# Risk Mitigation: A Strategy for Reducing Risk Through a Single-Vendor Integrated Network

## High-Level Overview

With the increased reliance on the network for application support, enterprise customers are increasingly focused on the availability of the network. While there are considerations to building a diverse vendor environment, a highly available single-vendor architecture is readily achievable. A single-vendor environment also allows the customer to use the network more effectively, by reducing operational expenses as well as providing a foundation for adoption of innovation.

The intent of this paper is to discuss the advantages of a single-vendor architecture and review whether a vendor can provide high availability for the entire network architecture.

## Advantages of a Single-Vendor Architecture

### Limited Complexity

By adopting a single-vendor architecture, the customer need only track a single implementation of services within the network. When using a single vendor, there is no requirement to understand and design for the lower common denominator of service that is available. In a single-vendor network, features are available ubiquitously across the entire network. The subsequent tracking of the implementations of protocols across multiple vendors in order to be able to use any new features, if they are ever offered across all vendors, is a time-consuming effort that will require additional time to accomplish

Complexity of management of the network will also be minimized as you factor in the disparate tools for provisioning, management, and troubleshooting.

### Minimal Mean Time to Repair

When implementing a single-vendor network, troubleshooting any issues that involve features or protocols that are implemented networkwide; for instance, any Interior Gateway Protocol (IGP) or Border Gateway Protocol (BGP), will be easier to resolve. There are no implementation inconsistencies, and there is no need to have people trained across multiple architectures, which results in a longer time to troubleshoot and implement any corrective actions.

Engaging only a single technical support center will also limit the coordination effort required to find a resolution, reducing issues in miscommunication, resolving multiple views, and so on.

As a result, it is uncommon for networks to be deployed using a multiple vendor strategy, either in enterprise or service provider, where a portion of the network such as the core is divided into two parallel infrastructures of differing manufacture. Note that service providers do employ a multiple-vendor strategy, but that strategy is typically based on awarding franchises in an area to a single vendor for that franchise, not by placing parallel vendor networks in a single functional area.

### Lower Operational Cost

The cost of implementing and operating a single-vendor network avoids the requirement to train the engineering and operations staff on two diverse architectures, as well as installing and operating two disparate management systems.

What is not obvious and often overlooked is the exponential effect that arises when implementing a single-vendor network. There are two main sources for this: troubleshooting in a dual-vendor environment (determining who is at fault) and the need to spend more in the application design process to help ensure that the application architecture for the entire company does not exceed that lower common denominator of service that is available in a dual-vendor approach as being offered. Tracking the implementations of protocols across multiple vendors in order to be able to understand, implement and troubleshoot multiple variations of a feature is costly as well.

For more information, read the paper about single-source network cost advantages at http://www.cisco.com/application/pdf/en/us/guest/products/ps2978/c1256/cdccont_0900aecd804cd4d1.pdf.

### Acceleration of Innovation Adoption

The ability to use vendor innovation for your own competitive advantage, and a higher level of service for features, results from a single-vendor architecture.

- **Ability to absorb innovation:** This provides a competitive advantage relative to your own company's competition by allowing a quicker rate of integration of advanced technologies and features. Our customers increasingly turn to Cisco® for innovation that they can use to provide increased value, faster time to market of their applications, and so on for applications in order to help ensure that their company is at a competitive advantage relative to their competition
- **Highest level of service capabilities:** The customer can implement any level of service that is available with a chosen network vendor. If there is an implementation of a service that is not available on the second, parallel network, then it cannot be implemented on the first because (1) the traffic might go over the second network under normal conditions, which will lead to abnormal and probably undesired behavior (or you would not use that feature in the first place) and (2) even if the second network was purely a backup, in a failure scenario the service or feature would not be available.

Examples of innovation include:

- IP service level agreements (SLAs)
- Performance Based Routing (PfR)
- Gateway Load Balancing Protocol (GLBP)
- Object tracking

Examples of disparate implementations include:

- Quality of service (QoS): Hierarchical QoS, scalability in number of classes
- IP multicast: Advanced features such as bidirectional Protocol Independent Multicast (PIM) or extranet mVPN (**multicast MPLS VPN**)
- Data-link switching (DLSw): Scalability features

- Open Shortest Path First (OSPF), BGP, BFD (**Bi-Directional Failure Detection**): Protocols that are standards based but have optional implementations and might require some functions such as subsecond timers and scalability enhancements

### Network High-Availability Considerations

Protocols that are common to the entire architecture such as OSPF, BGP, and BFD might suffer from diverse implementations that create unusual states even under normal network situations, that the customer will have to understand and resolve. Any instance of a failure or instability, security issues, and so on that involves the control plane of architecture will put the entire network at risk, since the control plane is universal to the entire network.

The network needs to be designed and implemented to adopt high availability as a basic requirement and use those features and best practices to deliver high availability. Utilizing hardening techniques such as control plane policing, and platform resiliency features such as Nonstop Forwarding/Stateful Switchover (NSF/SSO), in addition to implementing best practices on Cisco IOS® Software release strategies, will provide the highest level of availability within either a single- or dual-network architecture.

### Common Implementations and Problems

Many of the issues that result in PSIRT (**Product Security Incident Response Team**) announcements are actually industry wide issues: for example, vulnerabilities found within Simple Network Management Protocol (SNMP). These vulnerabilities are common to all vendor implementations since they are results of the design of the specific protocol involved.

Responding to issues or vulnerabilities across multiple vendor implementations could slow down the ability to implement resolutions to those vulnerabilities, especially as not all vendors announce vulnerabilities and resolutions openly.

## How to Select a Vendor to Reduce Risk

- Look for a well-defined and detailed design validation program, including high availability and network security.
  - Design guidance based on large-scale validation tests
  - Inclusive of enterprise applications and other advanced technologies such as unified communications, application acceleration
  - Specific architectures to address enterprise customer needs for different network requirements, with an integration approach
- Ask for experience in deployment of the recommended architecture.
- Evaluate advisory processes (for example, how do First and CERT.Org members treat internally found defects, vulnerability testing in the release/regression process).
- Support organization and coverage across your enterprise.
  - Account coverage focused on enterprise, with an understanding of applications and business requirements
- Channel partner community trained to support vendor's equipment
- Vendor's financial strength

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C11-430265-00 9/07

 