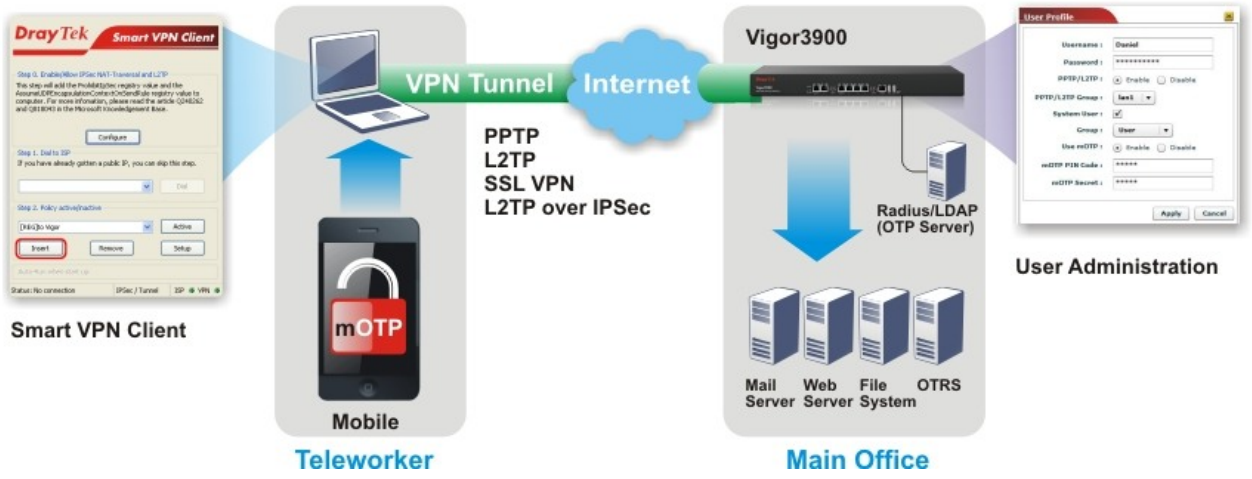
Enterprise-level central site VPN gateway



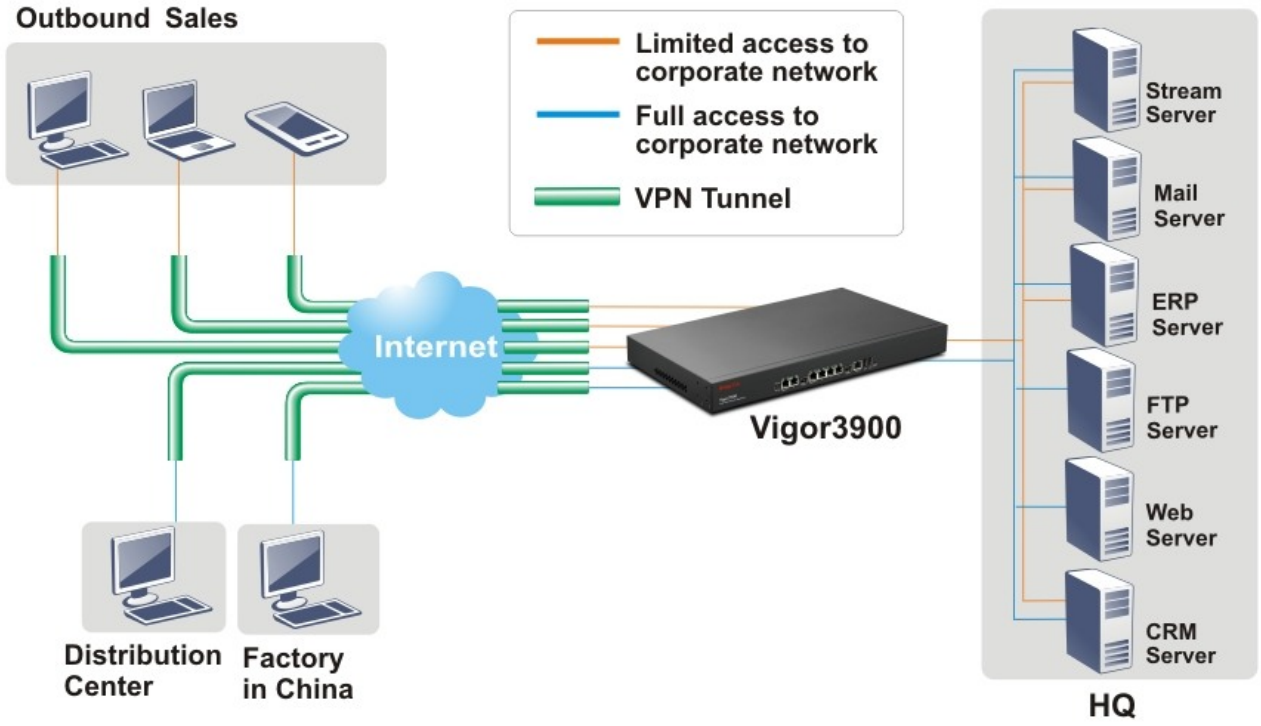
High Availability



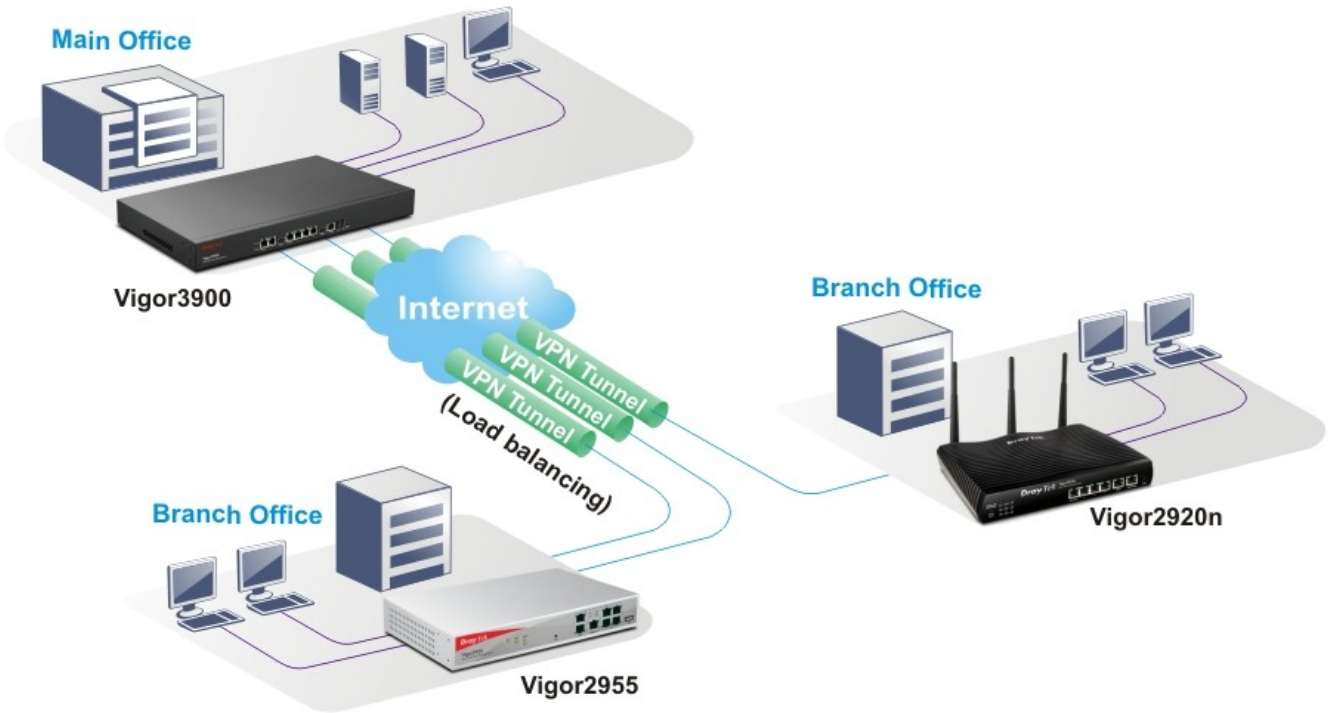
Mobile-OTP



User Management



VPN Trunking



Technical Specification

WAN Protocol

Ethernet	• PPPoE, PPTP, DHCP client, static IP, L2TP*, IPv6.

Multi WAN

Outbound policy based load balance	• Allow your local network to access Internet using multiple Internet connections with high-level of Internet connectivity availability.
	• 4 dedicated Ethernet WAN ports (10/100/1000Mbps) and 1 active fiber (SFP) slot.
	• WAN fail-over or load-balanced connectivity.
	• Redundancy.
	• By WAN interfaces traffic volume.
	• By destination IP address range.
	• By fixed VPN connection.
	• Flexible pooling rule setting.
	• Auto-detect line status.
Bandwidth on demand	• Service/IP based preference rules or auto-weight.

VPN

Prevent Replay Attack	
Protocols	• PPTP, IPSec, L2TP, L2TP over IPSec.
Up to 500 connections simultaneously	• LAN to LAN, remote access (teleworker-to-LAN), dial-in or dial-out.
VPN trunking	• VPN load-balancing and VPN backup .
VPN throughput	• 760Mbps.
NAT-traversal (NAT-T)	• VPN over routes without VPN pass-through.
PKI certificate	• Digital signature (X.509).
IKE authentication	• Pre-shared key; IKE.
Authentication	• Hardware-based MD5, SHA-1.
Encryption	• MPPE and hardware-based AES/DES/3DES.
RADIUS client	• Authentication for PPTP remote dial-in.
DHCP over IPSec*	• Because DrayTek add a virtual NIC on the PC, thus, while connecting to the server via IPSec tunnel, PC will obtain an IP address from the remote side through DHCP protocol, which is quite similar with PPTP.
GRE over IPSec	• Creating a virtual point-to-point link to various brands of routers at remote sites over an IP internetwork.
Dead Peer Detection (DPD)	• When there is traffic between the peers, it is not necessary for one peer to send a keep-alive to check for liveness of the peer because the IPSec traffic serves as implicit proof of the availability of the peer.
Smart VPN software utility	• Provided free of charge for teleworker convenience (Windows environment).
Easy of adoption	• No additional client or remote site licensing required.
Industrial-standard interoperability	• Compatible with other leading 3rd party vendor VPN devices.

SSL VPN

	• Allow users to use a web browser for secure remote user login tunnel mode, application mode, proxy mode
	• Support 200 SSL tunnels*

Content filter

IM/P2P blocking	• Java applet, cookies, active X, compressed, executable, multimedia file blocking.
Web content filter	• Dynamic URL filtering database.
Time schedule control*	• Set rule according to your specific office hours.

Firewall

Stateful Packet Inspection (SPI)	• Outgoing/Incoming traffic inspection based on connection information.
Multi-NAT	• You have been allocated multiple public IP address by your ISP. You hence can have a one-to-one relationship between a public IP address and an internal/private IP address. This means that you have the protection of NAT (see earlier) but the PC can be addressed directly from the outside world by its aliased public IP address, but still by only opening specific ports to it (for example TCP port 80 for an http/web server).
Port redirection	• The packet is forwarded to a specific local PC if the port number matches with the defined port number. You can also translate the external port to another port locally.
DMZ host	• This opens up a single PC completely. All incoming packets will be forwarded onto the PC with the local IP address you set. The only exceptions are packets received in response to outgoing requests from other local PCs or incoming packets which match rules in the other two methods.
Policy-based IP packet filter	• The header information of an IP packet (IP or Mac source/destination addresses; source /destination ports; DiffServ attribute; direction dependent, bandwidth dependent, remote-site dependent.
DoS/DDoS prevention	• Act of preventing customers, users, clients or other computers from accessing data on a computer.
IP address anti-spoofing	• Source IP address check on all interfaces only IP addresses classified within the defined IP networks are allowed.
Notification	• E-mail alert* and logging via syslog.
Bind IP to MAC address	• Flexible DHCP with 'IP-MAC binding'.

System management

Web-based user interface (HTTP)	• Integrated web server for the configuration of routers via Internet browsers with HTTP.
Quick start wizard	• Let administrator adjust time zone and promptly set up the Internet (PPPoE, PPTP, Static IP, DHCP).
User management	• Dial-in access management (PPTP/L2TP and mOTP) .
CLI(Command Line Interface, Telnet/SSH)	• Remotely administer computers via the telnet.
DHCP client/relay/server	• Provides an easy-to configure function for your local IP network.
Dynamic DNS	• When you connect to your ISP, by broadband or ISDN you are normally allocated an dynamic IP address. i.e. the public IP address your router is allocated changes each time you connect to the ISP. If you want to run a local server, remote users cannot predict your current IP address to find you.
Administration access control	• The password can be applied to authentication of administrators.
Configuration backup/restore	• If the hardware breaks down, you can recover the failed system within an acceptable time. Through TFTP, the effective way is to backup and restore configuration between remote hosts.
Built-in diagnostic function	• Dial-out trigger, routing table, ARP cache table, DHCP table, NAT sessions table, data flow monitor, traffic graph, ping diagnosis, trace route.
NTP client/call scheduling	• The Vigor has a real time clock which can update itself from your browser manually or more conveniently automatically from an Internet time server (NTP). This enables you to schedule the router to dial-out to the Internet at a preset time, or restrict Internet access to certain hours. A schedule can also be applied to LAN-to-LAN profiles (VPN or direct dial) or some of the content filtering options.
Tag-based VLAN (802.1Q)	• By means of using a VLAN ID, a tag-based VLAN can identify VLAN group membership. The VLAN ID provides the information required to process the traffic across a network. Furthermore, the VLAN ID associates traffic with a specific VLAN group.
Firmware upgrade via TFTP/ HTTP	• Using the TFTP server and the firmware upgrade utility software, you may easily upgrade to the latest firmware whenever enhanced features are added.
Remote maintenance	• With Telnet/SSL, SSH (with password or public key), browser (HTTP/HTTPS), TFTP or SNMP, firmware upgrade via HTTP or TFTP.
Logging via syslog	• Syslog is a method of logging router activity.
SNMP management	• SNMP management via SNMP v1/v2, MIB II.
VigorACS SI Centralized Management	• TR-069 based.

Certificate management

Advance encrypted method	• A pair of public/priviate key for encryption/decryption.
Comprehensive Certificate Authentication	• Trusted CA / Local Certificate / CA server.

Bandwidth management

Traffic shaping	• Dynamic bandwidth management with IP traffic shaping.
Bandwidth reservation	• Reserve minimum and maximum bandwidths by connection based or total data through send/ receive directions.
DiffServ codepoint classifying	• Priority queuing of packets based on DiffServ.
Individual IP bandwidth/session limitation	• Define session /bandwidth limitation based on IP address.
User-defined class-based rules	• More flexibility.
QoS	• Ingress/Egress Filter Rules monitor both LAN/WAN packets / 8 priority level setting.

Routing functions

Router	• IP and NetBIOS/IP-multi-protocol router.
Advanced routing and forwarding	• Complete independent management and configuration of IP networks in the device, i.e. individual settings for DHCP, DNS, firewall, VLAN, routing, QoS etc.
DNS	• DNS cache/proxy.
DHCP	• DHCP client/relay/server.
NTP	• NTP client, automatic adjustment for daylight-saving time.
Dynamic routing	• It is with routing protocol of RIP v2. Learning and propagating routes.
Static routing	• An instruction to re-route particular traffic through to another local gateway, instead of sending it onto the Internet with the rest of the traffic. A static route is just like a 'diversion sign' on a road.

High availability

CARP	• Common address redundancy protocol. • Enhanced security with encrypted packet.

Hardware

LAN	• 2 x 10/100/1000M Base-TX LAN switch, RJ-45 1 x active fiber (SFP) slot
WAN	• 4 x 10/100/1000M Base-TX WAN switch, RJ-45 1 x active fiber (SFP) slot
Console	• 1 x console, RJ-45
Reset	• 1 x factory reset button
USB	• 2 x USB host 2.0

Support

Warranty	• 2-year limited warranty, technical support through e-mail and Internet FAQ/application notes.
Firmware upgrade	• Free firmware upgrade from Internet.

Declaration of conformity

CE FC

* Firmware upgradeable

www.draytek.com E-mail:info@draytek.com Tel:+886 3 597 2727 Fax:+886 3 597 2121