

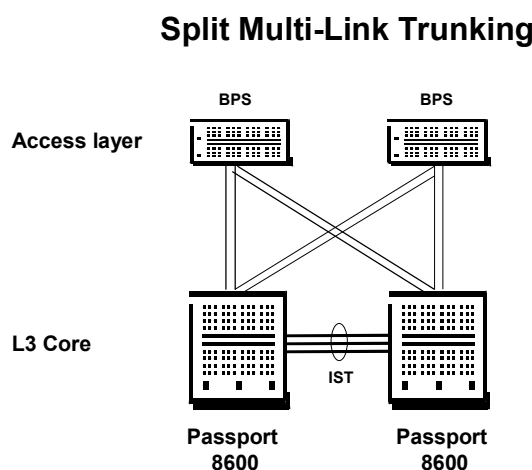
Passport 8600 Split Multi-Link Trunking Frequently Asked Questions

FAQs

This document answers the most frequently asked questions concerning the Split Multi-Link Trunking feature for the Passport 8600.

1. What is Split Multi-Link Trunking (SMLT)?

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. It also works to reroute failures as quickly as possible. Building on the redundancy offered by Nortel Networks DMLT (Distributed MLT), SMLT improves network redundancy and resiliency even further by dual homing edge switches to a pair of aggregation or core switches.



2. What are the benefits of SMLT?

SMLT improves the reliability of a layer 2 (L2) network operating between a building's user access switches and the network center aggregation switch. It does so by providing load sharing among all the links and fast fail over in case of link failures.

SMLT provides much faster convergence than Spanning Tree (typically one second versus 30-60 seconds). SMLT also eliminates the blocking of ports, thus increasing network bandwidth, since all trunks between switches can be utilized for user traffic (with Spanning Tree this requires the use of multiple spanning tree groups, making troubleshooting extremely complex).

3. What are the components of SMLT?

SMLT aggregation switch

A switch that connects to multiple wiring closet switches, edge switches or CPE devices, typically within a single building. An SMLT aggregation switch shares an IST link with another SMLT capable switch to form a redundant core.

Inter Switch Trunk (IST)

One or more aggregated parallel point-to-point links that connect two aggregation switches together. The two Aggregation switches utilize this channel to share information so that they may operate as a single logical switch for bridging.

Split Multi-Link Trunk (SMLT)

A Multi-Link Trunk, which is, split between two Aggregation switches.

SMLT Client

A switch, capable of link aggregation, located at the edge of the network, such as in a wiring closet or CPE.

SMLT ID

An ID that is shared between the two SMLT aggregation switches connecting to one SMLT client. Each SMLT client requires a new SMLT id.

4. Where would I use SMLT?

In LAN aggregation points (e.g. a building basement where two switches are used to distribute connections to each floor); a campus LAN backbone (where two core switches are used to aggregate the connections from each building); and/or a server farm where two switches are used to provide redundant server connections.

5. What products support SMLT?

SMLT code is supported on Passport 8600 Routing Switches. It was released as part of v3.2 software.

6. Is SMLT available for the BayStack and BPS2000?

SMLT is not required on the edge switches (SMLT client switches), only on the core Routing Switches (SMLT Aggregation switches). One end of a SMLT trunk **MUST** be a Passport 8600; the other end can be any Layer 2 switch that support MLT (e.g. BayStack, BPS, Centillion, Passport 8100, Passport 8600 etc.).

7. Does SMLT work with non-Nortel products?

Yes. Layer 2 switches that interoperate with Multi-Link Trunking (MLT) will work with SMLT.

8. Does SMLT with work Cisco's Fast EtherChannel?

SMLT has been tested with and works with Fast EtherChannel in most instances.

9. Can I use SMLT with servers?

Yes. Servers using a Network Interface Card (NIC) that is interoperable with MLT will work with SMLT.

10. Do I still need Spanning Tree?

Spanning Tree Protocol (STP) is disabled on the SMLT ports (e.g. disable STP on all core switches using SMLT AND all edge switches connected to those core switches).

11. How does it compare to competitors' offerings?

Other vendors have proprietary Spanning Tree 'enhancements' on their Layer 2 switches. These modifications improve the convergence time for Spanning Tree, but do not allow blocked ports to be used for user traffic unless multiple spanning tree groups are used (increases complexity). Convergence times may be as low as 5 seconds, but are still much slower than SMLT. These schemes are proprietary and require the software feature to be supported on all switches in the network, thus they only work in single vendor environments.

12. What's special about the IST?

The IST allows the two core switches to share forwarding tables, making them appear to the edge switches or servers as a single core switch using a 'normal' MLT trunk.

13. How are failures detected?

Link failures are detected by the LOS (loss of signal) mechanism on the SMLT links. The LOS of an SMLT link is exchanged between the SMLT aggregation pair through the IST protocol... Edge switches also detect failure of a trunk to the core switches using the standard MLT algorithm. Nortel Networks recommends enabling Auto-Negotiation on Gigabit Ethernet links to enable Remote fault indication, which is part of IEEE 802.3z. This will allow the detection of single-fiber failures.

14. How fast does it converge?

SMLT typically converges in less than one second, but is dependent on the edge switch fail over mechanism. If a one second ping trace is used for testing, expect to see either no pings lost or a single ping lost when a link is broken or a core switch is powered off.

15. What happens if the IST fails?

The IST is a critical element of SMLT, allowing exchange of forwarding tables between the core switches. If the IST fails, the forwarding tables for single-attached devices (e.g. a server which is attached to only one of the core switches) may become inaccurate and network problems may occur on that device. The IST should be protected from failures by using multiple ports on different slots in each core switch (Distributed MLT) and diversely routed fiber cabling. Up to 8 separate fibers and 8 separate ports on each core switch can be grouped together to form the IST. Edge switches and servers should be dual-homed to both core switches to avoid possible impact of an IST failure.

16. Can I use more than two SMLT aggregation switches?

Yes. You can do so by interconnecting them using a square or a full-mesh configuration. All links between the two sets must be of type SMLT and must have the same SMLT ID.

17. Are there any scaling limitations?

Yes. SMLT uses MLT groups and there is a limit of 32 MLT groups per switch. An IST uses one MLT group. A pair of core switches can support up to 31 edge switches.

18. Does SMLT work for protocols other than IP?

Yes. SMLT is a Layer 2 technology and is protocol independent for Layer 3 protocols such as IP, IPX, AppleTalk etc.

19. Can I use VRRP with SMLT?

Yes. SMLT is transparent to Layer 3 protocols such as VRRP. A VRRP extension for SMLT allows for VRRP active-active configurations where both SMLT aggregation switches will be forwarding/routing traffic received on SMLT links. This VRRP extension is called VRRP BackupMaster.

20. Is SMLT limited to the LAN?

No. SMLT can be used in Metro networks by using either long-haul GBICs (XD or ZX) or CWDM GBICs and Optical Add/Drop Muxes. (See SMLT/CWDM Application Note for more information).

Additional terms to know

Multi-Link Trunk (MLT)

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth.

Distributed Multi-Link Trunk (DMLT)

A group of ports (trunk) where trunk members (ports) can reside on multiple cards (modular solution) or multiple units (stackable solution) for increased redundancy and reliability.

Spanning Tree Protocol

STP is a protocol that detects and eliminates logical loops in a bridged or switched network.

21. Where can I get more information?

- Networking Concepts Guide
- Passport 8600 technical documents are located on the Nortel Networks web site:
<http://www.nortelnetworks.com/products/01/passport/8600com/index.html>

Nortel, Nortel Networks, the Nortel Networks corporate logo, the globemark design, OPTera, and Preside are trademarks of Nortel Networks. All other trademarks are the property of their respective owners.
Copyright (C) 2002 Nortel Networks Corporation. All rights reserved. Information in this document is subject to change without notice.

Nortel Networks Corporation assumes no responsibility for any errors that may appear in this document.

#####

