



THOUGHT LEADERSHIP ZONE: INFORMATION INFRASTRUCTURE

SUMMARY

- The pressures on IT infrastructure to support business needs results in the majority of resources being spent on maintenance and routine operations in a running battle with productivity-impacting network degradation.
- To free resources and enable IT to play a greater strategic role, many of these routine tasks need to be automated. But this predicates that network infrastructure elements possess of the necessary intelligence to feed the management tool with the information it requires to build a unified view for automated network management.
- Therefore CIOs need to rethink their view of IT infrastructure, beyond the traditional view of the network as a dumb carrier of data to an intelligent infrastructure that enforces security, enhances application performance, enables converged applications, automates routine operations and provides network management information.

For more infrastructure resources go to www.itleadershipforum.com/infrastructure

The value of the IT infrastructure to today's businesses can hardly be overstated. Organisations look to their corporate network to provide the connectivity between their employees and external business partners that is essential to the information flow on which business thrives. And for many, the infrastructure is a source of revenue in the form of web-based sales.

However, the demands on the network infrastructure are growing. Employees expect seamless access to and rapid response from applications such as ERP, CRM and legacy databases; they expect constant availability and rapid deployment of new applications and systems. Customers expect an instant response, 24/7 availability and unbreakable security from self-service applications such as online ordering systems.

To these demands are added the growing number of desktops, the increasing variety of applications using converged media, multiple heterogeneous systems, the rollout of web-based applications which consume 10 to 20 times the bandwidth of their conventional client-server predecessors, the clamour for remote and mobile access at LAN-equivalent performance levels, ever-more sophisticated cyber attacks, and the need to manage data within an increasingly complex and stringently enforced regulatory framework.

It is little wonder, then, that in a survey of \$1 billion-plus-turnover European enterprises conducted by Forrester Research, the issue that enterprise IT infrastructure managers said they struggle with most is ensuring consistent end-to-end application and service performance guarantees.

NETWORK DEGRADATION

For IT, the day-to-day management of enterprise infrastructure is a constant battle

with network degradation which strangles the free flow of information. Over the course of a year, productivity losses from mundane network degradation are far greater than from total network outages. According to Infonetics, outages account for 31 percent of productivity losses in large organisations; degradation for 69 percent.

Consequently, IT spends much of its effort in routine operations. IDC estimates that 70 percent of IT budget and time is spent maintaining existing systems.

AUTOMATION

Network maintenance cannot be shirked, but the proportion of IT department resources spent on maintenance and freeing up time to tackle strategic initiatives is through automating as many of the maintenance tasks and routine operations as possible (see [box-out!] [Automating routine operations, page 2](#)).

Therefore, CIOs need to rethink the role of infrastructure. The elements that make up an organisation's IT infrastructure – switches, routers, cabling etc – may be very familiar, but the resulting whole is not just dumb pipes.

Infrastructure should have integrated and distributed intelligence to manage information flows by enforcing security, enhancing application performance, enabling converged applications, carrying out provisioning tasks and providing network management information that allow the CIO to align network resources with business objectives.

ENFORCING SECURITY, ENHANCING PERFORMANCE

Through automated and pervasive security systems, infrastructure is critical in enforcing total enterprise security. Beyond the role of firewalls and intrusion prevention systems (IPS), the individual elements and overall

in association with





THOUGHT LEADERSHIP ZONE: INFORMATION INFRASTRUCTURE

AUTOMATING OPERATIONS

Benefits of automating routine tasks:

- Decreases costs by requiring fewer IT staff, less training and enabling IT expertise to be centralised.
- Increases the availability of applications by reducing human error and time-to-fix.
- Increases productivity through improved security and more efficient technical support
- Increases IT personnel productivity to concentrate on strategic and tactical initiatives for the business

Tasks suitable for automation:

- configuration changes
- deployment of new equipment
- network monitoring
- traffic control
- network access control
- network protection
- remote technical support
- end-user initiated service requests

For more infrastructure resources go to www.itleadershipforum.com/infrastructure

intelligence of the infrastructure should combine to provide access control, user and device authentication and quarantine services to contain and eliminate threats. Switches should segregate network traffic into virtual LANs, thereby improving data integrity, security, manageability and performance for applications. Access control lists should control traffic to and from the VLANs on a per-IP address basis, reinforcing security by preventing unauthorised access.

Switches should have firewall-type capabilities to filter traffic based on user, device or traffic type, permitting limited access or denying access altogether accordingly. They can use this information to control how users access the network, what they can access, and the performance they experience, setting service levels appropriate to the type of access.

For example, you would permit a customer accessing an order-entry system by mobile phone only very limited network access, but you would want to give priority to the traffic so that the customer experiences a high level of service performance.

PROVISIONING

Infrastructure elements should have sufficient built-in intelligence to enable provisioning tasks to be automated to the point where deployment requires little human intervention. This "low-touch deployment" can be achieved by configuring network parameters in an infrastructure management tool so that when a new device is connected, provisioning occurs automatically.

Changing the infrastructure manually can result in poorly configured or conflicting network nodes which will disrupt applications and cause expensive network degradation. Hence most analysts recommend implementing automation technologies and a change management

process based on the IT Infrastructure Library (ITIL) standard for best practice.

Therefore, CIOs should ensure that the core switching products acquired at IT departmental level contribute to the overall security, convergence and intelligence of the company infrastructure. This is not about a checklist of features, but how the features are integrated over the whole infrastructure. Clearly, infrastructure elements based on open standards are critical to achieve this.

NETWORK MANAGEMENT

To automate routine tasks beyond the simplest level requires a holistic view of the infrastructure via a comprehensive network management tool. Without this global view of the network it is impossible to predict what effects the changes, manual or automatic, will have.

This is especially true when converging media types. In fact, analysts at Gartner say that without a robust network management structure, converging data, voice and video cost-effectively is impossible.

In many organisations, network management tools have proliferated in an unplanned manner. This can create problems where one automated management tool, governing, say provisioning, allocates bandwidth and server resources to a session that the security management tool has identified as a denial of service (DoS) attack. The result is that the provisioning tool adds fuel to the DoS fire which the security system is trying to extinguish. Clearly, there is a need for these disparate tools to communicate.

Intelligent infrastructure elements that are based on open industry standards can be of assistance here, providing the information required by network management tools to furnish a single view.

in association with





THOUGHT LEADERSHIP ZONE: INFORMATION INFRASTRUCTURE

CONVERGED APPLICATIONS

Organisations are looking to deploy web-based applications and applications converging different data and media types, for example, voice over IP (VoIP) to take advantage of IP telephony facilities such as automated call distribution, mobility and conferencing.

These demand an intelligent and feature-rich switching infrastructure to manage the real-time nature of voice communications. See [\[boxout2\]](#) Voice over IP, pages 4 & 5.

Quality of service (QoS) capabilities are required for latency-sensitive traffic, such as voice, and for business-critical applications and information flow. At the same time, bandwidth management is required to align network resources with business priorities so that bandwidth-hungry converged applications don't consume more resources than is appropriate to their business use and to ensure that non-business traffic, such as music downloads, online sports commentaries and movie trailers, is throttled off.

For more infrastructure resources go to www.itleadershipforum.com/infrastructure

However, flagging a problem with a network element is of little use without knowing how it will affect real business operations. Thus network management tools need to show a view of the infrastructure mapped to business processes, using application behavioural patterns learned over time. IT management needs to know which applications, processes and users are affected when an application exceeds acceptable behavioural thresholds so that they can schedule resources appropriately to investigate and fix the problem. In addition, IT personnel need to know which particular network device needs attention.

VOICE OVER IP

The financial and efficiency benefits for organisations moving from separate voice, video and data networks to a single integrated voice and data IP-based infrastructure are well established. Broadly they are: cost savings from maintaining one instead of two or more networks and reduced call and service charges; and the flexibility that comes from integrating voice and video into business applications enabling organisations to use a mix of services – fixed line, wireless, email, IM, audio and video – to communicate with employees, customers and other business partners.

More cost and efficiency benefits will be realised as VoIP technologies develop. For example, the most recent VoIP systems enable calls to be routed so they “hop on” the company WAN and “hop off” at the location that offers the most savings.

Currently VoIP is used mainly to connect multiple disparate intra-company sites, for example, providing retail outlets with low-cost and flexible voice communications with each other and head office.

The next stage, which some leading-edge organisations are adopting, is to provide indi-

vidual remote and mobile workers with voice facilities that are equivalent to those afforded to office workers.

For example, using an IP soft-phone on a laptop, mobile employees can have the same feature set, such as voice mail, and voice quality as if they were at their desk. The VoIP system handles calls in IP from end point to end point, using QoS to manage latency at every hop of the route by prioritising voice traffic over less time-sensitive traffic such as email.

IP mobility facilities are a boon to workers who frequently roam on campus and the organisation will benefit from the reduced call charges and added security.

To use such applications does not require wholesale replacement of a legacy PBX: they can be deployed selectively and used alongside the PBX until the organisation is ready to deploy IP telephony exclusively throughout the organisation.

VOIP SECURITY

Many organisations gamble with VoIP, leaving the firewall open for VoIP traffic and applying low-level encryption as a form of protection, trading off the risk of attack against the convenience and cost reduction VoIP brings.

However, massively parallel intrusion protection filters mean can inspect voice packets without causing latency. Sophisticated systems will isolate the IP end point – say an IP phone identified by individual MAC address – onto a virtual LAN of its own.

Such a system can further be augmented by security modules that sit behind the firewall and add more encryption and virtual LAN capability to IP telephony. As soon as a remote user plugs in an IP phone the module authenticates it and encrypts the traffic.

in association with



THOUGHT LEADERSHIP ZONE: INFORMATION INFRASTRUCTURE

CONCLUSION

IT infrastructure can no longer be regarded as a system of dumb pipes carrying data. Infrastructure elements need to have integrated intelligence to enforce security, enhance application performance, enable converged applications, automate routine operations tasks and provide network management tools with information to construct a single view of the network.

As organisations move to converged data, voice and video networks, the built-in intelligence of their infrastructure becomes increasingly important.

Therefore, CIOs should ensure that the core switching products acquired at the IT departmental level contribute to the overall security, convergence and intelligence of the infrastructure, ensuring the free flow of information throughout the organisation. This is not about a checklist of features, but how well the features are integrated over the whole infrastructure.

For more infrastructure resources go to www.itleadershipforum.com/infrastructure

© 3Com 2006. All trademarks used are the property of their respective owners

JERSEY'S CONVERGED NETWORK

The island of Jersey has been a UK Crown Protectorate for eight centuries; its autonomous government, States of Jersey, administers public services for nearly 90,000 citizens, barring defence and foreign policy.

As States of Jersey (States) began to streamline 47 departments into 12 ministries in 2002 under its "States of Change" programme, it became apparent that the communications infrastructures posed a major barrier to delivering services efficiently.

Using more than 30 separate PBX systems, some 60 percent of the island's 7,500 government employees lacked voice mail or department directories, making it difficult to process callers' inquiries efficiently. Departments also were paying for interdepartmental calls.

To improve services, States of Jersey sought a secure, converged voice and data network that would reduce costs, increase productivity, and accommodate growth. The protectorate also wanted the voice solution to enable it to provide callers with a single phone number to reach any government resource.

WHY 3COM

States of Jersey evaluated VoIP offerings from 3Com, Cisco, Nortel, and Marconi Soft Switch. The government chose 3Com secure, converged network solutions because they offered the highest levels of security, reliability, scalability, and industry-standard converged services at the most affordable price point and with the lowest cost of ownership. 3Com Global Services also provided project management, system design and implementation, training, and support

States' 3Com secure, converged infrastructure is based on two redundant, carrier-class 3Com VCXV7000 IP Telephony Solutions that provide non-stop telephony services using resilient dual fibre channels. The modular VCX solutions reside in the St Helier General Hospital, which has the largest voice and data requirements, and in Cyril Le Marquand House, where the States' IT team, judiciary, and most administrative ministries are located.

BENEFITS

The systems connect seamlessly to States' 3Com Gigabit data networks, which provide email, web access, and shared applications, and to five pre-existing 3Com NBX 100 IP telephony platforms, which deliver premium quality voice services to the island's library and schools. They perform call control, signaling, application creation, and media control independent of access medium and speed.

The 3Com solution also provides a single phone number to the government call centre. States users can also make and receive calls from their computers using 3Com VoIP handsets and quickly transfer callers between offices using the online central databases of government services.

Using its 3Com solution, States of Jersey eliminated redundancies and incompatibilities between ministries, dramatically increased productivity and will save more than US\$1.5m annually in telephony costs, such as line leases, equipment service and replacement, and charges for long-distance and interdepartmental calls. The solution will also accommodate the States' future plans for wireless services and audio/video/data conferencing.

in association with

