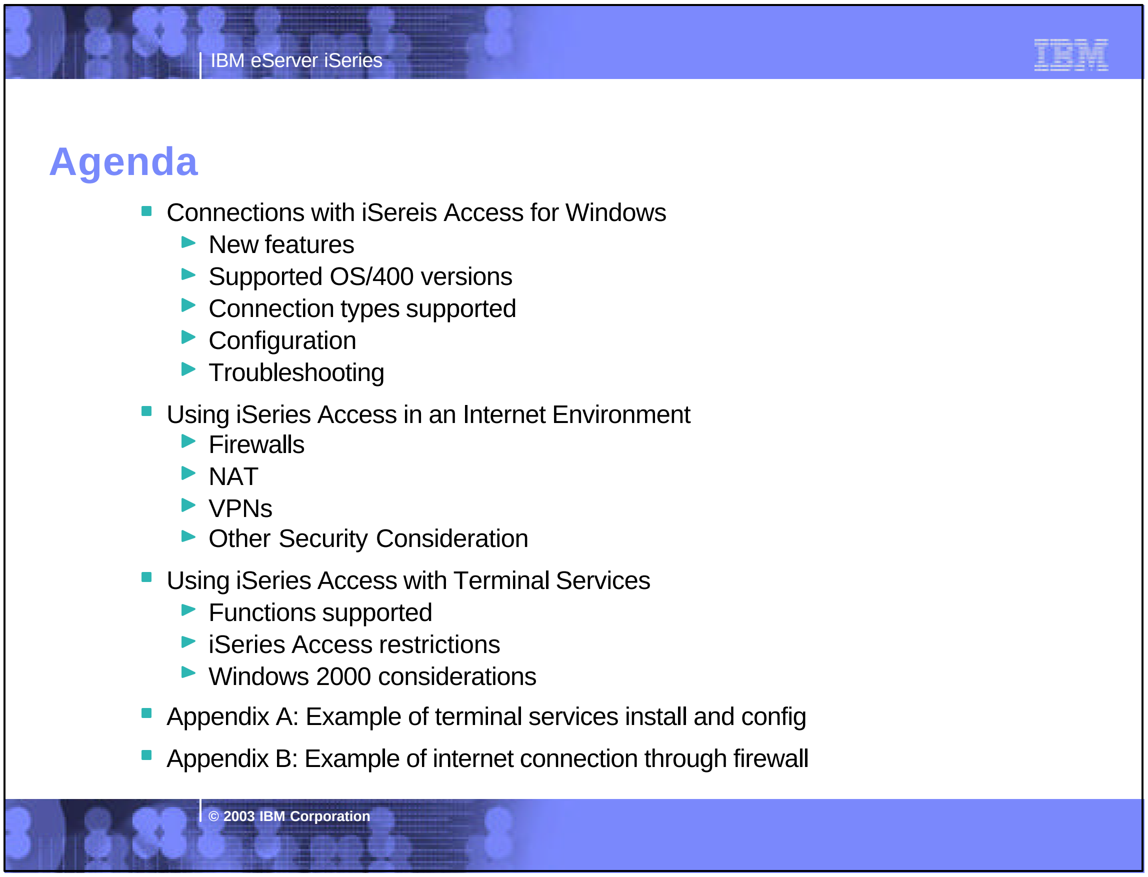
IBM eServer J iSeries J

Session: 403971

iSeries Access Connectivity Environments

Jeff Van Heuklon
www.as400.ibm.com/clientaccess

This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.



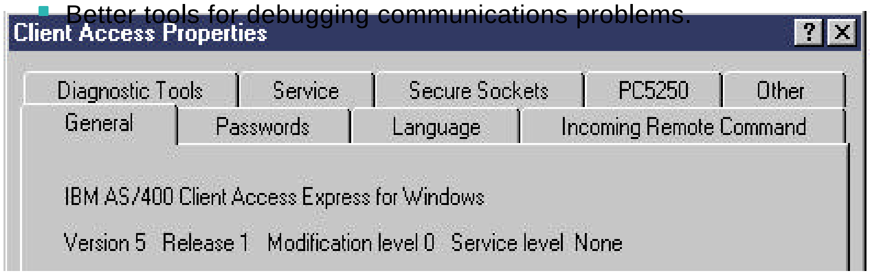
IBM eServer iSeries

Agenda

- Connections with iSereis Access for Windows
  - New features
  - Supported OS/400 versions
  - Connection types supported
  - Configuration
  - Troubleshooting
- Using iSeries Access in an Internet Environment
  - Firewalls
  - NAT
  - VPNs
  - Other Security Consideration
- Using iSeries Access with Terminal Services
  - Functions supported
  - iSeries Access restrictions
  - Windows 2000 considerations
- Appendix A: Example of terminal services install and config
- Appendix B: Example of internet connection through firewall

Changes for V5R1

- V5R1M0 Express client supports connections to V4R4, V4R5, and V5R1 versions of OS/400.
- Support for long passwords when connecting to iSeries systems at V5R1.
- Compression of some communications
- Provide user capability to change timeout for connections
- Client Authentication for SSL
- Removal of CE1 (40-bit encryption)
- Better tools for debugging communications problems.

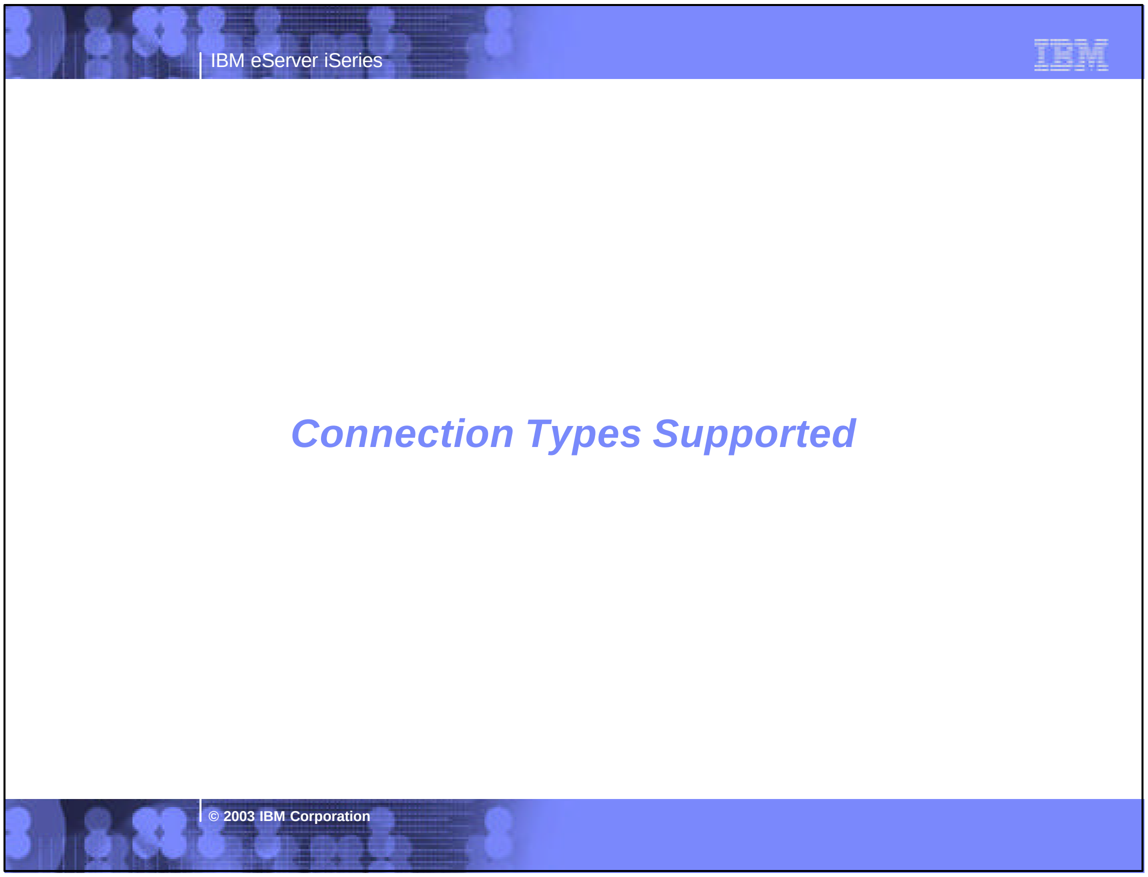


IBM AS/400 Client Access Express for Windows

Version 5 Release 1 Modification level 0 Service level None

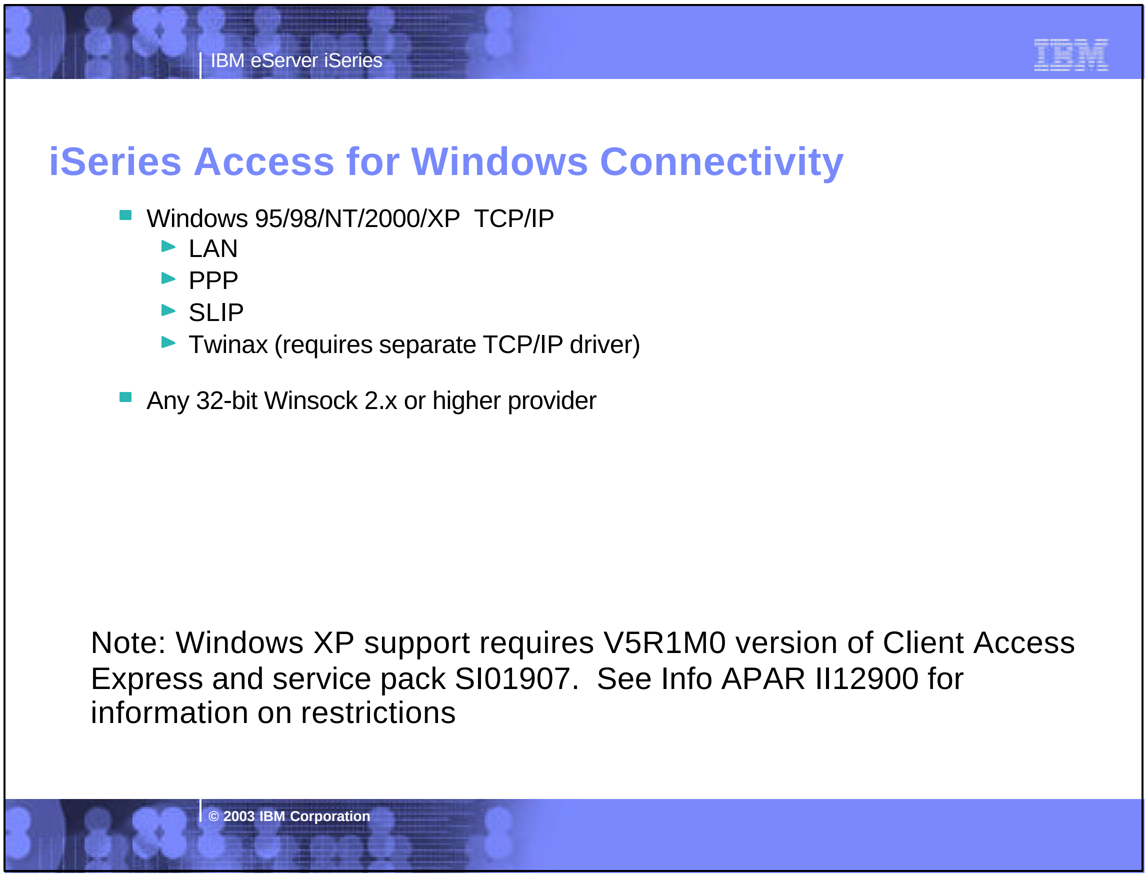
What's new in V5R2?

- Product renamed from Client Access Express to iSeries Access for Windows
- Support for Kerberos authentication of users
  - Kerberos ticket can replace the sending of userid and password from a PC to the iSeries.
  - Kerberos authentication as a new connection property to select
- Removal of CE2 (56-bit encryption)
- Removal of support for Windows 95
  - Dependence on Winsock 2
  - Winsock 2 for Windows 95 can be downloaded from Microsoft's web site, but iSeries Access for Windows does not plan to officially support



IBM eServer iSeries

Connection Types Supported

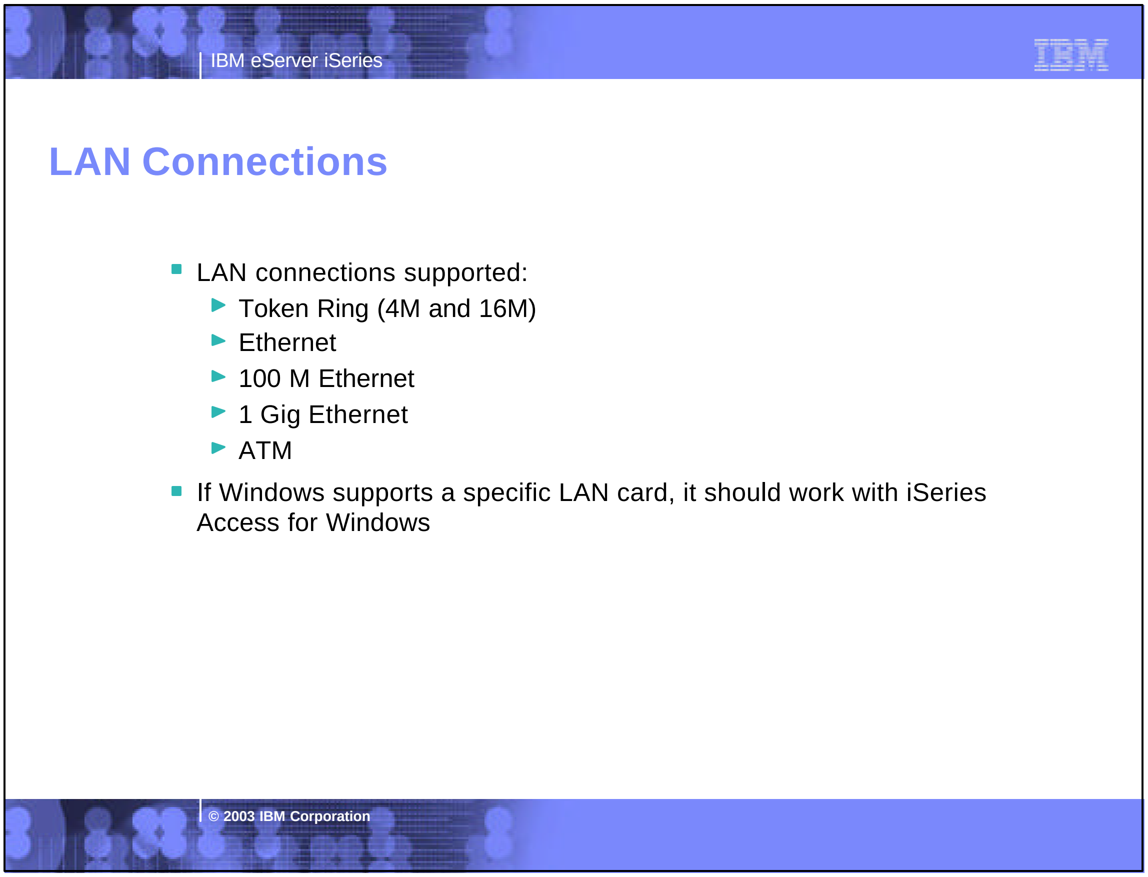


IBM eServer iSeries

iSeries Access for Windows Connectivity

- Windows 95/98/NT/2000/XP TCP/IP
  - LAN
  - PPP
  - SLIP
  - Twinax (requires separate TCP/IP driver)
- Any 32-bit Winsock 2.x or higher provider

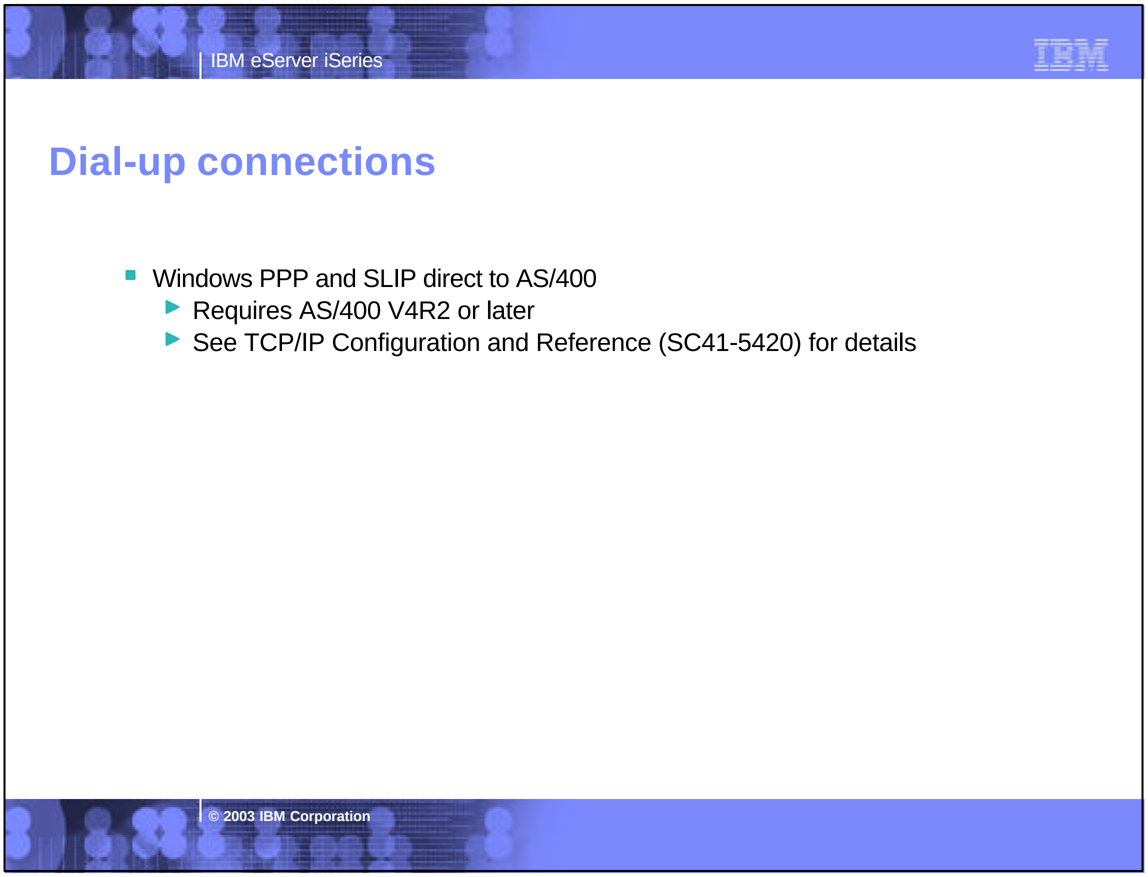
Note: Windows XP support requires V5R1M0 version of Client Access Express and service pack SI01907. See Info APAR II12900 for information on restrictions



IBM eServer iSeries

LAN Connections

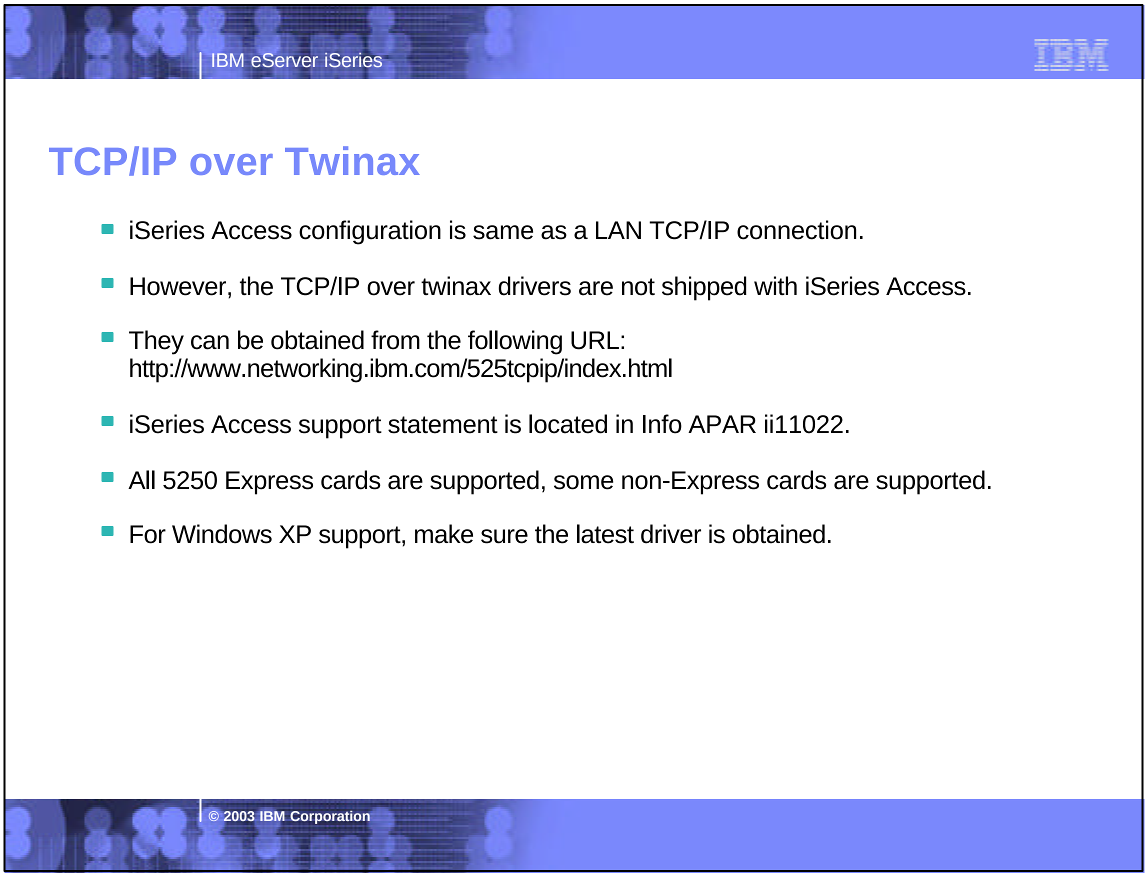
- LAN connections supported:
  - Token Ring (4M and 16M)
  - Ethernet
  - 100 M Ethernet
  - 1 Gig Ethernet
  - ATM
- If Windows supports a specific LAN card, it should work with iSeries Access for Windows



IBM eServer iSeries

Dial-up connections

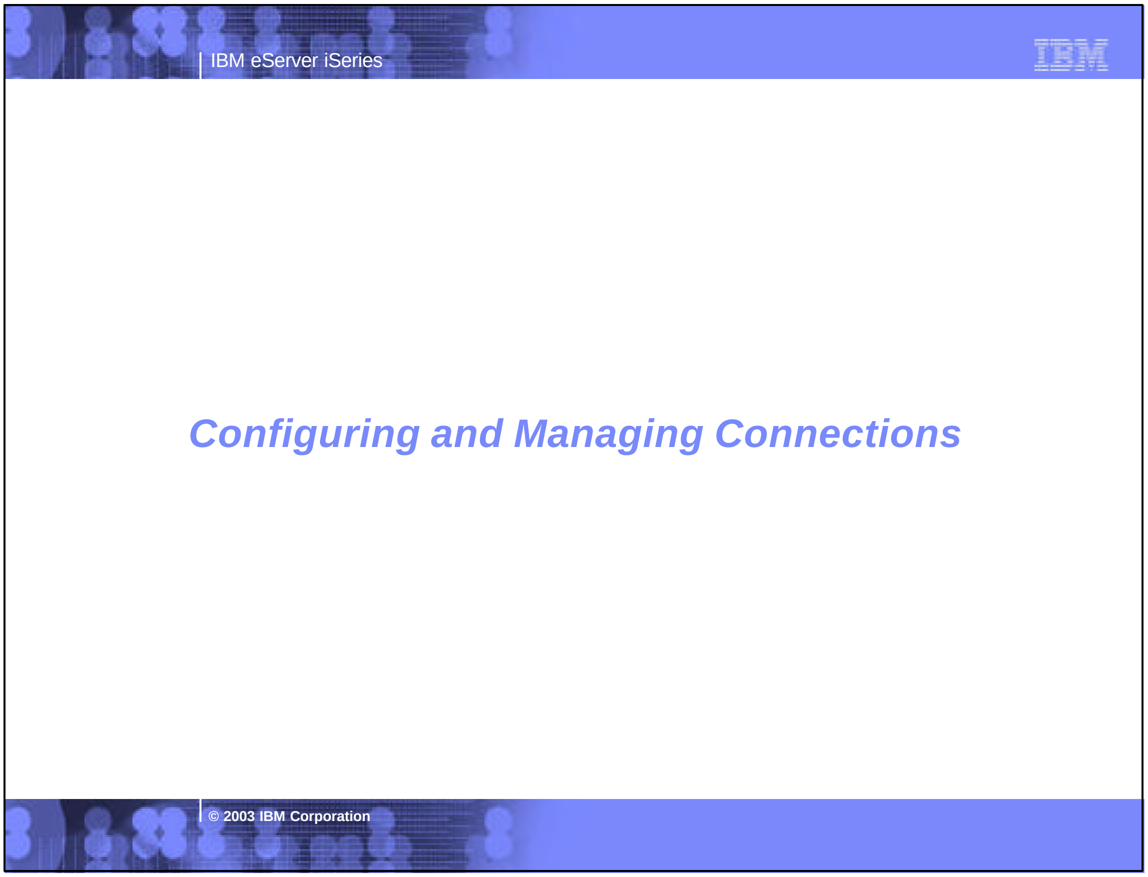
- Windows PPP and SLIP direct to AS/400
  - Requires AS/400 V4R2 or later
  - See TCP/IP Configuration and Reference (SC41-5420) for details



IBM eServer iSeries

TCP/IP over Twinax

- iSeries Access configuration is same as a LAN TCP/IP connection.
- However, the TCP/IP over twinax drivers are not shipped with iSeries Access.
- They can be obtained from the following URL: http://www.networking.ibm.com/525tcpip/index.html
- iSeries Access support statement is located in Info APAR ii11022.
- All 5250 Express cards are supported, some non-Express cards are supported.
- For Windows XP support, make sure the latest driver is obtained.



IBM eServer iSeries

Configuring and Managing Connections

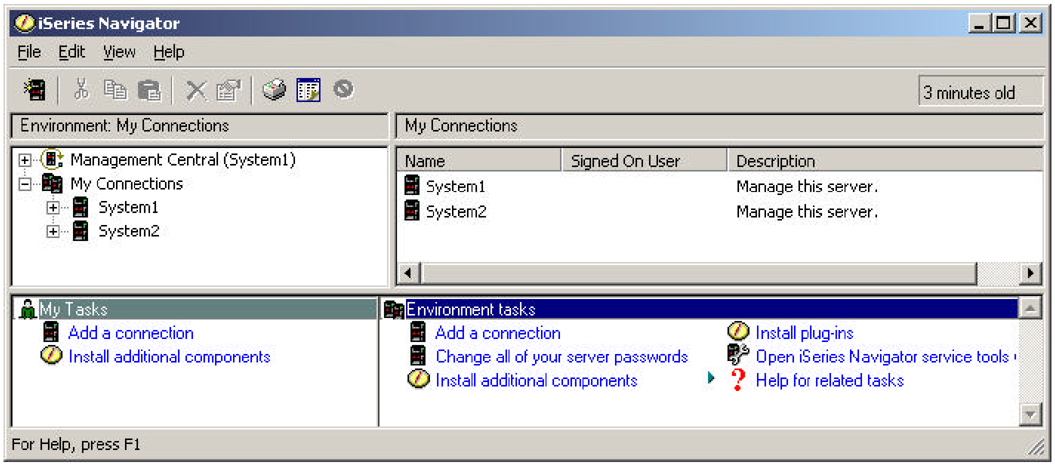
Managing Connections

- "AS/400 Connections" program does not exist in iSeries Access for Windows.
- Managing of connections has been integrated into iSeries Navigator.
- iSeries Navigator can be used to create, delete, and change properties of connections.
- Connections can also be created by simply specifying the iSeries system name in the desired applications.
- If migrating from Client Access for Windows 95/NT, existing TCP/IP connections can be migrated (run Migration Wizard).

iSeries Navigator Main Windows

- Left Window shows active environment and configured systems.

- Right Window shows contents of current selection.

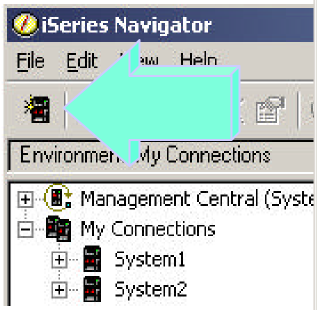


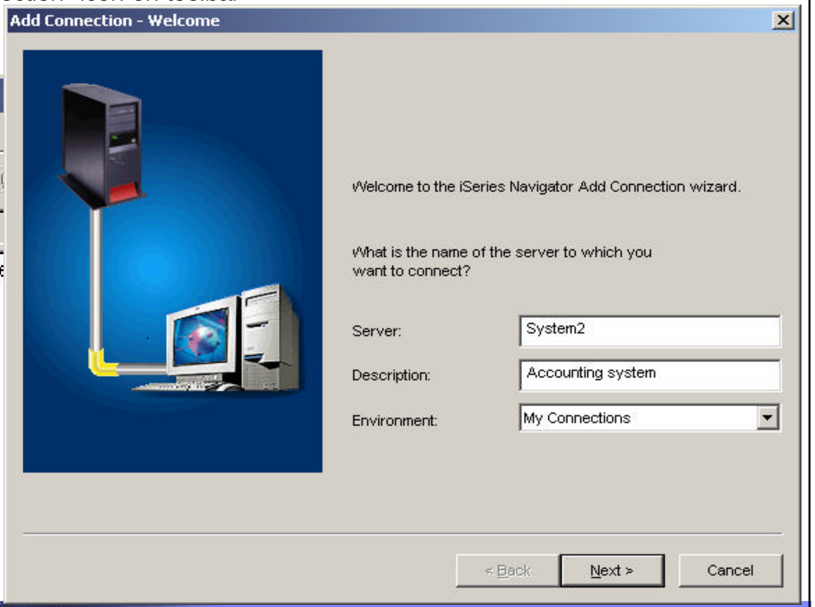
Name	Signed On User	Description
System1		Manage this server.
System2		Manage this server.

IBM eServer iSeries

Creating a new connection

- Adding a new connection
  - Click on "Add Connection" icon on toolbar





Welcome to the iSeries Navigator Add Connection wizard.

What is the name of the server to which you want to connect?

Server: System2

Description: Accounting system

Environment: My Connections

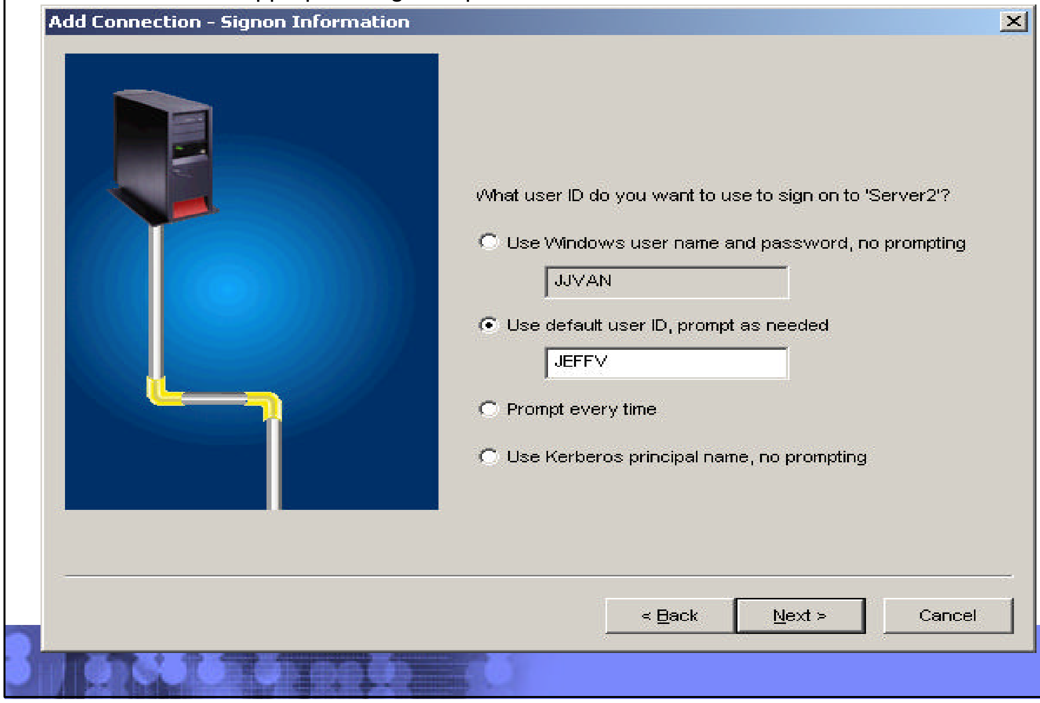
Enter System Name or IP address

© 2003 IBM Corporation

IBM eServer iSeries

Sign-on Options

- Enter appropriate signon option



What user ID do you want to use to sign on to 'Server2'?

○ Use Windows user name and password, no prompting

JJVAN

● Use default user ID, prompt as needed

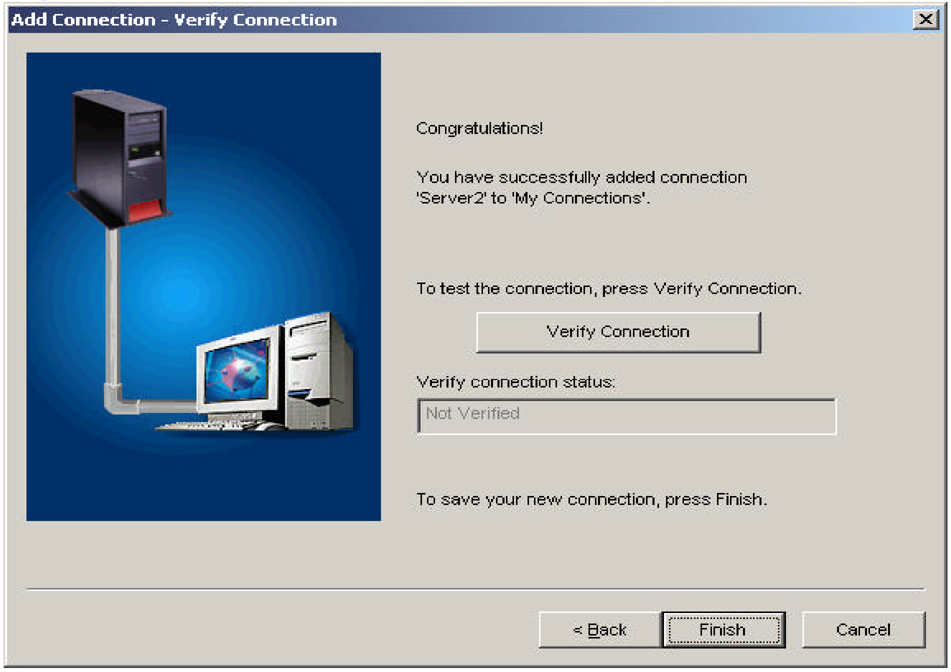
JEFFV

○ Prompt every time

○ Use Kerberos principal name, no prompting

IBM eServer iSeries

Verify Connection



Add Connection - Verify Connection

Congratulations!

You have successfully added connection 'Server2' to 'My Connections'.

To test the connection, press Verify Connection.

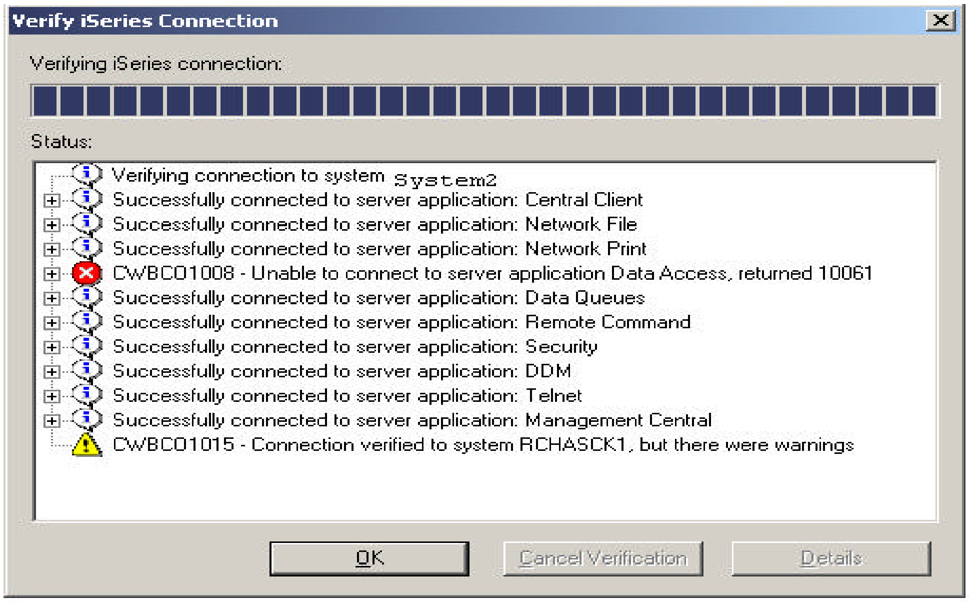
Verify connection status: Not Verified

To save your new connection, press Finish.

IBM eServer iSeries

Verification

- Verification screen allows detailed messages to be displayed when the "+" is clicked on.



Verify iSeries Connection

Verifying iSeries connection:

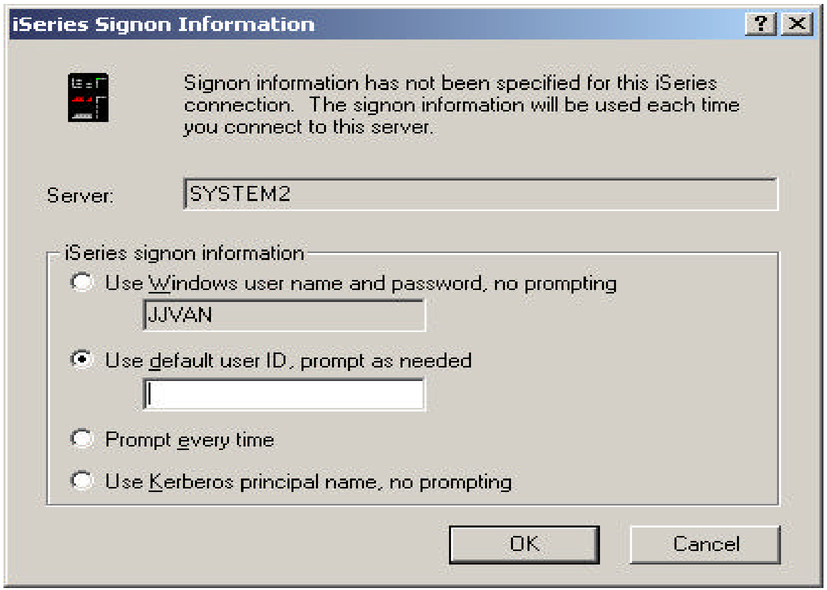
Status:

```
Verifying connection to system System2
Successfully connected to server application: Central Client
Successfully connected to server application: Network File
Successfully connected to server application: Network Print
CWBCO1008 - Unable to connect to server application Data Access, returned 10061
Successfully connected to server application: Data Queues
Successfully connected to server application: Remote Command
Successfully connected to server application: Security
Successfully connected to server application: DDM
Successfully connected to server application: Telnet
Successfully connected to server application: Management Central
CWBCO1015 - Connection verified to system RCHASCK1, but there were warnings
```

IBM eServer iSeries

Config-free connection

- Simply start up an application (like Data Transfer), specify a new system name, and you'll be prompted for signon option.



iSeries Signon Information

Signon information has not been specified for this iSeries connection. The signon information will be used each time you connect to this server.

Server: SYSTEM2

iSeries signon information

○ Use Windows user name and password, no prompting

JJVAN

● Use default user ID, prompt as needed

○ Prompt every time

○ Use Kerberos principal name, no prompting

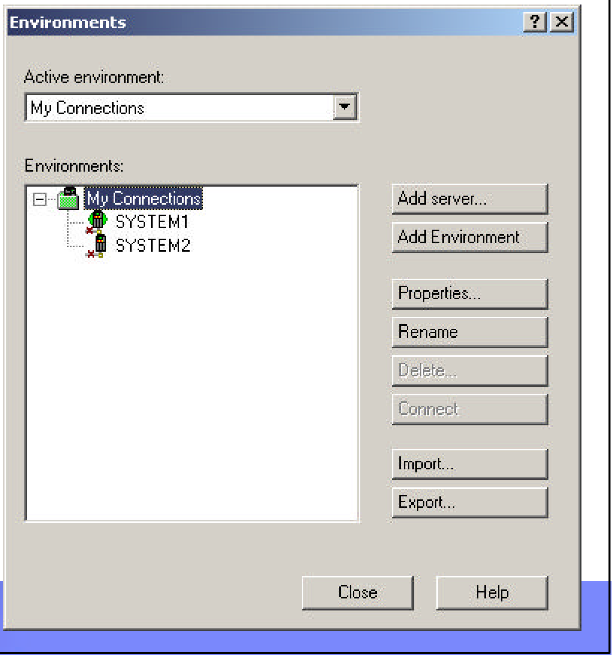
IBM eServer iSeries

Managing Environments & Connections

The Environments View offers a lot more interaction with the environments and connections.

The Environments View is opened from Operations Navigator by selecting Connections to Servers ->Environments from the File menu.

This will bring up the screen shown, which allows the user to manage all defined environments and iSeries connections. One can also define new ones.



Environments

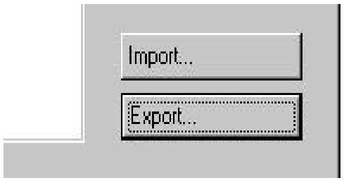
Active environment: My Connections

Environments:

- My Connections
  - SYSTEM1
  - SYSTEM2

Importing & Exporting Environments

The Export option allows the user to save the environment definition, including all connections it contains.



The environment will save the environment as a *.ENV file. The default name of the file will be the name of the environment.

Then the Import option can be used to restore the environment, and the connections.

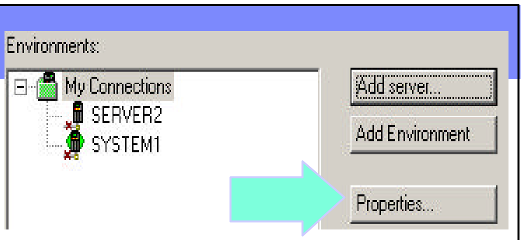
This can be useful to distribute common connection definitions to several PCs. The connections can be defined on one PC and then exported to a location where the other PCs can import the environment.

Importing & Exporting Environments

Even though iSeries Access for Windows allows environments to be created with names that contain the characters \ / : * ? " < > and |, the Windows operating systems will not accept these characters as part of a file name. So environments that contain these characters will not be able to be exported or imported.

IBM eServer iSeries

Properties


Environments:

- My Connections
  - SERVER2
  - SYSTEM1

Selecting the Properties button allows the user to view or change the properties of either connections or environments.

Whatever connection or environment that is highlighted when the Properties button is selected will be displayed.

The only property of an environment is the default system.

- The default system will specify which of the connections within the environment will be used to download a language conversion table from if the table isn't on the PC, if this environment is set to the active environment.
- The default system will also be the default system name presented when configuring a new PC5250 or Data Transfer session.

IBM eServer iSeries

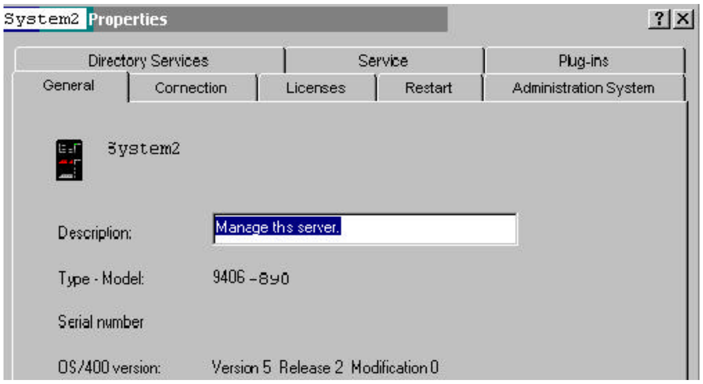
System Connection Properties

IBM eServer iSeries

Properties

The properties of a connection display a lot more information.
The following property tabs are available.

- General
- Connection
- Secure Sockets
- Licenses
- Restart
- Directory Services
- Plug-ins



System2

Description: Manage ths server.

Type - Model: 9406 -890

Serial number

OS/400 version: Version 5 Release 2 Modification 0

Some of these properties will not be able to be interacted with if the connection isn't currently active. So the user might be prompted to signon to the system while interacting with the properties.

Note: Properties can also be accessed by right-clicking on the system name in iSeries Navigator

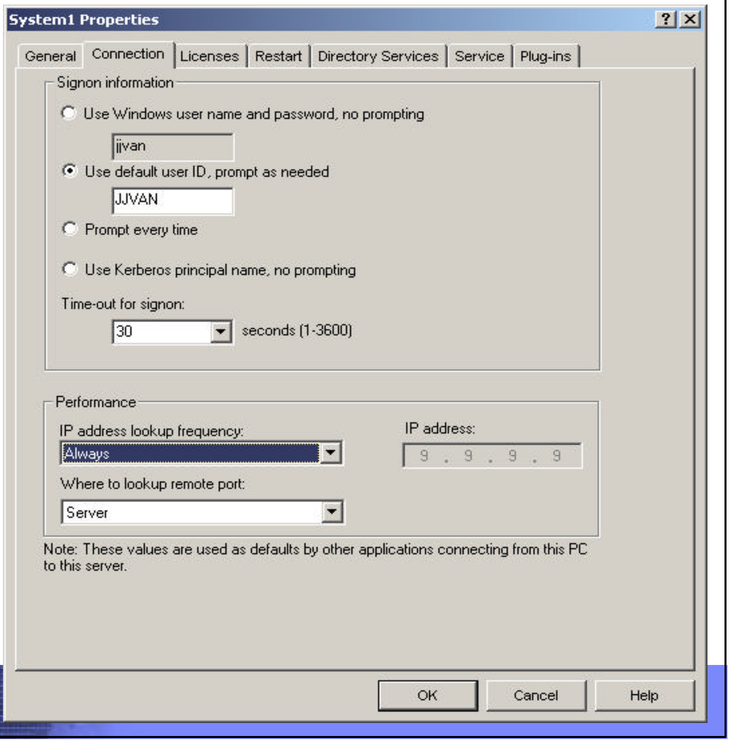
IBM eServer iSeries

More on Properties

- Changing Connection and Secure Sockets properties does not change active connections (including the iSeries Navigator session).
- After changing any properties, end any applications that are using a connection to that iSeries.
- Individual iSeries Access applications each can set their own connection properties, which may take precedence over the global properties set in iSeries Navigator.

Connection Properties

- The Connection tab allows the user to modify the iSeries Signon Information and Performance preferences of the connection. Each of these will be discussed.



Signon information

○ Use Windows user name and password, no prompting

jjvan

● Use default user ID, prompt as needed

JJVAN

○ Prompt every time

○ Use Kerberos principal name, no prompting

Time-out for signon:

30 seconds (1-3600)

Performance

IP address lookup frequency: Always

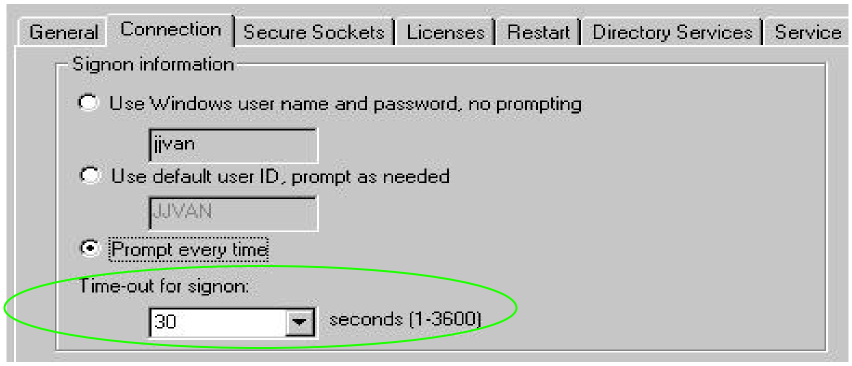
IP address: 9 . 9 . 9 . 9

Where to lookup remote port: Server

Note: These values are used as defaults by other applications connecting from this PC to this server.

Connection Timeout Value - New for V5R1

- Rather than wait for a significant number of minutes for a connection attempt to timeout, shorten the timeout period for this PC.
- If the network is slow, you can give yourself a longer period of time to connect.
- The default is 30 seconds. If you had slow connections that worked on previous releases, but fail with V5R1, try increasing this value.



Signon information

○ Use Windows user name and password, no prompting

jjvan

○ Use default user ID, prompt as needed

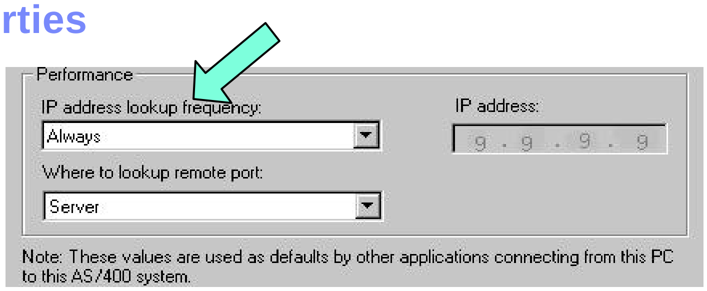
JJVAN

● Prompt every time

Time-out for signon:

30 seconds (1-3600)

Performance Properties



Performance

IP address lookup frequency: Always

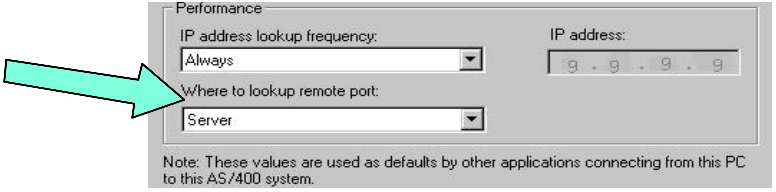
IP address: 9 . 9 . 9 . 9

Where to lookup remote port: Server

Note: These values are used as defaults by other applications connecting from this PC to this AS/400 system.

- IP address lookup options
  - Always
  - One hour
  - One day
  - One week
  - Never - Specify an IP address (host file entry needed for PC5250)
  - After startup of PC
- Depending on your network, IP address resolution may take several seconds.
- Less frequent lookups improve performance.
- If IP address given as system name, no lookup occurs and no host file entry needed for PC5250

Performance Properties



Performance

IP address lookup frequency: Always

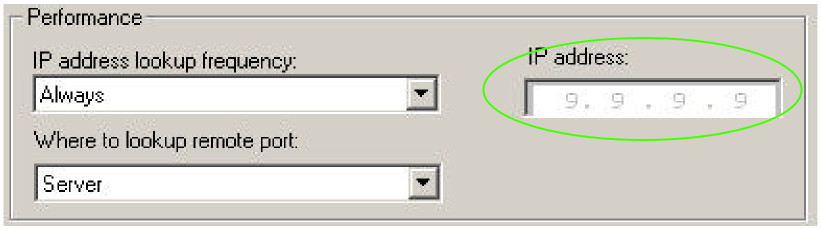
IP address: 9 . 9 . 9 . 9

Where to lookup remote port: Server

Note: These values are used as defaults by other applications connecting from this PC to this AS/400 system.

- "Where to lookup remote port" options
  - Server
    - Server mapper is always used for port resolution
  - Local
    - Use the local Services file on PC to resolve. Note: All Client Access servers must then be added manually into this file.
  - Standard
    - Always use the default port, no lookup
- Local and Standard will result in better performance, since server mapper does not have to be contacted first.

Performance properties



Performance

IP address lookup frequency: Always

Where to lookup remote port: Server

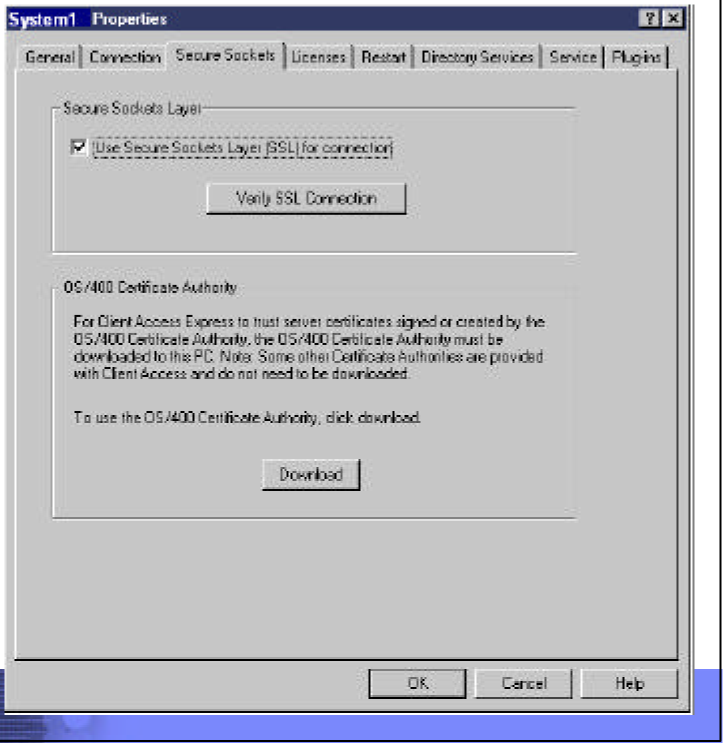
IP address: 9 . 9 . 9 . 9

- IP Address
  - Lists last IP address used to access this iSeries
  - Cannot be changed from properties page, unless IP address lookup is changed to "Never".
- Note: iSeries Access for Windows does not update the Hosts file on your PC. Client Access for Windows 95/NT does update it at connect time in some situations, but this has caused confusion for customers that expect iSeries Access to then manage that file.

Secure Sockets Properties and Support

SSL Properties

- Secure Sockets
  - Enable/Disable SSL
  - Verify SSL Connections
  - Download Certificate Authority



Secure Sockets Layer

☑ Use Secure Sockets Layer (SSL) for connection

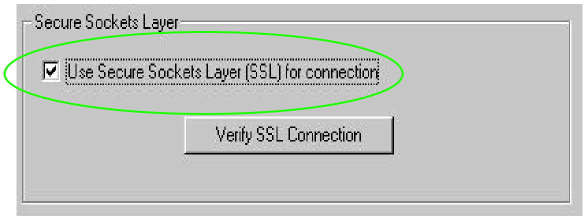
OS/400 Certificate Authority

For Client Access Express to trust server certificates signed or created by the OS/400 Certificate Authority, the OS/400 Certificate Authority must be downloaded to this PC. Note: Some other Certificate Authorities are provided with Client Access and do not need to be downloaded.

To use the OS/400 Certificate Authority, click download.

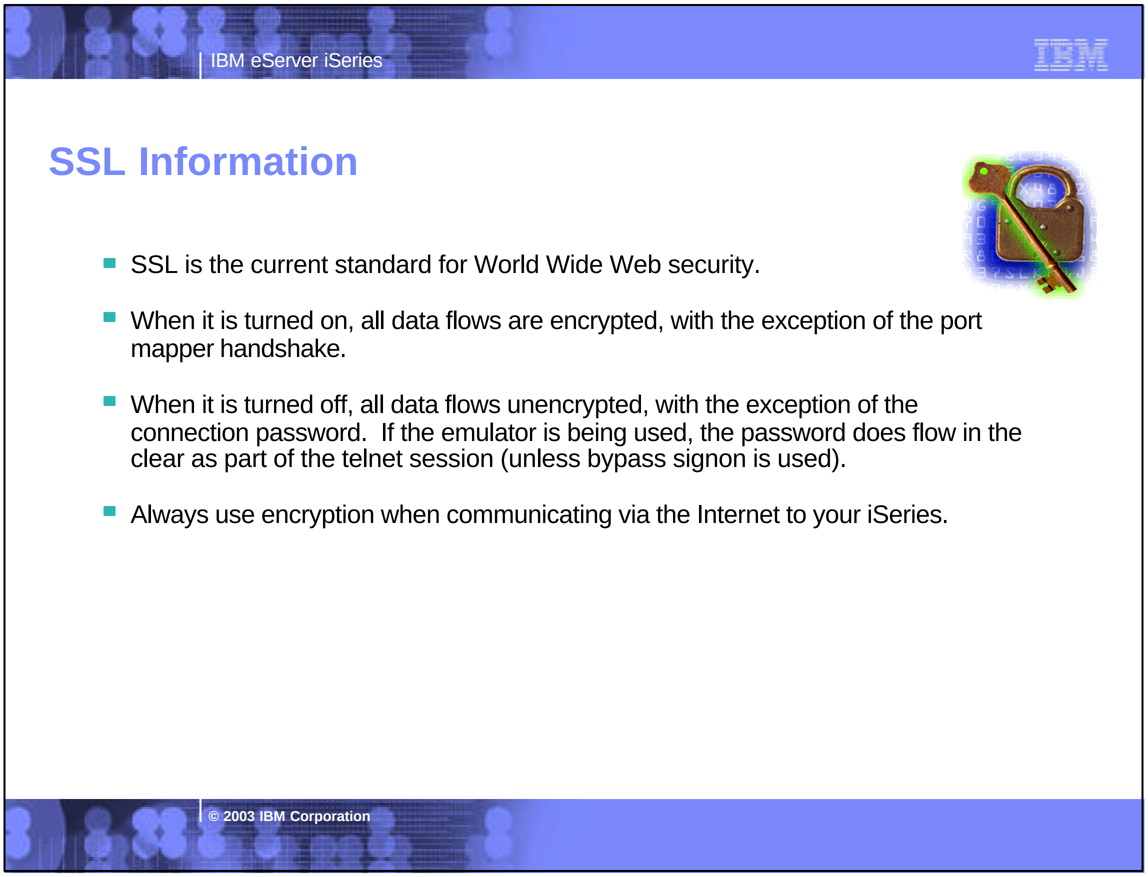
Security Properties

- Specify if SSL should be used or not.
- SSL stands for Secure Sockets Layer, and specifies that encryption will be used for the sessions.
- Only SSL server authentication is supported. The exception is that client authentication has been added for PC5250 only in V5R1 and later.
- This option will be greyed out unless the 5769-CE1, CE2, or CE3 LPP is installed on the iSeries and the PC. The user must have access to: QIBM/ProdData/CA400/Express/SSL/SSLxxx, where xxx is 40, 56, or 128.
  - CE1 = 40-bit encryption **(no longer available in V5R1)**
  - CE2 = 56-bit encryption **(no longer available in V5R2)**
  - CE3 = 128-bit encryption



Secure Sockets Layer

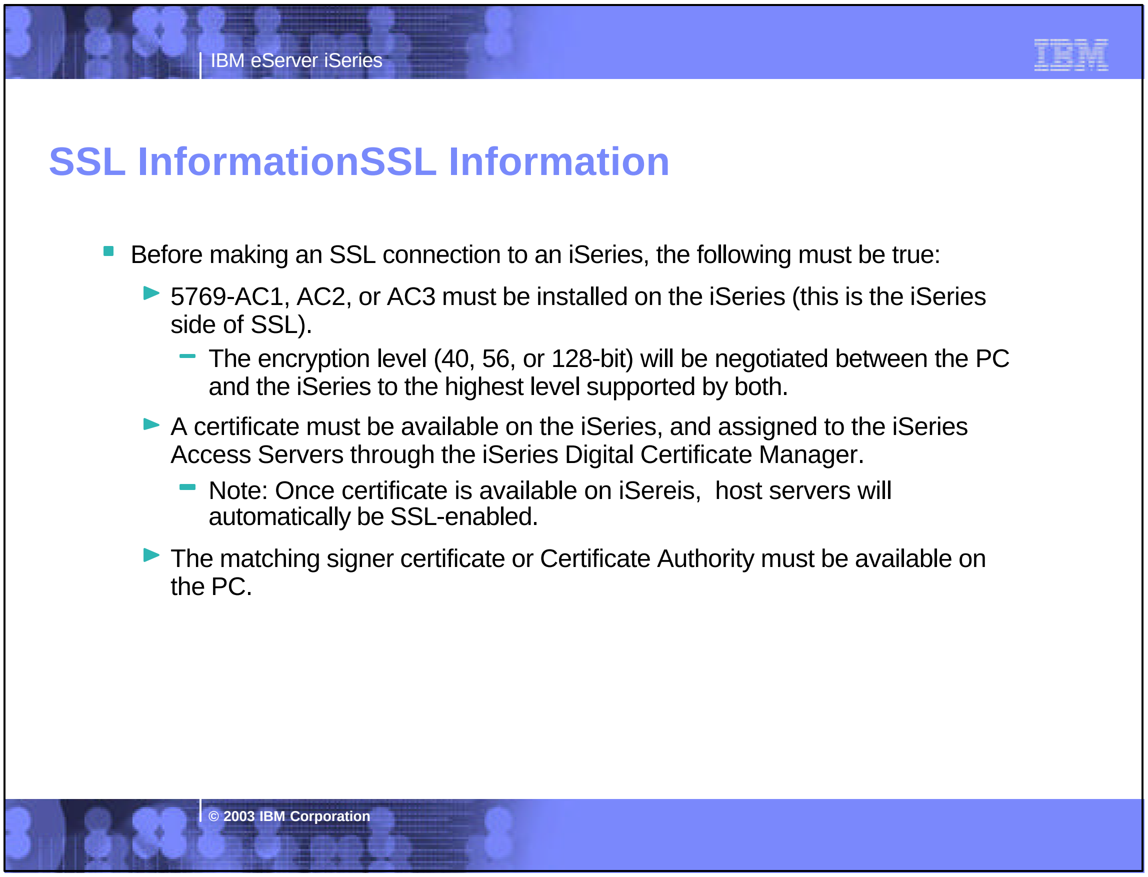
☑ Use Secure Sockets Layer (SSL) for connection



IBM eServer iSeries

SSL Information

- SSL is the current standard for World Wide Web security.
- When it is turned on, all data flows are encrypted, with the exception of the port mapper handshake.
- When it is turned off, all data flows unencrypted, with the exception of the connection password. If the emulator is being used, the password does flow in the clear as part of the telnet session (unless bypass signon is used).
- Always use encryption when communicating via the Internet to your iSeries.



IBM eServer iSeries

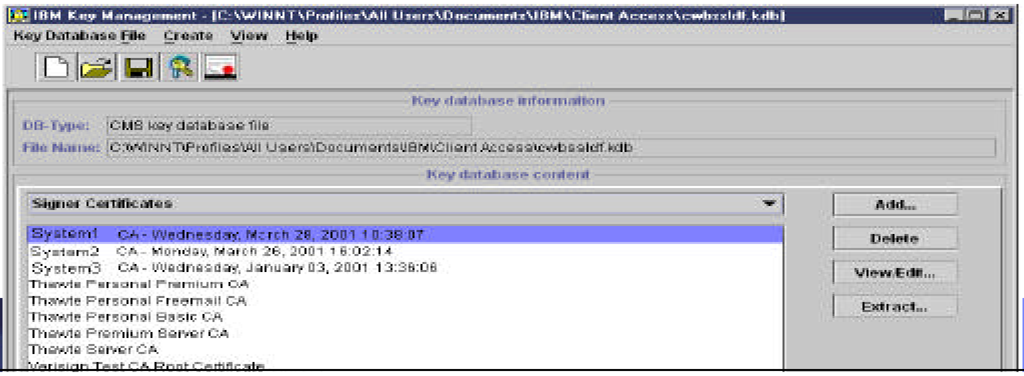
SSL InformationSSL Information

- Before making an SSL connection to an iSeries, the following must be true:
  - 5769-AC1, AC2, or AC3 must be installed on the iSeries (this is the iSeries side of SSL).
    - The encryption level (40, 56, or 128-bit) will be negotiated between the PC and the iSeries to the highest level supported by both.
  - A certificate must be available on the iSeries, and assigned to the iSeries Access Servers through the iSeries Digital Certificate Manager.
    - Note: Once certificate is available on iSereis, host servers will automatically be SSL-enabled.
  - The matching signer certificate or Certificate Authority must be available on the PC.

IBM eServer iSeries

Certificate Management

- IBM Key Management utility is included as part of installing CE1,2, or 3 on the PC.
- Can be accessed through Control Panel, under iSeries Access for Windows properties for Secure Sockets
- Recommend that a certificate by a well-known certificate authority (such as Verisign®) be used.
- A number of well-known certificate authorities are already stored in the key database.
- Using any other type of certificate will require transferring certificate authorities from other sources.



DB-Type: CMS key database file

File Name: C:\WINNT\Profiles\All Users\Documents\IBM\Client Access\cwbssldf.kdb

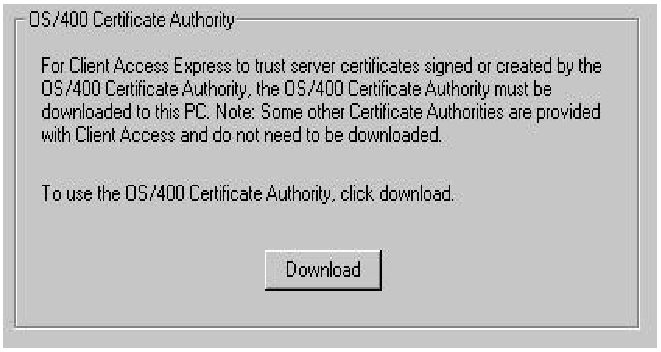
Signer Certificates

```
System1   CA - Wednesday, March 28, 2001 10:38:07
System2   CA - Monday, March 26, 2001 16:02:14
System3   CA - Wednesday, January 03, 2001 13:36:06
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
```

IBM eServer iSeries

Downloading Certificate Authorities

- New for V5R1, button is available to download CA from the iSeries
- The CA is automatically imported into the iSeries Access key database and the Java key database (required by iSeries Navigator).
- Previously, a separately downloadable utility had to be downloaded from the web to do this.



OS/400 Certificate Authority

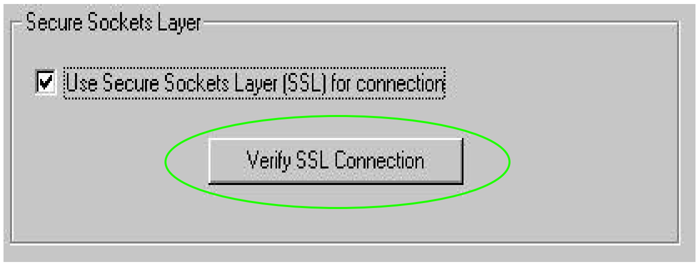
For Client Access Express to trust server certificates signed or created by the OS/400 Certificate Authority, the OS/400 Certificate Authority must be downloaded to this PC. Note: Some other Certificate Authorities are provided with Client Access and do not need to be downloaded.

To use the OS/400 Certificate Authority, click download.

IBM eServer iSeries

Verify SSL Connections

- Also new for V5R1, a verify button has been added to the Secure Sockets properties page.
- This allow you to check if the iSeries Access servers are enabled for SSL.



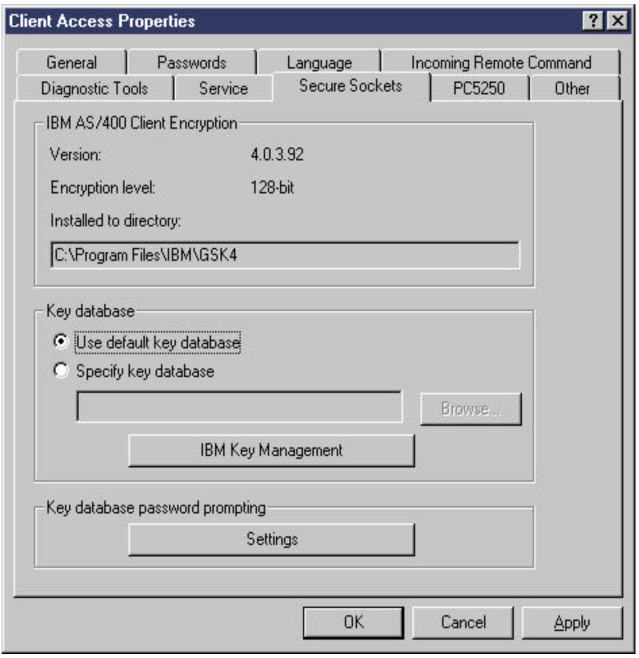
Secure Sockets Layer

☑ Use Secure Sockets Layer (SSL) for connection

IBM eServer iSeries

PC5250 Client Authentication

- New in V5R1, SSL client authentication can be enabled for the OS/400 Telnet server.
- iSeries Access for Windows PC5250 support has been enhanced to take advantage of this.
- SSL server authentication must always be configured before client authentication will work.
- No settings are required on the client to enable client authentication, but some preferences can be set.



Client Access Properties

IBM AS/400 Client Encryption

Version: 4.0.3.92

Encryption level: 128-bit

Installed to directory: C:\Program Files\IBM\GSK4

Key database

● Use default key database

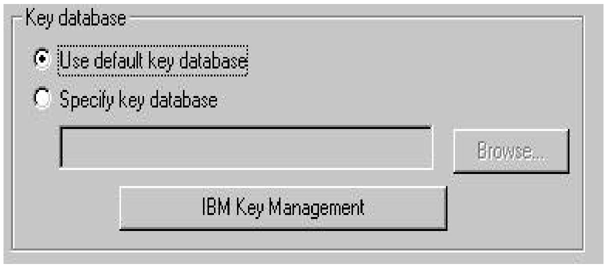
○ Specify key database

Key database password prompting

IBM eServer iSeries

Key Database Selection

- User can select which key database to use on their PC.
- For most users, keeping the default key database selection selected is fine.
- The IBM Key Management Utility can also be invoked from here to view the contents of key databases on your PC.



Key database

● Use default key database

○ Specify key database

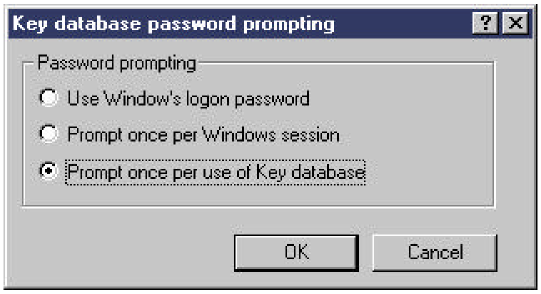
IBM eServer iSeries

Client Authentication Prompting modes

- Users can choose how often they are prompted for access to the key database.
- Its important to authenticate that the user has access to the key database before the certificate is sent up to the iSeries. Otherwise, someone could simply move the key database file to another PC and have access to the certificate.

Key database password prompting

Note: A policy can be used by an administrator to force one of these.



Key database password prompting

Password prompting

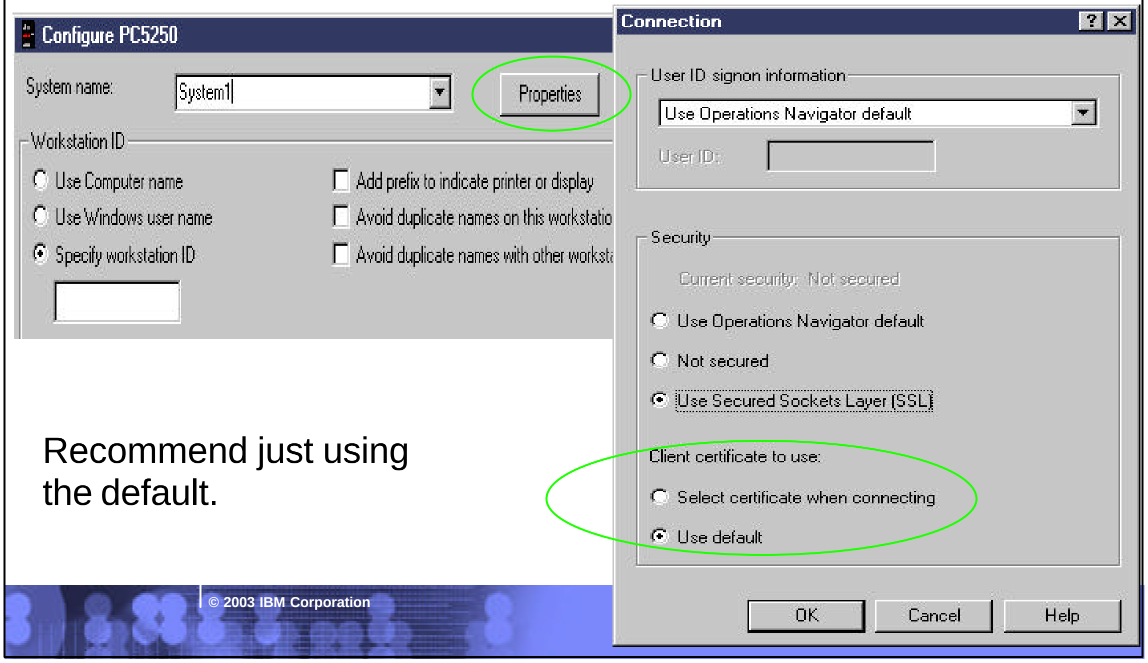
○ Use Window's logon password

○ Prompt once per Windows session

● Prompt once per use of Key database

Certificate Selection

- PC5250 configuration allows user to choose if they want to be prompted with a list of certificates to choose from to send to iSeries.



Configure PC5250

System name: System1

Workstation ID

○ Use Computer name
○ Use Windows user name
● Specify workstation ID

☐ Add prefix to indicate printer or display
☐ Avoid duplicate names on this workstatio
☐ Avoid duplicate names with other worksta

Connection

User ID signon information

Use Operations Navigator default

User ID:

Security

Current security: Not secured

○ Use Operations Navigator default
○ Not secured
● Use Secured Sockets Layer (SSL)

Client certificate to use:

○ Select certificate when connecting
● Use default

Recommend just using the default.

More Info

- For more info On configuring SSL, recommend getting handouts for:
  - Session 26TC - Configuring iSeries Access to use SSL

IBM eServer iSeries

IBM

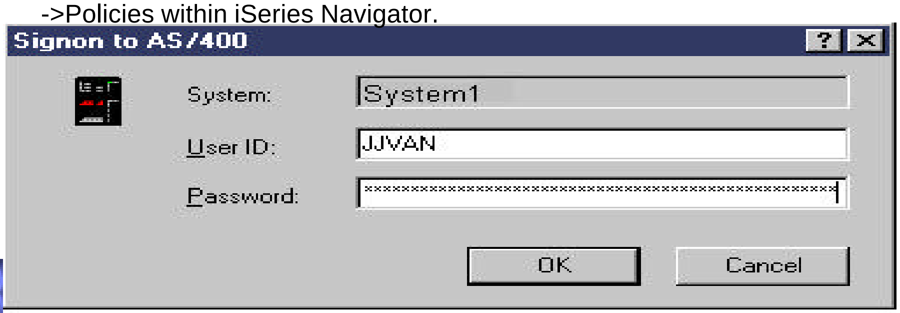
Other new Communication Support

IBM eServer iSeries

IBM

Long Password Support

- Connections to V5R1 iSeries servers can now be done with 128-character passwords, for better security.
- The Password Level (QPWDLVL) must be set to 2 or 3 for these long passwords to be used.
  - A value of 0 is the default and allows 1 to 10-character passwords.
  - A value of 1 allows 1 to 10-character passwords and iSeries Netserver passwords for Windows 95,98,Me will be removed from the system.
  - A value of 2 enables 1 to 128-bit passwords.
  - A value of 3 enables 1 to 128-bit passwords, and iSeries Netserver passwords for Windows 95,98,Me will be removed from the system.
- Password level can be modified in green screen, or through Security ->Policies within iSeries Navigator.

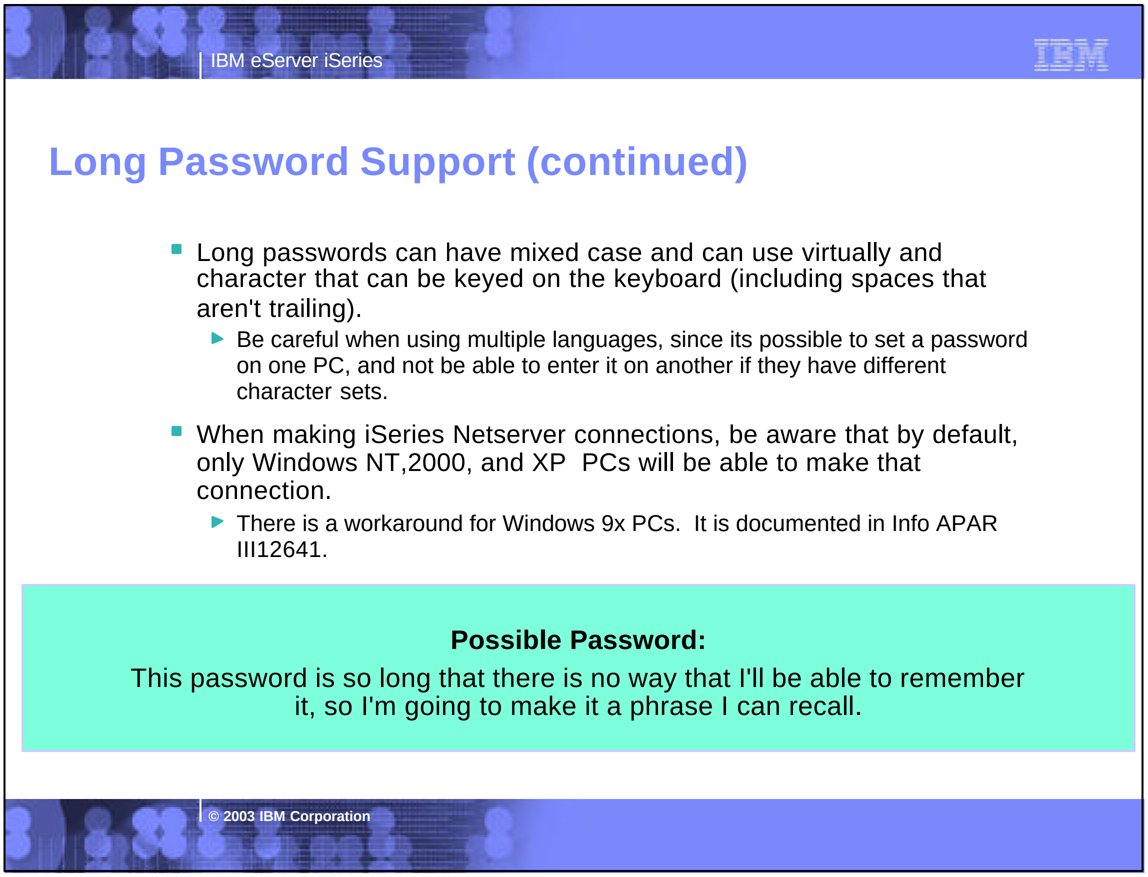


Signon to AS/400

System: System1

User ID: JJVAN

Password: ***



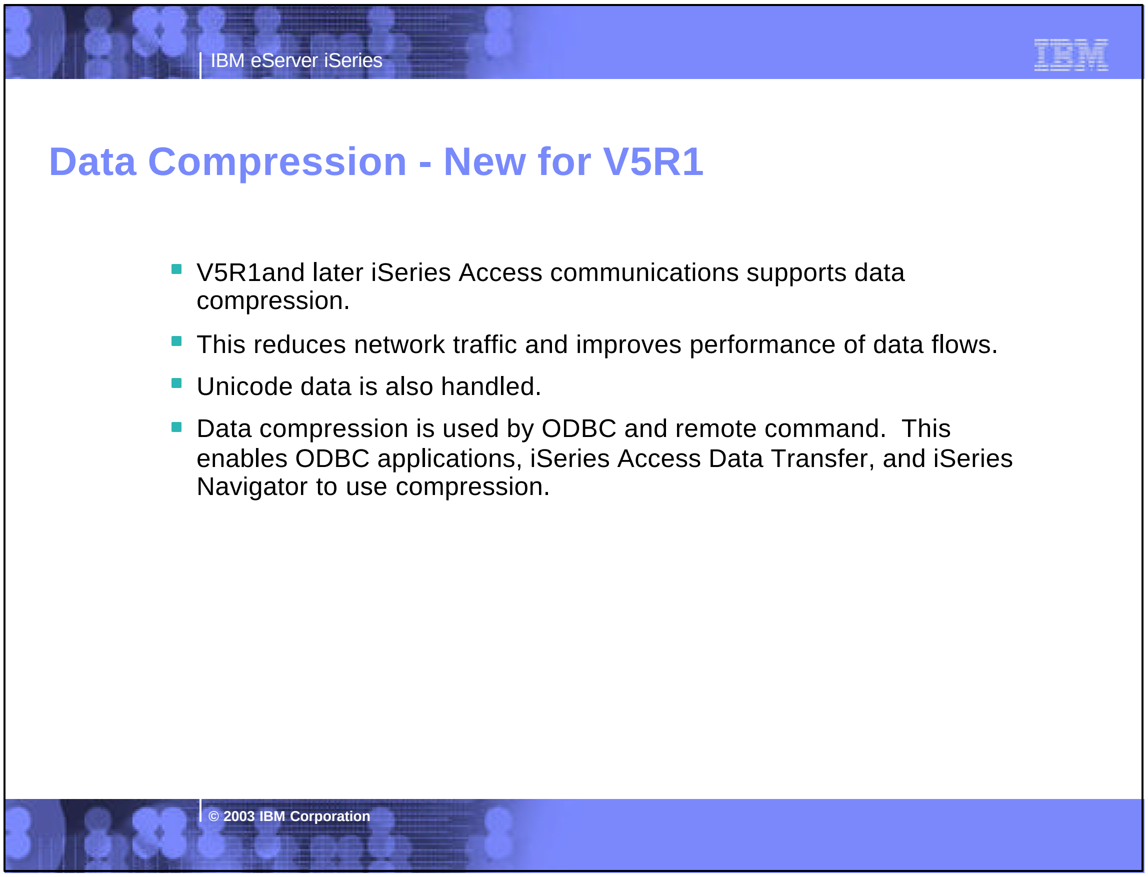
IBM eServer iSeries

Long Password Support (continued)

- Long passwords can have mixed case and can use virtually and character that can be keyed on the keyboard (including spaces that aren't trailing).
  - Be careful when using multiple languages, since its possible to set a password on one PC, and not be able to enter it on another if they have different character sets.
- When making iSeries Netserver connections, be aware that by default, only Windows NT,2000, and XP PCs will be able to make that connection.
  - There is a workaround for Windows 9x PCs. It is documented in Info APAR III12641.

Possible Password:

This password is so long that there is no way that I'll be able to remember it, so I'm going to make it a phrase I can recall.



IBM eServer iSeries

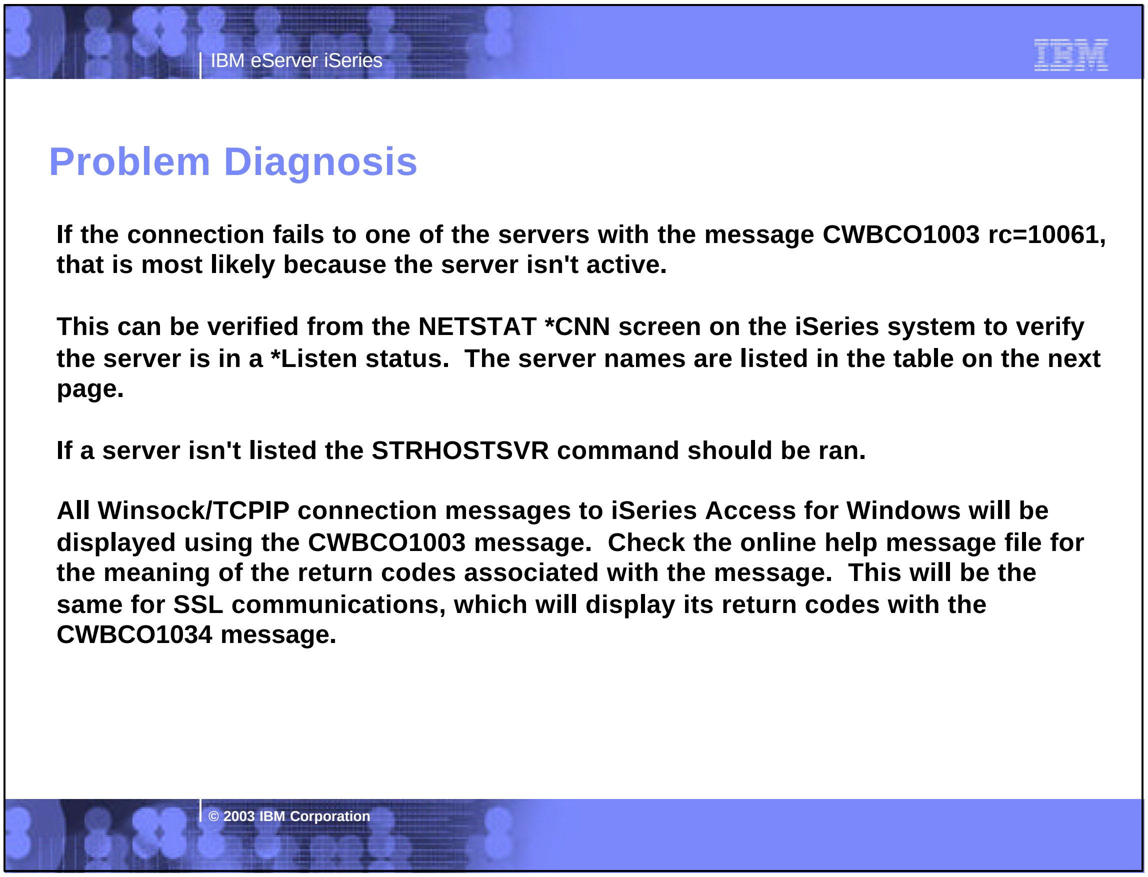
Data Compression - New for V5R1

- V5R1and later iSeries Access communications supports data compression.
- This reduces network traffic and improves performance of data flows.
- Unicode data is also handled.
- Data compression is used by ODBC and remote command. This enables ODBC applications, iSeries Access Data Transfer, and iSeries Navigator to use compression.

IBM eServer iSeries

Troubleshooting

© 2003 IBM Corporation



IBM eServer iSeries

Problem Diagnosis

If the connection fails to one of the servers with the message CWBCO1003 rc=10061, that is most likely because the server isn't active.

This can be verified from the NETSTAT *CNN screen on the iSeries system to verify the server is in a *Listen status. The server names are listed in the table on the next page.

If a server isn't listed the STRHOSTSVR command should be ran.

All Winsock/TCPIP connection messages to iSeries Access for Windows will be displayed using the CWBCO1003 message. Check the online help message file for the meaning of the return codes associated with the message. This will be the same for SSL communications, which will display its return codes with the CWBCO1034 message.

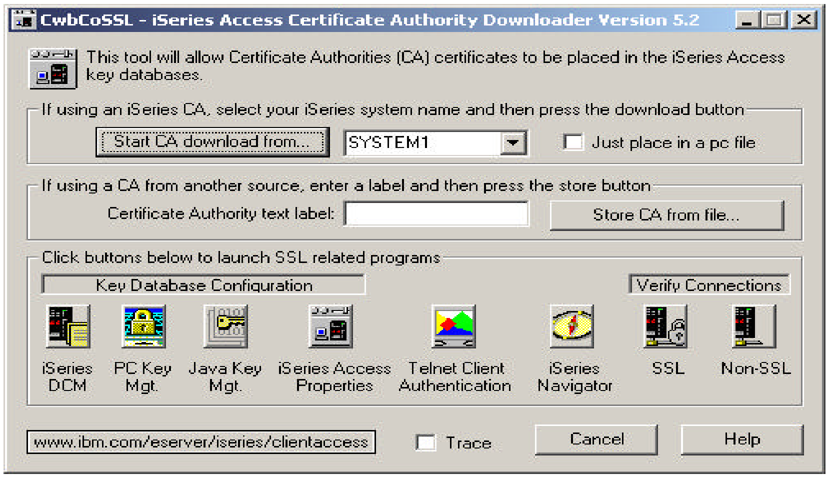
© 2003 IBM Corporation

Tools for Troubleshooting

- CWBPING
  - Checks to see if iSeries can be connected to.
  - Checks to see if host servers are up.
  - If problems, messages indicate what is wrong.
- CWBCOTRC
  - Traces communications flows. Output can be sent into IBM Service personnel.

CWBCOSSL tool

- New tool shipped with first V5R1 Client Access Express service pack.
  - CWBCOSSL.EXE installed into Client Access install directory.
- Makes it easier to debug problems with SSL connections.



CwbCoSSL - iSeries Access Certificate Authority Downloader Version 5.2

This tool will allow Certificate Authorities (CA) certificates to be placed in the iSeries Access key databases.

If using an iSeries CA, select your iSeries system name and then press the download button

SYSTEM1

□ Just place in a pc file

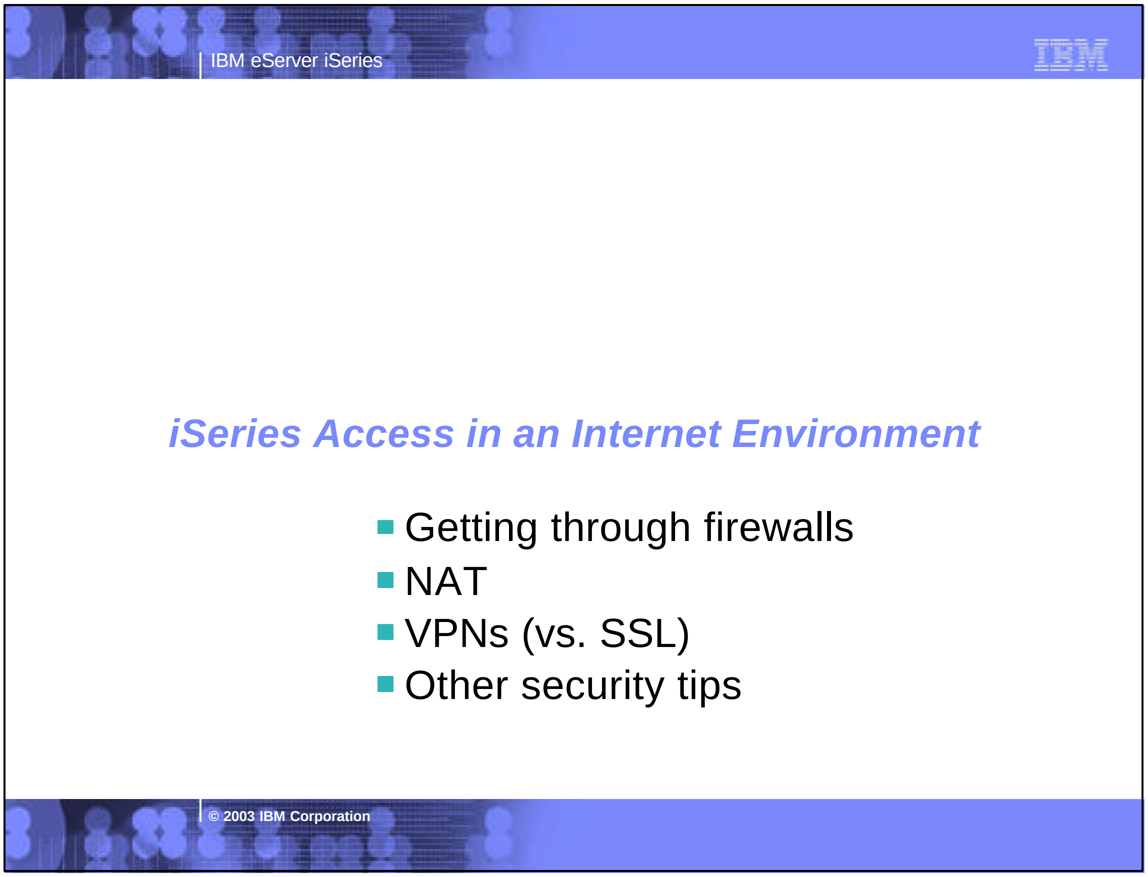
If using a CA from another source, enter a label and then press the store button

Certificate Authority text label:

Click buttons below to launch SSL related programs

www.ibm.com/eserver/iseries/clientaccess

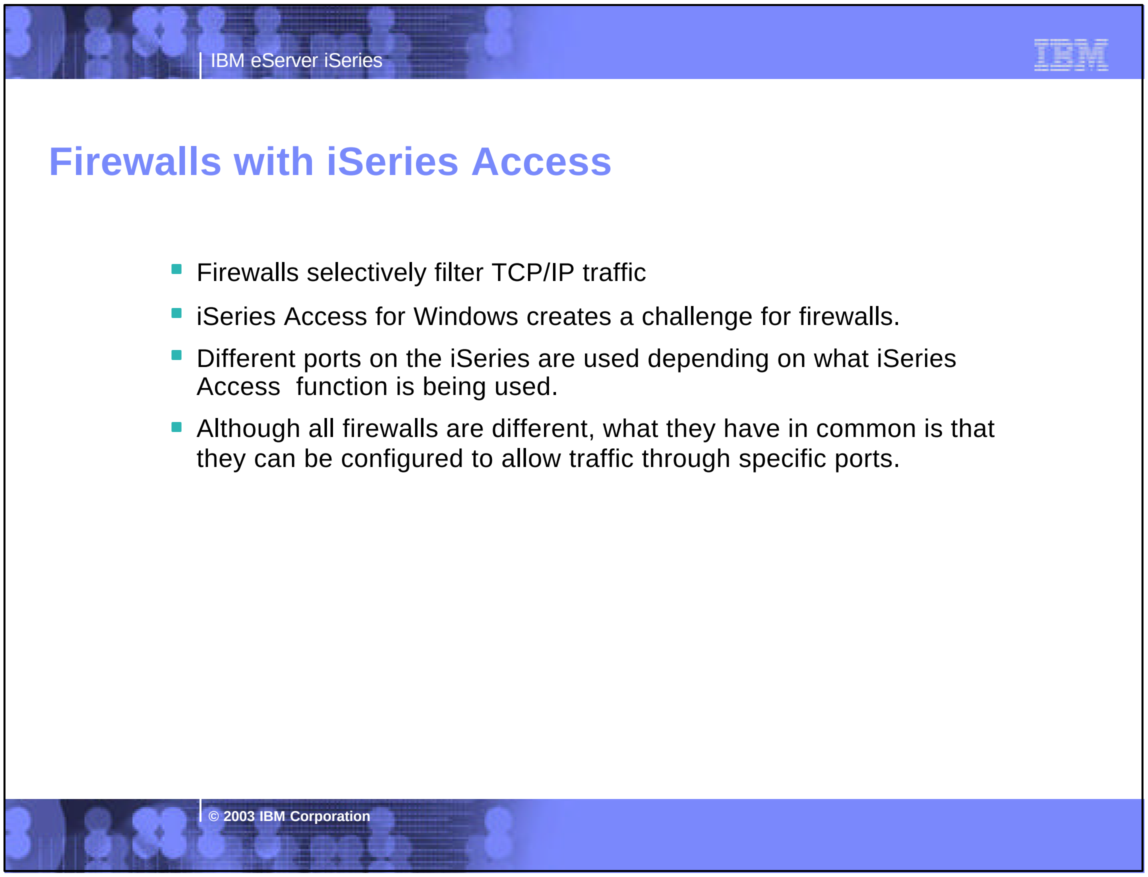
□ Trace



IBM eServer iSeries

iSeries Access in an Internet Environment

- Getting through firewalls
- NAT
- VPNs (vs. SSL)
- Other security tips



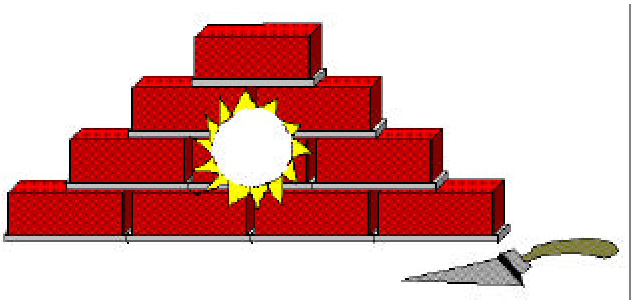
IBM eServer iSeries

Firewalls with iSeries Access

- Firewalls selectively filter TCP/IP traffic
- iSeries Access for Windows creates a challenge for firewalls.
- Different ports on the iSeries are used depending on what iSeries Access function is being used.
- Although all firewalls are different, what they have in common is that they can be configured to allow traffic through specific ports.

IP Packet Filtering

- Firewall must be configured to allow specific ports to be opened.
- Use of IP packet filtering allows administrator to control this.
- This is so that each of the iSeries Access Servers on the iSeries can be reached (Telnet Server, Database Server, etc.).



Servers and ports used

The following servers are used by iSeries Access for Windows. In addition to the servers listed, the Port Mapper (Port 449) is also used by all functions. However, if the user changes the Connection properties for an AS/400 connection so that "Where to look up Remote Port" is set to 'Standard' or 'Local', then the Port Mapper will not be used. In addition, if a DNS server is to be accessed, Port 53 should be made available to the client.

Servers	Ports	Description
Port Mapper	449	Port mapper returns the port number for the requested server
Sign-on	8476 (9476)	Sign-on server is used for every iSeries Access connection to authenticate users and to change passwords
Central	8470 (9470)	Central server is used when an iSeries Access license is required, and also for downloading translation tables
Data Queue	8472 (9472)	Data Queue server allows access to the OS/400 data queues, used for passing data between applications
Database	8471 (9471)	Database server is used for accessing the OS/400 database
Remote Command	8475 (9475)	Remote command server is used to send commands from a PC to an iSeries and for program calls
File	8473 (9473)	File Server is used for accessing any part of the OS/400 file system
Print	8474 (9474)	Print Server is used to access printers known to the iSeries

Servers and Ports Used (continued)

Servers	Ports	Description
Web Admin	2001 (2010)	Used to access web applications served by the iSeries
DDM	446 (448)	DDM server is used to access data via DRDA and for record level access
Telnet	23 (992)	Telnet server is used to access 5250 emulation
Netserver	137, 138, 139, 8474	iSeries Netserver allows access to iSeries integrated file system from Windows PCs
USF	8480	Ultimedia services is used for multimedia data
LDAP	389 (636)	Provides a network directory service
Mgmt Central	5555 5544 5577 (5566)	Management Central server is used to manage multiple iSeries in a network

Notes on ports and servers

Note 1: the port number in parenthesis is the one used to connect to the server via SSL (encrypted session).

Note 2: Ports 449, 8xxx, and 9xxx can be started with the STRHOSTSVR *ALL command. The others need to be started individually, or can be set to autostart when TCP/IP is started (as can 449, 8xxx, and 9xxx).

Note 3: Although 8474 is listed next to Netserver, it is only used internally, so does not have to be set in your firewall IP filtering. However, that server (Print server) must be started for Netserver to work properly.

Note 4: If any applications are registered under Application Administration, then the remote command server will be required in addition to what is listed below.

IBM eServer iSeries

Servers used by specific functions

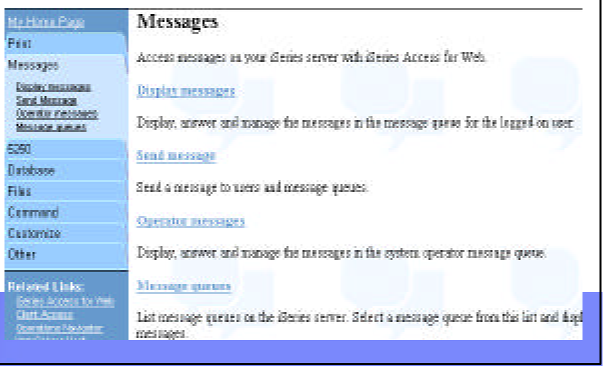
iSeries Access Function	Servers Used
PC5250 display and printer emulation	Sign-on, Central, Telnet
Data Transfer	Sign-on, Central, Database
Base iSeries Navigator support	Sign-on, Remote Command
All Operations Navigator functions	Sign-on, Remote Command, File, Print, Database, Web Admin, Mgmt Central, USF, Netserver, LDAP,Data Queue
ODBC	Sign-on, Database
OLE DB	Sign-on, Database, DDM, Remote Command, Data Queue
AFP Viewer	Sign-on, Print
iSeries Access Install	Netserver
Incoming Remote Command	Uses no specific server, and iSeries port will vary. PC-side port is 512.
Fax support	Sign-on, Print

IBM eServer iSeries

The iSeries Access for Web Alternative

Depending on your needs, if you don't want to mess with all the ports, iSeries Access for Web may be a solution:

- All traffic goes through a single HTTP port.
- SSL will also work using a single HTTPS port.
- All functions run as servlets on the iSeries
- No code to download to the client
- Good set of functions designed for end users:
  - Database access
  - File/Share access
  - printer and print output access
  - Messages
  - 5250 support
  - Customizable user interface
  - Commands



Messages

Access messages on your iSeries server with iSeries Access for Web.

Display messages

Display, answer and manage the messages in the message queue for the logged on user.

Send message

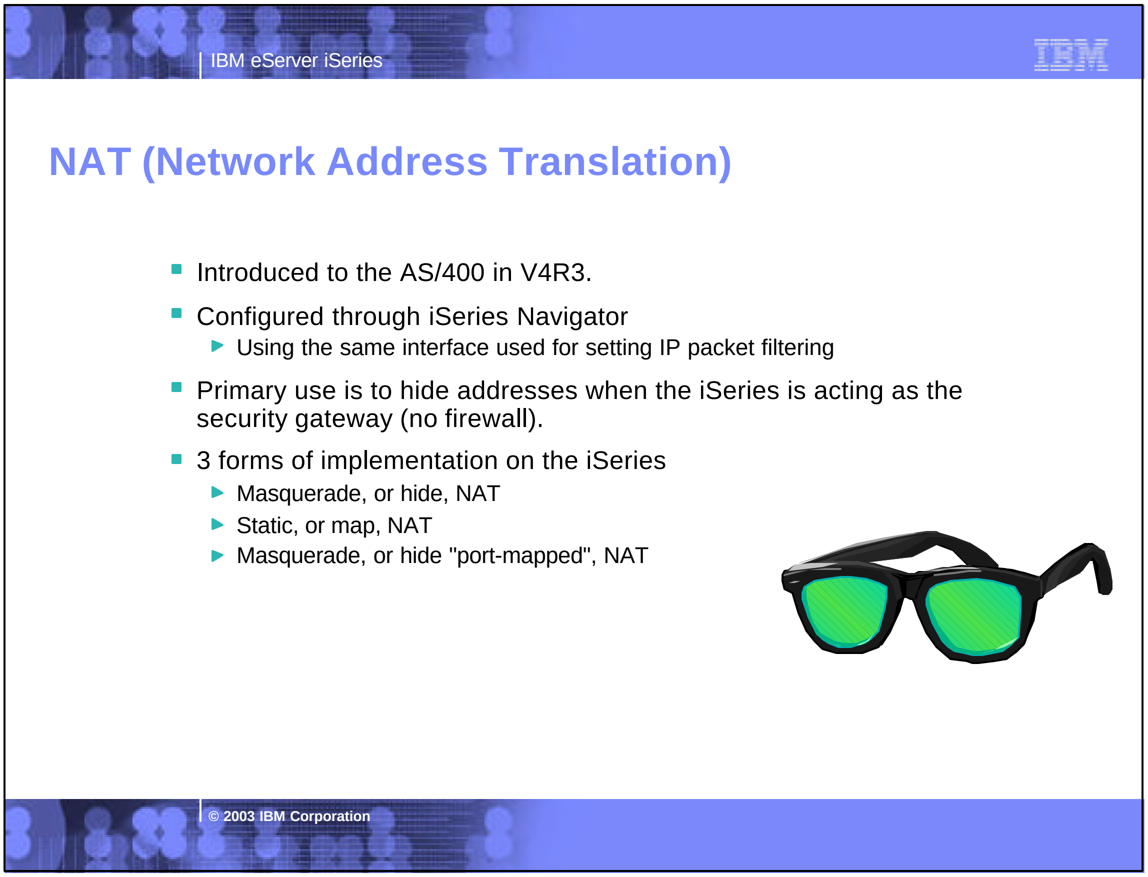
Send a message to users and message queues.

Operator messages

Display, answer and manage the messages in the system operator message queue.

Message queues

List message queues on the iSeries server. Select a message queue from this list and displ messages.

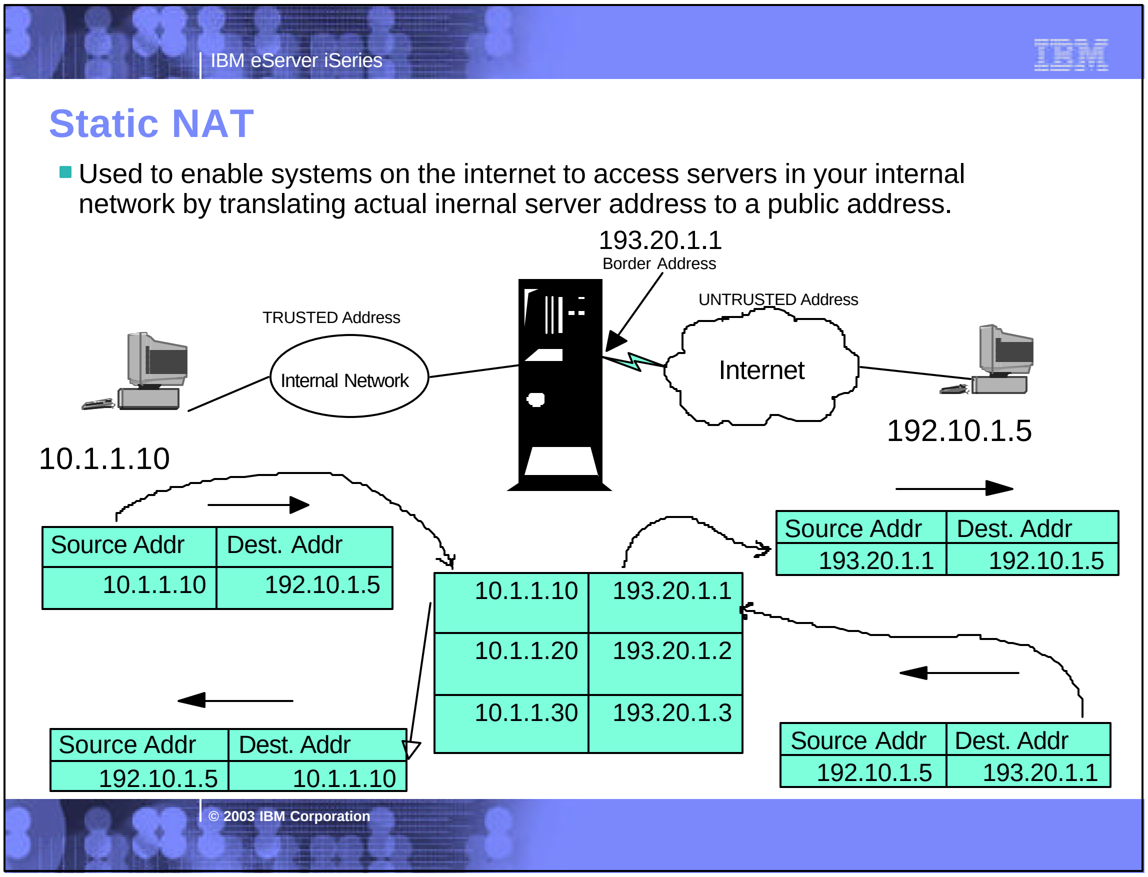


IBM eServer iSeries

NAT (Network Address Translation)

- Introduced to the AS/400 in V4R3.
- Configured through iSeries Navigator
  - Using the same interface used for setting IP packet filtering
- Primary use is to hide addresses when the iSeries is acting as the security gateway (no firewall).
- 3 forms of implementation on the iSeries
  - Masquerade, or hide, NAT
  - Static, or map, NAT
  - Masquerade, or hide "port-mapped", NAT

© 2003 IBM Corporation



IBM eServer iSeries

Static NAT

- Used to enable systems on the internet to access servers in your internal network by translating actual inernal server address to a public address.

193.20.1.1
Border Address

UNTRUSTED Address

TRUSTED Address

Internal Network

Internet

192.10.1.5

10.1.1.10

Source Addr	Dest. Addr
10.1.1.10	192.10.1.5

Source Addr	Dest. Addr
193.20.1.1	192.10.1.5

10.1.1.10	193.20.1.1
10.1.1.20	193.20.1.2
10.1.1.30	193.20.1.3

Source Addr	Dest. Addr
192.10.1.5	10.1.1.10

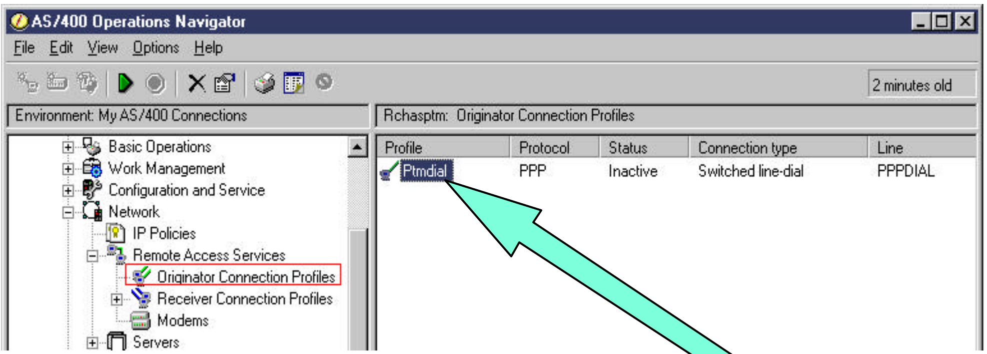
Source Addr	Dest. Addr
192.10.1.5	193.20.1.1

© 2003 IBM Corporation

IBM eServer iSeries

Configuring NAT

- All configuration is done using iSeries Navigator



Environment: My AS/400 Connections

- Basic Operations
- Work Management
- Configuration and Service
- Network
  - IP Policies
  - Remote Access Services
    - Originator Connection Profiles
    - Receiver Connection Profiles
    - Modems
  - Servers

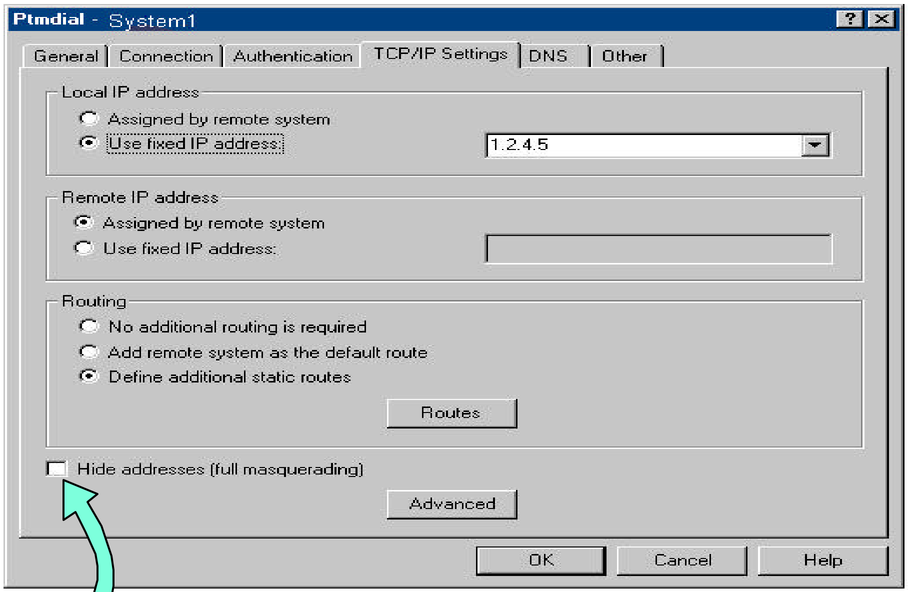
Rchasptm: Originator Connection Profiles

Profile	Protocol	Status	Connection type	Line
Ptmdial	PPP	Inactive	Switched line-dial	PPPDIAL

Right-click here and go to properties

IBM eServer iSeries

Configuring NAT



Local IP address
○ Assigned by remote system
● Use fixed IP address: 1.2.4.5

Remote IP address
● Assigned by remote system
○ Use fixed IP address:

Routing
○ No additional routing is required
○ Add remote system as the default route
● Define additional static routes

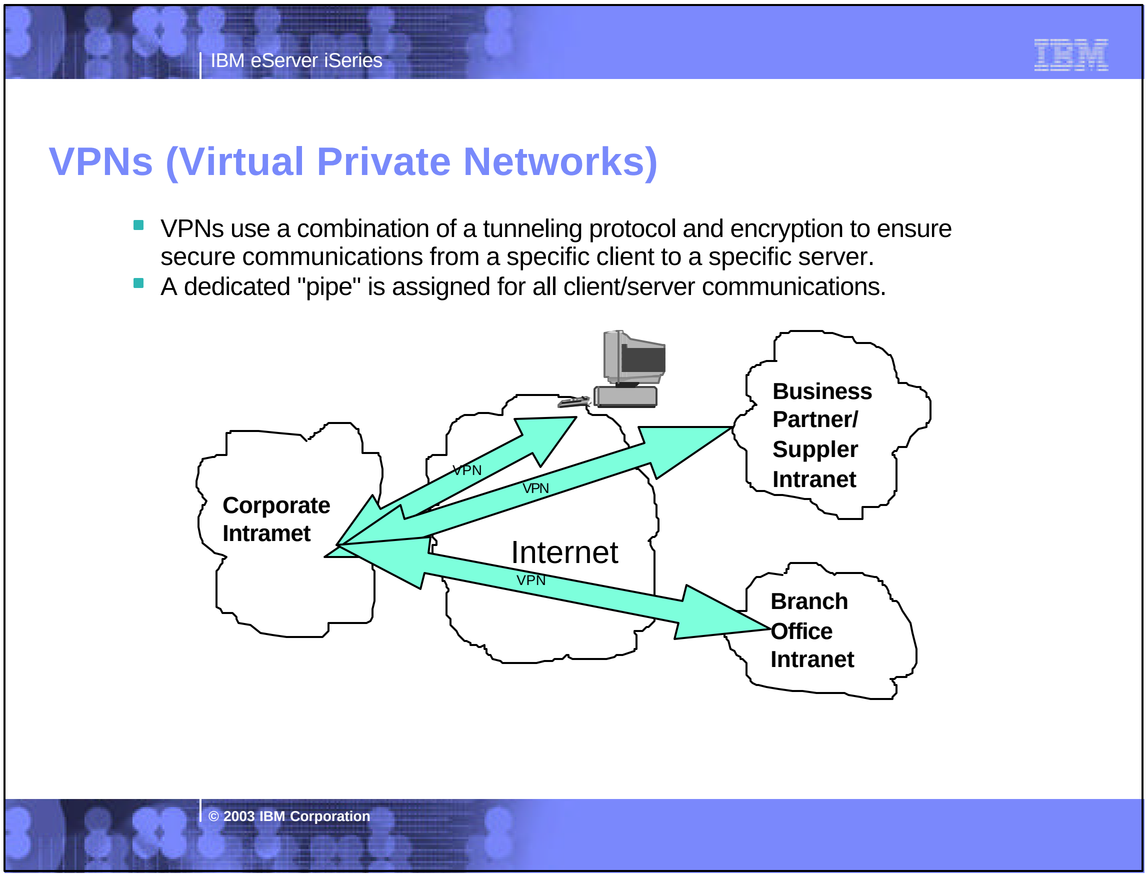
□ Hide addresses (full masquerading)

Click here to turn on hiding

IBM eServer iSeries

IBM

VPN Support

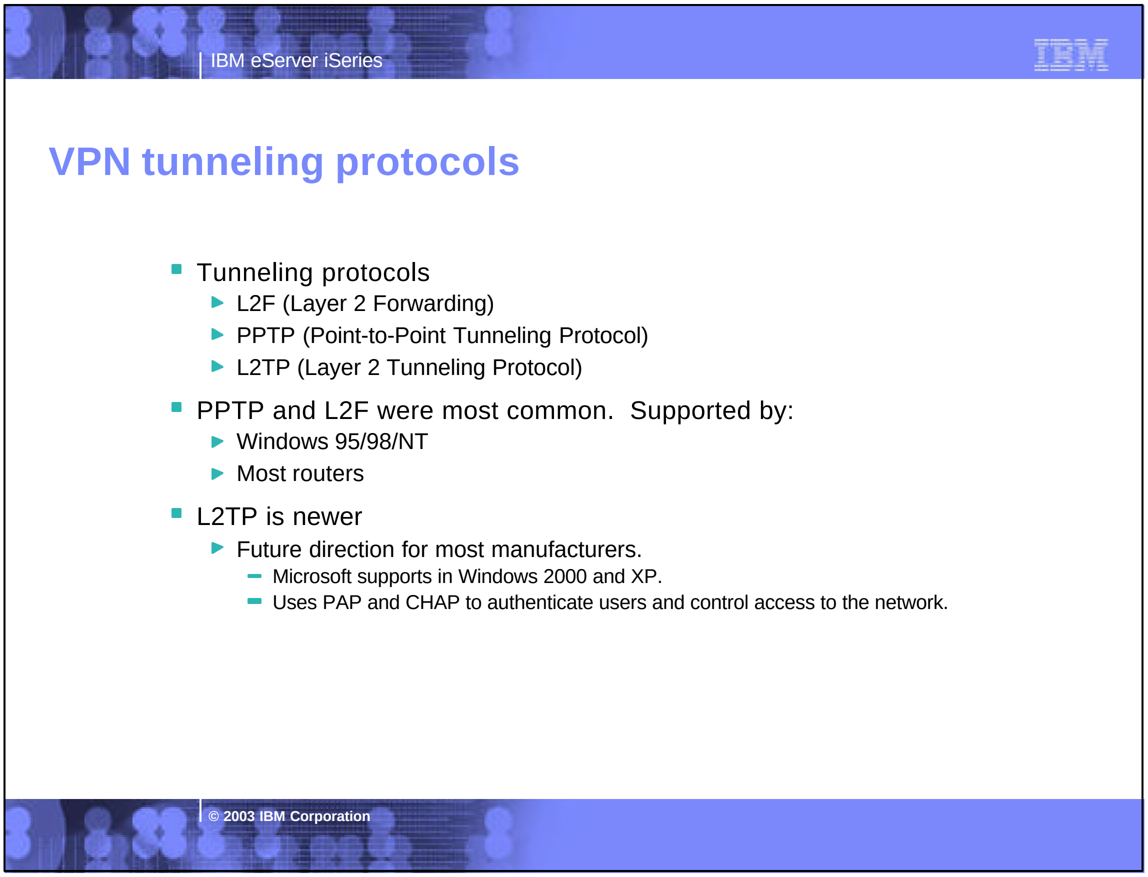


IBM eServer iSeries

IBM

VPNs (Virtual Private Networks)

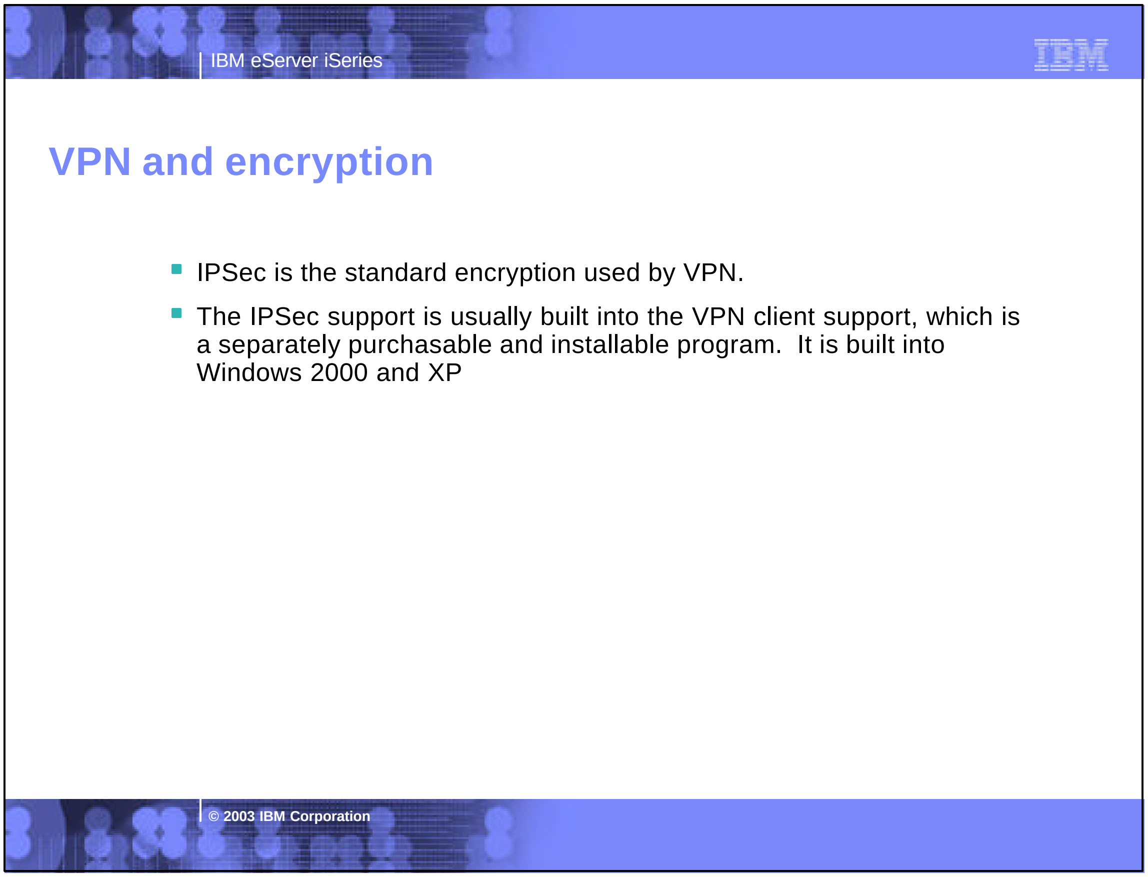
- VPNs use a combination of a tunneling protocol and encryption to ensure secure communications from a specific client to a specific server.
- A dedicated "pipe" is assigned for all client/server communications.



IBM eServer iSeries

VPN tunneling protocols

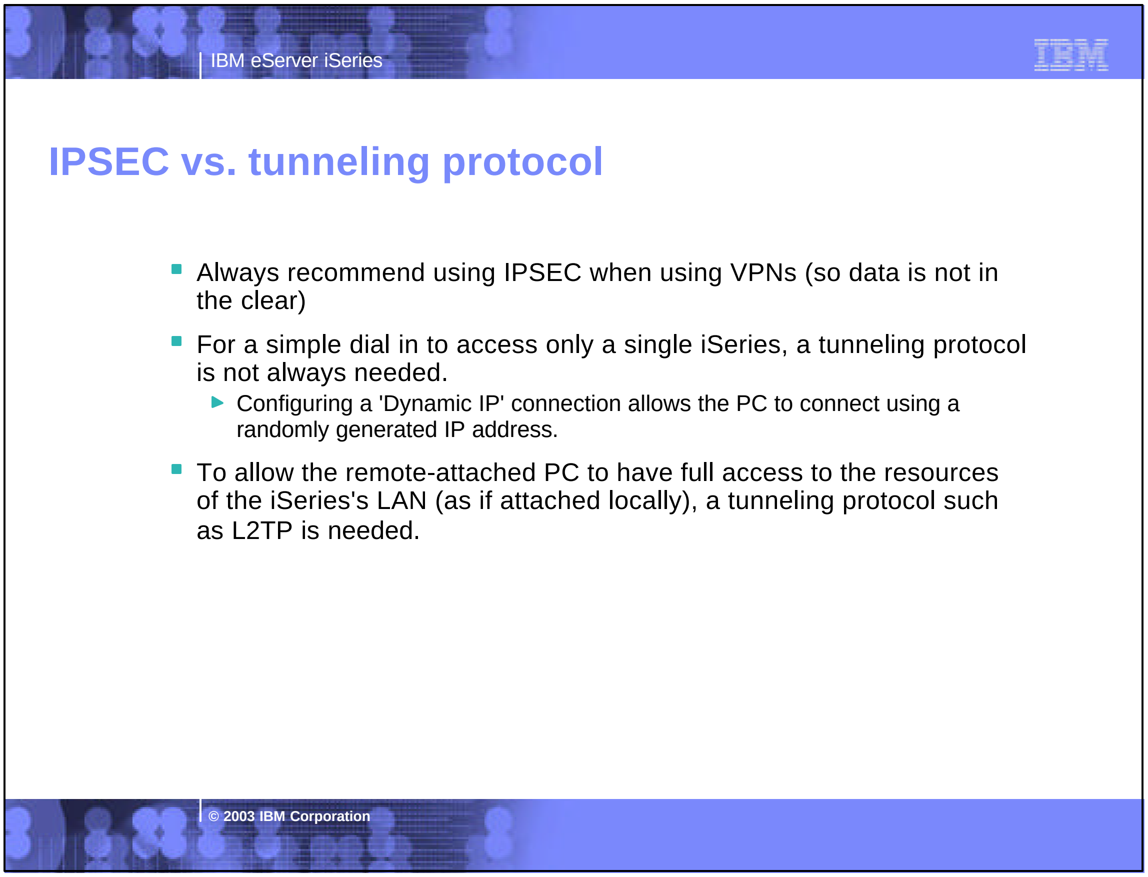
- Tunneling protocols
  - L2F (Layer 2 Forwarding)
  - PPTP (Point-to-Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
- PPTP and L2F were most common. Supported by:
  - Windows 95/98/NT
  - Most routers
- L2TP is newer
  - Future direction for most manufacturers.
    - Microsoft supports in Windows 2000 and XP.
    - Uses PAP and CHAP to authenticate users and control access to the network.



IBM eServer iSeries

VPN and encryption

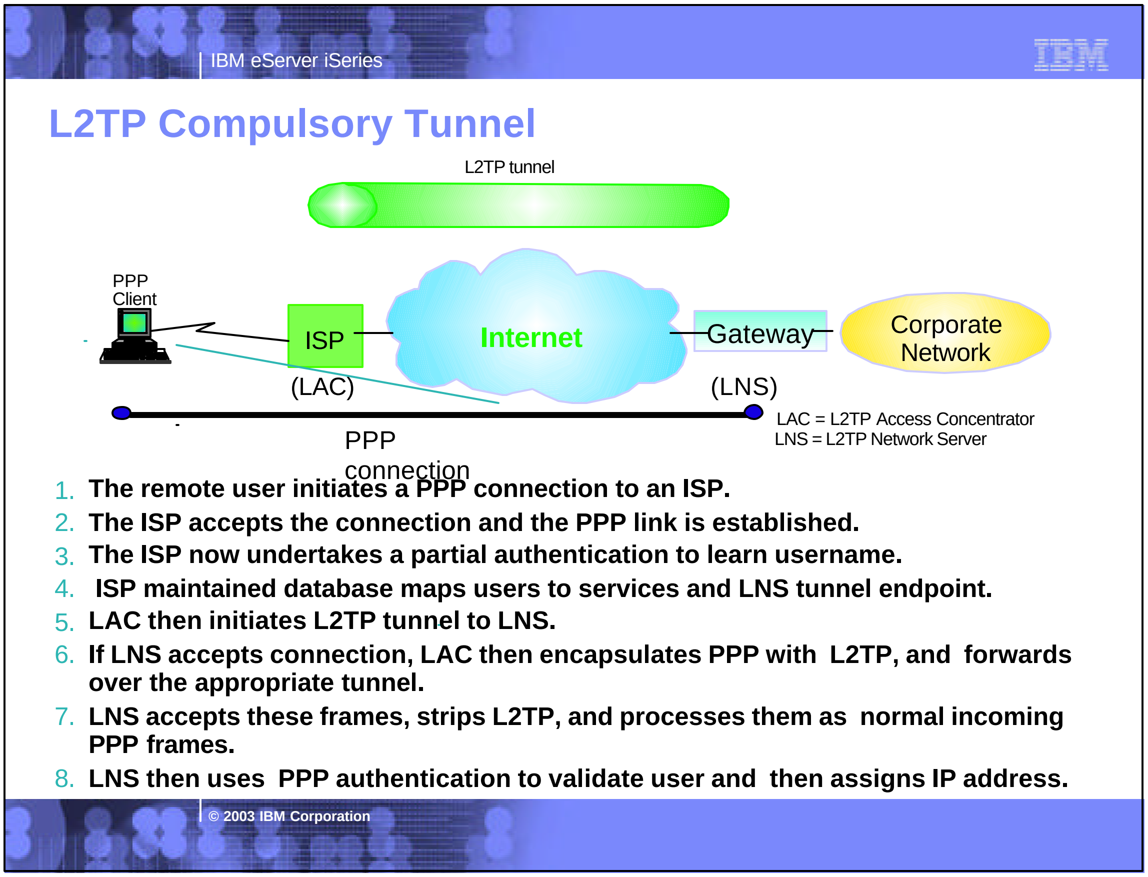
- IPSec is the standard encryption used by VPN.
- The IPSec support is usually built into the VPN client support, which is a separately purchasable and installable program. It is built into Windows 2000 and XP



IBM eServer iSeries

IPSEC vs. tunneling protocol

- Always recommend using IPSEC when using VPNs (so data is not in the clear)
- For a simple dial in to access only a single iSeries, a tunneling protocol is not always needed.
  - Configuring a 'Dynamic IP' connection allows the PC to connect using a randomly generated IP address.
- To allow the remote-attached PC to have full access to the resources of the iSeries's LAN (as if attached locally), a tunneling protocol such as L2TP is needed.

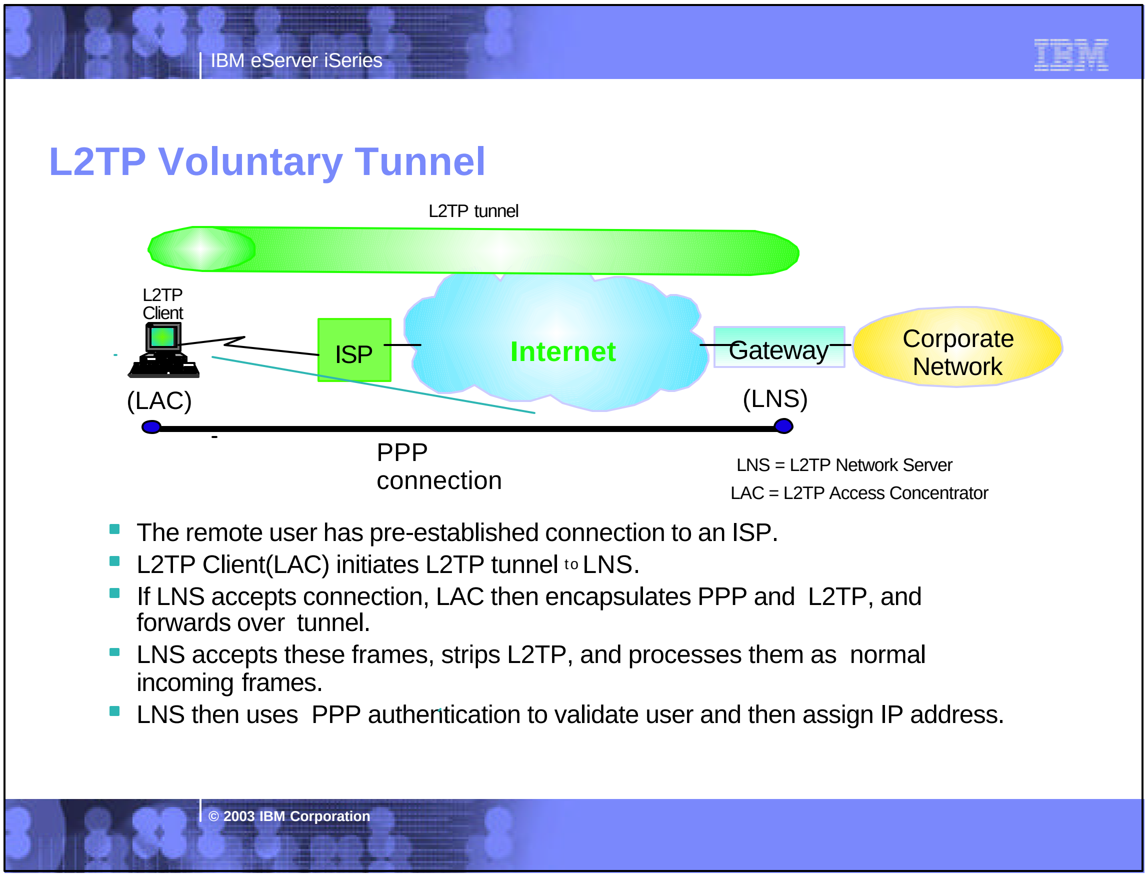


IBM eServer iSeries

L2TP Compulsory Tunnel

LAC = L2TP Access Concentrator
LNS = L2TP Network Server

1. The remote user initiates a PPP connection to an ISP.
2. The ISP accepts the connection and the PPP link is established.
3. The ISP now undertakes a partial authentication to learn username.
4. ISP maintained database maps users to services and LNS tunnel endpoint.
5. LAC then initiates L2TP tunnel to LNS.
6. If LNS accepts connection, LAC then encapsulates PPP with L2TP, and forwards over the appropriate tunnel.
7. LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.
8. LNS then uses PPP authentication to validate user and then assigns IP address.



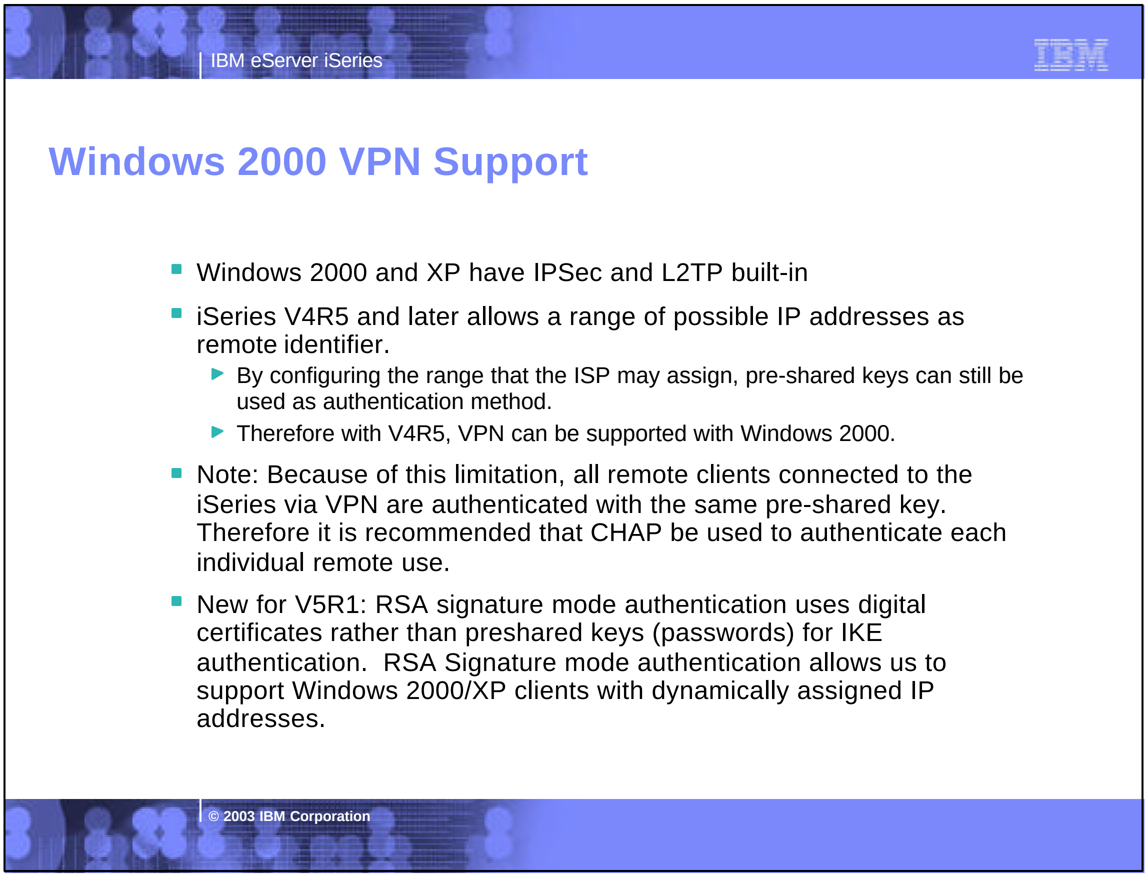
IBM eServer iSeries

L2TP Voluntary Tunnel

LNS = L2TP Network Server

LAC = L2TP Access Concentrator

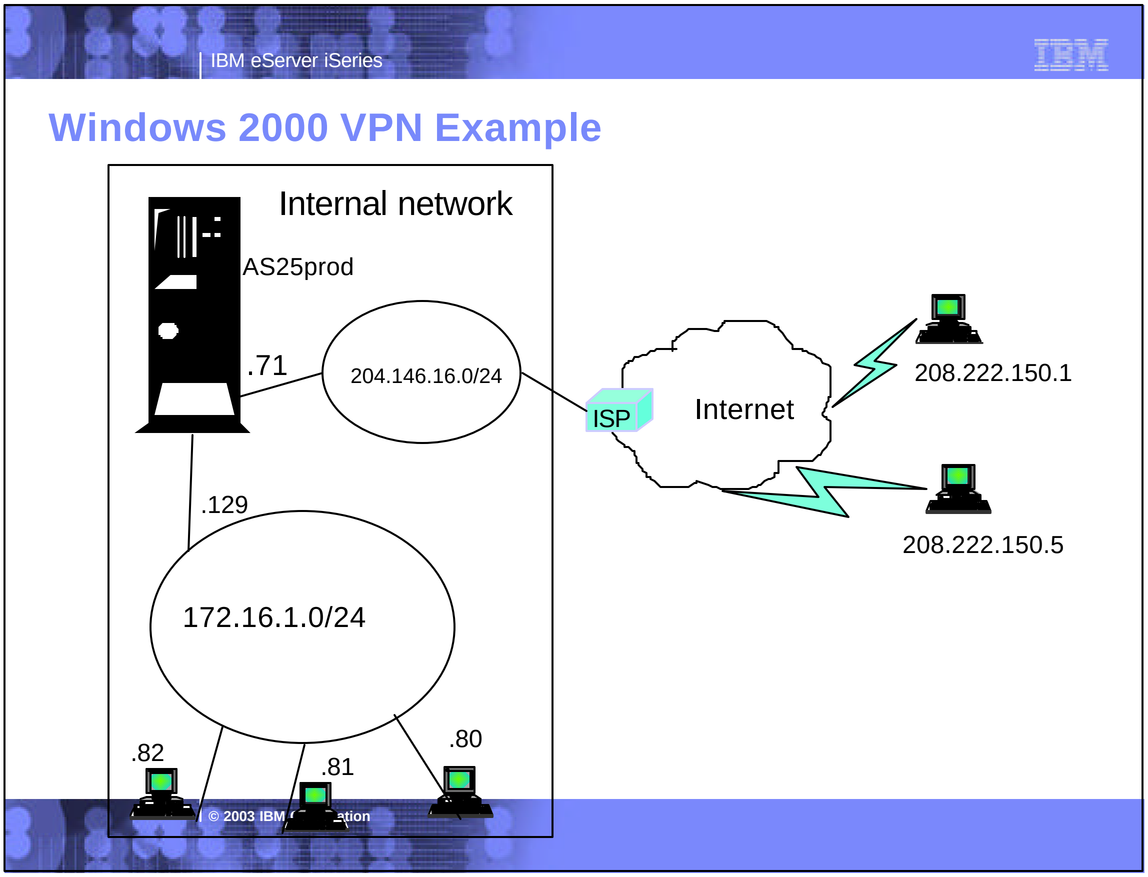
- The remote user has pre-established connection to an ISP.
- L2TP Client(LAC) initiates L2TP tunnel to LNS.
- If LNS accepts connection, LAC then encapsulates PPP and L2TP, and forwards over tunnel.
- LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.
- LNS then uses PPP authentication to validate user and then assign IP address.



IBM eServer iSeries

Windows 2000 VPN Support

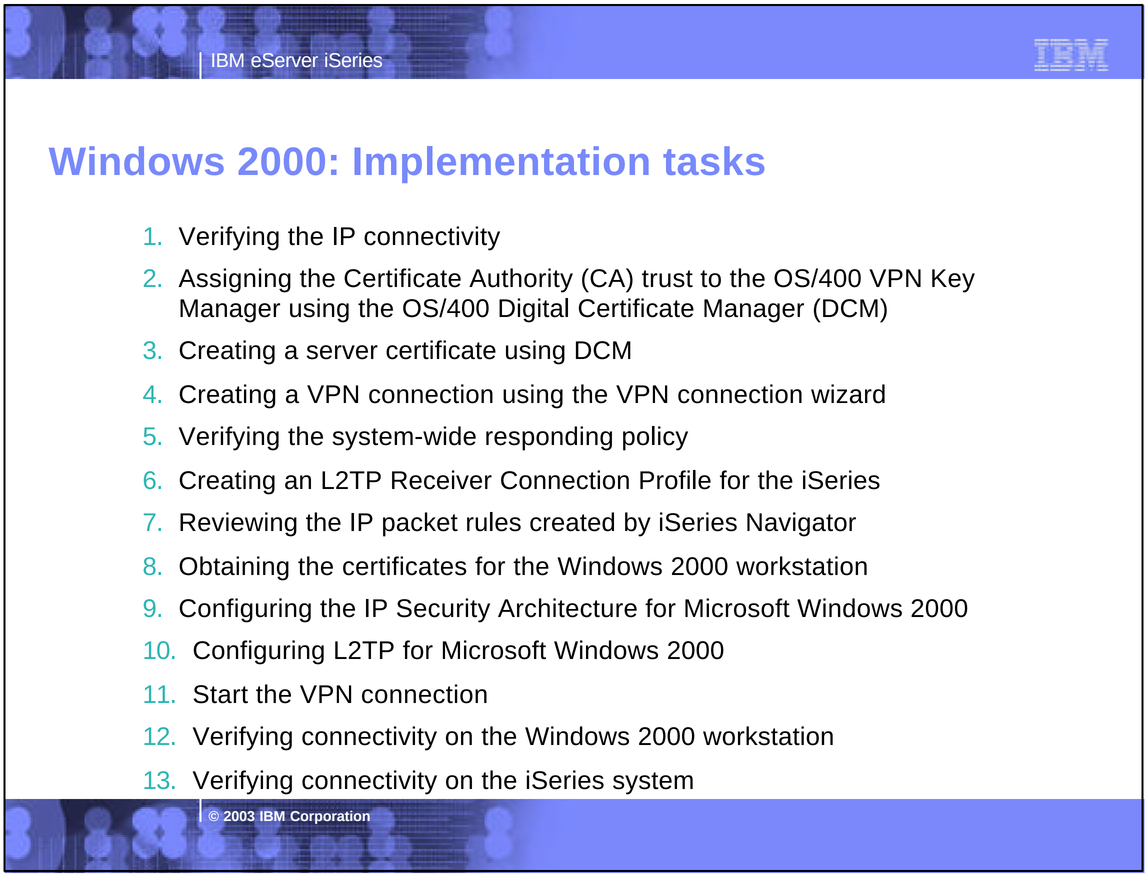
- Windows 2000 and XP have IPSec and L2TP built-in
- iSeries V4R5 and later allows a range of possible IP addresses as remote identifier.
  - By configuring the range that the ISP may assign, pre-shared keys can still be used as authentication method.
  - Therefore with V4R5, VPN can be supported with Windows 2000.
- Note: Because of this limitation, all remote clients connected to the iSeries via VPN are authenticated with the same pre-shared key. Therefore it is recommended that CHAP be used to authenticate each individual remote use.
- New for V5R1: RSA signature mode authentication uses digital certificates rather than preshared keys (passwords) for IKE authentication. RSA Signature mode authentication allows us to support Windows 2000/XP clients with dynamically assigned IP addresses.



IBM eServer iSeries

Windows 2000 VPN Example

© 2003 IBM Corporation

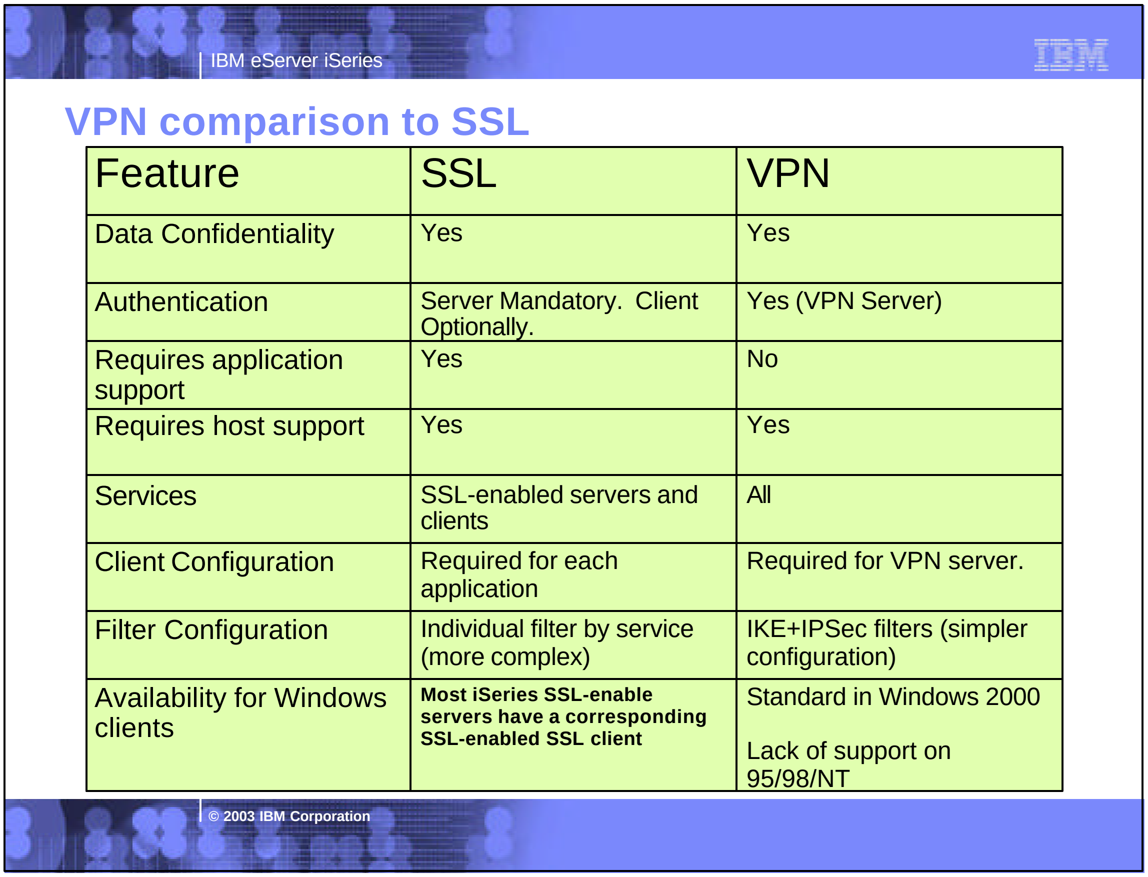


IBM eServer iSeries

Windows 2000: Implementation tasks

1. Verifying the IP connectivity
2. Assigning the Certificate Authority (CA) trust to the OS/400 VPN Key Manager using the OS/400 Digital Certificate Manager (DCM)
3. Creating a server certificate using DCM
4. Creating a VPN connection using the VPN connection wizard
5. Verifying the system-wide responding policy
6. Creating an L2TP Receiver Connection Profile for the iSeries
7. Reviewing the IP packet rules created by iSeries Navigator
8. Obtaining the certificates for the Windows 2000 workstation
9. Configuring the IP Security Architecture for Microsoft Windows 2000
10. Configuring L2TP for Microsoft Windows 2000
11. Start the VPN connection
12. Verifying connectivity on the Windows 2000 workstation
13. Verifying connectivity on the iSeries system

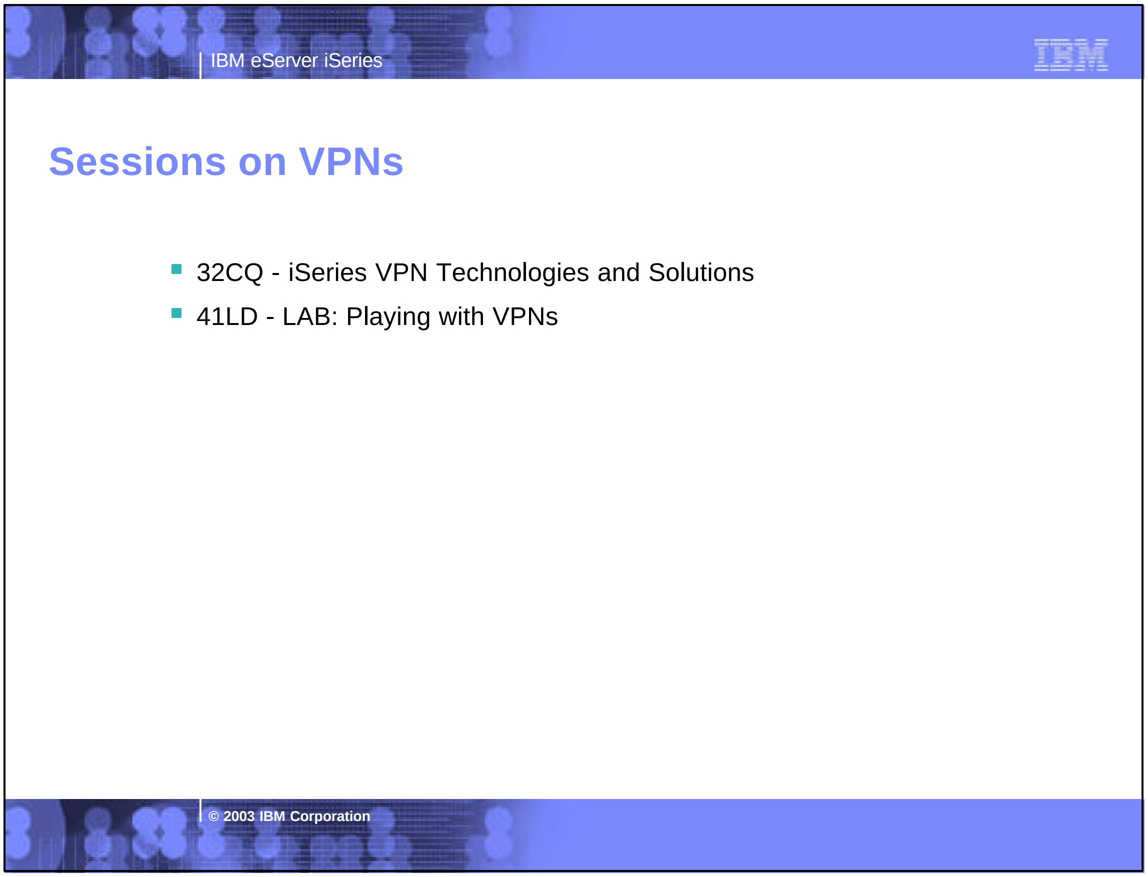
© 2003 IBM Corporation



IBM eServer iSeries

VPN comparison to SSL

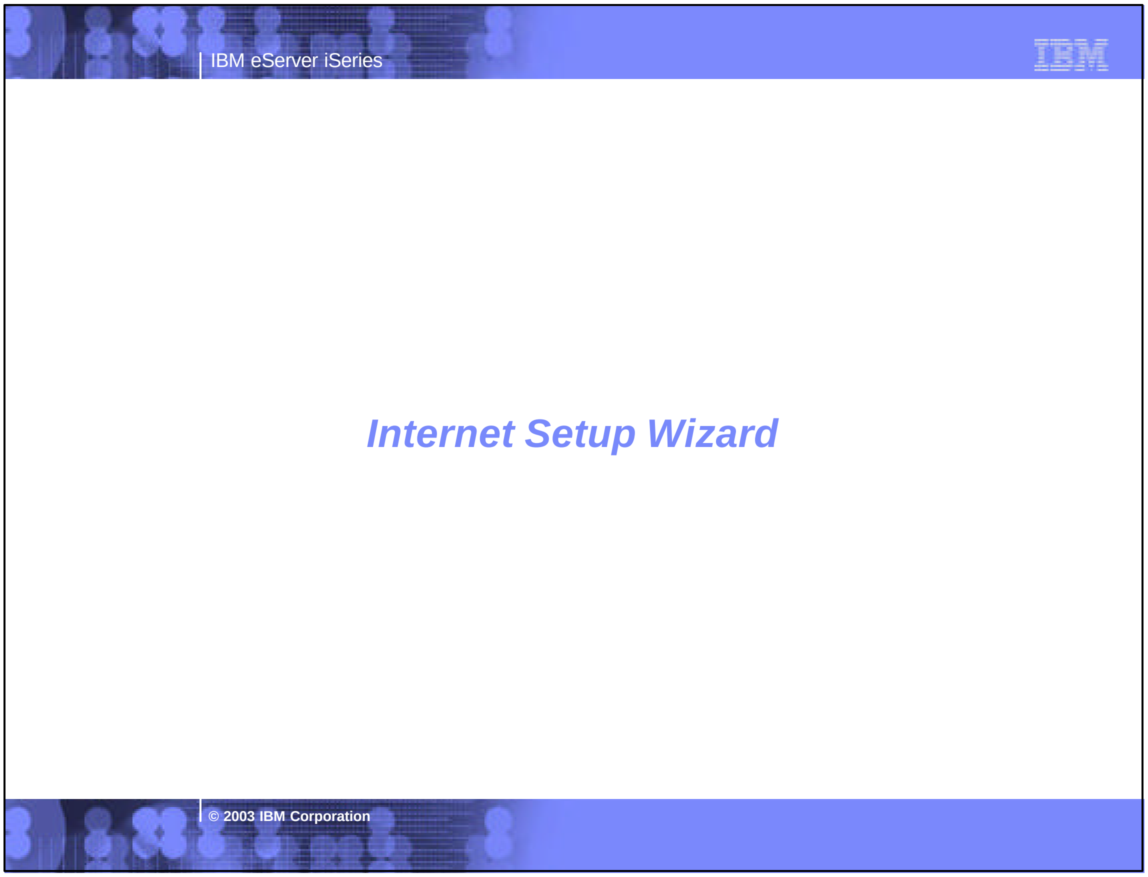
Feature	SSL	VPN
Data Confidentiality	Yes	Yes
Authentication	Server Mandatory. Client Optionally.	Yes (VPN Server)
Requires application support	Yes	No
Requires host support	Yes	Yes
Services	SSL-enabled servers and clients	All
Client Configuration	Required for each application	Required for VPN server.
Filter Configuration	Individual filter by service (more complex)	IKE+IPSec filters (simpler configuration)
Availability for Windows clients	**Most iSeries SSL-enable servers have a corresponding SSL-enabled SSL client**	Standard in Windows 2000 Lack of support on 95/98/NT



IBM eServer iSeries

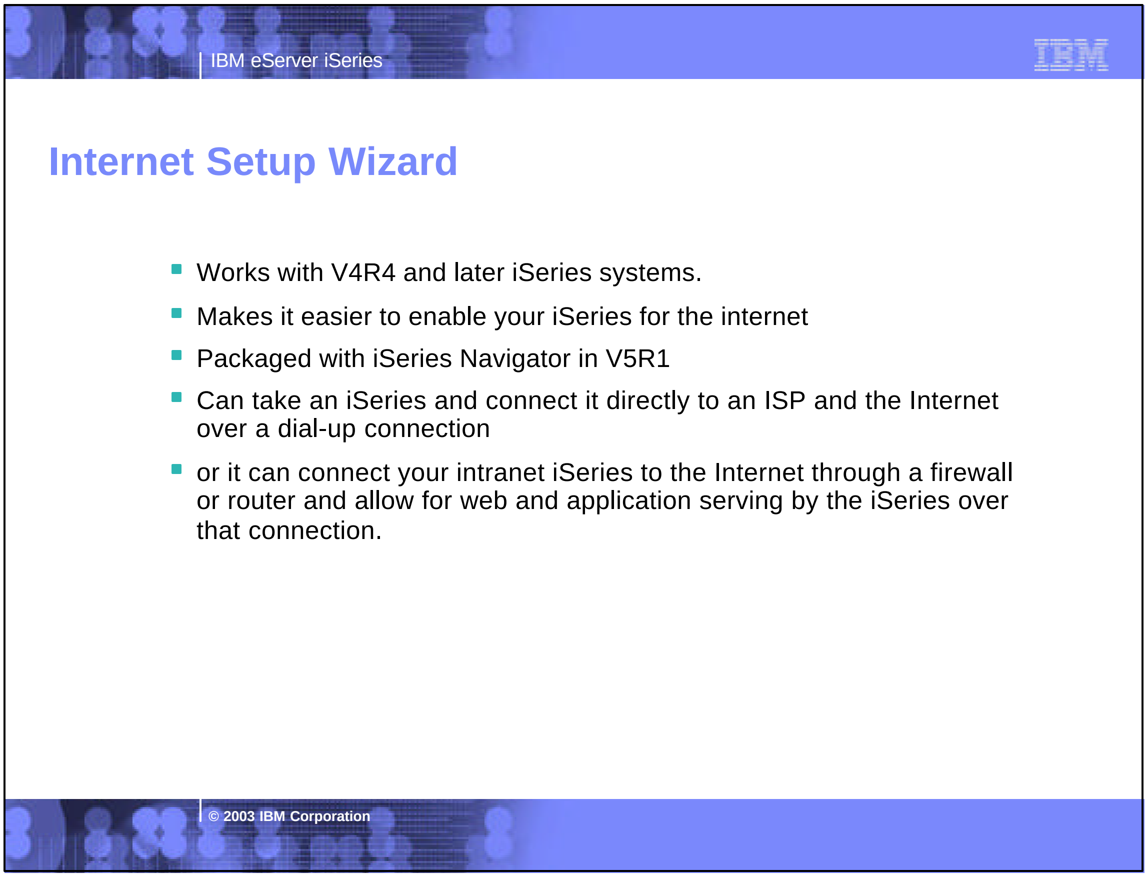
Sessions on VPNs

- 32CQ - iSeries VPN Technologies and Solutions
- 41LD - LAB: Playing with VPNs



IBM eServer iSeries

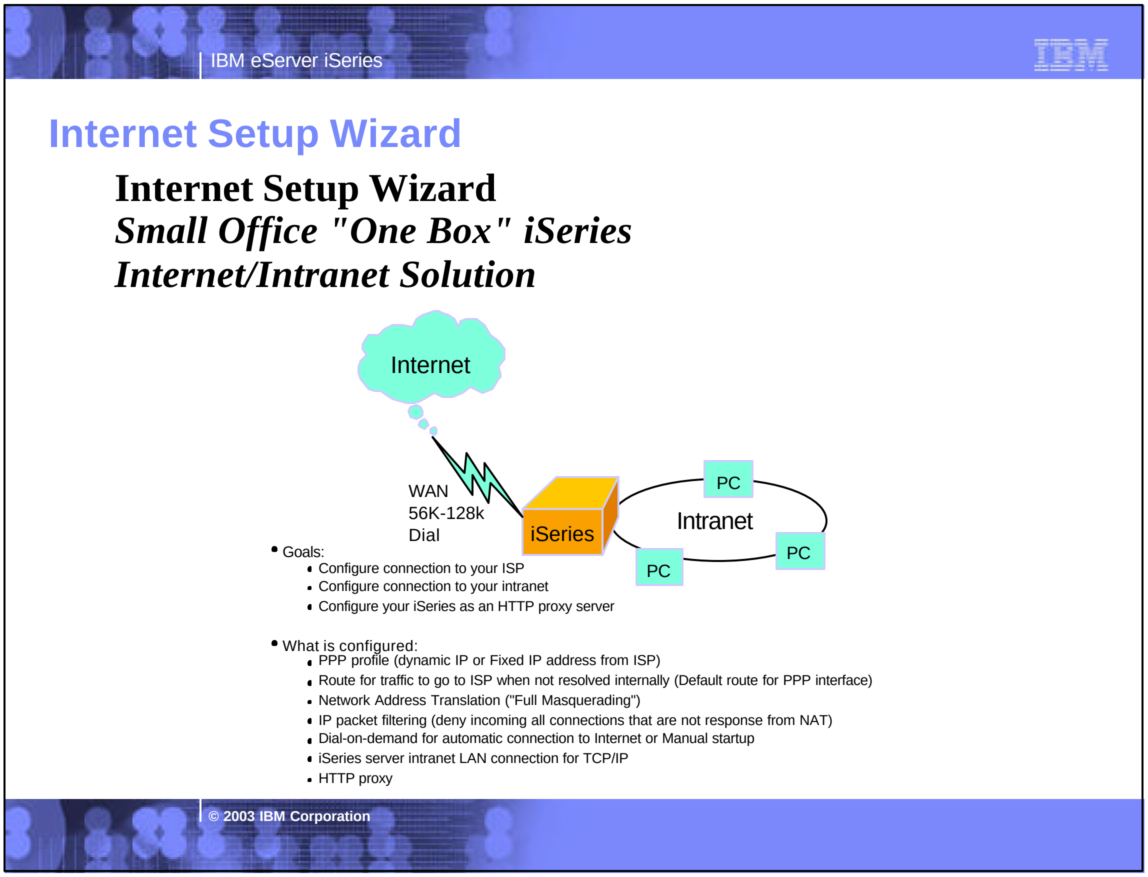
Internet Setup Wizard



IBM eServer iSeries

Internet Setup Wizard

- Works with V4R4 and later iSeries systems.
- Makes it easier to enable your iSeries for the internet
- Packaged with iSeries Navigator in V5R1
- Can take an iSeries and connect it directly to an ISP and the Internet over a dial-up connection
- or it can connect your intranet iSeries to the Internet through a firewall or router and allow for web and application serving by the iSeries over that connection.

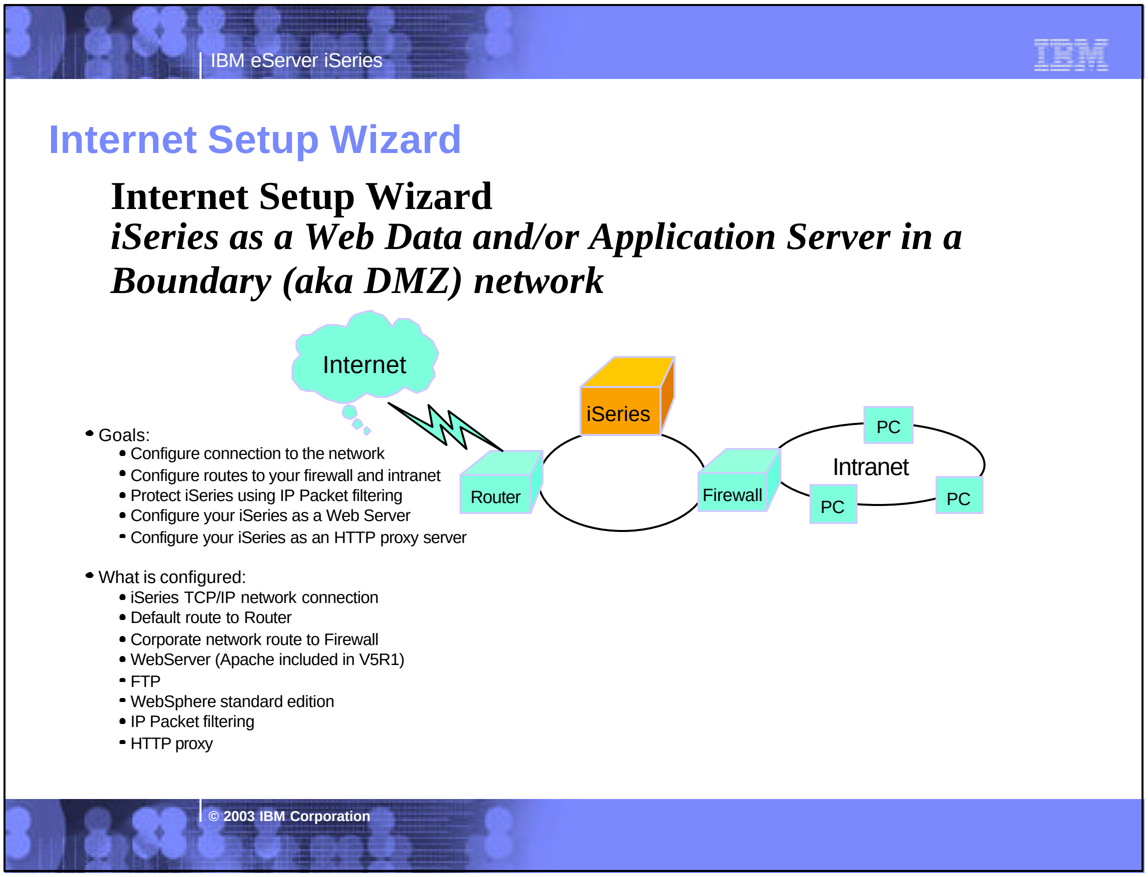


Internet Setup Wizard

Internet Setup Wizard
Small Office "One Box" iSeries
Internet/Intranet Solution

- Goals:
  - Configure connection to your ISP
  - Configure connection to your intranet
  - Configure your iSeries as an HTTP proxy server

- What is configured:
  - PPP profile (dynamic IP or Fixed IP address from ISP)
  - Route for traffic to go to ISP when not resolved internally (Default route for PPP interface)
  - Network Address Translation ("Full Masquerading")
  - IP packet filtering (deny incoming all connections that are not response from NAT)
  - Dial-on-demand for automatic connection to Internet or Manual startup
  - iSeries server intranet LAN connection for TCP/IP
  - HTTP proxy

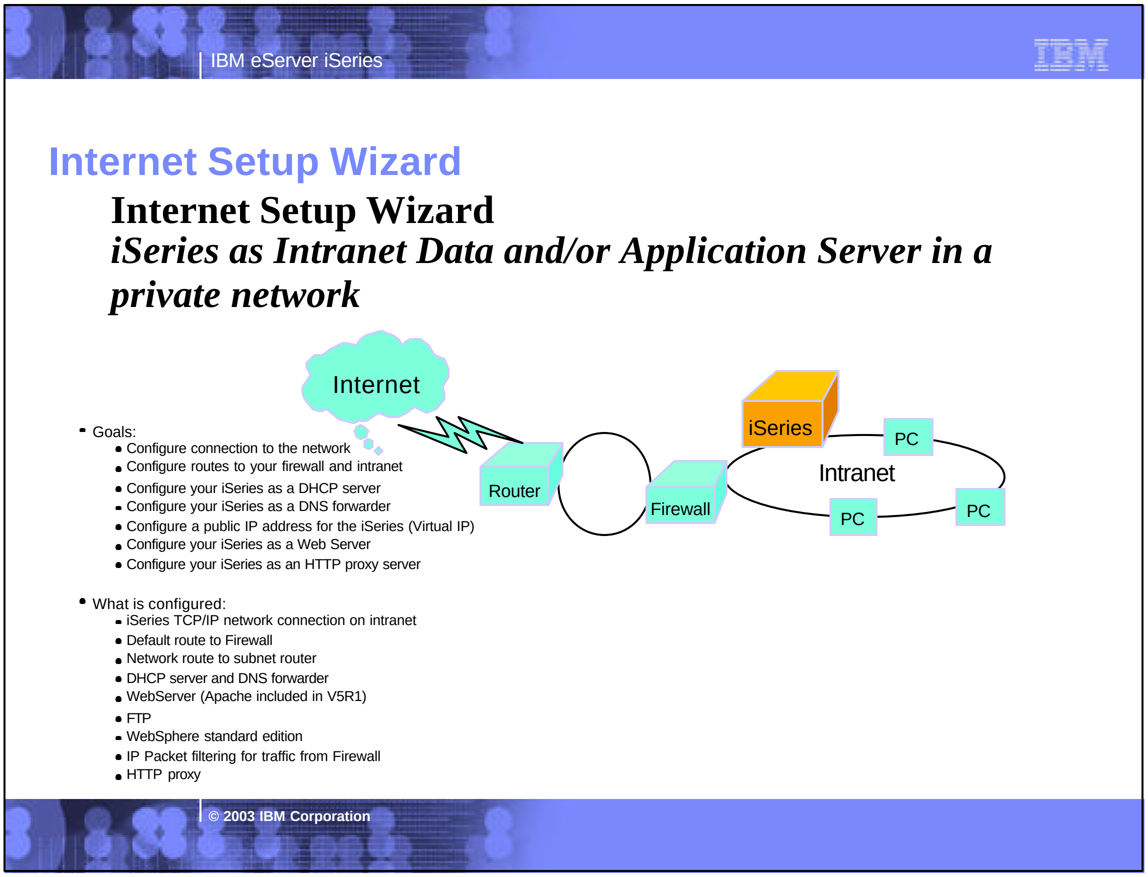


Internet Setup Wizard

Internet Setup Wizard
iSeries as a Web Data and/or Application Server in a Boundary (aka DMZ) network

- Goals:
  - Configure connection to the network
  - Configure routes to your firewall and intranet
  - Protect iSeries using IP Packet filtering
  - Configure your iSeries as a Web Server
  - Configure your iSeries as an HTTP proxy server

- What is configured:
  - iSeries TCP/IP network connection
  - Default route to Router
  - Corporate network route to Firewall
  - WebServer (Apache included in V5R1)
  - FTP
  - WebSphere standard edition
  - IP Packet filtering
  - HTTP proxy



IBM eServer iSeries

Internet Setup Wizard

Internet Setup Wizard
iSeries as Intranet Data and/or Application Server in a private network

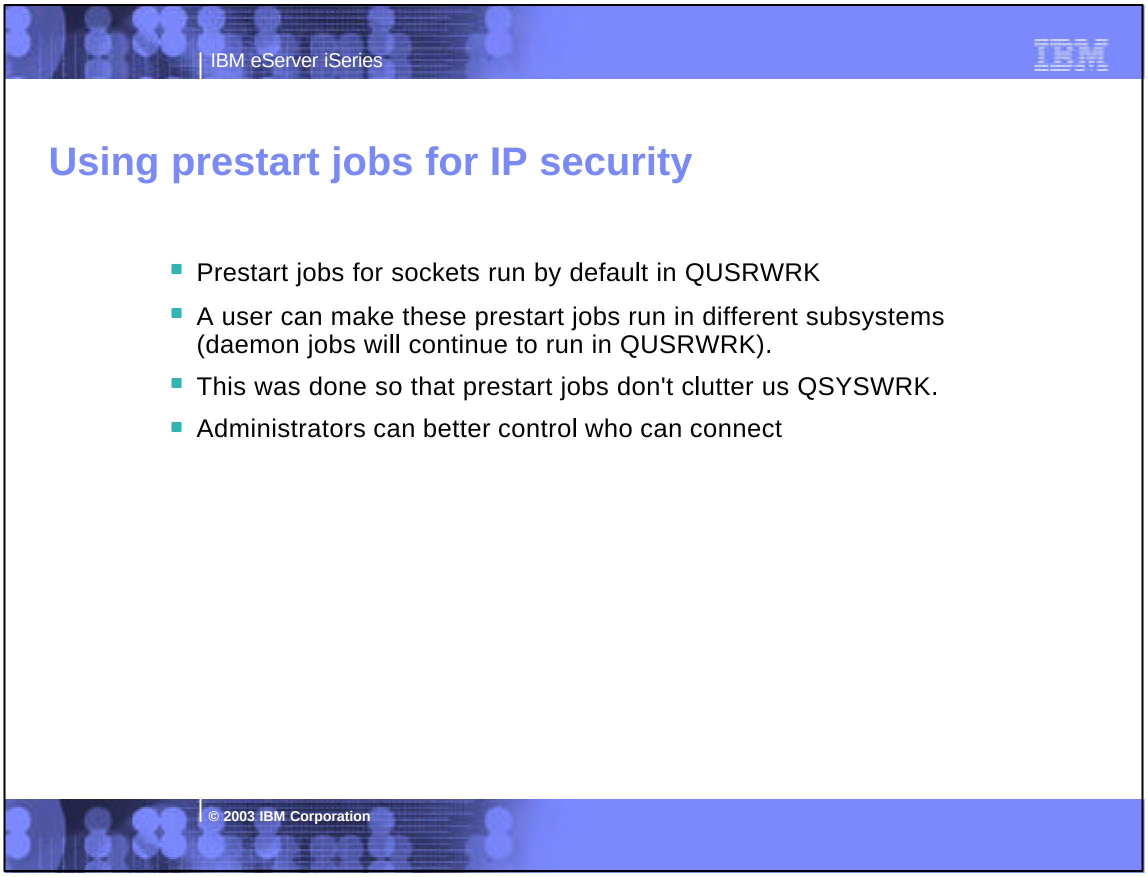
Internet
Router
Firewall
iSeries
PC
Intranet
PC
PC

- Goals:
  - Configure connection to the network
  - Configure routes to your firewall and intranet
  - Configure your iSeries as a DHCP server
  - Configure your iSeries as a DNS forwarder
  - Configure a public IP address for the iSeries (Virtual IP)
  - Configure your iSeries as a Web Server
  - Configure your iSeries as an HTTP proxy server

- What is configured:
  - iSeries TCP/IP network connection on intranet
  - Default route to Firewall
  - Network route to subnet router
  - DHCP server and DNS forwarder
  - WebServer (Apache included in V5R1)
  - FTP
  - WebSphere standard edition
  - IP Packet filtering for traffic from Firewall
  - HTTP proxy

IBM eServer iSeries

Prestart jobs

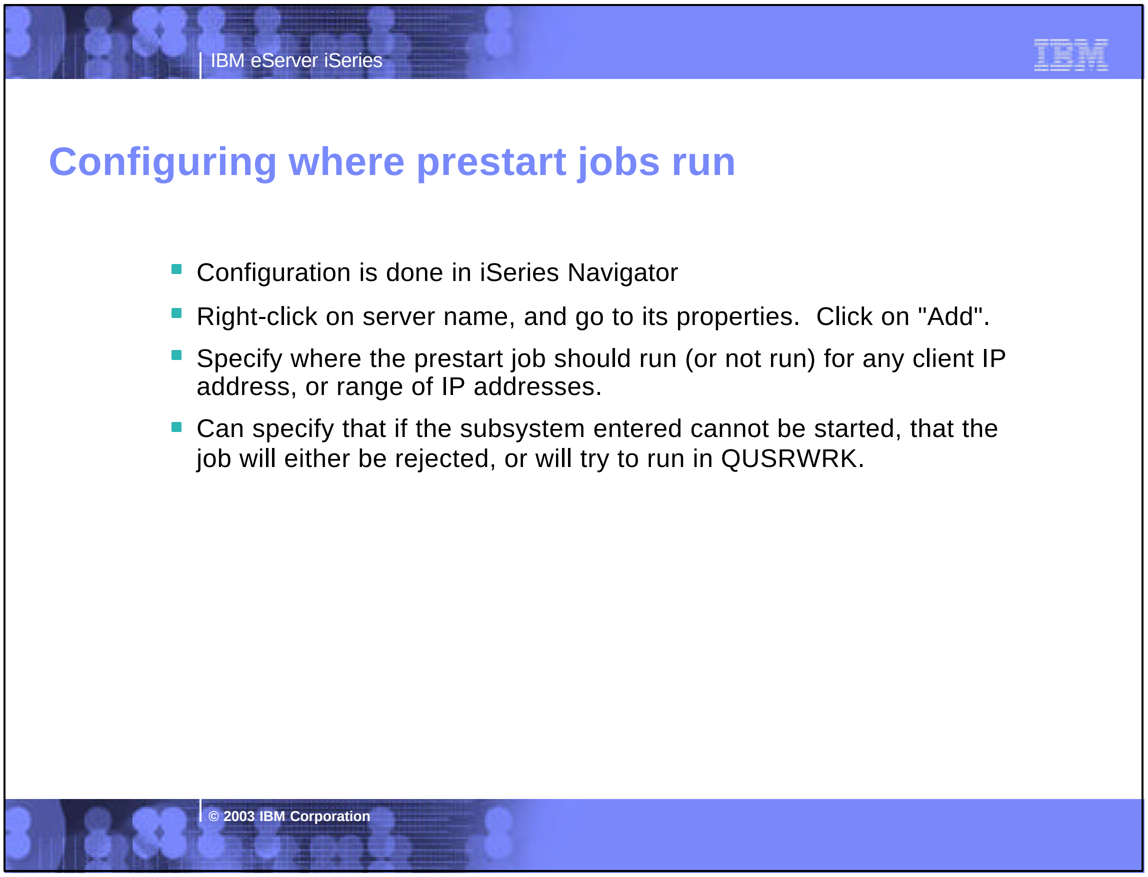


IBM eServer iSeries

IBM

Using prestart jobs for IP security

- Prestart jobs for sockets run by default in QUSRWRK
- A user can make these prestart jobs run in different subsystems (daemon jobs will continue to run in QUSRWRK).
- This was done so that prestart jobs don't clutter us QSYSWRK.
- Administrators can better control who can connect



IBM eServer iSeries

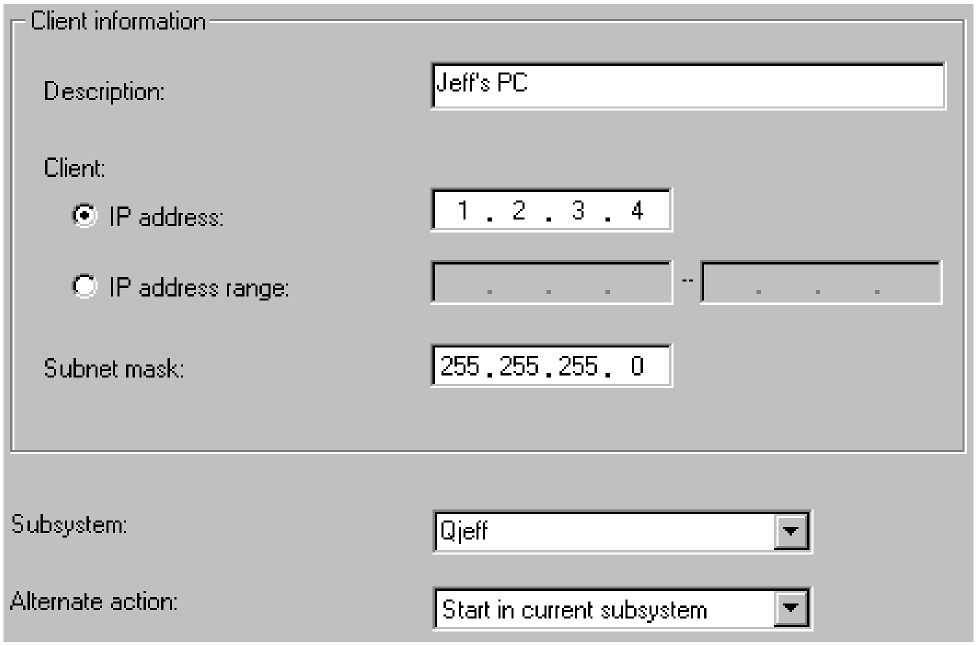
IBM

Configuring where prestart jobs run

- Configuration is done in iSeries Navigator
- Right-click on server name, and go to its properties. Click on "Add".
- Specify where the prestart job should run (or not run) for any client IP address, or range of IP addresses.
- Can specify that if the subsystem entered cannot be started, that the job will either be rejected, or will try to run in QUSRWRK.

IBM eServer iSeries

Prestart job config screen



Client information

Description: Jeff's PC

Client:

● IP address: 1 . 2 . 3 . 4

○ IP address range: . . . -- . . .

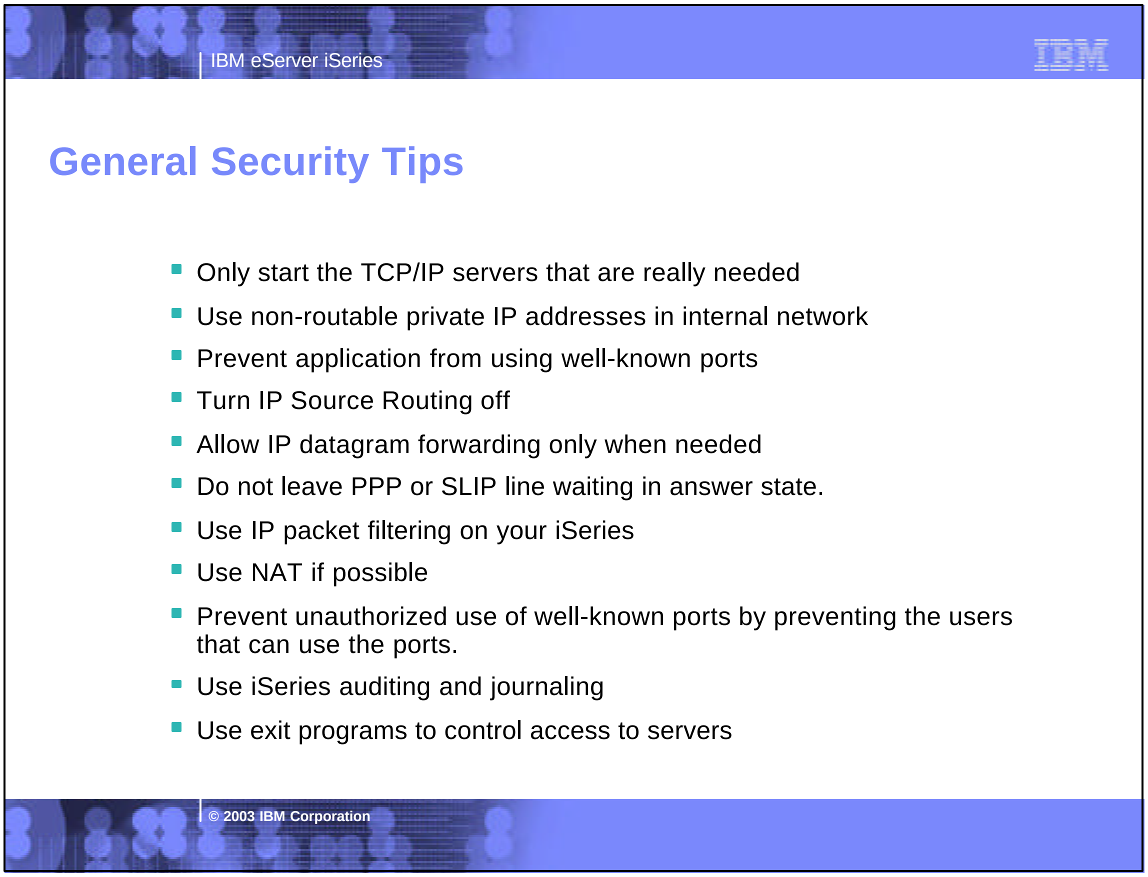
Subnet mask: 255 . 255 . 255 . 0

Subsystem: Qjeff

Alternate action: Start in current subsystem

IBM eServer iSeries

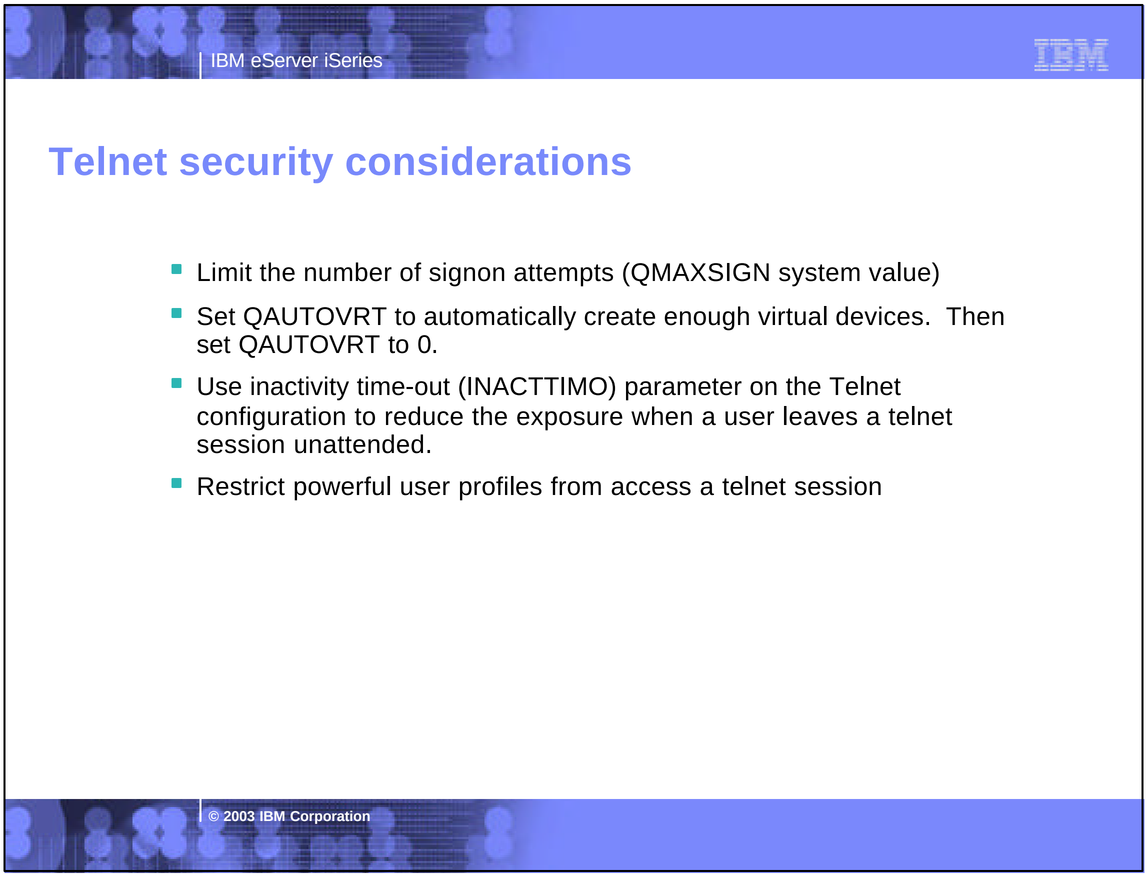
Other Security Tips



IBM eServer iSeries

General Security Tips

- Only start the TCP/IP servers that are really needed
- Use non-routable private IP addresses in internal network
- Prevent application from using well-known ports
- Turn IP Source Routing off
- Allow IP datagram forwarding only when needed
- Do not leave PPP or SLIP line waiting in answer state.
- Use IP packet filtering on your iSeries
- Use NAT if possible
- Prevent unauthorized use of well-known ports by preventing the users that can use the ports.
- Use iSeries auditing and journaling
- Use exit programs to control access to servers



IBM eServer iSeries

Telnet security considerations

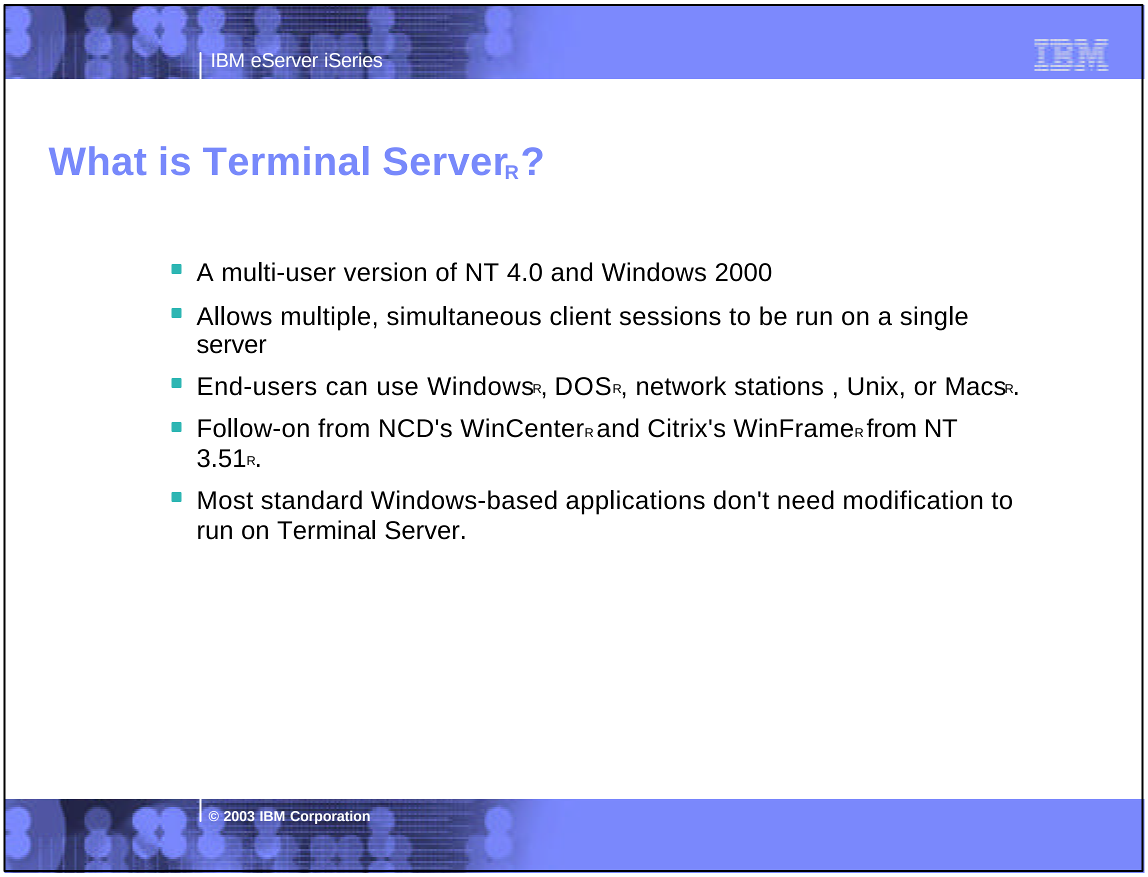
- Limit the number of signon attempts (QMAXSIGN system value)
- Set QAUTOVRT to automatically create enough virtual devices. Then set QAUTOVRT to 0.
- Use inactivity time-out (INACTTIMO) parameter on the Telnet configuration to reduce the exposure when a user leaves a telnet session unattended.
- Restrict powerful user profiles from access a telnet session

IBM eServer iSeries

IBM

Terminal Server Environment

© 2003 IBM Corporation



IBM eServer iSeries

IBM

What is Terminal Server$_R$?

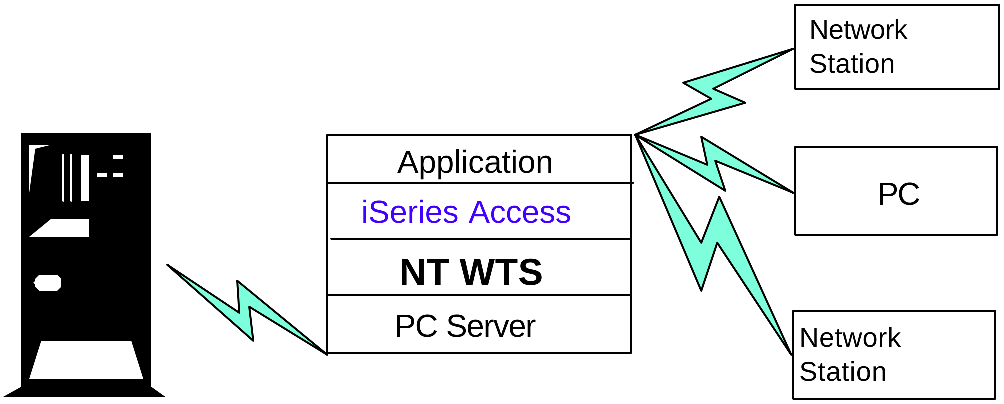
- A multi-user version of NT 4.0 and Windows 2000
- Allows multiple, simultaneous client sessions to be run on a single server
- End-users can use Windows$_R$, DOS$_R$, network stations , Unix, or Macs$_R$.
- Follow-on from NCD's WinCenter$_R$ and Citrix's WinFrame$_R$ from NT 3.51$_R$.
- Most standard Windows-based applications don't need modification to run on Terminal Server.

© 2003 IBM Corporation

IBM eServer iSeries

Where iSeries Access fits in

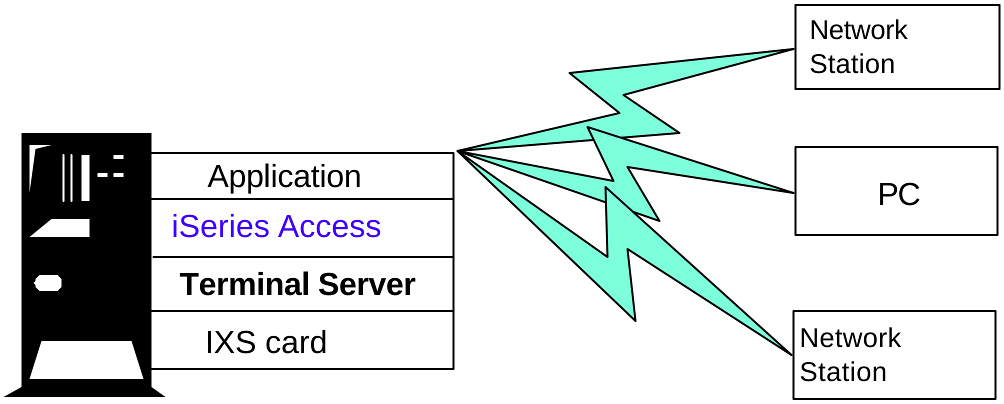
- iSeries Access R for Windows can run on Terminal Server, either on a standalone server.....

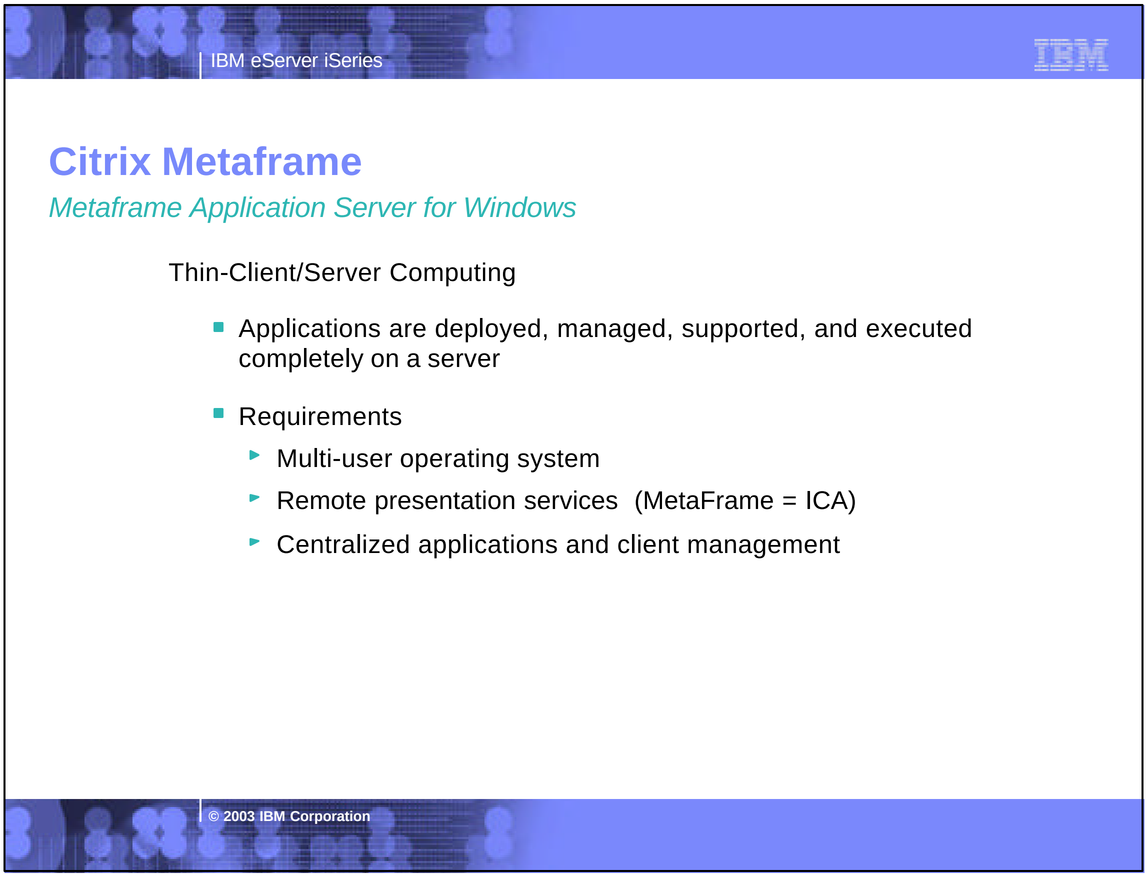


IBM eServer iSeries

Where Client Access fits in

- Or on an Integrated XSeries Server card in the iSeries





IBM eServer iSeries

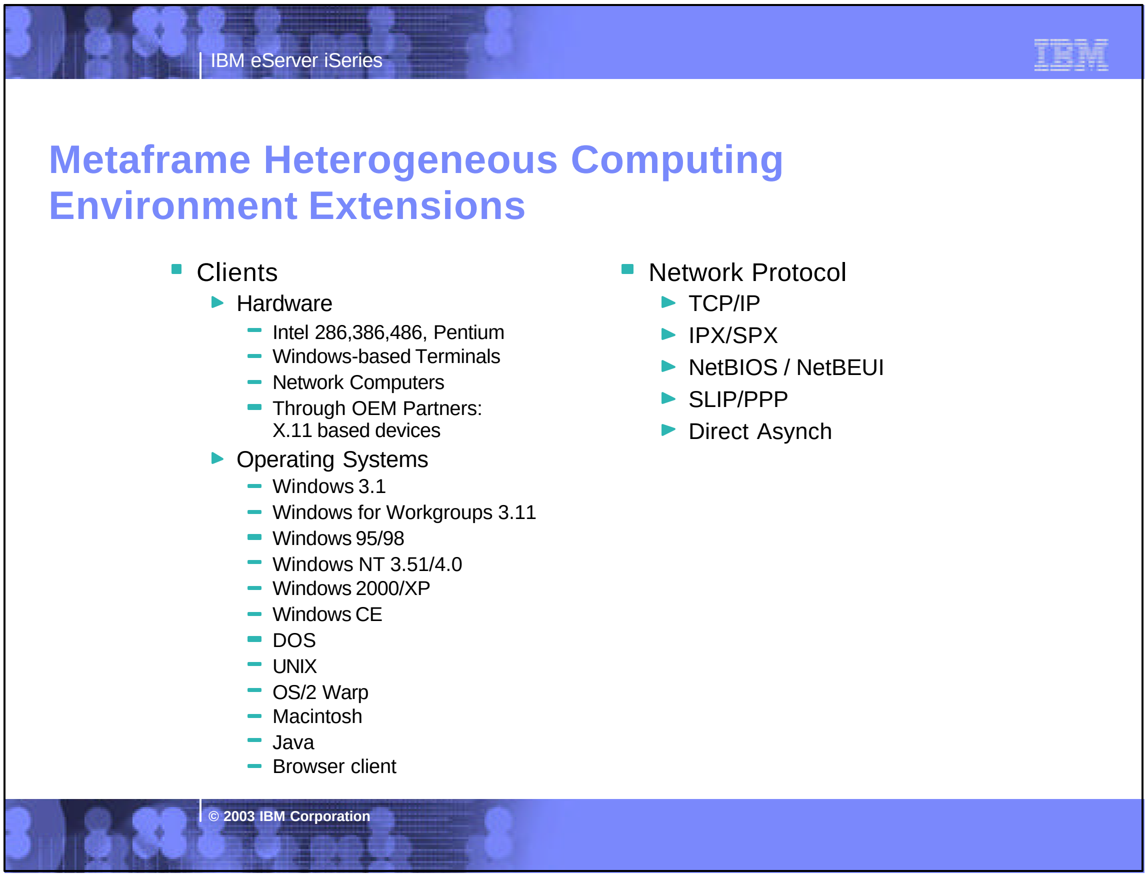
IBM

Citrix Metaframe

Metaframe Application Server for Windows

Thin-Client/Server Computing

- Applications are deployed, managed, supported, and executed completely on a server
- Requirements
  - Multi-user operating system
  - Remote presentation services (MetaFrame = ICA)
  - Centralized applications and client management

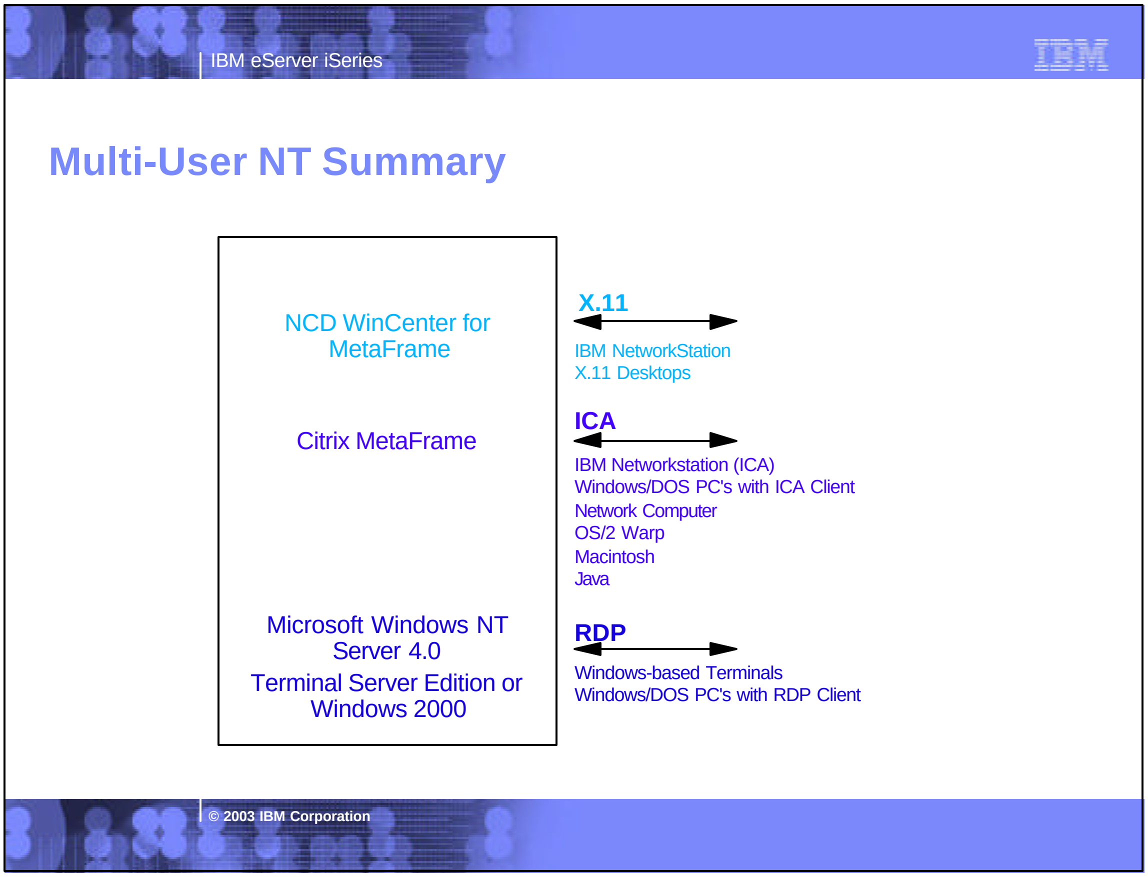


IBM eServer iSeries

IBM

Metaframe Heterogeneous Computing Environment Extensions

- Clients
  - Hardware
    - Intel 286,386,486, Pentium
    - Windows-based Terminals
    - Network Computers
    - Through OEM Partners: X.11 based devices
  - Operating Systems
    - Windows 3.1
    - Windows for Workgroups 3.11
    - Windows 95/98
    - Windows NT 3.51/4.0
    - Windows 2000/XP
    - Windows CE
    - DOS
    - UNIX
    - OS/2 Warp
    - Macintosh
    - Java
    - Browser client
- Network Protocol
  - TCP/IP
  - IPX/SPX
  - NetBIOS / NetBEUI
  - SLIP/PPP
  - Direct Asynch



IBM eServer iSeries

Multi-User NT Summary

NCD WinCenter for MetaFrame

Citrix MetaFrame

Microsoft Windows NT Server 4.0

Terminal Server Edition or Windows 2000

X.11

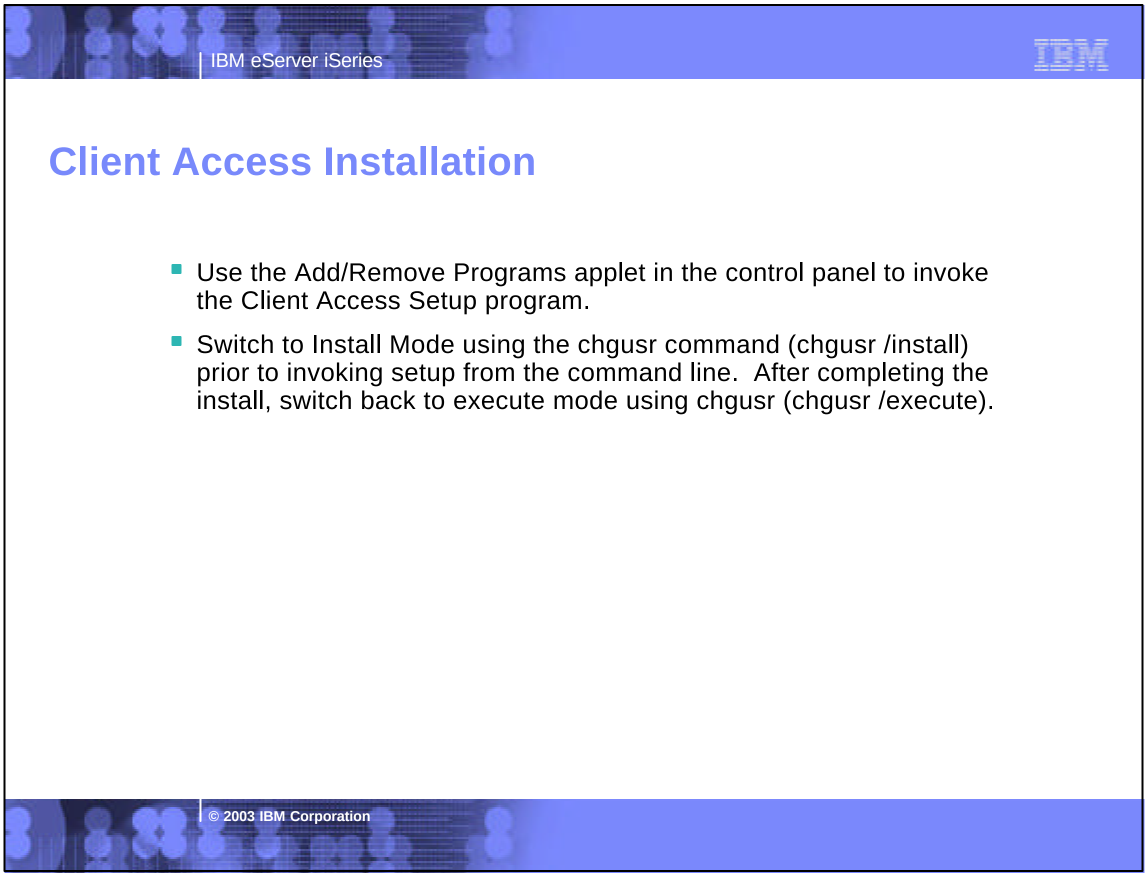
IBM NetworkStation
X.11 Desktops

ICA

IBM Networkstation (ICA)
Windows/DOS PC's with ICA Client
Network Computer
OS/2 Warp
Macintosh
Java

RDP

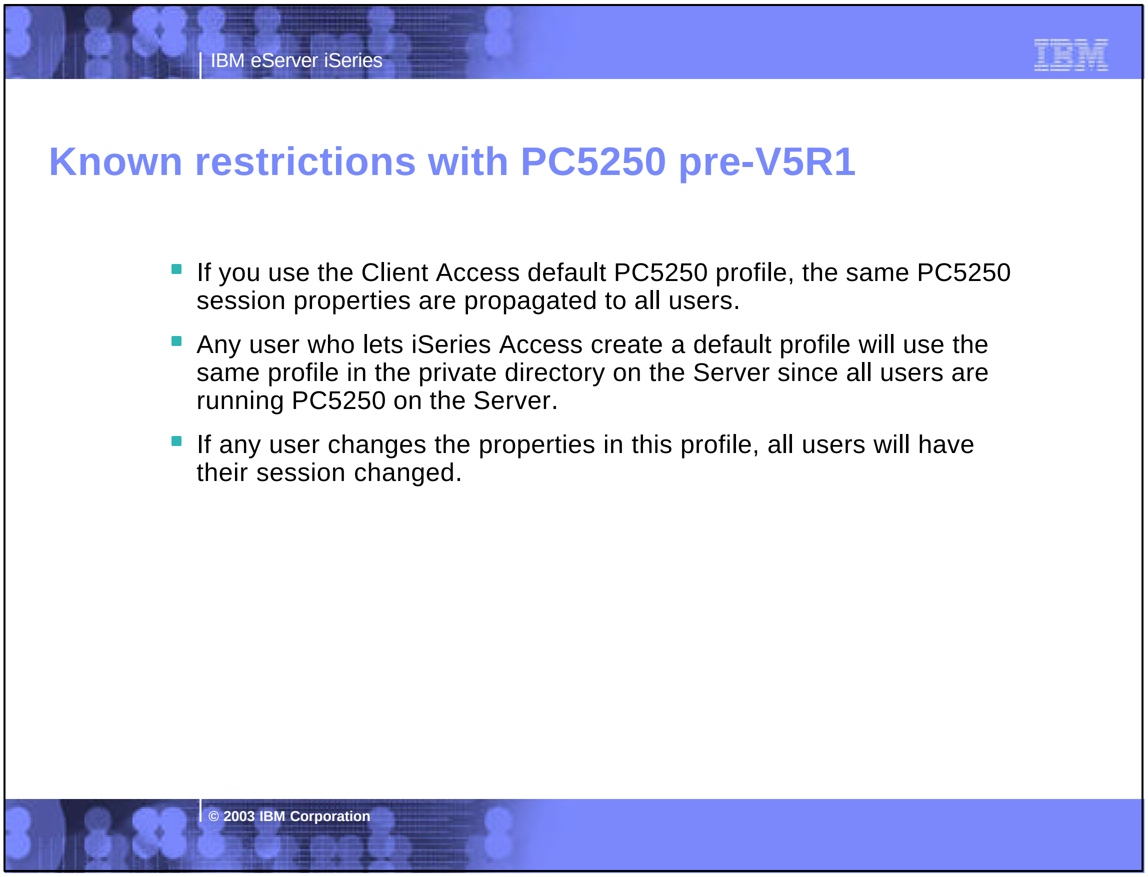
Windows-based Terminals
Windows/DOS PC's with RDP Client



IBM eServer iSeries

Client Access Installation

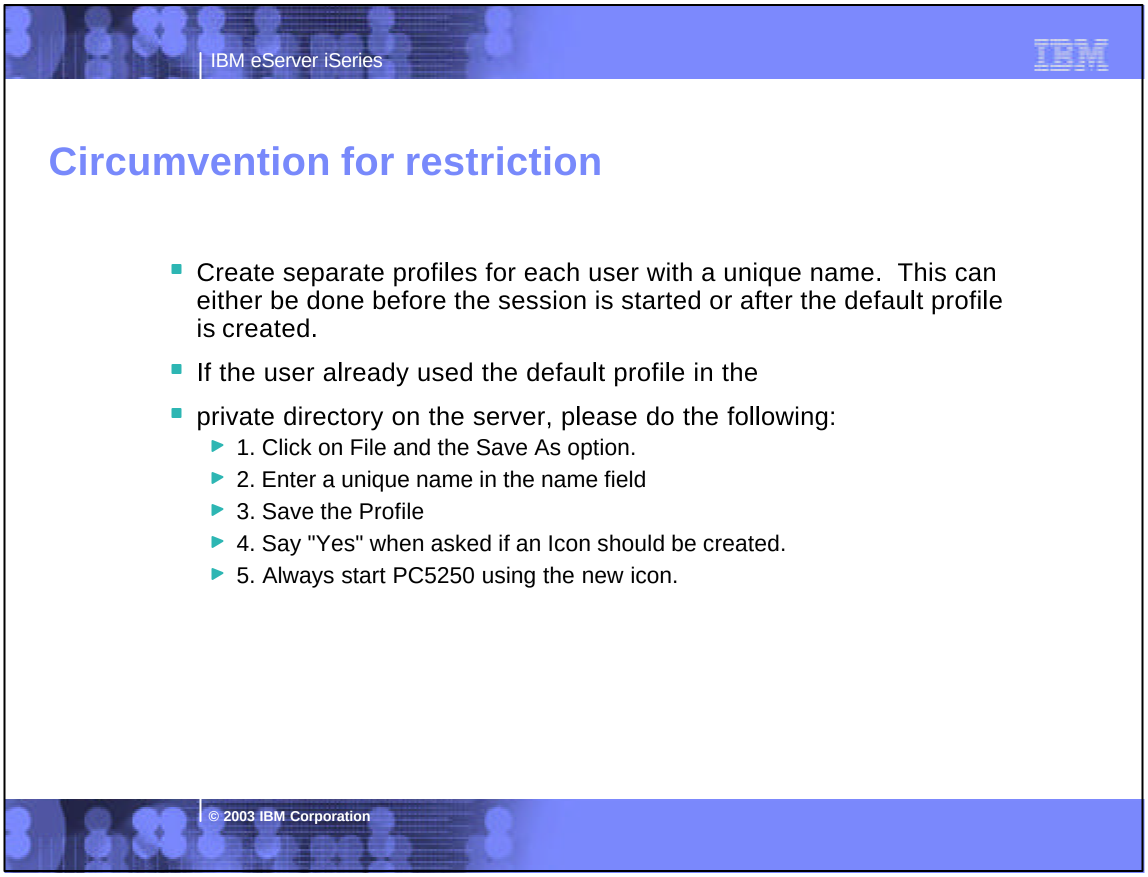
- Use the Add/Remove Programs applet in the control panel to invoke the Client Access Setup program.
- Switch to Install Mode using the chgusr command (chgusr /install) prior to invoking setup from the command line. After completing the install, switch back to execute mode using chgusr (chgusr /execute).



IBM eServer iSeries

Known restrictions with PC5250 pre-V5R1

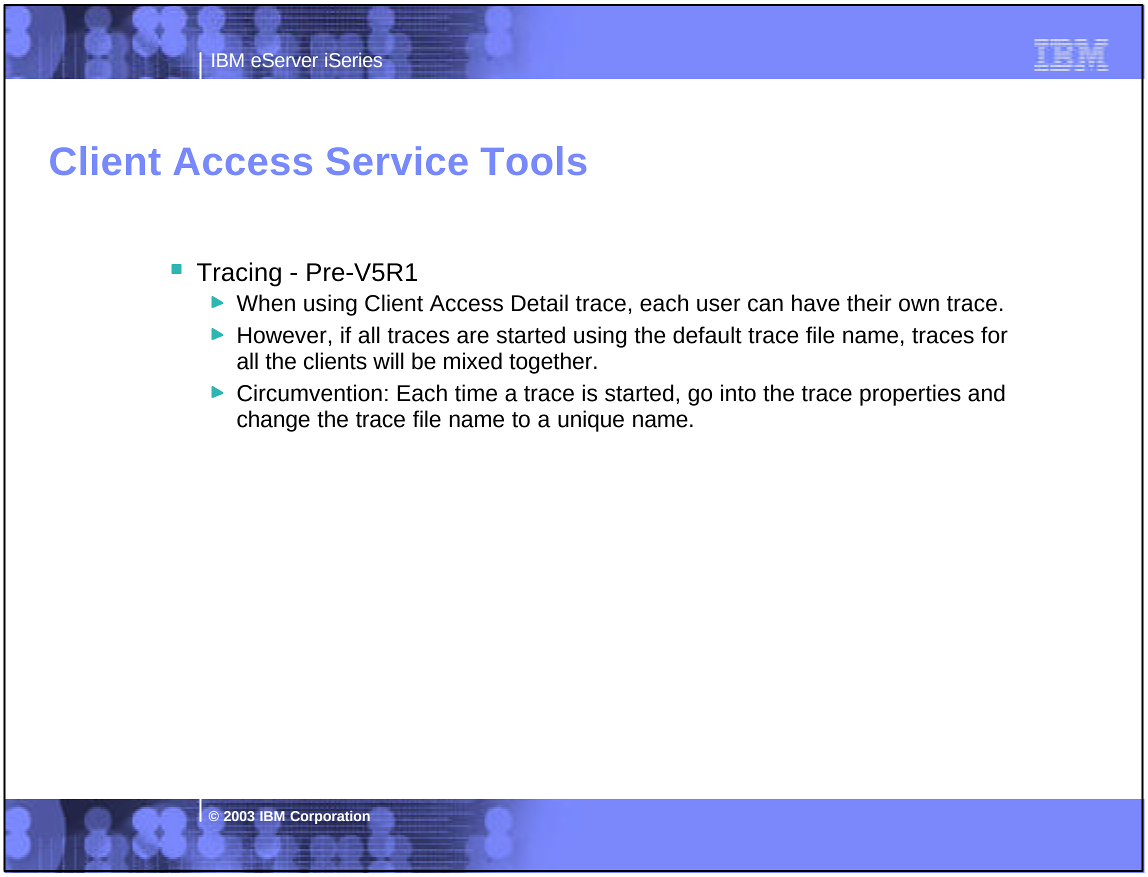
- If you use the Client Access default PC5250 profile, the same PC5250 session properties are propagated to all users.
- Any user who lets iSeries Access create a default profile will use the same profile in the private directory on the Server since all users are running PC5250 on the Server.
- If any user changes the properties in this profile, all users will have their session changed.



IBM eServer iSeries

Circumvention for restriction

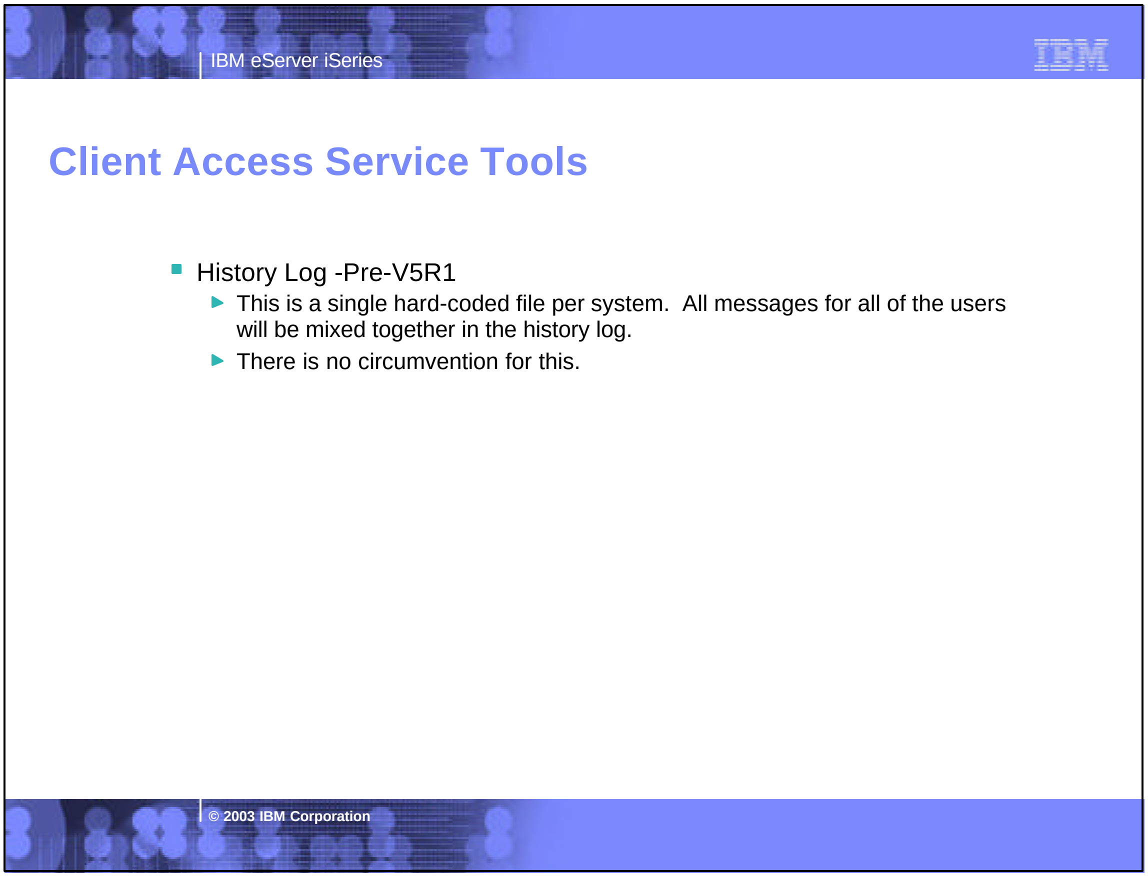
- Create separate profiles for each user with a unique name. This can either be done before the session is started or after the default profile is created.
- If the user already used the default profile in the
- private directory on the server, please do the following:
  - 1. Click on File and the Save As option.
  - 2. Enter a unique name in the name field
  - 3. Save the Profile
  - 4. Say "Yes" when asked if an Icon should be created.
  - 5. Always start PC5250 using the new icon.



IBM eServer iSeries

Client Access Service Tools

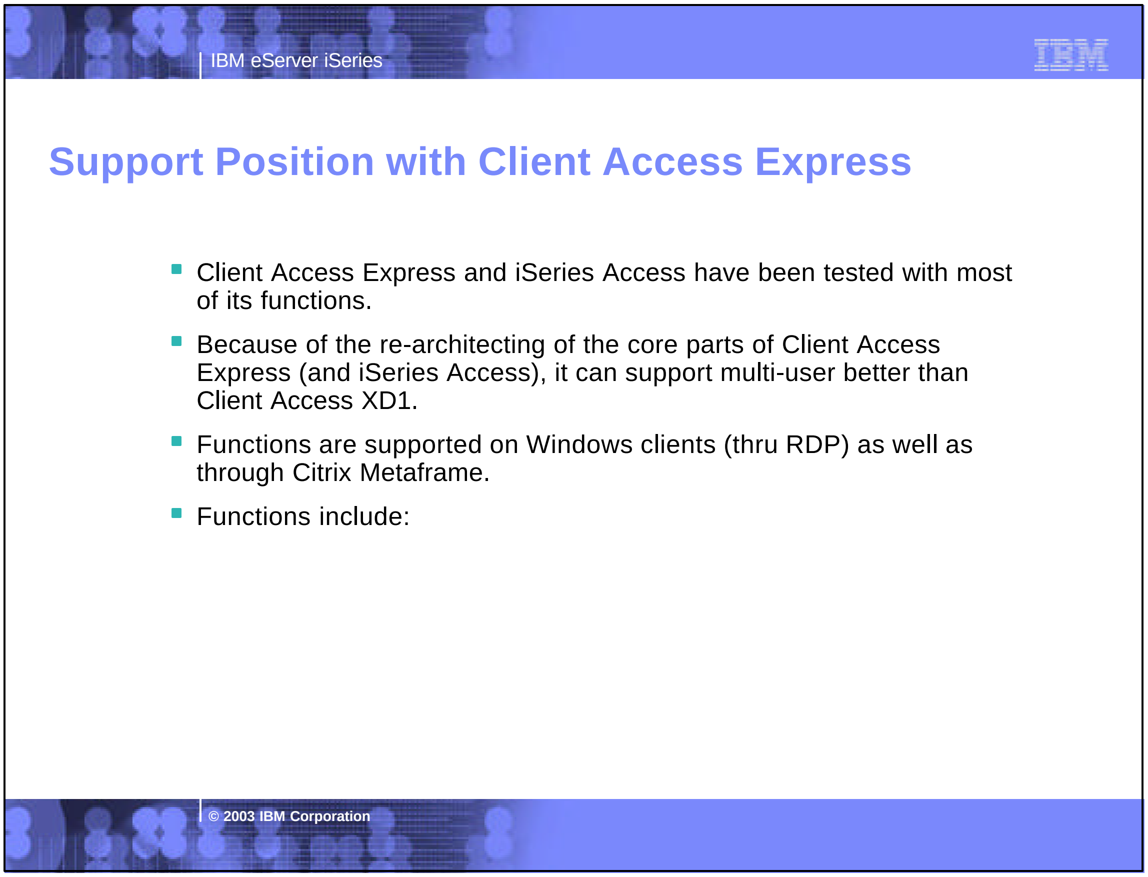
- Tracing - Pre-V5R1
  - When using Client Access Detail trace, each user can have their own trace.
  - However, if all traces are started using the default trace file name, traces for all the clients will be mixed together.
  - Circumvention: Each time a trace is started, go into the trace properties and change the trace file name to a unique name.



IBM eServer iSeries

Client Access Service Tools

- History Log -Pre-V5R1
  - This is a single hard-coded file per system. All messages for all of the users will be mixed together in the history log.
  - There is no circumvention for this.

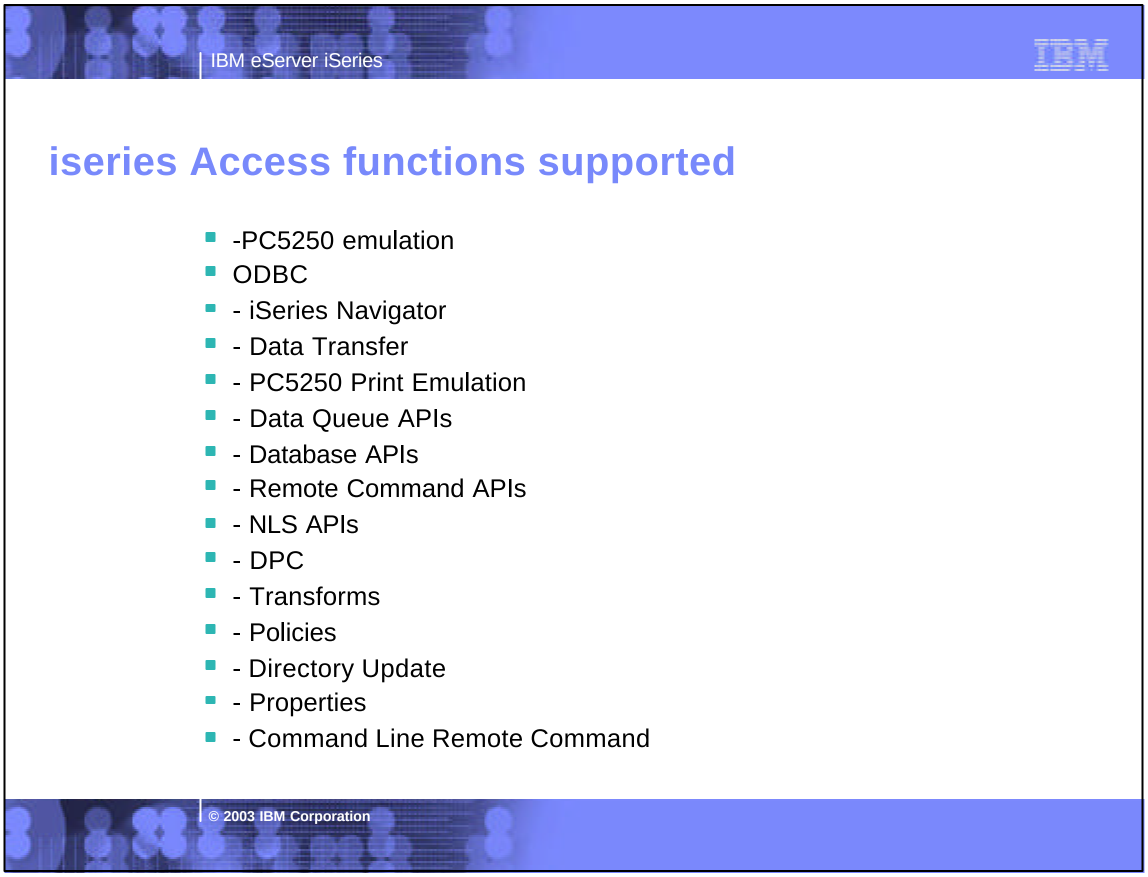


IBM eServer iSeries

Support Position with Client Access Express

- Client Access Express and iSeries Access have been tested with most of its functions.
- Because of the re-architecting of the core parts of Client Access Express (and iSeries Access), it can support multi-user better than Client Access XD1.
- Functions are supported on Windows clients (thru RDP) as well as through Citrix Metaframe.
- Functions include:

© 2003 IBM Corporation

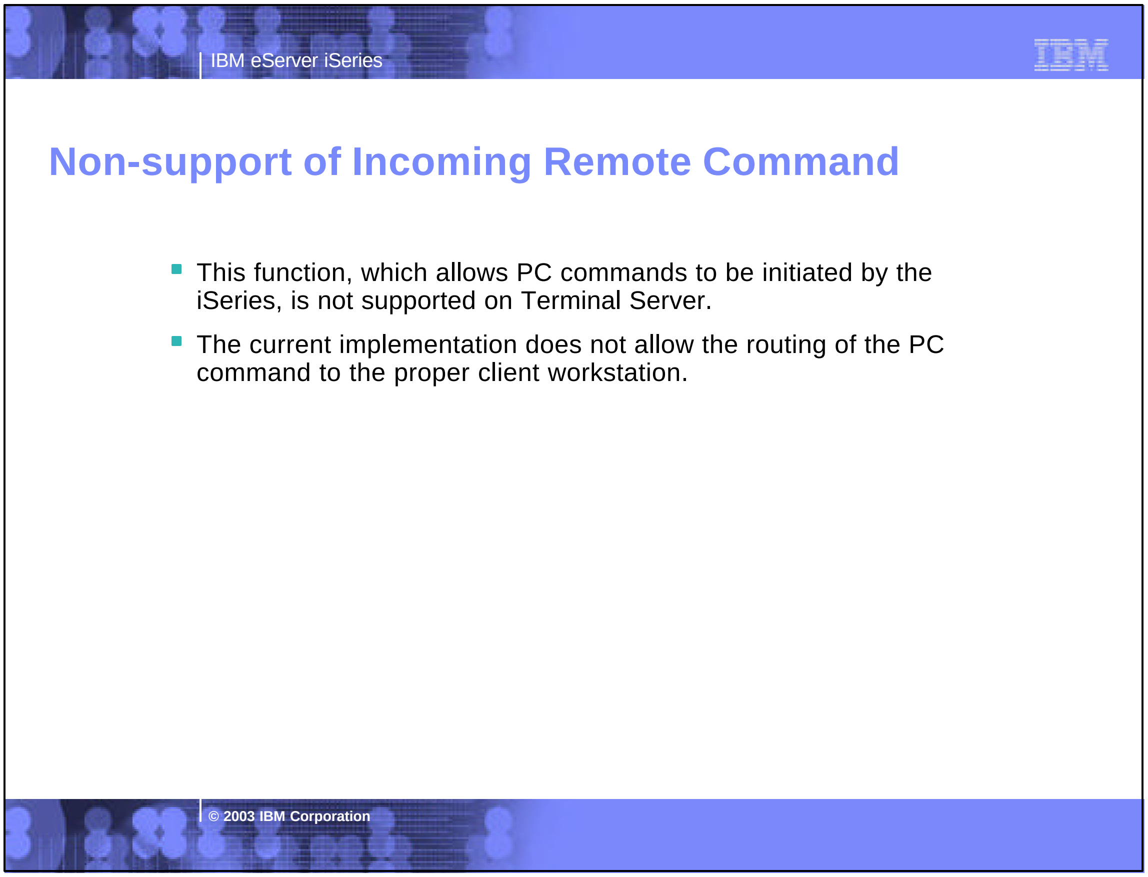


IBM eServer iSeries

iseries Access functions supported

- -PC5250 emulation
- ODBC
- - iSeries Navigator
- - Data Transfer
- - PC5250 Print Emulation
- - Data Queue APIs
- - Database APIs
- - Remote Command APIs
- - NLS APIs
- - DPC
- - Transforms
- - Policies
- - Directory Update
- - Properties
- - Command Line Remote Command

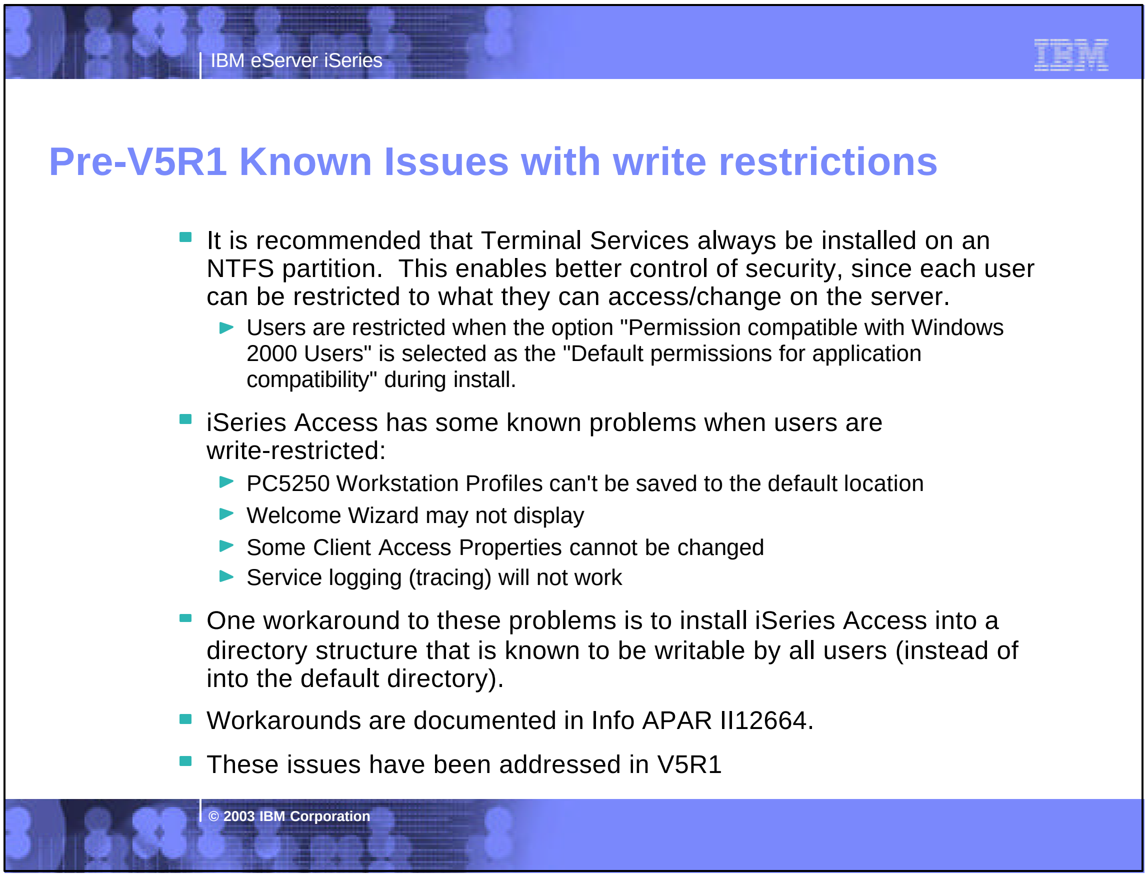
© 2003 IBM Corporation



IBM eServer iSeries

Non-support of Incoming Remote Command

- This function, which allows PC commands to be initiated by the iSeries, is not supported on Terminal Server.
- The current implementation does not allow the routing of the PC command to the proper client workstation.



IBM eServer iSeries

Pre-V5R1 Known Issues with write restrictions

- It is recommended that Terminal Services always be installed on an NTFS partition. This enables better control of security, since each user can be restricted to what they can access/change on the server.
  - ► Users are restricted when the option "Permission compatible with Windows 2000 Users" is selected as the "Default permissions for application compatibility" during install.
- iSeries Access has some known problems when users are write-restricted:
  - ► PC5250 Workstation Profiles can't be saved to the default location
  - ► Welcome Wizard may not display
  - ► Some Client Access Properties cannot be changed
  - ► Service logging (tracing) will not work
- One workaround to these problems is to install iSeries Access into a directory structure that is known to be writable by all users (instead of into the default directory).
- Workarounds are documented in Info APAR II12664.
- These issues have been addressed in V5R1

IBM eServer iSeries

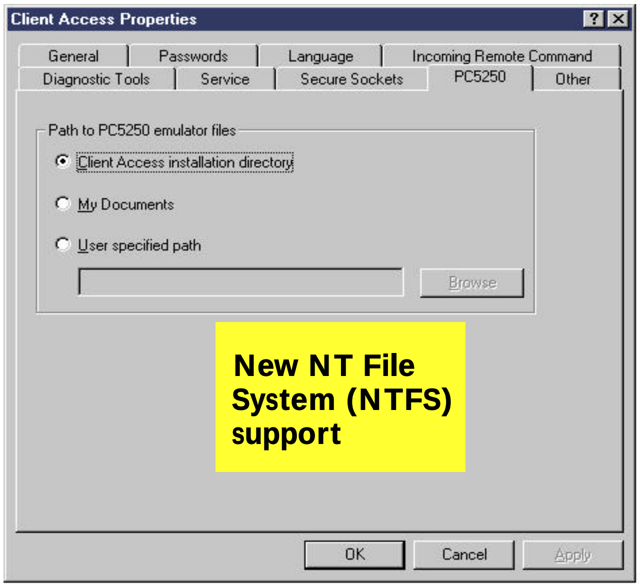
Solutions in V5R1 and later

- In V5R1, problems accessing directories and registry entries with the NTFS file system have been addressed.
- Strategy was to store most user-writable files in " My Documents" directory where it made sense. That is the Microsoft-recommended way to handle.
- Tried not to move existing files when upgrading from an older release to V5R1.

IBM eServer iSeries

Windows NT and 2000 NTFS Users

- By default, PC5250 files still go into the Client Access Install directory.
- Recommend changing to "My documents".
- Always should be writable.
- User can specify any path, but there is no guarantee that it will be writable.



Path to PC5250 emulator files

● Client Access installation directory

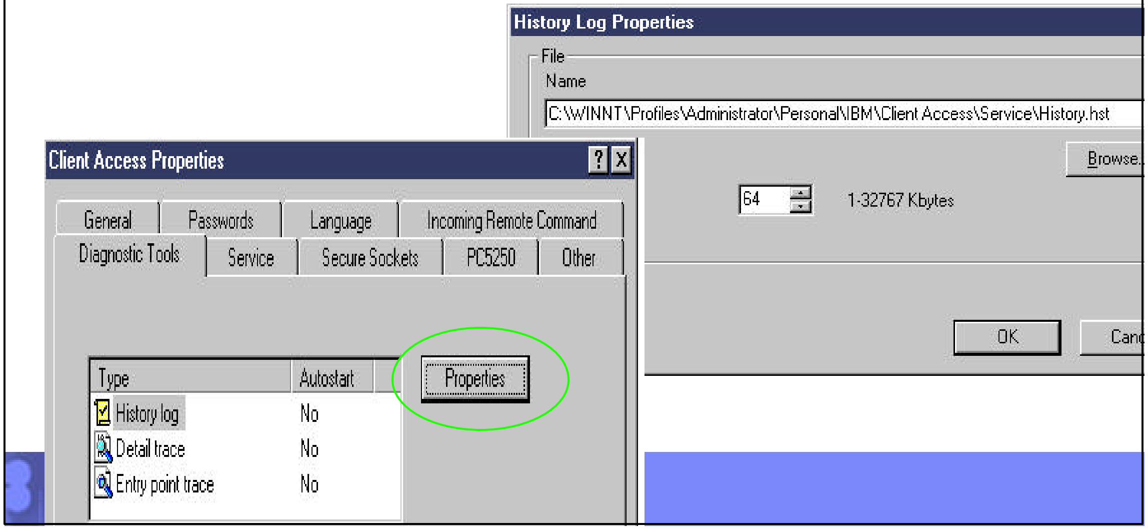
○ My Documents

○ User specified path

New NT File System (NTFS) support

Service Locations

- Service
  - History Log
    - Personal or My Documents location (different for each operating system)
  - Detail and Entry Point Trace files
    - Personal or My Documents location (different for each operating system)
  - Change the locations from Control Panel->Client Acccess, Diagnostics Tools page



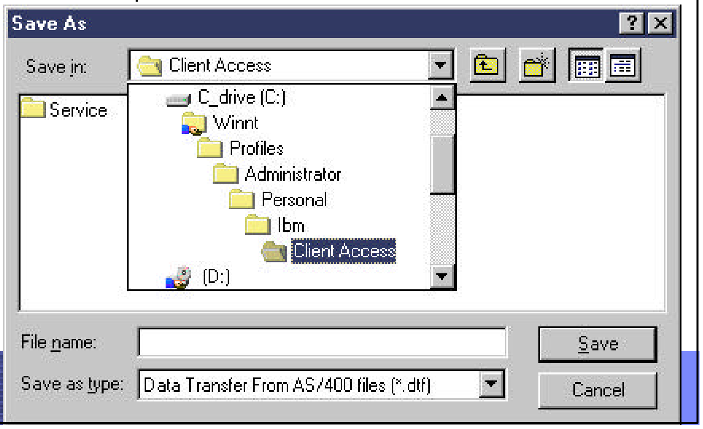
Name: C:\WINNT\Profiles\Administrator\Personal\IBM\Client Access\Service\History.hst

64 1-32767 Kbytes

Type	Autostart
☑ History log	No
Detail trace	No
Entry point trace	No

Data Transfer Requests

- Save and Open locations
- Default location
  - Personal or My Documents location (different for each operating system)
- If users have saved to or opened from a different location before, that location will displayed.
- Data Transfer "remembers" this location. This way, users on upgraded systems that have saved transfer requests will continue to see them where they saved before.



Save in: Client Access

File name:

Save as type: Data Transfer From AS/400 files (*.dtf)

IBM eServer iSeries

iSeries Netserver support of Terminal Server

- iSeries Access for Windows support relies on iSeries Netserver for installation and for file serving.
- Also supports print serving through Terminal Server
- Be aware that multiple Netserver sessions can now have the same workstation name.
- When displaying session Properties in iSeries Navigator for a workstation name, a cummulative total from all the sessions with the same workstations name will be displayed (number of connections, files opened, etc.)
- When workstation has multiple sessions with different user names, NetServer will still lump them together for the purposes of determining Properties values, and the User names will contain an asterisk.
- When you attempt to end a Netserver session via iSeries Navigator, Netserver ends the first Netbios-over-TCP/IP (NBT) session found for the workstation on which the session is running. All user activity on the NBT session ends, which means that when you attempt to end a session on a workstation on which multiple sessions are established, and unpredictable subset of sessions is ended.
- Additional information available in Info APAR II11435

IBM eServer iSeries

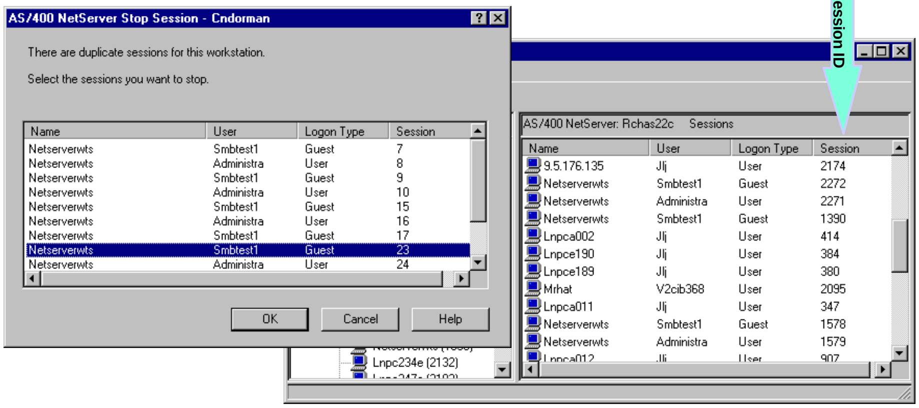
V5R1 Session Improvements

✓ Unique Session Identifier

- Can view properties share usage for individual WTS sessions
- Can stop individual WTS sessions

✓ Support for Windows Background Services

- Piggybacking virtual users



AS/400 NetServer Stop Session - Cndorman

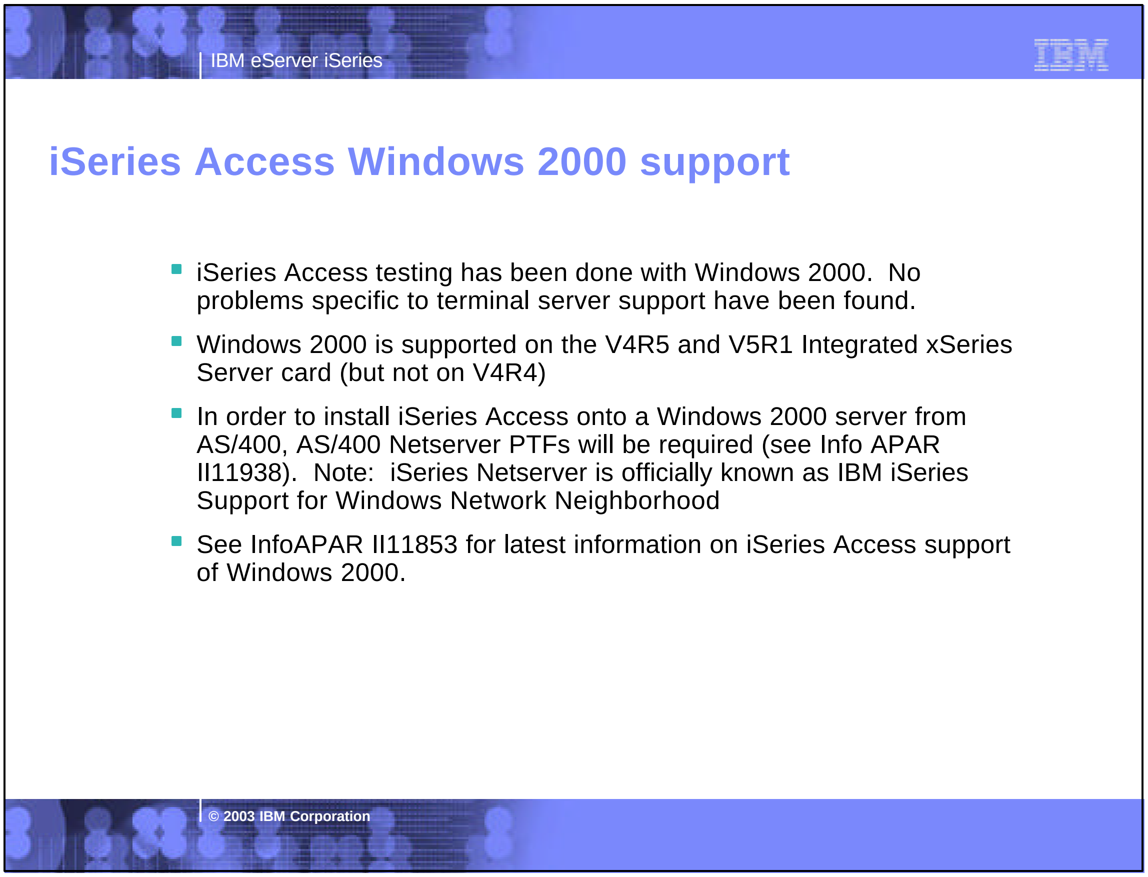
There are duplicate sessions for this workstation.

Select the sessions you want to stop.

Name	User	Logon Type	Session
Netserverwts	Smbtest1	Guest	7
Netserverwts	Administra	User	8
Netserverwts	Smbtest1	Guest	9
Netserverwts	Administra	User	10
Netserverwts	Smbtest1	Guest	15
Netserverwts	Administra	User	16
Netserverwts	Smbtest1	Guest	17
Netserverwts	Smbtest1	Guest	23
Netserverwts	Administra	User	24

AS/400 NetServer: Rchas22c Sessions

Name	User	Logon Type	Session
9.5.176.135	Jlj	User	2174
Netserverwts	Smbtest1	Guest	2272
Netserverwts	Administra	User	2271
Netserverwts	Smbtest1	Guest	1390
Lnpca002	Jlj	User	414
Lnpce190	Jlj	User	384
Lnpce189	Jlj	User	380
Mrhat	V2cib368	User	2095
Lnpca011	Jlj	User	347
Netserverwts	Smbtest1	Guest	1578
Netserverwts	Administra	User	1579
Lnpca012	Jlj	User	907

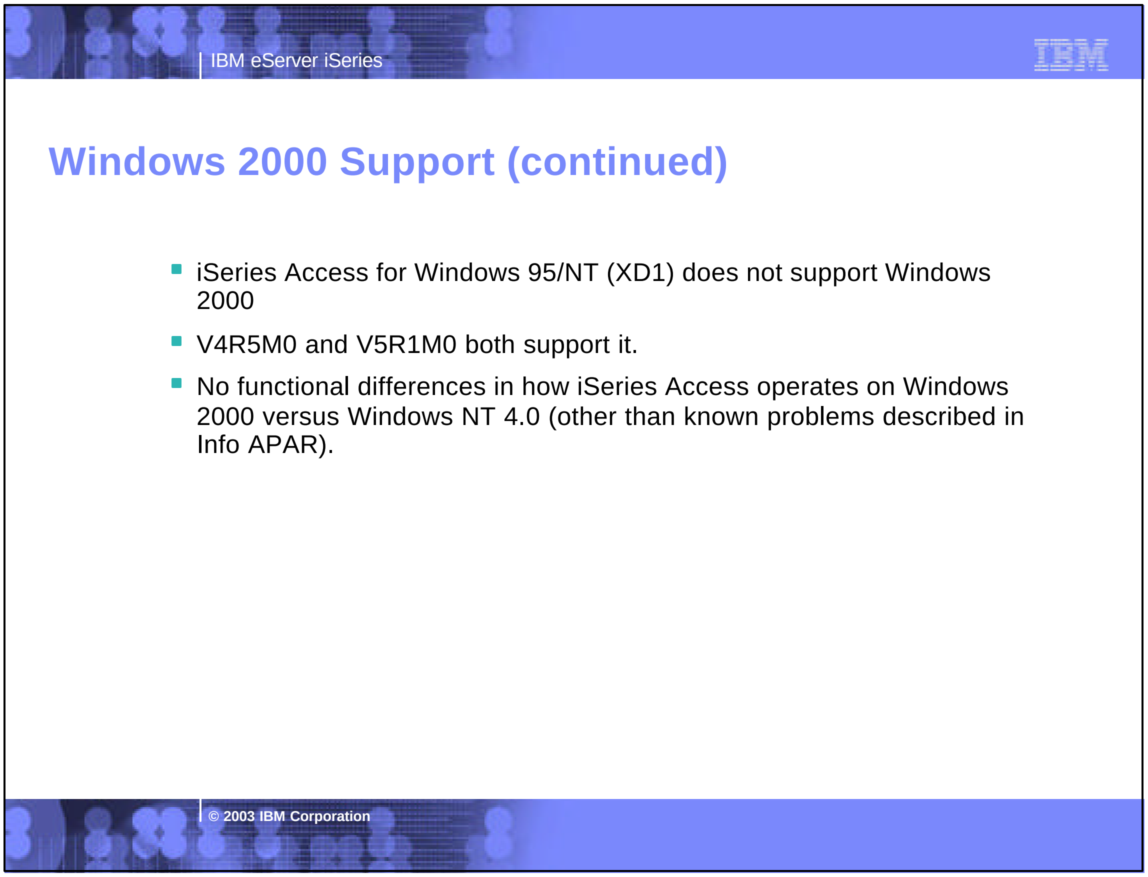


IBM eServer iSeries

IBM

iSeries Access Windows 2000 support

- iSeries Access testing has been done with Windows 2000. No problems specific to terminal server support have been found.
- Windows 2000 is supported on the V4R5 and V5R1 Integrated xSeries Server card (but not on V4R4)
- In order to install iSeries Access onto a Windows 2000 server from AS/400, AS/400 Netserver PTFs will be required (see Info APAR II11938). Note: iSeries Netserver is officially known as IBM iSeries Support for Windows Network Neighborhood
- See InfoAPAR II11853 for latest information on iSeries Access support of Windows 2000.



IBM eServer iSeries

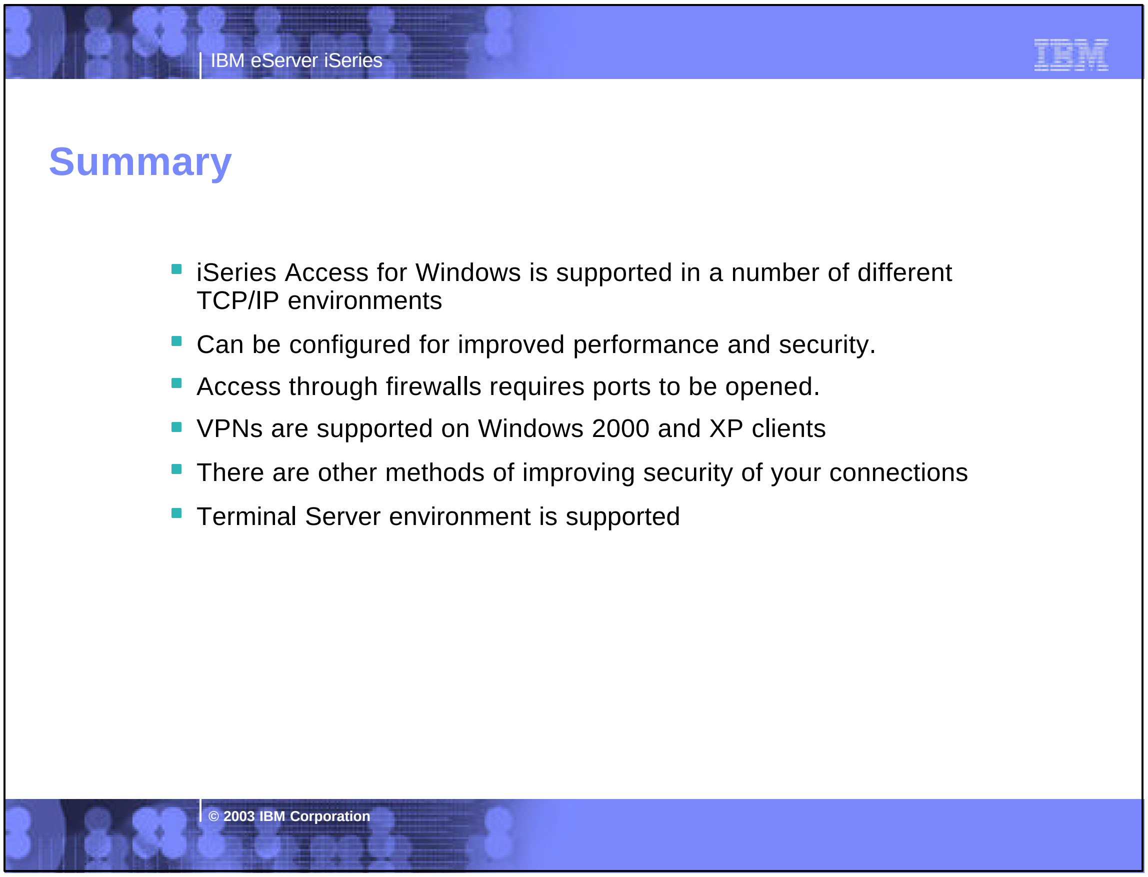
IBM

Windows 2000 Support (continued)

- iSeries Access for Windows 95/NT (XD1) does not support Windows 2000
- V4R5M0 and V5R1M0 both support it.
- No functional differences in how iSeries Access operates on Windows 2000 versus Windows NT 4.0 (other than known problems described in Info APAR).

IBM eServer iSeries

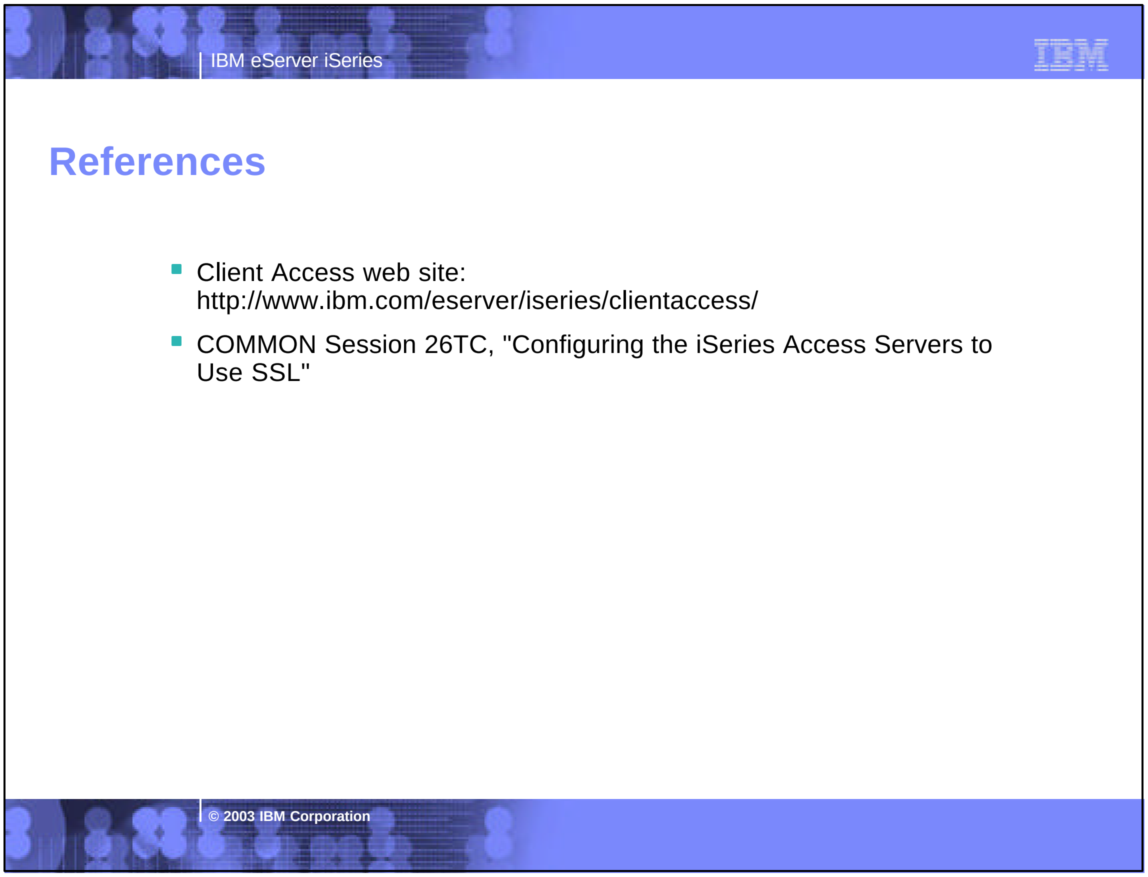
Summary



IBM eServer iSeries

Summary

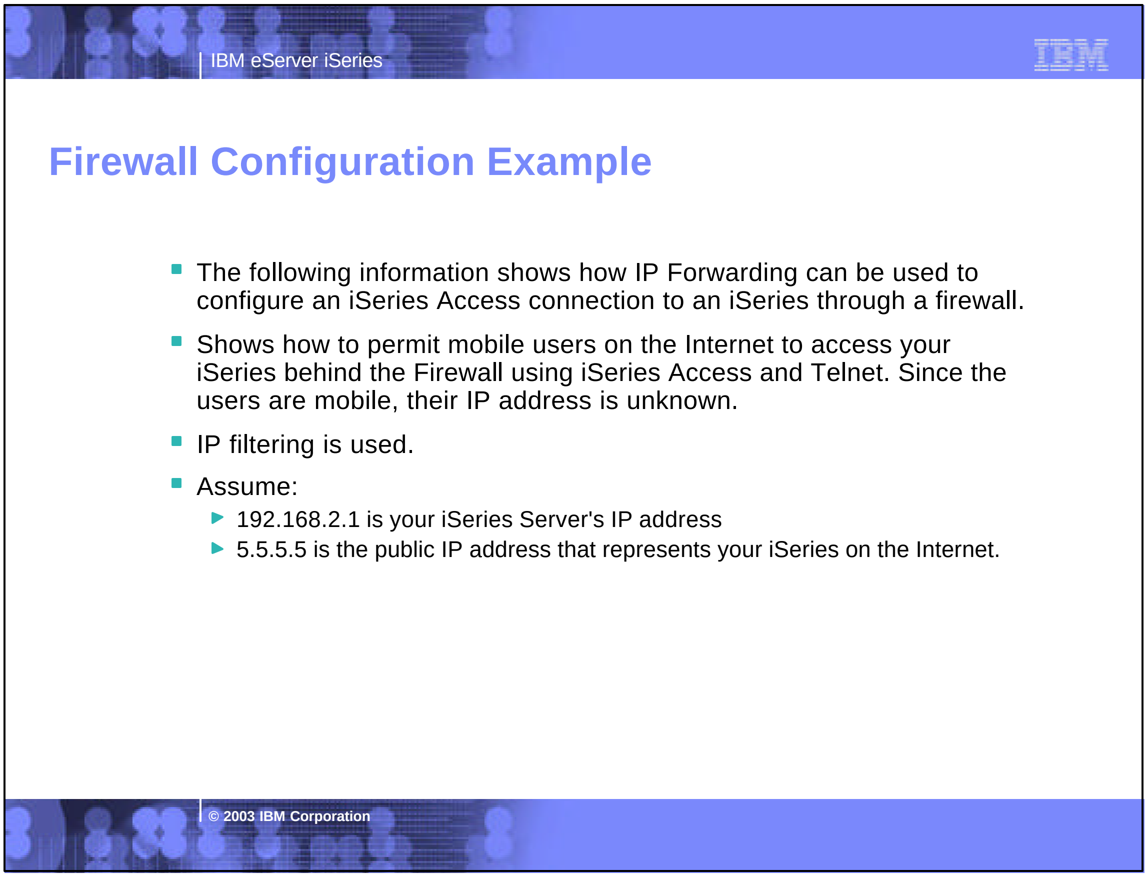
- iSeries Access for Windows is supported in a number of different TCP/IP environments
- Can be configured for improved performance and security.
- Access through firewalls requires ports to be opened.
- VPNs are supported on Windows 2000 and XP clients
- There are other methods of improving security of your connections
- Terminal Server environment is supported



References

- Client Access web site: http://www.ibm.com/eserver/iseries/clientaccess/
- COMMON Session 26TC, "Configuring the iSeries Access Servers to Use SSL"

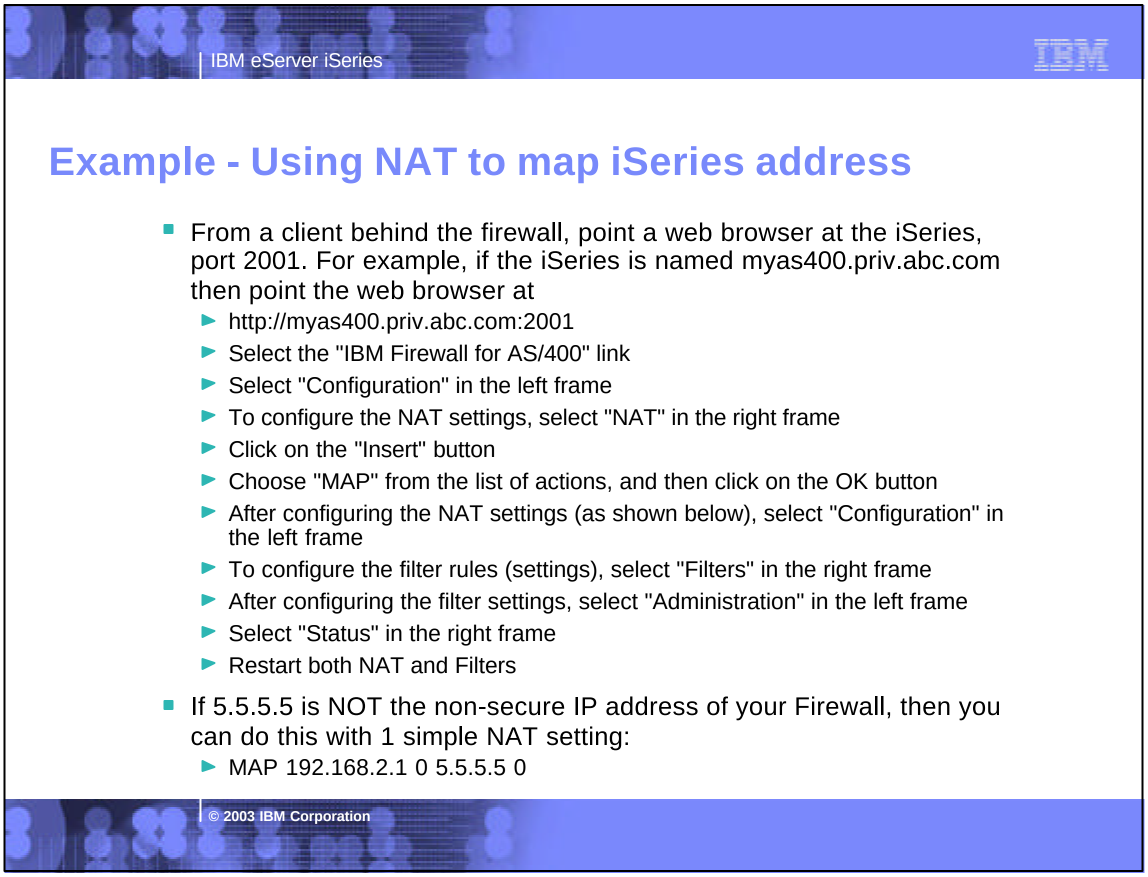
Apendix: Firewall/NAT example with Client Access



IBM eServer iSeries

Firewall Configuration Example

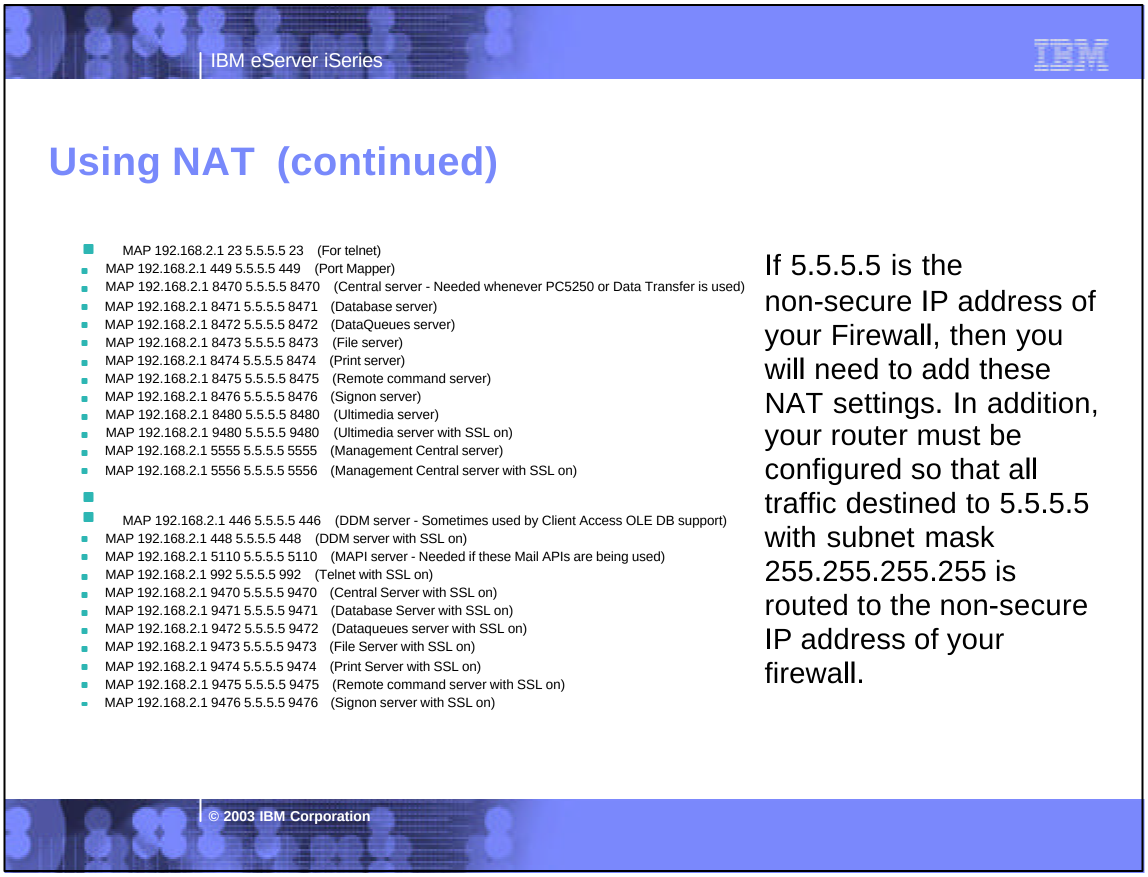
- The following information shows how IP Forwarding can be used to configure an iSeries Access connection to an iSeries through a firewall.
- Shows how to permit mobile users on the Internet to access your iSeries behind the Firewall using iSeries Access and Telnet. Since the users are mobile, their IP address is unknown.
- IP filtering is used.
- Assume:
  - 192.168.2.1 is your iSeries Server's IP address
  - 5.5.5.5 is the public IP address that represents your iSeries on the Internet.



IBM eServer iSeries

Example - Using NAT to map iSeries address

- From a client behind the firewall, point a web browser at the iSeries, port 2001. For example, if the iSeries is named myas400.priv.abc.com then point the web browser at
  - http://myas400.priv.abc.com:2001
  - Select the "IBM Firewall for AS/400" link
  - Select "Configuration" in the left frame
  - To configure the NAT settings, select "NAT" in the right frame
  - Click on the "Insert" button
  - Choose "MAP" from the list of actions, and then click on the OK button
  - After configuring the NAT settings (as shown below), select "Configuration" in the left frame
  - To configure the filter rules (settings), select "Filters" in the right frame
  - After configuring the filter settings, select "Administration" in the left frame
  - Select "Status" in the right frame
  - Restart both NAT and Filters
- If 5.5.5.5 is NOT the non-secure IP address of your Firewall, then you can do this with 1 simple NAT setting:
  - MAP 192.168.2.1 0 5.5.5.5 0



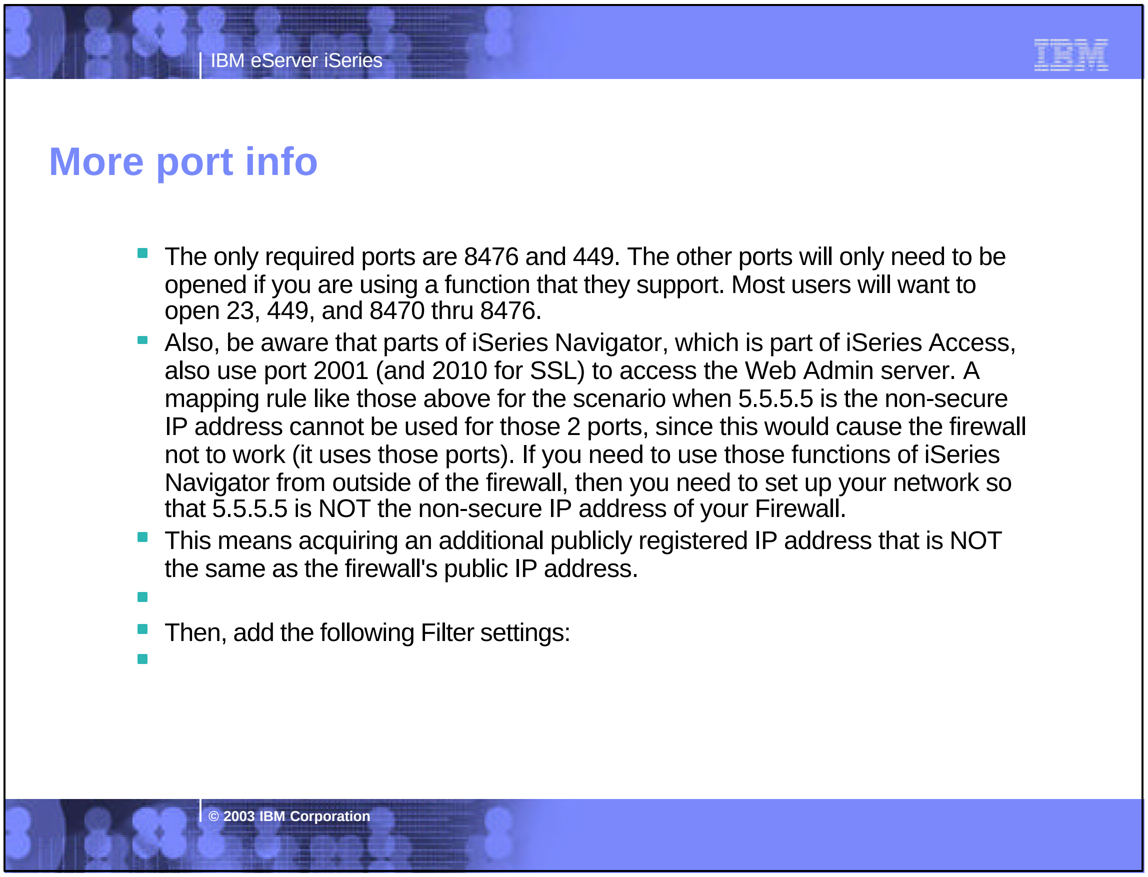
IBM eServer iSeries

Using NAT (continued)

- MAP 192.168.2.1 23 5.5.5.5 23   (For telnet)
- MAP 192.168.2.1 449 5.5.5.5 449   (Port Mapper)
- MAP 192.168.2.1 8470 5.5.5.5 8470   (Central server - Needed whenever PC5250 or Data Transfer is used)
- MAP 192.168.2.1 8471 5.5.5.5 8471   (Database server)
- MAP 192.168.2.1 8472 5.5.5.5 8472   (DataQueues server)
- MAP 192.168.2.1 8473 5.5.5.5 8473   (File server)
- MAP 192.168.2.1 8474 5.5.5.5 8474   (Print server)
- MAP 192.168.2.1 8475 5.5.5.5 8475   (Remote command server)
- MAP 192.168.2.1 8476 5.5.5.5 8476   (Signon server)
- MAP 192.168.2.1 8480 5.5.5.5 8480   (Ultimedia server)
- MAP 192.168.2.1 9480 5.5.5.5 9480   (Ultimedia server with SSL on)
- MAP 192.168.2.1 5555 5.5.5.5 5555   (Management Central server)
- MAP 192.168.2.1 5556 5.5.5.5 5556   (Management Central server with SSL on)

- MAP 192.168.2.1 446 5.5.5.5 446   (DDM server - Sometimes used by Client Access OLE DB support)
- MAP 192.168.2.1 448 5.5.5.5 448   (DDM server with SSL on)
- MAP 192.168.2.1 5110 5.5.5.5 5110   (MAPI server - Needed if these Mail APIs are being used)
- MAP 192.168.2.1 992 5.5.5.5 992   (Telnet with SSL on)
- MAP 192.168.2.1 9470 5.5.5.5 9470   (Central Server with SSL on)
- MAP 192.168.2.1 9471 5.5.5.5 9471   (Database Server with SSL on)
- MAP 192.168.2.1 9472 5.5.5.5 9472   (Dataqueues server with SSL on)
- MAP 192.168.2.1 9473 5.5.5.5 9473   (File Server with SSL on)
- MAP 192.168.2.1 9474 5.5.5.5 9474   (Print Server with SSL on)
- MAP 192.168.2.1 9475 5.5.5.5 9475   (Remote command server with SSL on)
- MAP 192.168.2.1 9476 5.5.5.5 9476   (Signon server with SSL on)

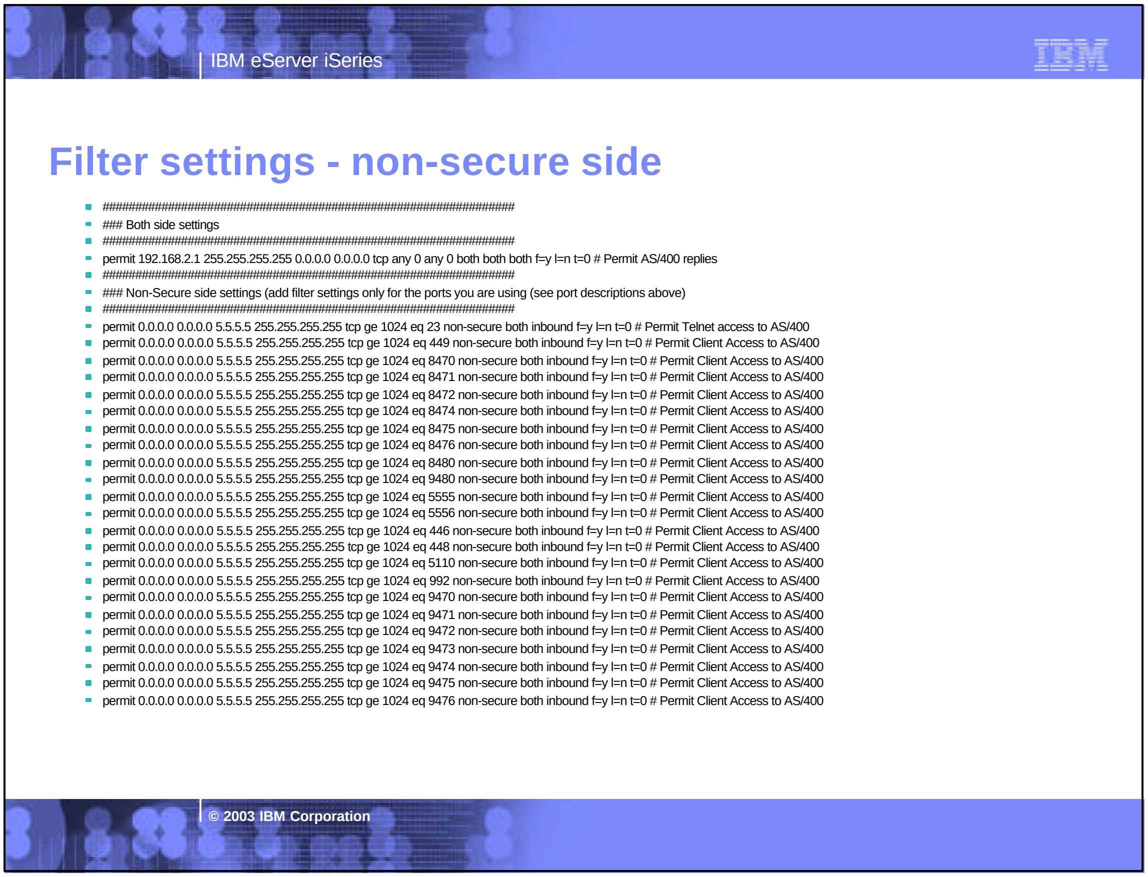
If 5.5.5.5 is the non-secure IP address of your Firewall, then you will need to add these NAT settings. In addition, your router must be configured so that all traffic destined to 5.5.5.5 with subnet mask 255.255.255.255 is routed to the non-secure IP address of your firewall.



IBM eServer iSeries

More port info

- The only required ports are 8476 and 449. The other ports will only need to be opened if you are using a function that they support. Most users will want to open 23, 449, and 8470 thru 8476.
- Also, be aware that parts of iSeries Navigator, which is part of iSeries Access, also use port 2001 (and 2010 for SSL) to access the Web Admin server. A mapping rule like those above for the scenario when 5.5.5.5 is the non-secure IP address cannot be used for those 2 ports, since this would cause the firewall not to work (it uses those ports). If you need to use those functions of iSeries Navigator from outside of the firewall, then you need to set up your network so that 5.5.5.5 is NOT the non-secure IP address of your Firewall.
- This means acquiring an additional publicly registered IP address that is NOT the same as the firewall's public IP address.
- Then, add the following Filter settings:

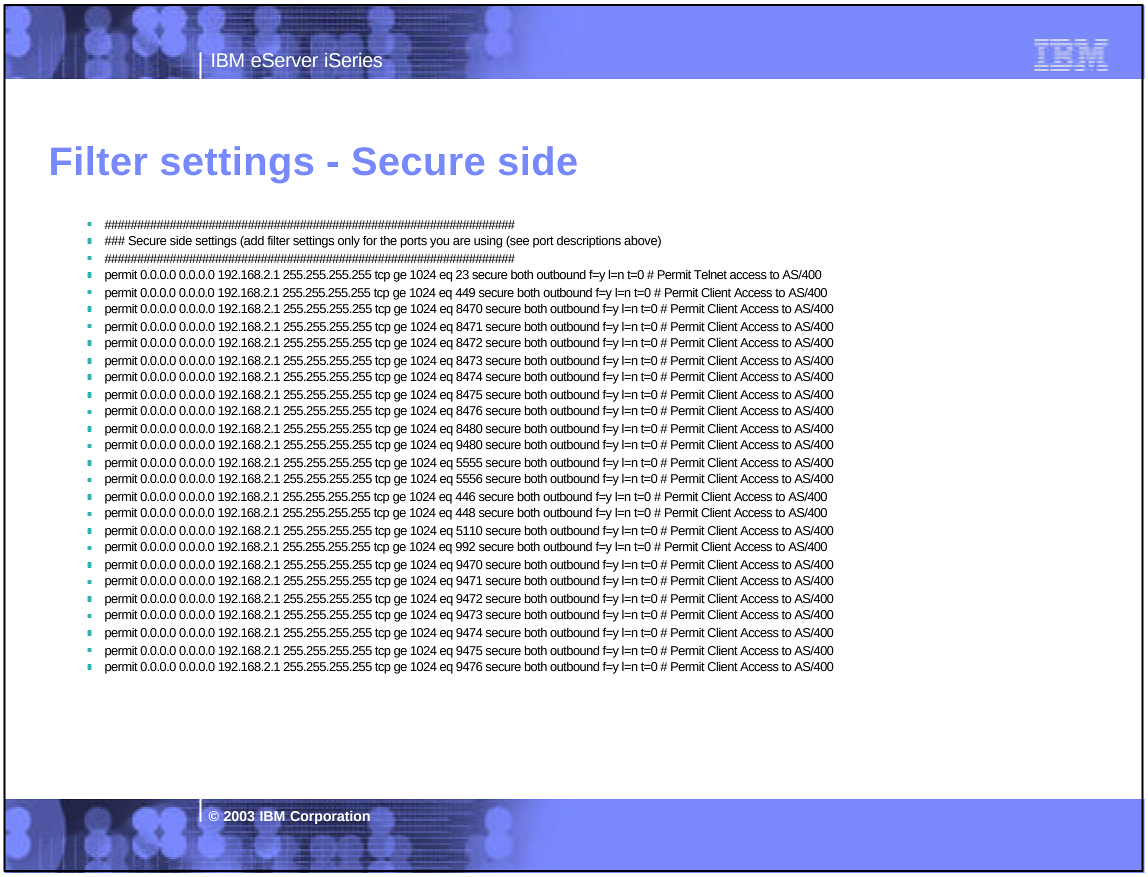


IBM eServer iSeries

Filter settings - non-secure side

- ##
- ### Both side settings
- ##
- permit 192.168.2.1 255.255.255.255 0.0.0.0 0.0.0.0 tcp any 0 any 0 both both both f=y l=n t=0 # Permit AS/400 replies
- ##
- ### Non-Secure side settings (add filter settings only for the ports you are using (see port descriptions above)
- ##
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 23 non-secure both inbound f=y l=n t=0 # Permit Telnet access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 449 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8470 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8471 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8472 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8474 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8475 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8476 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 8480 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9480 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 5555 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 5556 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 446 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 448 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 5110 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 992 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9470 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9471 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9472 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9473 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9474 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9475 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 5.5.5.5 255.255.255.255 tcp ge 1024 eq 9476 non-secure both inbound f=y l=n t=0 # Permit Client Access to AS/400

© 2003 IBM Corporation



IBM eServer iSeries

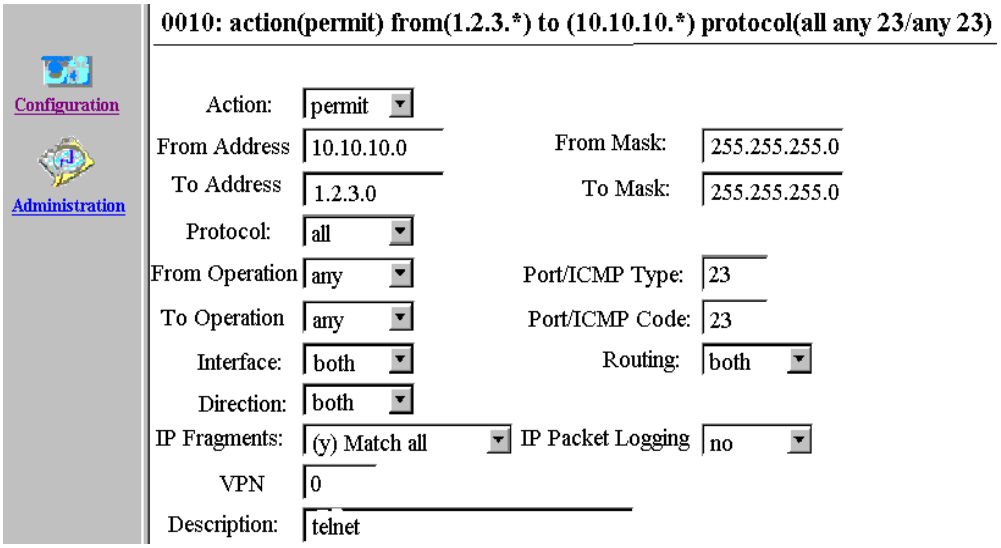
Filter settings - Secure side

- ##
- ### Secure side settings (add filter settings only for the ports you are using (see port descriptions above)
- ##
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 23 secure both outbound f=y l=n t=0 # Permit Telnet access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 449 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8470 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8471 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8472 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8473 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8474 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8475 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8476 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 8480 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9480 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 5555 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 5556 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 446 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 448 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 5110 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 992 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9470 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9471 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9472 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9473 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9474 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9475 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400
- permit 0.0.0.0 0.0.0.0 192.168.2.1 255.255.255.255 tcp ge 1024 eq 9476 secure both outbound f=y l=n t=0 # Permit Client Access to AS/400

© 2003 IBM Corporation

IBM eServer iSeries

Example of setting filter rules



0010: action(permit) from(1.2.3.*) to (10.10.10.*) protocol(all any 23/any 23)

Action: permit

From Address: 10.10.10.0   From Mask: 255.255.255.0

To Address: 1.2.3.0   To Mask: 255.255.255.0

Protocol: all

From Operation: any   Port/ICMP Type: 23

To Operation: any   Port/ICMP Code: 23

Interface: both   Routing: both

Direction: both

IP Fragments: (y) Match all   IP Packet Logging: no

VPN: 0

Description: telnet

IBM eServer iSeries

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:
Instruction: Refer to the following URL: http://w3.ibm.com/legal/ipl/wtts. Edit the list below, IBM subsidiary statement, and special attribution companies which follow so they coincide with your presentation.

AS/400
AS/400e
eServer
eServer

IBM
IBM (logo)
iSeries
OS/400

Lotus and SmartSuite are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.
Instruction: For a complete list of Lotus/IBM trademarks, see www.lotus.com/lotus/information.nsf/firstpages/copyright and edit the above statements to coincide with your presentation.
MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.
Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Other company, product or 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.