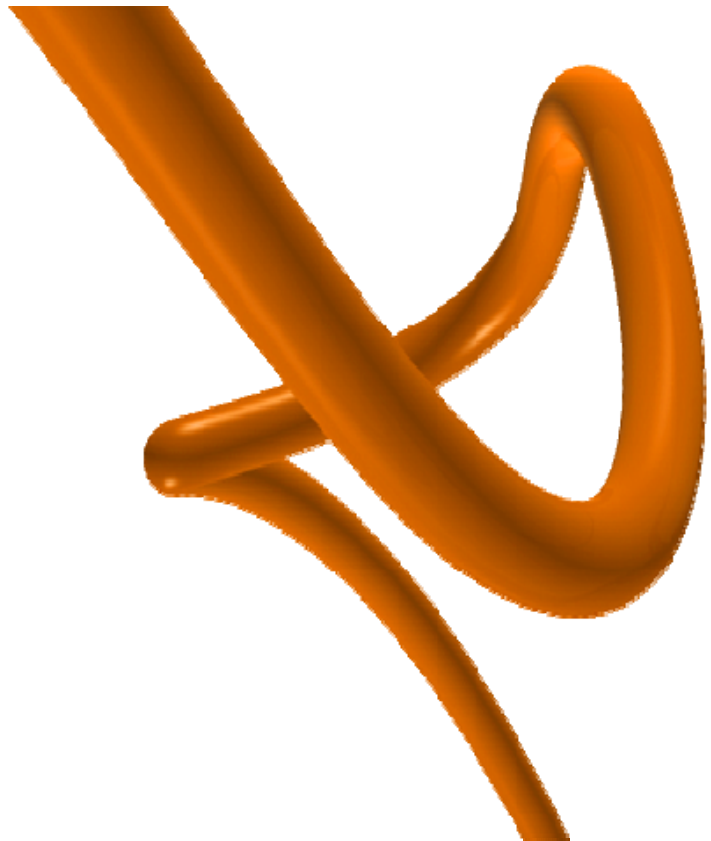


A thick, solid orange diagonal bar that starts from the top left and extends towards the center of the page.

Simplifying Data Centers & Networks by Creating a Virtual Infrastructure Layer

Larry Cantwell, Vice President and Chief Technology Officer



Introduction

On a daily basis, data center managers and network administrators face significant challenges in managing complex multi-tiered IT environments—often on a global basis. There is a need to maximize resource usage 24/7/365 while simultaneously reducing management costs and maintaining a highly available, secure environment, all within strict budget constraints.

This paper discusses the characteristics and benefits of a virtual infrastructure layer (VIL) and how a solution can be realized in an integrated “virtual infrastructure switch” that will help reduce network management costs and overall total cost of ownership (TCO).

Overview

Products have emerged that enable the virtualization of server and storage platforms. These products provide a means for customers to more effectively utilize and manage diverse endpoint IT equipment (servers and storage) efficiently and homogeneously, helping to reduce their TCO. To take the virtualized data center environment to the next level, the virtualization of the physical connectivity infrastructure layer (switching, patch panels and cabling) needs to be addressed. Typically, all data center networks are composed of some combination of SAN (ESCON, Fibre Channel, and FICON), LAN (Ethernet/TCP/IP), WAN (SONET/SDH) and MAN (DWDM) components. Regardless of the mix of IT equipment and network protocols and interfaces, data center networks require a flexible and adaptable infrastructure to physically connect devices together.

A virtual infrastructure layer allows for automated and secure equipment additions, moves or changes, thus enabling seamless reconfiguration and growth of the network. In order to adapt to the dynamic needs of a virtualized data center, a virtual infrastructure layer provides a much more secure environment by enabling a hands-off approach to managing the network. Finally, it will provide resiliency, monitoring and diagnostic tools that assist in managing the network. It is easiest to visualize the value of a product that enables virtualization of the physical layer as the core of the network such that it interconnects each node in the network, as shown in Figure 1.

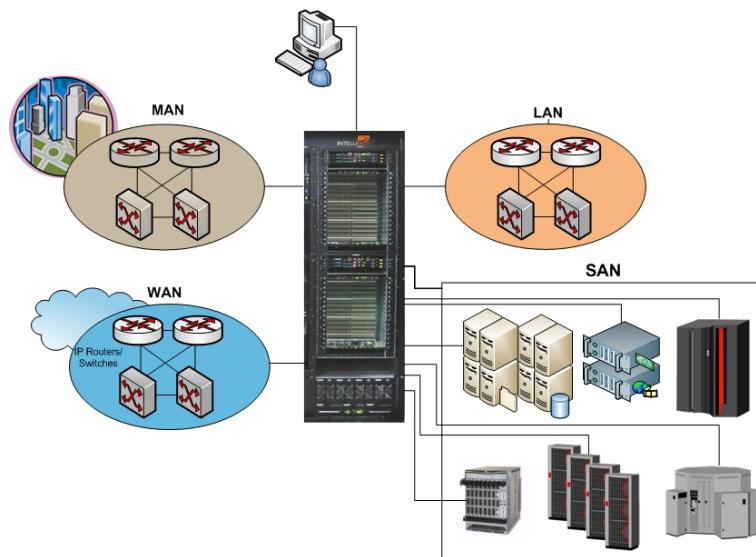


Figure 1. The above illustration shows how the infrastructure layer can be ‘virtualized’ such that all changes, migrations and monitoring are automated, scalable and integrated while the overall network management is simplified, more robust and more secure.

What are the characteristics of a virtual infrastructure?

There are multiple layers in the virtual infrastructure layer that are explored in this paper. The virtual infrastructure switch provides an integrated solution that addresses each of the layers.

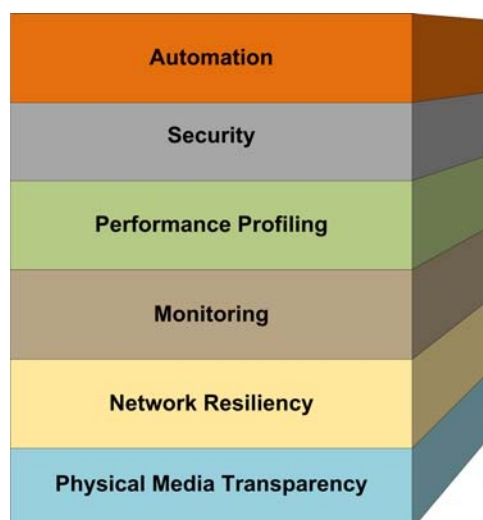


Figure 2. Virtualized Infrastructure Breakdown

Let's explore the components of the virtual infrastructure layer in more detail:

Automation

Traditionally, network physical connectivity has been achieved through a passive, labor intensive and error prone manual process using physical patch panels. Due to physical cable lengths—and the evolution in which those cables are routed over time—moving, adding, migrating infrastructure becomes time consuming, prone to error, and expensive due to the sheer number of fiber and copper jumpers required. In fact, in many cases data center evolution becomes next to impossible due to the sheer mass accumulation of copper and fiber cables at the patch panel and beneath the raised floor resulting in complexity as well as inefficiency in airflow for data center cooling.

The core of a virtual infrastructure layer is a non-blocking, high-availability switch that can scale to several thousand ports. This automates the physical layer so that minor changes that can take minutes are reduced to seconds; and major changes that can take days can be made transparently in minutes—without ever having to go on the data center floor. By utilizing a management interface that provides comprehensive infrastructure visibility and ease of change, locally or remotely, data center staff can implement established change control processes more rapidly, and as required, to optimize resource utilization.

A virtual infrastructure layer also provides the capability to quickly add or migrate IT equipment as needs evolve without introducing “push-pull” changes that can cause significant down time and risk. This enables the data center to scale easily and become “future proof” against unanticipated changes. For example, if storage needs unexpectedly increase, new equipment can be installed, connected to the virtual infrastructure switch and put through test paces prior to being brought into the production network. At the appropriate time, the new equipment can be quickly merged into the network via the instantaneous digital cross connection provided in the virtual infrastructure switch. Similarly, older IO devices can be transitioned out in such a way that disruption is minimized and the migration is simplified.

Another key value proposition related to automation in the virtual infrastructure is the ability to efficiently share resources, thus lowering overall IT costs. Consider the case where expensive data center equipment is purchased on a department or division basis, causing a considerable overlap and duplication of costs. In today's more competitive and enabled world, frequently lab and production environments are attempting to share IT equipment based on time-sliced needs between departments, divisions—and in some cases continents—in order to be efficient as an organization. A virtual infrastructure enables this ability and cost benefits are realized on day one.

Security

Eliminating the need for physical access to the infrastructure to make equipment additions, moves or changes significantly reduces the possibility of both malicious and unintentional security breaches. With a virtual infrastructure switch, the administrator can control user access and roles on an individual basis. Departments can also be assigned groups of ports, constituted by an access control list.

Mis-plugged cables are not only a security threat but often require significant troubleshooting time to resolve. A virtual infrastructure layer minimizes physical access to IT equipment thus helping to create a centrally managed, “hands off,” ultra-secure environment.

Performance Profiling

Many tools available today attempt to balance network loading. Common issues that occur with these tools include:

- Specification to a particular piece of network equipment, but usually not able to control the network bottlenecks;
- Lack of the proper visibility into end-to-end network traffic; and
- Load balancing algorithms that have a tendency to oscillate due to overcompensation based on limited heuristics, or only partial network visibility.

Often, unbalanced network situations are left unchecked resulting in IT equipment degrading to its breaking point, as well being sparsely used or underutilized. In short, complete visibility into what is truly going on in the infrastructure is simply not available. To provide the necessary visibility, a key component of the virtual infrastructure switch is to leverage its central location to provide end-to-end visibility in a manner that is graphical and easy for administrators to interpret and act accordingly on to balance the network and resource utilization. See Figure 3.

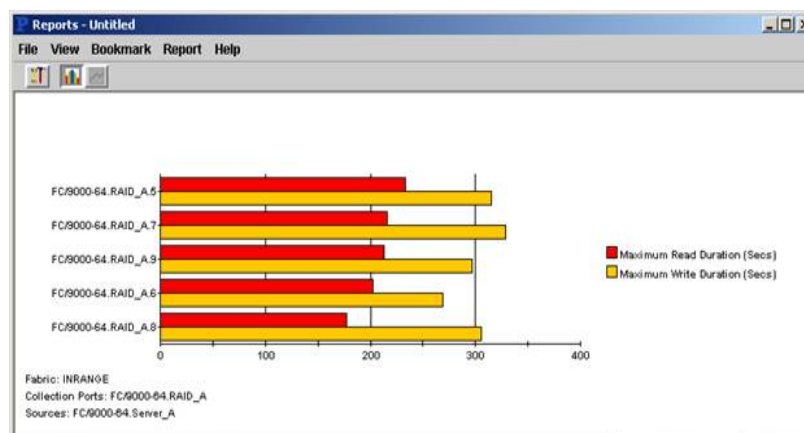


Figure 3. Example of performance profile information that is provided by the virtual infrastructure switch.

Monitoring

Typically, standalone diagnostic tools are connected in-line with problematic paths in the network; this approach is saddled with scalability issues. This equipment needs to be placed actively and disruptively into the data path thus changing its characteristics (latency, bandwidth, etc). The virtual infrastructure switch provides a much more integrated and scalable solution to monitoring and diagnostics. For example, administrators have the ability to route any path(s) within the infrastructure passively into a desired test device without ever moving a physical cable or changing its end-to-end circuit characteristics. Further, virtual infrastructure switching devices will provide increasing levels of diagnostic and tracing facilities that are integrated into the product and act quickly to expose and enable correction of network problems.

Diagnostic tool examples include the capability to scan data paths and capture protocol traces automatically on error conditions, or the ability to test network reaction to loss of signal by issuing a test command. The virtual infrastructure switch merges network performance monitoring and diagnostics with the automated infrastructure function. Management interface tools need to provide visibility into the virtual connectivity infrastructure including the supported networks providing alarms in multiple formats when issues arise. In addition to visible alarms, some management formats even include SNMP alerts and e-mail home capabilities.

Network Resiliency

It is imperative that enterprise class IT equipment guarantee a fault tolerant architecture providing at least five 9's (99.999% uptime) availability. This requires that each component in the network have no single point of failure (Redundant AC Power, DC Power, Functional Failover/Fail-Through, etc.). Often, what is forgotten in the data center design is that infrastructure failures are among the most common. Components including cables, patch panels, and optical interfaces are among the most frequent failures in the network resulting in points of vulnerability that result in a weak link in the network chain.

Therefore, it is important that resiliency is built into the connectivity infrastructure layer to help ensure maximum availability. The virtual infrastructure must be architected to include features including N+1 power and 2X switching capacity for redundancy and non-blocking. Administrators must also be able to configure failover paths for critical data connections. Then, if an infrastructure component, such as a cable, fails operations will automatically fail over to the alternate and continue to function seamlessly.

In a fiber environment, marginal signals are a common cause of intermittent problems and can take a long period of time to isolate. With each patch and bend in an optical cable, there is signal attenuation. An inherent benefit of the virtual infrastructure is that signals are monitored and re-driven at each port, enabling a more resilient physical layer in the data center. The virtual infrastructure switch can also be leveraged to extend distance via long haul small form pluggable (SFP) optics.

Physical Media Transparency

As the network grows, boundaries and physical interface mediums change. For example, a business unit may expand beyond the confines of a room, floor or building requiring different network interfaces for connectivity. In the case of expanding infrastructure connectivity outside of a building, it may be necessary to expand from local copper cabling to campus metropolitan area network (MAN) distance optical devices.

The virtual infrastructure layer facilitates a media agnostic environment by allowing connections through the infrastructure switch to adapt these diverse physical media to co-exist seamlessly. In order to implement a virtual infrastructure layer that is flexible, each port on the infrastructure switch needs to allow for pluggable SFP (small form pluggable) devices that can be copper, short haul optical or long haul optical for network interface connectivity. In addition to physical media independence and transparency, the virtual infrastructure switch needs to support hard partitions or virtual fences to segregate and isolate network ports in a shared environment enabling mixed application workloads and customers to co-exist.

Common Applications

There are numerous applications where a virtual infrastructure has been implemented successfully, including:

- Disaster recovery and business continuance;
- Test and research lab along with data center automation;
- Transportation and seasonal transaction processing;
- Telecommunications and network based media services;
- Managed service provider and web service hosting;
- Remote data center infrastructure management;
- Server, storage and network technology migration and changes; and
- Computer cluster, server farms and grid computing.

Conclusion

Today's enterprise data center customers demand highly available, fault tolerant, scalable connectivity infrastructures to support their mission-critical LAN, SAN, MAN and WAN network environments. As IT dollars become tighter and data center environments become more complex, a virtual infrastructure layer simplifies and secures the underlying physical network cabling and its management. Quantifiable in many ways, the net benefits include significantly reduced time to make changes, ease of migration, faster troubleshooting, enhanced resource utilization, visibility and security, resulting in lower overall network management and data center infrastructure costs.

About OnPATH Technologies

OnPATH Technologies provides automated connectivity solutions to help organizations simplify their physical layer infrastructure to improve the availability, manageability, and performance of their IT environments. Through the delivery of automated connectivity solutions, OnPATH Technologies simplifies management and reduces costs associated with this critical virtual connectivity infrastructure. The company's solutions meet the stringent requirements of enterprise organizations and government entities with complex, dynamic and mission-critical IT environments. OnPATH Technologies is located in Lumberton, New Jersey. For more information, visit www.onpathtech.com, e-mail info.request@onpathtech.com, or phone 1.609.518.4100.