

PowerLink Pro100 Technical Brief

WAN Traffic Management with PowerLink Pro100

Overview

Optimizing your online presence is crucial for business success. WAN/ISP link failover and traffic management have grown from “good-to-have” to “must-have” features, and businesses of all sizes are using them on a daily basis. Here’s why:

- Small and medium-sized businesses need both incoming and outgoing failover and aggregation of an increasing assortment of critical business traffic, from applications to VoIP to email. These businesses can range from the local corner store that does online banking and bill-pay over the Internet to a manufacturing company that needs email, web services, hosted ERP and ecommerce applications available 100% of the time.
- Companies with a centrally located headquarters and a number of branch offices need secure and reliable data communication among those locations. These businesses frequently use VPN tunnels between their remote locations and headquarters and have intense company traffic 24/7. They need reliable performance and high availability of their VPN data, including the ability of the tunnel to automatically failover if a WAN link goes down.
- Web hosting companies/ASPs/Small ISPs need incoming aggregation and failover to their services, with extra bandwidth and redundancy available to their servers. Their mission-critical e-commerce applications need to be up and running 24/7. If a WAN link goes down, the failover process has to be smooth and transparent to the user.
- Many companies now need Quality of Service (QoS) levels and traffic shaping for guaranteed bandwidth to critical services/applications. These companies are attempting to deploy reliable and affordable VoIP solutions to cut expenses and enhance productivity. However, by design, VoIP technology is dependent on the available bandwidth and the quality of the circuit over which it is routed.

PowerLink Pro100

Astrocom’s PowerLink Pro100 is an affordable, scalable solution designed to meet all of these requirements. The Pro100 guarantees 100% Internet uptime at one-third the cost of most competitive products—making it an attractive option to small and medium enterprises that need a simple, affordable and foolproof method to maximize availability for critical applications.

The Pro100 also provides a cost-effective way to scale up as Internet usage grows and becomes more mission critical—businesses can add up to 15 low-cost ISP links to meet virtually any capacity need. The alternative is adding T1 or other dedicated links that are expensive and in all likelihood will be underutilized.

The PowerLink Pro100 provides:

- WAN link redundancy with automatic failover
- Bandwidth aggregation/intelligent load balancing for any type of WAN technology
- Multi-homing of multiple ISPs (up to 15)
- Transparent bridging to firewall
- VoIP failover
- QoS and traffic shaping
- DoS and DDoS protection
- High availability/hardware failover

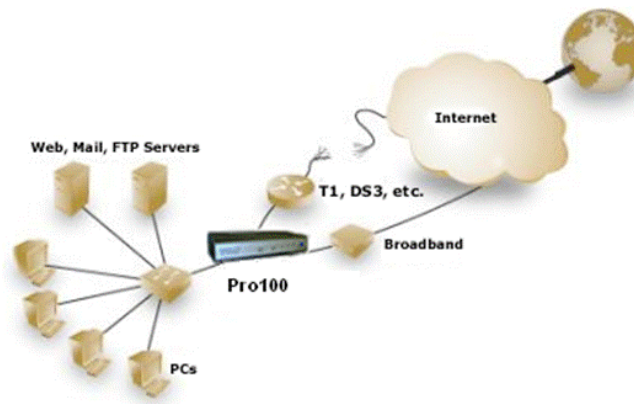


Here is a closer look at each individual feature.

WAN Link Redundancy with Automatic Failover

WAN link redundancy can be implemented in several ways and at various levels. The Pro100 typically sits between the CPE routers (the endpoints where 2 or more broadband connections are delivered) and the WAN port of the firewall, where it can manage all outgoing and incoming traffic. In the event that a WAN link, or ISP, goes down, the Pro100 automatically senses the failure and moves the traffic to the up-and-running WAN link(s). When the failed link comes back up, it immediately gets placed back into service.

The Pro100 provides failover on both outgoing and incoming traffic. Outgoing failover is based on monitoring the health of the WAN link(s) by polling/checking data from trusted hosts on the Internet.



Incoming failover is accomplished by designating the Pro100 as the primary and secondary authoritative DNS name server for all the domains being hosted. The Pro100 advertises the addresses of all healthy available links. Should a link go down, the Pro100 will stop advertising that particular link's IP address, resulting in the caching servers dropping that address from its records. By

setting the host name record "Time to Live" to a small number (typically 30 seconds or less), the failed link will be quickly removed and reinstated automatically when link health is restored.

The Pro100 is transparent to VPN tunnels (either IPSec or PPTP) and will facilitate tunnel failover on loss of a WAN link. Astrocom has developed a number of VPN failover solutions in conjunction with the most popular major firewall manufacturers, i.e. Cisco PIX, SonicWALL, Watchguard, Net Screen, Checkpoint, etc. A typical VPN tunnel is built between the firewalls and the remote client over a specific WAN link. In the event of a WAN link failure, the Pro100 will automatically move the tunnel to one of the up-and-running available links.

Depending on the firewall manufacturer, there are two configuration scenarios used: (1) resolving VPN tunnel failover based on host names; (2) resolving VPN tunnel failover based IP peers. For specific information and configuration diagrams, please refer to the specific solution whitepaper located on our website: (1) For host name resolution, see "[VPN redundancy and ISP failover using PowerLink and SonicWall.](#)" (2) For IP peer resolution, see "[VPN failover using PowerLink and Cisco PIX.](#)" (3) For Watchguard regarding manual IPSEC configuration, see "[VPN redundancy using PowerLink and Watchguard.](#)"

Bandwidth Aggregation from Multiple ISPs

The Pro100 allows businesses to incrementally increase WAN bandwidth by aggregating multiple access lines to achieve a virtual high bandwidth line to the LAN. This avoids the high expense and single point of failure of having to jump to the next higher available single line access technology. For example, if you have a T1 line now and need additional bandwidth, you would typically have to migrate to a T3 line. This would take you from your current 1.5 Mbps to 45 Mbps. This is probably significantly more bandwidth than required and is a dramatic increase in cost.

This same scenario can be accomplished at a fraction of the cost with two 768 kbps DSL lines that can be combined for a total aggregated bandwidth equivalent to a T1. With the Pro100, you could simply add additional lower speed lines, i.e. xDSL, cable or wireless etc., incur



a relatively small increase in cost and match your exact needs. In addition to getting more cost-effective bandwidth, you are also dramatically increasing the reliability of your connection due to the new levels of redundancy in your aggregated Internet connection. The average T1 connection is down for over 8 hours per year. The average Pro100 site will avoid these outages all together and save your organization downtime, frustration and a countless amount of money due to lost business.

The Pro100 is independent of the WAN technologies and is fully compatible with xDSL, cable, wireless, T1/E1, T3/E3, satellite, fiber channel, Frame Relay, etc. (mix and match). The total bandwidth aggregation capacity of the Pro100 allows for up to 150 Mbps (full duplex) and will accept up to 15 different WAN connections. Further, the Pro100 has the ability to host up to 128 domain names.

Outgoing bandwidth aggregation is offered at the TCP/UDP session layer. The user defines weights for the WAN links based on the bandwidth of the link. When a session is generated from the LAN, the Pro100 computes which link has the most available bandwidth and routes traffic from that session over that particular WAN link. The Pro100 allows selection of 2 load-balancing algorithms: (1) symmetrical round robin or (2) intelligent (weighted) load balancing. The symmetrical round robin will route sessions to all links in a round-robin manner. The intelligent load balancing will compute a ratio between the weight (bandwidth capacity) of the different lines and route sessions accordingly. That is, the faster the link, the more sessions that will be sent over that link to make the most efficient use of all the bandwidth available.

Incoming bandwidth aggregation is accomplished by the Pro100 being the authoritative DNS server for the domain. The Pro100 advertises all available WAN lines to the (Internet) cache servers, which in turn resolve the domain names to queries in a round-robin format. In this manner, all externally initiated sessions are load balanced over all available links. Since the Pro100 is resident at the domain site and is able to directly monitor the link status, failed links are removed from the DNS tables immediately upon failure. By setting the host name record Time to Live (TTL) to a short period, the caching servers will flush their address tables and will update them from the Pro100 regularly and thus be informed when a link fails.

Multi-homing without BGP

The Pro100 uses a multi-homing technique and NAT in order to unify traffic coming from and going to different destination IP addresses on the Internet. The Pro100 will be configured with at least one routable IP address for each router/WAN link to which it is connected. Incoming traffic to any of the Pro100's WAN addresses is forwarded to specific LAN destinations based on port forwarding rules configured in the Pro100. i.e. all port 80 traffic to WAN address x.y.z.1 could be forwarded to WEB server 1 on the LAN, and all port 80 traffic to WAN address x.y.z.2 could be forwarded to WEB server 2 on the LAN. Up to 128 port forwarding rules can be defined, which means that up to 128 different servers/services can be hosted in a single LAN.

The biggest benefit of multi-homing resides in the Pro100's ability to achieve outgoing and incoming load balancing and failover without defining BGP routing tables or utilizing any of the underlying complicated routing techniques. The ability to offer this functionality without the expensive or complicated networks/equipment necessary to achieve BGP is what makes the Pro100 such an exceptional value, especially for small and medium-sized organizations. (See our White Paper: "Multi-homing Without BGP.")

Transparent Bridging to Firewall

This feature is equivalent to the "drop and insert" feature of most firewalls. In this configuration, the Pro100 is simply a bridge between the firewall and the WAN router. There is no need to reconfigure the IP address of the firewall; you simply change the firewall's gateway to point to the Pro100. All other firewall settings remain as they were prior to installing the Pro100. The Pro100 will bridge traffic that is destined for the original WAN link and will NAT traffic to the additional links that are added.



The main benefit of this feature resides in the fact that the firewall's NAT rules will not need to be reconfigured. The only reconfiguration needed on the firewall will be to change the default gateway to reflect the Pro100's LAN/WAN IP address. Transparent firewall/bridging dramatically improves the customer's experience in terms of installation and configuration and the overall interaction with all the other devices in the network.

VPN Failover

The Pro100 provides VPN tunnel failover. Should the WAN link carrying the tunnel fail, the Pro100 will remove the failed link and direct the firewall/VPN server to a healthy link so it can re-establish the tunnel. The mechanism used for tunnel failover is dependent on the firewall/VPN server used. For example, Sonic Wall and Watchguard use DNS hostnames for tunnel identification, while Cisco uses an IP peering technique.

QoS and Traffic Shaping

QoS/Traffic Shaping is accomplished with the Pro100 by defining rules that designate the minimum and maximum bandwidth to be allowed for the traffic defined by the rule. For example, you could define a rule that stated that all port 80 (Web browser) traffic would be allowed a minimum of 50 kbps and a maximum of 500 kbps. Under this Rule, port 80 traffic would be assured of 50 kbps if the links were busy and could use up to 500 kbps if bandwidth were available. Rules can include such things as ports, protocols, packet size, etc.

DoS and DDoS Protection

In order to increase security and high availability, the Pro100 implements sophisticated anti-DoS (Denial of Service) and DDoS (Distributed Denial of Service) mechanisms. This feature allows for the prevention and blocking of a wide variety attacks including basic and distributed attacks. Other features include support for anti flood ping, ping of death and spoofing. For more, see our White Paper "DDoS Effects Preventable via Multi-Homing Solutions."

High Availability and Hardware Failover

To eliminate the possibility of the Pro100 becoming a potential "single point of failure" in the network, two Pro100s can be utilized in failover mode. In this mode, two Pro100 units are placed in the network and communicate to each other to establish a hardware failover/cluster device. The first Pro100 is configured as primary and is, by default, active. The second Pro100 is configured as secondary and is, by default, idle. The units are configured identically with the exception of the primary/secondary parameter. The configuration files in both units are automatically updated whenever a change is activated in one of the units. If the active unit fails, the idle unit takes over. The heartbeat between the two devices is over Ethernet, which makes the solution robust and eliminates the need for additional proprietary cabling. The heartbeat works over an internal set of IP addresses and port numbers that are specific to the hardware failover solution and is transparent to the general traffic management of the Pro100.

Summary

Astrocom's PowerLink Pro100 is an affordable, scalable solution designed to meet all of these requirements. The Pro100 guarantees 100% Internet uptime at one-third the cost of most competitive products—making it an attractive option to small and medium enterprises that need a simple, affordable and foolproof method to maximize availability for critical applications.

The Pro100 also provides a cost-effective way to scale up as Internet usage grows and becomes more mission critical—businesses can add up to 15 low-cost ISP links to meet virtually any capacity need. The alternative is adding T1 or other dedicated links that are expensive and in all likelihood will be underutilized.