

## ViPNet for MS Windows: Backup-Coordinator

VPN-Gateways (in the case of ViPNet – the ViPNet[Coordinator]) are the central network knots of a VPN environment.

The failure of such a gateway, regardless whether it was a hardware malfunction, power fluctuation or misconfiguration, may lead to enormous financial damage.

ViPNet technology provides you with a solution to this problem.

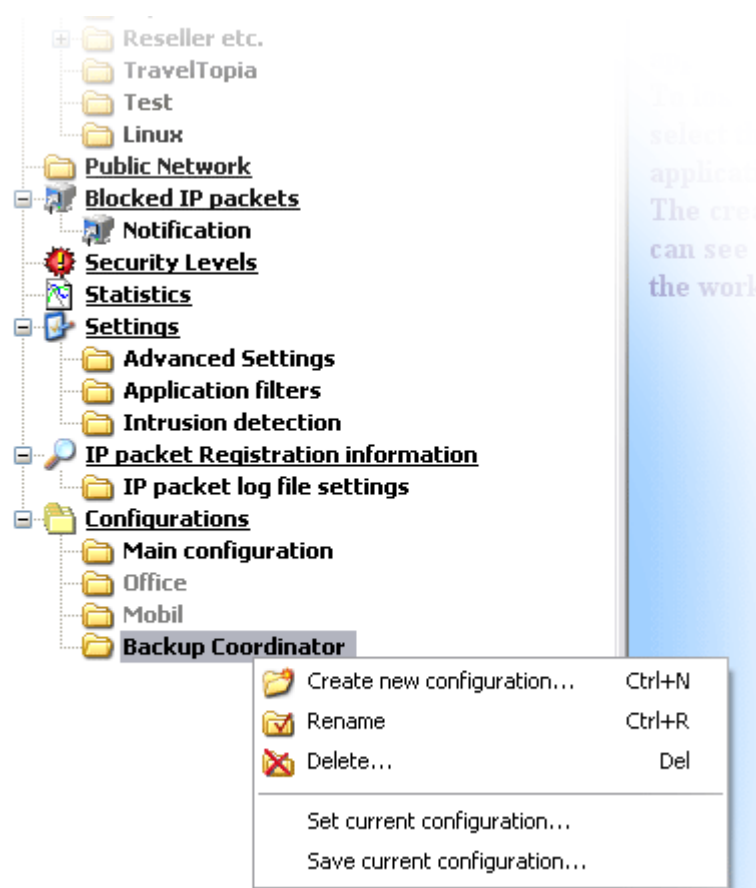
The client-to-client connection type, which is used as the basic principle of the ViPNet technology, allows the VPN users to be able to change the VPN topology according to their needs. This does not only benefit mobile users, which need to connect to the corporate intranet from the most various network environments; this also provides an uncomplicated way to implement a high availability solution for a failsave VPN.

Usually each ViPNet[Client] is connected to a VPN gateway (ViPNet[Coordinator]), which it receives information about the other VPN users from and uses to communicate with the other clients. However, this is not the only possible connection type in ViPNet technology.

For a ViPNet[Client] it is possible to quickly switch to a different coordinator in the case of a coordinator-failure (somebody pulled the power cord, hardware failure, nuclear meltdown, etc.) and continue to work almost without interruption, by selecting a different configuration. These configurations are predefined and can the user can switch between them anytime.

A ViPNet[Client] may have different server connections available to it, like i.e. "Office", "Mobile", or "Backup-Coordinator".

If the coordinator which is used in the "Office" configuration is unreachable, the user can switch to the backup coordinator simply by clicking on "Backup-Coordinator" in the main ViPNet screen. In this case the backup coordinator takes over the being the default server.





## ViPNet for Linux/Solaris: Failover Function

The failover function in Linux is realized by implementing a cluster of two coordinators. Only one of the 2 physically redundant systems is active, the other coordinator is in passive mode. In case of network interface or line issues as well as internal problems, the active coordinator is restarted and put into passive mode automatically, while the previously passive coordinator is switched to active mode automatically.

All other ViPNet network nodes see the cluster only through maximum 1 IP address per network adapter. This IP address is used by the active coordinator. The passive coordinator has a different IP address, which is not used by other ViPNet network nodes to connect to the cluster. In comparison to the active mode, the coordinators have different IP addresses assigned to each of their network adapters when they are in passive mode.

Both coordinators IP stack is configured to use their "passive" IP addresses after a reboot. On startup, a reservation daemon is started in passive mode. The passive coordinator sends out broadcast requests periodically and searches for the IP addresses of the active coordinator. If all IP addresses of the active coordinator are unreachable during a specific time period, the passive coordinator switches to active mode. In this process, the IP addresses of the active coordinator are assigned to the network adapters of the passive coordinator (which are known by the other ViPNet network nodes), and the ViPNet daemon and network interface test-routine is loaded.

Periodically, the active coordinator tests the network on its integrity, by sending out broadcast requests to routing devices. It is seen as a network problem, if a routing device does not respond several times after each other. In such a case, the coordinator will reboot (this will take about 30 seconds). During these 30 seconds, the network adapters of the active coordinator are unreachable; this is the sign for the passive coordinator to switch into active mode.

The reservation daemon, looks for the ViPNet daemon in the memory of the active coordinator. If it cannot find the ViPNet daemon, it will try to start it. If several tests show that the ViPNet daemon is not loaded in the memory, it is seen as an error after which the active coordinator will reboot.

To synchronize the configuration files and ViPNet databases on both coordinators, a reserved line is established between the coordinators, which is used to permanently transfer all needed data to the passive coordinator.

The reservation daemon can be registered in the Watchdog driver. This is a low-level daemon, which even stays functional if the system does not respond to external events anymore. When registering the daemon, an interval is set up. This value defines how often the reservation daemon should look for the driver. If this interval is exceeded, the system is rebooted. In this case the driver tries to write the information from the crash buffer to the hard disk, to minimize filesystem integrity problems.

When using SNMP, a message (Trap) is sent to the device, which was defined in the SNMP-configuration file as trap sink everytime the ViPNet daemon is started. This can be used to notify the administrator of a failure.

Both coordinators in the cluster are equal: on cluster startup, the first started up computer becomes the active coordinator.

The cluster may include both a Linux and Solaris computer.