

iSeries Communications Overview

2001 Announcements
ITSO Technical Overview
May 2001

IBM @server. For the next generation of e-business.

TCP/IP Configuration Enhancements

More GUI Tools for Configuring TCP/IP

STRTCP *YES now inn IPL attributes

Protocols Folder is removed

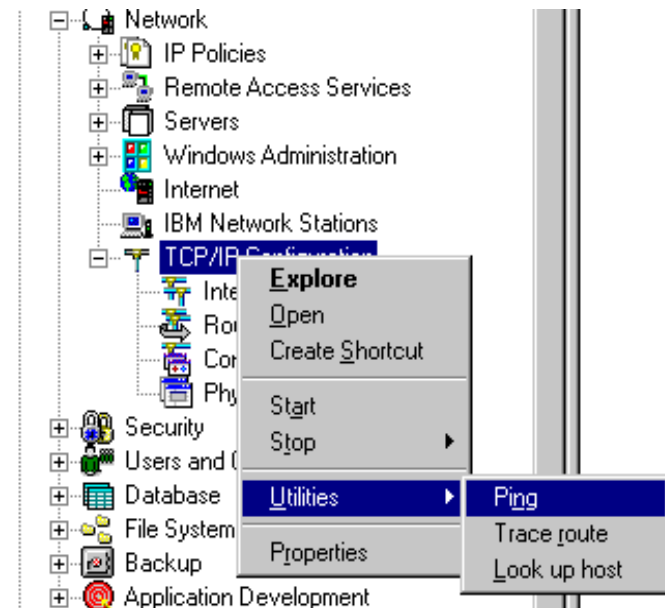
TCP/IP Folder moved under Network

Added TCP/IP utilities

- Ping
- Trace Route
- Look up Host

Four new Folders:

- Interfaces
- Routes
- Connections
- Physical Interfaces Activity



Please look at the *Operations Navigator* section at this presentation to have a look at the new interfacing for TCP/IP configuration options.

With this release, many more functions have been added to Operations Navigator to configure a TCP/IP environment and its associated services. New wizards are introduced to make configuration easier than ever before.

In this overview, we will guide you through the most eye-catching enhancements of this announcement.

The IPL attributes (Display IPL Attributes (DSPIPLA) or Change IPL Attributes (CHGIPLA) commands) support a start TCP parameter. V5R1 ships with this defaulted to *YES).

Most areas affected:

- FTP
- Telnet
- SMTP
- LDAP
- Point-to-Point and RADIUS
- Quality of Service
- Dynamic Domain Name System
- Virtual Private Network

Huge volume of enhancements and new functions

New iSeries communications attachment features

FTP Enhancements

IBM @server. For the next generation of e-business.

FTP Enhancements

Internationalization support (Unicode, UTF-8)

Performance optimization

Defense against hacking

Subsystem selection

Client can select a specific port

Support for SSL and TLS

Access restriction for specific operations

The capability to use UNICODE for path names and UTF-8 encoding to exchange path names between clients and servers is added with FTP Internationalization support. This is an implementation of RFC 2640 on *Internationalization of the File Transfer Protocol*. The current pre-V5R1 capability cannot support the wide range of characters needed by multinational systems. Global compatibility is achieved by the use of UTF-8 encoding when exchanging path names. To use UTF-8 format the client issues a FEAT command to determine if the LANG command is supported by the FTP server. The LANG command is issued to signal that path name exchanges will be done in UNICODE encoded in UTF-8 format. The V5R1 FTP client and server both support the LANG, FEAT, and OPT command.

V5R1 OS/400 addresses security concerns stated in RFC 2577 (*FTP Security Considerations*):

▶ **Password attacks**

The V5R1 FTP server currently uses QMAXSIGN system value to limit password attempts per session. The iSeries will now add a time delay following each invalid password received to slow down the password attacks.

▶ **Port stealing**

In the past the OS/400 FTP client and server would select ports in sequential increasing order. This could allow someone to predict the next port used by FTP. The FTP code is changed in V5R1 so that it will bind to a randomly-chosen TCP port instead of using sequential increasing order ports.

▶ **Bounce attack**

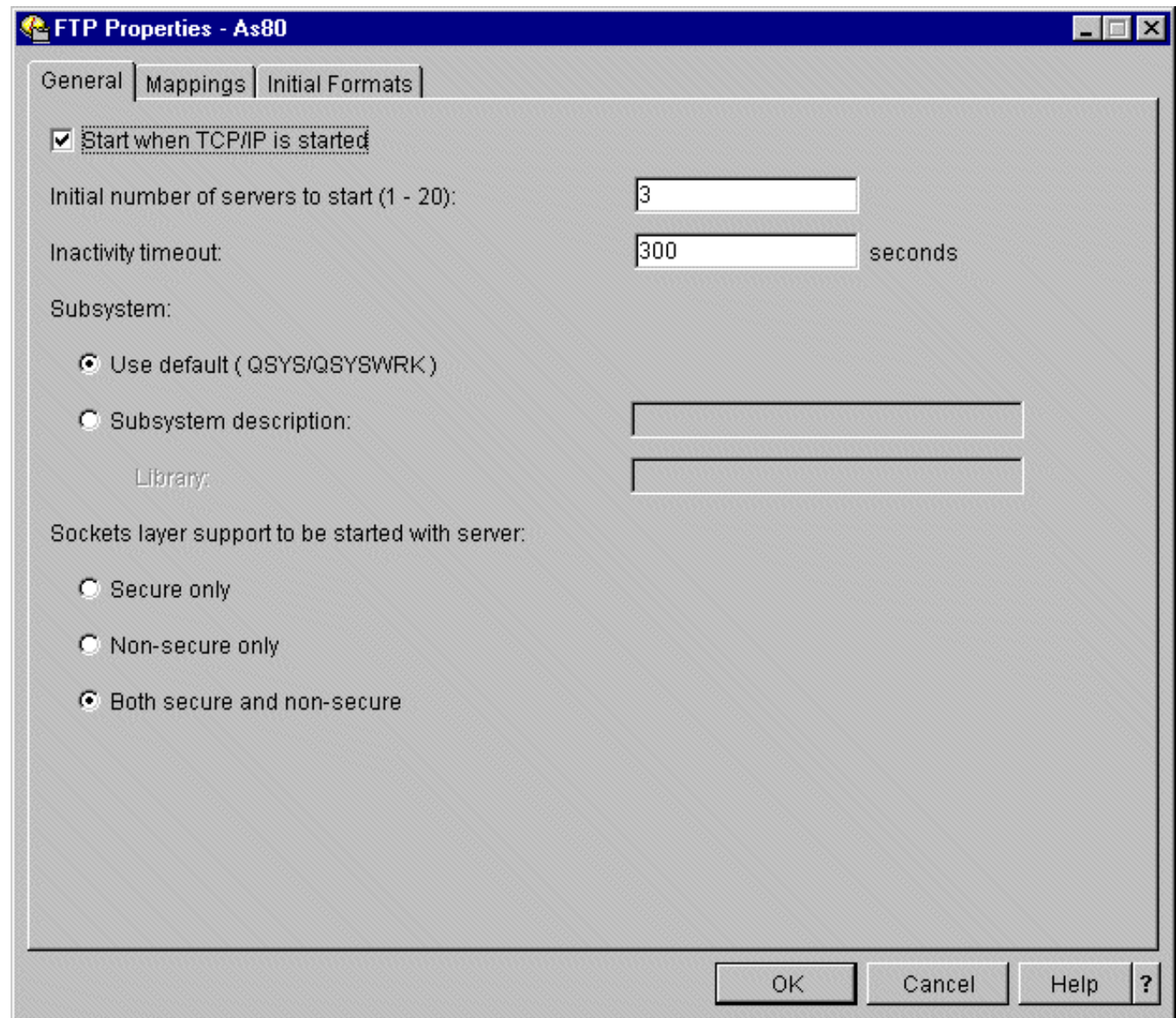
This occurs when a hacker uses the FTP server as an intermediary to send an untraceable datastream to another server. The implementation of the PORT subcommand will be changed to disallow TCP port values of less than 1024. This will prevent the server from being used to mount a bounce attack against most of the well-known TCP services.

The subsystem in which the FTP server job will run in can be set from either operations navigator or via the CL Command *Change FTP Attributes* (CHGFTPA). This can eliminate performance issues that can arise with sharing the resources in the QSYSWRK subsystem.

The FTP client can now specify the port it will use to communicate with the server. The PORT parameter can be selected when initiating an FTP client connection.

SSL or TLS

Client certificate enabling



The iSeries FTP server can now provide a secure link in which data can be transferred over. The FTP server has been enabled to provide a secure connection using Secure Socket Layer (SSL)/Transport Layer Security (TLS). RFC 2228 (*FTP Security Extensions*) provides the framework for providing secure FTP. The FTP server subcommands AUTH, PBSZ, and PROT have been added to the FTP server. SSL for the FTP server can be enabled from either operations navigator or using the CL command *Change FTP Attributes* (CHGFTPA) command. Digital Certificate Manager is used to identify which certificate will be used by the FTP server.

An FTP client can connect directly to a "secure FTP" port (TCP port 990), in which case the session is set up with SSL/TLS initially. Another way is for the FTP client to connect to the FTP server on the regular (non-encrypted) port (TCP port 21) and then negotiate authentication and encryption options (by sending commands to the FTP server and interpreting the server's responses to those commands).

Client authentication is enabled via the Digital Certificate Manager. When the iSeries receives a client certificate, the FTP server will check the user specified on the USER subcommand against the user profile specified by the client certificate. If these match, the user be logged on without requiring a password prompt. If the user name does not match (with the exception of anonymous), the logon will be rejected.

From operations navigator, there are three options related to SSL/TLS:

▶ **Secure only**

SSL connections are only allowed

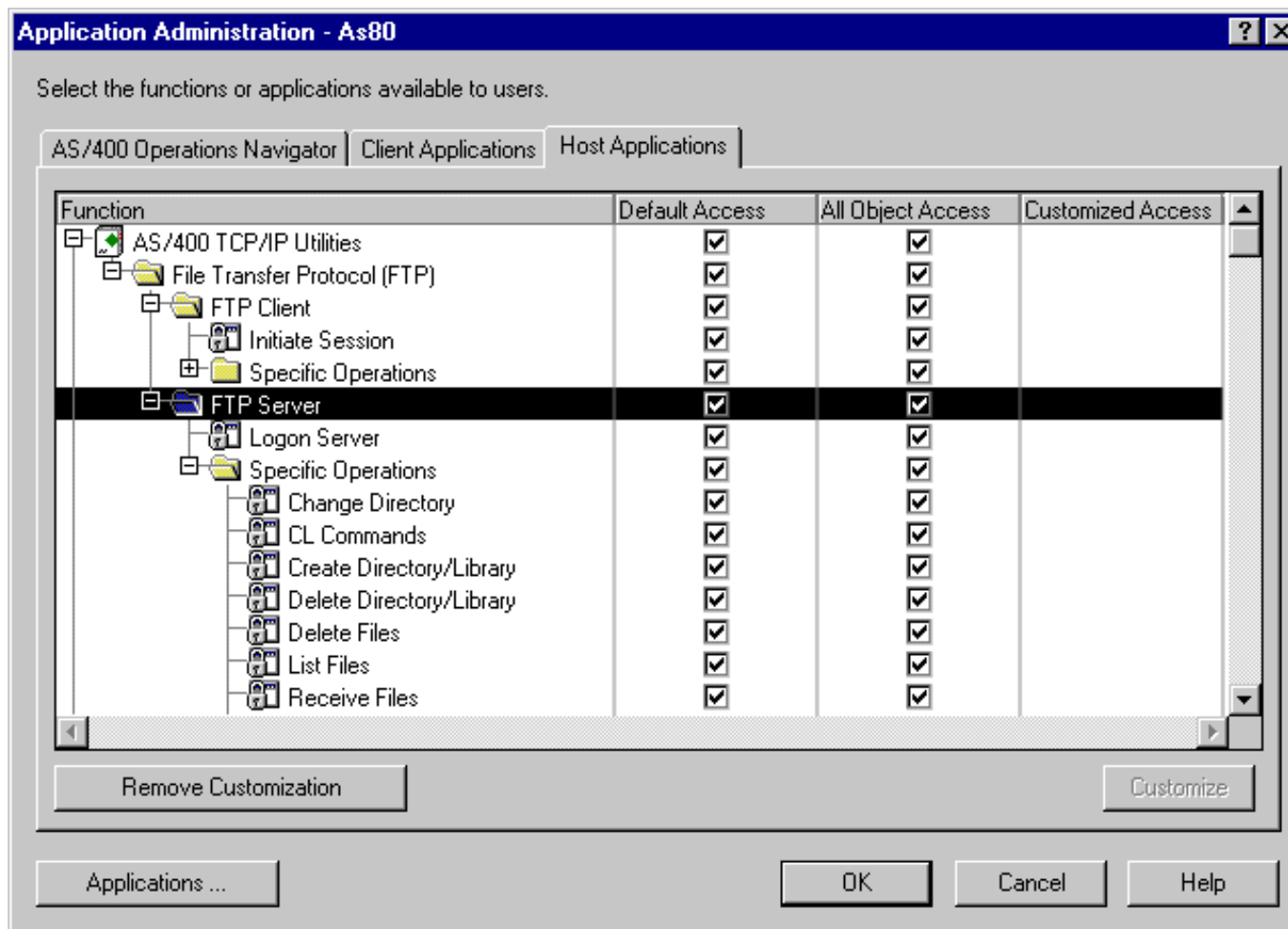
▶ **Non-secure only**

SSL connections are not allowed. FTP server will still allow non-encrypted anonymous FTP session as an exception. Since enabling anonymous FTP requires a customer written exit program, allowing this exception does not compromise the security of the system.

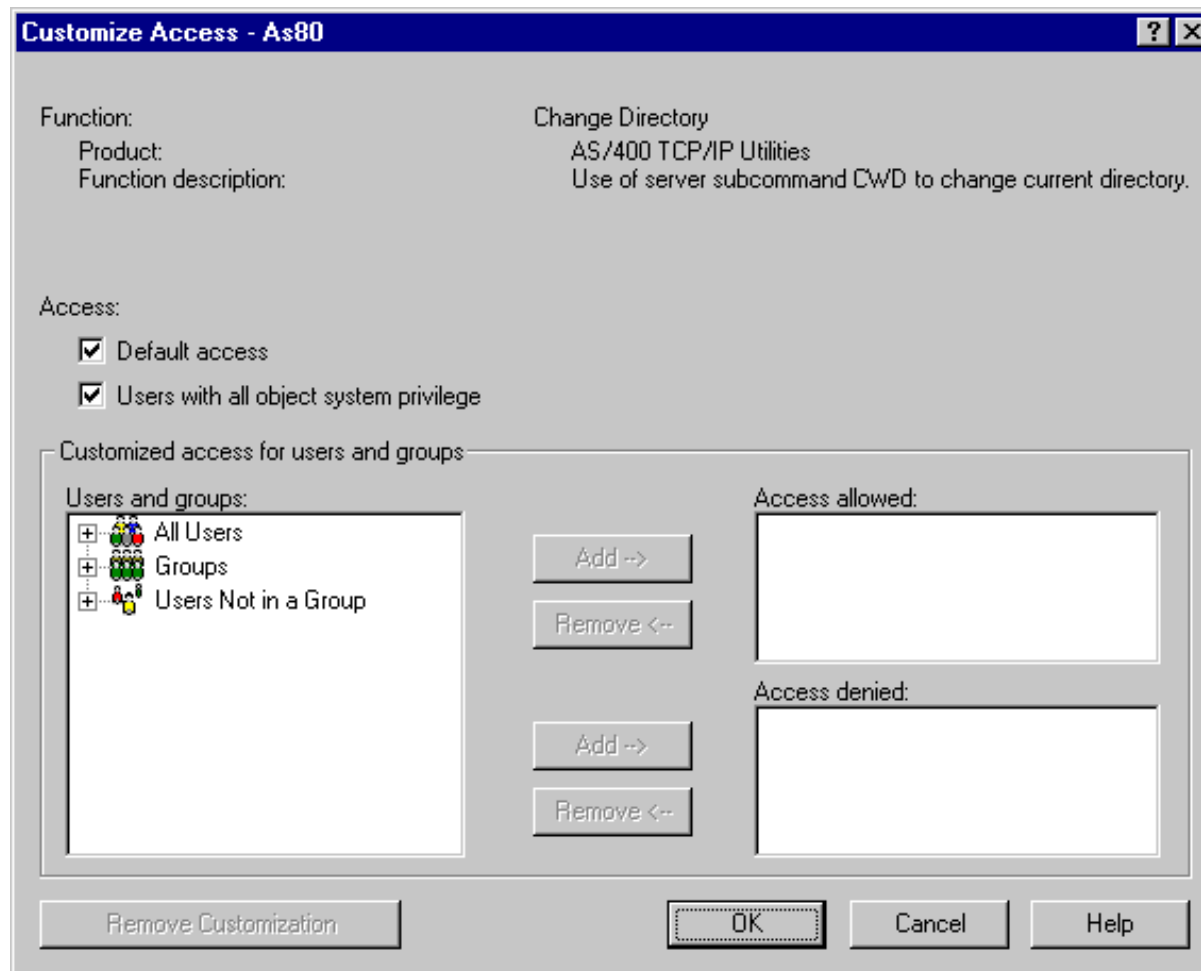
▶ **Both secure and non-secure**

FTP Application Administration

Replacement for exit programs allowing or denying client or server FTP logons/commands



FTP Application Administration



Previously, the Request Validation Exit Point was the only method for controlling FTP access. A new capability for limiting access to specific FTP operations is provided through the use of the Operations Navigator **Applications Administration** interface. This capability allows a system administrator to control the FTP operations that each user can perform. The FTP operations that can be controlled are the same as those supported by the present TCP/IP Request Validation Exit Point. This new capability is an easier alternative because it does not require the customer to provide an Exit Program for Exit Point. This new capability is not as robust as the Request Validation Exit Point which enables additional information (i.e. User IP address, file names, etc.) to be used as a decision basis for allowing or denying an operation.

The limit function capability allows each user to have an ALLOW or DENY setting for each registered FTP application function. When it is set to DENY, the user will never be allowed to use that FTP function.

The default setting for allow registered FTP functions is ALLOW. The system administrator can change this using the **Application Administration** interface. The following steps explain how to access it.

- ▶ Right click on system name
- ▶ Left click on **Application Administration**
- ▶ Click on the **Host Applications** tab
- ▶ Expand **AS/400 TCP/IP Utilities**
- ▶ Expand **File Transfer Protocol (FTP), FTP Client** and/or **FTP Server**
- ▶ Select the function you want to control and press **Customize**

If the limit function capability is used to allow access, the user may still be disallowed usage via an Exit Program.

Telnet Enhancements

IBM @server. For the next generation of e-business.

Telnet Server Enhancements

Enhanced Telnet Server Security

Client certificate authentication set from the Digital Certificate Manager interface

Support for 128 byte password

Support for SHA-1 password encryption in addition to DES7

Connection feedback to client

Client certificate authentication was available at earlier releases with PTF SF61406 (V4R4) and SF61427 (V4R5). It was enabled through the use of a data area. At V5R1, client authentication enablement is now handled through Digital Certificate Manager (DCM). Client certificate authentication gives additional security to your Telnet connections. This can be beneficial when making connections from the Internet. The Telnet server listens for SSL traffic on port 992.

Note: Configuration of client certificate authentication done at V4R4 or V4R5 will not migrate to V5R1.

The OS/400 Telnet server will now support 128 byte passwords. Enabling 128 byte passwords on the iSeries is done by setting the *Maximum Password Length* system value (QPWDMAXLEN) to 128.

Before V5R1, the OS/400 Telnet server supported DES7 password encryption. At V5R1, the Telnet server can additionally support *Secure Hash Algorithm-1* (SHA-1). The *Password Level* system value (QPWDLVL) determines whether DES7 or SHA-1 is used. If it has a value of '0' or '1', then DES7 will be used. If the value is '2' or '3', then SHA-1 will be used. Encryption is used for automatic sign-on. If the encryption used by the client does not match the server, the automatic sign-on will fail and user will be presented with a sign-on display on the target system or a failure message on the source system.

SHA-1 provides a better encryption algorithm than DES7 but is a little bit slower.

The Telnet server supports a new option which allows diagnostic information to be sent to the client. If the iSeries Telnet server receives this new parameter it will then provide information to the client on such things as why automatic sign-on failed.

Automatic Signon

Feedback information

```
Start TCP/IP TELNET (TELNET)

Type choices, press Enter.

ASCII tab stops . . . . . *DFT          0-133, *DFT, *NONE
      + for more values
Coded character set identifier *MULTINAT 1-65533, *MULTINAT...
ASCII operating mode ID . . . . *VT220B7 , *VT220B8, *VT100...
Port . . . . . *DFT          1-65534, *DFT
Remote virtual display . . . . . *DFT          Name, *DFT
Remote user . . . . . *NONE          Name, *NONE, *CURRENT
Remote password . . . . . *NONE

Remote password encryption . . . *DES7          , *SHA1, *NONE
Remote initial program . . . . . *RMTUSRPRF Name, *RMTUSRPRF, *NONE
Remote initial menu . . . . . *RMTUSRPRF Name, *RMTUSRPRF, *SIGNOFF
Remote current library . . . . . *RMTUSRPRF Name, *RMTUSRPRF
Remote keyboard type . . . . . *RMTSYS          , *LCL
Remote codepage . . . . . *RMTSYS          , *LCL
Remote character set . . . . . *RMTSYS          , *LCL

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```


Notes: Telnet Client Enhancements

The existing Pascal logic in the iSeries Telnet client has been rewritten using sockets. This transition away from the Pascal based design will free the TCP/IP Transport Stack from continuing to maintain and support the Pascal API interface. As a result, TCP/IP support for Pascal APIs will most likely be dropped in the future.

The V5R1 client supports the new option which allows for diagnostic information to be sent to the client. The client will inform the server that it will accept and handle Display Confirmation Records. These records will contain a return code indicating if the connection attempt was successful or not and why it was unsuccessful. The return code information can be viewed in the joblog for this client.

The iSeries will now support TN5250E negotiations. The iSeries Telnet client will now be able to specify device name, session settings and automatic signon features for terminal sessions only. There are no plans at this time to support these features for printer sessions. The client supports password encryption DES7 and SHA-1. Also, the password can now be 128 byte in length.

SMTP Enhancements

IBM @server. For the next generation of e-business.

SMTP Extensions:

- Dial-Up Retrieval (ETRN)
- Delivery Status Notification (DSN)
- 8-bit MIME transport service

Selectable subsystem for SMTP

Mail filtering to prevent virus proliferation

Dual stack support

Multiple domain support

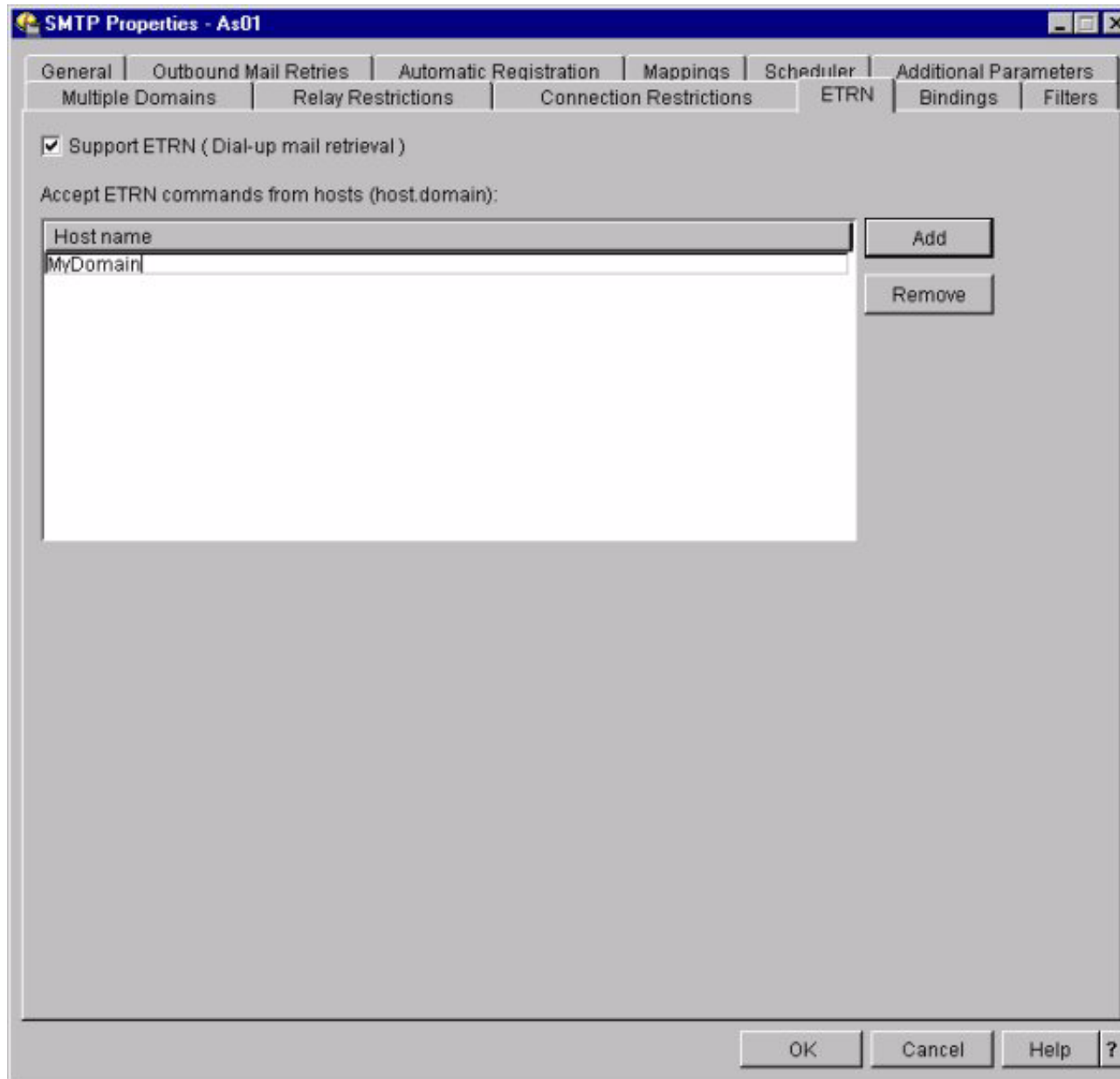
Anti-spam: mail traffic restriction

ETRN or dial-up retrieval uses a mechanism to define extensions to the SMTP service whereby a client ("sender-SMTP") may request that the server ("receiver-SMTP") start the processing of its mail queues for messages that are waiting at the server for the client machine. If any messages are at the server for the client, then the server should create a new SMTP session and send the messages at that time. The ETRN command is sent when a dial up connection (PPP) is made to the ISP's mail server. The ISP's server responds by sending all mail queued for the registered domain over the connection. The ISP defines a "domain" for the subscriber (SMTP server). It is registered by the ISP with the Mail record being that of the ISP provider. Any mail directed to a user on this domain (userid@domain) will be resolved to the provider's mail hub and queued for delivery. The iSeries SMTP server can also play the role of ISP and respond to a ETRN command by sending queued to a subscriber.

Delivery Status Notification (DSN) is a MIME content-type that may be used by a message transfer agent (MTA) or electronic mail gateway to report the result of an attempt to deliver a message to one or more recipients. This content-type is intended as a machine-processable replacement for the various types of delivery status notifications currently used in Internet electronic mail.

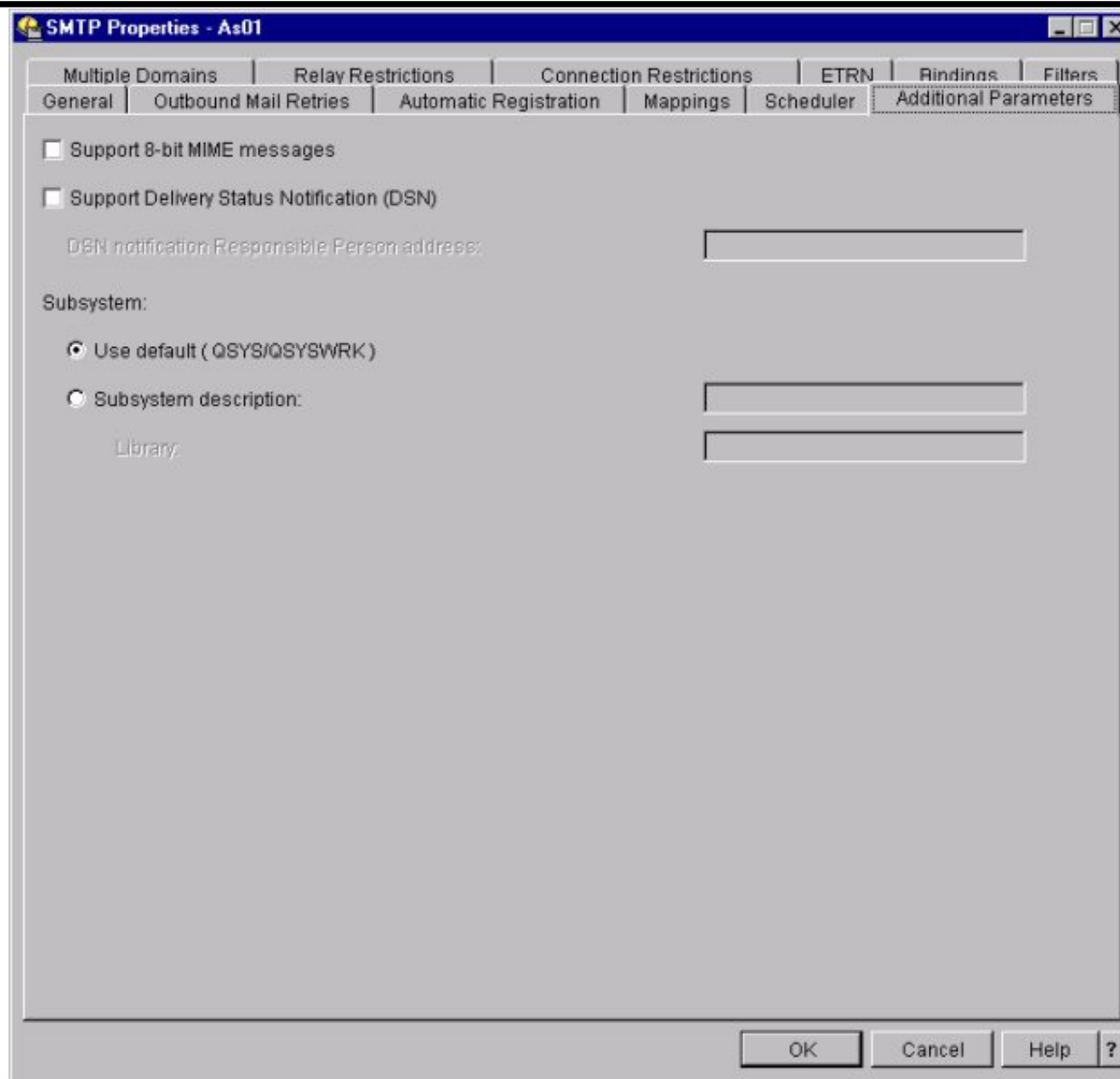
The **8-bit MIME transport service** extension allows a client SMTP to submit, using the MAIL command, a content body consisting of a MIME message containing arbitrary lines of octet-aligned material, it first issues the EHLO command to the server SMTP. If the server SMTP responds with code 250 to the EHLO command, and the response includes the EHLO keyword value 8BITMIME, then the server SMTP is indicating that it supports the extended MAIL command and will accept MIME messages containing arbitrary octet-aligned material.

Dial-Up Retrieval (ETRN)



IBM  server. For the next generation of e-business.

SMTP Enhancements

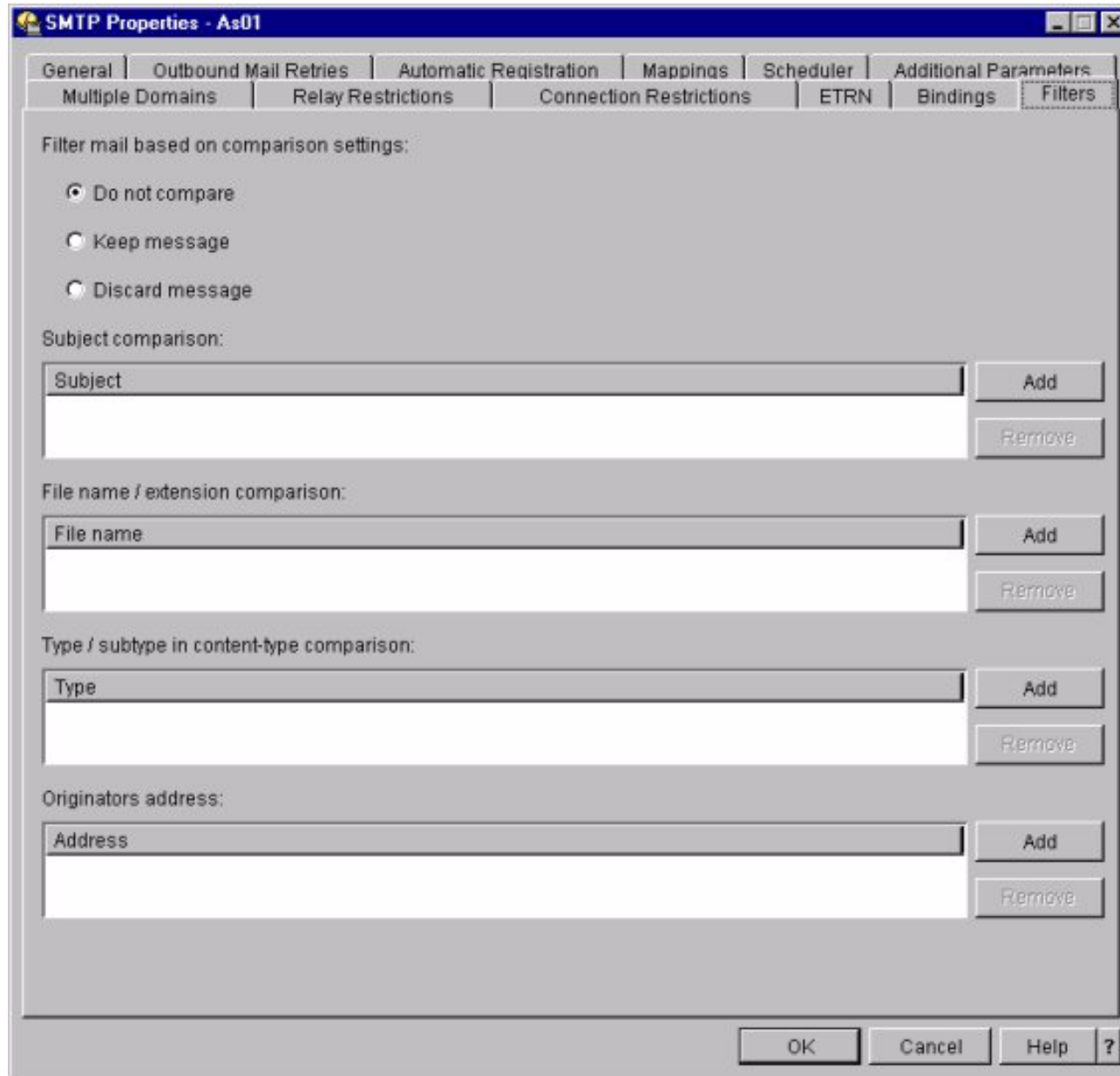


The screenshot shows a window titled "SMTP Properties - As01" with several tabs: "Multiple Domains", "Relay Restrictions", "Connection Restrictions", "ETRN", "Bindings", "Filters", "General", "Outbound Mail Retries", "Automatic Registration", "Mappings", "Scheduler", and "Additional Parameters". The "Additional Parameters" tab is active. It contains the following options and fields:

- Support 8-bit MIME messages
- Support Delivery Status Notification (DSN)
- DSN notification Responsible Person address:
- Subsystem:
 - Use default (QSYS/QSYSWRK)
 - Subsystem description:
- Library:

At the bottom right, there are buttons for "OK", "Cancel", "Help", and a question mark icon.

IBM  server. For the next generation of e-business.



The screenshot shows the 'SMTP Properties - As01' dialog box with the 'Filters' tab selected. The dialog has a menu bar with 'General', 'Outbound Mail Retries', 'Automatic Registration', 'Mappings', 'Scheduler', 'Additional Parameters', 'Multiple Domains', 'Relay Restrictions', 'Connection Restrictions', 'ETRN', 'Bindings', and 'Filters'. The 'Filters' tab contains the following sections:

- Filter mail based on comparison settings:**
 - Do not compare
 - Keep message
 - Discard message
- Subject comparison:**
 - Text box: Subject
 - Buttons: Add, Remove
- File name / extension comparison:**
 - Text box: File name
 - Buttons: Add, Remove
- Type / subtype in content-type comparison:**
 - Text box: Type
 - Buttons: Add, Remove
- Originators address:**
 - Text box: Address
 - Buttons: Add, Remove

At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Help', and a question mark icon.

The V5R1 SMTP server will provide filtering by subject, type/subtype, filename/extension, and originator's address. The filename/extension filter will have the option of changing the extension to prevent Windows, as an example, from recognizing it as an executable application. An additional header will be inserted stating that an unacceptable filename/extension was detected and that it was altered. An example would be the LOVE-LETTER-FOR-YOU.TXT.VBS

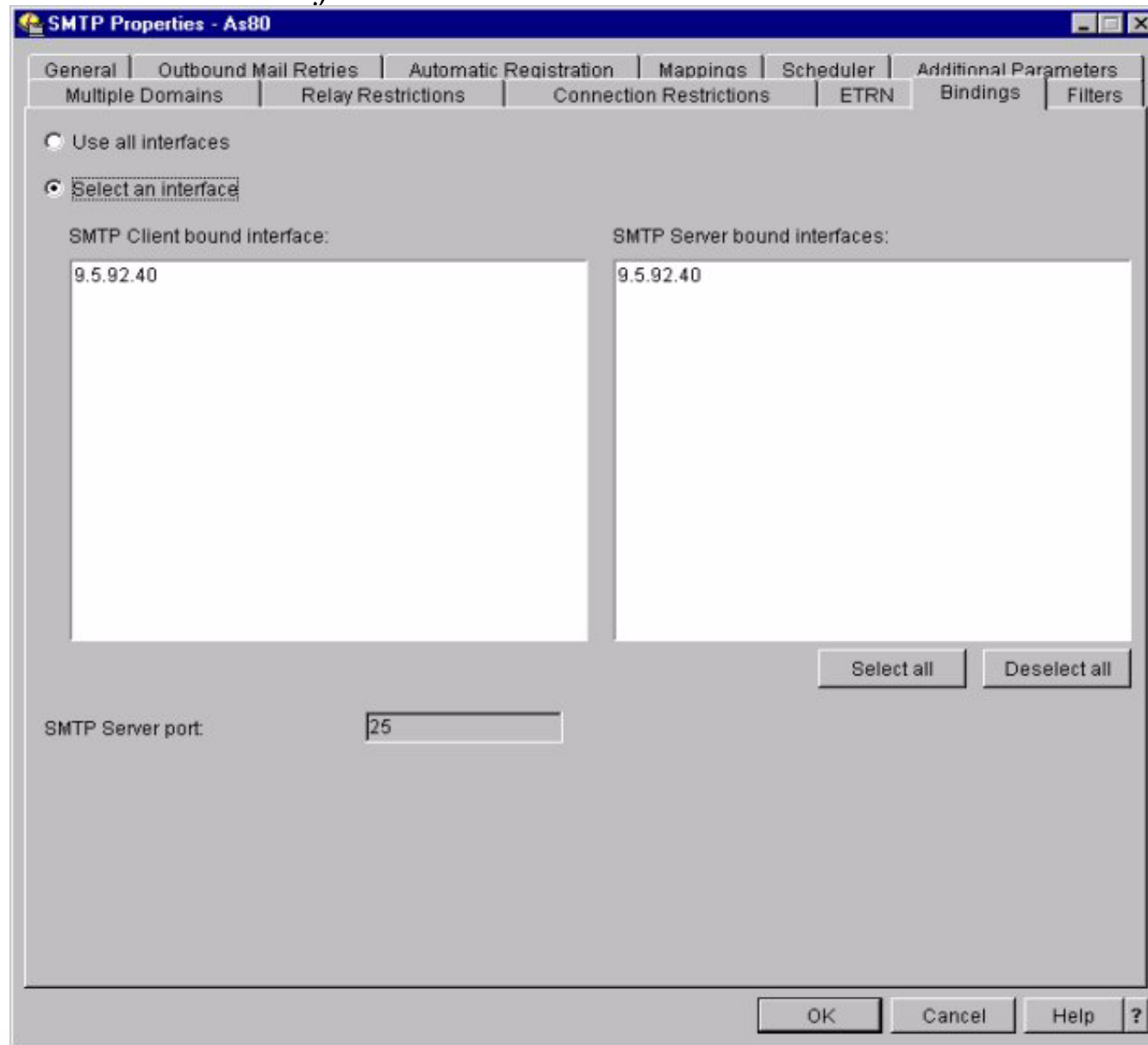
The filtering criteria will be stored in QUSRSYS/QATMFTRLST under the following members:

- ▶ FTRSUBJECT
- ▶ FTRFILENAME
- ▶ FTRTYPE
- ▶ FTRORIGIN

These members can be displayed by using Operation's Navigator SMTP server's filters page or by using the *Display Physical File Member* (DSPPFM) command. The file can be replicated to remote systems allowing the filtering data to be composed once and then distributed to supported systems.

SMTP Dual Stack Support

Configuration via GUI Interface



Dual Stack Support is available at V4R2 through V5R1. Dual Stack Support allows a customer to run Domino and iSeries SMTP server natively. It also allows a customer to bind an iSeries SMTP client to a particular interface. The V4R2 through V4R5 support uses a data area to enable the function. The following PTFs enable the data area:

- V4R2: SF58556
- V4R3: SF58661
- V4R4: SF60787
- V4R5: SF60827

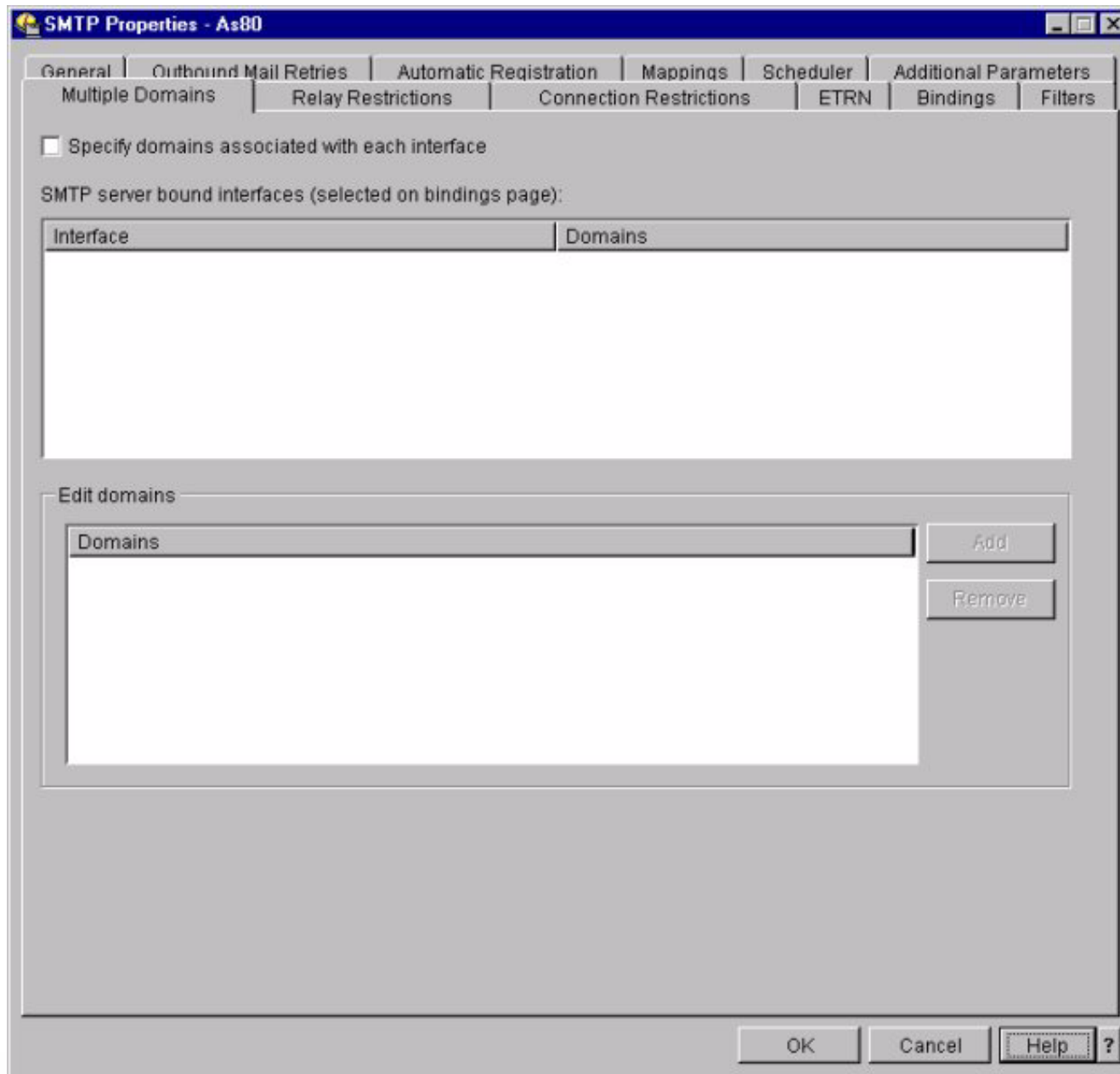
The support in V5R1 will migrate the current support using the data areas (QUSRSYS/QTMSBNDIP for the server and QUSRSYS/QTMSCBNDIP for the client) that are used as input of the IP addresses to bind to, to physical file QTCP/QATMIFCLST and member CLNTBNDIP (for the client binding address) and SVRBNDIP (for the server binding address).

The configuration for Dual Stack Support at V5R1 is handled via Operations Navigator. To access the configuration, select **Properties** for SMTP, then select the **Bindings** tab. Select **Use all interfaces** to have the SMTP server port (TCP port 25), dedicated to the SMTP server on all interfaces. Select **an interface** to specify the client and server bound interfaces for the SMTP client and server to bind to. The remaining interfaces are available for other services.

Example: You want to have an SMTP server and a Domino mail server running on the same system. You would bind the SMTP server to one or more of the interfaces and use one of the remaining interfaces for the Domino server (configurable within Domino).

Don't forget to update the Domain Name Server, Local Host Table or System Distribution Directory entries to reflect the changes on your SMTP configuration.

SMTP Multiple Domain Support



IBM  server. For the next generation of e-business.

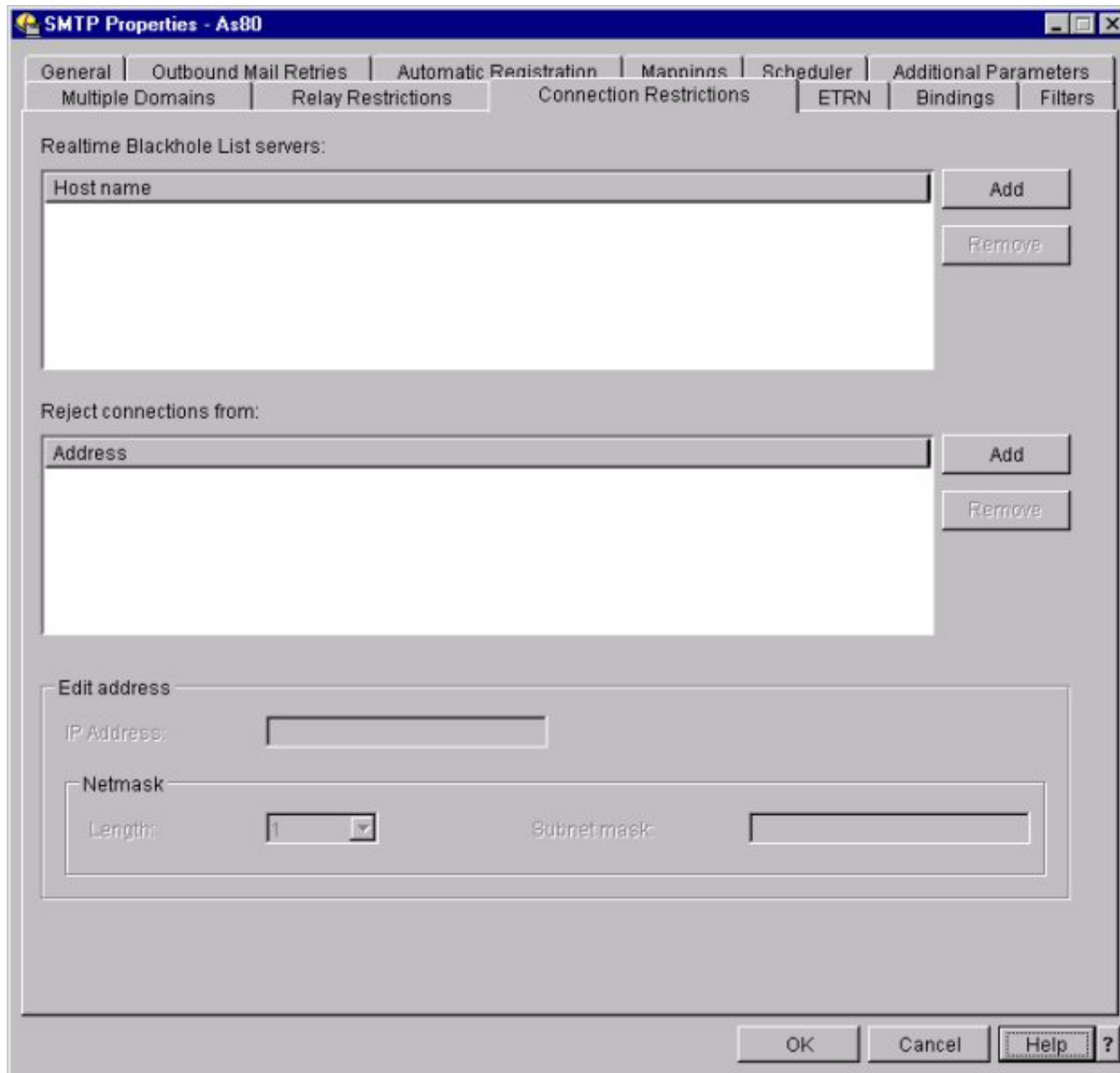
Notes: SMTP Multiple Domain Support

In order for the iSeries SMTP to host ISP functions, it is necessary for the SMTP server to appear to operate in multiple domains. Based upon the configuration, the iSeries SMTP server will know how to build the "Received:" line at the top of the e-mail so that it appears to have been received by the user's domain.

The SMTP client will use this configuration to know which interface to bind to when it sends e-mail, which mail to consider local (resolve and send on its own) or forward to a configured firewall mail daemon (mail router with firewall parameter on).

If Dual Stack is also being used, then the GUI will pull the list of interfaces from this file to display to the administrator for selecting which domains to fill in for each interface.

SMTP: Restricting Mail Traffic (SPAM)



SMTP Properties - As80

General | Outbound Mail Retries | Automatic Registration | Mappings | Scheduler | Additional Parameters
Multiple Domains | Relay Restrictions | Connection Restrictions | ETRN | Bindings | Filters

Realtime Blackhole List servers:

Host name Add
Remove

Reject connections from:

Address Add
Remove

Edit address

IP Address:

Netmask
Length: Subnet mask:

OK Cancel Help ?

IBM  server. For the next generation of e-business.

Notes: SMTP: Restricting Mail Traffic (SPAM)

The method of controlling unwanted mail traffic, aka "SPAM", was introduced in V4R2, V4R3, and V4R4. The SPAM code was added in the following releases for 5769-TC1 using a new function PTF:

- V4R2: SF52864
- V4R3: SF53421
- V4R4: SF54014

These PTFs enabled a method to specify particular IP addresses that are allowed or refused to use the OS/400 SMTP server to relay mail. This method used a file (QUSRSYS/QTMSADRLST with members ACCEPTRLY and REJECTCNN) to specify the addresses that were allowed or rejected to relay. There was also a method, using a data area (QUSRSYS/QTMSORLY), for blocking all mail relay. At V5R1, Operations Navigator is able to access the configuration files through the SMTP properties pane. The data area that is used in previous releases to block relay entirely is migrated to the SMTP attributes which can be set using the *Change SMTP Attributes* (CHGSMTPA) command. The CL equivalent for the GUI interface of Operations Navigator is found in the commands *Add SMTP List Entry* (ADDSMTPLE) and *Remove SMTP List Entry* (RMVSMTPLE).

A new method (**Real-time Black-hole List** or RBL) will be added to allow the use of a configurable site that stores addresses of known mail abusers. The address of the originator of any mail can be sent to this site (via DNS queries) and a value will be returned indicating whether this address is listed. Mail will be accepted for relay or delivery based on the result returned.

Specify up to 3 fully qualified host names of real time blacklist (RBL) servers. The SMTP server queries these sites each time a client connects to it. See yyy on the World Wide Web for a list of known e-mail abusers. See xxx on the World Wide Web for a list of IP addresses with open relays, which are potential sources for unwanted e-mail. When your SMTP server queries these RBL servers, it finds a list of IP addresses of potential or known "spammers," e-mail clients that have sent unsolicited bulk e-mail to e-mail users. When you add these RBL servers, you give your SMTP server access to these Internet-wide e-mail abusers' IP addresses and prevent them from attacking your server.

Note: Before specifying the name of a real-time blacklist server, like MAPS RBL, please go to their Web site and follow any instructions they have on how to enable your SMTP server to query their list of IP addresses. Click Add to specify the name of a RBL server. To remove a RBL server from the list, select it and click Remove.

Notes: Mail Abuse Prevention System

IBM @server iSeries

http://mail-abuse.org



IBM @server. For the next generation of e-business.

Change SMTP Attributes (CHGSMTPA)

Type choices, press Enter.

Delivery status notification:

Responsible person	*NONE		
Subsystem description	QSYSWRK	Name, *SAME, *DFT	
Library	QSYS	Name	
Realtime Blackhole List	*NONE		
Allow relayed mail	*NONE	*SAME, *NONE, *ALL, *LIST...	
Interface/domain association	*NONE	*SAME, *NONE, *LIST	
Filter mail for virus	*DISCARD	*SAME, *NONE, *KEEP, *DISCARD	

Add SMTP List Entry (ADDSMTPLE)

Type choices, press Enter.

List type	> *ACCEPT	, *REJECT, *NEAR...
Internet address	'9.5.20.1'	
Subnet mask	'255.255.0.0'	

LDAP Enhancements

IBM @server. For the next generation of e-business.

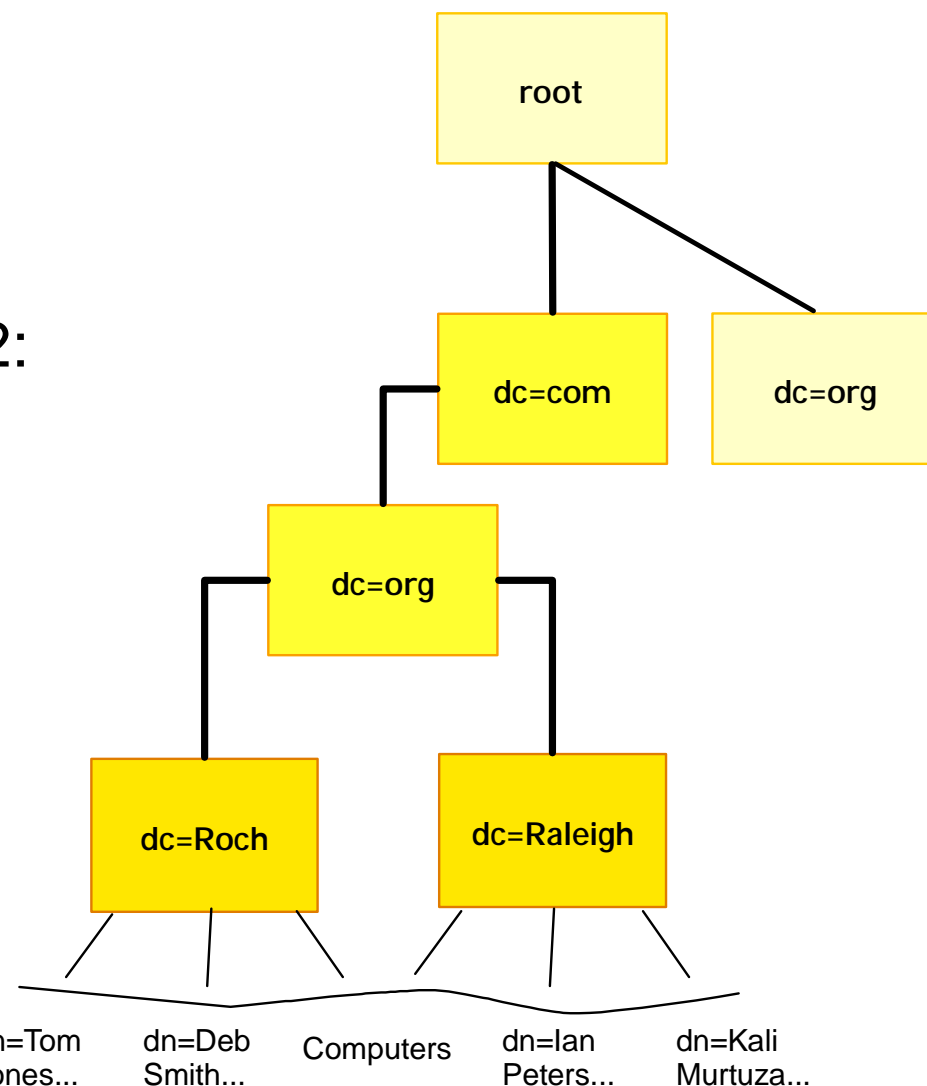
Lightweight Directory Access Protocol now part of OS/400

Automatic Configuration

Security auditing

Implements SecureWay Directory V3.2:

- Kerberos
- GSKit
- Event notification
- Transaction support
- Fine grained ACL support
- for unlimited number of connections



dn=TomJones..mail=tjones@ibm.com...telephoneNumber=101-507-1234 ▲

This foil highlights what is new with V5R1 Directory Services, which includes a default (automatic) configuration, additional security auditing and IBM SecureWay Lightweight Directory Access Protocol version 3.2 functions listed on this foil.

With V 3.2 you are not limited to the traditional hierarchy when structuring your directory. The .domain component (dc) structure, for example, is gaining popularity. With this structure, entries are composed of the parts of TCP/IP domain names. For example, dc=ibm,dc=com may be preferable to o=ibm, c=us used in previous directory structures.

Note, every server and client intending to communicate directory information needs to be using the same structure for best results.

Background information

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs over Transmission Control Protocol/Internet Protocol (TCP/IP). LDAP version 2 is formally defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, Lightweight Directory Access Protocol. LDAP version 3 is formally defined in IETF RFC 2251, Lightweight Directory Access Protocol (v3). You can view these RFCs on the Internet at the following URL:

<http://www.ietf.org>

The LDAP directory service follows a client/server model. One or more LDAP servers contain the directory data. An LDAP client connects to an LDAP Server and makes a request. The server responds with a reply, or with a pointer (a referral) to another LDAPserver.

Because LDAP is a directory service, rather than a database, the information in an LDAP directory is usually descriptive, attribute-based information. LDAP users generally read the information in the directory much more often than they change it. Updates are typically simple all-or-nothing changes. Common uses of LDAP directories include online telephone directories and e-mail directories.

The LDAP directory service model is based on entries (which are also referred to as objects). Each entry consists of one or more attributes, such as a name or address, and a type. The types typically consist of mnemonic strings, such as cn for common name or mail for e-mail address.

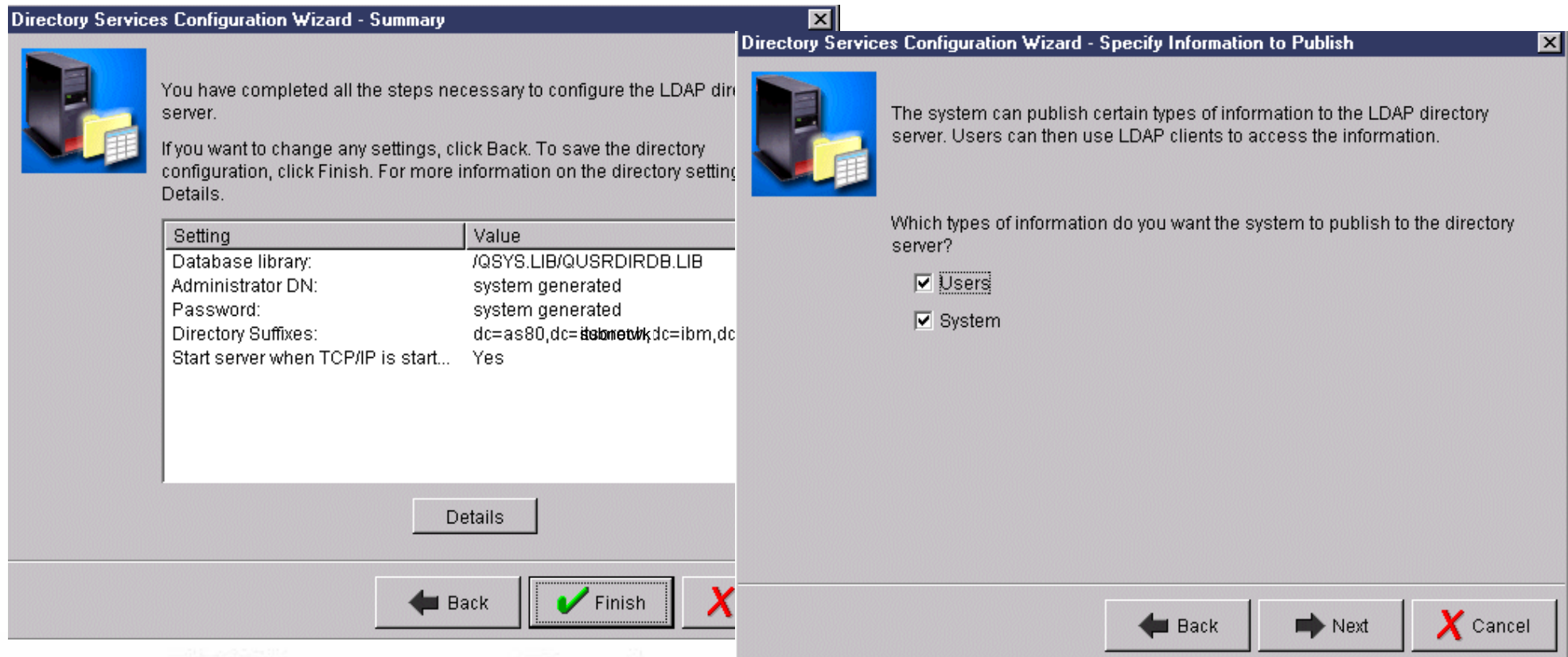
Distinguished Names (dn) uniquely identify users by the set of attributes. Directories typically also include a set of "computer" (system) entries and a set of users, along with a hierarchical schema.

For complete coverage of LDAP under OS/400 refer to V5R1 Information Center - Directory Services. There you can find a PDF document titled *Networking Directory Services (LDAP)*.

The next foils summarize the V5R1 LDAP support.

Automatic (Default) Directory Configuration

- Network -> Servers -> TCP/IP servers -> Configure
- Default cn=Administrator, password
- Default directory suffixes
- Publish "computers" (Systems) only
- Can Reconfigure to add "Publish users"



The image shows two overlapping windows from the Directory Services Configuration Wizard. The 'Summary' window on the left displays a table of configuration settings and a 'Finish' button. The 'Specify Information to Publish' window on the right shows options to publish 'Users' and 'System' information.

Directory Services Configuration Wizard - Summary

You have completed all the steps necessary to configure the LDAP directory server.

If you want to change any settings, click Back. To save the directory configuration, click Finish. For more information on the directory settings, click Details.

Setting	Value
Database library:	/QSYS.LIB/QUSRDIRDB.LIB
Administrator DN:	system generated
Password:	system generated
Directory Suffixes:	dc=as80,dc=ibmnetwk,dc=ibm,dc=
Start server when TCP/IP is start...	Yes

Details

Back Finish X

Directory Services Configuration Wizard - Specify Information to Publish

The system can publish certain types of information to the LDAP directory server. Users can then use LDAP clients to access the information.

Which types of information do you want the system to publish to the directory server?

Users

System

Back Next X Cancel

Beginning with V5R1, Directory Services comes automatically installed with a limited default configuration. Directory Services provides a wizard in to assist you in configuring the LDAP directory server for your specific situation. You may select to run the default configuration or complete your own configuration.

You may run this wizard as part of EZ-Setup, or run it later from Operations Navigator. Use this wizard when you initially configure the directory server. You may also use the wizard to reconfigure the directory server.

Notes:

- When you use the wizard to reconfigure the directory server, you start configuring from "nothing". The original configuration is deleted rather than changed. The directory data, however, is not deleted. It remains stored in the library that you selected upon installation (QUSRDIRDB by default). The change log also remains intact, in the QUSRDIRDCL library by default.
- If you want to start completely from scratch, clear those two libraries before starting the wizard.
- If you want to change the directory server configuration, but not clear it completely, right-click Directory and select Properties. This does not delete the original configuration.

You must have *ALLOBJ and *IOSYSCFG special authorities to configure the server. If you want to configure OS/400 security auditing, you must also have *AUDIT special authority.

To start the Directory Services Configuration Wizard, take these steps:

- In Operations Navigator, expand Network.
- Expand Servers.
- Click TCP/IP.
- Right-click Directory and select Configure.

Note, if you have already configured the directory server, click Reconfigure rather than Configure. Follow the on-screen instructions that the Configure Directory Server wizard gives to configure your LDAP directory server.

Using the default directory configuration

The directory server uses the default configuration when all of the following are true:

- Administrators have not run the Directory Services Configuration Wizard or changed directory settings with the properties pages
- Directory Services publishing is not configured
- The LDAP directory server cannot find any LDAP DNS information

If the LDAP directory server uses the default configuration, then the following occurs:

- The LDAP directory server automatically starts when TCP/IP starts.
- The system creates a default administrator, "cn=Administrator". It also generates a password that is used internally. If you need to use an administrator password later, you can set a new one from the Directory Services property page.
- A default suffix is created that is based on the system's IP name. For example, if your system's IP name is "mary.acme.com", the suffix is "dc=mary,dc=acme,dc=com".
- The LDAP directory server uses the default data library QUSRDIRDB. The system creates it in the system ASP.
- The server uses port 389 for unsecure communications. If a digital certificate has been configured for LDAP, secure sockets layer (SSL) is enabled and port 636 is used for secure communications

The following defaults then exist for Directory Services publishing:

- The system publishes information to the local LDAP directory server
- Publishing does not use SSL
- Publishing uses containers under the default suffix
- For authentication to the directory server, OS/400 uses the "cn=Administrator" ID and the system-generated password
- The system publishes only "computer" information. There is no "user information" in the default configuration.

You may want to put the library that stores the directory data in a user auxiliary storage pool (ASP) rather than the system ASP.

When the wizard finishes, your LDAP directory server has a basic configuration. If you are running Lotus Domino on your system, then port 389, the default port for the LDAP server, may already be in use by Domino's LDAP function. You must either change the port that Lotus Domino uses or change the port that Directory Services uses. If you want to use another port for a different reason, you can change it now as well.

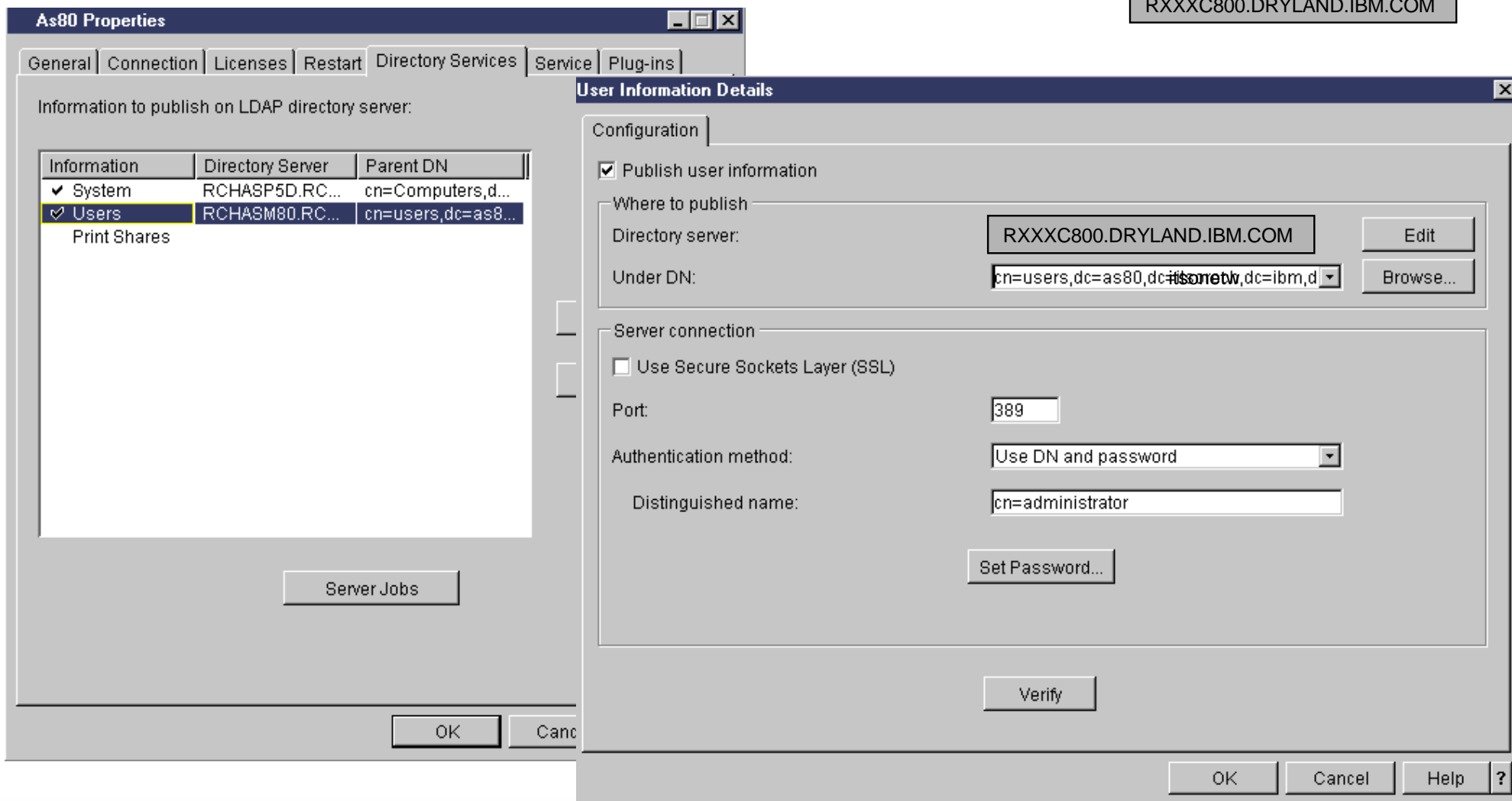
If you want to, you can start the server at this point. Before starting the server, however, you may want to do some or all of the following things:

- Import data to the server
- Enable Secure Sockets Layer (SSL) security
- Enable Kerberos authentication
- Set up a referral

Simple Update to Default Directory Example

IBM  server iSeries

- Specify/change default Administrator Password
- Configure Directory to "Publish Users"



The screenshot shows the 'As80 Properties' dialog box with the 'Directory Services' tab selected. The 'Information to publish on LDAP directory server:' section contains a table with the following data:

Information	Directory Server	Parent DN
<input checked="" type="checkbox"/> System	RCHASP5D.RC...	cn=Computers,d...
<input checked="" type="checkbox"/> Users	RCHASM80.RC...	cn=users,dc=as8...

Below the table is a 'Print Shares' button. The 'User Information Details' dialog box is open over the 'Users' entry, showing the following configuration:

- Publish user information
- Where to publish:
 - Directory server: RXXXC800.DRYLAND.IBM.COM (Edit)
 - Under DN: cn=users,dc=as80,dc=ibm,d... (Browse...)
- Server connection:
 - Use Secure Sockets Layer (SSL)
 - Port: 389
 - Authentication method: Use DN and password
 - Distinguished name: cn=administrator
 - Set Password...

Buttons for 'OK', 'Cancel', and 'Verify' are visible at the bottom of the 'User Information Details' dialog.

IBM  server. For the next generation of e-business.

In Operations Navigator right click system name under "My Connections."

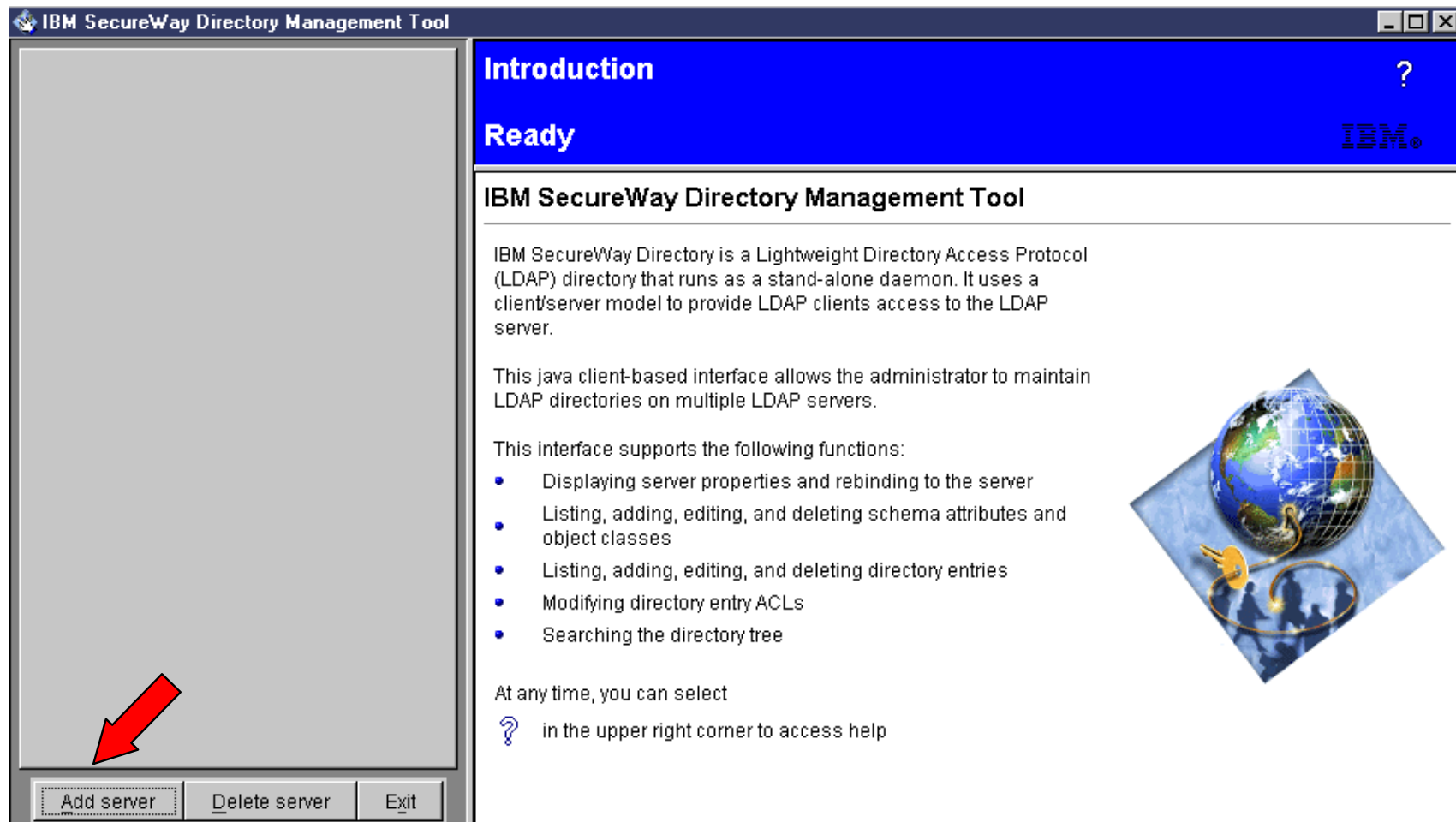
- Select **Properties**, then **Directory Tab**
- Check Users under the Information column and click the Details button
- Check "Publish user information" to change the defaults shown here.
 - Distinguished Name under which "user entries" are stored
 - Use SSL to encrypt published data. Note, if SSL is to be used you must use OS/400 Digital Certificate Manager (DCM) to set up certificates and assign one or more certificates to the Directory Server. DCM is accessed under the ADMIN server provided under OS/400 HTTP Server for AS/400.
You can use the OS/400 command STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN) to start this server.
On a browser, use `http://host-name:2001/` to connect to the ADMIN server and display the **AS/400 Tasks** frame.
 - Change the LDAP port to another port. Note, if Directory Services and Domino servers are to be active at the same time either Directory Services or Domino must change their default port from 389.
 - Authentication method: Specifies the method OS/400 and Operations Navigator use to connect to the LDAP directory server when publishing AS/400 information. Options include:
 - ✓ **Use DN and password:** Uses the distinguished name (DN) and password of an object on the directory server to connect to the directory server.
 - ✓ **Use Kerberos name and password:** Uses a Kerberos principal name and password to connect to the directory server. Select this option only if Kerberos is enabled for the directory server, or if you plan to enable it immediately.
 - ✓ **Use Kerberos key tab file and name:** Uses a Kerberos key tab file name and Kerberos principal name to connect. Select this option only if Kerberos is enabled for the directory server, or if you plan to enable it immediately.

Use of Kerberos support is new for V5R1 - a foil later in this presentation shows more about this support.

Before describing V5R1 LDAP support functional enhancements, the next foils give some background on use of the Directory Management Tool to manage the directory entries after Operations Navigator is used to configure the directory server.

Directory Management Tool

- On client Command Prompt, enter dmt
- Click OK to first window
- Click Add Server



Directory Management Tool

Note: Starting with V4R5, OS/400 includes the IBM SecureWay Directory Management Tool (DMT) which provides you with a graphical user interface for managing LDAP directory content from a Windows client workstations. The tasks that you can perform with the DMT include the following:

- Browsing directory schema
- Adding, editing, and deleting object classes
- Adding, editing, and deleting attributes
- Browsing and searching the directory tree
- Adding, editing, viewing, and deleting entries
- Editing entry RDNs (Relative Distinguished Names)

The DMT is part of the Windows LDAP client that is included with V4R5 and V5R1 OS/400 Directory Services support. The client software is shipped in an integrated file system directory. On OS/400 you must use Operations Navigator to "define (configure) the directory server" per the previous foil notes. DMT can manage entries, but cannot define the directory itself.

To install the Windows LDAP client, including the DMT, onto a PC, follow these steps:

- In Operations Navigator, expand **File Systems**. Expand **File Shares**.
- Double-click **Qdirsrv**.
- Double-click **UserTools**.
- Double-click **Windows**.
- Double-click **setup.exe** to start installing the DMT. Follow the on-screen instructions to complete the installation

Once you have DMT installed you need to configure one or more directory servers you wish DMT to connect to and manage entries for. DMT "user's guide" information is contained in the path (US example):

- C:\Program Files\IBM\LDAP\web\enUS1253\dmtdparent.htm

Enter "dmt" from a client workstation's command screen. DMT has optional parameters:

- -f flag can be used to override the default dmt.conf configuration file. Values must specify the fully qualified path and file name of this other configuration file. You can configure this tool to automatically connect to one or more directory servers and to log in as particular Distinguished Names (DNs) when it is started.

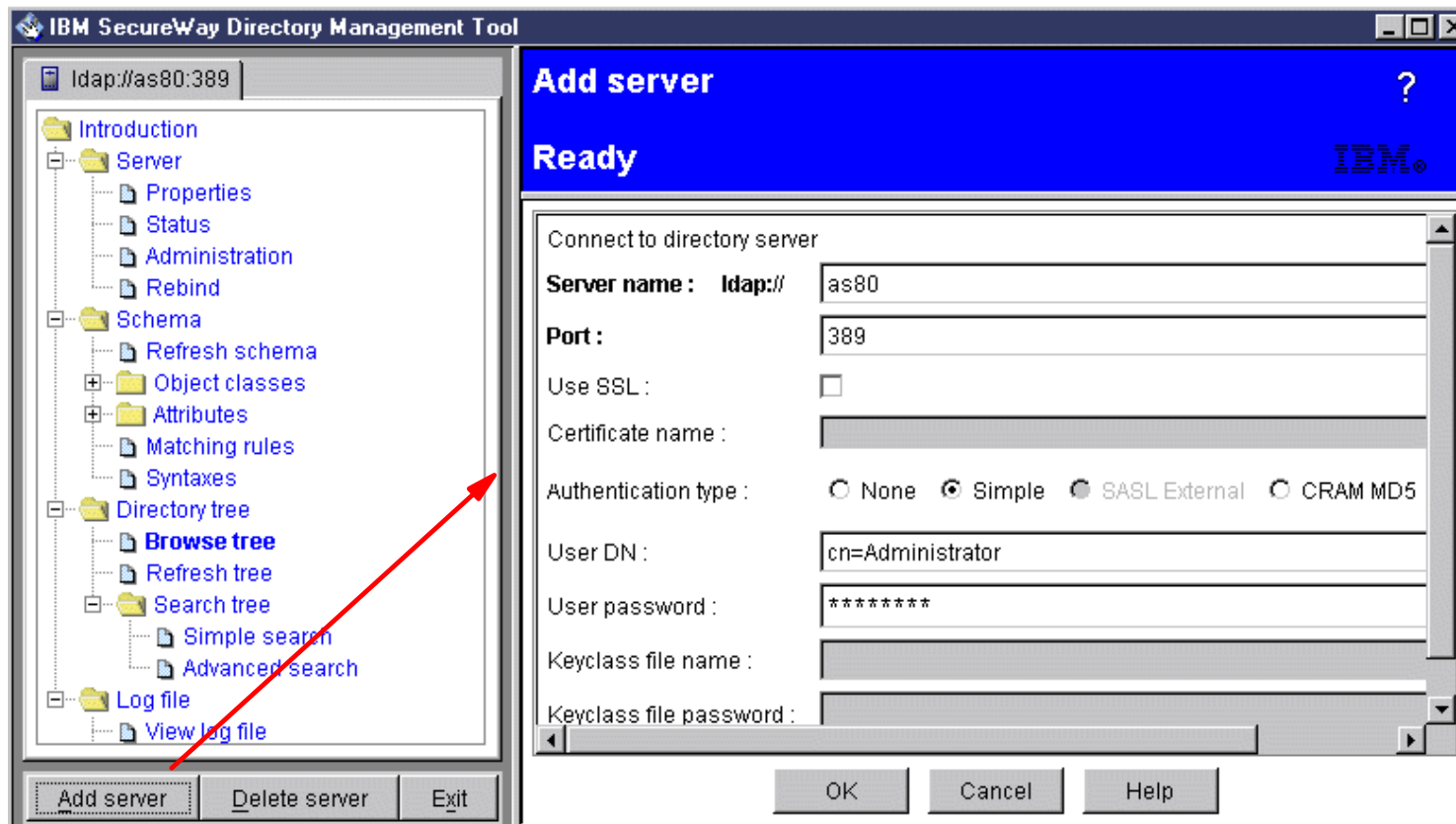
If you just key in "dmt" before you do any customizing of DMT, you get an error window as the default tries to connect to the client workstation's "localhost:389." Click the OK button to get the screen shown on this foil.

- -k flag which specifies the path to the keyclass file used for encryption when encryption is being used.

If using a Windows NT client you can start DMT from the Start menu: Start -> Programs -> IBM SecureWay Directory -> Directory Management Tool

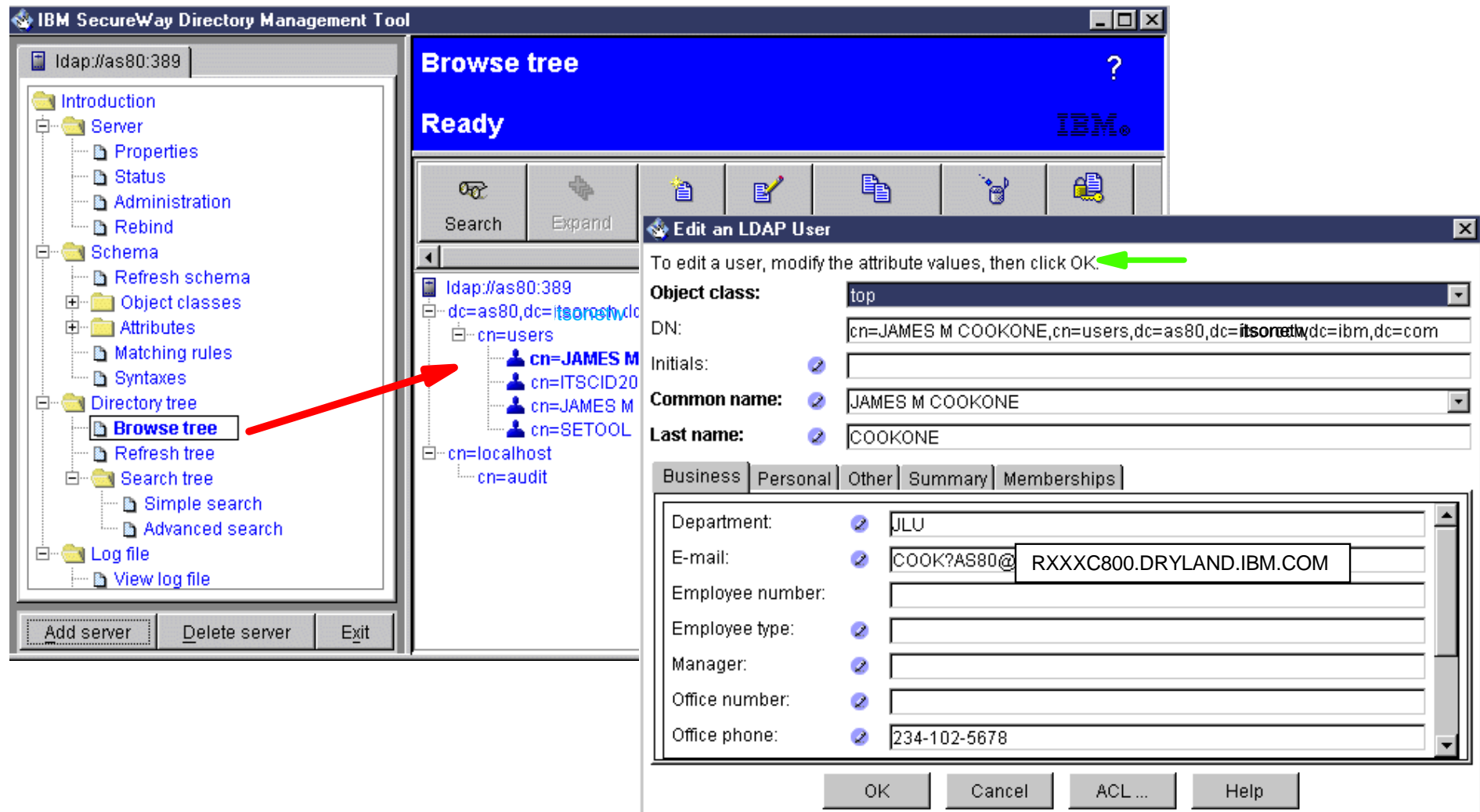
DMT - Connecting to a Directory Server

- DSN Name, Port number
- Select SSL use, Authentication Type
- Enter Administrator Distinguished Name, Password



Showing Directory Entries

- Connect to LDAP server
- Click function.... **edit user**, or



Notes: Showing Directory Entries

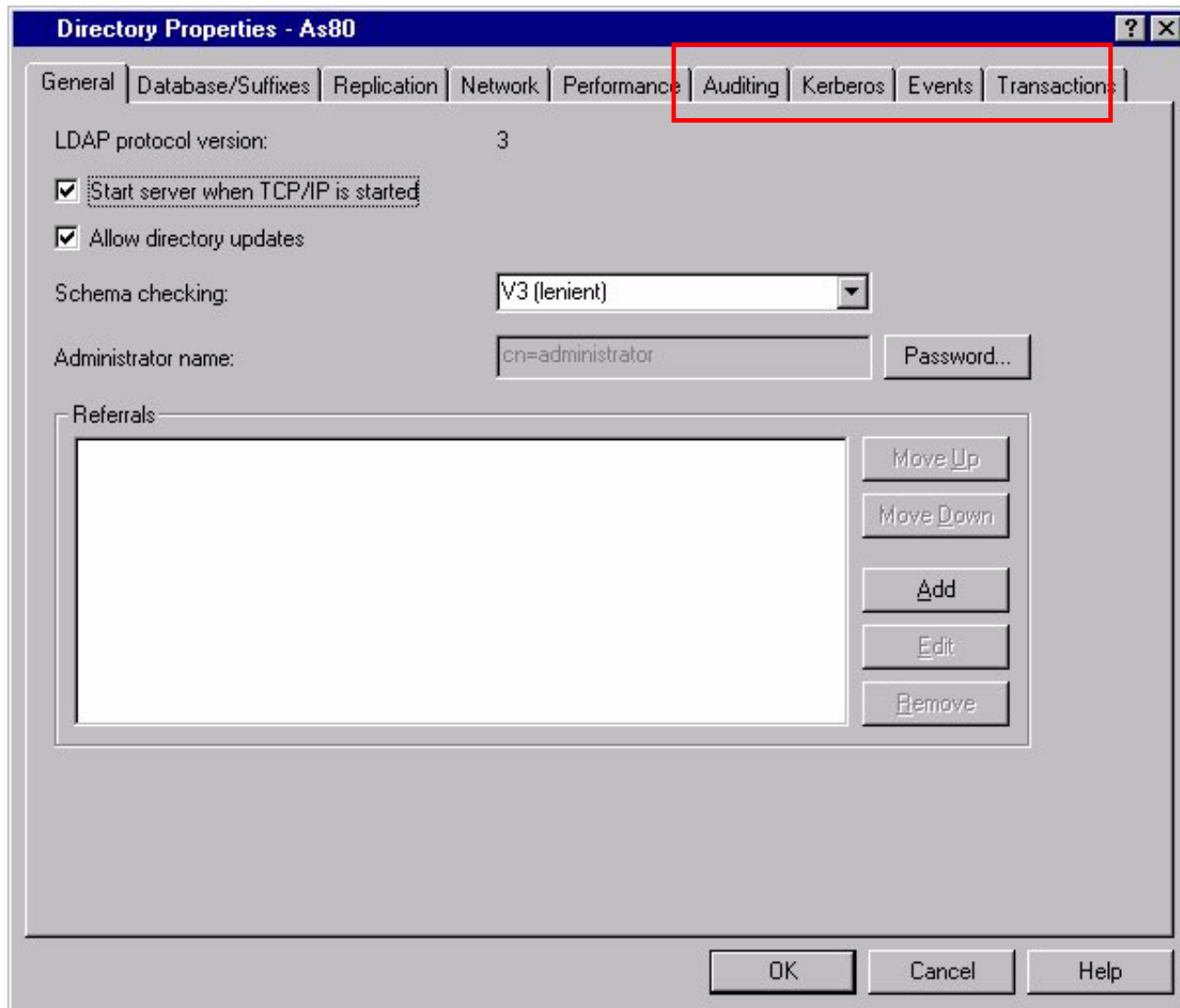
Once you have successfully connected to a Directory server, AS80 in this case, you get a tree of capabilities in the right pane.

In this example we browsed the directory. Since we had previously configured the Directory server to publish users and restarted it, the directory contains published users from the OS/400 System Distribution Directory. In this example we only have 4 users.

At the green arrow, you see, from the text, that the DMT tool supports editing the specific user we selected.

The next foils show specific V5R1 LDAP functional enhancements.

LDAP Properties Interface - General



Directory Properties - As80

General Database/Suffixes Replication Network Performance **Auditing** Kerberos Events Transactions

LDAP protocol version: 3

Start server when TCP/IP is started

Allow directory updates

Schema checking: V3 (lenient)

Administrator name: cn=administrator Password...

Referrals

Move Up

Move Down

Add

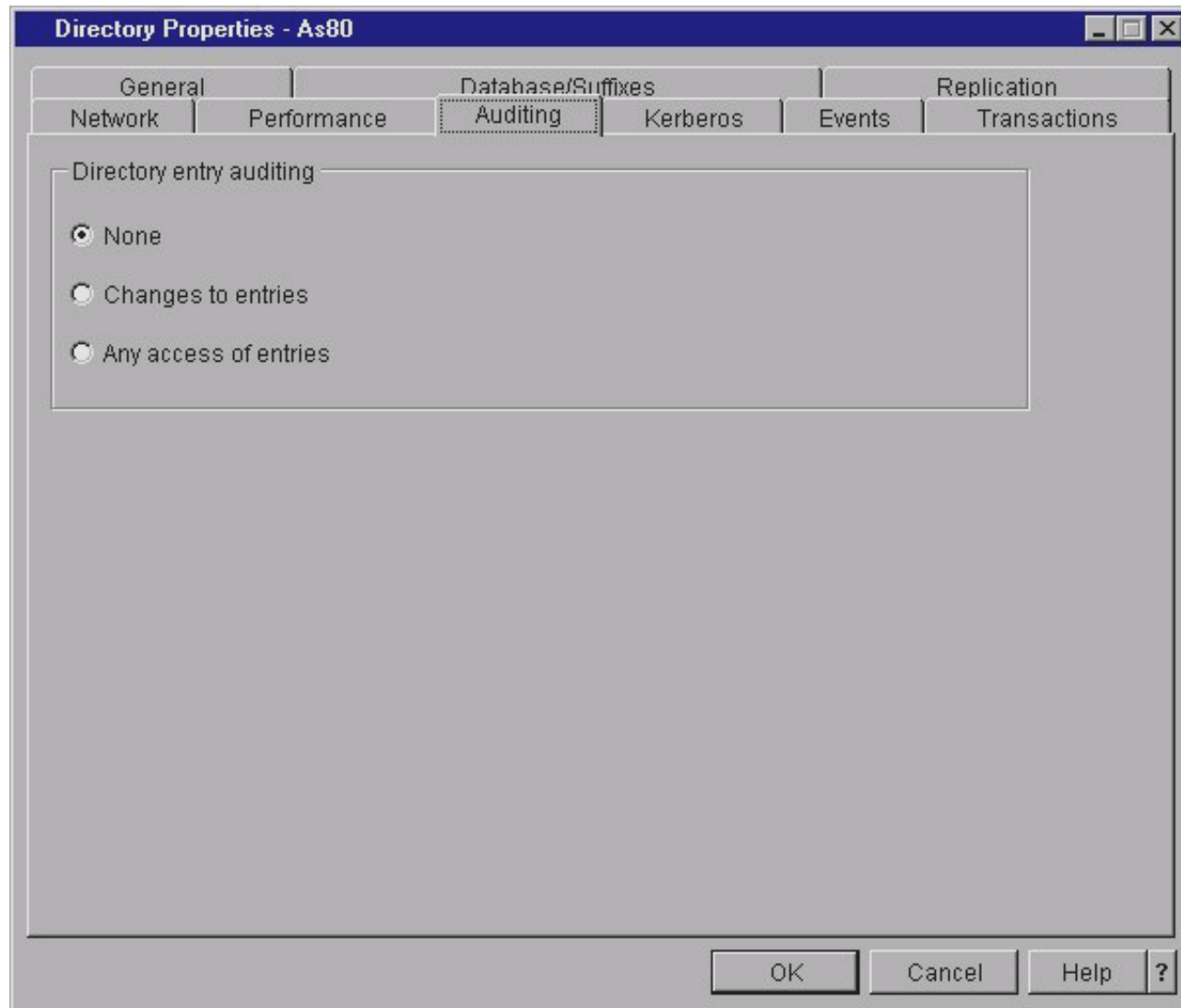
Edit

Remove

OK Cancel Help

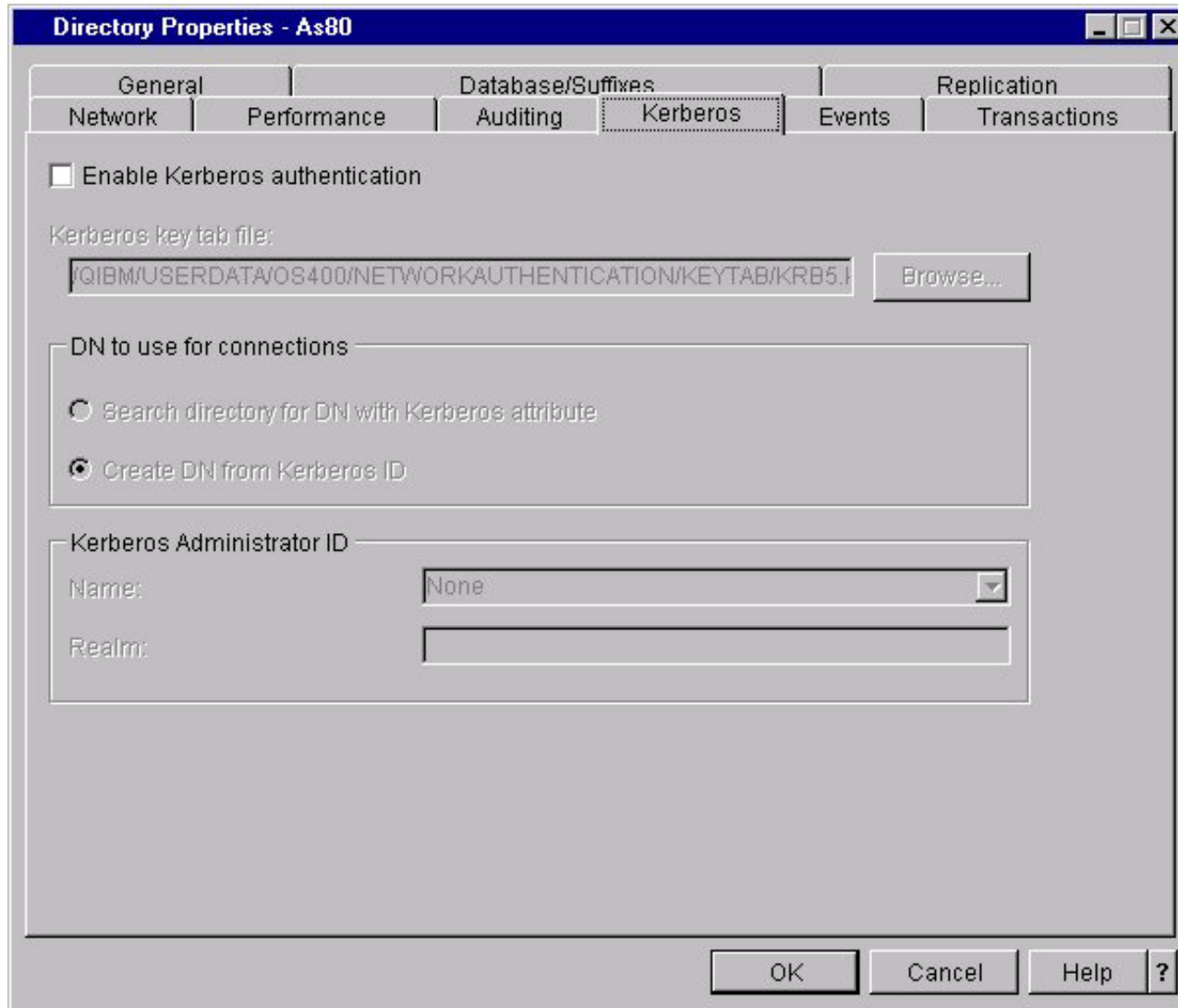


LDAP Properties Interface - Auditing



Security auditing can now be enabled for the LDAP server. When object auditing is enabled on OS/400, use the **Auditing** page from the properties for **Directory** panel to specify what information about directory entry actions are audited by OS/400. You can audit 'changes to entries' or 'Any access of entries'. The value specified on this page is only used when object auditing is enabled on OS/400 (QAUDccc system values). Auditing logs events so that you can review them later.

LDAP Properties Interface - Kerberos



The screenshot shows a window titled "Directory Properties - As80" with several tabs: General, Database/Suffixes, Replication, Network, Performance, Auditing, Kerberos (selected), Events, and Transactions. The Kerberos tab contains the following elements:

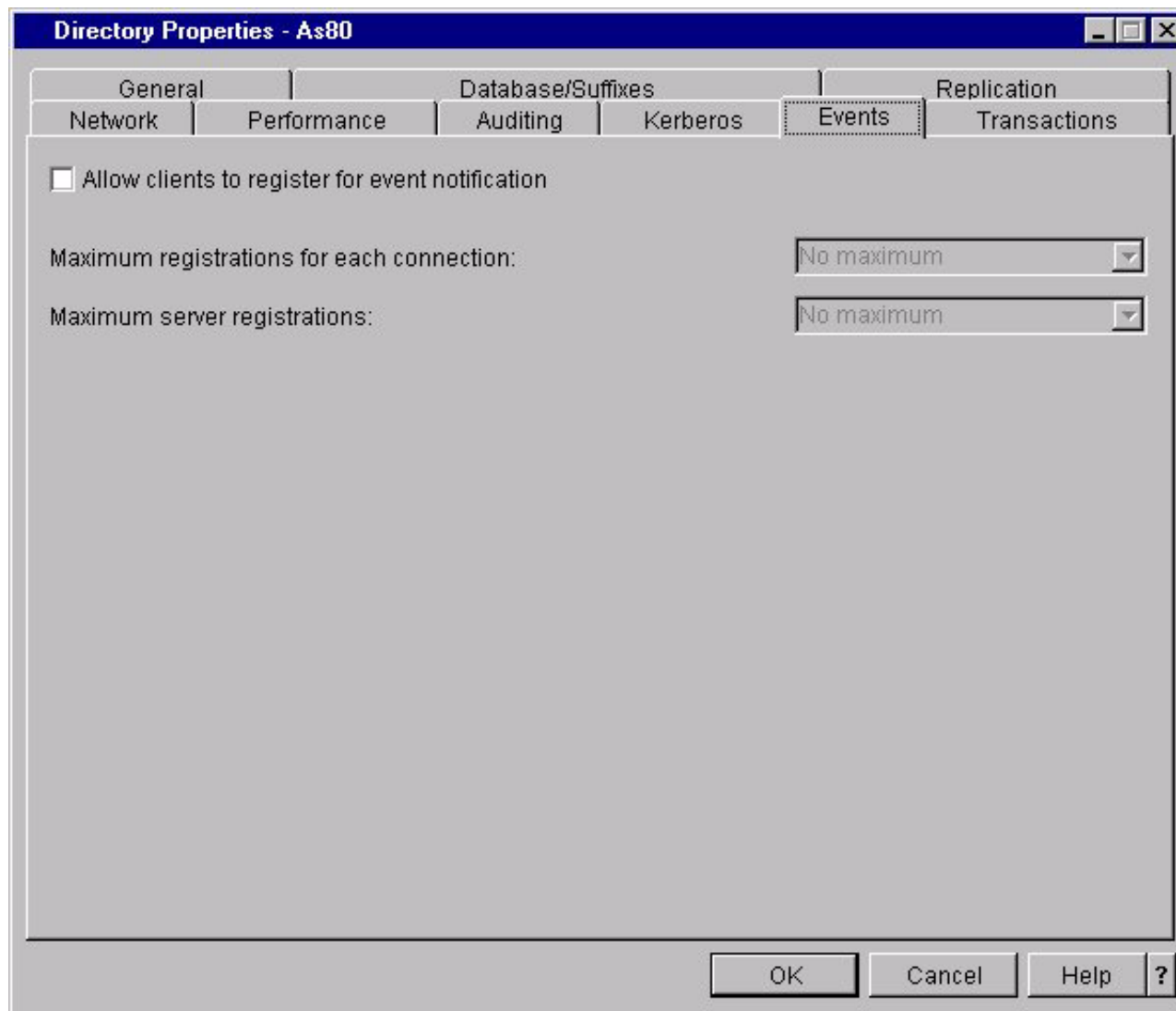
- Enable Kerberos authentication
- Kerberos key tab file:
- DN to use for connections:
 Search directory for DN with Kerberos attribute
 Create DN from Kerberos ID
- Kerberos Administrator ID:
Name:
Realm:

At the bottom of the window are buttons for OK, Cancel, Help, and a question mark icon.

Use the new **Kerberos** page to specify settings that enable your LDAP directory server to use Kerberos authentication. Kerberos is a network authentication protocol that uses secret key cryptography to provide strong authentication to client/server applications. To enable Kerberos authentication, you must have one of the Cryptographic Service Provider products (5722AC2 or 5722AC3) installed on your AS/400. You must also have a default Kerberos realm specified in the system's Kerberos configuration file.

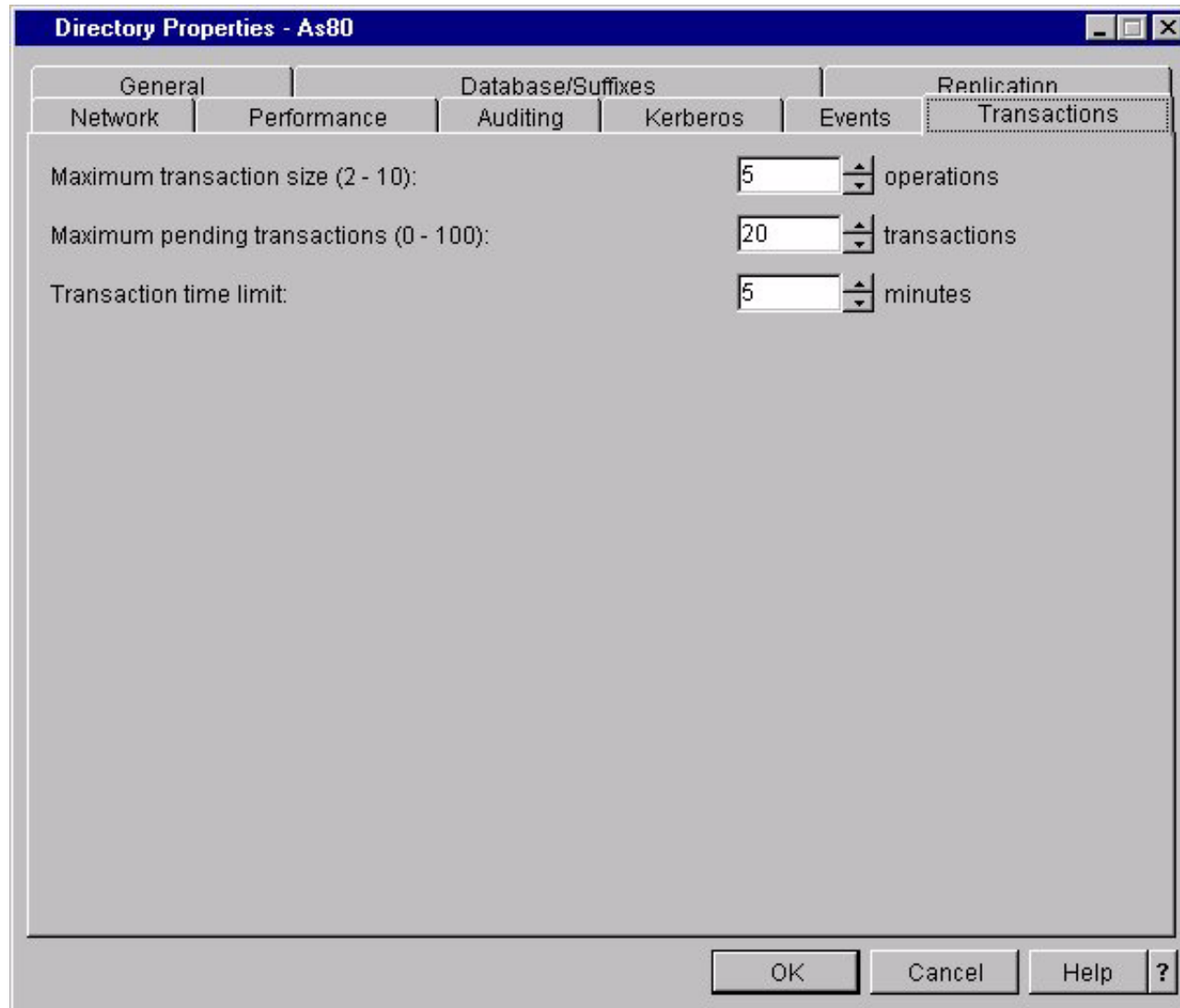
When the OS/400 directory server uses Kerberos authentication, the Kerberos principal name used by the server is in the form *service-name/host-name@realm*, where the service name is LDAP, the host name is the fully qualified TCP/IP name of the system, and the realm is the default realm that is specified in the system's Kerberos configuration. For example, if a system in the *acme.com* TCP/IP domain was named *my-as400* and had a default Kerberos realm of *ACME.COM*, the LDAP server Kerberos principal name would be *LDAP/my-as400.acme.com@ACME.COM*.

LDAP Properties Interface - Events



Use the **Events** page to specify settings for LDAP client event notification. Event notification allows clients to register with the LDAP directory server to be notified when a specified event, such as something being added to the directory, occurs. If event notification is enabled, a client can register to receive event notifications for the length of a single client connection, or until the client unregisters its request.

LDAP Properties Interface - Transactions



Use the **Transactions** page to specify settings for sets of operations that LDAP clients perform with the server. A transaction is a group of LDAP directory operations that are treated as one unit. The LDAP operations are not permanent until all operations in the transaction have completed successfully. If any of the operations fail, the other operations are undone. While a transaction is being processed, the directory server places all other operations on hold. Therefore, using large or frequent transactions from one client will impact the performance that other clients receive from the server.

The following LDAP operations may be part of a transaction:

- add
- modify
- RDN
- delete

PPP Enhancements

IBM @server. For the next generation of e-business.

PPP Enhancements

DHCP enablement for PPP

Multilink support

Remote Authentication Dial-in User Support (RADIUS)

GUI Interface changes

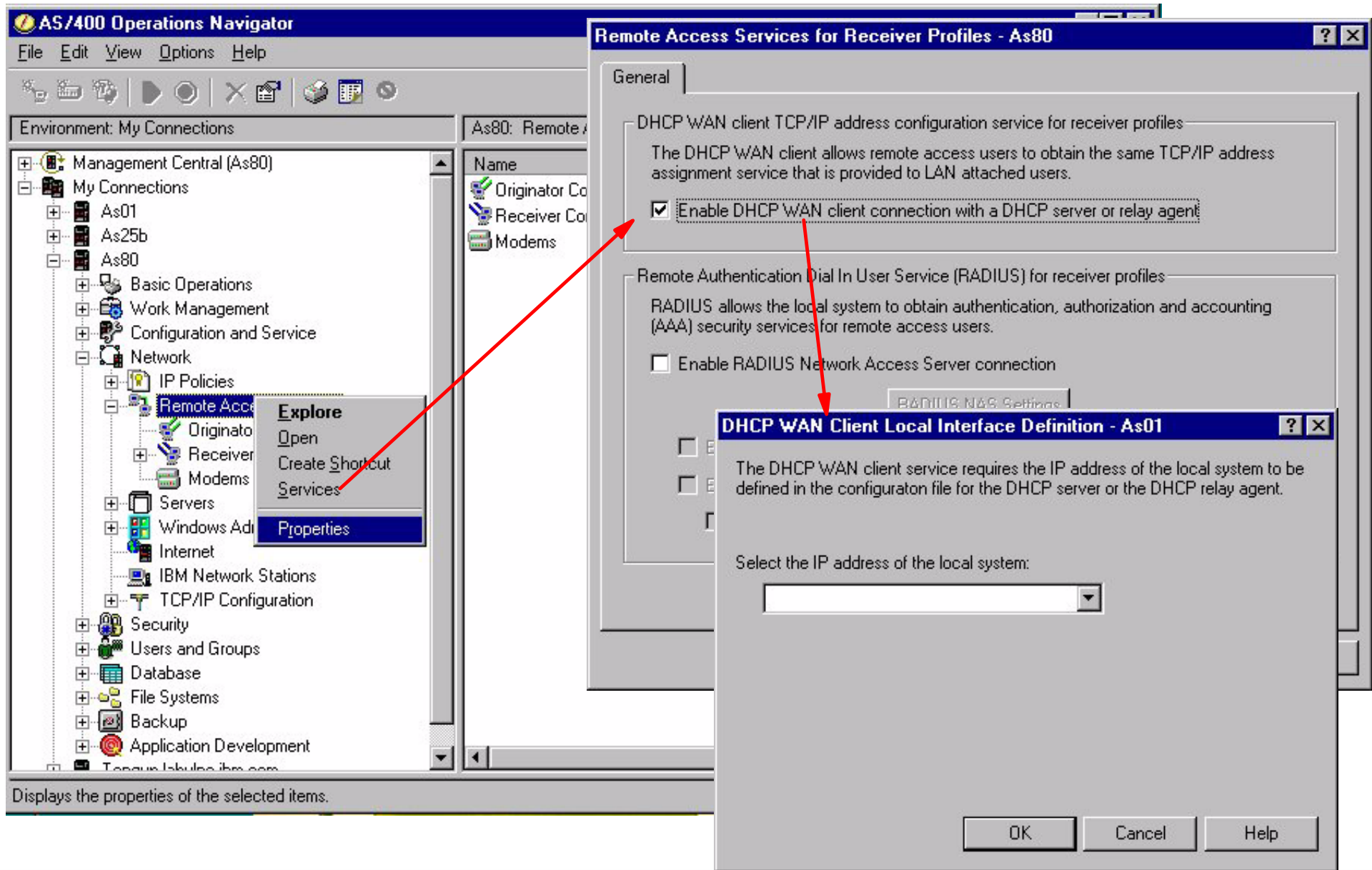
CL Commands and APIs

Group Access Policies

New documentation collection

SLIP support over asynchronous lines removed

DHCP Enablement for PPP



The screenshot displays the AS/400 Operations Navigator interface. On the left, the 'Management Central (As80)' tree is expanded to 'Remote Access Services'. A context menu is open over 'Remote Access Services', with 'Properties' selected. A red arrow points from this menu to the 'Remote Access Services for Receiver Profiles - As80' dialog box. In this dialog, the 'General' tab is active, and the checkbox 'Enable DHCP WAN client connection with a DHCP server or relay agent' is checked. A second red arrow points from this checkbox to a smaller dialog box titled 'DHCP WAN Client Local Interface Definition - As01'. This dialog prompts the user to 'Select the IP address of the local system:' and features a text input field. The 'OK', 'Cancel', and 'Help' buttons are visible at the bottom of the dialog.

Notes: DHCP Enablement for PPP

The iSeries server will now act as a DHCP WAN Client for remote access dial-in and L2TP tunnel users. This will enable wide area network remote access users to obtain the same IP address services as do LAN attached network DHCP clients. The DHCP WAN client will send its request to either a DHCP server or DHCP relay agent.

The Remote Access Services folder will provide a property sheet with a selection for enabling DHCP WAN client. When the DHCP WAN client is enabled, a dialog box will be launched requesting the user to specify the IP address (es) of the local interface (s) to be used to connect to the DHCP server or relay agent. If it is detected that neither DHCP server or relay agent are running, the GUI code will launch a dialog box to configure the relay agent.

The PPP profile can now be set to use DHCP. **TCP/IP Settings** tab is selected. The Remote IP address can then be selected. By selecting the pull down box, the DHCP option will be available for selection.

Point-to-Point Multilink Support

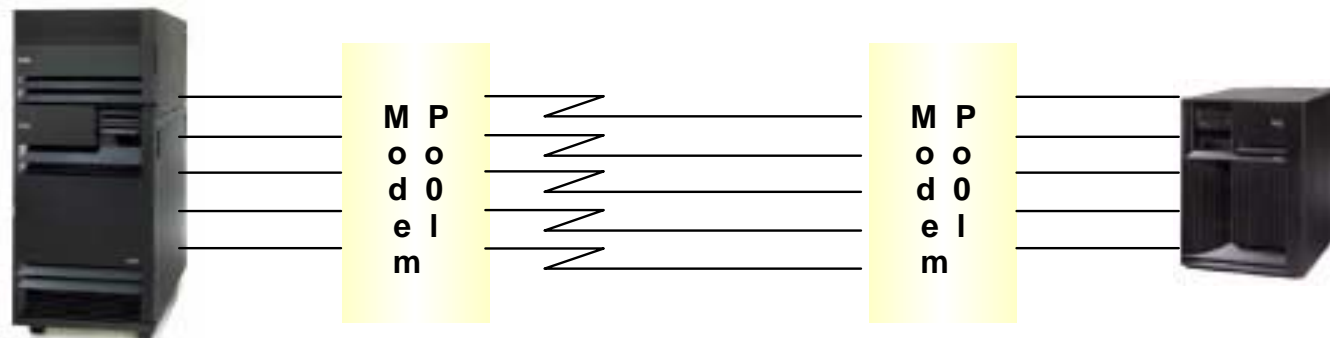
Increased reliability

Increased bandwidth

Allocation Protocol (BAP) and Bandwidth Allocation Control Protocol (BACP)

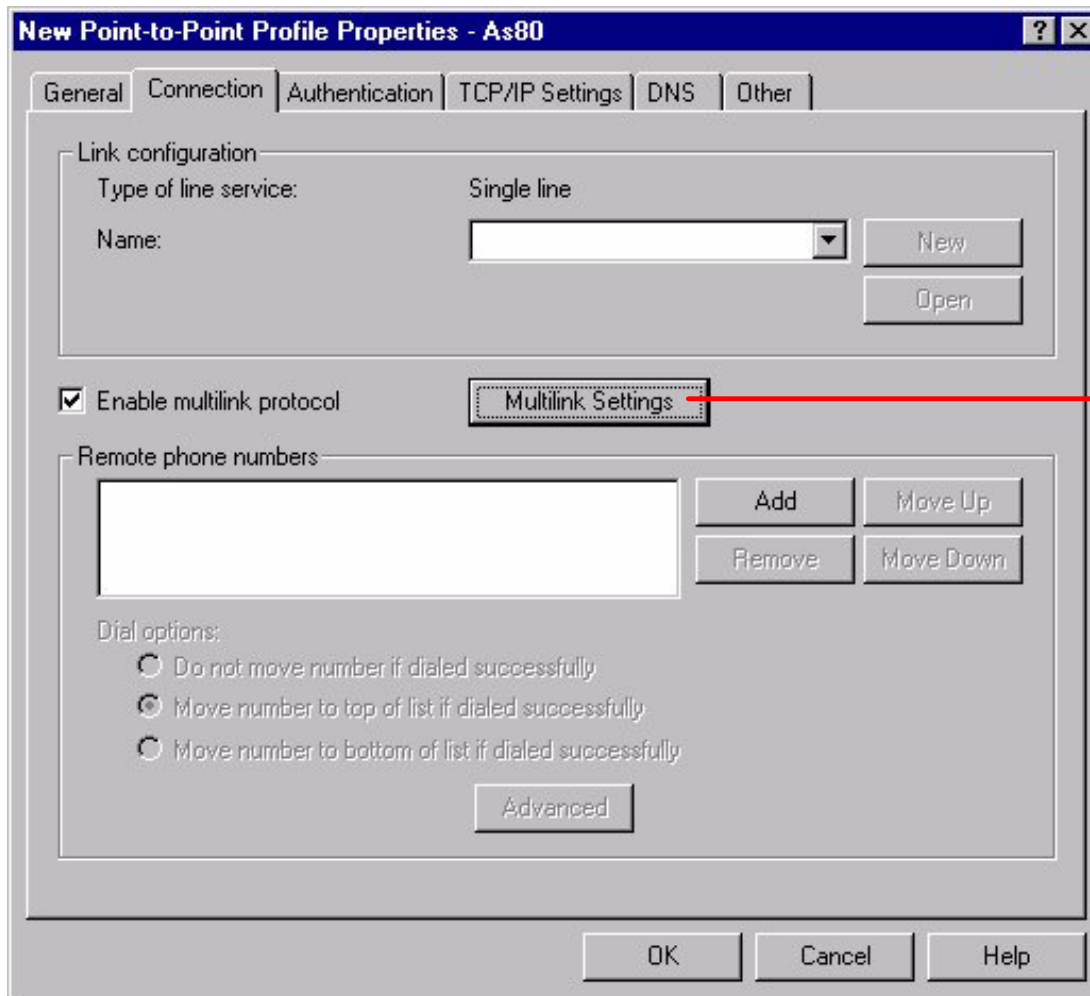
Bandwidth Utilization Monitoring

Works with Originator and Receiver Profiles



IBM  server. For the next generation of e-business.

Multilink Configuration



New Point-to-Point Profile Properties - As80

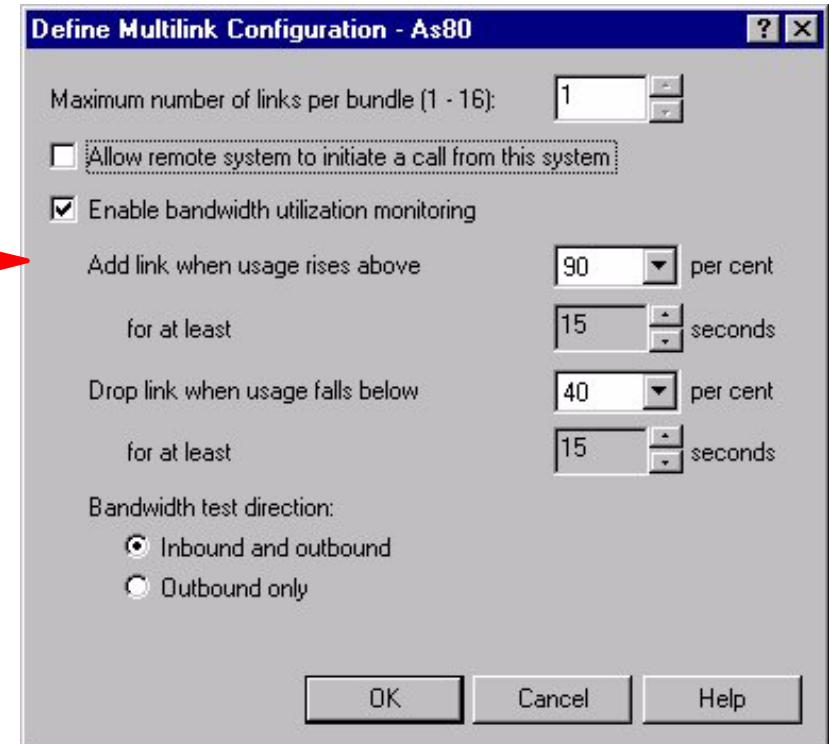
General | **Connection** | Authentication | TCP/IP Settings | DNS | Other

Link configuration
Type of line service: Single line
Name:

Enable multilink protocol

Remote phone numbers

Dial options:
 Do not move number if dialed successfully
 Move number to top of list if dialed successfully
 Move number to bottom of list if dialed successfully



Define Multilink Configuration - As80

Maximum number of links per bundle (1 - 16):

Allow remote system to initiate a call from this system

Enable bandwidth utilization monitoring

Add link when usage rises above per cent
for at least seconds

Drop link when usage falls below per cent
for at least seconds

Bandwidth test direction:
 Inbound and outbound
 Outbound only

The PPP Multilink Protocol (MP) is described in RFC 1990. MP is a method for splitting, recombining and sequencing datagrams across multiple logical data links. It allows multiple PPP links to be grouped together to form a single virtual link or bundle. This method is similar to the multilink protocol described in ISO 7776, but offers the additional ability to split and recombine packets, thereby reducing latency, and potentially increase the effective maximum receive unit (MRU). Furthermore, there is no requirement here for acknowledged-mode operation on the link layer, although that is optionally permitted. Multilink is based on an Link Control Protocol (LCP) option negotiation that permits a system to indicate to its peer that it is capable of combining multiple physical links into a "bundle".

Multilink is negotiated during the initial LCP option negotiation. A system indicates to its peer that it is willing to do multilink by sending the multilink option as part of the initial LCP option negotiation. This negotiation indicates three things:

- The system offering the option is capable of combining multiple physical links into one logical link.
- The system is capable of receiving upper layer protocol data units (PDU) fragmented using the multilink header and reassembling the fragments back into the original PDU for processing.
- The system is capable of receiving PDUs of size N bytes where N is specified as part of the option even if N is larger than the maximum receive unit (MRU) for a single physical link.

If a switched line connection is utilized, the PPP connection could be configured to use multiple links for one connection. MP can be implemented with both Originator and Receiver Connection Profiles. The benefits of MP include:

- Reducing the latency of data sent between systems by increasing the total effective bandwidth.
- Increased reliability through the use of multiple lines. If a line fails, the link is maintained as long as one line in the MP bundle remains operational.
- The ability to dynamically add and remove lines from a bundle allows bandwidth to be supplied as needed, making more efficient use of the bandwidth available.

PPP multilink support needs a method to manage the dynamic bandwidth allocation. This is achieved by implementing the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle. BAP defines datagrams to coordinate adding and removing individual links in a multilink bundle, as well as specifying which peer is responsible for which decisions regarding managing bandwidth during a multilink connection.

In order to realize the benefits of changing the bandwidth depending upon the demand, at least one peer must be capable of monitoring the utilization of total bandwidth currently available in a MP bundle. This is called Bandwidth Utilization Monitoring (BUM). Links may be added or removed from a bundle as needed. The iSeries supports BUM for Originator Profiles, but not Receiver profiles.

As can be seen in the figure to the right, links can be added and removed depending upon the utilization. The utilization is set as a percentage. There is also a parameter (Allow remote system to initiate a call from this system) which allows the remote system to request the iSeries to initiate another connection to the remote system. A person may not want to check this in order that their system may control when an additional link is added.

Further details on Multilink support and BAP is beyond the scope of this document.

Remote Authentication Dial-In User Service

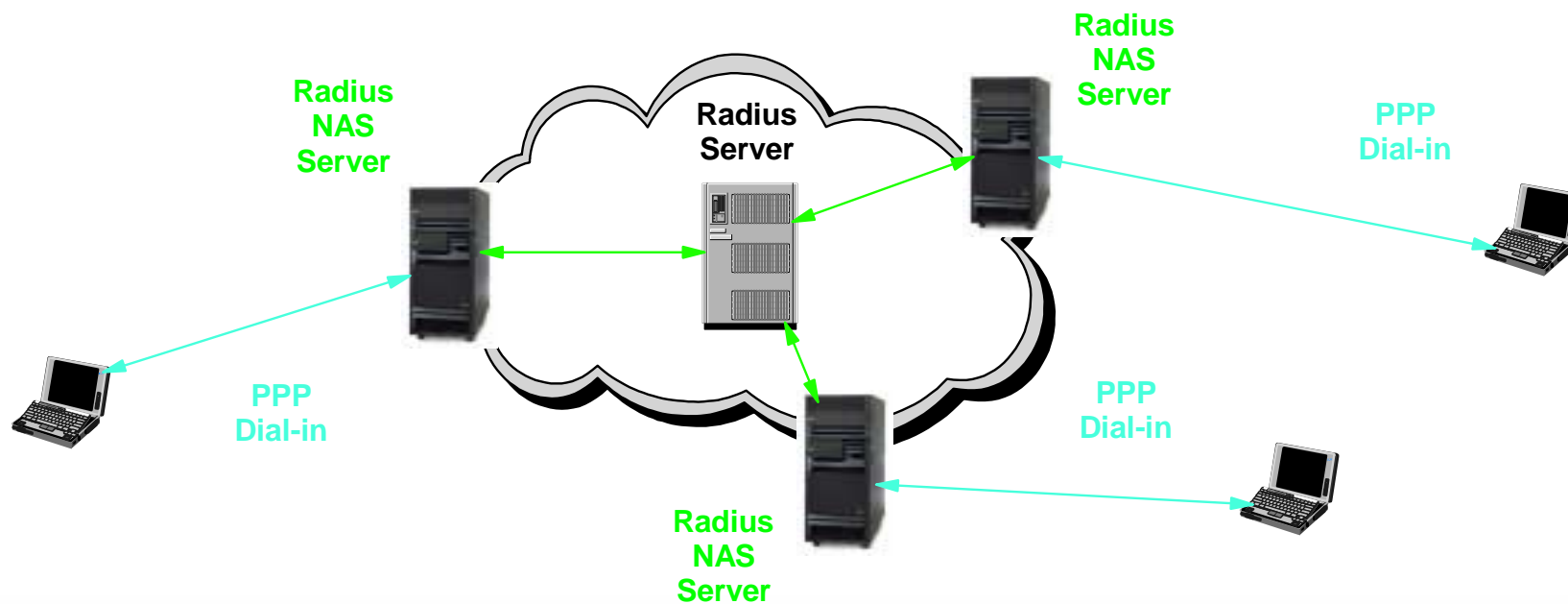
IBM  server iSeries

Single focal point for access management

RADIUS is the widely used standard in the industry for user authentication, authorization, and accounting

Centralizes secure access for remote clients (Point-to-Point)

iSeries is capable of being a Network Access Server (NAS)



IBM  server. For the next generation of e-business.

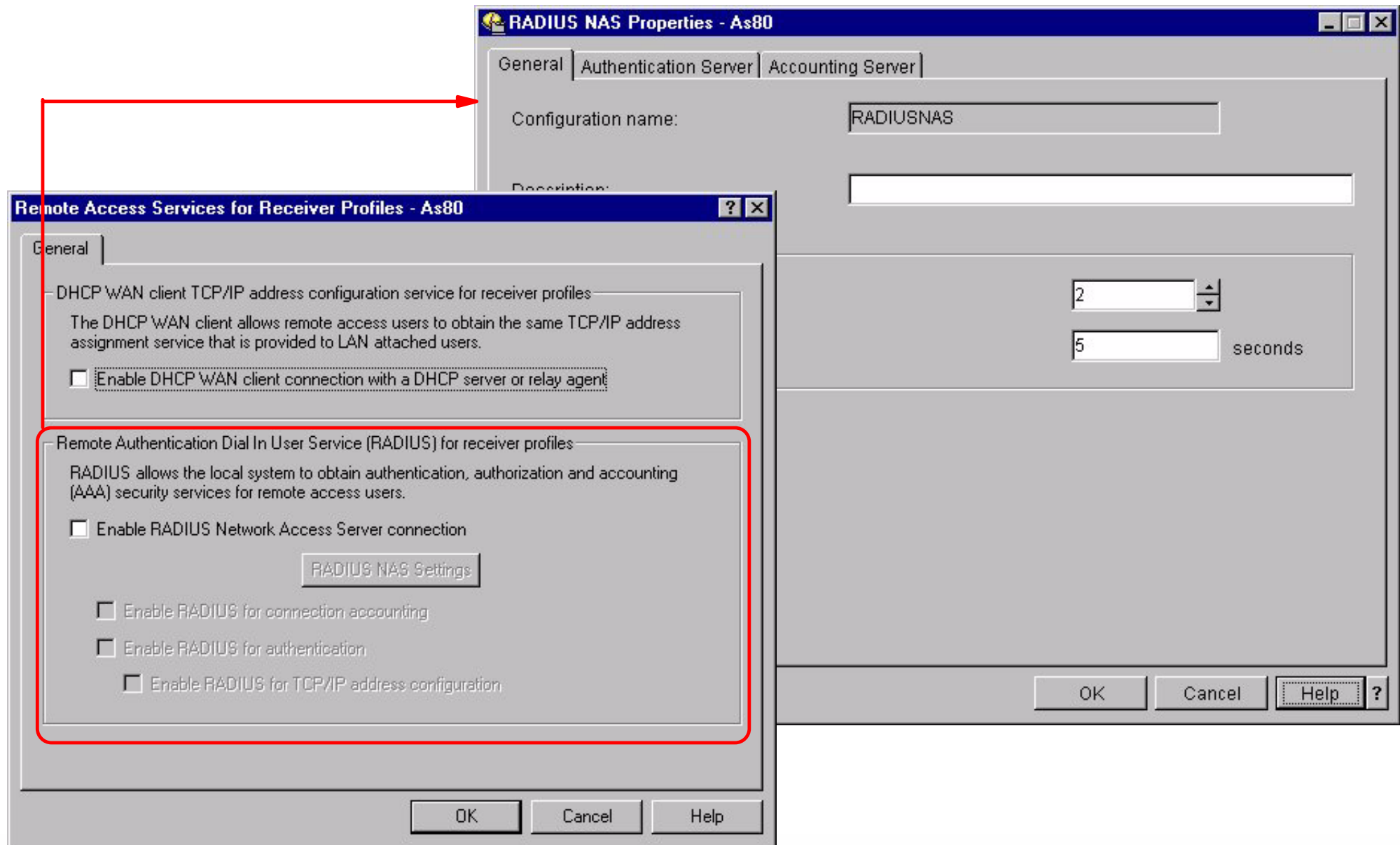
Remote Authentication Dial-In service (RADIUS) is a distributed security system developed by Lucent Technologies InterNetworking Systems. RADIUS was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. RADIUS is the de facto industry standard for user authentication, authorization, and accounting.

Radius has three main functions:

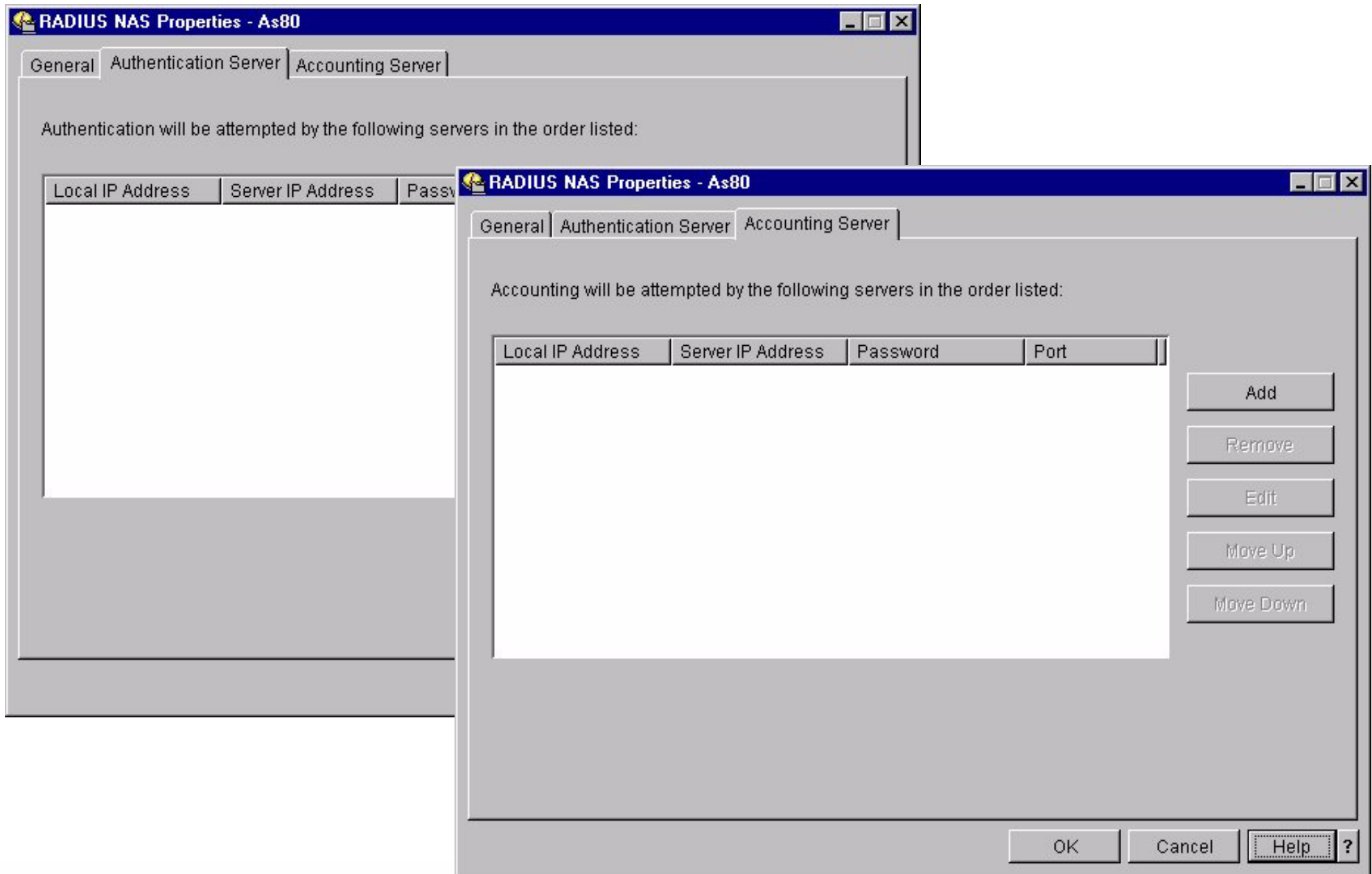
- Authentication - RADIUS server will authenticate users for dial-in remote access. (It can distribute IP addresses to clients)
- Authorization - the RADIUS server can be configured to control access to specific services on the network for an authenticated user. Such services are routes, time-outs and port limits.
- Accounting - RADIUS server accounting permits system administrators to track dial-in use. This is often used for billing purposes.

The RADIUS server is installed on a central computer at the customer's site. The RADIUS Network Access Server (NAS) can be installed on the iSeries. The NAS is responsible for passing user information designated for the RADIUS servers and then acting on the response which is returned.

Enabling Radius



Enabling RADIUS



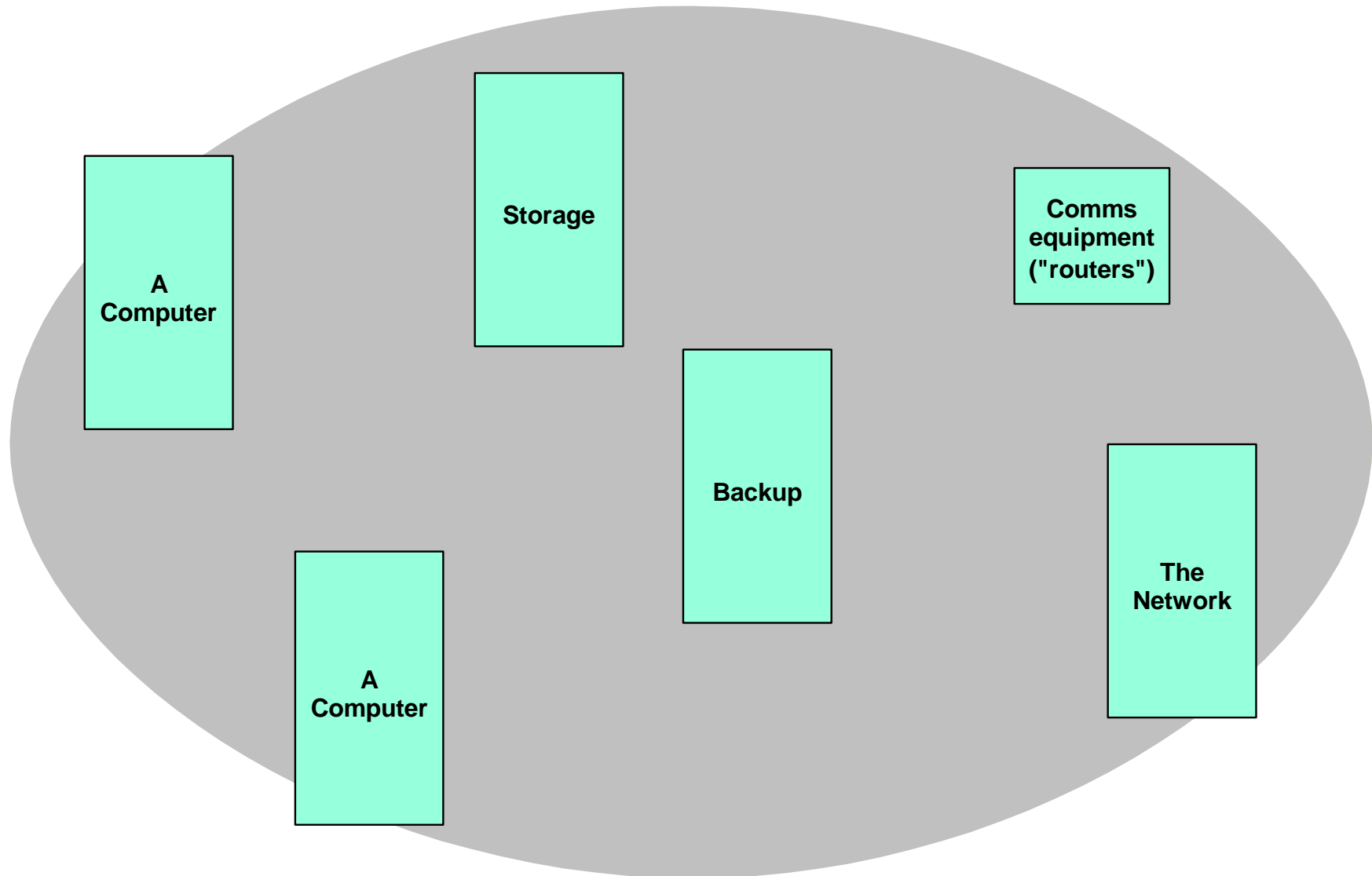
Remote Access Services must be enabled for RADIUS in order for PPP and L2TP. You have the option of enabling some or all of the RADIUS functions. If the RADIUS NAS server has not been configured, a configuration wizard will be initiated when Enable RADIUS Network Access Server connection is selected. Separate RADIUS servers can be used for authentication and accounting. The following is required when setting up the configuration:

- Local IP address
- Server IP address (RADIUS server)
- Password (shared secret)
- Port number - This is the port under which the RADIUS server listens to authentication or accounting requests initiated from a NAS server. When RADIUS was first introduced in the market, servers listened on UDP port 1645 for authentication and 1646 for accounting requests. Newer implementations default to UDP port 1812 for authentication and 1813 for accounting requests. Always refer to the RADIUS server user's guide or help text to determine which ports this server listens for RADIUS NAS requests.

Quality of Service

IBM @server. For the next generation of e-business.

Service Delivery Components



IBM  server. For the next generation of e-business.

Notes: Service Delivery Components

Any organization that delivers IT services to end users implements practices to meet the required service level. These practices rely on the characteristics of the implementation and operation facilities of the components within the service delivery infrastructure. For instance, the availability of the service delivered to company executives can be enhanced by creating and maintaining business copies of production data, which copies might be used for analysis purposes without disturbing the transactional work that creates and updates the source of the business copy, or one might use certain Enterprise Storage solutions to increase the resiliency of data repositories. Tools might be used to, for instance, monitor the performance and throughput of computer systems or parts thereof, in order to maintain a predefined and guaranteed response time.

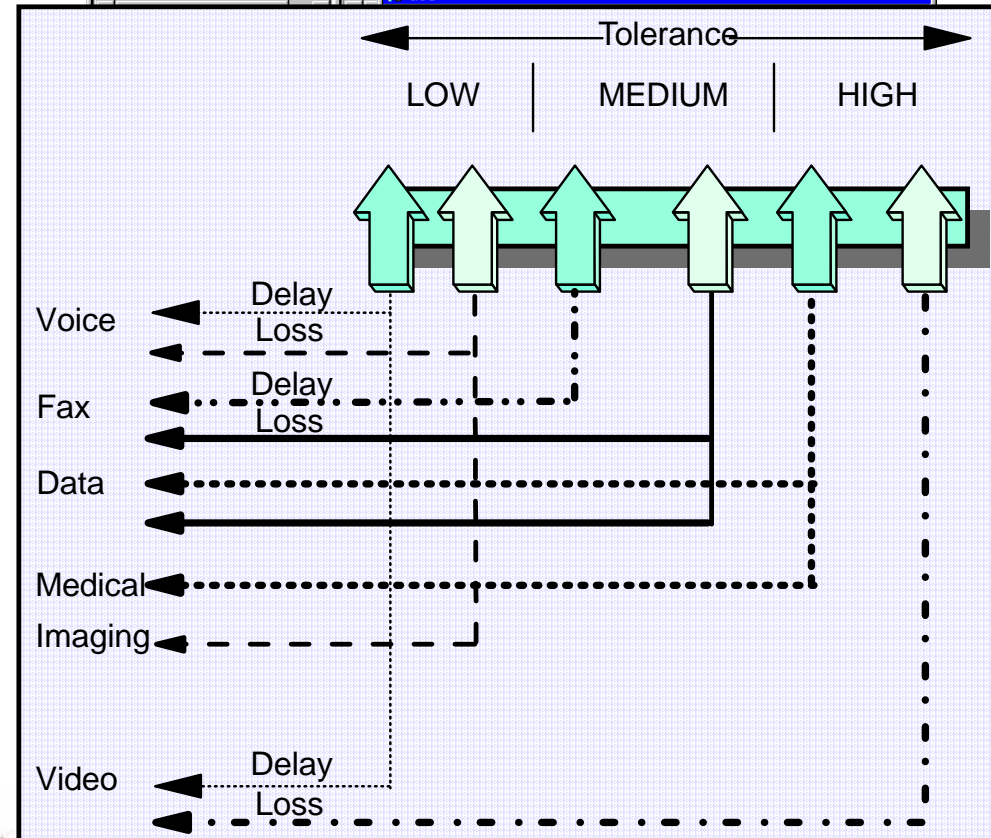
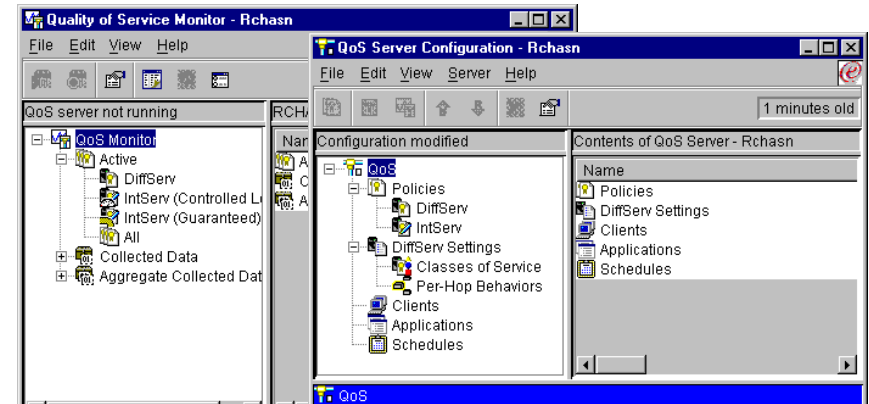
The network that connects the end user with the IT service delivery center(s) has its own characteristics for performance delivery. The usage of the available bandwidth and the routes however cannot always be predicted or adapted, since the currently used applications mostly run over a TCP/IP network, which is by nature a connection-less protocol that does not consider fixed routes over well known nodes such as SNA did.

However, the specifications for TCP/IP allow defining settings for obtaining certain levels of service delivery over a network, which uses different active components. Implementing the protocols that allows to define and/or reserve resources so that traffic can be differentiated

TCP/IP Quality of Service

What is QoS?

- A collection of functions that allows specific TCP/IP traffic to have certain priority or bandwidth across the network
- Important in multi-workload environments
- Mission critical applications can be given higher priority
- MQoS "aware" router required for best performance
- Two QoS algorithms supported:
 - Integrated Services
 - Differentiated Services



In V5R1, OS/400 provides the ability to control and manage TCP/IP traffic in the network and take advantage of the leading-edge networking Quality of Service (QoS) functions contained in routers and switches. The iSeries QoS functions for managing TCP/IP traffic provide the ability to drop, mark, and shape TCP/IP traffic based on the QoS policy being applied. In addition, QoS admission control capability is provided for controlling bandwidth management requests. Support is provided for both integrated and differentiated services. Applications can either be written to use QoS APIs, or they can simply use QoS policies without making application changes. QoS can be monitored and policies maintained using Operations Navigator. APIs are also provided for network devices to monitor iSeries QoS functions.

Quality of Service (QoS) is a collection of functions that allow the user to define what kind of network priority or bandwidth to assign to a TCP/IP application program. As intranets and the Internet fill with more traffic, QoS provides a means for prioritizing system traffic. This will become a key factor in the success of e-business systems. QoS will be a key ingredient in the multi-load environment which is typical for the iSeries servers. The chart on the previous page illustrates how different types of data require different priorities. In the past, packets requesting information on sports scores received the same priority as a mission critical business application. With QoS, you can give that mission critical application the differentiation it needs.

QoS will be desired by users who are running mission critical applications. For Application Service Providers (ASP) and Business to Business (B2B), QoS will allow them to provide predictable e-business service. This is often a requirement of a Service Level Agreement. QoS, combined with Virtual Private Network (VPN), provides guaranteed security and predictable e-business flows.

QoS occurs across the network. QoS enabled routers are required to provide the requested bandwidth. If there are routers in the path that are not QoS enabled, the desired performance may not be obtained.

Note: The iSeries server is not a QoS aware IP router in V5R1 (or earlier). The iSeries server role in QoS, instead, is at the end points (the client or server) of the application.

QoS requires complex set up; the V5R1 Operations Navigator interface can assist in this area. The next foils give a somewhat detailed description of the 2 QoS protocols supported with V5R1. The objective is to give an indication of the differences in the two protocols.

Quality of Service (QoS) is a collection of functions that will allow the user to define what kind of network priority or bandwidth to assign to a TCP/IP application program. As intranets and the internet fill with more traffic, QoS will provide a means for prioritizing system traffic. This is a key to the success of e-business systems as being the ingredient in the multi-load environment which is typical for the iSeries servers. In the past, packets requesting information on sports scores received the same priority as a mission critical business application. With QoS, you can give that mission critical application the differentiation it needs. QoS will be desired by those who are running mission critical applications. For Application Service Providers (ASP) and Business to Business (B2B), it will allow them to provide predictable e-business service. This is many times a requirement of a Service Level Agreement. QoS combined with Virtual Private Network (VPN) provide guaranteed security and predictable e-business flows.

Routing deployed in today's Internet is focused on connectivity and typically supports only one type of datagram service called "best effort". The default service offering associated with the Internet is characterized as a best-effort variable service response. Current Internet routing protocols, e.g. OSPF, RIP, use "shortest path routing", i.e. routing that is optimized for a single arbitrary metric, administrative weight or hop count. These routing protocols are also "opportunistic," using the current shortest path or route to a destination. Alternate paths with acceptable but non-optimal cost can not be used to route traffic (shortest path routing protocols do allow a router to alternate among several equal cost paths to a destination).

QoS-based routing extends the current routing paradigm in three basic ways.

First, to support traffic using integrated-services class of services, multiple paths between node pairs are calculated. Some of these classes of service require the distribution of additional routing metrics, e.g. delay, and available bandwidth. If any of these metrics change frequently, routing updates can become more frequent thereby consuming network bandwidth and router CPU cycles.

Second, today's opportunistic routing shifts traffic from one path to another as soon as a "better" path is found. The traffic will be shifted even if the existing path can meet the service requirements of the existing traffic. If routing calculation is tied to frequently changing consumable resources (e.g. available bandwidth) this change will happen more often and can introduce routing oscillations as traffic shifts back and forth between alternate paths. Furthermore, frequently changing routes can increase the variation in the delay and jitter experienced by the end users.

Third, today's optimal path routing algorithms do not support alternate routing. If the best existing path cannot admit a new flow, the associated traffic cannot be forwarded even if an adequate alternate path exists.

IBM  server. For the next generation of e-business.

Under QoS-based routing, paths for flows would be determined based on some knowledge of resource availability in the network, as well as the QoS requirement of flows. The main objectives of QoS-based routing are:

- Dynamic determination of feasible paths: QoS-based routing can determine a path, from among possibly many choices, that has a good chance of accommodating the QoS of the given flow. Feasible path selection may be subject to policy constraints, such as path cost, provider selection, etc.
- Optimization of resource usage: A network state-dependent QoS-based routing scheme can aid in the efficient utilization of network resources by improving the total network throughput. Such a routing scheme can be the basis for efficient network engineering.
- Graceful performance degradation: State-dependent routing can compensate for transient inadequacies in network engineering (e.g., during focused overload conditions), giving better throughput and a more graceful performance degradation as compared to a state-insensitive routing scheme.

QoS-based routing in the Internet, however, raises many issues:

- How do routers determine the QoS capability of each outgoing link and reserve link resources? Note that some of these links may be virtual, over ATM networks and others may be broadcast multi-access links.
- What is the granularity of routing decision (i.e., destination-based, source and destination-based, or flow-based)?
- What routing metrics are used and how are QoS-accommodating paths computed for unicast flows?
- How are QoS-accommodating paths computed for multicast flows with different reservation styles and receiver heterogeneity?
- What are the performance objectives while computing QoS-based paths?
- What are the administrative control issues?
- What factors affect the routing overheads?
- How is scalability achieved?

Integrated service

- Negotiated end-to-end and dedicated for duration of request
- Uses Resource Reservation Protocol (RSVP) and X/Open RSVP API
- Can dynamically change bandwidth
- Good for applications requiring dedicated quality of service

Differentiated service

- Traffic is classified, each class can be given different treatment
- Each class is best effort
- Use instead of the current Type of Service (TOS)
- Transparent to applications

At V5R1, the iSeries implements Quality of Service (QoS). The two methods of QoS that iSeries implements are Integrated Service and Differentiated Service. The following pages will go into further detail about each type.

Integrated Service

Framework to deliver the ability for applications to choose among multiple, controlled levels of delivery service for their data packets

Requires:

- Elements of the network must support mechanisms to control the quality of service
- Methods to communicate requirements of the application to the elements of the network

Several IETF RFCs define the framework and the components

Integrated Service will reserve bandwidth between the server and client. Resource Reservation Protocol (RSVP) is the Internet Engineering Task Force (IETF) standard for supporting end-to-end quality of service. RSVP provides a mechanism and the ability to reserve bandwidth for end-to-end IP traffic using signaling at every hop. X/Open RSVP API (RAPI) enables applications to use RSVP to request, reserve, and dynamically change bandwidth for end-to-end QoS.

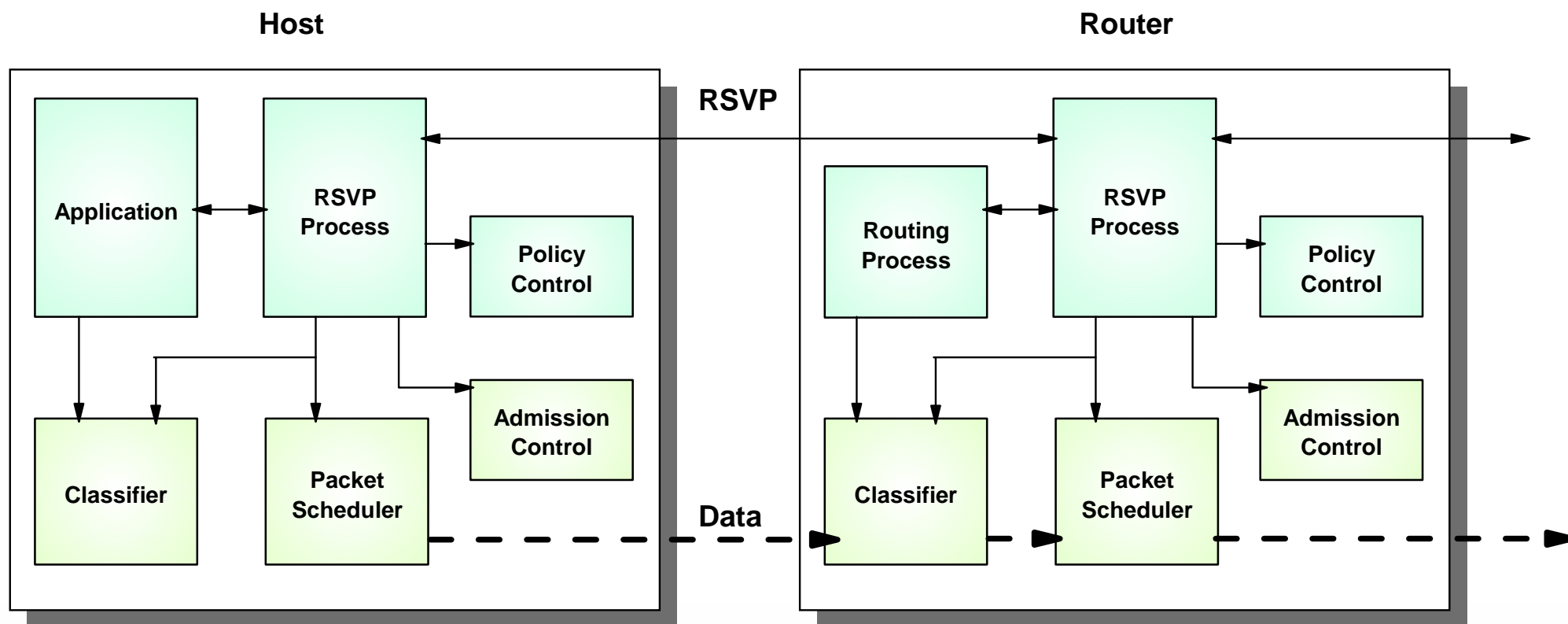
RSVP is explained in the next foils.

Resource Reservation Protocol (RSVP)

RSVP NOT a routing protocol; works on current and future unicast and multicast routing protocols

Protocol used to request specific quality of service from the network

RSVP requests resources in only one direction



RSVP is a resource reservation setup protocol designed for an integrated services Internet. The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path.

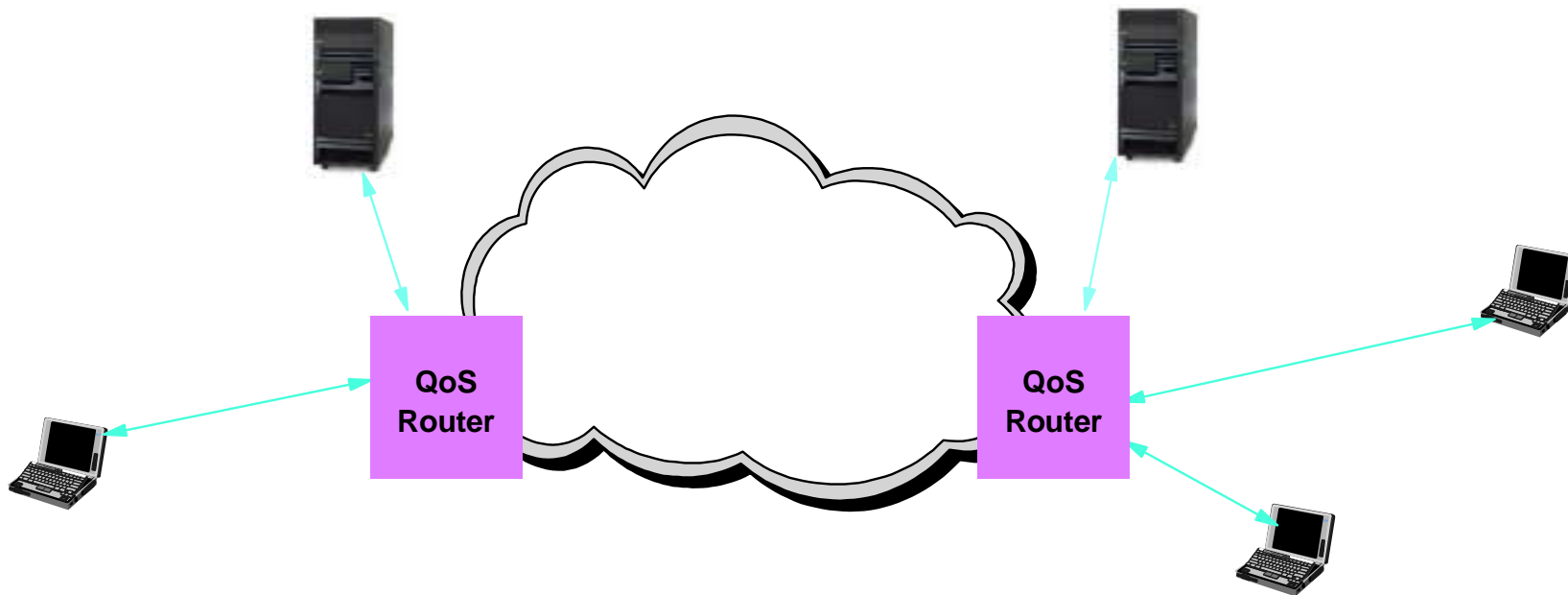
RSVP requests resources for simplex flows, i.e., it requests resources in only one direction. Therefore, RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver at the same time. RSVP operates on top of IPv4 or IPv6, occupying the place of a transport protocol in the protocol stack. However, RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. Like the implementations of routing and management protocols, an implementation of RSVP will typically execute in the background, not in the data forwarding path.

RSVP is not itself a routing protocol; RSVP is designed to operate with current and future unicast and multicast routing protocols. An RSVP process consults the local routing database(s) to obtain routes. In the multicast case, for example, a host sends IGMP messages to join a multicast group and then sends RSVP messages to reserve resources along the delivery path(s) of that group. Routing protocols determine where packets get forwarded; RSVP is only concerned with the QoS of those packets that are forwarded in accordance with routing.

In order to efficiently accommodate large groups, dynamic group membership, and heterogeneous receiver requirements, RSVP makes receivers responsible for requesting a specific QoS. A QoS request from a receiver host application is passed to the local RSVP process. The RSVP protocol then carries the request to all the nodes (routers and hosts) along the reverse data path(s) to the data source(s), but only as far as the router where the receiver's data path joins the multicast distribution tree. As a result, RSVP's reservation overhead is in general logarithmic rather than linear in the number of receivers.

Differentiated Service

Easy to Implement



Use bits in IP header to identify packet's level of service

Packets can be marked at source or other part of the network

Does not require end-to-end signaling

Does require router and switches that are Differentiated Services enabled

Differentiated services enhancements to the Internet protocol are intended to enable scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop. A variety of services may be built from a small, well-defined set of building blocks which are deployed in network nodes. The services may be either end-to-end or intra-domain; they include both those that can satisfy quantitative performance requirements (e.g., peak bandwidth) and those based on relative performance (e.g., "class" differentiation). Services can be constructed by a combination of:

- Setting bits in an IP header field at network boundaries (autonomous system boundaries, internal administrative boundaries, or hosts).
- Using those bits to determine how packets are forwarded by the nodes inside the network.
- Conditioning the marked packets at network boundaries in accordance with the requirements or rules of each service.

Differentiated Services in V5R1 use classes to determine what type of per-hop treatment the traffic should be given. The Classes are built by using the *Per-Hop Behavior* (PHB). The per-hop behavior is a description of a forwarding treatment for IP packets; it addresses a set of parameters inside a router that networks use to control how packets are scheduled, dropped, and queued. A network must be capable of handling differentiated services to uphold these per-hop behaviors. IP packets have an IP header which contains *codepoint* information. This codepoint information tells the routers how to treat the assigned IP packets. PHBs may be specified in terms of their resource (e.g., buffer, bandwidth) priority relative to other PHBs, or in terms of their relative observable traffic characteristics (e.g., delay, loss). The PHB describe what kind of delay/thruput/loss characteristics are desired for the packet of data. The *Type of Service* (TOS) bits in the IP header are used to support the Differentiated Service Classes of service. The first six bits are used and are referred to as *Differentiated Services Codepoint* (DSCP).

The pre-V5R1 TOS support can be used instead of QoS and will be used for route selection only. When QoS is used the same TOS bits in the IP header are used. Therefore either TOS or QoS, not both may be used. When the data is sent, the TOS field will be looked at by the router to determine what kind of service is desired. The router will then attempt to provide the service on a best effort basis.

The Classes currently do not have specific bandwidth values assigned to them. Therefore, it will be necessary for the customer and the service provider of the routers to agree upon what bandwidth corresponds to a class. Routers and switches that are Differentiated Services enabled are required in order to take full advantage of Differentiated Service. Non-Differentiated Service routers would only be able to process the first 3 bits of TOS field as TOS. The first 3 TOS bits relate to precedence and match up with the DSCP Class Selector codepoints. An advantage of the Differentiated Service over the Integrated Service is that the Differentiated Service is less router intensive. The Integrated Service requires more of the routers processor time.

Note: Routers must be configured to use the "same bits" to mean the "same thing." Otherwise there will be disruption in the correct use of QoS within the network.

The table on the next page shows the recommended values for DSCP (the first six bits).

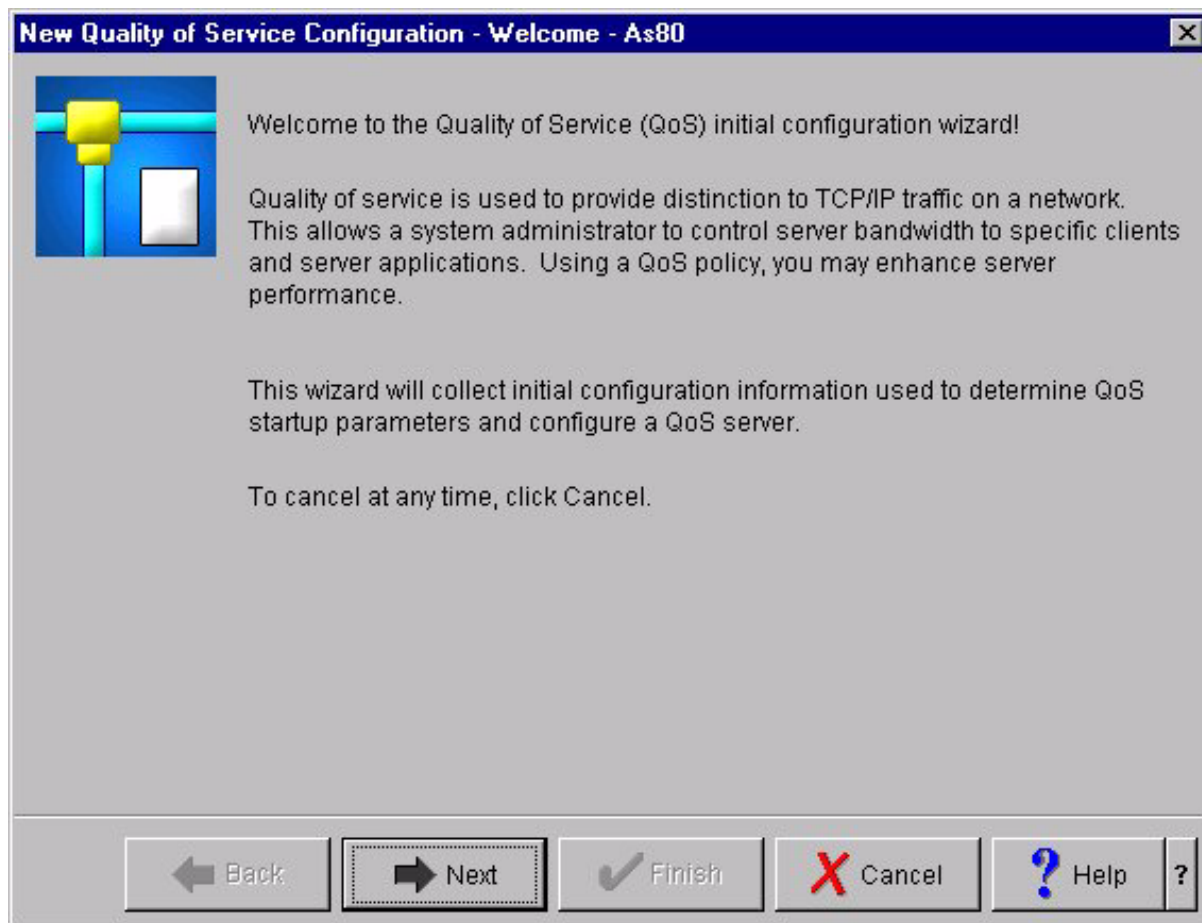
Expedited forwarding gives traffic a low-loss, low-jitter end-to-end service by guaranteeing bandwidth across networks. The reservation is made before the packet is sent. The main goal is to avoid delay and deliver the packet on a timely basis.

Class 0 gives packets the lowest priority and Class 7 gives packets the highest priority within the **class selector codepoint** values. This is the most common group of per-hop behaviors, because most routers already use similar codepoints.

Assured forwarding is divided into four per-hop behavior classes, which each have drop precedence levels of low, medium, or high. A drop precedence level determines how likely it is for the packets to be dropped. The classes each have their own bandwidth specifications. *Class 1, High* gives the policy the lowest priority and *Class 4, Low* gives policies the highest priority. A low drop level means the packets in this policy have the lowest chance of being dropped in this particular class level.

Notes: Differentiated Service-3

<u>Expedited forwarding</u>	<u>Class Selector</u>	<u>Assured forwarding</u>
101110	Class 0 - 000000	Assured forwarding, Class 1, Low - 001010
	Class 1 - 001000	Assured forwarding, Class 1, Medium - 001100
	Class 2 - 010000	Assured forwarding, Class 1, High - 001110
	Class 3 - 010010	Assured forwarding, Class 2, Low - 010010
	Class 4 - 100000	Assured forwarding, Class 2, Medium - 010010
	Class 5 - 101000	Assured forwarding, Class 2, Low - 010010
	Class 6 - 110000	Assured forwarding, Class 3 Low - 011010
	Class 7 - 111000	Assured forwarding, Class 3, Medium - 011100
		Assured forwarding, Class 3, High - 011110
		Assured forwarding, Class 4, Low - 100010
		Assured forwarding, Class 4, Medium - 100100
		Assured forwarding, Class 4, High - 100110



Use the **New QoS Configuration - Welcome** wizard to begin policy configuration. The wizard asks you to define a set of start up instructions for the different QoS parameters, such as QoS server, journaling, and monitoring.

QoS Wizard - Start Server



Use the **New QoS Configuration - Start Server** page to set the autostart values for the QoS server. The system updates the QATOCSTRT file with your selections.

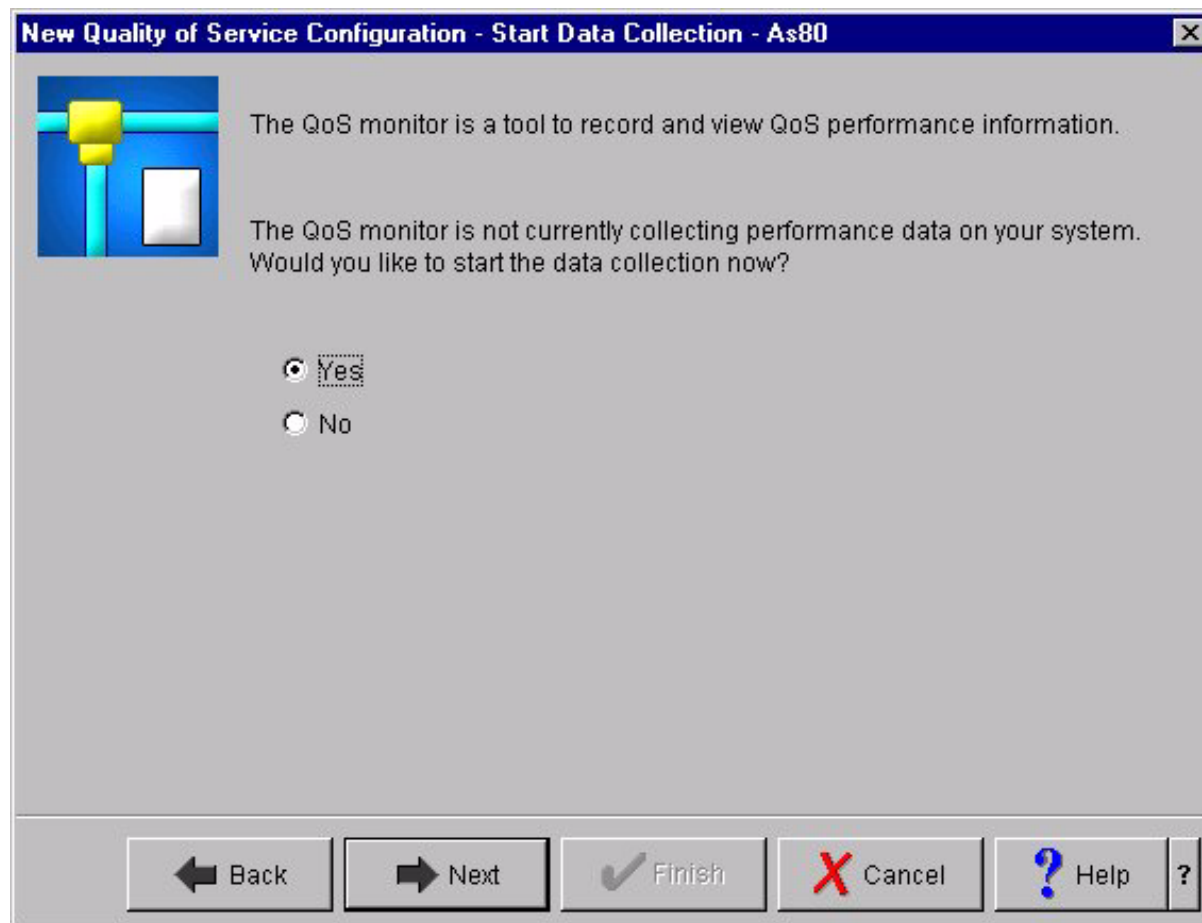
Autostart the QoS server with TCP/IP

Specifies whether or not you want the QoS server to automatically start with TCP/IP.

Start the server now

Specifies whether or not you want the QoS server to start immediately.

QoS Server - Start Data Collection



Notes: QoS Server - Start Data Collection

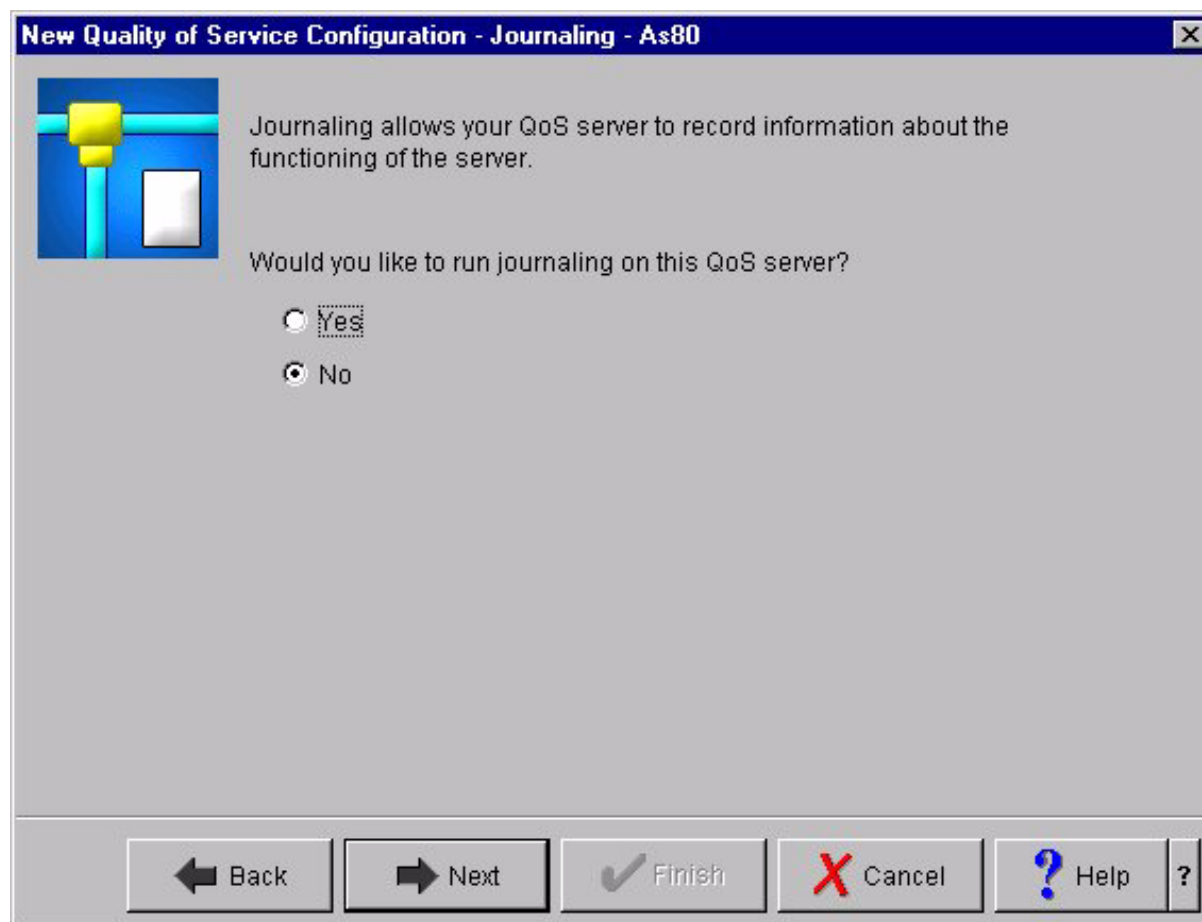
If you specified that you want to start the QoS now, this panel will pop up.

Use the **New QoS Configuration - Start Data Collection** page to have the QoS monitor start collecting data.

Do you want to start it now?

Select whether or not you want to start QoS data collection immediately.

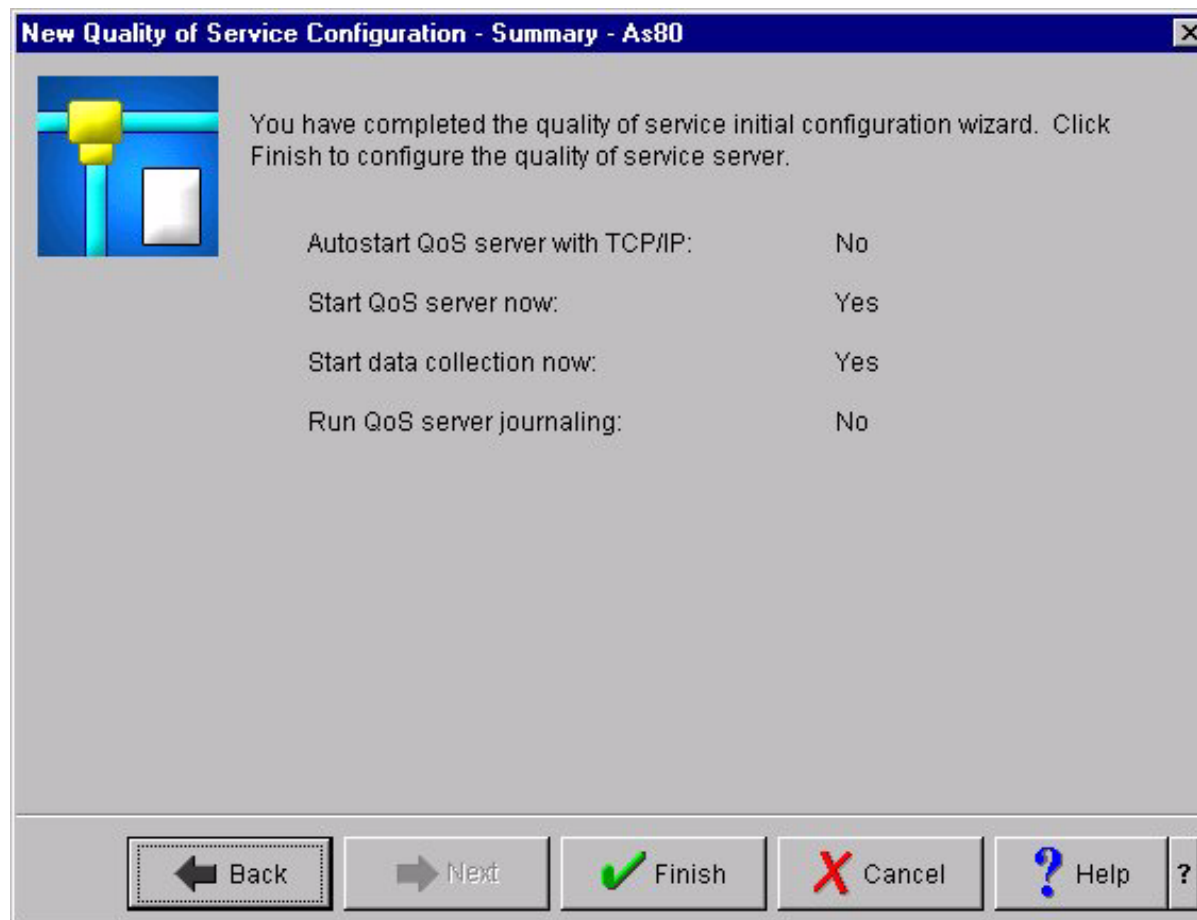
QoS Server - Journaling



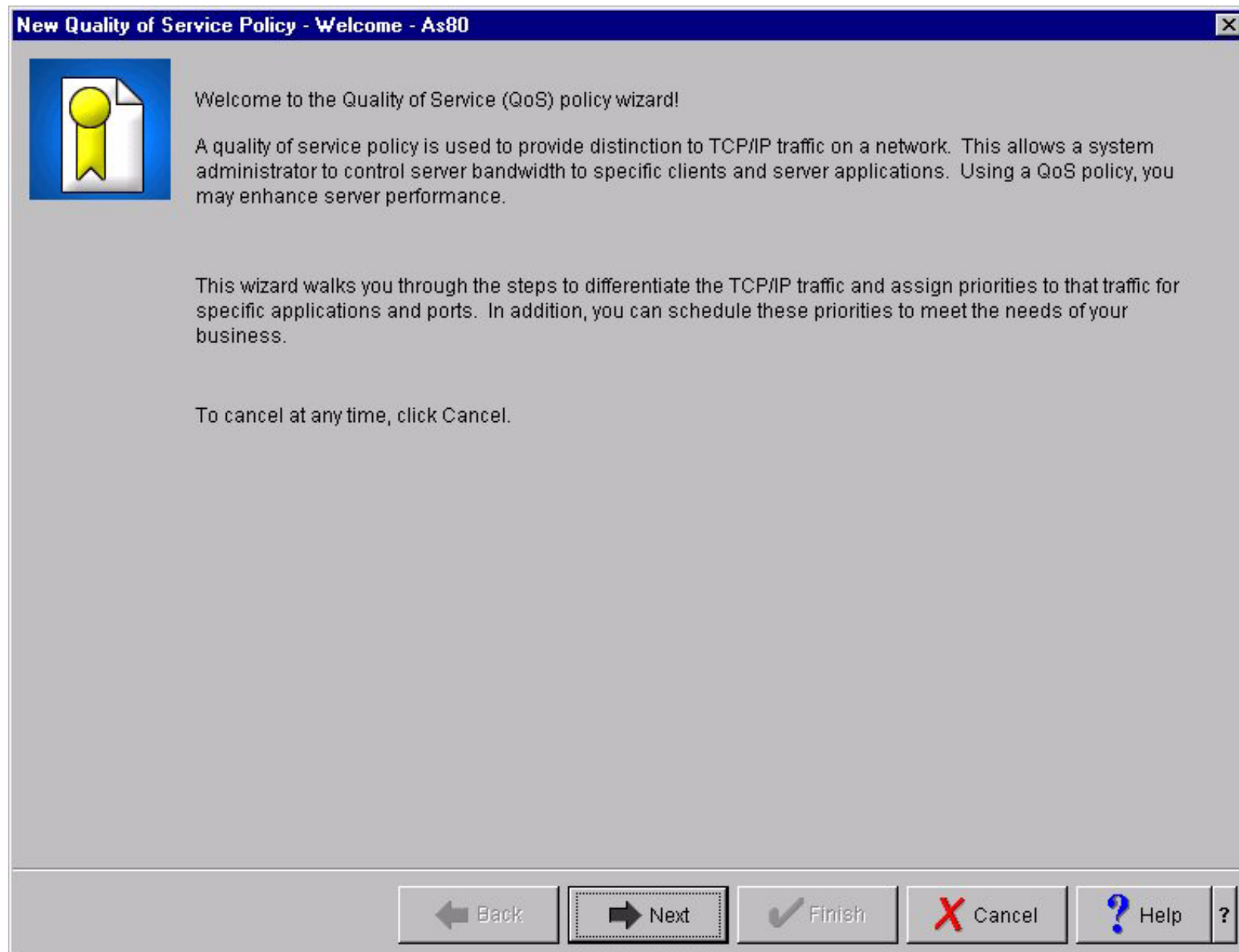
Use the **New QoS Configuration - Journaling** page to activate the run QoS journal feature.

Journaling tracks a specific set of QoS actions that take place on your server. This is a good way to audit and make sure that your policies are operating the way you intend them to operate. The following events on your AS/400 are journaled: Loading rules, Unloading rules, and Modifying rules.

QoS Server - Configuration Summary

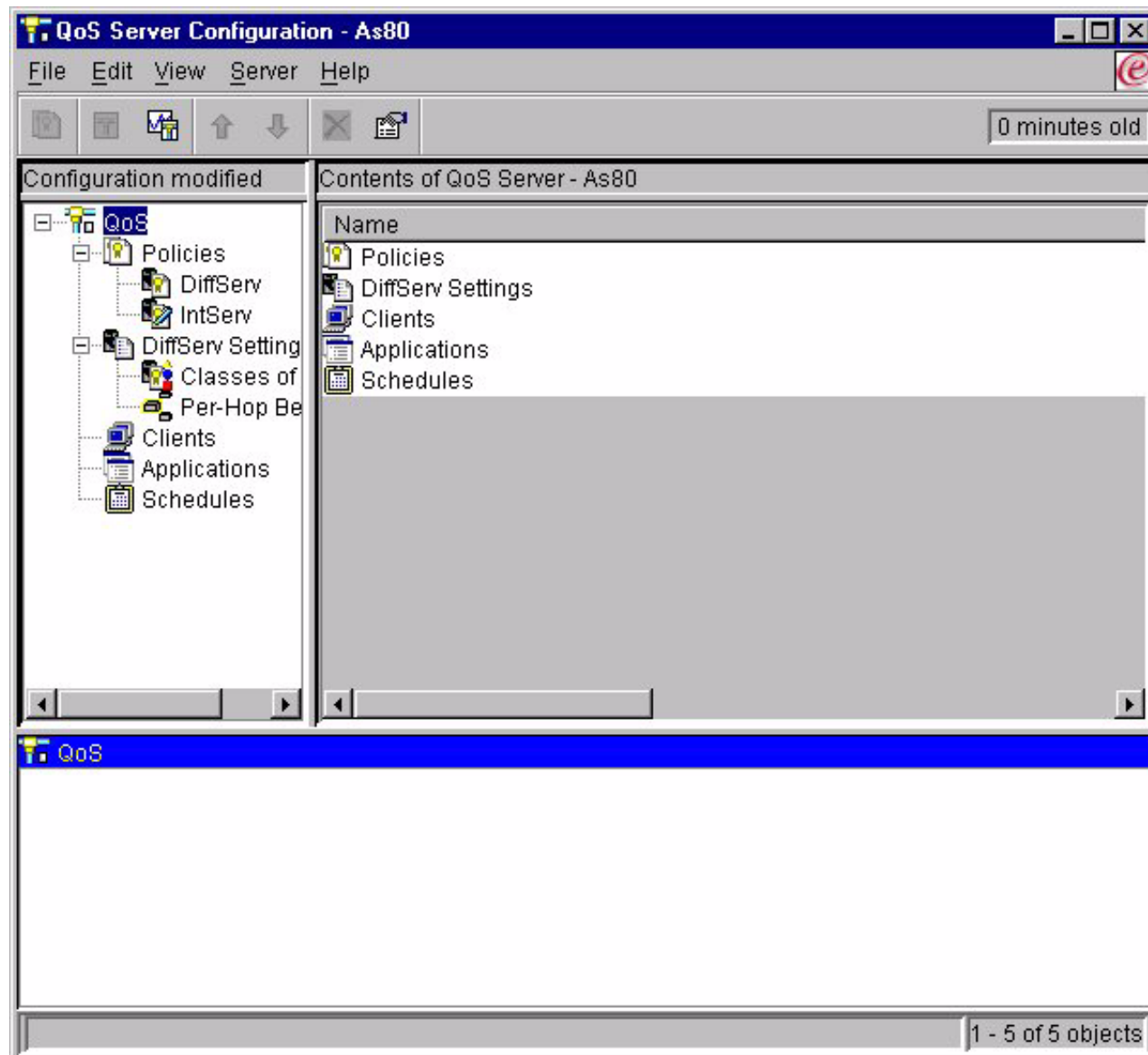


QoS - Configuration Wizard



QoS - Server Configuration

IBM @server iSeries



IBM @server. For the next generation of e-business.

The GUI interface for configuring QoS allows you to define all elements required for its setup:

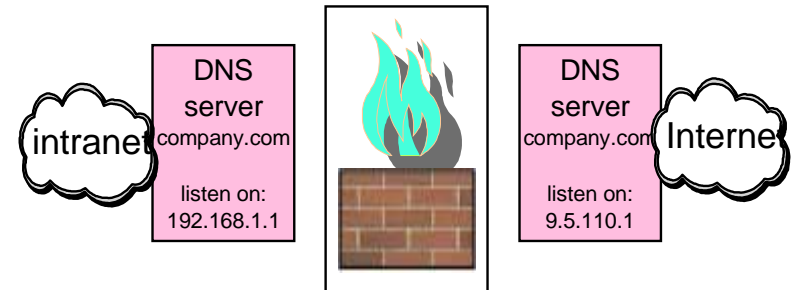
- Policies for both integrated and differentiated services
- Differentiated Services settings and per-hop behaviors
- Clients
- Applications
- Schedules

Domain Name System Enhancements

IBM @server. For the next generation of e-business.

Support for Berkeley Internet Name Domain (BIND) 8:

- Secure Dynamic Updates
- Multiple DNS servers on a single system
- Conditional forwarding
- NOTIFY
- Incremental zone transfer (IXFR)



Requires Portable Application Solutions Environment (PASE) to be installed

Performs automatic migration from previous DNS versions

New Configuration Wizard

For Version 5 Release 1 (V5R1), the DNS interface has been redesigned. V5R1 DNS services are based on the industry standard DNS implementation known as BIND (Berkeley Internet Name Domain) version 8. Previous OS/400 DNS services were based on BIND version 4.9.3.

Secure Dynamic Update

In the past, all DNS resource records had to be created and maintained by the administrator. Now, DNS servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically. You can configure your DHCP server to send update requests to the DNS server each time it assigns a new address to a host. This automated process reduces DNS server administration in rapidly growing or changing TCP/IP networks, and in networks where hosts change locations frequently. When a client using DHCP receives an IP address, that data is immediately sent to the DNS server. Using this method, DNS can continue to successfully resolve queries for hosts, even when their IP addresses change.

You can configure DHCP to update address mapping (A) records, reverse-lookup pointer (PTR) records, or both on behalf of a client. The A record maps a machine's host name to its IP address. The PTR record maps a machine's IP address to its host name. When a client's address changes, DHCP can automatically send an update to the DNS server so other hosts in the network can locate the client through DNS queries at its new IP address. For each record that is updated dynamically, an associated Text (TXT) record will be written to identify that the record was written by DHCP.

Dynamic zones are secured by creating a list of authorized sources that are allowed to send updates. You can define authorized sources using individual IP addresses, whole subnets, packets that have been signed using a shared secret key (called a Transaction Signature, or TSIG), or any combination of those methods. DNS verifies that incoming request packets are coming from an authorized source before updating the resource records.

Dynamic updates can be performed between DNS and DHCP on a single iSeries server, between different iSeries servers, or between an iSeries and other servers that are capable of dynamic updates.

Multiple DNS servers running on a single iSeries 400

In past releases, only one DNS server could be configured. Now you can configure multiple DNS servers, or instances. This allows you to set up logical division between servers. When you create multiple instances, you must explicitly define the listen-on interface IP addresses for each one. Two DNS instances cannot listen on the same interface. One practical application of multiple servers is split DNS, where one server is authoritative for an internal network, and a second server is used for external queries.

Conditional forwarding

Conditional forwarding allows you to configure your DNS server to fine-tune your forwarding preferences. You can set a server to forward all queries for which it does not know the answer. You could set forwarding at a global level, but add exceptions to domains for which you want to force normal iterative resolution. Or, you could set normal iterative resolution at the global level, then force forwarding within certain domains.

NOTIFY

When NOTIFY is turned on, the DNS NOTIFY function is activated whenever zone data is updated on the primary server. The primary server sends out a message to all known secondary servers that indicates data has changed. Secondary servers may then respond with a zone transfer request for updated zone data. This helps improve secondary server support by keeping backup zone data current.

Zone transfers (IXFR and AXFR)

In the past, whenever secondary servers needed to reload zone data, they had to load the entire data set in an *All zone transfer* (AXFR). BIND 8 supports a new zone transfer method: *incremental zone transfer* (IXFR). IXFR is a way that other servers can transfer only changed data, instead of the entire zone. When enabled on the primary server, data changes are assigned a flag to indicate that a change has occurred. When a secondary server requests a zone update in an IXFR, the primary server will send just the new data. IXFR is especially useful when a zone is dynamically updated, and reduces the traffic load by sending smaller amounts of data.

Prerequisites

If you want to run the Domain Name System (DNS) server BIND 8.2.3 you need to install the following options on the iSeries:

- OS/400 Option 12 (Host Servers)
- OS/400 Option 31 (Domain Name System)
- OS/400 Option 33 (PASE)

PASE is supported on all iSeries 400 models and on all RISC-based AS/400s, with the exception of the 4xx and 5xx models. For a complete list of the supported systems, check

<http://www.as400.ibm.com/developer/factory/pase/ehardware.html>

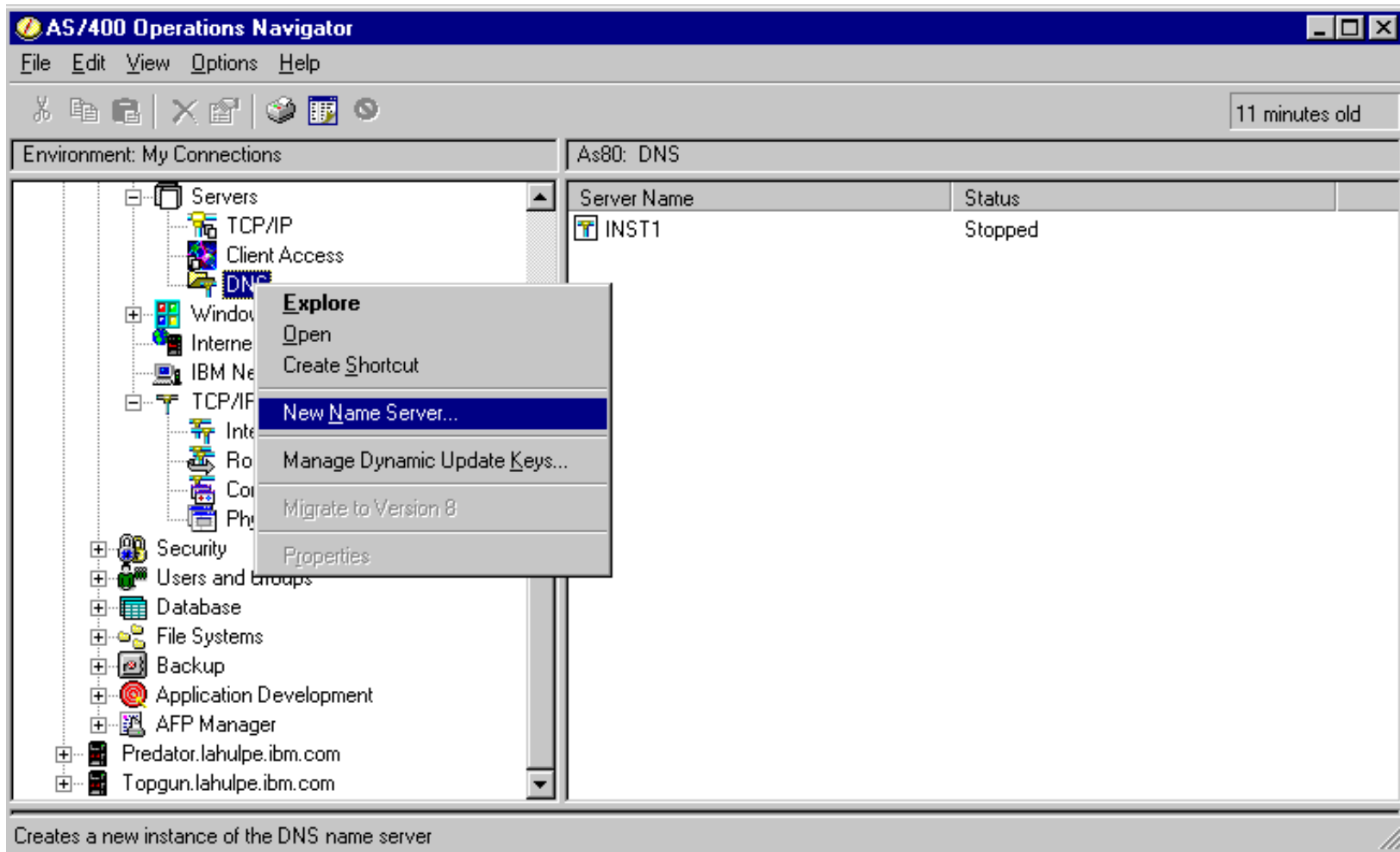
Remember you can decide to continue to run the "non-dynamic" DNS configuration on the iSeries as well as the new "dynamic DNS."

Migration

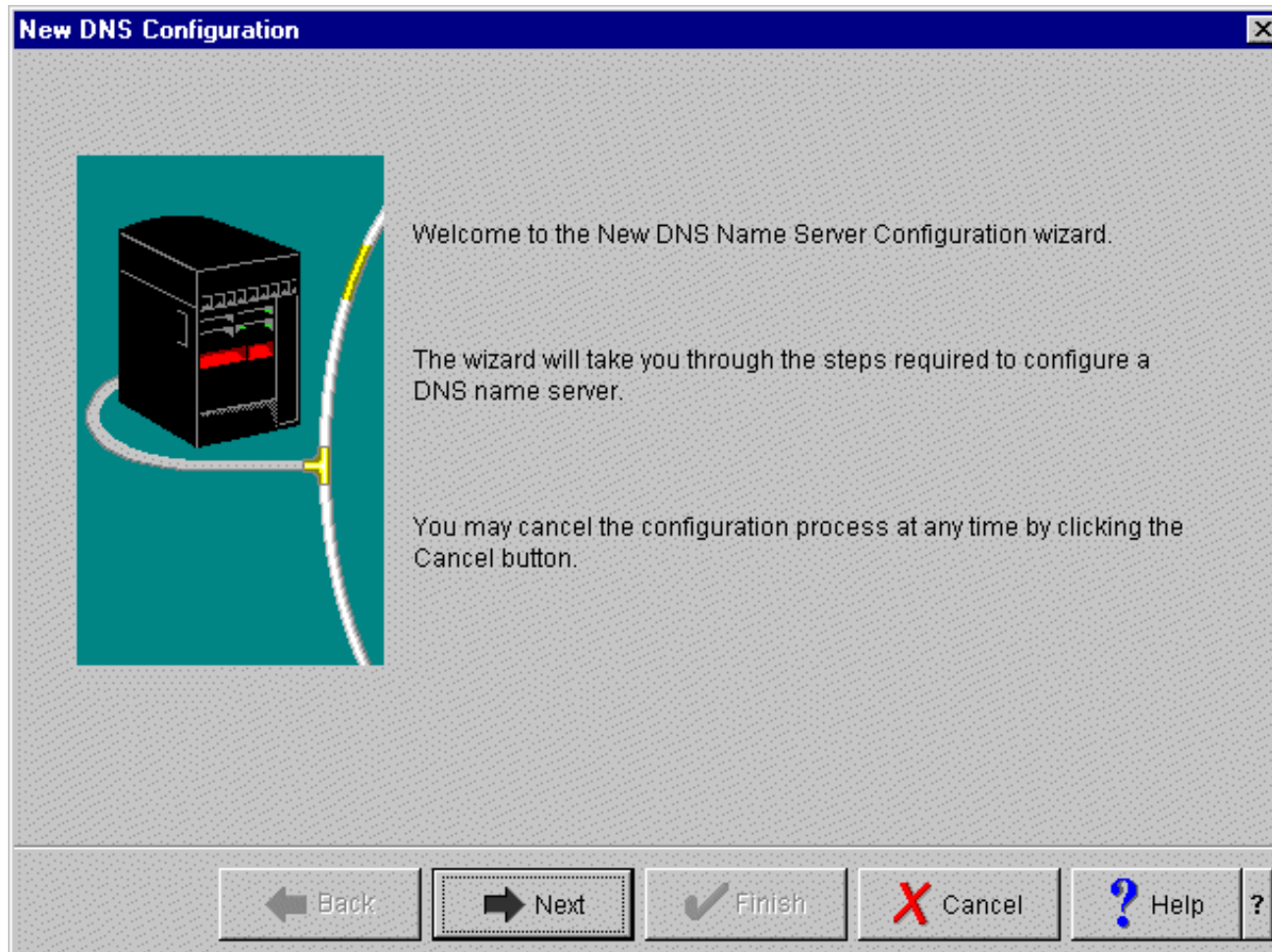
from BIND 4xx will be executed automatically before any DNS server is started or is being configured.

The next foils give an overview of the panels shown when configuring DNS using Operations Navigator.

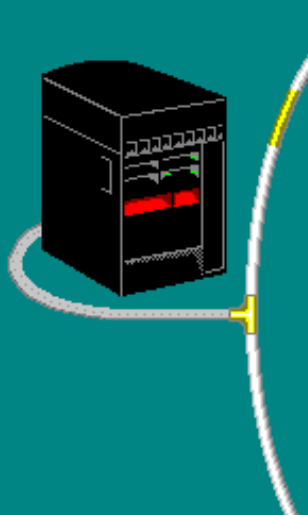
Access to DNS Configuration



Start DNS Configuration Wizard



DNS Server Name [X]



A DNS name server must have a unique name to differentiate it from other DNS name servers defined on the AS80 system.

What is the name of this DNS name server?

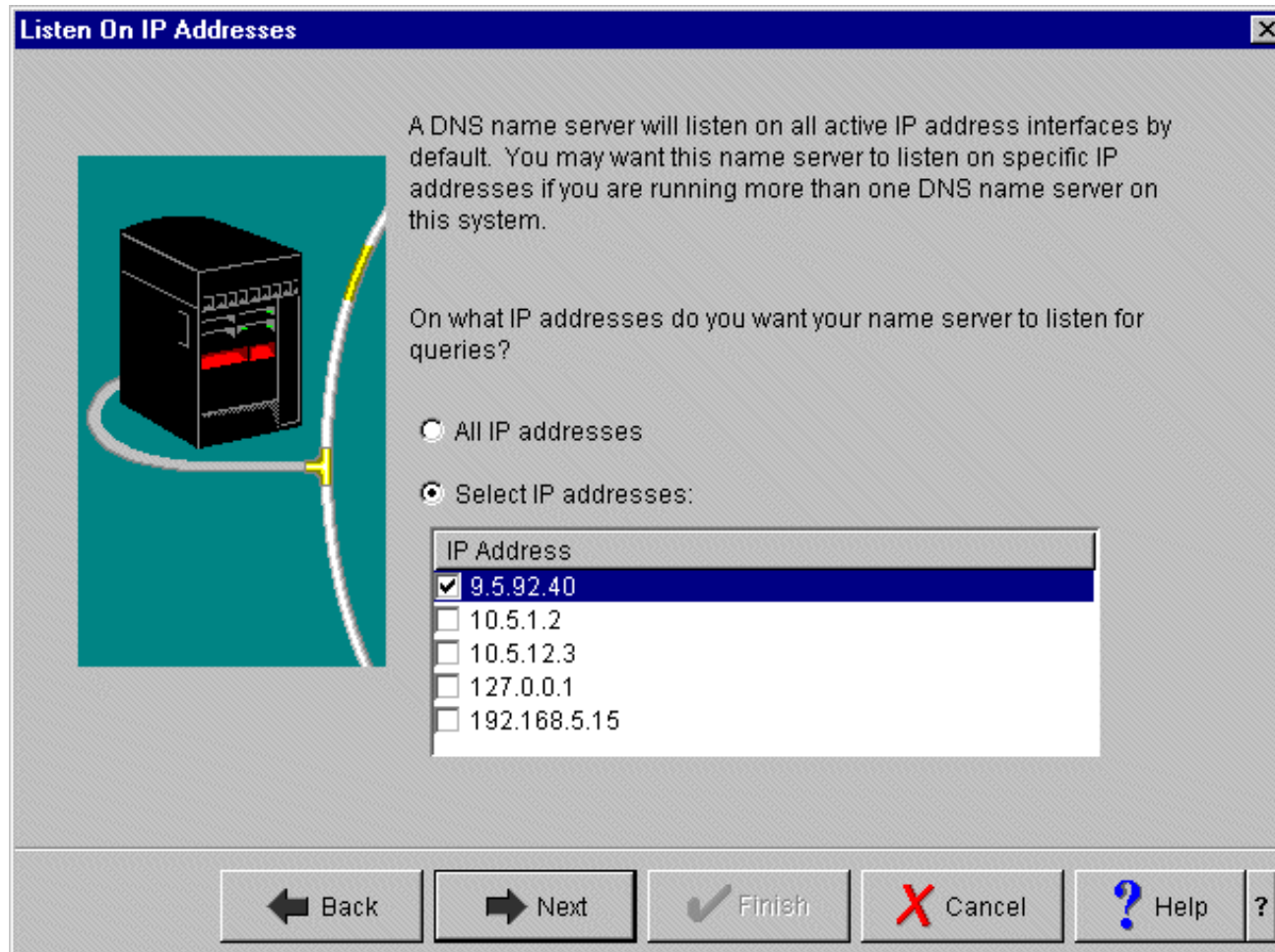
Name:

← Back → Next ✓ Finish ✗ Cancel ? Help ?

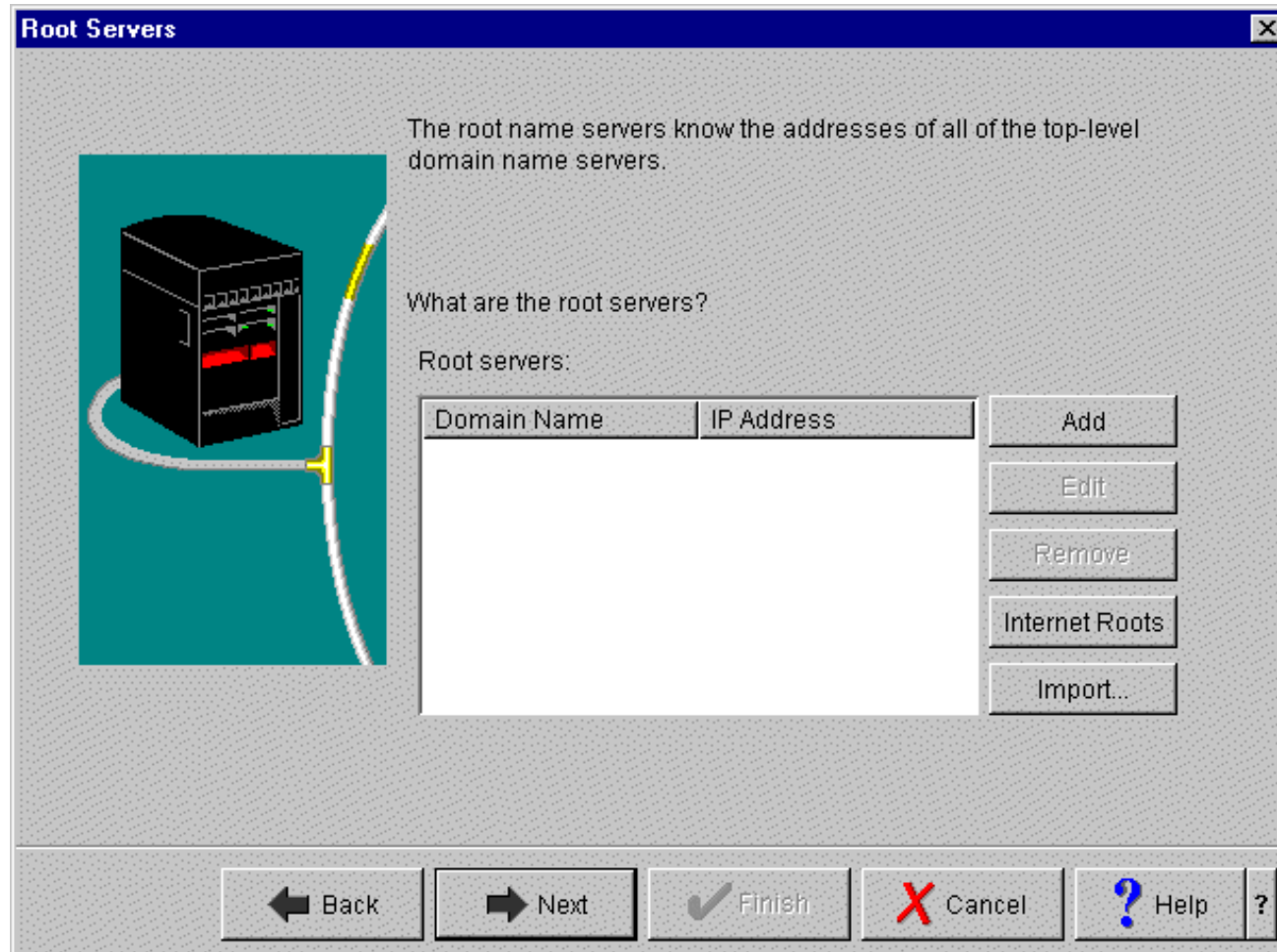
Notes: DNS Name

The name of the DNS must begin with an alphabetic character (A-Z), followed by 0 to 4 alphanumeric (A-Z, 0-9) characters.

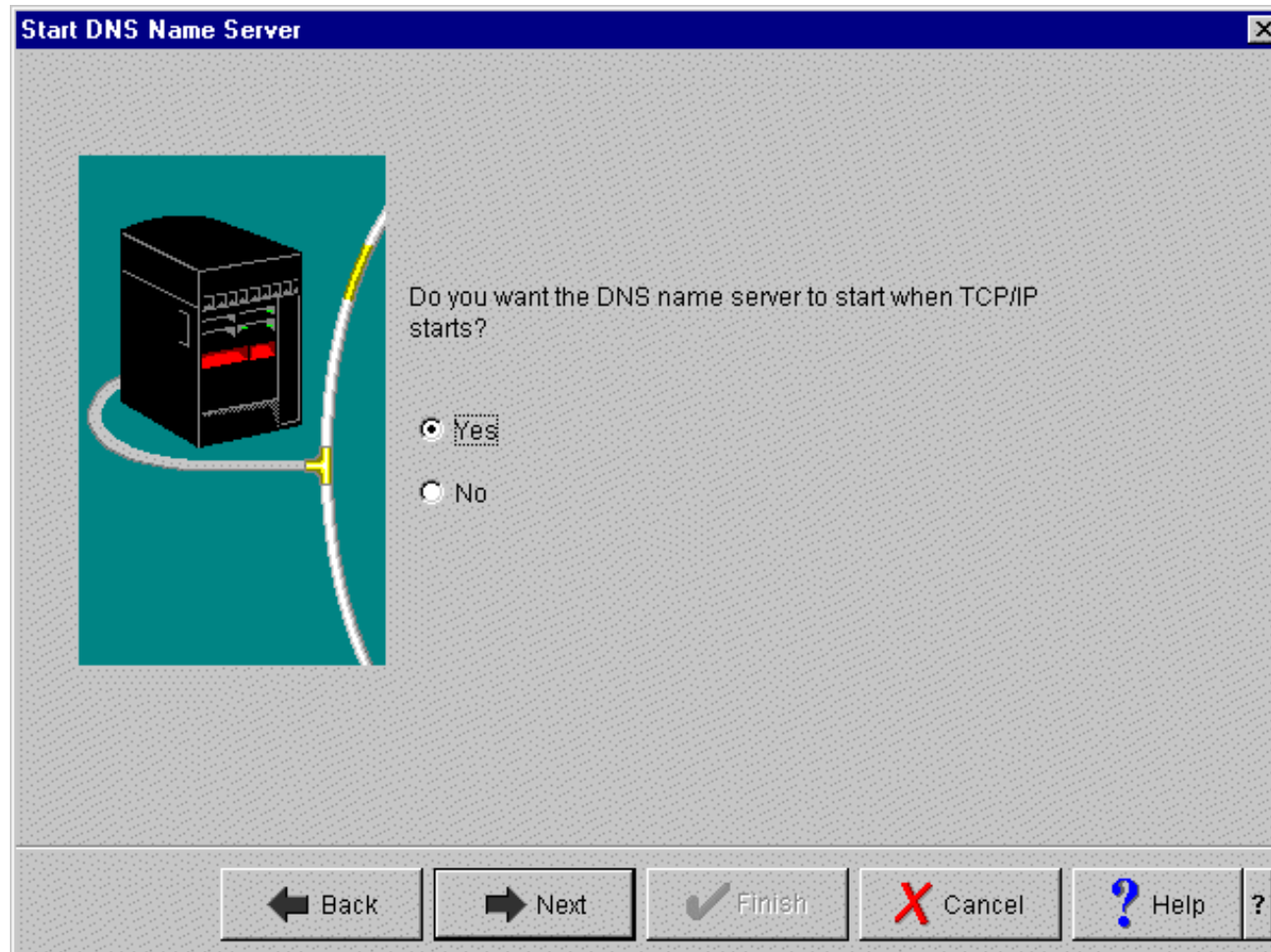
DNS Listens on IP Addresses



Root Server Specifications



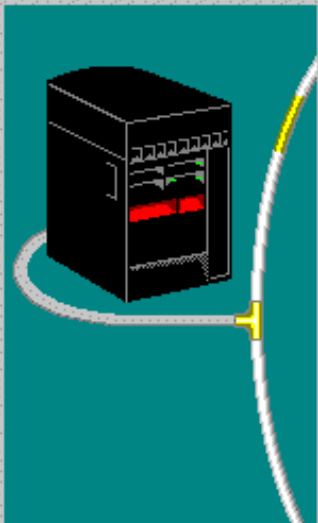
DNS Startup Options



IBM  server. For the next generation of e-business.

DNS Configuration Complete

Summary



Congratulations!

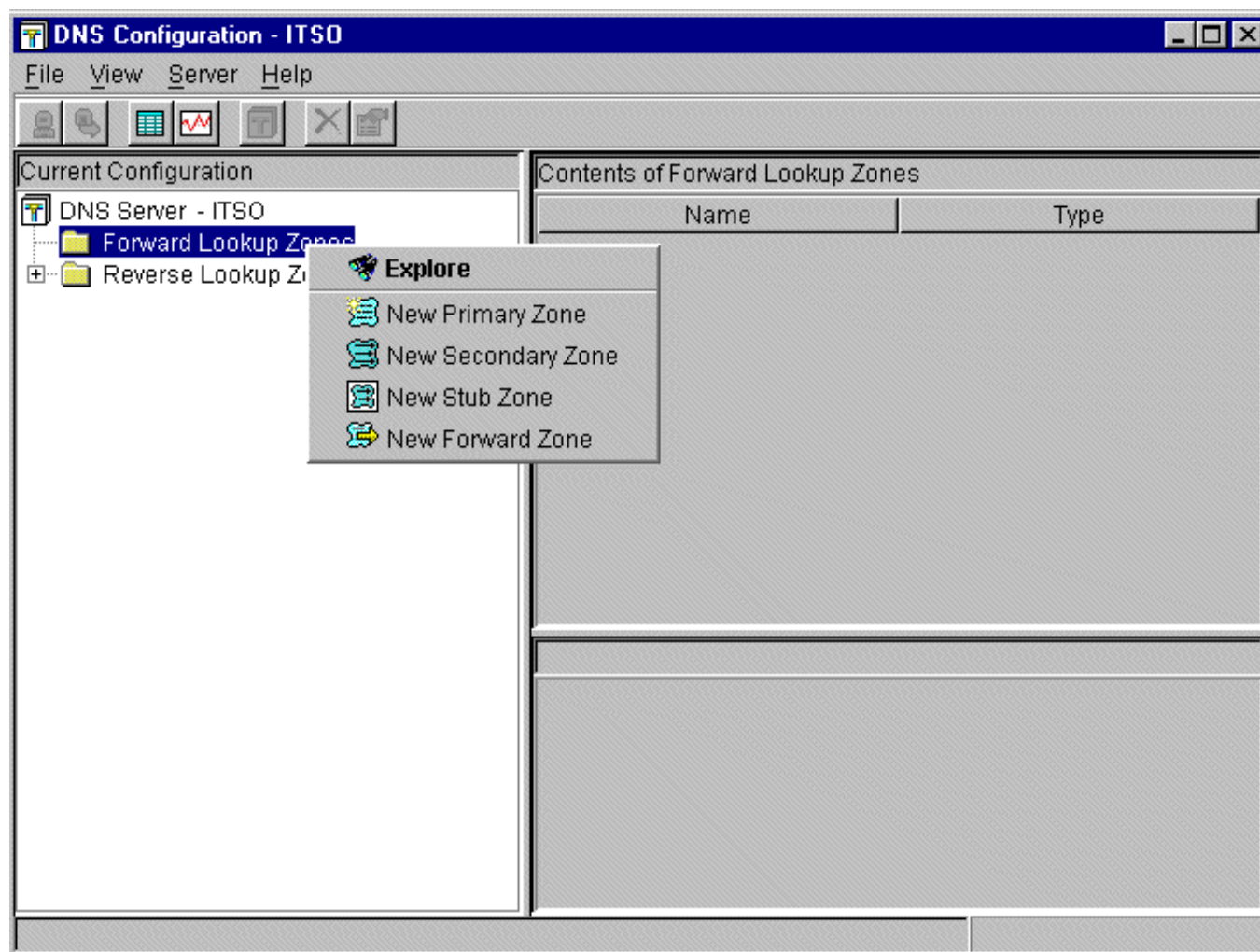
You have successfully created a new DNS name server. Review the summary of your configuration data below.

Summary:

Step	Result
Host name of DNS server:	ITSO
Listen On IP Address:	{9.5.92.40}
Start the DNS server when TC...	Yes
Root servers:	None

← Back → Next ✓ Finish ✗ Cancel ? Help ?

DNS Zone Specifications



Virtual Private Network Enhancements

IBM @server. For the next generation of e-business.

Information Key Exchange (IKE)
phase 1 authentication - system wide
IKE responder

Support for on-demand connections

Automatic migration from V4R4/V4R5
setups

IP Compression (IPComp) support

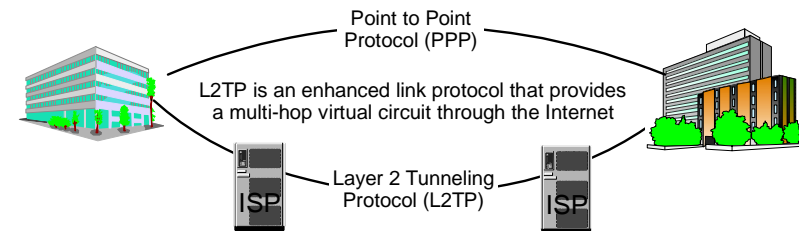
Automatic generation of policy filter
rules

New GUI interfaces

Key VPN Protocols

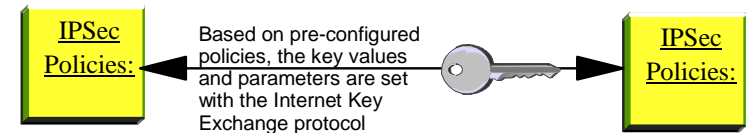
1. L2TP

open the link
that creates
the circuit



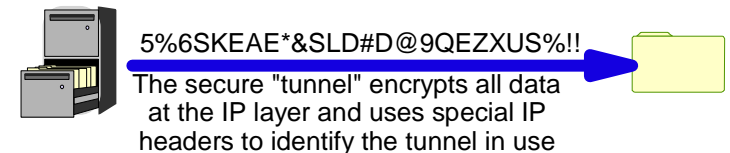
2. IKE

exchange the
encryption keys
and policies



3. IPSec

transfer the
data encrypted
at the IP layer



Other, not listed, changes to the Version 5 Release 1 (V5R1) Virtual private networking topic include:

- Enhancements to the basic configuration scenarios from last release.
- Additional network address translation for VPN (VPN NAT) support.
- VPN connections can now be applied to *OPC interfaces (OptiConnect).
- 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.
- More troubleshooting information including a table that lists error messages, result codes, and recovery information.
- Information about migrating from a prior release of the operating system.

Enhancements to the V5R1 OS/400 VPN function include:

- The addition of digital signature support for Internet Key Exchange (IKE) phase 1 authentication. In prior releases, OS/400 VPN only supported preshared keys as the authentication method it used for phase 1 negotiations. A system-wide responder IKE policy that lists which algorithms your system will accept when it responds to an IKE request.
- Support for on-demand connections. An on-demand connection starts only after IP datagrams that are destined for a specific VPN connection attempt to flow. In other words, the connection is only enabled when it is needed. On-demand connections require that the policy filter be loaded, the VPN server be running, and the appropriate interface be active on the system. After a period of inactivity on the connection, the VPN connection will become inactive while it waits for more IP datagrams to flow.
- Support for the IP Compression (IPComp) protocol. IPComp reduces the size of an IP datagram by compressing it to increase the communication performance between two VPN partners.
- Policy filter rules can be generated automatically by the VPN graphical user interface (GUI). In prior releases of the operating system, you had to configure the VPN packet rules, by hand, as a separate step. They were not generated automatically as part of your VPN configurations. In V5R1, OS/400 VPN can now create these packet rules automatically. However, there are several items you need to consider if you created policy filter rules (rules where action=IPSEC) in V4R4 or V4R5, and you want to use those same rules in V5R1.

New Communications Features

IBM @server. For the next generation of e-business.

#2817 155 Mbps MMF ATM

- Replaces #4816 155 Mbps ATM, when OS/400 V5R1 is ordered

#2760 1 Gbps / 100Mbps / 10Mbps UTP Ethernet UTP IOA

- Unshielded twisted pair (UTP) lower cost than current #2743 1 Gbps Ethernet IOA (multi-mode fibre optic cable)
- Negotiates to 1 Gbps, 100 Mbps, or 10 Mbps
- TCP/IP only, full or half duplex

#2772 and #2773 two line WAN adapters (RJ11) for V.90 support

- Integrated modem on both lines (similar to first line of #9771 shipped with every iSeries system)

#2817 155 Mbps MMF ATM

#2817 is a 155Mbps Asynchronous Transfer Mode (ATM) PCI card that allows the server to be attached into an ATM network using the Multi-Mode Fiber (MMF) 62.5 micron interface. This interface is intended for connection to both local area switches and direct connection to service provider equipment. #2817 will typically be used where 155Mbps speeds are required over distances of less than 2Km. This card is a 64-bit card, but is allowed to plug into any 32-bit or 64-bit slot. This feature replaces #4816, on orders with V5R1 OS/400 in the configuration.

The #2817 ATM is a Non-Assist IOA. Functions that the card might handle are moved to the system level. Such things as fragmentation reassembly, address verification, IP filtering, and checksum generation verification are handled by the system. This allows the card to process data faster. Increased performance has also come from the more optimized transmit/receive path.

#2760 1 Gbps Ethernet

The #2760 PCI 1Gbps Ethernet IOA feature will allow to attach to IEEE standard 802.3Z high speed Ethernet LANs (1Gbps) to provide a significant performance improvement over other LAN solutions. The adapter supports a UTP CAT 5 media interface. This adapter only supports TCP/IP. This adapter can directly attach to 10Mbps or 100Mbps networks - the 1 Gbps, 100 Mbps, or 10 Mbps speed is negotiated. A #2760 is supported under a #2790, #2791, #2890 or #2891 Integrated Netfinity Servers with V5R1. It is recommended that Enhanced Category 5 cable be used for the best results. The Enhanced Category 5 cable will be less likely to experience problems.

iSeries Ethernet support details

The Gigabit Ethernet Adapter Card (features 2743 (optical fibre) or 2760 (unshielded twisted pair) are one gigabit per second input/output adapters (IOAs) that supports **only TCP/IP**. The #2760 supports half and full-duplex mode while the #2743 supports only full-duplex. The sending and receiving channels can transfer data at approximately one Gbps.

#2760 is lower cost than #2743, but runs at a slightly lower maximum throughput.

Both 1Gbps IOAs support the IEEE 802.3 and the Ethernet Version 2 standards. It also supports frame sizes that include 1496 to 8996 bytes. This card attaches to the 2842 PCI IOP(270), or 2843 PCI IOP(8xx).

#2743 requirement: You must ensure that all "devices" (switches, routers, bridges) within the communications path can handle the 1 Gbps speed . This card does not negotiate to a lower speed. Speed negotiation is performed only on the #2760 1 Gbps Ethernet adapter, #4838 100 Mbps/10 Mbps Ethernet adapter, or the #2744 100/16/4 Mbps Token Ring adapter.

The industry standard states that gigabit Ethernet frames are to be the same size as 10/100 Ethernet frames, which ranges from 64 to 1518 bytes. All known Ethernet vendors know and meet this requirement. Since the card technology used with #2743 and #2760 supports larger frame sizes you can realize maximum throughput over the 1Gbps communication link by using switches that support frame sizes in the 1518 through 8996 bytes range. At the time of publication there is only one known vendor switch that supports the larger frames. See the Notes that follow. If you are in doubt about the switch frame size capacity you must not specify a frame size greater than 1496 on the AS/400 Ethernet Line description MAXFRAME parameter.

1 Gbps Ethernet support continued

If the maximum frame size specified is greater than 1496 bytes, LINESPEED(1G) or LINESPEED(*AUTO) and DUPLEX(*FULL) or DUPLEX(*AUTO) must be specified for the #2743. For the 2760 DUPLEX(*FULL or *HALF or *AUTO) may be specified..

For the #2743:

- The technology used in the 2743 card does not negotiate to a lower speed than 1 Gbps. The #2743 1 Gbps Ethernet Adapter) requires a 1 Gbps-capable switch with at least one port that supports a 1000BASE-SX interface with IEEE 802.3z and 802.3u compliance. The 2743 supports only a multi-mode fiber optic cable connection from the AS/400 adapter to the switch.
- Depending on the switch capabilities, other devices on the network could use different cable types (UTP) and speeds (100 Mbps or 10 Mbps).
- A customer-supplied cable with the following specifications is used to attach the adapter to the switch: SC (fiber optic) connector, multi-mode fiber cable (62.5/125 micron fiber or 50/125 micron fiber).

Vendors that provide the required 1 Gbps switch hardware interface include the following. There are others.:

- Alteon Web Systems - <http://alteonwebsystems.com>
This vendor provides 1 Gbps switches with the capability to process 8996 byte frames
- N Base Communications Giga Frame Switch - <http://www.3com.com/util/contact.html>
- 3COM Super Stack II Switch 9000 - <http://www.nbase-xyplex.com/contactus/index.cfm>

Notes: Communication Adapters...

#2772 and #2773 two line WAN adapters

#2772 and #2773 are basically the same interface, the #2772 is the non-CIM (Complex Impedance Matching) version of this card. Both are 2-line WAN adapters, with two ports (RJ11) supporting V.90 56K Async PPP and FAX applications at data rates up to 14.4K via internal modems. Connection to the V.90 ports is via telephone cable. Both these features do not support remote power on. The new cards can be used for the purpose of Multilink. These cards need country specific telephone cables (minimum one and maximum two per card). **Feature #2773, the Complex Impedance Matching version is intended for Australia and New Zealand only.**

Compared with the existing #4761 with eight analog modem ports, the #2772/#2773 and #4761 both have fax capabilities, but the #4761 is more robust in this area. This is because the #4761 handles the fax process in the card whereas the #2772/#2773 passes it off to the system. The #2772/#2773 is a good option for those wanting to add some additional ports, but not wanting to add eight and if you do not need V.34 synchronous support that is provided by the #4761.

The feature code #9771 integrated V.90 modem will continue to be shipped with new systems. The two ports of the #2772 or #2773 are the same as the V.90 port of the #9771.

Minimum of one modem cable, maximum of two must be selected/ordered for each #2772 / #2773. Cable features that can be ordered:

#1010 Modem Cable - Austria	#1014 Modem Cable - Italy	#1018 Modem Cable - Iceland/Sweden	#1022 Modem Cable - Netherlands
#1011 Modem Cable - Belgium	#1015 Modem Cable - France	#1019 Modem Cable - Australia	#1023 Modem Cable - Swiss
#1012 Modem Cable - Africa	#1016 Modem Cable - Germany	#1020 Modem Cable - HK/NZ	#1024 Modem Cable - Denmark
#1013 Modem Cable - Israel	#1017 Modem Cable - UK	#1021 Modem Cable - Fin/Nor	#1025 Modem Cable - US/Canada

Remark: All modem cables for #2772 / #2773 that are ordered/present on one iSeries server must have the same feature number.

CRTLINETH for 1 Gigabit/second Ethernet

1 Gbps Ethernet LAN Line (features 2743, 2760)*

Create Line Description (Ethernet) (CRTLINETH)

Type choices, press Enter.

Line description	> ETHlin1	Name
Resource name	> CMN01	Name, *NWID, *NWSID
Online at IPL	*YES	, *NO
Vary on wait	*NOWAIT	, 15-180 seconds
Local adapter address	*ADPT	020000000000-FEFFFFFFF...
Exchange identifier	*SYSGEN	05600000-056FFFFF, *SYSGEN
Ethernet standard	*ALL	*ETHV2, *IEEE8023, *ALL
Enable for TCP/IP	*YES	, *NO
Line speed	1G	10M, 100M, 1G, *AUTO
Duplex	*AUTO	*HALF, *FULL, *AUTO
SSAP list:		
Source service access point	*SYSGEN	02-FE, *SYSGEN
SSAP maximum frame		*MAXFRAME, 265-8996, 265...
SSAP type		*CALC, *NONSNA, *SNA, *HPR
	+ for more values	

More...

* TCP/IP only