

# COMMUNICATING WITH SAM

## Intelligent Networks Require Intelligent Switch Architecture



Sam Johnston

### Question:

Our LAN infrastructure was designed and implemented to meet our network requirements for Y2K. It consists of numerous workgroup switches uplinked together into another workgroup switch acting as our main data server switch. We have a variety of 3COM, Cisco and DLink switches in our network. My predecessors just added another switch as we need more ports. The current total port requirement is 225 ports in our main computer room with 2 remote closets with 50 users each closet. Recently we have been having network slowdowns

and it is difficult to pinpoint the problem and figure out a solution. My management wants to deploy new applications to enhance employee productivity and security of our information. Obviously we aren't ready for new applications until our infrastructure is upgraded. What key features should I look for in my replacement switches and how can I deploy the switches in a manner that will maximize flexibility and efficiency?

### Response:

The first step in planning your replacement switches should be an enterprise architecture design. You should be looking at your switching requirements from a capacity, throughput, scalability, redundancy, resiliency, security, and operations point of view. Once you have completed your architecture, then you can work on reviewing features and vendors to select the best solution for your needs. How well you design your network will influence how easily you can add business applications and sustain rapid growth to meet changing business needs.

Network Design in medium and large organizations follows the traditional layered approach consisting of different layers with different capabilities. **Figure 1** is an outline of the layers most commonly deployed in large data centres with an outline of key characteristics within the layer.

The benefits of a layered approach to the infrastructure is that it permits rapid growth and scalability at various levels within the network, it permits easier troubleshooting, it can be designed to reduce the scope of L2 issues, and it facilitates the design and implementation of security mechanisms within the enterprise to ensure that the appropriate users and systems can be isolated.

Depending upon the size of the deployment, it is not always economical to include all the layers within an enterprise and sometimes with smaller deployments the core layer will be rolled up into the distribution layer. In other cases all three layers may be rolled up into a single computer room

implementation with a single set of stackable switches or chassis based solution, in which the capacity of the system exceeds the total number of ports required. The geography of your wiring closets will dictate, to a degree, how much you can collapse your infrastructure if you want to. ➔

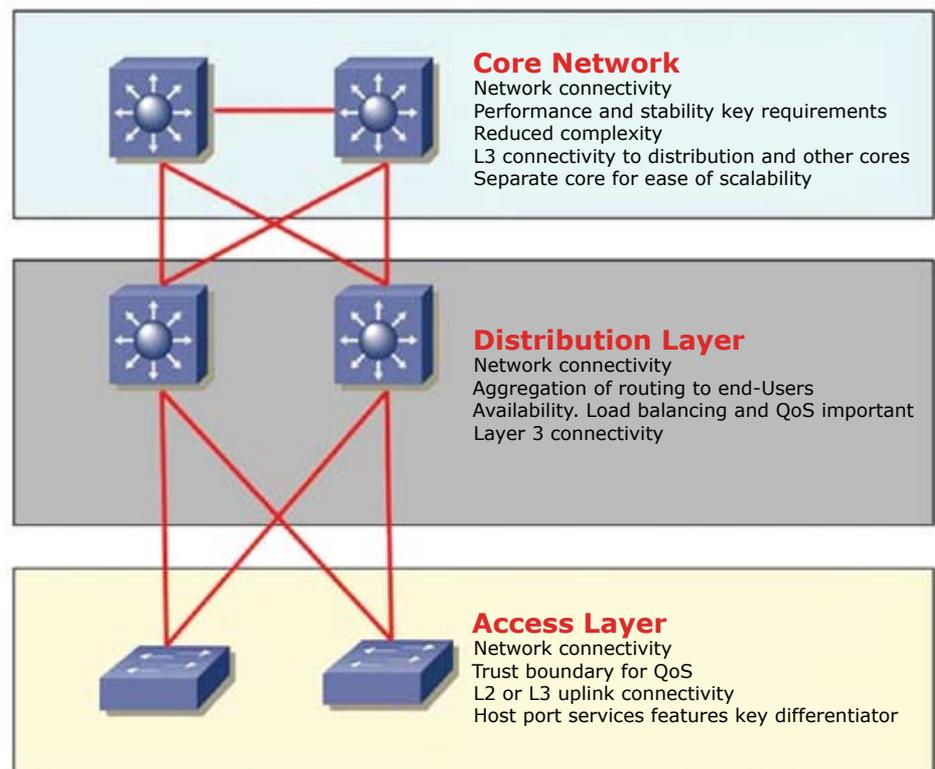


Figure 1.

Keynote speaker  
Paul Tuohy

# TEC '007

Education: Shaken not stirred



Are you  
licensed  
to skill?

Plan to attend **TEC '007**, TUG's annual three-day secret Technical Education Conference & Showcase at the Sheraton Parkway Hotel, Richmond Hill, Ontario April 17 - 19, 2007.

The conference includes: two full days of tutorials, plus hands-on labs on Day 3 · complimentary lunch at the Vendor Showcase · sit-down luncheon at the Keynote Address · optional Executive Breakfast · certification exams · top-drawer speakers · technical & professional development topics · and special agent handouts from Q-branch.

**Sign-up any time before Feb. 28,** and receive an early-bird discount! Regular Price: \$795 (members) **Discount Price: \$745 (members)**

Contact Miss Wendepenny at the TUG office: 905-607-2546, admin@tug.ca

**TUG**  
TORONTO  
USERS GROUP  
for System i

Based upon your port breakdown you could consider 3 high-level options within your network:

- (i) You could look at installing a chassis based solution in your computer that can act as core/distribution and access and run fibre to your remote closets where access switches are installed, or
- (ii) you could leverage workgroup switches in a stacked configuration in your computer room with the same configuration as (i) for the remote closets, or
- (iii) you could install a distribution layer set of fibre switches as aggregation points and install separate access switches for the access layer and server farm top of rack switches.

All solutions have their benefits and all solutions should be designed with redundancy and high availability. In option (i) the chassis can have dual power supplies, you can configure dual switching engines and redundant fans and provision redundant blades for the connections. For option (ii) usually the redundancy is limited to intelligent stack technology supporting a single switch failure. For option (iii) the redundancy should be configured in dual distribution switches linked in a stack and redundant uplinks to the distribution switches so there is no single point of failure. Typically "out-of-the-box" redundant power supplies can be used for the workgroup switches if desired.

Where possible it is a best practice to leverage L3 uplinks between switches to limit the scope of the L2 domain and enable faster convergence and load balancing technologies to take over and assist in performance.

Operationally, all solutions implemented should be configured with the appropriate support and maintenance agreement with a trusted and skilled third party offering round the clock support for the mission critical network. Additionally, network management systems should be appropriately deployed. This would include notification and alerting for fault or threshold conditions and stats and log

gathering for more proactive network capacity and health reviews. Having the discipline of monthly reporting is highly recommended as it forces a continuous look at the network capacity.

Security is also a key enterprise network consideration and while it can be a topic unto itself, I would like to quickly address how an effectively architected network can assist in the deployment of security devices. For example, Intrusion Prevention Systems (IPS), Network Access Control Appliances (NAC), and firewall devices are usually installed inline. Therefore, if you have separated the key network components in your network then the implementation of these devices is much more effective, as traffic paths are already determined within your network. In the event of a single chassis solution, the key network hardware vendors will have solutions on blades that can be virtually configured to be inline in the data path.

Now that you have an overview of the key architecture points lets spend a few minutes discussing key features of your switches. The first key investment protection question you should ask is whether you are considering an IP Telephony solution in the future. If so, you should provision—at a minimum—your access switches with Power over Ethernet POE support. I would also highly recommend that you pick a single switch vendor for your enterprise and stick with this vendor.

Do not make switching infrastructure decisions based on price alone. Ensure that the vendor you choose has a wide variety of products for each layer within the infrastructure, is supporting industry standard applications and ensure that the integration of the platforms with peripherals such as security devices for LAN and wireless network are a consideration.

Additionally, strong Layer 3 support and QoS are key in today's evolving networking space. One example of an integrated solution is Cisco access switches, which are 802.1x aware. This means that all switches can talk to a central server for authentication of end users and the feature is extended across multiple platforms to fit within the enterprise. If you always shop

for the cheapest switch ports, the features required for an intelligent network may not be present or compatible with other elements of your environment.

Speed is also emerging again as a key feature in switch requirements. 1Gb Servers have been around for years. The migration of 1Gb Ethernet to the desktops is starting to gain momentum as new applications come on stream. 10Gb Ethernet core switching will become more common as desktops get faster and storage devices based on Ethernet take over from Fibre Channel-based solutions. Even though you may not need that speed today, a well-designed network will be able to accommodate this requirement with a minimal investment and effort when you decide it is necessary.

Ethernet switching technology is the foundation upon which today's information services are built. Providing these services in a cost effective, secure, and scalable manner requires a solid design methodology and a robust compatible set of features across the switching platform. An intelligent enterprise architecture design will lead to an intelligent multi-service network. 

---

**Sam Johnston** is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at [sjohnston@intesys-ncl.com](mailto:sjohnston@intesys-ncl.com). Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday February 9, 2007.