

TOPICS

A z/OS Newsletter, Issue 7

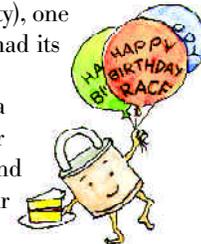
August, 2002



Security: New challenges, building on a solid base

BY LINDA DISTEL

Security has been a major focus for zSeries starting with the 360 architecture. RACF® (Resource Access Control Facility), one of the oldest and best security products of all time, had its 25th birthday last year. We started doing hardware encryption in 1991, way before e-business was even a term. Our customers depended on the isolation of our architecture to build and secure their applications and data, or they looked for example LPARs to isolate their production from their test systems.



PAUL ROWNTREE

Then e-business hit, and we were able to build off our existing security technology to extend our current security capabilities. We extended our hardware encryption to focus on RSA algorithms that support SSL (Secure Sockets Layer) and VPNs (Virtual Private Networks). With the focus on performance, we were able to drive SSL performance on zSeries from poor to outstanding, which took the efforts of zSeries hardware, the Crypto team, the ICSF team, the SSL team, Performance, the WebSphere® team, Research, and Tivoli®. We were able to extend RACF to not only be able to accept a digital certificate, but to create and manage large numbers of them. We added Firewall Technologies and started to Ethically Hack OS/390® and z/OS. With the knowledge we gained, Communication Server added Intrusion Detection capabilities in z/OS V1R2. We added Java® security libraries to z/OS and provided extensions to utilize our embedded hardware encryption. We continued to focus on LPAR isolation, staying up with security certifications, and this provided new opportunities for customers to isolate WebServing and Linux workloads from existing business applications.

Our next focus was to create new function that would:

- Make distributed applications easier to secure
- Make the set up of the server security easier.

As a cross Server Group team, we worked to provide solutions to both of these foci.

(continued on page 59) ▶

PAUL ROWNTREE

TOPICS

A z/OS Newsletter
Issue 7 August, 2002

Contents

| | |
|---|--------------|
| Security: New challenges, building on a solid base | cover |
| Letter from the editors | 3 |
| Linda Distel on cross-platform security | |
| Why a securing a business means working across platforms | 4 |
| IBM unveils new planner to help security administrators | 6 |
| Speeding up secure handshakes across the Internet | 10 |
| z/OS Communications Server...TCP/IP security controls | 12 |
| TN3270 and Enterprise Extender: | |
| Your keys to SNA/IP integration | 15 |
| Policy Based Networking in z/OS: | |
| Quality of Service and Intrusion Detection Services | 20 |
| z/OS TCP/IP Dynamic VIPAs, Sysplex Distributor, | |
| and how they are exploited | 24 |
| zSeries and z/OS Hipersockets overview | 28 |
| IPv6 – Here we come! | |
| z/OS Communication Server introduces IPv6 | 33 |
| IPv6: Better and more | 36 |
| IPv6 Resolver support | 36 |
| z/OS.e: An operating system for new workloads | 37 |
| “WAS” up? z/OS.e SystemPac is! | 39 |
| And you don’t need a new library | 41 |
| Journey through space and time with z/OS.e | 42 |
| IBM z/OS SCLM Suite: Then, now and in the future | 43 |
| Performance management: | |
| Quick, easy and inexpensive | 47 |
| The Library Center prototype: | |
| Know where you want to go and get there quick | 48 |
| State your preference ... for autorunning z/OS library discs | 49 |
| Alert! Alert! ... | |
| for swapping and using those CD-ROM library discs | 50 |
| Fine-tuning the WLC picture | 51 |
| z/OS RRS Multisystem Cascaded Transaction | |
| exploitation in IMS V8 | 53 |
| Our contributors | 55 |
| Top ten list of late night outages | back |
| | cover |

A letter from the editors

In this issue...



TRACY BONDI

The Hot Topics Newsletter has reached its seventh issue—does that mean it’s time for some bad luck to befall us? If so, the spectres of misfortune certainly haven’t appeared yet—we keep cranking the newsletters out, with no end in sight, and your incoming reader comment cards keep our egos bursting at the seams! These past few months, however, we took some time off from congratulating ourselves to put together what we think is an issue you’ll love.

The topic de jour for Issue 7 is security. Because our only reason for living is to make you folks happy, we set our minds to bring in the local guru on the topic, Linda Distel. She graciously wrote us a security mission statement for the eServer platform (“Security: New challenges, building on a solid base”) and even allowed Wayne O’Brien and J.D. Ross to pick her brain and share the wealth in their article “Linda Distel on cross-platform security.” Be sure to also check out Wayne and J.D.’s other article on the eServer Security planner and the Cryptography piece by Michael Kelly and Suzanne McHugh.

This issue is, as always, chock-full of other helpful morsels as well. Check out our quintet of Communications Server articles, our IPv6 triplets, and the informative mass about the new and exciting z/OS.e operating system. Of special note (because we all know that nobody is perfect) is the outage-avoidance article on the back page. Refer to it for some very useful information if you find yourself in that unfortunate predicament.

You may notice that the index is missing from this issue. Actually, it isn’t missing—it’s just playing hide-and-seek. When you rev up the included zFavorites mini-CD, you’ll see that the updated Hot Topics index is nestled within, along with the plethora of other tidbits that you always find so valuable.

As always, your comments are most welcome, whether you want to give us reason to think we’re wonderful enough to deserve a vacation in Italy or you want to humble us a bit. We also like to hear suggestions for future “Hot Topics hot topics” if you have them. Please let us know what you think with the attached comment card or with an email to newsletr@us.ibm.com. Until we hear from you, we’ll assume you are ordering collections or attending SHARE for the sole purpose of getting your hands on the latest Hot Topics issue, and we’ll “keep on doin’ what we’re doin’.” Enjoy!

—The Editors ■

| | |
|------------------|--|
| EXECUTIVE EDITOR | SUE SHUMWAY |
| MANAGING EDITOR | JOHN URBANIC |
| ART DIRECTOR | TRACY BONDI |
| ILLUSTRATORS | DIANE ATTEBURY TRACY BONDI NATASHA FRAY PAUL ROWNTREE |

Linda Distel on cross-platform security

Why securing a business means working across platforms

BY WAYNE O'BRIEN AND J.D. ROSS

If your business requires top-to-bottom security for a collection of unruly platforms, you'll likely be interested in Linda Distel's "to-do" list at IBM®. As Director of IBM eServer Security, Linda owns the security strategy for IBM's diverse family of eServer platforms: i-, p-, x- and zSeries, and Linux. Her recent projects include hardware encryption and Web Services.

We had a chance to interview Linda recently. In the talk that follows, Linda shares her views on the new security challenges facing today's multiple platform, interconnected world, and what help lies on the horizon. Interestingly, Linda's plan for protecting your business has as much to do with promoting ease of use and enabling new technologies, as it does with providing traditional I/T safeguards.

Why is it important for IBM to take a cross-platform approach to providing security?

For many reasons, but let's talk about two: business enablement and ease of use.

Our customers' workloads are becoming much more distributed. Years ago, a business would have its entire workload on one server. Today, businesses have applications in which the user interface is a Web browser, the application code resides on an application server, the data is on a database server, and so on. An application that starts with someone purchasing stock through a Web browser on a Windows® machine, for example, might end with a transaction that updates a bank account on a zSeries server.



DIANE ATTEBURY

With transactions being so distributed, our customers need security functions that can interrelate with each other. Think of open standards, secure socket layer (SSL), and virtual private networks (VPNs). For distributed workloads, customers need common security building blocks that not only protect, but enable their businesses.

As it happens, IBM has been creating these building blocks for some time now. We have been adding quite a few security enhancements to support e-business, such as SSL, VPNs, hardware encryption, Kerberos, LDAP, and digital certificates, and so we have these common elements already.

Now, we're ready for the next phase: making your distributed transactions work better.

Another reason for a cross-platform approach to security is simplicity and ease of use. Customers aren't going to remember that a new security function is available on

one of our platforms, but not on another. If we announce a new function, we would like to deliver it across all eServer platforms.

Given the challenges of distributed processing, what can IBM do to support multi-platform businesses?

Near term, we have delivered things like the eServer Security Planner, which are common pieces of function that cross platforms and deal with issues like ease of use.

We're also going to deliver Enterprise Identity Mapping (EIM), which allows you to associate a user ID in one directory with a user ID in another. EIM will allow your distributed transaction to know that, for example, "Linda Distel" in one server's directory is also LDISTEL on another server. Using EIM, in conjunction with a technology like Kerberos, you have single sign-on, simplified auditing, and easier security administration in a multi-platform environment.

Longer term, we're moving towards an IBM Web Services approach, which will be highly influenced by IBM's WebSphere and Tivoli security products.

We expect that Web Services will be so generic, you will need to be able to run them on any server. So, we plan to distinguish our servers running underneath. Besides allowing Web Services to work seamlessly on our servers, we plan to also provide a distinct security value-add for Web Services. For example, our hardware crypto is highly certified. A Web Service sitting on an eServer with our encryption card plugged in runs with unique security characteristics, such as tamper resistance and improved performance.

Also, we plan to enable all that data on our servers. With 70% of the world's data residing on IBM servers, we have to well-enable all of that data for a Web Services environment.

So, we're doing the right things to support Web Services. But we also want to provide value across all servers and layers, from Web Services down to the eServer level.

Sorting this stuff out is my biggest job. We're really just beginning to sort out the "end-to-end story." Enabling Web Services is a major, long-term challenge for IBM and it's where we plan to focus much of our time in the future.

Back to simplicity: The eServer Security Planner is one example of something we've done to make setting up security easier. It doesn't effect Web Services directly, but we might make it easier for a customer to put a workload on our machine if we provide you with recommendations that make setting up security on that machine easier. This is very important, since Security skills are in short supply.

It's the eServer Value Proposition: Business Enablement and Ease of Use, together.

How do IBM's new strategic initiatives, Grid Computing and Project eLiza™, influence your strategy for eServer Security?

Grid computing and Project eLiza are at the core. Things are becoming more complex, with more end user devices, and more transactions crossing servers. We need to make things easier to connect, easier to configure, easier to distribute, easier to work heterogeneously, within enterprises and across them. That's Project eLiza.

There are huge implications for doing this. Imagine, for example, that there is an outbreak of a disease in one part of the world, and a second outbreak follows in another part. How will the medical facilities in every country correlate their data, regardless of differences in hardware and software? That's Grid Computing.

What is it going to take to do this, with regard to security? There are pieces in place already. Think of VPN, which we enable in our operating systems and in our hardware crypto. Think, also, of our customers using digital certificates and Public Key Infrastructure (PKI) on zSeries mainframes.

And, we are planning to add to our existing functions to better support heterogeneously distributed transactions, through new technologies such as EIM. Also, we're planning to provide a common security architecture by tying Web Services security to the security inherent in the operating system and the hardware.

IBM recently added Linux support to its stable of eServer platforms. What unique security challenges are presented by Linux?

Huge question. Linux makes "end-to-end security" even more important, because it can run on any of the eServer platforms.

Something we've done well is enabling hardware encryption for servers running Linux.

There are other issues to resolve, such as questions regarding certification of the Linux operating system. For example, should someone do Common Criteria Certification of Linux? IBM doesn't own Linux, nor are we a Linux distributor, so it's hard to determine how far to go with certification.

Governments are encouraging certifications now more than ever. AIX® has issued a Statement of Direction, and we are examining the certification requirements for our other operating systems. Linux adds one more operating system to certify. We plan to include Linux as we develop our strategies.

How are we interacting with the Linux distributors with whom we have partnerships?

Some of our discussions are regarding whether we should add a secure distributor to our list of partners. What that means is you get a Linux system with certain functions locked down. You're more limited in what you can do with Linux, but the security holes may be closed. ▶

(continued on page 36)

IBM unveils new planner to help security administrators

BY WAYNE O'BRIEN AND J.D. ROSS

By this time, you've heard of our wizards, which help with complex tasks, such as setting up a Parallel Sysplex® or configuring z/OS UNIX® System Services. Now there's a new tool available, specially designed to help protect an evolving, high intensity, mission critical type of computing environment.

Like your business, for example. Increasingly, much of the security setup work at a typical z/OS installation requires you to work across platforms so that security can be carried out consistently throughout the enterprise. According to a recent survey of SHARE attendees, more than 50% of you use at least four different operating systems in your day-to-day operations.

With this added complexity comes additional challenges to face and potential threats to guard against. In today's vastly distributed, interconnected world, your business's security might well be determined by the least secure platform in your enterprise.

When it comes to security, what is your weakest link?

In IBM, we've been looking at simplifying some of the security setup tasks that you perform for each of IBM's eServer platforms: i-, p-, x- and zSeries, and Linux. Imagine having some help with establishing a common password policy for these platforms. Or, how about a tool that enables auditing options for some operating systems, and provides an easy-to-use, Web-based interface for structuring your RACF audit jobs?

Our cross-platform work is just beginning, but now you can view the first result of our efforts: The IBM eServer Security Planner. This tool is available, free of charge, at the following URL: <http://www.ibm.com/servers/security/planner/>.

Before we take a closer look at the Security Planner, let's review some common difficulties associated with setting up security. Right now, if you work in an environment with



PAUL ROWNTREE

multiple platforms and you need information about security setup, you probably find yourself checking... well, *multiple* places for it!

You probably also:

- Work with other departments and I/T groups in your company to synchronize the security changes for each platform.
- Devote significant time to helping new staff learn the security particulars of unfamiliar operating systems.

This is where the eServer Security Planner steps in to assist you. The Security Planner guides you through a series of questions about your business environment and security goals. Based on your answers to these questions, the Security Planner provides you with recommendations for setting password rules, controlling access to system resources, enabling logging and auditing, and other OS-specific, security-related activities.

Most often, the audience for the Security Planner will be security administrators and auditors who are new to one or more of the eServer platforms. For this audience, the Security Planner offers practical tips, tools, and programs for auditing.

There are some limitations to be aware of. Running as an isolated Web-based tool, the Security Planner cannot directly implement its recommendations on your operating systems. Rather, it provides you with worksheets to assist you with configuring security. In some cases, the Security Planner also provides you with a program you can download to implement the policy recommendations.

Consider the eServer Security Planner to be one part of the overall comprehensive security plan for your business. The Security Planner can help you visualize the cross-platform implications of security when you plan security-related setup.

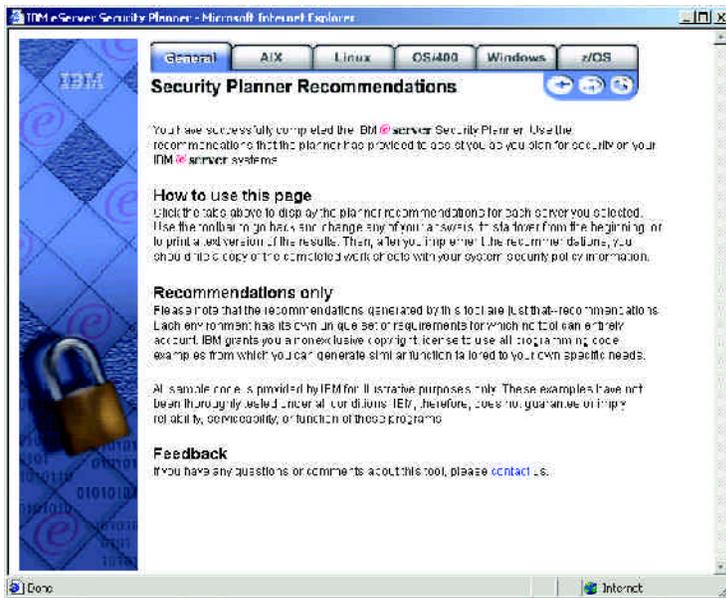


FIGURE 1

Getting started: Tell us about your environment

The Security Planner does not scan your system or interrogate it in any way. Therefore, you must provide some information to allow the Security Planner to make its recommendations.

After reviewing the Security Planner's "Terms of Service" notice and the Welcome page, click Start. Begin the interview by selecting the operating systems in use at your installation. This lets the Security Planner know which set of platforms to include in its recommendations.

If your business requires a different level of security for each of its environments (for example, a production system, a test system, and a sandbox development system), you must repeat the Security Planner tool once for each environment.

Specifying the "Server Use" value

How you use your systems influences the amount of security the

systems require. Select the "Server Use" category that best reflects your environment's role: production, test, or both production and test. A production system running mission critical application, for example, usually requires a higher level of security (and thus a stricter security policy) than a test system.

Remember, if your environment has servers that are used for different purposes, with different security characteristics and requirements, you must run the Security Planner again for each distinct level of security you require for your systems.

Selecting the security level

The Security Planner prompts you to specify the overall level of security required for your environment, based on (among other things) the degree of risk your company can tolerate for a particular environment, and the sensitivity of the accessible data. As a general rule, choose a high level of security for production environments used for mission-critical workloads, a medium level of security to rely

primarily on system defaults (with greater security for critical system resources and moderate security for others). Select low security only for non-critical environments that contain no sensitive data and present no risks should the environment be compromised. Remember that the effectiveness of your security policy depends on your knowledge of your system resources and their uses. Always consider the risks to your company, should any of your servers be compromised. A cautious approach is best!

Enabling logging and auditing for your environment

When you implement a security policy, you will want to monitor the effectiveness of the policy on an ongoing basis. Auditing your environment helps to detect actions that can compromise its security. When you select "Logging and Auditing" for an environment, the Security Planner suggests an appropriate level of auditing, based on how you've responded to its questions so far.

Like other aspects of security, setting up logging and auditing involves trade-offs. For each action you choose to log, you can experience a loss (often negligible) in system performance or disk space, or both. Effective auditing of any system depends largely on your knowledge of system resources and their uses.

Using the recommendations

When you complete the Security Planner's questions, the Recommendations General page is displayed. Click the operating system tabs to display the Security Planner's recommendations for each server you selected. Use the ▶

(continued on next page)

toolbar to go back and change any of your answers, to start over from the beginning, or to print a text version of the results.

If you implement any of the recommendations, you should file a copy of the completed work sheets with your system security policy information.

In some cases, the Security Planner provides sample programs to run. This code is provided by IBM for illustrative purposes only. These examples have not been thoroughly tested under all conditions. IBM, therefore, does not guarantee or imply the reliability, serviceability, or function of these programs.

z/OS recommendations

Based on your answers, the IBM Security Planner provides recommendations for data sets and system resources to protect, suggestions for password protection, and help with organizing your audits. Use these recommendations in several ways: As a “health check” of your current audit processes, as a preparatory step prior to an audit of your system’s security setup, or as an aid to training personnel who are new to the platform. Consider these recommendations to be a minimum set. The Security Planner simply provides a starting point for your work. As always, you must ensure that the recommended settings are workable in your environment and consistent with your installation’s security practices.

Using the sample z/OS audit jobs

For auditing a z/OS system, the Security Planner recommends audit reports to use, based on the security objectives you specified. These reports are created by running the z/OS auditing

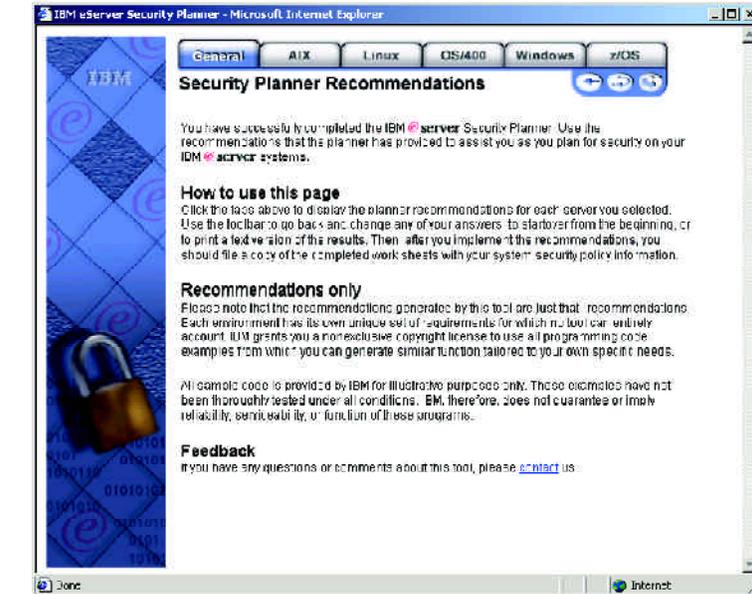


FIGURE 2

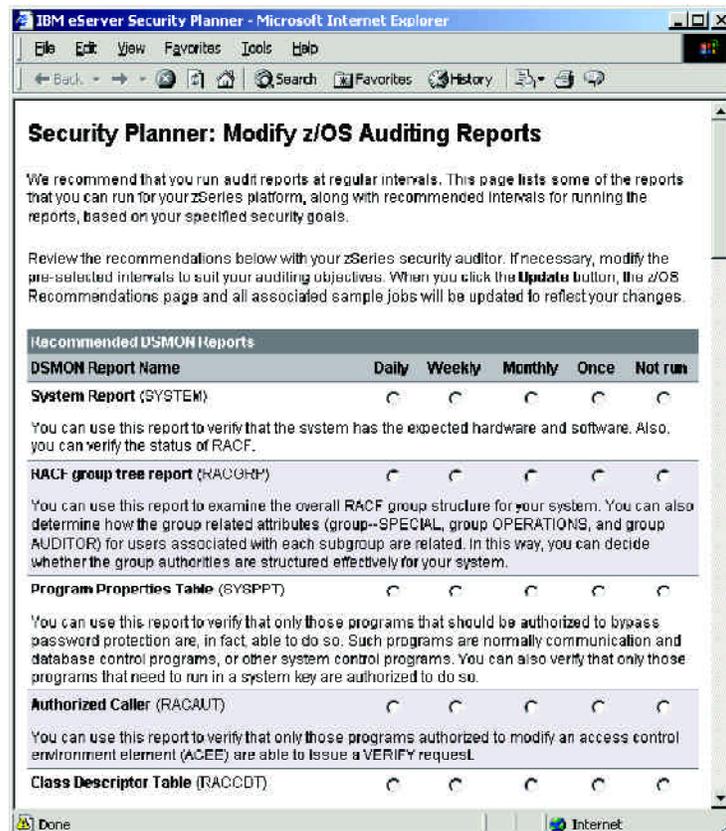


FIGURE 3

utilities: DSMON, RACF Database Unload, and SMF Database Unload. The Security Planner includes links to JCL that you can use to create the audit reports on your z/OS system.

Again, consider these reports to be a minimum set. Depending on your auditing requirements, you might determine that you need to vary the frequency of running these reports, run additional report types

not shown in the Security Planner's recommendations, or use alternative products and tools to accomplish your auditing objectives.

Review the recommended reports with your security auditor and modify them if necessary. If you want to modify the recommended list of reports for your installation, the Security Planner provides a simple panel for doing so: see figure 3.

You can alter the list of reports—and the frequency at which they are run—on this panel.

When you complete your updates, press Next to return to the recommendations.

Using the Linux recommendations

IBM is committed to Linux across all of the eServer platforms. Therefore, the Security Planner supports the SuSE 7.3 distribution, and the SuSE Linux Enterprise Server 7 distribution.

For configuring security for Linux, the Security Planner recommends using SuSE's YaST for making any changes. YaST is a powerful and simple installation and configuration program provided with SuSE Linux distributions. The Security Planner's recommendations for Linux explain the YaST values and suggest settings for them, helping to take some of the mystery out of getting your Linux system running securely.

Using the AIX recommendations

For the IBM eServer pSeries™, the eServer Security Planner supports AIX versions 4.3.3 and 5.1. After you supply the Security Planner with your system's security requirements, the Security Planner generates a korn shell script for

you to download and run.

Besides the downloadable script, the Security Planner also provides you with a list of system values, their definitions, and the setting value that will be implemented upon running the script.

Using the OS/400® recommendations

The Security Planner supports OS/400 Version 4, Release 4, Version 4, Release 5, and Version 5, Release 1. For an OS/400 system, the Security Planner provides a CL program to assist you with applying the recommendations. You can download the program, edit it as necessary in your favorite text editor, and run it to invoke the new security settings.

Besides the CL program, the Security Planner also provides definitions and values to input into Operations Navigator, the graphical interface to OS/400.

Using the Windows recommendations

For the world of Windows computing, the Security Planner offers a solution for Microsoft® Windows 2000 system administrators. Directed primarily to Windows 2000 on an IBM eServer xSeries™, the Security Planner recommends BIOS settings, offers advice on adding Windows 2000 servers to your network, and prompts you to check Microsoft's Web site for important security fixes and downloads.

As with the other eServer platforms, the Security Planner also provides you with a list of security policies and their recommended value settings.

Lastly...

The eServer Security Planner is but one part of a comprehensive plan to simplify security setup across the eServer platforms. Be aware that the Security Planner's recommendations are just that—recommendations. Each environment has its own unique set of requirements for which no tool can entirely account.

Give it a try and let us know what you think. Please e-mail your comments, questions, and suggestions regarding the Security Planner to: secadv@us.ibm.com. ■

Speeding up secure handshakes across the Internet

BY MICHAEL KELLY AND SUZANNE L. MCHUGH

Cryptography is the algorithmic “scrambling” or enciphering of information based on a key such that the information may be “un-scrambled” or deciphered later with a complementary algorithm and decryption key. Typical uses of cryptography include providing the confidentiality and integrity of data detailing financial transfers between institutions, protecting the confidentiality of personal identification numbers that flow between automated teller machines and issuing banks, and generating electronic signatures that often have the same legal validity as personal written signatures. Secure Sockets Layer (SSL), which has become the dominant technique for providing private communications between parties on the Internet, uses cryptography both for authentication of clients and servers, and for data confidentiality. SSL is a public-key, cryptography-based extension to TCP/IP networking.

An example of the importance of SSL authentication is a Web commerce application requesting a customer’s credit card number. The customer wants to be assured that the application is the one intended and not a “Trojan horse” impostor that is stealing credit card numbers. SSL provides this extremely important security function. SSL also allows credit card number to be passed from the customer to the marketing application without being observed by a hacker.



PAUL ROWNTREE

SSL represents the single most important use of cryptography in the spectrum of secure e-business applications. Over the years, zSeries and S/390® have focused on improving SSL encryption performance.

Since 1991, IBM’s integrated hardware encryption has consistently been the industry leader both in the level of security provided and in performance. Hardware encryption devices provide a security boundary that can be an important requirement for financial applications. When compared to application software implementations of computationally intensive public-key cryptography, hardware devices can provide huge performance advantages.

The CMOS (complementary metal oxide semiconductor) cryptographic coprocessor, the follow-on to the original bipolar technology ICRF (Integrated Cryptographic Feature) that first shipped on S/390 in 1991, was introduced in 1997.

The CMOS cryptographic coprocessor provides very fast Data Encryption Standard (DES) encryption, message authentication code checking (MACing), key management, and PIN functions. These functions have extensive customer use throughout the world, particularly in the financial community.

The CMOS cryptographic coprocessor also has a highly secure, fast RSA (Rivest, Shamir, Adleman) signature and key distribution capability. The RSA key distribution functions are becoming critical to the enablement of SSL implementations on z/OS. While the CMOS cryptographic coprocessor offers spectacular performance for DES functions and exceptional reliability, it is somewhat inflexible in that it is difficult to add new function that executes within the highly secure hardware boundary. A single CMOS cryptographic coprocessor can support about 75 1024-bit RSA operations per second. The RSA performance—while good—has not kept pace with the exponentially growing demands of SSL.

IBM’s answer to both problems was to incorporate the PCI (peripheral component interface) Cryptographic Coprocessor (PCICC) as an optional feature on zSeries and S/390 systems. The PCICC feature is built around IBM 4758-2 PCI cryptographic coprocessor cards with special enhancements and adaptation packaging. The PCICC feature has excellent RSA performance, especially for the 1024-bit RSA

private key operation that is used in the SSL handshake. A single card can support about 135 RSA operations per second. The Integrated Cryptographic Service Facility (ICSF) routing algorithms for RSA functions scale well as PCICC features are added, so that in an environment where 16 PCICC coprocessors and two CMOS cryptographic coprocessors are active, support for over 2000 RSA operations per second is possible.

With the introduction of the PCI Cryptographic Accelerator (PCICA) in April 2002, IBM has further increased SSL performance capabilities on the z900 Turbo models, as well as all processors that were limited by the PCICC configuration. Each zSeries PCICA feature contains two cryptographic accelerator cards and can support up to 2100 RSA operations per second. zSeries PCI cryptographic coprocessors and accelerators (PCICC and PCICA) and CMOS cryptographic coprocessors are complementary elements that work together to provide exceptional performance and function.

IBM's zSeries Performance Evaluation and Support team recently conducted studies running z/OS VIR3 on a z900 Model 2064 with 4 CPUs. They measured the number of single (modulus-exponent form) 1024-bit RSA operations per second as well as the number of Chinese Remainder Theorem (CRT) 1024-bit RSA operations per second. CRT is a mathematical technique in which the cryptographic key can be expressed in a manner such that a single 1024-bit exponentiation can

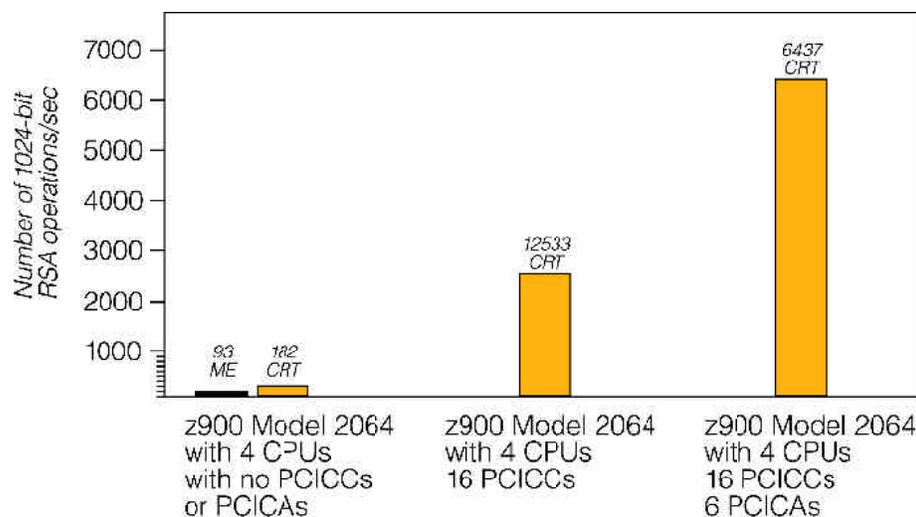


FIGURE 1

be replaced with two simultaneous 512-bit exponentiations, thus decreasing the overall processing time. For example, under the above conditions, the team was able to accomplish 93 single 1024-bit RSA operations per second or

182 CRT 1024-bit RSA operations per second on the CMOS cryptographic coprocessor. Note that the CMOS cryptographic coprocessor performance on the z900 is improved over the 75 RSA operations achieved on previous processors.

Adding 16 PCICC coprocessors to a z900 16-way processor resulted in 2533 CRT 1024-bit RSA operations per second. Equipping the z900 16-way processor with 6 PCICA cards in addition to the two other cryptographic elements increased the total number of 1024-bit CRT operations to 6437/second. Refer to the results in Figure 1.

What does all this mean in the real world of e-business on the Internet? These performance numbers are for 1024-bit RSA operations, which are the heart of the SSL handshake. There are many more instructions involved in the actual SSL transaction, however,

so these raw performance rates do not represent the number of possible SSL handshakes. In a purely software implementation of SSL on a z900 4-way processor we actually obtained 122 SSL handshakes per second at a cost of almost 100% CPU usage. On a z900 16-way processor, the result was 497 software-only SSL handshakes per second, again at 100% capacity. Moving the 1024-bit operations to the cryptographic hardware available with a 16-way z900 (in this case, 2 CMOS cryptographic coprocessors, 16 PCICCs and 4 PICAs), you may be able to achieve 3499 SSL handshakes per second before using 100% of your processor capacity. So your e-business application can transact a lot of SSL handshakes and still have a significant percentage of your CPU cycles available for other work. This translates to more customers getting to your highly secure e-business application and more computing power left over to help you process their orders. ■

z/OS Communications Server TCP/IP Security Controls

BY LIN OVERBY

With increased use of TCP/IP and the Internet, enterprise security requirements have become more stringent and complex. Because the sources of many transactions are from untrusted networks such as the Internet, and sometimes unknown users, increased attention is paid to host and user authentication, data integrity and privacy in the network, as well as denial of service attacks. The z/OS Communications Server provides security controls to address these TCP/IP security concerns.

The Communications Server *protects data in the network* by supporting a variety of cryptographic-based network security protocols such as IPSec, SSL, Kerberos, and SNA Session Level Encryption. These security protocols help allow that received data originated at the claimed sender (data origin authentication), contents were unchanged in transit (message integrity), and sensitive data is concealed using encryption (data privacy).

The Communications Server also *protects system resources and data from unauthorized access*. Communications Server applications and the TCP/IP protocol stack protect data and resources on the system using standard SAF.¹ services.

The Communications Server *safeguards the availability of the system* by protecting against denial of service attacks from the network. The Communications Server has built-in defenses, and also provides services that an installation can optionally deploy, such as Intrusion Detection Services, to defend against attacks from the network.

This article gives an overview of the network and resource security controls that enable a safe and secure z/OS TCP/IP deployment.

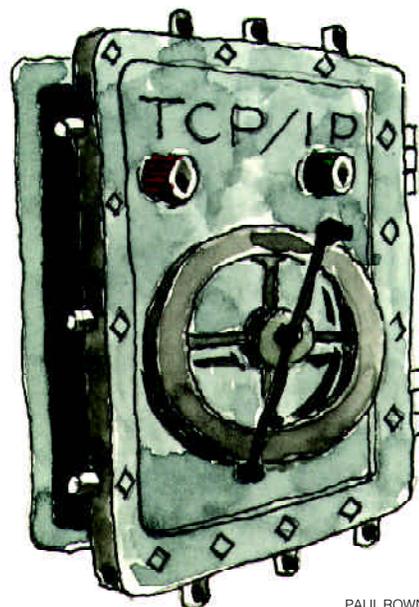
Protecting data in the network

As TCP/IP applications are rolled out on the zSeries and throughout the enterprise, security in the IP network may be required to protect data traffic, depending on the sensitivity of the data and the level of trust that the installation has in the IP network. Applications can be enabled for network security, or they can take advantage of transparent network security protocols that require no application change.

One method of building security into the application on z/OS is to use a system socket API-level security service such as *z/OS System Secure Sockets Layer (SSL)*, or *z/OS Network Authentication Services* (Kerberos).

Alternatively, newer versions of network services such as SNMPv3, supported by the Communications Server, have security built directly into the application protocol at the message level using standards-based specifications for highly secure interoperability.

In z/OS Communications Server V1R2, more built-in security has been added to its applications. The FTP server and FTP client have been enabled to use SSL for highly secure file transfers. The FTP SSL support can be configured to protect the FTP control connection or both the control and data



PAUL ROWNTREE

connections. The FTP server and FTP client, along with the USS Telnetd and RSHD, have been enabled to use Kerberos protocols. Security has been added to network services such as OSPF (OSPF MD5 authentication) and DNS (Secure DNS).

If a zSeries TCP/IP application is not enabled to use SSL or Kerberos, *IP Security* (IPSec) can be used for transparent network security. Furthermore, as enterprises seek to engage in B2B or same-business communications using the Internet as a portion of the data path, IPSec can be used to protect not only the application data but also the IP header information. IPSec can be used to build a *Virtual Private Network* (VPN) to support these e-business configurations. A VPN enables an enterprise to extend its network across a public network such as the Internet through a highly secure tunnel (or IPSec security association).

IPSec is implemented at the IP layer, providing authentication, integrity, and data privacy between any two IP entities. IPSec can protect a segment of the data path (for example, between two routers), or it can secure the data path end-to-end. Management of cryptographic keys and security associations can be manual or automated via the *Internet Key Exchange* (IKE), a key management protocol defined by the Internet Engineering Task Force (IETF).

The Communications Server and Security Server elements of z/OS together provide IPSec and VPN support for z/OS. z/OS IPSec support is implemented at the latest IETF standards and includes Triple DES for strong encryption. A crypto coprocessor provides hardware assist for IPSec encryption and decryption. z/OS IKE supports both the pre-shared key and RSA Signature (which uses host-based X.509 certificates) methods of IP host authentication. In an upcoming release, z/OS VIR4, workload distribution and availability in the sysplex is improved with a new function called Sysplex Wide Security Association (SWSA). With SWSA, IPSec-protected traffic that is targeted to a Dynamic VIPA (DVIPA) can be distributed using the Sysplex Distributor function. Additionally, during a DVIPA takeover, any existing security associations with a DVIPA endpoint will be automatically renegotiated on the system that is taking over the DVIPA.

As SNA networks are replaced by IP networks, the TN3270 protocol provides a means for client workstations to continue to access 3270-based SNA applications over an IP network. With TN3270, it is transparent to the SNA application that an IP network is being used. In order to protect data over the IP portion of the network, the

Communications Server has enabled its TN3270 server to use SSL. If the TN3270 server resides on a different host than the target SNA application, *SNA Session Level Encryption* can be used to help secure the SNA portion of the data path. The TN3270 SSL support provides several extensions for SAF access control to the TN3270 server. These extensions are based on using a client-provided X.509 certificate to determine the SAF identity of the end user. The SAFCERT function prevents a client from receiving a logon (USSMSG) screen unless the client's authority to access the TN3270 server is verified. The *Express Logon Feature* (ELF) simplifies user ID and password administration for users signing on to SNA applications using TN3270. ELF allows an end user using a TN3270 client with an X.509 certificate to logon to a SNA application without entering a user ID and password. The WebSphere Host On-Demand and Personal Communications program products provide SSL-enabled TN3270 clients. Client support for ELF requires WebSphere Host On-Demand at V5.0 or Personal Communication at V5.5.

An alternate method of accessing SNA applications over an IP network is Enterprise Extender. Enterprise Extender carries SNA sessions over an IP network. A portion or the entire data path can be over an IP network. SNA Session Level Encryption can secure the SNA session end-to-end. Additionally, IPSec can protect the IP portion of the data path. Either or both of these security protocols can be used, depending on the security requirements and network topology.

Protecting resources and data from unauthorized access

The Communications Server protects data and other system resources accessed by applications included in the Communications Server element. Protection requires verification of the identity of the end user requesting access in a process called *identification* and *authentication*. Access to resources also must be limited to those users with permission. This process is called access control.

Communications Server applications use SAF services for all identification, authentication, and access control decisions. Authenticated users are granted access only to SAF resources for which they have permission. The Communications Server also provides access to resources via applications that allow “anonymous” access (like anonymous FTP) to be controlled. The Communications Server uses SAF services to protect TCP/IP resources from unauthorized access. The TCP/IP stack allows the local user access to resources, which are defined as SAF resources in the *SERVAUTH class*, based on permissions associated with the SAF resource. SERVAUTH can be used to protect a wide range of TCP/IP resources. A primary use is to protect local user access to a specified TCP/IP stack, TCP or UDP port, or IP network resource (or group of IP network resources). SERVAUTH can also be used to protect local user access to netstat and pasearch command output, to control authority to start functions that consume large amounts of system resources such as FTP SITE DEBUG or DUMP commands, and to control SNMP subagent connections to an SNMP agent. Safeguarding the availability of the system. ▶

(continued on next page)

The Communications Server can be configured to perform IP packet filtering. IP packet filters are rules defined to either discard or permit packets. IP packet filtering can control either traffic being routed through a host, or traffic in the host that has the communication endpoint. Even when an external firewall provides filtering protection for a host, Communications Server IP packet filtering can provide a secondary line of defense.

Syslogd Isolation controls write access to a syslogd facility on a jobname and/or user ID basis in order to allow the segregation of system and application syslogd records and to segregate syslogd records from different applications. This function prevents an application level process from flooding a syslogd facility intended for system use, possibly causing system syslogd records to be lost.

In z/OS V1R2, the z/OS Communications Server added support for integrated *Intrusion Detection Services* (IDS) which enables the detection of attacks and the application of defensive mechanisms on the z/OS server. The focus of IDS is self-detection and self-protection. The z/OS Communications Server is integrated into the z/OS Communications Server TCP/IP stack and performs “in context” intrusion detection on the data path. IDS events detected include ICMP and TCP/UDP port scans, and a variety of single and multiple packet attacks against the TCP/IP stack. It also incorporates a Traffic Regulation Manager function (TRM), which limits the number of inbound TCP connections, and controls UDP internal receive queue depths. The IDS can discard packets, limit connections, and provide IDS event recording. IDS event information can be recorded in syslog files and/or written to the console. IDS

statistics can be recorded in syslog. Packet trace samples can be recorded to document suspicious activities. An IDS report program, TRMDSTAT, provides summary and detailed reporting of IDS events and statistics. Messages written to the console can drive message automation.

Summary

Through its network security and system resource security features, z/OS Communications Server:

- Provides the enterprise-strength security services necessary for safe and highly secure e-business deployment. Strong encryption and data authentication services are available to protect the most sensitive enterprise data in the network. Network security protocols can be deployed end-to-end for the highest degree of security
- Is designed to protect mission-critical data and other system resources. Using the SERVAUTH class, the Communications Server uses SAF to protect access to system resources, such as the TCP/IP stack, ports, and the IP network. Additionally, the Communications Server applications use SAF to protect files and datasets.
- Provides, via the TCP/IP stack, the high availability required for e-business by protecting against over consumption of system resources when excessive demands are made from the network. This built-in high availability is further extended by Intrusion Detection Services which are integrated into the TCP/IP stack for policy-driven self-detection and self-protection from attacks against TCP/IP. ■

¹ RACF is an IBM resource security manager that provides identification, authentication, and access control services through the SAF interface.

TN3270 and Enterprise Extender: Your keys to SNA/IP integration

BY MICHAEL J. KELLY AND SUZANNE L. MCHUGH

With the latest releases of Communications Server for OS/390® and z/OS™ Communications Server, S/390 and the IBM zSeries are world-class platforms for native e-business (TCP/IP-based) applications. However, conversion of existing SNA applications to TCP/IP-enabled applications can be economically impractical. In many cases such conversions may even be technically impractical due to the lack of source code and adequate skills for the specific application. An additional complication is the wide variety of SNA-based endpoint devices, such as banking ATMs. So, how can we enable IP applications and preserve SNA application and endpoint investment, while converging toward a single network protocol?

This article focuses on aspects and features of two key mechanisms for SNA/IP integration: TN3270 and Enterprise Extender.

TN3270 servers— outboard or inboard?

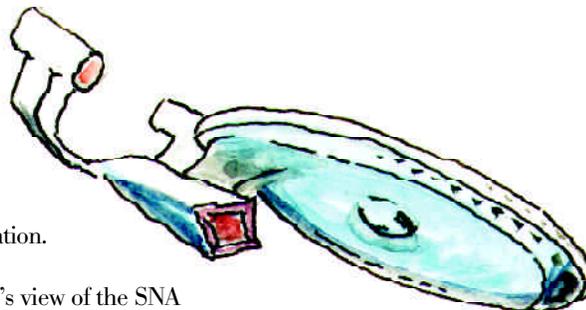
While there are many different vendors of TN3270 servers¹ in the market, there are really only two types of TN3270 servers, outboard servers and inboard servers. Before making functional comparisons between the two types of TN3270 server solutions, however, it is vital that one understand the basic differences in the structural models used by the outboard TN3270 servers and the inboard z/OS TN3270 server. From an SNA perspective, the outboard TN3270 server looks like a SNA PU type 2 and the TN3270 clients look like dependent LUs (i.e. SNA 3270 LUs) while the inboard z/OS TN3270 server² looks like an SNA

session manager with each TN3270 client being represented by a separate VTAM® application.

Because S/390's view of the SNA session remained unchanged for the outboard TN3270 servers, the migration impact for a customer moving from SNA 3270 LUs to TN3270 clients was minimized. This aspect more than any other originally made the outboard TN3270 server the server of choice for most customers. This structural model also allowed certain key VTAM functions to work identically as in a pure SNA 3270 environment (e.g. USS support). While the dependent LU-based model has proven beneficial in the short term, it also has aspects (e.g. SNA needed in the WAN) which will make it much less desirable as networks move to take greater advantage of the Internet for their SNA business applications. In addition, the functions which were only supported by outboard TN3270 servers in the past are now available on the z/OS TN3270 server and additional functions have been added which give the z/OS TN3270 server some major competitive advantages over outboard TN3270 servers.

Advantages of a S/390 or zSeries-based TN3270 server

Since the z/OS TN3270 server structure is that of a SNA session manager, there are certain functions provided by VTAM for applications in the areas of



PAUL ROWNTREE

usability, scalability and management which are not provided or are very limited for dependent LUs. Likewise, since the z/OS TN3270 server is also a z/OS TCP/IP application, there are functions which are provided by z/OS CS which greatly enhance the security, performance and availability of the TN3270 application server.

Scalability

In addition to the scalability provided by the S/390 or zSeries hardware itself, there are two VTAM scalability features, enhanced addressing for session managers and application cloning, that the z/OS TN3270 server can use since it is a full function SNA application.

Enhanced addressing for session managers allows high order addressing for single session capable applications. This support allows/ or provides that the TN3270 clients are not counted in the 64K resource limit enforced by the owning VTAM and therefore allows far greater scalability than in prior releases.

Application cloning improves usability while providing superior scalability. A model application, ▶

(continued on next page)

one which consists of wild cards (“*” or “?”), can be used to represent a group of TN3270 clients with the same characteristics. This not only reduces the amount of definitions needed to represent the TN3270 client population but also reduces all of the associated network resources and storage needed to define a TN3270 workload. In addition, the application representing a TN3270 client is dynamically created upon client connect (via OPEN ACB) and deleted during disconnect of the client (via CLOSE ACB) thus provides network resources and storage to be used only while the client has an active connection. By exploiting application cloning with the z/OS TN3270 server, the customer also has the flexibility of relocating the z/OS TN3270 server to another z/OS image or redirecting the client to another z/OS TN3270 server without the fear of residual definitions in the original VTAM causing confusion in the SNA network.

Management

The z/OS TN3270 server supports full visibility of the IP characteristics (IP address, IP port, and DNS name) of the TN3270 client. This visibility of the client’s IP characteristics from the SNA side of the TN3270 session is key for network/application management. It is available on operator commands and USS messages so that operators and end users can know the identity of the client on both the IP and SNA portions of the connection. This allows problems in the connection between the TN3270 client and the SNA application to be quickly identified and resolved. Furthermore, as of CS for OS/390 V2R10, the IP characteristics are also available to session managers, the Session Management Exit (SME), and the Network Performance Monitor (NPM) allowing for even better customization and problem

determination, as well as authorization and accounting capability.

Performance

Communications Server³ provides the customer with control over the priority of a particular application workload through specification of a QoS policy with the Service Policy Agent. The Service Policy Agent is a daemon on the Communications Server TCP/IP stack and one of its responsibilities is to provide that the differentiated services field in the outbound IP datagrams correspond to the priority specified for that application workload. The OSA Express uses the differentiated services field setting for its priority queuing algorithm as does Cisco in its Weight Fair Queuing. In short, the setting of the differentiated services field is mapped to four priority queues corresponding to network, high, medium, and low priority. During a IBM/Cisco joint quality of service test incorporating OSA Express and Weight Fair Queuing, a four times improvement in average response time for interactive traffic (e.g. TN3270) was obtained.

Security

The z/OS TN3270 server supports SSL client authentication which validates the connection via RACF using the digital X.509 certificate passed from the TN3270E client on the initial SSL connection exchange. This allows that the client is a trusted client prior to allowing any access to the TN3270 server and its corresponding host. This additional level of security is especially important if the TN3270 clients are using the Internet to gain access to the data center. z/OS V1R2 added SSL Express Logon Support which (when used with a compatible client such as Host-on-Demand v5) validates the session while bypassing logon panels. z/OS V1R4 CS will add support for Transport Layer Security (TLS), the successor to SSL.

Availability

The z/OS TN3270 Server benefits from z/OS availability and workload distribution functions such as VIPA takeover and sysplex distributor. Dynamic VIPA support can be used to relocate the VIPA representing the TN3270 server, and allows TN3270 clients that experience an outage to establish a new connection to another TN3270 server (or the same server restarted) much quicker than ever before. Using this capability, our measurements have shown an average reduction of 60% in the time needed for recovery of a TN3270 workload.

Sysplex Distributor is a function that forwards TCP/IP connection requests to replicated application servers within a parallel sysplex which are identified by a specific dynamic VIPA and port. By allowing a dynamic VIPA to become a sysplex wide VIPA address, workload can be distributed to the replicated server instances without requiring changes to clients or networking hardware and without delays in connection setup. Because the Sysplex Distributor function resides in the parallel sysplex itself, it has the ability to factor “real-time” information concerning the replicated server instances including server status as well as QoS and Policy information provided by Communications Server’s Service Policy Agent. By combining these “real-time” factors with the information obtained from WLM, the Sysplex Distributor has the unique ability to provide that the best destination server instance is chosen for a particular client connection while providing that client/server specific Service Level Agreements are maintained. Since the z/OS TN3270 server is a full function z/OS TCP/IP application server, it can take full advantage of the Sysplex Distributor and Dynamic VIPA to balance workload

among multiple TN3270 server instances and to maximize the overall availability of the parallel sysplex for TN3270 workloads.

Fast reconnect enhancement
One of the more common availability problems in a TN3270E environment is that a loss of the TCP/IP connection between the TN3270E client and the TN3270E server also results in a loss of the SNA session between the TN3270E server and the SNA primary application.

Beginning with CS for OS/390 V2R10, the TN3270 Server preserves the SNA session across the reconnect of the TN3270E client. Once the reconnect has been accomplished, there must be a resync of the TN3270E client and the SNA primary application so that normal operation of the session is allowed to continue. Since the client retains no knowledge of the SNA session across the reconnect, it is left to the TN3270E server and the SNA primary application to supply the session information needed by the TN3270E client so that a “bounce” of the SNA session can be avoided. Unfortunately, the TN3270E server simply passes the session data between the SNA primary application and the TN3270E client and therefore has no way of knowing the last session data successfully sent across the SNA session. However, several SNA primary applications (e.g. TSO/VTAM) maintain the last 3270 data screen sent to the TN3270E client and therefore all that must be done is for the TN3270E server to ask for a screen refresh by sending LUSTAT to the primary SNA application. It is also important to remember that even for SNA primary applications which do not support full reconnect (i.e. last screen refreshed), sending the LUSTAT still results in superior network availability. This is due to the fact that these

applications will simply re-prompt the TN3270E client to re-logon via the application logon screen and thus avoiding the negative impacts due to the tearing down and rebuilding the SNA session from a network perspective (i.e. even though the client must re-logon to the application from scratch, the network still sees this as non-disruptive).

Continuing improvements in usability and customization

The already rich definitional capabilities of the z/OS TN3270 Server are further enhanced in z/OS V1R4 CS with additional “goodies” such as:

- The ability to have multiple parameter sets differentiated by IP address or linkname
- More LU naming flexibility provided by more flexible wildcarding capability and the provision for an LU naming exit
- An option to preserve the client IP address to LU name association for a specified period of time after disconnect

How about non-3270 applications?

This leaves the question of how to access non-3270-based applications without requiring a parallel SNA network path into the S/390 or z900.

Enterprise Extender enables e-business applications on the S/390 and IBM zSeries 900, while preserving the investment in Systems Network Architecture (SNA)-based applications and endpoints and leveraging high-speed, industry-standard TCP/IP connectivity.

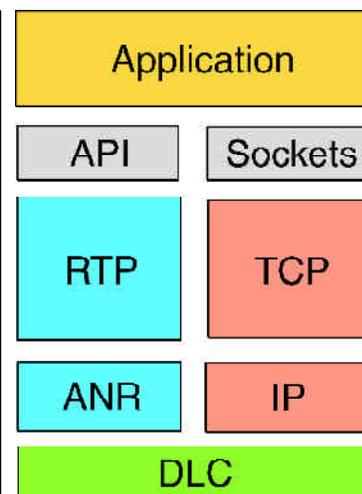


FIGURE 1

From sub-area SNA to enterprise extender

Systems Network Architecture has evolved from the traditional sub-area networks that have dominated the enterprise network landscape for years. Advanced Peer-to-Peer Networking® (APPN®) was an enhancement to SNA that brought the ability to move logical units and change routing without coordinated system definition. High Performance Routing (HPR) was an enhancement to APPN that enabled unparalleled availability by nondisruptively switching sessions around failures. Enterprise Extender (EE) is yet another evolution, providing a means for the efficient transport of SNA data across an IP network.

With Enterprise Extender, the Rapid Transport Protocol (RTP) endpoint views its interface with the UDP layer of the stack as just another data link control, and treats the connection across the IP network the same as it would any SNA connection. ▶

(continued on next page)

HPR's Rapid Transport Protocol component is designed to provide:

- Error detection with selective retransmission of lost packets.
- Nondisruptive reroute based on class of service requirements. HPR preserves the session without impact to the end user for planned and unplanned outages in the session path. In the event that no alternate path is available, HPR can even be configured to preserve the session while the failing component is recovered.
- Proactive congestion control. Enterprise Extender brings with it an enhanced version of HPR's Adaptive Rate-Based (ARB) congestion control algorithm. The new version, Responsive-Mode ARB, is more aggressive in using available bandwidth and more tolerant of variations in network latency. Responsive-Mode ARB was introduced with EE to better allow HPR traffic to coexist with native IP traffic in the backbone network.
- Prioritization. The SNA priority field is mapped to the IP Type of Service (TOS) byte which is used by routing algorithms such as the Cisco Weight-Fair-Queueing algorithm. A set of standard UDP ports are also reserved based on priority with packets mapped to them according to the SNA priority field. Furthermore, the Service Policy Agent (available on Communications Server for OS/390 V2R7 and higher) provides the ability to further refine priority schemes, allowing for options such as setting the Type of Service (TOS) priority based on the time of day or the specific client IP address.

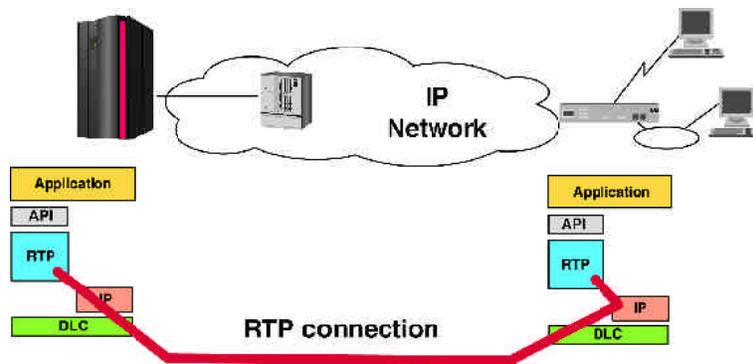


FIGURE 2

The IP layer handles packet forwarding for Enterprise Extender, is designed to provide the following advantages:

- The use of native IP routing maximizes router efficiency.
- By using EE, SNA applications are positioned to take full advantage of advances in IP routing technology.
- Enablement of a single network transport reduces costs, simplifies network management, and simplifies network architecture.

See figure 2 above.

Enterprise Extender: multi-platform, multi-vendor, industry standard

As previously stated, Enterprise Extender is an industry-standard solution defined by the APPN Implementer's Workshop and the IETF. It has been available on IBM's Communications Server for OS/390 product since V2R7 (V2R6 via PTF), and is supported on a number of other products,

including CS/2, CS/NT, and Cisco's SNASw feature for IOS. The multi-platform, multi-vendor support for EE was recently underscored by the successful conclusion of a joint IBM/Cisco scalability and interoperability test.

Enterprise Extender for inter-enterprise connectivity

Enterprise Extender provides an ideal migration tool to enable an alternate inter-enterprise connectivity path for existing users of SNA Network Interconnect (SNI). See figure 3 below.

The APPN replacement for SNI is Extended Border Node (EBN). EBN is a proven technology first shipped on VTAM in 1994, and now used by numerous customers to facilitate inter-enterprise communication, and to ease network consolidation after mergers and takeovers. Unlike SNI, which requires a Gateway NCP to act as the network boundary, the boundary between two EBNs is

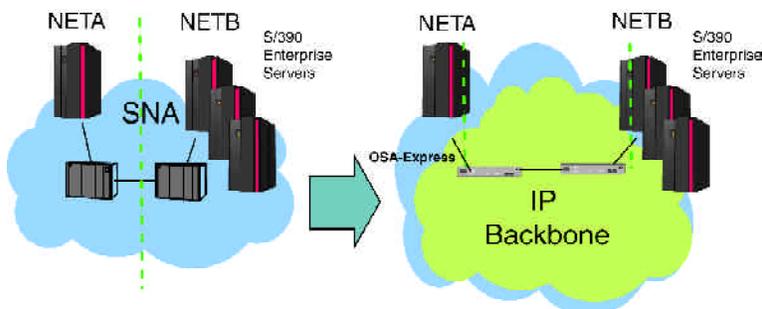


FIGURE 3

represented by the intersubnet link (ISL) itself. Therefore, the ISL is not limited to only NCP-based connections, but instead allows other options such as MPC+ and Enterprise Extender.

Since most enterprises today connect to an IP network (the Internet, intranet, or an extranet), EE emerges as an ideal way to connect multiple enterprises by using the existing IP connectivity. The two S/390 or z900 hosts that formerly acted as gateway SSCPs and ran the SNI protocol over NCP-based connectivity now act as APPN Extended Border Nodes with an Enterprise Extender connection mapped over the IP connectivity. Thus, gateway SSCP/NCP functions are no longer required, and SNA applications can achieve inter-enterprise communication via any IP network attachment and connectivity supported by Communications Server.

Enterprise Extender enables high speed, industry-standard host connectivity

OSA-Express provides an economical, high speed method for host access. The adapter provides access to industry-standard network attachment options via a direct memory access (DMA) model that utilizes a set of priority queues shared between the adapter and Communications Server's TCP/IP stack. Communications Server accesses OSA-Express through the Queued Direct I/O (QDIO) interface, which provides higher bandwidth, lower latency, and reduced CPU consumption.

The QDIO interface is efficient because it treats the OSA-Express adapter as a logical extension of the TCP/IP stack, thereby allowing for an intelligent division of workload between the stack and the adapter. A consequence of this is that the

adapter expects to receive only IP packets across the QDIO interface, and does not support native SNA communication when running in QDIO mode. However, while there is no support for native SNA with the QDIO interface, SNA applications can still utilize this high-speed path by using Enterprise Extender.

Combining the use of Enterprise Extender with OSA-Express provides an ideal way to preserve existing SNA applications, while using industry-standard network attachments with performance characteristics that exceed those of native HPR attachment. Furthermore, by relying on the IP layer for the underlying transport, the EE/OSA-Express combination positions existing SNA applications to take advantage of future advances in IP routing technology and protects customers' SNA device and endpoint investments.

Scalability

Despite some early claims to the contrary, HPR has been shown to be a very scalable architecture. During joint IBM/Cisco testing, 10,000 RTP connections (pipes) were activated on a single S/390. Furthermore, performance studies based on those tests implied continued scalability well beyond the 10K test point.

Recent EE enhancements

Despite the advantages of APPN and HPR, many HPR (and therefore EE) migrations have been delayed or inhibited by a restriction that has existed since the earliest releases of HPR on Communications Server for OS/390. Prior to V2R10, an interchange node (ICN) would not allow HPR on the first hop from the ICN for interchange sessions (those sessions from a sub-area partner, such as an SNI partner, crossing into the APPN network). Given that Enterprise Extender

requires HPR, this restriction was a significant inhibitor to some EE migrations.

This restriction was lifted (with the exception noted below) by CS for OS/390 V2R10. Relief from this restriction is so important in enabling customer migrations to Enterprise Extender, that Communications Server has also provided this function for prior releases (V2R6-V2R8) via APAR OW44611.

There is one remaining limitation for interchange sessions. While V2R10 now allows interchange sessions to enter the APPN network via HPR-capable connections, those connections cannot be over a connection-network (virtual routing node). This remaining restriction is lifted in z/OS V1R4 CS.

Until migration to V1R4, the following recommendations apply for customers deploying EE with connection network:

- Define the EE virtual routing node (VRN) at all ENs, MDHs, branch extenders (BX), and pure network nodes, but not at the ICNs.
- Use only defined (non-VRN) connections at the ICNs.

In most situations, the above recommendations do not imply a great deal of definition beyond what is already required. The ICNs are typically also functioning as network node servers (primary and backup) for the end nodes and branch extenders, and there must be defined connectivity between an EN (or a BX) and its network node server for the CP-CP session.

z/OS V1R2 CS delivers a function called Global Connection Network (GCN) which allows sessions to utilize a shared IP backbone without requiring the data packets traverse the Extended Border ▶

(continued on next page)

Nodes. With GCN, each node has the option of defining a connection network that is “globally known,” that is, known by the same name across multiple APPN subnets. The session setup path still must traverse the EBNs, but the actual session data path is allowed to utilize the direct path via the connection network. (The traditional path through the EBNs is still available, and would typically serve as a backup path.)

z/OS V1R4 CS is planned to provide more improvements for Enterprise Extender in the areas of scalability, usability, and problem determination:

- EE LINEs and PUs can now utilize high-order element addresses.
- EE dial usability is improved by providing a number of controls that allow for automatic recovery of EE connections after failures.

- The RTP display is enhanced to include a number of additional statistics concerning the RTP connection.

Summary

For 3270-based applications, an inboard S/390 or z900-based TN3270 server can be a key component to the solution, allowing TN3270 clients to access SNA applications through an IP network, and limiting the SNA network path to the inside of a single Communications Server image.

Enterprise Extender provides an additional highly-scalable and reliable component for SNA/IP integration strategies. EE allows you to preserve your SNA application and device investment, while maintaining the session prioritization and availability characteristics of SNA and HPR.

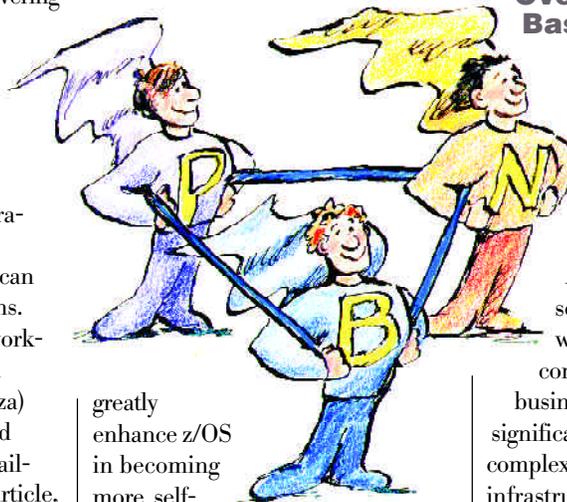
Furthermore, EE allows for a simplified network architecture that positions applications for exploitation of future advances in IP networking technologies. ■

- 1 The term TN3270 server used in this article represents a server which supports both standard TN3270 clients as well as TN3270E clients. If a function is specific to TN3270E client support then the term TN3270E server will be used.
- 2 Except where noted, comments concerning the z/OS TN3270 server also apply to the Communications Server for OS/390 TN3270 server.
- 3 In this article Communications Server refers to Communications Server for OS/390 and z/OS Communications Server.

Policy Based Networking in z/OS: Quality of Service and Intrusion Detection Services

BY LAP HUYNH AND LIN OVERBY

Following the tradition of delivering the best and most advanced features for z/OS, the Policy Based Networking (PBN) support of CS for z/OS allows customers to differentiate e-business applications, to optimize their e-business infrastructure, and to protect and defend it from intrusion that can disrupt e-business transactions. Therefore, Policy Based Networking plays an important role in enabling a self-managed (eLiza) system achieve a set of desired objectives in performance, availability, and security. In this article, we will highlight the PBN functions for network Quality of Service (QoS), and Intrusion Detection Services (IDS). These functions



DIANE ATTEBURY

greatly enhance z/OS in becoming more self-managing in two areas: self-optimizing and self-protecting.

Overview of Policy Based Networking

A policy is a set of directives that control the behavior of a computing infrastructure to achieve a set of desired objectives. Advances in hardware and software technology together with the necessity for companies to conduct business on the Internet have significantly increased the complexity of companies' computing infrastructure. This trend has led to eLiza, a leading new initiative spearheaded by IBM. This new initiative has brought increased focus on the importance of a policy

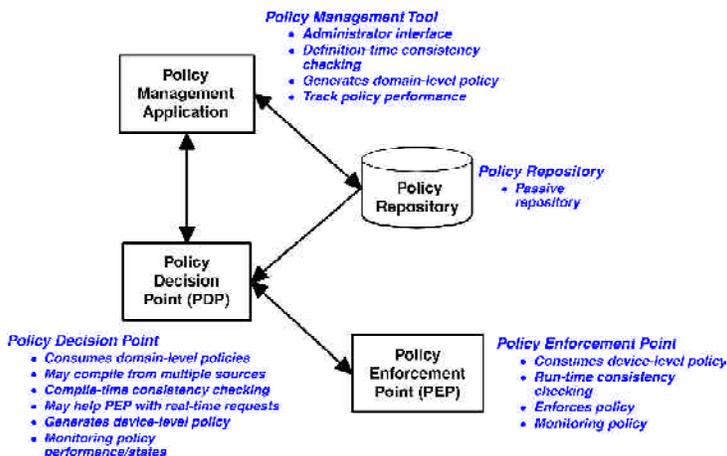


FIGURE 1 - IETF POLICY ARCHITECTURE MODEL

based management system that would allow I/T professionals to manage their infrastructure more simply and effectively. Several standard bodies, notably the Internet Engineering Task Force (IETF)

and the Distributed Management Task Force (DMTF), have formed new working groups to address policy based management in general and policy based networking in particular. The IETF policy based networking architecture model is depicted in figure 1. Figure 1 also includes the functional role of each respective component. It is important to emphasize the importance of policy monitoring in this model since that's how administrator or a management application can get feedback on the operational efficiency and correctness of the infrastructure.

The Policy Based Networking (PBN) in z/OS closely follows this architecture model. Its components are shown in Figure 2. The Policy agent (Pagent) and the z/OS TCP/IP stack play the PDP and the PEP roles in the IETF policy model. Figure 2 also shows various components that support Quality of Service (QoS) function, and the Intrusion Detection Services (IDS) function.

The semantic of policy can be simply illustrated as follows:
If condition then action

Condition specifies a set of filters to identify certain network activities/events or traffic. For example, a filter can identify traffic from a client's node IP address attempting to access a server's node IP address to request specific service from an application (a Web-application server). Additionally, a filter can identify certain networking events that constitute an attack (e.g., scan event). Action specifies how the identified activity/event or traffic must be treated. For example, a Web-application request from an important client should be assigned to high priority with a minimum throughput; or a detected intrusion event/packet

should be logged, sent notification, and/or discarded.

Policy Based Networking—Quality of Service (QoS)

The Internet Engineering Task Force (IETF) has defined two mechanisms for providing Quality of Service: the first form, namely the Integrated Services (IntServ), is an end-to-end reservation based service that uses explicit Resource Reservation Protocol (RSVP is a signaling protocol) to request an appropriate level of service for specific traffic “sessions/flows”. This reservation state corresponds to how much resource (e.g., bandwidth, buffer space) is allocated to the reservation. IntServ is appropriate for traffic types that require bandwidth and delay guarantee such as VoIP (Voice over IP), or video streaming. RSVP signaling protocol has also found its way into the newly emerging Multi-Protocol Label Switching (MPLS) service that is becoming popular with service providers to provision Virtual Private Network (VPN). Services of the second form, namely the Differentiated Services (DiffServ), provide service differentiation between broad classes of users and applications. In other words, it is a form of aggregation of traffic class with the same

(continued on next page)

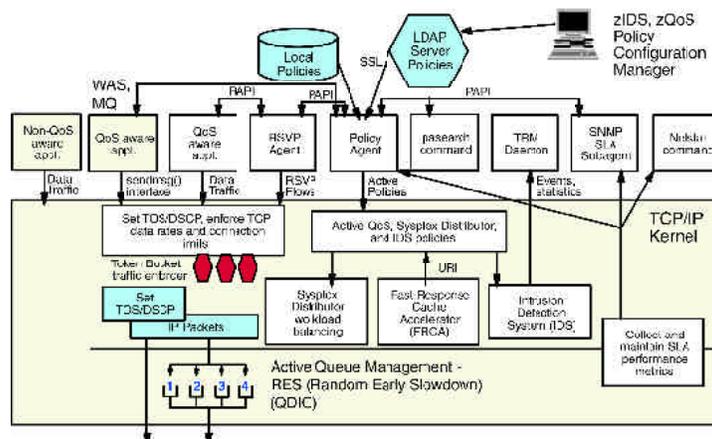


FIGURE 2 - COMPONENT STRUCTURE OF POLICY BASED NETWORKING IN Z/OS

network service provision. *DiffServ* uses the Differentiated Services Code Point (DSCP—RFC2474) in the IP header to indicate different QoS service levels. Note that DSCP redefines the Type of Service (ToS) field in the IP header. Each host/networking device will, based on the DSCP value, provide appropriate QoS treatment to the corresponding traffic class. For zSeries's QDIO devices, the ToS/DSCP value will be mapped to appropriate QDIO priority queues for transmission as shown in Figure 2. DiffServ depends on hosts and networking devices to respect the QoS service level setting to provide consistent end-to-end behavior. Most z/OS customers should be familiar with QoS service level because of similar function that has always been available in IBM's SNA/APPN-HPR networking architecture using COS names (Classes Of Service) and Transmission Priority. With Enterprise Extender (EE) and PBN QoS, SNA/APPN-HPR applications can now transported across TCP/IP networks with the same quality and predictability as it was always expected with SNA/APPN-HPR.

Policy Based Networking QoS feature in z/OS supports an extensive set of condition (refer to the discussion on policy semantic above) filters that allow administrators different ways to identify and differentiate service levels for different hosts (clients/servers), applications (e.g., Web, MQ, FTP), times (including time of day, days of week, months etc.), and application specific data (e.g., URL/URI for Web traffic, message queue priority for MQ). Once a class of traffic is identified by the condition, a corresponding QoS service level is assigned (often identified as gold, silver, bronze, etc.) in the action. A set of QoS service level parameters can be used in the action for service differentiation

ranging from setting the ToS/DSCP (including the VLAN priorities in VLAN header) of the corresponding packets to controlling TCP throughput and connections, to limiting bandwidth of a traffic class by using the token bucket mechanism, to denying traffic from utilizing network resources.

Figure 3 shows, using the PBN QoS feature in z/OS along with Cisco's routers that support service differentiation based on ToS/DSCP value, how critical Web traffic (generated with WebSphere Application Server) competing with

from Pagent. In other words, SD function optimizes computing resource usage not only within a Sysplex but also the network.

Additionally, with the policy based routing feature, SD can also direct incoming requests to a particular target server(s) that is designated to serve those requests. This feature can be particularly useful for differentiating a set of clients from others, e.g., those that are assigned to a reserved server(s) for better response time. Also, it is quite useful in providing fail-over scenario where in normal operation

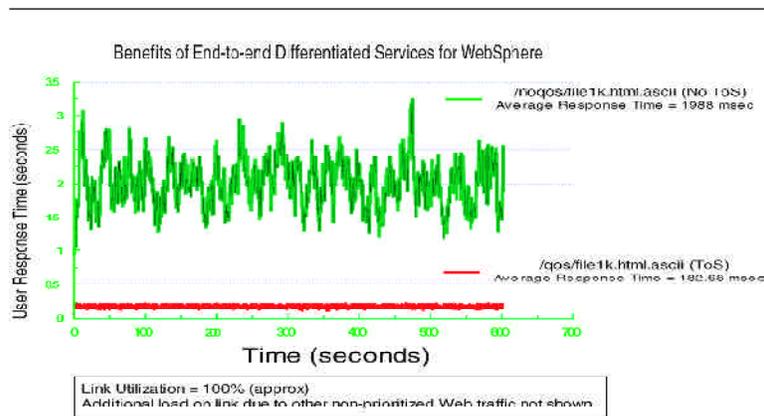


FIGURE 3

less important traffic can achieve consistent response times (lower lines) compared with the widely oscillating response times (up lines) without PBN QoS.

Sysplex Distributor routing policy and dynamic load distribution

One important function of PBN QoS involves Sysplex Distributor (SD) function. Briefly, SD is a workload balancing entity that distributes incoming work requests (TCP connections) to a set of target servers. For each request, the most efficient target is selected to which the request is routed. The selection of the most efficient target is based on z/OS Workload Manager (WLM) information (node/server capacity) and network QoS performance load

requests are routed to a set of targets but if non is available, a back-up target will then and only then be used.

Policy performance and networking SLA MIB

As shown in Figure 1, once QoS policy are defined and enforced, it is important to monitor their performance for the purpose of network planning and for monitoring any deviations in order to be proactive in addressing clients' overall end-to-end Service Level Agreements (SLAs). PBN in z/OS provides network SLA Management Information Base (SLA MIB), which can be used to monitor the performance of respective network QoS policy. Thresholds can be defined for different QoS perfor-

mance attributes (e.g., delay, throughput) such that when a deviation occurs, traps will be sent to the attention of the right SNMP manager for appropriate actions. The information on a per-policy rule basis that is reported in the SLA MIB can also be effectively used for accounting/billing data: information such as the bytes/packets sent/received, in-profile versus out-profile counts. Netstat command can also be used to retrieve policy performance data locally on the system.

Policy Based Networking—Intrusion Detection Services (IDS)

The value of intrusion detection has been long recognized for scenarios where an enterprise network is connected to an “untrusted” network such as the Internet. The need for intrusion detection is now being elevated as the threat of hackers and cyber-terrorists increases. Studies are now revealing that the internal network is also a source of many attacks. The attacker could be either a malicious user within the enterprise, or could be a server compromised, either from internal or external sources, that is unknowingly launching an attack on internal network resources. Network-based intrusion detection sensors placed in the network can detect many of these attacks, however, there are additional benefits gained by including network intrusion detection function in the target server.

In z/OS V1R2, the z/OS Communications Server added support for integrated Intrusion Detection Services (IDS) which enable the detection of attacks against the TCP/IP system and the application of defensive mechanisms on the z/OS server. The focus of IDS is self-detection and self-protection.

The IDS is policy-driven and its intrusion detection points are integrated into the z/OS Communications Server TCP/IP system on the data path. The IDS is viewed as complementary to external network-based intrusion detection sensors. By exploiting its position as a communications endpoint, the IDS broadens the set of detectable intrusions and can detect intrusions that otherwise could go undetected. By integrating this function in the target server, the IDS can efficiently evaluate data that is unavailable to external network intrusion detection sensors. For example, data that has been encrypted end-to-end by IPSec can be examined in clear-text after decryption. The IDS also has access to internal information such as system resource usage, connection state information, and internal thresholds and counters that can further determine whether an intrusion event is surfaced.

The z/OS Communications Server IDS can also implement real-time online defensive policies against attacking packets that cannot be implemented by external network-based intrusion detection sensors. A typical external sensor analyzes network traffic by “sniffing” data in promiscuous mode as it traverses a network segment. After the data is read from the network, the network sensor can perform “pattern matching” on the data against a table of known attack signatures. When a match is found, an alert can be raised to an IDS manager. Because the data is read in promiscuous mode, the delivery of packets to the target is not delayed, leaving no opportunity for the external sensor to discard an attacking packet before it reaches its destination.

Rather than using an attack signature approach which requires the definition of each specific known attack, the Communications

Server uses policy to define intrusion types by category. The defined policies inform the TCP/IP stack which categories of intrusions are of interest to the installation. By classifying the attacks into categories the IDS can avoid the overhead of evaluating each packet against a table of signatures. The IDS can perform “in context” intrusion detection on the data path, classify the detected intrusion, and then consult the policy to determine the action to take. The design of the detection points in the TCP/IP stack allows for the detection of intrusions without requiring precise “pattern matching” of attack signature to packet contents. Using this approach to intrusion detection, the z/OS IDS has capability to detect intrusions not yet invented, and without requiring an update to policy.

The Communications Server IDS classification of intrusions in policy are *Scan*, *Attack*, and *Traffic Regulation*. *Scans* are the category of activities related to gathering information prior to an intrusion. Information collected by a scanner may include network topology and location of services. The Communications Server IDS can detect ICMP (network) scans and TCP and UDP port (services) scans. *Attacks* include single packet or multiple packet attacks that are launched in an attempt to bring the system down or otherwise render the system unusable. The IDS classifies the Attack category into subcategories which include malformed packets, inbound fragment restrictions, IP option restrictions, IP protocol restrictions, ICMP redirect restrictions, outbound raw sockets restrictions, synflood, and UDP perpetual echo. *Traffic Regulation* includes detection of an unexpected peak of either valid request or malicious traffic. The Communications

(continued on next page) ▶

Server IDS performs inbound traffic regulation for both TCP and UDP traffic.

IDS policy conditions are defined using the intrusion categories and subcategories described previously. These conditions can be further qualified by restricting a policy to a certain TCP or UDP port, by excluding certain network resources, or by including an event sensitivity level in order to reduce event volume and the number of false positives. IDS actions can specify a defensive action such as packet discard or connection limiting. It can also specify a notification action such as recording an event via console messages or syslog records, recording statistics to syslog, or tracing a sample of packets that are associated with an intrusion event.

An IDS report program, TRMDSTAT, provides summary and detailed reporting of IDS events and statistics. IDS messages can drive NetView® message automation. Possible message automation actions include routing messages to a NetView console, notifying a system administrator via email or pager, or running TRMDSTAT reports and attaching the reports to an email to the system administrator. Sample NetView clists are available at http://www.tivoli.com/support/downloads/netview_390/tools/idsauto.html.

Policy configuration managers

IDS and QoS policy configuration managers are made available for free download on the Web. These

policy configuration managers shield the administrator from the complexity of LDAP policy object classes and attributes and presents a simple interface for configuring IDS and QoS policy. The URLs for these managers are:

<http://www.ibm.com/software/network/commserver/downloads/zidsmanager.html>

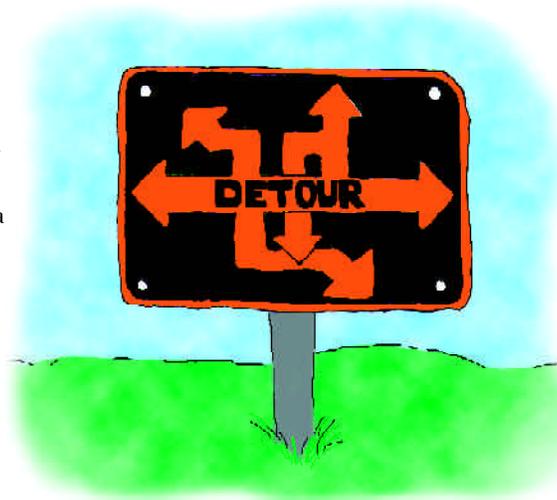
<http://www.ibm.com/software/network/commserver/downloads/zqosmanager.html>

For more information on the z/OS Communications Server Policy Based Networking Quality of Service and Intrusion Detection Services, refer to chapters 12 and 13 of the *IP Configuration Guide, SC31-8775-01* at <http://www.ibm.com/servers/eserver/zseries/zos/bkserv/r2pdf/commserv.html>. ■

z/OS TCP/IP Dynamic VIPAs, Sysplex Distributor, and how they are exploited

BY JAY AIKEN

Availability and workload balancing in z/OS—Dynamic VIPA and Sysplex Distributor. The basic function of a TCP/IP stack is to provide a sockets-based interface to application programs, and to help transport application data from one place to another within an IP network. However, as IP networks are increasingly used for business-critical applications, availability and workload balancing are of increasing concern to enterprises. Web-based interfaces to customers, employees, and suppliers need to be available continuously, and the unpredictable nature of workload means that work needs to be distributed among multiple servers



NATASHA FRAY

in a way that is available, reliable, scalable, and easily expandable.

Since OS/390 V2R7, released in March, 2000, OS/390 and z/OS TCP/IP have increasingly exploited the underlying Sysplex technology

of S/390 and zSeries to provide enhanced availability and workload balancing. A previous Hot Topics article introduced Dynamic VIPAs (DVIPAs), and this article will expand to cover Sysplex Distributor, as well as show how they are exploited by selected IBM middleware.

The IBM middleware exploiters described here are:

- DB2®
- LDAP
- WebSphere

The examples are intended not only to show how IBM products work with synergy, but also to suggest

possible ways in which other middleware and your applications might benefit from these technologies. The examples are high-level overviews. For more complete information, please refer to the respective product documentation.

VIPAs—Virtual IP Addresses

Each adapter in the IP network has to have an IP Address to allow the network to route traffic to the right place. The Virtual IP Address, or VIPA, introduced in OS/390 V2R5, provides an IP address that is not associated with any particular physical adapter, and which therefore is always available as long as its owning TCP/IP stack is functioning. Most large systems such as S/390 and zSeries machines, have multiple IP adapters. As long as one of them is working and connected to the IP network, others may fail without disrupting service to the applications using the VIPA on that system.

TCP/IP on OS/390 and z/OS now provide a function which allows automated movement among TCP/IP stacks in a Sysplex for new kinds of VIPAs, and such VIPAs are called Dynamic VIPAs.

Dynamic VIPAs—two kinds

Client/server applications may be structured in different ways, and Dynamic VIPAs have to take into account two basically different models. The first kind, Multiple Instances DVIPAs, is used when any of several application instances can handle a client request, and is also used as the mechanism by which the Sysplex Distributor routing stack is backed up. Since such application instances generally also use Sysplex Distributor, these DVIPAs will not be covered further here.

(Application) instance-specific DVIPAs

A client may need to maintain a relationship with a particular server, either for multiple connections over normal operation, or to reconnect to a particular server for failure recovery. For example, a client may need to reconnect to the same transaction server while a transaction is in progress. The IP address must be associated with the particular instance, and the TCP/IP stacks in the Sysplex have no idea ahead of time where the instance may be started—or where it may move.

Fortunately, TCP/IP can use the application instance itself to tell the stack where to activate the DVIPA. An application may be

configured to bind its listening socket to a particular IP address, rather than any IP address (INADDR_ANY). Given configuration on z/OS TCP/IP to allow this IP address to be activated dynamically, TCP/IP will verify that the DVIPA is not active elsewhere in the Sysplex, and will then activate the DVIPA automatically before reporting successful completion to the application.

If the application later closes its listening socket, TCP/IP will deactivate the DVIPA. If the application is restarted on another stack, similarly configured to allow this dynamic activation, the DVIPA will be activated there.

If the application cannot be configured to bind to a particular

(continued on next page)

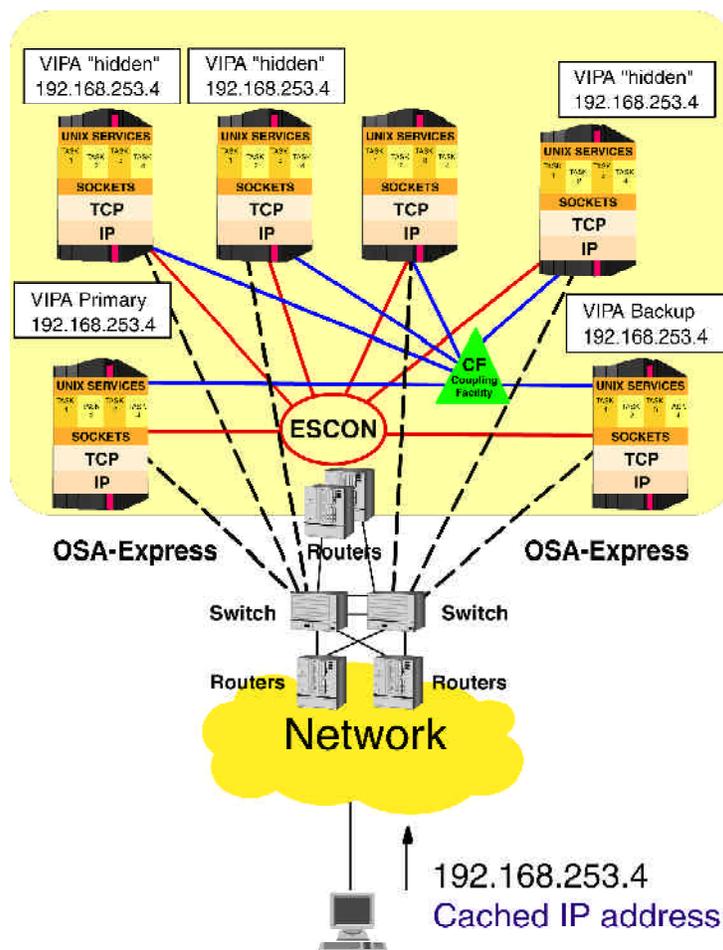


FIGURE 1

IP address, but always binds its listening socket to INADDR_ANY, TCP/IP provides two solutions: a utility called moddvipa which will activate the DVIPA as a job step in the application JCL and delete it later, or the BIND parameter on the PORT statement that will convert the application's bind (INADDR_ANY) to bind to a specific IP address. Either mechanism may be used to activate an instance-specific DVIPA.

Sysplex Distributor

Sysplex Distributor is the strategic IBM solution for connection workload balancing in the Sysplex. A cluster of server instances is represented by a single IP address, called a Distributed DVIPA. A multiple-instance DVIPA is defined on a primary Sysplex Distributor routing stack and on backup stacks as appropriate, and designated as Distributed. The application ports are also identified. On all candidate target stacks which may host an application instance, the same DVIPA address is activated as "hidden," similar to a loopback address. The target stack knows when an application establishes a listening socket bound to one of the Distributed DVIPA ports, and notifies the routing stack, in essence, "I've got a live one..." The routing stack will send future TCP connections for that application (port) to that target stack. If the server should terminate or close its listening socket, the hosting target stack is immediately aware of this, and notifies the routing stack.

When a TCP connection request arrives, the Sysplex Distributor routing stack consults Workload Manager for relative capacities on the LPARs hosting the target stacks, and Service Policy Agent for network performance and defined policies that might affect the distribution decision. The routing stack then selects a target

stack with a listening application, and forwards the request to that target stack for processing.

The routing stack also remembers the full connection information so that future TCP segments for that connection can be sent on to the

reachable via a specific IP address (the member-specific DVIPA in this case). To address the case when the DB2 itself terminates and is restarted on another image, possibly with another DB2 instance, each DB2 instance configures its restart address with

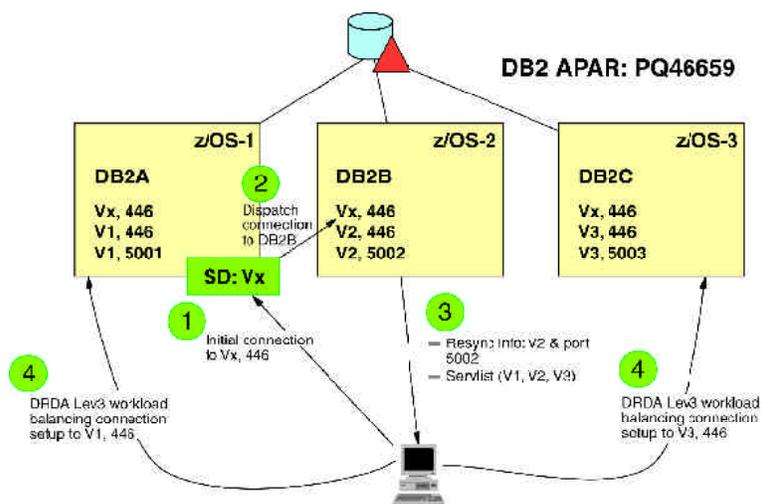


FIGURE 2

same target stack for processing. Exploiting Dynamic VIPAs and Sysplex Distributor—DB2 DB2 Distributed Data Facility adds functionality to exploit both instance-specific (member-specific) Dynamic VIPAs, and Distributed DVIPAs with Sysplex Distributor. DB2 calls the Distributed DVIPA the DB2 location or group Dynamic VIPA, and the instance specific DVIPA the member-specific Dynamic VIPA, used as follows:

The DRDA protocol provides an initial contact port and a resync port. The initial contact port is normally DB2's registered well-known port of 446. The resync port is used by a DRDA client when the initial connection is broken, and the client and server need to resynchronize after the error.

Obviously, resynchronization needs to occur with the specific DB2 instance with which the client was in session, so this instance must be

a port number unique to that instance, such as ports 5001, 5002, and 5003, for instances DB2A, DB2B, and DB2C, respectively. The initial contact point is bound to the location (Distributed) DVIPA on port 446, and the resynchronization port is bound to the member-specific DVIPA, with the BIND parameter on the PORT reservation statement in TCP/IP configuration. The location of a particular DB2 instance at any point in time is thus transparent to the DRDA® clients.

The initial contact request from any type of DRDA client may go to any of the DB2 instances in the datasharing group. This connection request goes to the location DVIPA, and Sysplex Distributor distributes it to one of the listening DB2 members. After the connection has been established, the DB2 server will send the client its member-specific DVIPA, and will also send the member-specific DVIPAs of all other DB2 instances in the

datasharing group to DRDA Level 3 clients so they can perform their own load balancing. DB2 initial client contact requests are thus distributed using Sysplex Distributor, but the clients may get in touch with a specific member of the datasharing group via its member-specific (instance-specific) DVIPA.

Exploiting Dynamic VIPAs and Sysplex Distributor—LDAP

Client requests for LDAP are fully atomic, in the sense that the requests are fully satisfied (or not) within a single connection. One way in which LDAP may be deployed is for one server to act as the master, and other servers to act as slave replicas of the master. The master LDAP server sends update requests to the slave servers to keep them in sync. Each slave server thus needs an instance-specific DVIPA to allow the master to locate a slave, to synchronize only what needed for that particular slave.

The ability for clients to locate the one and only master server is also critical. The master server is given an instance-specific DVIPA for handling client requests, known also to the slave servers. Client requests are sent to slaves using Sysplex Distributor. When a slave determines that the client must use the master, the slave sends the DVIPA of the master to the client using LDAP protocols. The client then reconnects to the master using the master's instance-specific DVIPA which it received from the slave server.

Thus, Sysplex Distributor assures availability and workload distribution for external client requests, while instance-specific DVIPAs assure that the master and slaves can locate each other no matter where any participating LDAP

server may move within the Sysplex. Exploiting Dynamic VIPAs and Sysplex Distributor—WebSphere WebSphere Application Server has two main TCP/IP means of entry, the HTTP catcher and Internet Interoperability Object Protocol (IIOP). WebSphere HTTP Catcher Hypertext Transport Protocol (HTTP) servers are candidates for workload distribution when each HTTP request connection results in no saved state or when the HTTP and application servers are configured to share persistent state. In those cases, Sysplex Distributor is a good candidate for workload distribution, as is the Network Dispatcher in WebSphere Edge Server (WSES). When WSES is used for workload distribution, each server on OS/390 or z/OS may be given an instance-specific DVIPA so that the Network Dispatcher can always locate the same server when there is an affinity.

WebSphere IIOP

Internet Interoperability Object Protocol (IIOP) is a means of making Remote Method Invocations (RMI). The requester gets in touch with an IIOP daemon to request the location of the application server with the object that can satisfy the method invocation. The daemon is fully aware of all such server instances, and manages the distribution of RMI requests very intelligently using domain names and DNS look-ups. Because this distribution takes into account the content of the request, the application servers are not good candidates for pure connection balancing via Sysplex Distributor, but the application servers may of course exploit instance-specific DVIPAs for location transparency. On the other hand, requests to the location daemons are entirely independent of each other, and Sysplex Distributor can and should be used to provide both high

availability and workload balancing for multiple IIOP daemons running in various OS/390 or z/OS partitions within the Sysplex.

Summary

Dynamic VIPAs were delivered in OS/390 V2R8, and Sysplex Distributor and other enhancements in OS/390 V2R10. These functions were designed to provide failure independence in the face of TCP/IP or OS/390 outages, as well as load balancing through distribution of TCP/IP connections to multiple instances of a server application deployed in an OS/390 or z/OS Sysplex environment.

Applications which could exploit Dynamic VIPAs and Sysplex Distributor are too numerous to mention. This white paper gives examples of IBM middleware products which exploit Dynamic VIPAs and Sysplex Distributor, or which may be deployed with these functions for enhanced availability and workload balancing. We hope these few examples are varied enough to give readers an idea of how other middleware and application products might similarly be deployed with Dynamic VIPAs and Sysplex Distributor for similar benefits.

References

- *z/OS V1R2.0-V1R3.0 Communications Server IP Configuration Reference, SG31-8776-02*
- *z/OS V1R2.0-V1R3.0 Communications Server IP Configuration Guide, SG31-8775-01*
- A significantly expanded version of this article will be available in June, 2002, at the IBM Networking Technologies Web page: <http://www.ibm.com/servers/eserver/zseries/networking/technology.html>. ■

zSeries and z/OS Hipersockets overview

BY JAY AIKEN, JIM GOETHALS, AND BOB PERRONE

By now you have heard a lot about IBM zSeries, and you have probably heard about Hipersockets—but what is Hipersockets, really? How can it benefit you, and why should you care about it? We'd like to give you an overview of Hipersockets, a new connectivity technology on z800 and z900 hardware, which is supported by z/OS 1.2, z/OS.e, z/VM™ 4.2, Linux for zSeries and Linux for S/390. This article will focus on z/OS software, but rest assured that the other supporting software environments also provide full support—and connect and interoperate with each other as well.

Overview of Hipersockets—what it is, and what it is not

What is Hipersockets? It is a new and very fast means of transporting TCP/IP traffic between logical partitions (LPARs)—operating system images, TCP/IP stacks, guest virtual servers under z/VM, and associated middleware and applications—on zSeries. If you know about OSA-Express with Queued Direct I/O (QDIO), the adapters which support Gigabit Ethernet, then you know a bit about Hipersockets already. From a z/OS perspective, Hipersockets has the characteristics of an OSA-Express device, including configuration, qualities of service, and manageability. The main difference is that Hipersockets only reaches within the covers of a single zSeries system, and you will

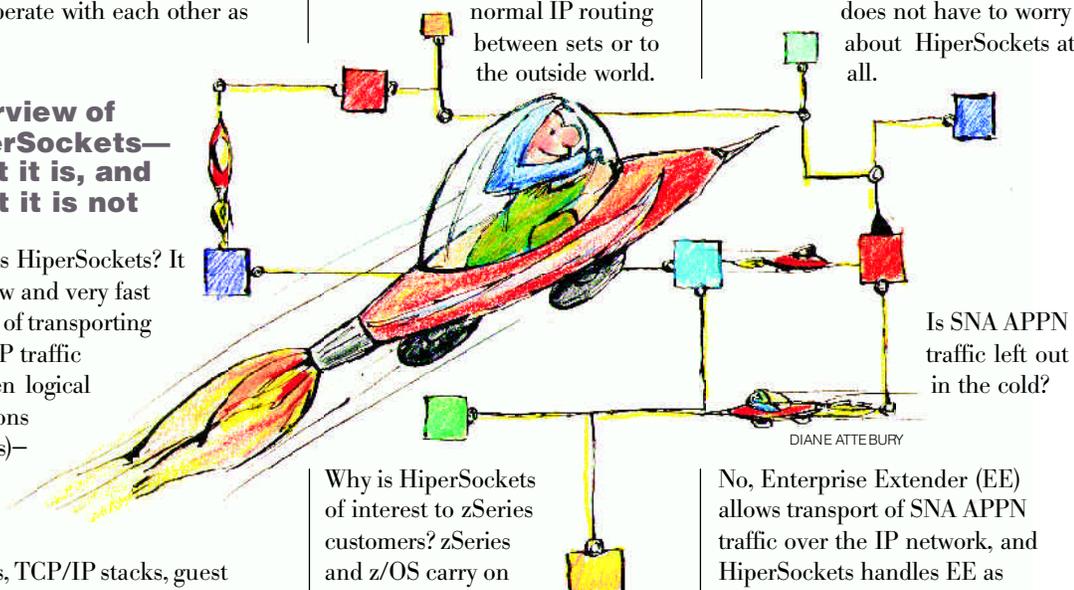
still need other adapters to connect externally to other servers or the rest of your TCP/IP network. So you can think of “it” as up to four shared OSA-Express adapters each connecting to a LAN. Each zSeries supports up to four Hipersockets devices, each entirely independent of each other as far as connectivity is concerned. If you have sets of logical partitions (LPARs) that need to communicate within a set, but not directly with other LPARs on another system, you can configure and use a Hipersockets device

within a set, and use normal IP routing between sets or to the outside world.

keep your partitions logically isolated and separated.

What Hipersockets is not: it is not something that requires a change to applications using sockets. Applications and middleware use it as they would an OSA-Express, which is to say they are entirely unaware of it, once the system programmer has activated it and made it available to the supporting TCP/IP stack. TCP/IP stack takes care of managing the device and sending IP packets via the most efficient route, and the software that uses sockets to communicate

does not have to worry about Hipersockets at all.



Is SNA APPN traffic left out in the cold?

Why is Hipersockets of interest to zSeries customers? zSeries and z/OS carry on the IBM tradition of managing corporate data in an exceptional manner, but customers also want to consolidate their e-business infrastructure to make it more cost-effective and manageable, while still maintaining the separation and heterogeneity that made the multiple platforms attractive. *See figure 1 on page 29.*

If you do not want all of your front end servers to communicate directly with all of your back end servers, you can also configure multiple Hipersockets devices to

No, Enterprise Extender (EE) allows transport of SNA APPN traffic over the IP network, and Hipersockets handles EE as typical IP traffic. Enterprise Extender over Hipersockets (or OSA-Express) can actually be more efficient in terms of CPU utilization, as well as faster than native APPN HPR over ESCON® links.

How does Hipersockets work?

Hipersockets is an I/O adapter that you cannot see and touch—all of the function is emulated in zSeries processor microcode and millicode. As with OSA-Express, Hipersockets uses the very

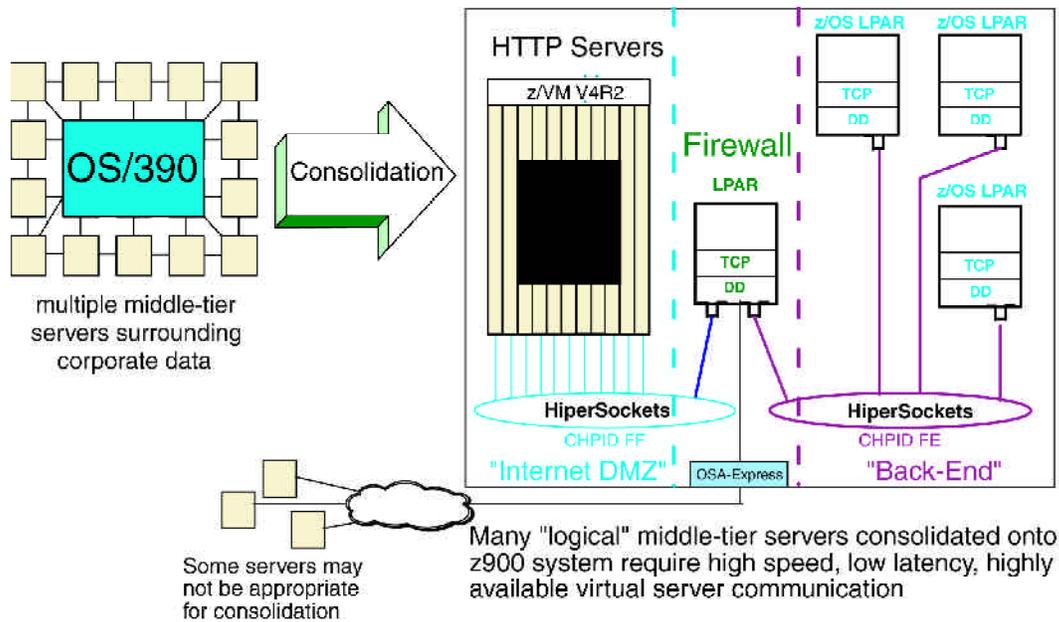


FIGURE 1

efficient Queued Direct I/O (QDIO) architecture, so that the “adapter” reads directly from and writes directly into IP data buffers, without requiring channel programs. HiperSockets is more advanced than OSA-Express.

Whereas a shared OSA-Express transmitting data from one LPAR to another on the same system will copy data from the sending buffer onto the OSA-Express adapter and then copy to the receiving buffer in the other LPAR, with HiperSockets, the processor emulation transfers data in a single move—like a cross-address-space memory to memory move—all in one synchronous operation.

In short, HiperSockets implements a control device emulation very much like OSA-Express with which each of the exploiting TCP/IP stacks register their respective IP addresses. Each input queue is identified by a specific address unique to a HiperSockets and is maintained in a common lookup table for that HiperSockets on the zSeries system. When a TCP/IP stack sends a packet, a lookup is performed, and the

processor handling the send will then directly copy the data from the sending buffer to the receiving buffer with all of the normal zSeries memory protections to prevent corruption of data and security exposures.

HiperSockets Accelerator—connectivity to the rest of the world

What about connectivity to the outside world? Fast transfer of IP data among LPARs on a zSeries system is interesting but it’s also important that data can get into and out of the server to the external network very efficiently and quickly. z/OS V1R2

contributes to that as well, with an extension to the z/OS TCP/IP stack we call the HiperSockets Accelerator.

Since both OSA-Express and HiperSockets use the same base QDIO architecture, and in particular the same structure of

I/O buffers, z/OS can take advantage of the similarities to route IP traffic very quickly from HiperSockets to an external QDIO OSA-Express adapter, and vice versa. See figure 2 below.

A z/OS TCP stack configured for HiperSockets Accelerator will monitor IP traffic being routed

(continued on next page)

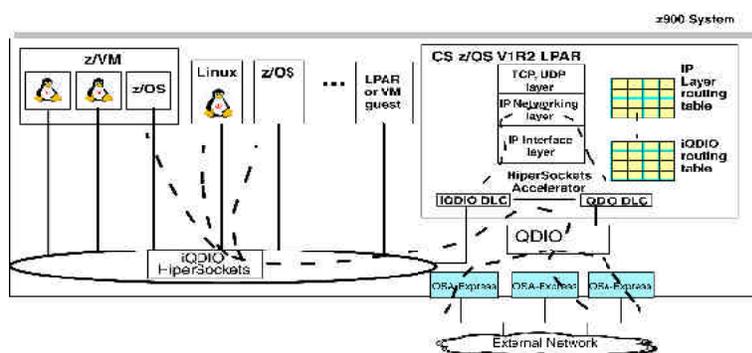


FIGURE 2

between OSA-Express and a HiperSockets device. The first packet will go through normal IP routing, but when z/OS sees a combination of source and destination IP addresses that can go directly between HiperSockets and the OSA-Express handling connectivity to the outside world, the z/OS TCP stack instructs its device drivers to perform routing for subsequent packets automatically.

All subsequent packets between the same source and destination will now be copied directly at the device driver level, without even involving the TCP/IP stack. Some restrictions include no fragmenting and need for IP forwarding, but with a properly configured HiperSockets and OSA-Express QDIO network pair, the performance and transfer cost savings can be substantial.

So how does HiperSockets perform?

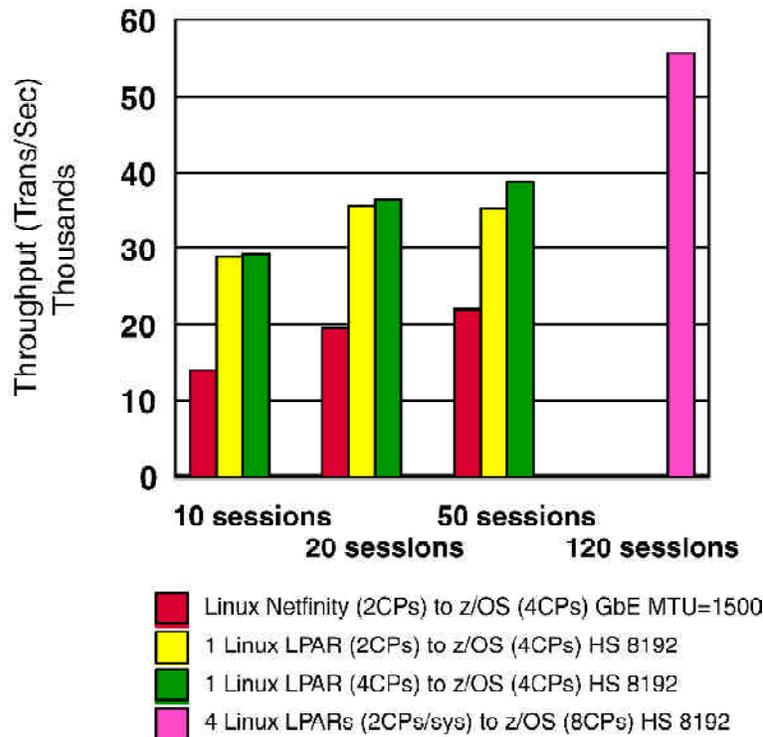
As a networking media, HiperSockets is the fastest TCP/IP connection within zSeries. Here are a few benchmark reference points that demonstrate the HiperSockets technology potential in interactive traffic and bulk data transfer environments: Interactive traffic using HiperSockets A Request-Response (RR) traffic profile, sending a 200 byte inquiry and receiving a 1000 byte response back, was repeatedly run and measured. Also, to demonstrate the consolidation value when using HiperSockets, the RR test contrasted the external Linux system and the consolidated Linux LPAR system environments. The test compared these two Linux client environments when connected to z/OS server LPAR. The Linux on a Netfinity was connected via

Gigabit Ethernet, and the Linux LPAR was connected via HiperSockets. *See figure 3.*

Results validated HiperSockets' performance and scalability superiority over Gigabit Ethernet:

- Throughput increased 1.6 to 2.1 times, comparing a Linux LPAR using HiperSockets to an outboard Linux on Netfinity® using OSA-Express GbE.
- When the z/OS server CPU Utilization approached 100% for the 50 sessions case, we added 4 CPUs to the z/OS LPAR and increased the number of sessions to 120. This increased throughput by 44.7%, to a maximum of 55,800 transactions per second.
- In a separate z/OS LPAR-to-z/OS LPAR test, HiperSockets (at 30,000 transactions per second) had 1.8 to 2.1 times the throughput, and 46% to 52% better response times than OSA-Express GbE.
- These tests show the benefits of increased throughput when consolidating onto zSeries. It also demonstrates the scalability of the HiperSockets technology, which goes far beyond the ability of an external Gigabit Ethernet connection.

RR Throughput Summary (Linux to z/OS)



HiperSockets performance (bulk data transfer):

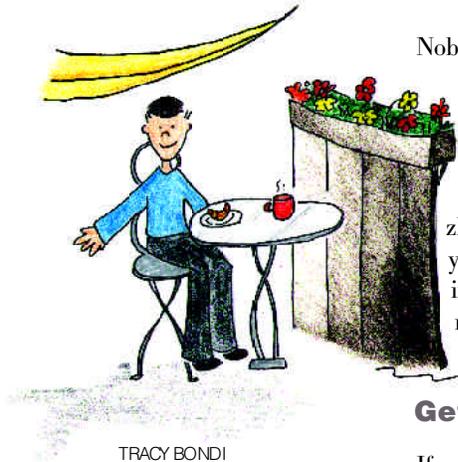
A Streams (bulk data) traffic profile, sending a 20 Megabyte file and receiving a 20 byte response back, was repeatedly run and measured. The Streams test contrasted the external Linux system and the consolidated Linux system environments. The test compared these two Linux client environments when connected to a z/OS server LPAR. The Linux on ▶

FIGURE 3

(continued on page 31)

zTour of zFavorites

BY GEOFF SMITH



TRACY BONDI

Nobody can deny that the Internet is a wonderful thing. You can find information on nearly any topic and information discovery can be a fun past time. However, when you need to get work done, when you need information on the latest release of a zSeries product or service, then you should find this little CD useful.

zFavorites is a small pocket-sized CD that you can carry anywhere with you. It contains “favorite” links to the major home pages for zSeries information all neatly categorized to help you locate the information you need quickly. It also contains PDF versions of some of the latest Redbooks and helpful links to download sites.

Getting started

If you haven’t already done so, take the zFavorites CD from the envelope in this edition of Hot Topics and put it in your CD drive. If you are running windows, the CD should auto load the first panel. If it doesn’t load, start your browser and choose file, open d:/index.html where d: is your CD drive.

Navigating zFavorites

The left-hand navigation bar lets you jump from subject to subject. There are tabs for zSeries products, service, documentation, support, education, solutions. There are also tabs to link you to areas of zSeries special interest information such as Installation/Migration, Java, Linux, WebSphere, Parallel Sysplex and Redbooks.

Using the Product Documentation tab

- The first link in takes you to the Library Site for z/OS.
- The second link lets you go to the library home page for that release of z/OS.
- If you are looking for product documentation on z/OS, the “Links to Books” will take you to the Information Roadmap that provides direct links to all the books in that release.
- If you are in a hurry, the search text will take you to a search dialog that lets you search all the information for that release of z/OS.



- The LookAt Messages link will take you to the LookAt site where you can enter a z/OS message and it will open directly to the message explanation.
- The Redbooks link at the top of the CD for a listing of the Redbooks on this edition of zFavorites.

Free downloads

There several links to downloads for things like the Softcopy Reader, Softcopy Librarian, Acrobat Reader.

Redbooks

With every new release of zFavorites we package some of the more recent Redbooks for zSeries directly on the CD, so you can access and use them without an Internet connection. Just click on

We hope that zFavorites will be useful to you. If you have any comments, feel free to send them to gksmith@us.ibm.com. ■

Tech Jumble 1

Unscramble these four computer-related words, then arrange the circled letters to answer the jumble.

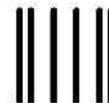
| | | | | | | |
|---------------|---|---|---|---|---|--|
| TRINP | | | | ○ | | |
| SDEAR | | | | ○ | | |
| WROBES | | | ○ | ○ | ○ | |
| RAWDIZ | ○ | ○ | | | | |

What the retired Assembler programmer said:
"I don't do _____."

Tech Jumble 2

| | | | | | | |
|---------------|---|---|--|---|---|--|
| CIBAS | ○ | ○ | | | | |
| RATTS | | ○ | | | | |
| TESSMY | | ○ | | ○ | | |
| ENCERS | | | | ○ | ○ | |

What the programmer did after work:
Got a _____ to _____.

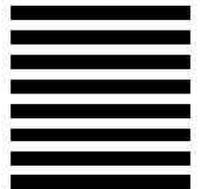


NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK
POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department H6MA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400



Tech Jumble 1 Answer

| | | | | | | |
|--------|---|---|---|---|---|---|
| TRINP | P | R | I | N | T | |
| SDEAR | R | E | A | D | S | |
| WROBES | B | R | O | W | S | E |
| RAWDIZ | W | I | Z | A | R | D |

What the retired Assembler programmer said:
"I don't do W I N D O W S."

Tech Jumble 2 Answer

| | | | | | | |
|--------|---|---|---|---|---|---|
| CIBAS | B | A | S | I | C | |
| RATTS | S | T | A | R | T | |
| TESSMY | S | Y | S | T | E | M |
| ENGERS | S | C | R | E | E | N |

What the programmer did after work:
Got a B Y T E to E A T.

To help us serve you better, please answer the following questions, and drop this card in you nearest mailbox.

1. Please indicate which editions of the Hot Topics Newsletter you have read.

Issue 4 (2/01) Issue 5 (8/01) Issue 6 (2/02) Issue 7 (8/02)

2. What is you overall satisfaction with the Newsletter?

Very satisfied Satisfied Neutral Dissatisfied Very dissatisfied

3. How do you prefer to access and read the Newsletter?
 Please choose one of the following:

Hardcopy Softcopy on CD or local repository
 Softcopy on the IBM Internet site or your intranet site
 All (depending on where I am and what I am doing)

4. How useful would it be when searching the entire product library to have the Hot Topics Newsletter included in the search?

Very useful Somewhat useful Neither Not very useful Not at all useful

5. The newsletter is published twice a year. How often would you like it to be published? Please choose one of the following:

Yearly Twice a year Three times a year Four times a year No opinion

6. How satisfied are you with the format and layout of the Newsletter (easy to navigate, pleasant to look at, etc.)?

Very satisfied Satisfied Neutral Dissatisfied Very dissatisfied

7. How satisfied are you with the writing style of the Newsletter (enjoyable to read, keeps your interest)?

Very satisfied Satisfied Neutral Dissatisfied Very dissatisfied

8. How do you obtain hardcopy issues of the Newsletter?

With the product At SHARE At other conferences
 Purchase separately Other (specify) _____

9. What topics would you like to read about in the next issue?

Name _____

Company _____

Job Description _____

Phone _____

e-mail _____

May we contact you? Yes No

Thank you for you comments!

© Copyright International Business Machines Corporation
 2002 All rights reserved.



zFavorites CD-ROM

To use the CD: Insert it in any standard CD-ROM and it should start automatically.

If it does not, then click on the **Start** button, choose **Run...** and then type **x:\index.htm** (where x is your CD-ROM drive letter) and press **Enter**.

Linux on the mainframe: An animated seminar

BY ALLAN EDMANDS

Featured on the zFavorites CD-ROM is a seminar animation exploring the concepts behind Linux for zSeries. Learn the advantages of running the Web-optimized, cost-effective Linux operating system on your zSeries mainframe. Discover how you can rapidly develop and port your Web applications from your desktop to the mainframe, and explore the possibilities for server consolidation. Learn how fast communication can be between your Linux LPAR and the DB2 database server in your z/OS LPAR.

These concepts and many more are graphically illustrated in the seminar, which you can peruse even off-line on the zFavorites CD-ROM. Find the seminar at Popular Subjects → Linux → Seminar, where you can choose the animation or a printer-friendly PDF. (For the latest version, you can check the Web at <http://www.ibm.com/servers/eserver/zseries/os/linux> and click the "Linux seminar" link featured on that page.)

Hey!

It's the zFavorites for zSeries credit card CD! You're gonna love this. It has all sorts of helpful Web links, like for:

Hardcopy

Operating systems

Software

Language and tools

ISV development and applications

Product documentation

Marketing information

Education

Support

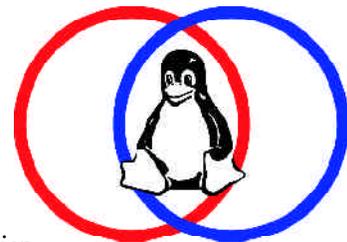
Links to FREE downloads

**Hot Topics Directory

Plus, it contains PDF versions of the z/OS and OS/390 Information Roadmaps and a preview of the Web sites linked to and from the CD.

Also, don't forget -- it has all existing issues of the Hot Topics Newsletter (including THIS issue) right on it for you to take anywhere!!

Additional copies of zFavorites CD-ROM (GK3T-4331-01), are now separately orderable.



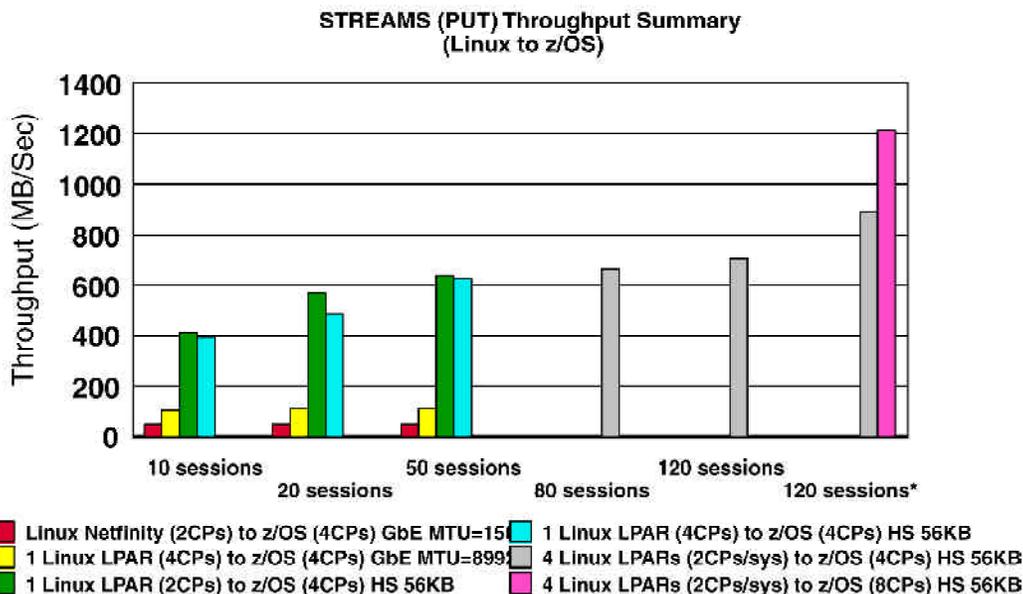


FIGURE 4

a Netfinity was connected via Gigabit Ethernet, and the Linux LPAR was connected via HiperSockets. *See figure 4. above.*

These Streams results were even more impressive than the interactive test results:

- Consolidated Linux LPAR had over three to five times more throughput than an external Gigabit connected Linux server.
- Comparing 120 sessions vs. 120 sessions* (gray bars), throughput increased 27.3% by increasing Linux LPAR's TCP Socket Send/Receive buffers from 64 KB to 128 KB. At this point z/OS's CPU utilization (99.5%) was limiting throughput, so we added four CPUs to the z/OS LPAR and increased throughput to 1.212 Gigabytes per second.
- In a separate z/OS LPAR to z/OS LPAR test, HiperSockets (maximum 805 MB/sec) was 6.2 to 6.8 times the throughput of OSA-Express GbE (maximum 118 MB/sec).

HiperSockets Accelerator performance (interactive transactions): To demonstrate the cost and performance benefits of z/OS HiperSockets Accelerator (HSA) technology, we ran Linux on a Netfinity system (two Pentium® III 866 MHz dedicated CPUs) connecting over Gigabit Ethernet

LAN to one of three TCP/IP routing stacks:

- z/OS HiperSockets Accelerator (4 CPUs in LPAR)
- z/OS TCP/IP LPAR (4 CPUs in LPAR)
- Linux TCP/IP LPAR (4 CPUs in LPAR)

The RR (200 bytes out, 1000 bytes in) throughput was very similar across all cases (varied by 5%) with maximum throughput at 13,543 transactions/sec.

- z/OS HiperSockets Accelerator (router) vs. z/OS TCP/IP (router) : increase (+3.7%)
- z/OS HiperSockets Accelerator (router) vs. no router: increase (+0.4%)
- z/OS HiperSockets Accelerator (router) vs. Linux TCP/IP (router): decrease (-1.2%)

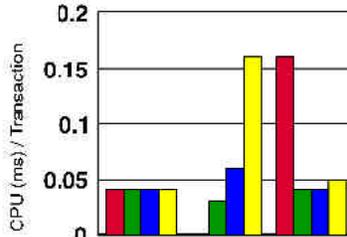
The real story is the cost per transaction decrease with HiperSockets Accelerator. *See figure 5 on the next page.*

These results show:

- Client CPU utilization was very similar in all cases. Server CPU utilization was very similar except for the base case when there was no intermediate router. This might be explained by packet blocking occurring in the router case, but not in the non-router case, thus more reads and writes had to be done in the non-router case.
- z/OS HiperSockets Accelerator (router) vs. Linux TCP/IP (router) : less cost (-81%)
- z/OS HiperSockets Accelerator (router) vs. z/OS TCP/IP (router) : less cost (-50%) ▶

(continued on next page)

RR CPU/Transaction



| | "Client LPAR" | "Routing LPAR" | "Server LPAR" |
|---|---------------|----------------|---------------|
| Linux Netfinity (GbE 1500) to Linux LPAR | 0.04 | 0 | 0.16 |
| Linux Netfinity (GbE 1500) to HS Accelerator, HS 56K to Linux LPAR | 0.04 | 0.03 | 0.04 |
| Linux Netfinity (GbE 1500) to z/OS TCP/IP LPAR, HS 56K to Linux LPAR | 0.04 | 0.06 | 0.04 |
| Linux Netfinity (GbE 1500) to Linux TCP/IP LPAR, HS 56K to Linux LPAR | 0.04 | 0.16 | 0.04 |

■ Linux Netfinity (GbE 1500) to Linux LPAR
■ Linux Netfinity (GbE 1500) to HS Accelerator, HS 56K to Linux LPAR
■ Linux Netfinity (GbE 1500) to z/OS TCP/IP LPAR, HS 56K to Linux LPAR
■ Linux Netfinity (GbE 1500) to Linux TCP/IP LPAR, HS 56K to Linux LPAR

FIGURE 5

HiperSockets Accelerator performance (bulk data transfer): For the HiperSockets Accelerator Streams PUT case, throughput was again very similar across all cases (varied by 1%) with a maximum throughput of 48.1 MB/sec.

- z/OS HSA (router) vs. z/OS TCP/IP (router) : less throughput (-0.8%)
- z/OS HSA (router) vs. no router: less throughput (-0.4%)
- z/OS HSA (router) vs. Linux TCP/IP (router) : more throughput (+0.2%)

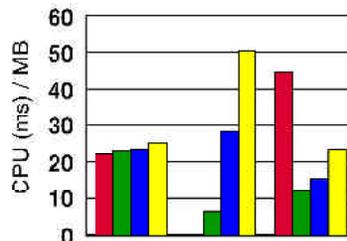
Again, the real story is the cost per MB decrease using HiperSockets Accelerator.

The “routing LPAR” depicts the routing technology comparison.

These results showed:

- HiperSockets Accelerator (router) vs. z/OS TCP/IP (router) : less cost (-77%)
- HiperSockets Accelerator (router) vs. Linux TCP/IP (router): less cost (-87%)
- Customers planning to use both Linux and z/OS on the same zSeries should consider HiperSockets Accelerator if a routing LPAR is required.

Streams (PUT) CPU/MB



| | "Client LPAR" | "Routing LPAR" | "Server LPAR" |
|---|---------------|----------------|---------------|
| Lin'Netfinity (GbE 1500) to Linux LPAR | 22.99 | 0 | 44.88 |
| Lin'Netfinity (GbE 1500) to HS Accelerator, HS 56K to Linux LPAR | 22.99 | 6.47 | 12.04 |
| Lin'Netfinity (GbE 1500) to z/OS TCP/IP LPAR, HS 56K to Linux LPAR | 23.21 | 28.28 | 15.5 |
| Lin'Netfinity (GbE 1500) to Linux TCP/IP LPAR, HS 56K to Linux LPAR | 25.14 | 50.28 | 23.2 |

■ Lin'Netfinity (GbE 1500) to Linux LPAR
■ Lin'Netfinity (GbE 1500) to HS Accelerator, HS 56K to Linux LPAR
■ Lin'Netfinity (GbE 1500) to z/OS TCP/IP LPAR, HS 56K to Linux LPAR
■ Lin'Netfinity (GbE 1500) to Linux TCP/IP LPAR, HS 56K to Linux LPAR

FIGURE 6

Summary and references

This article has just scratched the surface of HiperSockets. HiperSockets provides high-speed and low-latency TCP/IP connectivity between partitions (LPARs) and virtual servers on a zSeries. The z/OS HiperSockets Accelerator leverages the intersection of internal HiperSockets and the QDIO OSA-Express connection to the external IP network. We provided real performance information to give you a glimpse of the technology’s raw performance—but obviously, performance in an application environment depends on the middleware and application, so your actual mileage will vary.

If we have succeeded in whetting your appetite, you will want to know more about environments that would benefit from HiperSockets, as well as how to set up and use HiperSockets.

For specific operating system support, consult the publications for that operating system (for example, *z/OS V1R2.0-V1R3.0 Communications Server IP Configuration Reference*).

For general positioning and how-to information, however, two excellent references are:

- *zSeries HiperSockets, SG28-6816-00*, published May 19, 2002
- *zSeries 900 HiperSockets, The ultimate in server network consolidation*, a white paper available at: <http://www.ibm.com/servers/eserver/zseries/networking/pdf/hiperguide.pdf>.

IPv6 Here we come!

z/OS Communication Server introduces IPv6

BY LORI NAPOLI



You have to think back only a few years to remember times when PCs weren't sitting on everyone's desks or in everyone's home; times when cell phones, Web-enabled television receivers and PDAs were not even available. Times have definitely changed. The new surge for IP addresses by these new technology devices and by areas of the world that were sluggish in requesting IP addresses, like Asia and Eastern Europe, is pushing the limits of what the existing Internet Protocol, IPv4, can support. This large demand for IP addresses is one of the major factors influencing the industry to start its transformation to the next the generation Internet Protocol, IPv6.

IPv6 addressing scheme

The existing IPv4 addressing scheme, with 32-bit addresses, provides for over 4 billion possible addresses, however only a subset of these addresses can actually be assigned, since addresses are assigned in network blocks instead of individual addresses. This address space will eventually be exhausted, which is projected to happen between 2005-2011. The

Internet Engineering Task Force (IETF) started a working group originally called IPNG, IP Next Generation, to research and provide standards for what eventually became known as IPv6. This work started in the early 1990's and is still evolving. Some major enhancements for IPv6 are expanded addressing, built-in security and Quality of Service (QoS), and Plug 'n Play and support for mobile clients.

IPv6 is not backwards compatible with IPv4 but compatibility methods to coexist and communicate with IPv4, along with transition methods to migrate from IPv4, are part of the IETF standards. These will be key elements of the transformation to IPv6 in the industry, since it is projected that both IPv4 and IPv6 protocols will coexist for many years. Some estimates project that by 2005 half the nodes on the Internet will be IPv6 nodes. Both the European Union and the Japanese government aim at widespread use of IPv6 by 2005.

The IPv6 addressing scheme expands the IP address from 32-bits to 128-bits. Whereas IPv4 protocol provides for over 4 billion possible addresses, the IPv6 protocol provides for *340,282,366,920,938,463,463,374,607,431,768,211,456* addresses. IPv4 addresses were represented in dotted-decimal format, *a.b.c.d*. IPv6 addresses are represented in colon-hexadecimal format, *aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh*. If an IPv6 address contains consecutive fields of zero, they can be compressed by using "::". This shorthand can occur only once in an IPv6 address: at the beginning,

in the middle or at the end.

For example, the IPv6 address `FEC0:0000:0000:0000:0206:2AFF:FE71:4400` can be written in shorthand as `FEC0::0206:2AFF:FE71:4400`. Leading zeroes within a field can also be omitted, so we can further simplify this address to `FEC0::206:2AFF:FE71:4400`.

IPv6 addresses are not divided in classes (A, B, C, D, E) like IPv4 addresses. Instead the high order bits of an IPv6 address determine what type of address it is.

Address type Binary prefix IPv6 notation

Unspecified 00...0 (128 bits) ::/128
 Loopback 00...1 (128 bits) ::1/128
 Multicast 11111111 FF00::/8
 Link-local unicast 11111110 10 FE80::/10
 Site-local unicast 11111110 11 FEC0::/10

Global unicast (everything else)

- A link-local unicast address is an address that is only valid on a single link. Routers must not forward any packets with link-local source or destination addresses to other links.
- A site-local unicast address is an address that is only valid within a particular site. The method of assigning sites is left up to each implementation.
- A global unicast address is an address that can be used throughout all the IPv6 networks.
- Multicast addresses for IPv6 provide similar functionality as multicast addresses for IPv4. The only difference is that IPv6 multicast addresses also have scopes that limit

(continued on next page)

- how far packets destined for these addresses can be routed.
- The Unspecified IPv6 address provides the similar function as the INADDR_ANY IPv4 address (0.0.0.0). If a server application has one socket bound to the unspecified IPv6 address, it is functionally equivalent to an application that opened a separate socket for each IPv4 and IPv6 address owned by the TCP/IP protocol stack (the stack), and bound each socket to one of these addresses. Therefore, one IPv6 socket, bound to the unspecified address, can receive connection requests for IPv4 and IPv6 addresses.

IPv6 addresses can be manually configured or autoconfigured. Autoconfigured addresses are created by learning the high order 64-bits from a router on the link and appending the 64-bit interface ID as the low order 64-bits. Since the interface ID can change when a stack is recycled, autoconfigured addresses cannot be easily maintained in DNS since the address changes if the interface ID changes. Virtual IP Address (VIPA) interfaces do not support autoconfiguration and must have manually configured addresses.

IPv6 addresses have states associated with them that enable site renumbering and duplicate address detection. The states are preferred, deprecated and tentative. When an IPv6 interface is activated, the addresses are in tentative state. When an address is in this state, it is not considered to be a valid IP address on the stack. During this time the address uniqueness is being validated on the link. Once the address is determined to be unique, the address state changes to preferred state. When an address is in preferred state, the address can be used for inbound and outbound communication. If a

site needs to change IP addresses, the IPv6 protocol technology architects a nondisruptive method to accomplish network renumbering activities, making it easier to manage than in the IPv4 world. The current addresses switch states to deprecated state at the same time the new addresses are added and go from tentative to preferred state. When an address is in deprecated state, it can still be used for inbound and outbound communication. The difference is that for new outbound communication this address will not be selected unless there is no alternative address to use. This enables existing connections to remain active using the original IPv6 addresses, but new connections will use the new address. This is a controlled way to transition between addresses.

Dual-mode stack support

As was mentioned earlier, compatibility and coexistence between IPv6 and IPv4 are critical. IPv6 applications not only can fully communicate with IPv6 nodes, but they can also communicate with existing IPv4 nodes. Dual-mode stack support is what enables IPv6 applications to communicate with both IPv4 and IPv6 nodes. A dual-mode stack is one stack that supports both IPv4 and IPv6 protocols, like z/OS Communication Server. One physical network can be used for both IPv4 and IPv6 protocols. Since IPv6 applications understand only 128-bit addresses, and an IPv4 node is represented by a 32-bit address, there is the need to be able to represent the IPv4 32-bit address in the form of an IPv6 address. A special IPv6 unicast address type called IPv4-mapped IPv6 address is used to represent an IPv4 address in IPv6 format.

This address has the following format:

```
80 bits 16 bits 32 bits
0000.....0000 FFFF IPv4 address
```

When an IPv6 application communicates with an IPv4 partner, the resolver and the TCP/IP protocol stack handle the translation of the 32-bit IPv4 address to the 128-bit IPv4-mapped IPv6 address. This is transparent to the application.

An IPv6 application communicating with an IPv4 partner is functionally equivalent to an IPv4 application communicating with an IPv4 partner. Given this, the transformation to IPv6 can easily begin with converting applications to the IPv6 API. Even if you are not ready to start using real IPv6 traffic in your network, you can enable your applications and not lose any functionality.

IPv4 server applications on dual-mode stacks

If you have server applications that are running on a dual-mode stack that are not yet enabled for IPv6, there are a few things to consider. If an IPv6 client application running a dual-mode stack wishes to connect to an IPv4 server running on a dual-mode stack, the address at the top of the list returned by Resolver will be the IPv6 address of the server stack, since both client and server support IPv6, and that is the preferred choice. Since this specific application is not IPv6 enabled, the client will not be able to connect to the server using the IPv6 address. To solve this, it is recommended that if you have a mix of IPv4 and IPv6 server applications on one dual-mode stack, you should create two distinct host names to store in DNS or use a similar technique to ensure unique host names in DNS. If the IPv6 client application

happens to be on an IPv6-only stack and it wishes to communicate with an IPv4 server on a dual-mode stack, the dual-mode stack cannot translate the addresses. The client is represented by only a 128-bit IPv6 address since it is running on an IPv6-only stack. Even though the stack on which the server application is running understands IPv6 addresses, the application does not, since it was not enabled for IPv6. There is no method for taking the 128-bit address representing the client and condensing it into a unique 32-bit address. The IETF has many proposed ways to address this, and one is using an Application Layer Gateway (ALG) like a SOCKS64 server. This socks server will act like a traditional socks server and, in this case, will be a gateway between IPv4 and IPv6. The client will connect to the SOCKS64 server using IPv6 addresses, and the SOCKS64 server will initiate a connection to the IPv4 server using IPv4 addresses. If you have an environment that requires IPv6-only clients to connect to IPv4 server applications, you will need to deploy this or a similar technique in your network.

Connecting IPv6 clouds across the Internet

Everyone will transition to IPv6 at different times. e already talked about how IPv4 and IPv6 applications can coexist, but we didn't mention how IPv4 and IPv6 networks coexist. If an IPv6 packet needs to be routed across an IPv4 network enroute to the IPv6 destination, it is "tunneled." Tunneling is the encapsulation of an IPv6 packet within an IPv4 packet. The encapsulated IPv6 packet is then sent to the other end of the tunnel via the IPv4 protocol. he tunnel endpoint removes the IPv4 header and sends the original IPv6 packet to the intended

destination. The time the packet travels through the tunnel is viewed as one hop to the IPv6 packet. Tunneling does not have to initiate/terminate at the connection endpoints; a router enroute to the final destination can tunnel the packet. f you need to connect two or more IPv6 networks through an IPv4 network, you will need to deploy one of the tunneling techniques.

Summary

IPv6 will become a reality in the near future. Many products are starting to announce IPv6 support in their products. Although many American companies have sufficient IPv4 addresses since they requested them early, other geographies will be moving to IPv6 more rapidly. In order to continue Business-to-Business communication with these areas, American companies will also have to support IPv6. The migration to IPv6 cannot be done overnight, so it is important to get started on this transition. The IPv6 support provided in the z/OS V1R4 release enables customers to build an IPv6 network, start using IPv6 specific applications and, more importantly, convert existing IPv4 applications to the IPv6 API without losing any functionality. If you are an application developer, take advantage of the IPv6 support available in z/OS V1R4 to start updating your applications for IPv6. The same source code can be used for IPv6-enabled stacks and traditional IPv4-only stacks. If the AF_INET6 (IPv6) socket cannot be created, the application can simply resort back to opening an AF_INET (IPv4) socket. To understand the details of what IPv6 support is provided in z/OS Communication Server V1R4, refer to:
z/OS Communication Server: IPv6 Network and Application Design Guide. ■

IPv6: Better and more

BY LESIA COX

Start dipping those IPv4 toes into the IPv6 pond...

Now that you have read a little about IPv6, we want to introduce you to a book that can assist in the transition to IPv6.

The *IPv6 Network and Application Design Guide* is available with z/OS CS V1R4. This book contains sections that are of specific interest to programmers and system administrators, and another section that is intended for application programmers. The first sections provide an overview of the z/OS Communications Server implementation of the IPv6 protocol and recommendations and guidance information for using new IPv6 function. The information will assist in understanding the major factors involved in planning the setup of an IPv6 network and provide recommendations for transforming your existing network. Later sections of the book discuss common issues and considerations for enabling applications for IPv6 and include examples of some of the approaches that may be taken.

Several customers provided positive feedback during the development of this book. Make the *IPv6 Network and Application Design Guide* part of your plan to swim with the big fish in the IPv6 pond. ■

IPv6 Resolver support

BY BARBARA NEUMANN

Internet Protocol Version 6 (IPv6) is the base technology of the next generation Internet. The z/OS V1R4 Language Environment® C/C++ Run-Time Library provides much of the basic, and some of the advanced, Application Programming Interfaces (APIs) in support of IPv6. z/OS UNIX support is also provided. For more information, see *z/OS UNIX System Services Planning*. ■

Linda Distel

(continued from page 5)

What is IBM doing to keep z/OS and the other eServer operating systems from being hacked?

Security starts with the customer's in-house security practices. If customers ignore recommended security practices, they risk the possibility of security exposures. When we do assessments of customers' security, for example, we sometimes find that they have not changed the default user IDs for a system.

Also, we work with IBM Research to try to ethically hack z/OS. We've been doing it since OS/390 Release 4. I've been working with pSeries and iSeries™ so that they take the same tests.

That doesn't mean we're perfect, but it follows from the long-standing security and integrity statement we've had for z/OS, OS/400, and VM. That is, if you find a security or integrity problem, we'll take an APAR. That policy was pretty much unheard of when we established it 15 years ago.

How is I/T security different today?

IBM has a long heritage in security. Years ago, we thought of security in terms of isolation. Things like access control, authentication, and LPAR isolation for a single system. The reason was that our customers, banks and governments especially, were building applications that needed all that isolation.

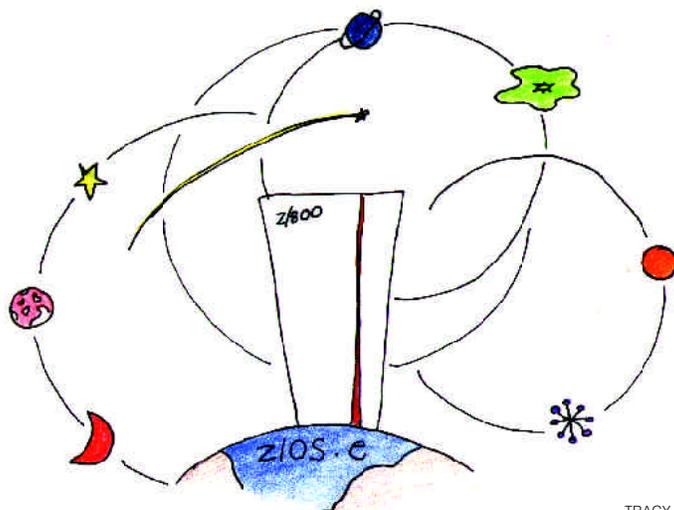
As we get into e-business, our customers are also concerned about threats to distributed applications, such as transactions over the Web. Intrusion detection is another area of concern. Even if I don't damage your system, what if I were able to tie up your system with so much traffic, you can't do real work?

People want to know that our systems are safe. We will continue to spend time on certifications, ethical hacking, and providing common security functions across platforms.

With the new threats to distributed applications, we now plan to focus on enabling highly secure transactions across platforms, rather than just building up walls around stuff. More than ever, I/T security is a balancing act between isolation and enablement. ■

z/OS.e: An operating system for new workloads

BY DICK WAGENAAR



TRACY BONDI

z/OS.e V1R3 is a specially-priced offering of z/OS V1R3 that provides select z/OS function. z/OS.e is available on only the IBM eServer zSeries (z800) or a comparable non-IBM server. z/OS.e V1R3 is intended to help customers exploit the fast growing world of next generation e-business by making the deployment of new applications on the z800 very attractively priced.

z/OS.e V1R3 uses the same code base as z/OS V1R3, customized with new system parameters, and invokes an operating environment that is comparable to z/OS in qualities of service, management, and reporting. In addition, z/OS.e invokes zSeries hardware functionality just as z/OS does—technology that allows the platform to adapt to your business priorities. No new z/OS skills and service structure are required for z/OS.e.

z/OS.e V1R3 is specifically for Java, Enterprise Java (J2EE), C/C++, and Web-based data transaction processing applications for new workload environments—

giving these workloads a price performance customers expect. This product will not support certain workloads described later.

At only a fraction of the cost of z/OS V1R3 in a traditional workload environment, z/OS.e makes the decision to run new workloads on the mainframe easy due to its reduced total cost of ownership and exceptional robustness and functionality. z/OS.e and z800 together may reduce the total cost of ownership of hardware, software, people, and environments—making the combination very cost-effective for deploying new applications or integrating existing ones.

New kinds of workloads

The Internet age has spawned totally new kinds of computer workloads. That's because more and more of the world's data transaction processing is Web-based. A business that does not participate in e-business risks losing business. Web-based processing is now

perceived, correctly, as a major contributing factor to achieving a competitive and successful business. This is true whether the business is a small, medium-sized, or large enterprise. Furthermore, for many, the entire length of the value chain from procurement to fulfillment is assisted by Web-use, involving suppliers at the beginning and satisfying customers at the end. Workloads such as supply chain management (SCM), enterprise resource planning (ERP), customer relationship management (CRM), and business intelligence (BI) all increasingly depend on Web-use. These workloads not only benefit from tight integration to Web-based data transaction processing, but also benefit from tight integration between each other and the back-end data.

The best platform

The best platform for integrating Web-based transaction processing, e-business, and enterprise applications and database serving is z/OS on zSeries, the premier platform for enterprise-scale workloads. Its qualities of service in terms of reliability, scalability, security, and availability are undisputed and unrivaled in the industry. The value is twofold, for z/OS is not only the most robust and reliable enterprise platform, it also has a history of managing a large percentage of the world's business data and transactions. The finance industry, the transportation industry, health, government—all rely on z/OS to store, manage, and use their data efficiently and securely. Offering the same value as this technology, IBM introduces z/OS.e. ▶

(continued on next page)

A total platform solution

IBM introduces z/OS.e as a cost-effective way to harness the power, value, and qualities of service of z/OS on zSeries for (and to extend it to) new applications—for example, to drive your business into the Web space with an application server such as WebSphere Application Server and access your DB2 data. z/OS.e opens up the possibility for that data to be available for all kinds of new Web applications. This data is a huge, still largely untapped resource for all kinds of new and exciting Web applications. The potential is tremendous.

Please note that z/OS.e is only available on the z800 processor. The new z800 processor puts the adoption of advanced zSeries mainframe technologies within reach for a wider audience. Those who always wanted to install more mainframe technological capabilities and capacity, but thought it was out of reach, too complex, or overkill for their situation, will find that the z800 machine can help make the transition easier.

Target customers

Available only on z800, z/OS.e is for those customers who require the qualities of service that the mainframe has to offer for their new workloads and growth applications. z/OS.e provides the robustness of z/OS with a price that makes adoption of new workloads and applications easier and more affordable. Traditional strengths of the zSeries platform are upheld. Sophistication such as Intelligent Resource Director, which allows customers to handle unexpected e-business workload spikes by dynamically moving resources to their defined and most important work, is maintained.

The z/OS.e alternative may be very attractive to you if you own a G4/G5/G6, a Multiprise® 3000, or a large Multiprise 2000 processor, and:

- Have existing new workload like ERP, CRM, SCM, BI, Web-based data transaction processing and other such applications written exclusively in C/C++ and Java and are considering re-hosting on the mainframe.
- Do not have these new workloads running yet on any platform, but plan to do so in the future.
- Are considering the purchase of a z/800 processor, and have z/OS, OS/390, or MVS™ skills in house (or plan to outsource these skills).

z/OS.e is for next-generation workloads

z/OS.e is for new next-generation enterprise, e-business and Web-based data transaction processing applications. Specifically, z/OS.e is for applications written in the object-oriented programming languages of Java, Enterprise Java (J2EE), and C/C++, giving these workloads excellent price performance.

This product will not support certain traditional workloads. It supports new workloads. They include:

- WebSphere Application Server, IBM Developer Kit for the Java Platform (includes J2EE), DB2 V7, V6, V5, C/C++
- WebSphere Commerce (WC), DB2 database serving, Domino™, and financial applications.

z/OS.e also supports MQSeries, MQSeries® Integrator, Host on Demand, VisualAge® Java, WebSphere Studio, and many more e-business related IBM and

Independent Software Vendor (ISV) applications, middleware, and tools. z/OS.e is manageable by many traditional independent software utility software vendor system management toolsets. In short, z/OS.e is an ideal way to enter, exploit, and profit from the world of next-generation applications.

z/OS.e is not for traditional workloads

Customers who choose z/OS.e are not licensed for the traditional workloads. z/OS.e disables traditional workloads. z/OS.e will not execute CICS®, IMS™, COBOL, or FORTRAN applications. However, precompiled COBOL stored procedures and other precompiled COBOL applications using the Language Environment preinitialization interface CEEPIPI are supported. You cannot use the compilers COBOL, PL/I, VisualAge PL/I, or FORTRAN. However, z/OS.e supports execution of precompiled PL/I and VisualAge PL/I applications. Also not licensed and not functional are selected z/OS base elements and optional features, as well as certain selected functions within those elements and features that support traditional workloads. In addition, selective applications and certain DB2 features will not be available to you when using z/OS.e. This includes QMF™ (host and HPO).

Not functional and not licensed elements, features, and functions include:

- BookManager® READ/BUILD
If you want to upload BookManager softcopy and create softcopy repositories to support BookManager BookServer on your z/OS.e host, the Softcopy Librarian is the strategic tool for uploading and managing BookManager files on z/OS and z/OS.e and on LANs and workstations.

- GDDM®
 - GDDM PGF feature
 - GDDM REXX feature
- DCE Application Support
- LANRES
- BDT File to File
- Language Environment cannot use:
 - Run-time Library Services
 - Library Routine Retention

Also not licensed in the z/OS.e environment are:

- Encina® Toolkit Executive
- MICR/OCR
- Language Environment Compatibility Preinitialization for C and PL/I

Not orderable is:

- Communications Server Network Print Facility (NPF) optional feature

Please note, non-IBM ISV and custom-written applications, which use the base elements, features, products, and are written in these programming languages above, may not be supported. Consult your ISV for more details.

For minimum releases of IBM software products that run with z/OS and z/OS.e, see Appendix C in *z/OS and z/OS.e Planning for Installation*.

For more information about z/OS.e, see *z/OS.e Overview (GA22-7869)*, and the related articles in this issue of *Hot Topics*. ■

“WAS” up? z/OS.e SystemPac is!

BY JUDY WASHO



You have probably all heard about z/OS.e by now and most certainly you know about WAS. WAS? Oh, that's WebSphere Application Server 4.0.1 for zSeries. It's the e-business application deployment environment built on open standards-based technology. It provides Web application development and production environments implementing the most advanced open systems architecture, such as, J2EE and CORBA specifications under the very powerful z/OS.e system.

In case you didn't know about z/OS.e, it's a specially priced offering of z/OS providing select function at an attractive price. z/OS.e is designed to help you exploit the fast growing world of next-generation e-business by making the deployment of new application workloads on the IBM eServer zSeries 800 (z800) server competitively priced. z/OS.e shares the same code base as z/OS. In other words, you get the full value of the z/OS qualities of service for

these new workloads on the midrange z800 server at a good price.

As a systems programmer, you know that migrating, installing, and maintaining your operating system-related products and independent software vendor products can be time consuming and resource-intensive. Not only that, but these tasks can sidetrack you from the critical business-related responsibilities you're supposed to be doing. This is where SystemPac® helps.

So now you might ask, "What's SystemPac?" This is my favorite topic. No, I did not spell it wrong. It's not ServerPac. It's SystemPac and it is built upon ServerPac. So, everything that ServerPac has, SystemPac has too. So what's the difference?

SystemPac is a worldwide system migration vehicle for z/OS.e and ▶

(continued on next page)

is the recommended IBM delivery vehicle for customers who want to save time, resources, and effort to migrate, install, exploit, and maintain their z/OS.e system related products, and selected independent software vendor products. SystemPac comes customized according to users' specified parameters with guidance from IBM services specialists. It is designed to exploit new technologies and comes with a lot of enablements which are required to build an e-business Application Server environment. With SystemPac, you can have a functional z/OS.e system, restored and IPLed within less than a day and independent software vendor products installed too.

Did I tell you that SystemPac is available in a "full volume dump format"? Well it is. This certainly reduces your time and effort for installation. You don't have to learn and use the installation dialog to perform the installation. Sound good? You bet! We even provide Dump by Dataset for those systems programmers that like to use the installation dialogs.

You can also select from a wide range of independent software vendor products to be installed on your SystemPac, including choices from BMC Software, Inc., Candle Corporation, Computer Associates International, Inc., Levi, Ray & Shoup Inc., and Allen Systems Group, Inc. Where else would you find that?

SystemPac provides a load and go system for z/OS.e and Websphere Application Server 4.0.1 for zSeries, providing a fully functional system on IPL in less than a day.

Customers ordering a z/OS.e SystemPac can take advantage of the default enablement of the MVS System Logger, Resources Recovery Services, and WorkLoad Manager

Goal Mode, including a sample policy.

Additionally, SystemPac comes with the option of having the z/OS.e Communications Server enabled. This feature, coupled with the enablement of z/OS.e UNIX System Services in full function mode, allows the customer to easily tailor the default setup provided to match their standard for Internet access after the system is restored and IPLed.

SystemPac is further enhanced with the setup, customization, and enablement of the following products, in a single package, when they are ordered:

- DB2 Universal Database™ Server for z/OS and OS/390 6.1.0 and 7.1.0
- DB2 ODBC
- DB2 JDBC
- DB2 Net.Data®
- WLM-established Stored Procedures
- MQSeries 5.2.0 for z/OS and OS/390
- Websphere Application Server 4.0.1 for zSeries, including its following required prerequisites:
 - z/OS UNIX System Services
 - OS/390 or z/OS System Logger
 - Resource Recovery Services
 - RACF
 - JAVA for OS/390 1.3.0
 - WorkLoad Manager Goal Mode
 - TCP/IP
 - HTTP Server
 - DB2 V7.1.0

All of the necessary customization for application enablement is performed during the SystemPac build process and most of the post installation jobs are run, as well. Basically, you have an e-business enabled system, restored and IPLed within less than a day. And

with very minimal effort, you should be able to further tailor your e-business Application Server environment.

One more thing—Selected products which are withdrawn from marketing, but are still available for services, can be ordered in a SystemPac. This enables you to recover a back-level system should a disaster occur or to enable a gradual migration of products.

And here's something else. SystemPacs include selective follow-on services (SFS) packages to help you stabilize the system, products, services or functions that you have installed over a period of time. SFS packages are ordered at the same time as the initial SystemPac and contain critical service information, which is applicable to a package order that has become available since the SystemPac or previous SFS package was built.

For this article, I just wanted to focus on z/OS.e, but everything in this article also applies to SystemPac with z/OS and OS/390, and in addition to the above, also includes the enabling and starting of CICS, IMS, and NCP, if ordered, in a single package.

So "WAS" up? With Full Volume Dump and the above enablements, you can now have a true load and go system for z/OS.e and the Websphere Application Server ready on IPL. This unique capability is only available with SystemPac.

I just hit on the highlights of what SystemPac can do for you. I hope that I peaked your interest and showed you how SystemPac can make your job easier. To find out even more information on SystemPac, visit: <http://www.ibm.com/ca/custompac>. ■

And you don't need a new library

BY FLORENCE KRUPA



NATASHA FRAY

Most of the documentation for z/OS.e is the same as the documentation for z/OS. Because z/OS.e and z/OS contain the same code base and have most of the same function, you can use z/OS books to manage and use z/OS.e. You don't need to learn a new library structure. Books that apply to z/OS elements and features not licensed or not functional in a z/OS.e environment do not apply to z/OS.e.

The z/OS books that support z/OS.e and several z/OS.e-specific books are available on the z/OS.e Internet Library Web site at <http://www.ibm.com/servers/eserver/zseries/zose/bkserv/>. Also available from this Web site, and updated to support z/OS.e, are the z/OS wizards and LookAt, a popular function that provides integrated online help for messages.

To help you painlessly learn about z/OS.e, we've developed a z/OS.e multimedia overview. See the article "Journey through space and time with z/OS.e" for the details. Overview information also appears in a book, *z/OS.e Overview*, GA22-7869. In addition to the usual overview information, this book contains reference information. In one place, you will find messages, codes, and information

about z/OS functions that are restricted from use in z/OS.e. This is the type of information that usually appears in the element and feature libraries. The book is available in BookManager and PDF format on the z/OS.e Internet Web site and you can also purchase it from IBM in hardcopy format.

With your z/OS.e order, you automatically receive the following basic material at no additional charge:

- *z/OS V1R4 Collection*, SK3T-4269
This release-specific collection includes books for the z/OS Version 1 Release 4 elements and features in BookManager and PDF format.
- *z/OS and z/OS.e Planning for Installation*, GA22-7504
If you have used z/OS or OS/390®, you are already familiar with this book. It helps you prepare to install z/OS or z/OS.e by giving you information about writing an installation plan.
- *z/OS.e Memo to New Licensees*, GI10-0684
Contains the key code and instructions that enable you to access z/OS licensed books on the Resource Link™ Web site.
- *z/OS Program Directory*, GI10-0670
z/OS.e does not require a program directory because it is not installed using CBPDO. However, this document is provided with your order because it contains useful reference information.

With your order, you can also optionally purchase a single copy

of the *z/OS Software Products Collection*, SK3T-4270, at a price of \$50. This collection includes libraries for many software products that run on z/OS. Not all of the products that run on z/OS are capable of running on z/OS.e.

For the latest list of products that are orderable with z/OS.e and also run on z/OS.e, see the ServerPac Web site at <http://www.ibm.com/servers/eserver/zseries/software/swinfo/serverpa.htm>.

Products that are no longer orderable but are still in service do not appear in this checklist.

The licensed z/OS books that apply to z/OS.e are available for purchase in softcopy on the z/OS Licensed Product Library, LK3T-4307, in both BookManager and PDF format. Because this collection contains licensed information, you must have a license for either z/OS or z/OS.e to order it. The licensed books are not available in hardcopy format from IBM, but they are available for free, to licensed users, in PDF format on the IBM Resource Link™ Web site. In order to access the licensed books on the Internet, you need a special key code as well as a Resource Link user ID and password. Instructions for accessing licensed books are available at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/resource_link.html.

All related z/OS softcopy collections and hardcopy books are available for purchase using the usual purchasing methods or by accessing the IBM Publications Center Web site at <http://www.ibm.com/shop/publication/order/>. ■

Journey through space and time with z/OS.e

BY TRACY BONDI, PATTY CURRY, AND FLORENCE KRUPA

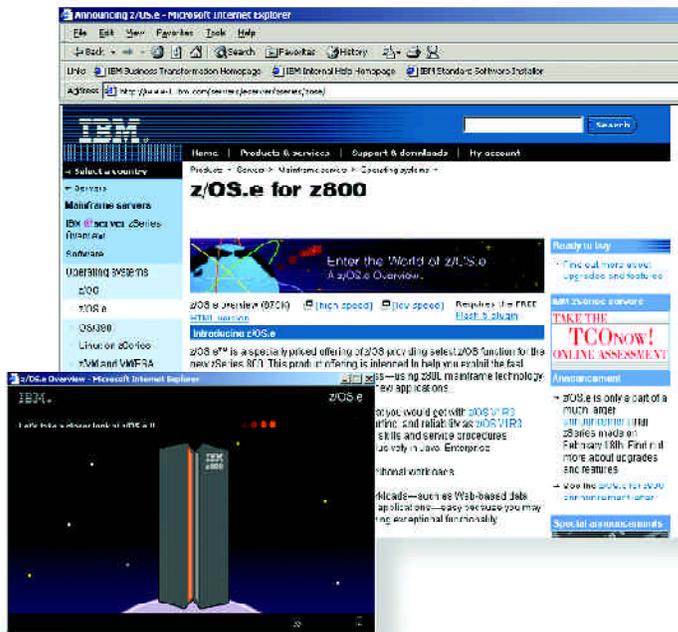
Do you want to take a dynamic journey through new information or sit and read it in a book?

Do you want to learn in a new way? If so, pack your bags and come with us on a trip through the z/OS.e multimedia overview to learn about z/OS.e. You'll find it on the z/OS.e Internet site at <http://www.ibm.com/servers/eserver/zseries/zose/>.

What makes this multimedia overview different from the usual IBM manual? It is designed to make learning fun. (Who would have thought you could learn and have fun at the same time?) What makes it fun? The space metaphor lightens the atmosphere allowing you to zero in on the information of your choice at your own speed. You are in control, in the driver's seat, so you can learn about the business value of z/OS.e at your own pace.

The overview starts with a brief introduction that sets the stage for a better understanding of how z/OS.e helps execute new workloads at a cost savings. It's followed by a graphical menu that allows you select any of the following choices:

1. Enterprise and e-business solutions
2. Economically priced
3. Environment comparable with z/OS
4. Enter the z/OS.e world
5. Expand your z/OS.e knowledge



Each of these sections goes into more detail about z/OS.e using charts, graphics and text. For example, option 4 contains a flowchart that shows the requirements for using z/OS.e at a glance. It also gives you the opportunity to select other related options:

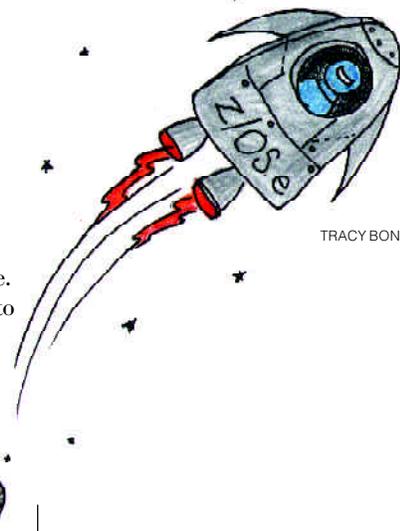
- What z/OS.e supports
- What z/OS.e doesn't support
- z/OS.e terms and conditions
- Ordering z/OS.e
- z/OS.e documentation



Take a look for yourself. You need the following to run this:

- A browser with an Internet connection
- The FREE Flash 5 plugin, which can be downloaded from the Web site.

Bon Voyage! ■

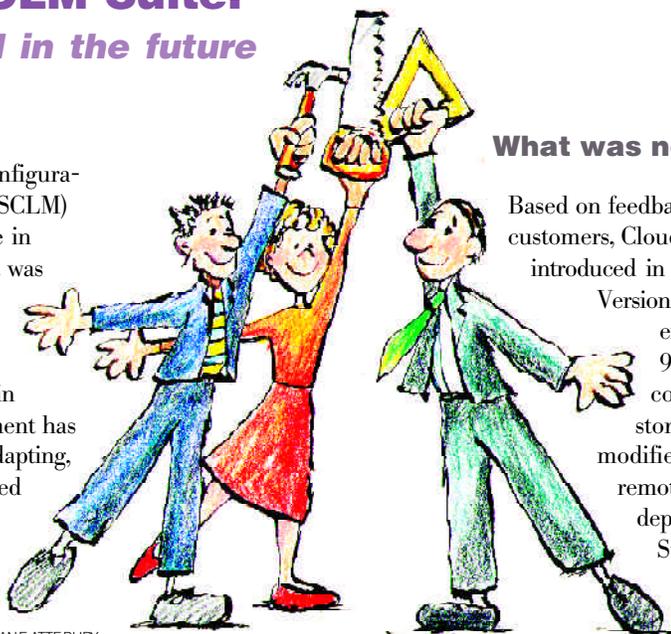


TRACY BONDI

IBM z/OS SCLM Suite: Then, now and in the future

BY MARSHA O'BRIEN

The IBM z/OS Software Configuration and Library Manager (SCLM) Suite first became available in November of 2000 (when it was called the IBM OS/390® SCLM Suite). IBM's low cost, high function solution for managing development in today's e-business environment has been evolving ever since—adapting, enhancing and adding related new products to meet our customers' needs.



DIANE ATTEBURY

What was new in 2001

Based on feedback from our customers, Cloud 9 Version 2 was introduced in September 2001.

Version 2 provides Java extensions to Cloud 9 that permit Java code which has been stored and modified in SCLM to be remotely built and deployed on UNIX System Services (USS).

SCLM Suite and related product introductions

| 2000 | 2001 | Spring/Summer 2002 | planned for the future* |
|---|---|---|--|
| IBM OS/390 SCLM Suite, November 2000. Consists of SCLM, IBM Cloud 9 for SCLM for OS/390 and IBM Breeze for SCLM for OS/390. | IBM z/OS SCLM Suite Vers on 2, September 2001. New Java development toolkit and SDSF batch viewer. Breeze Refresh, October 2001 | SCLM enhancements: Package Backout, Version Viewer and Version History Browser Cloud 9 enhancements: VA/Java integration via SCCI New IBM Migration Utility for z/OS and OS/390 New IBM Merge Tool for z/OS and OS/390 | Breeze enhancements: New web-based administrator workbench New tool to provide enhanced control over access to SCLM libraries SCLM integration with WSED Cloud 9 integration with WSAD and WSED More new tools and additional product enhancements! |

*Disclaimer: IBM's plans are subject to change. Nothing in this document is intended to create any representations or warranties. IBM warranties are contained in the applicable IBM license agreements.

FIGURE 1

A brief review of the SCLM Suite

The IBM SCLM Suite provides a comprehensive, integrated S/390 Web-based SCM that enables the management of e-business as well as S/390 objects in a centralized S/390 environment.

The SCLM Suite at first consisted of 3 products: SCLM (which is part of base z/OS or OS/390), IBM Cloud 9 for SCLM for z/OS, and

IBM Breeze for SCLM for z/OS. SCLM provides a robust library and configuration management solution for S/390. Cloud 9 adds a Web-based developer's workbench for SCLM which enables traditional S/390 and e-business objects to be managed as a single application. Breeze provides software developers and managers with a browser-based software package notification, review and approval system for SCLM.

It also introduced a new SDSF Batch Job Viewer. The Viewer allows you to monitor and process items in your JES2 job queue from a Web browser.

The Breeze component of the SCLM Suite was also enhanced in 2001. The Breeze changes were made available via a PTF, rather than as a new version of the product. The Breeze enhancements included additional viewing options for the Web-based Breeze approval interface, as well as modifications to the process for initiating package notification/approval and in promoting approved packages.

Spring/summer 2002

In the spring of this year, SCLM, the base component of the SCLM Suite, was updated to provide a new package backout capability as well as a version viewer and version history browser. These new functions make the recovery of your application data quicker and easier than ever. You do not have to wait for a new release of z/OS or OS/390 to take advantage of these enhancements. Contact IBM

(continued on next page)

Service to order the PTF.

In the summer, we plan to release enhancements to Cloud 9 to allow integration with Visual Age for Java (VA/Java) Version 4 via the Microsoft Source Code Control (SCC) API. This integration uses the VA/Java Tool actions for external version control. You can now add and remove Java parts from SCLM control and check them in and check them out of SCLM via Cloud 9 from within the VA/Java environment. You can also launch the Cloud 9 browser interface from within VA/Java in order to build and promote your completed application.

The new VA/Java integration is available via a PTF and can be ordered by calling IBM Service. Although our initial shipment of this functionality is based on VA/Java, we plan to continue to explore support for additional environments that support the SCC API, such as Visual Basic, Visual C++ and PowerBuilder.

We also delivered two new products to complement the SCLM Suite: IBM Migration Utility for z/OS and OS/390 and IBM Merge Tool for z/OS and OS/390.

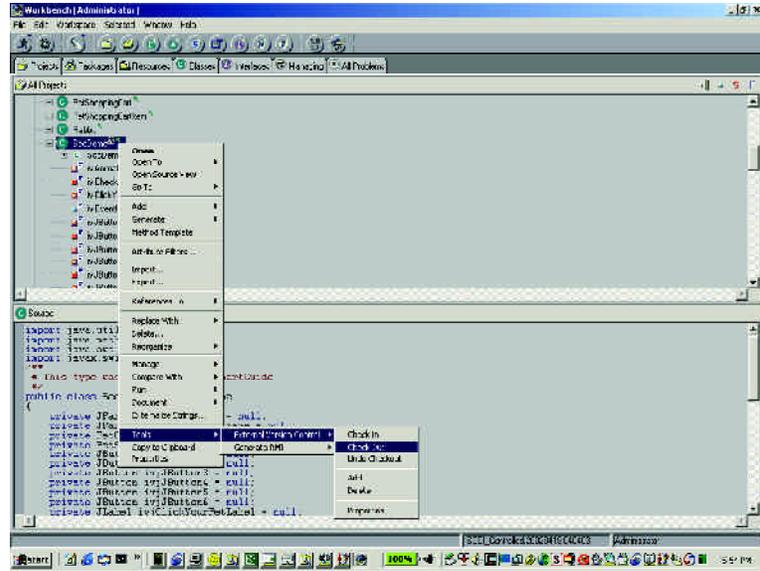


FIGURE 2

In April, we introduced the Migration Utility. The Migration Utility allows you to convert programs written in Computer Associates' Easytrieve Plus into IBM mainframe COBOL. The IBM Migration Utility gives you a choice:

- You can continue developing programs using the Easytrieve format. The only thing that changes is the JCL. The Migration Utility translator and COBOL compiler replace the Easytrieve run-time interpreter. You can continue to maintain the program source in Easytrieve format.
- OR**
- You can convert the Easytrieve programs to COBOL. You can convert both existing and newly developed programs. After the conversion, you can choose to update the programs using either the Easytrieve format or standard COBOL statements.

New IBM Migration Utility for z/OS and OS/390

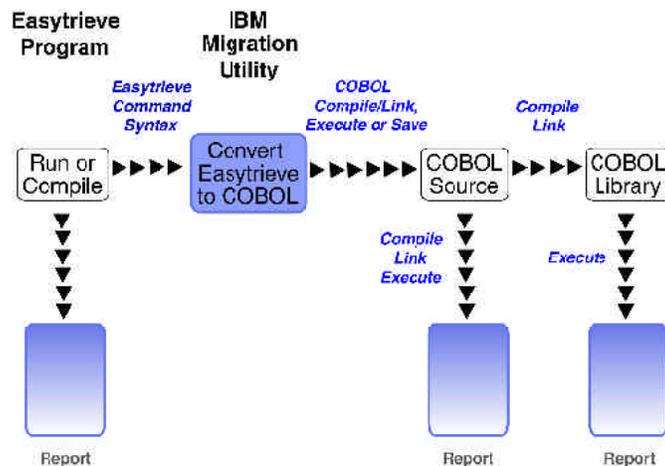


FIGURE 3

Even if you do not own an Easytrieve product, you can still use the IBM Migration Utility and enjoy the benefits of the Easytrieve language.

The IBM Migration Utility converts standard Easytrieve batch programs. It supports VSAM, QSAM, SAM, SQL/DB2®, tape files and unit record devices. It also supports the Easytrieve Macro Language and COPY directive. In most instances there will be no changes required to your existing Easytrieve programs.

The IBM Migration Utility reads Easytrieve language statements, converts them to a neutral meta-format, generates standard IBM COBOL statements, compiles (and optionally saves), and executes the compiled COBOL code. The generated COBOL source can be edited to include additional logic not supported by the Easytrieve language, or to make modifications to report content as required by changing business conditions.

Sample JCL is provided for each job step in the translation process, which can be adapted to the user's operating standards. The IBM Migration Utility for z/OS and OS/390 ships as a set of macros which interpret the Easytrieve syntax, generate the meta-format, and load modules which perform the rest of the conversion to COBOL. The sample JCL then invokes the COBOL compile, link, and go steps.

Some of the benefits of using IBM Migration Utility and COBOL include:

- COBOL I/O handling is more efficient
- COBOL sorting and searching is more efficient
- COBOL better coexists with other languages and environments
- All COBOL debugging tools can be used for debugging
- More people are available for program support
- COBOL is portable to other platforms

In the summer, we released the Merge Tool. The IBM Merge Tool is an easy to use ISPF-based 3-way merge facility that provides both project managers and S/390 application developers with the tools they need to identify, analyze and consolidate (merge) independently coded changes.

New! IBM Merge Tool! for z/OS and OS/390

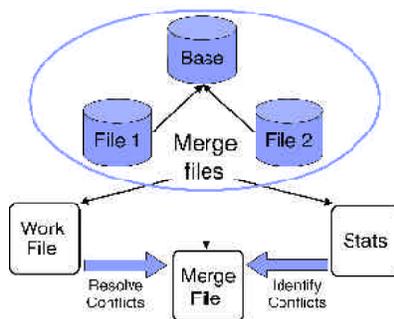


FIGURE 4

There are many reasons why changes may need to be made in parallel—an emergency fix, concurrent development, multiple release development or maintenance, customization of vendor application code—but a common process for managing the consolidation of those changes is necessary. You need to:

- Identify the changed components
- Analyze the complexity
- Merge and review the changes
- Address any merge conflicts
- Create merged source
- Test the merged output.

The IBM Merge Tool can help you efficiently use and manage this process to merge up to three versions of source code. In situations where the code complexity is low and there is no overlap among the changes, the Merge Tool can be used to perform a merge automatically. In most cases, though, you are going to want to produce a Work File and Statistics first. The Statistics File will show you the number of inserted, deleted and reformatted lines. The Statistics File will also tell you whether or not you have any merge conflicts and will help you estimate the size of the effort to resolve the conflicts and merge the changes. The Work File allows you to preview the merged output and correct any merge conflicts by editing the file. The Work File is used to generate the final Merge File. Once the code has been merged, whether automatically or by first reviewing and resolving conflicts in the Work File, the merged source code can be stored back into your Software Configuration Management (SCM) system. The merged source then becomes the basis for any future modifications to or compiling of the source part.

The IBM Merge Tool:

The IBM Merge Tool:

- Assists project managers with analysis, providing the details required to accurately determine what resources are needed for the consolidation effort.
- Assists developers in identifying changes being merged.
- Assists developers in isolating source code conflicts and resolving those conflicts.
- Assists developers in the actual consolidation of independently coded versions of a source part. ▶

(continued on next page)

We have no intention of slowing down...

We plan to provide additional enhancements to the Breeze product including a new browser interface to the Breeze administrative tasks and a separate 'seal' function that will allow you to launch the approval process from outside SCLM promote.

We also plan to launch a new product to provide additional control over access to SCLM-managed libraries. Currently, access to SCLM-controlled data is restricted based on RACF or other security packages and is done on a data set basis. This tool will allow you to further restrict access to SCLM data so that it can be accessed using only the SCLM Suite products. It will also allow you to restrict access from within the SCLM Suite based on function, so that you can decide which users should have access to which SCLM functions.

When WebSphere Studio Enterprise Developer (WSED) ships in the third quarter of this year, it is expected to include external library support for base SCLM. In the future, we would like to provide this support for both WebSphere Studio Application Developer (WSAD) and WSED via Cloud 9 in order to provide long file name support.

As you can see, we have been busy and have a lot more planned for the future. For more information on the SCLM Suite and related products, visit our Web sites at <http://www.software.ibm.com/ad/sclmsuite> and <http://www.software.ibm.com/ad/migration>, or contact:

In the US:

Bjorn Houston
bhouston@us.ibm.com
1-408-463-5872

Michael Larsen
larsenm@us.ibm.com
1-714-438-5726

In EMEA/AP:

Anthony Lawrence
Anthony_lawrence@uk.ibm.com
+44-20-88185069

Edwin Van De Grift
Edwin_vandegrift@nl.ibm.com
+31-653263470 ■

Performance management:

Quick, easy and inexpensive!

BY RICHARD MIKOLAJCZAK

IBM Operational Support Services for eServer zSeries performance management is an inexpensive, Web-based service that uses the z/OS Service Agent product to automate the collection and summarization of z/OS or OS/390 system measurements regarding system resources for up to 3 LPARs. With it, you are able to access graphical reports through the Internet that help identify areas of contention for resources. These reports also contain information you can use as input for your capacity planning responsibilities.

A remote IBM site processes your data and stores the resulting charts at the IBM site. These charts are then available for retrieval through your Web browser. The charts/graphs focus on how well your z/OS or OS/390 system is performing with regard to processor cycles, storage and DASD resource conflicts. The information is presented in a graphical format with goodness guidelines applied to highlight resource contention.

These charts/reports include:

- **System Health Management Summary:** Displays an executive summary of the system for the requested time period that includes contention levels of the three major resources (processor, storage and DASD).
- **Performance fact sheet:** Provides a tabular summary of the performance data for the reporting cycle.
- **OS/390 System Busy:** Shows the system busy based on the number of engines assigned to the LPAR for partitioned systems or on the number of processor engines for native mode systems.
- **Processor Busy by LPAR:** Shows the partition processor busy.
- **Processor Storage Contention:** Shows paging activity between central and expanded storage and between expanded and auxiliary storage.
- **System Busy by Workload:** Shows CPU busy by workload.
- **Central Storage Used/Available:** Indicates the number of megabytes of central storage used by the various workloads and the number of unallocated megabytes.
- **Expanded Storage Used/Available:** Shows the number of megabytes of expanded storage used by the various workloads and the number of unallocated megabytes.
- **Processor Storage by Workload:** Indicates the number of megabytes of processor storage used by each workload.
- **DASD Physical Controller Busy Summary (a DASD control unit summary chart):** Shows the shift average I/O rate for each physical controller.
- **I/O Rates and Response time (the next level down):** Shows I/O rate and response time by component for a physical controller.

Customer Benefits

This service is targeted towards the zSeries and S/390 clients who have a minimal systems programming staff with no dedicated performance analysts and do not have the skills for extensive performance tools usage. This service will provide these clients with a cost effective process that will measure the performance and capacity of their environments and identify hot spots.

For More Information

For more information regarding this service go to:

<http://perf.services.ibm.com/pmweb>.



NATASHA FRAY

The Library Center prototype: Know where you want to go and get there quick

BY GEOFF SMITH



FIGURE 1

As a zSeries customer you are probably well aware of the size and complexity of our zSeries libraries. Retrievability has been a consistent concern from our customers. We are continually working on improving your access to our information.

LookAt for messages (<http://www.ibm.com/servers/s390/os390/bkserv/lookat/lookat.html>) is one example of improving information retrieval. To use LookAt, all you need to know is a message id and what level of operating system you are running. Enter the message, pick your OS, and click on GO, and LookAt finds the explanation for you. You do not need to know what IBM element or product library to look in.

The zFavorites is another way that we improve retrievability, by providing all the links to popular zSeries home pages. It's a customized, categorized list designed the zSeries user.

Our Internet Libraries use the IBM BookServer product to serve in HTML format exactly the same information you receive on the

popular CD collections. The Library Center is based on BookServer technology. It is a prototype to see how we can best improve navigation and retrieval of our large BookManager based zSeries

libraries. Building on the traditional strengths of BookServer the Library Center prototype offers several new features.

Some of the key features of the Library Center are:

- The ability to visually browse Bookshelves and Books via an expandable, collapsible navigation bar. This feature is designed to help the reader see in context a chunked view of the subject matter.
- The ability to change your navigational view to select "Bookshelves or Books"
- One of the most significant change is the ability navigate by "Concepts," "Tasks," "Procedures," "Reference" and "Examples". For this prototype, we enabled one book to highlight these new views into the information.
- In addition seeing these new views of topics classified as "Tasks," "Concepts," and so on, once in this view, you can choose to do a subsetted search on only those topics.
- LookAt messages are integrated into the

search pulldowns

- Integrated PDF and BookManager book download
- Handheld enablement for users of Pocket PC 2002 and Palm/OS handhelds

Why WebSphere?

WebSphere for z/OS is one of IBM's most popular subject areas right now. It is a well defined, and manageable subset of the z/OS library. The WebSphere for z/OS books are relatively new library and topics were already classified into Tasks, Concepts and Reference. One of the most important reasons WebSphere was chosen for the prototype is that many of the procedures in the WebSphere for z/OS books rely on books in the base z/OS library and since both use BookManager it was easy to create custom bookshelves that let the user search across both libraries. (The workstation based WebSphere products publish their information as HTML-based Info Centers and we hope to eventually be able to include this information in the Library Center search as well).

Give it a test drive

We are very interested in your feedback on the Library Center. It's located at (<http://librarycenter.raleigh.ibm.com>). Once you have some experience with it, please use the feedback button on the site to send us your comments. Specifically: Do you like it? Do you find the new view and search by "Concept, Task, Procedures, Reference and Example" helpful? How could we improve the site? ■

State your preference... for autorunning z/OS library discs

BY SHIRLEY SWENSON

Are you annoyed that the collection index loads and runs automatically when you insert a z/OS library disc? Would you rather have the IBM Softcopy Reader start instead of the collection index when you insert a disc containing BookManager files? Now the choice is yours! This change was prompted by requests from customers who are accustomed to accessing BookManager files directly from an IBM Reader.

Beginning in March 2002, collections include SETUP.EXE, a program to set or change preferences that control how programs run when a collection disc is inserted. The first time you insert a disc from a March 2002

or later collection that contains the setup program, it runs automatically. In the window that opens, you can select your preferences for each type of collection disc. You can preview a preference before setting it by clicking on one of the "Open... now" buttons. After you save your preferences, they remain in effect for collections from March 2002 or later, until you change your preferences by running SETUP.EXE (found in the root directory on the collection discs) again.

For each type of disc (BookManager, PDF, or mixed BookManager and PDF disc), these are the preferences you can set:

The autorun preferences program, SETUP.EXE, provides flexibility for all users of our collections to choose how they want to access softcopy books. ■



PAUL ROWNTREE

| Available preferences | Discs with only BookManager files | Discs with only PDF files | Discs with both BookManager and PDF files |
|--|-----------------------------------|---------------------------|---|
| Open the IBM Softcopy Reader - Bookshelf Organizer | X | | X |
| Open the disc index | X | X | X |
| Open the collection index | X | X | X |
| Do nothing. Don't start any programs. | X | X | X |
| Don't set a preference for this type of disc. | | | |
| Show this preferences window again the next time. | X | X | X |

FIGURE 1

Alert! Alert!...for swapping and using those CD-ROM library discs

BY SHIRLEY SWENSON

We've finally done it—given you a truly meaningful message to help swap CD-ROM library discs in those large multi-disc collections. Remember that obscure message about book not found, which left you wondering where the book was if the Softcopy Reader couldn't find it? Surprise! When using the collection index, you'll now see "Please insert disc number" if you select to open a file that is not on the disc currently in your disc drive.

IBM Softcopy Reader 2.3.5 (available on the March 2002 collections) or later also includes a new "auto refresh" option that works with the alert "Please insert disc number." If "auto refresh" is selected when you swap discs in a device whose drive is included in the user-defined directories, Softcopy Reader's Bookshelf Organizer automatically refreshes the list of bookshelves. You'll like it! This is much easier than having to issue the commands View-Refresh each time you swap discs, isn't it?

To provide more options for accessing and using softcopy, beginning in March 2002, multi-disc collections (that is, collections with more than one disc) include separate softcopy indexes for each disc, as well as the softcopy index for the entire collection. We've also made it easy to switch between the disc and collection indexes by clicking on the "index" tab when a softcopy index is displayed. Or, you can choose to automatically open the disc or collection index by setting the appropriate autorun preference (see the article "State your preference...for autorunning z/OS library discs" on page 49).

In addition to the new disc indexes, beginning in June 2002, collections containing both BookManager and PDF files also include an index to just the PDF files in the collection. The PDF index is available in both HTML and text formats (PDFINDEX.HTM and PDFINDEX.TXT) in the root directory of the discs containing the softcopy files. It will help users upload PDFs to their local repositories.

These improvements should help you find the information you want more quickly and easily. ■



Fine-tuning the WLC picture

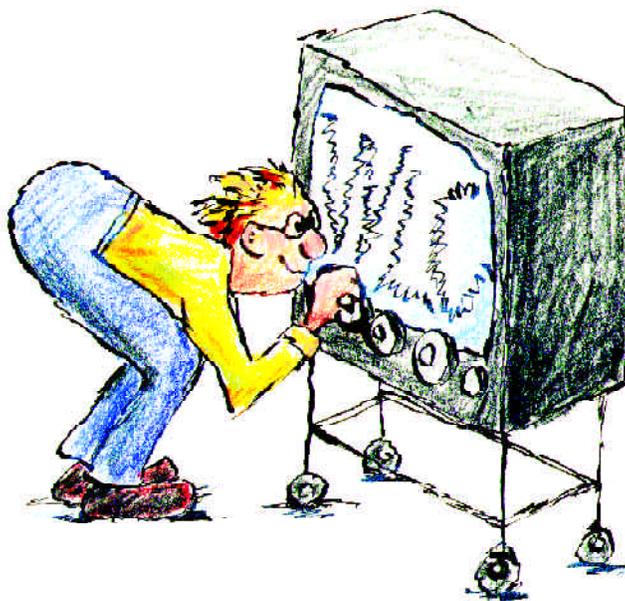
BY JOHN URBANIC

My friendly cable TV provider now gives me the capability to receive up to 200 channels. 200 channels! Are you serious? Who can watch that many? Just flipping through 200 channels, if you stop at each channel for just 10 seconds, would take over 30 minutes! The point is, I don't have time for 200 channels. And if I happen to like only the Rugby Channel and the Linear Algebra channel, I still have to pay for the whole lot. I wish I could selectively pay for just the channels I watch. And if I could pay according to how much I "use" my favorite channels—how much time I spent watching them—all the better!

IBM's software pricing method, called Workload License Charges (WLC), has been fine-tuned to provide the kind of granularity in billing that you wish the cable company provided. WLC is now based on LPAR utilization capacity: the highest measured 4-hour rolling MSU average for the combination of LPARs in which a Variable Workload License Charge (VWLC) product runs during a given month.

Let's say a zSeries CPC has a specific VWLC product running concurrently in three LPARs. The sum of the utilizations of these three LPARs over a given month is used to determine your cost for the product.

For example, a 200-MSU zSeries CPC has three LPAR sizes (maximum potential capacities) and associated products are the listed in figure 1.



DIANE ATTEBURY

Suppose for this example that the LPAR utilization capacities of the following LPARs (and combinations of LPARs) are:

- LPAR 1: 80 MSUs
- LPAR 2 plus LPAR 3: 70 MSUs
- LPAR 1 plus LPAR 2 plus LPAR 3: 150 MSUs

These LPAR utilization capacities would result in the VWLC products running in these LPARs to be priced based on the following capacities:

- z/OS is priced based on 150 MSUs—the LPAR utilization capacity of the LPARs where z/OS runs (LPARs 1, 2, and 3).
- MQ is priced based on 150 MSUs—the LPAR utilization capacity of the LPARs where MQ runs (LPARs 1, 2, and 3).
- IMS is priced based on 80 MSUs—the LPAR utilization capacity of the LPAR where IMS runs (LPAR 1).

(continued on next page)

| | LPAR1 | LPAR2 | LPAR3 |
|-----------------------|-------------------|---------------------------|---------------------------|
| LPAR size (in MSUs) | 100 | 50 | 50 |
| VWLC products running | z/OS MQ IMS | z/OS MQ CICS DB2 | z/OS MQ CICS DB2 |

FIGURE 1

- CICS is priced based on 70 MSUs—the LPAR utilization capacity of the LPARs where CICS runs (LPARs 2 and 3).
- DB2 is priced based on 70 MSUs—the LPAR utilization capacity of the LPARs where DB2 runs (LPARs 2 and 3).

The 4-hour rolling average for each LPAR is calculated for a month. The highest 4-hour rolling average measured is used for each LPAR and each combination of LPARs running concurrently (this assumes that all VWLC products contained in these LPARs are running for the entire month). Note that since LPARs can peak at different times, the LPAR utilization capacity for a combination of LPARs is not likely to be the sum of the individual utilization capacities of those LPARs.

What about defined capacity?

WLC was previously based on the defined capacity of the LPARs in which a VWLC product runs. (When you set up a defined capacity for an LPAR, the z/OS Workload Manager may constrain the performance of the LPAR to match its defined capacity and thereby apply a “soft cap” to the LPAR.) A defined capacity is still a useful way to help you control your use of an LPAR and thereby control your cost.

Why did IBM fine-tune WLC?

The change to LPAR utilization capacity should benefit customers who have LPARs with peak utilizations at different times during a given month. It should also help customers who find it difficult to set up a defined capacity for each LPAR due to widely varying LPAR utilizations and the desire to avoid having LPARs “soft-capped.”

For more information, visit the zSeries software pricing Web site at <http://www.ibm.com/zseries/swprice>.

I hope we’ve cleared up the changes to the WLC picture. Now if you’ll excuse me, I think the match between Queensland and Northern Transvaal is about start on the Rugby Channel. ■

z/OS RRS Multisystem Cascaded Transaction exploitation in IMS V8

BY JULIET CANDEE AND JACK YUAN

In z/OS V1R2, Resource Recovery Services (RRS) component introduced Multisystem Cascaded Transactions (MSCT) support. A cascaded transaction is a type of distributed transaction in which the representation of separate pieces of a distributed transaction is reduced into a single transaction. In a cascaded transaction, each branch of the distributed transaction is represented by a unit of recovery (UR), each with its work context. The RRS MSCT support coordinates a cascaded transaction which crosses multiple systems in a sysplex.

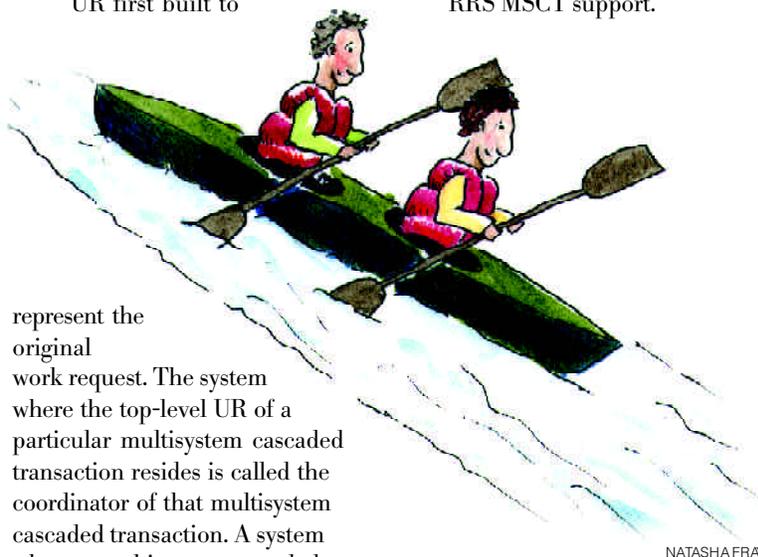
A cascaded UR family is created when a work manager tells RRS to create a new UR from an existing UR. Typically, a work manager would create a cascaded UR when a single work request involves multiple work managers. The work manager running in the environment where the transaction was first originated would obtain the initial work context that represented the work request and inform RRS to create a UR for the work request. When the work request moved from the execution environment of the original work manager into another work manager's environment, the second work manager could obtain a new work context, and inform RRS to create a new UR, cascaded from the original UR, for the new work context. The UR representing the original work request is called a top-level UR or a parent UR. The new UR is a child UR, or a cascaded UR of the parent UR. This set of units of recovery is coordinated by RRS as a single transaction within a single commit scope. The changes made

by all of the URs in a UR family are either all committed or all backed out.

A cascaded transaction can exist across multiple systems in a sysplex, as long as all of the systems involved in the transaction use the same RRS logging group. An RRS logging group is a group of systems that share an RRS workload. A cascaded transaction that has URs on multiple systems in a sysplex in which the cross system coordination is being provided by RRS is known as a multisystem cascaded transaction. The top-level UR of a multisystem cascaded transaction is the UR first built to

through the RRS system management facilities.

IMS V8 exploited the z/OS V1R2 RRS MSCT feature to provide the extended functions for protected and non-protected transactions for IMS/OTMA and IMS/APPC. With the RRS MSCT support, the synchronous OTMA or APPC workload can be distributed and executed on any IMS system in the Shared Queues group. The following figure provides a general flow of an OTMA synchronous (send-then-commit with synclevel CONFIRM) message as it is processed in an IMS Shared Queue (SQ) environment with the RRS MSCT support.



represent the original work request. The system where the top-level UR of a particular multisystem cascaded transaction resides is called the coordinator of that multisystem cascaded transaction. A system where a multisystem cascaded child UR resides is called a subordinate. A multisystem cascaded transaction will have a work identifier, known as a SURID (sysplex UR identifier) associated with it. All of the URs in a multisystem cascaded transaction will have the same SURID.

An installation can observe and manage all of the parts of a multisystem cascaded UR family

In the figure on page 54, MQSeries submits a synchronous (CM1) message to IMS/OTMA. IMS determines if the message is synchronous, checks to see if the Shared Queues capability is enabled, and invokes RRS callable services to obtain its work context and to create the parent UR. The input message is then placed on the global Shared Queues to be

(continued on next page)

IMS V8 using RRS MSCT

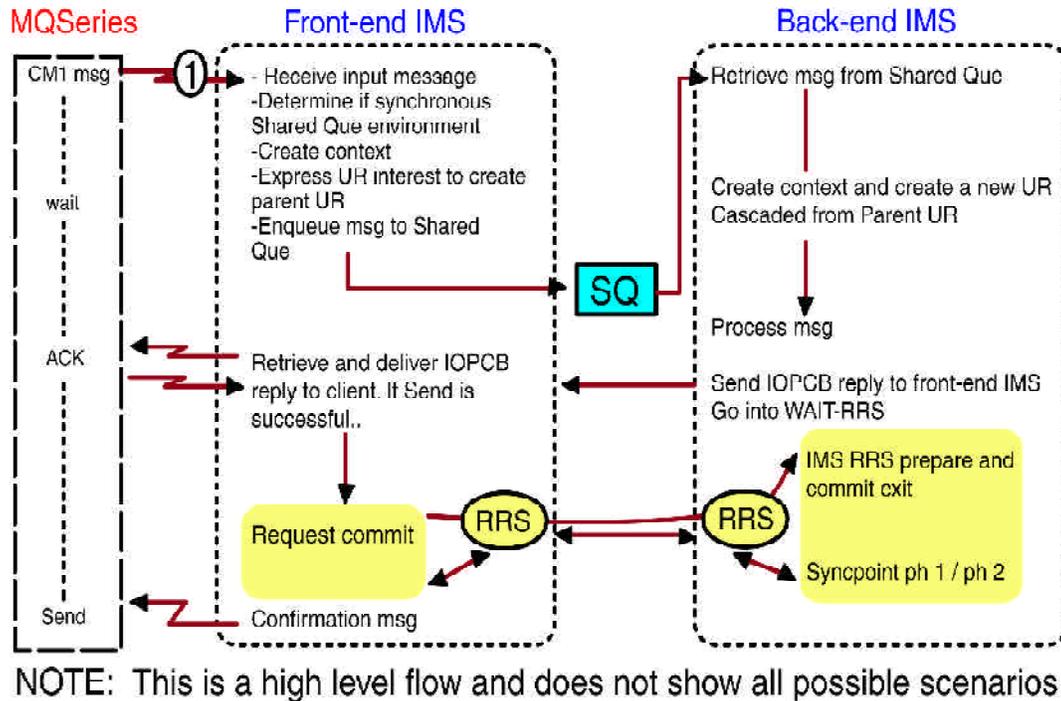


FIGURE 1

processed by a back-end IMS where the transaction is defined. After the back-end IMS retrieves the message from Shared Queue, it invokes RRS callable services to obtain a new work context and to create a child UR, cascaded from the parent UR. When the back-end IMS inserts back to IOPCB, an IOPCB reply is then sent to the front-end IMS. The IMS resources in the back-end IMS are held pending syncpoint processing until either a RRS commit or backout indicator is received.

The front-end IMS which is notified by the back-end IMS obtains the IOPCB reply and delivers it to MQSeries. Based on the success/failure of MQSeries interaction, the front-end IMS invokes RRS to either commit or backout the transaction. The RRS commit/backout is communicated to the back-end IMS for the corresponding commit/backout.

RRS on both sides provide the support for the synchronization of commit/backout using MSCT support. At the completion of commit/backout, the front-end

IMS/OTMA interacts with MQSeries by sending a confirmation message with the result of the syncpoint status.

In addition, IMS V8 will support the input parent UR specified in the OTMA message prefix for a protected transaction from any e-business connector. With this extended support in V8, IMS and any OTMA e-business connector can run in separate systems in a sysplex to process a protected transaction.

In summary, the z/OS V1R2 RRS Multisystem Cascaded Transaction support coordinates a cascaded transaction which crosses multiple systems in a sysplex. IMS V8 exploits the z/OS feature to provide extended shared queue function for OTMA/APPC and e-business connectors. ■

Our contributors

Jay Aiken

Jay has been with IBM for nearly 29 years and has had a checkered past. He has had assignments at the Office Products Division in Austin, in IBM Japan, and in Kingston, NY with Communication Products Division hardware staff. He has worked with Bellcore to develop the telephone company's Intelligent Network, he had a stint at IBM Corporate Headquarters in Armonk, and he was with VTAM and TCP/IP for the last ten years. Jay's current responsibilities revolve around Parallel Sysplex exploitation in TCP/IP.

Tracy Bondi

Tracy is a Graphic Designer for the IBM eServer Information Solutions organization in Poughkeepsie, NY. She has been at IBM for 3 year working on graphic design, animation, multimedia and Web design.

Juliet Candee

Juliet is a Senior Software Engineer at IBM Server Group in Poughkeepsie, NY. She has been with IBM for 13 years and is currently working in zSeries System Software Design with a focus on transaction processing.

Lesia Cox

Lesia's background includes marketing, technical support at IBM's International Technical Support Centers, as well as many years as a technical writer.

Patty Curry

Patty is a Software Engineer in the IBM eServer Information Solutions organization in Poughkeepsie, NY.

Mac Devine

Mac (wdevine@us.ibm.com) spent seven years in Communications Server development and was the Chief Programmer of several major releases before joining the Communications Server Strategy and Design group for four years and serving as the Chief Designer of several major releases. Mac then served as the lead solutions architect for networking alliances (Cisco, Nortel, etc.), responsible for the development of joint solutions which leverage IBM's eServer and e-business framework, before becoming the manager of the WebSphere Networking Solutions Architecture, Strategy and Design group, responsible for the strategy and design of solutions which leverage IBM's eServer and e-business framework.

Linda Distel

Linda is the Program Director for eServer Security and is responsible for leading the security strategy and investment planning for IBM Servers. This spans security items that are a part of the operating system, including operation systems and hardware cryptography for IBM eServers. Ms. Distel joined IBM as a programmer in 1983 and has held a number of positions in S/390 hardware and software development. Ms. Distel is a graduate of SUNY Albany with a bachelor's degree in Computer Science and Mathematics. She holds a master's degree in Computer Science from Marist College. She has a master's certificate in Project Management from George Washington University and is PMP certified.

Allan Edmands

Allan is an Advisory Software Engineer on the Creative Services team in Poughkeepsie, NY. He involves himself in projects that use multimedia to make complex technical concepts easier to grasp. He is in his third decade with IBM.

Jim Goethals

Jim has been associated with IBM networking products for 24 of his 32 years at IBM. Currently the zSeries Networking Offering Manager, Jim specializes in enterprise customer networking requirements and solutions. Jim is responsible for marketing the OSA-Express adapter and HiperSockets, for the IBM zSeries and Cisco joint e-business solutions, for TCP/IP and SNA solutions using CS for OS/390, and for helping customers leverage TCP/IP and their current SNA investments while evolving to the world of e-business on zSeries and S/390 servers.

Lap Huynh

Lap is an IBM Senior Software Engineer in the WebSphere and eServer Networking Solutions strategy and design group, focusing on TCP/IP Policy Based Networking and network Quality of Service. He has been the lead designer for many features in this area for both z/OS and the WebSphere Edge Server component.

Michael J. Kelly

Michael has worked for IBM since 1980, with assignments in JES2/MVS system test and in product development for cryptographic products. He is currently a Senior Software Engineer in the ICSF development organization. He has been a lead designer of ICSF continuously since the product was started in 1987. Prior to joining IBM, Mike worked as a Cryptologic Mathematician for the U. S. Department of Defense. Mike holds a Master's degree in Mathematics from Syracuse University.

Florence Krupa

Florence is a Senior Software Engineer in the eServer Information Solutions organization in Poughkeepsie, responsible for the documentation associated with z/OS.e. Her career with IBM spans 27 years and includes programming, writing, and planning.

Suzanne L. McHugh

Suzanne has worked for IBM since 1981, with assignments in technical marketing support for analytical chemistry instrumentation, information development for software and hardware products, and as a software engineer. She was the lead writer for the ICSF product library from 1990 through 1999. Suzanne is currently an Advisory Software Engineer in eServer Information Solutions organization. Prior to joining IBM, Suzanne was an analytical chemist in the Drug Metabolism Department at Wyeth Laboratories. She holds a BS degree in Biology from Slippery Rock University and Chemistry from Saint Joseph's University.

Richard Mikolajczak, Sr.

Dick is a Technical Support Marketing Specialist for IBM Global Services in Poughkeepsie, NY. He joined IBM in 1961 and has been involved in a multitude of large system customer support and service roles throughout his career. For the past eight years he has been team leader in the development of Internet and e-business services in IGS.

Lori Napoli

Lori is currently a Senior Software Engineer working in z/OS Communication Server. She designed, coded, and led the z/OS Communication Server team in repositioning z/OS IP for the new IPv6 protocol.

Barbara Neumann

Barbara is an Advisory Software Engineer in zSeries Information Solutions in Poughkeepsie.

Marsha O'Brien

Marsha started working at IBM as a programmer in 1985. Since then, she has held a variety of positions within IBM, including development, test, and product planning. Her current assignment is in marketing for the IBM SCLM Suite and other related products.

Wayne O'Brien

Wayne is an Advisory Software Engineer at IBM's Poughkeepsie Lab. Since joining IBM in 1988, Wayne has developed user assistance information for a variety of IBM software products. His current assignments include ServerPac usability and security wizard design.

Lin Overby

Lin is an IBM Senior Software Engineer in the WebSphere and eServer Networking Solutions strategy and design area, focusing on TCP/IP security. He has been lead designer on numerous z/OS Communications Server security functions including IPsec, TN3270 SSL, and Integrated Intrusion Detection Services.

Bob Perrone

Bob is an Advisory Software Engineer at IBM in Raleigh, NC. He works in the CS/390 performance group and was the CS/390 V1R2 performance team lead. Recent focus areas include HiperSockets Performance, HiperSockets Accelerator Performance, and Enterprise Extender performance.

David Raften

David has been involved with Parallel Sysplex technical marketing since 1994. He has also visited many customers, helping them obtain their availability objectives through technical and procedural changes.

Sam Reynolds

Sam (samr@us.ibm.com) has been associated with the design and development of host networking products since joining IBM in 1990. He is currently a designer for z/OS Communications Server, a product that provides TCP/IP and SNA connectivity.

J.D. Ross

J.D. is a Staff Software Engineer at IBM Poughkeepsie and has worked on documentation for z/OS UNIX System Services and Linux for zSeries. He is also the Webmaster of the Linux for zSeries Web site. Before joining IBM, J.D. served for several years as a system administrator, working with both the UNIX and Linux operating systems.

Geoff Smith

Geoff is a Senior Software Engineer at the eServer Information Solutions organization. He has been with IBM for 20 years and is responsible for technical documentation strategy.

Shirley Swenson

Shirley is a Senior Software Engineer with 22 years of experience in writing, managing, and planning large systems software and hardware information. She is currently the team leader and planner for the IBM Poughkeepsie Softcopy Center, focusing on customer delivery and feedback.

John Urbanic

John is an Advisory Software Engineer in the z/OS organization. Although John can not take credit for creating the Internet, he did write one of IBM's first softcopy-only Web books in 1992.

Dick Wagenaar

Dick is an Advisory Software Engineer and has documented MVS, OS/390, and z/OS programming concepts for more than twenty years. His latest book, z/OS.e Overview, explains the benefits and uses of this new offering.

Judy Washo

Judy has been with IBM for 22 years, starting as a system programmer enabling ISVs to the latest technology. She is now the SystemPac ISV business manager.

Jack Yuan

Jack is a Senior Software Engineer at IBM's Silicon Valley Laboratory in San Jose, California. He has been with IBM for 15 years and is currently working with IMS/TM for Open Transaction Manager Access development.

Top Ten List of Late Night Outages

(continued from back cover)

Outage number nine: (Operator education / automation)

One failure seen was a customer took a TEST system out of a 2-system plex to make it a monoplex, but kept it pointing to the same Sysplex Couple Data Sets. When they IPLed it and responded to have it initialize the plex, the PROD system came down. In another example, one operator re-IPLed instead of using the FORCE command to terminate a hung address space.

In both of these cases, proper automation procedures for start-up and shut-down of address spaces and systems could prevent the outages.

Operating a computer center becomes more complex as the use of technology increases. Multiple systems and large networks add even more complexity to data-center operations. As systems and resources grow in numbers and usage, the demands on them also grow. This places an increasing demand on operators and system programmers. z/OS has incorporated many common automation activities into the product itself with msys for Operations for self-monitoring and self-healing, but still, an external automation product is required to run the center. Providing many benefits to system and network operations by simplifying the operating environment. It can reduce the amount of manual intervention required to manage operating systems, subsystems, application programs, network devices, and many other products. This in turn may reduce costs and improves system and application availability.

Examples of activities that should be targeted for automation include startup and shutdown of systems and subsystems, automatic restart of failed address spaces with all communication connectivity reestablished, and error recovery for when logging or messages backs up. System Automation for OS/390 includes templates for many of the multi-system management activities. Together with good up to date operator procedure manuals, this can help in meeting required service levels, containing costs, and making efficient use of the operation staff.

Outage number eight: Disk inaccessibility

Three out of four systems in the sysplex had page volumes on the same disk subsystem. These failed when the disk subsystem failed.

A well set up Parallel Sysplex cluster eliminates most single points of failure at the zSeries / S/390 layer. It provides multiple ways for work to get in to the system from the network without changes to the interface (MQSeries Clusters, CICS MRO, and VIPA Takeover are some examples). By itself, it can not resolve single points of failure issues from the network or disk subsystem layer.

Single Points of Failure (SPOFs) in the network are easy to identify. Multiple routers can be installed with SNA and IP requests distributed across the sysplex. Disk subsystem SPOFs are more problematic to identify and solve due to the expense and the dynamic nature of data sets locations. As disk subsystems become ever more larger, what was once isolated now is consolidated on the same box. Key data sets include Page data sets, Couple Data Sets, JES2 Checkpoint, load libraries, etc.

A tool, XISOLATE, can help so that each copy of the data set resides on separate physical DASD subsystems. XISOLATE can be downloaded from <ftp://ftp.software.ibm.com/s390/mvs/tools/>.

Outage number seven: msys for Operations not used

A customer had a failed IPL after a processor replacement. The processor being replaced had an ICF LPAR, but the CF was removed without deallocating all the structures.

In another case, a customer had a DASD failure which caused the sysplex to switch to the alternate Couple Data Sets. When the DASD was recovered and the customer attempted to move back to using the original primary CDSs, they could not. They IPLed the entire sysplex to fix the problem.

There are many complex tasks required to manage a Parallel Sysplex Cluster. msys for Operations in z/OS 1.2 was designed to automate many of these functions. It can help with structure management, allocation of new primary couple data sets when it is down to one, as well as manage WTO buffers, page data sets, and many more.

Outage number six: Lack of sysplex exploitation

One customer had an elongated outage after a CEC failure in a sysplex. Hard coded MQSeries dependencies in the front-end processor applications needed to be changed before they could connect to the surviving members of the data sharing group. No customer impact should have occurred as MQSeries clustering support had been available to

handle just this situation. It was not being used.

Another customer had a CICSplex® set up for some, but not all of the critical applications. These applications were unavailable during planned outages.

Many installations have installed Parallel Sysplex clustering to solve capacity and/or availability problems for selected critical applications, but not all critical work. Once the targeted goal was met, the project was declared complete. In many cases, enabling data sharing for additional applications can be done at a minimal cost to add significant end-user availability.

Outage number five: No back-up system

While running in a single system environment, a customer deleted a proclib, but failed to remove it from the proclib concatenation in their JES2 proc. to reflect the changes. When JES2 could not start due to data sets not found, the customer did not have a back-up system to get to TSO to change the proc. The customer had to install a new system from scratch to get TSO up. This outage ended up being over 24 hours.

For emergency recovery capabilities, it is recommended that every installation have a small, isolated “Get-Well” system to help in situations of finger checks or corrupted shared system data sets. This system should have access to all production DASD and catalogs, but not require any production data sets, have access to IBM link and FTP capability, and all its key system data sets on separate control units from the production system. This can help in situations of applying emergency maintenance, fixing procs/parms, as well as disk problems.

JES2 in z/OS 1.2 has additional support to avoid a situation described above. With dynamic proclib support, one can put the proclib concatenation inside the JES2 Initialization deck.

Outage number four: Downlevel maintenance

SNA links were receiving more packets than could be processed with outbound queues building up. Each outbound element used ECSA storage. When a user brought down a session partner, SNALINK did not go through the outbound queues to clean up elements. Eventually all ECSA storage was used up, affecting all network routers. In this case, a fix was available for over 6 months.

Installing maintenance is a labor intensive task for system programmers, many of whom are busy providing system support and fighting fires. Much “installation” time is spent researching PTFs that are held for special actions to be taken. Researching HIPER and PE APARs is also very time consuming. However, availability depends on a proactive maintenance process. The resources required to support the maintenance process are a trade off between the work effort and System Availability.

IBM seeks to make fixes as soon as we can and are focused on high quality fixes. As part of IBM’s commitment to quality and continuous improvement, we established an additional service testing environment called Consolidated Service Test (CST). This provides a consolidated, tested, and recommended set of service for z/OS or OS/390 and their key subsystems on a quarterly basis with published results. It is recommended that this resulting Recommended Service Upgrade (RSU) be installed as soon as

available with a high confidence of minimal risk. The RSU process also reduces the research requirements as all the prerequisites have already been resolved within the service level. More information on the RSU process can be found at <http://www.ibm.com/servers/eserver/zseries/zos/servicetst>.

Outage number three: Didn’t read the documentation

One customer reported, “Some systems weren’t recovered after a Coupling Facility failure.” Investigation of what happened and actions taken by the customer revealed that there are clearly documented procedures for recovering from hangs such as this, but the customer did none of the steps in the procedure.

During a crisis situation, everyone’s thoughts are on recovering service as soon as possible. To do this, system support and operations need to take the correct action quickly. Understanding what action to take needs to be well documented in an easy to find media.

When in college, there was a saying, “Real Programmers Don’t Document. If it was hard to write, it should be hard to understand.” Another saying was “Real Men Don’t Ask Directions.” IBM programmers are no longer in college. We spend a lot of time making sure that recovery actions for errors are well documented with search capabilities either on CD-ROM or online in reference manuals, Redbooks™, and Informational APARs. There are a lot of sysplex recovery steps documented in “z/OS MVS Setting Up a Sysplex” SA22-7625-00. Don’t let that book get dusty once you’ve set up the sysplex. ▶

(continued on next page)

Operator procedure guides should have actions for various situations as well. Education is available so system support and operators know what to do and can practice this hands-on in simulation mode. One such offering, the “Parallel Sysplex Trainer,” is a micro-Parallel Sysplex environment that can be installed on site or under VM. The CMOS Complex Systems Availability and Recovery (CSAR) class is another option to improve your ability to recognize and respond correctly to error situations.

As mentioned earlier, Automation is critical to manage a large environment. Automating recovery actions is less error-prone and faster than having humans perform the work. If a procedure could be documented, it could be automated.

Outage number two: OEM failure / testing

A third party product caused a VTAM failure on four systems in a six-way sysplex after applying RSU maintenance. This resulted in recursive ABEND0C4 dumps.

IBM does not test its products together with OEM within the lab. There are too many different possible combinations for any IBM testing to be effective. Because of that, it is up to the customer to test their own environment before migrating system code into production.

Stress testing is a time consuming process and it is difficult to keep the simulation scripts current, yet there is a place for it when putting in major application or system level changes. For other changes going into the system there should be a documented testing process. This key to this process is track production problems that escaped the testing, look for trends, and then go back to modify and improve the process in a cost-effective manner.

Outage number one: msys for Setup not used

A customer attempted to start an FTP server and got a bind error, permission denied when they try to start it. Customer misnamed the FTP task in the port reservation. (Four systems affected for 11 hours). In this case, a parameter was set incorrectly.

z/OS allows system programmers to modify and adjust settings for just about everything that falls under its scope. This is a powerful tuning tool, but requires care as many parameters are dependent upon each other and “finger checks” are always possibilities. This is especially true in the networking area.

msys for Setup available with z/OS 1.1, was designed to address this issue. Intelligent wizards direct the definition of the environment using “best practices” recommended values for many of the fields. With subsequent z/OS releases, more and more products and features can be configured with msys for Setup.

Conclusion

And so, ladies and gentlemen, z/OS Parallel Sysplex and its program products provides the ability to obtain a high availability environment. IBM is doing many things to understand and address the root causes of the outages including redesigning components when needed. Customers can take actions as well to prepare for and protect themselves from outages. ■

Reference information

| | |
|--|--|
| <u>ITSO Redbooks</u> | <u>http://www.redbooks.ibm.com/</u> |
| <u>Message lookup tool</u> | <u>http://www.ibm.com/servers/s390/os390/bkserv/lookat/lookat.html</u> |
| <u>Parallel Sysplex Information</u> | <u>http://www.ibm.com/servers/eserver/zseries/psol/</u> |
| <u>RSU maintenance</u> | <u>http://www.ibm.com/servers/eserver/zseries/zos/servicetst/</u> |
| <u>Technical Support</u> | <u>http://www.ibm.com/support/techdocs/atmastr.nsf</u> |
| <u>XISOLATE tool</u> | <u>ftp://ftp.software.ibm.com/s390/mvs/tools/</u> |
| <u>z/OS library</u> | <u>http://www.ibm.com/servers/eserver/zseries/zos/bkserv/</u> |
| <u>z/OS wizards</u> | <u>http://www.ibm.com/servers/eserver/zseries/zos/wizards/</u> |
| SC33-7968 | <i>z/OS V1R2.0-V1R3.0 Setting up and Using Managed System Infrastructure for Operations (msys for Operations)</i> |
| SA22-7625 | <i>z/OS MVS Setting Up a Sysplex</i> |

Security: New challenges, building on a solid base

(continued from cover)

In May 2002, we made available to our customers an eServer Security Planner that allows them to more easily configure their eServers with security settings. Over the past several years, customers have asked us for our insight on how to set up the security of their systems. As they open their systems to the Internet, they have a renewed fear of who they could be letting in. Creating a planner allows us to provide them with recommendations for security settings by answering some easy questions about their configuration.

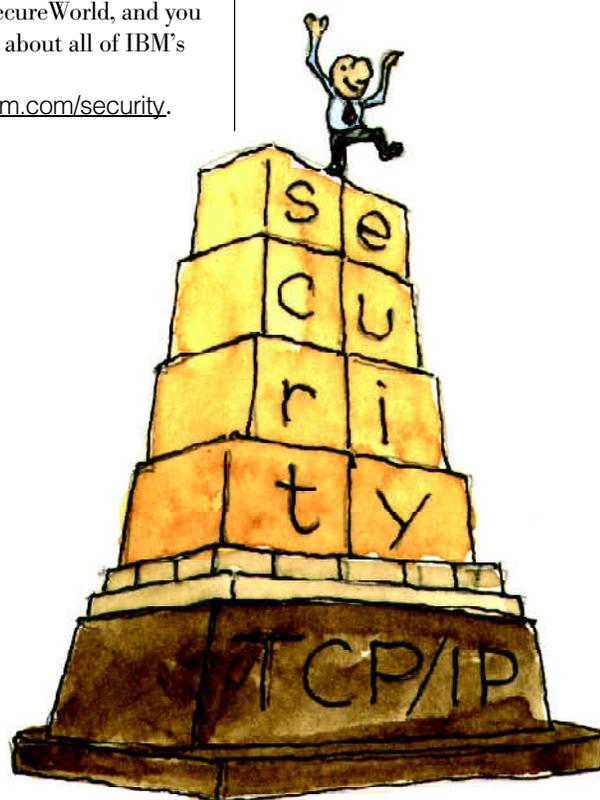
The operating systems and programs that run on them have had a hard time associating a user with the many userids that they have. "Single sign-on" products just hide the end user from the complexity, so Pat Botz invented Enterprise Identity Mapping (EIM). EIM is focused on allowing a transaction to associate a user from one security directory to his/her identity on another security directory (RACF on z/OS to Kerberos on OS/400, for example). Using EIM in concert with Kerberos, we are able to provide a single sign-on environment for a transaction. This function has been already announced on iSeries and is planned to be announced and delivered across all the eServer platforms in the future.

Our next challenge is to define and deliver the value add of our eServer platforms in a Web Services environment. In this model, the security interfaces live in the middleware layer, and we expect that the following security characteristics will be most important to the servers:

- Server intrusion detection
- Security certifications
- VPNs
- Hardware encryption
- Integrity
- LDAP (Lightweight Directory Access Protocol)
- Security advisors and wizards
- Tight WebSphere integration.

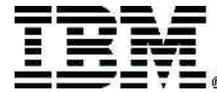
Server Group is also tied into the larger IBM security team. We have been part of an effort to approach system integrators to educate them on IBM's security technologies, and we are part of an overall IBM effort to educate our sales force on IBM's end-to-end security capabilities. Server Group is an active participant in IBM's security conference, SecureWorld, and you can find more about all of IBM's security at <http://www.ibm.com/security>.

Overall, I see security continuing to be a major focus in the industry, with IBM's strength being that it provides solutions at every level (servers, software, services). Our focus will be to continue to support new security standards, provide more common function across eServers, make security easier in a distributed heterogeneous environment, and integrate well with WebSphere and Tivoli security products. ■



Top Ten List of Late Night Outages

BY DAVID RAFTEN



Good evening ladies and gentlemen. Yes, it is time for the “Top Ten” list. Tonight, based on actual experiences, we have the list of “Outages whose impact could be minimized!” Despite being designed to run in a 24x7x52 environment, service outages do occur. For this reason, z/OS has been developed with robust recovery mechanisms so that many

outages can be hidden from end users or their impact minimized. Tools are also provided to help reduce operational complexity

and to recovery quickly from errors when they do occur. New function and new component designs are constantly coming out to avoid problems in the future. This article looks at examples from 10 categories of outages seen with a description of what could be done to reduce their impact. Although “late night” outages do affect system programmers the most, many of these examples have been in the middle of the day where they impact customers the most.

Outage number ten: Sysplex Failure Manager not enabled

One customer had a system failure. Message IXC102A or IXC402D (REPLY DOWN AFTER SYSTEM RESET) was not seen for over an hour due to the quantity of other messages being produced and operations busy handling the

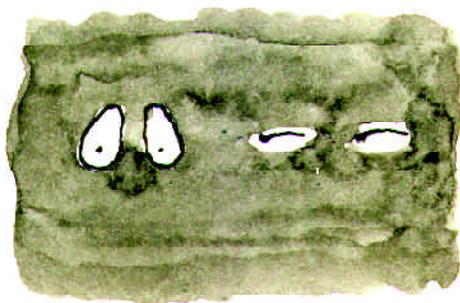
system failure. This resulted in GRS and data base locks being held with other systems not knowing of the failure. Exclusive IRLM locks were not converted to “Retained Locks”, and so data base requests started backing up, stalling all the other systems in the sysplex. Attempting to re-IPL the failed system before replying to these messages would not have

worked since at IPL time the system tries to communicate with all the systems that the Couple Data Set thinks is active,

including the failed instance of itself. This would not work and the re-IPL would fail.

Sysplex Failure Manager was added to MVS 5.1 to help in this situation. By enabling SFM with the ISOLATETIME parameter, a failure of one member of the Parallel Sysplex would be automatically detected and isolated from other members. System isolation allows a system to be removed from the sysplex without operator intervention. Specifically, system isolation terminates I/O and coupling facility accesses, resets channel paths, and loads a non-restartable wait state on the failing system, freeing up shared resources while ensuring that data integrity in the sysplex is preserved. ▶

(continued on page 56)



PAULROWNTREE

© International Business Machines Corporation, 1999, 2002

Produced in the United States of America

8-2002

All Rights Reserved

The z/OS Hot Topics Newsletter is published twice yearly as a service to customers, providing articles of interest to the z/OS and OS/390 community.

The information in this Newsletter is presented as is and is based on the best knowledge of the authors. No warranty is provided (neither expressed nor implied).

IBM may not offer the products, features or services discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM representative for information on the products or services available in your area.

© Advanced Peer-to-Peer Networking, AIX, BookManager, CICS, CICSplex, DB2, DRDA, Encina, ESCON, GDMM, IBM, Language Environment, MQSeries, Multiprise, Netfinity, NetView, Net.Data, OS/390, OS/400, Parallel Sysplex, RACF, SystemPac, S/390, Tivoli, VisualAge, VTAM, WebSphere, are registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

™ DB2 Universal Database, eLiza, IMS, iSeries, MVS, pSeries, QMF, Redbooks, Resource Link, xSeries, z/VM are trademarks of International Business Machines Corporation.

zSeries and z/OS are trademarks of IBM. zSeries and z/OS are trademarks of IBM.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, or other countries, or both.

Domino is a registered trademarks of Lotus Development Corporation.

LINUX is a registered trademark of Linus Torvalds.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

Other company, product, and service names may be trademarks or service marks of others.



GA22-7501-03