Enterprise IT Management Made Simple

IBM @server iSeries

iSeries e-Business

V5R2 and Beyond

Enterprise IT Management Made Simple

Capacity Upgrade on Demand

OS/400 V5R2

WebSphere Development Studio

64-Bit Linux

32-way, 64-Bit POWER4 i890

Enterprise Identity Mapping

Adaptive e-transaction Server

Innovative Technology

Application Flexibility

Apache Web Caching Accelerator

Lotus Domino 6

Virtual Ethernet

Switched Disk Clustering

iSeries Navigator

Microsoft[7] Cluster Service

SAN Switch Fabric

OS/400 PASE with AIX 5L

Secure Sockets Accelerator

Wireless-Web Micro Edition

LPAR Sub-capacity Pricing

New Tools for e-business

Multiple DB2™ UDB Namespaces

Project eLiza

WebSphere Portal Server

iSeries Access for Web

DB2 UDB Open SQL Standards

Notes: iSeries Announcement at A Glance

On April 29 2002, IBM eServer iSeries announced OS/400 V5R2 and the iSeries Model 890, featuring the award-winning[1] POWER4 microprocessor. The i890 delivers unprecedented performance at the high end of the iSeries product line, with up to 1.85 times the performance of the existing i840 24-way server.

Since e-business is really just an extension to your existing business, there are many, many enhancements in the new V5R2 that
.....
Included in the new V5R2 are significant enhancements in the area of e-business..

This announcement also signals new flexibility to add new workloads to iSeries with expanded options for Capacity Upgrade on Demand (CUoD), extending base processor features across the product line and sub-capacity pricing for WebSphere products running in logical partitions.

The i890 availability with OS/400 V5R2 (English only with enablement for DBCS) begins on June 14, 2002.

General availability for OS/400 V5R2 and additional language versions is planned for August, 2002.

New Capacity on Demand options and base processor features for the i830 and i840 are available April 29, 2002.

(1) In **January 2000**, the IBM POWER4 processor was awarded Microprocessor Report's 2000 Microprocessor Technology Award in recognition of its innovations and technology.
April 30, 2002: -- IBM received the coveted Microprocessor Report Analysts' Choice Award for Best Workstation/Server Processor of 2001 at a microprocessor industry event. Cahners In-Stat/MDR, a leading microprocessor research firm, chose the POWER4 processor over Intel's Itanium and Compaq's Alpha 21264C 1 processors.

iSeries J eBusiness at A Glance

- Networking
- IBM HTTP Server *Powered by Apache*
- Cryptography and Security
- IBM DB2 UDB
- e-Output
- Grid Computing and Project eLiza

Notes: Enterprise IT Management Challenge

This chart describes information from IBM research with the institute of high performance of business computing. The study shows common approaches to large corporation's enabling of their e-business infrastructure, deploying multiple applications, resources and server workloads.

Some companies will chose to deploy multiple server platforms in their datacenter, each optimized for a specific workload. Multiple server platforms, however, also lead to more complex management tasks, driving higher level skills requirements and associated costs.

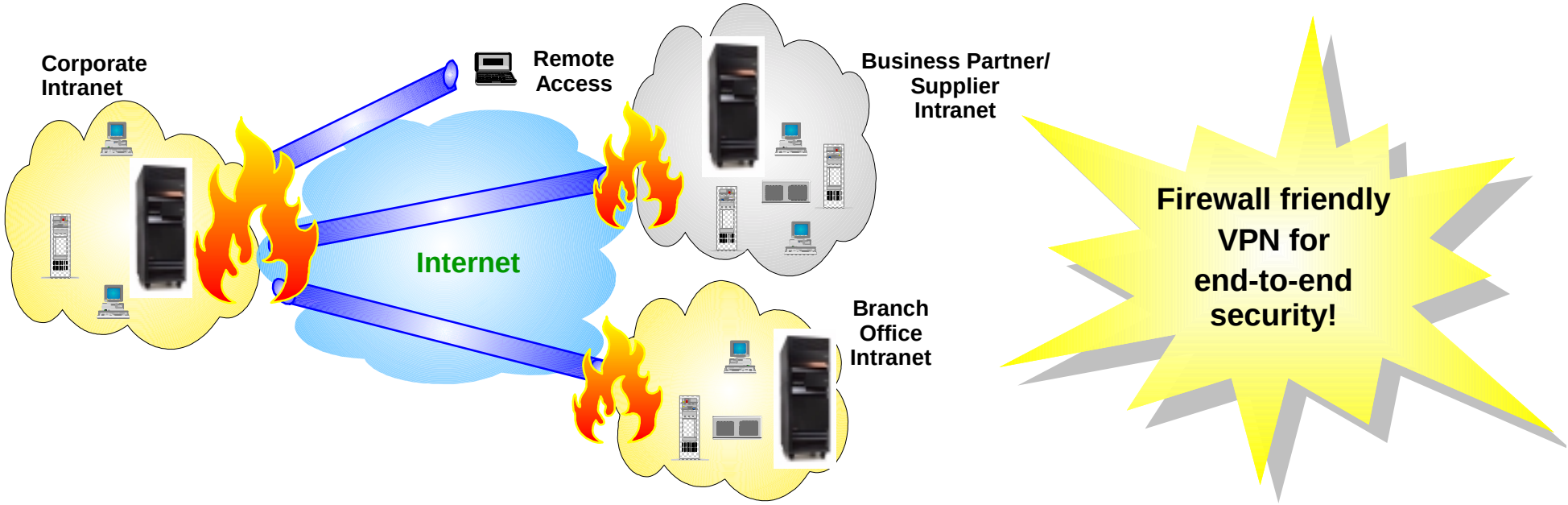
iSeries provides one opportunity to address the challenges associated with managing multiple workload environments by providing flexible consolidation options for multiple workloads, applications and operating system environments, all within a single server infrastructure. So, for example, iSeries can handle multiple partitions running database and transaction workloads, alongside WebSphere partitions for e-business application serving and Linux partitions for e-business infrastructure applications like web serving and firewalls. Combined with support for Windows-based applications, iSeries offers a single management infrastructure that can help customers reduce datacenter operations costs and total cost of ownership.

Networking

Networking - What's new in V5R2

- Network Security Enhancements
  - VPN and IP Filtering
  - FTP Client SSL support
  - Telnet Kerberos Authentication
- QoS Enhancements
- IPv6 Application Development Platform
- Remote Access Enhancements
- JavaMail

Firewall friendly VPN



- **VPN connections don't work through conventional Firewall technology**
  - With NAT and SOCKS, source address changes, invalidating the IPSec packet
- **Solution: UDP Encapsulation of IPSec**
  - Allows VPN systems to be protected by a firewall
  - Transparent to the application
  - Transparent to the firewall

Notes: Firewall Friendly VPN

Network Address Translation (NAT) allows you to hide your unregistered private IP addresses behind a set of registered IP addresses at your firewall. This helps to protect your internal network from outside networkds. NAT also helps to alleviate the IP address depletion problem, since many private addresses can be represented by a small set of registered addresses.

Unfortunately, conventional NAT does not work on IPSec packets because when the packet goes through a NAT device, the source address in the packet changes, thereby invalidating the packet. The receiving end of the VPN connection discards the packet and the VPN connection negotiations fail.

UDP encapsulation wraps an IPSec packet inside a new, but duplicate, IP/UDP header. The address of the new IP header gets translated when it goes through the NAT device. When the packet reaches its destination, the receiving end strips off the additional header, leaving the original IPSec packet which should now pass all other validations.

NOTES; You can only apply UDP encapsulation to VPNs that use IPSec ESP in either tunnel mode or transport mode. The iSeries can only initiate UDP encapsulated traffic. The packet is sent over UDP port 500 (IKE negotiations are performed over UDP port 500 already), so additional ports are not necessary. The receiving end can determine whether the packet is an IKE packet or a UDP encapsulated packet because the first 8 bytes of the UDP payload are set to zero.

VPN Simplification

- **Documented Scenarios for VPN planning and configuration**
- **Planning Advisor Updates**
- **New Editor and Wizards**
  - ASCII text editor for packet filters
  - Wizards for Migration, Permit Service, Spoof Protection, Address Translation (NAT)
- **Dynamic Policy Filters**
  - Don't need to configure packet rules to have VPN connection
  - System manages filters dynamically for the connection

Notes: VPN Simplification

For V5R2, there were significant enhancements in the area of VPN simplification. Additional scenarios have been documented to further understanding of how VPN works and is configured in a corporate setting.

There were also updates to the VPN planning advisor that helps you determine what type of VPN you should create to address your specific business needs. The advisor also suggests what steps you must take to configure the VPN..

NOTES: Use the planning advisor only for connections that support Internet Key Exchange (IKE) protocol. Use the planning worksheet for manual connections for your manual connection types.

When you configure VPN, it will automatically generated the VPN packet rules for you. However, if you decide you want to delve into the nitty-gritty details of packet rules, there is a new ASCII text editor that will allow you to directly modify them. However, use it with caution as it is easy to make mistakes at this level.

In addition to the New Connection Wizard, which was available in V5R1, four new wizards have been provided to guide you in VPN configuration.

The migration wizard will migrate V4R4/V4R5 VPN policy filters to the new format for V5R2. You'll need to perform this step if you're going to be creating new VPN connections. Otherwise, t is not necessary.

There are also wizards for permitting a service on the connection, setting up spoof protection, and setting up NAT

NOTE: The New Connection Wizard also creates your IKE policy and data policy for you

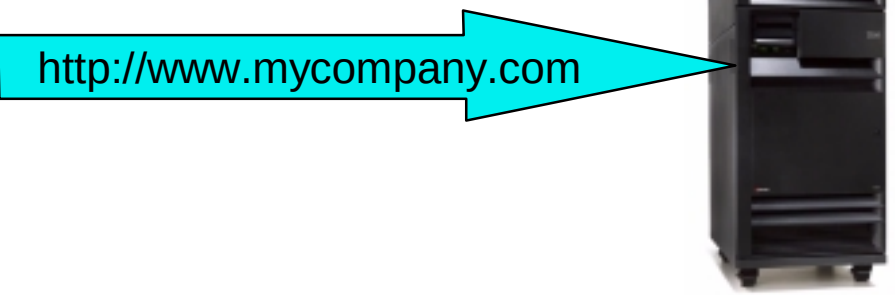
Most VPN connections require filter rules to work properly. The filter rules required depend on the type of VPN connection that you are configuring as well as the type of traffic you want to control. Since V5R1, VPN can generate these rules automatically. In some cases, you may want to configure a connection that does not require a VPN policy filter rule. For example, you may have non-VPN packet rules activated on the interface that your VPN connection will use. Rather than deactivating those rules, you can configure the VPN so that your system manages all filters dynamically for the connection. This is referred to as a dynamic policy filter.

Before you can use a dynamic policy filter, all of the following must be true:

- the connection can only be initiated by the local server
- the data endpoints of the connection must be single systems (not a subnet or range of addresses)
- No policy filter rule can be loaded for the connection

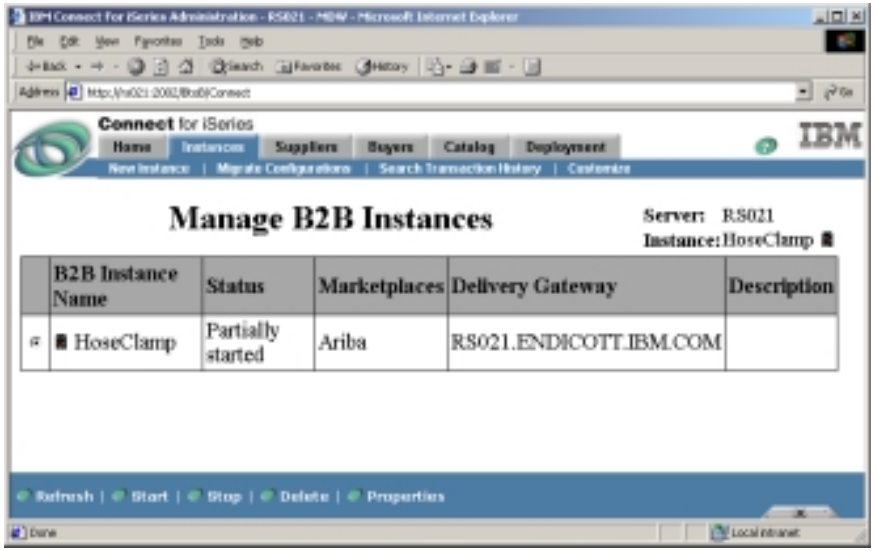
Network Quality of Service Enhancements

- **Inbound connection rate control**
  - URL & Connection Based Policy
- **More flexible Policy definitions**
- **Simplified RSVP Sockets APIs**
- **QoS policy support in LDAP**
  - Populate policy from Op Nav



/home.html

/B2B



Notes: QoS Enhancements

Without QoS, all traffic in your network receives equal priority. Noncritical browser traffic as well as business critical transactions. QoS allows you to request network priority and bandwidth for TCP/IP applications - allowing you to have predictable and reliable results.

In V5R2, there are several enhancements to our QoS support.

Inbound Connection Rate Control

Inbound policies are used to control traffic attempting to connect to your server. There are two types of policies: URI policies and connection rate policies. Wizards are provided.

- URI request rate policies are part of a solution to help protect services against overload. This type of policy controls incoming traffic based on application-level information (aka header-based connection request control). URI policies have more control than connection rate policies since they examine content, not just packet headers. For iSeries, the relative URI name is used to define the policy. NOTE: The URI has an implicit wildcard at the end.
- Connection rate policies also help protect servers against overload. This type of policy controls incoming traffic based on connection-level information. (aka TCP SYN policing). New incoming connections are accepted or denied based on the average number of connections established per second and the maximum number of established connections defined by the policy. As part of this policy, you can specify the priority of the connection after they have been accepted. HINT: to determine what limits to set, you can collect and monitor current network statistics and adjust the limits appropriately.

More flexible policy definitions

Associate policies with local interfaces - policy depends on the interface the client packet arrives on

Associate policies with multiple clients

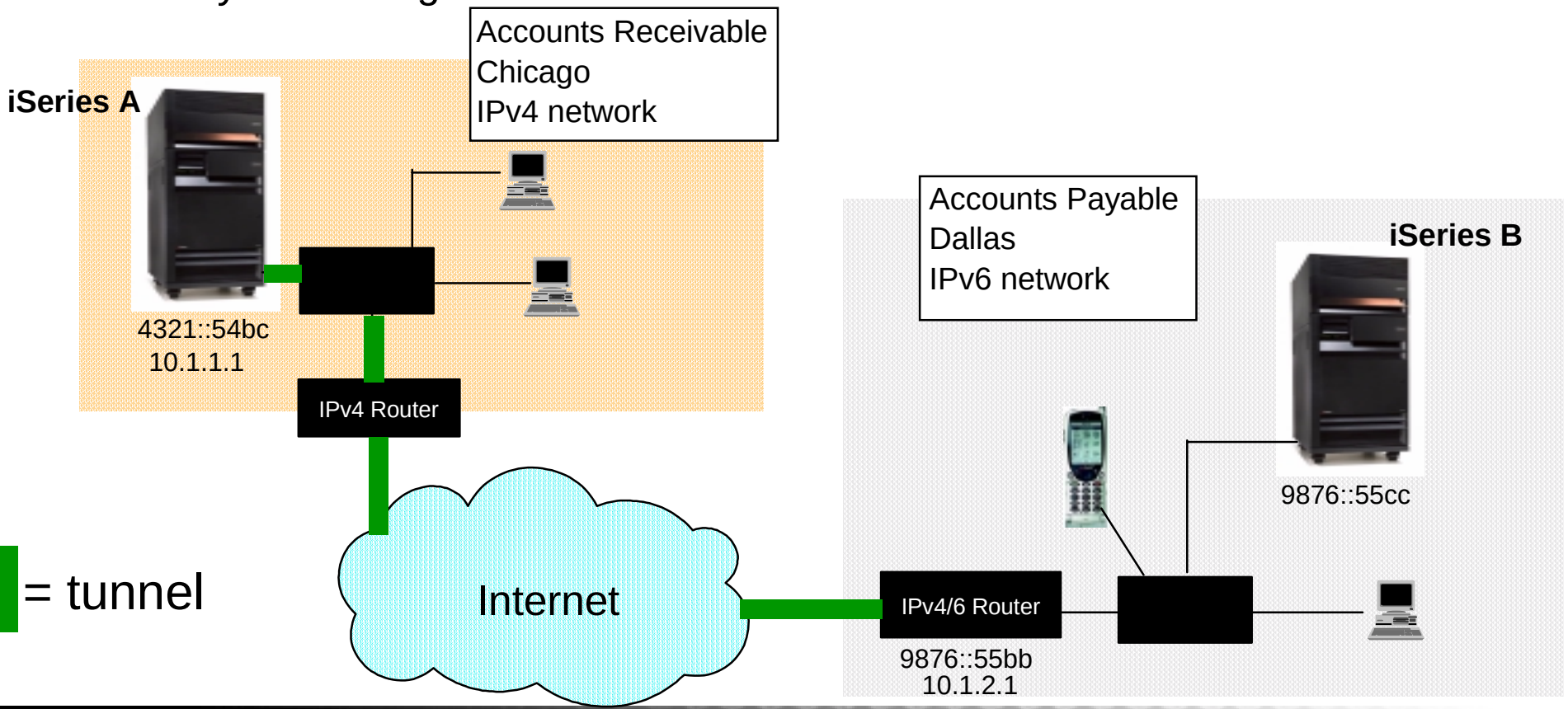
Schedules (time ranges when policies are active) can be specified to span days

Guaranteed connections are specified using integrated service policies. These policies require RSVP(Resource Reservation Protocol)-enabled applications and routers. The routers are signaled before data transfer and the network agrees to and manages (end-to-end) data transfer based on the policy specified using RSVP. There are APIs provided to RSVP-enable your applications. In V5R2, new options were added to the qtoq sockets APIs to simplify the work required to use RSVP on your iSeries system. They call the RAPI under the covers and perform some of the more complex tasks.

Policies are now exported to a LDAP v3 directory server. Using a directory server allows you to share policies across servers, or centralize your data for backup. The wizards will walk you through the directory setup and iSeries Navigator can be used to manage your policies once they are created.

IPv6 Development Platform

- Get Started with IPv6
  - Larger address space
  - "Plug-n-Play" - autoconfiguration
  - "Designed-in" Security
  - Scalability of Routing



Notes: IPv6

IPv6 is the next evolution in Internet Protocol. Most of the Internet currently uses IPv4, but there is a growing shortage of IPv4 addresses as more and more devices (esp wireless) connect to the Internet. IPv6 expands the IP address space from 32 bits to 128 bits. Initially, gaining strong momentum in Asia & Europe.

IPv4 Address Facts...

What percentage of the available IPv4 addresses are in use today? Answer: 75%

True/False, Stanford University has more IPv4 address than China? Answer: True

IPv6 Address Facts...

If every person had their own network, how many addresses could each have? Answer: 18,000,000,000,000,000,000

How many IPv6 addresses could be assigned to each square inch of the earth? Answer: 300

IBM is implementing IPv6 for iSeries over several software releases. In V5R2, IPv6 is provided as an application development platform for the purpose of developing and testing IPv6 applications. IPv6 functions are transparent to existing TCP/IP apps and coexist with IPv4 functions. You configure a line for IPv6 and use sockets API extensions to IPv6-enable applications.

IPv6 tunneling enables the iSeries to connect to IPv6 nodes (hosts & routers) across IPv4 domains. This provides a transitional method of implementing IPv6 while retaining IPv4 connectivity.

In addition to more addresses, IPv6 reduces configuration & management workload via automation.

Stateless Address Autoconfig is the process that IPv6 nodes use to auto config IPv6 addresses for interfaces. It combines an address prefix with either the MAC address of the node or a user-specified interface identifier. The node performs duplicate address detection to verify uniqueness before assigning.

Neighbor Discovery functions are used by IPv6 nodes to discover the presence of other IPv6 nodes, to determine the link-layer addresses of nodes, to find routers that are capable of forwarding IPv6 packets, and to maintain a cache of IPv6 neighbors.

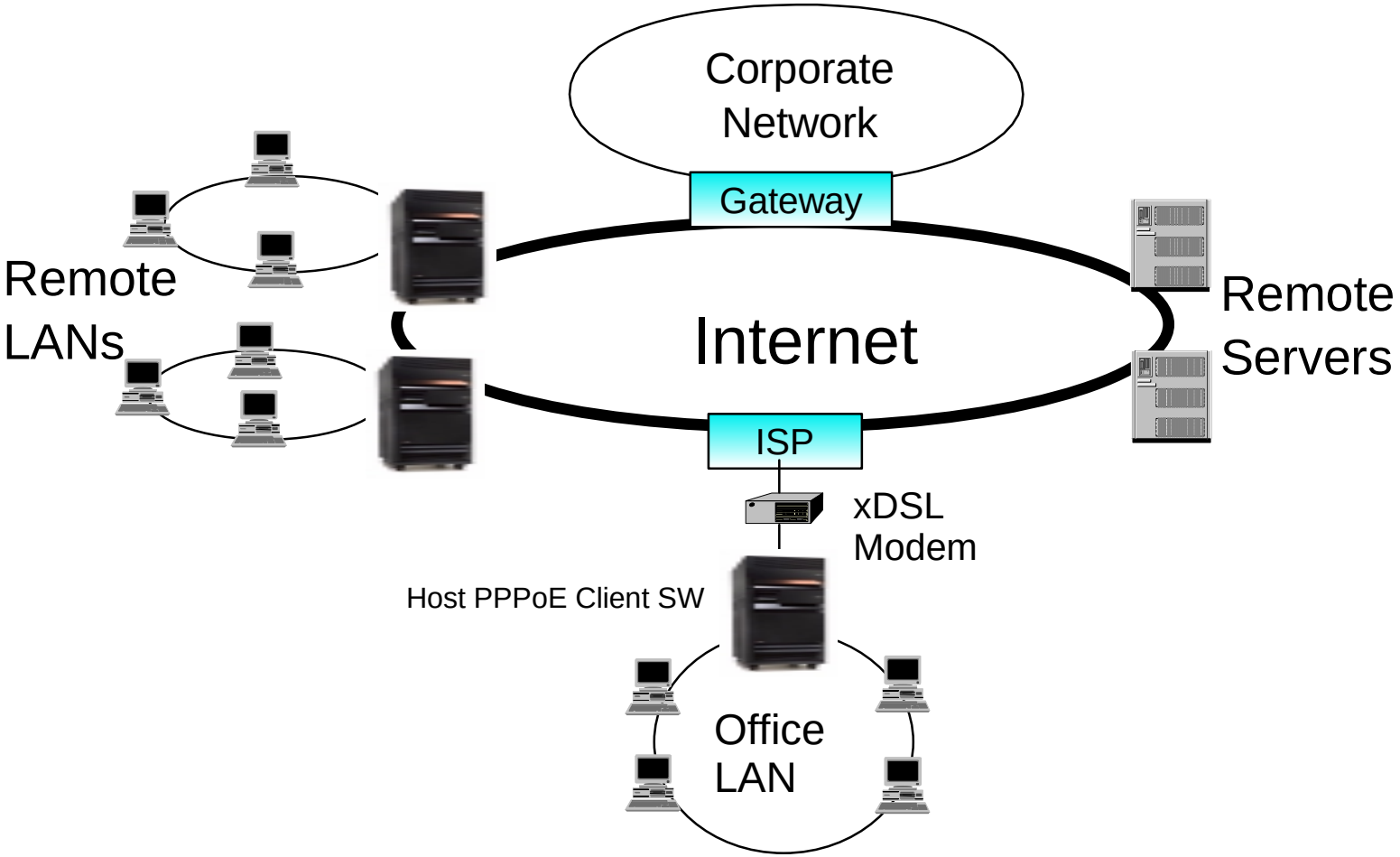
- Uses five Internet Control MessageProtocol version 6 (ICMPv6) messages - RFC 2461

Security - IPSec is mandatory, less likely to be broken by new technologies in the future

Scenario: Your firm uses an accounting application for accounts receivable on the server in its Chicago office. You need to connect the app to a server in the Dallas office. This application uses IPv6 addressing on the servers in both cities. Because your ISP cannot provide IPv6 routers between your two sites, you need to configure a tunnel between your two servers. The application packets travel thru the tunnel, across the IPv4 network between your two servers. In the picture, the 10.x.x.x addresses represent public IP addresses that can be globally routed. You must create a configured tunnel line and several associated routes. The tunnel begins at iSeries A and ends at the IPv4/6 router in Dallas. When the application on iSeries A needs to connect to iSeries B, iSeries A encapsulates the IPv6 packet within an IPv4 packet and sends it over the tunnel to the IPv4/6 router, which decapsulates the packet and forwards the IPv6 packet to iSeries B. The packet returns by taking the reverse path. The tunnel connection is point-to-point, so the remote endpoint of the tunnel must be defined. This is done by creating a route that is associated with the tunnel line. The route defines the remote endpoint as the next hop and the destination address as iSeries B.

Remote Access Enhancements

- Support PPP over Ethernet (PPPoE) for DSL.
- Shared incoming/outgoing access to modems.
- Connect directly to ISP or Corporate Network



Notes: Remote Access

For V5R2, iSeries Navigator can enable PPP over Ethernet (PPPoE) connections originating from the iSeries. PPP (Point-to-Point Protocol) is a TCP/IP protocol used for computers to communicate over the Internet thru phone lines. It is an Internet standard (RFC 1661) and is the most widely used connection protocol among ISPs. In V5R2, you can specify a new PPPoE virtual line type, which is bound to a physical Ethernet line, to establish a PPP connection using an Ethernet LAN adapter attached to a DSL modem. Once the connection between the iSeries and the ISP has started, individual users on the LAN can access the ISP over the iSeries PPPoE connection. PPP allows interoperability among the remote access software of different manufacturers and allows multiple network communication protocols to use the same physical communication line.

Advantages:
- Leverages existing Ethernet infrastructure
- Preservation of Dial model - PPP session-based communication
- Allows multiple PPP sessions to be initiated within home LAN
- enables destination selection

There have also been several additions to iSeries Navigator now make it easier to configure and manage PPP connections.

With V5R2 iSeries runs Host PPPoE Client SW
Requires dedicated 2838 10/100 ethernet adapter

NOTE: Group Policy support enables network administrators to define user based group policies to help manage resources and allows access control policies to be assigned to individual users when logging into the network with a PPP session.

JavaMail™

- Industry standard Java™ APIs for sending and receiving e-mail
- Packaged in IBM Developer Kit for Java
- Supports sending mail from a Java program
  - Simple Mail Transport Protocol (SMTP) - sending e-mail
  - Post Office Protocol (POP3) - receiving e-mail
  - Internet Mail Access Protocol (IMAP) - receiving e-mail
  - Processing and encoding Multipurpose Internet Mail Extensions (MIME) - non-text
- JavaMail™ FAQ available from Sun at http://java.sun.com/products/javamail/FAQ.html

Notes: JavaMail

JavaMail

In V5R2, JavaMail is shipped as part of the IBM Developer Kit for Java. The JavaMail API provides a platform-independent and protocol-independent framework you can use to build Java technology based e-mail client applications. You can use the JavaMail API to create a mail client capable of sending multimedia mail messages, as well as enabling a full fledged IMAP (Internet Mail Access Protocol) implementation supporting folders, authentication, and attachment handling.

Since SMTP only supports character data, it uses MIME to represent complex data such as formatted text, file attachments (text & binary), and multimedia content. If you use the iSeries QTMMSENDMAIL API, your application must take care of converting the data into the appropriate content. The JavaMail implementation provides MIME procesing capabilities natively.

The JavaMail API provides a set of abstract classes that models an e-mail system. The API provides general mail functions for reading and sending mail, and requires service providers to implement the protocols. For example, SMTP is a transport protocol for sending e-mail. Post Office Protocol 3 (POP3) is the standard protocol for receiving e-mail. IMAP is an alternative protocol to POP3. In addition to service providers, JavaMail requires the JavaBeans Activation Framework (JAF) to handle mail content that is not plain text. This includes MIME (Multipurpose Internet Mail Extensions), URL pages, and file attachments.

All of the JavaMail components are shipped as part of the IBM Developer Kit for Java. These components include:

- mail.jar - Contains JavaMail APIs, the SMTP service provider, the POP3 service provider, and the IMAP service provider.
- activation.jar - Contains the JAF.

IBM HTTP Server

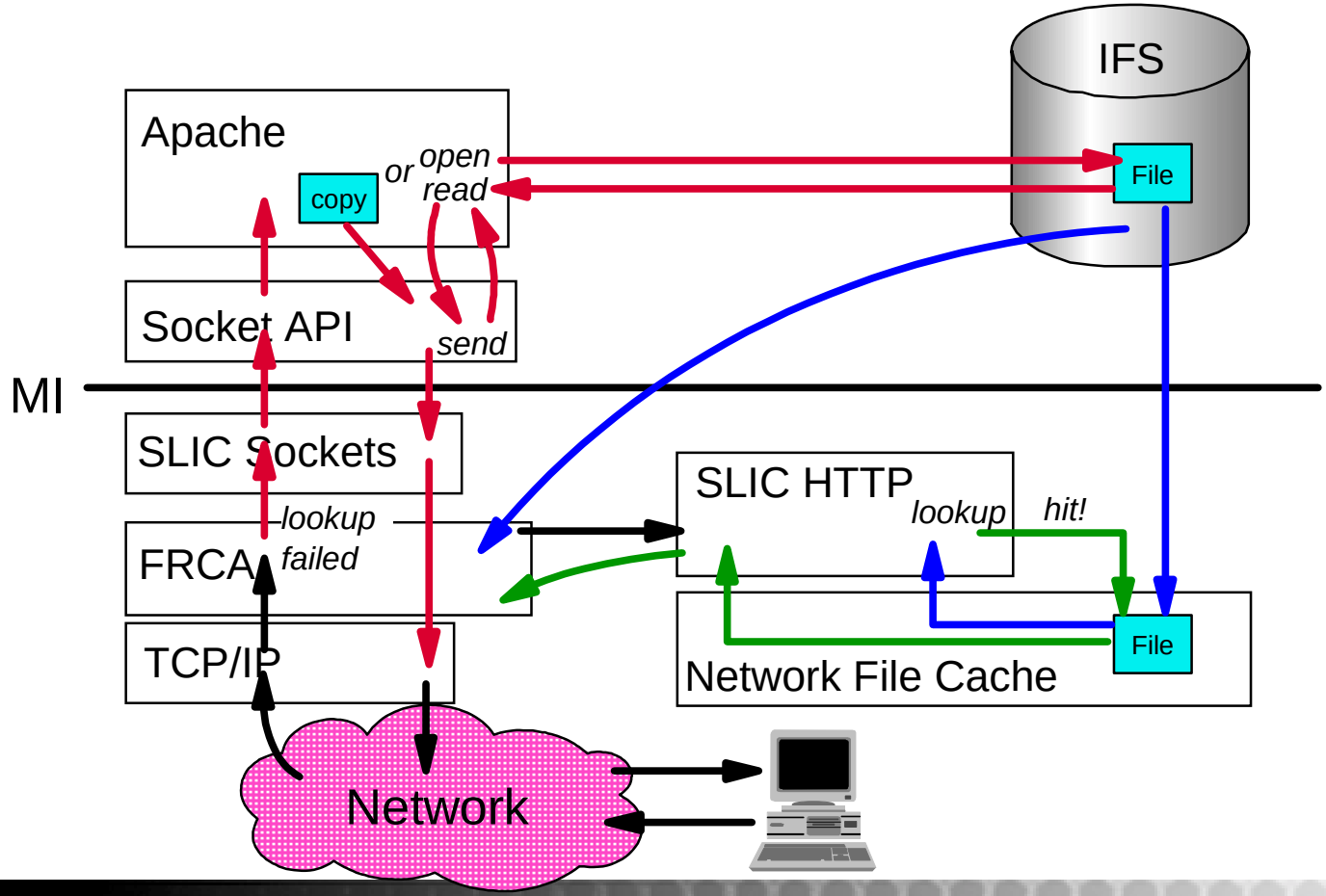
Powered by Apache

IBM HTTP Server - What's new in V5R2

- Performance
  - Fast Response Cache Accelerator (FRCA)
- Business Continuity
  - Highly Available Web Serving
- Improved Management and Usability
  - Log Rollover and Archiving
  - Collection Services
  - Migration
  - GUI Navigation and Accessibility
- Industry Standards
  - TLS Upgrade

Fast Response Cache Accelerator (FRCA)

- More than doubles web serving capacity
- Exploits caching techniques pioneered by IBM Research
- Pre-load Static files, reverse proxy dynamic or remote files



Notes: FRCA

Fast Response Cache Accelerator (FRCA) is caching technology that can more than double capacity for serving static content compared to conventional server architectures and has allowed IBM to establish a leadership position in Web server performance. FRCA is a general purpose architecture that will enable the iSeries to move performance critical TCP/IP Application functions such as HTTP server (Powered by Apache) into lower levels of the operating system, greatly improving web serving performance. The focus in V5R2 is HTTP, however the design will accommodate a variety of TCP servers, even those that don't require the use of the network file cache

Two new components that work together
- Fast Response Cache Accelerator (FRCA)
  - Provides system API set and framework for socket applications
  - Accelerates file serving performance for the HTTP server
  - The *one V5R2* example is the HTTP Server (powered by Apache)
- Network File Cache (NFC)
  - Provides SLIC level cache

Configurable by new FRCA directives in Apache server config
- Can be enabled for each listen port
- Local cache: Specify file name (with wild cards) for "static" content caching
  - When content is updated NFC automatically uses new file
- Reverse proxy cache: Specify URI for "dynamic" or remote content caching
  - Timer used to determine when cached items are stale

No SSL/TLS supported for the FRCA enabled sessions/ports

No authentication protection for the file in FRCA (NFC)
- Contents should be for public access under FRCA

No NLS code page conversion performed
- IFS files are read in binary and loaded into the NFC cache as is

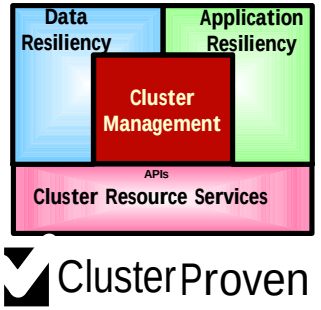
Ability to turn off FRCA without having to comment out numerous local cache or reverve proxy cache directives.

Can limit the size of the Local Cache and files

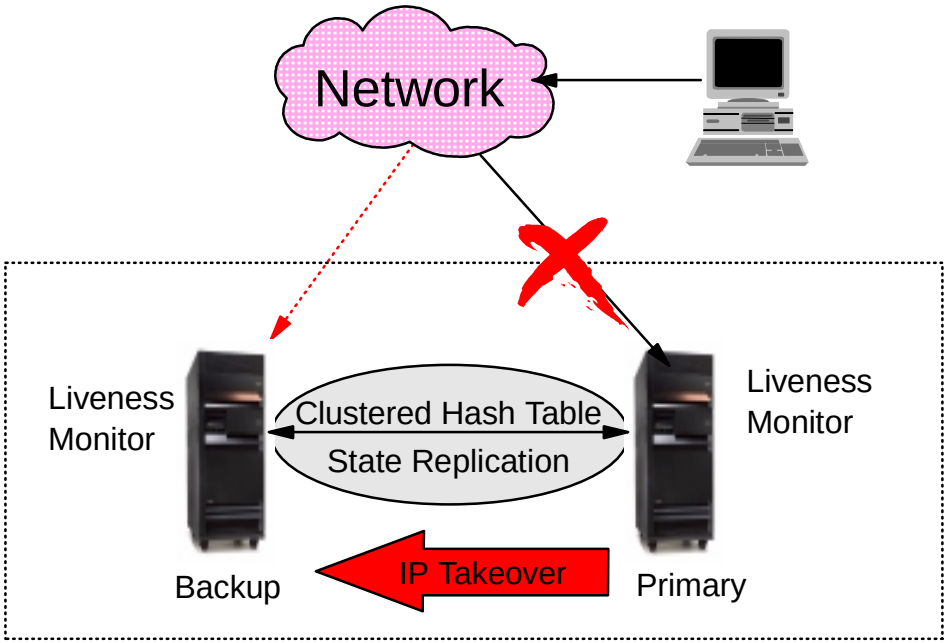
Can define when (startup or runtime) and what files are to be cached in the NFC
- Does not operate recursively through sub-directories

Highly Available Apache Web Server

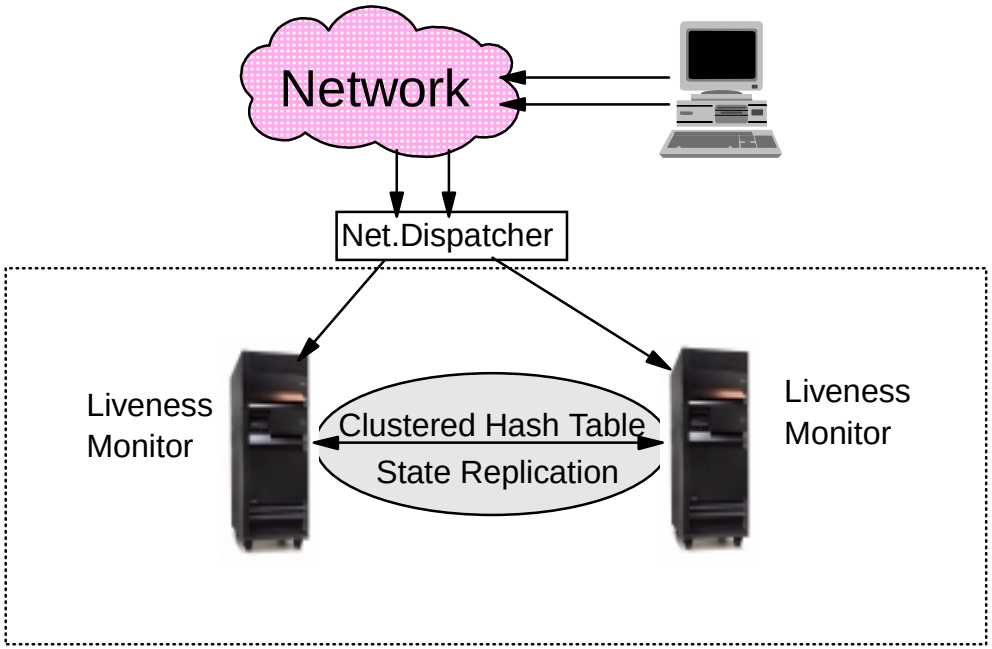
- Exploits iSeries clustering technology
  - Continuously available servers, data, and applications
  - Seamless horizontal growth



Primary/Backup with IP Takeover



Peer-Peer with Network Dispatcher



Notes: Highly Available

As a complimentary addition to our built-in "Hotbackup" capability, the Highly Available HTTP Server (Powered by Apache) takes advantage of iSeries Clustering technology and makes it possible to build a highly available Web site, improving the availability of business critical Web applications built with Common Gateway Interface (CGI) programs. Highly available HTTP servers provide function that monitors a URL that is part of your web site (for example, your home page) and will take recovery action if the web server is no longer serving your web content. For example, the monitor function will try to end and start your web server or may initiate a switch-over to move your HTTP server function to the backup node in the cluster. In addition, you may choose to write your CGI programs using highly available CGI APIs to save CGI state into the iSeries cluster. In the event of a failed node in the cluster, a stateful CGI can maintain its state, even after the application switches to a new node in the cluster.

- Use of high-availability business partner (HABP) software is needed only if data resiliency is required
- Support for different models :
  - Availability
    - Primary/Backup with IP-Takeover
    - Primary/Backup with IBM's e-Network Dispatcher
  - Availability & Scalability
    - Peer with e-Network Dispatcher
- Replication of HA CGI state data
  - CGI programs store Persistent CGI state in Web server
  - State is then available on other nodes in cluster
- Integration with Cluster Resource Services to detect failures.

Improved Management and Usability

- Logging Enhancements
  - Log Rollover
  - Log Maintenance
  - Maximum Log size
  - QSYS logs
- HTTP performance data in Collection Services
- Migration Wizard Improvements
- Improved navigation, usability, and accessibility enhancements for the administration GUI.

Notes: Management

- Log rollover is the ability to automatically close the current log file and open a new one based on a set of user-defined parameters
  - Hourly, Daily, Weekly, Monthly - Default is Daily
- Log maintenance (archival) provides the ability to automatically delete log files based on age, aggregate size, or both
- Maximum log size
- Logging to QSYS source physical files
- HTTP data collection category to contain HTTP performance data for Collection Services. The HTTP performance data can then be queried to analyze HTTP server activity and better understand what types of HTTP transactions are being processed by the iSeries (for example, static files, CGI, or Java Servlets).
- Types of information
  - Number of requests, responses, error responses
  - Processing time
  - Responses served from a cache
  - Number of bytes sent and received
- Running counters
  - Compare intervals to determine what occurred since the last interval
- Finishing to migrate all original server directives
  - Highly Available, Log rollover and archiving, Proxy, Protection setups, Virtual hosting, Server Side Include (SSI)
- Adding a new request routing directive, Map, to eliminate ordering problems with request routing differences
- Also adding a decision point - Do you want the migration wizard to migrate request routing directives

HTTP Server for iSeries

Welcome | Setup | Manage | TCM | Related Links

Server: MAPTEST - Apache Server area: Global configuration

Stopped

- Tasks and Wizards
  - Create new HTTP Server
  - LDAP Configuration
  - Add a Directory to the Web
  - Servlet and JSP Enablement
- Server Properties
  - General Server Configuration
  - Container Management
  - Virtual Hosts
  - URL Mapping
  - Request Processing
  - HTTP Responses
  - Content Settings
  - Directory Handling
  - Security
  - Dynamic Content and CGI
  - Logging
  - Proxy
  - System Resources
  - FRCA
  - ASF Tomcat Setup task
  - ASF Tomcat Settings
- Tools
  - Display Configuration File
  - Edit Configuration File
  - Directive Index

All servers -> MAPTEST

Manage Apache server 'MAPTEST'

This "Manage" tab allows you to manage your Apache and Original servers, as well as out-of-process ASF Tomcat servers.

Server and Server area

Select a particular server or "All servers" to manage. When an Apache server is selected, the "Server area" will show the area of the server that you are managing.

Status

This is where you see the current status of the server and can start, restart and stop the server or refresh the status display.

Tasks and Wizards

Look here for common tasks and wizards.

Server Properties

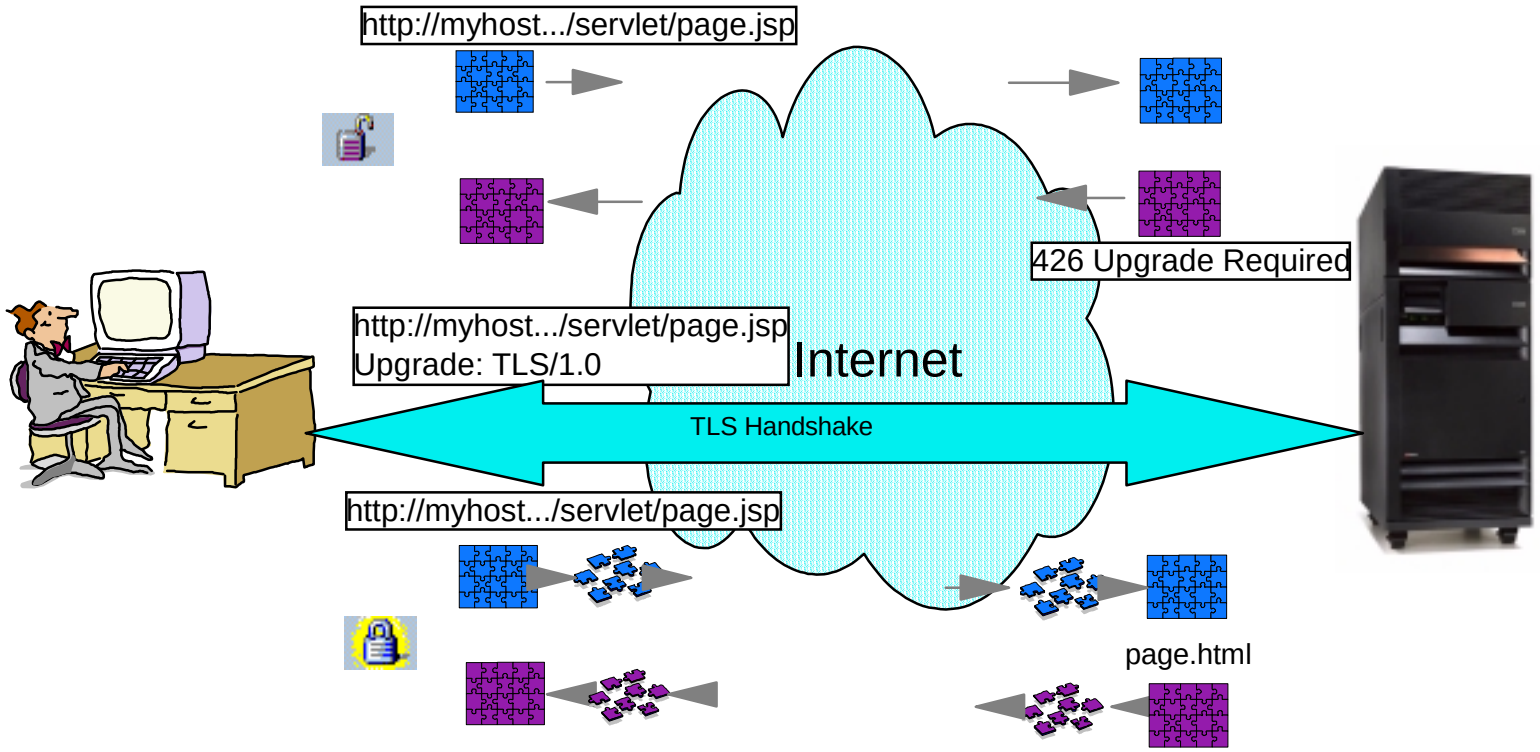
Manage detailed settings for a variety of areas. Hover over each form to learn more about what each one provides.

Tools

Work with these tools to trouble-shoot problems and learn how this console works "under the covers."

TLS Upgrade

- **RFC 2817**
- **Client or server can request an upgrade to TLS encryption on an existing unencrypted connection**
  - First user is Internet Print Protocol (IPP)
- **New applications only need one port for both normal and SSL traffic**



Notes: TLS Upgrade

The historical practice of deploying HTTP over SSL3 has distinguished the combination from HTTP alone by a unique URI scheme and TCP port number. The scheme 'http' meant HTTP alone on port 80 (by default), while 'https' meant HTTP over SSL on port 443 (by default). Other protocols follow a similar pattern. The IESG decided back in 1997 to deprecate the practice of issuing parallel "secure" port numbers to preserve the available well known ports. New application protocols built atop HTTP, such as the Internet Print Protocol are requiring the capability to use the same port and connection for both HTTP and HTTP over SSL traffic.

The Upgrade mechanism also solves the "virtual hosting" problem. Rather than allocating multiple IP addresses to a single host, an HTTP/1.1 server will use the Host: header to disambiguate the intended web service. As HTTP/1.1 usage has grown more prevalent, more ISPs are offering name-based virtual hosting, thus delaying IP address space exhaustion. TLS and SSL have not been able to take advantage of this since the initial handshake does not specify the intended hostname, relying exclusively on IP address. Using the HTTP/1.1 Upgrade: preamble to the TLS handshake -- choosing the certificates based on the initial Host: header -- will allow ISPs to provide secure name-based virtual hosting as well.

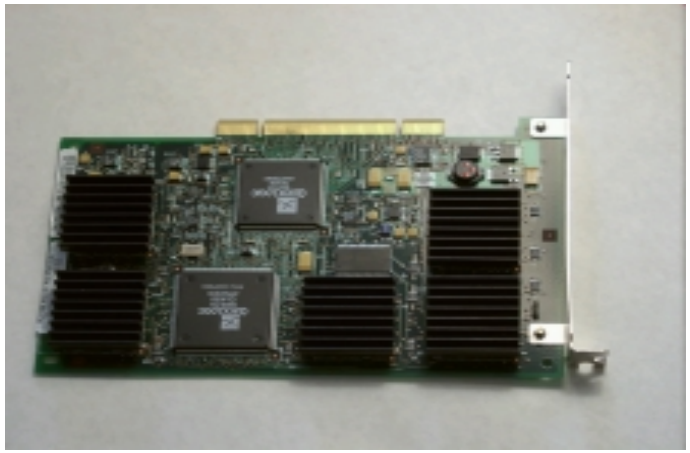
The new RFC describes the HTTP/1.1 Upgrade: header, the TLS/1.0 Upgrade token, and a new HTTP Status Code, "426 Upgrade Required" to allow either the client or the server to indicate that a TLS-secured connection is desired or necessary.

Cryptography and Security

Cryptography and Security - What's new in V5R2

- SSL/TLS Performance
  - New Cryptographic Hardware
  - Global Secure Toolkit (GSKit API)
- Interoperability
  - Enterprise Identity Mapping (EIM)
  - Network Authentication Service
- Business Continuity
  - Object Signing and Signature Verification
  - Directory Services (LDAP) Secure Store

SSL/TLS Performance



- Crypto Hardware
  - New 2058 Cryptographic Accelerator
    - Faster high volume SSL transactions
    - Private key in system keystore
  - Existing 4758 Crypto Copressor
    - Store keys in hardware -- more secure
  - Transparent to the application (just faster!)
- New OS/400 Global Secure Toolkit (GSKIT) API for creating asynchronous SSL sessions
  - Can provide better throughput when incoming requests are high and require multiple jobs

Notes: SSL/TLS Performance

Cryptography is the art and science of keeping data secure. Since V4R5, you can use the 4758 Cryptographic Coprocessor along with DCM to generate and store private keys associated with SSL digital certificates. In addition, the 4758 Coprocessor provides a boost in performance by handling SSL private key processing during SSL session establishment.

In V5R2, the IBM 2058 e-Business Cryptographic Accelerator is available in addition to the 4758 Coprocessor. It is designed to improve iSeries SSL/TLS performance by rerouting the processing of private keys away from the system processors, improving SSL throughput by over 7 times. It is easy to install and initialize, but is limited in its configuration options that the 4758 Coprocessor offers.

Utilizes cryptography assist hardware to optimize Secure Socket connections - results in 1000's of "handshakes" a second

Multiple accelerators can be employed per system to increase total throughput

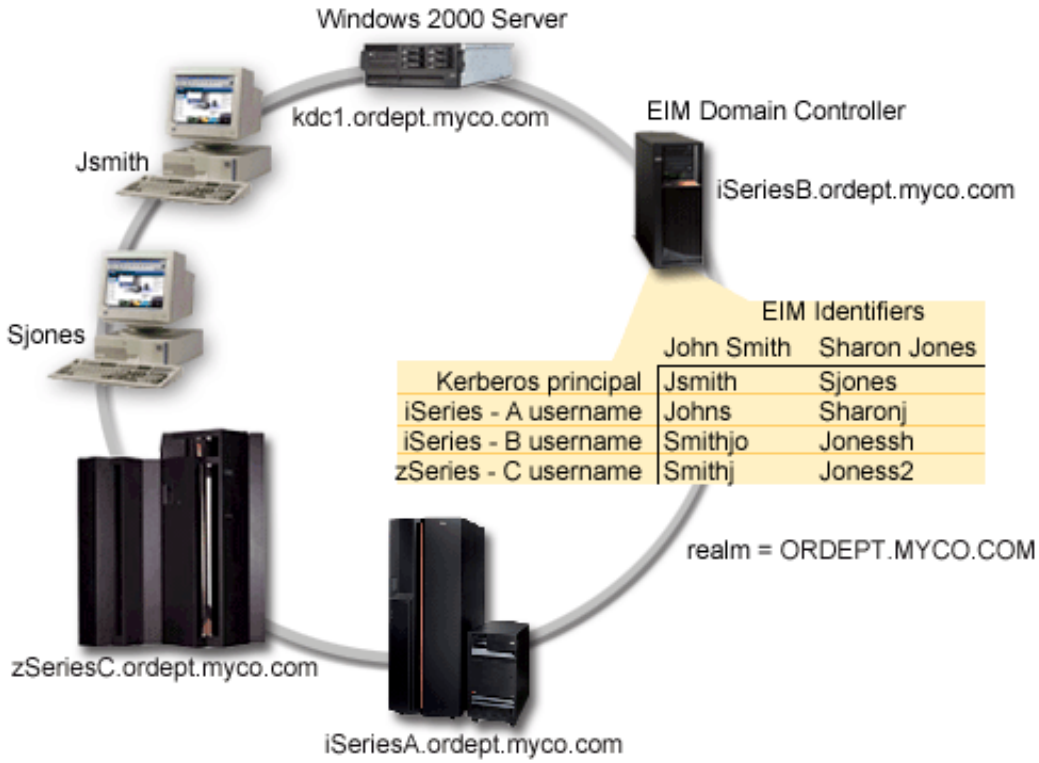
Easily configured - integrated with iSeries security administration

You can now use a new OS/400 Global Secure Toolkit (GSKit) API to create an asynchronous instance of a SSL session. This API provides a secure connection for handling multiple clients or if the number of incoming requests are high and require multiple jobs. Asynchronous I/O APIs provide a method for threaded client server models to perform highly concurrent and memory efficient I/O. There were typically two models previously, the first dedicated one thread per client connection. This consumes too many threads and could incur a substantial sleep/wakeup cost. The second minimizes the number of threads by issuing the select() API on a large set of client connections and delegating a readied client connection to a thread. In this model, you must select or mark on each subsequent select, which can cuase a substantial amount of redundant work.

Asynchronous I/O and overlapped I/O resolves both problems by passing data to and from user buffers after control has been returned to the user application. Asynch I/O notifies these worker threads when data is available to read or when a connection has become ready to send. Since copying to and from user buffers occurs asynchronously to the processes, wait time for client request diminishes. Note: the IBM HTTP Server was enabled for Asynch I/O in V5R1. Domino also uses the technology.

Security Interoperability

- **Enterprise Identity Mapping**
  - The industry's first Enterprise Identity Mapping implementation
  - Simplifies authentication process for users
  - Enables single signon
  - Reduces costs of user identity, password and network administration
  - Simplifies the development of multi-tier, multi-server applications
- **Network Authentication Service**
  - Kerberos Participation



Notes: Security Interoperability

Most computer users today access multiple servers and applications with different user identities and passwords. As a result, the most common help desk call is to reset a password driving up the cost of security administration. Aside from complex security administration, there is also no common standard today for application developers to enable security, resulting in unique and complex implementations of user registries and security semantics for each major application..

OS/400 V5R2 delivers the first implementation of Enterprise Identity Mapping (EIM), a self-protecting security element of IBM's Project eLiza. EIM is a mechanism for mapping (associating) a person or entity to the appropriate user identities in various registries throughout the enterprise, helping customers reduce the cost of security administration. iSeries Navigator provides GUI and a configuration wizard to help you in configuring and managing EIM. You can also use iSeries user management to manage the EIM relationships for user profiles. The iSeries system uses EIM to enable OS/400 interfaces to authenticate users with network authentication service and Kerberos authentication. The iSeries operating system and applications can accept Kerberos tickets and use EIM to map to a user profile on the system that is associated with the Kerberos principal.

EIM also provides an infrastructure that lowers the expense for application developers because they can easily and inexpensively build applications that participate in a single sign-on environment, regardless of platform. OS/400's exploitation of EIM and Kerberos, along with exploitation by other e(logo)Server and IBM software, provides single sign-on capabilities at the operating system layer in addition to the application layer. Single sign-on capabilities provide users, administrators, and application developers with the benefits of easier password and user identity management across multiple platforms -- without forcing administrators to use multiple sets of security controls for a single resource.

Network authentication service - You can use the Network Authentication Service wizard to easily configure an iSeries server to participate in a Kerberos network. The Kerberos protocol, developed by MIT, allows a principal (user or service) to prove it's identify to another service (a key distribution center or KDC) within an insecure network. The KDC authenticates a user with a Kerberos ticket which proves the principal's identity throughout the network. The new wizard allows you to configure the iSeries server to participate in the Kerberos realm. Using the Kerberos protocol, tickets can then be passed to services on a user's behalf, authenticating the user to resources on the network. Users can request and work with tickets by using Qshell commands. And, you can now use the kpasswd command to change users' passwords on the key distribution center. In addition to Windows® 2000, XP, AIX® and zSeries™, several iSeries applications provide Kerberos authentication support in V5R2: SQL, DRDA, iSeries Access, iSeries Access Host Servers, and QFileSvr.400.

Business Continuity - Security Enhancements

- Object Signing and Signature Verification
  - iSeries Navigator Object Signing Function
    - Use Mgmt Central Product Definition Wizard to sign objects packaged for distribution
  - Sign command (*CMD) objects
  - New signing and verification APIs
    - Sign buffer
    - Verify buffer
    - Add Verifier
- Directory Services (LDAP) Secure Store

Notes: Business Continuity - Security Enhancements

Digital signatures on OS/400 objects ensures the integrity of software and data. Business partners, customers, as well as IBM can sign information to provide improved integrity in their products.. With digital signatures, data tampering, virus introduction, or any modification to an object can be detected. The signature also provides positive identification of the originator of the data or software. The infrastructure and APIs for signing programs were provided in V5R1 and OS/400 itself was signed. In V5R2, more general-purpose objects can be signed, such as program data, command (*CMD) objects, digital receipts, and B2B transactions.

In V5R2, you can:

- use the Management Central product definition wizard to sign objects that you package for distribution to iSeries endpoint systems
- sign command (*CMD) objects - you can sign an entire *CMD object or sign only the core components of a *CMD object. You can do this through DCM.
- New signing and verification APIs allow a program to sign & verify signed objects.
  - Sign Buffer (QYDOSGNB, QydoSignBuffer) - allows the local system to digitally sign a buffer & returns the digital signature to the caller. You could use this API to sign part of an XML file and store the signature in another part of the XML file. Or you could read database file records into a buffer and sign them.
  - Verify Buffer (QYDOVFYB, QydoVerifyBuffer) - allows the local system to verify the digital signature on a previously signed buffer.
  - Add Verifier (QYDOADDV, QydoAddVerifier) - adds a certificate to a system's *SIGNATUREVERIFICATION certificate store. The system uses this to verify signatures on objects that the certificate created. - Certificate Authorities are not allowed to be added via this API. To prevent anyone from using this API, disable it using SST to disallow changes to security-related system values.

You can sign any object (*STMF) in IFS. If the object has an attached Java program, the program will also be signed. You can sign these objects in QSYS.LIB: *PGM, *SRVPGM, *MODULE, *SQLPKG, *SAVF, *CMD

Objects must be local (not QNTC - IXS file system)

Directory Services (LDAP) had several enhancements in V5R2. New integrity enhancements were made to further protect any data stored on the directory server, making it a secure store for the enterprise that can now be exploited in more situations. It can be used as a domain controller for EIM, and several usability enhancements have been made.

IBM DB2 UDB

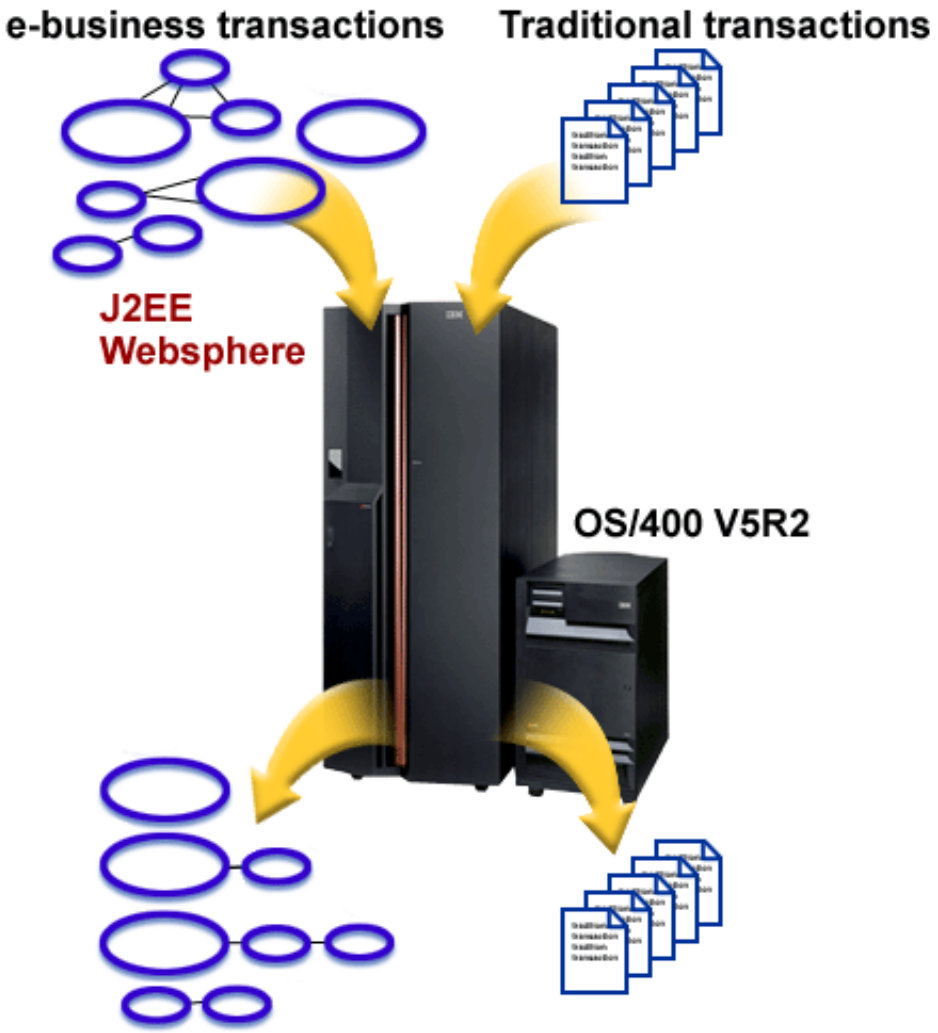
Enterprise Class Adaptive e-transaction Services

iSeries optimized for both traditional and e-business transactions

Adaptive e-transaction Services

- Extends robust iSeries transaction services to e-business applications
- Transaction server automatically adapts to application requirements
- No programming changes required

Further optimizes iSeries for highly scalable WebSphere and Java™ transaction performance



Notes: Enterprise Class Adaptive e-transaction Services

The iSeries and AS/400 reputations as business servers have largely been built around their ability to process transactions. OS/400 has always featured a sophisticated transaction manager, and has been optimized to manage multiple applications transactions together with advanced workload management tools such as subsystems and dynamic performance management.

Many commercial applications, such as those in the banking, manufacturing or distribution industry. fit a common profile: small, single threaded order entry or account transactions that write an update to a single file in the database. Many of today's e-business transactions running in WebSphere Application Server and using Java are much more complex, require more processor and memory resources and often spawn multiple other tasks to complete the transaction.

The new adaptive e-transaction services is designed to enable OS/400 to adapt and self-optimize for both traditional transactions and new e-business applications. Now OS/400 has the ability to detect the transaction type and automatically adapt its transaction manager as appropriate. Traditional transactions will detected and handled as before, with no degradation in performance. When detecting a more complex, e-business transaction, however, the OS/400 transaction manager will automatically adapt to process multiple tasks.

The result is that WebSphere and Java transactions will now benefit from better operating system optimization and gain higher performance.

IBM DB2 UDB for iSeries

Availability enhancements

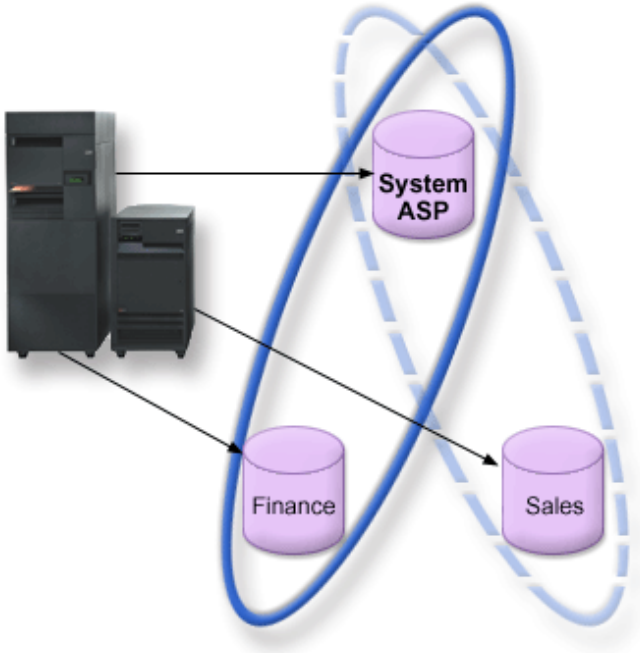
- Multiple independent name spaces
- Switched disk (IASP)

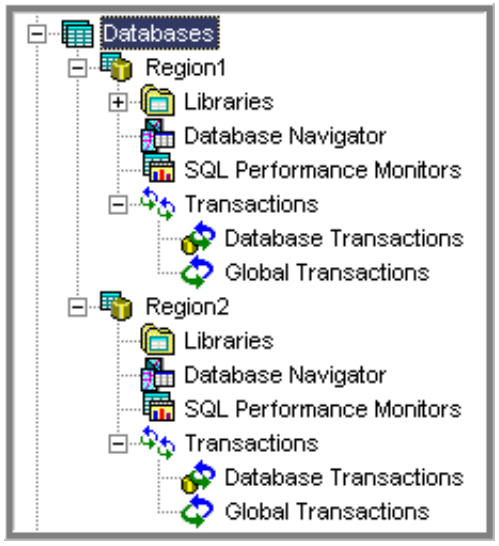
Open standards support

- SQL enhancements
- Java Transaction API (JTA)
- X/Open Distributed Transaction Processing (XA-DTP)
- Enhanced DB2 UDB family compatibility

iSeries Navigator Enhancements

- Self-optimizing automatic index advisor and statistics collection
- Graphical management for local DB2 UDB and global WebSphere transactions





Notes: IBM DB2 UDB for iSeries

In V5R1, we introduced Independent Auxiliary Storage Pools (IASPs) to support switch disk capability for application using the integrated file system, such as Domino and Windows servers. With OS/400 V5R2, this capability is extended to support database objects. Support for multiple independent name spaces allows multiple databases in separate storage pool on iSeries.

V5R2 is also a significant release for the iSeries as it continues to be at the forefront of meeting the requirements of open SQL standards, along with much greater compatibility between IBM DB2 UDB on iSeries and with DB2 UDB on our other IBM platforms.

New DB2 transaction services provide consistency for two established e-business industry standards - the x/Open Distributed Transaction Processing (XA-DTP) standard, and the Java Transaction Services API (JTS). Products like WebSphere Application Server should show performance improvements because of how we are handling multiple jobs using the new adaptive e-transaction services.

iSeries Navigator also provides a graphical view of database or global transactions. Database transactions are transactions that are local jobs using the iSeries database. These transactions are completely under the control of the application running within a single job. They would typically use SQL statements begin, followed by commit or rollback to identify transactional work. Global transactions may span multiple jobs, databases, or systems. These transactions are coordinated by an external Transaction Manager, such as WebSphere or Tuxedo. They use a standard set of APIs, such as the APIs defined in the XA or JTA specifications to identify transactional work.

e-Output

iSeries e-Output

InfoPrint Server for iSeries

- New PDF and e-mail capabilities

InfoPrint Designer for iSeries

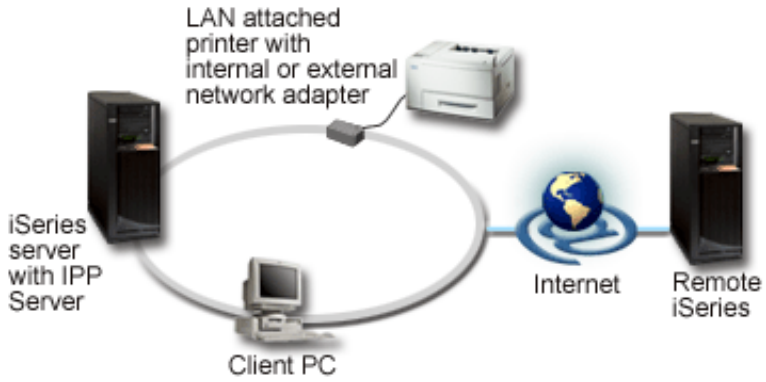
- Enhanced graphical output design

e-Output server in OS/400

- PDF output distribution integrated with iSeries Access
- Standard API access to PDF and e-mail functions
- Internet Print Protocol (IPP)

Infoprint 85 and 105 printers

- Supported with Print Services Facility for OS/400



Notes: iSeries e-Output

Infoprint Server is focused on enterprise and e-business driven output management. On the e-output side, Infoprint Server provides PDF and portable AFP support for the iSeries. Any standard iSeries-AS/400 output format can be transformed into PDF. The PDF is text-based, fully navigable, and provides high-performance. In addition, you can segment an output file, triggering the PDF server to create multiple PDF files - this is an "electronic burst and bind" function. In addition, e-mail options are fully integrated and automated so that output files can be transformed to PDF and automatically sent to any destination .

Infoprint Server is also focused on allowing the iSeries to manage network output. Infoprint Server provides transforms for PCL, Postscript, and PDF into AFP so output generated in those formats can be brought into the iSeries and effectively managed to the printer.

Infoprint Designer for iSeries provides a fully-graphical document composition interface to the iSeries-AS/400 printing and e-output system. It supports the requirements of today's complex documents and reports, producing fully electronic documents combining data, text, electronic forms, graphics, image, bar coding, and typographic fonts. Infoprint Designer for iSeries can be used for the design of new output applications or the re-engineering of existing applications.

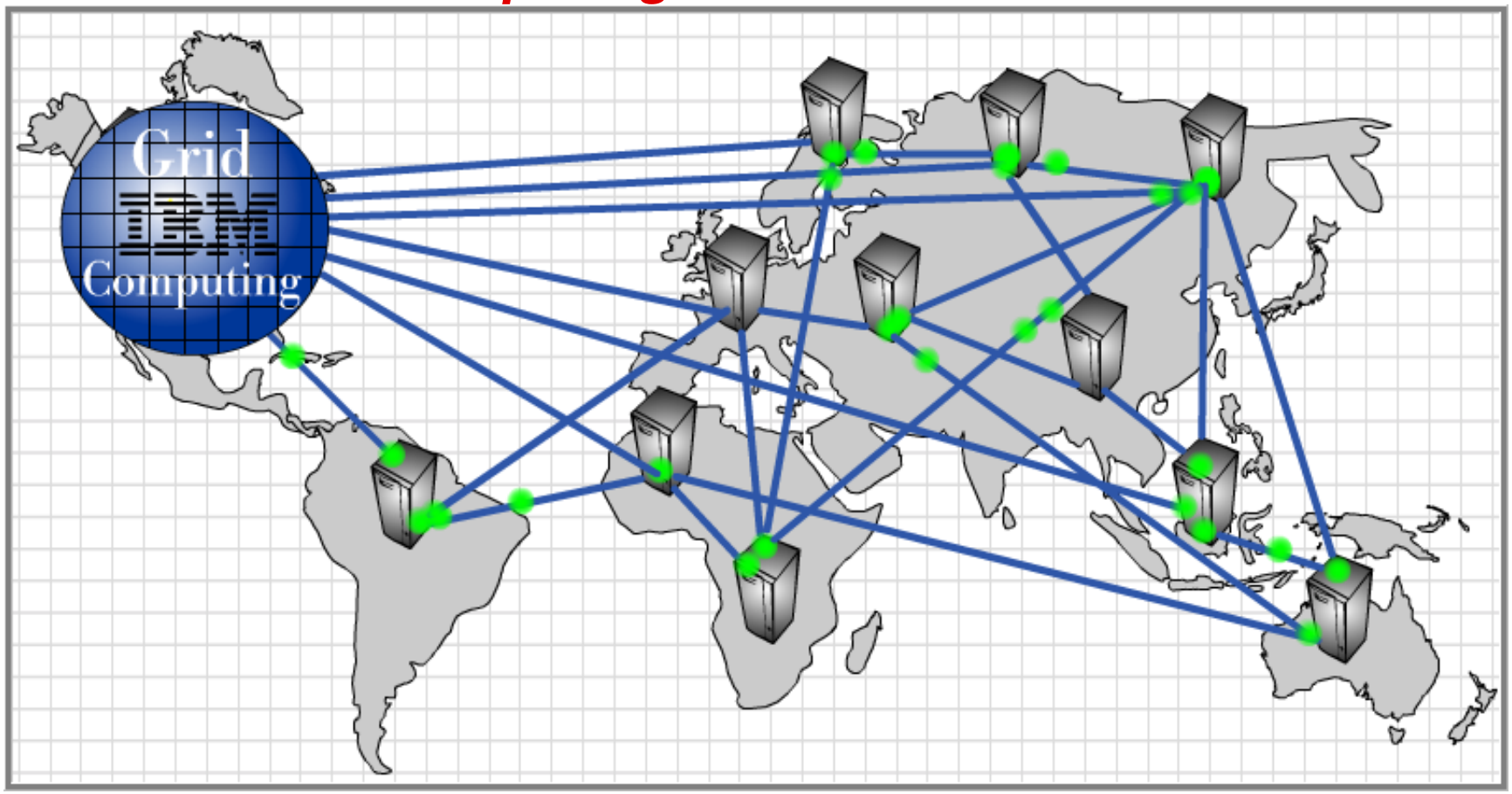
IPP is the emerging standard for Internet printing, allowing you to submit print jobs direct to a URL anywhere in the network. With V5R1, the iSeries enabled IPP (Internet Print Protocol) server support and with V5R2 IPP client support is now enabled.

The Future....

GRID Computing

Project eLiza

iSeries and Grid Computing



Flexible, secure, standards-based access to shared computing resources

iSeries support signals growth of commercial grid applications

OS/400 V5R2 provides support for Globus Toolkit J

Available with OS/400 PASE or Linux

Notes: iSeries and Grid Computing

Grid is a further stage in internet evolution -- the ability, using a set of open standards and protocols, to gain access to applications and data, processing power, storage capacity and a vast array of other computing resources over the Internet. Just as the user looks at the Internet and sees content via the World Wide Web, the user looking at a Grid sees essentially one, large virtual computer.

IBM's focus is to extend the technology used to today's Grid computing implementations that primarily address the needs of very specialized scientific and engineering applications environments to the robust infrastructure needed to support commercial applications enabling them to harness the full potential of the Internet. To accomplish this, IBM intends to collaborate with the Grid community, such as Globus, to establish an open architecture which provides resource aggregation across a heterogeneous set of servers and software, providing the qualities of service necessary to meet commercial application demands.

Project eLiza, IBM's initiative to provide self managing systems, is a key element of enabling Grid computing for commercial applications. Project eLiza is focused on delivering end-to-end systems management and self optimization across the entire IT infrastructure. This capability will allow a variety of dissimilar systems to be aggregated and shared in a transparent manner. Using industry standard interfaces allows the entire suite of organizational resources to be included and shared creating a Grid environment across all the servers and systems within the IT infrastructure.

Grid computing will continue to evolve, and shows the potential of running commercial applications across the virtual organizations. The iSeries is poised to take advantage of Grid Computing as business applications are made available. Research and development to exploit Grid computing has already started in the Development Laboratory, as demonstrated by the recent successful connection of iSeries to the IBM BlueGrid using the Globus Toolkit through OS/400 Portable Applications Solutions Environment (OS/400 PASE), and iSeries PowerPC Linux.

For more information on Grid computing, see: http://www.globus.org , http://www.gridforum.org , http://www.gridcomputing.com/

Project eLiza

OS/400 exploits IBM's blueprint for self-managing systems

- Self-protecting
  - Enterprise Identity Mapping
  - Digital signatures and intrusion detection
- Self-optimizing
  - Dynamic LPAR
  - Self-learning DB2 UDB Automatic Index Advisor
- Self-healing
  - Switched disk support for improved availability
  - Agent Building Learning Environment (ABLE) for problem management*
- Self-configuring graphical wizards for managing
  - Performance and multiple workloads
  - Switched disk clusters and high availability
  - Security and network
  - Storage and system backups

Notes: Project eLiza

Many of the founding elements for Project eLiza already manifest into today's iSeries systems. One year after announcing Project eLiza initiative to develop self-managing for Autonomic Computing[1], iSeries continues to exploit IBM's blueprint for delivering technology and tools to ease management of systems.

V5R2 continues to build on many of eLiza elements that were available with V5R1 such as, such as self-optimizing dynamic LPAR and workload management, self-configuring graphical wizards, self-healing performance monitors, and self-protecting digital certificates. Extensive additional graphical wizards have been added with V5R2 to the iSeries Navigator to automate several complex configuration tasks along with increased flexibility to monitor and manage storage, jobs, and database tasks.

Some of the highlights for V5R2 include:

- Self-protecting Enterprise Identity Mapping for easing user identity management
- Self-protecting Digital certificate APIs for ISV applications to assist with unauthorized application modifications
- Self-optimizing dynamic LPAR to allow resource movement for virtual processing units between Linux and OS/400 partitions
- Self-optimizing index advisor and statistic collections for DB2 UDB for OS/400, allowing users to avoid manual tasks associated with SQL optimization
- Self-healing Independent disk pools for switched disk clustering
- Self-healing Agent Building Learning Environment (ABLE) enablement through building intelligent agents on the iSeries to assist with problem determination and diagnosis processes. The ABLE research project is made available by the IBM T. J. Watson Research Center. For additional information, see: http://www.alphaworks.ibm.com/tech/able
- Extensive self-configuring graphical wizards to simplify network, performance, security, storage, work management and LPAR configuration tasks.

Note 1: Autonomic Computing reflects a vision to develop and deploy intelligent systems that self manage and regulate themselves, much the way the human autonomic nervous system manages the human body. This vision is motivated by the tremendous complexity in today's computing environments and the resultant difficulties, and expense, of managing them. The biological metaphor suggest a systemic approach, coordinating activity across the many components of computing systems, achieving a much higher level of automation. For a complete discussion of the autonomic computing direction see the Autonomic Computing Manifesto (http://www.research.ibm.com/autonomic/manifesto/).

Enterprise IT Management Made Simple

Capacity Upgrade on Demand

OS/400 V5R2

WebSphere Development Studio

64-Bit Linux

32-way, 64-Bit POWER4 i890

Enterprise Identity Mapping

Adaptive e-transaction Server

Innovative Technology

Application Flexibility

Apache Web Caching Accelerator

Lotus Domino 6

Virtual Ethernet

Switched Disk Clustering

iSeries Navigator

Microsoft[7] Cluster Service

SAN Switch Fabric

OS/400 PASE with AIX 5L

Secure Sockets Accelerator

Wireless-Web Micro Edition

LPAR Sub-capacity Pricing

New Tools for e-business

Multiple DB2™ UDB Namespaces

Project eLiza

WebSphere Portal Server

iSeries Access for Web

DB2 UDB Open SQL Standards

Trademarks and Disclaimers

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.
The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

400	BRMS	Host Integration Series	JustMail	Payment Manager	Stylized e
ADSTAR	Client Series	Host on Demand	MQSeries	Payment Server	SystemView
Advanced Function Printing	ClusterProven	Host Publisher	MQSeries Integrator	PCOM	VisualAge for Java
AFP	CODE/400	HTTP Server for AS/400	Net.Commerce	PowerPC	VisualAge for RPG
AIX	DataGuide	IBM	Net.Data	PowerPC AS	WebSphere
AnyNet	DB2	IBM Logo	Netfinity	Print Service Facility	WebSphere Advanced Edition
Application Development	DB2 Extenders	IBM Network Station	NetView	pSeries	WebSphere Commerce Suite
APPN	DB2 UDB for AS/400	Information Warehouse	NUMA-Q	PSF	WebSphere Development Tools for AS/400
AS/400	DB2 Universal	Integrated Language Environment	OfficeVision	S/390	WebSphere Standard Edition
AS/400e	e-business logo	Intelligent Printer Data Stream	OS/2	SanFrancisco	Workpad
AT	e(logo) Server	IPDS	Operating System/400	Screen Publisher	xSeries
BrioQuery	Enterprise Storage Server	iSeries	OS/400	SmoothStart	

cc:Mail, Domino.Doc, Freelance, LearningSpace, Lotus, Lotus Domino, Lotus Notes, iNotes, QuickPlace, Sametime, and Word Pro are trademarks of Lotus Development Corporation in the United States, other countries, or both.
Tivoli and NetView are trademarks of Tivoli Systems Inc. in the United States, other countries, or both.
C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
PC Direct is a trademark of Ziff Communications Company in the United States, other countries, or both and is used by IBM Corporation under license.
ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.
IBM's VisualAge products and services are not associated with or sponsored by Visual Edge Software, Ltd.
Linux is a registered trademark of Linus Torvalds.
UNIX is a registered trademark of The Open Group in the United States and other countries.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
Other company, product and service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.