When "Good Enough" Is Not Good Enough

Debunking the Myths of a "Good Enough" Network

Hundreds of Cisco customers have debated the trade-off of prioritizing the lowest price for a point product or service in their network over a strategic plan for how they architect their network infrastructure. Through interactions with many of these customers, we have analyzed various network designs and implementations.

Our findings show that although there is a place for building out a low-cost tactical network, the ongoing operations, upgrades, and lack of preparedness to meet new business challenges prove to be hindrances to organizations in the long run. Rather than just considering capital costs, organizations must look at total cost of ownership, including their operations, and return on investment (ROI), and also including business capabilities enabled by a strategic network, as they build out their networks to address their business needs for today and tomorrow. Customer and employee experience must also figure into the equation.

As device proliferation continues along with the demand for mobility, the network provides the context for ensuring compliance and security. When coupled with the trend toward virtualization and cloud computing services, the network becomes the common thread that brings all these systems together, providing a consistent flow of intelligence end to end. Looking to the future, as more demanding applications such as video and desktop virtualization become part of everyday business, the strategic role of the network is even more critical. Trading off price for capability and strategic value is a risky proposition and one we have seen fail time and again.

Key Findings

- Building a tactical network based on low-cost point products and services increases the total cost of ownership (TCO) for most organizations by at least 20 to 35 percent over a three-year timeframe.

- The network is only as reliable as its weakest link. The cost of an outage quickly eliminates any capital equipment savings. It's like putting cheap oil in your car. The weakest link can be in both products and services.

- The risks of not implementing a next-generation network are considerable. From a TCO and ROI perspective, a tactical network will miss the benefits of a reduction in energy use, the economics of easily moving to the cloud, the ability to embrace desktop virtualization and device consumerization, and the ability to affordably respond to compliance requirements. More fundamentally, business agility is severely hampered when new business requirements require a major network overhaul.

- The Lowest Common Denominator law applies. Because of the inherent end-to-end characteristics of the network, the innovations from one vendor are lost if they are not available across all vendors in the system.

- In terms of warranty, service, and support, you get what you pay for.

- Multivendor networks increase the focus of IT on operations, not on driving strategic business value. They inherently increase OpEx and decrease ROI and business value.

- Good enough networks don't offer the policy tools and integrated security capabilities to allow the business to respond to current and future compliance requirements , such as Payment Card Industry (PCI) in retail, the Health Insurance Portability and Accountability Act (HIPAA) requirements in healthcare, European data protection rules, IPv6 deployment requirements, Federal Information Processing Standards (FIPS), and more.

Recommendations

- Network architects and CIOs must consider a service-centric approach—whether the services are network services, endpoint services or application services—so that their architectures can support increasing business requirements through a total cost of ownership lens that focuses on capital, ongoing operations, and new service rollouts.
- Network operations teams should prepare for the increased business requirements and opportunities of the network, specifically:
  - **Video:** Ensure that networking investments provide the needed intelligence to preplan, auto-configure, and troubleshoot video endpoints and video flows.
  - **Mobility and device consumerization:** Architect your network with the assumption you will be supporting a mobile workforce using devices they select.
  - **Energy management:** Ensure that your infrastructure can monitor and manage carbon emissions or face significant fines.
  - **Security and network policies:** Provide pervasive visibility and control using the network to enforce security policies.
- Customers should consider TCO and ROI assessments as equally important factors in making a network investment.
- **Consider future requirements:** A "good enough network" may make it more difficult for organizations to remain competitive, limiting their ability to engage with their customers and partners as globalization becomes a critical imperative. Do not trade off business capabilities for upfront capital savings.

Strategic Planning Assumption(s)

Through 2015, the device proliferation trend will continue, supported by a matching demand in user mobility. In addition, the focus on cloud services—whether the cloud is private, public, or hybrid—as well as the focus on virtualization will create new business models that IT organizations must consider as they estimate five-year TCO for network infrastructure and operations. The demand on networks will continue growing significantly. Consider that:

- In 2009 alone, humans created more data than in all prior years combined.[1]
- By 2015, there will be nearly one mobile-connected device for every person on Earth: 7.2 billion people, 7.1 billion devices.[2]
- Over the last 15 years, network speeds have increased 18 million times.[3]
- 60 percent of employees believe they don't need to be in the office to be productive and efficient.[4]

[1] MIT Sloan Management Review, "Big Data, Analytics and the Path from Insights to Value."
[2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015.
[3] "Technology Avalanche," David Evans, Cisco Internet Business Solutions Group, 2010.

- Two-thirds of employees believe they should be able to access either work or personal information using company devices at any time from any location.[5]
- By 2014, video is forecast to constitute 91 percent of global network traffic.[6]
- By 2015, companies will generate 50 percent of web sales via their presence on social media and mobile devices.[7]

Analysis

What You Need to Know

The Good Enough Network Versus the Enterprise Next-Generation Network
For the purpose of this discussion, let's consider a tactical network—a network capable of addressing existing business requirements and focused on current challenges—as the "Good Enough Network." We'll call a strategically developed network—one that optimizes today's requirements but is also architected to deal with future technology disruptions and provide investment protection—an "Enterprise Next-Generation Network." Depending on the relevance of technology for the business, a Good Enough Network may suffice. However, over the last 25 years, we've seen innovations in IT that have had a profound impact on various businesses—whether e-commerce, online banking, virtual physicians, or distance learning centers. In these businesses, IT has truly transformed how work is conducted and a Good Enough Network is too risky to consider.

The reality is that a Good Enough Network isn't necessarily less complex, easier to manage or more cost-effective than an Enterprise Next Generation Network. It is just a network that was optimized for one thing only: initial acquisition cost. In every case we reviewed, when running services on the Good Enough Network that extended beyond simple connectivity (such as security or mobility or desktop virtualization), the network required additional operating expenditures and resulted in more troubleshooting and a lower quality of experience for the end users.

Network architects and CIOs should evaluate a Good Enough Network for their business needs on a periodic basis. In doing so, they will quickly realize that the short-term capital gain comes with a suboptimal business outcome that is likely to include more outages, less security, less service consistency, and much finger pointing across multiple vendors. If risk mitigation is not a concern, a Good Enough Network may suffice. However, as the enterprise network equipment market continues to evolve with increasing mobility, cloud services, and virtualization trends, customers are increasingly asking:

- What are the main considerations for a next-generation network?
- Can I afford a Good Enough Network long-term?
- Is it possible to shift from a Good Enough Network to an Enterprise Next-Generation Network?

Research Approach

The foundation of this paper is the thousands of customer request for proposals (RFPs) Cisco receives in the network equipment marketplace from customers who need to manage their existing environments and those considering major project upgrades. These RFPs represent a significant portion of the competitive marketplace for network infrastructure. Network RFPs were examined for both private and public sector organizations.

---

[4] Cisco Connected World Report, 2010.
[5] Cisco Connected World Report, 2010.
[6] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015.
[7] Gartner Top Predictions for 2011.

To supplement these RFPs, we also looked at various network designs. Those representing a Good Enough Network were made up of a mix of low-cost products and services. In contrast, networks at the Enterprise Next-Generation Network end of the scale consisted of a portfolio of systems, usually form a single vendor, for unified access across the extended wide area network and from the next-generation data center and the cloud. We examined customer designs for organizations that ranged in size from roughly 1000 users up to Fortune 500 organizations with more than 1000 locations and more than 10,000 employees.

Our research shows that Cisco is the leader in delivering the Enterprise Next-Generation Network. For creating a Good Enough Network, any number of vendors can be used based on the lowest purchase price contender. Cisco demonstrates Enterprise Next-Generation Network leadership on a number of fronts. These include:

- Marketshare leadership enables Cisco to understand customer requirements better and innovate for future services.
- The breadth of product offerings at Cisco (including switching, WLANs, WAN routing, IP telephony [IPT], network security, and other network-related areas) enables Cisco to take a holistic view of the network end-to-end.
- Cisco offers innovative products and best-in-class services built on years of experience in customer deployments, with 20 worldwide centers, more than 630 Cisco CCIE® professionals, and over 20 years of collected networking intelligence.
- Cisco offers centralized policy that enables IT personnel to define business rules once and apply them holistically across the entire network.

Organizations often consider a change in their approach toward networking for at least one of the following reasons:

- **New business models:** Over time, an organization may be exploring more IT-centric approaches to transforming their business. For example, a business may want to provide virtual experts in areas of unique specialization, such as medicine or banking. Or it may want to implement telepresence and video to completely reinvent how R&D is done.
- **More-competitive marketplace:** New entrants into the market place may disrupt the way the business has traditionally operated along with their long-standing end-customer relationships. To remain competitive, they have to offer additional services or provide enhanced customer support.
- **Changing demands on the network:** Scaling of the business, expanding to new geographies, supporting a mobile workforce, exploiting cloud services, and addressing new security threats—these are just some examples of where a Good Enough Network may no longer be good enough.

The main criteria expressed by our customers when they start to consider an Enterprise Next-Generation Network include:

- Creating consistent and secure access to the network, whether over wired, wireless, or VPN technologies
- Ensuring that inherent automation and orchestration is embedded in the network to minimize operating expense
- Assessing the training required and the availability of skilled talent to deal with new technologies like virtualization and demanding applications like video
- Implementing security across virtual machines and establishing trusted systems for virtualized infrastructure
- Providing the mechanism for differentiating real-time traffic based on context as video becomes more pervasive
- Gaining network visibility into and control of various applications while ensuring that traffic is encrypted as it traverses the network
- Migrating from a Good Enough Network and whether there are design guides to support this migration
- Managing services end-to-end across the network and having the network management tools to support this capability
- Raising the reliability expectations from box-based to service- and network-based resiliency
- Quantifying the business savings, employee productivity, and ROI for new capabilities

The Blind Spots and Other Follies Behind the Good Enough Network

The rest of this paper focuses on some of the pervasive misconceptions, habits of short-term thinking, and misguided ideas that lead organizations to choose Good Enough solutions to their networking needs.

The Application and Endpoint Ignorant Myth

Good Enough Networks operate on the notion that data is data—all just ones and zeroes—while Enterprise Next-Generation Networks are built on innovative products that adjust to the application being delivered and the endpoint device on which it appears.

Let's look at one of the most demanding applications in business use today: video. For an optimal user experience, video requires a network that is media-aware and can track and optimize video flows end-to-end. This way, video applications are treated like a presidential motorcade that requires other traffic to stop as it whizzes by.

Fortunately, vendors like Cisco have developed medianet technology that understands the video endpoint and whether it's a smartphone or a telepresence unit. Additionally, Cisco products can auto-configure and tag the video flow with metadata so it can be understood and prioritized across the routing and switching infrastructure, saving many hours of configuration and providing an optimal-quality experience. With built-in capabilities to inject synthetic video traffic into the network, network planners have an easy tool for preplanning video deployments. For troubleshooting, capabilities like Cisco Mediatrace can look at the video flow on a hop-by-hop basis as it traverses the network to identify congestion or other potential problems.

Let's look at a specific example of an airport that uses 6000 IP video surveillance cameras. This would be a nightmare to set up on a Good Enough Network because each device needs to be configured individually. But medianet includes a feature called Media Services Interface (MSI), which automatically identifies the device and sets up the configuration and the policies associated with each camera.

Recommendation

We encourage organizations to take advantage of these built-in capabilities across platforms from vendors like Cisco. They result in significant savings for service rollout. While a customer may not see these savings if their focus is only on network connectivity, as soon as they try to roll out any services or applications across it, the benefits and savings become very clear.

The Basic QoS Myth

Quality of service (QoS) is an industry measure for how a network should perform. QoS dictates how the network should deliver data, voice, and video under a particular service-level agreement. But today's Good Enough Network is built on the basic QoS standards of DiffServ and is centered on a set of classes or queues on which to qualify a traffic stream. Unfortunately, as real-time video communications becomes more of the norm, the good enough QoS would prioritize real-time video to the video queue, an approach that will not suffice as video traffic increases. What happens when most of the traffic on the network is video? How do you differentiate between different video flows? With the Good Enough Network, it's simply not possible. The result will be loss of video quality or serious impact on other real-time traffic.

Another increasingly common situation in which basic QoS doesn't suffice is customers who implement virtual desktops but want to run interactive multimedia applications on the virtual desktop. Good Enough Networks treat the virtual data stream as data, producing a suboptimal user experience.

Fortunately, vendors who develop products for the Enterprise Next-Generation Network observe trends in the industry and have developed networking infrastructure that enables resource reservation (RSVP-TE) and supports media-aware QoS. Media-aware QoS, also a feature of medianet, tags the application to prioritize one application over another depending on what network resources it needs and what policy the business sets.

Performance testing conducted for Cisco by Miercom on its Cisco Catalyst® family of switches compared Catalyst switches to those of other vendors. These studies showed that when Cisco switches were oversubscribed, only one packet was dropped. Competing switches, however, experienced packet loss rates ranging from 25 percent to 90 percent or more. Catalyst switches are based on custom application-specific integrated circuit (ASIC) architecture that is better able to handle oversubscription than switches built with merchant silicon chips.

"A network switch whose architecture does not provide strict queue prioritization will allow the user experience to be compromised when oversubscription occurs," Miercom stated. But it's not just about giving video priority over data. Network administrators can give business-critical data applications from SAP or Oracle priority over someone's web chat. The beauty of QoS as enhanced by Cisco is that once a policy is set or revised, it is automatically distributed to all devices on the network rather than having to individually configure devices, as would be the case on a tactical network. Again, this saves time and money and provides a better user experience.

Recommendation

If a company has no plans for video applications or rolling out virtual desktops, a Good Enough Network and basic QoS may suffice. If, however, the business wants to take advantage of video conferencing to save on travel costs or to reap the benefits of a virtual desktop environment without compromising the end-user experience, they need to invest in the QoS capabilities available in an Enterprise Next-Generation Network.

Single Purpose Myth

A Good Enough Network is constrained because it is built to serve the single purpose of connecting a user to IT resources. An Enterprise Next-Generation Network can serve multiple purposes, including machine-to-machine connectivity, as may be required for new sensor networks or for data center backup applications. An example of this includes machine-to-machine computing for inventory management by reading RFID tags on materials as they move through the supply chain. Another example is to assist in locating wheelchairs or crash carts in hospital environments.

As mobility demands on the enterprise increase, it becomes critical that an end user is consistently managed as they access the network, whether over a wired or wireless connection. Fortunately, vendors like Cisco have the right converged user and access management for wired and wireless networks in products like Cisco Prime® for Unified Management. Access policy is also administered through integration with the Cisco Identity Services Engine (ISE). Businesses gain complete visibility into endpoint connectivity—regardless of device, network, or location—and can monitor security policy compliance across the entire wired and wireless network.

Additionally, with Cisco technology built for these Enterprise Next-Generation Networks, the capability of the network extends to energy management. As regulations on carbon emissions are being developed and applied, especially in some European markets, businesses need to be ready both to monitor and manage carbon or face significant fines. Currently, office buildings account for 70 percent of business energy

consumption[8]. This includes lighting, heating, and cooling systems in addition to the IT infrastructure.

Cisco EnergyWise is an innovative feature of Cisco Catalyst switches. This new technology manages building systems to improve energy efficiency. The network can tell if a conference room is vacant and power down the lights, HVAC, or other devices. IT managers can set policies based on business needs and power down endpoints like IP phones or desktops based on usage needs. Cisco is also aggressively adopting Power over Ethernet (PoE) technology to use the network to deliver electricity, as well as data, to endpoints. PoE enables the network to control the device—and the energy it consumes—in a way that devices plugged into an outlet can't be controlled. As the number of PoE-enabled devices increases to include access points, downstream switches, and virtual machines, taking advantage of the embedded energy management capabilities in Cisco switches can result is significant savings. And while current PoE technology is limited to devices that consume no more than 30 watts of electricity, universal PoE will support devices running at up to 60 watts.

Recommendation

Customers investing in networks for a single purpose are missing opportunities to use the power of the network to improve carbon footprint, save energy costs, and provide unified management for wired and wireless networks. A more strategic and cost saving option is to invest in EnergyWise and the Cisco Prime management portfolio.

Basic Warranty Myth

Customers often hear that products come with a lifetime warranty, and this is usually the case for products that have few moving parts. Often Good Enough Networks come with a form of limited support for maintenance and a warranty statement. Customers should clearly understand what this actually entails and be cautious. With some vendors, a warranty service call consists of advice to reboot the troubled machine and if that doesn't work, ship a replacement. There's no effort made to troubleshoot the problem. Worse yet, service is often provided on a first-come first-served basis, with no effort to prioritize calls.

Enterprise Next-Generation Networks understand that customers need more than a hardware warranty and basic support if the network is critical for the business. Companies that design for next-generation networks offer warranties, but they also offer smart services, including technical and professional services. Many of these smart services are software-enabled—they proactively seek out, diagnose, and remediate issues before they even become problems. This can improve the uptime of networks as well as the user experience.

---

[8] Energy Information Administration, Commercial Building Consumption Survey.

The unique services that Cisco offers utilize the intellectual property that Cisco has built up with over 20 years of supporting its customers' networks, as well as the knowledge gained from multiple scenarios and customer environments where Cisco is deployed.

Basic warranties also don't account for the business cost of downtime. Companies lose an average of 3.6 percent of revenue per year to downtime, according to Infonetics Research.[9] Unplanned downtime also damages the reputation of the business, a significant cost even if it is difficult to quantify. If a company makes that narrow TCO calculation of upfront discounts on products and maintenance, they are not looking at the total operating environment that they're actually creating.

Recommendation

Service contracts and warranties are not created equal. You usually get what you pay for. Unfortunately, you never realize how good a service contract is until you need it. Be prepared and look at the fine print. Cisco has won multiple industry awards and receives high satisfaction ratings on support like Cisco SMARTnet® service.

Security as a Bolt-On Myth

Good Enough Networks deliver "bolt-on" security, which typically consists of more point products that don't communicate with each other very well. Often, different point products are stove-piped so different security elements don't share information, which makes it difficult to create consistent security across the entire IT environment and can leave the customer exposed to costly security incidents. Network security has to keep pace with an ever-changing threat profile and the increased use of mobile devices. Security risks are everywhere. There's been a 46 percent increase in the spread of malware on mobile devices in 2010 while at the same time, 20 percent of workers have left devices unattended, and 46 percent have let others use their devices.

While Good Enough Networks advocate the bolt-on security methodology, what is actually needed is pervasive visibility and control that uses the power of the network to enforce security policies. Cisco offers the Cisco SecureX architecture. It delivers pervasive visibility and control with full context-awareness to provide security across the network, from headquarters to branch offices, for in-house employees and remote workers on wired or wireless devices. An important aspect of SecureX is context-aware policy with distributed enforcement delivered through the Cisco Identity Services Engine (ISE). As the industry's only network-wide policy engine appliance, ISE creates, distributes, and monitors policies based on a contextual language, such as who, what, where, when, and how. Enforcement may include actions such as blocking access to data or devices or initiating data encryption.

For example, when an employee connects to the corporate network from a smartphone, the network identifies the device and the user as well as the privileges granted them. If Bob is in marketing, then based on the business policies, he can access marketing materials but not the payroll server. Or if Linda is in finance, she can't access financial information from a coffee shop Wi-Fi connection. However, the same location-based policy will allow her to access this information at her office behind the firewall. Cisco ISE not only establishes policies for each device and user, but also shares these policies with all points on the network, and instantly updates information when a new device appears on the network.

As the trend toward cloud services accelerates, the network can be the facilitator or the impediment in the effort to securely adopt cloud capabilities. A critical element of the SecureX architecture is the market- leading security solutions delivered by Cisco ScanSafe Web Security. With the flick of a switch across a widely distributed network, businesses can intelligently redirect web traffic to enforce granular security and control policies. Companies without a next-generation network will face significant challenges in the move to cloud-based computing and services.

---

[9] The Costs of Enterprise Downtime, Infonetics Research.

Recommendation

Seek vendors who look at security holistically and understand that threats have multiple vectors. For example, a spam email may lead to a site containing malware that can take control of a personal computer, making it part of a botnet. But by consolidating on a single vendor with a holistic security strategy, business can get firewalls, VPN clients, web content security, and a centralized, global threat correlation engine that delivers critical intelligence and protection.

Acquisition Cost Myth

Generally, in building an IT network, about 20 percent of the budget is for acquiring the hardware and 80 percent is for operating costs. But saving money on that 20 percent upfront can be more than offset by increases in the 80 percent if, for example, there are higher integration costs, more downtime or serious security breaches. While Good Enough Network vendors ignore these costs, Enterprise Next-Generation Network vendors promote a systems approach that not only reduces networking costs related to the 80 percent of the pie, but also drives IT service improvements and new business opportunities.

This is the approach endorsed by industry experts: "The integration of the network with business processes and applications requires that organizations treat the network as a holistic entity by taking a systems approach," said Zeus Kerravala of the Yankee Group.

Enterprise Next-Generation Network vendors like Cisco understand the costs involved in integration. As a result, they invest in testing and documenting systems to ease network IT acquisition, configuration, and deployment. Cisco accomplishes this through its Smart Business Architecture (SBA), a set of pretested and preintegrated solutions. SBA solves the problem presented by tactical networks that cobble together a variety of point products, which the customer has to then assemble. SBA does that ahead of time with tested and proven systems.

Acquisition costs don't take into account capabilities like its exclusive in-service software upgrade (ISSU) technology that keep the business running, ISSU eliminates the downtime costs associated with software upgrades and can deploy an upgrade in less than 200 milliseconds without having to take the network down in order to do so. In some mission-critical situations such as global financial trading systems, the network simply can't be taken down because it would be too costly. With ISSU, upgrades can be done without interrupting production. ISSU offers many benefits to the bottom line of an enterprise. It means the benefits of an upgrade become available sooner than if people had to wait until 1:00 a.m. Sunday when it would be least inconvenient to take down the network. Not only would upgrades happen faster which saves labor costs, the enterprise also saves the labor costs of having technicians do that work late at night.

Recommendation

Customers need to include the cost of integration and system testing of the solution that they deploy in their network. Unfortunately, this can be lost in financial calculations that focus merely on capital acquisition costs. Although some customers make decisions based on their capital budget, we encourage a business view that looks at the complete financial impact. We believe that when this is taken into account, the tactical network quickly becomes the more expensive network.

Just Look for Standards Myth

The tactical Good Enough Network advocates being "standards based," taking the approach that if a customer buys industry-standard servers, storage, and networking technology, they will save money. The theory is that the network will be easy to set up and everything will work together because it's worked in thousands of other businesses.

Cisco has a deep respect for industry standards and participates in many of the standards bodies. However, vendors interpret and deploy standards differently in their equipment, which may result in integration challenges. While industry standards are extremely important, relying only on existing standards as you plan for future needs is misguided. When companies lock themselves into standards-based networks, they miss out on higher-level service innovation and occasionally underestimate the integration cost involved in making the components of a standards-based system work together. Standards should be used but businesses looking for a competitive edge should to offer solutions that are also innovative.

Let's look at a few examples. Consider the Cisco Discovery Protocol (CDP), for instance. Cisco developed CDP years ago as a way for the network to discover the device being plugged into it and to apply the appropriate configuration. Medianet was the next advance in CDP. Today, Link Layer Discovery Protocol (LLDP) is an industry standard based, in part, on Cisco's innovation.

Cisco is developing innovations for the virtual data center with technology such as Overlay Transport Virtualization (OTV), which allows a customer to combine two or more separate data centers into one virtual data center. Cisco also just introduced the Locator/ID Separation Protocol (LISP), which can move a virtual machine carrying workloads between data centers without having to change the address of the virtual machine. These innovations avoid the complexity of managing protocols such as Multiprotocol Label Switching (MPLS) and reduce other administrative tasks; this, in turn, leads to quicker time to deployment, all of which saves money.

Cisco has also fundamentally changed the way networks are designed with Virtual Switching System (VSS) technology, which satisfies three major demands of networks for high availability, better capacity utilization, and simplicity. VSS combines two Cisco Catalyst 6500 Series Switches into one logical switch, with the immediate benefit of reducing the number of switches that have to be managed by half and doubling the redundancy. In addition, with VSS the access layer device doesn't see the merged switches as two separate data paths but as one giant pipe. The cost savings are in reduced device management expenses, improved uptime, and greater utilization.

Recommendation

Standards are important, but businesses also seek innovation in how they collaborate with their end customers, and in how to better manage their infrastructure and how to reduce complexity. This often means investing in next-generation technology that may not yet be standards-based. Whatever future technology a customer chooses to invest in, they should select a vendor who is committed to making it a standard.

Net Results

Our research found that low-cost, tactical networking vendors obfuscate the real total cost of ownership by basing it solely on equipment and maintenance pricing. They also ignore the added expense to the customer to integrate disparate technologies (or the cost of hiring an integrator). Integration costs aren't just imposed at the beginning when the network is set up; they can be ongoing. Integration issues come up at the time of system upgrades and when a breakdown occurs, and locating and remediating the problem is complicated by trying to determine who owns the problem. Integration issues cost the customer time and money that can be avoided with a single-vendor network. A limited TCO calculation also ignores the possibly of increased downtime if low-priced equipment results in increased support calls, which also cuts into revenue and productivity.

In any market, there are people who buy on price and people who buy on value. But given the millions of dollars enterprises spend on IT—even for the "good enough" stuff—and given how strategic IT is to the success of any business, buying IT based solely on initial price is limiting. A network some consider "good enough" is actually not good enough:

- Good enough isn't good enough on a network dominated by video traffic.

- Good enough isn't good enough for security where mobile devices are misplaced or stolen and the malware threat continues to rise.

- Good enough isn't good enough for downtime, which costs companies an average of 3.6 percent of revenue per year.

- Good enough isn't good enough for energy efficiency in a world where 70 percent of energy consumption is by office buildings and can be better managed.

- Good enough isn't good enough for customers who increasingly rely on social networks to make purchase decisions, usually on mobile devices.

- Good enough isn't good enough for employees who want the flexibility to work remotely on devices of their choice.

There are some vendors that say the network just connects things. To accept a tactical network as all that a company needs is to believe that network innovation has ended. Our customers view the network as a source of innovation and one of the most strategic assets in IT.

TCO calculations based solely on capital expenses and operating expenses are useful, but it's also important to consider the number one constituent of that network, which is the end user. Networking industry standards are very important, but they must serve innovation, operational efficiency, and service excellence. Companies that settle for tactical networks will miss out on the business benefits and customer engagement enabled with a next-generation network. Simply put, a good enough network is not good enough.