

Why an Intelligent WAN Solution is Essential for Mission Critical Networks

White Paper Series WP100135

Charles Tucker
Director of Marketing

June 1, 2006

Abstract:

Reliable Internet connectivity is now viewed as mission critical by a growing number of smaller businesses, including startup Service Providers, whose customers view connection disruptions as a fundamental criterion for changing to another vendor.

This white paper discusses the components of WAN intelligence for the small and medium organization. The technology market is fraught with choices, both complex and simplistic, to the question of WAN reliability. Those businesses who wish to closely mimic the quality of reliability deployed by Enterprise carriers yet be manageable be smaller organization IT staff, will need to analyze their needs carefully to avoid compounding the affects of under or over scaled infrastructure.

Sohoware offers BroadLink™ as an intelligent WAN solution to serve the mission critical needs of the small and medium organization. The combination of performance, features, and scalability achieve carrier reliability in a platform with a fraction of the complexity.

White Paper: Why an Intelligent WAN Solution is Essential for Mission Critical Networks

BroadLink™ Offers ISPs and Enterprise a Comprehensive Failover Approach With Less Complexity

June 1, 2006

As small and medium ISPs expand their deployment of services to residential and commercial multi-tenant properties, their backend networks become increasingly mission critical to their success. Subscribers have choices, and connection reliability tops the list of criteria for renewing their service contract. Yet investing in carrier-grade solutions designed around global Service Provider requirements is complexity overkill, not to mention cost prohibitive in both infrastructure investment and ongoing management for the smaller ISP.

Enterprise networks, particularly mid-size businesses with under 1000 stations and several branch locations, are increasingly supporting their own data centers and web servers making their IT backbone ever more mission critical. These businesses are increasingly intolerant of service disruptions that interfere with customer, channel partner and mobile staff access to corporate information and resources.

Sohoware's BroadLink™ WAN load balancers are ideally suited for the small to medium ISP and Enterprise who need a high performance method to support service reliability in their mission critical operations. This paper breaks down the components of an intelligent WAN solution and explains their value to the ISP or Enterprise in achieving carrier-class reliability with lower complexity and cost. BroadLink™ answers the overall goal of guaranteed access without the investment of carrier infrastructure.



BroadLink Family of WAN Solutions

Auto Routing

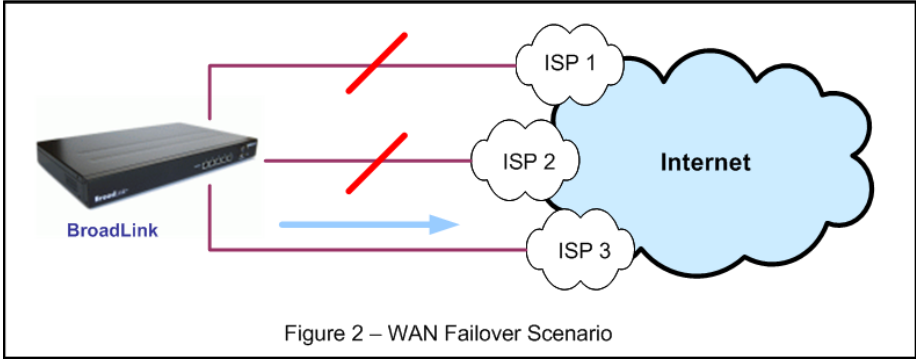
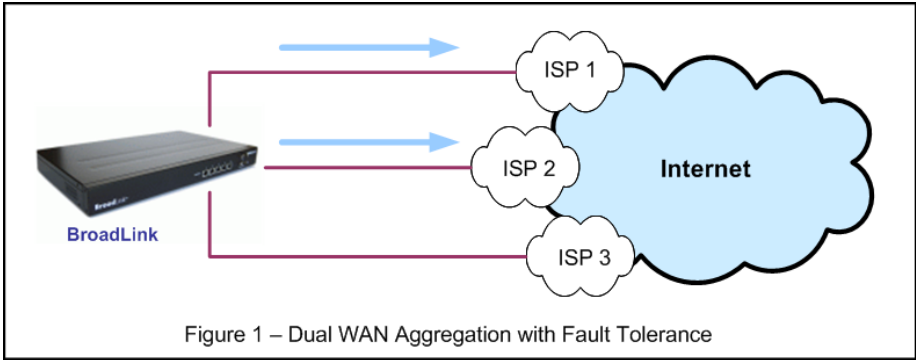
BroadLink™ can control how packets are delivered to multiple WAN links as defined by routing and load balancing policies. Auto routing effectively controls outbound traffic, adding resiliency, higher availability, and superior load balancing to the network, and involves sophisticated planning at Layer 3 and 4 for source, destination and port related protocols.

Yet, as opposed to being complex to setup, enabling auto routing requires only the definition of a policy and a filter in BroadLink™. Policies let you define the way auto routing operates and filters act as the criteria to trigger the policy. Auto routing can be summarized as:

Auto Routing = Filter + Policy + Failover Policy

Filter settings are defined by time schedule, source and destination IP addresses, or service ports. Policies are defined by the type of algorithm selected for distributing outbound traffic across the available WAN links, including fixed, round robin, weighted round robin, or traffic direction. Failover Policy defines the contingency plan when multiple WAN links are disrupted.

In Figure 1, a network uses two WAN links on a filter/policy basis, and reserves a third link for failover. Figure 2 shows a failover scenario where the effect of catastrophic disruptions is nonetheless mitigated.



Bandwidth Management

The strategy to optimize network performance is key to a cost efficient approach to network reliability. With the growing number of bandwidth intensive applications available to subscribers and Enterprise staff, effective bandwidth management an essential tool that must be integral for both the Enterprise and Service Provider networks.

BroadLink™ defines bandwidth usage as a policy, where allocation is based on priority as well as demand to minimize performance deterioration at times of peak use. Policies can apply to traffic on each WAN link separately, in both inbound and outbound directions. As with routing policies, bandwidth management applies to Layer 3 and 4 for TCP/IP and port protocols, plus, specified time periods to address peak and idle phases of traffic.

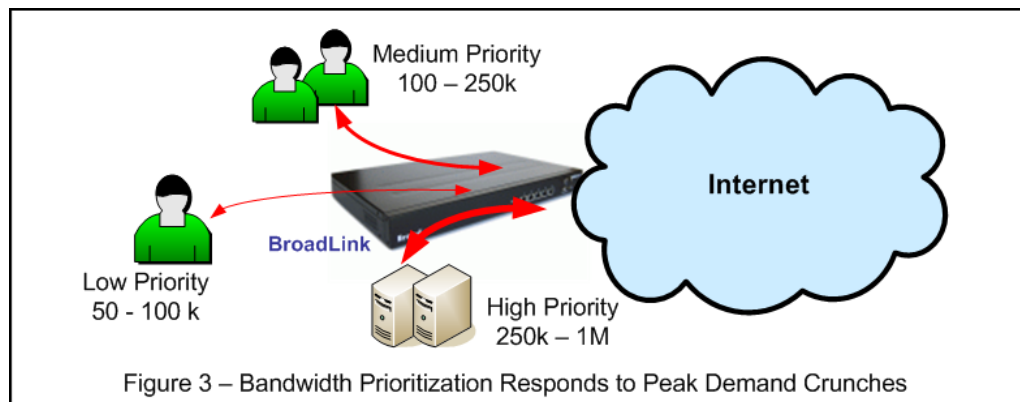
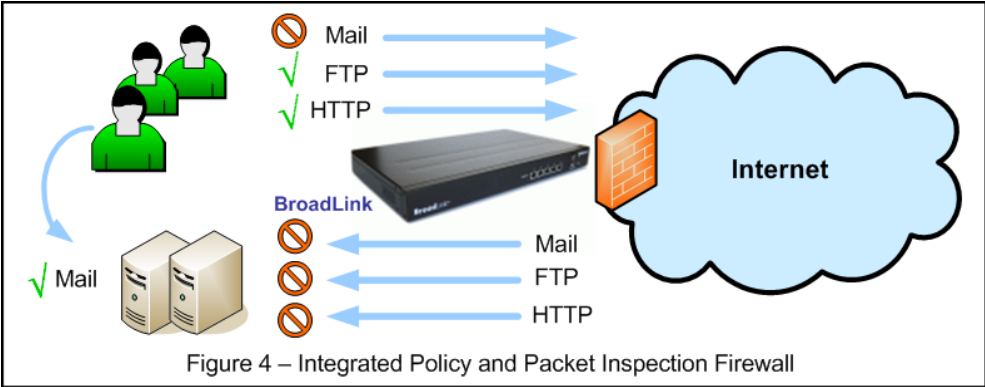


Figure 3 illustrates prioritization as it applies to the needs of the organization from within and without. In this case, access to network servers takes precedence, insuring that in peak demand their resources remain available at the minimum quality of service expectation. Certain users, or their applications, are sacrificed if necessary as part of the overall performance optimization strategy, which allows the organization to plan their network infrastructure investment more efficiently rather than having to over scale for heaviest demand or demand period.

Firewall

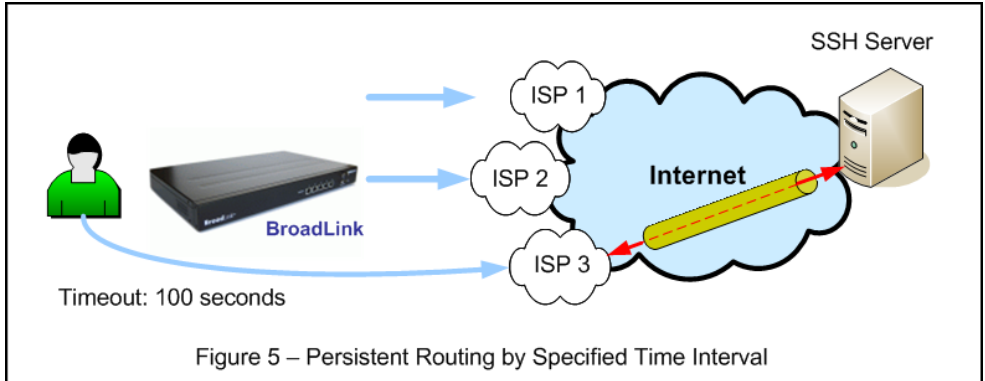
With its rich routing policy configuration, BroadLink™ is able to offer comprehensive protection at Layer 3 and 4 protocols, seamlessly integrated as part of an organization's WAN optimization strategy. Threats at this level directly affect network performance and availability. To alleviate these vulnerabilities, BroadLink™ employs deep packet inspection to filter unknown or suspicious traffic combined with policy based routing to screen for both inbound and outbound Denial of Service (DoS) attacks.

The Stateful Packet Inspection (SPI) firewall is an essential component to block unauthorized access from outside the network. Add to this BroadLink's policy control, and essential protection against application based Denial of Service is fortified, as shown in Figure 4, where policy requirements combined with packet inspection prevent the introduction of infected email by restricting delivery from local servers only. Alone or in combination with other UTM firewalls, BroadLink™ adds essential perimeter protection to prevent malicious sources of network downtime.



Persistent Routing

Certain user applications require a fixed link to conduct uninterrupted communications across the WAN. For limited time frame use, such as online ecommerce transactions, persistent routing allows the creation of a temporary exception to the auto routing policy currently in use. Duplicated traffic matching the definition given for persistent routing will be directed to the applicable link. Once the time frame has expired all traffic will resume according to the existing auto routing policy.



As shown in Figure 5, persistent routing adds flexibility to the configuration options available in BroadLink™, allowing administrators to support a range of user desirable applications more effectively without disrupting policies in place for other network users.

Multi-Homing

Carrier networks rely on BGP protocol to implement multi-homing for large scale Enterprise networks requiring guaranteed service connections. Complexity and cost associated with the configuration and support of a BGP network make it an ineffective choice for small to medium business and Service Providers. BroadLink's multi-homing approach achieves the same failover service guarantee as BGP at a fraction of the complexity.

The key to access failover is the aggregation of multiple ISP links, over which intelligent load balancing policies are applied as defined by quality of service requirements previously discussed under auto routing. Each WAN link is given a public IP address.

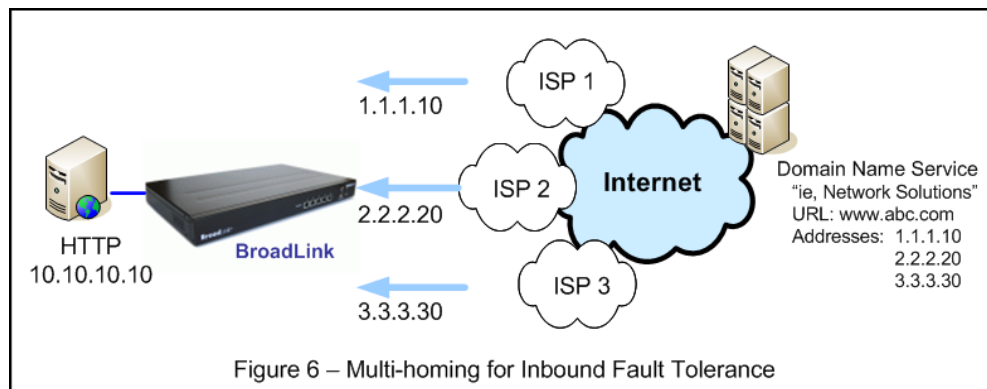
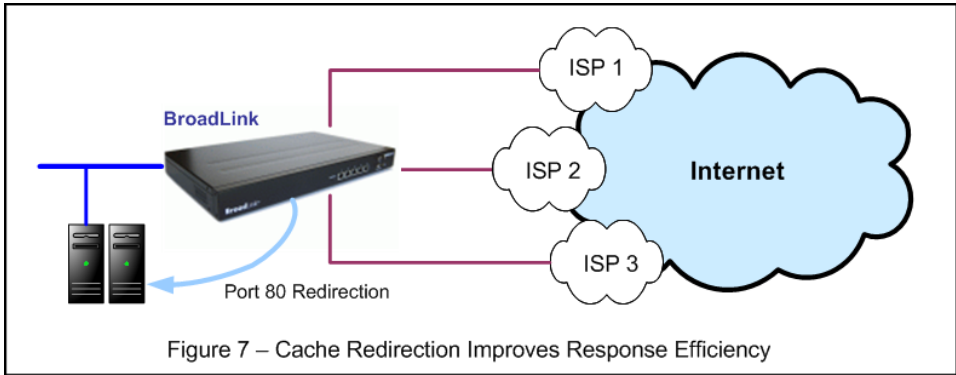


Figure 6 shows a public Web server accessible from three WAN links, each associated with a registered domain name. The dynamic DNS function in BroadLink™ supports URL association with the IP addresses, while the multi-homing function allows the administrator to define the desired load balancing policy for inbound traffic. Service continuity is assured through BroadLink's active link monitoring procedure that constantly verifies the status of each ISP link. Should a link disruption occur, BroadLink transparently redirects traffic to the remaining active links. The configuration is performed within the Web administration screens of the BroadLink™ unit, dramatically simplifying setup and configuration over conventional BGP.

Cache Redirection

For Enterprise networks supporting continuous outbound Internet traffic, the repetitive requests to particular Web sites can add significant burden to bandwidth usage. As part of BroadLink's strategy to optimize network performance, duplicate requests can avoid the consumption of bandwidth by accessing cache servers associated on the network. The cache redirection process can be conducted on a policy basis, by assigned weight on a per server group.



Administrators can optimize traffic on Port 80 and other ports as desired to reduce outbound query duplication. The redirection function also serves as a health monitor for cache servers to avoid request delays due to server downtime. The comprehensive intelligence associated with health detection, weight allocation, and port configuration is essential to effectively implement cache redirection.

Policy Grouping

Further to the configuration options available under auto routing, BroadLink™ provides logical grouping options by IP and service association, which provides more scalable support for administrators who manage large distributed organizations. A group can be created in the interface menu under which various IP or service objects are assigned, reducing repetitive configuration on a user-by-user basis. Groups simplify network administration and minimize configuration error, assuring uniform policy assignment and reducing demand on administrative time.

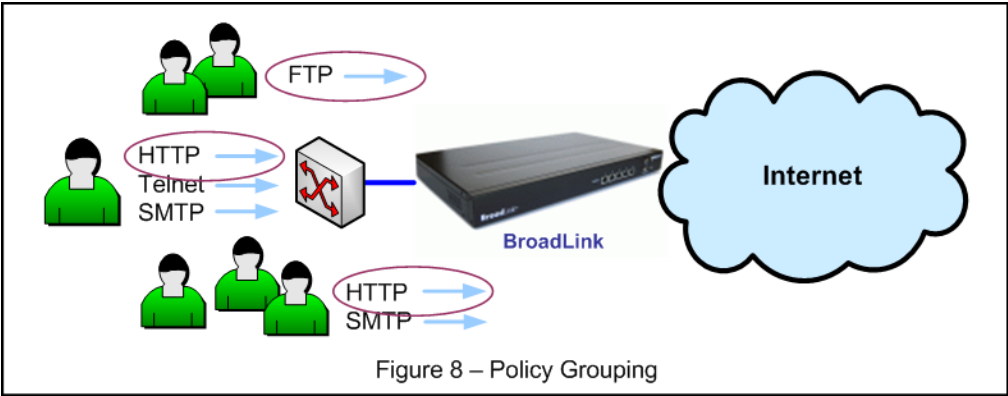
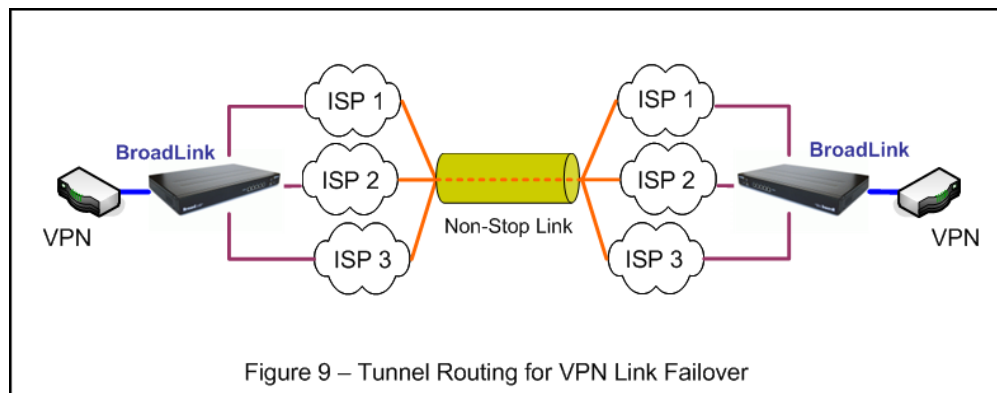


Figure 8 shows a grouping of services that share a distinct configuration policy even though applied to users in different departments. Policy assignment is performed once, rather than three separate times. Each policy can be selected later from a pull down menu for modification and refinement, such as the addition of firewall and bandwidth policies.

Tunnel Routing

Numerous site-to-site applications require a permanent IP address to sustain services, including VPN, NetMeeting, and other conferencing tools. As organizations expand their operations to multiple sites, the ability to unify network resources and communications between these locations becomes increasingly mission critical. BroadLink's multi-homing function can be further enhanced to support tunnel routing between sites, enabling these applications while maintaining multiple WAN connections.



In Figure 9, two branch offices communicate through a secure VPN tunnel across multiple WAN links without disruption. Here, BroadLink™ units are positioned on the WAN side of the VPN concentrators at each site, and are responsible for performing outbound and inbound load balancing of the VPN encrypted traffic. Configuring this tunnel requires simply adding the destination IP addresses of the corresponding BroadLink™ into the tunnel routing table. BroadLink's intelligent routing capabilities make transparent the receiving of continuous communications traffic regardless of dynamic WAN link changes as part of the normal load balancing, multi-homing, or even failover routing functions being performed at each end.

Summary

Alternatives to carrier-grade, BGP based load balancing solutions are available to the small and medium Enterprise and Service Provider for achieving high availability service connections. These alternative solutions, like BroadLink™, are now an essential network component where mission critical operations directly impact the customer and subscriber experience, and thereby the organization's competitive stance.

BroadLink™ offers the right combination of performance and features that mimic the high availability of more complex and costly solutions in a platform designed to be manageable by a smaller organization's IT staff. Now mission critical operations can be supported in a wider range of network sizes and offer the scalability these growing businesses need.