SAP NetWeaver magazine

BEST PRACTICES | Don't let network bottlenecks slow performance

Optimizing the Network for SAP NetWeaver Applications

by **Ron Carovano,** F5 Networks, Inc.

Even a perfectly configured SAP application does not guarantee good performance and reliability. You also need to consider the impact of the network. This is especially true when other challenges are imposed, such as servicing globally distributed users or consolidating data center operations to comply with governance and security requirements.

It helps to understand end-to-end application delivery and the associated technologies while optimizing shared network resources across multiple services (such as email, voice over IP [VoIP], file services, and general Internet access), limiting access to trusted sources, and protecting against unexpected business disruptions. I'll explain how your network affects SAP performance and reliability, and I'll describe a class of products, called application delivery controllers (ADCs), that can help reduce the impact of some network bottlenecks.

Role of Networks

Recently, SAP recognized the critical role of the network in ensuring that SAP NetWeaver-based applications run smoothly and formed a network advisory group under the SAP Enterprise Services Community. Comprised of leading networking vendors and SAP experts, the advisory group identified the following trends as impacting the way enterprises use IT ("SAP Enterprise Services Community: SAP Best Practices." SAP Labs. September 27, 2006):

- **Globalization and mobility:** An organization might have a design facility in Europe, manufacturing operations in Asia, and sales offices throughout the world. Ensuring real-time access of critical business systems to mobile users is increasingly important to stay competitive.
- **The extended enterprise:** Engaging employees, corporate partners (such as resellers and suppliers), and customers provides an economic edge for companies that embrace the entire value chain (what SAP calls the extended enterprise) in order to drive their business.
- **Web-enabled applications:** Just as client/server computing replaced the mainframe, Web-enabled applications are replacing client/server apps. SAP has embraced enterprise service-oriented architecture (enterprise SOA) as the foundation for its current generation of enterprise applications.
- **Centralization and compliance:** In stark contrast to the trends toward expansion because of globalization and mobility, the necessity to reduce costs and comply with regulations (including Sarbanes-Oxley, HIPPA, Basel II) drives many organizations toward consolidation.

The following statements summarize these trends:

- The distance between people and critical systems continues to grow.
- You need anytime/anywhere/anyone access in order to be competitive.
- You must tightly control access to sensitive information and systems.

Applications based on the SAP NetWeaver platform for enterprise SOA hold the promise of addressing all these trends, but fulfilling this promise comes at a price. The underlying application technology inherently increases network traffic, introduces new security issues, and poses new performance challenges. Fortunately, these challenges are well understood and

have proven solutions that an optimized network can easily enhance.

A network that is optimized for application delivery can provide measurable business value in four areas.

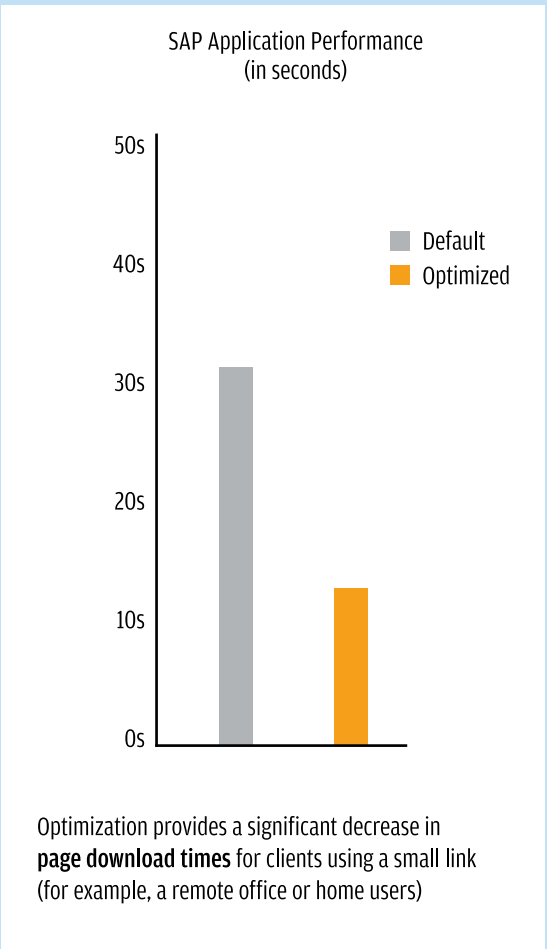
1. User Experience and Application Performance

Achieving the business benefits of a new application hinges on user experience and performance. At best, users will be faced with learning how to use the new application, though they may be reluctant to change how they do business. Poor performance due to network conditions, infrastructure limitations, or other factors can hinder the software's adoption rate. Slow adoption means delays in reaping the benefits of new business processes, as well as increased costs and a lower return on investment (ROI). While internal employees may suffer through a rough adoption phase, issues with supply-chain partners can result in shortages and strained relations. Worse, customers could simply move their business to competing companies.

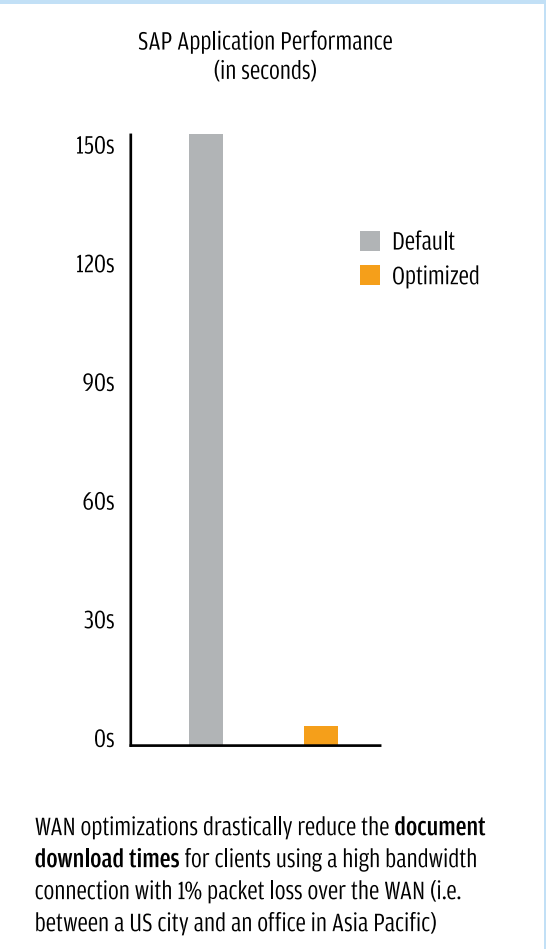
When application performance is poor, the first response is often to increase bandwidth or server capacity. However, this approach ignores the fundamental issue of latency — the time it takes to transmit data over the network. Consider an enterprise that has a manufacturing facility in Asia and a sales office in the United States. Even with a dedicated, high-bandwidth wide area network (WAN), the physical distance between the two locations limits how quickly you can transmit the data. Furthermore, when networking conditions are less than favorable (for example, packet loss, suboptimal routing, and low-bandwidth connection), the performance degrades even further.

Although you can't completely eliminate the effect of

Application delivery controllers (ADCs) improve the performance of Web-based applications.



Optimization provides a significant decrease in **page download times** for clients using a small link (for example, a remote office or home users)



WAN optimizations drastically reduce the **document download times** for clients using a high bandwidth connection with 1% packet loss over the WAN (i.e. between a US city and an office in Asia Pacific)

latency, you can substantially reduce it. When inserted into the network, ADCs effectively optimize WAN performance with:

- **Compression**, reducing the amount of data that is transmitted
- **Caching**, placing data closer to the end user
- **TCP optimization**, decreasing the number of roundtrips inherent in TCP/IP communications

Tests conducted at SAP's Enterprise Networking Lab show that ADCs can reduce page download times by as much as 60% and document download times by as much as 99% (see figure on previous page).

If you optimize the servers and the data center, you can enhance the user experience and application in addition to optimizing the WAN. By offloading processor-intensive tasks from the servers, you can free resources to focus on executing your core business logic. For example, you can offload compression and caching from servers to an ADC residing on the data center network. For secure data transmission, an ADC can also handle secure sockets layer (SSL) encryption and decryption for additional server savings. ADCs balance the processing load across the servers within a cluster, and they minimize the overhead of handling network connections, further reducing the load.

Tests conducted at SAP Labs, simulating 500 users connecting and interacting with an SAP application over the WAN, showed that the net result of all these server offload capabilities was a 44% decrease in CPU utilization. Expanding this concept to multiple data centers, ADCs can provide global load balancing, directing users and traffic to the data center for optimum performance and availability. The net impacts of using ADCs are:

- Improved user experience
- Decreased server-resource requirements
- More efficient use of existing network bandwidth
- High availability, improved reliability, and scalability

2. Application Security

If applications and networks are not secure, you run the risk that business-critical systems won't be available and sensitive data may be improperly accessed or damaged. Security can often be a complex and multidimensional challenge, spanning from the network layer to the application layer, from the data center to the end user, across the entire network. ADCs include application firewall technology, which enacts a number of security measures to ensure that SAP applications are as secure as possible.

In contrast to traditional network firewalls, which focus on inspecting data packets, application firewalls can detect which applications are in use and can inspect entire business transactions. This level of application fluency enables the application firewall to employ a positive security model, thereby allowing only known, acceptable traffic through to the servers. Traditional firewalls block known generic attack exploits, but they can't prevent attacks targeted at a specific weakness within a specific application.

An application firewall, on the other hand, can protect against more advanced attacks, such as cross-site scripting, cookie tampering, and SQL injection. As an added safeguard, the ADC can mask information that would otherwise give hackers clues to the underlying infrastructure, such as the operating system information, Web server data, message headers, and application error codes.

Endpoint security is another concern, particularly with Web-enabled applications. While it may be possible to secure all clients and the network within the corporation, the picture changes completely when you add partners and customers to the mix. For Web applications, some ADCs offer SSL-based virtual private network (VPN) capabilities, which can provide a secure connection between clients and SAP applications, even over public networks. This solution incorporates a plug-in into the client's Web browser, thus circumventing the need to install a specific client-side application and greatly simplifying the administration for partners and customers in an extended enterprise.

Furthermore, SSL VPNs can provide granular, endpoint security for all remote users who connect to your SAP applications. On the front end, pre-logon checks can verify that the operating system, antivirus software, and Web browser all run on the most current patches and updates. If one or more of them is not current, you can redirect users to a remediation page for further guidance. On the back end, when remote users finish their remote access session, you can perform a comprehensive browser clean-up to remove cookies, site history, auto-complete information, and other cached content.

3. Unified Security Enforcement and Access Control

With a strong security infrastructure in place, the next performance challenge is managing access to SAP

applications. Different users throughout the extended enterprise have different access needs. For example, employees may need access to a human resource self-service portal, partners may need access to a supply chain management portal, and customers may need to access an order-fulfillment and secure-payment portal. ADCs provide a means to establish and deploy access policies at the group and individual level.

The challenge of managing access expands further when supporting mobile devices, such as smart phones, PDAs, and laptop computers, that connect to SAP applications via public networks. ADCs can gather device information to determine which applications and resources comply with established policies and, therefore, should be offered. For example, many corporations have policies dictating that certain sensitive information, such as credit card and social security numbers, may never leave the data center. ADCs enable you to create a policy in one location and deploy it globally, which greatly simplifies the management that is needed to meet corporate governance, risk, and compliance requirements.

4. Business Continuity and Disaster Recovery

Organizations rely on SAP applications to run their businesses. These applications always need to be available, regardless of unexpected disruptive events. One way to help ensure this availability is to use an SSL VPN. Even when employees cannot get to the office, an SSL VPN can provide secure remote access to critical systems.

Another consideration is any disruption in your WAN or Internet service provider (ISP) connections. ADCs can monitor multiple WAN connections and seamlessly reroute traffic to the best performing resource. If an entire data center becomes unavailable, an ADC can automatically direct users to a secondary data center, ensuring the continuity of operations.

Corporate disaster recovery plans typically specify recovery point objectives and recovery time objectives. A recovery point objective establishes the earlier point in time to which you must recover systems and data after an outage; it defines the maximum amount of data that the organization can sacrifice after a disaster. A recovery time objective is the maximum amount of downtime allowed to recover from an outage. A critical factor in determining an organization's ability to meet these recovery objectives is the amount of time it takes to move data over the WAN, from the primary data center to a secondary data center for data replication.

One approach is to use a dedicated high-bandwidth network between data centers. However, this can be expensive, and you may still overwhelm the WAN when you load it with SAP application databases containing multiple terabytes of data. Latency is also a critical factor in meeting established recovery objectives. To address these challenges, ADCs provide specialized data replication services, including the following:

- **Data compression** to reduce the volume of data transmitted over the WAN
- **Protocol optimization** to mitigate the "chatty" nature of TCP and HTTP protocols and adapt to variations in latency and connection quality
- **Encryption** to make sure that data transmission is secure
- **Quality of service** to ensure that lower-priority traffic on the network does not impact critical data replication processing

ADCs provide important benefits to SAP NetWeaver applications. They optimize WAN performance using compression, caching, and network protocol optimizations. Offloading CPU-intensive processes, such as SSL encryption and connection management, enhances performance in the data center, thus increasing server availability for core business-logic functions. Optimization across the WAN ensures that users will have secure remote access that is provided by the best performing resource.

Application security and data replication capabilities ensure that critical systems and data are always safe. Together, these technologies optimize the user's experience and application performance, strengthen application security, unify security enforcement and access control, and enable business continuity and disaster recovery. The result is that critical business applications are always fast, secure, and available for the global extended enterprise of employees, partners, and customers. NWM

Ron Carovano is a business development manager with F5 Networks. Responsible for the global relationship with SAP, Carovano oversees integration, testing, certification, and co-innovation efforts conducted between F5 and SAP. He is also responsible for aligning F5 business programs with SAP's go-to-market initiatives. Carovano has 20 years of experience in high-tech industries, ranging from medical device development, to health care simulation and education, to enterprise Application Delivery Networking. He holds a B.S. in Electrical Engineering and an M.B.A. from the University of Florida, and is also listed as an inventor on 14 U.S. patents.