



Functionality of the Viprinet Multichannel VPN Router™

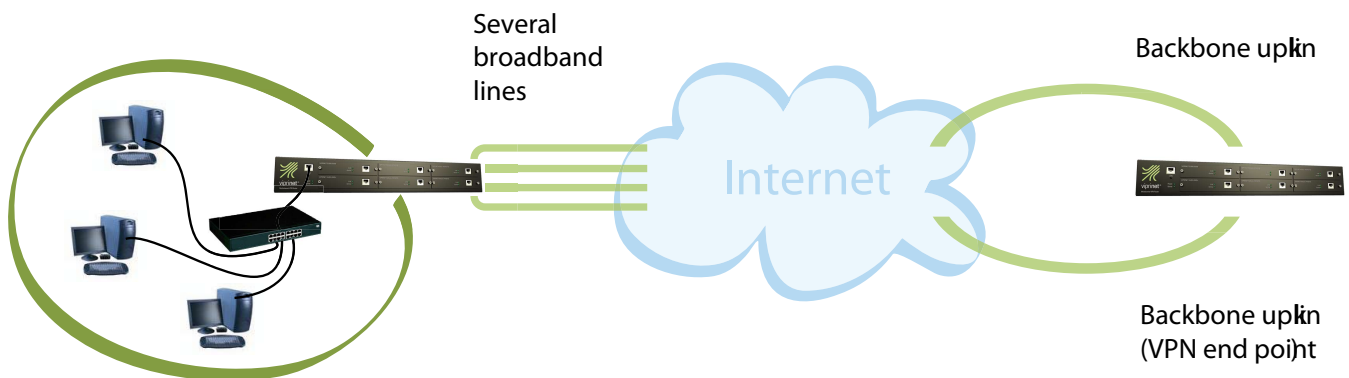
1. Basic functionality and networking infrastructure	2
2. The device	4
3. The peer (VPN concentrator)	5
4. VPN Clients / Road Warriors	6
5. IP routing	7
6. The VPN technology	9
7. Administration, management and monitoring	11
8. Excellent support	12

1. Basic functionality and networking infrastructure

The Multichannel VPN Router connects a local network with a VPN peer using up to six broadband lines. Modems that can be plugged into the router's slots are available as modules for the most common line types. Currently available are modules for ADSL, ADSL2+, Euro-ISDN and Fast Ethernet. External modems (e.g. WLAN, SDSL, SHDSL) can be connected using the Fast Ethernet module. All modems using PPPOE or assigning an IP address to the Ethernet module side via DHCP are supported.

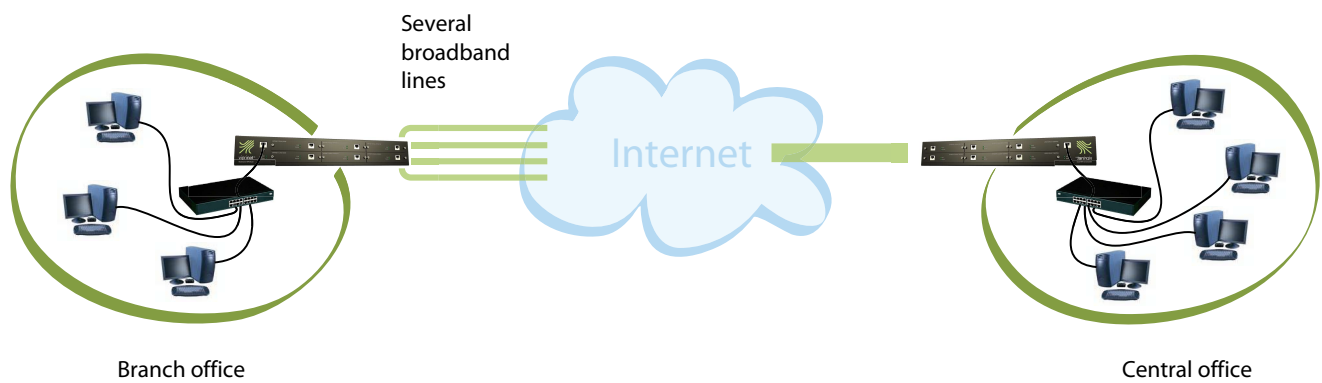
The Multichannel VPN Router acts as a layer 3 router which means it negotiates between different networks on the IP layer. Incoming IP streams are accepted on the LAN interface and distributed across all available lines/modem cards. A Viprinet peer is always required to reassemble those streams after transferring them.

A separate encrypted VPN tunnel (using SSL technology with selectable encryption level) to a configured peer is set up for each physical line. These encrypted tunnels are used for bundled data transfer.



From this it follows that the peer used should be well reachable from all physical line providers. We recommend setting this peer up in a data center directly connected to a backbone provider or directly at an ISP exchange point. Alternatively you can operate the peer in a "branch office networking" use case, provided that the branch office is equipped with a reliable broadband Internet connection.

If this is not the case or the central office is to be connected with a Viprinet bundled line as well, a star topology where the peer for all offices is located in a data center should be used.



2. The device

The Multichannel VPN Router is a high-performance, modular device. The system is enclosed in a 19", 1.5 height units case. It can be used as a desktop device, but the supplied mounting brackets also make it a breeze to mount the device in a 19" rack.

Internally the router uses a 1GHz CPU capable of encrypting data in hardware. The standard configuration comes with 256MB RAM, most of which is used for caching channel bundling packets.

Robustness and durability were the primary design concerns. The system does not contain any moving parts and is 100% passively cooled. All components have been designed to achieve maximum efficiency, lowering the typical power consumption with all modem slots filled to just 40 Watts. The device uses a robust internal power adapter (1) which (is connected to a socket using a regular power cord and) supports 90-265VAC, 47-63Hz AC power.

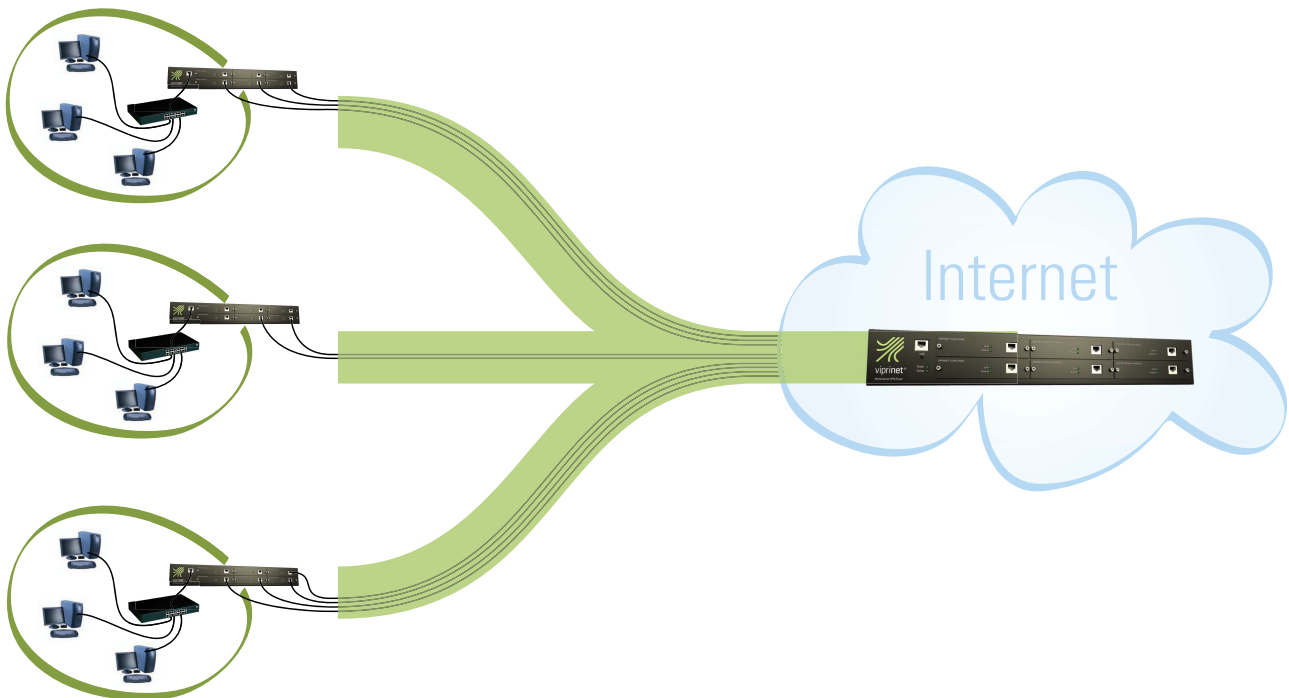
The device is connected to the LAN or a LAN switch using the Fast Ethernet socket (2). An arbitrary combination of Viprinet modems can be plugged into the six available module slots (3). These modules are connected (4) to physical access lines (ADSL and ISDN module) or external modems (Ethernet module). In its minimum configuration the device is equipped with a single module, a maximum of six modules can be installed - an upgrade that can be made by the user at any time.

The main status LEDs (5) indicate whether the device is connected to AC power and if at least one physical line is connected to the VPN peer (online LED). Additionally every module is equipped with LEDs (6) which indicate a working line connection (link LED) and the VPN connection status over this line (online LED).



3. The peer (VPN Concentrator)

The Multichannel VPN Router requires a peer to operate. If placed in a central office or a data center, this peer can be another Multichannel VPN Router equipped with a Fast Ethernet module for each branch that is to be connected. These modules are connected to the Internet backbone. All VPN tunnels established from a branch office over several physical lines terminate at the module responsible for that office. The router reassembles the data streams. If the destination of an IP connection lies inside another branch office, the data will be transmitted encrypted over the respective module. If the destination lies outside the controllable network, the data is output unencrypted to the Internet over the LAN socket which is connected to the Internet backbone.



The endpoints can be virtualized at the junction point if a large number of branch offices needs to be serviced. In this case, instead of a physical Multichannel VPN Router a high-performance server is deployed. The required Ethernet interfaces are mapped to virtual network devices on a physical network interface card. In particular, virtual endpoints are used by ISPs – this way, VPN endpoints for a large number of customers can be implemented with little hardware requirements. Data streams of different customers are individually encrypted and strictly separated from each other.

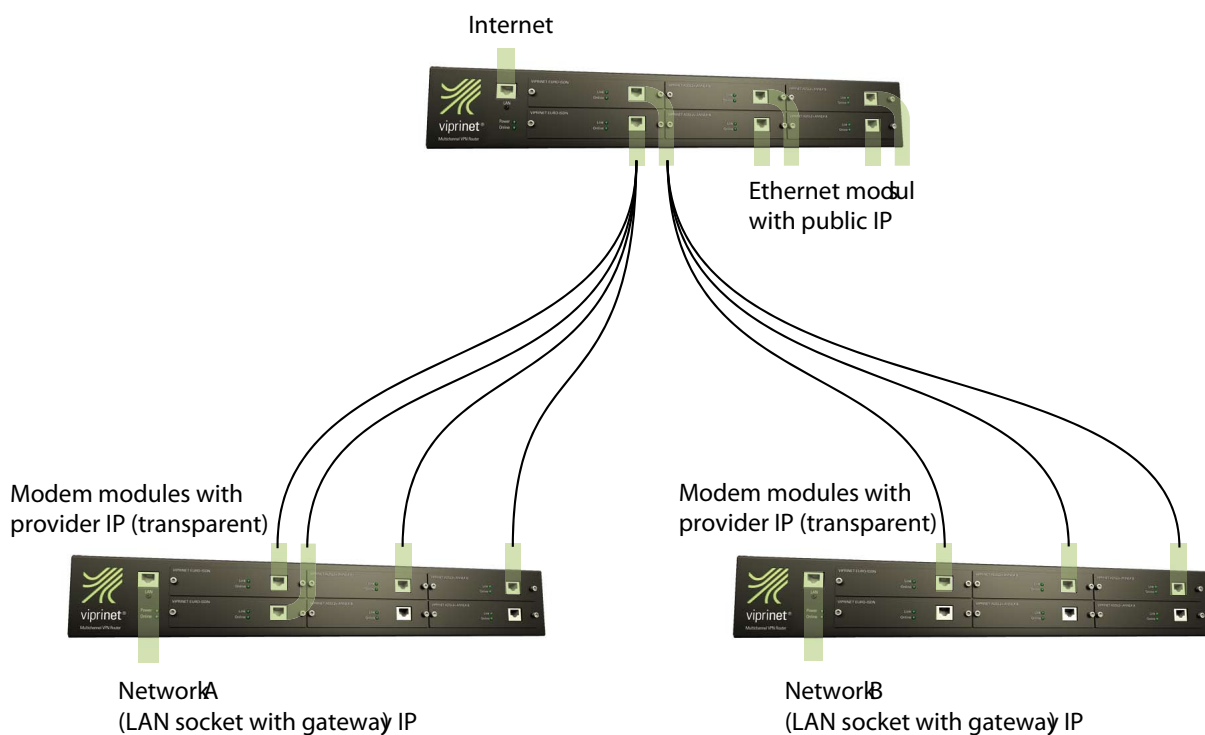
4. VPN-Clients / Road Warriors

Apart from its main task – interconnecting networks – every Multichannel VPN Router is able to accept an arbitrary number of single connections by VPN clients. A VPN client is a single host which is located outside a group of networks connected with a VPN. Such workstations are connected to the VPN pool via VPN client connections. The VPN clients integrates into the operating system as a virtual network device and dynamically utilizes – comparable to the Multichannel VPN Router – all available online connections (e.g. UMTS and WLAN). This is a significant advantage compared to previously available VPN client systems.

5. IP routing

The Multichannel VPN Router works on layer 3 of the OSI layer model, connecting IP networks on different locations via IP routing. A separate subnet, with the Multichannel VPN Router serving as a gateway, is assigned to each location. Additional external VPN clients are located in a separate subnet as well.

The tunneling method used makes the dynamic IP addresses of the physical access lines “transparent”. They are only being used inside the router itself. The IP addresses belonging to the LAN interface and the LAN itself are completely virtualized.



This technology makes it possible to assign arbitrary IP address spaces to your network without the need for support from or knowledge about the physical line providers. A peer (e.g. the Viprinet VPN Concentrator) located in a data center can route arbitrary address spaces assigned to it to the branch offices, enabling the flexible distribution of public IP addresses according to changing requirements.

The Viprinet Multichannel VPN Router is also capable of NAT (network address translation), where private IP addresses are used in the branch offices. On connections leaving the VPN towards the Internet via the peer those addresses are replaced by a public IP address. It is also possible to operate the device in mixed mode, using one Multichannel VPN Router to route several public and private networks.

Example configuration using public IP addresses:

Network A:

Network range: 89.207.250.0/24 (89.207.250.2 - 89.207.250.254 usable in the LAN)

Gateway IP: 89.207.250.1

Network B:

Network Range: 89.207.251.0/24 (89.207.251.2 - 89.207.251.254 usable in the LAN)

Gateway IP: 89.207.251.1

Both networks reach each other using the peer located at the Internet backbone. Packets going out from network A and directed to network B or vice versa are directly being transferred inside the router from VPN tunnel A to VPN tunnel B. Packets to the Internet use the public IP address from that network as source address. Both networks are reachable from the Internet.

Example configuration with private IP addresses:

Network A:

Network range: 192.168.0.0/24 (192.168.0.2 - 192.168.0.254 usable in the LAN)

Gateway-IP: 192.168.0.1

Network B:

Network range: 192.168.1.0/24 (192.168.1.2 - 192.168.1.254 usable in the LAN)

Gateway-IP: 192.168.1.1

Once again both networks reach each other using the peer located at the Internet backbone – it's not a problem that their private addresses cannot be routed in the Internet, since the packets are transferred over a VPN tunnel. Packets from network A to network B or vice versa are directly transferred from VPN tunnel A to VPN tunnel B inside the router. Packets towards the Internet get assigned a new, public source address via NAT at the peer.

6. The VPN technology

An independent tunnel connection is established by every connected physical line through the respective ISP's backbone. The Multichannel VPN Router internally treats those tunnel connections like a single virtual dedicated line. The tunnel connections use the established and proven SSL/TLS method for authentication and encryption. The encryption strength can be freely chosen. The router's bundling technology which distributes the data across different VPN tunnels enabled additional security. It would be necessary to break the encryption of every VPN tunnel on all physical lines to decrypt the data streams.

The bundling technique

The Multichannel VPN Router distributes IP data streams (e.g. TCP connections) across the VPN tunnels connected over the physical lines. A novel bundling technique is employed instead of the widely used Round-robin method.

- If the number of concurrent data streams is lower than the number of available lines, even single connections are multiplexed over several physical lines. A single TCP connection can thereby completely harness the bundled bandwidth of all existing lines at once.
- No connections are aborted if one of the physical lines should go down during operation. Non-bundled connections are transferred to a different line ready to use. With bundled connections spanning over several lines the packets lost because of the failure are retransmitted over the lines that are still intact fully automatically. Of course this is completely transparent for all applications.

Quality of Service and bandwidth management

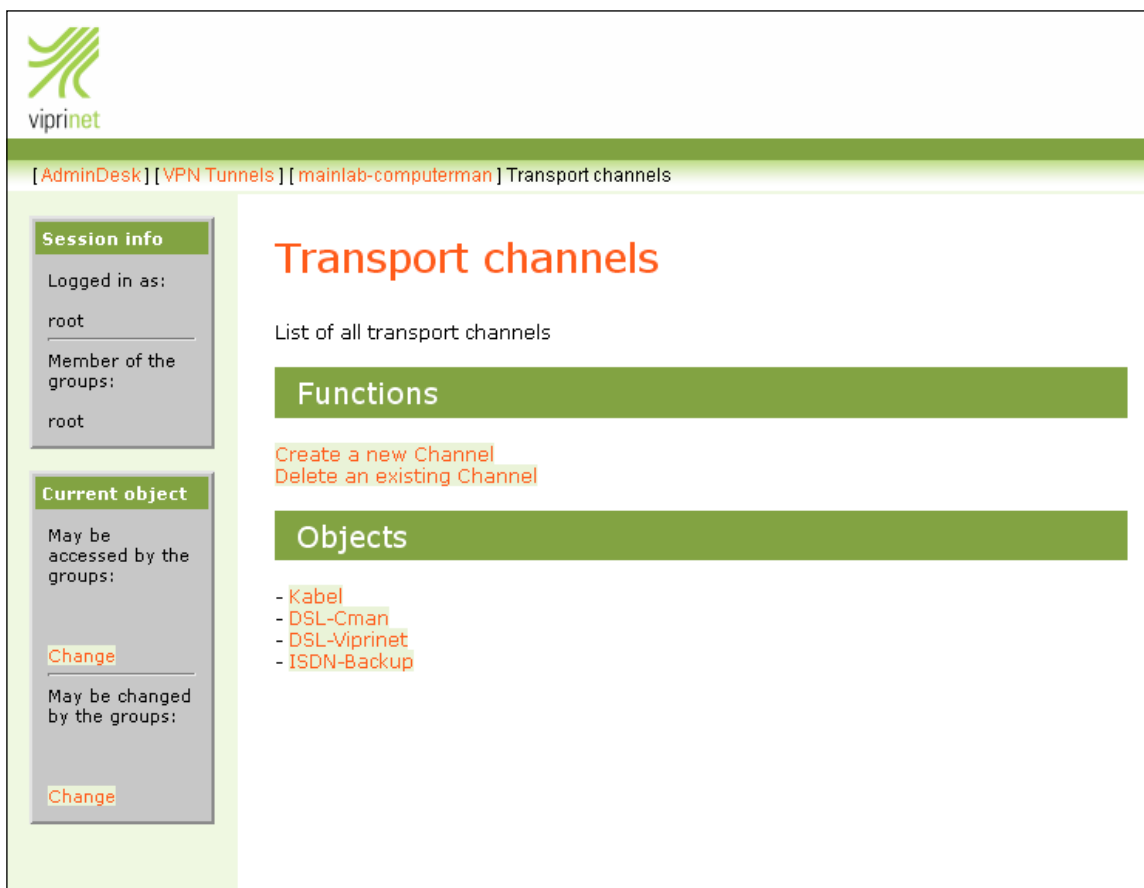
In principle the Multichannel VPN Router treats the total bandwidth provided by all the physical lines together as a single unit. This capacity can be divided among single departments or services in a branch. For example, certain service types can be guaranteed a minimum bandwidth, while others are being throttled. Corresponding rules can be set based on various data sources like IP network range, port numbers or packet properties.

The Multichannel VPN Router employs two concepts for this: First, there are traffic classes that determine how a certain kind of data streams is to be treated – for example, latency-sensitive traffic like Voice over IP calls can be assigned to the line with the lowest current latency, while regular HTTP downloads are distributed across all lines. An integrated rule system then determines the traffic classes that are used to sort data streams into traffic classes.

This intuitive way of bandwidth management and QoS enables a comfortable mapping of existing real business process onto the network infrastructure.

7. Administration, management and monitoring

The Multichannel VPN Router is configured via an easy-to-use and extensive web interface. Access to parts of the administration system can be granted to sub-administrators (read-only or read-write). This enables to delegate parts of the configuration (e.g. bandwidth management/QoS) to departments or customers while the basic configuration remains under the control of a central administration (or the ISP).

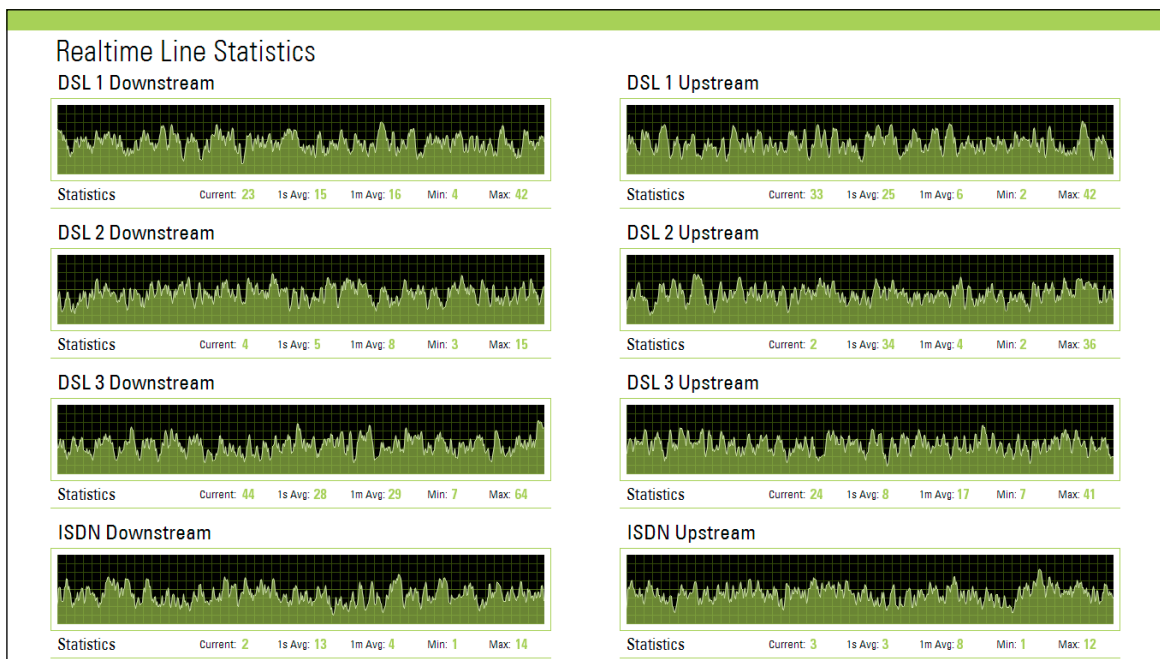


The screenshot displays the Viprinet web interface for managing transport channels. The interface includes a navigation breadcrumb: [AdminDesk] [VPN Tunnels] [mainlab-computerman] Transport channels. On the left, there are two panels: 'Session info' showing the user is logged in as 'root' and is a member of the 'root' group; and 'Current object' showing that the user can be accessed by and changed by the 'root' group, with 'Change' links provided for both. The main content area is titled 'Transport channels' and contains a 'List of all transport channels' section. Below this, there are two green bars: 'Functions' with links for 'Create a new Channel' and 'Delete an existing Channel'; and 'Objects' with a list of channel types: 'Kabel', 'DSL-Cman', 'DSL-Viprinet', and 'ISDN-Backup'.

The Multichannel VPN Router supports the SNMP protocol for integration into existing monitoring and management setups in larger networks.

A comfortable monitoring tool visually analyzes the currently present data streams and usage quota of the available lines in real-time – an ideal way to diagnose performance problems.

Last but not least the system provides extensive accounting and billing functionality. For example, statistics about the users' behavior on different services can be directly logged to a SQL server inside the network, enabling them to be comfortably analyzed or processed.



8. Excellent support

Another important point – Viprinet offers you comprehensive customer support from qualified employees located directly in Germany. Do not hesitate to contact our distribution department if you have any questions concerning the possibilities of our Multichannel VPN Router and the corresponding technology.

We'll gladly help you optimizing your company's connectivity.

Contact us

Viprinet GmbH
Basilikastraße 3
55411 Bingen am Rhein

Phone +49 (0)6721 4 90 30-0
Telefax +49 (0)6721 4 90 30-15
E-mail info@viprinet.com
Web www.viprinet.com