Vigor3300V+

Multi-WAN Security Router

DrayTek

www.draytek.com

- *4 WAN/DMZ ports for Internet/LAN facing configuration providing greater total bandwidth capacity or fault-tolerance*
- *Intelligent Multi-WAN utilization for load-balancing and failover backup*
- *Ethernet port based VLANs for data security or efficient file sharing*
- *Integration of FXO/FXS/ISDN interface module for various telephony needs*
- *Quality of Service (QoS) for prioritizing bandwidth for essential applications*
- *CSM (Content Security Management) for keeping confidential and essential data from modification or theft*
- *High performance VPN server – up to 200 simultaneous VPN sesssions*
- *EMS central management and user-friendly WUI for easing admin tasks*

The Vigor3300V+ series serve as multi WAN solutions and professional VPN gateway to take care of SMB's HQ and remote sites at the same time.

For HQ / Main office:

With four WAN/DMZ ports which can be configured as either an Internet-facing WAN interface or as a LAN-facing physical DMZ, the combination of WAN interface ports can let you use multiple Internet connections to provide greater total bandwidth capacity or fault-tolerance.

For remote sites:

Employees in remote sites would need to have VPN connection with their HQ to execute their daily job. Most single teleworkers can use the VPN capabilities embedded inside iPhone/PC/notebook. The branch offices/small offices can make use of other Vigor routers (or other brand VPN) for the VPN termination.

Utilization of Multiple WAN

VLAN & Multiple LAN subnets

The Vigor3300V+ provides Ethernet port based VLANs, where each of the four LAN (RJ45/Ethernet) ports can be defined into distinct or common groups-i.e. isolated or joined to each other. That would provide SMB the flexibility to either secure corporate confidential data or escalate information sharing between teams/Depts. Moreover, the Vigor3300V+ supports up to four independent LAN-side private IP subnets, with the Vigor providing each with its own DHCP server.

Load balancing

Vigor3300V+ distributes WAN traffic requests evenly in basic load-balancing mode. Two LAN users can download at 256Kb/s simultaneously if you have two 256Kb/s feeds. You can select traffic preferences for the load balancing, selecting specific Internet feeds for choosing types of traffic (e.g. VPN, VoIP), by source/destination IP address or UDP/TCP port ranges.

Backup

Vigor3300V+ can intelligently switch to secondary/backup Internet feed to remain SMB's productivity once the primary Internet feed drops. Those WAN ports of Vigor3300V+ can also be configured to back up the primary Internet feed and only activate while the primary Internet feed drops. The backup WAN port will go idle again once the primary Internet feed is restored.

Integration of FXO/FXS/ISDN interface module

The Vigor3300V+ is equipped with rich-featured supplementary call-handling facilities which facilitates you to make and receive VoIP calls as well as transfer calls around the office. You can select different interface modules dependant upon your communication needs.

FXO interface module:

If you have an FXO interface module, you can also access your analogue lines or connect to PSTN PBX.

ISDN interface module:

You will be able to integrate the ISDN MSN (multiple subscriber numbering) with SIP calls if you install ISDN

The Vigor3300V+ hence converges the PSTN, ISDN, Voice-over-IP, and robust firewall to leverage your existing networking infrastructure.

Prioritize your bandwidth for versatile applications

Bandwidth Management & QoS

The administrators can set Quality of Service (QoS) preferences to utilize bandwidth efficiently for essential applications.

Multi-WAN Firewall VPN VoIP ISDN

For example, the Vigor3300V+ grants highest priority to Voice-over-IP (VoIP) telephony so that VoIP calls can be made with crystal-clear quality. In contrast, administrators set a maximum percentage of your bandwidth for P2P (e.g. movie downloading) or FTP downloads for remaining your valuable bandwidth.

Security without compromise

The enterprise-level CSM (Content Security Management) embedded in Vigor3300V+ 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. With CSM, you can protect confidential and essential data from modification or theft.

Besides, Vigor3300V+ series feature high-security firewall options with both IP-layer and content based protection. The DoS/DDoS prevention and URL/Web content filter strengthen the security outside and inside the network.

More extendability

The Vigor3300V+ can establish VPN tunnels across the public Internet. The tunnels can be to remote networks, or from a single dial-in teleworker, needing to access your headquarters' LAN where DrayTek Vigor3300V+ is installed.

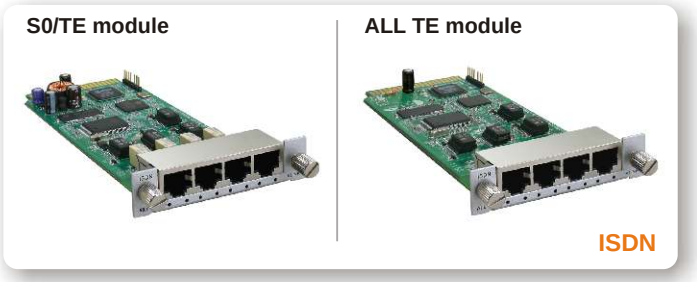
With a dedicated VPN co-processor, the hardware encryption of AES/DES/3DES and hardware key hash of SHA-1/MD5 are seamlessly handled, thus maintaining maximum router performance. For remote tele-workers and inter-office links, the Vigor3300V+ supports up to 200 simultaneous VPN tunnels (such as IPSec/PPTP/L2TP protocols).

High user-friendliness and efficiency

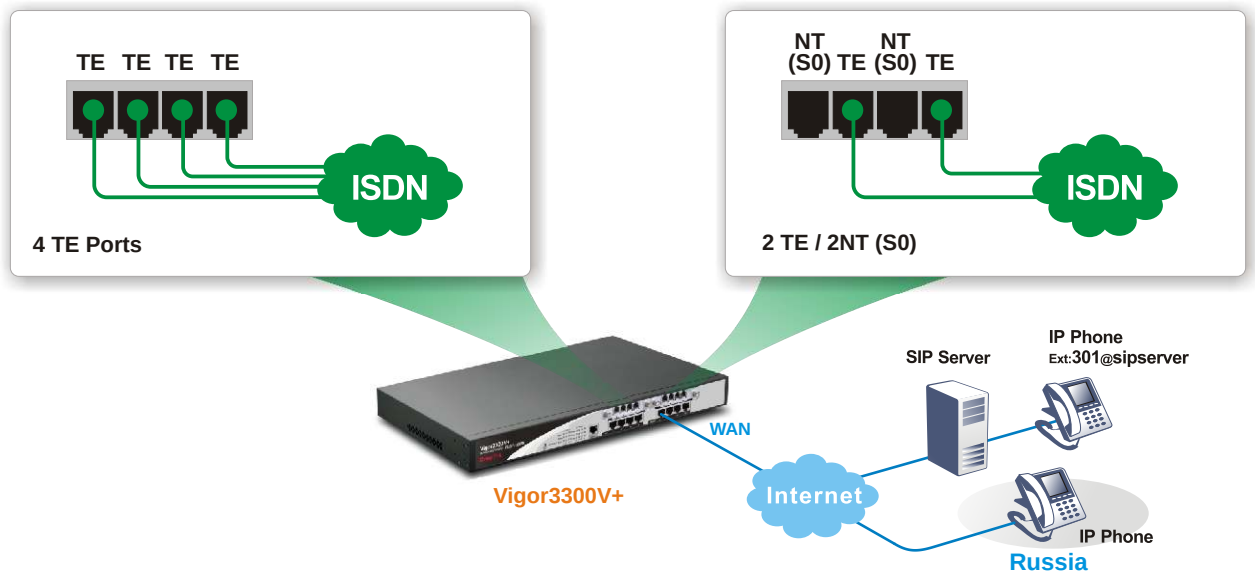
Its well-structured Web User Interface offers user-friendly configuration and make the net-admin job become an easy task. For instance, the WUI provides IP layer QoS (Quality of Service), NAT session/bandwidth management to help users control and allocate the bandwidth on networks.

More benefits

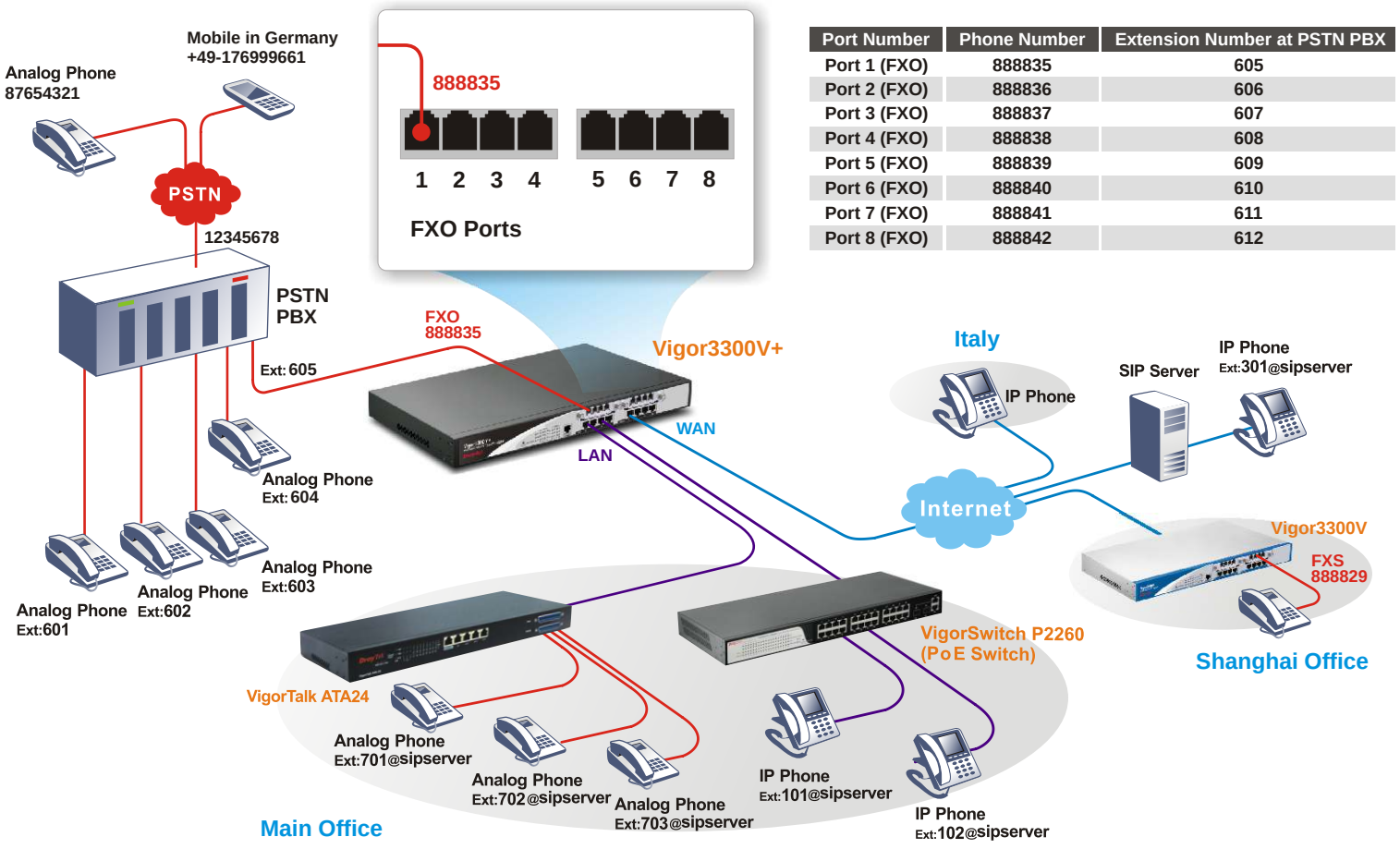
The platform of Vigor3300V+ is able to let you choose 4-port ISDN BRI card (4 ISDN TE or 2 TE/2 NT interface card) in terms of your voice environment. The ISDN phone can connect to NT -interface of 2 TE/2 NT interface card. The ISDN line can be connected to TE-interface. If you have ISDN PBX, you can connect one of internal extension to TE-interface of 4-port ISDN TE card. The call routing of Vigor3300V+ will enable ISDN MSN mapping to IP extensions for forming compound extensions.



Off-Net via ISDN Network

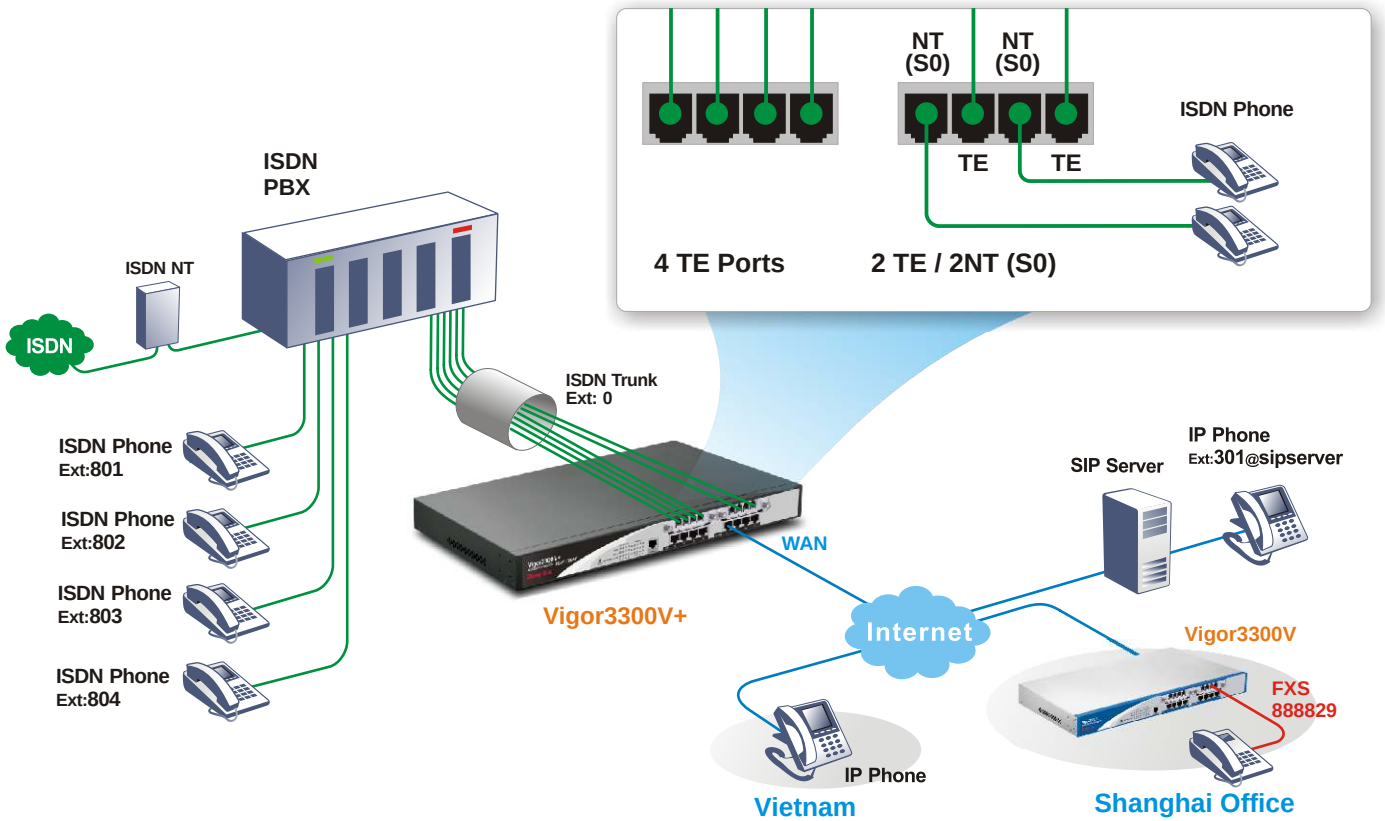


On/Off Net



Port Number	Phone Number	Extension Number at PSTN PBX
Port 1 (FXO)	888835	605
Port 2 (FXO)	888836	606
Port 3 (FXO)	888837	607
Port 4 (FXO)	888838	608
Port 5 (FXO)	888839	609
Port 6 (FXO)	888840	610
Port 7 (FXO)	888841	611
Port 8 (FXO)	888842	612

ISDN



Technical Specification

VoIP

- Protocol:SIPv2(RFC3261), MGCP, RTP / RTCP
- Multiple SIP proxies registrars
- Jitter buffer (125ms)
- G.168 line echo-cancellation
- Automatic gain control
- Packet loss concealment
- Outbound proxy
- FXO-PIN code
- NAT traversal (STUN, RFC 3489)
- Voice codec:
  G.711 A/u laws, G.723.1, G.726, G.729 A/B, VAD/CNG
- Tone generation and detection:
  DTMF, dial, busy, ring back, call progress
- DTMF Tone :
  Out band (RFC-2833), SIP Info
- FAX/Modem support :
  - Tone detection
  - G.711 pass-through
  - T.38 FAX relay, T.30 transparent
  - Modem support rate up V.92. (G.711 only)
- Supplemental services :
  - Internal call
  - Call hold/retrieve
  - Call waiting
  - Call waiting with caller ID
  - Call transfer
  - Call forwarding (always, busy, answer)
  - Call barring (incoming / outgoing)
  - DND (do not disturb)
  - Hotline
  - Incoming call barring
  - FXS incoming/outgoing preset number
  - Feature phone*
- Dial plan :
  - Phone book
  - Digit map
  - Call barring
  - Regional
- Caller ID support: bellcore, ETSI, NTT, DTMF-based(nor-europe)

*Future release

ISDN Features

- ISDN Failover (Loop through) [available on 2 TE/NT (S0) interface module].
- ISDN On-Net/Off-Net
- 10MSN (Multiple Subscriber Numbers) on each ISDN S0 port for VoIP call.
- Signaling compliance: ITU-T Rec. Q. 920, Q921, Q930, Q931.

WAN Protocol

Ethernet	• PPPoE, PPTP, DHCP client, static IP, L2TP, BPA
ISDN	• DSS1 (Euro ISDN), PPP, ML-PPP(64/128Kbps)

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 (10/100Mb/s).
	• WAN fail-over or load-balanced connectivity.
	• Redundancy
	• By PC clients
	• By WAN interfaces traffic volume
	• By destination IP address range
	• By fixed VPN connection
	• By fixed VoIP packets
	• Robust detection mechanism
	• IP aliasing
	• Auto-detect line status
Bandwidth on demand	• Service/IP based preference rules or auto-weight.

VPN

PFS (DH Group)	
Prevent Replay Attack	
Protocols	• PPTP, IPSec, L2TP, L2TP over IPSec
Up to 200 sessions simultaneously	• LAN to LAN, remote access (teleworker-to-LAN), dial-in or dial-out.
VPN trunking	• VPN load-balancing and VPN backup .
VPN throughput	• 50Mbps
NAT-traversal (NAT-T)	• VPN over routes without VPN pass-through.
PKI certificate	• Digital signature (X.509)
IKE authentication	• Pre-shared key; IKE phase 1 agressive/standard modes & phase 2 selectable lifetimes.
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.
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.

Content filter

URL keyword blocking	• Whitelist and Blacklist. • 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.
Open ports	• As port redirection (above) but allows you to define a range of ports.
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. The precedence is as follows : Port Redirection > Open Ports > DMZ
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.
Object-based firewall	• Utilizes object-oriented approach to firewall policy.
notification	• E-mail alert and logging via syslog.
Bind IP to MAC address	• Flexible DHCP with 'IP-MAC binding'.
WDS security	• The use of authentication and encryption techniques on a Wireless Distribution System (WDS) link between compatible access points.

System management

Web-based user interface (HTTP/HTTPS)	• Integrated web server for the configuration of routers via Internet browsers with HTTP or HTTPS.
DrayTek's quick start wizard	• Let administrator adjust time zone and promptly set up the Internet (PPPoE, PPTP, Static IP, DHCP).
User administration	• RADIUS user administration for dial-in access (PPP/PPTP and ISDN CLIP).
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, wireless VLAN online station 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/FTP	• Using the TFTP server and the firmware upgrade utility software, you may easily upgrade to the latest firmware whenever enhanced features are added.
ISDN remote maintenance	• The system manager can remotely manage the routers through an ISDN remote dial-in with secure call back mechanism.
Remote maintenance	• With Telnet/SSL, SSH (with password or public key), browser (HTTP/HTTPS), TFTP or SNMP, firmware upgrade via HTTP/HTTPS or TFTP.
Wake On LAN	• A PC on LAN can be woken up from an idle/standby state by the router it connects when it receives a special 'wake up' packet on its Ethernet interface.
Logging via syslog	• Syslog is a method of logging router activity.
SNMP management	• SNMP management via SNMP v2, MIB II
Future release	• Configuration file encryption* • Attack alter by email* • SNMP agent : firewall, VPN, alarm*

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.
Packet size control	• Specify size of data packet.
DiffServ codepoint classifying	• Priority queuing of packets based on DiffServ.
4 priority levels(inbound/outbound)	• Prioritization in terms of Internet usage.
Individual IP bandwidth/session limitation	• Define session /bandwidth limitation based on IP address.
Bandwidth borrowing	• Transmission rates control of data services through packet scheduler.
User-defined class-based rules	• More flexibility.

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.
Policy-based routing	• Based on firewall rules, certain data types are marked for specific routing, e.g. to particular remote sites or lines.
Dynamic routing	• It is with routing protocol of RIP v2. Learning and propagating routes; separate settings for WAN and LAN.
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.

Working with VigorCSM central management

- Basic configuration
- Performance monitoring
- Topology
- Security
- Log
- Alarm
- Polling
- VPN/firewall configuration
- VoIP configuration
- Alarm for VPN/firewall

High availability

- VRRP (RFC 2338)

Hardware

LAN	• 4 x 10/100M Base-TX LAN switch, RJ-45
WAN	• 4 x 10/100M Base-TX WAN/DMZ switch, RJ-45
Console	• 1 x console, RJ-45
Reset	• 1 x factory reset button
VoIP	• 2 x slots for FXS/FXO/ISDN S0,TE/ISDN all TE

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

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