

Introducing a Second Network Vendor Saves Money and Solidifies Operations

Gartner RAS Core Research Note G00165103, Mark Fabbi, Debra Curtis, 18 May 2009, R3144 02052010

Gartner clients are increasingly expressing interest in adding a second vendor to their enterprise network infrastructures to achieve competitive leverage and avoid vendor lock-in. However, they are concerned that this will multiply the complexity of their network operations. With adequate foresight in addressing specific operational considerations, successful integration of a second vendor can be achieved with little operational risk.

Key Findings

- The operational impacts of introducing a second vendor for basic network infrastructure are modest and easily handled by most organizations.
- The changes required to successfully integrate a second vendor are largely based on best practices for running a single vendor network.
- Introducing a second vendor will reduce capital expenditures (capex) by at least 30% (and often more), while only minimally increasing operational expenditures (opex).
- There is a set of network management tools that offers capabilities to manage across multivendor environments without adding complexity to network operations.

Recommendations

- Enterprises introducing a second vendor into the infrastructure must approach the problem in an organized, systematic fashion to maximize benefits while minimizing operational risk.
- Enterprises should invest in multivendor network management tools that address the disciplines of configuration, fault and performance management.

WHAT YOU NEED TO KNOW

Operational challenges have long been used as a reason not to introduce a second vendor into the network infrastructure. However, by taking an organized approach and using well-established multivendor network management tools and disciplines, enterprises can reduce operational challenges to a minimum, while reaping the benefits of a lower-cost, better-performing infrastructure.

ANALYSIS

With tightening economic conditions and shifting landscapes in enterprise networking, we are getting an increasing number of client calls considering a second vendor for their infrastructure. We believe this is a positive trend that shows enterprises are focused on features, products and vendors to be included in their infrastructure. A second network infrastructure vendor, either as a direct alternative or, more commonly, as a provider in an adjacent market (for example, splitting LAN to use different providers for workgroup and core switching), provides three primary benefits:

- Cost
- Improved functional alignment with requirements
- Improved operational processes

Clearly considering alternative solutions will improve your negotiating position, help reduce capital costs and avoid vendor lock-in. In addition, it will refocus attention back on requirements to ensure the right feature mix and architectural decisions, and will not constrain solutions to one vendor's view of the world. A final consideration is the mergers and acquisitions due to economic conditions. Many organizations will end up in a mixed environment due to consolidation. Typically, we see clients achieving at least a 30% reduction in capital costs just by considering alternative vendors, and, often, savings are much higher. Organizations must start considering alternative vendors for their infrastructure. The decision on how and where to use these vendors will be based on functional, operational and financial objectives. By following the recommendations in this research, organizations can realize these savings with little impact on long-term operational costs.

In client discussions, operational issues are perceived to be the major hurdle in acting on their desire for more choice and vendor leverage. We feel there are four specific areas that need to be addressed to deal with these operational challenges:

- Interoperability
- Training
- Network management
- Support escalation

However, by taking a systematic approach to the architecture and following network management best practices (described below), the objections raised by incumbent vendors can be easily overcome — often to the benefit of network operations.

Interoperability

Networking at Layer 2 and Layer 3 is highly standardized, with a major emphasis on interoperability during the standardization process. When considering a second vendor, the following will ensure successful integration of the new vendor:

- Define the boundary between the existing vendor's equipment and the new deployment into clear, logical building blocks.
- Investigate current implementations and determine the protocols that run between the building blocks. For example, for workgroup switching, you need to determine what protocols are running between the devices connected to the switch, and between the switch and the aggregation layer (examples include trunking protocols, quality of service [QoS], virtual LANs [VLANs], Power over Ethernet [PoE] and link layer/device discovery).
- Determine which protocols are standard or proprietary.
- Migrate proprietary protocols to widely deployed open standards. This should be a regular part of network maintenance and support; however, we see many networks still running old proprietary protocols (such as Cisco's ISL protocol, which was superseded by 802.1Q and 802.3ad nearly 10 years ago). More recent examples are the migration from Cisco Discovery Protocol (CDP) to Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED). (Our position is that proprietary protocols are acceptable within a building block, but should be avoided between building blocks.)

In mainstream enterprise networks, there are few proprietary protocols that prevent network architects from considering alternative vendors. However, in the data center, there are a number of emerging protocols (such as Fibre Channel over Ethernet [FCoE] and Converged Enhanced Ethernet [CEE]) that are not finalized, and we see proprietary implementations in the market. Organizations adopting any of the prestandard solutions should migrate to standard solutions as they become available.

With a well-defined, open standards boundary between vendors, integration is able to proceed.

One other aspect is critically important. Operational overhead and risk can be limited by keeping the number of boundary points to a minimum. Using the LAN example, it makes more sense to replace all the workgroup switches in one building, rather than deploying a few switches scattered in multiple buildings. Think about the homogeneous building blocks of a vendor kit, rather than a random mix across the network. In the LAN, you might take two distinct approaches:

- Layer approach, with edge switching from one vendor and core from a second vendor

- Location-based approach, with certain buildings or geographies with one vendor, and others with a second vendor

Using a homogeneous, open standards approach has proven to ensure a high level of interoperability between vendors, and minimizes risk. However, proof-of-concept testing is still needed to ensure consistent behavior across the boundary. This testing ensures that conflicting protocol defaults are dealt with. This is not dissimilar from the testing that should take place in a single-vendor environment, where different product families are used that exhibit different features sets.

Training

The level of standardization and interoperability of networking protocols eases the integration of a second vendor because the basic constructs between the vendors are all similar. Assisting the operational impact is that nearly all vendors use a command line interface (CLI) for interacting with their devices. For many network operations staff, they will feel immediately comfortable with the interface of most network products. Those that don't emphasize a CLI tend to have focused on a set of tools to make managing the network easier and more intuitive. These tools are often the same ones we discuss below that offer a unified way to manage a heterogeneous network architecture. From talking to clients, we would estimate that training an existing network operations resource on a second network vendor would take one to two days. Many vendors offer this type of "delta training," assuming a solid understanding of networking and network operations. The focus of this training is on what is different or unique about a vendor's operational approach.

Network Management

Most network equipment manufacturers (NEMs) provide element management tools, sometimes with just basic capabilities needed to install, configure and maintain individual network devices, and sometimes with sophisticated capabilities that address multiple network management disciplines for groups of interconnected network devices. Although some provide basic support for any Simple Network Management Protocol (SNMP)-enabled network device, these element management tools generally only provide the full or enhanced set of capabilities for the NEM's own proprietary devices. Examples include Cisco's CiscoWorks, F5's Enterprise Manager, HP's ProCurve Manager, Juniper Network's Network and Security Manager (NSM), Alcatel-Lucent's OmniVista, Nortel's Enterprise Network Management System and 3Com's Intelligent Management Center.

To prepare to add a second network infrastructure vendor, network managers should establish a foundation of multivendor network management tools that works with their current network infrastructure vendor, and supports the other vendors they are considering as their second vendor. This will allow time for staff training and the conversion of skills to the new tools. Three critical network management disciplines should be considered: network configuration management, network fault management and network performance management.

Network Configuration Management

For many network engineers, much of network configuration management is a labor-intensive, manual process involving remote access (for example, telnetting) to individual network devices and typing commands into vendor-specific CLIs, creating homegrown scripts and using NEM-specific element management tools. A new generation of network configuration and change management (NCCM) vendors created tools that operate in multivendor environments, enable automated configuration management, and bring more-rigorous adherence to the change management process, as well as compliance audit capability.

NCCM tools discover, back up and restore network device configurations. They detect and alert on configuration changes, perform a differential audit between configuration versions, and make configuration changes to network devices. NCCM vendors include AlterPoint, BMC (Emprisa Networks), EMC (Voyence), HP (Opware), Intelliden and SolarWinds. Prior to introducing a second network infrastructure vendor, replace manual network configuration management processes and vendor-specific tools with automated NCCM tools that operate in a multivendor environment. Establish standard network device configuration policies that apply to your current network vendor's devices, but that will also apply to any other vendor's devices that you will introduce to the network. This will reduce operational complexity and enable more-effective automated network configuration management.

Network Fault Management

Network fault management tools use the industry-standard, vendor-independent SNMP, so no additional complexity will be suffered when introducing a second network infrastructure vendor. Network fault management tools provide features such as discovery and mapping of network topology, status monitoring and troubleshooting. The market share leader of this segment is HP Network Node Manager. Yet, this market space is shared by many large and small vendors, including AdventNet, ASG Software Solutions, CA (Spectrum), EMC (Smarts), Entuity, IBM Tivoli (Micromuse), Ipswitch and SolarWinds, plus open-source alternatives such as Nagios.

If no network fault management tools are in use at all, prior to introducing a second network infrastructure vendor, then investigate adding this functionality. Focus on evaluating network fault management tools that are appropriate to the size, scope and scale of your network. Lack of network management foresight can cause new mission-critical network technologies and services to not fully deliver on their potential. Rather than becoming the "scapegoat," get involved early in the purchase planning, and justify the investment in network management tools by making it a prerequisite for achieving the desired results from the second vendor's technology being introduced.

Network Performance Management

Some network performance management tools also use industry-standard, vendor-independent SNMP and poll network devices to collect data for performance reporting and trend analysis. Vendors that provide products in this category include CA (Concord), Entuity, HP (Trinagy), InfoVista, Statseeker and the open-source alternative MRTG. Adding a second network infrastructure vendor will have no affect on these products, except in the case where the licensing needs to be expanded to accommodate additional network devices.

There are other network performance management tools capable of analyzing the makeup of the network traffic for performance monitoring and troubleshooting that may depend on NEM vendor-specific instrumentation. Some network traffic analysis is accomplished by installing specialized network probes or appliances to monitor and analyze the network traffic, such as those from Compuware, Fluke Networks, NetQoS, NetScout, Network Instruments and Opnet Technologies.

Adding a second network infrastructure won't affect these, either. However, we are finding more and more interest in the network traffic flow statistics collected by instrumentation that NEMs have embedded in their network devices, such as NetFlow, sFlow, J-Flow and IP Flow Information Export. The embedded instrumentation can be an alternative in locations where the expense of a dedicated probe or appliance cannot be justified. You will still require a separate tool to collect, analyze and report on the flow data. The previously mentioned network traffic analysis vendors all support NetFlow and variants as a data source. In addition, AdventNet, InfoVista (Accellent), SolarWinds and the open source ntop.org also provide traffic analysis and reporting for NetFlow and variants.

For enterprises using flow-based data that are considering adding a second network infrastructure vendor, the availability of embedded flow-based instrumentation should be included on your list of evaluation criteria. In addition, confirm that your existing network traffic analysis vendor also supports the NetFlow variant provided by the second network infrastructure vendors being considered.

Support Escalation

A final issue that is common in client discussions is problem escalation and dealing with vendors. It is our experience that problems generally arise when there is not a well-defined architecture and boundary between vendors, or when network management best practices are not followed. Organizations with well-defined boundaries using proper management tools should be able to segment problems and address the proper vendor. We are also seeing many of the networking vendors become more customer-focused when dealing with more-complex issues, especially ones that potentially cross a vendor boundary.

Organizations should review service terms and conditions between the two vendors to ensure consistency between similar devices. For example, if a four-hour response is required for both vendors in a single location, then either both vendors must commit to this level of service or, perhaps, the IT organization will need to hold spares to cover this requirement.

Clients that have taken a systematic approach to dealing with multiple vendors have seen their vendors become more attentive and focused on their specific business requirements.

Tactical Guidelines

- Don't randomly mix multiple network infrastructure vendors. Look at introducing a second vendor with your network strategy and architecture in mind.
- Prepare for introducing a second vendor by establishing a foundation of multivendor network management tools that work with your current network infrastructure vendor to allow time for staff training and conversion of skills to the new tools.