Connectivity

Ethernet WAN
- IPv4 - DHCP Client, Static IP, PPPoE, PPTP, L2TP, 802.1q Multi-VLAN Tagging
- IPv6 - Tunnel Mode: TSPC, AICCU, 6rd, Static 6in4 Dual Stack: PPP, DHCPv6 Client, Static IPv6
- WAN Connection Fail-over
- WAN Budgets
- Load Balance/Route Policy

Ethernet LAN
- IPv4/IPv6 DHCP Server
- Static Routing/RIP
- Multiple Subnet
- Port/Tag-based VLAN

USB
- 3.5G/4G LTE(PPP, DHCP) as WAN5/WAN6
  Printer Server/File Sharing

Management

System Maintenance
- HTTP/HTTPS with 2-level Management (Admin/User)
- Logging via Syslog
- SNMP Management MIB-II (v2/v3)
- CLI (Command Line Interface, Telnet/SSH)
- Administration Access Control
- Web-based Diagnostic Functionality
- Firmware Upgrade via TFTP/FTP/HTTP/TR-069
- CWMP Support (TR-069/TR-104)
- LAN Port Monitoring

Network Management
- Bandwidth Management by session/bandwidth
- User Management by Time/Data Quota
- LAND DNS and DNS Proxy/Cache
- Dynamic DNS
- IGMP Snooping/Proxy v2 and v3
- QoS (DSCP/Class-based/4-level priority)
- Guarantee Bandwidth for VoIP
- Support Smart Monitor (Up to 200 nodes)
- Central AP Management
- Central VPN Management
- Switch Management

WLAN (n model)

- 802.11n with 2.4GHz
- Multiple SSID
- Encryption (64/128-bit WEP,WPA/WPA2,802.1x)
- Hidden SSID
- Wireless Rate Control by SSID
- Wireless VLAN
- Wireless LAN Isolation
- MAC Address Access Control
- Access Point Discovery
- Wireless Client List
- WDS (Wireless Distribution System)
- WMM (Wi-Fi Multimedia)

Security

- Multi-NAT, DMZ Host, Port-redirection and Open Port
- Object-based Firewall, Object IPv6, Group IPv6
- MAC Address Filter
- SPI (Stateful Packet Inspection) (Flow Track)
- DoS/DDoS Prevention
- IP Address Anti-spoofing
- E-mail Alert and Logging via Syslog
- Bind IP to MAC Address
- Time Schedule Control
- Content Security (IM/P2P, URL, Keywords, Cookies,...)

VPN

- Up to 100 VPN Tunnels
- Protocol : PPTP, IPsec, L2TP, L2TP over IPsec
- Encryption : MPPE and Hardware-based AES/DES/3DES
- Authentication : MD5, SHA-1
- IKE Authentication : Pre-shared Key and Digital Signature (X.509)
- LAN-to-LAN, Teleworker-to-LAN
- DHCP over IPsec
- IPsec NAT-traversal (NAT-T)
- Dead Peer Detection (DPD)
- VPN Pass-through
- VPN Wizard
- mOTP
- Supports 50 SSL VPN Tunnels
- VPN Trunk: VPN Backup and Load Balance

Hardware Interface

- 4 x 10/100/1000Base-Tx WAN Port, RJ-45
- 1 x 10/100/1000Base-Tx LAN Switch, RJ-45
- 1 x 10/100/1000Base-Tx DMZ Port, RJ-45
- 2 x USB Host (USB1 is 2.0 and USB2 is 3.0)
- 2 x Detachable Antennas (n Model)
- 1 x Wireless On/ Off/ WPS Button (n Model)
- 1 x Console Port, RJ-45
- 1 x Factory Reset Button

	WLAN
Vigor3220n	●
Vigor3220	

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

991-3220000-00

DrayTek

working with ACS SI Utility

Vigor3220 Series

Multi-WAN Security Router

- Four Gigabit WAN and Two USB WANs (One USB WAN is 3.0)
- WAN Load Balancing and Failover
- VPN Load Balancing and VPN Backup
- Concurrent 100 VPN tunnels and 50 SSL VPN tunnels
- Central AP Management
- Central VPN Management
- Working with TR-069 VigorACS SI Central Management

Features of the Vigor3220 series Multi-Subnet security routers will satisfy the network requirements of small to medium business networks. Its Multi-Subnet interface with Multi-VLAN function allows users to easily divide network into different sections based on applications, such as VoIP, web or FTP server or user groups, such as Sales, Technical Support or HR dept. Each usage/ application or user group can get its dedicated bandwidth and administrator can have security control between user groups for preventing possible data leakage. The said series are equipped with four Gigabit Ethernet WAN ports, one gigabit Ethernet LAN port, one DMZ port, two USB ports, one console port and IEEE802.11n WLAN on n model. The console port allows a dedicated computer to be used for configuring the router. The Vigor3220 and Vigor3220n are designed for small offices using multi super-fast broadband for better business continuity and productivity.

Multi-WAN with Bandwidth Management
All these 4 x Gbps WAN ports support current xDSL/ Cable/ Satellite broadband and the USB ports also allow connection to the 3.5G/4G LTE Mobile Broadband. The WAN ports can be configured to increase data throughput, backup each other (Failover mode), or share the traffic (Load Balance). If you have your own Web server, FTP server and mail server, the 4 WAN ports will provide additional bandwidth for customers. In addition, the 1 x Gbps LAN port switch compatible with PoE switch (e.g. VigorSwitch P2261) and Gigabit switch (e.g. VigorSwitch G2260) can support large data transfer and connect to multiple client devices (PC/ servers) in small to medium LAN networks.

Vigor3220 series embedded with tag-based multi-subnet function can maximize the investment of your obtained bandwidth. For example, you can allocate your 100Mbps broadband connection(s) to timing critical applications such as VoIP, web or FTP severs and business essential departments such as Sales and Technical Support team. Your additional low monthly fee DSL or cable line can be used by mail server or HR team which don't need fast data/voice packet transmission for daily operation. SMB can get highly cost-effective and secure network as adopting Vigor3220 series.

USB Ports for 4G/LTE or FTP/Printer Server
The capability of the USB ports (One is USB 2.0, the other is USB 3.0) to connect to 4G/LTE mobile broadband means that the router can be used in anywhere with 3.5G/4G coverage, such as moving vehicles, temporary events, offices where xDSL or Cable are not available, etc.

Apart from supporting printer servers, the USB ports also allow the connection of a USB disk or hard drive for FTP file transfer through the Internet or local networks. The network administrator can set username /password and directory/file access privilege for individual users.

DMZ Port for providing servers with extra protection
The DMZ port of Vigor3220 series can provide additional layer protection to servers, such as Web server, which need to expose resources from untrusted network: e.g. Internet but also have uncompromising internal LAN security requirements.

Through the user-friendly WUI of Vigor3220 series, admin can activate DMZ by NAT or Physical mode to the chosen server. That would makes external attacks only have access to the external-facing equipment in the DMZ, not entire LAN to insert extra layer of protection to SMB's internal network.

Combination of VLAN, Tagging and QoS
With all this connectivity, your LAN and WAN increases in complexity, but the comprehensive VLAN and QoS enables your efficient utilization of your bandwidth on your LAN and WAN side. The 802.1q VLAN is supported on both the LAN and WAN ports. By applying 802.1q VLAN tagging, the marked packets will be transmitted together and split further along in your network topology, as required, or merely dropped/ ignored if they fall outside a device's VLAN settings. The Quality of Service (QoS) allows you to give specific traffic types or clients different levels of priority when it comes to transmitting data so that the most appropriate amount of total bandwidth is reserved for the most important data. The VLAN groups and QoS (802.1p & TOS/DSCP Methods) can be combined with QoS rules for transmission to the Internet. After you set up VLAN groups for your office network, you can define firewall rules together with VLAN groups to let remote VPN links to only access the specific LAN ports. The Vigor3220 series are with four LAN subnets which are very useful for multi-tenanted applications or where there is necessity of department segmentation. The VLAN setup can be applied to the four LAN subnets for isolated connection. For example, you are running a public web server on your network. The VLAN segmentation with different subnets will give a fully isolated connection to the said public web server.

Firewall and Security
The Vigor3220 series offer you robust 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. 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.

The "User Management" implemented on your router firmware can allow you to prevent any computer from accessing your Internet connection without a username or password. You can also allocate time budgets to your employees within office network.

Comprehensive VPNS
Simultaneous hardware based VPN tunnels are supported providing a throughput up to 40Mbps. Each of these can be configured to use any of the common VPN protocols: PPTP, IPsec, L2TP, L2TP over IPsec, etc., and with any of the most up-to-date encryption (MPPE, AES/DES/3DES), Authentication (MD5, SHA-1), Pre-shared Key, Digital Signature (X.509). These tunnels can be used for LAN-to-LAN or remote dial-in.

The Vigor3220 series support concurrent VPN tunnels for LAN-to-LAN and remote access. There are concurrent tunnels of SSL Web Proxy and SSL Applications on Vigor3220 series for teleworkers. Along with multiple WAN ports, the VPN trunking (VPN load-balancing and VPN backup) are available on Vigor3220 series. The Central VPN Management let main site set up VPN with remote routers.

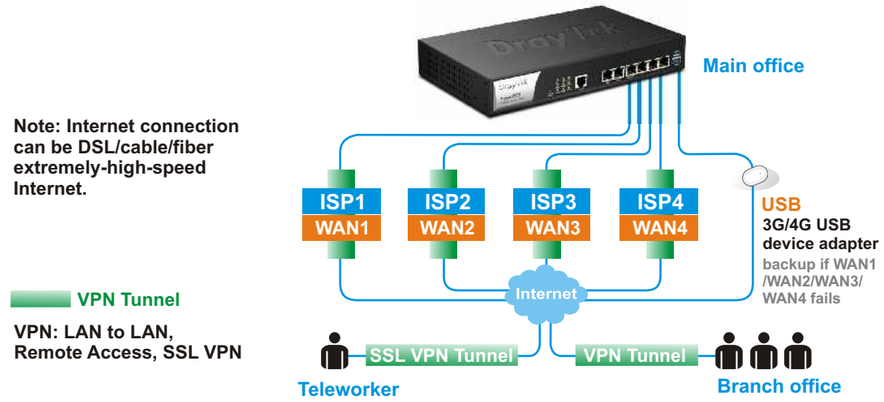
Working with Smart Monitor Traffic Analyzer and VigorACS SI Central Management
Vigor3220 supports 200-Node. DrayTek Smart Monitor Traffic Analyzer which enables you to analyze in great depth your Internet traffic, as a professional aid to improving efficiency and detecting potential problems.

For IT managed service providers, the self-host/cloud-host TR-069 VigorACS SI can facilitate deployment and management of Vigor3220 series. The multi-nation companies can also deploy Vigor routers for remote offices via the rich-featured VigorACS SI central management.

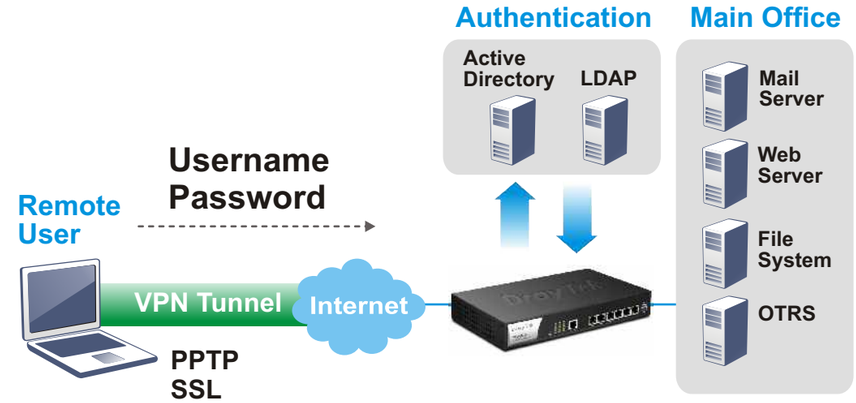
Easy Network Management
Configuring Vigor3220 router is easy with the web based configuration pages, plus the CLI/Telnet/SSH methods. Tools allowing network administrators to manage and maintain the networks with ease include:
- Diagnostic Tables that show network connection status
- SNMP for network traffic monitoring
- Two levels of Access Control to prevent unauthorized access to the router
- TR-069 for service providers to manage user devices remotely

Active Directory / LDAP for Authentication
DrayTek makes authentication for VPN Remote Access with ease by Vigor3220 Series.
Network administrator doesn't have to create new Remote Dial-in User Profiles for authentication mechanism but applies existed user accounts saved in the external server (e.g. Active Directory/LDAP). This enhancement significantly saves the time of IT Dept while establishing the secure remote access network for tele-workers.

Advance Business Network (Multi-WAN / SSL VPN)



Active Directory/LDAP Group Management for VPN remote dial-in authentication



Central AP Management

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