SCC Sequoia

Solutions that Endure

NETWORK INFRASTRUCTURE – Time to think about it is NOW!

Prof. Terry D. Curtis, JD, Associate Dean, Communication Faculty
at California State University, Chico, © 2015, SCC Sequoia

It's time to think about your network infrastructure. That sounds silly, I know. Every CEO and CFO is aware of the complexity, architecture, and cost of the corporate network. But two ongoing changes in corporate IT have made it essential to revisit the essentials of network operation, management, and security.

Let's start with the cloud. Cloud computing terminology is shorthand for centralizing various parts of IT - data warehousing, application management, data processing, data mining, etc. In a private cloud, the centralized functions are internal to the organization. In a pubic, cloud, the centralized functions are outsourced. Both private and public cloud computing services are being used

1. In pursuit of economies of scale through centralized, shared IT functions,
2. To facilitate rapid deployment of new applications to end users and new services to clients and customers,
3. To ensure consistent currency in applications,
4. To ensure consistently formatted data records and minimize data dropout across systems.

In addition, public cloud computing (shared virtual) services are being implemented to outsource the risks and management burdens of technology upgrades

These efforts have been underway for some years now, and momentum is building. There is evidence that each of the objectives listed above is attainable in some measure. There is also evidence that network data traffic patterns driven by cloud computing are significantly different than the patterns consistent with traditional client/server architectures for providing IT services. These differences occur within the data centers where cloud services are provided, among multiple data centers maintained for redundancy and reliability, and between data centers and end users.

To achieve agility, reliability, and efficiency in provision of services through the cloud, the configuration of network infrastructure over which those services will be accessed and provided will need to be regularly and repeatedly optimized for new patterns of traffic. Manually redesigning and re-provisioning network capacity won't handle the job. The solution will come from software defined networks (SDN), with network management systems that are constituent elements of service management and business intelligence systems. As businesses change, and the services necessary to support them must consequently change, necessary modifications in the network over which those services flow will need to be predicted, designed, and provisioned. Most corporate networks are currently being managed as reactive, infrastructural cost centers. They need to become strategic proactive elements of business planning, with both their potential and their vulnerabilities made visible through the lenses of business intelligence and service management.

Now let's turn to the changing nature of IT security threats. Not so long ago, defending against IT security threats was somewhat akin to defending your home against the threat of burglary. The threat was real, but attempts were rare and the primary defenses were the IT equivalent of strong locks and alarms. But the nature of the IT threat has changed over the last few years, with the changes gaining momentum in 2012. The nature of the threat is now more analogous to swarming mosquitoes on a late summer day in Alaska. And some of them carry fatal disease. Advanced persistent threats (APT) are beating a tatoo on everyone's networks, with multiple malicious objectives, from corporate and state-sponsored espionage to insider sabotage. The proliferation of wireless mobile devices being used to access the network, as well as the migration of corporate resources to the cloud have massively increased the potential points of access for attackers.

Much of the defense against this new storm of security threats will depend on education and motivation. Security and convenience are mutually inconsistent values. A campaign to match - or even exceed - the WWII *Loose Lips Sink Ships!* effort will be necessary. But much of the defense effort will have to be in network design and management. Each of the three parameters of network security -

confidentiality, integrity, and availability - requires rethinking in the new environment.

Granular access control isn't easy to administer, but if we are going to ask our employees to sacrifice convenience in order to maintain security, then the organization has to walk the talk. Authentication and access controls must be tightly tied to the importance of the resources to which access is sought. Espionage and sabotage are aimed at the crown jewels: trade secrets; strategic plans; competitive analyses; and audits of vulnerabilities. No one should have access to any resources not relevant to her/his position. And all access to corporate resources through the network must be logged and audited. Consider Edward Snowden.

Access through mobile devices, over wireless networks, poses new and different risks. And the evidence is that employees have strong preference for using their own devices. If employees want to use their own mobile devices to access the network, then there need to be different access rules for different devices used by the same person - devices that aren't owned and controlled by the organization should require more secure authentication and shouldn't be allowed the same degree of access.

Cloud computing raises issues of both confidentiality and integrity, not only because of the network connections through which these services are accessed, but in the public cloud also through the sharing of resources. Virtualization, which means making a shared resource seem like parts of it are dedicated to each of its users, creates potential points of entry that don't exist in private IT infrastructure. Even in the private cloud, access to shared resources puts extra pressure on access controls, transparent accountability for changes, access logging and audits. For services provided in the public cloud, there must be instantly accessible reporting on performance according to explicitly set service level agreements as to security events, such as attacks, breaches, viruses, denied hosts, and denied protocols.

These last two types of security events are attacks on the third parameter of security, availability. All organizations' networks, and especially those in the gaming and financial sectors, are vulnerable to distributed reflection denial of service (DrDoS) attacks that have peaked at 120Gbps of traffic aimed at one IP address. The appropriate place to defend against these attacks is upstream from the targeted resources, either at the edges of the network or as a cloud-based service from network service providers. In either case this requires dedicated hardware and elaborate monitoring and reporting.

To sum up, cloud computing and security threats have added new concerns to the design, architecture, and management of corporate data networks. It is time to rethink them.

ABOUT THE AUTHOR – Professor Terry D. Curtis, JD, serves as the Associate Dean of the Communication Faculty at California State University, Chico. Additionally, he has served for well over a decade as a member of SCC Sequoia's Core Team. His focus is the strategic application of new information and communication technologies (ICT). He is a member of the State Bar of California with expertise in the regulatory and legal constraints on the application of new ICT. He has assessed network architectures and performed reliability analyses, and has developed evaluation metrics and meaningful SLAs with service providers. He has a BS degree from UC Santa Barbara, a JD from the University of Chicago, and a MA from the University of Southern California (USC). His email address is tcurtis@csuchico.edu