
soap
HTTP
SSL
XML
QoS

++++network agility++++++++++++++++

Here comes the SON

SOA and web services place unprecedented demands on networks to be more intelligent and proactive than ever—in other words, to be service-oriented.

BY BILL LABERIS

Illustration by Chris Sharp

Thirteen years ago, the following words appeared in the conclusion of an editorial in the *Wall Street Journal* on the subject of deploying a new enterprise information technology: "Just bear in mind that there are serious consequences to rushing this process beyond the ability of the underlying technology to sustain it."

I wrote that article, and I was talking then about client/server computing. But these exact same words could be written today—a technology-generation later—as organizations around the world rush to deploy solutions based on service-oriented architecture (SOA). The core issue is that a traditional network infrastructure cannot and will not support SOA traffic without suffering serious performance, reliability, and security problems.

What's needed is a service-oriented network, or SON. A principal feature of a SON is having network devices that are far more intelligent than those found on traditional networks—devices that recognize that SOA traffic is fundamentally different from other network traffic. The SON must clearly and unambiguously understand web services language while loosely coupling network resources. Then the SON must virtualize these resources and the commands and business logic to execute the transaction.

Trouble that slips beneath the IT radar

Oddly enough, many IT managers have yet to grasp this reality: Yesterday's network won't support tomorrow's applications. In the last year, both *InfoWorld* and *NetworkWorld* fielded major research surveys of senior IT managers regarding SOA plans. When asked what obstacles might litter the path to broader SOA deployments, respondents in both surveys cited factors like security, organizational barriers, and slow standards development at the top of their lists.

Surprisingly, very few managers considered that their traditional network infrastructures very well may not support this new and different kind of network traffic. The ones who didn't are dead wrong.

For starters, SOA is heavily standards-based compared with non-SOA environments, where applications and databases have their own servers to communicate relatively simply from one server to another. Also, SOA relies on XML and SOAP (Simple Object Access Protocol) as communications protocols. "XML is text-based, big and bulky," notes Julie Craig, senior analyst with Enterprise Management Associates. In fact, XML is so bulky that XML can take anywhere from two to 10 times more bits to send the same message as other non-SOA protocols. "This means we're sending bulky SOAP and XML across the WAN, not just the LAN, and this likely means a bigger investment in WAN bandwidth as well as in acceleration technology."

Perhaps the biggest difference between SOA and a traditional environment is in the execution of the application itself. Craig says that in a typical client/server system, the application executes on a single server, possibly two. "In SOA, pieces of the application are scattered across multiple servers and platforms inside and even outside the enterprise," she notes. What occurs is an orchestrated sequence of services executing one after another, with SOA messaging sent between services as they execute. Thus, the network becomes intrinsic to the execution of the application itself. Craig's advice? "You might want to start saving for infrastructure upgrades."

Many IT managers have yet to grasp this reality: Yesterday's network won't support tomorrow's applications.

Go deep on packet inspection

Another significant requirement SOA places on the network is the need for deep packet inspection. Typical packet-based networks today fall back upon quality of service (QoS) to speed the delivery of traffic that cannot withstand delays or latency, such as the data that is part of business-critical processes. An example of this would be data from various sources on currency exchange rates for firms that regularly trade currencies for investors.

Suppose there are 10 or more services built to support this business activity. If using QoS causes a one-second delay on each service due to packet inspection, you suddenly have a big latency problem. In many cases, QoS simply cannot inspect very-high-value packets individually and deeply enough, and certainly not quickly enough.

"Traditional network devices are connection-specific and do not have the intelligence to natively understand the traffic flowing through them," observes Jeff Browning, director of product management at F5 Networks. "They rarely dig into the application payload, where much of the application logic resides within web services traffic."

What are needed as part of the SON, Browning says, are intelligent full-proxy devices, which can identify SOAP faults or exceptions. Browning says smart network devices in the SON can also prioritize requests based on enforcing rules and logic, actually removing the overhead from the servers that support the requests.

There are other complicating factors that further point to the need for significant changes in the underlying network infrastructure to support SOA and web services traffic. Many companies seeking to either dive, or at least dip their toes, into SOA waters turn initially to various development tool vendors to build connected applications and services. According to Joe Pruitt, senior architect at F5 Networks, these early adopters find out too late the overwhelming stress these applications place on the network. Compounding the matter further, the tool vendors are making it easier than ever for internal enterprise developers to build SOA applications themselves.

New security specter

"We know all this to be true because so many customers have been coming to us at F5, desperate for a solution to optimizing this expanded network traffic, and for securing it too," Pruitt says. "They don't realize it at first, but the fact is that XML provides the opportunity for new threats and attacks that can be hidden within XML—threats that firewalls in existing networks usually cannot detect until the attack is under way."

With SOA and web services, encrypted tokens are built right into the actual content for authentication and authorization, Pruitt notes. Absent a smart network agent or router built into the SON, back-end servers will very quickly become overwhelmed with requests for encryption and decryption.

"SOA makes it more important than ever to optimize cross-functional processes and to manage systems in a much more structured manner than IT is typically used to," concludes Enterprise Management Associates' Craig. "Organizations will have no choice but to move toward automating their support activities … offloading some of the traditional tuning and optimization roles to appliances with built-in intelligence."

SON TO-DO LIST

- **Carefully assess the network impact of web services and SOA prior to deployment.**
- **Make sure that representatives from each of the security, application, and network groups are involved in SOA planning.**
- **Devise strategies and deploy network devices that intelligently offload the additional overhead that XML and related traffic places on CPUs.**
- **Rethink security requirements due to the new threats XML can bring to SOA deployments.**
- **Choose network products that are inherently flexible within an architecture that can easily accommodate future applications and protocols with enterprise-grade security.**

Additional resources

White paper: *"The Impact of Web Services on the Network" (www.f5.com/solutions/technology/webservices_wp.html)*
White paper: *"Keeping Up with Multi-Service Applications" (www.f5.com/solutions/technology/gtm_multiservice_wp.html)*
Article: *"SOA Success Depends on a SON" (www.f5.com/communication/articles)*