Position Paper

Nortel Networks

Alteon Link Optimizer

Maximizing high availability, utilization, and security in multi-homed networks

NORTEL NETWORKS™

Contents

Executive summary 3

Introduction 4

High availability 4

Utilization 4

Outbound traffic optimization 6

Inbound traffic optimization 6

Security 7

Multi-homing evaluation criteria 8

Business case 8

Alteon Link Optimizer—Link load balancing solution 10

Summary 11

Executive summary

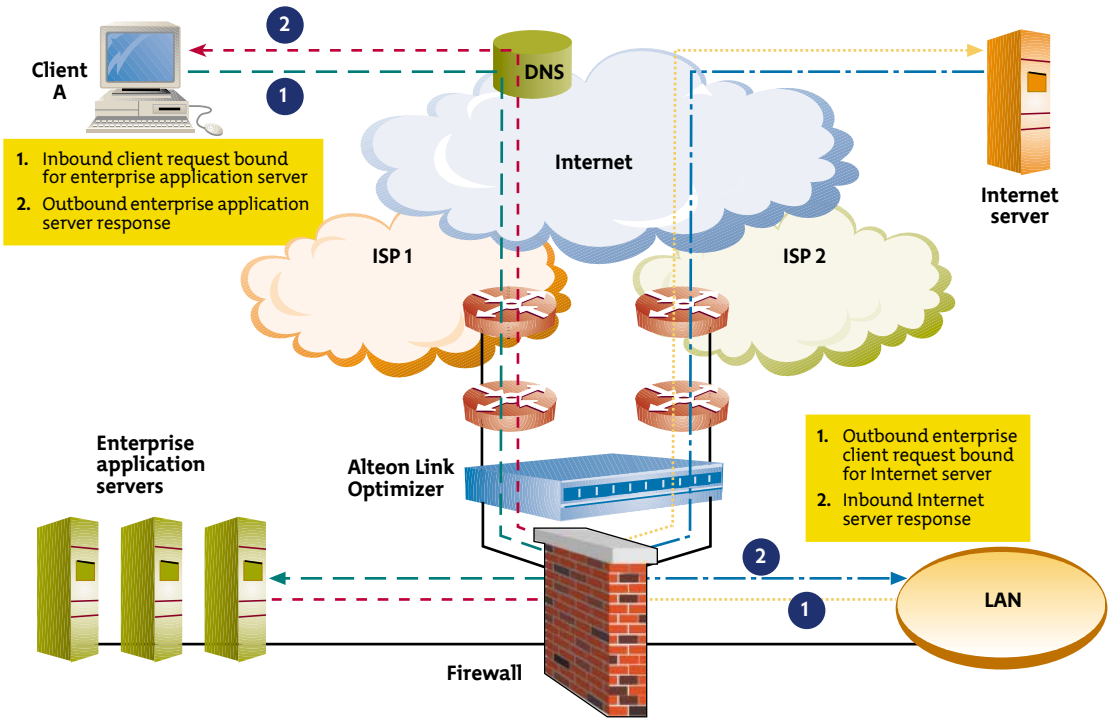
Nortel Networks Alteon Link Optimizer simplifies multi-homing by utilizing intelligent traffic management, bandwidth management, and health checking to optimize the availability and utilization of multi-homed network connections. Sophisticated integrated security such as Denial of Service protection, application abuse protection, access lists, filtering, and Intrusion Detection System load balancing also provide a first layer of application and network security.

The Alteon Link Optimizer implements dual mode link load balancing and utilizes a full set of load balancing and health checking algorithms along with bandwidth rate limiting to ensure that applications and client access receive the network resources needed to maximize productivity. *Figure 1* provides a simple overview of the Alteon Link Optimizer dual mode operation.

An Alteon Link Optimizer provides the enterprise significant operating and capital expenditure savings. Increased application and network performance/availability translates into increased corporate productivity.

Previously idled backup WAN links or trunked combinations of less expensive WAN links can be utilized to carry traffic. Less expensive burstable WAN links can be purchased while bandwidth spike control allows for minimum overuse charges. Bandwidth robbing security attacks are stopped at the network door step. The Alteon Link Optimizer provides all these opportunities to increase enterprise IT Return on Investment (ROI) at a cost up to 80 percent less than competitive products.

Figure 1. Dual mode link load balancing—Inbound and outbound



Introduction

In today's business environment, more and more applications (VoIP, CRM, ERP, etc.) are being run over the Internet and intranet. As dependence on these applications increases, network reliability becomes critical. Enterprises that suffer from WAN and ISP link reliability problems risk significant decreases in employee/partner productivity and lost revenue opportunities. Most enterprises implement redundant (multi-homed) links to increase the reliability of their WAN and Internet access. If not managed correctly, multiple ISP links can result in idle resources and ineffective failover schemes. Security attacks and their defenses can also rob network link performance. New expense constraints placed on IT managers make it even harder to provide cost-effective, highly available links. To ensure maximum availability, utilization, and security of multi-homed links, IT managers must carefully design network architectures that leverage sophisticated link optimization solutions, without breaking the budget.

High availability

It's critical that enterprises maintain business continuity by ensuring their Internet access is always available to support today's high value-add business applications. To provide 24x7x365 uptime, corporate enterprises must support multiple connections per location to their WAN and the Internet. More than two Internet or WAN links connected to a single enterprise location and working as one large logical link is referred to as multi-homing. The enterprise can implement multi-homing utilizing Border Gateway Protocol (BGP) or a link load balancing solution. BGP identifies the best link to the upstream router via routing table updates. If a corporate IT staff can manage the BGP table, and the enterprise can obtain the necessary prerequisite to participate in BGP routing (such as obtaining an Autonomous System Number), standard BGP-based routers can be utilized for multi-homing. While BGP routers can support multi-homing, they are normally complicated to set up and manage. BGP-based solutions can also suffer from significant failover latency and support only simple concurrent link operation and traffic direction features. Congestion issues can also be a limitation of routers running BGP. This congestion results from the algorithm BGP uses to direct traffic. BGP looks for the nearest router hop between two connection points regardless of the traffic load or number of packets waiting in the queue for a link. Alteon Application Switches are excellent choices for enterprises that are interested in a BGP-based multi-homing solution.

An alternative to BGP-based multi-homing is link load balancing. Link load balancing is an excellent multi-homing solution and has many benefits over BGP-based solutions. Link load balancing solutions can provide more than just the high availability benefits of BGP. Link load balancing does not suffer from the failover latency inherent in BGP-based solutions. Link load balancers are transparent to users and significantly easier to engineer and manage than BGP multi-homing. Link load balancers provide true load balancing of multi-homed links, and sophisticated link load balancers offer high availability, link optimization, and persistency (required for applications to assure traffic for the same client in the same session always traverses over the same ISP link).

The next section covers how link load balancing can provide more than high availability by optimizing the utilization of multi-homed networks.

Utilization

Without the ability to manage and prioritize traffic based on business policies and link health, a multi-homing solution can provide high availability, but does not guarantee the most cost-effective and maximum link performance. Nortel Networks Alteon Link Optimizer provides the capability to prioritize traffic so that high value-add applications get the network resources required to optimize their use. The Alteon Link Optimizer uses Dynamic Data Path (DDP) technology to monitor the health and performance of the data path while simultaneously inspecting and classifying packets using information such as TCP port. DDP allows the Alteon Link Optimizer to dynamically alter the data path for traffic. This capability provides the ability to send traffic to the healthiest or highest performing links, increase network efficiency and performance, seamlessly integrate multi-homing, and apply different service levels to traffic based on attributes such as application, user, and user access device. DDP allows flexible adaptation of the network to achieve business requirements instead of adjusting business applications to compensate for network limitations. Many user selectable load balancing algorithms can be employed with DDP to ensure that each link is utilized most

cost effectively. These algorithms include Least Connections, Round Robin, Weight-based, Bandwidth, Response Time, etc. Using these metrics, enterprises can choose to balance traffic based on their unique business needs. For example, traffic can be load balanced based on the relative cost of links, the capacity of links, or simply in a round robin fashion.

Bandwidth management support is a key feature for link load balancers. Bandwidth rate limiting complements standard load balancing algorithms by attempting to ensure that applications receive the bandwidth required to maximize performance. The Alteon Link Optimizer provides bandwidth rate limiting contracts. For each contract, an administrator associates an application with a predefined maximum bandwidth. Utilizing bandwidth rate limiting enables enterprises to ensure that important applications such as VoIP, CRM databases, ordering tools, online engineering tools, etc. have reserved bandwidth, while other less important applications such as online backups only use ISP bandwidth upon availability.

Bandwidth contracts can be assigned in a variety of ways. Administrators can assign contracts on a per application basis, per port basis, per VLAN basis, and per source IP basis. The administrator can also define bandwidth allocation per individual ISP link. For example, administrators can assign 5 Mbps of bandwidth to VoIP applications that utilize ISP link number one, and 10 Mbps of bandwidth for VoIP traffic that utilizes ISP link number two. Similarly, bandwidth can also be assigned irrespective of the ISP links traversed. For example, administrators can assign 15 Mbps of total aggregate traffic allotment for VoIP, where the determination of which ISP link handles the traffic is left up to the Alteon Link Optimizer—ensuring that the total bandwidth allocated does not exceed 15 Mbps. The key to bandwidth rate limiting is to ensure that high value-added and latency sensitivity applications always receive priority in a bandwidth restricted environment.

The standard network configuration for the Alteon Link Optimizer is shown in *Figure 2*. This figure contains an example of an enterprise that has established three ISP links to the Internet. Using the Alteon Link Optimizer, link performance is maximized as traffic is load balanced across all three links. The Alteon Link Optimizer regularly checks the health and performance of upstream routers. When traffic enters or leaves the enterprise, the Alteon Link Optimizer routes the traffic across the optimal link on a per session basis. Making traffic management decisions on such a granular basis can be crippling to link load balancers that don't have extremely high performance architectures.

The Alteon Link Optimizer combines the load balancing intelligence of award-winning and market-leading Alteon Switches with a fast packet processing engine built on mature Alteon distributed processing ASIC technology. This architecture is referred to as the Alteon Virtual Matrix Architecture (VMA) and enables a high-performance distributed processing architecture with the resource aggregation and the flexibility of a centralized architecture. All processing and memory resources on the switch are applied to ports handling the traffic as needed. This means no single processor will be overloaded with all traffic, even if that processor is supporting all the ports with traffic. Alteon VMA also prevents network engineers from being required to provision the network to

Figure 2. Common Alteon Link Optimizer network architecture

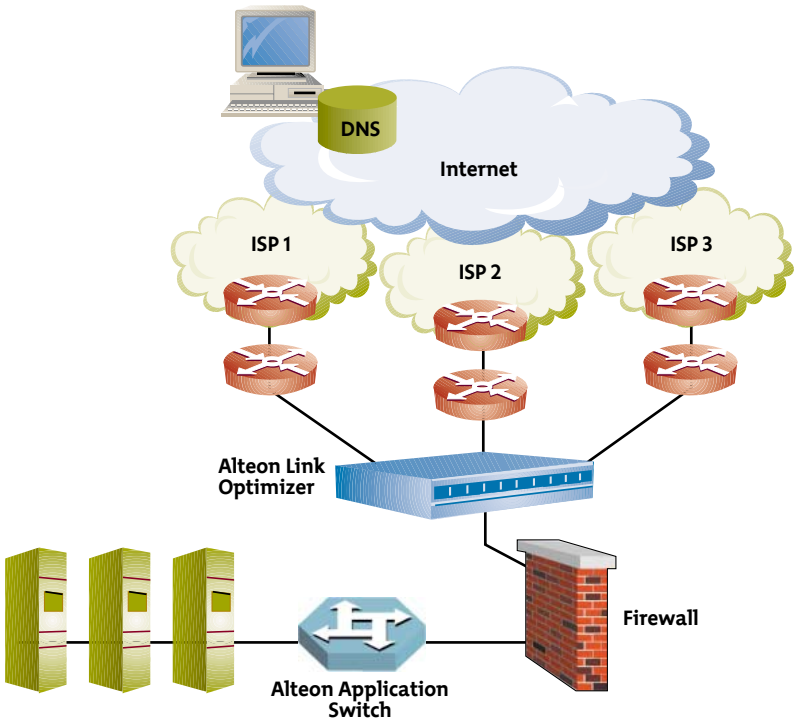
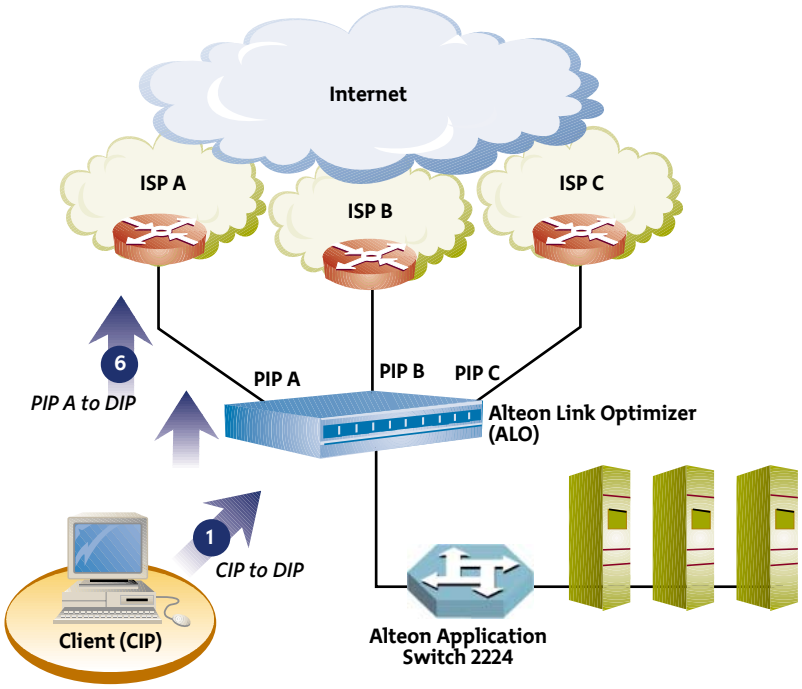


Figure 3. Outbound link load balancing traffic flow diagram



Outbound load balancing steps

1. Client makes a request to destination IP (DIP).
2. ALO monitors links A, B, and C.
3. ALO measures the link condition of A, B, and C.
4. ALO chooses link A as the best link.
5. ALO source NATs the request to Port IP A (PIP A).
6. ALO sends the request to DIP using PIP A.
7. DIP responds to PIP A.
8. ISP A handles the packet and forwards to ALO.
9. ALO reverse NAT by converting PIP A to CIP.

balance traffic levels entering Alteon Link Optimizer ports. The Alteon Link Optimizer allocates processing power in real time to ports that need it the most. Therefore, VMA simplifies network provisioning.

The Alteon Link Optimizer is a solution leading link load balancer that provides dual mode link load balancing. Dual mode assures that both inbound and outbound traffic is load balanced. Without dual mode link load balancing, a link load balancer is only managing the utilization of traffic flowing one way across multi-homed connections. Single mode link load balancers only provide half the utilization benefit and ROI that an enterprise should expect.

Outbound traffic optimization

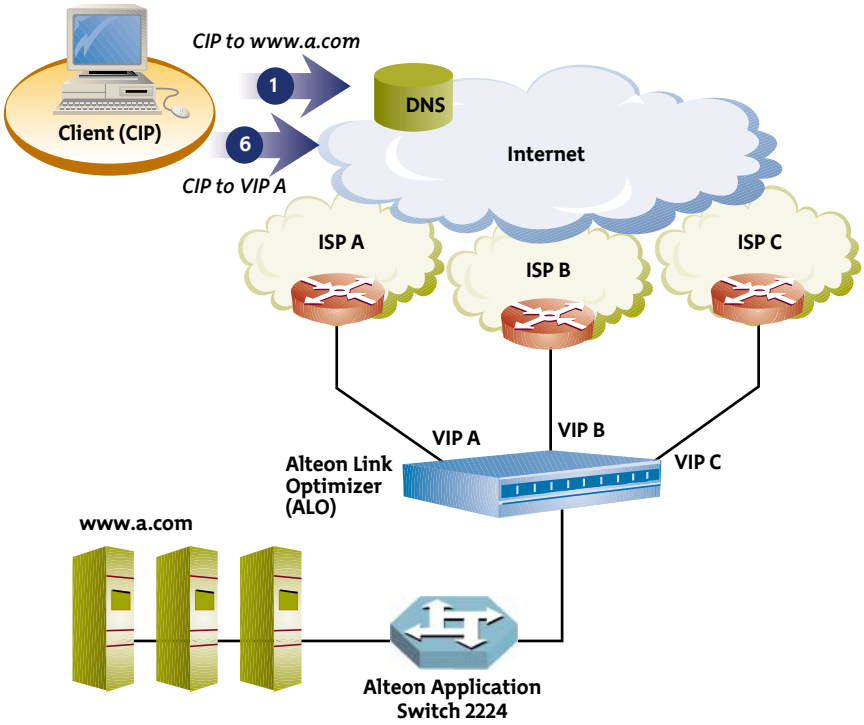
As outbound traffic (traffic initiated from inside the network) traverses out of the enterprise, the Alteon Link Optimizer determines which is the optimal ISP link to carry the packet. After this determination, the Alteon Link Optimizer changes the source IP address of the packet to match the address range of the ISP that hosts the link the traffic will traverse. By modifying the source IP address of the packet, link persistency (ensuring that outbound traffic and inbound traffic take the same ISP path, required for certain stateful firewalls, etc.), is maintained. The measurement of the optimal ISP link to forward traffic is determined on a sliding average weighted window designed to ensure that the best link is always chosen and short term transient issues are not considered. This symmetric flow is designed to ensure that each ISP handles both the ingress and the egress portion of the session. The Alteon Link Optimizer checks each upstream router regularly to ensure that the router can properly handle traffic and dynamically adjusts traffic flow in reaction to network conditions. *Figure 3* provides a detailed step-by-step view of how outbound link load balancing works.

Outbound load balancing is most heavily utilized within enterprises with a significant amount of their traffic originating within their network. This is typical of enterprises with a large employee base.

Inbound traffic optimization

When a client on the Internet makes a request to retrieve content from an enterprise (for example, client requesting product information on the corporate www.a.com sales catalogue page), traffic carrying the request to the enterprise can take different paths depending on a number of factors. The Alteon Link Optimizer initiates control of the path that the inbound traffic traverses by acting as an intelligent authoritative domain name server (for example, in this case, www.a.com). When the client located in the Internet makes a request to www.a.com to retrieve the product information, the client first makes a query to its local DNS table to resolve the IP address. If the local DNS does not have the entry for www.a.com, the local DNS asks a

Figure 4. Inbound link load balancing traffic flow diagram



Inbound load balancing steps

1. Client (CIP) makes a request to www.a.com.
2. Local DNS does not have www.a.com in its DB.
3. DNS queries the Authoritative Domain NS (ADNS); ALO acts as ADNS.
4. ALO monitors the link of ISP A, B, and C.
5. ALO measures the link of ISP A, B, and C.
6. ALO responds with the best VIP selection, VIP A.
7. Client makes the request to www.a.com to VIP A.
8. Servers respond with the content by sending via ISP A.
9. RTS feature allows the traffic to return via ISP A.

higher authority DNS for resolution assistance. Eventually, it is the authoritative domain name server that provides the IP address associated with the URL in the client request. The Alteon Link Optimizer in its role as the authoritative DNS will resolve the DNS request with an 'optimized' IP address. The resolution of this 'optimized' IP address is determined by administrator set link load balancing policies. The 'optimized' IP address is an address associated with the address range of the ISP that hosts the link the Alteon Link Optimizer has determined is the optimal link for the inbound traffic to traverse. The DDP load balancing algorithms used to select the optimal link periodically measure link conditions and provide the optimal IP address to the local DNS table.

To achieve ISP link persistency, a special algorithm is performed by the Alteon Link Optimizer port that carries the inbound traffic. This algorithm performs a "Return to Sender" function. The Return to Sender capability creates a session on the Alteon Link Optimizer when traffic enters the switch. When the response to the initial request returns to the client, the Alteon Link Optimizer will intelligently return this traffic to the ISP that originated the traffic. This intelligent persistence is designed to ensure that stateful sensitive protocols and devices (firewalls, etc.) are not disrupted and appropriate metering is negotiated with each traffic-carrying ISP link. *Figure 4* highlights key packet flows for inbound load balancing.

Inbound load balancing is most heavily utilized within enterprises with a significant amount of their traffic originating outside their network. This is typical of companies with large numbers of road warriors and telecommuters, significant extranet related partner relationships, or a significant Web-based business model.

Security

While multi-homed connections implemented through a link load balancing architecture can provide high availability and maximize link utilization, they are still susceptible to security threats. Security threats such as Denial of Service (DoS) attacks can rob enterprise networks of bandwidth and even bring network access to a screeching halt. Leading edge link load balancers provide the first line of perimeter security for enterprise networks. They can even enhance the performance of firewalls by offloading tasks such as Network Address Translation, Denial of Service protection, and filtering. The Alteon Link Optimizer provides the first line of network defense by utilizing sophisticated multi-layered security including Denial of Service and application abuse protection, port mirroring, access lists, filtering, NAT, and Intrusion Detection System load balancing.

Protection from application abuse is a key feature of the Alteon Link Optimizer. This enables the Alteon Link Optimizer to monitor the use of all enterprise services, thus protecting network resources from external and internal threats. For example, this feature can be used to thwart disgruntled ex-employees who might write application scripts to gain access to unauthorized areas of the network, such as payroll services.

Intrusion Detection Systems (IDSs) are an important component of network security. The Alteon Link Optimizer IDS load balancing feature eliminates the inherent lack of scalability and throughput limitations of IDSs. This feature balances loads across IDSs and is designed to ensure server availability via health checking. Multiple IDS servers can operate in parallel. All session entries are maintained and all frames of a given session are forwarded to the same IDS server. An administrator can use this feature to support multiple IDS vendors simultaneously and allow the use of optimal vendors for specific threats. Traffic can be sent simultaneously to each system. An example where utilizing multiple IDS vendors is valuable would be utilizing an off-the-shelf IDS for inspecting and alerting of network intrusions; another IDS for detecting application intrusions.

The Alteon Link Optimizer includes Network Address Translation and extensive filtering capabilities ranging from IP addresses to Layer 4. Filters can be configured to allow or deny traffic according to various IP address, protocol, Application, and Layer 4 port criteria. While not a substitute for a firewall in most cases, filtering provides added protection against unwanted traffic.

Alteon Link Optimizers can thwart Denial of Service attacks or TCP SYN attacks without blocking valid session requests. Through "delayed binding" the Alteon Link Optimizer intercepts client SYN requests before they reach the server. The Alteon Link Optimizer then responds to the client with a SYN ACK that contains embedded client information and does not allocate a session until a valid SYN ACK is received from the client or the three-way handshake is complete. By temporarily terminating each TCP connection until content has been received, the Alteon Link Optimizer prevents the server from being inundated with SYN requests. Half-open sessions are a result of an incomplete three-way handshake between the server and client. To detect SYN attacks, Alteon Link Optimizers enable tracking of the number of new half-open sessions over a set period of time. If the value exceeds a specified threshold, the Alteon Link Optimizer alerts the administrator of the DoS attack.

Multi-homing evaluation criteria

When evaluating multi-homing architecture solutions, several things should be considered. An effective multi-homing solution is one that maximizes link utilization, and provides perimeter security plus high availability. Implementation and management of multi-homing can be very complicated. To simplify multi-homing, link load balancing solutions are preferred over BGP. When choosing a link load balancing solution, a feature-rich product with many link load balancing algorithms is favored because it allows administrators the flexibility to optimize link load balancing to meet individual business priorities. Due to the demanding nature of optimizing traffic distribution at hundreds of megabits per second and solution placement at the gateway to a network, the performance of link load balancing solutions is very critical. High-performance architectures like the Alteon Link Optimizer's VMA distributed processing engine provide the wire speed processing required to optimize multi-homed links without adding latency. Given the network perimeter placement of multi-homed solutions, integrated security is a requirement. This integrated security provides a first defense to network intrusion and can negate performance impacting security threats.

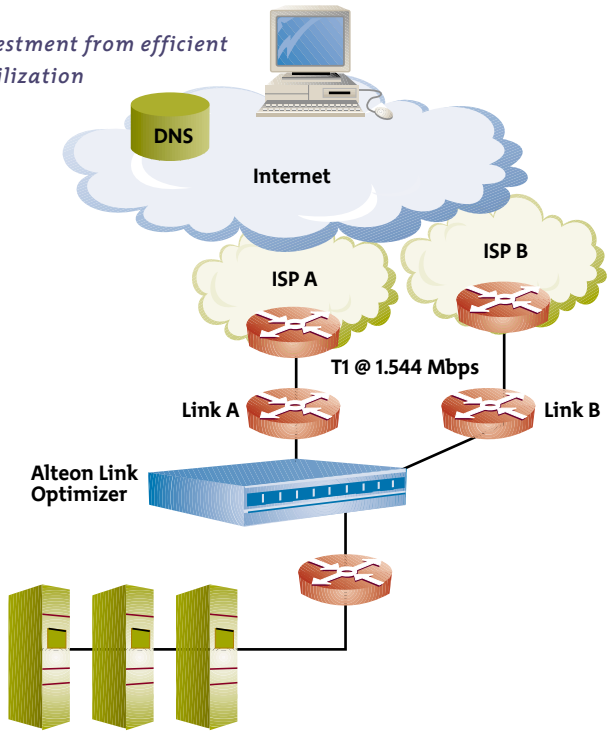
Business case

The Alteon Link Optimizer supports several business cases that increase network ROI from Opex savings based on enhanced bandwidth utilization to ISP link flexibility. Below are several examples of business cases that justify utilizing an Alteon Link Optimizer.

Opex savings from efficient bandwidth utilization

Many enterprises overprovision the bandwidth they need in an attempt to obtain a predictable fixed cost instead of purchasing burstable links that increase in cost as usage spikes. Utilizing an Alteon Link Optimizer allows the enterprise to purchase burstable links, control bandwidth spikes, and obtain a fixed monthly charge. This is accomplished by

Figure 5.
Return on investment from efficient bandwidth utilization



An enterprise has redundant Internet connectivity through dual ISP links with overusage protection from ISP A

Bandwidth cost of non-optimized solution

Link A: ISP A - T1	$1,000/month
Link A: ISP A - Overuse charge	$1,300/month
Link B: ISP B - T1	$1,100/month
Total bandwidth charge/month	$3,400
Total bandwidth charge (2 years)	$81,600

Alteon Link Optimizer removes costly bandwidth overuse charges

Bandwidth cost with Alteon Link Optimizer

Link A: ISP A - T1	$1,000/month
Link B: ISP B - T1	$1,100/month
Total bandwidth charge/month	$2,100
Total bandwidth charge (2 years)	$50,400
Cost savings (2 years)	$31,200
Cost of Alteon Link Optimizer	$9,595

2 year ROI (($31,200/$9,595) -1)) = 225%

Payback period = 7.5 months

managing bandwidth and fully utilizing ISP links without costly bandwidth spikes. *Figure 5* shows an example of an enterprise leveraging an Alteon Link Optimizer and generating greater than 200 percent ROI in less than 2 years with a 7.5 month payback.

Opex savings from simplifying multi-homing deployment

One of the simplest ways to save money is to avoid spending it. An Alteon Link Optimizer deployment implements multi-homing through link persistency, address management, and DNS support. It negates the need to implement a complicated BGP based multi-homing solution because the Alteon Link Optimizer does not require an Autonomous System Number (ASN) for multi-homing. BGP-based multi-homing can also introduce significant latency in routing traffic. The Alteon Link Optimizer dynamically routes traffic, utilizing DDP, over WAN links with sub-second redirection based on a full set of user selectable traffic management algorithms. The Alteon Link Optimizer's simplification of multi-homing is designed to generate significant administrative cost savings.

Opex savings and revenue enhancement from application and network high performance/availability

When your network is performing poorly or is down, your applications are down and this costs money and impacts revenue generation. Through load balancing, bandwidth management, and health checking, the Alteon Link Optimizer removes single points of failure and can greatly improve the performance and availability of network links so that your business productivity isn't impacted by network performance interruptions.

Lower Opex through ISP link flexibility

Utilizing the Alteon Link Optimizer allows previously idled backup WAN links or trunked combinations of inexpensive WAN links to carry traffic instead of a single expensive link. This flexibility can greatly reduce the expense and enhance the availability of network connections.

The Alteon Link Optimizer-Link load balancing solution

Nortel Networks Alteon Link Optimizer family of switches was designed to provide high availability capabilities to enterprises facing the challenges of providing continuous uptime within multi-homed networks. The Alteon Link Optimizer comes in two models. The Alteon Link Optimizer 143 provides Fast Ethernet connectivity and the Alteon Link Optimizer 150 provides Gigabit connectivity concurrently to multiple ISP Internet links.

The Alteon Link Optimizer:

- *Helps ensure fail-safe business continuity by efficiently load balancing multiple WAN links and providing link failover.* Constant link monitoring ensures availability, bypassing unhealthy links when distributing new sessions and automatically re-enrolling them upon service restoration. Link outages become transparent to users.
- *Improves business productivity and simplifies operations by optimizing WAN links for application performance.* The Alteon Link Optimizer greatly simplifies the deployment of multi-homing by providing link persistency, address management, and DNS support. It negates the need to implement a more complicated BGP solution. Utilizing a full set of load balancing and health checking algorithms along with bandwidth rate limiting helps ensure that applications and client access receive the network resources needed to maximize productivity.
- *Protects applications and networks with multi-layer security.* The Alteon Link Optimizer provides the first line of network defense by utilizing sophisticated Denial of Service and application abuse protection, port mirroring, access lists, filtering, and Intrusion Detection System load balancing.
- *Scales business applications and network capacity efficiently without downtime.*
- *Maximizes return on IT investment* by allowing enterprises to use existing infrastructure more efficiently, simplify network design, provide security and scalability, and adjust the network quickly to meet rapidly changing business requirements. Utilizing previously idled backup WAN links or trunked combinations of less expensive WAN links can greatly reduce expenses and enhances the availability of network connections. Pay as you go functionality—upgrade Alteon Link Optimizers to full Alteon Web Switch functionality (server load balancing, VPN load balancing, etc.).

Alteon Link Optimizer Technical specifications

Alteon Link Optimizer	143	150
Total ports	9	9
10/100 Ethernet ports	8	8
Gigabit Ethernet ports (1000Base-SX)	1	8+1
Concurrent sessions	336,000	336,000
Sessions per second	24,000 *	24,000 *
IP routing interfaces	256	256
Policy filters	224	224
VLANs	246	246
Default gateways	250	250
Trunk groups	4	4
Switch capacity	8 Gbps	8 Gbps
Height	3.47 inches (2-RU)	3.47 inches (2-RU)

**"Real-world" testing scenarios with zero packet loss*

The Alteon Link Optimizer provides much higher performance and the broadest set of value-add features of any competing product. These features include, but are not limited to, IDS server load balancing, bandwidth management (rate limiting), Application Abuse Protection, and SYN Attack Alarms. The Alteon Link Optimizer is 40 to 80 percent less expensive than competitive products.

Summary

Today's business-critical applications demand highly available application optimized networks to ensure they provide maximum value to the enterprise. Multi-homed networks are a significant component to ensuring that WAN and Internet access is always available. Implementing multi-homed networks without sophisticated load balancing can cause WAN and Internet links to be significantly underutilized.

Nortel Networks Alteon Link Optimizer simplifies multi-homing networks and helps ensure maximum utilization and ROI from high availability ISP link investments. The Alteon Link Optimizer provides these benefits by utilizing intelligent traffic management, bandwidth rate limiting, and health checking to optimize the availability and utilization of multi-homed network connections. The Alteon Link Optimizer also provides sophisticated integrated security such as Denial of Service protection, Application Abuse Protection, access lists, filtering, and Intrusion Detection System load balancing.

In the United States:
Nortel Networks
35 Davis Drive
Research Triangle Park, NC 27709
USA

In Canada:
Nortel Networks
8200 Dixie Road,
Suite 100
Brampton, Ontario L6T 5P6
Canada

In Caribbean and Latin America:
Nortel Networks
1500 Concorde Terrace
Sunrise, FL 33323
USA

In Europe:
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead Berkshire SL6 3QH
UK

In Asia:
Nortel Networks Asia
6/F Cityplaza 4,
Taikooshing,
12 Taikoo Wan Road,
Hong Kong



Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The Company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global Company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at:

www.nortelnetworks.com

For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

*Nortel Networks, the Nortel Networks logo, the globemark design, and Alteon are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2003 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

NN102801-010203