ProLiant Essentials Intelligent Networking Pack - Microsoft® Windows® Edition white paper

Abstract

This paper describes the ProLiant Essentials Intelligent Networking Pack advanced teaming features and how it can enhance the functionality of a network that includes HP ProLiant Servers and HP Integrity Servers. This paper is intended for IT professionals familiar with ProLiant network adapter teaming. For readers who are not already familiar with this technology, it is described in the white paper "HP ProLiant Network Adapter Teaming," which is available at this URL: http://h18004.www1.hp.com/products/servers/networking/whitepapers.html.

Introduction

The ProLiant Essentials Intelligent Networking Pack (INP) is an innovative networking product designed and developed by HP. INP enables ProLiant and Integrity servers that are running basic teaming software to adapt to and change the network path to achieve maximum reliability and performance. INP can monitor and analyze network conditions and redirect traffic to the optimum path.

To illustrate, Table 1 identifies several common causes of network disruption and the effect of the disruption in a computing environment without INP, which is loss of client access to applications. If INP is installed in the environment when any of these problems arise, however, most or all clients retain access to business-critical applications on the server.

Table 1. Common causes of network disruption

Possible Network connectivity problem	Result without Intelligent Networking Pack
Cable between the first tier switch and the core network becomes unplugged.	Clients lose access to business-critical applications on the server because the path is blocked.
Cable between the router and the NIC becomes unplugged	Clients lose access to business-critical applications on the server because the router path is blocked.
Server has ports configured for a virtual LAN (VLAN), but second tier switch has been incorrectly configured in support of the VLAN.	Clients lose access to business-critical applications because the switch cannot route traffic to the VLAN on the server.
A switch in the path to the core network crashes, experiences a firmware malfunction, or is removed for maintenance.	Clients lose access to business-critical applications because the path is unavailable, or the alternate path is very slow.
A port or a fiber connector (GBIC) beyond the second tier switch fails.	Clients lose access to business-critical applications because the path is unavailable.
A nearby device is configured incorrectly	Clients lose access to business-critical applications because the nearby device cannot be accessed

INP includes these features:

- Fast Path Failover — Allows a ProLiant or Integrity server to use the quickest available path to the core network for all server traffic.
- Active Path Failover — Allows a ProLiant or Integrity server to detect blocked paths and to redirect data along an unblocked path to the core network.
- Router Path Failover — Allows a ProLiant server to detect blocked and degraded paths to a router and to redirect data along an unblocked path to the specified router

- Dual Channel Teaming —Allows users to configure a team that spans two switches and supports receive and transmit load balancing by means of Switch-assisted Load Balancing (SLB) teams.
- Dynamic Dual Channel Teaming — Allows Dual Channel groups to be configured dynamically by selecting 802.3ad Dynamic Dual Channel Load Balancing and connecting ports to 802.3ad enabled switches.
- Discovery Protocols -- Provides information about neighboring teamed network devices and can help detect mistakes in configurations.

Note:
Not all features may be supported on the HP Integrity servers. Please check the Integrity Essentials website at http://h71028.www7.hp.com/enterprise/cache/270561-0-0-0-121.html for the latest support.

Fast Path Failover

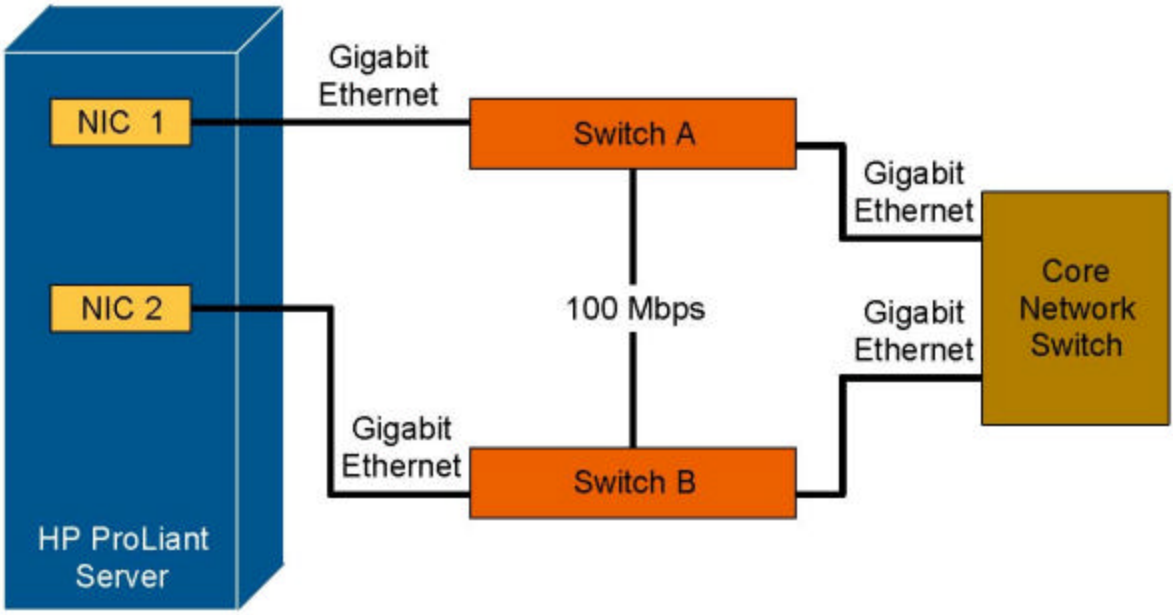
The Fast Path Failover feature of the Intelligent Networking Pack uses the failover capabilities of NIC teams, triggering a failover based on the speed of the path from team member to the destination. For example, the primary port may experience a slowdown in its path to the core network. With Fast Path Failover, this slowdown triggers a failover to a backup port in the team that has a faster path to the core network. In this way, the server always sends network communications by the fastest path to the core network available.

How Fast Path Failover works

This section describes and illustrates how Fast Path Failover works in a typical business configuration and network failover scenario.

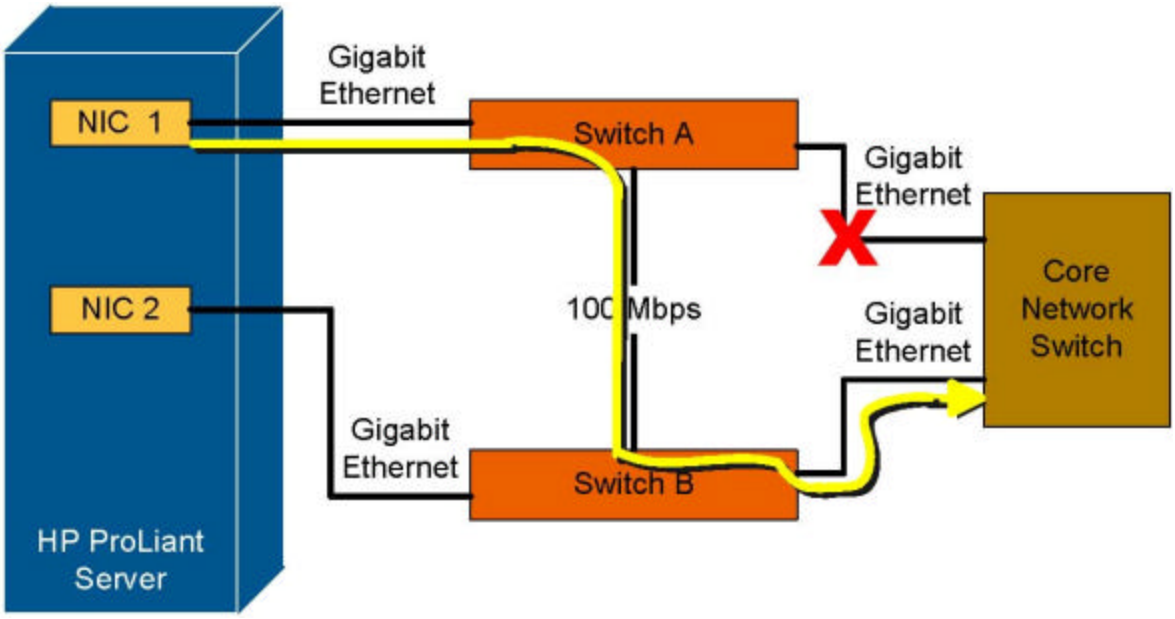
In Figure 1 below, the network has been configured for load balancing in order to use all ports, regardless of speed. Note that the ports are Gigabit speed to each switch, but the redundant link between the switches exists over a Fast Ethernet 100 Mbps line. Network traffic flows to and from the core at Gigabit speed.

Figure 1. Redundancy configuration



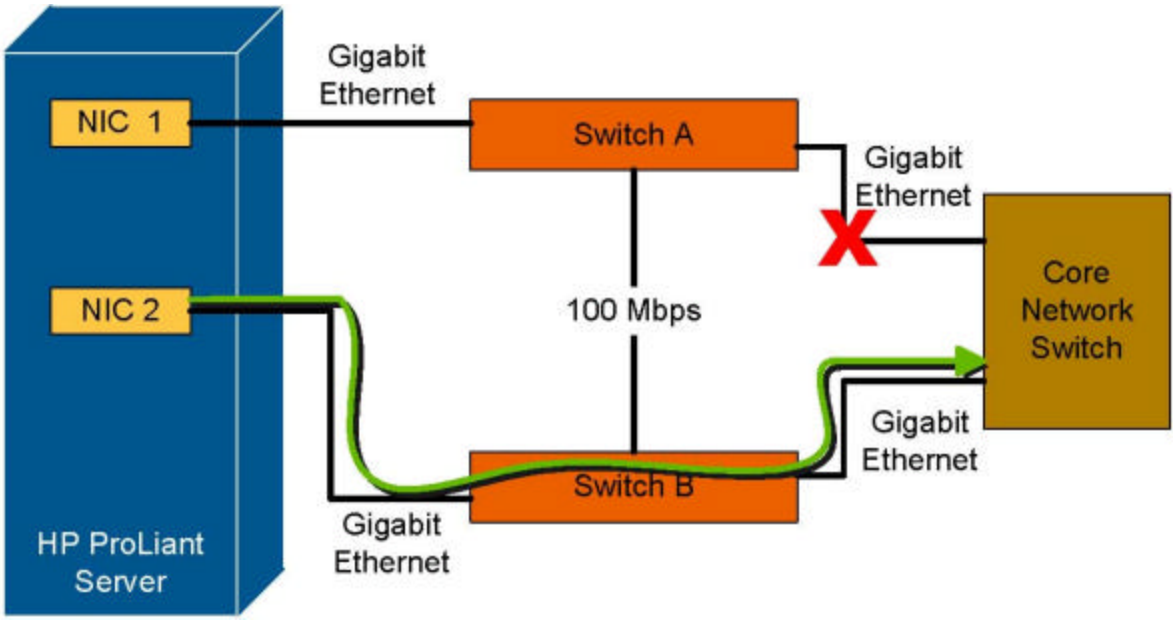
In Figure 2 below, a failure from Switch A to the network core causes traffic to be rerouted through a 100-Mbps path. Without HP Intelligent Networking software, traffic from the primary port slows to 100 Mb, and clients experience wait times.

Figure 2. Network slowdown without INP installed



In Figure 3 below, the Fast Path Failover feature of Intelligent Networking causes the now-faster backup port in the NIC team to take over as primary, and the server uses the fastest path to the network core. Network traffic flows to and from the core at Gigabit speeds, and client wait time is negligible. The failed hardware can be replaced without disrupting server traffic.

Figure 3. With the INP Fast Path Failover feature, the server uses the fastest path to the network core.



Active Path Failover

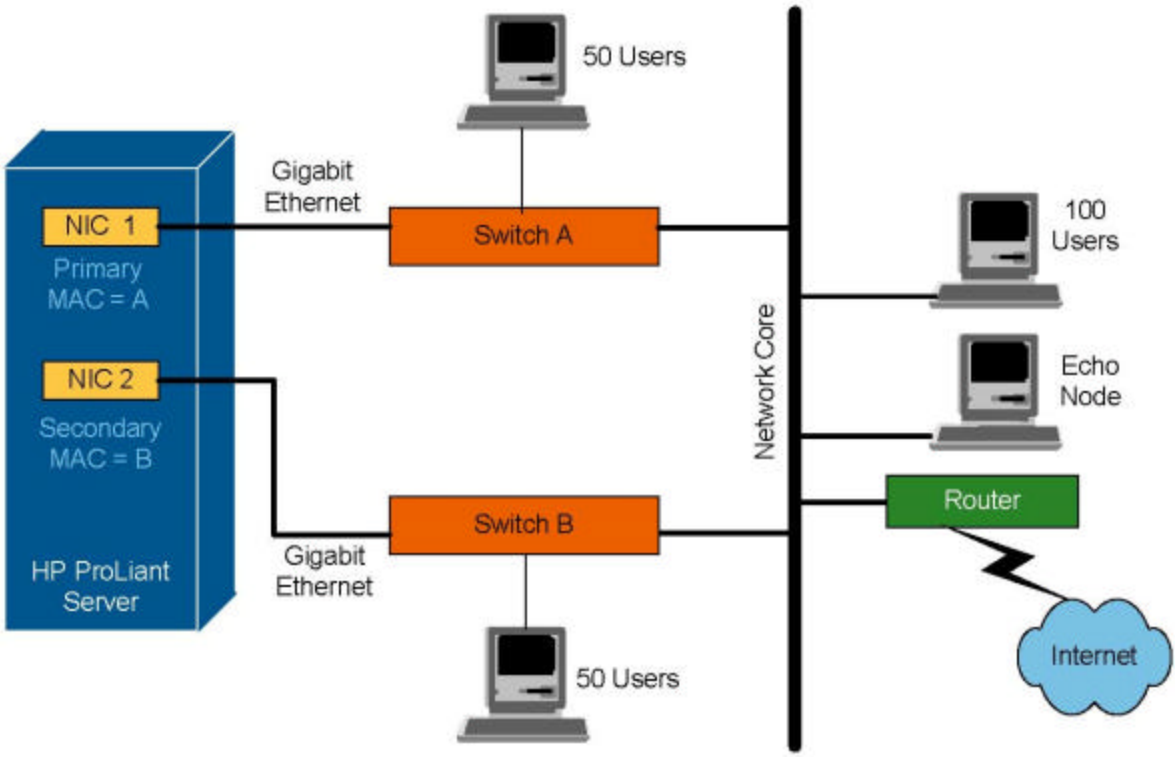
The Active Path Failover feature of INP uses the failover capabilities of NIC teams, allowing users to configure for a failover based on network path availability to a user-selected device in the network. The ports in a team constantly check for path availability to the core network, and the primary port fails over as soon as its path becomes unavailable. As a result, the server always sends data along an unblocked network path.

The Active Path Failover option uses a user-selected device on the network, called the Echo Node, to confirm connectivity to the core network. The Echo Node needs no special software because standard packets are used to determine connectivity of the teamed NICs.

How the Active Path Failover feature works

This section illustrates how Active Path Failover works in a typical business configuration and network failover scenario. Figure 4 below shows the primary and secondary ports in a ProLiant server, the network core, and the echo node attached to the network core.

Figure 4. Typical Active Path Failover configuration showing the Echo Node attached to the network core



In Figure 5 below, a failure has occurred in the connection between Switch A and the network core. Without Intelligent Networking software, this failure results in server connectivity loss. Clients lose access to the server.

Figure 5. Primary NIC loses network connectivity. This isolates the server so that only users connected to Switch A have access to the server.

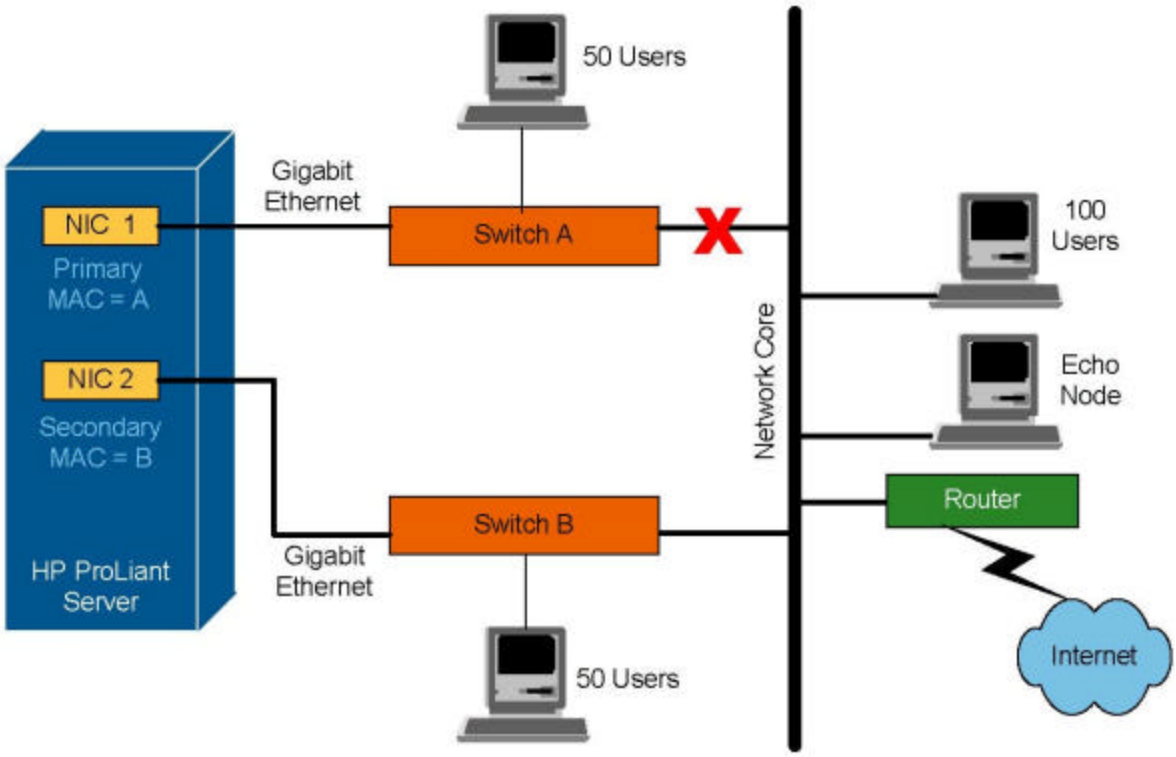
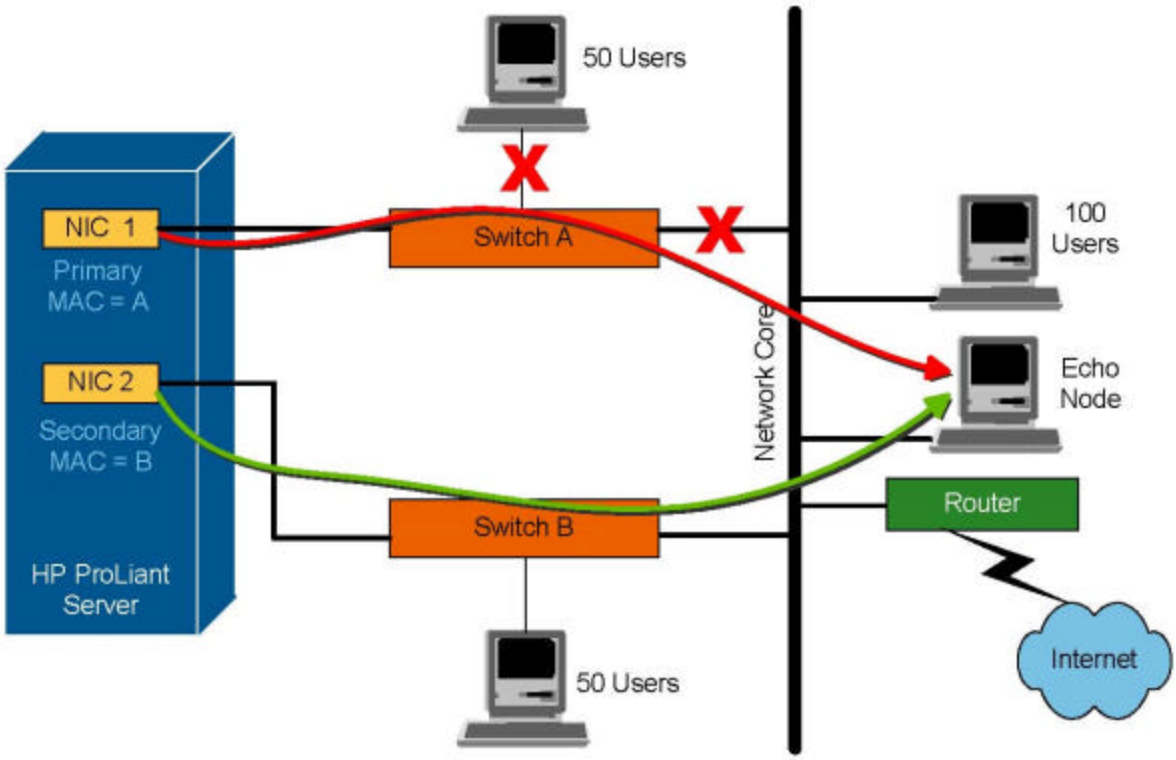


Figure 6 below shows the failure scenario with Intelligent Networking software installed on the ProLiant server. The INP software detects the loss of connection, fails over to the port with the active path, and retains connectivity to the server. Network clients continue to have full access to the server.

Figure 6. Failover to the open path to the network core restores server access for all network clients except for those connected to Switch A.



Router Path Failover

The Router Path Failover feature of INP uses the failover capabilities of NIC teams, allowing users to configure for a failover based on router path availability to a user-specified router group on the network. The ports in a team constantly check for path availability to the router group, and the primary port fails over as soon as its path to the router group becomes degraded or unavailable. As a result, the server always sends data along an unblocked router path.

How the Router Path feature works

This section illustrates how Router Path Failover works in a typical business configuration and network failover scenario. Figure 7 below shows the primary and secondary NICs in a ProLiant server, the switches on the network connected to the team, and the router group attached to the core switch.

Figure 7. Typical router path configuration showing the team, the switches and the router group.

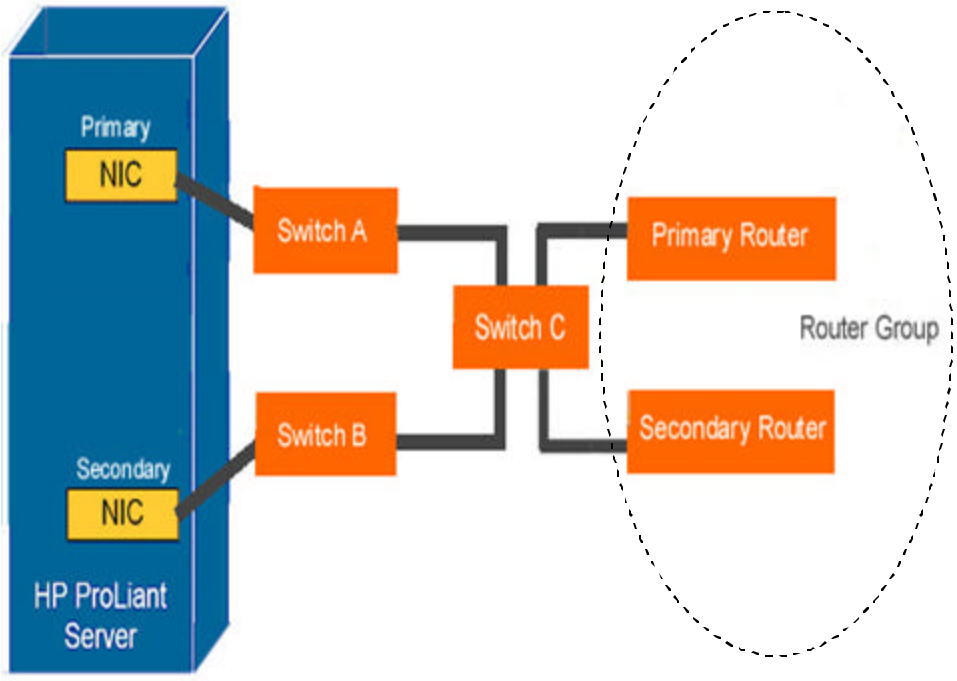
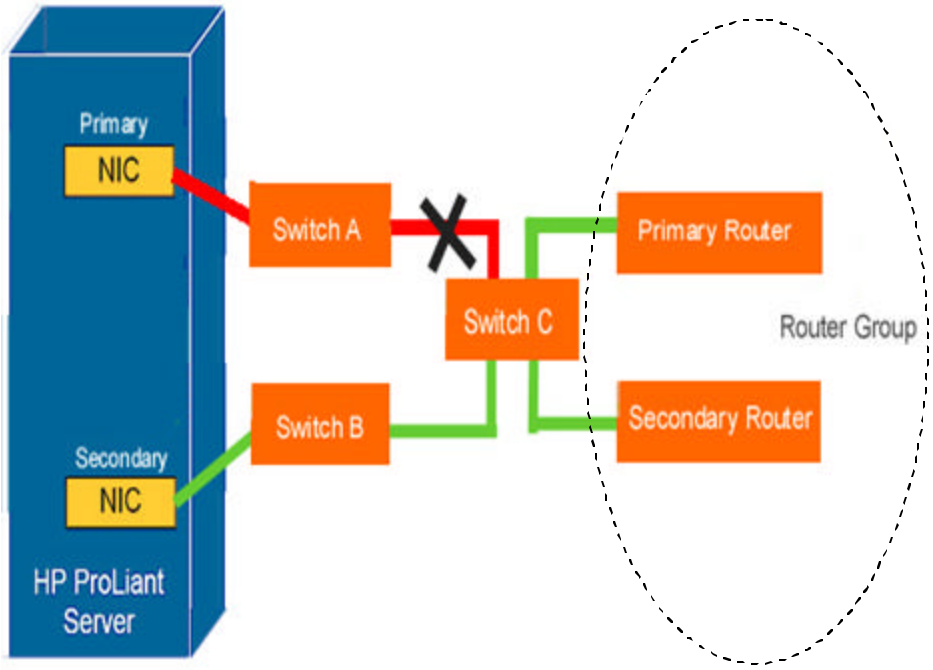


Figure 8 below shows the failure scenario with Intelligent Networking software installed on the ProLiant server. The INP software detects the loss of connection, fails over to the NIC with the active router path, and retains connectivity to the server. Network clients continue to have full access to the server.

Figure 8. Failover to the open path to the core switch and router group commences when the INP software detects the blocked router path beyond switch A.



Dual Channel Teaming

Dual Channel Teaming enables system administrators to create a team of NIC teams that spans two switches and allows for receive and transmit load balancing. Currently, Switch-assisted Load Balancing (SLB) and 802.3ad dynamic channels provide transmit and receive load balancing and fault tolerance on a single switch, but it cannot span multiple switches due to switch limitations. To reduce the impact of a switch failure, system administrators can configure Network Fault Tolerant (NFT) NIC teams and Transmit Load Balancing (TLB) NIC teams across multiple switches.

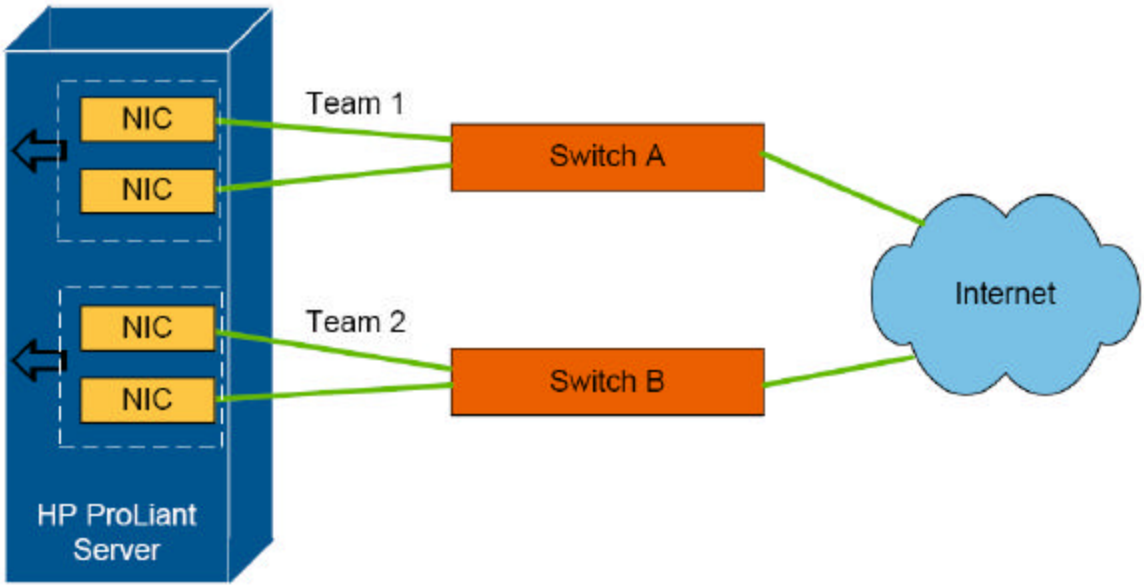
However, NFT and TLB teams limit receive traffic to a single port. If that receiving port is connected to a switch that loses its upstream connectivity, the team may not fail over at all; or it may fail over very slowly. If the receiving port is not able to receive client traffic, clients lose access to the server. Because of these teaming and switch limitations, networks that use more than one switch have a single point of failure and the potential for server connectivity loss.

How the Dual Channel Teaming feature works

This section describes and illustrates the results of a switch failure on ProLiant systems with and without Dual Channel Teaming.

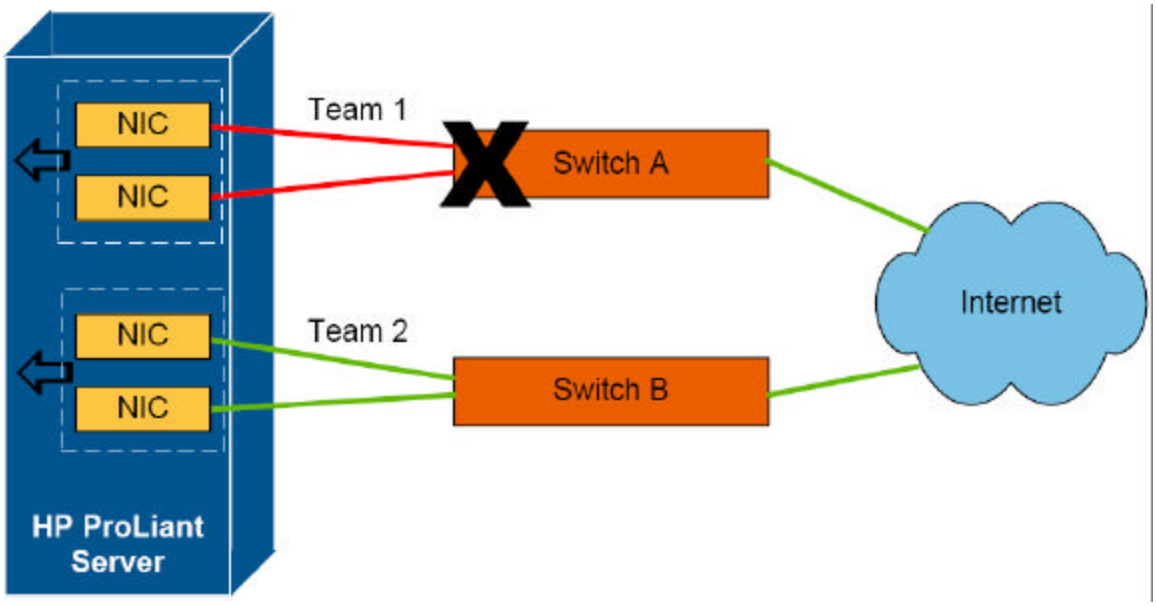
In Figure 9 below, a ProLiant server contains two SLB or 802.3ad dynamic NIC teams, each connected to a different switch and presenting its own network connection to the server.

Figure 9. Two SLB or 802.3ad dynamic teams connected to two switches without INP installed. Each team presents a single connection to the server.



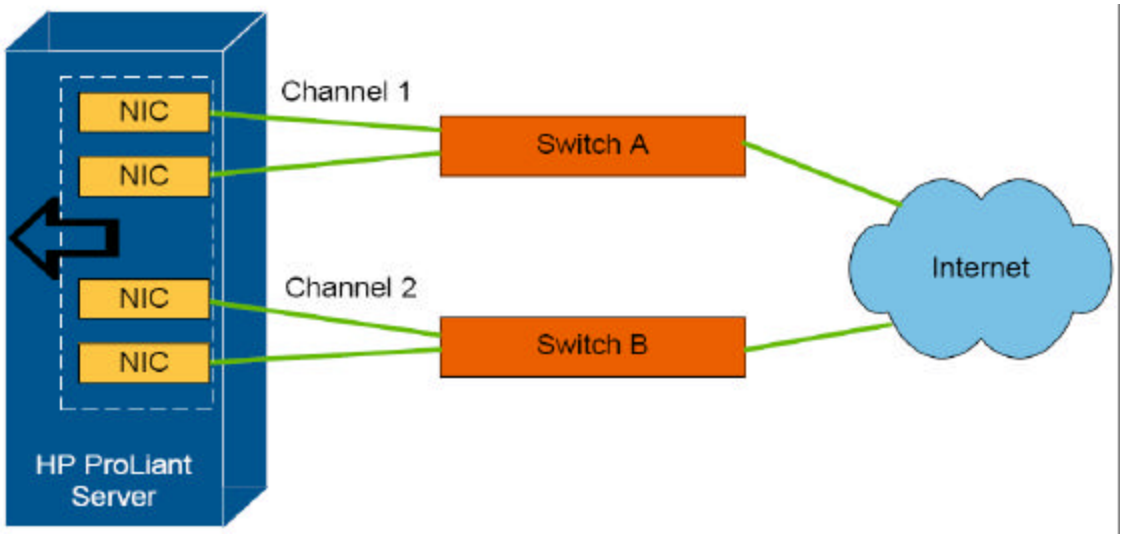
In Figure 10 below, a failure has occurred in Switch A. As a result, Team 1 is unable to receive; so clients lose access to the server and to business-critical applications and data located there.

Figure 10. Switch failure with two SLB or 802.3ad dynamic Teams without INP installed



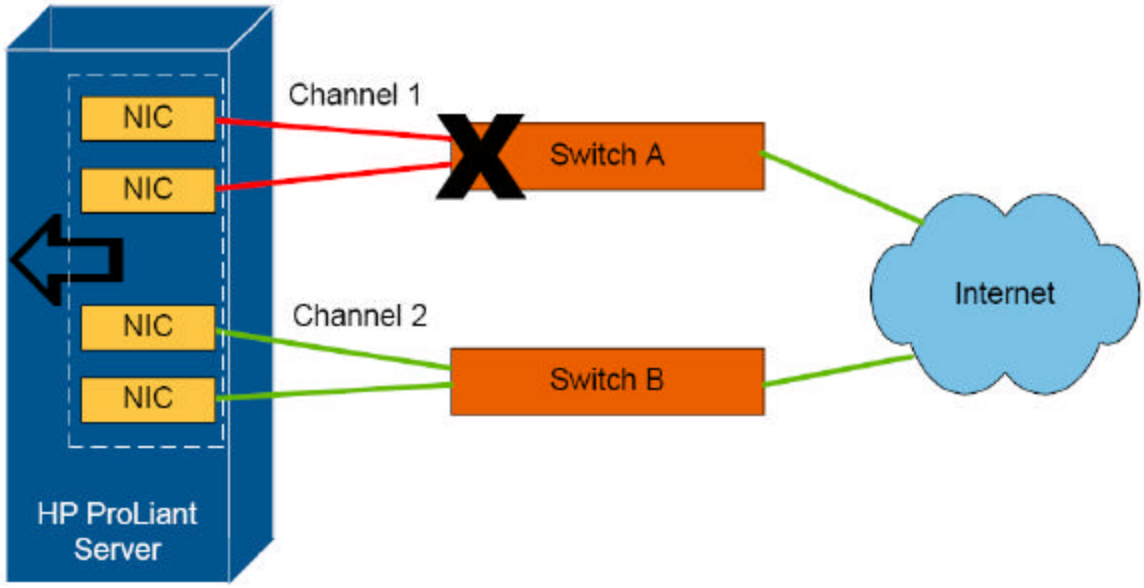
In Figure 11 below, Intelligent Networking Dual Channel Teaming has been installed and configured on the ProLiant server. With this configuration, the two NIC teams present a single connection to the server.

Figure 11. INP Dual Channel Team configuration. A single connection is presented to the server.



In Figure 12 below, once again a failure has occurred in Switch A. With the Dual Channel Failover feature enabled, however, there is no connection loss and the failed hardware can be replaced without affecting server traffic.

Figure 12. INP Dual Channel Failover scenario



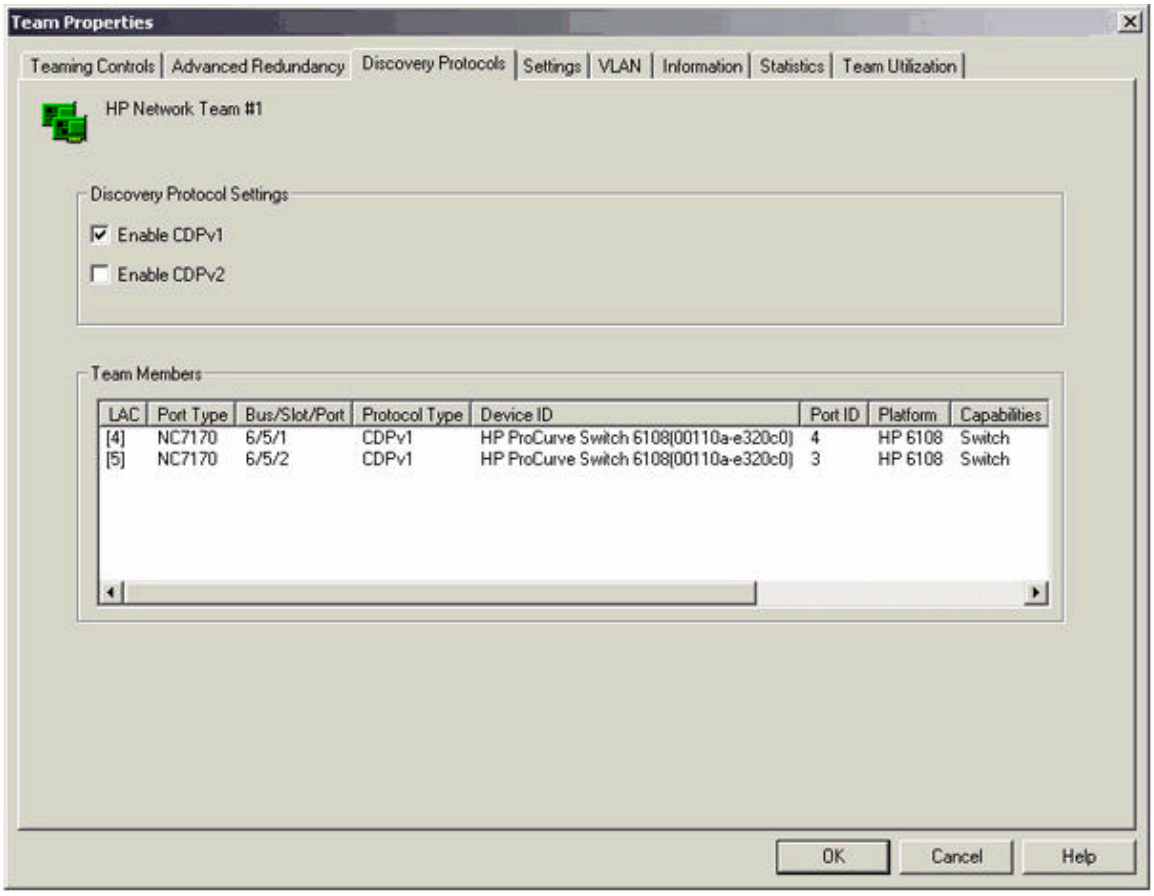
Discovery Protocols feature

The Discovery Protocols feature enables system administrators to view the configurations of remote (neighbor) network team member devices, including protocol addresses, platform of the device, and information about the interfaces used by routers for teamed devices. The feature uses Cisco Discovery Protocols (CDP) and is media and network protocol independent. It works with all networking devices including router, access servers, bridges and switches.

How the Discovery Protocols feature works

The familiar Network Configuration Utility (NCU) provides the interface to the Discovery Protocols feature. Figure 13 below shows the NCU interface Discovery Protocols tab.

Figure 13. The NCU Team Properties Discovery Protocols page.



The Discovery Protocols tab provides the following information about the team of NICs:

- Supported protocols: CDPv1 or CDPv2
- Local Device Identification
  - Name of the Local Area Connection (LAC)
  - NC model number of the port (Port Type)
  - Location of the port in bus/slot/port format
- Remote Device Identification
  - Protocol used to discover remote (neighbor) devise (Protocol Type)
  - Name of the remote device (Device ID)
  - Switch port of remote device to which the NIC connects (Port ID)
  - Device platform of remote device (Platform)
  - Device capability code for remote device (Capabilities
  - VTP management domain name of remote device (FTP Management)

- Native VLAN ID of remote device (Native VLAN)
- Duplex information of remote device (Duplex)

This information can help system administrators check the neighboring teamed devices for errors in configuration and set up. The information can also assist with troubleshooting.

Conclusion

The ProLiant Intelligent Networking Pack offers several features that protect ProLiant networks from single points of failure and provide robust network capabilities and information to make ProLiant servers aware of the network around them.

For more information

For more information and other white papers about HP ProLiant network adapters, including the Virus Throttle feature, go to this web page: For additional ProLiant networking White Papers, see: www.hp.com/networking/info.

For more information on Networking Pack features for HP Integrity Servers, visit the Integrity Essentials website at: http://www.hp.com/go/integrityessentials

For information about how to purchase an HP ProLiant Essential Intelligent Networking Pack license, go to the HP website at http://h18004.www1.hp.com/products/servers/proliantessentials/inp/index.html or contact your HP reseller.

4AA0-3515ENW, 9/2005