

Designing a

resilient

network

Technical Brief

Split Multi-Link Trunking Passport 8600

Market requirements for a resilient network

Unplanned network outages can affect all aspects of a business. Lost sales, increased overtime, loss of employee productivity, and even declining customer loyalty can be attributed to issues surrounding network outages. The current business environment is more competitive than ever. Any company that possesses even a slight advantage whether with collaborative applications or customer relationship management tools can dominate a market. Now more than ever, companies are looking for a competitive edge.

Business-critical applications are greatly affected by network outages. An unreliable network does not allow applications like IP Telephony to provide the benefits they were designed to provide. When applications on the network don't perform as expected, service issues can quickly become overwhelming. Converged applications can, and usually do, require predictable response times. Call servers, IP phones, and gateways all possess requirements for network uptime and network quality of service. Properly designed network solutions can minimize the risk of network downtime and alleviate convergence application apprehension.

Integrating network resiliency into core networking devices can provide a manageable solution to a growing problem. By incorporating resiliency into the network core, user access points can remain connected to the network even in the event of a failure. By ensuring the availability of the network, core converged applications can provide the services and benefits they were designed to without impediments.

Technology solutions

Routing protocols inherently provide a basic level of resiliency. The ability to “route” around problem areas defines the efficiency of a routing protocol. However, the time to re-converge the network can vary greatly depending on the protocol being used; for example, routing protocols including RIP and OSPF can take anywhere from seconds to minutes to establish a new route after a failure.

Equal Cost Multi-Path Routing (ECMP) provides multiple routed paths to an end destination; however, designing a network with truly equal cost paths greatly increases the complexity of the network design and often times is not possible.

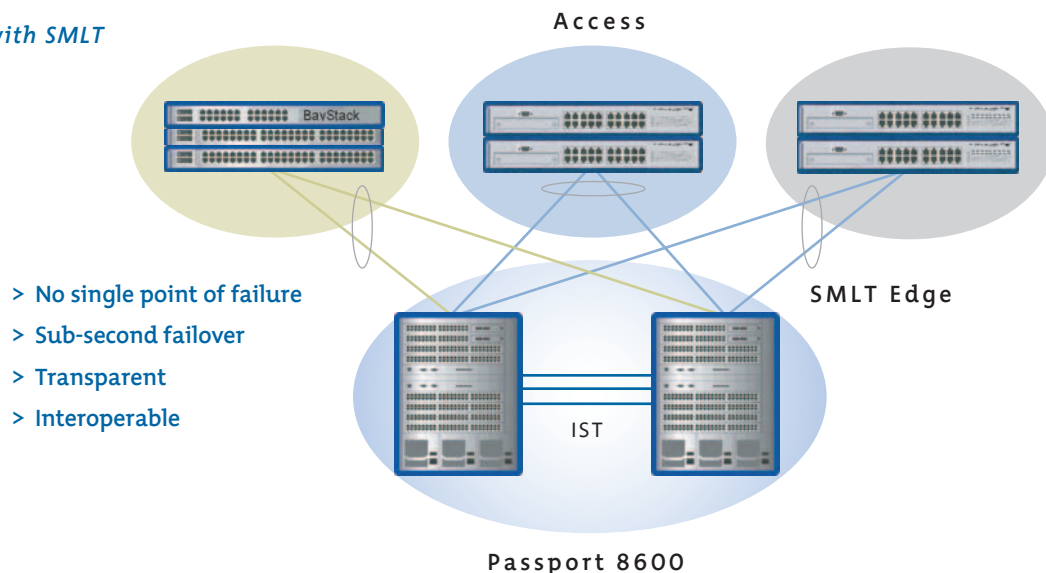
Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure that can occur when the single static default gateway router for an end station is lost. VRRP introduces the concept of a virtual IP address, which provides a dynamic default gateway redundancy in the event of failover. However, VRRP can take up to 3 seconds to reconverge after an outage, and up to 90 seconds when used with other routing protocols. Converged applications can begin to fall apart as network delays increase.

Split Multi-Link Trunking (SMLT) is a Nortel Networks architecture that helps eliminate single points of failure and creates multiple paths from user access switches to the core of the network. Compatible with 802.3ad, SMLT does more than prevent network loops. SMLT provides an architecture to design resiliency directly into the network. It also works to reroute failures as quickly as possible. In most cases, network reconvergence is sub-second.

Nortel Networks SMLT is an extension to the IEEE 802.3ad link aggregation specification. SMLT avoids loops due to its superior enhanced link aggregation-control protocol. If 802.1d is used, multiple Spanning Tree groups are required and VLANs must be manually assigned to those groups—all of which makes ongoing administration and troubleshooting extremely complex.

With SMLT it is no longer necessary to use the Spanning Tree protocols to design resilient networks. SMLT provides much faster convergence times than Spanning Tree (typically one second versus 30 to 60 seconds). SMLT also eliminates the blocking of ports by Spanning Tree protocols, thus increasing network bandwidth since all links in a trunk can be utilized for forwarding traffic.

Figure 1. Reliability with SMLT



SMLT allows two aggregation switches to appear as a single device to dual homed switches. The aggregation switches make use of an InterSwitch Trunk (IST) over which they exchange information, permitting rapid fault detection and forwarding path modification. To achieve network element protection, SMLT extends link aggregation to allow dual homing of IEEE 802.3ad attached devices. Both of the dual homed connected devices are active and pass traffic. This architecture provides twice the available bandwidth of merely using the Spanning Tree Protocol.

SMLT improves the reliability of a Layer 2 network operating between the user access switches in a building and the network center aggregation switch, as well as with the connections to multi-homed servers. It does so by providing load sharing among all available links and fast failover in the case of a link or core switch failure.

Routed Split Multi-Link Trunking

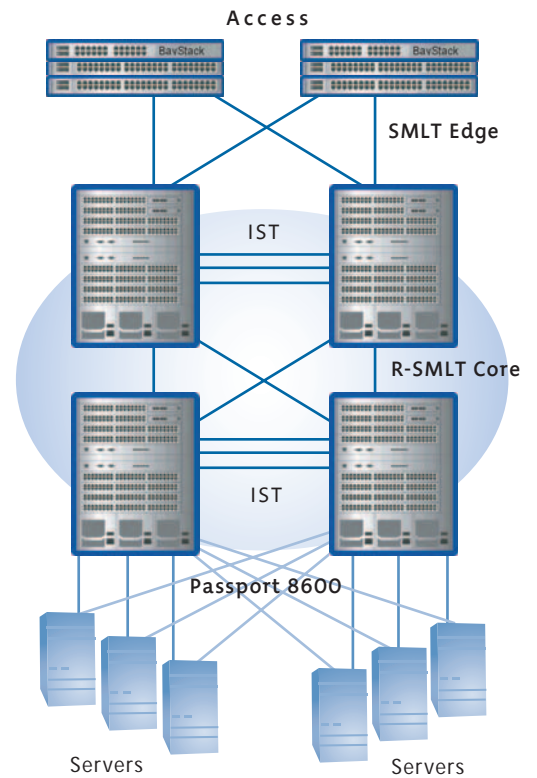
Routed SMLT (R-SMLT) is an extension of the Split Multi-Link Trunking architecture, providing sub-second failover for routed core networks using Layer 3 routing protocols such as RIP, OSPF, and BGP. R-SMLT brings resiliency to the network core similar to the way SMLT brings resiliency to the network edge. Two Passport 8600s operate as one logical unit within the network core, allowing all connections to the network core to be utilized. In addition, each unit provides backup for the other. R-SMLT and SMLT look beyond merely eliminating network loops and provide an architecture to design for network resilience.

R-SMLT extends the reliability of SMLT to routed core networks. By providing sub-second failover for Layer 3 information, R-SMLT ensures converged applications are viable and maintainable throughout the network. This sub-second IP data recovery solution provides the first resiliency solution for IPX traffic in the SMLT network. R-SMLT with SMLT provides a complete Layer 2 and Layer 3 resiliency solution that spans the network end-to-end.

Choosing the right technology solution

Other vendors implement resiliency protocols into their switches. Some use a pure standards approach with VRRP and ECMP providing the bulk of the resiliency services. Unfortunately, these protocols rarely meet the resilient bandwidth requirements for converged applications like IP Telephony. VRRP can have recovery times measured in minutes as opposed to seconds and can be difficult to implement. Some vendors are developing their own proprietary solutions that work solely with their own products. These solutions can only work in a single vendor environment and become very complicated as remote sites and users are added.

Figure 2. Reliability with R-SMLT



- > Sub-second failover
- > Transparent
- > Fully automatic
- > Routed resiliency



Nortel Networks SMLT architecture provides a fully resilient 802.3ad compatible network core with the ability to support multiple vendors in the wiring closets or access points. SMLT does not require special hardware or complicated configurations. In addition to providing the most advanced resilient solution, SMLT can increase the available bandwidth from the wiring closet to the network core by merely enabling a software feature. Connections that were once unused due to Spanning Tree's loop protection can now be used to their highest potential.

With the blossoming of converged applications throughout the network, resiliency has never been more critical. Applications like IP Telephony, multicast, and e-learning present valuable business benefits; however, without adequate bandwidth and network resiliency these applications can't perform their tasks. With SMLT, the ability to provide a return on investment from a resiliency feature has never been more pronounced.

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 are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 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.

NN107680-031804

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
6/F Cityplaza 4
Taikooshing
12 Taikoo Wan Road
Hong Kong

NORTEL
NETWORKS
BUSINESS WITHOUT BOUNDARIES