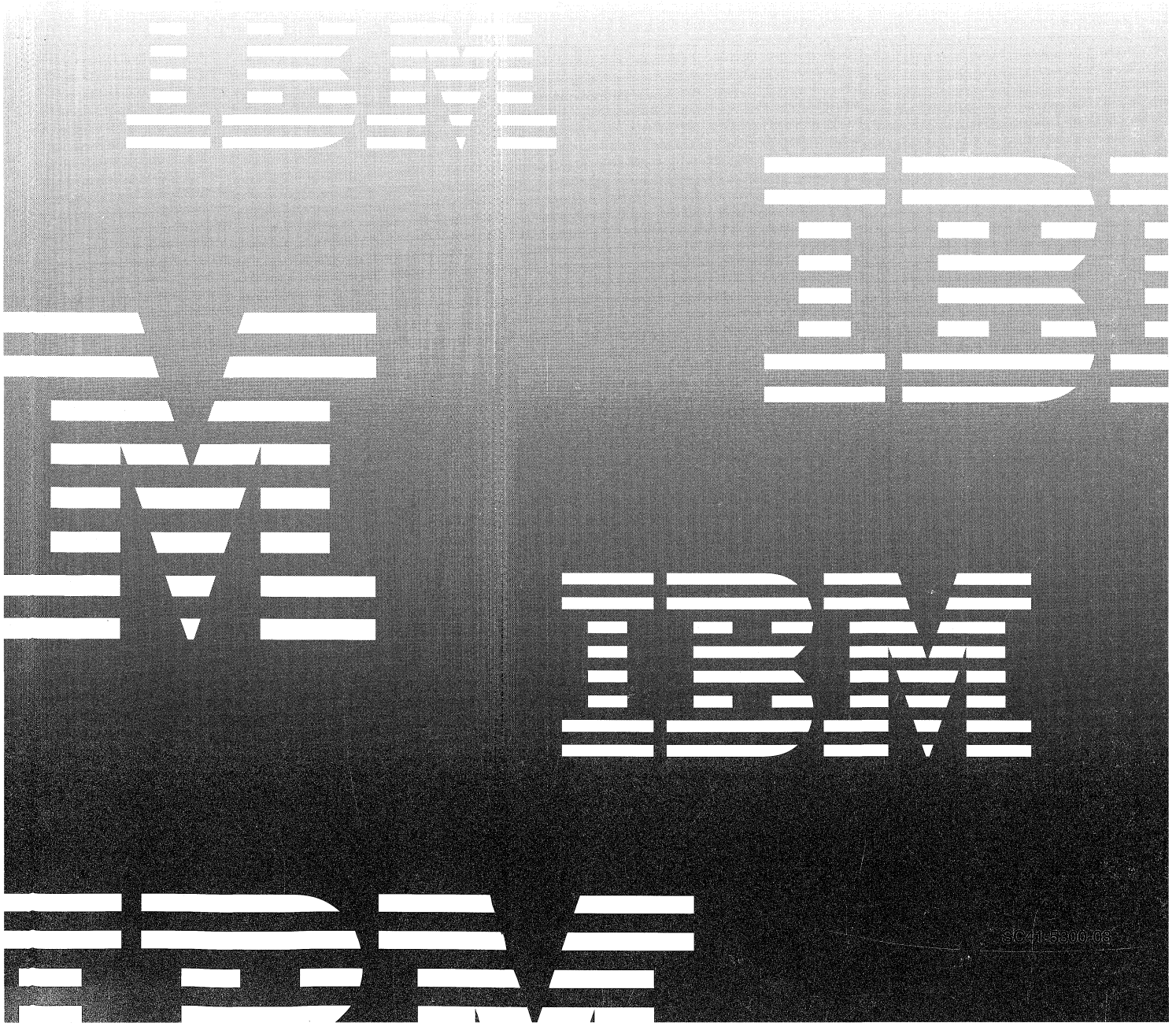
AS/400e

IBM

Tips and Tools for Securing Your AS/400

Version 4



SC41-5300-03

AS/400e

Tips and Tools for Securing Your AS/400

Version 4

SC41-5300-03

Note

Before using this information and the product it supports, be sure to read the information in "Appendix. Notices" on page 231.

Fourth Edition (May 1999)

This edition replaces SC41-5300-02. This edition applies only to V4R1 of OS/400 and above.

Contents

Figures

Tables

About Tips and Tools for Securing Your AS/400 (SC41-5300)

The role of computers in organizations is changing rapidly. IT managers, software providers, security administrators, and auditors need to take a new look at many areas that they have taken for granted in the past. AS/400 security should be on that list.

Systems are providing many new functions that are vastly different from traditional accounting applications. Users are entering systems in new ways: LANs, switched lines (dial-up), wireless, networks of all types. Often, users never see a sign-on display. Many organizations are expanding to become an "extended enterprise", either with proprietary networks or with the Internet.

Suddenly, systems seem to have a whole new set of doors and windows. Systems managers and security administrators are justifiably concerned about how to protect information assets in this rapidly changing environment.

This book provides a set of practical suggestions for using the security features of AS/400 and for establishing operating procedures that are security-conscious. The recommendations in this book apply to an installation with average security requirements and exposures. This book does not provide a complete description of the available AS/400 security features. If you want to read about additional options or you need more complete background information, consult the publications that are described in "Related Publications" on page 237.

This book also describes how to set up and use security tools that are part of OS/400. "Chapter 6. How to Set Up Your System to Use the Security Tools" on page 33 and "Commands and Menus for Security Commands" on page 34 provide reference information about the security tools. The entire book provides examples for using the tools.

Who should read this book

A **security officer** or **security administrator** is responsible for the security on a system. That responsibility usually includes the following tasks:

- Setting up and managing user profiles
- Setting system-wide values that affect security
- Administering the authority to objects
- Enforcing and monitoring the security policies

If you are responsible for security administration for one or more AS/400 systems, this book is for you. The instructions in this book assume the following:

- You are familiar with basic AS/400 operating procedures, such as signing on and using commands.
- You are familiar with the basic elements of AS/400 security: security levels, security system values, user profiles, and object security. "Chapter 3. Basic Elements of AS/400 Security" on page 13 provides a review of these elements. But if these basic elements are new to you, you should read the *Security - Basic* book before you use this book.
- You have activated security on your system by setting the security level (QSECURITY) system value to at least 30.

IBM continually enhances the security capabilities of AS/400. To take advantage of these enhancements, you should regularly evaluate the cumulative PTF package that is currently available for your release. See if it contains PTFs that are relevant to security. In addition, "Chapter 1. AS/400 Security Enhancements" on page 3 describes the significant enhancements to AS/400 security that IBM has made in recent releases of the operating system.

How to Use This Book

If you have not set up your system to use the security tools or if you had the Security ToolKit for OS/400 installed for an earlier release, do the following:

1. Start with "Chapter 6. How to Set Up Your System to Use the Security Tools" on page 33 of this book. It describes how to set up the security tools and how to get started with them.
2. Review "Commands and Menus for Security Commands" on page 34 to learn about the commands and menus for the security tools.
3. Then start reading with "Chapter 3. Basic Elements of AS/400 Security" on page 13. This book provides both general security tips and suggestions for using the commands and menus that are part of the security tools.

If you are reading for general interest (perhaps you are an auditor or a software developer), start reading with "Chapter 3. Basic Elements of AS/400 Security" on page 13. Read the chapters that apply to your situation.

Pick What Is Right for You

This book has *many* tips for securing AS/400. Your system may only need protection in some areas. Use this book to educate yourself on possible security exposures and their remedies. Then focus your efforts on the areas that are most critical for your system.

AS/400 Operations Navigator

AS/400 Operations Navigator is a powerful graphical interface for Windows clients. With AS/400 Operations Navigator, you can manage and administer your AS/400 systems from your Windows desktop.

You can use Operations Navigator to manage communications, printing, database, security, and other system operations. Operations Navigator includes Management Central for managing multiple AS/400 systems centrally.

Figure 1 on page xv shows an example of the Operations Navigator display:

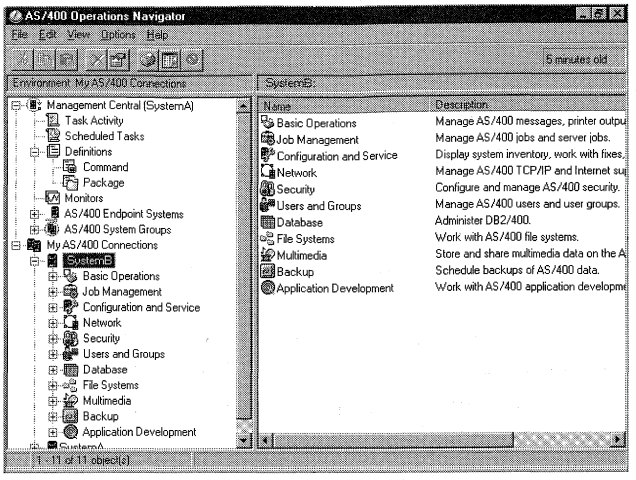


Figure 1. AS/400 Operations Navigator Display

This new interface has been designed to make you more productive and is the only user interface to new, advanced features of OS/400. Therefore, IBM recommends that you use AS/400 Operations Navigator, which has online help to guide you. While this interface is being developed, you may still need to use a traditional emulator such as PC5250 to do some of your tasks.

Installing Operations Navigator

To use AS/400 Operations Navigator, you must have Client Access installed on your Windows PC. For help in connecting your Windows PC to your AS/400 system, consult *Client Access Express for Windows - Setup*, SC41-5507-00.

AS/400 Operations Navigator is a separately installable component of Client Access that contains many subcomponents. If you are installing for the first time and you use the **Typical** installation option, the following options are installed by default:

- Operations Navigator base support
- Basic operations (messages, printer output, and printers)

To select the subcomponents that you want to install, select the **Custom** installation option. (After Operations Navigator has been installed, you can add subcomponents by using Client Access Selective Setup.)

1. Display the list of currently installed subcomponents in the **Component Selection** window of **Custom** installation or Selective Setup.
2. Select AS/400 Operations Navigator.
3. Select any additional subcomponents that you want to install and continue with **Custom** installation or Selective Setup.

After you install Client Access, double-click the **AS400 Operations Navigator** icon on your desktop to access Operations Navigator and create an AS/400 connection.

Prerequisite and related information

Use the AS/400 Information Center as your starting point for looking up AS/400 technical information. You can access the Information Center from the AS/400e Information Center CD-ROM (English version: *SK3T-2027*) or from one of these Web sites:

http://www.as400.ibm.com/infocenter

The AS/400 Information Center contains important topics such as logical partitioning, clustering, Java, TCP/IP, Web serving, and secured networks. It also contains Internet links to Web sites such as the AS/400 Online Library and the AS/400 Technical Studio. Included in the Information Center is a link that describes at a high level the differences in information between the Information Center and the Online Library.

For a list of related publications, see "Where to Get More Information and Assistance" on page 235.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other AS/400 documentation, fill out the readers' comment form at the back of this book.

- If you prefer to send comments by mail, use the readers' comment form with the address that is printed on the back. If you are mailing a readers' comment form from a country other than the United States, you can give the form to the local IBM branch office or IBM representative for postage-paid mailing.
- If you prefer to send comments by FAX, use either of the following numbers:
  - United States and Canada: 1-800-937-3430
  - Other countries: 1-507-253-5192
- If you prefer to send comments electronically, use one of these e-mail addresses:
  - Comments on books:

    RCHCLERK@us.ibm.com

    IBMMAIL, to IBMMAIL(USIB56RZ)
  - Comments on the AS/400 Information Center:

    RCHINFOC@us.ibm.com

Be sure to include the following:

- The name of the book.
- The publication number of the book.
- The page number or topic to which your comment applies.

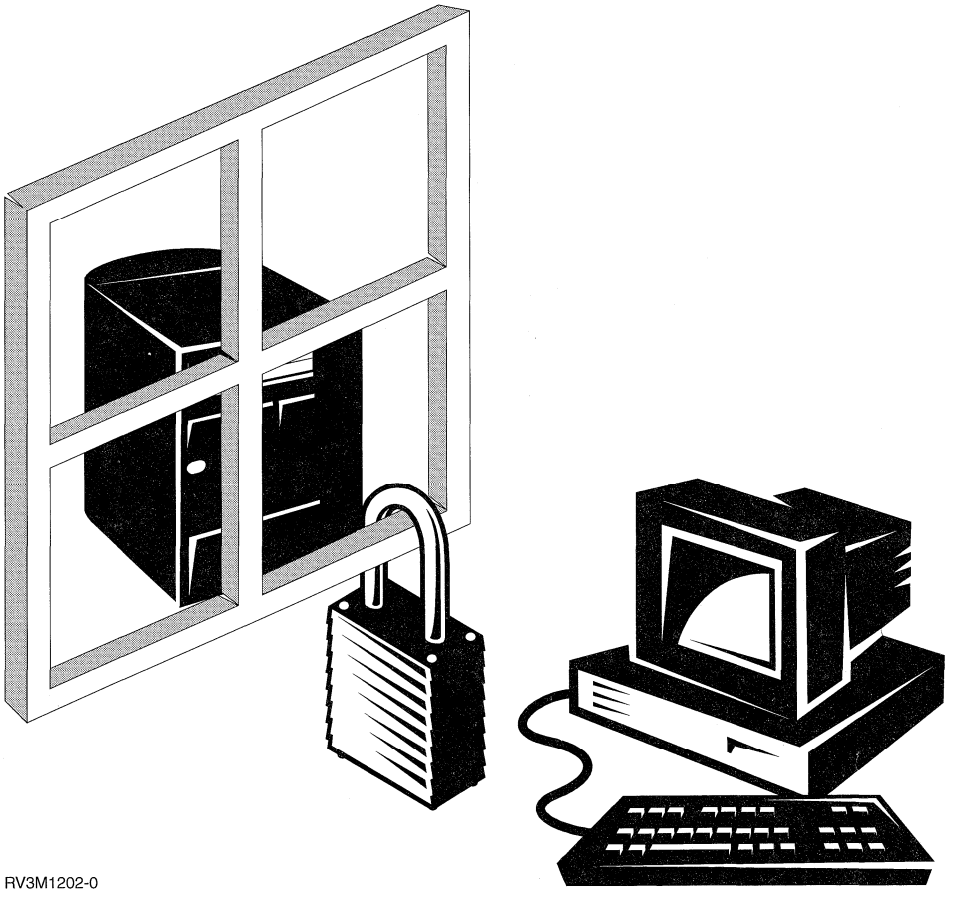
Summary of Changes

This is the sixth edition of *Tips and Tools for Securing Your AS/400*. This edition supports the versions V4R1, V4R2, V4R3, and V4R4 of OS/400. See "Chapter 1. AS/400 Security Enhancements" on page 3, for a description of new information.

Other minor technical and wording changes have been made throughout this book. A vertical line (|) to the left of the text indicates a change or addition.

Part 1. Read this First

By the pricking of my thumbs,
Something wicked this way comes.
Open, locks,
Whoever knocks!
Shakespeare Macbeth



RV3M1202-0

Chapter 1. AS/400 Security Enhancements

This section provides an overview of recent changes to AS/400 security.

Security Enhancements for V4R4

Following are security-relevant enhancements that are part of V4R4:

- ***Virtual Private Network (VPN):*** Native VPN on OS/400 allows you to selectively protect your Transmission Control Protocol/Internet Protocol (TCP/IP) applications.
- ***Additional Secure Sockets Layer (SSL) support:*** Beginning with V4R4, you can use SSL to encrypt communications between Telnet clients and your AS/400 server. Also beginning with V4R4, all Client Access Express functions except MAPI can communicate over SSL. Client Access Express allows SSL communications with the AS/400 server at three levels of encryption (40-bit, 56-bit, 128-bit).
- ***System state programs and objects that adopt allowed when loading PTFs:*** A new value, *ALWPTF, has been added to the system value QALWOBJRST. When you specify this value, system state programs and objects that adopt are allowed onto your system when loading PTFs.

Security Enhancements for V4R3

Following are security-relevant enhancements that are part of V4R3:

Limit access to program function: Beginning with V4R3, you can limit which users can access program function. Program function may be an application, parts of an application, or different functions within a program. This support is not a replacement for resource security; it is another method to helps you control access to your system. For more information see, "Limit Access to Program Function" on page 15.

Operations Navigator Application Administration: You can use the Application Adminsitration support of the *OpNav* to manage user access to program function. See "Security and Operations Navigator" on page 169 for details.

AS/400e Security Advisor: The AS/400e Security Advisor is a browser-based tool that provides recommendations for most of the crucial system values you use. If you are a new AS/400 user or your environment has changed, you can also use the AS/400e Security Advisor to generate a list of recommendations that you can use to plan and create your security policies. See "AS/400e Security Advisor" on page 22 for details.

AS/400 Security Wizard: The AS/400e Security Wizard help you configure security on your AS/400 by asking a series of questions about your business. After your responses to the questions are *processed* by the wizard, a panel is displayed with information about implementing security. You can use the AS/400 Security Wizard to configure:

- Security-related system values and network attributes
- Security-related reporting for monitoring the system
- Command defaults for creating user profiles

See "Chapter 4. AS/400e Security Wizard and Security Advisor" on page 21 for details.

Print Profile Internals (PRTPRFINT) command: You can use the Print Profile Internals command to print a report containing information on the number of entries contained in a user profile.

Print Private Authority (PRTPVTAUT) command and Print Public Authority command (PRTPUBAUT): You can now use the PRTPVTAUT and the PRTPUBAUT command to manage authorities for objects in the integrated file system.

Restore User Profile (RSTUSRPRF) command: *ALLOBJ special authority is no longer removed from user profiles in some cases. It is removed when a user profile is restored to a system at security level 30 or higher in either of these situations:

- The profile was saved from a different system, and the user performing the RSTUSRPRFF does not have *ALLOBJ and *SECADM special authorities.
- The profile was saved from the same system at security level 10 or 20.

It is never removed from these IBM-supplied user profiles:

- QSYS (system)
- QSECOFR (security officer)
- QLPAUTO (licensed program-automatic install)
- QLPINSTALL (licensed program install)

Internet Protocol (IP) Packet Filtering: This provides the ability to selectively block IP traffice based on information in the IP and protocol specific packet headers. See the "Chapter 13. Tips for Securing TCP/IP Communications" on page 123 for details.

HTTP proxy server: The HTTP proxy server comes with the IBM HTTP Server for AS/400. The proxy server receives HTTP requests from Web browsers and resends them to Web Servers. See the "Chapter 13. Tips for Securing TCP/IP Communications" on page 123 for details.

NAT (network address translation): Network Address Translation (NAT) modifies the source or the destination IP addresses of packets that flow through the system. Using NAT, you can use the AS/400 system as a gateway between two networks which have conflicting or incompatible addressing schemes. You can also use NAT to hide the real IP addresses of one network by dynamically substituting a different address. See the "Chapter 13. Tips for Securing TCP/IP Communications" on page 123 for details.

VPN on the IBM Firewall for AS/400: IBM Firewall for AS/400 provides virtual private network (VPN) technologies. When you use VPNs, you can create encrypted connections between the firewall and several other IBM firewall products.

HTTP Server for AS/400: The Internet Connection Server (ICS) is now known as IBM HTTP Server for AS/400. There is no longer a separate Secure HTTP Server product. Instead, to enable SSL on your AS/400, you must install one of the following cryptographic products:

- 5769–AC1
- 5769–AC2
- 5769–AC3

Once you have installed one of these products, SSL is enabled for all products that use SSL, including the HTTP Server.

Security Enhancements for V4R2

Following are security-relevant enhancements that are part of V4R2:

Column-level authority for database files: Beginning with V4R2, you can specify authorities for specific fields in a DB2/400 file. DB2/400 supports the following field-level authorities:

Update authority:
You can specify which users can make changes to the value of a field.

References authority:
You can control which users can specify a field as a parent key in a referential constraint.

The capability to grant and revoke field-level authority is available through SQL statements. You can use the Display Object Authority (DSPOBJAUT) command to view the field-level authorities for a file. For more information about field-level authority, see the *DB2 UDB for AS/400 SQL Reference* book.

TELNET exit points: Beginning with V4R2, two exit points are available for TELNET: session initiation and session end. These exit points provide you with the capability to both control and monitor TELNET access to your system. Following are examples of possible actions you can take in your TELNET user-written exit program:

- Accept or deny a session request
- Assign a specific AS/400 device description to the request
- Assign a specific user profile for the session
- Log connections and disconnections from the system through the TELNET server

"Security Tips for TELNET" on page 132 in this book and the *TCP/IP Configuration and Reference* book provide more information about the new TELNET exit points.

Point-to-point protocol (PPP): Beginning with V4R2, TCP/IP includes support for PPP. PPP provides increased performance and enhanced security capabilities when compared to SLIP. With PPP, user authentication is architected and not dependent on user-created scripts. Encryption of user names and passwords is available when both sides in a connection support it. PPP also supports IP address validation. This ensures that a user has an address within a specified range to protect against IP spoofing. PPP also provides the ability to configure your connection profile to periodically rechallenge to protect against session piggy-backing.

"Security Considerations for Point-to-Point Protocol" on page 131 in this book and the *TCP/IP Configuration and Reference* book provide more information about PPP.

Password caching for Windows 95 clients:The Windows 95 client for Client Access provides the capability to save passwords to the Windows 95 password cache (with a Save Password checkbox at sign-on). It also provides the capability to clear passwords from the cache (with a Clear Passwords button). It removes all Client Access passwords from the Windows 95 password cache. When you uninstall Client Access, the process also clears all Client Access passwords from the Windows 95 password cache.

Security Enhancements for V4R1

Following are security-relevant enhancements that are part of V4R1:

Internet Connection Server: With V4R1, the TCP/IP HTTP server is reintroduced as the Internet Connection Server (ICS). The ICS provides both enhanced function (over the HTTP server) and compatibility across multiple IBM platforms. It also provides new security capabilities:

- New directives allow you to require authentication (user ID and password) before accepting requests for some or all of your ICS resources (URLs and CGI programs). You can use either normal AS/400 user profiles or a new AS/400 validation object to provide the authentication.
- With new directives, you can also swap to a different AS/400 user profile before accessing ICS resources (instead of using the default user profiles that are provided with the server). With this capability, you can, for example, take advantage of AS/400 resource security when you serve multiple Web sites on the same system.

"Security Tips for Web Serving from AS/400" on page 150 provides more information about the security considerations for this new server. *HTTP Server for AS/400 Webmaster's Guide* describes how to configure and manage the new server.

Internet Connection Secure Server: With V4R1, the new Internet Connection Secure Server (ICSS) provides the capability to establish a secure connection between your AS/400 and an SSL-enabled browser. The ICSS uses the Secure Sockets Layer (SSL) protocol to authenticate servers and to encrypt the transmitted data. (Most popular Web browsers are SSL-enabled.) The Internet Connection Secure Server provides the foundation for secure electronic commerce using an AS/400 server.

"Security Tips for Using SSL with IBM HTTP Server for AS/400" on page 156 provides more information about the security considerations for this new server. *HTTP Server for AS/400 Webmaster's Guide* describes how to configure and manage the new server.

Firewall for AS/400: The IBM Firewall for AS/400 (5769-FW1) is a software product that enables the Integrated Netfinity Server for AS/400 on your AS/400 to perform the functions of a firewall. The firewall separates your internal (secure) network from an external (non-secure) network (usually the Internet). You can run the IBM Firewall for AS/400 on your production AS/400 system (to protect both your production system and other connected systems). For maximum security protection, you would normally use a separate, dedicated AS/400 system as your Internet server. You might also choose to run the firewall on a multi-use AS/400 system that runs your production applications and provides Internet services. However, the success of this implementation depends heavily upon both your application design and the thoroughness of your configuration rules.

The IBM Firewall for AS/400 provides the following capabilities:

- Packet filtering support TCP, UDP and ICMP. Dynamic packet filtering support for RealAudio (Progressive Networks).
- A domain name server
- Proxy servers for common applications such as HTTP, TELNET, and FTP.
- A socks server that is application-independent.

- A mail server.
- Extensive logging and monitoring.
- Administration through a Web browser.

For the AS/400 administrator, the IBM Firewall for AS/400 provides the advantage of using technology and an environment that you already understand. It provides an economical method to protect your internal network as you branch out to connect to other, non-secure networks. *Getting Started with IBM Firewall for AS/400* provides complete information about how to set up the firewall and how to use it capabilities. The Firewall for AS/400 web site provides current information, tips, and frequently asked questions. Visit the Web site at the following URL:

`http://www.as400.ibm.com/firewall`

Net.Commerce for AS/400: The Internet Connection Server and the Internet Connection Secure Server provide the foundations for electronic commerce on your AS/400. Two new licensed programs provide you with tools to develop a full-function shopping mall on your Web site.

- IBM Net.Commerce for AS/400 (5798-NC2) provides tools for you to design and administer your Web site. You can create and maintain product catalogs and use a shopping basket metaphor for your Web-site visitors.

For the latest information about IBM's electronic commerce offerings, visit the following Web site:

`http://www.internet.ibm.com/commercepoint/net.commerce/`

TCP/IP Exit Points: Beginning with V4R1, more TCP/IP applications use the exit points that were previously available only for the FTP server. You can now use exit programs to control activity for both the REXEC server and the TFTP server.

"Tips for Controlling FTP Access" on page 138 provides an overview of the exit points. "TCP/IP User Exits" in the *TCP/IP Configuration and Reference* book provides more information about how to use the FTP exit points.

Chapter 2. C2 Security

By using security level 50 and following the instructions in the *Security–Enabling for C2* book, you can bring your AS/400 system to a C2 level of security. C2 is a security standard defined by the U.S. government in the *Department of Defense Trusted System Evaluation Criteria* (DoD 5200.28.STD).

In October, 1995, AS/400 formally received its first C2 security rating from the United States Department of Defense. This original C2 security rating is for V2R3 of OS/400, Source Entry Utility, Query/400, SAA Structured Query Language/400, and Common Cryptographic Architecture Services/400. The C2 security rating was awarded after a rigorous, multi-year period of evaluation. AS/400 is the first system to achieve a C2 security rating for a system (hardware and operating system) with an integrated, full-function database.

Since receiving its initial C2 rating, IBM has continued to pursue C2 ratings for additional AS/400 hardware and OS/400 releases through the United States Department of Defense's RAMP (Ratings Maintenance Phase) process. To date, AS/400 has received C2 ratings for Version 3 Release 0 Mod 5 (V3R0M5), Version 3 Release 2 (V3R2) and Version 4 Release 1 (V4R1). IBM plans to continue to pursue C2 ratings for AS/400.

To achieve a C2 rating, a system must meet strict criteria in the following areas:

- Discretionary access control
- User accountability
- Security auditing
- Resource isolation

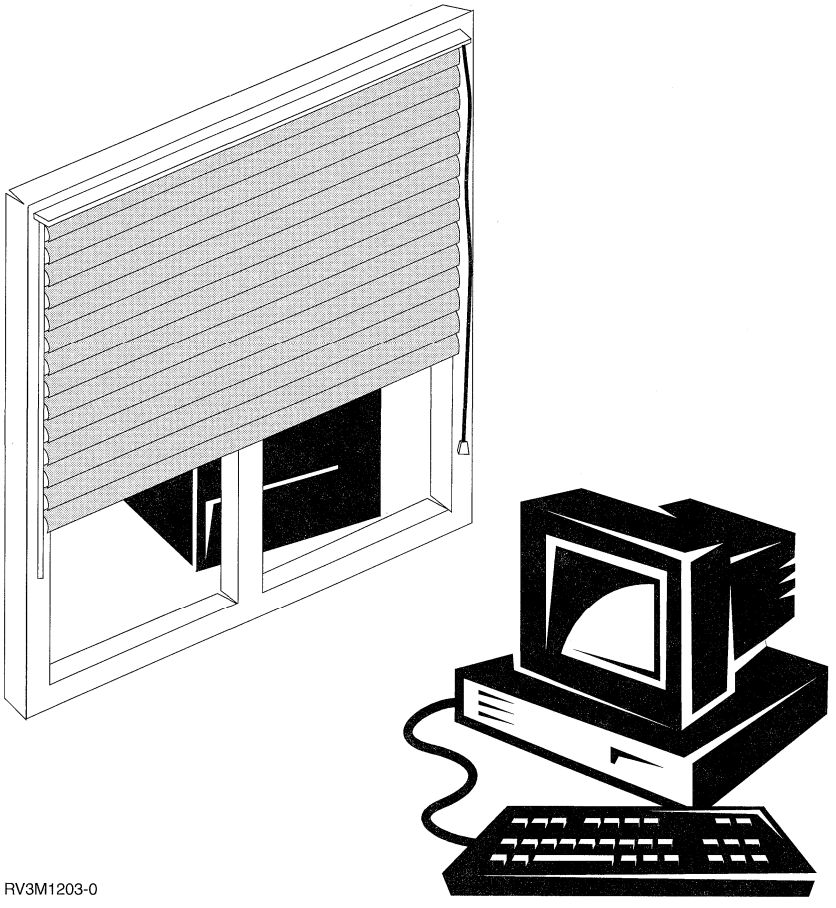
Part 2. Tips for Basic AS/400 System Security

Curiosity is one of the permanent and certain characteristics of a vigorous mind.

Samuel Johnson: The Rambler

While we stop to think, we often miss our opportunity.

Publilius Syrus: Maxim 185



RV3M1203-0

Chapter 3. Basic Elements of AS/400 Security

This chapter provides a brief review of the basic elements that work together to provide AS/400 security. Each topic in this chapter tells where you can find out more information. The other chapters of this book go beyond the basics to provide tips for using these security elements to meet the needs of your organization.

Security Levels

You can choose how much security you want the system to enforce by setting the security level (QSECURITY) system value. The system offers five levels of security:

Level 10:

The system does not enforce any security. No password is necessary. If the specified user profile does not exist on the system when someone signs on, the system creates one.

ATTENTION:

Beginning in V4R3, you cannot set the QSECURITY system value to 10. If your system is currently at security level 10, it will remain at level 10 when you install Version 4 Release 3. If you change the security level to some other value, you cannot change it back to level 10. Because level 10 provides no security protection, security level 10 is not recommended by IBM. **IBM will not provide support for any problems that occur at security level 10 unless the problem can also be created at a higher security level.**

Level 20:

The system requires a user ID and password for signing on. Security level 20 is often referred to as **sign-on security**. By default, all users have access to all objects because all users have *ALLOBJ special authority.

Level 30:

The system requires a user ID and password for signing on. Users must have authority to use objects because users do not have any authority by default. This is called **resource security**.

Level 40:

The system requires a user ID and password for signing on. In addition to resource security, the system provides **integrity protection** functions. The integrity protection functions are intended to protect both your system and the objects on your system from tampering by experienced system users. For most installations, level 40 is the recommended security level. When you receive a new AS/400 system with V3R7 or a later release, the security level is set to 40.

Level 50:

The system requires a user ID and password for signing on. The system enforces both resource security and the integrity protection of level 40. Security level 50 adds **enhanced integrity protection**, such as the following:

- Validation of parameters for interfaces to the operating system.
- Restriction of message-handling between system state programs and user state programs.

Security level 50 is intended for AS/400 systems with high security requirements.

Chapter 2 of the *Security - Reference* provides more information about the security levels and describes how to move from one security level to another.

Global Settings

Your system has global settings that affect how work enters the system and how the system appears to system users. These settings include the following:

System values:
Several topics in this book discuss the security implications of specific system values. Chapter 3 in the *Security - Reference* book describes all the security-relevant system values.

Network attributes:
Network attributes control how your system participates (or chooses not to participate) in a network with other systems. You can read more about network attributes in the *Work Management* book.

Subsystem descriptions and other work management elements:
Work management elements determine how work enters the system and what environment the work runs in. Several topics in this book discuss the security implications of some work management values. The *Work Management* book provides complete information.

Communications configuration:
Your communications configuration also affects how work enters your system. Several topics in this book provide suggestions for protecting your system when it participates in a network. The topic "Related Publications" on page 237 describes where you can read more about specific communications methods.

User Profiles

Every system user has a user profile. At security level 10 (which is not supported beginning with V4R3), the system automatically creates a profile when a user first signs on. At higher security levels, you must create a user profile before a user can sign on.

The user profile is a powerful and flexible tool. It controls what the user can do and customizes the way the system appears to the user. Chapter 4 in the *Security - Reference* book describes all the parameters in the user profile.

Group Profiles

A group profile is a special type of user profile. You can use a group profile to define authority for a group of users, rather than giving authority to each user individually. You can also use a group profile as a pattern when you create individual user profiles by using the copy-profile function.

Chapter 5 and Chapter 7 in the *Security - Reference* book provide more information about planning and using group profiles.

Resource Security

Resource security on the system allows you to define who can use objects and how those objects can be used. The ability to access an object is called **authority**. When you set up object authority, you can specify detailed authorities, such as adding records or changing records. Or you can specify the system-defined subsets of authorities: *ALL, *CHANGE, *USE, and *EXCLUDE.

Files, programs, libraries, and directories are the most common objects that require security protection, but you can specify authority for any object on the system.

Chapter 7. Using Object Authority to Protect Information Assets discusses the importance of setting up object authority on your system. Chapter 5 of the *Security - Reference* book describes the options for setting up resource security.

Limit Access to Program Function

The limit access to program function allows you to provide security to some portion of an application program when you do not have an AS/400 object to secure. Before the limit access to program function support was added in V4R3, you could accomplish this by creating an authorization list or other object, and checking the authority to the object to control access to the program function. Now you can use the limit access to program function to more easily control access to an application, parts of an application, or functions within a program.

There are two methods that you can use to manage user access to application functions through Operations Navigator. The first uses Application Administration support:

1. Right-click the AS/400 running your application.
2. Click **Application Administration**. This opens a window which contains lists of registered functions for Operations Navigator, host applications, and client applications (see Figure 2 on page 16).

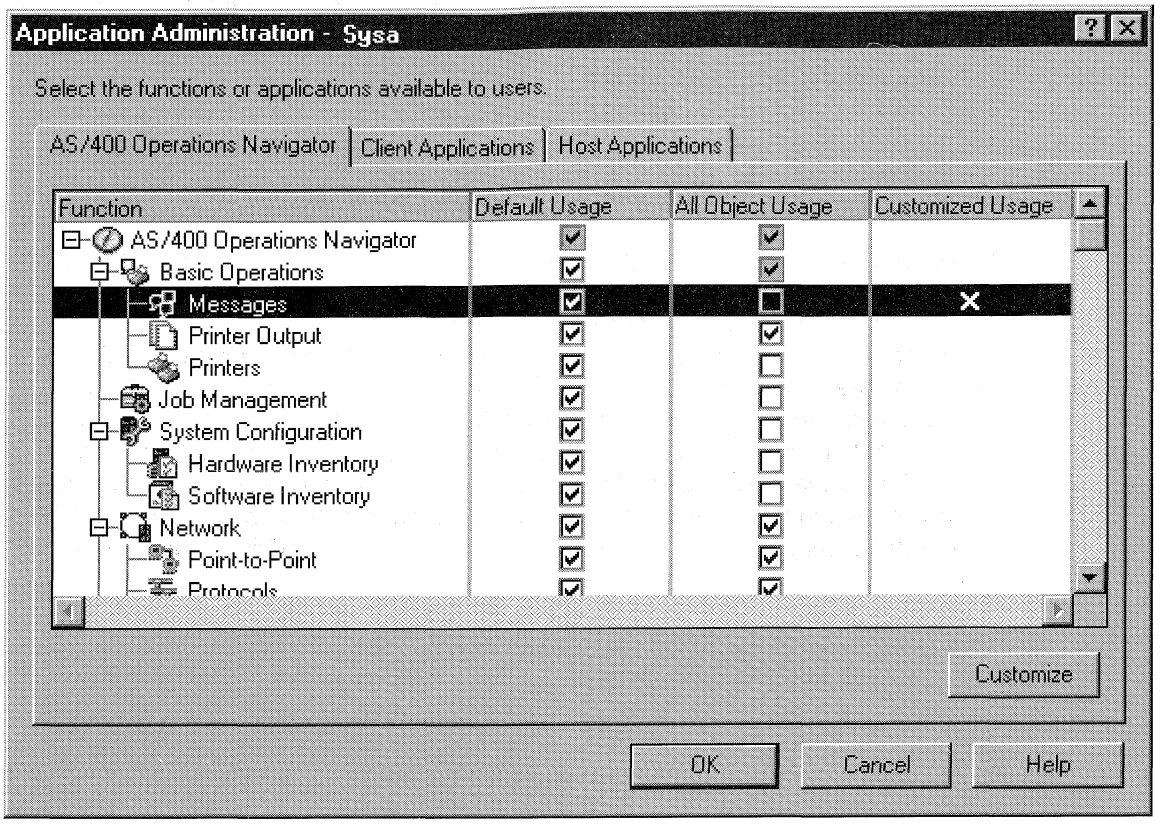


Figure 2. Application Administration

3. From the Application Administration window, change the default usage setting and the allow *ALLOBJ indicator as desired.

   Note: When a function has a list of users that have been given or denied access to the function, the Customized Usage column contains an X.
4. Highlight a function to enable the **Customize** button.
5. Click the **Customize** button to display the Customize Usage dialog box.
6. Within the **Customize Usage** dialog box, change the list of users and groups allowed or denied access to the function.

The second method of managing user access involves Operations Navigator's Users and Groups support:

1. Access the **Properties** window for a user or group.
2. Click the **Capabilities** button.
3. Choose the **Applications** tab. This displays a list of registered functions and the access (or usage) the user or group has to each function.

   The **Usage Derived From** column shows where the access is from.
4. At the **Capabilities** window, change the user's settings for the listed functions. From this window you can also do the following:
   - Change the settings for all functions in a hierarchy grouping by changing the setting for the "parent" function.
   - Manage access to functions using group profiles.

See "Security and Operations Navigator" on page 169 for more information on Operations Navigator security issues.

If you are an application writer, you can use limit access to program function APIs to do the following:

- Register a function
- Retrieve information about the function
- Define who can or cannot use the function
- Check to see if the user is allowed to use the function

Note: This support is **not** a replacement for resource security. Limit access to program function does not prevent a user from accessing a resource (such as a file or program) from another interface.

To use this support within an application, the application provider must register the functions when the application is installed. The registered function corresponds to a code block for specific functions in the application. When the application is run by the user, the application calls the API before the application calls the code block. The API calls the check usage API to see if the user is allowed to use the function. If the user is allowed to use the registered function, the code block is run. If the user is not allowed to use the function, the user is prevented from running the code block.

The system administrator specifies who is allowed or denied access to a function. The administrator can either use the API to manage the access to program function or use the Operations Navigator Application Administration GUI. The *System API Reference* book provides information about the limit access to program function API's. For additional information about controlling access to functions, see "Security and Operations Navigator" on page 169.

Security Auditing

Several functions exist on the system to help you audit the effectiveness of security. In particular, the system provides the ability to log selected security-related events in a security audit journal. Several system values, user profile values, and object values control which events are logged.

Chapter 9 of the *Security - Reference* book provides information about auditing security.

System Security Attributes Report–Example

Figure 3 on page 18 shows an example of the output from the Print System Security Attributes (PRTSYSSECA) command. The report shows the settings for security-relevant system values and network attributes that are recommended for systems with normal security requirements. It also shows the current settings on your system.

Note: The *Current Value* column on the report shows the current setting on your system. Compare this to the recommended value to see where you may have security exposures.

```
System Security Attributes

System Value
Name            Current value          Recommended value
QALWOBJRST      *NONE                  *NONE
QALWUSRDMN      *ALL                   QTEMP
QATNPGM         QEZMAIN   QSYS         *NONE
QAUDENDACN      *NOTIFY                *NOTIFY
QAUDFRCLVL      *SYS                   *SYS
QAUDCTL         *AUDLVL                *AUDLVL   *OBJAUD
QAUDLVL         *SECURITY              *AUTFAIL  *CREATE
                                       *DELETE   *SECURITY
                                       *SAVRST   *NOQTEMP
```

Figure 3. System Security Attributes Report-Sample (Part 1 of 4)

```
QAUTOCFG        0                      0
QAUTOVRT        9999                   0
QCMNRCYLMT      0 0                    0 0
QCRTAUT         *CHANGE                Control at library level.
QCRTOBJAUD      *NONE                  Control at library level.
QDEVRCYACN      *DSCMSG                *DSCMSG
QDSCJOBITV      120                    120
QDSPSGNINF      1                      1
QINACTITV       60                     60
QINACTMSGQ      *ENDJOB                *ENDJOB
QLMTDEVSSN      0                      1
QLMTSECOFR      0                      1
QMAXSGNACN      2                      3
QMAXSIGN        3                      3
```

Figure 3. System Security Attributes Report-Sample (Part 2 of 4)

```
QPWDEXPITV      60                     60
QPWDLMTAJC      1                      1
QPWDLMTCHR      *NONE                  AEIOU@$#
QPWDLMTREP      1                      2
QPWDMAXLEN      8                      8
QPWDMINLEN      6                      6
QPWDPOSDIF      1                      1
QPWDRQDDGT      1                      1
QPWDRQDDIF      0                      1
QPWDVLDPGM      *NONE                  *NONE
QRETSVRSEC      0                      0
QRMTIPL         0                      0
QRMTSIGN        *FRCSIGNON             *FRCSIGNON
QSECURITY       50                     50
QSRVDMP         *DMPUSRJOB             *NONE
```

Figure 3. System Security Attributes Report-Sample (Part 3 of 4)

System Security Attributes

Network Attribute Name	Current value	Recommended value
DDMACC	*OBJAUT	*REJECT
JOBACN	*FILE	*REJECT
PCSACC	*OBJAUT	*REJECT

Figure 3. System Security Attributes Report-Sample (Part 4 of 4)

Chapter 4. AS/400e Security Wizard and Security Advisor

The AS/400e Security Wizard and Security Advisor tools can help you decide what security values to put into effect on your AS/400 system.

AS/400e Security Wizard

Deciding which AS/400 system security values you should use for your business can be perplexing. If you are new to AS/400, new to security implementation on AS/400, or the environment in which you run your AS/400 has recently changed, the AS/400e Security Wizard can help you with decisions. The Security Wizard asks you several questions about your business, then based on your answers does the following things:

- Generates an Administrator Information Report and a User Information Report:
  - The Administrator Information Report contains recommended security settings and any procedures that should be followed prior to putting the recommendations into effect.
  - The User Information Report contains information that can be used for the business security policy. For example, password compositions rules are included in this report.
- Recommends settings for various security-related items on the system. These items put basic security policy into effect on your system.
- Recommends audit journal reports that you should schedule to run periodically. When scheduled, these reports help:
  - Ensure that security policies are followed.
  - Ensure that security policies are only changed with your approval.
  - Schedule reports to monitor security-related events on your system.
- Allows you to save the recommendations or to apply some or all of the recommendations to your system.

To access the Security Wizard, do the following:

1. Double-click the **Operations Navigator** icon to open Operations Navigator.

   Note: To use AS/400 Operations Navigator, you must have Client Access installed on your Windows 95/NT PC and have an AS/400 connection from that PC. For help in connecting your Windows 95/NT PC to your AS/400 system, consult *Client Access for Windows 95/NT - Setup*, SC41-3512-05 .

2. Right-click on the **Security** folder, then select **configure** to start the Security Wizard.

The Security Wizard will present you with one of three welcome screens. Which screen you see depends on which of the following conditions exists:

- The wizard has never been run for the target AS/400.
- The wizard has been run before and the security changes were deferred.
- The wizard has been run before and the security changes were put into effect.

AS/400e Security Advisor

The Security Advisor is an online version of the Security Wizard. To access the Security Advisor point your Internet browser to the following URL:

`http://www.as400.ibm.com/tstudio/secure1/index_av.htm`

The Security Advisor is part of the AS/400e Technical Studio. This Web site answers many of your security questions and offers timely information on workshops, classes, and other resources. The URL for the Technical Studio address is:

`http://www.as400.ibm.com/techstudio`

The URL for the AS/400 Security section of the Technical Studio is:

`http://www.AS400.ibm.com/tstudio/secure1/secdex.htm`

The Security Advisor asks the same questions as the Security Wizard and, based on your answers, generates the same recommendations. The main differences between the two tools are that:

- The Security Advisor does not generate the Administrator Information Report and the User Information Report.
- You cannot apply recommendations automatically from the Security Advisor.

The Security Advisor generates a CL program that you can cut-and-paste and edit for your own use to automate security configuration. You can also link directly to the AS/400 documentation from the Security Advisor. This provides information about the system value or report that can help you determine if this setting is appropriate for your environment.

Chapter 5. Tips for Controlling Interactive Sign-On

When you think about restricting entry to your system, start with the obvious, the Sign On display. Following are steps that you can take to make it difficult for an outsider to walk up (or dial up) and sign on to your system by using the Sign On display.

Setting Password Rules

Set a policy that states that passwords must not be trivial and must not be shared. Set system values to help you with enforcement. Table 1 shows recommended system value settings.

The combination of values in Table 1 is fairly restrictive and is intended to significantly reduce the likelihood of trivial passwords. However, your users may find it difficult and frustrating to select a password that meets these restrictions. Consider providing users with the following:

- A list of the criteria for passwords.
- Examples of passwords that are and are not valid.
- Suggestions for how to think of a good password.

You can run the Configure System Security (CFGSYSSEC) command to set these values. You can use the Print System Security Attributes (PRTSYSSECA) command to print your current settings for these system values.

You can read more about these system values in Chapter 3 of the *Security - Reference* book. "Values That Are Set by the Configure System Security Command" on page 43 provides more information about the CFGSYSSEC command.

Table 1. System Values for Passwords

System Value Name	Description	Recommended Value
QPWDEXPITV	How often the system users must change their passwords. You can specify a different value for individual users in the user profile.	60 (days)
QPWDMINLEN	The minimum number of characters in a password.	6
QPWDMAXLEN	The maximum number of characters in a password.	8
QPWDRQDDIF	How long a user must wait before using the same password again.	5 or less (expiration intervals)[1]
QPWDLMTCHR	What characters may not be used in passwords.	AEIOU#$@
QPWDLMTAJC	Whether the system prevents adjacent characters that are the same.	1 (yes)
QPWDLMTREP	Whether the system prevents the same character from appearing more than once in the password.	2 (not allowed consecutively)
QPWDPOSDIF	Whether each character in a password must be different from the character in the same position on the previous password.	1 (yes)
QPWDRQDDGT	Whether the password must have at least one numeric character.	1 (yes)
QPWDVLDPGM	What exit program is called to validate a newly assigned password.	*NONE

Table 1. System Values for Passwords (continued)

System Value Name	Description	Recommended Value

Notes:

1. The QPWDEXPITV system value specifies how often you must change your password, such as every 60 days. This is the **expiration interval**. The QPWDRQDDIF system value specifies how many expiration intervals must pass before you can use the same password again. Chapter 3 of the *Security - Reference* book provides more information about how these system values work together.

Changing Well-Known Passwords

Do the following to close some well-known entrances into AS/400 that may exist on your system.

__ Step 1. Make sure that no user profiles still have default passwords (equal to the user profile name). You can use the Analyze Default Passwords (ANZDFTPWD) command. (See "Avoiding Default Passwords" on page 30.)

__ Step 2. Try to sign on to your system with the combinations of user profiles and passwords that are shown in Table 2 on page 26. These passwords are published, and they are the first choice of anyone who is trying to break into your system. If you can sign on, use the Change User Profile (CHGUSRPRF) command to change the password to the recommended value.

__ Step 3. Now start Dedicated Service Tools (DST) and try to sign on with the passwords that are shown in Table 3 on page 26.

You start DST by using one of the following methods:

- Perform an IPL with the system in `Manual` mode and select Dedicated Service Tools from the IPL or Install the System menu.
- Place the console in DST mode by doing the following:
  - __ Step a. Make sure that all jobs at the console are ended.
  - __ Step b. Place the system unit in manual mode.
  - __ Step c. Use the system panel to select function 21.
  - __ Step d. Press the enter button on the system panel.
  - __ Step e. From the IPL of Install the System menu, select DST.

__ Step 4. If you can sign on to DST with any of these passwords, change the passwords by doing the following:

__ Step a. From the Dedicated Service Tools (DST) menu, select option 5 (Work with DST environment):

__ Step b. From the Work with DST Environment menu, select option 11 (Change DST Passwords).

Note: The menu option numbers may be different on your system, depending on the release of OS/400 that you are running.

Remember the new passwords

Write down the passwords that you select and store them in a safe place. You or your hardware service representative may need these passwords to work on your system in the future.

__ Step c. From the Change DST Passwords menu, select option 3 (Change the DST security capability password).

Note: DST full capability has the user ID of QSECOFR. You can change this user ID if you want, but be sure to write down the new user ID.

__ Step d. On the Change DST Security Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ Step e. Press the Enter key.

__ Step f. From the Change DST Passwords menu, select option 2 (Change the DST full capability password).

Note: DST full capability has the user ID of 22222222. You can change this user ID if you want, but be sure to write down the new user ID.

__ Step g. On the Change DST Full Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ Step h. Press the Enter key.

__ Step i. From the Change DST Passwords menu, select option 1 (Change the DST basic capability password).

Note: DST basic capability has the user ID of 11111111. You can change this user ID if you want, but be sure to write down the new user ID.

__ Step j. On the Change DST Basic Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ Step k. Press the Enter key.

__ Step l. Press F3 until you see the Dedicated Service Tools (DST) menu.

__ Step 5. Finally, make sure that you cannot sign on just by pressing the Enter key at the Sign On display without entering a user ID and password. Try several different displays. If you can sign on without entering information on the Sign On display, do one of the following:

- Change to security level 40 or 50 (QSECURITY system value).

  Note: Your applications might run differently when you change to security level 40 or 50 from a lower security level. Review the information in Chapter 2 of the *Security - Reference* book before you change to security level 40 or 50.

- Change all of the workstation entries for interactive subsystems to point to job descriptions that specify USER(*RQD).

Table 2. Passwords for IBM-Supplied Profiles

User ID	Password	Recommended Value
QSECOFR	QSECOFR[1]	A nontrivial value known only to the security administrator. **Write down the password that you have selected and store it in a safe place.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Notes:

1. Beginning with V3R2, the system arrives with the *Set password to expired* value for the QSECOFR set to *YES. The first time that you sign on to a new system, you must change the QSECOFR password.
2. The system needs these user profiles for system functions, but you should not allow users to sign on with these profiles. For new systems installed with V3R1 or later releases, this password is shipped as *NONE.

   When you run the CFGSYSSEC command, the system sets these passwords to *NONE.
3. To run AS/400 Client Access for Windows 95/NT using TCP/IP, the QUSER user profile must be enabled.

Table 3. Passwords for Dedicated Service Tools

DST Level	User ID[1]	Password	Recommended Value
Basic capability	11111111	11111111	A nontrivial value known only to the security administrator.[2]
Full capability	22222222	22222222	A nontrivial value known only to the security administrator.[2]
Security capability	QSECOFR	QSECOFR	A nontrivial value known only to the security administrator.[2]

Notes:

1. A user ID is only required for PowerPC AS (RISC) releases of the operating system.
2. If your hardware service representative needs to sign on with this user ID and password, change the password to a new value after the hardware service representative leaves.

Setting Sign-On Values

Table 4 shows several values that you can set to make it more difficult for an unauthorized person to sign on to your system. If you run the CFGSYSSEC command, it sets these system values to the recommended settings. You can read more about these system values in Chapter 3 of the *Security - Reference* book.

Table 4. Sign-On System Values

System Value Name	Description	Recommended Setting
QAUTOCFG	Whether the system automatically configures new devices.	0 (No)
QAUTOVRT	The number of virtual device descriptions that the system will automatically create if no device is available for use.	0

Table 4. Sign-On System Values (continued)

System Value Name	Description	Recommended Setting
QDEVRCYACN	What the system does when a device reconnects after an error.[1]	*DSCMSG
QDSCJOBITV	How long the system waits before ending a disconnected job.	120
QDSPSGNINF	Whether the system displays information about previous sign-on activity when a user signs on.	1 (Yes)
QINACTITV	How long the system waits before taking action when an interactive job is inactive.	60
QINACTMSG	What the system does when the QINACTITV time period is reached.	*DSCJOB
QLMTDEVSSN	Whether the system prevents a user from signing on at more than one work station at the same time.	1 (Yes)
QLMTSECOFR	Whether users with *ALLOBJ or *SERVICE special authority can sign on only at specific work stations.	1 (Yes)[2]
QMAXSIGN	Maximum consecutive, incorrect sign-on attempts (user profile or password is incorrect).	3
QMAXSGNACN	What the system does when the QMAXSIGN limit is reached.	3 (Disable both user profile and device)

Notes:

1. Beginning with V4R2, the system can disconnect and reconnect TELNET sessions when the device description for the session is explicitly assigned.
2. If you set the system value to 1 (Yes), you will need to explicitly authorize users with *ALLOBJ or *SERVICE special authority to devices. The simplest way to do this is to give the QSECOFR user profile *CHANGE authority to specific devices.

Changing Sign-On Error Messages

Hackers like to know when they are making progress toward breaking into a system. When an error message on the Sign On display says `Password not correct`, the hacker can assume that the user ID is correct. You can frustrate the hacker by using the Change Message Description (CHGMSGD) command to change the text for two sign-on error messages. Table 5 shows the recommended text.

Table 5. Sign-On Error Messages

Message ID	Shipped Text	Recommended Text
CPF1107	CPF1107 – Password not correct for user profile.	Sign-on information is not correct **Note:** Do not include the message ID in the message text.
CPF1120	CPF1120 – User `XXXXX` does not exist.	Sign-on information is not correct. **Note:** Do not include the message ID in the message text.

Scheduling Availability of User Profiles

You may want some user profiles to be available for sign-on only at certain times of the day or certain days of the week. For example, if you have a profile set up for a security auditor, you may want to enable that user profile only during the hours that the auditor is scheduled to work. You might also want to disable user profiles with *ALLOBJ special authority (including the QSECOFR user profile) during off-hours.

You can use the Change Activation Schedule Entry (CHGACTSCDE) command to set up user profiles to be enabled and disabled automatically. For each user profile that you want to schedule, you create an entry that defines the user profile's schedule.

For example, if you want the QSECOFR profile to be available only between 7 in the morning and 10 in the evening, you would type the following on the CHGACTSCDE display:

```
              Change Activation Scd Entry (CHGACTSCDE)

Type choices, press Enter.

User profile . . . . . > QSECOFR       Name
Enable time  . . . . . > '7:00'        Time, *NONE
Disable time . . . . . > '22:00'       Time, *NONE
Days . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                       > *TUE
                       > *WED
                       > *THU
               + for more values > *FRI
```

Figure 4. Schedule Profile Activation Display–Sample

In fact, you might want to have the QSECOFR profile available only for a very limited number of hours each day. You can use another user profile with the *SECOFR class to perform most system functions. Thus, you avoid exposing a well-known user profile to hacking attempts.

You can use the Display Audit Journal Entries (DSPAUDJRNE) command periodically to print the CP (Change Profile) audit journal entries. Use these entries to verify that the system is enabling and disabling user profiles according to your planned schedule.

Another method for checking to ensure that user profiles are being disabled on your planned schedule is to use the Print User Profile (PRTUSRPRF) command. When you specify *PWDINFO for the report type, the report includes the status of each selected user profile. If, for example, you regularly disable all user profiles with *ALLOBJ special authority, you can schedule the following command to run immediately after the profiles are disabled:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Removing Inactive User Profiles

Your system should contain only user profiles that are necessary. If you no longer need a user profile because the user either has left or has taken a different job within the organization, remove the user profile. If someone is gone from the organization for an extended period, disable (deactivate) that user's profile. An unnecessary user profile may provide unauthorized entry to your system.

Disabling User Profiles Automatically

You can use the Analyze Profile Activity (ANZPRFACT) command to regularly disable user profiles that have been inactive for a specified number of days. When you use the ANZPRFACT command, you specify the number of inactive days that the system looks for. The system looks at the last used date, the restore date, and the creation date for the user profile.

Once you have specified a value for the ANZPRFACT command, the system schedules a job to run weekly at 1 a.m. (starting with the day after you first specified a value). The job examines all profiles and disables inactive profiles. You do not need to use the ANZPRFACT command again unless you want to change the number of inactive days.

You can use the Change Active Profile List (CHGACTPRFL) command to make some profiles exempt from ANZPRFACT processing. The CHGACTPRFL command creates a list of user profiles that the ANZPRFACT command will not disable, no matter how long those profiles have been inactive.

When the system runs the ANZPRFACT command, it writes a CP entry in the audit journal for each user profile that is disabled. You can use the DSPAUDJRNE command to list the user profiles that are newly disabled.

Note: The system writes audit entries only if the QAUDCTL value specifies *AUDLVL and the QAUDLVL system value specifies *SECURITY.

Another method for checking to ensure that user profiles are being disabled on your planned schedule is to use the Print User Profile (PRTUSRPRF) command. When you specify *PWDINFO for the report type, the report includes the status of each selected user profile.

Removing User Profiles Automatically

You can use the Change Expiration Schedule Entry (CHGEXPSCDE) command to manage the removing or disabling of user profiles. If you know that a user is leaving for an extended period, you can schedule the user profile to be removed or disabled.

The first time that you use the CHGEXPSCDE command, it creates a job schedule entry that runs at 1 minute after midnight every day. The job looks at the QASECEXP file to determine whether any user profiles are scheduled for removal on that day.

With the CHGEXPSCDE command, you either disable or delete a user profile. If you choose to delete a user profile, you must specify what the system will do with the objects that the user owns. Before you schedule a user profile for deletion, you need to research the objects that the user owns. For example, if the user owns

programs that adopt authority, do you want those programs to adopt the ownership of the new owner? Or does the new owner have more authority than necessary (such as special authority)? Perhaps, you need to create a new user profile with specific authorities to own the programs that need to adopt authority.

You also need to research whether any application problems will occur if you delete the user profile. For example, do any job descriptions specify the user profile as the default user?

You can use the Display Expiration Schedule (DSPEXPSCD) command to display the list of profiles that are scheduled to be disabled or removed.

You can use the Display Authorized Users (DSPAUTUSR) command to list all of the user profiles on your system. Use the Delete User Profile (DLTUSRPRF) command to delete outdated profiles.

Security Note: You disable a user profile by setting its status to *DISABLED. When you disable a user profile, you make it unavailable for interactive use. You cannot sign on with or change your job to a disabled user profile. Batch jobs can run under a user profile that is disabled.

Avoiding Default Passwords

When you create a new user profile, the default is to make the password the same as the user profile name. This provides an opportunity for someone to enter your system, if someone knows your policy for assigning profile names and knows that a new person is joining your organization.

When you create new user profiles, consider assigning a unique, non-trivial password instead of using the default password. Tell the new user the password confidentially, such as in a "Welcome to the System" letter that outlines your security policies. Require the user to change the password the first time that the user signs on by setting the user profile to PWDEXP(*YES).

You can use the Analyze Default Passwords (ANZDFTPWD) command to check all the user profiles on your system for default passwords. When you print the report, you have the option of specifying that the system should take action (such as disabling the user profile) if the password is the same as the user profile name. The ANZDFTPWD command prints a list of the profiles that it found and any action that it took.

Note: Passwords are stored on your system in one-way encrypted form. They cannot be decrypted. The system encrypts the specified password and compares it to the stored password just as it would check a password when you sign on the system. If you are auditing authority failures (*AUTFAIL), the system will write a PW audit journal entry for each user profile that does *not* have a default password (for systems running V4R1 or earlier releases). Beginning with V4R2, the system does not write PW audit journal entries when you run the ANZDFTPWD command.

Monitoring Sign-On and Password Activity

If you are concerned about unauthorized attempts to enter your system, you can use the PRTUSRPRF command to help you monitor sign-on and password activity. Figure 5 shows an example of the report:

```
                                User Profile Information
                                                                    SYSTEM4
Report type  . . . . . . . . . . :   *PWDINFO
Select by  . . . . . . . . . . . :   *SPCAUT
Special authorities  . . . . . . :   *ALLOBJ     *SERVICE
QPWDEXPITV system value  . . . . :       60
User                        Not Valid         No       Previous     Password     Expiration     Password
Profile        Status       Sign-ons       Password     Sign-on      Changed       Interval      Expired
USERA          *DISABLED           1                   07/19/95     05/25/95      *SYSVAL         *YES
USERB          *ENABLED            2                   06/30/95     03/02/95      *SYSVAL         *YES
USERX          *DISABLED           0          X          / /        11/28/95      *SYSVAL         *NO
USERY          *ENABLED            0                   04/25/95     04/25/95      120             *YES
```

Figure 5. User Information Report–Password Information Example

Following are several suggestions for using this report:

- Determine whether the password expiration interval for some user profiles is longer than the system value and whether the longer expiration interval is justified. For example, in the report, USERY has a password expiration interval of 120 days.
- Run this report regularly to monitor unsuccessful sign-on attempts. Someone who is trying to break into your system may be aware that your system takes action after a certain number of unsuccessful attempts. Each night, the would-be intruder might try fewer times than your QMAXSIGN value to avoid alerting you to the attempts. However, if you run this report early each morning and notice that certain profiles often have unsuccessful sign-on attempts, you might suspect that you have a problem.
- Identify user profiles that have not been used for a long time or whose passwords have not been changed for a long time.

Tips for Storing Password Information

To support some network functions and communications requirements, AS/400 provides a secure method for storing passwords that can be decrypted. Your system uses these passwords, for example, to establish a SLIP connection with another system. ("Security and Dial-Out Sessions" on page 130 describes this use of stored passwords.)

AS/400 stores these special passwords in a secure area that is not accessible to any user programs or interfaces. Only explicitly authorized system functions can set these passwords and retrieve them.

For example, when you use a stored password for dial-out SLIP connections, you set the password with the system command that creates the configuration profile (WRKTCPPTP). You must have *IOSYSCFG to use the command. A specially coded connection script retrieves the password and decrypts it during the dial-out procedure. The decrypted password is not visible to the user or in any job log.

As a security administrator, you need to decide whether you will allow passwords that can be decrypted to be stored on your system. You use the Retain Server

Security Data (QRETSVRSEC) system value to specify this. The default is 0 (No). Therefore, your system will not store passwords that can be decrypted unless you explicitly set this system value.

If you have network or communications requirements for stored passwords, you should set appropriate policies and understand the policies and practices of your communications partners. For example, when you use SLIP to communicate with another AS/400, both systems should consider setting up special user profiles for establishing the sessions. The special profiles should have limited authority on the system. This limits the impact to your system if a stored password is compromised on a partner system.

Chapter 6. How to Set Up Your System to Use the Security Tools

This chapter describes how to set up your system to use the security tools that are part of Operating System/400.

Getting Started with the Security Tools

When you install OS/400, the security tools tools are ready to use. The topics that follow provide suggestions for operating procedures with the security tools.

Securing the Security Tools

When you install OS/400, the objects that are associated with the security tools are secure. To operate the security tools securely, avoid making authority changes to any security tool objects.

Following are the security settings and requirements for security tool objects:

- The security tool programs and commands are in the QSYS product library. The commands and the programs ship with the public authority of *EXCLUDE. Many of the security tool commands create files in the QUSRSYS library. When the system creates these files, the public authority for the files is *EXCLUDE.

  Files that contain information for producing changed reports have names that begin with QSEC. Files that contain information for managing user profiles have names that begin with QASEC. These files contain confidential information about your system. Therefore, you should not change the public authority to the files.
- The security tools use your normal system setup for directing printed output. These reports contain confidential information about your system. To direct the output to a protect output queue, make appropriate changes to the user profile or job description for users who will be running the security tools.
- Because of their security functions and because they access many objects on the system, the security tool commands require *ALLOBJ special authority. Some of the commands also require *SECADM, *AUDIT, or *IOSYSCFG special authority. To ensure that the commands run successfully, you should sign on as a security officer when you use the security tools. Therefore, you should not need to grant private authority to any security tool commands.

Avoiding File Conflicts

Many of the security tool report commands create a database file that you can use to print a changed version of the report. Commands and Menus for Security Commands tells the file name for each command. You can only run a command from one job at a time. Most of the commands now have checks that enforce this. If you run a command when another job has not yet finished running it, you will receive an error message.

Many print jobs are long-running jobs. You need to be careful to avoid file conflicts when you submit reports to batch or add them to the job scheduler. For example, you might want to print two versions of the PRTUSRPRF report with different selection criteria. If you are submitting reports to batch, you should use a job queue that runs only one job at a time to ensure that the report jobs run sequentially.

If you are using the job scheduler, you need to schedule the two jobs far enough apart that the first version completes before the second job starts.

Saving the Security Tools

You save the security tool programs whenever you run either the Save System (SAVSYS) command or an option from the Save menu that runs the SAVSYS command.

The security tool files are in the QUSRSYS library. You should already be saving this library as part of your normal operating procedures. The QUSRSYS library contains data for many licensed programs on your system. See the *Backup and Recovery* book for more information about what commands and options save the QUSRSYS library.

Commands and Menus for Security Commands

This section describes the commands and menus for security tools. Examples of how to use the commands are included throughout this book.

Two menus are available for security tools:

- The SECTOOLS (Security Tools) menu to run commands interactively.
- The SECBATCH (Submit or Schedule Security Reports to Batch) menu to run the report commands in batch. The SECBATCH menu has two parts. The first part of the menu uses the Submit Job (SBMJOB) command to submit reports for immediate processing in batch.

  The second part of the menu uses the Add Job Schedule Entry (ADDJOBSCDE) command. You use it to schedule security reports to be run regularly at a specified day and time.

Options on the Security Tools Menu

Following is the part of the SECTOOLS menu that relates to user profiles. To access this menu, type `GO SECTOOLS`

```
SECTOOLS                        Security Tools

Select one of the following:

  Work with profiles
     1. Analyze default passwords

     2. Display active profile list
     3. Change active profile list
     4. Analyze profile activity

     5. Display activation schedule
     6. Change activation schedule entry

     7. Display expiration schedule
     8. Change expiration schedule entry
     9. Print profile internals
```

Table 6 on page 35 describes these menu options and the associated commands:

Table 6. Tool Commands for User Profiles

Menu[1] Option	Command Name	Description	Database File Used
1	ANZDFTPWD	Use the Analyze Default Passwords command to report on and take action on user profiles that have a password equal to the user profile name.	QASECPWD[2]
2	DSPACTPRFL	Use the Display Active Profile List command to display or print the list of user profiles that are exempt from ANZPRFACT processing.	QASECIDL[2]
3	CHGACTPRFL	Use the Change Active Profile List command to add and remove user profiles from the exemption list for the ANZPRFACT command. A user profile that is on the active profile list is permanently active (until you remove the profile from the list). The ANZPRFACT command does not disable a profile that is on the active profile list, no matter how long the profile has been inactive.	QASECIDL[2]
4	ANZPRFACT	Use the Analyze Profile Activity command to disable user profiles that have not been used for a specified number of days. After you use the ANZPRFACT command to specify the number of days, the system runs the ANZPRFACT job nightly. You can use the CHGACTPRFL command to exempt user profiles from being disabled.	QASECIDL[2]
5	DSPACTSCD	Use the Display Profile Activation Schedule command to display or print information about the schedule for enabling and disabling specific user profiles. You create the schedule with the CHGACTSCDE command.	QASECACT[2]
6	CHGACTSCDE	Use the Change Activation Schedule Entry command to make a user profile available for sign on only at certain times of the day or week. For each user profile that you schedule, the system creates job schedule entries for the enable and disable times.	QASECACT[2]
7	DSPEXPSCD	Use the Display Expiration Schedule command to display or print the list of user profiles that are scheduled to be disabled or removed from the system in the future. You use the CHGEXPSCDE command to set up user profiles to expire.	QASECEXP[2]
8	CHGEXPSCDE	Use the Change Expiration Schedule Entry command to schedule a user profile for removal. You can remove it temporarily (by disabling it) or you can delete it from the system. This command uses a job schedule entry that runs every day at 00:01 (1 minute after midnight). The job looks at the QASECEXP file to determine whether any user profiles are set up to expire on that day. Use the DSPEXPSCD command to display the user profiles that are scheduled to expire.	QASECEXP[2]

Table 6. Tool Commands for User Profiles (continued)

Menu[1] Option	Command Name	Description	Database File Used
9	PRTPRFINT	Use the Print Profile Internals command to print a report containing information on the number of entries contained in a user profile. The number of entries determines the size of the user profile.	

Notes:

1. Options are from the SECTOOLS menu.
2. This file is in the QUSRSYS library.

You can page down on the menu to see additional options. Table 7 describes the menu options and associated commands for security auditing:

Table 7. Tool Commands for Security Auditing

Menu[1] Option	Command Name	Description	Database File Used
10	CHGSECAUD	Use the Change Security Auditing command to set up security auditing and to change the system values that control security auditing. When you run the CHGSECAUD command, the system creates the security audit (QAUDJRN) journal if it does not exist. The CHGSECAUD command provides options that make it simpler to set the QAUDLVL (audit level) system value. You can specify *ALL to activate all of the possible audit level settings. Or, you can specify *DFTSET to activate the most commonly used settings (*AUTFAIL, *CREATE, *DELETE, *SECURITY, and *SAVRST). **Note:** If you use the security tools to set up auditing, be sure to plan for management of your audit journal receivers. Otherwise, you might quickly encounter problems with disk utilization.	
11	DSPSECAUD	Use the Display Security Auditing command to display information about the security audit journal and the system values that control security auditing.	

Notes:

1. Options are from the SECTOOLS menu.

How to Use the Security Batch Menu

Following is the first part of the SECBATCH menu:

```
SECBATCH          Submit or Schedule Security Reports To Batch
                                                          System:
Select one of the following:

  Submit Reports to Batch
     1. Adopting objects
     2. Audit journal entries
     3. Authorization list authorities
     4. Command authority
     5. Command private authorities
     6. Communications security
     7. Directory authority
     8. Directory private authority
     9. Document authority
    10. Document private authority
    11. File authority
    12. File private authority
    13. Folder authority
```

When you select an option from this menu, you see the Submit Job (SBMJOB) display, such as the following:

```
                              Submit Job (SBMJOB)
Type choices, press Enter.
 Command to run . . . . . . . . . PRTADPOBJ USRPRF(*ALL)_____________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________ ...
Job name . . . . . . . . . . . .  *JOBD          Name, *JOBD
Job description  . . . . . . . .  *USRPRF        Name, *USRPRF
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Job queue  . . . . . . . . . . .  *JOBD          Name, *JOBD
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Job priority (on JOBQ) . . . . .  *JOBD          1-9, *JOBD
Output priority (on OUTQ)  . . .  *JOBD          1-9, *JOBD
Print device . . . . . . . . . .  *CURRENT       Name, *CURRENT, *USRPRF...
```

If you want to change the default options for the command, you can press F4 (Prompt) on the *Command to run* line.

To see the Schedule Batch Reports, page down on the SECBATCH menu. By using the options on this part of the menu, you can, for example, set up your system to run changed versions of reports regularly.

```
SECBATCH          Submit or Schedule Security Reports To Batch
                                                          System:
Select one of the following:

    28. User objects
    29. User profile information
    30. User profile internals

    31. Check object integrity

  Schedule Batch Reports
    40. Adopting objects
    41. Audit journal entries
    42. Authorization list authorities
    43. Command authority
    44. Command private authority
    45. Communications security
    46. Directory authority
```

You can page down for additional menu options. When you select an option from this part of the menu, you see the Add Job Schedule Entry (ADDJOBSCDE) display:

```
                      Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . .  _____                  Name, *JOBD
Command to run . . . . . > PRTADPOBJ USRPRF(*ALL)_____________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________
                                                          ...
Frequency  . . . . . .  _______  *ONCE, *WEEKLY, *MONTHLY
Schedule date, or  . . .  *CURRENT    Date, *CURRENT, *MONTHST
Schedule day . . . . . .  *NONE       *NONE, *ALL, *MON, *TUE.
+ for more values
Schedule time  . . . . .  *CURRENT    Time, *CURRENT
```

You can position your cursor on the *Command to run* line and press F4 (Prompt) to choose different settings for the report. You should assign a meaningful job name so that you can recognize the entry when you display the job schedule entries.

Options on the Security Batch Menu

Table 8 on page 39 describes the menu options and associated commands for security reports.

When you run security reports, the system prints only information that meets both the selection criteria that you specify and the selection criteria for the tool. For example, job descriptions that specify a user profile name are security-relevant. Therefore, the job description (PRTJOBDAUT) report prints job descriptions in the specified library only if the public authority for the job description is not *EXCLUDE *and* if the job description specifies a user profile name in the USER parameter.

Similarly, when you print subsystem information (PRTSBSDAUT command), the system prints information about a subsystem only when the subsystem description has a communications entry that specifies a user profile.

If a particular report prints less information than you expect, consult the online help information to find out the selection criteria for the report.

Table 8. Commands for Security Reports

Menu[1] Option	Command Name	Description	Database File Used
1, 40	PRTADPOBJ	Use the Print Adopting Objects command to print a list of objects that adopt the authority of the specified user profile. You can specify a single profile, a generic profile name (such as all profiles that begin with Q), or all user profiles on the system. This report has two versions. The full report lists all adopted objects that meet the selection criteria. The changed report lists differences between adopted objects that are currently on the system and adopted objects that were on the system the last time that you ran the report.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Use the Display Audit Journal Entries command to display or print information about entries in the security audit journal. You can select specific entry types, specific users, and a time period.	QASYxxJE[3]
3, 42	PRTPVTAUT *AUTL	When you use the Print Private Authorities command for *AUTL objects, you receive a list of all the authorization lists on the system. The report includes the users who are authorized to each list and what authority the users have to the list. Use this information to help you analyze sources of object authority on your system. This report has three versions. The full report lists all authorization lists on the system. The changed report lists additions and changes to authorization since you last ran the report. The deleted report lists users whose authority to the authorization list has been deleted since you last ran the report. When you print the full report, you have the option to print a list of objects that each authorization list secures. The system will create a separate report for each authorization list.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Use the Print Communications Security command to print the security-relevant settings for objects that affect communications on your system. These settings affect how users and jobs can enter your system. This command produces two reports: a report that displays the settings for configuration lists on the system and a report that lists security-relevant parameters for line descriptions, controllers, and device descriptions. Each of these reports has a full version and a changed version.	QSECCMNOLD[2]

Table 8. Commands for Security Reports (continued)

Menu[1] Option	Command Name	Description	Database File Used
15, 54	PRTJOBDAUT	Use the Print Job Description Authority command to print a list of job descriptions that specify a user profile and have public authority that is not *EXCLUDE. The report shows the special authorities for the user profile that is specified in the job description. This report has two versions. The full report lists all job description objects that meet the selection criteria. The changed report lists differences between job description objects that are currently on the system and job description objects that were on the system the last time that you ran the report.	QSECJBDOLD[2]
See note 4	PRTPUBAUT	Use the Print Publicly Authorized Objects command to print a list of objects whose public authority is not *EXCLUDE. When you run the command, you specify the type of object and the library or libraries for the report. Use the PRTPUBAUT command to print information about objects that every user on the system can access. This report has two versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report.	QPBxxxxxx[5]
See note 5.	PRTPVTAUT	Use the Print Private Authorities command to print a list of the private authorities to objects of the specified type in the specified library. Use this report to help you determine the sources of authority to objects. This report has three versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report. The deleted report lists users whose authority to an object has been deleted since you last printed the report.	QPVxxxxxx[5]
24, 63	PRTQAUT	Use the Print Queue Report to print the security settings for output queues and job queues on your system. These settings control who can view and change entries in the output queue or job queue. This report has two versions. The full report lists all output queue and job queue objects that meet the selection criteria. The changed report lists differences between output queue and job queue objects that are currently on the system and output queue and job queue objects that were on the system the last time that you ran the report.	QSECQOLD[2]

Table 8. Commands for Security Reports (continued)

Menu[1] Option	Command Name	Description	Database File Used
25, 64	PRTSBSDAUT	Use the Print Subsystem Description command to print the security-relevant communications entries for subsystem descriptions on your system. These settings control how work can enter your system and how jobs run. The report prints a subsystem description only if it has communications entries that specify a user profile name. This report has two versions. The full report lists all subsystem description objects that meet the selection criteria. The changed report lists differences between subsystem description objects that are currently on the system and subsystem description objects that were on the system the last time that you ran the report.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Use the Print System Security Attributes command to print a list of security-relevant system values and network attributes. The report shows the current value and the recommended value.	
27, 66	PRTTRGPGM	Use the Print Trigger Programs command to print a list of trigger programs that are associated with database files on your system. This report has two versions. The full report lists every trigger program that is assigned and meets your selection criteria. The changed report lists trigger programs that have been assigned since the last time that you ran the report.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Use the Print User Objects command to print a list of the user objects (objects not supplied by IBM) that are in a library. You might use this report to print a list of user objects that are in a library (such as QSYS) that is in the system portion of the library list. This report has two versions. The full report lists all user objects that meet the selection criteria. The changed report lists differences between user objects that are currently on the system and user objects that were on the system the last time that you ran the report.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Use the Print User Profile command to analyze user profiles that meet specified criteria. You can select user profiles based on special authorities, user class, or a mismatch between special authorities and user class. You can print authority information, environment information, or password information.	
30, 69	PRTPRFINT	Use the Print Profile Internals command to print a report of internal information on the number of entries.	

Table 8. Commands for Security Reports (continued)

Menu[1] Option	Command Name	Description	Database File Used
31, 70	CHKOBJITG	Use the Check Object Integrity command to determine whether operable objects (such as programs) have been changed without using a compiler. This command can help you to detect attempts to introduce a virus program on your system or to change a program to perform unauthorized instructions. The *Security - Reference* book provides more information about the CHKOBJITG command.	

Notes:

1. Options are from the SECBATCH menu.
2. This file is in the QUSRSYS library.
3. xx is the two-character journal entry type. For example, the model output file for AE journal entries is QSYS/QASYAEJE. The model output files are described in Appendix F of the *Security - Reference* book.
4. The SECBATCH menu contains options for the object types that are typically of concern to security administrators. For example, use options 11 or 50 to run the PRTPUBAUT command against *FILE objects. Use the general options (18 and 57) to specify the object type.
5. The SECBATCH menu contains options for the object types that are typically of concern to security administrators. For example, options 12 or 51 run the PRTPVTAUT command against *FILE objects. Use the general options (19 and 58) to specify the object type.
6. The xxxxxx in the name of the file is the object type. For example, the file for program objects is called QPBPGM for public authorities and QPVPGM for private authorities. The files are in the QUSRSYS library.

   The file contains a member for each library for which you have printed the report. The member name is the same as the library name.

Commands for Customizing Security

Table 9 describes the commands that you can use to customize the security on your system. These commands are on the SECTOOLS menu.

Table 9. Commands for Customizing Your System

Menu[1] Option	Command Name	Description	Database File Used
60	CFGSYSSEC	Use the Configure System Security command to set security-relevant system values to their recommended settings. The command also sets up security auditing on your system. "Values That Are Set by the Configure System Security Command" on page 43 describes what the command does. **Note:** To obtain security recommendations customized for your situation, run the AS/400e Security Wizard or the AS/400e Security Advisor instead of running this command. See "Chapter 4. AS/400e Security Wizard and Security Advisor" on page 21 for information on these tools.	
61	RVKPUBAUT	Use the Revoke Public Authority command to set the public authority to *EXCLUDE for a set of security-sensitive commands on your system. "What the Revoke Public Authority Command Does" on page 45 lists the actions that the RVKPUBAUT command performs.	

Table 9. Commands for Customizing Your System (continued)

Menu[1] Option	Command Name	Description	Database File Used
Notes:			
1. Options are from the SECTOOLS menu.			

Values That Are Set by the Configure System Security Command

Table 10 lists the system values that are set when you run the CFGSYSSEC command. The CFGSYSSEC command runs a program that is called QSYS/QSECCFGS.

Table 10. Values Set by the CFGSYSSEC Command

System Value Name	Setting	System Value Description
QAUTOCFG	0 (No)	Automatic configuration of new devices
QAUTOVRT	0	The number of virtual device descriptions that the system will automatically create if no device is available for use.
QALWOBJRST	*NONE	Whether system state programs and programs that adopt authority can be restored
QDEVRCYACN	*DSCMSG (Disconnect with message)	System action when communications is re-established
QDSCJOBITV	120	Time period before the system takes action on a disconnected job
QDSPSGNINF	1 (Yes)	Whether users see the sign-on information display
QINACTITV	60	Time period before the system takes action on an inactive interactive job
QINACTMSGQ	*ENDJOB	Action that the system takes for an inactive job
QLMTDEVSSN	1 (Yes)	Whether users are limited to signing on at one device at a time
QLMTSECOFR	1 (Yes)	Whether *ALLOBJ and *SERVICE users are limited to specific devices
QMAXSIGN	3	How many consecutive, unsuccessful sign-on attempts are allowed
QMAXSGNACN	3 (Both)	Whether the system disables the workstation or the user profile when the QMAXSIGN limit is reached.
QRMTSIGN	*FRCSIGNON	How the system handles a remote (pass-through or TELNET) sign-on attempt.
QRMTSVRATR	0 (Off)	Allows the system to be analyzed remotely.
QSECURITY [1 on page 44]	50	The level of security that is enforced
QPWDEXPITV	60	How often users must change their passwords
QPWDMINLEN	6	Minimum length for passwords
QPWDMAXLEN	8	Maximum length for passwords
QPWDPOSDIF	1 (Yes)	Whether every position in a new password must differ from the same position in the last password
QPWDLMTCHR	See note 2 on page 44	Characters that are not allowed in passwords
QPWDLMTAJC	1 (Yes)	Whether adjacent numbers are prohibited in passwords
QPWDLMTREP	2 (Cannot be repeated consecutively)	Whether repeating characters in are prohibited in passwords
QPWDRQDDGT	1 (Yes)	Whether passwords must have at least one number

Table 10. Values Set by the CFGSYSSEC Command (continued)

System Value Name	Setting	System Value Description
QPWDRQDDIF	1 (32 unique passwords)	How many unique passwords are required before a password can be repeated
QPWDVLDPGM	*NONE	The user exit program that the system calls to validate passwords

Notes:

1. If you are currently running with a QSECURITY value of 40 or lower, be sure to review the information in Chapter 2 of the *Security - Reference* book before you change to a higher security level.
2. The restricted characters are stored in message ID CPXB302 in the message file QSYS/QCPFMSG. They are shipped as AEIOU@$#. You can use the Change Message Description (CHGMSGD) command to change the restricted characters.

The CFGSYSSEC command also sets the password to *NONE for the following IBM-supplied user profiles:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

Finally, the CFGSYSSEC command sets up security auditing using the Change Security Auditing (CHGSECAUD) command. The CFGSYSSEC command turns on action and object auditing and also, specifies the default set of actions to audit on the CHGSECAUD command.

Changing the Program

If some of these settings are not appropriate for your installation, you can create your own version of the program that processes the command. Do the following:

__ Step 1. Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the CFGSYSSEC command. The program to retrieve is QSYS/QSECCFGS. When you retrieve it, give it a *different name*.

__ Step 2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you *do not* replace the IBM-supplied QSYS/QSECCFGS program. Your program should have a different name.

__ Step 3. Use the Change Command (CHGCMD) command to change the program to process command (PGM) parameter for the CFGSYSSEC command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYSECCFG, you would type the following:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

Note: If you change the QSYS/QSECCFGS program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.

What the Revoke Public Authority Command Does

You can use the Revoke Public Authority (RVKPUBAUT) command to set the public authority to *EXCLUDE for a set of commands and programs. The RVKPUBAUT command runs a program that is called QSYS/QSECRVKP. As it is shipped, the QSECRVKP revokes public authority (by setting public authority to *EXCLUDE) for the commands that are listed in Table 11 and the application programming interfaces (APIs) that are listed in Table 12. When your system arrives, these commands and APIs have their public authority set to *USE.

The commands that are listed in Table 11 and the APIs that are listed in Table 12 all perform functions on your system that may provide an opportunity for mischief. As security administrator, you should explicitly authorize users to run these commands and programs rather than make them available to all system users.

When you run the RVKPUBAUT command, you specify the library that contains the commands. The default is the QSYS library. If you have more than one national language on your system, you need to run the command for each QSYSxxx library.

Table 11. Commands Whose Public Authority Is Set by the RVKPUBAUT Command

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

The APIs in Table 12 are all in the QSYS library:

Table 12. Programs Whose Public Authority Is Set by the RVKPUBAUT Command

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Beginning with V3R7, when you run the RVKPUBAUT command, the system sets the public authority for the root directory to *USE (unless it is already *USE or less).

Changing the Program

If some of these settings are not appropriate for your installation, you can create your own version of the program that processes the command. Do the following:

__ Step 1. Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the RVKPUBAUT command. The program to retrieve is QSYS/QSECRVKP. When you retrieve it, give it a *different name*.

__ Step 2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you *do not* replace the IBM-supplied QSYS/QSECRVKP program. Your program should have a different name.

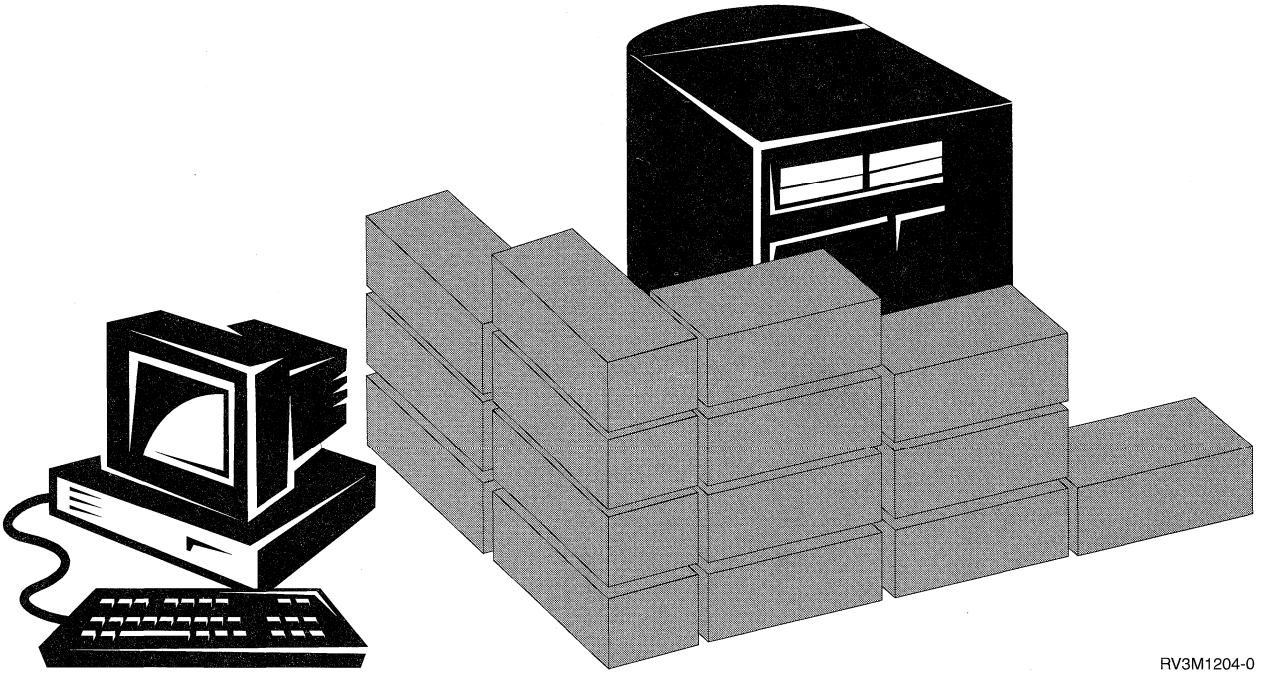
__ Step 3. Use the Change Command (CHGCMD) command to change the program to process command (PGM) parameter for the RVKPUBAUT command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYRVKPGM, you would type the following:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

Note: If you change the QSYS/QSECRVKP program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.

Part 3. Tips for Advanced System Security

If all the good people were clever,
And all clever people were good,
The world would be a nicer place than ever
We thought that it possibly could.
Elizabeth Wordsworth



RV3M1204-0

Chapter 7. Using Object Authority to Protect Information Assets

Your challenge as security administrator is to protect your organization's information assets without frustrating the users on your system. You need to make sure that users have enough authority to do their jobs without giving them the authority to browse throughout the system and to make unauthorized changes.

Security Tip: Authority that is too tight can backfire. Users sometimes react to authority restrictions that are too tight by sharing passwords with each other.

The OS/400 operating system provides integrated object security. Users must use the interfaces that the system provides to access objects. For example, if you want to access a database file, you must use commands or programs that are intended for accessing database files. You cannot use a command that is intended for accessing a message queue or a job log.

Whenever you use a system interface to access an object, the system verifies that you have the authority to the object that is required by that interface. Object authority is a powerful and flexible tool for protecting the assets on your system. Your challenge as a security administrator is to set up an effective object security scheme that you can manage and maintain.

Does the System Always Enforce Object Authority?

The answer is yes and no. Whenever you try to access an object, the operating system checks your authority to that object. However, if the security level on your system (QSECURITY system value) is set to 10 or 20, every user automatically has authority to access every object because every user profile has *ALLOBJ special authority.

Object Authority Tip: If you are not sure whether you are using object security, check the QSECURITY (security level) system value. If QSECURITY is 10 or 20, you are not using object security.

You must plan and prepare before you change to security level 30 or higher. Otherwise, your users may not be able to access the information that they need.

The *Security - Basic* book provides a method for analyzing your applications and deciding how you should set up object security. If you are not yet using object security or if your object security scheme is outdated and convoluted, read this chapter to help you get started.

The Legacy of Menu Security

AS/400 was originally designed as a follow-on product for S/36 and S/38. Many AS/400 installations were, at one time, S/36 installations or S/38 installations. To control what users could do, security administrators on those earlier systems often used a technique that is referred to as **menu security** or **menu access control**.

Menu access control means that when a user signs on, the user gets a menu such as the following:

```
OEMENU      Order Entry Menu

1. Work with customer records
2. Work with orders
3. Work with order history
4. Work with prices
5. Work with contracts

Select option number:  ___
```

Figure 6. Sample Order Entry Menu

The user can perform only the functions that are on the menu. The user cannot get to a command line on the system to perform any functions that are not on the menu. In theory, the security administrator does not have to worry about authority to objects because menus and programs control what users can do.

AS/400 provides several user profile options to assist with menu access control:

- You can use the initial menu (INLMNU) parameter to control what menu the user first sees after the user signs on.
- You can use the initial program (INLPGM) parameter to run a setup program before the user sees a menu. Or, you can use the INLPGM parameter to restrict a user to running a single program.
- You can use the limit capabilities (LMTCPB) parameter to restrict a user to a limited set of commands. It also prevents the user from specifying a different initial program or menu on the Sign On display. (The LMTCPB parameter only limits commands that are entered from the command line.)

Limitations of Menu Access Control

Computers and computer users have changed a great deal in the past few years. Many tools, such as query programs and spreadsheets, are available so that users can do some of their own programming to off-load IS departments. Some tools, such as SQL or ODBC, provide the capability to view information and to change information. To enable these tools within a menu structure is very difficult.

Fixed-function ("green-screen") workstations are rapidly being replaced by personal computers and computer-to-computer networks. If your system participates in a network, users may enter your system without ever seeing a sign-on display or a menu.

As a security administrator who is trying to enforce menu access control, you have two basic problems:

- If you are successful in limiting users to menus, your users will probably be unhappy because their ability to use modern tools is limited.
- If you are not successful, you could jeopardize critical, confidential information that menu access control is supposed to protect. When your system participates in a network, your ability to enforce menu access control decreases. For example, the LMTCPB parameter applies only to commands that are entered from a command line in an interactive session. The LMTCPB parameter has no affect on requests from communications sessions, such as PC file transfer, FTP, or remote commands.

Tips for Enhancing Menu Access Control with Object Security

With the many new options that are available to connect to systems, a viable AS/400 security scheme for the future cannot rely solely on menu access control. This topic provides suggestions for moving toward an object security environment to complement your menu access control.

The *Security - Basic* book describes a technique for analyzing the authority that users must have to objects to run your current applications. You then assign users to groups and give the groups appropriate authority. This approach is reasonable and logical. However, if your system has been operational for many years and has many applications, the task of analyzing applications and setting up object authority probably seems overwhelming.

Object Authority Tip: Your current menus combined with programs that adopt the authority of the program owners may provide a transition beyond menu access control. Be sure to protect both the programs that adopt authority and the user profiles that own them.

You may be able to use your current menus to help you set up a transition environment while you gradually analyze your applications and objects. Following is an example that uses the Order Entry (OEMENU) menu (Figure 6 on page 50) and the associated files and programs.

Setting Up a Transition Environment–Example

This example starts with the following assumptions and requirements:

- All of the files are in the library ORDERLIB.
- You do not know the names of all the files. You also do not know what authority the menu options require to different files.
- The menu and all the programs that it calls are in a library called ORDERPGM.
- You want everyone who can sign on to your system to be able to view information in all the order files, customer files, and item files (with queries or spreadsheets, for example).
- Only users whose current sign-on menu is the OEMENU should be able to change the files. And, they must use the programs on the menu to do this.
- System users other than the security administrators do not have *ALLOBJ or *SECADM special authority.

Do the following to change this menu-access-control environment to accommodate the need for queries:

__ Step 1. Make a list of the users whose initial menu is the OEMENU. You can use the Print User Profile (PRTUSRPRF *ENVINFO) command to list the environment for every user profile on your system. The report includes the initial menu, initial program, and current library. Figure 14 on page 61 shows an example of the report.

__ Step 2. Make sure that the OEMENU object (it may be a *PGM object or a *MENU object) is owned by a user profile that is not used for sign on. The user profile should be disabled or have a password of *NONE. For this example, assume that OEOWNER owns the OEMENU program object.

__ Step 3. Make sure that the user profile that owns the OEMENU program object is not a group profile. You can use the following command:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ Step 4. Change the OEMENU program to adopt the authority of the OEOWNER user profile. (Use the CHGPGM command to change the USRPRF parameter to *OWNER.)

Note: *MENU objects cannot adopt authority. IF OEMENU is a *MENU object, you can adapt this example by doing one of the following:

- Create a program to display the menu.
- Use adopted authority for the programs that run when the user selects options from the OEMENU menu.

__ Step 5. Set the public authority to all of the files in ORDERLIB to *USE by typing the following two commands:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

Remember that if you select *USE authority, users can copy the file by using PC file transfer or FTP.

__ Step 6. Give the profile that owns the menu program *ALL authority to the files by typing the following:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

For most applications, *CHANGE authority to files is sufficient. However, your applications may perform functions, such as clearing physical file members, that require more authority than *CHANGE. Eventually, you should analyze your applications and provide only the minimum authority that is necessary for the application. However, during the transition period, by adopting *ALL authority, you avoid applications failures that may be caused by insufficient authority.

__ Step 7. Restrict authority to the programs in the order library by typing the following:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ Step 8. Give the OEOWNER profile authority to the programs in the library by typing the following:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ Step 9. Give the users that you identified in step 1 authority to the menu program by typing the following for each user:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

When you have completed these steps, all system users who are not explicitly excluded will be able to access (but not change) the files in the ORDERLIB library. Users who have authority to the OEMENU program will be able to use the programs that are on the menu to update files in the ORDERLIB library. Only users who have authority to the OEMENU program will now be able to change the files in this library. A combination of object security and menu access control protects the files.

When you complete similar steps for all the libraries that contain user data, you have created a simple scheme for controlling database updates. This method

prevents system users from updating database files except when they use the approved menus and programs. At the same time, you have made database files available for viewing, analyzing, and copying by users with decision-support tools or with links from another system or from a PC.

Object Authority Tip: When your system participates in a network, *USE authority may provide more authority than you expect. For example, with FTP, you can make a copy of a file to another system (including a PC) if you have *USE authority to the file.

Using Library Security to Complement Menu Security

To access an object in a library, you must have authority both to the object and to the library. Most operations require either *EXECUTE authority or *USE authority to the library.

Depending on your situation, you may be able to use library authority as a simple means for securing objects. For example, assume that for the Order-Entry menu example, everyone who has authority to the Order Entry menu can use all of the programs in the ORDERPGM library. Rather than securing individual programs, you can set the public authority to the ORDERPGM library to *EXCLUDE. You can then grant *USE authority to the library to specific user profiles, which will allow them to use the programs in the library. (This assumes that public authority to the programs is *USE or greater.)

Library authority can be a simple, efficient method for administering object authority. However, you must ensure that you are familiar with the contents of the libraries that you are securing so that you do not provide unintended access to objects.

Tips for Setting Up Object Ownership

The ownership of objects on your system is an important part of your object authority scheme. By default, the owner of an object has *ALL authority to the object. Chapter 5 in the *Security - Reference* book provides recommendations and examples for planning object ownership. Following are a few tips:

- In general, group profiles should not own objects. If a group profile owns an object, all group members have *ALL authority to the object unless the group member is explicitly excluded.
- If you use adopted authority, consider whether the user profiles that own programs should also own application objects, such as files. You may not want the users who run the programs that adopt authority to have *ALL authority to files.

Tips for Object Authority to System Commands and Programs

Following are several suggestions when you restrict authority to IBM-supplied objects:

- When you have more than one national language on your system, your system has more than one system (QSYS) library. Your system has a QSYSxxxx library for each national language on your system. If you are using object authority to control access to system commands, remember to secure the command in the QSYS library and in every QSYSxxx library on your system.

- The System/38 library sometimes provides a command with function that is equivalent to the commands that you want to restrict. Be sure you restrict the equivalent command in the QSYS38 library.
- If you have the System/36 environment, you may need to restrict additional programs. For example, the QY2FTML program provides System/36 file transfer.

Chapter 8. Tips for Managing and Monitoring Authority

A set of security reports are available to help you keep track of how the authority is set up on your system. When you run these reports initially, you can print everything (authority for all the files or for all the programs, for example).

After you have established your base of information, you can run the changed versions of reports regularly. The changed versions help you identify security-relevant changes on your system that require your attention. For example, you can run the report that shows the public authority for files every week. You can request only the changed version of the report. It will show you both new files on the system that are available to everyone and existing files whose public authority has changed since the last report.

Two menus are available to run security tools:

- Use the SECTOOLS menu for running programs interactively. "Options on the Security Tools Menu" on page 34 provides more information about the menu.
- Use the SECBATCH menu for running programs in batch. The SECBATCH menu has two parts: one for submitting jobs to the job queue immediately, and the other for placing jobs on the job scheduler. "Options on the Security Batch Menu" on page 38 provides more information about the menu.

This chapter provides examples of how you can monitor the authority on your system.

Monitoring Public Authority to Objects

For both simplicity and performance, most systems are set up so that most objects are available to most users. Users are explicitly denied access to certain confidential, security-sensitive objects rather than having to be explicitly authorized to use every object. A few systems with high security requirements take the opposite approach and authorize objects on a need-to-know basis. On those systems, most objects are created with the public authority set to *EXCLUDE.

AS/400 is an object-based system with many different types of objects. Most object types do not contain sensitive information or perform security-relevant functions. As a security administrator on an AS/400 system with typical security needs, you probably want to focus your attention on objects that require protection, such as database files and programs. For other object types, you can just set public authority that is sufficient for your applications, which for most object types is *USE authority.

You can use the Print Public Authority (PRTPUBAUT) command to print information about objects that public users can access. (A **public user** is anyone with sign-on authority who does not have explicit authority to an object.) When you use the PRTPUBAUT command, you can specify the object types, and libraries or directories, that you want to examine. Options are available on the SECBATCH and SECTOOLS menus to print the Publicly Authorized Objects Report for the object types that most commonly have security implications.

Figure 7 on page 56 shows an example of the Publicly Authorized Objects Report for the *FILE objects in the CUSTLIB library:

```
Publicly Authorized Objects (Full Report)
SYSTEM4
Object type  . . . . . :   *FILE
Specified library  . . . . . :   CUSTLIB
                              Authorization                ----------Object----------  ------------Data------------
Library     Object      Owner      List          Authority  Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
CUSTLIB     CUSTMAST    AROWNER    *NONE         *USE        X                           X                          X
CUSTLIB     ORDERS      AROWNER    *NONE         *CHANGE     X                           X     X    X    X       X
CUSTLIB     PRICES      AROWNER    *NONE         *USE        X                           X                          X
CUSTLIB     TAXES       AROWNER    *NONE         *CHANGE     X                           X     X    X    X       X
```

Figure 7. Publicly Authorized Objects Report-Sample

You can print the changed version of this report regularly to see what objects might require your attention.

Managing Authority for New Objects

OS/400 provides functions to help you manage the authority and ownership for new objects on your system. When a user creates a new object, the system determines the following:

- Who will own the object
- What the public authority for the object is
- Whether the object has any private authorities
- Where to put the object (what library or directory)
- Whether access to the object will be audited

The system uses system values, library parameters, and user profile parameters to make these decisions. "Assigning Authority and Ownership to New Objects" in chapter 5 of the *Security - Reference* book provides several examples of the options that are available.

You can use the PRTUSRPRF command to print the user profile parameters that affect ownership and authority for new objects. Figure 12 on page 59 shows an example of this report.

Monitoring Authorization Lists

SECBATCH menu options:
3 *to submit immediately* **42** *to use the job scheduler*

You can group objects with similar security requirements by using an authorization list. Conceptually, an authorization list contains a list of users and the authority that the users have to the objects that are secured by the list. Authorization lists provide an efficient way to manage the authority to similar objects on the system. However, in some cases, they make it difficult to keep track of authorities to objects.

You can use the Print Private Authority (PRTPVTAUT) command to print information about authorization list authorities. Figure 8 on page 57 shows a sample of the report.

```
                              Private Authorities (Full Report)
SYSTEM4
Authorization                  Primary                                List  ----------Object----------  ------------Data------------
List            Owner          Group       User        Authority  Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1           QSECOFR        *NONE       *PUBLIC     *EXCLUDE
LIST2           BUDNIKR        *NONE       BUDNIKR     *ALL        X     X    X     X      X     X    X     X    X    X     X
                                           *PUBLIC     *CHANGE           X                              X     X    X    X     X
LIST3           QSECOFR        *NONE       *PUBLIC     *EXCLUDE
LIST4           CJWLDR         *NONE       CJWLDR      *ALL        X     X    X     X      X     X    X     X    X    X     X
                                           GROUP1      *ALL              X    X     X      X     X    X     X    X    X     X
                                           *PUBLIC     *EXCLUDE
```

Figure 8. Private Authorities Report for Authorization Lists

This report shows the same information that you see on the Edit Authorization List (EDTAUTL) display. The advantage of the report is that it provides information about all authorization lists in one place. If you are setting up security for a new group of objects, for example, you can quickly scan the report to see if an existing authorization list meets your needs for those objects.

You can print a changed version of the report to see new authorization lists or authorization lists with authority changes since you last printed the report. You also have the option of printing a list of the objects that are secured by each authorization list. Figure 9 shows an example of the report for one authorization list:

```
                    Display Authorization List Objects
Authorization list . . . . . :   CUSTAUTL
Library  . . . . . :             QSYS
Owner  . . . . . :               AROWNER
Primary group  . . . . . :       *NONE

                                                          Primary
Object          Library         Type          Owner       group          Text
CUSTMAS         CUSTLIB         *FILE         AROWNER     *NONE
CUSTORD         CUSTORD         *FILE         OEOWNER     *NONE
```

Figure 9. Display Authorization List Objects Report

You can use this report, for example, to understand the effect of adding a new user to an authorization list (what authorities that user will receive).

Monitoring Private Authority to Objects

SECBATCH menu options:
12 *to submit immediately* **41** *to use the job scheduler*

You can use the Print Private Authority (PRTPVTAUT) command to print a list of all the private authorities for objects of a specified type in a specified library.

You can use this report to help you detect new authorities to objects. It can also help you keep your private authority scheme from becoming convoluted and unmanageable. Figure 10 on page 58 shows an example of the report:

```
                                Private Authorities (Full Report)
5769SS1 VxRxMx  000000                                                    TESTSYS  00/00/00  00:00:00
 Directory . . . . . . . . . . :   /qibm
  *PUBLIC authority . . . . . :   *RX
 Object type . . . . . . . . . :   *DIR

                          Primary       Auth
Object                    Group         List          User        Data       ----------Object----------
ProdData                  QSYS          *NONE         *NONE                   Authority   Mgt    Exist    Alter    Ref
                                                                   *PUBLIC     *RX
                                                                   QSYS        *RWX        X      X        X        X
UserData                  QSYS          *NONE         *NONE       *PUBLIC     *RX
                                                                   QSYS        *RWX        X      X        X        X
include                   QSYS          *NONE         *NONE       *PUBLIC     *RX
                                                                   QSYS        *RWX        X      X        X        X
locales                   QLPINSTALL    *NONE         *NONE       *PUBLIC     *RX
                                                                   QLPINSTA    *RWX        X      X        X        X
```

Figure 10. Private Authorities Report–Sample

Monitoring Access to Output Queues and Job Queues

Sometimes a security administrator does a great job of protecting access to files and then forgets about what happens when the contents of a file are printed. AS/400 provides functions for you to protect sensitive output queues and job queues. You protect an output queue so that unauthorized users cannot, for example, view or copy confidential spooled files that are waiting to print. You protect job queues so that an unauthorized user cannot either redirect a confidential job to a nonconfidential output queue or cancel the job entirely.

SECBATCH menu options:
24 to submit immediately 63 *to use the job scheduler*

The *Security - Basic* and *Security - Reference* books describe how to protect your output queues and job queues.

You can use the Print Queue Authority (PRTQAUT) command to print the security settings for the job queues and output queues on your system. You can then evaluate printing jobs that print confidential information and ensure that they are going to output queues and job queues that are protected. Figure 11 shows an example of the PRTQAUT report:

```
                                  Queue Authority (Full Report)
                                                                                    SYSTEM4
Specified library . . . . . :   *ALL
Library       Object        Type          Owner         Authority     DSPDTA        OPRCTL        AUTCHK
BASQLIB       OUTQ1         *OUTQ         BASMLYR       *USE          *NO           *YES          *OWNER
BASQLIB       OUTQ2         *OUTQ         BASMLYR       *ALL          *YES          *YES          *OWNER
BASQLIB       OUTQ3         *OUTQ         BASMLYR       *CHANGE       *OWNER        *YES          *OWNER
BASQLIB       OUTQ4         *OUTQ         BASMLYR       *EXCLUDE      *NO           *NO           *OWNER
BASQLIB       OUTQ5         *OUTQ         BASMLYR       *EXCLUDE      *NO           *NO           *DTAAUT
BASQLIB       JOBQ2         *JOBQ         BASMLYR       *CHANGE       *NONE         *NO           *OWNER
BASQLIB       JOBQ3         *JOBQ         BASMLYR       *EXCLUDE      *NONE         *NO           *DTAAUT
```

Figure 11. Queue Authority Report–Sample

For output queues and job queues that you consider to be security-sensitive, you can compare your security settings to the information in Appendix D of the *Security*

- *Reference* book. The tables in Appendix D tell what settings are required to perform different output queue and job queue functions.

Monitoring Special Authorities

When users on your system have unnecessary special authorities, your efforts to develop a good object-authority scheme may be wasted. Object authority is meaningless when a user profile has *ALLOBJ special authority. A user with *SPLCTL special authority can see any spooled file on the system, no matter what efforts you make to secure your output queues. A user with *JOBCTL special authority can affect system operations and redirect jobs. A user with *SERVICE special authority may be able to use service tools to access data without going through the operating system.

SECBATCH menu options:
29 to submit immediately 68 *to use the job scheduler*

You can use the Print User Profile (PRTUSRPRF) command to print information about the special authorities and user classes for user profiles on your system. When you run the report, you have several options:

- All user profiles
- User profiles with specific special authorities
- User profiles that have specific user classes
- User profiles with a mismatch between user class and special authorities.

Figure 12 shows an example of the report that shows the special authorities for all user profiles:

```
                                    User Profile Information
  Report type  . . . . . . . . . . :   *AUTINFO
  Select by  . . . . . . . . . . . :   *SPCAUT
  Special authorities  . . . . . . :   *ALL
                    ------------Special Authorities-------------
                                *IO                                                    Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User              Group      Authority  Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class     Owner   Authority  Type       Capability
USERA     *NONE      X     X     X    X     X     X     X     X    *SECOFR   *USRPRF *NONE      *PRIVATE   *NO
USERB     *NONE                       X     X                      *PGMR     *USRPRF *NONE      *PRIVATE   *NO
USERC     *NONE      X     X     X    X     X     X     X     X    *SECOFR   *USRPRF *NONE      *PRIVATE   *NO
USERD     *NONE                                                    *USER     *USRPRF *NONE      *PRIVATE   *NO
```

Figure 12. User Information Report–Example 1

In addition to the special authorities, the report shows the following:

- Whether the user profile has limited capability.
- Whether the user or the user's group owns new objects that the user creates.
- What authority the user's group automatically receives to new objects that the user creates.

Figure 13 on page 60 shows an example of the report for mismatched special authorities and user classes:

```
User Profile Information
Report type  . . . . . :   *AUTINFO
Select by  . . . . . :   *MISMATCH
------------------------------Special Authorities-------------
                              *IO                                                    Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User            Group      Authority   Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class     Owner  Authority  Type        Capability
USERX     *NONE       X                X     X                  X   *SYSOPR   *USRPRF  *NONE      *PRIVATE    *NO
USERY     *NONE                                      X             *USER     *USRPRF  *NONE      *PRIVATE    *NO
USERZ                                                X             *USER     *USRPRF  *NONE      *PRIVATE    *NO
          QPGMR                          X     X
```

Figure 13. User Information Report–Example 2

In Figure 13, notice the following:

- USERX has a system operator (*SYSOPR) user class but has *ALLOBJ and *SPLCTL special authorities.
- USERY has a user (*USER) user class but has *SECADM special authority.
- USERZ also has a user (*USER) class and *SECADM special authority. You can also see that USERZ is a member of the QPGMR group, which has *JOBCTL and *SAVSYS special authorities.

You can run these reports regularly to help you monitor the administration of user profiles.

Monitoring User Environments

One role of the user profile is to define the environment for the user, including the output queue, the initial menu, and the job description. The user's environment affects how the user sees the system and, to some extent, what the user is allowed to do. The user must have authority to the objects that are specified in the user profile. However, if your authority scheme is still in progress or is not very restrictive, the user environment that is defined in a user profile may produce results that you do not intend. Following are several examples:

SECBATCH menu options:
29/ph> to submit immediately 68 *to use the job scheduler*

- The user's job description may specify a user profile that has more authority than the user.
- The user may have an initial menu that does not have a command line. However, the user's attention-key-handling program may provide a command line.
- The user may be authorized to run confidential reports. However, the user's output may be directed to an output queue that is available to users who should not see the reports.

You can use the *ENVINFO option of the Print User Profile (PRTUSRPRF) command to help you monitor the environments that are defined for system users. Figure 14 on page 61 shows an example of the report:

```
                                    User Profile Information
  Report type  . . . . . :   *ENVINFO
  Select by  . . . . . :   *USRCLS
                        Initial       Initial          Job          Message       Output        Attention
User                    Menu/         Program/     Description/     Queue/        Queue/        Program/
Profile       Current   Library       Library        Library        Library       Library       Library
AUDSECOFR     AUDITOR   MAIN          *NONE          QDFTJOBD       QSYSOPR       *WRKSTN       *SYSVAL
                        *LIBL                        QGPL            QSYS
USERA         *CRTDFT   OEMENU        *NONE          QDFTJOBD       USERA         *WRKSTN       *SYSVAL
                        *LIBL                        QGPL            QUSRSYS
USERB         *CRTDFT   INVMENU       *NONE          QDFTJOBD       USERB         *WRKSTN       *SYSVAL
                        *LIBL                        QGPL            QUSRSYS
USERC         *CRTDFT   PAYROLL       *NONE          QDFTJOBD       USERC         PAYROLL       *SYSVAL
                        *LIBL                        QGPL            QUSRSYS       PRPGMLIB
```

Figure 14. Print User Profile-User Environment Example

Chapter 9. Tips for Detecting Suspicious Programs

Recent trends in computer usage have increased the likelihood that your system has programs from untrusted sources or programs that perform unknown functions. Following are examples:

- A personal computer user sometimes obtains programs from other PC users. If the PC is attached to your AS/400 system, that program can affect your AS/400.
- Users who connect to networks can also obtain programs, for example from bulletin boards.
- Hackers have become more active and renowned. They often publish their methods and their results. This can lead to imitation by normally law-abiding programmers.

These trends have led to a new problem in computer security that is called a **computer virus**. A virus is a program that can change other programs to include a copy of itself. The other programs are then said to be infected by the virus. Additionally, the virus can perform other operations that can take up system resources or destroy data.

The architecture of AS/400 provides some protection from the infectious characteristics of a computer virus. "Protecting Against Computer Viruses" describes this. An AS/400 security administrator needs to be more concerned about programs that perform unauthorized functions. The remaining topics in this chapter describe ways that someone with ill intentions might set up harmful programs to run on your system. The topics provide tips for preventing programs from performing unauthorized functions.

Security Tip

Object authority is always your first line of defense. If you do not have a good plan for protecting your objects, your system is defenseless. This chapter discusses ways that an authorized user might try to take advantage of loop-holes in your object authority scheme.

Protecting Against Computer Viruses

A computer that has a virus infection has a program that can change other programs. The object-based architecture of AS/400 makes it more difficult for a mischief-maker to produce and spread this type of virus than it is with other computer architectures. On AS/400, you use specific commands and instructions to work on each type of object. You cannot use a file instruction to change an operable program object (which is what most virus-creators do). Nor can you easily create a program that changes another program object. To do this requires considerable time, effort, and expertise, and it requires access to tools and documentation that are not generally available.

However, as new AS/400 functions become available to participate in the open-systems environment, some of the object-based protection functions of AS/400 no longer apply. For example, with the integrated file system, users can directly manipulate some objects in directories, such as stream files.

Also, although AS/400 architecture makes it difficult for a virus to spread among AS/400 programs, its architecture does not prevent AS/400 from being a virus-carrier. As a file server, AS/400 can store programs that many PC users share. Any one of these programs might contain a virus that AS/400 does not detect. To prevent this type of virus from infecting the PCs that are attached to your AS/400 server, you must use PC virus-scan software.

Several functions exist on AS/400 to prevent someone from using a low-level language with pointer capability to alter an operable object program:

- If your system runs at security level 40 or higher, the integrity protection includes protections against changing program objects. For example, you cannot successfully run a program that contains blocked (protected) machine instructions.
- At security level 40 or higher, the program validation value is also intended to protect you when you restore a program that was saved (and potentially changed) on another system. Chapter 2 in the *Security - Reference* book describes the integrity protection functions for security level 40 and higher, including program validation values.

  Note: The program validation value is not foolproof, and it is not a replacement for vigilance in evaluating programs that are restored to your system.

Several tools are also available to help you detect the introduction of an altered program into your system:

- You can use the Check Object Integrity (CHKOBJITG) command to scan objects (operable objects) that meet your search values to ensure that those objects have not been altered. This is similar to a virus-scan function.
- You can use the security auditing function to monitor programs that are changed or restored. The *PGMFAIL, *SAVRST, and *SECURITY values for the authority level system value provide audit records that can help you detect attempts to introduce a virus-type program into your system. Chapter 9 and Appendix F in the *Security - Reference* book provide more information about audit values and the audit journal entries.
- You can use the force create (FRCCRT) parameter of the Change Program (CHGPGM) command to re-create any program that has been restored to your system. The system uses the program template (observable information) to re-create the program. If the program object has been changed after it was compiled, the system re-creates the changed object and replaces it. If the program template contains blocked (protected) instructions and you are running security level 40 or higher, the system will not re-create the program successfully.

Monitoring the Use of Adopted Authority

On AS/400, you can create a program that adopts the authority of the owner of the program. This means that any user who runs the program has the same authorities (private authorities and special authorities) as the user profile that owns the program.

Adopted authority is a valuable security tool when it is used correctly. "Tips for Enhancing Menu Access Control with Object Security" on page 51, for example, describes how to combine adopted authority and menus to help you expand beyond menu access control. You can use adopted authority to protect your important files from being changed outside of your approved application programs while you still allow queries against the files.

As security administrator, you should make sure that adopted authority is used properly:

- Programs should adopt the authority of a user profile that has only enough authority to do the necessary functions, not excessive authority. You should be particularly cautious of programs that adopt the authority of a user profile that either has *ALLOBJ special authority or owns important objects.
- Programs that adopt authority should have a specific, limited function and should not provide command-entry capability.
- Programs that adopt authority should be secured properly.
- Excessive use of adopted authority may have a negative impact on your system performance. To help you avoid performance problems, review the authority-checking flowcharts and the suggestions for using adopted authority in Chapter 5 of the *Security - Reference* book.

SECBATCH menu options:
1 *to submit immediately* **40 to use the job scheduler**

You can use the Print Adopting Objects (PRTADPOBJ) command (option 21 on the SECTOOLS menu) to help you monitor the use of adopted authority on your system.

Figure 15 shows an example of the output from this command:

```
                    Adopted Objects by User Profile (Full Report)

User profile . . . . . . . . . :   CJWLDR
Special authorities  . . . . . :   *ALLOBJ  *AUDIT   *IOSYSCFG  *JOBCTL
                                   *SAVSYS  *SECADM  *SERVICE   *SPLCTL
----------Object-------------     ------Library--------
                    Public                    Public        Private
Name      Type      Authority     Name        Authority     Authorities
PGM1      *PGM      *USE          LIB1        *USE               Y
PGM2      *PGM      *CHANGE       LIB2        *USE               N
```

Figure 15. Adopted Objects by User Profile Report-Full Report

Figure 15 shows information for one user profile, CJWLDR. It shows the special authorities that CJWLDR has and the programs that adopt CJWLDR's authority. In this example, anyone who has access to a command line can run the programs that adopt CJWLDR's authority because the programs have public authority of *USE. This example demonstrates a potentially serious security exposure because of CJWLDR's special authorities.

After you have established a base of information, you can print the changed version of the adopted objects report regularly. It lists new programs that adopt authority and programs that have been changed to adopt authority since you last ran the report. Figure 16 on page 66 shows an example of the changed report:

```
                    Adopted Objects by User Profile (Changed Report)
User profile . . . . . :   CJWLDR
Special authorities  . . . . . :   *ALLOBJ  *AUDIT   *IOSYSCFG  *JOBCTL
                                   *SAVSYS  *SECADM  *SERVICE   *SPLCTL
Last changed report  . . . . . :   01/21/96  14:23:53
----------Object-------------     --------Library---------
                    Public                      Public        Private
Name      Type      Authority     Name          Authority     Authorities
PGMX      *PGM      *CHANGE       LIB3          *CHANGE            Y
PGMY      *PGM      *USE          LIB4          *USE               N
```

Figure 16. Adopted Objects by User Profile Report-Changed Report

If you suspect that adopted authority is being misused on your system, you can set the QAUDLVL system value to include *PGMADP. When this value is active, the system creates an audit journal entry whenever someone starts or ends a program that adopts authority. The entry includes the name of the user who started the program and the name of the program.

Limiting the Use of Adopted Authority

When an AS/400 program runs, the program can use adopted authority to gain access to objects in two different ways:

- The program itself can adopt the authority of its owner. This is specified in the user profile (USRPRF) parameter of the program or service program.
- The program can use (inherit) adopted authority from a previous program that is still in the job's call stack. A program can inherit the adopted authority from previous programs even if the program itself does not adopt authority. The use adopted authority (USEADPAUT) parameter of a program or a service program controls whether the program inherits adopted authority from previous programs in the program stack.

Following is an example of how using adopted authority from previous programs works.

Assume that the ICOWNER user profile has *CHANGE authority to the ITEM file and that the public authority to the ITEM file is *USE. No other user profiles have any explicitly defined authority to the ITEM file. Table 13 shows the attributes for three programs that use the ITEM file:

Table 13. Use Adopted Authority (USEADPAUT) Example

Program Name	Program Owner	USRPRF Value	USEADPAUT Value
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Example 1–Adopting Authority:

1. USERA runs the PGMA program.
2. The PGMA program attempts to open the ITEM file with update capability.

Result: Attempt is successful. USERA has *CHANGE access to the ITEM file because PGMA adopts ICOWNER's authority.

Example 2–Using Adopted Authority:

1. USERA runs the PGMA program.
2. The PGMA program calls the PGMB program.
3. The PGMB program attempts to open the ITEM file with update capability.

Result: Attempt is successful. Although the PGMB program does not adopt authority (*USRPRF is *USER), it allows the use of previous adopted authority (*USEADPAUT is *YES). The PGMA program is still in the program stack. Therefore, USERA gets *CHANGE access to the ITEM file because PGMA adopts ICOWNER's authority.

Example 3–Not Using Adopted Authority:

1. USERA runs the PGMA program.
2. The PGMA program calls the PGMC program.
3. The PGMC program attempts to open the ITEM file with update capability.

Result: Authority failure. The PGMC program does not adopt authority. The PGMC program also does not allow the use of adopted authority from previous programs. Although PGMA is still in the call stack, its adopted authority is not used.

Preventing New Programs from Using Adopted Authority

The passing of adopted authority to later programs in the stack provides an opportunity for a knowledgeable programmer to create a Trojan horse program. The Trojan horse program can rely on previous programs in the stack to get the authority that it needs to perform mischief. To prevent this, you can limit which users are allowed to create programs that use the adopted authority of previous programs.

When you create a new program, the system automatically sets the USEADPAUT parameter to *YES. If you do not want the program to inherit adopted authority, you must use the Change Program (CHGPGM) command or the Change Service Program (CHGSRVPGM) to set the USEADPAUT parameter to *NO.

With V3R2 and V3R7, you can use an authorization list and the use adopted authority (QUSEADPAUT) system value to control who can create programs that inherit adopted authority. When you specify an authorization list name in the QUSEADPAUT system value, the system uses this authorization list to determine how to create new programs.

When a user creates a program or service program, the system checks the user's authority to the authorization list. If the user has *USE authority, the USEADPAUT parameter for the new program is set to *YES. If the user does not have *USE authority, the USEADPAUT parameter is set to *NO. The user's authority to the authorization list cannot come from adopted authority.

The authorization list that you specify in the QUSEADPAUT system value also controls whether a user can use a CHGxxx command to set the USEADPAUT value for a program or a service program.

Following are two alternatives for using this function for working with the QUSEADPAUT system value.

Notes:

1. You do not need to call your authorization list QUSEADPAUT. You can create an authorization list with a different name. Then specify that authorization list for the QUSEADPAUT system value. In the commands in this example, substitute the name of your authorization list.
2. The QUSEADPAUT system value does not affect existing programs on your system. Use the CHGPGM command or the CHGSRVPGM command to set the USEADPAUT parameter for existing programs.

More Restrictive Environment: If you want most users to create new programs with the USEADPAUT parameter set to *NO, do the following:

1. To set the public authority for the authorization list to *EXCLUDE, type the following:

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
   AUT(*EXCLUDE)
```

2. To set up specific users to create programs that use the adopted authority of previous programs, type the following:

```
ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
   AUT(*USE)
```

Less Restrictive Environment: If you want most users to create new programs with the USEADPAUT parameter set to *YES, do the following:

1. Leave the public authority for the authorization list set to *USE.
2. To prevent specific users from creating programs that use the adopted authority of previous programs, type the following:

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(user-name) AUT(*EXCLUDE)
```

Monitoring the Use of Trigger Programs

DB2 UDB for AS/400 provides the capability to associate trigger programs with database files. Trigger-program capability is common across the industry for high-function database managers.

When you associate a trigger program with a database file, you specify when the trigger program runs. For example, you can set up the customer order file to run a trigger program whenever a new record is added to the file. When the customer's outstanding balance exceeds the credit limit, the trigger program can print a warning letter to the customer and send a message to the credit manager.

Trigger programs are a productive way both to provide application functions and to manage information. Trigger programs also provide the ability for someone with devious intentions to create a "Trojan horse" on your system. A destructive program may be sitting and waiting to run when a certain event occurs in a database file on your system.

Note: In history, the Trojan horse was a large hollow wooden horse that was filled with Greek soldiers. After the horse was introduced within the walls of Troy, the soldiers climbed out of the horse and fought the Trojans. In the computer world, a program that hides destructive functions is often called a Trojan horse.

SECBATCH menu options:
27 *to submit immediately* **66** *to use the job scheduler*

When your system ships, the ability to add a trigger program to a database file is restricted. If you are managing object authority carefully, the typical user will not have sufficient authority to add a trigger program to a database file. (Appendix D in the *Security - Reference* book tells the authority that is required or all commands, including the Add Physical File Trigger (ADDPFTRG) command.

You can use the Print Trigger Programs (PRTTRGPGM) command to print a list of all the trigger programs in a specific library or in all libraries. Figure 17 shows an example of the report:

```
                                Trigger Programs (Full Report)

Specified library  . . . . . :   CUSTLIB
                                 Trigger       Trigger       Trigger       Trigger       Trigger
Library       File               Library       Program       Time          Event         Condition
CUSTLIB       MB106              ARPGMLIB      INITADDR      Before        Update        Always
CUSTLIB       MB107              ARPGMLIB      INITNAME      Before        Update        Always
```

Figure 17. Print Trigger Programs Report-Full Report Example

You can use the initial report as a base to evaluate any trigger programs that already exist on your system. Then, you can print the changed report regularly to see whether new trigger programs have been added to your system.

When you evaluate trigger programs, consider the following:

- Who created the trigger program? You can use the Display Object Description (DSPOBJD) command to determine this.
- What does the program do? You will have to look at the source program or talk to the program creator to determine this. For example, does the trigger program check to see who the user is? Perhaps the trigger program is waiting for a particular user (QSECOFR) in order to gain access to system resources.

After you have established a base of information, you can print the changed report regularly to monitor new trigger programs that have been added to your system. Figure 18 shows an example of the changed report:

```
                                Trigger Programs (Changed Report)

Specified library  . . . . . :   LIBX
Last changed report  . . . . . :   96/01/21  14:33:37
                                 Trigger       Trigger       Trigger       Trigger       Trigger
Library       File               Library       Program       Time          Event         Condition
INVLIB        MB108              INVPGM        NEWPRICE      After         Delete        Always
INVLIB        MB110              INVPGM        NEWDSCNT      After         Delete        Always
```

Figure 18. Print Trigger Programs Report-Changed Report Example

The *DB2 UDB for AS/400 Database Programming* book has more information about the security issues that are associated with using trigger programs.

Checking for Hidden Programs

Trigger programs are not the only possible way to introduce a Trojan horse into your system. Trigger programs are an example of an **exit program**. When a certain event occurs, such as a file update in the case of a trigger program, the system runs the exit program that is associated with that event.

Table 14 describes other examples of exit programs that might be on your system. You should use the same methods for evaluating the use and content of these exit programs that you use for trigger programs.

Note: Table 14 is not a complete list of possible exit programs.

Table 14. System-Provided Exit Programs

Program Name	When the Program Runs
User-specified name on the DDMACC network attribute.	When a user attempts to open a DDM file on your system or makes a DRDA connection.
User-specified name on the PCSACC network attribute.	When a user attempts to use Client Access functions using the Original Clients to access objects on your system.
User-specified name on the QPWDVLDPGM system value	When a user runs the Change Password function.
User-specified name on the QRMTSIGN system value.	When a user attempts to sign on interactively from a remote system.
QSYS/QEZUSRCLNP	When the automatic cleanup function runs.
User-specified name on the EXITPGM parameter of the CHGBCKUP command.	When you use the Operation Assistant backup function.
User-specified names on the CRTPRDLOD command.	Before and after you save, restore, or delete the product that was created with the command.
User-specified name on the DFTPGM parameter of the CHGMSGD command.	If a default program is specified for a message, the system runs the program when the message is issued. Because of the large number of message descriptions on a typical system, the use of default programs is difficult to monitor. To prevent public users from adding default programs for messages, consider setting the public authority for message files (*MSGF objects) to *USE.
User-specified name on the FKEYPGM parameter of the STREML3270 command.	When the user presses a function key during the 3270 device emulation session. The system returns control to the 3270 device emulation session when the exit program ends.
User-specified name on the EXITPGM parameter of the performance monitor commands	To process data that is collected by the following commands: STRPFRMON, ENDPFRMON, ADDPFRCOL, and CHGPFRCOL. The program runs when data collection ends.
User-specified name on the EXITPGM parameter of the RCVJRNE command.	For each journal entry that it reads from the specified journal receiver.
User-specified name on the QTNADDCR API.	During a COMMIT or ROLLBACK operation.
User-specified names on the QHFRGFS API.	To perform the file system functions.
User-specified name on the SEPPGM parameter of a printer device description	To determine what to print on the separator page before or after a spooled file or a print job.
QGPL/QUSCLSXT	When a database file is closed to allow the capture of file usage information.

Table 14. System-Provided Exit Programs (continued)

Program Name	When the Program Runs
User-specified name on the FMTSLR parameter of a logical file.	When a record is written to the database file and a record format name is not included in the high-level language program. The selector program receives the record as input, determines the record format used, and returns it to the database.
User-specified name that is specified in the QATNPGM system value, the ATNPGM parameter in a user profile, or the PGM parameter of the SETATNPGM command.	When a user presses the Attention key.
User-specified name on the EXITPGM parameter of the TRCJOB command.	Before starting the Trace Job procedure.

For commands that allow you to specify an exit program, you should ensure that the command default has not been changed to specify an exit program. You should also ensure that the public authority for these commands is not sufficient to change the command default. The CHGCMDDFT command requires *OBJMGT authority to the command. You do not need *OBJMGT authority to run a command.

Evaluating Registered Exit Programs

You can use the system registration function to register exit programs that should be run when certain events occur. To list the registration information on your system, type `WRKREGINF OUTPUT(*PRINT)`. Figure 19 shows an example of the report:

```
                Work with Registration Information
Exit point . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Exit point format  . . . . . . . . . . . :   NJE00100
Exit point registered  . . . . . . . . . :   *YES
Allow deregister . . . . . . . . . . . . :   *YES
Maximum number of exit programs  . . . . :   *NOMAX
Current number of exit programs  . . . . :   0
Preprocessing for add  . . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for remove . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for retrieve . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
```

Figure 19. Work with Registration Information-Example

For each exit point on the system, the report shows whether any exit programs are currently registered. When an exit point has programs that are currently registered, you can select option 8 (Display programs) from the display version of WRKREGINF to display information about the programs:

```
                    Work with Registration Information

Type options, press Enter.
5=Display exit point   8=Work with exit programs

                          Exit
     Exit                 Point
Opt  Point                Format    Registered  Text
     QIBM_QGW_NJEOUTBOUND NJE00100     *YES     Network Job Entry outbound ex
8    QIBM_QHQ_DTAQ        DTAQ0100     *YES     Original Data Queue Server
     QIBM_QLZP_LICENSE    LICM0100     *YES     Original License Mgmt Server
     QIBM_QMF_MESSAGE     MESS0100     *YES     Original Message Server
     QIBM_QNPS_ENTRY      ENTR0100     *YES     Network Print Server - entry
     QIBM_QNPS_SPLF       SPLF0100     *YES     Network Print Server - spool
     QIBM_QNS_CRADDACT    ADDA0100     *YES     Add CRQ description activity
     QIBM_QNS_CRCHGACT    CHGA0100     *YES     Change CRQ description activi
```

Use the same method for evaluating these exit programs that you use for other exit programs and trigger programs.

Checking Scheduled Programs

AS/400 provides several methods for scheduling jobs to run at a later time, including the job scheduler and the OfficeVision calendar. Normally, these methods do not represent a security exposure because the user who schedules the job must have the same authority that is required to submit the job to batch.

However, you should periodically check for jobs scheduled in the future. A disgruntled user who is no longer in the organization may use this method to schedule a disaster.

Restricting Save and Restore Capability

Most users do not need to save and restore objects on your system. The save commands provide the possibility of copying important assets of your organization to media or to another system. Most save commands support save files that can be sent to another system (by using the SNDNETF file command) without having access to media or a save/restore device.

Restore commands provide the opportunity to restore unauthorized objects, such as programs, commands, and files, to your system. You can also restore information without access to media or to a save/restore device by using save files. Save files can be sent from another system by using the SNDNETF command or by using the FTP function.

Following are suggestions for restricting save and restore operations on your system:

- Control which users have *SAVSYS special authority. *SAVSYS special authority allows the user to save and restore objects even when the user does not have the necessary authority to the objects.
- Control physical access to save and restore devices (tape units).
- Restrict access to the save and restore commands. When you install either V4R3 or V3R7 of the OS/400 licensed programs, the public authority for the RSTxxx commands is *EXCLUDE. Public authority for the SAVxxx commands is *USE. Consider changing the public authority for SAVxxx commands to *EXCLUDE. Carefully limit the users that you authorize to the RSTxxx commands.

- Use the QALWOBJRST system value to restrict restoration of system-state programs and programs that adopt authority.
- Use security auditing to monitor restore operations. Include *SAVRST in the QAUDLVL system value, and periodically print audit records that are created by restore operations. (Chapter 9 and Appendix F of the *Security - Reference* book provide more information about the audit entries operations.)

Checking for User Objects in Protected Libraries

Every AS/400 job has a library list. The library list determines the sequence in which the system searches for an object if a library name is not specified with the object name. For example, when you call a program without specifying where the program is, the system searches your library list in order and runs the first copy of the program that it finds.

The *Security - Reference* book provides more information about the security exposures of library lists and calling programs without a library name (called an **unqualified call**). It also provides suggestions for controlling the content of library lists and the ability to change the system library lists.

For your system to run properly, certain system libraries, such as QSYS and QGPL, must be in the library list for every job. You should use object authority to control who can add programs to these libraries. This helps to prevent someone from placing an imposter program in one of these libraries with the same name as a program that appears in a library later in the library list.

You should also evaluate who has authority to the CHGSYSLIBL command and monitor SV records in the security audit journal. A devious user could place a library ahead of QSYS in the library list and cause other users to run unauthorized commands with the same names as IBM-supplied commands.

SECBATCH menu options:
28 *to submit immediately* **67** *to use the job scheduler*

You can use the Print User Objects (PRTUSROBJ) command to print a list of user objects (objects not created by IBM) that are in a specified library. You can then evaluate the programs on the list to determine who created them and what function they perform.

User objects other than programs can also represent a security exposure when they are in system libraries. For example, if a program writes confidential data to a file whose name is not qualified, that program might be fooled into opening an imposter version of that file in a system library.

Figure 20 on page 74 shows an example of the report:

User Objects (Full Report)

Library	Object	Type	Attribute	Owner	Description
QSYS	PRTCUSTL	*PGM	RPG	GEORGE	
QSYS	CHGLMT	*PGM	RPG	GEORGE	
QSYS	TESTINV	*PGM	CLP	ROSE	

Figure 20. Print User Objects Report-Sample

Note: This report includes objects that PTF exit programs create in the library.

Chapter 10. More Tips for Preventing and Detecting Mischief

This chapter is a collection of miscellaneous tips to help you to detect potential security exposures and mischief-makers.

Tips for Physical Security

Your system unit represents an important business asset and a potential door into your system. Some system components inside the system are both small and valuable. You should place the system unit in a controlled location to prevent someone from removing valuable system components.

The system unit has a control panel that provides the ability to perform basic functions without a workstation. For example, you can use the control panel to do the following:

- Stop the system.
- Start the system.
- Load the operating system.
- Start service functions.

All of these activities can disrupt your system users. They also represent a potential security exposure to your system. You can use the keylock that comes with your system to control when these activities are allowed. To prevent the use of the control panel, place the keylock in the Secure position, remove the key, and store it in a safe place.

Notes:

1. If you need to perform remote IPLs or perform remote diagnostics on your system, you may need to choose another setting for the keylock. The *Basic System Operation, Administration, and Problem Handling* book provides more information about the keylock settings.
2. Not all system models come with a keylock as a standard feature.

Tips for Monitoring User Profile Activity

User profiles provide entry to your system. Parameters in the user profile determine a user's environment and a user's security characteristics. As a security administrator, you need to control and audit changes that occur to user profiles on your system.

You can set up security auditing so that your system writes a record of changes to user profiles. You can use the DSPAUDJRNE command to print a report of those changes.

You can create exit programs to evaluate requested actions to user profiles. Table 15 on page 76 shows the exit points that are available for user profile commands.

Note: User profile exits are available beginning with V3R2.

Table 15. Exit Points for User Profile Activity

User Profile Command	Exit Point Name
Create User Profile (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Change User Profile (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Delete User Profile (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Restore User Profile (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

Your exit program can, for example, look for changes that might cause the user to run an unauthorized version of a program. These changes might be assigning either a different job description or a new current library. Your exit program might either notify a message queue or take some action (like changing or disabling the user profile) based on the information that the exit program receives.

The *Security - Reference* book provides more information about the exit programs for user profile actions.

Tips for Monitoring Subsystem Descriptions

When you start a subsystem on AS/400, the system creates an environment for work to enter the system and run. A subsystem description defines what that environment looks like. Subsystem descriptions, therefore, can provide an opportunity for devious users. A mischief-maker might use a subsystem description to start a program automatically or to make it possible to sign on without a user profile.

When you run the Revoke Public Authority (RVKPUBAUT) command, the system sets public authority to subsystem description commands to *EXCLUDE. This prevents users who are not specifically authorized (and who do not have *ALLOBJ special authority) from changing or creating subsystem descriptions.

The topics that follow provide suggestions for reviewing the subsystem descriptions that currently exist on your system. You can use the Work with Subsystem Descriptions (WRKSBSD) command to create a list of all the subsystem descriptions. When you select 5 (Display) from the list, you see a menu like the one shown in Figure 21 for the system description that you selected. It shows a list of the parts of a subsystem environment.

```
                    Display Subsystem Description

Subsystem description:   QINTER         Library:   QSYS
Status:   ACTIVE

Select one of the following:

     1. Operational attributes
     2. Pool definitions
     3. Autostart job entries
     4. Work station name entries
     5. Work station type entries
     6. Job queue entries
     7. Routing entries
     8. Communications entries
     9. Remote location name entries
    10. Prestart job entries
```

Figure 21. Display Subsystem Description Display

You select options to see details about the parts. Use the Change Subsystem Description (CHGSBSD) command to change the first two items on the menu. To change other items, use the appropriate add, remove, or change command for the entry type. For example, to change a workstation entry, use the Change Workstation Entry (CHGWSE) command.

The *Work Management* book provides more information about working with subsystem descriptions. It also lists the shipped values for IBM-supplied subsystem descriptions.

Tips for Autostart Job Entries

An autostart job entry contains the name of a job description. The job description may contain request data (RQSDTA) that causes a program or a command to run. For example, the RQSDTA might be `CALL LIB1/PROGRAM1`. Whenever the subsystem starts, the system will run the program PROGRAM1 in library LIB1.

Look at your autostart job entries and the associated job descriptions. Ensure that you understand the function of any program that runs automatically when a subsystem starts.

Tips for Workstation Names and Workstation Types

When a subsystem starts, it allocates all unallocated workstations that are listed (specifically or generically) in its entries for workstation names and workstations types. When a user signs on, the user is signing on to the subsystem that has allocated the workstation.

The workstation entry tells what job description will be used when a job starts at that workstation. The job description may contain request data that causes a program or a command to run. For example, the RQSDTA parameter might be `CALL LIB1/PROGRAM1`. Whenever a user signs on to a workstation in that subsystem, the system will run PROGRAM1 in LIB1.

Look at your workstation entries and the associated job descriptions. Ensure that no one has added or updated any entries to run programs that you are not aware of.

A workstation entry might also specify a default user profile. For certain subsystem configurations, this allows someone to sign on simply by pressing the Enter key. If the security level (QSECURITY system value) on your system is less than 40, you should review your workstation entries for default users.

Tips for Job Queue Entries

When a subsystem starts, it allocates any unallocated job queues that are listed in the subsystem description. Job queue entries do not provide any direct security exposure. However, they do provide an opportunity for someone to tamper with system performance by causing jobs to run in unintended environments.

You should periodically review the job queue entries in your subsystem descriptions to ensure that batch jobs are running where you expect them to run.

Tips for Routing Entries

A routing entry defines what a job does once it enters the subsystem. The subsystem uses routing entries for all job types: batch, interactive, and communications jobs. A routing entry specifies the following:

- The class for the job. Like job queue entries, the class that is associated with a job can affect its performance but does not represent a security exposure.
- The program that runs when the job starts. Look at the routing entries and ensure that no one has added or updated any entries to run programs that you are not aware of.

Tips for Communications Entries and Remote Location Names

When a communications job enters your system, the system uses the communications entries and the remote location name entries in the active subsystem to determine how the communications job will run. Look at the following for these entries:

- All subsystems are capable of running communications jobs. If a subsystem that you intend for communications is not active, a job that is trying to enter your system might find an entry in another subsystem description that meets its needs. You need to look at the entries in all subsystem descriptions.
- A communications entry contains a job description. The job description may contain request data that runs a command or program. Look at your communications entries and their associated job descriptions to ensure that you understand how jobs will start.
- A communications entry also specifies a default user profile that the system uses in some situations. Make sure that you understand the role of default profiles. If your system contains default profiles, you should ensure that they are profiles with minimal authority. See Chapter 12. Tips for Securing APPC Communications for more information about default user profiles.

  You can use the Print Subsystem Description (PRTSBSDAUT) command to identify communications entries that specify a user profile name.

Tips for Prestart Job Entries

You can use prestart job entries to make a subsystem ready for certain kinds of jobs so that the jobs start more quickly. Prestart jobs may start when the subsystem starts or when they are needed. A prestart job entry specifies the following:

A program to run

A default user profile

A job description

All of these provide the potential for security exposures. You should make sure that prestart job entries perform only authorized, intended functions.

Tips for Jobs and Job Descriptions

Job descriptions contain request data and routing data that can cause a specific program to run when that job description is used. When the job description specifies a program in the request data parameter, the system runs the program. When the job description specifies routing data, the system runs the program that is specified in the routing entry that matches the routing data.

The system uses job descriptions for both interactive and batch jobs. For interactive jobs, the workstation entry specifies the job description. Typically, the workstation entry value is *USRPRF, so the system uses the job description that is specified in the user profile. For batch jobs, you specify the job description when you submit the job.

You should periodically review job descriptions to make sure that they do not run unintended programs. You should also use object authority to prevent changes to job descriptions. *USE authority is sufficient to run a job with a job description. A typical user does not need *CHANGE authority to job descriptions.

SECBATCH menu options:
15 *to submit immediately* **54** *to use the job scheduler*

Job descriptions can also specify what user profile the job should run under. With security level 40 and higher, you must have *USE authority to the job description and to the user profile that is specified in the job description. With security levels lower than 40, you need *USE authority only to the job description.

You can use the Print Job Description Authority (PRTJOBDAUT) command to print a list of job descriptions that specify user profiles and have public authority of *USE. Figure 22 on page 80 shows an example of the report:

```
                    Job Descriptions with Excess Authority (Full Report)

                                                                SYSTEM4
  Specified library . . . . . :  QGPL
                                                  ---------------------Special Authorities----------------------
          Job                            User     *ALL   *AUD    *IOSYS    *JOB    *SAV    *SEC    *SER    *SPL
Library   Description    Owner           Profile   OBJ    IT       CFG      CTL     SYS     ADM     VICE     CTL
QGPL      JOBD1          QSECOFR         USERA
QGPL      JOBD2          QSECOFR         USERB      X      X        X        X       X       X       X       X
```

Figure 22. Job Descriptions with Excess Authority Report-Example

The report shows the special authorities of the user profile that is specified in the job description. The report includes the special authorities of any group profiles that the user profile has. You can use the following command to display the user profile's private authorities:

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

The job description specifies the library list that the job uses when it runs. If someone can change a user's library list, that user might run an unintended version of a program in a different library. You should periodically review the library lists that are specified in the job descriptions on your system.

Finally, you should ensure that the default values for the Submit Job (SBMJOB) command and the Create User Profile (CRTUSRPRF) command have not been changed to point to unintended job descriptions.

Tips for Architected Transaction Program Names

Some communications requests send a specific type of signal to your system. This request is called an **architecture transaction program name (TPN)** because the name of the transaction program is part of the APPC architecture for the system. A request for display station pass-through request is an example of an architecture TPN. Architecture TPNs are a normal way for communications to function and do not necessarily represent a security exposure. However, architecture TPNs may provide an unexpected entrance into your system.

Some TPNs do not pass a profile on the request. If the request becomes associated with a communications entry whose default user is *SYS, the request may be initiated on your system. However, the *SYS profile can run system functions only, not user applications.

If you do not want architecture TPNs to run with a default profile, you can change the default user from *SYS to *NONE in communications entries. Table 16 on page 81 lists the architecture TPNs and the associated user profiles.

If you do not want a specific TPN to run on your system at all, do the following:

1. Create a CL program that accepts several parameters. The program should perform no function. It should simply have the Declare (DCL) statements for parameters and then end.
2. Add a routing entry for the TPN to each subsystem that has communications entries or remote location name entries. The routing entry should specify the following:
   - A *Compare value* (CMPVAL) value equal to the program name for the TPN (see Table 16) with a starting position of 37.

- A *Program to call* (PGM) value equal to the name of the program that you created in step 1 on page 80. This prevents the TPN from locating another routing entry, such as *ANY.

Several TPNs already have their own routing entry in the QCMN subsystem. These have been added for performance reasons.

Architected TPN Requests

Table 16. Programs and Users for Architected TPN Requests

TPN Request	Program	User Profile	Description
X'30F0F8F1'	AMQCRC6A	*NONE	Message queuing
X'06F3F0F1'	QACSOTP	QUSER	APPC sign-on transaction program
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC configuration
X'30F0F1F9'	QCNPCSUP	*NONE	Shared folders
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Remote SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–PC receiver
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–PC sender
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 Server
X'30F0F6F0'	QHQTRGT	*NONE	PC data queue
X'30F0F8F0'	QLZPSERV	*NONE	Client Access license manager
X'30F0F1F7'	QMFRCVR	*NONE	PC message receiver
X'30F0F1F8'	QMFSNDR	*NONE	PC message sender
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 workstation controller
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	System management utilities
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I network print server
X'30F0F7F9'	QOCEVOKE	*NONE	Cross-system calendar
X'30F0F6F1'	QOKCSUP	QDOC	Directory shadowing
X'20F0F0F7'	QOQSESRV	QUSER	DIA Version 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA Version 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA Version 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA Version 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 pass-through
X'30F0F0F9'	QPAPAST2	QUSER	Printer pass-through
X'30F0F4F6'	QPWFSTP0	*NONE	Shared Folders Type 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access file server
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access file server
X'30F0F6F9'	QRQSRVX	*NONE	Remote SQL–converged server
X'30F0F6F5'	QRQSRV0	*NONE	Remote SQL without commit
X'30F0F6F4'	QRQSRV1	*NONE	Remote SQL without commit
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT

Table 16. Programs and Users for Architected TPN Requests (continued)

TPN Request	Program	User Profile	Description
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 receiver
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 sender
X'30F0F1F6'	QTFDWNLD	*NONE	PC transfer function
X'30F0F2F4'	QTIHNPCS	QUSER	TIE function
X'30F0F1F5'	QVPPRINT	*NONE	PC virtual print
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I data access server
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS receiver
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS sender
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I data queue server
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I remote command server
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I central server

Methods for Monitoring Security Events

Setting up security is not a one-time effort. You need to constantly evaluate both the changes on your system and your security failures. Then make adjustments to your security environment to respond to what you have discovered.

The security reports help you to monitor security-relevant changes that occur on your system. Following are other system functions that you can use to help you to detect security failures or exposures:

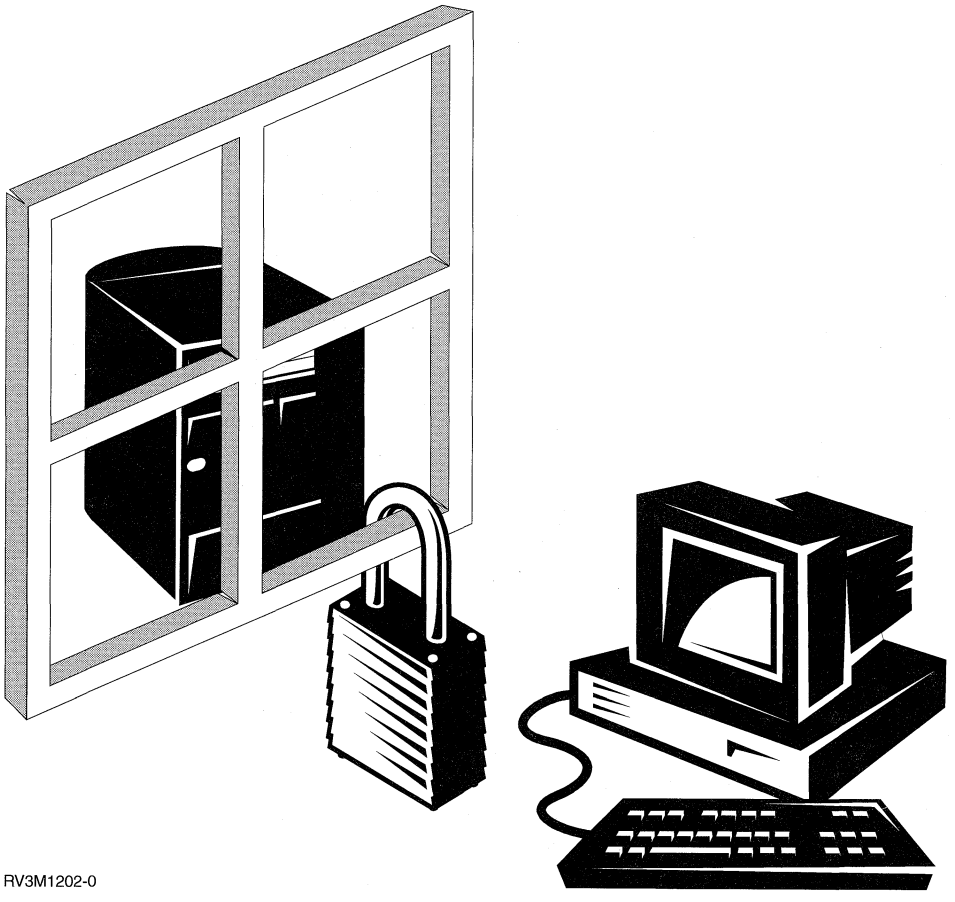
- Security auditing is a powerful tool that you can use to observe many different types of security-relevant events that occur on your system. For example, you can set up the system to write an audit record every time a user opens a particular database file for updating. You can audit all changes to system values. You can audit actions that happen when users restore objects.

  Chapter 9 in the *Security - Reference* book provides complete information about the security auditing function. You can use the Change Security Auditing (CHGSECAUD) command to set up security auditing on your system. You can also use the Display Audit Journal Entries (DSPAUDJRNE) command to print selected information from the security audit journal.
- You can create the QSYSMSG message queue to capture critical system-operator messages. The QSYSOPR message queue receives many messages of varying importance throughout a typical business day. Critical, security-relevant messages may be overlooked because of the sheer volume of messages in the QSYSOPR message queue.

  If you create a QSYSMSG message queue in the QSYS library on your system, the system automatically directs certain critical messages to the QSYSMSG message queue instead of to the QSYSOPR message queue.

  Either you can create a program to monitor the QSYSMSG message queue, or you can assign it in break mode to yourself or to another trusted user.

Part 4. Tips for Applications and Network Communications



RV3M1202-0

Chapter 11. Tips for Securing the Integrated File System

The integrated file system provides you with multiple ways to store and view information on AS/400. The integrated file system is a part of the OS/400 operating system that supports stream input and output operations. It provides storage management methods that are similar to (and compatible with) personal computer operating systems and UNIX operating systems.

Prior to V3R1, AS/400 stored and presented objects from the perspective of libraries (or folders for document library objects). With the integrated file system, all objects on the system can be viewed from the perspective of a hierarchical directory structure. However, in most cases, users view objects in the way that is most common for a particular file system. For example, "traditional" AS/400 objects are in the QSYS.LIB file system. Typically, users view these objects from the perspective of libraries. Users typically view objects in the QDLS file system from the perspective of documents within folders. The root (/), QOpenSys, and user-defined file systems present a structure of hierarchical (nested) directories.

As a security administrator, you need to understand the following:

- Which file systems are used on your system
- The unique security characteristics of each file system

The topics that follow provide some general considerations for the security of the integrated file system.

The Integrated File System Approach to Security

The root file system acts as an umbrella (or a foundation) for all other file systems on AS/400. At a high level, it provides an integrated view of all of the objects on the system. Other file systems that can exist on AS/400 provide varying approaches to object management and integration, depending on the underlying purpose of each file system. The QOPT (optical) file system, for example, allows AS/400 applications and servers (including the Client Access file server) to access the CD-ROM drive on the AS/400. Similarly, the QFileSvr.400 file system allows applications to access integrated file system data on remote AS/400s. The QLANSrv file server allows access to files stored on Integrated Netfinity Server for AS/400s or other connected servers in the network.

The security approach for each file system depends on the data that the file system makes available. The QOPT file system, for example, does not provide object-level security because no technology exists to write authority information to a CD-ROM. For the QFileSvr.400 file system, access control occurs at the remote system (where the files are physically stored and managed). For file systems like QLANSrv, the Integrated Netfinity Server for AS/400 provides access control. Despite the differing security models, many file systems support consistent management of access control through the integrated file system commands, such as Change Authority (CHGAUT) and Change Owner (CHGOWN).

Following are considerations for several representative file systems. For more information about a specific file system on your AS/400, you will need to consult the documentation for the licensed program that uses the file system.

Security Tips for the Root (/), QOpenSys, and User-Defined File Systems

Following are security considerations for the root, QOpenSys, and user-defined file systems.

How Authority Works for the Root (/), QOpenSys, and User-Defined File Systems

The root, QOpenSys, and user-defined file systems provide a blending of AS/400, PC, and UNIX** capabilities both for object management and for security. When you use the integrated file system commands from an AS/400 session (WRKAUT and CHGAUT), you can set all the normal AS/400 object authorities. This includes the *R, *W, and *X authorities that are compatible with Spec 1170 (UNIX-type operating systems).

Note: The root, QOpenSys, and user-defined file systems are functionally equivalent. The QOpenSys file system is case-sensitive. The root file system is not. User-defined file systems can be defined as case-sensitive. Because these file systems have the same security characteristics, you can assume in the topics that follow that their names are used interchangeably.

When you access the root file system as an administrator from a PC session, you can set object attributes that the PC uses to restrict certain types of access:

- System
- Hidden
- Archive
- Read-only

These PC attributes are in addition to, not replacements for, AS/400 object authority values.

When a user attempts to access an object in the root file system, OS/400 enforces all of the object authority values and attributes for the object, whether or not those authorities are "visible" from the user's interface. For example, assume that the read-only attribute for an object is set on. A PC user cannot delete the object through a Client Access interface. An AS/400 user with a fixed function workstation cannot delete the object either, even if the AS/400 user has *ALLOBJ special authority. Before the object can be deleted, an authorized user must use a PC function to reset the read-only value to `off`. Similarly, a PC user might not have sufficient OS/400 authority to change the PC-relevant security attributes of an object.

UNIX-type applications that run on AS/400 use UNIX-like application programming interfaces (APIs) to access data in the root file system. With UNIX-like APIs, applications can recognize and maintain the following security information:

- Object owner
- Group owner (AS/400 primary group authority)
- Read (files)
- Write (change contents)
- Execute (run programs or search directories)

The system maps these data authorities to existing AS/400 object and data authorities:

- Read (*R) = *OBJOPR and *READ
- Write (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Execute (*X) = *OBJOPR and *EXECUTE

The concepts for other object authorities (*OBJMGT, *OBJEXIST, *OBJALTER, and *OBJREF) do not exist in a UNIX-type environment.

However, these object authorities do exist for all of the objects in the root file system. When you create an object using a UNIX-like API, that object inherits these authorities from the parent directory, resulting in the following:

- The new object's owner has the same object authority as the parent directory's owner.
- The new object's primary group has the same object authority as the parent directory's primary group.
- The new object's public has the same object authority as the parent directory's public.

The new object's data authority for owner, primary group, and public are specified on the API with the mode parameter. When all of the object authorities are set 'on', you get the authority behavior that you would expect in a UNIX-type environment. It is best to leave them set 'on', unless you do not want the POSIX-like behavior.

When you run applications that use UNIX-like APIs, the system enforces all object authorities, whether or not they are "visible" to UNIX-type applications. For example, the system will enforce the authority of authorization lists even though the concept of authorization lists does not exist in UNIX-type operating systems.

When you have a mixed-application environment, you need to ensure that you do not make authority changes in one environment that will break your applications in another environment.

Working with Security for the Root (/), QOpenSys, and User-Defined File Systems

With the introduction of the integrated file system, AS/400 also provided a new set of commands for working with objects in multiple file systems. This command set includes commands for working with security:

- Change Auditing (CHGAUD)
- Change Authority (CHGAUT)
- Change Owner (CHGOWN)
- Change Primary Group (CHGPGP)
- Display Authority (DSPAUT)
- Work with Authority (WRKAUT)

These commands group the underlying data and object authorities into the UNIX-like authority subsets:

***RWX** Read/write/execute

***RW** Read/write

***R** Read

***WX** Write/execute

***W** Write

***X** Execute

In addition, UNIX-like APIs are available to work with security.

Public Authority to the Root Directory

When your system ships, the public authority to the root directory is *ALL (all object authorities and all data authorities). This setting provides flexibility and compatibility with both what UNIX-like applications expect and what typical AS/400 users expect. An AS/400 user with command-line capability can create a new library in the QSYS.LIB file system simply by using the CRTLIB command. Normally, authority on a typical AS/400 system allows this. Similarly, with the shipped setting for the root file system, a typical user can create a new directory in the root file system (just like you can create a new directory on your PC).

As a security administrator, you must educate your users about adequately protecting the objects that they create. When a user creates a library, probably the public authority to the library should not be *CHANGE (the default). The user should set public authority either to *USE or to *EXCLUDE, depending on the contents of the library.

If your users need to create new directories in the root (/), QOpenSys, or user-defined file systems, you have several security options:

- You can educate your users to override the default authority when they create new directories. The default is to inherit authority from the immediate parent directory. In the case of a newly created directory in the root directory, by default the public authority will be *ALL.
- You can create a "master" subdirectory under the root directory. Set the public authority on that master directory to an appropriate setting for your organization. Then instruct users to create any new personal directories in this master subdirectory. Their new directories will inherit its authority.
- You can consider changing the public authority for the root directory to prevent users from creating objects in that directory. (Remove *W, *OBJEXIST, *OBJALTER, *OBJREF, and *OBJMGT authorities.) However, you need to evaluate whether this change will cause problems for any of your applications. You might, for example, have UNIX-like applications that expect to be able to delete objects from the root directory.

Print Private Authorities Objects (PRTPVTAUT) command

The Print Private Authorities (PRTPVTAUT) command allows you to print a report of all the private authorities for objects of a specified type in a specified library, folder, or directory. The report lists all objects of the specified type and the users that are authorized to the object. This is a way to check for different sources of authority to objects.

This command prints three reports for the selected objects. The first report (Full Report) contains all of the private authorities for each of the selected objects. The second report (Changed Report) contains additions and changes to the private authorities to the selected objects if the PRTPVTAUT command was previously run for the specified objects in the specified library, folder, or directory. Any new objects of the selected type, new authorities to existing objects, or changes to existing authorities to the existing objects are listed in the 'Changed Report'. If the

PRTPVTAUT command was not previously run for the specified objects in the specified library, folder, or directory, there will be no 'Changed Report'. If the command has been previously run but no changes have been made to the authorities on the objects, then the 'Changed Report' is printed but there are no objects listed.

The third report (Deleted Report) contains any deletions of privately authorized users from the specified objects since the PRTPVTAUT command was previously run. Any objects that were deleted or any users that were removed as privately authorized users are listed in the 'Deleted Report'. If the PRTPVTAUT command was not previously run, there will be no 'Deleted Report'. If the command has been previously run but no delete operations have been done to the objects, then the 'Deleted Report' is printed but there are no objects listed.

Restriction: You must have *ALLOBJ special authority to use this command.

Examples:

This command creates the full, changed, and deleted reports for all file objects in the PAYROLLLIB:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

This command creates the full, changed, and deleted reports for all the stream file objects in the directory garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

This command creates the full, changed, and deleted reports for all the stream file objects in the subdirectory structure that starts at the directory garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

Print Publicly Authorized Objects (PRTPUBAUT) command

The Print Publicly Authorized Objects (PRTPUBAUT) command allows you to print a report of the specified objects that do not have public authority of *EXCLUDE. For *PGM objects, only the programs that do not have public authority of *EXCLUDE that a user can call (the program is either user domain or the system security level (QSECURITY system value) is 30 or below) will be included in the report. This is a way to check for objects that every user on the system is authorized to access.

This command will print two reports. The first report (Full Report) will contain all of the specified objects that do not have public authority of *EXCLUDE. The second report (Changed Report) will contain the objects that now do not have public authority of *EXCLUDE that did have public authority of *EXCLUDE or did not exist when the PRTPUBAUT command was previously run. If the PRTPUBAUT command was not previously run for the specified objects and library, folder, or directory, there will be no 'Changed Report'. If the command has been previously run, but no additional objects do not have public authority of *EXCLUDE, then the 'Changed Report' will be printed but there will be no objects listed.

Restrictions: You must have *ALLOBJ special authority to use this command.

Examples:

This command creates the full, and changed reports for all the file objects in the library GARRY that do not have a public authority of *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

This command creates the full, changed, and deleted reports for all the stream file objects in the subdirectory structure that starts at the directory garry that do not have a public authority of *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

Restricting Access to the QSYS.LIB File System

Because the root file system is the umbrella file system, the QSYS.LIB file system appears as a subdirectory within the root directory. Therefore, any PC user with access to your AS/400 can manipulate objects stored in AS/400 libraries (the QSYS.LIB file system) with normal PC commands and actions. A PC user could, for example, drag a QSYS.LIB object (such as the library with your critical data files) to the shredder.

As you learned in "Security Tips for the Root (/), QOpenSys, and User-Defined File Systems" on page 86, the system enforces all object authority whether or not it is visible to the interface. Therefore, a user cannot shred (delete) an object unless the user has *OBJEXIST authority to the object. However, if your AS/400 depends on menu access security rather than object security, the PC user might very well discover objects in the QSYS.LIB file system that are available for shredding.

As you expand the uses of your system and the different methods of access that you provide, you will soon discover that menu access security is not sufficient. "Chapter 7. Using Object Authority to Protect Information Assets" on page 49 discusses your strategies for supplementing menu access control with object security. However, AS/400 also provides a simple way for you to prevent access to the QSYS.LIB file system through the root file system directory structure. You can use the QPWFSERVER authorization list to control which users can access the QSYS.LIB file system through the root directory.

When a user's authority to the QPWFSERVER authorization list is *EXCLUDE, the user cannot enter the QSYS.LIB directory from the root directory structure. When a user's authority is *USE, the user can enter the directory. Once the user has authority to enter the directory, normal object authority applies for any action the user attempts to perform on an object within the QSYS.LIB file system. In other words, the authority to the QPWFSERVER authorization list acts like a door to the entire QSYS.LIB file system. For the user with *EXCLUDE authority, the door is locked. For the user with *USE authority (or any greater authority), the door is open.

For most situations, users do not need to use a directory interface to access objects in the QSYS.LIB file system. Probably, you will want to set the public authority to the QPWFSERVER authorization list to *EXCLUDE. Keep in mind, that authority to the authorization list opens or closes the door to all libraries within the QSYS.LIB file system, including user libraries. If you encounter users who object to this exclusion, you can evaluate their requirements on an individual basis. If appropriate, you can explicitly authorize an individual user to the authorization list. However, you need to ensure that the user has appropriate authority to objects within the QSYS.LIB file system. Otherwise, the user might unintentionally delete objects or entire libraries.

Notes:

1. When your system ships, the public authority to the QPWFSERVER authorization list is *USE.
2. If you explicitly authorize an individual user, the authorization list controls access only with Client Access file serving and NetServer file serving. This does not prevent access to the same directories via FTP, ODBC, and other networks.

Securing Directories

To access an object within the root file system, you read through the entire path to that object. To search a directory, you must have *X (*OBJOPR and *EXECUTE) authority to that directory. Assume, for example, that you want to access the following object:

```
/companya/customers/custfile.dat
```

You must have *X authority to the `companya` directory and to the `customers` directory.

With the root file system, you can create a symbolic link to an object. Conceptually, a symbolic link is an alias for a path name. Usually, it is shorter and easier to remember than the full path name. A symbolic link does not, however, create a different physical path to the object. The user still needs *X authority to every directory and subdirectory in the physical path to the object.

For objects in the root file system, you can use directory security just as you might use library security in the QSYS.LIB file system. You can, for example, set the public authority of a directory to *EXCLUDE to prevent public users from accessing any objects within that tree.

Security for New Objects

When you create a new object in the root file system, the interface that you use to create it determines its authorities. For example, if you use the CRTDIR command and its defaults, the new directory inherits all of the authority characteristics of its parent directory, including private authorities, primary group authority, and authorization list association. The following sections describe how authorities are determined for each type of interface.

Authority comes from the immediate parent directory, not from directories higher up in the tree. Therefore, as a security administrator, you need to view the authority that you assign to directories in a hierarchy from two perspectives:

- How the authority affects access to objects in the tree (like library authority).
- How the authority affects newly created objects (like the CRTAUT value for libraries).

Recommendation: You may want to give users who work in the integrated file system a home directory (for example, /home/usrxxx), then set the security appropriately (such as PUBLIC *EXCLUDE). Any directories the user creates under their home directory will then inherit the authorities.

Following are the descriptions of authority inheritance for different interfaces:

Using the AS/400 Create Directory Command

When you create a new subdirectory by using the CRTDIR command, you have two options for specifying authority:

- You can specify the public authority (data authority, object authority, or both).
- You can specify *INDIR for the data authority, object authority, or both. When you specify *INDIR for both data authority and object authority, the system makes an exact copy of all the authority information from the parent directory to the new object, including authorization list, primary group, public authority, and private authorities. (The system does not copy private authority that the QSYS profile or the QSECOFR profile has to the object.)

Creating a Directory with an API

When you create a directory by using the mkdir() API, you specify the data authorities for the owner, the primary group, and public (using the authority map of *R, *W, and *X). The system uses the information in the parent directory to set the object authorities for the owner, primary group, and public.

Because UNIX-type operating systems do not have the concept of object authorities, the mkdir() API does not support specifying object authorities. If you want different object authorities, you can use the AS/400 command (CHGAUT). However, when you remove some object authorities, the UNIX-like application might not work as you expect it to work.

Creating a Stream File with the open() or creat() API

When you use the creat() API to create a stream file, you can specify the data authorities for the owner, the primary group, and public (using the UNIX-like authorities of *R, *W, and *X). The system uses the information in the parent directory to set the object authorities for the owner, primary group, and public.

You can also specify these authorities when you use the open() API to create a stream file. Alternatively, when you use the open() API you can specify that the object should inherit all authorities from the parent directory. This is called `inherit mode`. When you specify inherit mode, the system then creates a complete match for the parent authorities, including authorization list, primary group, public authority, and private authorities. This option works like specifying *INDIR on the CRTDIR command.

Creating an Object by Using a PC Interface

When you use a PC application to create an object in the root file system, the system automatically inherits all authority from the parent directory. This includes authorization list, primary group, public authority, and private authorities. PC applications do not have any equivalent to specifying authority when you create an object.

Security Tips for the QLANSrv and QNetWare File Systems

The purpose of both the QLANSrv file system and the QNetWare file system is to provide AS/400 jobs with the ability to access data on a network server. An AS/400 job uses the QLANSrv file system to make a client request for data to the LAN Server program. The LAN Server program can be running on an Integrated PC Server on the same AS/400 system, or it might be running on a physically separate server in the network.

Note: The QLANSrv file system is not supported beyond V4R3.
Similarly, an AS/400 job uses the QNetWare file system to make a client request for data to the NetWare Integration program, which might be running on an Integrated Netfinity Server for AS/400 or another server.

Neither the QLANSrv file system nor the QNetWare file system actually stores or maintains any data. They provide the client function to allow AS/400 jobs to access data that is stored and maintained on a server. Therefore, the server program (LAN Server or NetWare Integration) has responsibility for securing the data.

As an AS/400 security administrator, you should consider several things when a server program runs on an Integrated PC Server or Integrated Netfinity Server for AS/400 that is part of your system:

- First, understand who has responsibility for server-related security. Do you have an administrator for the server and does that person have responsibility for security? Or is that data considered part of your AS/400 application suite and thus, part of your responsibility? Be sure that server security is not ignored simply because the administrative roles are not well-defined.
- If your security responsibility is broader than your traditional AS/400 applications, you need to understand how server security works. The following suggestions use the LAN Server program as a starting point. Other server programs have similar security considerations.
  - LAN Server users do not pose a direct threat to your system. They cannot access data outside the QLANSrv file system from the LAN Server program.
  - You and the LAN administrator need to understand that recovering LAN Server users and authorities is different from recovering AS/400 users and authorities. You need to make plans to ensure that your LAN Server security information is being saved correctly.

Security Tips for the QFileSvr.400 File System

With the QFileSvr.400 file system, a user (USERX) on one AS/400 system (SYSTEMA) can access data on another connected AS/400 system (SYSTEMB). The USERX has an interface that is just like the Client Access interface. The remote AS/400 (SYSTEMB) appears as a directory with all its file systems as subdirectories.

When USERX attempts to access SYSTEMB with this interface, SYSTEMA sends USERX's user profile name and encrypted password to SYSTEMB. The same user profile and password must exist on SYSTEMB or SYSTEMB rejects the request.

If SYSTEMB accepts the request, USERX appears to SYSTEMB just like any Client Access user. The same authority-checking rules apply to any actions that USERX attempts.

As a security administrator, you need to be aware that the QFileSvr.400 file system represents another possible door to your system. You cannot assume that you are limiting your remote users to an interactive sign on with display station passthrough. If you have the QSERVER subsystem running and your system is connected to another AS/400 system, remote users can access your system as if they are on a local PC running Client Access. More than likely, your system will have a connection that needs to have the QSERVER subsystem running. This is yet another reason why a good object authority scheme is essential.

Security Tips for the Network File System

The Network File System (NFS) provides access to and from systems that have NFS implementations. NFS is an industry-standard method for sharing information among users on networked systems. Most major operating system (including PC operating systems) provide NFS. For UNIX systems, NFS is the primary method for accessing data. AS/400 can act as both an NFS client and an NFS server.

When you are the security administrator of an AS/400 system that acts as an NFS server, you need to understand and manage the security aspects of NFS. Following are suggestions and considerations:

- You must explicitly start the NFS server function by using the STRNFSSVR command. Control who has authority to use this command.
- You make a directory or an object available to NFS clients by `exporting` it. Therefore, you have very specific control over which parts of your system you will make available to NFS clients in your network.
- When you export, you can specify which clients have access to the objects. You identify a client by system name or IP address. A client can be an individual PC or an entire AS/400 or UNIX system. In NFS terminology, the client (IP address) is called a `machine`.
- When you export, you can specify read-only access or read/write access for each machine that has access to an exported directory or object. In most cases, you will probably want to provide read-only access.
- The NFS does not provide password protection. It is designed and intended for data sharing within a trusted community of systems. When a user requests access, the server receives the user's `uid`. Following are some `uid` considerations:
  - The AS/400 attempts to locate a user profile with the same `uid`. If it finds a matching `uid`, it uses the credentials of the user profile. Credentials is an NFS term to describe using the authority of a user. This is similar to profile swapping in other AS/400 applications.
  - When you export a directory or object, you can specify whether you will allow access by a profile with root authority. The NFS server on AS/400 equates root authority to *ALLOBJ special authority. If you specify that you will not allow root authority, an NFS user with a `uid` that maps to a user profile with *ALLOBJ special authority will not be able to will not be able to access the object under that profile. Instead, if anonymous access is allowed, the requester will be mapped to the anonymous profile.
  - When you export a directory or object, you can specify whether you will allow anonymous requests. An anonymous request is a request with a `uid` that does not match any `uid` on your system. If you choose to allow anonymous requests, the system maps the anonymous user to the IBM-supplied QNFSANON user profile. This user profile does not have any special

authorities or explicit authority. (On the export, you can specify a different user profile for anonymous requests if you want.)

- When your AS/400 participates in an NFS network (or any network with UNIX systems that depend on `uids`), you probably need to manage your own `uids` instead of letting the system assign them automatically. You will need to coordinate `uids` with other systems in your network.

  You might discover that you need to change `uids` (even for IBM-supplied user profiles) to have compatibility with other systems in your network. Beginning with V3R7, a program is available to make it simpler to change the `uid` for a user profile. (When you change the `uid` for a user profile, you also need to change the `uid` for all the objects that the profile owns in either the root directory or the QOpenSrv directory.) The QSYCHGID program automatically changes the `uid` in both the user profile and all the owned objects. For information about how to use this program, see the *System API Reference*, SC41-5801-03 book.

Chapter 12. Tips for Securing APPC Communications

When your system participates in a network with other systems, a new set of doors and windows to your system becomes available. As security administrator, you should be aware of the options that you can use to control the entrances to your system in an APPC environment.

Advanced program-to-program communications (APPC) is a way that computers, including personal computers, communicate with each other. Display station passthrough, distributed data management, and Client Access can all use APPC communications.

The topics that follow provide some basic information about how APPC communications works and how you can set up appropriate security. These topics concentrate primarily on the security-relevant elements of an APPC configuration. To adapt this example to your situation, you will need to work with the people who manage your communications network and perhaps your application providers. Use this information as a foundation to help you understand the security issues and the options that are available for APPC.

Security is never "free". Some suggestions for making network security easier may make network administration more difficult. For example, this book does not emphasize APPN (Advanced Peer-to-Peer Networking), because security is easier to understand and manage without APPN. However, without APPN, the network administrator must manually create configuration information that APPN creates automatically.

PCs Use Communications, too

Many methods for connecting PCs to your AS/400 depend on communications, such as APPC or TCP/IP. When you read the topics the following, be sure to consider the security issues for connecting both to other systems and to PCs. When you plan your network protection, make sure that you do not adversely affect the PCs that are attached to your system.

APPC Terminology

APPC provides the ability for a user on one system to perform work on another system. The system from which the request starts is called any of the following:

- **Source system**
- **Local system**
- **Client**

The system that receives the request is called any of the following:

- **Target system**
- **Remote system**
- **Server**

Basic Elements of APPC Communications

From the perspective of a security administrator, the following must happen before a user on one system (SYSTEMA) can perform meaningful work on another system (SYSTEMB):

- The source system (SYSTEMA) must provide a path to the target system (SYSTEMB). This path is called an **APPC session**.
- The target system must identify the user and associate the user with a user profile.
- The target system must start a job for the user with an appropriate environment (work management values).

The topics that follow discuss these elements and how they relate to security. The security administrator on the target system has primary responsibility for ensuring that APPC users do not violate security. However, when the security administrators on both systems work together, the job of managing APPC security is much easier.

The Basics of an APPC Session

In an APPC environment, when a user or application on one system (such as SYSTEMA in Figure 23) requests access to another system (SYSTEMB), the two systems set up a session. To establish the session, the systems must link two matching APPC device descriptions. The remote location name (RMTLOCNAME) parameter in the SYSTEMA device description must match the local location name (LCLLOCNAME) parameter in the SYSTEMB device description and vice versa.

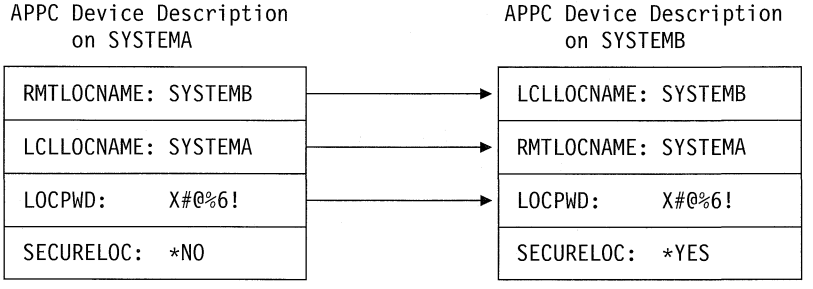


Figure 23. APPC Device Description Parameters

For the two systems to establish an APPC session, the location passwords in the APPC device descriptions on SYSTEMA and SYSTEMB must be identical. Both must specify *NONE, or both must specify the same value.

If the passwords are a value other than *NONE, they are stored and transmitted in encrypted format. If the passwords match, the systems establish a session. If the passwords do not match, the user's request is rejected. When systems specify location passwords to establish a session, this is called a **secure bind**.

Note: Not all computer systems provide support for the secure bind function.

Tips for Restricting APPC Sessions

As security administrator on a source system, you can use object authority to control who can attempt to access other systems. Set the public authority for APPC

device descriptions to *EXCLUDE and give *CHANGE authority to specific users. Use the QLMTSECOFR system value to prevent users with *ALLOBJ special authority from using APPC communications.

As security administrator on a target system, you can also use authority to APPC devices to prevent users from starting an APPC session on your system. However, you need to understand what user ID will be attempting to access the APPC device description. "How an APPC User Gains Entrance to the Target System" describes how AS/400 associates a user ID with a request for an APPC session.

Note: You can use the Print Publicly Authorized Objects (PRTPUBAUT *DEVD) command and the Print Private Authorities (PRTPVTAUT *DEVD) command to find out who has authority to device descriptions on your system.

When your system uses APPN, it automatically creates a new APPC device when no existing device is available for the route that the system has chosen. One method for restricting access to APPC devices on a system that is using APPN is to create an authorization list. The authorization list contains the list of users who should be authorized to APPC devices. You then use the Change Command Default (CHGCMDDFT) command to change the CRTDEVAPPC command. For the authority (AUT) parameter on the CRTDEVAPPC command, set the default value to the authorization list that you created.

Note: If your system has a language other than English, you need to change the command default in the QSYSxxxx library for each national language that is on your system.

You use the location password (LOCPWD) parameter in the APPC device description to validate the identity of another system that is requesting a session on your system (on behalf of a user or an application). The location password can help you detect an imposter system.

When you use location passwords, you must coordinate with security administrators for other systems in the network. You must also control who can create or change APPC device descriptions and configuration lists. The system requires *IOSYSCFG special authority to use the commands that work with APPC devices and configuration lists.

Note: When you use APPN, the location passwords are stored in the QAPPNRMT configuration list rather than in device descriptions.

How an APPC User Gains Entrance to the Target System

When the systems establish the APPC session, they create a path for the requesting user to get to the door of the target system. Several other elements determine what the user must do to gain entrance to the other system.

The topics that follow describe the elements that determine how an APPC user gains entrance to the target system.

Methods That the System Uses to Send Information about a User

APPC architecture provides three methods for sending security information about a user from the source system to the target system. These methods are referred to as the **architected security values**. Table 17 shows these methods:

Note: The *APPC Programming* book provides more information about the architected security values.

Table 17. Security Values in the APPC Architecture

Architected Security Value	User ID Sent to Target System	Password Sent to Target System
None	No	No
Same	Yes[1]	See note 2.
Program	Yes	Yes[3]

Notes:

1. The source system sends the user ID if the target system specifies SECURELOC(*YES) or SECURELOC(*VFYENCPWD).
2. The user does not enter a password on the request because the password is already verified by the source system. For SECURELOC(*YES) and SECURELOC(*NO), the source system does not send the password. For SECURELOC(*VFYENCPWD), the source system retrieves the stored, encrypted password and sends it (in encrypted form).
3. On V3R1 and later versions, the system sends the password in encrypted form if both the source and target systems support password encryption. Otherwise, the password is not encrypted.

The application that the user requests determines the architected security value. For example, SNADS always uses SECURITY(NONE). DDM uses SECURITY(SAME). With display station passthrough, the user specifies the security value by using parameters on the STRPASTHR command.

In all cases, the target system chooses whether to accept a request with the security value that is specified on the source system. In some situations, the target system may reject the request completely. In other situations, the target system may force a different security value. For example, when a user specifies both a user ID and a password on the STRPASTHR command, the request uses SECURITY(PGM). However, if the QRMTSIGN system value is *FRCSIGNON on the target system, the user still sees a Sign On display. With the *FRCSIGNON setting, the systems always use SECURITY(NONE), which is the equivalent of the user entering no user ID and password on the STRPASTHR command.

Notes:

1. The source and target systems negotiate the security value before data is sent. In the situation where the target system specifies SECURELOC(*NO) and the request is SECURITY(SAME), for example, the target system tells the source system to use SECURITY(NONE). The source system does not send the user ID.
2. Beginning with V4R2, the target system rejects a session request when the user's password on the target system has expired. This applies only to connection requests that send a password, including the following:
   - Session requests of type SECURITY(PROGRAM).
   - Session requests of type SECURITY(SAME) when the SECURELOC value is *VFYENCPWD.

Options for Dividing Security Responsibility in a Network

When your system participates in a network, you must decide whether to trust the other systems to validate the identity of a user who is trying to enter your system. Will you trust SYSTEMA to ensure that USERA is really USERA (or QSECOFR is really QSECOFR)? Or will you require a user to provide a user ID and password again?

The secure location (SECURELOC) parameter on the APPC device description on the target system specifies whether the source system is a secure (trusted) location. For example, in Figure 23 on page 98, SYSTEMB trusts SYSTEMA to validate user identities (the SECURELOC parameter in the device description on SYSTEMB is *YES). SYSTEMA does not trust SYSTEMB to validate user identities.

When both systems are running a release that supports *VFYENCPWD (V3R2 or later), SECURELOC(*VFYENCPWD) provides additional protection when applications use SECURITY(SAME). Although the requester does not enter a password on the request, the source system retrieves the user's password and sends it with the request. For the request to be successful, the user must have the same user ID and password on both systems.

When the target system specifies SECURELOC(*VFYENCPWD) and the source system does not support this value, the target system handles the request as SECURITY(NONE).

Table 18 shows how the architected security value and the SECURELOC value work together:

Table 18. How the APPC Security Value and the SECURELOC Value Work Together

Source System	**Target System**	
Architected Security Value	**SECURELOC Value**	**User Profile for Job**
None	Any	Default user[1]
Same	*NO	Default user[1]
	*YES	Same user profile name as requester from source system
	*VFYENCPWD	Same user profile name as requester from source system. The user must have the same password on both systems.
Program	Any	The user profiles that is specified on the request from the source system.

Notes:

1. The default user is determined by the communications entry in the subsystem description. "How the Target System Assigns a User Profile for the Job" describes this.

How the Target System Assigns a User Profile for the Job

When a user requests an APPC job on another system, the request has a mode name associated with it. The mode name may come from the user's request, or it may be a default value from the network attributes of the source system.

The target system uses the mode name and the APPC device name to determine how the job will run. The target system searches the active subsystems for a communications entry that is the best match for the APPC device name and the mode name.

The communications entry specifies what user profile the system will use for SECURITY(NONE) requests. Following is an example of a communications entry in a subsystem description:

```
                        Display Communications Entries

Subsystem description:   QCMN           Status:   ACTIVE

                          Job                             Default         Max
Device        Mode        Description    Library          User          Active
*ALL          *ANY        *USRPRF                         *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                         *NONE         *NOMAX
```

Table 19 shows the possible values for the default user parameter in a communications entry:

Table 19. Possible Values for the Default User Parameter

Value	Result
***NONE**	No default user is available. If the source system does not supply a user ID on the request, the job will not run.
***SYS**	Only IBM-supplied programs (system jobs) will run. No user applications will run.
user-name	If the source system does not send a user ID, the job runs under this user profile.

You can use the Print Subsystem Description (PRTSBSDAUT) command to print a list of all subsystems that have communications entries with a default user profile.

Options for Display Station Passthrough

Display station passthrough is an example of an application that uses APPC communications. You can use display station passthrough to sign on to another system that is connected to your system through a network.

Table 20 on page 103 shows examples of passthrough requests (STRPASTHR command) and how the target system handles them. For display station passthrough, the system uses the basic elements of APPC communications and the remote sign-on (QRMTSIGN) system value.

Note: Display Station Passthrough requests are no longer routed through the QCMN or QBASE subsystems. Beginning with V4R1, they are routed through the QSYSWRK subsystem. Prior to V4R1 you could assume that by not having QCMD or QBASE subsystems started, Display Station Passthrough would not work. This is no longer true. You can force Display Station Passthrough to go through QCMN (or QBASE if it is active) by changing the QPASTHRSVR system value to 0.

Table 20. Sample Pass-Through Sign-On Requests

Values on STRPASTHR Command		Target System		
User ID	**Password**	**SECURELOC Value**	**QRMTSIGN Value**	**Result**
*NONE	*NONE	Any	Any	The user must sign on the target system.
A user profile name	Not entered	Any	Any	The request fails.
*CURRENT	Not entered	*NO	Any	The request fails
		*YES	*SAMEPRF	An interactive job starts with the same user profile name as the user profile on the source system.No password is passed to the remote system.The user profile name must exist on the target system.
			*VERIFY	
			*FRCSIGNON	The user must sign on the target system.
		*VFYENCPWD	*SAMEPRF	An interactive job starts with the same user profile name as the user profile on the source system.The source system retrieves the user's password and sends it to the remote system.The user profile name must exist on the target system.
			*VERIFY	
			*FRCSIGNON	The user must sign on the target system.
*CURRENT (or the name of the current user profile for the job)	Entered	Any	*SAMEPRF	An interactive job starts with the same user profile name as the user profile on the source system.The password *is* sent to the remote system.The user profile name must exist on the target system.
			*VERIFY	
			*FRCSIGNON	The user must sign on the target system.
A user profile name (a name different from the current user profile for the job)	Entered	Any	*SAMEPRF	The request fails.
			*VERIFY	An interactive job starts with the same user profile name as the user profile on the source system.The password *is* sent to the remote system.The user profile name must exist on the target system.
			*FRCSIGNON	An interactive job starts with the specified user profile name. The password is sent to the target system. The user profile name must exist on the target system.

Tips for Avoiding Unexpected Device Assignments

When a failure occurs on an active device, the system attempts to recover. In some circumstances, when the connection is broken, another user can unintentionally reestablish the session that had the failure. For example, assume that USERA powered off a workstation without signing off. USERB could power on the workstation and restart USERA's session without signing on.

To prevent this possibility, set the Device I/O Error Action (QDEVRCYACN) system value to *DSCMSG. When a device fails, the system will end the user's job.

Tips for Controlling Remote Commands and Batch Jobs

Several options are available to help you control what remote commands and jobs can run on your system, including the following:

- If your system uses DDM, you can restrict access to DDM files to prevent users from using the Submit Remote Command (SBMRMTCMD) command from another system. To use the SBMRMTCMD, the user must be able to open a DDM file. You also need to restrict the ability to create DDM files.
- You can specify an exit program for the DDM request access (DDMACC) system value. In the exit program, you can evaluate all DDM requests before allowing them.
- You can use the network job action (JOBACN) network attribute to prevent network jobs from being submitted or to prevent them from running automatically.
- You can specify explicitly which program requests can run in a communications environment by removing the PGMEVOKE routing entry from subsystem descriptions. The PGMEVOKE routing entry allows the requester to specify the program that runs. When you remove this routing entry from subsystem descriptions, such as the QCMN subsystem description, you must add routing entries for the communications requests that need to run successfully.

  Table 16 on page 81 lists the program names for the communications requests by IBM-supplied applications. For each request that you want to allow, you can add a routing entry with the compare value and the program name both equal to the program name.

  When you use this method, you need to understand the work management environment on your system and the types of communications requests that occur on your system. If possible, you should test all types of communications requests to ensure that they work properly after you change the routing entries. When a communications request does not find an available routing entry, you receive a CPF1269 message. Another alternative (less error-prone but perhaps slightly less effective) is to set the public authority to *EXCLUDE for the transaction programs that you do not want to run on your system.

  Note: The *Work Management* book provides more information about routing entries and how the system handles program-start requests.

Security Tips for Evaluating Your APPC Configuration

You can use the Print Communications Security (PRTCMNSEC) command or menu options to print the security-relevant values in your APPC configuration. The topics that follow describe the information on the reports.

Security-Relevant Parameters for APPC Devices

Figure 24 shows an example of the Communications Information Report for device descriptions. Figure 25 shows an example of the report for configuration lists. Following the reports are explanations of fields on the reports.

Communications Information (Full Report)

SYSTEM4

Object type . . . . : *DEVD

Object Name	Object Type	Device Category	Secure Location	Location Password	APPN Capable	Single Session	Pre Establish Session	SNUF Program Start
CDMDEV1	*DEVD	*APPC	*NO	*NO	*NO	*YES	*NO	
CDMDEV2	*DEVD	*APPC	*NO	*NO	*NO	*YES	*NO	

Figure 24. APPC Device Descriptions-Sample Report

Display Configuration List Page 1

SYSTEM4 12/17/95 07:24:36

Configuration list . . . . : QAPPNRMT
Configuration list type . . . . . : *APPNRMT
Text . . . . :

-----------------APPN Remote Locations-----------------

Remote Location	Remote Network ID	Local Location	Remote Control Point	Control Point Net ID	Secure Loc
SYSTEM36	APPN	SYSTEM4	SYSTEM36	APPN	*NO
SYSTEM32	APPN	SYSTEM4	SYSTEM32	APPN	*NO
SYSTEMU	APPN	SYSTEM4	SYSTEM33	APPN	*YES
SYSTEMJ	APPN	SYSTEM4	SYSTEMJ	APPN	*NO
SYSTEMR2	APPN	SYSTEM4	SYSTEM1	APPN	*NO

-------------------------APPN Remote Locations-------------------------

Remote Location	Remote Network ID	Local Location	Single Session	Number of Conversations	Local Control Point	Pre-established Session
SYSTEM36	APPN	SYSTEM4	*NO	10	*NO	*NO
SYSTEM32	APPN	SYSTEM4	*NO	10	*NO	*NO

Figure 25. Configuration List Report-Example

Secure Location Field

The secure location (SECURELOC) field specifies whether the local system trusts the remote system to do password verification on behalf of the local system. The SECURELOC field applies only to applications that use the SECURITY(SAME) value, such as DDM and applications that use the CPI-Communications API.

SECURELOC(*YES) makes the local system vulnerable to possible weaknesses in the remote system. Any user that exists on both systems can call programs on the local system. This is particularly dangerous because the QSECOFR (security officer) user profile exists on all AS/400 systems and has *ALLOBJ special authority. If a system in the network does not do a good job of protecting the QSECOFR password, other systems that treat that system as a secure location are at risk.

When you use SECURELOC(*VFYENCPWD), your system is less vulnerable to other systems that do not adequately protect passwords. A user who requests an application that uses SECURITY(SAME) must have the same user ID and

password on both systems. SECURELOC(*VFYENCPWD) requires password administration policies across your network so that users have the same password on all systems.

Note: SECURELOC(*VFYENCPWD) is supported only between systems that are running V3R2, V3R7, or V4R1. If the target system specifies SECURELOC(*VFYENCPWD) and the source system does not support this function, the request is treated as SECURITY(NONE).

If a system specifies SECURELOC(*NO), applications that use SECURITY(SAME) will need a default user to run programs. The default user depends on both the device description and the mode that are associated with the request. (See "How the Target System Assigns a User Profile for the Job" on page 101.)

Location Password Field

The location password field determines whether the two systems will exchange passwords to verify that the requesting system is not an imposter system. "The Basics of an APPC Session" on page 98 provides more information about location passwords.

APPN-Capable Field

The APPN-capable (APPN) field specifies whether the remote system can support advanced networking functions or is limited to single-hop connections. APPN(*YES) means the following:

- If the remote system is a network node, the remote system may be capable of connecting the local system to other systems. This is called **intermediate node routing**. It means that users on your system may be able to use the remote system as a route to a larger network.
- If the local system is a network node, the remote system can use the local system to connect to other systems. Users on the remote system may be able to use your system as a route to a larger network.

  Note: You can use the DSPNETA command to determine whether a system is a network node or an end node.

Single Session Field

The single session (SNGSSN) field specifies whether the remote system can run more than one session at a time by using the same APPC device description. SNGSSN(*NO) is commonly used because it eliminates the need to create multiple device descriptions for a remote system. For example, a PC user often wants more than one 5250-emulation session and sessions for file-server and print-server functions. With SNGSSN(*NO), you can provide this function with one device description for the PC on the AS/400 system.

SNGSSN(*NO) means that you must rely on the security-conscious operating procedures of PC users and other APPC users. Your system is vulnerable to someone on the remote system who starts an unauthorized session that uses the same device description as an existing session. (This practice is sometimes referred to as **piggy-backing**.)

Pre-Establish Session Field

The pre-establish (PREESTSSN) session field for a single-session device controls whether the local system starts a session with the remote system when the remote system first contacts the local system. PREESTSSN(*NO) means that the local system waits to start a session until an application requests a session with the system. PREESTSSN(*YES) is useful for minimizing how long it takes for an application program to complete the connection.

PREESTSSN(*YES) prevents the system from disconnecting a switched (dial-up) line that is no longer being used. The application or the user must explicitly vary off the line. PREESTSSN(*YES) may lengthen the time that the local system is vulnerable to piggy-backing on the session.

SNUF Program Start Field

The SNUF program start field specifies whether the remote system is allowed to start programs on the local system. *YES means that the object authority scheme on the local system must be adequate to protect objects when users on the remote system start jobs and run programs on the local system.

Security-Relevant Parameters for APPC Controllers

Figure 26 shows an example of the Communications Information Report for controller descriptions. Following the report, you will find explanations of fields on the report.

```
                                 Communications Information (Full Report)
                                                                          SYSTEM4
Object type . . . . . . . . . :  *CTLD

Object    Object    Controller   Auto     Switched     Call       APPN      CP         Disconnect   Delete    Device
Name      Type      Category     Create   Controller   Direction  Capable   Sessions     Timer      Seconds   Name
CTL01     *CTLD     *APPC        *YES       *YES        *DIAL      *YES      *YES           0        1440     AARON
CTL02     *CTLD     *APPC        *YES       *YES        *DIAL      *YES      *YES           0        1440     BASIC
CTL03     *CTLD     *APPC        *YES       *YES        *DIAL      *YES      *YES           0        1440     *NONE
```

Figure 26. APPC Controller Descriptions-Sample Report

Auto-Create Field

On a line description, the auto-create (AUTOCRTCTL) field specifies whether the local system automatically creates a controller description when an incoming request cannot find a matching controller description. On a controller description, the auto-create (AUTOCRTDEV) field specifies whether the local system automatically creates a device description when an incoming request cannot find a matching device description.

For controllers that are APPN-capable, the auto-create field has no effect. The system automatically creates device descriptions when necessary, regardless of how you have set the auto-create field.

When you specify *YES for a line description, anyone with access to the line can connect to your system. This includes sites that are connected by bridges and routers.

Control Point Sessions Field

For APPN-capable controllers, the control point sessions (CPSSN) field controls whether the system establishes an APPC connection with the remote system automatically. The system uses the CP session to exchange network information and status with the remote system. The exchange of up-to-date information between APPN network nodes is particularly important so that your network functions smoothly.

When you specify *YES, an idle switched line does not disconnect automatically. This makes your system more vulnerable to a piggy-back session.

Disconnect Timer Field

For an APPC controller, the disconnect timer field specifies how long a controller must be unused (no active sessions) before the system disconnects the line to the remote system. This field has two values. The first value specifies how long the controller will stay active from the time it is initially contacted. The second value determines how long the system waits after the last session has ended on the controller before the system drops the line.

The system uses the disconnect timer only when the switched disconnect (SWTDSC) field is *YES.

If you make these values large, your system is more vulnerable to piggy-back sessions.

Security-Relevant Parameters for Line Descriptions

Figure 27 shows an example of the Communications Information Report for line descriptions. Following the report, you will find explanations of fields on the report.

```
                    Communications Information (Full Report)

Object type  . . . . . . . . . :   *LIND
Auto
Object         Object         Line           Auto      Delete      Auto      Auto
Name           Type           Category       Create    Seconds     Answer    Dial
LINE01          *LIND          *SDLC          *NO             0      *NO       *NO
LINE02          *LIND          *SDLC          *NO             0      *YES      *NO
LINE03          *LIND          *SDLC          *NO             0      *NO       *NO
LINE04          *LIND          *SDLC          *NO             0      *YES      *NO
```

Figure 27. APPC Line Descriptions-Sample Report

Auto Answer Field

The auto answer (AUTOANS) field specifies whether the switched line will accept incoming calls without operator intervention.

When you specify *YES, your system is less secure because it can be accessed more easily. To minimize the security exposure when you specify *YES, you should vary off the line when you do not need it.

Auto Dial Field

The auto dial (AUTODIAL) field specifies whether the switched line can make outgoing calls without operator intervention.

When you specify *YES, you allow local users who do not have physical access to communications lines and modems to connect to other systems.

Protecting Your System in an APPN Environment

APPN networks provide open connectivity and require minimal configuration by each system in the network. When a system has a connection into an APPN network, that system can establish sessions with other systems that are connected within that APPN network.

APPN reduces the physical, configuration barriers to communications. However, you might want to build some logical barriers between systems in the network for security reasons. AS/400 provides network administrators with the capability to specify which connections between APPC locations are allowed. For example, you might want to allow SYSTEMB to communicate with SYSTEMA and SYSTEMD, but not with SYSTEMC. The ability to control which systems can connect to your system is often called **firewall support**.

The topics that follow provide tips on how you can use APPN filtering support to create a control traffic function for your AS/400 network.

The following commands have parameters and options for APPN filtering support:

- ADDCFGLE (Add Configuration List Entries)
- CHGCFGL (Change Configuration List)
- CRTCFGL (Create Configuration List)
- RMVCFGLE (Remove Configuration List Entries)
- WRKCFGL (Work with Configuration Lists)

Note: The topics that follow provide security tips for an APPN network. For complete information about configuring and managing an APPN network, see the *APPN Support* book. For information about audit journal entries that are available for APPN filtering support, see Appendix F in the *Security - Reference* book.

System Types in an APPN Network–Overview

Figure 28 on page 110 shows an example of two connected APPN networks:

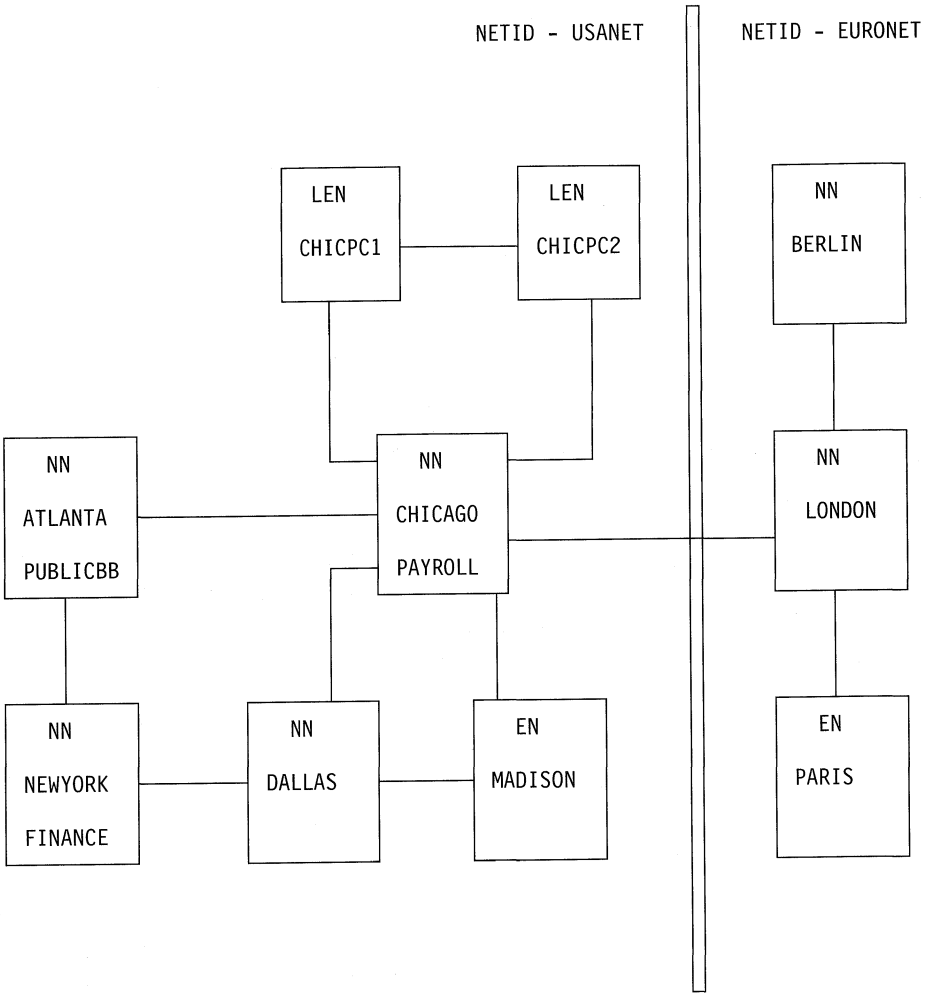


Figure 28. Sample APPN Network

The boxes in Figure 28 represent the following types of nodes in an APPN network:

- A **peripheral node** is at the edge of a network. It can participate in the network, but it cannot provide intermediate routing to other systems in the network. A peripheral node can be an **end node (EN)** such as MADISON and PARIS in Figure 28. A peripheral node can be a **low-entry networking node (LEN)**, such as CHICPC1 and CHICPC2 in Figure 28. A peripheral node can also be a network node in a different network (NETID). From CHICAGO's perspective, LONDON is a peripheral node.
- A **network node (NN)** provides routing services among systems in the network. In Figure 28, CHICAGO and ATLANTA are examples of network nodes.

APPN Filtering Support–Overview

APPN filtering support provides the ability to create a firewall that is based on APPC location names. You use two different types of filter lists:

- A **session endpoint filter** controls access to and from a location. For example, in Figure 28, the session endpoint filter on the CHICAGO system specifies which locations can establish a session with CHICAGO or with PAYROLL. CHICAGO and PAYROLL are two different locations on the CHICAGO system.

Similarly, the session endpoint filter on the MADISON system specifies which locations can establish a session with the MADISON location.

On AS/400, you can use the new QAPPNSSN configuration list, by itself or in conjunction with the QAPPNRMT configuration list, to create a session endpoint filter.

- A **directory search filter** on a network node determines the following for its associated peripheral nodes:
  - Access *from* the peripheral node (when the peripheral node is the requester). For example, in Figure 28, you can use the directory search filter on LONDON to control the possible destinations for users on the PARIS system. Similarly, you can use the directory search filter on CHICAGO to control the possible destinations for users on CHICPC1 and CHICPC2.
  - Access *to* the peripheral node (when the peripheral node is the destination). In Figure 28, for example, you can use the directory search filter on CHICAGO to determine which locations can access CHICPC1. Because both CHICAGO and DALLAS provide connections to MADISON, you must set up the directory search filters on both CHICAGO and DALLAS to restrict connections to MADISON.

    Similarly, you can use the directory search filter on CHICAGO to specify which USANET locations are permissible destinations for EURONET users.

  On AS/400, you use the new QAPPNDIR configuration list to create a directory search filter.

Tips for Using the Session Endpoint Filter

Figure 29 shows the display for viewing a session endpoint filter:

```
                  Display APPN Session Endpoint Filter CFGL
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNSSN
Default filter action . :   *REJECT
APPN remote CFGL filter :   *ACCEPT
Text description    . . :   Chicago's Session Endpoint Filter

Type options, press Enter.
5=Display

      Local
      location   Filter    Entry
Opt   name       action    description
```

Figure 29. Display APPN Session Endpoint Filter CFGL Display

The top part of the display specifies global attributes for the system. The bottom part of the display specifies information about specific locations.

The *Default filter action* field indicates whether the system accepts or rejects requests to connect with a system by using a local location that is not explicitly listed. The *APPN remote CFGL filter* field indicates how the QAPPNSSN configuration list (the session endpoint filter) works with the QAPPNRMT configuration list.

When you specify *ACCEPT for the *APPN remote CFGL filter* field, the system accepts remote location pairs that are specified in the QAPPNRMT configuration

list. This avoids the need to specify the same pair in both the QAPPNSSN configuration list and the QAPPNRMT configuration list.

Following are two different methods for creating a session endpoint filter on the CHICAGO system to satisfy the following requirements for the network inFigure 28 on page 110:

1. Only the FINANCE location can establish a session with the PAYROLL location.
2. The CHICAGO location can communicate with any USANET location except PAYROLL.
3. The CHICAGO location can communicate with LONDON.

Using the QAPPNSSN and QAPPNRMT Configuration Lists Together

The most secure method for creating a session endpoint filter is to use the QAPPNSSN configuration list and the QAPPNRMT configuration list together. The QAPPNRMT configuration list provides password security between systems, which helps to protect from an imposter system (a system or user that is pretending to be another system).

When you use this method, you create the QAPPNSSN configuration list to look like the example in Figure 29 on page 111. The QAPPNSSN configuration list does not specify any remote locations. It points to the QAPPNRMT configuration list.

The QAPPNRMT configuration list looks like Figure 30:

```
                          Display Configuration List

Configuration list . . . . . :   QAPPNRMT
Configuration list type  . . . . :   *APPNRMT
Text . . . . . :   Chicago's remote location list

-----------------------------------------APPN Remote Locations----------------
          Remote              Remote    Control
Remote    Network   Local     Control   Point     Secure      Single
Location  ID        Location  Point     Net ID    Loc         Session
FINANCE   USANET    PAYROLL             USANET    *NO         *NO
ATLANTA   USANET    CHICAGO             USANET    *NO         *NO
CHICPC1   USANET    CHICAGO             USANET    *NO         *NO
CHICPC2   USANET    CHICAGO             USANET    *NO         *NO
DALLAS    USANET    CHICAGO             USANET    *NO         *NO
FINANCE   USANET    CHICAGO             USANET    *NO         *NO
LONDON    EURONET   CHICAGO             USANET    *NO         *NO
MADISON   USANET    CHICAGO             USANET    *NO         *NO
NEWYORK   USANET    CHICAGO             USANET    *NO         *NO
PUBLICBB  USANET    CHICAGO             USANET    *NO         *NO
```

Figure 30. QAPPNRMT Configuration List Example

The drawback to this method is that you must explicitly define each location pair on the QAPPNRMT configuration list. If you want the CHICAGO location (which is on the same system as the PAYROLL location) to communicate with other locations, you need to add an entry for each pair.

Using the QAPPNSSN Configuration List by Itself

When you specify remote locations in the QAPPNSSN configuration list, your configuration task is simpler because you can use generic names and wildcard entries. However, when you use this method, you do not have the protection of password verification between locations. In addition, when you use generic names and wildcards, the system might accept or reject requests in a different way than you intended. "QAPPNSSN Configuration List–Search Sequence" on page 114 has more information about using generic names.

Figure 31 shows an example of what the QAPPNSSN configuration list would look like for the CHICAGO system when the CHICAGO system does not use the QAPPNRMT configuration list:

```
                  Display APPN Session Endpoint Filter CFGL
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNSSN
Default filter action . :   *REJECT
APPN remote CFGL filter :   *ACCEPT
Text description    . . :   Chicago's Session Endpoint Filter

Type options, press Enter.
5=Display

      Local
      location   Filter    Entry
Opt   name       action    description
      CHICAGO    *ACCEPT
      PAYROLL    *ACCEPT
```

Figure 31. QAPPNSSN Configuration List–Local Locations

When you type a 5 (Display) in the option column next to the CHICAGO location, you see the list of remote locations that can communicate with CHICAGO:

```
                Display APPN Session Endpoint Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNSSN
Default filter action . :   *REJECT
APPN remote CFGL filter :   *ACCEPT
Text description . . :   Chicago's Session Endpoint Filter

Remote        Remote
location      network       Entry
name          identifier    description
*ANY          USANET        All remote locations in USANET allowed
LONDON        EURONET       Only location from EURONET allowed
```

Figure 32. QAPPNSSN Configuration List–Remote Locations

When you type a 5 (Display) in the option column next to the PAYROLL location on Figure 31, you see the list of remote locations that can communicate with PAYROLL:

```
                    Display APPN Session Endpoint Filter Entries
                                                              System:   CHICAGO
Configuration list  . . :   QAPPNSSN
Default filter action . :   *REJECT
APPN remote CFGL filter :   *ACCEPT
Text description . . :   Chicago's Session Endpoint Filter

Remote          Remote
location        network       Entry
name            identifier    description
FINANCE         USANET        Only FINANCE can communicate with PAYROLL
```

Figure 33. QAPPNSSN Configuration List–Remote Locations

How the System Verifies that a Session Is Allowed

The session endpoint filter controls sessions when the local system is either the source system or the target system. The session endpoint filter validates both user sessions and control point sessions. When the local system is the source system, the system checks the session endpoint filter before it searches for the remote location. Assume that a PAYROLL user attempts to establish a session with MADISON. The system will not search for a route to MADISON because the endpoint session filter on the CHICAGO system does not allow a session between PAYROLL and MADISON.

When the local system is the target system, the system checks the endpoint session filter when the SNA bind request is received. For example, if a LONDON user requests a session with PAYROLL, the CHICAGO system will reject the bind request

When the local system rejects a session because the session endpoint filter does not allow the session, the SNA sense data is X'080F0001'. When the local system rejects a session because the QAPPNSSN configuration list is damaged, the SNA sense data is X'084F0002'. If the QAPPNSSN configuration list is damaged, you must delete it and re-create it. You can either create the configuration list again or use the Restore Configuration (RSTCFG) command to restore a backup copy.

QAPPNSSN Configuration List–Search Sequence

When a session request arrives, the local system searches the QAPPNSSN configuration list for the closest matching local location name. The system then searches for the closest matching remote location for that local location. The system takes action that is based on the value (*ACCEPT or *REJECT) of the entry that it finds.

Keep the search sequence in mind when you use generic names. Figure 34 shows an example of a generic location name that might be specified in the QAPPNSSN configuration list:

```
Local Location - LOCXYZ
   Remote Locations -   RLOC1
                        RLOC2
                        RLOC3

Local Location - LOC*
   Remote Locations -   LURMT1
                        LURMT2
                        LURMT3
```

Figure 34. Generic Location Names–Example

Assume that the local system receives the following bind request:

```
Local location   = LOCXYZ
Remote location  = LURMT1
```

The local system rejects this bind request because it starts by finding the closest match for the local location. The system finds LOCXYZ and searches the allowed remote locations for LOCXYZ. LURMT1 is not on the remote location list for LOCXYZ, so the system rejects the bind.

When the system finds entries that match in both the QAPPNSSN configuration list and the QAPPNRMT configuration list, the system uses the value in the QAPPNSSN configuration list. Although you can create location entries in both configuration lists, you should use one method or the other rather than a combination. When you place entries in both configuration lists, network management and problem analysis are more difficult.

Tips for Using the Directory Search Filter

The directory search filter on a network node controls how it handles intermediate routing requests to and from peripheral nodes. For example, in Figure 28 on page 110, you can use a directory search filter on CHICAGO to control which session requests are sent to the CHICPC1 system. In fact, if you are confident that your directory search filter on CHICAGO is correct and complete, you might not need to create an endpoint session filter on CHICPC1.

When your network provides more than one route to a system, you need to ensure that the entries in the directory search filter are the same in each network node. In Figure 28 on page 110, the directory search filters in both CHICAGO and DALLAS must provide protection for MADISON. Your protection is only as strong as your weakest network node.

Following are two examples of how you might use a directory search filter to protect the USANET network in Figure 28. The simple example focuses on protecting USANET locations from unauthorized access by EURONET locations. The extended example also uses the CHICAGO directory search filter to control access between USANET locations.

Directory Search Filter–Simple Example

The following list shows what connections should be allowed in the network in Figure 28 for this example:

1. Any USANET location can communicate with any other USANET location.
2. Any EURONET location can communicate with PUBLICBB, and PUBLICBB can communicate with any EURONET location.

Figure 35 shows the Directory Search Filter for the CHICAGO system to meet these requirements:

```
                  Display APPN Directory Search Filter CFGL
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description  . . :   Chicago's directory search filter

Type options, press Enter.
5=Display

     Filtered   Filtered
     control       CP
     point      network    Filter   Entry
Opt  name       identifier action   description
     *ANY        USANET    *ACCEPT
     LONDON      EURONET   *ACCEPT
```

Figure 35. Directory Search Filter–Example 1

On the display, the filtered control point is an adjacent node in the network. For example, LONDON is an adjacent node to CHICAGO. Logically, you can think of a filtered control point as outside the firewall.

When you use option 5 to display the details about the *ANY entry, you see the following:

```
                  Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered            Partner
CP        CP         Partner  location
location  location   location network   Entry
name      NETID      name     ID        description
*ANY      USANET     *ANY     USANET
```

Figure 36. Directory Search Filter–Example 2

When you use option 5 to display the details about LONDON, you see the following:

```
                  Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered            Partner
CP        CP         Partner  location
location  location   location network   Entry
name      NETID      name     ID        description
*ANY      EURONET    PUBLICBB USANET
```

Figure 37. Directory Search Filter–Example 3

On the display, a **filtered control point location** is a location on a peripheral node that is trying to gain access to the network. It is a location that can access the network through the filtered control point. In the example, LONDON, PARIS, and BERLIN are possible filtered control point locations.

A **partner location** is a location for which the network node has responsibility. Logically, a partner location is inside the firewall.

Keep in mind that APPC sessions are bidirectional. When you set up your system so that EURONET locations can establish a session with PUBLICBB, then PUBLICBB can also establish sessions with EURONET locations unless you explicitly prevent it.

Note: The administrator for the EURONET network can set up a similar directory search filter on the LONDON system to protect EURONET locations from unauthorized access by USANET locations.

Directory Search Filter–Extended Example

In this extended example, the CHICAGO system has the additional responsibility of limiting some connections *within* the USANET network. In this example, the CHICAGO system provides an internal firewall *and* an external firewall.

The following list shows what connections should be allowed in the network in Figure 28 on page 110:

1. All locations except PAYROLL can communicate with PUBLICBB.
2. Only FINANCE can communicate with PAYROLL.
3. CHICAGO can communicate with ATLANTA, CHICPC1, CHICPC2, DALLAS, FINANCE, LONDON, MADISON, NEWYORK.
4. LONDON can communicate with CHICAGO.
5. CHICPC1 can communicate with CHICAGO, CHICPC2, MADISON.
6. CHICPC2 can communicate with CHICAGO, CHICPC1, ATLANTA.
7. MADISON can communicate with CHICAGO, DALLAS, CHICPC1.

Figure 38 shows the Directory Search Filter for the CHICAGO system:

```
                  Display APPN Directory Search Filter CFGL
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description  . . :   Chicago's directory search filter

Type options, press Enter.
5=Display

     Filtered   Filtered
     control       CP
     point      network    Filter   Entry
Opt  name      identifier  action   description
     CHICPC1    USANET     *ACCEPT
     CHICPC2    USANET     *ACCEPT
     LONDON     EURONET    *ACCEPT
     MADISON    USANET     *ACCEPT
```

Figure 38. Directory Search Filter–Example 4

Figure 39 shows the directory search filter information for CHICPC1 (requirements 1 and 5 on page 117). Notice that in this example, the filtered control point is a system in the same network. From CHICAGO's perspective, a filtered control point can be any peripheral node that is trying to access locations in the network via CHICAGO.

```
                  Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered           Partner
CP        CP        Partner  location
location  location  location network   Entry
name      NETID     name     ID        description
CHICPC1   USANET    CHICPC2  USANET
CHICPC1   USANET    MADISON  USANET
CHICPC1   USANET    PUBLICBB USANET
```

Figure 39. Directory Search Filter–Example 5

Figure 40 shows the directory search filter information for CHICPC2 (requirements 1 and 6):

```
                  Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered           Partner
CP        CP        Partner  location
location  location  location network   Entry
name      NETID     name     ID        description
CHICPC2   USANET    ATLANTA  USANET
CHICPC2   USANET    CHICPC1  USANET
CHICPC2   USANET    PUBLICBB USANET
```

Figure 40. Directory Search Filter–Example 6

Figure 41 shows the directory search filter information for LONDON (requirement 1):

```
                  Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered           Partner
CP        CP        Partner  location
location  location  location network   Entry
name      NETID     name     ID        description
*ANY      EURONET   PUBLICBB USANET
```

Figure 41. Directory Search Filter–Example 7

Figure 42 on page 119 shows the directory search filter information for MADISON (requirements 1 and 7):

```
                Display APPN Directory Search Filter Entries
                                                          System:   CHICAGO
Configuration list  . . :   QAPPNDIR
Default filter action . :   *REJECT
Text description    . . :   Chicago's directory search filter

Filtered  Filtered            Partner
CP        CP        Partner   location
location  location  location  network   Entry
name      NETID     name      ID        description
MADISON   USANET    CHICPC1   USANET
MADISON   USANET    DALLAS    USANET
MADISON   USANET    PUBLICBB  USANET
```

Figure 42. Directory Search Filter–Example 8

Notice that CHICAGO's directory search filter does not address requirements 2 and 3. CHICAGO's session endpoint filter handles these requirements.

How a Network Node Evaluates a Request

A network node, such as CHICAGO in Figure 28 on page 110, can have both an endpoint session filter (QAPPNSSN) and a directory search filter (QAPPNDIR). When a network node receives a session request, the system determines whether it is the target of the session request or whether the target is on another system in the network. When the network node is the target, it uses the QAPPNSSN configuration list to determine whether the requested session is allowed. For example, if the CHICAGO system receives a request for a session with either CHICAGO or PAYROLL, the system uses the QAPPNSSN configuration list on the CHICAGO system to make the decision.

When the network node is not the target, it uses the QAPPNDIR configuration list to decide whether to route the request or to reject it. For example, if the CHICAGO system receives a request from LONDON for a session with MADISON, it would reject the request because LONDON is not defined as a partner location for MADISON. If the CHICAGO system receives a request from PARIS for a session with PUBLICBB, it would route the request to the ATLANTA system. This is because the QAPPNDIR entry for PUBLICBB allows a connection with any system on the EURONET network.

Note: When a network node does not have an endpoint session filter, the system evaluates all requests by using the entries in the directory search filter. Therefore, to be targets of sessions, allowable local locations must appear as partner locations on the directory search filter.

When the local system rejects a request because the directory search filter does not allow the session, the SNA sense data is X'080E0000'. When the local system rejects a session because the QAPPNDIR configuration list is damaged, the SNA sense data is X'084F0000'. If the QAPPNDIR configuration list is damaged, you must delete it and re-create it. You can either create the configuration list again or use the Restore Configuration (RSTCFG) command to restore a backup copy.

QAPPNDIR Configuration List–Search Sequence

When a network node receives a session request, it determines whether the request is for a local session or for intermediate routing. When the request is for a

local session, the system uses the QAPPNSSN configuration list, if it exists. The system follows the procedure that is described in "QAPPNSSN Configuration List–Search Sequence" on page 114.

When the request is for intermediate routing or when the QAPPNSSN configuration does not exist, the system begins by finding the closest match for the filtered control point name in the QAPPNDIR configuration list. The system then searches the entries for that filtered control point to find the closest filtered location name that matches. Finally, the system searches for the closest partner location name that matches. The system takes the action that is specified in that entry.

Additional Tips for Using APPN Filtering Support

Following are some additional suggestions for using the APPN filtering support to protect systems in your APPN network:

- Within a network, each network node should have responsibility for protecting itself and the peripheral nodes that are in its domain. In Figure 28, for example, CHICAGO has responsibility for what locations can access MADISON, CHICPC1, and CHICPC2. (CHICAGO and DALLAS share responsibility for MADISON.) CHICAGO also has responsibility for what locations can access locations in the EURONET network. CHICAGO would normally not have responsibility for controlling access between ATLANTA and DALLAS or between ATLANTA and NEWYORK.
- Figure 28 shows two networks that are connected: USANET and EURONET. Typically, when you connect two APPN networks, one network node in each network serves as the connection (gateway) to the other network. CHICAGO and LONDON provide that function in the example.

  The directory search filter (QAPPNDIR) on the gateway system protects its network in two ways:

  – It prevents unwanted connections. For example, the directory search filter on CHICAGO prevents BERLIN from accessing ATLANTA.
  – It prevents unnecessary demands on network resources. The directory search filter on CHICAGO blocks all unauthorized attempts from EURONET users *before* the USANET network spends any resources in trying to find a route. For example, if a user on the BERLIN system tries to establish a session with CHICPC1, the directory search filter on CHICAGO will cause the system to reject that attempt. The CHICAGO system will not attempt to find a route to the CHICPC1 location, and the CHICPC1 will not receive a bind request.

    Similarly, if a hacker on the PARIS system tries to establish a connection in the USANET network by guessing location names, the CHICAGO system will reject the requests. The USANET network will not search for the locations because the location pairs are not in the directory search filter.

Auditing APPN Filtering Support

When you set up APPN filtering support, you can use the security auditing function to capture information about requests that your system rejects. After you have set up security auditing, specify *NETCMN for the audit level (QAUDLVL) system value. When your system rejects a connection request because of the directory search filter, the system writes an ND record to the audit journal. When your system rejects a communications request because of the session endpoint filter, the system writes an NE record to the audit journal.

You can use the DSPAUDJRNE command to display the audit journal entries that relate to APPN filtering support. The ND and NE entries provide information about what location is requesting the session and what location is the target for the session. If you are setting up APPN filtering support and your system is rejecting sessions that you think should be allowed, you can use the journal entries to help you diagnose problems. When your APPN filtering support is operational, you can use the journal entries to monitor unauthorized attempts to access locations in your network.

Chapter 9 in the *Security - Reference* book describes how to work with security auditing. Appendix F describes the layouts for entries in the security audit (QAUDJRN) journal.

Chapter 13. Tips for Securing TCP/IP Communications

TCP/IP (Transmission Control Protocol/Internet Protocol) is a common way that computers of all types communicate with each other. TCP/IP applications are well-known and widely used throughout the "information highway".

This chapter provides tips for the following:

- Preventing TCP/IP applications from running on your system.
- Protecting system resources when you allow TCP/IP applications to run on your system.

The *TCP/IP Configuration and Reference* book has complete information about all the TCP/IP applications. "Part 5. Tips and Tools for Internet Security on AS/400" on page 195 describes security considerations when you connect your AS/400 either to the Internet (a very large TCP/IP network) or to an intranet.

Keep in mind that AS/400 supports many possible TCP/IP applications. When you decide to allow one TCP/IP application on your system, you may also be enabling other TCP/IP applications. As security administrator, you need to be aware of the range of TCP/IP applications and the security implications of these applications.

Tips for Preventing Any TCP/IP Processing

TCP/IP server jobs run in the QSYSWRK subsystem. You use the Start TCP/IP (STRTCP) command to start TCP/IP on your system. If you do not want any TCP/IP processing or applications to run, do not use the STRTCP command. Your system ships with the public authority for the STRTCP command set to *EXCLUDE.

If you suspect that someone with access to the command is starting TCP/IP (during off-hours, for example), you can set up object auditing on the STRTCP command. The system will write an audit journal entry whenever a user runs the command.

TCP/IP Security Components

As of Version 4 Release 3, you can take advantage of several TCP/IP security components that enhance your network security and add flexibility. Though some of these technologies are also found in firewall products such as the IBM Firewall for AS/400, these TCP/IP security components for OS/400 are not intended to be used as a firewall. However, you may be able to use some of these features, in some instances to eliminate the need for a separate firewall product. You also may be able to use these TCP/IP features to provide additional security in environments where you already use a firewall.

General Tips for Securing Your TCP/IP Environment

This topic provides general suggestions for steps that you can take to reduce the security exposures in the TCP/IP environment on your system. These tips apply to your entire TCP/IP environment rather than to the specific applications that are discussed in the topics that follow.

- When you write an application for a TCP/IP port, make sure that the application is properly secure. You should assume that an outsider might try to access that application through that port. A knowledgeable outsider may attempt to TELNET to that application.
- Monitor the use of TCP/IP ports on your system. A user application that is associated with a TCP/IP port can provide "back-door" entry to your system without a user ID or a password. Someone with sufficient authority on your system can associate an application with a TCP or UDP port.
- As a security administrator, you should be aware of a technique called *IP spoofing* that is used by hackers. Every system in a TCP/IP network has an IP address. Someone who uses IP spoofing sets up a system (usually a PC) to pretend to be an existing IP address or a trusted IP address. Thus, the imposter can establish a connection with your system by pretending to be a system that you normally connect with.

  If you run TCP/IP on your system and your system participates in a network that is not physically protected (all nonswitched lines and predefined links), you are vulnerable to IP spoofing. To protect your system from damage by a "spoofer", start with the suggestions in this chapter, such as sign-on protection and object security. You should also ensure that your system has reasonable auxiliary storage limits set. This prevents a spoofer from flooding your system with mail or spooled files to the point that your system becomes inoperable.

  In addition, you should regularly monitor TCP/IP activity on your system. If you detect IP spoofing, you can try to discover the weak points in your TCP/IP setup and to make adjustments.
- For your intranet (network of systems that do not need to connect directly to the outside), use IP addresses that are reusable. Reusable addresses are intended for use within a private network. The Internet backbone does not route packets that have a reusable IP address. Therefore, reusable addresses provide an added layer of protection inside your firewall.

  The *TCP/IP Configuration and Reference* provides more information about how IP addresses are assigned and about the ranges of IP addresses.
- If you are considering connecting your system to the Internet or an intranet, review the security information in Part 5
- The *TCP/IP Configuration and Reference* book has an appendix that provides security information about TCP/IP. Review the information in the appendix.

Packet Security Features for Securing TCP/IP Traffic

The Packet Security feature is available through AS/400 Operations Navigator. It allows you to create Internet Protocol (IP) filtering rules and Network Address Translation (NAT) settings. With these, you can control TCP/IP traffic into and out of your AS/400 system.

Internet Protocol (IP) Packet Filtering

Internet Protocol (IP) packet filtering provides the ability to selectively block IP traffic based on information in the IP and protocol specific packet headers. Examples of specific headers include those forTCP and UDP. You can create a set of filter rules to specify which IP packets to permit into your network and which to deny access into your network. When you create filter rules, you apply them to a physical interface (for example, a Token ring or Ethernet line). You can apply the rules to multiple physical interfaces, or you can apply different rules to each interface.

Based on the following header information, you can create rules to either permit or deny specific packets :

- Destination IP address
- Source IP address Protocol (for example, TCP, UDP, and so forth)
- Destination port (for example, port 80 for HTTP)
- Source port
- IP datagram direction (inbound or outbound)
- Forwarded or Local

You can use IP packet filtering to prevent undesirable or unneeded traffic from reaching applications on the system or being forwarded to other systems. This includes low-level ICMP packets (for example, PING packets) for which no specific application server is required.

You can specify whether a filter rule creates a log entry with information about packets matching the rule in a system journal. Once the information is written in a system journal, you cannot change the log entry. Consequently, the log is an ideal tool for auditing network activity.

You can use OS/400 IP packet filtering to provide additional protection for a particular AS/400 system. For example, this system might be running sensitive applications or performing Web serving to the Internet. You can also use packet filtering to protect an entire subnet when the AS/400 is acting in the role of a "casual" router.

You can find more information about using OS/400 IP Packet Filtering in the AS/400 Information Center.

Network Address Translation (NAT)

Network Address Translation (NAT) changes the source, the destination IP addresses, or both the source and destionation IP addresses, of packets that flow through the system. Using NAT, you can use the AS/400 system as a gateway between two networks which have conflicting or incompatible addressing schemes. You can also use NAT to hide the real IP addresses of one network by dynamically substituting a different address.

To use NAT, you must create a set of rules to specify how address translation will work. A "Map" rule translates one static address to another (for example "a.b.c.d" translates to "e.f.g.h"). You can use a map rule when the system with a real address of "e.f.g.h" provides services that you want to access from another network. At that other network, it is necessary or desirable to know the system by address "a.b.c.d.". A "Hide" rule translates all addresses in a subnetwork to a specific IP address. You can use a hide rule when client systems need to access services in another network and it is necessary or desirable to use an alternative addressing structure.

Note: Because IP Packet Filtering and Network Address Translation complement each other, you will often use them together to enhance network security.

You should consider using Network Address Translation (NAT) functions of OS/400 when connecting two previously disjoint networks that have inconsistent or incompatible IP addressing structures.

You can find more information about using OS/400 Network Address Translation in the Information Center

Controlling Which TCP/IP Servers Start Automatically

As security administrator, you need to control which TCP/IP applications start automatically when you start TCP/IP. Two commands are available for starting TCP/IP. For each command, the system uses a different method to determine which applications (servers) to start.

Table 21 shows the two commands and security recommendations for them. Table 22 shows the default autostart values for the servers. To change the autostart value for a server, use the CHGxxxA (Change xxx Attributes) command for the server. For example, the command for TELNET is CHGTELNA.

Table 21. How TCP/IP Commands Determine Which Servers to Start

Command	What Servers Start	Security Recommendations
Start TCP/IP (STRTCP)	The system starts every server that specifies AUTOSTART(*YES). Table 22shows the shipped value for each TCP/IP server.	• Assign *IOSYSCFG special authority carefully to control who can change the autostart settings. • Carefully control who has authority to use the STRTCP command. The default public authority for the command is *EXCLUDE. • Set up object auditing for the Change *server-name* Attributes commands (such as CHGTELNA) to monitor users who attempt to change the AUTOSTART value for a server.
Start TCP/IP Server (STRTCPSVR)	You use a parameter to specify which servers to start. The default when this command ships is to start all servers.	• Use the Change Command Default (CHGCMDDFT) command to set up the STRTCPSVR command to start only a specific server. This does not prevent users from starting other servers. However, by changing the command default, you make it less likely that users will start all servers by accident. For example, use the following command to set the default to start only the TELNET server:`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **Note:** When you change the default value, you can specify only a single server. Choose either a server that you use regularly or a server that is least likely to cause security exposures (such as TFTP). • Carefully control who has authority to use the STRTCPSVR command. The default public authority for the command is *EXCLUDE.

Table 22. Autostart Values for TCP/IP Servers

Server	Default Value	Your Value	Where to Read about Security Considerations for the Server
TELNET	AUTOSTART(*YES)		"Security Tips for TELNET" on page 132
FTP (file transfer protocol)	AUTOSTART(*YES)		"Security Tips for File Transfer Protocol" on page 137
BOOTP (Bootstrap Protocol)	AUTOSTART(*NO)		"Security Tips for the Bootstrap Protocol Server" on page 139
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)		"Security Tips for the Trivial File Transfer Protocol Server" on page 142

Table 22. Autostart Values for TCP/IP Servers (continued)

Server	Default Value	Your Value	Where to Read about Security Considerations for the Server
REXEC (Remote EXECution server)	AUTOSTART(*NO)		"Security Tips for the Remote EXECution Server" on page 144
RouteD (Route Daemon)	AUTOSTART(*NO)		"Security Tips for the Route Daemon" on page 145
SMTP (simple mail transfer protocol)	AUTOSTART(*YES)		"Security Tips for Simple Mail Transfer Protocol" on page 147
POP (Post Office Protocol)	AUTOSTART(*NO)		"Security Tips for Post Office Protocol" on page 148
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)		"Security Tips for Web Serving from AS/400" on page 150
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)		"Security Tips for Web Serving from AS/400" on page 150
WSG (Workstation Gateway Server)	AUTOSTART(*NO)		"Security Tips for Workstation Gateway Server" on page 158
LPD (line printer daemon)	AUTOSTART(*YES)		"Security Tips for Line Printer Daemon" on page 160
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)		"Security Tips for Simple Network Management Protocol" on page 161
DNS (domain name system)	AUTOSTART(*NO)		"Security Tips for the Domain Name System Server" on page 146
DDM	AUTOSTART(*NO)		
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)		"Security Tips for the Dynamic Host Configuration Protocol Server" on page 140
NSMI	AUTOSTART(*NO)		
INETD	AUTOSTART(*NO)		"Security Tips for the INETD Server" on page 162

Notes:

1. Beginning with V4R1, with the IBM HTTP Server for AS/400, you use the CHGHTTPA command to set the AUTOSTART value.

Tips for Controlling the Use of SLIP

AS/400 TCP/IP support includes Serial Interface Line Protocol (SLIP). SLIP provides low-cost point-to-point connectivity. A SLIP user can connect to a LAN or a WAN by establishing a point-to-point connection with a system that is part of the LAN or WAN.

SLIP runs on an asynchronous connection. You can use SLIP for dial-up connection to and from AS/400. For example, you might use SLIP to dial in from your PC to an AS/400 system. After the connection is established, you can use the TELNET application on your PC to connect to the AS/400 TELNET server. Or, you can use the FTP application to transfer files between the two systems.

No SLIP configuration exists on your system when it ships. Therefore, if you do not want SLIP (and dial-up TCP/IP) to run on your system, do not configure any

configuration profiles for SLIP. You use the Work with TCP/IP Point-to-Point (WRKTCPPTP) command to create SLIP configurations. You must have *IOSYSCFG special authority to use the WRKTCPPTP command.

If you want SLIP to run on your system, you create one or more SLIP (point-to-point) configuration profiles. You can create configuration profiles with the following operating modes:

- Dial in (*ANS)
- Dial out (*DIAL)

The topics that follow discuss how you can set up security for SLIP configuration profiles.

Note: A **user profile** is an AS/400 object that allows sign-on. Every AS/400 job must have a user profile to run. A **configuration profile** stores information that is used to establish a SLIP connection with an AS/400 system. When you start a SLIP connection to AS/400, you are simply establishing a link. You have not yet signed on and started an AS/400 job. Therefore, you do not necessarily need an AS/400 user profile to start a SLIP connection to AS/400. However, as you will see in the discussions that follow, the SLIP configuration profile may require an AS/400 user profile to determine whether to allow the connection.

Controlling Dial-In SLIP Connections

Before someone can establish a dial-in connection to your system with SLIP, you must start a SLIP *ANS configuration profile. To create or change a SLIP configuration profile, you use the Work with TCP/IP Point-to-Point (WRKTCPPTP) command. To start a configuration profile, you use either the Start TCP/IP Point-to-Point (STRTCPPTP) command or an option from the WRKTCPPTP display. When your system ships, the public authority for the STRTCPPTP and ENDTCPPTP commands are *EXCLUDE. The options to add, change, and delete SLIP configuration profiles are available only if you have *IOSYSCFG special authority. As security administrator, you can use both command authority and special authority determine who can set up your system to allow dial-in connections.

Securing a Dial-In SLIP Connection

If you want to validate systems that dial in to your system, then you want the requesting system to send a user ID and a password. Your system can then verify the user ID and password. If the user ID and password are not valid, your system can reject the session request.

To set up dial-in validation, do the following:

__ Step 1. Create a user profile that the requesting system can use to establish the connection. The user ID and password that the requester sends must match this user profile name and password.

Note: For the system to perform password validation, the QSECURITY system value must be set to 20 or higher.

As additional protection, you probably want to create user profiles specifically for establishing SLIP connections. The user profiles should have limited authority on the system. If you do not plan to use the

profiles for any function except establishing SLIP connections, you can set the following values in the user profiles:

- An initial menu (INLMNU) of *SIGNOFF
- An initial program (INLPGM) of *NONE.
- Limit capabilities (LMTCPB) of *YES

These values prevent anyone from signing on interactively with the user profile.

__ Step 2. Create an authorization list for the system to check when a requester tries to establish a SLIP connection.

Note: You specify this authorization list in the *System access authorization list* field when you create or change the SLIP profile. (See step 4.)

__ Step 3. Use the Add Authorization Entry (ADDAUTLE) command to add the user profile that you created in step 1 to the authorization list. You can create a unique authorization list for each point-to-point configuration profile, or you can create an authorization list that several configuration profiles share.

__ Step 4. Use the WRKTCPPTP command to set up a TCP/IP point-to-point *ANS profile that has the following characteristics:

- The configuration profile must use a connection dialog script that includes the user-validation function. User validation includes accepting a user ID and password from the requester and validating them. The system ships with several sample dialog scripts that provide this function.
- The configuration profile must specify the name of the authorization list that you created in step 2. The user ID that the connection dialog script receives must be in the authorization list.

Keep in mind that the value of setting up dial-in security is affected by the security practices and capabilities of the systems that dial in. If you require a user ID and password, then the connection dialog script on the requesting system must send that user ID and password. Some systems, such as AS/400, provide a secure method for storing the user IDs and passwords. (“Security and Dial-Out Sessions” on page 130 describes the method.) Other systems store the user ID and password in the script which might be accessible to anyone who knows where to find the script on the system.

Because of the differing security practices and capabilities of your communications partners, you might want to create different configuration profiles for different requesting environments. You use STRTCPPTP command to set your system up to accept a session for a specific configuration profile. You can start sessions for some configuration profiles only at certain times of the day, for example. You might use security auditing to log the activity for the associated user profiles.

Preventing Dial-In Users from Accessing Other Systems

Depending on your system and network configuration, a user who starts a SLIP connection might be able to access another system in your network without signing on to your system. For example, a user could establish a SLIP connection to your system. Then the user could establish an FTP connection to another system in your network that does not allow dial-in.

You can prevent a SLIP user from accessing other systems in your network by specifying N (No) for the *Allow IP datagram forwarding* field in the configuration profile. This prevents a user from accessing your network before the user logs on to your system. However, after the user has successfully logged on to your system, the datagram forwarding value has no effect. It does not limit the user's ability to use a TCP/IP application on your AS/400 system (such as FTP or TELNET), to establish a connection with another system in your network.

Controlling Dial-Out Sessions

Before someone can use SLIP to establish a dial-out connection from your system, you must start a SLIP *DIAL configuration profile. To create or change a SLIP configuration profile, you use the WRKTCPPTP command. To start a configuration profile, you use either the Start TCP/IP Point-to-Point (STRTCPPTP) command or an option from the WRKTCPPTP display. When your system ships, the public authority for the STRTCPPTP and ENDTCPPTP commands are *EXCLUDE. The options to add, change, and delete SLIP configuration profiles are available only if you have *IOSYSCFG special authority. As security administrator, you can use both command authority and special authority determine who can set up your system to allow dial-out connections.

Security and Dial-Out Sessions

Users on your AS/400 system might want to establish dial-out connections to systems that require user validation. The connection dialog script on your AS/400 must send a user ID and a password to the remote system. AS/400 provides a secure method for storing that password. The password does not need to be stored in the connection dialog script.

Notes:

1. Even though your system stores the connection password in encrypted form, your system decrypts the password before sending it. SLIP passwords, like FTP and TELNET passwords, are sent unencrypted ("in the clear"). However, unlike with FTP and TELNET, the SLIP password is sent before the systems establish TCP/IP mode.

   Because SLIP uses a point-to-point connection in asynchronous mode, the security exposure when sending unencrypted passwords is different from the exposure with FTP and TELNET passwords. Unencrypted FTP and TELNET passwords might be sent as IP traffic on a network and are, therefore, vulnerable to electronic sniffing. The transmission of your SLIP password is as secure as the telephone connection between the two systems.
2. The default file for storing SLIP connection dialog scripts is QUSRSYS/QATOCPPSCR. The public authority for this file is *USE, which prevents public users from changing the default connection dialog scripts.

When you create a connection profile for a remote session that requires validation, do the following:

__ Step 1. Ensure that the Retain Server Security Data (QRETSVRSEC) system value is 1 (Yes). This system value determines whether you will allow passwords that can be decrypted to be stored in a protected area on your system.

__ Step 2. Use the WRKTCPPTP command to create a configuration profile that has the following characteristics:

- For the mode of the configuration profile, specify *DIAL.

- For the *Remote service access name*, specify the user ID that the remote system expects. For example, if you are connecting to another AS/400, specify the user profile name on that AS/400.
- For the *Remote service access password*, specify the password that the remote system expects for this user ID. On your AS/400, this password is stored in a protected area in a form that can be decrypted. The names and passwords that you assign for configuration profiles are associated with the QTCP user profile. The names and passwords are not accessible with any user commands or interfaces. Only registered system programs can access this password information.

  Note: Keep in mind that the passwords for your connection profiles are not saved when your save the TCP/IP configuration files. To save SLIP passwords, you need to use the Save Security Data (SAVSECDTA) command to save the QTCP user profile.
- For the connection dialog script, specify a script that sends the user ID and password. The system ships with several sample dialog scripts that provide this function. When the system runs the script, the system retrieves the password, decrypts it, and sends it to the remote system.

Security Considerations for Point-to-Point Protocol

Beginning with V4R2, point-to-point protocol (PPP) is available as part of TCP/IP. PPP is an industry standard for point-to-point connections that provides additional function over what is available with SLIP.

With PPP, your AS/400 can have high-speed connections directly to an Internet Service Provider or to other systems in an intranet or extranet. Remote LANs can realistically make dial-in connections to your AS/400.

Remember that PPP, like SLIP, provides a network connection to your AS/400. A PPP connection essentially brings the requester to your system's door. The requester still needs a user ID and password to enter your system and connect to a TCP/IP server like TELNET or FTP. Following are security considerations with this new connection capability:

Note: You configure PPP by using Operations Navigator on a AS/400 Client Access for Windows 95/NT workstation.

- PPP provides the ability to have dedicated connections (where the same user always has the same IP address). With a dedicated address, you have the potential for IP spoofing (an imposter system that pretends to be a trusted system with a known IP address). However, the enhanced authentication capabilities that PPP provides help protect against IP spoofing.
- With PPP, as with SLIP, you create connection profiles that have a user name and an associated password. However, unlike SLIP, the user does not need tot have a valid AS/400 user profile and password. The user name and password are not associated with an AS/400 user profile. Instead, validation lists are used for PPP authentication. Additionally, PPP does not require a connection script. The authentication (exchange of user name and password) is part of the PPP architecture and happens at a lower level than with SLIP.

- With PPP, you have the option to use CHAP (challenge handshake authentication protocol). You will no longer need to worry about an eavesdropper sniffing passwords because CHAP encrypts user names and passwords.

  Your PPP connection uses CHAP only if both sides have CHAP support. During the exchange signals to set up communications between two modems, the two systems negotiate. For example, if SYSTEMA supports CHAP and SYSTEMB does not, SYSTEMA can either deny the session or agree to use an unencrypted user name and password. Agreeing to use an unencrypted user name and password is referred to as negotiating down. The decision to negotiate down is a configuration option. On your intranet, for example, where you know that all your systems have CHAP capability, you should configure your connection profile so that it will not negotiate down. On a public connection where your system is dialing out, you might be willing to negotiate down.

  The connection profile for PPP provides the ability to specify valid IP addresses. You can, for example, indicate that you expect a specific address or range of addresses for a specific user. This capability, together with the ability for encrypted passwords, provides further protection against spoofing.

  As additional protection against spoofing or piggy-backing on an active session, you can configure PPP to rechallenge at designated intervals. For example, while a PPP session is active, your AS/400 might challenge the other system for a user and password. It does this every 15 minutes to ensure that 'it is the same connection profile. (The end-user will not be aware of this rechallenge activity. The systems exchange names and passwords below the level that the end-user sees.)

  With PPP, it is realistic to expect that remote LANs might establish a dial-in connection to your AS/400 and to your extended network. In this environment, having IP forwarding turned on is probably a requirement. IP forwarding has the potential to allow an intruder to roam through your network. However, PPP has stronger protections (such as encryption of passwords and IP address validation). This makes it less likely that an intruder can establish a network connection in the first place.

For more information about PPP, see the *TCP/IP Configuration and Reference* book.

Security Tips for TELNET

TELNET provides an interactive session on your system. Your system presents the Sign On display to anyone who attempts to enter your system by using TELNET. TELNET requires a password if your system is running security level 20 or higher.

Note: When you have Network Stations attached to your AS/400, you must have TELNET running. Network Stations use TN5250 (TELNET) for AS/400 sessions.

Tips for Preventing TELNET Access

If you *do not* want anyone to use TELNET to access your system, you should prevent the TELNET server from running. Do the following:

__ Step 1. To prevent TELNET server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGTELNA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*YES) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for TELNET, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `23` (for non-SSL TELNET) or `992` (for SSL TELNET).

Note: These port numbers are specified in the Work with Service Table Entries (WRKSRVTBLE) table under "telnet" and "telnet-ssl". They may be mapped to ports other than 23 and 992.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users. If the port is restricted to profile QTCP, then TELNET servers can run. If restricted to a profile other than QTCP, then TELNET servers cannot use that port.

Note: If you want to prevent access to both non-SSL TELNET and SSL TELNET, repeat step 2 and specify the other port in part 2.d.

Tips for Controlling TELNET Access

Following are security considerations and suggestions when you want TELNET clients to access your system:

Protecting passwords: TELNET passwords are not encrypted when they are sent between the traditional client and the server. Depending on your connection methods, your system may be vulnerable to password theft through "line sniffing".

Note: Monitoring a line by using electronic equipment is often referred to as **sniffing**.

However, if you use the SSL TELNET server (new in V4R4) and an SSL-enabled

TELNET client, then all transactions, including passwords, are encrypted and protected. The Telnet SSL port is defined in the WRKSRVTBLE entry under "telnet-ssl".

Note: Though the SSL TELNET server was not available prior to V4R4, a TELNET SSL Proxy Server is available for V4R2 and V4R3 that will allow you to establish secure TELNET connections. See the following URL for information on this proxy server:

```
http://www.as400.ibm.com/tstudio/tech_ref/tcp/sslproxy/index.htm
```

Limiting the number of sign-on attempts: Although the QMAXSIGN system value applies to TELNET, you reduce the effectiveness of this system value if you set up your system to configure virtual devices automatically. When the QAUTOVRT system value has a value greater than 0, the unsuccessful TELNET user can reconnect and attach to a newly-created virtual device. This can continue until one of the following occurs:

- All virtual devices are disabled, and the system has exceeded the limit for creating new virtual devices.
- All user profiles are disabled.
- The hacker succeeds in signing on to your system.

Automatically configuring virtual devices multiplies the number of TELNET attempts that are available.

Note: To make it easier to control virtual devices, you might want to set the QAUTOVRT system value to a value that is greater than 0 for a short period of time. Either use TELNET yourself to force the system to create devices or wait until other users have caused the system to create sufficient virtual devices. Then set the QAUTOVRT system value to 0.

The V4R2 TELNET enhancements provide an option for limiting the number of times a hacker can attempt to enter your system. You can create an exit program that the system calls whenever a client attempts to start a TELNET session. The exit program receives the IP address of the requester. If your program sees a series of requests from the same IP address within a short time span, your program can take action, such as denying further requests from the address and sending a message to the QSYSOPR message queue. "Overview of the TELNET Exit Program Capability" on page 136 provides an overview of the TELNET exit program capability.

Note: Alternatively, you could use your TELNET exit program to provide logging. Rather than having your program make decisions about potential break-in attempts, you could use the logging capability to monitor attempts to start TELNET sessions.

Ending inactive sessions: You can use the *Inactivity timeout* (INACTTIMO) parameter on the TELNET configuration to reduce the exposure when a user leaves a TELNET session unattended. Be sure to read the documentation or online help to understand how the INACTTIMO parameter and the connection timer (for server startup) work together.

Beginning with V4R3, TELNET sessions are included in the system's QINACTITV processing. The QINACTMSGQ system value defines the action for the interactive TELNET sessions that are inactive when the inactive job time-out interval expires. If

the QINACTMSGQ specifies that the job should be disconnected, the session must support the disconnect job function. Otherwise, the job will end rather than be disconnected.

TELNET sessions that continue to use device descriptions that are named QPDEVxxxx will not allow users to disconnect from those jobs. Disconnection from these jobs is not allowed because the device description to which a user is reconnected is unpredictable. Disconnecting a job requires the same device description for the user when the job is reconnected. The inactive job time-out is supported for all types of TELNET, including TCP/IP TELNET, IPX TELNET, and Workstation Gateway. If you are using the TELNET or INACTTIMO parameter to time-out sessions, you should change to use the QINACTITV system value. The Workstation Gateway uses an independent timer in the INACTTIMO value that functions in addition to the QINACTITV value. Either value can trigger a session time-out in Workstation Gateway.

Restricting powerful user profiles: You can use the QLMTSECOFR system value to restrict users with *ALLOBJ or *SERVICE special authority. The user or QSECOFR must be explicitly authorized to a device to sign on. Thus, you can prevent anyone with *ALLOBJ special authority from using TELNET to access your system by ensuring that QSECOFR does not have authority to any virtual devices.

Rather than preventing any TELNET users who have *ALLOBJ special authority, you might to restrict powerful TELNET users by location. With the TELNET initiation exit point in V4R2, you can create an exit program that assigns a specific AS/400 device description to a session request based on the IP address of the requester.

Controlling function by location: You might want to control what functions you allow or what menu the user sees based on the location where the TELNET request originates. The QDCRDEVD API (application programming interface) provides you with access to the IP address of the requester. Following are some suggestions for using this support:

- For V4R1, you might use the API in an initial program for all users (if TELNET activity is significant in your environment). Based on the IP address of the user who requests sign-on, you could set the menu for the user or even swap to a specific user profile.
- Beginning with V4R2, you can use the TELNET exit program to make decisions based on the IP address of the requester. This eliminates the need to define an initial program in every user profile. You can, for example, set the initial menu for the user, set the initial program for the user, or specify what user profile the TELNET session will run under.

Note: In addition, with access to the IP address of the user, you can now provide dynamic printing to a printer associated with the user's IP address. The QDCRDEVD API will also return IP addresses for printers, as well as for displays. Select the DEVD1100 format for printers, and DEVD0600 for displays.

Controlling automatic sign-on: Beginning with V4R2, TELNET supports the capability for a Client Access user to bypass the Sign On display by sending a user profile name and password with the TELNET session request. The system uses the setting for the QRMTSIGN (Remote sign-on) system value to determine how to handle requests for automatic sign-on. Table 23 on page 136 shows the options. These options apply only when the TELNET request includes a user ID and password.

Table 23. How QRMTSIGN Works with TELNET

*REJECT	TELNET sessions that request automatic sign-on are not allowed
*VERIFY	If the user profile and password combination is valid, the TELNET session starts.[1]
*SAMEPRF	If the user profile and password combination is valid, the TELNET session starts.[1]
*FRCSIGNON	The system ignores the user profile and password. The user sees the Sign-On display .

Notes:

1. This validation occurs before the TELNET exit program runs. The exit program receives an indication that the validation was successful or unsuccessful. The exit program can still allow or deny the session, regardless of the indicator. The indication has one of the following values:
   - Client password not validated (or no password received).
   - Client clear-text password validated
   - Client encrypted password validated

Note: A registered TELNET exit program can override the setting of QRMTSIGN by choosing whether or not to allow automatic sign-on for a requester (probably based on IP address).

Allowing anonymous sign-on: Beginning with V4R2, you can use the TELNET exit programs to provide "anonymous" or "guest" TELNET on your system. With your exit program, you can detect the IP address of the requester. If the IP address comes from outside your organization, you can assign the TELNET session to a user profile that has limited authority on your system and a specific menu. You can bypass the Sign-On display so the visitor does not have the opportunity to use another, more powerful user profile. With this option, the user does not need to provide a user ID and password.

Overview of the TELNET Exit Program Capability

Beginning with V4R2, you can register user-written exit programs that run both when a TELNET session starts (initiation) and when it ends. Following are examples of what you can do in the initiation exit program:

- Allow or deny the session, based on any known criteria, such as the user's IP address, the time of day, and the requested user profile.
- Assign a specific AS/400 device description for the session. This allows routing of the interactive job to any sub-system set up to receive those devices.
- Assign specific National Language values for the session, such as keyboard and character set.
- Assign a specific user profile for the session.
- Automatically sign the requestor on (without displaying a Sign On display).
- Set up audit logging for the session.

For more information about the TELNET exit programs, see the *TCP/IP Configuration and Reference* book. You can find a sample program at the following Web location:

`http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr.htm`

Security Tips for File Transfer Protocol

FTP (file transfer protocol) provides the capability of transferring files between the client (a user on another system) and the server (your system). You can also use the remote command capability of FTP to submit commands to the server system.

FTP requires a user ID and a password. However, you can use the FTP Server exit points to provide an **anonymous FTP** function for guest users (users who do not have a user ID and password on your system). For secure anonymous FTP, you must write exit programs for both the FTP Server Logon and FTP Server Request Validation exit points.

Tips for Preventing FTP Access

If you *do not* want anyone to use FTP to access your system, you should prevent the FTP server from running. Do the following:

__ Step 1. To prevent FTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGFTPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*YES) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for FTP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `20`.

__ Step e. For the upper port range, specify `21`.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Notes:

a. The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

b. RFC1700 provides information about assigned port numbers.

c. If ports 20 or 21 are restricted to a user profile other than QTCP, attempting to start the FTP server will cause it to immediately end with errors.

d. This method works only for completely restricting an application such as the FTP server. It does not work for restricting specific

users. When a user connects to the FTP server, the request uses the QTCP profile initially. The system changes to the individual user profile after the connection is successful. Every user of the FTP server uses QTCP's authority to the port.

Tips for Controlling FTP Access

If you want to allow FTP clients to access your system, be aware of the following security issues:

- Your object authority scheme might not provide detailed enough protection when you allow FTP on your system. For example, when a user has the authority to view a file (*USE authority), the user can also copy the file to a PC or to another system. You might want to protect some files from being copied to another system.

  You can use FTP exit programs to restrict the FTP operations that users can perform. You can use the FTP Request Validation Exit to control what operations you allow. For example, you can reject GET requests for specific database files. You can use the FTP Server Logon Exit to authenticate users who log on to the FTP server. "TCP/IP User Exits" in the *TCP/IP Configuration and Reference* book describes this exit point and provides sample programs.

  The "TCP/IP User Exits" appendix of the book *TCP/IP Configuration and Reference* also describes how to use exit programs to set up support for anonymous FTP on your system.
- FTP passwords are not encrypted when they are sent between the client system and the server system. Depending on your connection methods, your system may be vulnerable to password theft through line sniffing.
- If the QMAXSGNACN system value is set to 1, the QMAXSIGN system value applies to TELNET but not to FTP. If QMAXSGNACN is set to 2 or 3 (values which disable the profile if the maximum sign on count is reached), FTP logon attempts are counted. In this case, a hacker can mount a "denial of service" attack through FTP by repeatedly attempting to log on with an incorrect password until the user profile is disabled.

  For each unsuccessful attempt, the system writes message CPF2234 to the QHST log. You can write a program to monitor the QHST log for the message. If the program detects repeated attempts, it can end the FTP servers.
- You can use the *Inactivity timeout* (INACTTIMO) parameter on the FTP configuration to reduce the exposure when a user leaves an FTP session unattended. Be sure to read the documentation or online help to understand how the INACTTIMO parameter and the connection timer (for server startup) work together.

  Note: The QINACTITV system value does not affect FTP sessions.
- The *TCP/IP Configuration and Reference* book describes how to use FTP batch support, for example, to send files between systems at night. When you use FTP batch support, the program must send both the user ID and the password to the server system. Either the user ID and password must be coded in the program, or the program must retrieve them from a file. Both these options for storing passwords and user IDs represent a potential security exposure. If you use FTP batch, you must ensure that you use object security to protect the user ID and password information. You should also use a single user ID that has very limited authority on the target system. It should have only enough authority to perform the function that you want, such as file transfer.

- FTP provides remote-command capability, just as advanced program-to-program communications (APPC) and Client Access do. The RCMD (Remote Command) FTP-server subcommand is the equivalent of having a command line on the system. Before you allow FTP, you must ensure that your object security scheme is adequate. You can also use the FTP exit program to limit or reject attempts to use the RCMD subcommand. "TCP/IP User Exits" in the *TCP/IP Configuration and Reference* book describes this exit point and provides sample programs.
- Beginning with V3R2 and V3R7, a user can access objects in the integrated file system with FTP. Therefore, you need to ensure that your authority scheme for the integrated file system is adequate when you run the FTP server on your system. "Chapter 11. Tips for Securing the Integrated File System" on page 85 provides suggestions for securing the integrated file system.
- A popular hacker activity is to set up an unsuspecting site as a repository for information. Sometimes, the information might be illegal or pornographic. If a hacker gains access to your site through FTP, the hacker uploads this undesirable information to your system. The hacker then informs other hackers of your system's address. They in turn access your system with FTP and download the undesirable information.

  You can use the FTP exit programs to help protect against this type of attack. For example, you might direct all requests to upload information to a directory that is write-only. This defeats the hacker's objective because the hacker's friends will not be able to download the information in the directory. *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* provides more information about the risks and possible solutions when you allow uploading through FTP.

Security Tips for the Bootstrap Protocol Server

Bootstrap Protocol (BOOTP) provides a dynamic method for associating workstations with servers and assigning workstation IP addresses and initial program load (IPL) sources. BOOTP and trivial file transfer protocol (TFTP) together provide support for the IBM Network Station for AS/400.

BOOTP is a TCP/IP protocol used to allow a media-less workstation (client) to request a file containing initial code from a server on the network. The BOOTP server listens on the well known BOOTP server port 67. When a client request is received, the server looks up the IP address defined for the client and returns a reply to the client with the client's IP address and the name of the load file. The client then initiates a TFTP request to the server for the load file. The mapping between the client hardware address and IP address is kept in the BOOTP table on the AS/400.

Tips for Preventing BOOTP Access

If you do not have any Network Stations attached to your AS/400, you do not need to run the BOOTP server on your system. It can be used for other devices, but the preferred solution for those devices is to use DHCP. Do the following to prevent the BOOTP server from running:

__ Step 1. To prevent BOOTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGBPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for BOOTP, do the following:

Note: Because DHCP and BOOTP use the same port number, this will also inhibit the port that is used by DHCP. Do not restrict the port if you want to use DHCP.

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `67`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.
2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Tips for Securing the BOOTP Server

The BOOTP server does not provide direct access to your AS/400 system, and thus represents a limited security exposure. Your primary concern as a security administrator is to ensure that the correct information is associated with the correct Network Station. (In other words, a mischief-maker could alter the BOOTP table and cause your Network Stations to work incorrectly or not at all.)

To administer the BOOTP server and the BOOTP table, you must have *IOSYSCFG special authority. You need to carefully control the user profiles that have *IOSYSCFG special authority on your system. The *IBM Network Station Manager for AS/400* book describes the procedures for working with the BOOTP table.

Security Tips for the Dynamic Host Configuration Protocol Server

Dynamic host configuration protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. For your client workstations, DHCP can provide a function similar to autoconfiguration. A DHCP-enabled program on the client workstation broadcasts a request for configuration information. If the DHCP server is running on your AS/400, the server responds to the request by sending the information that the client workstation needs to correctly configure TCP/IP.

You can use DHCP to make it simpler for users to connect to your AS/400 for the first time. This is because the user does not need to enter TCP/IP configuration information. You can also use DHCP to reduce the number of internal TCP/IP addresses that you need in a subnetwork. The DHCP server can temporarily allocate IP addresses to active users (from its pool of IP addresses).

For Network Stations, you can use DHCP in place of BOOTP. DHCP provides more function than BOOTP, and it can support dynamic configuration of both Network Stations and PCs.

Tips for Preventing DHCP Access

If you do *not* want anyone to use the DHCP server on your system, do the following:

1. To prevent DHCP server jobs from starting automatically when you start TCP/IP, type the following:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Notes:

   a. AUTOSTART(*NO) is the default value.

   b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for DHCP, do the following:

   a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

   b. Select option 4 (Work with TCP/IP port restrictions).

   c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

   d. For the lower port range, specify `67`.

   e. For the upper port range, specify `68`.

      Notes:

      1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

      2) RFC1700 provides information about common port number assignments.

   f. For the protocol, specify `*UDP`.

   g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Tips for Securing the DHCP Server

Following are security considerations when you choose to run DHCP on your AS/400 system:

- Restrict the number of users who have authority to administer DHCP. Administering DHCP requires the following authority:
  - *IOSYSCFG special authority
  - *RW authority to the following files:

```
/QIBM/UserData/OS400/DHCP/dhcpsd.cfg
/QIBM/UserData/OS400/DHCP/dhcprd.cfg
```

- Evaluate how physically accessible your LAN is. Could an outsider easily walk into your location with a laptop and physically connect it to your LAN? If this is an exposure, DHCP provides the capability to create a list of clients (hardware addresses) that the DHCP server will configure. When you use this feature, you remove some of the productivity benefit that DHCP provides to your network administrators. However, you prevent the system from configuring unknown workstations.
- If possible, use a pool of IP addresses that is reusable (not architected for the Internet). This helps prevent a workstation from outside your network from gaining usable configuration information from the server.
- Use the DHCP exit points if you need additional security protection. Following is an overview of the exit points and their capabilities. The *System API Reference* describes how to use these exit points.

  Port entry
  The system calls your exit program whenever it reads a data packet from port 67 (the DHCP port). Your exit program receives the full data packet. It can decide whether the system should process or discard the packet. You can use this exit point when existing DHCP screening features are not sufficient for your needs.

  Address assignment
  The system calls your exit program whenever DHCP formally assigns an address to a client.

  Address release
  The system calls your exit program whenever DHCP formally releases an address and places it back in the address pool.

Security Tips for the Trivial File Transfer Protocol Server

Trivial file transfer protocol (TFTP) provides basic file transfer with no user authentication. TFTP works with either Bootstrap Protocol (BOOTP) or Dynamic Host Configuration Protocol (DHCP) to provide support for the IBM Network Station for AS/400.

The IBM Network Station for AS/400 (a media-less workstation client) connects initially to either the BOOTP server or the DHCP server. The BOOTP server or the DHCP server replies with the client's IP address and the name of the load file. The client then initiates a TFTP request to the server for the load file. When the client completes downloading of the load file, it ends the TFTP session.

Tips for Preventing TFTP Access

If you do not have any Network Stations attached to your AS/400, you probably do not need to run the TFTP server on your system. Do the following to prevent the TFTP server from running:

__ Step 1. To prevent TFTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGTFTPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for TFTP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `69`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Tips for Securing the TFTP Server

By default, the TFTP server provides very limited access to your AS/400 system. It is specifically configured to provide the initial code for Network Stations. As a security administrator, you should be aware of the following characteristics of the TFTP server:

- The TFTP server does not require authentication (a user ID and password). All TFTP jobs run under the QTFTP user profile. The QTFTP user profile does not have a password. Therefore, it is not available for interactive sign-on. The QTFTP user profile does not have any special authorities, nor is it explicitly authorized to system resources. It uses public authority to access the resources that it needs for the Network Stations.
- When the TFTP server arrives, it is configured to access the directory that contains Network Station information. You must have *PUBLIC or QTFTP authorized to read or write to that directory. To write to the directory you must have *CREATE specified on the "Allow file writes" parameter of the CHGTFTPA command. To write to an existing file you must have the *REPLACE specified on the "Allow file writes" parameter of CHGTFTPA.

  A TFTP client cannot access any other directory unless you explicitly define the directory with the Change TFTP Attributes (CHGTFTPA) command. Therefore, if a local or remote user does attempt to start a TFTP session to your system, the user's ability to access information or cause damage is extremely limited.
- If you choose to configure your TFTP server to provide other services in addition to handling Network Stations, you can define an exit program to evaluate and

authorize every TFTP request. The TFTP server provides a request validation exit similar to the exit that is available for the FTP server.

Note: "TCP/IP User Exits" in the *TCP/IP Configuration and Reference* book describes the FTP exit point and provides sample programs. You can use this same technique for the TFTP exit point.

Security Tips for the Remote EXECution Server

The Remote EXECution server (REXEC) receives and runs commands from an REXEC client. A REXEC client is typically a PC or UNIX application that supports sending REXEC commands. The support that this server provides is similar to the capability that is available when you use the RCMD (Remote Command) sub-command for the FTP server.

Tips for Preventing REXEC Access

If you do not want your AS/400 to accept commands from an REXEC client, do the following to prevent the REXEC server from running:

__ Step 1. To prevent REXEC server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGRXCA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for REXEC, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `512`.

__ Step e. For the upper port range, specify `*ONLY`.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Notes:

a. The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

b. RFC1700 provides information about common port number assignments.

Tips for Securing the REXEC Server

Following are considerations when you choose to run the Remote EXECution server on your system:

- An REXCD request includes a user ID, a password, and the command to run. Normal AS/400 authentication and authority checking applies:
  - The user profile and password combination must be valid.
  - The system enforces the *Limit capabilities* (LMTCPB) value for the user profile.
  - The user must be authorized to the command and to all of the resources that the command uses.
- The REXEC server provides exit points similar to the exit points that are available for the FTP server. You can use the Validation exit point to evaluate the command and decide whether to allow it.

  Note: "TCP/IP User Exits" in the *TCP/IP Configuration and Reference* book describes the FTP exit point and provides sample programs. You can use this same technique for the TFTP exit point.
- When you choose to run the REXEC server, you are running outside any menu access control that you have on your system. You must ensure that your object authority scheme is adequate to protect your resources.

Security Tips for the Route Daemon

The Route Daemon (RouteD) server provides support for the Routing Information Protocol (RIP) on AS/400. RIP is the most widely used of routing protocols. It is an Interior Gateway Protocol that assists TCP/IP in the routing of IP packets within an autonomous system.

RouteD is intended to increase the efficiency of network traffic by allowing systems within a trusted network to update each other with current route information. When you run RouteD, your system can receive updates from other participating systems about how transmissions (packets) should be routed. Therefore, if your RouteD server is accessible to a hacker, the hacker might use it to reroute your packets through a system that can sniff or modify those packets. Following are suggestions for RouteD security:

- For V4R1, AS/400 uses RIPv1, which does not provide any method for authenticating routers. It is intended for use within a trusted network. If your system is in a network with other systems that you do not "trust," you should not run the RouteD server. To ensure that the RouteD server does not start automatically, type the following:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Notes:

  1. AUTOSTART(*NO) is the default value.
  2. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.
- Make sure that you control who can change the RouteD configuration, which requires *IOSYSCFG special authority.
- If your system participates in more than one network (for example, an intranet and the Internet), you can configure the RouteD server to send and accept updates only with the secure network.

Security Tips for the Domain Name System Server

The Domain Name System (DNS) server provides translation of host name to IP addresses and vice versa. On AS/400, the DNS server is intended to provide address translation for the internal, secure network (intranet). The DNS that is part of the Firewall for AS/400 is intended to provide address translation between the internal protected network and the external, unsecure network.

Tips for Preventing DNS Access

If you do *not* want anyone to use the DNS server on your system, do the following:

1. To prevent DNS server jobs from starting automatically when you start TCP/IP, type the following:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Notes:

   a. AUTOSTART(*NO) is the default value.

   b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for DNS, do the following:

   a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

   b. Select option 4 (Work with TCP/IP port restrictions).

   c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

   d. For the lower port range, specify `53`.

   e. For the upper port range, specify `*ONLY`.

      Notes:

      1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

      2) RFC1700 provides information about common port number assignments.

   f. For the protocol, specify `*TCP`.

   g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

   h. Repeat steps 2.c through 2.g for the *UDP protocol.

Tips for Securing the DNS Server

Following are security considerations when you choose to run DNS on your AS/400 system:

- The function that the DNS server provides is IP address translation and name translation. It does not provide any access to objects on your AS/400 system. Your risk when an outsider accesses your DNS server is that the server provides an easy way to view the topology of your network. Your DNS might save a

hacker some effort in determining the addresses of potential targets. However, your DNS does not provide information that will help to break into those target systems.

- Typically, you use the AS/400 DNS server for your intranet. Therefore, you probably do not have a need to restrict the ability to query the DNS. However, you might, for example, have several subnetworks within your intranet. You might not want users from a different subnetwork to be able to query the DNS on your AS/400. A security option of DNS lets you limit access to a primary domain. Use Operations Navigator to specify IP addresses to which the DNS server should respond .

  Another security option lets you specify which secondary servers can copy information from your primary DNS server. When you use this option, your server will accept zone transfer requests (a request to copy information) only from the secondary servers that you explicitly list.
- Be sure to carefully restrict the ability to change the configuration file for your DNS server. Someone with malicious intent could, for example, change your DNS file to point to an IP address outside your network. They could simulate a server in your network and, perhaps, gain access to confidential information from users that visit the server.

Security Tips for Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) provides the capability to distribute documents and e-mail messages to and from other systems. The system does not perform any sign-on processing for SMTP.

Tips for Preventing SMTP Access

If you *do not* want anyone to use SMTP to distribute mail to or from your system, you should prevent the SMTP server from running. Do the following:

__ Step 1. If you do not plan to use SMTP at all, do not configure it on your system (or allow anyone else to configure it). If you need SMTP occasionally, but you normally do not want it to run, continue with the next steps.

__ Step 2. To prevent SMTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGSMTPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*YES) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 3. To prevent SMTP from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for SMTP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `25`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.
2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

__ Step h. Repeat steps 3.c through 3.g for the *UDP protocol.

__ Step 4. To provide extra protection, hold the SNADS distribution queues that the SMTP application uses by typing the following commands:

```
HLDDSTQ DSTQ(QSMTPQ) PTY(*NORMAL)
HLDDSTQ DSTQ(QSMTPQ) PTY(*HIGH)
```

Tips for Controlling SMTP Access

If you want to allow SMTP clients to access your system, be aware of the following security issues:

- If possible, avoid using an *ANY *ANY entry in the system distribution directory. When your system does not have an *ANY *ANY entry, it is more difficult for someone to attempt to use SMTP to flood your system or overwhelm your network. **Flooding** occurs when your auxiliary storage is filled with unwanted mail that is being routed through your system to another system.
- To prevent a user from swamping your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST). The *Backup and Recovery* book provides more information about ASP thresholds.
- The *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* book describes steps for cleaning up your AS/400 if your system is the victim of a flooding attack.

Security Tips for Post Office Protocol

The POP (Post Office Protocol) server provides a simple store-and-forward mail system. The POP server holds mail temporarily until a mail client retrieves it. The client/server interface of the POP server requires the services of the SMTP server. A mail client must have a user ID and a password to retrieve mail from the POP server.

Tips for Preventing POP Access

If you *do not* want anyone to use POP to access your system, you should prevent the POP server from running. Do the following:

__ Step 1. If you do not plan to use POP at all, do not configure it on your system (or allow anyone else to configure it). If you need POP occasionally, but you normally do not want the POP server to run, continue with the next steps.

__ Step 2. To prevent POP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGPOPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 3. To prevent POP from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for POP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `109`.

__ Step e. For the upper port range, specify `110`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

__ Step h. Repeat steps 3.c through 3.g for the *UDP protocol.

__ Step 4. Review "Security Tips for Simple Mail Transfer Protocol" on page 147 for suggestions for protecting the SMTP server. (The POP server requires the services of the SMTP server.)

Tips for Controlling POP Access

If you want to allow POP clients to access your system, be aware of the following security issues:

- The POP mail server provides authentication for clients who attempt to access their mailboxes. The client sends a user ID and password to the server. The POP mail server verifies the user ID and password against the AS/400 user profile and password for that user.

  Because you do not have control over how the user ID and password are stored on the POP client, you might want to create a special user profile that has very

limited authority on your AS/400 system. To prevent anyone from using the user profile for an interactive session, you can set the following values in the user profile:
  - Set initial menu (INLMNU) to *SIGNOFF
  - Set initial program (INLPGM) to *NONE
  - Set limit capabilities (LMTCPB) to *YES
- To prevent a malicious intruder from flooding your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). The ASP storage threshold prevents your system from stopping because the operating system does not have sufficient working space. You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST). The *Backup and Recovery* book provides more information about ASP thresholds.
- Although you need to ensure that your ASP threshold prevents your system from being flooded, you also need to ensure that your system has adequate space to properly store and deliver mail. If your system cannot deliver mail because the system does not have adequate storage for transient mail, this is an integrity problem for your users.

  Note: Usually storage space is not a significant problem. When a client receives mail, the system deletes the mail from the server.

Security Tips for Web Serving from AS/400

In V4R1 and V4R2, the Internet Connection Server product provided web serving capability to AS/400. In V4R3, the IBM HTTP Server for AS/400 product replaced Internet Connection Server. Each product provides a Hypertext Transfer Protocol (HTTP) server on AS/400. The two products share many security issues, though there are also some differences between them. In this section, the general terms "HTTP server" and "Internet server" are used to describe issues that pertain to both products. When an issue applies specifically to either Internet Connection Server or IBM HTTP Server for AS/400, its full name is used.

The HTTP server provides World Wide Web browser clients with access to AS/400 multimedia objects, such as HTML (Hypertext Markup Language) documents. It also supports the *Common Gateway Interface (CGI)* specification. Application programmers can write CGI programs to extend the functionality of the server.

The administrator can use Internet Connection Server or IBM HTTP Server for AS/400 to run multiple servers concurrently on the same AS/400. Each server that is running is called a **server instance**. Each server instance has a unique name. The administrator controls which instances are started and what each instance can do.

Note: You must have the *ADMIN instance of the HTTP server running when you use a Web browser to configure or administer any of the following:
- Firewall for AS/400
- Network Station
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for AS/400

A user (Web site visitor) never sees an AS/400 Sign On display. However, the administrator on AS/400 must explicitly authorize all HTML documents and CGI programs by defining them in HTTP directives. In addition, the administrator can set up both resource security and user authentication (user ID and password) for some or all requests.

An attack by a hacker could result in a denial of service to your Web server. Your server can detect a denial-of-service attack by measuring the time-out of certain clients' requests. If the server does not receive a request from the client, then your server determines that a denial-of-service attack is in progress. This occurs after making the initial client connection to your server. The server's default is to perform attack detection and penalization.

Tips for Preventing Access

If you *do not* want anyone to use the program to access your system, you should prevent the HTTP server from running. Do the following:

__ Step 1. To prevent HTTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGHTTPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. By default, the HTTP server job uses the QTMHHTTP user profile. To prevent the HTTP server from starting, set the status of the QTMHHTTP user profile to *DISABLED.

Tips for Controlling Access

The primary purpose of running an HTTP server is to provide access for visitors to a Web site on your AS/400 system. You might think of someone who visits your Web site as you would think of someone who views an advertisement in a trade journal. The visitor is not aware of the hardware and software running your Web site, such as the type of server you are using, and where your server is physically located. Usually, you do not want to put any barrier (such as a Sign On display) between a potential visitor and your Web site. However, you might want to restrict access to some of the documents or CGI programs that your Web site provides.

You might also want a single AS/400 system to provide multiple logical Web sites. For example, your AS/400 system might support different branches of your business that have different customer sets. For each of these branches of the business, you want a unique Web site that appears totally independent to the visitor. Additionally, you might want to provide internal Web sites (an intranet) with confidential information about your business.

As a security administrator, you need to protect the contents of your Web site while, at the same time, you need to ensure that your security practices do not negatively affect the value of your Web site. In addition, you need to ensure that HTTP activity does not jeopardize the integrity of your system or your network. The topics that follow provide security suggestions when you use the program.

Administration Considerations

Following are some security considerations for administering your Internet server.

- You perform setup and configuration functions by using a Web browser and the *ADMIN instance. For some functions, such as creating additional instances on the server, you *must* use the *ADMIN server.
- The default URL for the administration home page (the home page for the *ADMIN server) is published in the documentation for products that provide browser administration functions. Therefore, the default URL will probably be known by hackers and published in hacker forums, just like the default passwords for IBM-supplied user profiles are known and published. You can protect yourself from this exposure in several ways:
  - Only run the *ADMIN instance of the HTTP server when you need to perform administrative functions. Do not have the *ADMIN instance running all the time.
  - Activate SSL support for the *ADMIN instance (by using Digital Certificate Manager). The *ADMIN instance uses HTTP protection directives to require a user ID and password. When you use SSL, your user ID and password are encrypted (along with all the other information about your configuration that appears on the administration forms).
  - Use a firewall both to prevent access to the *ADMIN server from the Internet and to hide your system and domain names, which are part of the URL.
- When you perform administration functions, you must sign on with a user profile that has *IOSYSCFG special authority. You might also need authority to specific objects on the system, such as the following:
  - The libraries or directories that contain your HTML documents and CGI programs.
  - Any user profiles that you plan to swap to within the directives for the server.
  - The Access Control Lists (ACLs) for any directories that your directives use.
  - A validation list object for creating and maintaining user IDs and passwords.

  With both the *ADMIN server and TELNET, you have the capability to perform administration functions remotely, perhaps over an Internet connection. Be aware that if you perform administration over a public link (the Internet), you might be exposing a powerful user ID and password to sniffing. The "sniffer" can then use this user ID and password to attempt to access your system using, for example, TELNET or FTP.

  Notes:

  1. With TELNET, the Sign On display is treated like any other display. Although the password does not display when you type it, the system transmits it without any encryption or encoding.
  2. With the *ADMIN server, the password is encoded not encrypted. The encoding scheme is an industry standard, and thus commonly known among the hacker community. Although the encoding is not easily understood by the casual "sniffer," a sophisticated sniffer probably has tools to attempt to decode the password.

Security Tip

If you plan to perform remote administration over the Internet, you should use the *ADMIN instance with SSL, so that your transmissions are encrypted. Do not use an insecure application, such as a pre-V4R4 version of TELNET (TELNET supports SSL beginning with V4R4). If you are using the *ADMIN server across an intranet of *trusted* users, you can probably safely use this for administration.

- The HTTP directives provide the foundation for all activity on your server. The shipped configuration provides the capability to serve a default Welcome page. A client cannot view any documents except the Welcome page until the server administrator defines directives for the server. To define directives, use a Web browser and the *ADMIN server or the Work with HTTP Configuration (WRKHTTPCFG) command. Both methods require *IOSYSCFG special authority. When you connect your AS/400 to the Internet, it becomes even more critical to evaluate and control the number of users in your organization who have *IOSYSCFG special authority.

Protecting Resources

Internet Connection Server and IBM HTTP Server for AS/400 both include HTTP directives that can provide detailed control of the information assets that the server uses. You can use directives to swap to other AS/400 user profiles and to require authentication for some resources. Following are some suggestions and considerations for using this support:

Note: The "Web serving with your IBM HTTP Server" in the AS/400 Information Center provides complete descriptions of the available HTTP directives and how to use them. It includes security examples and considerations.

- The HTTP server starts from the basis of "explicit authority." The server does not accept a request unless that request is explicitly defined in the directives. In other words, the server immediately rejects any request for a URL unless that URL is defined in the directives (either by name or generically). To take advantage of this initial protection that the directives provide, consider the following:
  - When you add a directive to the HTTP server, make the template value for the path as specific as possible. This reduces the chance that someone can browse through your system and discover files. Avoid using generic file names and wildcards.
  - Use Map or Pass directives to mask the file names on your AS/400 web server. (Both Map and Pass directives are methods for equating the URL that the client sends with a different name or resource on the server.) For example, the client (browser) might issue a URL that looks like the following:

    ```
    http://hostname/webdata/products
    ```

    Use the browser-based configuration and administration forms (or the WRKHTTPCFG command) to add a Pass directive to HTTP server configuration that looks like the following:

    ```
    Pass /webdata/products
         /QSYS.LIB/WEBDATA.LIB/WWWDATA.FILE/PRODUCTS.MBR
    ```

    The requester who sees this URL has no idea that the product data is in the WWWDATA file in the WEBDATA library on your AS/400 system. This method

protects (hides) your AS/400 file names and library names from potential hackers. It also gives you the flexibility to change your AS/400 application without having to change the URL.

- You can use protection directives to require a user ID and password before accepting a request for some or all of your resources. Following are some considerations for using this support:
  - When a user (client) requests a protected resource, the server challenges the browser for a user ID and password. The browser prompts the user to enter a user ID and password, and then sends the information to the server. Some browsers store the user ID and password and send them automatically with subsequent requests. This frees the user from repeatedly entering the same user ID and password on each request.

    Because some browsers store the user ID and password, you have the same user education task that you have when users enter your system through the AS/400 Sign On display or through a router. An unattended browser session represents a potential security exposure.
  - You have three options for how the system handles user IDs and passwords (specified in the protection directives):
    1. You can use normal AS/400 user profile and password validation. This is most commonly used to protect resources in an intranet (secure network).
    2. You can create "Internet users": users that can be validated but do not have a user profile on the AS/400 system. Internet users are implemented through an AS/400 object called a "validation list". Validation list objects contain lists of users and passwords that are specifically defined for use with a particular application.

       You decide how Internet user IDs and passwords are supplied (such as by an application, or by an administrator in response to an e-mail request), as well as how to manage Internet users. Use the HTTP server's browser-based interface to set this up.

       For nonsecure networks (the Internet), using Internet users provides better overall protection than using normal AS/400 user profiles and passwords. The unique set of user IDs and passwords creates a built-in limitation on what those users can do. The user IDs and passwords are not available for normal sign-on (such as with TELNET or FTP). In addition, you are not exposing normal AS/400 user IDs and passwords to sniffing.
    3. Lightweight directory access protocol (LDAP) is a directory service protocol that provides access to a directory over a Transmission Control Protocol (TCP) or SSL connection. It lets you store information in that directory service and query it in a database fashion. LDAP is now supported as a choice for user authentication.

    Notes:

    1. When the browser sends the user ID and the password (whether for an AS/400 user profile or an Internet user), they are encoded, not encrypted. The encoding scheme is an industry standard, and thus commonly known among the hacker community. Although the encoding is not easily understood by the casual "sniffer," a sophisticated sniffer probably has tools to attempt to decode them.
    2. AS/400 stores the validation object in a protected system area. You can access it only with defined system interfaces (APIs) and proper authorization.
  - You can use Digital Certificate Manager (DCM) to create your own intranet Certifcate Authority. Digital Certificate automatically associates a certificate

with the owner's AS/400 user profile. The certificate has the same authorizations and permissions as the associated profile.

- When the server accepts a request, normal AS/400 resource security takes over. The AS/400 user profile that requests the resource must have authority to the resource (such as the folder or source physical file that contains the HTML document). By default, jobs run under the QTMHHTTP user profile. You can use a directive to swap to a different AS/400 user profile. The system then uses that user profile's authority to access objects. Following are some considerations for this support:
  - Swapping user profiles can be particularly useful when your server provides more than one logical Web site. You can associate a different user profile with the directives for each Web site, and thus use normal AS/400 resource security to protect the documents for each site.
  - You can use the ability to swap user profiles in combination with the validation object. The server uses a unique user ID and password (separate from your normal AS/400 user ID and password) to evaluate the initial request. After the server has authenticated the user, the system then swaps to a different AS/400 user profile and thus takes advantage of AS/400 resource security. The user is, thus, not aware of the true user profile name and cannot attempt to use it in other ways (such as FTP).
- Some HTTP server requests need to run a program on the HTTP server. For example, a program might access data on your system. Before the program can run, the server administrator must map the request (URL) to a specific user-defined program that conforms to CGI user-interface standards. Following are some considerations for CGI programs:
  - You can use the protection directives for CGI programs just as you do for HTML documents. Thus, you can require a user ID and password before running the program.
  - By default, CGI programs run under the QTMHHTP1 user profile. You can swap to a different AS/400 user profile before running the program. Therefore, you can set up normal AS/400 resource security for the resources that your CGI programs access.
  - As security administrator, you should perform a security review before authorizing the use of any CGI program on your system. You should know where the program came from and what functions the CGI program performs. You should also monitor the capabilities of the user profiles under which you run CGI programs. You should also perform testing with CGI programs to determine, for example, whether you can gain access to a command line. Treat CGI programs with the same vigilance that you treat programs that adopt authority.
  - In addition, be sure to evaluate what sensitive objects might have inappropriate public authority. A poorly designed CGI program might, in rare cases, allow a knowledgeable, devious user to attempt to roam your system.
  - Use a specific user library, such as CGILIB, to hold all your CGI programs. Use object authority to control both who can place new objects in this library and who can run programs in this library. Use the directives to limit the HTTP server to running CGI programs that are in this library.

    Note: If your server provides multiple logical Web sites, you might want to set up a separate library for the CGI programs for each site.

Other Security Considerations

Following are additional security considerations:

- HTTP provides read-only access to your AS/400 system. HTTP server requests cannot update or delete data on your system directly. However, you might have CGI programs that update data. Additionally, you can enable the Net.Data CGI program to access your AS/400 database. The system uses a script (which is similar to an exit program) to evaluate requests to the Net.Data program. Therefore, the system administrator can control what actions the Net.Data program can take.

  Note: Prior to V4R3, the DB2WWW program provided the function that Net.Data provides.
- The HTTP server provides an access log that you can use to monitor both accesses and attempted accesses through the server.
- The *HTTP Server for AS/400 Webmaster's Guide* provides more information about security considerations.

HTTP Proxy Server

The HTTP proxy server comes with the IBM HTTP Server for AS/400. The HTTP Server is part of OS/400. The proxy server receives HTTP requests from Web browsers and resends them to Web servers. Web servers that receive the requests are only aware of the IP address of the proxy server and cannot determine the names or addresses of the PCs that originated the requests. The proxy server can handle URL requests for HTTP, FTP, Gopher and WAIS.

The proxy server caches returned Web pages from requests made by all proxy server users. Consequently, when users request a page, the proxy server checks whether the page is in the cache. If it is, the proxy server returns the cached page. By using cached pages, the proxy server is able to server Web pages more quickly, which eliminates potentially time-consuming requests to the Web server.

The proxy server can also log all URL requests for tracking purposes. You can then review the logs to monitor use and misuse of network resources.

You can use the HTTP proxy support in the IBM HTTP Server to consolidate Web access. Addresses of PC clients are hidden from the Web servers they access; only the IP address of the proxy server is known. Web page caching can also reduce communication bandwidth requirements and firewall workload.

Security Tips for Using SSL with IBM HTTP Server for AS/400

Both Internet Connection Server and IBM HTTP Server for AS/400 can provide secure Web connections to your AS/400. A **secure Web site** means that transmissions between the client and the server (in both directions) are encrypted. These encrypted transmissions are safe both from the scrutiny of sniffers and from those who attempt either to capture or to alter the transmissions.

Note: Keep in mind that a secure Web site applies strictly to the security of the information that passes between client and server. The intent of this is not to reduce your server's vulnerability to hackers. However, it certainly limits the information that a would-be hacker can obtain easily through sniffing.

The *HTTP Server for AS/400 Webmaster's Guide* provides complete information for installing, configuring, and managing the encryption process. This topic provides both an overview of the server features and some considerations for using the server.

Internet Connection Server provides http and https support when one of the following licensed programs is installed:

- 5769–NC1
- 5769–NCE

When these options are installed, the product is referred to as the Internet Connection Secure Server.

IBM HTTP Server for AS/400 (5769–DG1) provides both http and https support. You must install one of the following cryptographic products to enable SSL:

- 5769–AC1
- 5769–AC2
- 5769–AC3

Security that depends on encryption has several requirements:

- Both the sender and receiver (server and client) must "understand" the encryption mechanism and be able to perform encryption and decryption. The HTTP server requires an SSL-enabled client. (Most popular Web browsers are SSL-enabled.) The AS/400 encryption licensed programs support several industry-standard encryption methods. When a client attempts to establish a secure session, the server and client negotiate to find the most secure encryption method that both of them support.
- The transmission must not be able to be decrypted by an eavesdropper. Thus, encryption methods require both parties to have an encryption/decryption **private key** that only they know. If you want to have a secure *external* Web site, you should use an independent certificate authority (CA) to create and issue digital certificates to users and servers. The certificate authority is known as a trusted party.

Encryption protects the confidentiality of transmitted information. However, for sensitive information, such as financial information, you want integrity and authenticity in addition to confidentiality. In other words, the client and (optionally) the server must trust the party on the other end (through an independent reference) and they must be sure that the transmission has not been altered. The digital signature that is provided by a certification authority (CA) provides these assurances of authenticity and integrity. The SSL protocol provides authentication by verifying the digital signature of the server's certificate (and optionally the client's certificate).

Encryption and decryption require processing time and will affect the performance of your transmissions. Therefore, AS/400 provides the capability to run both the programs for secure and insecure serving at the same time. You can use the insecure HTTP server to serve documents that do not require security, such as your product catalog. These documents will have a URL that starts with `http://`. You can use a secure HTTP server for sensitive information such as the form where the customer enters credit card information. The program can serve documents whose URL starts either with `http://` or with `https://`.

Reminder

It is good Internet etiquette to inform your clients when transmissions are secure and not secure, particularly when your Web site only uses a secure server for some documents.

Keep in mind that encryption requires both a secure client and a secure server. Secure browsers (HTTP clients) have become fairly common.

Security Tips for Workstation Gateway Server

The Workstation Gateway Server (WSG) provides a TCP/IP application that transforms AS/400 5250 applications to Hypertext Markup Language (HTML) for dynamic display on Web browsers. When you set up the Workstation Gateway Server, you control whether users see a Sign On display or whether an exit program handles sign-on.

Note: AS/400 does not offer a secure version of the Workstation Gateway Server. Therefore, if your program gives control to the WSG server (perhaps for forms fill-in), remember that the WSG transmission is not encrypted.

Tips for Preventing WSG Access

If you *do not* want anyone to use WSG to access your system, you should prevent the WSG server from running. Do the following:

__ Step 1. To prevent WSG server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGWSGA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*NO) is the default value.

b. The DSPSGN attribute controls whether the system can display sign-on panels. DSPSGN(*NO) is the default value.

c. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent WSG from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for HTTP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `5061`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and

does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

Tips for Controlling WSG Access

As security administrator, you need to understand the purposes for the WSG server on your system and the client environments that will use the WSG server. For example, some users of the WSG server might be travelling employees who are using an intranet and accessing your system from inside a firewall. Other users might be anonymous visitors to your WEB site who want to request additional information about something they have seen.

Users can access the WSG server in these ways:

- From a direct request by a client browser.
- From an indirect request, when the HTTP server gives control to the WSG server.
- From a specific HTTP connect request. For example, a WEB site visitor might select an area of the WEB site that says `Send me additional information`. The HTTP server can send a request to the WSG server to display a panel that asks for the name and mailing address of the visitor.

Following are security considerations when you allow the WSG server to run on your system:

- To configure the WSG server, you use the Change Workstation Gateway Attributes (CHGWSGA) command. This command requires *IOSYSCFG special authority. One configuration controls all WSG sessions on your system. You can specify the following security-relevant values:
  - *Inactivity timeout*. The WSG server does not use the QINACTITV system value. The WSG server has its own value for determining how long the system will wait before it ends an inactive session. This value is particularly important in an environment where you may have WSG users who have more than minimum authority on your system.
  - *Display sign on panel*. When a WSG request comes from a World Wide Web browser, this value controls whether the system sends your system-defined sign-on display. You can use a WSG logon exit program to bypass the sign-on process and perform user validation.

    Often, a request to the WSG server performs a specific, limited function, such as presenting a form for completion. The Sign On display is not necessary in this environment. In fact, the Sign On display provides an opportunity for "hacking" that is not available when your exit program bypasses sign-on and uses a user profile with very limited authority. Instead, bypass the Sign On display and run WSG under a user profile that has limited authority on your system.
  - *Access logging*. You may find it useful to have your system keep a record of the accesses to your WSG server, particularly when you provide a new application.
- Some requests to the WSG server include a user ID and password. You have the same issues here that you have with SLIP connection scripts. Your security is dependent on the practices and capabilities of your communications partners. If the user ID and password are stored in a document on the client, they may be

accessible to potential intruders into your system. In addition, when the WSG session is an unsecure (Internet) session, the user ID and password are subject to sniffing.

- You can use the QLMTSECOFR system value as one method to limit the capability of WSG users. When the QLMTSECOFR value is 1, you can prevent any user with *ALLOBJ special authority from signing on to the WSG virtual workstations unless the user or QSECOFR is explicitly authorized.
- Remember that AS/400 does not provide a secure WSG server. Therefore, even if the Internet Connection Secure Server passes a request to the WSG server, the WSG transmission is not secure (encrypted).

Security Tips for Line Printer Daemon

LPD (line printer daemon) provides the capability to distribute printer output to your system. The system does not perform any sign-on processing for LPD.

Tips for Preventing LPD Access

If you *do not* want anyone to use LPD to access your system, you should prevent the LPD server from running. Do the following:

__ Step 1. To prevent LPD server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGLPDA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*YES) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for LPD, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `515`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

__ Step h. Repeat steps 2.c through 2.g for the *UDP protocol.

Tips for Controlling LPD Access

If you want to allow LPD clients to access your system, be aware of the following security issues:

- To prevent a user from swamping your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST). The *Backup and Recovery* book provides more information about ASP thresholds.
- You can use the authority to output queues to restrict who can send spooled files to your system. LPD users without an AS/400 user ID use the QTMPLPD user profile. You can give this user profile access to only a few output queues.

Security Tips for Simple Network Management Protocol

AS/400 can act as an agent in a simple network management protocol (SNMP) network. SNMP provides a means for managing the gateways, routers, and hosts in an Internet environment. An SNMP agent gathers information about the system and performs functions that remote SNMP network managers request.

Tips for Preventing SNMP Access

If you *do not* want anyone to use SNMP to access your system, you should prevent the SNMP server from running. Do the following:

__ Step 1. To prevent SNMP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGSNMPA AUTOSTART(*NO)
```

Notes:

a. AUTOSTART(*YES) is the default value.

b. "Controlling Which TCP/IP Servers Start Automatically" on page 126 provides more information about controlling which TCP/IP servers start automatically.

__ Step 2. To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for SNMP, do the following:

__ Step a. Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ Step b. Select option 4 (Work with TCP/IP port restrictions).

__ Step c. On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ Step d. For the lower port range, specify `161`.

__ Step e. For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) RFC1700 provides information about common port number assignments.

__ Step f. For the protocol, specify `*TCP`.

__ Step g. For the user profile field, specify a user profile name that is protected on your system. (A protected user profile is a user profile that does not own programs that adopt authority and does not have a password that is known by other users.) By restricting the port to a specific user, you automatically exclude all other users.

__ Step h. Repeat steps 2.c through 2.g for the *UDP protocol.

Tips for Controlling SNMP Access

If you want to allow SNMP clients to access your system, be aware of the following security issues:

- Someone who can access your network with SNMP can gather information about your network. Information that you have hidden by using aliases and a domain-name server becomes available to the would-be intruder through SNMP. Additionally, an intruder might use SNMP to alter your network configuration and disrupt your communications.
- SNMP relies on a community name for access. Conceptually, the community name is similar to a password. The community name is not encrypted. Therefore, it is vulnerable to sniffing. If your system is connected to the Internet, use the Add Community for SNMP (ADDCOMSNMP) command to set the manager Internet address (INTNETADR) parameter to one or more specific IP addresses instead of *ANY. You can also set the OBJACC parameter of the ADDCOMSNMP or CHGCOMSNMP commands to *NONE to prevent the managers in a community from accessing any MIB objects. This is intended to just be done temporarily to deny access to managers in a community without removing the community.

Security Tips for the INETD Server

Unlike most TCP/IP servers, the INETD server does not provide one single service to clients. Instead, it provides a variety of miscellaneous services that administrators can customize. For that reason, the INETD server is sometimes called "the super server". The INETD server has the following built-in services:

- time
- daytime
- echo
- discard
- chargen

These services are supported for both TCP and UDP. For UDP, the echo, time, daytime, and chargen services receive UDP packets, then send the packets back to the originator. The echo server echoes back packets that it receives, the time and daytime servers generate the time in a specific format and sends it back, and the chargen server generates a packet of printable ASCII characters and sends it back.

The nature of these UDP services makes a system vulnerable to a denial of service attack. For example, assume that you have two AS/400 systems: SYSTEMA and SYSTEMB. A malicious programmer could forge the IP header and the UDP header with a source address of SYSTEMA and a UDP port number of the time server. He can then send that packet to the time server on SYSTEMB, which will send the time

to SYSTEMA, which will respond back to SYSTEMB, and so on, generating a continuous loop and consuming CPU resources on both systems, as well as network bandwidth.

Therefore, you should consider the risk of such an attack on your AS/400 system, and only run these services on a secure network. The INETD server is shipped to not be autostarted when you start TCP/IP. You can configure whether or not to start the services when INETD is started. By default, the TCP and UDP time servers and daytime servers are both started when you start the INETD server.

There are two configuration files for the INETD server:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

These files determine what programs start when the INETD server starts. If a malicious programmer got access to these files, she could configure them to start any program when INETD started. Therefore it is very important to protect these files. By default they require QSECOFR special authority to make changes. You should not reduce the authority required to access them.

Note: Do not modify the configuration file in the ProdData directory. That file is replaced each time that the system is reloaded. Customer configuration changes should only be placed in the file in the UserData directory tree, as that file is not updated during release upgrades.

Tips for Limiting TCP/IP Roaming

If your system is connected to a network, you may want to limit your users' ability to roam the network with TCP/IP applications. One way to do this is to restrict access to the following client TCP/IP commands:

Note: These commands might exist in several libraries on your system. They are in both the QSYS library and the QTCP library, at a minimum. Be sure to locate and secure all occurrences.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC client)

Your users' possible destinations are determined by the following:

- Entries in your TCP/IP host table.
- *DFTROUTE entry in the TCP/IP route table. This allows users to enter the IP address of the next-hop system when their destination is an unknown network. A user can reach or contact a remote network by using the default route.
- Remote name server configuration. This support allows another server in the network to locate host names for your users.
- Remote system table.

You need to control who can add entries to these tables and change your configuration. You also need to understand the implications of your table entries and your configuration.

Be aware that a knowledgeable user with access to an ILE C compiler can create a socket program that can attach to a TCP or UDP port. You can make this more difficult by restricting access to the following sockets interface files in the QSYSINC library:

- SYS
- NETINET
- H
- ARPA
- sockets and SSL

For service programs, you can restrict use of socket and SSL applications (that are already compiled) by restricting use of these service programs:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

The service programs are shipped with public authority *USE, but the authority can be changed to *EXCLUDE (or another value as needed).

However, equivalent files are also available in many other environments. A determined programmer could upload the necessary files to the AS/400 from a PC. If you have an ILE C compiler, you probably need to restrict access to TCP ports and to UDP ports if you want to prevent network roaming. Also, Java does not use the service programs listed above to access sockets. You will need to restrict access to ports if you want to prevent roaming by Java programs.

Tips for Securing the TCP/IP File Server Support for OS/400 Licensed Program

Attention V3R7 and V4R1 Users

The Network File System (NFS) in the integrated file system replaces the function of the TCP/IP File Server Support for OS/400 licensed program. See "Security Tips for the Network File System" on page 94 for more information.

When you have the TCP/IP File Server Support for OS/400 licensed program, your AS/400 system can act as a network file server for other systems in a TCP/IP network. A client system can "mount" an AS/400 directory as if it is a local directory. The QSYS library, which includes all libraries on the AS/400 system, can look like a directory and subdirectories on the client system.

To a great extent, the File Server Support product relies on the security capabilities of the client system to control access to AS/400 resources. If you are a AS/400 security administrator and you have this product installed on your system, you should review the product documentation to understand both the functions that it

provides and the security implications. With the shipped configuration for File Server Support, your system resources are vulnerable to unintended use by File Server Support users.

Following are some suggestions for protecting your AS/400 system when TCP/IP File Server Support for OS/400 is installed:

- Remove all root-level user profile entries from the export table and from the authorized users table. Do not allow the shipped profile, Q7FSOWN, to have root authority. On other systems that can be client systems for File Server Support, it is possible to set up a user that pretends to have root authority. You need to protect your system from this.
- For the configuration database files for File Server Support, set the database capabilities value to *NO for all attributes except *READ. This protects the contents of File Server Support database files from unauthorized changes outside the commands and the menu interfaces that are part of the product.
- Set up your system to reject any requests that do not have a user identification (uid) specified explicitly. Do not allow such requests to use a default user.
- Review all the entries in the export table to ensure that they meet your security requirements. Consider removing all of the default entries that are provided with the product and setting up only entries that you know will not cause a security exposure.
- For the CL commands that start and stop the File Server Support function, set the public authority to *EXCLUDE. This allows you to control when the File Server Support environment is active and who can activate it. Grant authority only to trusted administrators on your system.
- When you add entries to the export table, in most cases you should set the write permission and the root access to *NO. Use other values cautiously. You can change the default values for the command to *NO to help you avoid oversights.
- Potentially serious security exposures exist when your AS/400 system is a server for a client that does not protect the ROOT uid with a nontrivial password.

Using VPN to Secure TCP/IP Applications

Beginning with V4R4, you can use Virtual Private Networking (VPN) to selectively protect any or all of your TCP/IP applications. See “Adding Virtual Private Networks (VPN)” on page 219 for information on VPN.

Chapter 14. Tips for Client-Server Security

Many of your system users have personal computers on their desks as their workstations. They use tools that run on the PC, and they use the PC to connect to AS/400.

Most methods of connecting a PC to AS/400 provide more function than workstation emulation. The PC may look like a display to AS/400 and provide the user with interactive sign-on sessions. In addition, the PC may look to AS/400 like another computer and provide functions such as file transfer and remote procedure call.

As an AS/400 security administrator, you need to be aware of the following:

- Functions that are available to PC users who are connected to your system
- AS/400 resources that PC users can access.

You may want to prevent advanced PC functions (such as file transfer and remote procedure call) if your AS/400 security scheme is not yet prepared for those functions. Probably, your long-range goal is to allow advanced PC functions while you still protect the information on your system. The topics that follow discuss some of the security issues that are associated with PC access.

Tips for Securing PC Data Access

Some PC client software, such as the Client Access for DOS with Extended Memory, uses shared folders to store information on AS/400. To access AS/400 database files, the PC user has a limited, well-defined set of interfaces. With the file transfer capability that is part of most client/server software, the PC user can copy files between the AS/400 system and the PC. With database access capability; such as a DDM file, remote SQL, or an ODBC driver; the PC user can access data on the AS/400 system.

In this environment, you can create programs to intercept and evaluate PC-user requests to access AS/400 resources. When the requests use a DDM file, you specify the exit program in the distributed data management access (DDMACC) network attribute. For some methods of PC file transfer, you specify the exit program in the client request access (PCSACC) network attribute. Or, you can specify PCSACC (*REGFAC) to use the registration function. When the requests use other server functions to access data, you can use the WRKREGINF command to register exit programs for those server functions.

Exit programs, however, can be difficult to design, and they are rarely foolproof. Exit programs are not a replacement for object authority, which is designed to protect your objects from unauthorized access from any source.

Some client software, such as AS/400 Client Access for Windows 95/NT client, uses the integrated file system to store and access data on AS/400. With the integrated file system, the entire AS/400 becomes more easily available to PC users. Object authority becomes even more essential. Through the integrated file system, a user with sufficient authority can view an AS/400 library as if it is a PC directory. Simple move and copy commands can instantly move data from an AS/400 library to a PC directory or vice versa. The system automatically makes the appropriate changes to the format of the data.

Notes:

1. You can use an authorization list to control the use of objects in the QSYS.LIB file system. See "Restricting Access to the QSYS.LIB File System" on page 90 for more information.
2. "Chapter 11. Tips for Securing the Integrated File System" on page 85 provides more information about security issues with the integrated file system.

The strength of the integrated file system is its simplicity for users and developers. With a single interface, the user can work with objects in multiple environments. The PC user does not need special software or APIs to access objects. Instead, the PC user can use familiar PC commands or "point and click" to work with objects directly.

For all systems that have PCs attached, but particularly for systems that have client software that uses the integrated file system, a good object authority scheme is critical. Because security is integrated into OS/400, any request to access data must go through the authority checking process. Authority checking applies to requests from any source and to data access that uses any method.

Object Authority with PC Access

When you set up authority for objects, you need to evaluate what that authority provides for the PC user. For example, when a user has *USE authority to a file, the user can view or print data in the file. The user cannot change information in the file or delete the file. For the PC user, viewing is equivalent to "reading", which provides sufficient authority for the user to make a copy of a file on the PC. This may not be what you intend.

For some critical files, you may need to set the public authority to *EXCLUDE to prevent downloading. You can then provide another method to "view" the file on AS/400, such as using a menu and programs that adopt authority.

Another option to prevent downloading is to use an exit program that runs whenever a PC user starts an AS/400 function (other than interactive sign-on). You can specify an exit program in the PCSACC network attribute by using the Change Network Attribute (CHGNETA) command. Or, you can register exit programs by using the Work with Registration Information (WRKREGINF) command. The method that you use depends on how PCs are accessing data on your system and which client program the PCs use. The exit program (QIBM_QPWFS_FILE_SERV) applies to Client Access and Net Server access to IFS. It does not prevent access from a PC with other mechanisms, such as FTP or ODBC.

PC software typically provides upload capability also, so that a user can copy data from the PC to an AS/400 database file. If you have not set up your authority scheme correctly, a PC user might overlay all of the data in a file with data from a PC. You need to assign *CHANGE authority carefully. Review Appendix D in the *Security - Reference* book to understand what authority is required for file operations.

The *Client Access Express for Windows Host Servers* book provides more information about the authority for PC functions and about using exit programs.

Using SSL with Client Access Express

Beginning with V4R4, you can use secure sockets layer (SSL) to protect communications between Client Access Express and AS/400. Client Access Express includes optionally installable support for SSL and a way to manage key databases using IBM Key Management. All Client Access Express functions can communicate over SSL except MAPI. Client Access Express allows SSL communications with the AS/400 server at three levels of encryption (40-bit, 56-bit, 128-bit). To use SSL with Client Access Express, you must install the following products on your AS/400.

- TCP/IP Connectivity Utilities for AS/400, 5769-TC1
- Cryptographic Access Provider, 5769-ACx
- IBM HTTP Server for AS/400, 5769-DG1
- Digital Certificate Manager, 5769-SS1
- Client Encryption, 5769-CEx

In order for the client PCs in your network to communicate over SSL, they must have one of the following products installed:

- 40-bit Client Encryption, 5769-CE1
- 56-bit Client Encryption, 5769-CE2
- 128-bit Client Encryption, 5769-CE3

For more information about using SSL with Client Access Express, see the topic "Client Access Express" in the AS/400 Information Center, or the book *Client Access Express for Windows - Setup*.

Security and Operations Navigator

Operations Navigator provides an easy-to-use interface to your AS/400 for users who have Client Access. With each new release of OS/400, more AS/400 function becomes available through Operations Navigator.

An easy-to-use interface provides many benefits, including reduced technical support costs and an improved image for your system. It also presents security challenges. As a security administrator, you can no longer rely on the ignorance of your users to protect resources. Operations Navigator makes many functions easy and visible for your users. You need to ensure that you have designed and implemented security policies for user profiles and for object security to meet your security needs.

Version 4 Release 4 Modification 0 of AS/400 Client Access Express for Windows provides the following methods to control the functions that users can perform through Operations Navigator:

- Selective Install
- Application Administration
- Windows NT System Policy support

Operations Navigator is packaged into multiple components in V4R4 that you can install separately. This allows you to install only the functions that you require. Application Administration allows an administrator to control the functions that a user or group can access through Operations Navigator. Application Administration organizes applications into the following categories:

AS/400 Operations Navigator
Includes Operations Navigator and any plug-ins.

Client Applications
Includes all other client applications, including Client Access Express, that provide functions on clients that are administered through Application Administration.

Host Applications
Includes all applications that reside entirely on your AS/400 and provide functions that are administered through Application Administration.

You can use selective install, Application Administration, and policies to limit the Operations Navigator functions that a user can access. None of these, however, should be used for resource security.

Beginning in V4R4, AS/400 Client Access Express for Windows also supports using the Windows NT System Policy Editor to control what functions can be performed from a particular PC client, regardless of who is using that PC.

See the AS/400 Information Center for additional information on selective installation, Application Administration and Policy Administration. The "Limit Access to Program Function" on page 15 section of this book also contains some discussion of application administration.

Tips for Open Database Connectivity Access

Open database connectivity (ODBC) is a tool that PC applications can use to access AS/400 data as if the data is PC data. The ODBC programmer can make the physical location of the data transparent to the user of the PC application. Following are several security considerations when ODBC applications access your AS/400:

- When attached PCs have ODBC applications that access AS/400 data, a good object authority scheme is essential. However, object authority may not provide detailed enough protection for your data. For example, you may want to prevent users from changing data in file FILEB except when using a specific program (PGMX).

  For applications that run directly on AS/400, such as an RPG or COBOL program, you can use adopted authority to control how users update database files. For example, assume that public users have *USE authority to FILEA, but certain users are authorized to program PGMX. PGMX adopts its owner's authority, which allows users to change the file when they run the PGMX program

  When you have ODBC applications on attached PCs, you can use stored procedures to provide a similar level of control over who can update data. A stored procedure can be an AS/400 program object that adopts authority. The ODBC application can send requests to update data to the stored procedure instead of accessing the file directly. Therefore, PC users do not need to have the authority to change the files. You can give specific PC users the authority to use the program (stored procedure) that updates the file.

  When you use stored procedures instead of directly accessing data with ODBC applications, you also keep your AS/400 database structure and application architecture private. When you require ODBC programmers to use stored procedures, they cannot use an ODBC spy program to monitor the database

access. This makes it more difficult for an ODBC programmer to reverse-engineer either your database design or your application design.

- When a user requests access to a database by using ODBC, you can set up exit programs to monitor (and approve or reject) the request. The following exit points are available for ODBC requests:
  - QIBM_QZDA_NDB1, QIBM_QZDA_SQL1, and QIBM_QZDA_SQL2 control read-only access to database files.
  - During server initialization (when the ODBC connection is made), the system calls the QIBM_QZDA_INIT program. You can use this exit point to validate a session and to set up the environment for that session. For example, you could start a query governor during initialization to limit long-running queries.
  - When a user requests an operation that affects an entire file (such as deleting or clearing a file), the system calls the QIBM_QZDA_NDB1 program. You can use the exit program to accept or reject these requests.
  - When an ODBC application sends a structured query language (SQL) request, the system calls the QIBM_QZDA_SQL1 and QIBM_QZDA_SQL2 program. Your exit program can evaluate the request and determine whether to permit the specific request. For example, the request might be to view a set of records or to add or delete records in a database file.
  - When your system receives a request for information about your database structure (a catalog request), the system calls the QIBM_QZDA_ROI1 program.—Keep in mind that the IBM Database Server uses these exit points. AS/400 ODBC drivers from other providers might not use the same exit points. They may provide their own server or they may use DRDA (Distributed relational database access) to access the AS/400. DRDA requests come through DDM (Distributed Database Management). Beginning in V4R3, if the exit point for DDM has a program defined for it, that program will be called on a DRDA connect. The following PTFs enable this function in V4R1 and V4R2:

    ```
    VRM410 SF46018                VRM420  SF46017
    ```

    An exit program for DDM can be defined using the CHGNETA (Change Network Attributes) command and specifying a program name for DDMACC parameter.
- The following publications provide information to help you and your ODBC programmers understand the security aspects of ODBC applications:
  - *Client Access Express for Windows Host Servers* book
  - *Client Access for Windows 3.1 ODBC User's Guide* book
  - *Distributed Data Management* book
  - *AS/400 Client/Server Performance using the Windows 3.1 Client* (SG24-4526)
  - *DATABASE 2/400 Advanced Database Functions* (GG24-4249)
- Two informational APARs are available that discuss ODBC security: II09333 and II09334. The information in these APARs is written from the perspective of the ODBC programmer who is not familiar with AS/400 capabilities. As a security administrator, you can provide these informational APARs to your ODBC programmers to help them understand the security issues and possible solutions. The information in these APARs should help you to bridge the terminology gap between the AS/400 environment and the ODBC and PC environment.

Security Considerations for PC Session Passwords

Typically, when a PC user starts the connection software, such as Client Access, the user types the user ID and password for the server once. The password is encrypted and stored in PC memory. Whenever the user establishes a new session to the same server, the PC sends the user ID and password automatically.

Some client/server software also provides the option of bypassing the Sign On display for interactive sessions. The software will send the user ID and encrypted password when the user starts an interactive (5250 emulation) session. To support this option, the QRMTSIGN system value on the AS/400 server must be set to *VERIFY.

When you choose to allow bypassing the Sign On display, you need to consider the security trade-offs.

Security Exposure When You Require the Sign On Display: For 5250 emulation or any other type of interactive session, the Sign On display is the same as any other display. Although the password is not displayed on the screen when it is typed, the password is sent over the link in unencrypted form just like any other data field. For some types of links, this may provide the opportunity for a would-be intruder to monitor the link and to detect a user ID and password. Monitoring a link by using electronic equipment is often referred to as **sniffing**. Beginning with V4R4, you can use secure sockets layer (SSL) to encrypt communication between Client Access Express and the AS/400 server. This protects your data, including passwords, from sniffing.

Security Exposure When You Bypass the Sign On Display: When you choose the option to bypass the Sign On display, the PC encrypts the password before it is sent. Encryption avoids the possibility of having a password stolen by sniffing. However, you must ensure that your PC users practice operational security. An unattended PC with an active session to the AS/400 system provides the opportunity for someone to start another session without knowing a user ID and password. PCs should be set up to lock when the system is inactive for an extended period, and they should require a password to resume the session.

Even if you do not choose to bypass the Sign On display, an unattended PC with an active session represents a security exposure. By using PC software, someone can start a server session and access data, again without knowing a user ID and a password. The exposure with 5250 emulation is somewhat greater because it requires less knowledge to start a session and begin accessing data.

You also need to educate your users about the effect of disconnecting their Client Access session. Many users assume (logically but incorrectly) that the disconnect option completely stops their connection to the AS/400. In fact, when a user selects the option to disconnect, the AS/400 makes the user's session (license) available for another user. However, the client's connection to the AS/400 is still open. Another user could walk up to the unprotected PC and get access to AS/400 resources without ever entering a user ID and password.

You can suggest two options for your users who need to disconnect their sessions:

- Ensure that their PCs have a lockup function that requires a password. This makes an unattended PC unavailable to anyone who does not know the password.

- To completely disconnect a session, either log off Windows or restart (reboot) the PC. This ends the session to the AS/400.

You also need to educate your users about a potential security exposure when they use AS/400 Client Access for Windows 95/NT. When a user specifies a UNC (universal naming convention) to identify an AS/400 resource, the Win95 or NT client builds a network connection to link to the AS/400. Because the user specifies a UNC, the user does not see this as a mapped Network Drive. Often, the user is not even aware of the existence of the network connection. However, this network connection represents a security exposure on an unattended PC because the AS/400 appears in the directory tree on the PC. If the user's AS/400 session has a powerful user profile, AS/400 resources might be exposed on an unattended PC. As with the previous example, the remedy is to ensure both that users understand the exposure and that they use their PC's lockup function.

Tips for Protecting AS/400 from Remote Commands and Procedures

A knowledgeable PC user with software such as Client Access can run commands on an AS/400 system without going through the Sign On display. The following are several methods that are available for PC users to run AS/400 commands. Your client/server software determines the methods that your PC users have available to them.

- A user can open a DDM file and use the remote command function to run a command.
- Some software, such as Client Access optimized clients, provides the remote command function through Distributed Program Call (DPC) APIs, without the use of DDM.
- Some software, such as remote SQL and ODBC, provides a remote command function without either DDM or DPC.

For client/server software that uses DDM for remote command support, you can use the DDMACC network attribute to prevent remote commands completely. For client/server software that uses other server support, you can register exit programs for the server. If you want to allow remote commands, you must make sure that your object authority scheme protects your data adequately. Remote command capability is equivalent to giving a user a command line. In addition, when AS/400 receives a remote command through DDM, the system does not enforce the user profiles Limited capability (LMTCPB) setting.

Tips for Protecting PCs from Remote Commands and Procedures

The AS/400 Client Access for Windows 95/NT client software, for example, provides the capability of receiving remote commands on the PC. You can use the Run Remote Command (RUNRMTCMD) command on AS/400 to run a procedure on an attached PC. The RUNRMTCMD capability is a valuable tool for system administrators and help-desk personnel. However, it also provides the opportunity for damaging PC data, either deliberately or accidentally.

PCs do not have the same object authority functions as AS/400. Your best protection against problems with the RUNRMTCMD command is to carefully restrict the AS/400 users who have access to the command. The AS/400 Client Access for Windows 95/NT client software provides the capability to register which users can run remote commands on a specific PC. When the connection is via TCP/IP, you can use the properties control panel on the client to control remote-command

access. You can authorize users by user ID or by the remote system name. When the connection is via SNA, some client software provides the capability to set up security for the conversation. With other client software, you simply choose whether or not to set up the incoming-command capability.

For each combination of client software and connection type (such as TCP/IP or SNA), you need to review the potential for incoming-commands to attached PCs. Consult the client documentation by searching for "incoming command" or "RUNRMTCMD". Be prepared to advise your PC users and network administrators about the correct (secure) way to configure clients to permit or prevent this capability.

Tips for Gateway Servers

Your system may participate in a network with an intermediate or gateway server between the AS/400 system and the PCs. For example, your AS/400 system might be attached to a LAN with a PC server that has PCs that are attached to the server. The security issues in this situation depend on the capabilities of the software that is running on the gateway server. Figure 43 shows an example of a gateway-server configuration:

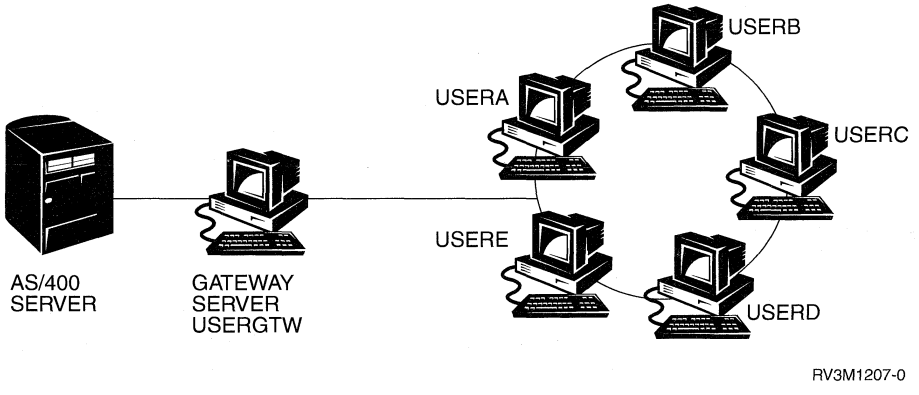


Figure 43. AS/400 with a Gateway Server–Example

With some software, your AS/400 system will not know about any users (such as USERA or USERC) who are downstream from the gateway server. The server will sign on to AS/400 as a single user (USERGTW). It will use the USERGTW user ID to handle all requests from downstream users. A request from USERA will look to AS/400 like a request from user USERGTW.

If this is the case, you must rely on the gateway server for security enforcement. You must understand and manage the security capabilities of the gateway server. From an AS/400 perspective, every user has the same authority as the user ID that the gateway server uses to start the session. You might think of this as equivalent to running a program that adopts authority and provides a command line.

With other software, the gateway server passes requests from individual users to AS/400. AS/400 knows that USERA is requesting access to a particular object. The gateway is almost transparent to AS/400.

If your system is in a network that has gateway servers, you need to evaluate how much authority to provide to the user IDs that are used by the gateway servers. You also need to understand the following:

- The security mechanisms that the gateway servers enforce.
- How downstream users will appear to your AS/400 system.

Tips for Wireless LAN Communications

Some clients might use the AS/400 Wireless LAN to communicate to your AS/400 system without wires. The AS/400 Wireless LAN uses radio-frequency communications technology. As a security administrator, you should be aware of the following security characteristics of AS/400 Wireless LAN products:

- These wireless LAN products use spread spectrum technology. This same technology has been used by the government in the past to secure radio transmissions. To someone who attempts to electronically monitor for data transmissions, the transmissions appear to be noise rather than an actual transmission.
- The wireless connection has three security-relevant configuration parameters:
  - Data rate (two possible data rates)
  - Frequency (five possible frequencies)
  - System identifier (8 million possible identifiers)

  These configuration elements combine to provide 80 million possible configurations, which makes a hacker's likelihood of guessing the correct configuration extremely slim.
- Just like with other communications methods, the security of wireless communications is affected by the security of the client device. The system ID information and other configuration parameters are in a file on the client device and should be protected.
- If a wireless device is lost or stolen, normal AS/400 security measures, such as sign-on passwords and object security, provide protection when an unauthorized user attempts to use the lost or stolen unit to access your system.
- If a wireless client unit is lost or stolen, you should consider changing the system ID information for all users, access points, and systems. Think of this as changing the locks on your doors if a set of keys is stolen.
- You might want to partition your server into groups of clients that have unique system IDs. This limits the impact if a unit is lost or stolen. This method works only if you can confine a group of users to a specific portion of your installation.
- Unlike wired LAN technology, wireless LAN technology is proprietary. Therefore, no electronic sniffers are publicly available for these wireless LAN products. (A sniffer is an electronic device that performs unauthorized monitoring of a transmission.)

Tips for using AS/400 Operations Console

In V4R3, IBM introduced AS/400 Operations Console, which allows you to use your PC to access and control your AS/400 system. Beginning with V4R4, the Operations Console function includes support for a remote console, enabling you to administer the system Console through a dial-up connection. When you use Operations Console, be aware of the following:

- Operations Console has an "attended mode". When Operations Console is in attended mode, an operator at the local PC must be present to grant or refuse access when a user at a remote PC attempts to establish a remote console session.
- You can do any tasks that you could do from a traditional console from Operations Console. For example, user profiles that have *SERVICE or *ALLOBJ special authority are able to sign on to the Operations Console session, even if they are disabled.
- Operations Console uses a DST userid and password to enable the connection to AS/400. This makes it especially important to change your DST userids and passwords. Hackers are likely to be familiar with the default DST userids and passwords, and could use them to establish a remote console session to your AS/400.
- To protect your information when using the Remote Console, use the call back option of Windows Dial-Up Networking.

For additional information about AS/400 Operations Console, see *Operations Console Setup*.

Chapter 15. Tips for Using Security Exit Programs

Some AS/400 functions provide an exit so that your system can run a user-created program to perform additional checking and validation. For example, you can set up your system to run an exit program every time that someone attempts to open a DDM (distributed data management) file on your system. You can use the registration function to specify exit programs that run under certain conditions.

Several AS/400 publications contain examples of exit programs that perform security functions. Table 24 provides a list of these exit programs and sources for example programs.

Table 24. Sources of Sample Exit Programs

Type of Exit Program	Purpose	Where to Find an Example
Password validation	You specify this program name in the QPWDVLDPGM system value to check a new password for additional requirements that are not handled by the QPWDxxx system values. The use of this program should be carefully monitored because it receives unencrypted passwords. This program should not store passwords in a file or pass them to another program.	• *An Implementation Guide for AS/400 Security and Auditing, GG24-4200* • *Security - Reference*, SC41-5302-03
PC Support/400 or Client Access access	You can specify this program name in the Client request access (PCSACC) parameter of the network attributes to control the following functions: • Virtual printer function • File transfer function • Shared folders Type 2 function • Client access message function • Data queues • Remote SQL function	• *An Implementation Guide for AS/400 Security and Auditing, GG24-4200* • *Client Access/400 for DOS and OS/2 Technical Reference*, SC41-3563-01 • *Client Access for Windows 3.1 ODBC User's Guide*, SC41-3533-01
Distributed Data Management (DDM) access	You can specify this program name in the DDM request access (DDMACC) parameter of the network attributes to control the following functions: • Shared folders Type 0 and 1 function • Submit Remote Command function	• *An Implementation Guide for AS/400 Security and Auditing, GG24-4200*
Remote sign on	You can specify a program in the QRMTSIGN system value to control what users can be automatically signed on from which locations (pass-through.)	• *An Implementation Guide for AS/400 Security and Auditing, GG24-4200*
Open Database Connectivity (ODBC) with Client Access	Control the following functions of ODBC: • Whether ODBC is allowed at all. • What functions are allowed for AS/400 database files. • What SQL statements are allowed. • What information can be retrieved about database server objects. • What SQL catalog functions are allowed.	• *Client Access for Windows 3.1 ODBC User's Guide*, SC41-3533-01 • *Client Access Express for Windows Host Servers*, SC41-5740-03

Table 24. Sources of Sample Exit Programs (continued)

Type of Exit Program	Purpose	Where to Find an Example
QSYSMSG break handling program	You can create a program to monitor the QSYSMSG message queue and take appropriate action (such as notifying the security administrator) depending on the type of message.	• *An Implementation Guide for AS/400 Security and Auditing, GG24-4200*
TCP/IP	Several TCP/IP servers (such as FTP, TFTP, TELNET, and REXEC) provide exit points. You can add exit programs to handle log-on and to validate user requests, such as requests to get or put a specific file. You can also use these exits to provide anonymous FTP on your system.	• "TCP/IP User Exits" in *TCP/IP Configuration and Reference*, SC41-5420-03
User profile changes	You can create exit programs for the following user profile commands: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *Security - Reference*, SC41-5302-03 • *System API Reference*, SC41-5801-03

Chapter 16. Security Considerations for Java

Java is rapidly becoming widely accepted and used. You might be using the AS/400 Toolbox for Java on your system to develop new applications. Your users who have Internet access might be accessing Web pages that run Java applets. While Java is a robust language that provides some tools and features to help programmers write secure programs, Java alone does not secure your information assets. This section discusses security considerations for:

- Java Applications
- Java Applets
- Java Servlets

Java Applications

Java applications reside on the AS/400 system or PC on which they execute, and are executed using the Java virtual machine that is installed on that system. The security concerns for Java applications on AS/400 are the same as those for other applications on AS/400.

The application can perform functions or access objects on the AS/400 system only if the user profile that it runs under has authorization to those functions or objects. Some applications run under the user profile of the current user, while others run under a default user profile, which may or may not have a significant amount of authority. When writing your own Java applications, it is a good idea to have it run under the current user profile.

A good resource security scheme is essential when you begin to use Java application to provide new application function. When the AS/400 system processes requests from any application, including Java applications, it does not use menu access control or the limited capability value in the user's profile. Menu access control is only in effect for menus and commands displayed or entered from a 5250 session. Requests that are processed by software servers are not subject to menu access control or limited capability.

Beginning with V4R4 AS/400 Java supports SSL (secure sockets layer). Data (including user IDs and passwords) can be encrypted when users access Java applications on your AS/400 from the Internet. However, prior to V4R4, SSL was not supported, and data could not be encrypted.

Also beginning with V4R4, Java programs may adopt the authority of their owner or use the adopted authority that is in effect when the Java application is started. Use the CRTJVAPGM command to set the User Profile attribute to *OWNER to adopt the owner's authority. To use the adopted authority in effect when the Java application is started, set the Use Adopted Authority attribute to USE. Adopted authority may be used on any Java entity that can be used as the Class File or Jar file parameter on the CRTJVAPGM command. A Java program that adopts the authority of its owner will not be automatically regenerated if the associated class file changes.

A Java application that runs on a PC can attempt to connect to any TCP/IP port on a server. The server application code determines whether or not a user ID and password are required. However, for servers with Java Toolbox, the application must provide a user ID and password when it wants to establish a connection back

to the server. In this case, the server is an AS/400 system. Typically, the Toolbox class prompts the user for a user ID and password for the first connection.

Java Applets

Java applets are small Java programs that reside on a web server. They are downloaded to a client, and run on the client through the Java provided by a web browser. Because applets run on the client, what they do is a client concern. Good AS/400 server security management protects AS/400 resources regardless of what the applet tries to do. On the other hand, who can access the applet is an AS/400 server concern. Use HTTP server directives and OS/400 resource security to control access to the applet.

Java applets do have the potential to access your AS/400 but, in general, Java applications can establish a session only with the server from which the application originated. Therefore, a Java application can access your AS/400 from a connected PC only when the application came from your AS/400 (such as from your Web server).

The appletviewer allows you to test an applet on the server system. The appletviewer is not subject to security restrictions implemented by a browser. For that reason, you should only use the appletviewer tool only to test your own applets, never to run applets from outside sources.

Java Servlets

Servlets are server side components, written in Java, which dynamically extend the functionality of a web server without changing web server code. The IBM WebSphere Application Server that is shipped with IBM HTTP Server for AS/400 provides support for servlets on AS/400.

Servlets are more complicated to secure than other types of Java programs. Applying resource security to a servlet does not sufficiently secure it. Once a servlet is loaded by a web server, resource security does not prevent others from running it.

You must use resource security on objects that the server uses. You can also improve the security of servlets by using the following IBM HTTP Server for AS/400 protection directives:

- Run servlets under the requester's user profile (UserID=%%CLIENT), or under a specified user profile.
- Do not allow servlets to run under the web server's profile.
- Control who can run the servlet (mask keywords in the protection directive).
- Use HTTP Server groups and Access Control Lists (ACLs).

Chapter 17. Security Considerations for Browsers

Many PC users in your organization have browsers on their workstations. They might connect to the Internet. They might also connect to your AS/400. Following are some security considerations both for the PCs and for your AS/400.

Risk: Damaging the Local PC

A Web page that your user visits might have an associated "program," such as a Java applet, an Active-X control, or some other type of plug-in. Although it is rare, this type of "program" when run on a PC has the potential to damage the information on the PC. As a security administrator, consider the following for protecting PCs in your organization:

- Understand the security options of the different browsers that your users have. For example, with some browsers, you can control the access that Java applets have outside the browser (the restricted operating environment of Java is called the *sandbox*). This can prevent applets from damaging PC data.

  Note: The sandbox concept and its associated security restrictions do not exist for Active-X and other plug-ins.
- Make recommendations to your users about their browser settings. You probably do not have either the time or the resources to ensure that users follow your recommendations. Therefore, you must educate them about the potential risks of improper settings.
- Consider standardizing on Web browsers that provide the security options that you need.
- Instruct your users to inform you of any suspicious behavior or symptoms that might be associated with particular Web sites.

Risk: Accessing AS/400 Directories through Mapped Drives

Assume that a PC is connected to your AS/400 with a AS/400 Client Access for Windows 95/NT session. The session set up mapped drives to link to the AS/400 integrated file system. For example, the PC's **G** drive might map to the integrated file system of the SYSTEM1 AS/400 in the network.

Now assume that the same PC user has a browser and can access the Internet. The user requests a Web page that runs a mischievous "program" such as a Java applet or Active-X control. Conceivably, the program could attempt to erase everything on the PC's G drive.

You have several protections against damage to mapped drives:

- Your most important protection is resource security on your AS/400. The Java applet or Active-X control looks to the AS/400 like the user who established the PC session. You need to carefully manage what PC users are authorized to do on your AS/400.
- You must advise your PC users to set their browsers to prevent attempts to access mapped drives. This works for Java applets but not for Active-X controls, which do not have the sandbox concept.
- You must educate your users about the dangers of being connected to your AS/400 and the Internet in the same session. Also, make sure your PC users

(with Windows 95 clients, for example) understand that drives remain mapped even when the Client Access session appears to be ended.

Risk: Trusting Signed Applets

Your users might have followed your advice and set up their browsers to prevent applets from writing to any PC drives. However, your PC users need to be aware that a *signed applet* can override the setting for their browser.

A signed applet has an associated digital signature to establish its authenticity. When a user accesses a Web page that has a signed applet, the user sees a message. The message indicates the applet's signature (who signed it and when it was signed). When your user accepts the applet, the user grants the applet an override to the security settings for the browser. The signed applet can write to the PC's local drives, even though the default setting for the browser prevents it. The signed applet can also write to mapped drives on your AS/400 because they appear to the PC to be local drives.

For your own Java applets that come from your AS/400, you might need to use signed applets. However, you should instruct your users in general not to accept signed applets from unknown sources.

Chapter 18. Tips for Domino for AS/400 security

Both AS/400 and Domino provide integrated security to protect the privacy and integrity of information. They provide authentication of users and access control to ensure that only authorized users can work with information and programs.

Domino for AS/400 takes advantage of the security characteristics of both platforms. Domino security behaves in the same way that it behaves on other servers to protect the portability of Domino applications. AS/400 security provides an additional layer of security protection beneath Domino security.

Review the following topics to understand how you work with these two complimentary security systems both to enable function and to protect resources.

Types of users for Domino for AS/400

Your Domino for AS/400 server can have three types of users:

Domino-only users
These users connect to the server from a Notes client or a browser. They do not use any AS/400 functions except the Domino for AS/400 server. These users do not need an AS/400 user profile.

Domino and AS/400 users
These users connect to the server from a Notes client or a browser. They also access your AS/400 in others ways, such as with 5250 workstation emulation or Client Access. These users need both an AS/400 user profile and a Domino registration.

Domino users who need DB2/400 access
These users connect to the server from a Notes client or browser. Although they do not use other AS/400 functions, these users run Domino applications that access DB2/400 database files. Whether these users need an AS/400 user profile depends on the strategy that you choose in your Domino applications for providing access to the data.

Authority requirements for Domino for AS/400 administrators

Users who perform Domino administrative functions need authority to perform those functions. (You do not want every Domino or AS/400 user to be able to administer your Domino server.) To help you plan the authority for your Domino administrators, think of the administrative tasks in two different categories:

Domino-only administrative tasks:

These tasks occur within the Domino server when it is running. They do not require any interaction with the AS/400 server environment outside of Domino. A Domino-only administrator does not need any special authorities on your AS/400. In fact, a Domino-only administrator does not even need an AS/400 user profile. The Domino documentation describes how to give this type of administrative authority within Domino.

Following are several examples of Domino-only administrative tasks:

Creating a new Domino database
From an AS/400 perspective, a task such as creating a new Domino

database runs under the QNOTES user profile. On a correctly configured Domino for AS/400 server, the QNOTES user profile either owns the Domino database directory or has sufficient authority to it. Therefore, a Domino administrator (running as QNOTES) has the necessary authority to create a new object in the Domino database directory.

Defining access to the database

By default, the system sets the authority for a new database correctly (from an AS/400 perspective). The Domino administrator does not need to worry about the AS/400 authority for a Domino database. The Domino administrator needs to define only Domino access control (through Domino functions).

Creating Domino-only users

Some users access only your Domino server. They do not need other access to your AS/400. These users do not need an AS/400 user profile. Your Domino administrator can register these users through Domino without accessing any AS/400 functions.

Mixed administrative tasks:

These tasks require interaction with the AS/400 server environment. Domino administrators who perform these tasks need an AS/400 user profile. Following are descriptions of these tasks and of the AS/400 authority these administrators need:

Starting and stopping the Domino server

From an AS/400 perspective, the administrator starts or stops both the server and the subsystem where the server job runs. The administrator can use either Operations Navigator or AS/400 commands. Both interfaces require *JOBCTL special authority to start and stop Domino servers.

Note: To give a user *JOBCTL special authority, change the special authority field in the user's profile. You can use either Operations Navigator or the Change User Profile (CHGUSRPRF) command to change a user's profile.

Working with the Domino console

From either Operations Navigator or an AS/400 command (WRKDOMCSL), an administrator can access the Domino console. The administrator can issue Domino server commands from this Domino console.

To work with the Domino console, an administrator needs *USE authority to the QNNINCSS program in the QNOTES library. To grant this authority, type the following command from an AS/400 command line:

```
GRTOBJAUT OBJ(QNOTES/QNNINCSS) OBJTYPE(*PGM)
   USER(admin-profile-name) AUT(*USE) REPLACE(*YES)
```

Note: By default, any AS/400 user can display the Domino console. Administrators need authority to the QNNINCSS program to be able to enter Domino server commands from the Domino console.

Setting up users for both Domino and AS/400

Some users need to access both the Domino server and other AS/400 functions. These users need an AS/400 user profile. To create an AS/400 user profile, your Domino administrator's AS/400 user profile must have *SECADM special authority.

Access control for Domino databases

IBM and Lotus designed the security for Domino for AS/400 databases with two objectives:

- To preserve the portability of Domino applications, the security for Domino databases on AS/400 needs to look just like other server platforms. A security model that works on a variety of servers is a strength of Domino.
- To preserve the security and integrity of other applications that might share the same AS/400, Domino for AS/400 must follow the security rules that apply to every other AS/400 application. Integrated security that is uniformly enforced is a strength of AS/400.

Building Blocks for Access Control

To understand how Domino security and AS/400 work together to achieve these objectives, start with basic information about how Domino security works and about how AS/400 stores Domino databases.

- Domino provides the capability to define an access control list for every Domino database. Access control lists provide authorities that are similar to AS/400 authorities. For example, in Domino, *editor* authority lets a user change any document in a database. However, an *editor* cannot delete a database or give other users authority to the database.

  Similarly, in DB2/400, *CHANGE authority lets a user add, change, or delete records in a database file. However, *CHANGE authority does not allow a user to delete the file or authorize others to use the file.

  Note: You can find out more about Domino authorities in the Domino books.
- When you configure a Domino for AS/400 server, you specify the directory for server databases. For example, you might specify /NOTES/DATA. Domino for AS/400 databases (files with a .NSF extension) always reside in the AS/400 integrated file system.

  AS/400 creates the Domino database directory with public authority set to *EXCLUDE. Whenever a Domino user creates a new database, the public authority for the new database is *EXCLUDE. This prevents AS/400 users from accessing Domino databases outside of Domino. (Of course, a user with *ALLOBJ special authority can access or delete any database.)
- By default, a user profile that is called QNOTES owns the Domino database directory and all the objects in the directory. The QNOTES user profile has *ALL authority to the objects. Domino server jobs run using the QNOTES user profile.

Sequence of Steps for Access Checking

Now you can put the pieces together and see what happens when a Notes user tries to access a Domino database:

1. OS/400 checks to see whether the user has authority to the object in the integrated file system (such as /NOTES/DATA/mydb.nsf). To OS/400, the user appears to be QNOTES. Therefore, QNOTES must have sufficient authority to the Domino database files in the integrated file system. When Domino for AS/400 creates the directories and databases, the QNOTES profile owns them. Therefore, unless the administrator has done something unusual, QNOTES has authority, and OS/400 allows access.
2. Control passes to Domino for AS/400. Domino knows the real user who has established a connection with the server and provided authentication. The

Domino server checks that user's authority on the access control list for the database. If the user has the correct authority, Domino for AS/400 allows the user's request to proceed.

Authority when Domino applications access DB2/400 databases

An important feature of Domino for AS/400 is the integration between Domino and DB2/400 databases. Three methods are available for Domino applications to access (and potentially update) DB2/400 databases:

- LotusScript applications use LS:DO (LotusScript data object) as an interface to DB2/400 data. Through LS:DO, the Domino application sends a request to the DB2/400 database.
- Domino applications in any supported programming language can use *@DB* instructions to interact with a relational database, including DB2/400.
- The NotesPump product (which is an add-on Domino product that you can order separately) provides easy-to-use methods for synchronizing information in Domino databases with information in DB2/400 databases.

Note: On other server platforms, LS:DO, and @DB functions use an ODBC interface to relational databases. On AS/400, the operating system intercepts the Domino database request and processes it directly without using ODBC. Therefore, the program looks the same as it does on other Domino server platforms, but the underlying processing on AS/400 is more direct.

All three methods for accessing DB2/400 from Domino establish a *connection* from Domino to AS/400. The connection specifies both the user profile whose authority the system uses to access DB2/400 database files and a password for that user profile.

Authority when Domino applications use LS:DO or @DB to access DB2/400 databases

A Domino application can use either LS:DO (LotusScript data object) or @DB functions to provide access to DB2/400 databases. With both methods, the application establishes a connection with the DB2/400 database. The connection specifies an AS/400 user profile and password. Before allowing the connection, OS/400 checks for the following:

- A valid user profile and password combination.
- The user's authority to the DB2/400 database file.

Following are security considerations for protecting your DB2/400 databases when you provide access from Domino applications.

1. For real-time applications (applications connected to a client), decide which AS/400 user profile the Domino applications will use to access DB2/400 data. You might decide based either on the Domino application or on the DB2/400 database. Following are the options:
   - Use the user profile of the user who is running the Domino application. With this method, you need an AS/400 user profile for every Domino user who needs to run an application that accesses DB2/400 data. "Details: Connecting a Domino application to DB2/400 with a matching AS/400 user profile" on page 187 describes how your Domino application can provide the AS/400 user profile and password.

- Set up special AS/400 user profiles whose only function is to provide Domino access to AS/400 data. This eliminates the need for each Domino user to have an AS/400 user profile. "Details: Connecting a Domino application to DB2/400 with a special AS/400 user profile" discusses considerations for this method.
- Use a combination of these methods. Create special user profiles to provide the equivalent of public (or anonymous) access to Domino users. This might be appropriate for database files that every user can view. Rely on the Domino user's AS/400 user profile either for higher levels of access or for confidential files.

2. For scheduled applications (such as agents), you also need to provide an AS/400 user profile when you connect to DB2/400. Scheduled applications run on the server without a connected client. Therefore, the application cannot request a user ID and password from a Domino user. Review "Details: Connecting a Domino application to DB2/400 with a special AS/400 user profile" for alternatives.
3. Consider using adopted authority to provide tighter control over the actions a Domino program can perform on DB2/400 data. See "Example: Using adopted authority for Domino access to DB2/400 data" on page 188.
4. Consider using the capability that Domino provides for design hiding to prevent users from viewing security-sensitive information about an application.

Details: Connecting a Domino application to DB2/400 with a matching AS/400 user profile

When a Domino application accesses a DB2/400 database, the Domino application needs to establish a connection with DB2/400. The connection requires a valid AS/400 user profile and password.

When you want your Domino application to connect by using the Domino user's AS/400 profile, do one of the following:

1. Your application can prompt the Domino user for an AS/400 user profile name and password during the first connection within a session. Be sure that your application protects this information carefully. You should avoid storing the passwords for individual AS/400 user profiles on your server.
2. You can provide a form and database for your Domino users who need AS/400 database access. The form prompts the user for the AS/400 user profile name and password. The application encrypts the information and stores it in a secure database on the client. Therefore, only the user or an application that is running on that user's behalf can decrypt the password.

   Using this method, your users do not need to enter their AS/400 user profile and password every time they make a connection from Domino to DB2/400. They will, however, need to use the form to update their database record when they change their AS/400 password.

Details: Connecting a Domino application to DB2/400 with a special AS/400 user profile

When a Domino application accesses a DB2/400 database, the Domino application needs to establish a connection with DB2/400. The connection requires a valid AS/400 user profile and password.

You might want to create special user profiles for the purpose of providing connections between Domino applications and DB2/400 databases. Do the following for your special user profiles:

1. Decide how many special user profiles to create:
   - Create a single AS/400 user profile to provide anonymous (or public) access to non-confidential databases.
   - Create multiple special-purpose profiles to provide access to DB2/400 data. You might think of these user profiles as similar to group profiles. Their role is to simplify the management of authority. Keep in mind that with this method, AS/400 does not know anything about the real Domino user. The Domino application sets the user profile name. You are relying on the Domino administrator to control who can use the application.
2. Decide whether to use passwords for the connection:
   - Your connection can specify a user profile name and *NOPWD. The QNOTES user profile must have *USE authority to the user profile. With this method, any Domino application can use this AS/400 user profile to attempt to access data.
   - Your application can store the user profile name and a password. You can protect this information so that only trusted programmers can view and update it. However, you will need to update the application whenever the AS/400 password changes.

     With this method, only Domino users who have authority to the program that contains the user profile and password can attempt to access DB2/400 data with it. The QNOTES profile does not need *USE authority to the user profile.
3. Set up the user profile to protect it from unintended use:
   a. Set the initial program to *NONE.
   b. Set the initial menu to *SIGNOFF.

Example: Using adopted authority for Domino access to DB2/400 data

On your AS/400, you might be using adopted authority to manage how users update information. For example, the typical user might have *USE authority to the open order file (which allows viewing but not creating, changing, or deleting). However, you want to make sure that only certain users can create or change orders. And you want to make sure that a new order passes edit checks before it goes into the open order file. You accomplish this kind of control on AS/400 with adopted authority. A user profile with *CHANGE authority to the open order file owns the program that provides the create and change function. Certain users have *USE authority to run the program.

To use a similar technique when you want to manage the ability to update DB2/400 data from Domino applications, do the following:

1. If necessary, design and create AS/400 programs that perform the tasks that you want to perform (such as changing a specific record in a database). You can probably adapt programs that you already have.
2. Set up the programs to adopt the authority of a user profile that has appropriate authority to the database file. Do the following:
   a. To transfer ownership of the program to the appropriate user profile, use the Change Object Owner (CHGOBJOWN) command.
   b. To specify that the program should adopt authority, use the Change Program (CHGPGM) command. Specify *OWNER for the User Profile (USRPRF) parameter.

3. Define the programs as a stored procedures for the DB2/400 database files that you want to update.
4. Design and create your Domino programs to use the stored procedures to update the DB2/400 database files.
5. When your Domino programs connect to DB2/400, specify a user profile name that has *USE authority to the stored-procedure programs.

Authority when NotesPump activities access DB2/400 databases

NotesPump is a separately-orderable Domino application that provides the capability to synchronize Domino databases with DB2/400 databases (and other relational databases). Typically, when you use NotesPump, you have one or more administrators who are responsible for defining and managing the synchronization that occurs between the databases. The administrator creates activity documents in a NotesPump database. Each document describes a specific synchronization activity and its schedule. For example, you might want to synchronize your DB2/400 customer master file with your Domino customer service database twice per day.

A NotesPump activity must establish a *connection* with the DB2/400 database. The connection specifies an AS/400 user profile and password. Before allowing the connection, OS/400 checks for the following:

- A valid user profile and password combination.
- The user's authority to the DB2/400 database file.

Following are some security considerations for protecting your DB2/400 databases when you provide access from NotesPump activities:

1. Decide which AS/400 user profiles to use on the connection request. "Details: Connecting a Domino application to DB2/400 with a special AS/400 user profile" on page 187 discusses the options.
2. Ensure that you protect the NotesPump activity database so that only trusted administrators can view or change it. You can also protect individual documents within the database. When you have more than one NotesPump administrator, for example, not every administrator needs to know the user profile and password for every activity.
3. Decide whether you want to synchronize either data and authorizations or only data.

The NotesPump documentation provides more information about how to set up NotesPump activities and about the related security issues. It also provides details about how authority synchronization works.

Authority when AS/400 programs access Domino databases

The database integration between Domino and AS/400 works in both directions. Your Domino applications can retrieve (and potentially update) DB2/400 databases. Similarly, AS/400 applications can retrieve (and potentially update) information in Domino databases. Following are the basics steps to gain access to a Domino database from an AS/400 program:

1. To access a Domino database, an AS/400 program uses Domino application programming interfaces (APIs). These Domino APIs are available for C, C++, and JAVA programming languages.

2. Domino processes the database request as a server program (not a client-server program). Therefore, the Domino user for the database request is the user who is associated with the server.
3. A Domino server can have more than one NOTES.INI file. The NOTES.INI file specifies the user for server jobs for that INI file.
4. Your AS/400 program can use an API to point to the INI file that is appropriate for the Domino databases that the program wants to access. If your AS/400 program does not explicitly specify an INI file, Domino uses the default user for the server.
5. The Domino user must have the necessary authority to the Domino database.
6. To gain access to the Domino server and the NOTES.INI file, the AS/400 program that contains the APIs must run under the QNOTES user profile. Adopting the authority of QNOTES to gain access does not work because the integrated file system does not recognize adopted authority. (Domino databases reside in the integrated file system on AS/400.)

For the Domino server product to work correctly, the QNOTES user profile must have *ALL authority to all of the Domino objects. Therefore, you should avoid giving users authority to the QNOTES user profile, and you should adopt the authority of QNOTES only when necessary. Instead, use specific programs for specific functions and use profile swapping. "Example: Authority for accessing Domino databases from AS/400 programs" provides an example of this technique.

Example: Authority for accessing Domino databases from AS/400 programs

Following is an example for providing access to Domino data from an AS/400 program while protecting the QNOTES user profile:

Steps:

1. Create an AS/400 program that contains the API instructions to access specific Domino databases. For the example, the program is a C++ program called ACCESSDOM. Following are the security characteristics of the ACCESSDOM program:
   - Public authority is *EXCLUDE.
   - The QNOTES user profile owns the program.
   - The program does not adopt authority.
   - No users have private authority to the program.
2. Create a program that provides the AS/400 user interface. The program might display information from both AS/400 databases and a Domino database. For the example, the program is an RPG program called USERDB1. Following are the security characteristics of the USERDB1 program:
   - Public authority is *EXCLUDE.
   - The QNOTES user profile owns the program.
   - The program adopts the authority of the QNOTES user profile.
   - Authorized users have private authority to the program.
3. Provide access to the Domino database through the following steps:
   a. An authorized user runs the USERDB1 program.
   b. Program USERDB1 uses an AS/400 API to swap to the QNOTES user profile. (The user does not have direct authority to swap to the QNOTES

user profile. However, the USERDB1 program adopts the authority of the QNOTES profile and, therefore, has sufficient authority to swap to the QNOTES user profile.)

c. Program USERDB1 calls the ACCESSDOM program and passes parameters about the database request.

d. The ACCESSDOM program runs the Domino APIs to retrieve the Domino data and return it to the USERDB1 program.

e. The USERDB1 program switches back to the user profile of the requesting user. It displays the Domino data for the user.

Security features of the example:

- Public authority to the ACCESSDOM program is *EXCLUDE. No user (except a user with *ALLOBJ special authority) can run this program directly. Therefore, AS/400 users cannot gain access to Domino databases outside the control of the USERDB1 program.
- Public authority to the USERDB1 program is also *EXCLUDE. Only specific AS/400 users have the authority to run the program.
- The ACCESSDOM program can specify a NOTES.INI file. The NOTES.INI file can point to a Domino user who has the desired database authorities.
- This example does not require that typical AS/400 users have *USE authority to the QNOTES user profile. The programmer will need authority to the QNOTES user profile.

Security recommendations for Domino for AS/400

Following are recommendations to protect both your Domino server and your other AS/400 applications and data when you run Domino for AS/400 on your system:

- For Domino for AS/400 to work properly, ensure that the QNOTES user profile owns all of the objects in the Domino data directory. (By default, this will occur automatically.)
- Because the QNOTES profile must have *ALL authority to Domino databases, the settings for the QNOTES user profile are designed to protect your Domino data. For example, the QNOTES user profile does not have a password. Its initial menu is *SIGNOFF. You should not change the settings for the QNOTES user profile.
- Public authority to the QNOTES user profile is *EXCLUDE. This prevents users from submitting jobs that run under the QNOTES user profile. You should not change the public authority to the QNOTES user profile. Grant private authority to the QNOTES user profile with extreme caution.

  Note: To ensure that users cannot submit jobs under the QNOTES user profile, the security level (QSECURITY system value) for your system must be 40 or higher. Otherwise, a job description that specifies the QNOTES user profile represents a potential security exposure.
- By default, the QNOTES user profile owns the Domino database directory and the objects in it. To ensure that Domino applications run properly, you should ensure that the QNOTES user profile has ownership to these objects.
- By default, public authority to the Domino database directory and the objects in it is *EXCLUDE. To ensure that Domino security works correctly, you should ensure that the public authority to the directory or the objects is *EXCLUDE.

Note: The *Domino database directory* is the default directory that you specify when you configure the Domino server. The default value is /NOTES/DATA

Chapter 19. Security Considerations for AS/400 NetServer

AS/400 NetServer is an IBM Operating System/400 Version 4 (OS/400) function that enables Windows PC clients to access AS/400 shared directory paths and shared output queues. PC clients on a network simply utilize the file and print-sharing functions that are included in their operating systems. Following is a list of security considerations of AS/400 NetServer:

Security considerations for user profiles that are disabled by AS/400 NetServer

AS/400 NetServer uses AS/400 user IDs and passwords to allow network administrators to control how users can access data. In addition, an AS/400 system value named QMAXSIGN specifies how many unauthorized sign-on attempts disable the user profile.

A user profile becomes disabled when the user tries to access AS/400 NetServer a specified number of times with an incorrect password. A user profile cannot become completely disabled when connecting to an AS/400 with AS/400 NetServer. If a user exceeds the maximum number of sign-on attempts the user profile becomes disabled for only AS/400 NetServer use. Other types of access, such as a system sign-on, are not prevented. If a user profile becomes disabled, you can enable it by changing the user profile. For example:

```
CHGUSRPRF USRPRF(AMANDA) ASTLVL(*SAME)
```

Stopping and then restarting AS/400 NetServer can also enable the user profile.

Note: The QSYSOPR message queue displays an error message that indicates whether an AS/400 user profile was disabled for use with AS/400 NetServer.

AS/400 NetServer uses the "last-changed" date on AS/400 user profiles to determine if they have changed since becoming disabled. If the "last-changed" date is newer than the date of becoming disabled, then the user profile becomes enabled again for use with AS/400 NetServer.

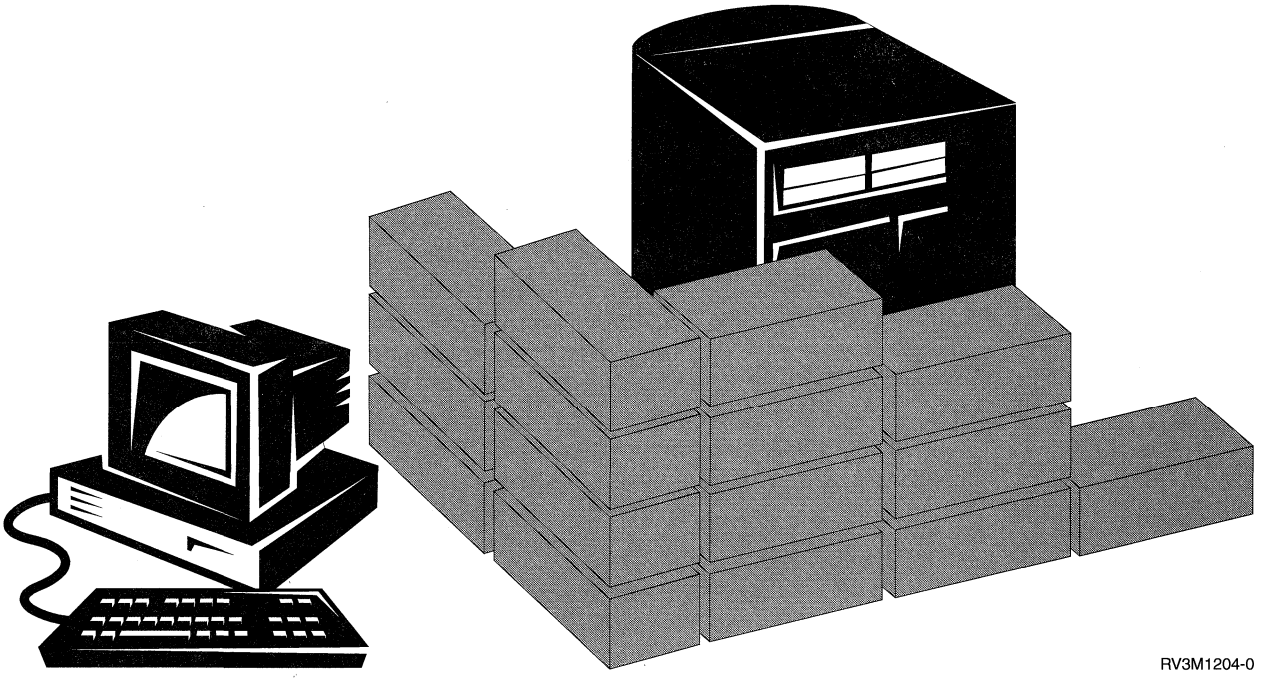
Security considerations for AS/400 NetServer guest user profiles

AS/400 NetServer supports guest user profiles (this is also known as an anonymous user profile). AS/400 can automatically map an unknown user to the guest user profile if you specify a guest user profile. Your network administrator can specify and change the guest user profile that AS/400 NetServer uses, if necessary, on the AS/400 NetServer **Advanced - Next start** page within Operations Navigator. In general, the guest user profile should have very few authorities because the guest user is considered a non-trusted user.

Security considerations for AS/400 NetServer user profile authority requirements

You must have *IOSYSCFG special authority to change AS/400 NetServer configuration properties. In addition, you must have *SECADM and *USE special authorities to set the guest user profile for AS/400 NetServer. If you specify a guest user profile, it should not have any special authorities.

Part 5. Tips and Tools for Internet Security on AS/400



RV3M1204-0

Note: The content of "Part 5. Tips and Tools for Internet Security on AS/400" is also avaiable in the AS/400 Information Center.

Chapter 20. Internet security tips and tools

Internet security tips and tools

Moving your business onto the Internet is a big step. Previously, your biggest security concern was probably protecting your local area network (LAN). Now you are connecting your systems to a global network, and you need to protect your systems from everyone on the Internet. Luckily, your AS/400's that has built in integrated software solutions and security architecture that lets you build a strong defense against potential Internet pitfalls.

To learn more about Internet security risks and AS/400 security solutions that you can use to protect your systems and resources, review these topics:

- "IBM SecureWay: AS/400 and the Internet"
- "Preparing for Internet security" on page 198
- "Basic corporate Internet usage" on page 209
- "Adding secure telnet access using SSL" on page 217
- "Adding Secure Client Access Express" on page 219
- "Adding Virtual Private Networks (VPN)" on page 219
- "AS/400 Internet security solutions" on page 221

IBM SecureWay: AS/400 and the Internet

AS/400 owners are exploring their options for linking their systems to the Internet. The first question they ask is usually, "How do I begin to use the Internet for business purposes?" The second question is, "What should I know about security and the Internet?" This topic attempts to answer the second question for AS/400 on the Internet: "What about security and the Internet ?"

To find more detailed information on how to begin using the Internet for business purposes, review these topics and online and books:

- "Connecting to the Internet" in the AS/400 Information Center.
- *Cool Title About the AS/400 and Internet*, SG24-4815.

Security issues as related to the Internet are significant. Which issues you need to address are based on how you plan to use the Internet. Are you using the Internet for e-mail and nothing else? Are you using the Internet to launch your company's web presence and provide opportunities for on-line shopping? Or, do you want to use Virtual private networks(VPNs) to provide secure communications for your extranet?

The good news is that IBM AS/400 is actively creating security solutions for protecting your system on the Internet. Additionally, AS/400 has very strong system security characteristics, such as:

- AS/400 integrated security is extremely difficult to circumvent compared to security offerings (on other systems) that are add-on software packages.
- AS/400 object-based architecture makes it technically difficult to create and propagate a virus. On AS/400, a file cannot pretend to be a program, nor can a

program modify another program. AS/400 system integrity features require you to use system-provided interfaces to access objects. You cannot access an object directly by its address in the system. You cannot take an offset and turn it into or "manufacture" a pointer. (Pointer manipulation is a popular technique for hackers on other system architectures.)

- AS/400 flexibility lets you set up your system security to meet your requirements.
- AS/400 provides several security offerings to enhance your system security when you connect to the Internet. Depending on how you use the Internet, you can use:
  - Virtual private networking (VPN): A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network, such as the Internet. You can use a VPN to create a secure private connection, essentially by creating a private "tunnel" over a public network. For more information about VPN, see the topic "Virtual private networking" in the AS/400 Information Center.
  - IBM Firewall for AS/400: Provides a fully functional firewall to serve as a logical barrier between your internal network and an external network, such as the Internet. The firewall runs on a separate processor (the Integrated Netfinity Server). For more information about Firewall for AS/400, see the topic "Firewall: Getting started" in the AS/400 Information Center.
  - IP packet security: An integrated feature of OS/400, IP packet security provides basic firewall separation and protection for your system. IP packet security allows you to create packet filter and network address translation (NAT) rules to control TCP/IP traffic in your network.For more information about IP packet security, see the topic "IP packet security" in the AS/400 Information Center.
  - Digital Certificate Manager (DCM): DCM allows you to create, manage, and apply digital certificates to your applications so that you can use SSL for secure communications and stronger authentication.For more information about DCM, see the topic "Digital certificate management" in the AS/400 Information Center.

.

Preparing for Internet security

The answer to the question, "What should I know about security and the Internet?", it depends on how you want to use the Internet. Your first venture into the Internet might be to provide your internal network users with access to the Web and Internet e-mail. You may also want the ability to transfer sensitive information from one site to another. Eventually, you may plan to use the Internet for e-commerce. Before you get involved with the Internet, you should think through what you want to doand how you want to do it. Then you can think about the security risks that are associated with your choices.

Making decisions about both Internet usage and Internet security can be complex. However, there are several options that are typical of how businesses use the Internet and secure that usage. These options may not reflect your own Internet situation exactly. Reviewing them, however, can help you understand typical Internet security risks and solutions. Also you will see how they may apply to your own Internet usage plans:

- "Basic corporate Internet usage" on page 209
- "Adding secure telnet access using SSL" on page 217

- "Adding Secure Client Access Express" on page 219
- "Adding Virtual Private Networks (VPN)" on page 219

The first scenario describes the Internet usage options most companies choose when they connect their networks to the Internet. Each successive scenario describes more advanced, secure Internet usage options you can use to extend the Internet usage that the first scenario describes.

AS/400 provides a strong set of security tools and functions, but you must take the time to learn about the tools and to use them. Once you understand the security issues and their possible solutions, you can develop a security plan for your system. A number of factors affect choices that you make in your security policy and implementation strategy. You must often make trade-offs between enforcing a strict security policy and other important needs. Examples of these needs include ensuring that users enjoy good function, either system and network performance, or addressing corporate liability issues.

To make educated decisions about what trade-offs you are willing to make, you must understand network security, both the exposures,and solutions available. Now is the time to update or develop your security policy. When you extend your organization onto the Internet, a security policy provides a critical cornerstone for making your Internet plans. If you have a security policy today, you probably need to revise it to address your plans for an Internet connection.

To learn about security basics, how they apply to the Internet, and related security terms, review these topics:

- "Internet security defined" on page 200
- "Planning your Internet security needs"
- "AS/400 system security for Internet readiness" on page 202
- "Internet security terminology" on page 203

Planning your Internet security needs

After you develop your Internet usage plans, you must carefully plan for your Internet security needs. To learn more about developing a security plan for adequately protecting your internet network resources from possible Internet usage risks, review these topics:

- "Internet security defined" on page 200.
- "About your security policy" on page 200.
- "About your security objectives" on page 201.

Additionally, you may be able to adapt the IBM Firewall for AS/400 planning work sheets to help you plan your security needs. You can print out these work sheets from the "Firewall: Getting started" topic in the AS/400 Information Center.These work sheets help you gather important detailed information about your Internet usage plans and internal network resources. Whether you decide to use a firewall or not, you need to gather much of this same data. For instance, you can use these work sheets to describe the following:

- Your current network configuration.
- Your connection to your Internet Service Provider (ISP).
- What services you want to use from the Internet.

- What services you want to provide to Internet users.

You want this type of information to help you determine where your security exposures are and what security measures you need to minimize these security risks.

For example, you decide that you want to allow your internal users to use Telnet to connect to hosts at a special research facility. They need this service to help them develop new products for your company. However, you have some concerns about confidential data flowing unprotected across the Internet. If competitors capture and exploit this data, your company could face a financial risk. Having identified your usage needs (Telnet), and their associated risks, you know that you need to carry out security measures to ensure data confidentiality for this usage.

Internet security defined

What do we mean by "security"? Internet system security has these basic components:

- A **security policy**: Defines what you want to protect and what you expect of your system users. It provides a basis for security planning when you design new applications or expand your current network. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords.

  You need to create and enact a security policy for your organization that minimizes the risks to your internal network. The inherent security features of AS/400, when properly configured, provide you with the ability to minimize many risks. When you connect your AS/400 to the Internet; however, you will need to provide additional security measures to ensure the safety of your internal network.
- **User authentication**: Ensures that only authorized individuals (or jobs) can enter your system. When you link your system to a public network like the Internet, user authentication takes on new dimensions. An important difference between the Internet and your intranet is your ability to trust the identity of a user who signs on. Consequently, you should consider seriously the idea of using stronger authentication methods than traditional user name and password logon procedures provide. Digital certificates provide a stronger alternative while providing other security benefits as well.
- **Resource protection**: Ensures that only authorized users can access objects on the system. The ability to secure all types of system resources is an AS/400 strength. You should carefully define the different categories of users that can access your system. Also, you should define what access you want to give these groups of users as part of creating your security policy.

Some Internet services are more vulnerable to certain types of attacks than others. Therefore, it is critical that you understand the risks that are imposed by each service you intend to use or provide. In addition, understanding possible security risks helps you to determine a clear set of security objectives. Once you understand the risks, you must ensure that your security policy provides a means of minimizing those risks.

About your security policy

Each Internet service that you use or provide poses risks to your AS/400 and the network to which it is connected. A security policy is a set of rules that apply to activities for the computer and communications resources that belong to an

organization. These rules cover areas such as physical security, personnel security, administrative security, and network security.

To develop your security policy, you must clearly define your security objectives. Once you create a security policy, you must take steps to put into effect the rules it contains. These steps include training employees and adding necessary software and hardware to enforce the rules. Also, when you make changes in your computing environment, you should update your security policy to ensure that you address any new risks that your changes impose.

About your security objectives

When you create and carry out a security policy, you must have clear objectives. Security objectives fall into one or more of the following categories:

- **Authentication**: Assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be.

  Authentication proves that a resource or user is what or who it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system. Traditionally, systems have used passwords and user names for authentication; digital certificates can provide a more secure method of authentication. Authenticated users may have different types of permissions based on their authorization levels.
- **Authorization**: Assurance that the person or computer at the other end of the session has permission to carry out the request.

  Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Usually, authorization is performed in the context of authentication. Authenticated users may have different types of permissions based on their authorization levels.

  When a user creates a digital certificate in Digital Certificate Manager, you can choose to associate the certificate with that user's AS/400 user profile. Consequently, the user's authorizations on a system are determined when the user presents the certificate to the server for authentication.
- **Integrity**: Assurance that arriving information is the same as that sent. Understanding integrity requires you to understand the concepts of data integrity and system integrity.
  - **Data integrity**: means that data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data stored within your network, you may need additional security to ensure data integrity when data enters your system from untrusted sources. When data that enters your system comes from a public network, you may need security methods so that you can:
    - Protect the data from being "sniffed" and interpreted, usually by encrypting it.
    - Ensure that the transmission has not been altered (data integrity).
    - Prove that the transmission occurred (non-repudiation). In the future, you might need the electronic equivalent of registered or certified mail.
  - **System integrity**: System integrity is your system's ability to provide consistent, expected results with expected performance. For AS/400, system integrity is the most commonly overlooked component of security because system integrity is a fundamental part of AS/400 architecture. AS/400 architecture, for example, makes it extremely difficult for a mischief-maker to

imitate or modify an operating system program when you use security level 40 or 50.When you think about connecting to the Internet, you need to think about your system's availability and how a hacker might try to assault it. A hacker can launch a **denial of service** attack without ever signing on to your system.

A hacker can, for example, compromise your system's ability to service user requests by flooding your system. Your disk storage can be flooded, for example, with unwanted mail or with printed output. Your processor can be overwhelmed, for example, by error recovery or simply by processing unauthorized requests.

Your legitimate users either cannot log on or they receive poor performance because your system is spending resources dealing with unauthorized requests.

- **Non-repudiation**: Assurance (accountability) that any transaction that takes place can subsequently be proven to have taken place. Both the sender and the receiver agree that the exchange took place.

  Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to "sign" transactions, messages, and documents supports non-repudiation.
- **Confidentiality**: Assurance that sensitive information remains private and is not visible to an eavesdropper.

  Confidentiality means keeping information protected from unauthorized viewers. Confidentiality is critical to total data security. Encrypting data by using digital certificates and the secure socket layer (SSL) helps ensure confidentiality when transmitting data across untrusted networks. Your security policy should address how you will provide confidentiality for information within your network as well as providing it when information leaves your network.
- **Security auditing:** Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access. Successful access records tell you who is doing what on your systems. Unsuccessful (denied) access records tell you either that someone is attempting to break your security or that someone is having difficulty accessing your system.

Understanding your security objectives helps you create a security policy that covers all your system and network security needs. Next, you should understand what is involved in setting your AS/400 system security for Internet readiness.

AS/400 system security for Internet readiness

The topics that follow assume that you are starting with an AS/400 system that is basically secure. At a minimum, your system should meet the following security guidelines:

- Set the security level (QSECURITY system value) to be at least 40. Level 40 or 50 are strongly recommended because they provide enhanced integrity protection.

  Note: If you are currently running at a lower security level than 40, you may need updates either to your operating procedures or to your applications. You should review chapter 2 of the book *Security - Reference.*, before changing to a higher security level.

- Set your security-relevant system values to be at least as restrictive as the recommended settings. You can use the Print System Security Attributes (PRTSYSSECA) command to compare your settings to the recommended settings.
- Ensure that no user profiles, including IBM-supplied user profiles, have default passwords. Use the Analyze Default Passwords (ANZDFTPWD) command to check this.
- Use object authority to protect your important system resources. Take a restrictive approach on your system. That is, by default everyone is restricted from system resources such as libraries and directories. Allow access to only a few users. Restricting access via menus is not sufficient in this environment.
- You must set up object authority on your system.

Internet security terminology

To establish a basis for the discussing Internet security, let's start by defining some Internet terms. If you are already Internet-literate, you can skip this section.

Authentication
Data authentication verifies that the claimed sender originated each datagram.

Cracker
A hacker with malicious intent.

Cryptography
The science of keeping data secure. Cryptography allows you to store information or to communicate with other parties while preventing non-involved parties from understanding the stored information or understanding the communication. Encryption transforms understandable text into an unintelligible piece of data (ciphertext). Decrypting restores the understandable text from the unintelligible data. Both processes involve a mathematical formula or algorithm and a secret sequence of data (the key).

There are two types of cryptography:

- In shared/secret key **(symmetric)** cryptography, one key is a shared secret between two communicating parties. Encryption and decryption both use the same key.
- In public key **(asymmetric)** cryptography, encryption, and decryption each use different keys. A party has two keys: A public key and a private key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. A message that is encrypted with someone's public key can be decrypted only with the associated private key. Alternately, a server or user can use a private key to "sign" a document and use a public key to decrypt a digital signature. This verifies the document's source.

Digital certificate
A digital certificate is a digital document that validates the identity of the certificate's owner, much as a passport does. A trusted party, called a Certificate Authority (CA) issues digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. Use them to:

- Identification - knowing whom is the user
- Authentication - ensuring that the user is who he says that he is

- Integrity - determining whether the contents of a document have been altered by verifying the sender's digital "signature".
- Non-repudiation - guaranteeing that a user cannot claim to not have performed some action. For example, the user cannot dispute that he authorized an electronic purchase with a credit card.

Digital signature
A digital signature on an electronic document is equivalent to a personal signature on a written document. A digital signature provides proof of the document's origin. The certificate owner "signs" a document by using the private key that is associated with the certificate. The recipient of the document uses the corresponding public key to decrypt the signature, which verifies the sender as the source.

Digital certificate manager (DCM)
Digital Certificate Manager registers certificates that you create on your AS/400 when it is acting as a Certificate Authority. You can also use the DCM to register certificates that other Certificate Authorities issue. DCM allows you to choose to associate a user's certificate with their AS/400 user profile. You can use DCM to associate digital certificates with various AS/400 applications so that these applications can use the Secure Sockets Layer for secure communications.

Distinguished name
A distinguished name is the name of the person or server to whom a Certificate Authority (CA) issues a digital certificate. The certificate provides this name to indicate certificate ownership. Depending on the policy of the CA that issues a certificate, the distinguished name can include other information.

Domain name server
An Internet host that converts Internet names to IP addresses, often by interacting with other domain name servers on the Internet. For example, many domain name servers might recognize

```
vnet.ibm.com
```

But perhaps only a few know the complete IP address for:

```
system1.vnet.ibm.com
```

When you attach to the Internet, your Internet client uses a domain name server to determine the IP address for the host system with which you wish to communicate .

Encryption
Encryption transforms data into a form that is unreadable by anyone who does not have the correct decryption method. Unauthorized parties can still intercept the information. However, without the correct decryption method, the information is incomprehensible.

Extranet
A private business network of several cooperating organizations located outside the corporate firewall. An Extranet service uses the existing Internet infrastructure, including standard servers, e-mail clients, and Web browsers. This makes an extranet more economical than the creation and maintenance of a proprietary network. It enables trading partners, suppliers, and customers with common interests to use the extended Internet to form both tight business relations and a strong communication bond.

Firewall
A logical barrier between your internal network and an external network, such as the Internet. A firewall consists of one or more hardware and software systems. It controls the access and flow of information between secure or trusted systems and unsecure or untrusted systems.

Hacker
Any unauthorized person who tries to break into your system. Hackers typically fall into three groups, separated by their motivation:

- Some hackers seek financial gain.
- Some hackers seek confidential information (industrial espionage).
- Some hackers do it for the challenge.

Hypertext
A way of presenting information on-line with connections—(called hypertext links) between one piece of information (called a hypertext node) and another.

Hypertext markup language (HTML)
The language that is used to define hypertext documents. You use HTML to indicate how your document should look (such as highlighting and type style) and how it should be linked to other documents or objects.

Hypertext transport protocol (HTTP)
The standard method for accessing hypertext documents.

Internet
The world-wide "network of networks" that are connected to each other. And a suite of cooperating applications that allow computers connected to this 'network of networks' to communicate with each other. The Internet provides browsable information, file transfer, remote log-on, electronic mail, news, and other services. The Internet is often called "the Net".

Internet client
A program (or user) that uses the Internet to make requests of and to receive results from an Internet server program. Different client programs are available to request different types of Internet services. A Web browser is one type of client program. File transfer protocol (FTP) is another.

Internet host
A computer that is connected to the Internet or an intranet. An Internet host might run more than one Internet server program. For example, the Internet host might run an FTP server to respond to requests from FTP client applications. The same host might run an HTTP server to respond to requests from clients using Web browsers. Server programs typically run in the background (in batch) on the host system.

Internet key exchange (IKE)
The IKE protocol, when used with IPSec, supports the automatic negotiaion of security associations, as well as the automatic generation and refresh of cryptographic keys. Generally, IKE is used as part of virtual private networking.

Internet name
An alias for an IP address. An IP address is in long numeric form and is difficult to remember, such as 10.5.100.75. You can assign this IP address to an Internet name, such as

```
system1.vnet.ibm.com
```

An Internet name is also called a fully qualified domain name. When you see an advertisement that says, "Visit our home page,"the home page address includes the Internet name, not the IP address, because the Internet name is easier to remember.

A fully qualified domain name has several parts. For example.,

`system1.vnet.ibm.com`

has the following parts:

com: All commercial networks. This part of the domain name is assigned by the *Internet* authority (an external organization). Different characters are assigned for different kinds of networks (such as `com` for commercial and `edu` for educational institutions).

ibm: The identifier for the organization. This part of the domain name is also assigned by the Internet authority, and it is unique. Only one organization in the world can have the identifier

`ibm.com`

vnet: A grouping of systems within

`ibm.com`

This identifier is assigned internally. The administrator of `ibm.com` can create one or more groupings.

system1:
The name of an Internet host within the `vnet.ibm.com` group.

Internet server
A program (or set of programs) that accepts requests from corresponding client programs over the Internet and responds to those clients over the Internet. You can think of an Internet server as a site that an Internet client can access or visit. Different server programs support different services, such as the following:

- Browsing (a "home page" and links to other documents and objects).
- File transfer. The client can request, for example, to transfer files from the server to the client. The files might be software updates, product listings, or documents.
- Electronic commerce, such as the ability to request information or order products.

Internet service provider (ISP)
An organization that provides your connection to the Internet in much the same way that your local telephone company provides your connection to worldwide telephony networks.

Intranet
An organization's internal network that uses Internet tools, such as a Web browser or FTP (file transfer protocol).

IP address
An Internet Protocol (IP) address is the way that you are known on a TCP/IP network (and the Internet is a very large TCP/IP network). An Internet server usually has an assigned, unique IP address. An Internet client might use a temporary but unique IP address that is allocated by the ISP.

IP datagram
A unit of information that is sent across a TCP/IP network. An IP datagram (also called a packet) contains both data and header information, such as the IP addresses of the origin and of the destination.

IP filters
IP filtering provides the basic protection mechanism for the firewall. It allows you to determine what traffic passes across it based on IP session details. This protects the secure network from outsiders that use unsophisticated techniques (such as scanning for secure servers) or even the most sophisticated techniques (such as IP address spoofing). You should think of the filtering feature as the base on which the other tools are constructed. It provides the infrastructure in which they operate and denies access to all but the determined cracker.

IPSec A set of protocols to support secure exchange of packets at the IP layer. IPsec is a set of standards that AS/400 and many other systems use to carry out Virtual Private Networks (VPNs).

IP spoofing
An attempt to access your system by pretending to be a system (IP address) that you normally trust. The would-be intruder sets up a system with an IP address that you trust. Router manufacturers have worked to build protections into their systems to detect and reject attempts to spoof.

Network address translation (NAT)
It provides a more transparent alternative to the proxy and SOCKS servers. It also simplifies network configuration by enabling networks with incompatible addressing structures to be connected. NAT provides two major functions: NAT can protect a public Web server that you want to operate from within your internal network. NAT provides this protection by allowing you to hide your server's "true" address behind an address that you make available to the public. And it provides a mechanism for internal users to access the Internet while hiding the private internal IP addresses.

- NAT provides protection when you allow internal users to access Internet services because you can hide their private addresses.

Non-repudiation
Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to "sign" transactions, messages, and documents supports non-repudiation.

Packet
A datagram that includes information about the line protocol, such as Ethernet**, token-ring, or frame-relay.

Proxy Proxy server is a TCP/IP application that re-sends requests and responses between clients on your secure internal network and servers on the untrusted network. The proxy server breaks the TCP/IP connection to hide your internal network information (such as internal Internet Protocol (IP) addresses). Hosts outside your network perceive the proxy server as the source of the communication.

Public key infrastructure (PKI)
A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Secure Sockets Layer (SSL)
Originally created by Netscape, the Secure Sockets Layer (SSL) is the industry standard for session encryption between clients and servers. SSL uses symmetric key encryption to encrypt the session between a server and client (user). The client and server negotiate this session key during an exchange of digital certificates . The key expires automatically after 24 hours, and a different key is created for each client and server connection. Consequently, even if unauthorized users intercept and decrypt a session key (which is unlikely), they cannot use it to eavesdrop on later sessions.

Sniffing
The practice of monitoring or eavesdropping on electronic transmissions. Information that is sent across the Internet might pass through many routers before it reaches its destination. Router manufacturers, ISPs, and operating system developers have worked very hard to ensure that sniffing cannot occur on the Internet backbone. Incidents of successful sniffing are becoming increasingly rare. Most occur on private LANs that are connected to the Internet, rather than on the Internet backbone itself. However, you need to be aware of the possibility of sniffing because most TCP/IP transmissions are not encrypted.

Spoofing
The attacker masquerades as a trusted system to try to persuade you to send secret information to him.

SOCKS
SOCKS is a client/server architecture that transports TCP/IP traffic through a secure gateway. A SOCKS server performs many of the same services that a proxy server does.

TCP/IP
The primary communications protocol that is used on the Internet. TCP/IP stands for Transmission Control Protocol/Internet Protocol. You might also use TCP/IP on your internal network.

Trojan horse
A trojan horse is a computer program that appears to perform a useful and innocent function. However, it contains hidden functions that use legitimate authorizations assigned to the user when they start the program. For example, it may copy your internal authorization information from your computer and send it back to the originator of the Trojan horse.

Virtual private network (VPN)
A virtual private network (VPN) is an extension of an enterprise's private intranet. You can use it across a public network such as the Internet, creating a secure private connection, essentially through a private "tunnel." VPNs securely convey information across the Internet connecting other users to your system. These include:

- Remote users
- Branch offices
- Business partners/suppliers

Web browser
The HTTP client application. A Web browser interprets HTML to display hypertext documents for the user. The user can access a hyperlinked object by clicking on (selecting) an area of the current document. That area is often called a **hot spot**. Internet Connection Web Explorer, Mosaic**, and Netscape** are examples of Web browsers.

World Wide Web (WWW)
A mesh of interconnected servers and clients that use the same standard format for creating documents (HTML) and accessing documents (HTTP). The mesh of links, both from server to server and from document to document, is metaphorically called **the Web**.

Basic corporate Internet usage

This scenario involves a medium size business that distributes products and services nationwide. The company is implementing an overall plan to increase its company presence on the Internet.

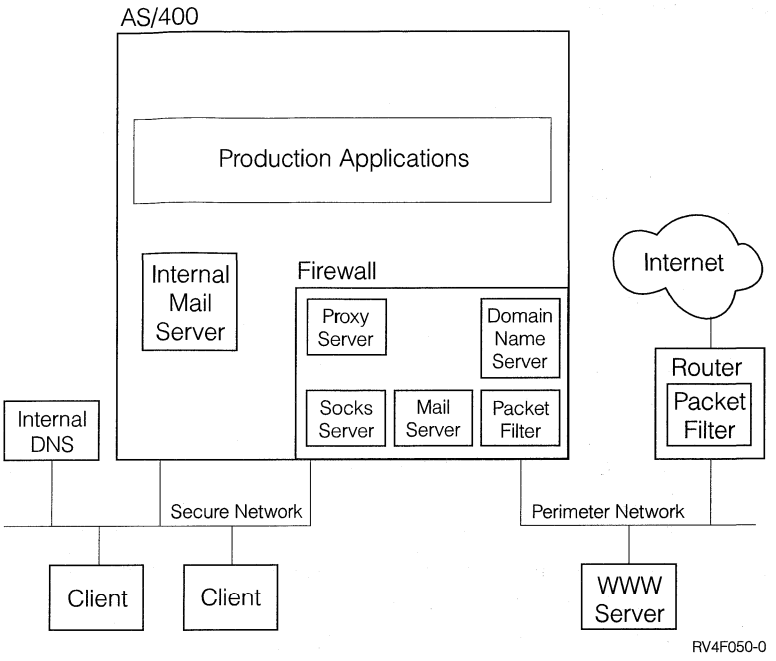
This scenario describes a fairly typical company Internet usage and security plan. Your company plans may be somewhat different from those this scenario describes. However, you may be able to use this information to help you determine how to develop your own Internet usage and security plans. It scenario involves a medium size business that distributes products and services nationwide. The company is implementing an overall plan to increase its company presence on the Internet.

The goals of this increased presence are:

- Promote general corporate image and presence as part of an overall marketing campaign.
- Provide an on-line product catalog for customers and sales staff.
- Improve customer service.
- Improve employee e-mail and World Wide Web access.

In addition, the company wants to provide a means for customers to order products and services directly over the Internet in the near future.

This company has chosen to implement the IBM Firewall for AS/400 (make this a link) as one part of its security plan to shield their internal network from risks associated with using the Internet. Below is an example of how this type of company Internet connection configuration may look.



As shown in the diagram, this company has two primary AS/400 systems, one of which they use for development and one for production applications. Both of these systems handle mission critical data and applications. Consequently, they have chosen to add a new AS/400 to their internal network to handle their Internet and Internet security applications.

The new system ensures that they have complete physical separation between their primary AS/400s and the Internet. This separation decreases the Internet risks to which these systems are vulnerable. By designating the new AS/400 as an Internet server only, the company also decreases the complexity of managing their network security.

The new system will run the IBM Firewall for AS/400 as their first line of defense for their network. They chose this firewall product because it is a fully functional firewall that runs on a separate processor in the AS/400. Consequently, the firewall also will protect the new AS/400 and its public applications.

In the following topics, you can find information for understanding the security risks associated with this Internet usage scenario. These topics also provide information about what security measures you can take to minimize these risks:

- Basic security risks and solutions
- JAVA security considerations
- E-mail security considerations
- FTP security considerations
- Web serving security considerations
- "Basic security risks and solutions" on page 211
- "Java security considerations" on page 211
- "E-mail -- security considerations" on page 213
- "File Transfer Protocol (FTP)-- security considerations" on page 215
- "Web serving-- security considerations" on page 215

Basic security risks and solutions

There are many risks that are associated with using Internet access to conduct business acitivites. Whenever you create a security policy, you must balance providing services against controlling access to functions and data. With networked computers, security is more difficult because the communication channel itself is open to attack.

The Internet is home to a variety of individuals who pose threats to the security of Internet communications. The following list describes some of the typical security risks you may encounter:

- **Passive attacks**. In a passive attack, the perpetrator simply monitors your network traffic to try to learn secrets. Such attacks can be either network-based (tracing the communications link) or system-based (replacing a system component with a Trojan Horse program that captures data insidiously). Passive attacks are the most difficult to detect. Therefore, you should assume that someone is eavesdropping on everything you send across the Internet.
- **Active attacks.** In an active attack, the perpetrator is trying to break through your defenses. There are several types of active attacks:
  - In **system access attempts**, the attacker attempts to exploit security loopholes to gain access and control over a system of a client or of a server
  - In **spoofing** attacks, the attacker attempts to break through masquerading as a trusted system, or a user persuades you to send secret information to them.
  - In **denial of service attacks** an attacker tries to interfere or shut down your operations by re-directing traffic or bombarding your system with junk.
  - In **cryptographic attacks**, an attacker will attempt to guess,or steal your passwords, or uses specialized tools to try to decrypt encrypted data.

One solution may the IBM firewall for AS/400 which is a blockade between a secure internal network and an untrusted network like the Internet. Most companies use the firewall to connect an internal network safely to the Internet. Also, you can use the IBM firewall for AS/400 to secure one internal network from another on an intranet.

A firewall is a good choice as the first major line of defense for your network because it:

- Lets users in your internal network use authorized resources that are located on the outside network.
- It prevents unauthorized users on the outside network from using resources on your internal network.

When you use the IBM Firewall for AS/400 as your gateway to the Internet (or other network), you reduce the risk to your internal network considerably. Using a firewall also makes administering network security easier because firewall functions carry out most of your Internet security policy.

Java security considerations

Java is rapidly becoming widely accepted and used. You might be using the AS/400 Toolbox for Java on your system to develop new applications. Consequently, you must prepare to deal with the security issues that are associated with Java. Although a firewall is a good defense against Internet security risks, it does not provide protection for many Java security risks. Your security policy should include details for protecting your system against three areas of concern for Java: Applications, applets, and servlets.

Your users who have Internet access might be accessing Web pages that run Java servlets or applets. The following are some security considerations for Java.

If you are planning to use Java, you must understand that there are security risks associated with Java. If you elect to allow internal access to the Web as well as to provide a public Web site. Consequently, you must ensure that your security policy covers all three types of Java concerns.

Java applications.

As a language, Java has some characteristics that protect Java programmers from unintentional errors that can cause integrity problems. (Other languages that are commonly used for PC applications, such as C or C++ do not protect the programmers from unintentional errors as strongly as Java does.) For example, Java uses strong typing which protects the programmer from using objects in unintended ways. Java does not allow pointer manipulation, which protects the programmer from accidentally going outside the memory boundaries of the program. Therefore, from an application development perspective, you can view Java as you do other high-level languages. You should apply the same security rules for application design that you apply with other languages on your AS/400.

A Java applet has the potential to access your AS/400. (An ODBC program or an advanced program-to-program communications (APPC) program operating on a PC in your network can also.) In general, Java applets can establish a session only with the server from which the applet originated. Therefore, a Java applet can access your AS/400 from a connected PC only when the applet came from your AS/400 (such as from your Web server).

An applet can attempt to connect to any TCP/IP port on a server. It does not have to talk to a software server that is written in Java. But, for servers written with the AS/400 toolbox for Java, the applet must provide a user ID and password when it establishes connections back to the server. In this article the servers described are all AS/400 servers (A server written in Java does not have to use the AS/400 toolbox for Java). Typically, the AS/400 toolbox for Java class prompts the user for a user ID and password for the first connection.

The applet can perform functions on the AS/400 system only if the user profile has authorization to those functions. Therefore, a good resource security scheme is essential when you begin to use Java applets to provide new application function. When the system processes the requests from applets, it does not use menu access control or the limited capability value in the user's profile.

Beginning with V4R4, it is possible to change Java to use Secure Sockets Layer (SSL). This ensures encryption of the data , including user IDs and passwords between the client and server. You can use Digital Certificate Manager to configure registered Java programs for SSL.

Java applets.

Java applets are small Java programs that you can include in HTML pages. Because applets run on the client, what they do are a client concern. Good AS/400 server security management protects AS/400 resources, regardless of what the applet tries to do. On the other hand, who can access the applet is an AS/400 server concern. Use HTTP server directives and OS/400 resource security to control access to the applet.

The appletviewer allows you to test an applet on the server system; however, it is not subject to browser security restrictions. Therefore, you should use the appletviewer to test your own applets only, never to run applets from outside sources. Java applets often writes to the user's PC drive, which may allow the applet the opportunity to perform a destructive action. However, you can associate a digital signature with a Java applet to establish its authenticity. The signed applet can write to the PC's local drives, even though the default setting for the browser prevents it. The signed applet can also write to mapped drives on your AS/400 because they appear to the PC to be local drives.

Note: The behavior described above is generally true for Netscape Navigator and MS Internet Explorer. What actually happens depends a lot on how you configure and manage the browsers you use.

For your own Java applets that come from your AS/400, you might need to use signed applets. However, you should instruct your users in general not to accept signed applets from unknown sources.

Java Servlets.

Servlets are server side components that are written in Java, which dynamically extend the functionality of a web server without changing web server code. The IBM WebSphere Application Server that is shipped with IBM HTTP Server for AS/400 provides support for servlets on AS/400. Servlets are more complicated to secure than other types of Java programs. Applying resource security to a servlet does not sufficiently secure it. Once a web server loads a servlet, resource security does not prevent others from running it. You must use resource security on objects that the server uses. Do not allow servlets to run under the web server's profile. You should control who can run the servlet (mask keywords in the protection directive). You should use HTTP Server groups and Access Control Lists (ACLs).

To understand and learn more about the following article will provide you with information for preparing for security when using Java. Use the security tools, tips, and suggestions you can find throughout *Tips and Tools for Securing Your AS/400*

E-mail -- security considerations

Using e-mail across the Internet, or other untrusted network, imposes security risks against which using a firewall may not protect. You must understand these risks to ensure that your security policy describes how you will minimize these risks. Although a firewall provides some protection, it does not protect you from many types of e-mail security risks.

E-mail notes are just like other forms of communications. It is very important to use discretion before sending any confidential information out through e-mail. Because your mail travels through many servers before you receive it, it is possible for someone to intercept and read your e-mail. Consequently, you may want to put into effect measures to protect the confidentiality of your e-mail. A firewall does not necessarily provide this type of protection.

Other risks that are associated with using e-mail are:

- **Flooding** (denial of service attack) is a common problem with e-mail.
- **Spamming** (junk e-mail) is another type of attack common to e-mail.

What security measures you need to use when using e-mail depend on what e-mail applications you use. Some applications provide integrated security features that may provide the protection you need. Lotus Notes, for instance, provides several integrated security features to help you protect your systems from many common risks.

Lotus Notes provides document security by letting you encrypt fields in documents. Encryption means encoding data so that only those who have the encryption key can read it. Notes also allows you to encrypt entire mail memos. There are some differences between encrypting document fields and encrypting Notes mail memos.

Encrypting a document means applying a public or secret encryption key to one or more fields. Then, if the key is secret, sending the key to users of your choice. Any user who has the correct keys can read any encrypted fields in a document. Be careful not to give out a key to one field and forget that you are providing access to some other secret field. Users who do not have a key can still read any unencrypted fields in an encrypted document.

To encrypt a document, its form must have one or more fields defined as encryptable by the application developer. If you have a color monitor, and you are composing a document, you can recognize encryptable fields by their red field brackets. To encrypt a field, use an existing encryption key of your own, or create a new encryption key. Using key or keys you select all encryptable fields in a document are encrypted . You cannot select a different key for each encryptable field in a single document. Digital certificates generate when the encryption takes place.

In order to encrypt mail, Lotus notes will create a unique public and private key for each user. If someone sends you encrypted mail, Lotus notes will use your public key to encrypt message- it is unreadable to any user except you. When it delivers the message to your mail database, Notes uses your private key to decrypt (decode) the message for you.

The procedural steps for using the Lotus notes encryption process are in the help files. They accompany your Lotus notes program. Topics include the following:

- Create a secret encryption key
- Encrypt one or more documents by using either a secret key or a public key
- Mail encryption keys
- Delete an encryption key
- Import an encryption key
- Export an encryption key

Lotus Domino for AS/400 server, powers the Lotus Notes to provide proven message handling. For more information on Notes, the topic "What is Lotus Domino?" in the AS/400 Information Center will help. You can also visit the Lotus Notes user assistance web pageat the following URL:

`http://notes.net/notesua.nsf`

If the e-mail in question is between branch offices, remote clients, or business partners, it may be possible to use VPN connections to secure mail. Digital certificates allow you to encrypt individual e-mail transactions. There are other solutions that you may want to consider, especially if you have regular e-mail traffic between specific hosts or networks. For instance, you may have business partners, branch offices, or remote clients that you use e-mail to communicate with regularly.

If you do, you may want to use virtual private networks (VPNs) as a possible solution. Virtual private networks allow you to encrypt all traffic between the communicating endpoints. If you use IBM Firewall for AS/400 you can use VPNs between it and other compatible firewalls. Or, as of V4R4, you can use your AS/400 to configure VPNs, including VPNs between remote clients and your system.

File Transfer Protocol (FTP)-- security considerations

FTP (File Transfer Protocol) provides the capability of transferring files between the client (a user on another system) and your system server. You can also use the remote command capability to submit commands to the server system. Consequently, FTP is very useful for working with remote systems or moving files between systems. However, using FTP across the Internet, or other untrusted network, exposes you to certain security risks. You must understand these risks to ensure that your security policy describes how you will minimize these risks. Fortunately, IBM Firewall for AS/400 can protect you from many of these risks because it allows you to control FTP access. However, unless you use the firewall's virtual private network capabilities, it does not provide confidentiality for FTP data, including user IDs, and passwords.

FTP requires a user ID and a password. However, you can use the FTP server exit points to provide an anonymous FTP function for guest users. Setting up a secure anonymous FTP server requires exit programs for both the FTP server logon **and** FTP server request validation exit points.

If you want to allow FTP clients to access your system, be aware of the following security risks:

- Your object authority scheme might not provide detailed enough protection when you allow FTP on your system.

  For example, the public authority for your objects may be *USE, but today you are preventing most users from accessing those objects by using "menu" security. (Menu security prevents users from doing anything that is not one of their menu options.) Since FTP users have no restrictions to menus, they can read all objects on your system.

  Note: *USE authority to a file allows the user to download the file. *CHANGE authority to a file allows the user to upload the file.
- FTP counts the logon attempts for each user profile as long as the QMAXSGNACN system value is set to 2 or 3. This option disables the profile if it reaches the maximum sign on count. Three is the default setting. However, the hacker uses this to mount a "denial of service" attack via FTP. A hacker can use FTP to disable user profiles on the system by repeatedly attempting to log on with an incorrect password. This will happen until the user profile is disabled.

You can learn more about using FTP, its risks, and possible security measures, in theFTP and security articles in the AS/400 Information Center. Also in the book"Security Tips for File Transfer Protocol" on page 137.

Web serving-- security considerations

When you provide access for visitors to your AS/400 based Web site, think of each visitor as someone who views an advertisement in an industry journal. Neither is interested in learning about how the advertisement is created or how your Web site runs. The visitor is not aware of your Web site characteristics: What kind of server

you are using, and where you physically locate your server. Nor do you want to put any barrier (such as a Sign On display) between a potential visitor and your Web site.

As an administrator, you want to ensure that your security practices do not negatively affect the value of your Web site.

When using your AS/400 as a Web server, consider these points:

- A client cannot do anything with the HTTP server until the server administrator defines directives for the server. You have two major methods for creating security checks that every request to the Web server must pass before the server honors the request: General server directives and server protection directives. You can create and edit these directives by using the server Admin web pages for server configuration. Server directives allow you to control the overall behavior of the Web server. Server protection directives allow you to specify and control the security models the server uses for specific URLs that the Web server handles.
- You can use both map or pass directives and the server admin web pages to configure the server.
  - Use Map or Pass directives to mask the file names on your AS/400 web server. More specifically there are PASS server directives and Manufacturing Automation Protocol (MAP) server directives that control the directories from which the web server serves URLs. You can also find an EXEC server directive that controls the libraries in which CGI-BIN programs reside. You define protection directives for each server URL. Not all URLs require a protection directive. But, if you want to control how a URL resource is accessed or by whom, then a protection directive for that URL is required. (Both Map and Pass directives are methods for equating the URL that the client sends with a different name or resource on the server.)
  - Also, you can use the server Admin web pages to configure the server rather than using wrkhttpcfg and typing the directives. Working with protection directives through the command line interface can be very complicated. Therefore, you should use the Admin web pages to ensure that you set up your directives correctly.
- When you add a directive to the HTTP server, make the template value for the path as specific as possible. This reduces the chance that someone can browse through your system and discover files. Avoid using generic file names and wildcards.
- Some HTTP server requests need to run aAS/400 program, for example to access data on your system. Before the program can run, the server administrator must map the request (URL) to a specific user-defined program that conforms to CGI user-interface standards.

  As security administrator, you should monitor the authorizations of that user profile and the functions that the CGI programs perform. Also, be sure to evaluate what sensitive objects might have inappropriate public authority. A poorly designed CGI program might, in rare cases, allows a knowledgeable, devious user to attempt to roam your system.

  Note: CGI (common gateway interface) is an industry standard for the exchange of information between a Web server and computer programs that are external to it. The programs are written in any programming language that is supported on the operating system where the Web server is running.

  HTTP provides read-only access to your system. However, you probably will use other applications within your Web pages, such as CGI-bin programs to create

forms, that do allow write access to your AS/400. For instance, you may want to create forms that, once users complete them, update an AS/400 database. If you use the DB2WWW CGI program for this purpose, you could be allowing direct access to your AS/400 database files. This is the only interface that, without further programming, allows such direct access. By using DB2WWW without significant reprogramming, your database is very open to attack. This is likely if you do not have object level security that is set to exclude most users. In addition to using CGI programs in your web pages, you may want touse Java. You should understand Java security considerations before you add Java to your web pages.

- The HTTP server provides an access log that you can use to monitor both accesses and attempted accesses through the server.
- The HTTP proxy server comes with the IBM HTTP Server for AS/400. The HTTP Server is part of IBM Operating System/400 Version 3 (OS/400). The proxy server receives HTTP requests from Web browsers and resends them to Web servers. Web servers that receive the requests are only aware of the IP address of the proxy server. They cannot determine the names or addresses of the PCs that originated the requests. The proxy server can handle URL requests for HTTP, File Transfer Protocol (FTP), Gopher, and WAIS.

  The proxy server caches returned Web pages from requests that are made by all proxy server users. Consequently, when users request a page, the proxy server checks whether the page is in the cache. If it is, the proxy server returns the cached page. By using cached pages, the proxy server is able to serve Web pages more quickly, which eliminates potentially time-consuming requests to the Web server.

  The proxy server can also log all URL requests that are for tracking purposes. You can then review the logs to monitor use and misuse of network resources.

  You can use the HTTP proxy support in the IBM HTTP Server to consolidate Web access. Web page caching can also reduce communication bandwidth requirements and firewall workload.

Review this topic to learn more about Web serving:

Getting started with your IBM HTTP Server.

"Security Tips for Web Serving from AS/400" on page 150.

Adding secure telnet access using SSL

You have decided that you want to allow Telnet access into and out of your network on a limited basis. This is in addition the other Internet services you use. For example, you have a business partner that you work with to develop applications and you want to allow Telnet access between a development server on each network. However, using Telnet across the Internet, or other untrusted network, exposes you to certain security risks. You must understand these risks to ensure that your security policy describes how you will minimize these risks. Fortunately, IBM Firewall for AS/400 can protect you from many of these risks because it allows you to control Telnet access. However, you need to carry out additional security measures to provide confidentiality for Telnet data, including user IDs, and passwords.

Telnet uses virtual device descriptions to maintain client workstation information for open Telnet sessions.

As of V4R4, you can use secure Telnet. You can use Digital Certificate Manager to configure Telnet to use digital certificates and the Secure Sockets Layer to encrypt all Telnet traffic for the connection. You can also configure Telnet to ensure that only secure Telnet sessions can operate. For more information about using secure Telnet, see the topic "Starting the Telnet server using Secure Sockets Layer (SSL) support" in the AS/400 Information Center.

SSL protocol provides privacy and reliability between applications that are communicating . Use SSL record protocol to enclose other higher level protocols. One such protocol is the SSL which exchanges signals to set up communications between two modems protocol. The SSL protocol, which uses exchange signals to set up communications between two modems, allows the server and client to authenticate each other. Also it negotiates encryption and cryptographic keys before the application protocol receives or transmits its data. An advantage of SSL is that it is application protocol independent. A higher level protocol can be layered transparently over the SSL protocol.

With SSL there are three basic security features:

- **Privacy:** Encryption defines a private key.
- **Identity validation**: It authenticates a user's identity.
- **Reliability:** The connect is reliable and the message integrity is checked by using a keyed message authentication code (MAC).

The SSL Telnet server requires all data from the SSL enabled Telnet client to be encrypted. On receiving the encrypted data from the client, the Telnet server decrypts the information. The most important factor to consider in using SSL Telnet server is the sensitivity of the information that you use in a client session. If the information is sensitive, or private, then you may find it beneficial to set up your AS/400 Telnet server using SSL. When you configure your digital certificate with the AS/400 Telnet application, the Telnet server is able to operate with both SSL and non-SSL clients. If your security policy requires that you always encrypt your Telnet sessions, you may disable all non-SSL Telnet sessions . When there is no need for you to use the SSL Telnet server, you can turn off the SSL port. Once you have turned off the port, the server provides non-SSL Telnet for the clients, and the SSL Telnet sessions will be disabled. The AS/400 service table entry defines the SSL port in the : telnet-ssl.

The most important factor to consider when using the SSL Telnet server is the sensitivity of the information that is used in a client session. If the information is sensitive, or private, then you may find it beneficial to set up your AS/400 Telnet server using SSL

To use SSL, you need the following:

- IBM HTTP Server for AS/400 (5769-DG1)
- Cryptographic Access Provider licensed program for AS/400 (AC1, AC2, or AC3)
- A digital certificate for your Telnet Server.
- And a Web browser that supports SSL.
- These articles will describe the procedures for establishing a Telnet session with SSL and a Telnet server.

Secure Telnet is one of several methods now available for AS/400 to secure remote client access to your AS/400. Other methods include and secureClient Access Express.

To learn more about Telnet and about security tips for Telnet without SSL, review these topics:

- The topic "Getting started with Telnet" in the AS/400 Information Center.
- "Security Tips for TELNET" on page 132.

Adding Secure Client Access Express

You've decided that you want to allow remote users to use the Internet to access your internal network as part of your overall Internet stategy. How do you make this happen and ensure that your internal systems remain protected? One option available as of V4R4 is to use Client access express, which you can now configure to use Secure Sockets Layer (SSL).

Client access express offers a powerful set of client/server capabilities for connecting PCs to AS/400 systems. It is similar to its predecessor, Client Access for Windows 95/NT, though there are some distinct differences between the two.

You use Digital Certificate Manager to configure Client Access Express applications to use digital certificates and the Secure Sockets Layer (SSL). Using SSL ensures that all traffic for the Client Access Express sessions is encrypted which keeps your valuable data confidential. For more information about using Client Access Express with SSL, review the AS/400 Information Center topic Secure Sockets Layer administration.

For more information about Client Access Express, see the AS/400 Information Center.

Adding Virtual Private Networks (VPN)

With the rise in Internet Protocol-based Virtual Private Networks (VPN) businesses are exploring their options to transmit data over the Internet in a secure environment. One advantage of using VPNs is that you may be able to reduce the need for, and the cost of leased lines that you use for your network. You can use VPNs to create secure, controlled connections with branch offices, mobile employees, suppliers, business partners, and others. Using VPNs can lead to the following economical benefits:

- Increased effectiveness in streamlining processes.
- A reduction in cycling time
- A reduction in inventory related tasks.
- And a viable means of increasing customer responsiveness.

Some users who will use VPNs for connectivity include the following:

- Remote and Mobile user.
- Branch office to the Home office or other off—site locations
- Employees who need Extranet connectivity.

There are security risks that occur if you do not not limit user access to sensitive areas. Without this limiting who can access your system files you may open your information up to an attack. You need a plan that will allow only those who need to share information access to specific system files. Not everyone needs global access to your files and system. VPNs limit what files each user has access to on your

system. Creating multiple VPNs allows you to determine the filter rules for each one and restrict who has access to sensitive information. For example Accounting and Human Resources may link through their own VPN.

AS/400 Virtual Private Networking (VPN) is one of many security offerings available for protecting your AS/400 and communications. IBM offers two VPN solutions:

- IBM Firewall for AS/400 VPN with connections between compatible IBM firewalls
- AS/400 VPN connections between V4R4 (or later) AS/400s.

Whether VPNs provide the security that you need depends on what you want to protect. Also, it depends on the trade-offs that you are willing to make to provide that security. As with any decision that you make about security, you should consider how VPNs can support your security policy. Also, should they be a part of your overall security plan?

VPNs provide a solution for a specific security need: securing communications between systems. While VPNs provide protection for data that flows between the two endpoints of the connection, they do not provide other kinds of protection. For instance, you may also need to protect your system from unwanted traffic. AS/400 VPNs allow you to restrict the type of traffic that flows through a specific connection. They do not however work in the same manner that a firewall does to regulate traffic into and out of your system. Also, VPNs are not the only means available to secure communications between your AS/400 and other systems. Depending on your security needs, you may find that using digital certificates, and SSL is a better fit to your needs. For example, you can now use secure Telnet and secure Client Access Express over SSL.

One security risk involves sensitive corporate data that travels public networks that may be subject to attacks. The solution is to use encryption and authentication methods for ensuring privacy and security from outsiders. This is what a VPN provides. Using a VPN is a one way to secure your information from those you do not want to view it.

VPNs allow you create secure connections to protect traffic that flows between controlled and trusted endpoints. However, you still must be wary about how much access you provide to your VPN partners. VPNs encrypt data while it travels over public networks. But, depending on how you accomplish them, they may not encrypt data as it flows across the internal networks that communicate through the connection. Consequently, you should carefully plan how to set up each connection. Ensure that you give your VPN partner access to those hosts or resources on your internal network that you mean to. For instance, you may have a vendor that needs to obtain information about what parts you have in stock. You have this information in a database that you use to update Web pages on your intranet with this information. You would like to allow this vendor to access these pages directly through a VPN connection. But you do not want the vendor to be able to access other system resources, such as the database itself. Fortunately, you can configure your VPN such that traffic between both endpoints is restricted to port 80. Port 80 is the default port that HTTP traffic uses. Consequently, your vendor can send and receive HTTP requests and responds over the connection only.

For more information and details on VPNsVPNs see the topic "Virtual private networking" in the AS/400 Information Center..

AS/400 Internet security solutions

AS/400 offers several Internet security solutions to help you protect your internal resources from the many risks that are associated with connecting to the Internet. Which security solutions you decide to put into effect depends on how you use the Internet, what resources you need to protect, and your overall *security objectives*.

Fortunately, IBM provides a wide variety of security solutions for your AS/400. Generally, these solutions fall into one of two categories (with some overlap): Solutions that provide access protection and solutions that provide secure communications between networks or systems.

Security solutions that provide access protection.

- IBM Firewall for the AS/400. A firewall is a blockade between a secure internal network and an untrusted network such as the Internet. IBM Firewall for AS/400 provides a variety of security technologies that you can use to control traffic flow into and out of your network.
- AS/400 IP packet security. While not a fully functional firewall in itself, IP packet security, which is an integrated feature of IBM Operating System/400 Version 3 (OS/400), contains two helpful TCP/IP security components: Network Address Translation (NAT) and IP packet filtering. You can use these components to control TCP/IP traffic that flows into and out of your network.

Security solutions that protect communications between networks or systems.

1. AS/400 Digital Certificate Manager (DCM). You can use Digital Certificate Manager to configure a number of AS/400 applications to use the Secure Sockets Layer (SSL) for secure communications. Also, Digital Certificate Manager allows you to use digital certificates within your network for stronger user authentication.
2. AS/400 Virtual private networks (VPNs) AS/400 VPNs mainly provide a solution for protecting your communications. However, you can precisely configure the endpoints for each connection and restrict the type of traffic that can use the connection. Therefore, VPNs also help you protect your network resources from unauthorized access.

This article will provide more information on choosing your security solutions.

IBM firewall for the AS/400

To understand how a firewall works, imagine that your network is a building to which you want to control access. Your building has a lobby as the only entry point. In this lobby, you have receptionists to welcome visitors, security guards to watch visitors, video cameras to record visitor actions, and badge readers to authenticate visitors who enter the building. These measures may work well to control access to your building. But, if an unauthorized person succeeds in entering your building, you have no way to protect the building against this intruderÆs actions. If you monitor the intruderÆs movements, however, you have a chance to detect any suspicious activity from the intruder.

When you define your firewall strategy, you may think it is sufficient to prohibit everything that presents a risk for the organization and allow everything else. However, because computer criminals constantly create new attack methods, you must anticipate ways to prevent these attacks. As in the example of the building,

you also need to monitor for signs that, somehow, someone has breached your defenses. Generally, it is much more damaging and costly to recover from a break-in than to prevent one.

In the case of a firewall, your best strategy is to permit only those applications that you have tested and have confidence in. If you follow this strategy, you must exhaustively define the list of services you must run on your firewall. You can characterize each service by the direction of the connection (from inside to outside, or outside to inside). You should also list users that you will authorize to use each service and the machines that can issue a connection for it.

IBM Firewall for AS/400 features an application gateway firewall and a circuit gateway firewall. You can use one or both types of functions. The firewall product provides a number of technologies that you can use to protect your internal network, including:

- Internet Protocol (IP) packet filtering for TCP, UDP, and ICMP packets
- Network address translation (NAT) services
- SOCKS server
- Proxy server for HTTP, HTTPS, FTP, and Gopher for Web browsers
- TELNET proxy
- Mail relay
- Split domain name services (DNS)
- Logging
- Real-time monitoring
- Virtual private network (VPN) services

IBM Firewall for AS/400 consolidates security administration to enforce I/T security policy and minimize the opportunity for security configuration errors. The firewall provides privacy by preventing outsiders from accessing network information through the Internet. You can log traffic to and from the Internet, which allows you to monitor network use and misuse. Firewall configuration is flexible, which enables support for various security policies. The administrator decides which services the firewall should permit and which the firewall should block.

The IBM Firewall for AS/400 software guides the administrator through the basic installation and configuration of the firewall. The software that the firewall uses resides on a read-only disk. This eliminates the possibility of virus introduction or modification of programs that perform communication security functions. The main processor and firewall communicate over an internal system bus that is not subject to sniffing programs on local area networks. You can set the firewall to issue notifications to the AS/400 system operator (QSYSOPR) when a pre-configured condition on the firewall occurs. The main processor can disable the firewall when it detects tampering, regardless of the state of the firewall.

You can administer the firewall through a Web browser on the internal (secure) network. You can use the Secure sockets layer (SSL) for session encryption to protect the administration session. The software authenticates the administrator with OS/400 security support so that you need not require separate user IDs and passwords.

You should install the IBM Firewall for AS/400 on a two-port Integrated netfinity server for AS/400. Configure one port of the Integrated netfinity server to connect the firewall to your internal secure network. Configure the other port to connect the firewall to the Internet or other untrusted network.

The firewall can distinguish which network (trusted or untrusted) sent an Internet protocol (IP) packet. The firewall can also distinguish which port is the appropriate port for the originating packets on each network. Consequently, the firewall is not susceptible to spoofing attacks in which untrusted hosts try to masquerade as trusted ones.

The AS/400 system operator receives notifications (in the QSYSOPR message queue) when important firewall events occur, such as attempted intrusions. The system sends all high severity error messages (Type = Alert) immediately. The system sends lower severity messages (Type = Error, Warning, Information, or Debug) when they reach a user-defined threshold. If the system detects an error condition that may result from tampering (such as the logging function ends), all firewall functions are set to end immediately.

Installing the firewall on an Integrated netfinity server separates the processor that you use for application programs from the processor that you use for security programs. This separation eliminates the possibility of the programs interfering with each other. Compromised security programs that are running on the firewall cannot directly affect the AS/400 main processor in functionality or performance. In addition, the IBM OS/400 TCP/IP protocol stack is completely independent of the TCP/IP stack on the Integrated netfinity server.

The firewall also has separate storage, which prevents attackers from accessing AS/400 data. This storage is on a read-only disk to eliminate the possibility of virus introduction or modification of programs that perform communication security functions.

You can use the firewall proxy or SOCKS servers or network address translation (NAT) to provide internal users with safe access to services on the Internet. The proxy and SOCKS servers break TCP/IP connections at the firewall to hide internal information from the untrusted network. The servers also provide additional logging capabilities.

You can use NAT to provide Internet users with easy access to a public server behind the firewall. The firewall still protects your network because NAT hides your internal IP addresses. The firewall also protects internal information by using two DNS servers, one that you provide on the internal network and one on the firewall.

The firewall name server contains names visible to the untrusted network only, such as an external Web server. The firewall name server resolves outside names in response to requests from the internal name server. Your internal name server contains only the names of the internal network. Your internal name server forwards requests that it cannot resolve to the firewall name server. The firewall DNS server does not provide name serving functions for the internal network. You are not required to have an internal DNS server to successfully implement a firewall. However, having one makes client configuration easier because you do not have to maintain host tables on each system. OS/400 includes DNS support, which you should use for your internal network.

The firewall protects your internal mail server from attack by providing a mail relay function. The mail relay function passes mail between an external mail server on the firewall and an internal one. The firewall translates addresses of outgoing mail to the public address of the firewall secure port. This translation hides any internal information from the untrusted network.

The firewall also provides virtual private network (VPN) technology so that you can set up encrypted sessions between your firewall and other compatible firewalls.

At this point you can begin the development of yoursecurity planning, with firewall being one part of the strategy.

AS/400 packet security

Network address translation (NAT) provides a more transparent alternative to the proxy and servers. It also simplifies network configuration by enabling networks with incompatible addressing structures to connect.

Network Address Translation (NAT) changes the source or the destination IP addresses of packets that flow through the system. When using NAT, you can use the AS/400 system as a gateway between two networks which have conflicting or incompatible addressing schemes. You can also use NAT to hide the real IP addresses of one network by dynamically substituting a different address.

To use NAT, you must create a set of rules to specify how address translation will work. A æMapÆ rule translates one static address to another (for example a.b.c.d translates to e.f.g.h). You can use a map rule when the system with a real address of e.f.g.h provides services that you want to access from another network. This is where it is necessary or desirable to know the system by address a.b.c.d. A æHideÆ rule translates all addresses in a subnetwork to a specific IP address. You can use a hide rule when client systems need to access services in another network. Sometimes, it is necessary or desirable to use an alternative addressing structure.

Note: Because IP Packet Filtering and Network Address Translation complement each other, you will often use them together to enhance network security.

You use NAT to allow the PCs in your network access the Internet through your AS/400 while hiding their IP addresses from other Internet servers. You can use packet filtering in conjunction with NAT to provide an effective barrier to incoming connections from the Internet.

Internet Protocol (IP) packet filtering provides the ability to selectively block IP traffic that is based on information in the IP and protocol-specific packet headers. (For example, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)). You can create a set of filter rules to specify which IP packets to permit into your network and which to deny access into your network. When you create filter rules, you apply them to a physical interface (for example, a Token ring or Ethernet line). You can apply the rules to multiple physical interfaces, or you can apply different rules to each interface.

You can create rules to either permit or deny specific packets that are based on the following header information:

- Destination IP address
- Source IP address Protocol (for example, TCP, UDP, and so forth)
- Destination port (for example, port 80 for HTTP)
- Source port
- IP datagram direction (inbound or outbound)
- Forwarded or Local

You can use IP packet filtering to prevent undesirable or unneeded traffic from reaching applications on the system. Also, you can prevent traffic from forwarding to other systems. This includes low-level ICMP packets (for example, PING packets) for which no specific application server is required.

You can specify whether a filter rule creates a log entry with information about packets and matching the rule in a system journal. Once the information writes to a system journal, you cannot change the log entry. Consequently, the log is an ideal tool for auditing network activity.

It makes it easier to operate a public web server behind the firewall. Public IP addresses for the web server translate to private internal IP addresses. This reduces the number of registered IP addresses that are required and minimizes impacts to the existing network. And it provides a mechanism for internal users to access the Internet while hiding the private internal IP addresses.

You can use OS/400 IP packet filtering to provide additional protection for a particular AS/400 system. An example of this is a system that runs sensitive applications or a system that performs by Web serving to the Internet. You can also use packet filtering to protect an entire subnet when the AS/400 is acting in the role of a ôcasualö router.

The reason you would choose to do packet filtering is that you do not want:

- A production system to be vulnerable to denial of service attacks from the Internet
- Hackers to have hundreds of possible user profile/password combinations to be able to try
- To worry about all the security considerations of every application on your production system that may provide an outside interface, and so forth.

In general, an AS/400 system running production applications should **NOT** connect directly to the Internet.

You can find more information about using OS/400 Network Address Translation in the *TCP/IP Configuration and Reference, SC41-5420.*

IBM digital certificate manager (DCM)

IBM Digital Certificate Manager is a feature of OS/400 that allows you to manage digital certificates for systems and users. You can use DCM to associate a certificate with various AS/400 applications as part of configuring these applications to use the Secure Sockets Layer (SSL). You can then use SSL with these applications for secure communications. Using digital certificates and SSL-enabled browsers (such as Netscape Navigator), your server and clients can communicate securely using the secure sockets layer (SSL). Your browser can also use certificates instead of user names and passwords for more secure authentication within your intranet.

A digital certificate is a digital document that validates the identity of the certificate's owner, much as a passport does. A trusted third party, called a **Certificate authority (CA)** issues digital certificates to users and servers. The trust in the CA is the foundation of trust in the certificate as a valid credential. Each CA has a policy to determine what identifying information the CA requires in order to issue a certificate. Some Internet Certificate Authorities may require very little information, such as a distinguished name(The name of the person or server to whom a

Certificate Authority (CA) issues a digital certificate) and e-mail address. A private key and a public key are generated for each certificate. The certificate contains the public key, while the browser or a secure file stores the private key. The owner of a certificate can use these keys to "sign" and encrypt data, such as messages and documents, sent between users and servers. Such digital signatures ensure the reliability of an item's origin and protect the integrity of the item.

You can use DCM to manage certificates that an independent CA issues or to create your own CA and issue private certificates.

Some tasks are available only to AS/400 security officers or administrators. The security officer or administrator must have *SECADM and *ALLOBJ special authorities to view and use these tasks. Users without these special authorities have access to user certificate functions only. This is a very secure way to handle your security needs in the area of confidentiality and integrity.

You can find some examples about how to use digital certificates in the AS/400 Information Center topic, "using DCM".

Choosing your security solutions

You must plan your Internet security needs carefully to ensure that you choose the combination of solutions that best meets your needs. You should also review the *scenario topics* as part of your planning process. You will get some ideas as to how you can apply the solutions that they describe to your own Internet usage plans.

The solutions that you choose will depend on what it is you are trying to protect. For example, if your concerns are about confidentiality and data integrity, you need to carry our security measures beyond those that a firewall provides. For example, you may want to use Digital Certificate Manager if you have concerns about data integrity and confidentiality.

Most companies use a firewall to connect an internal network safely to the Internet. You can use a firewall to secure one internal network from another on an intranet also. A firewall provides a controlled single point of contact that is called a chokepoint, between your secure internal network and the untrusted network. The firewall:

- Lets users in your internal network use authorized resources that are located on the outside network
- It prevents unauthorized users on the outside network from using resources on your internal network

When you use a firewall as your gateway to the Internet (or other network), you reduce the risk to your internal network considerably. Using a firewall also makes administering network security easier because firewall functions carry out most of your security policy. To provide for Digital Certificates, cryptography, and enhanced security features you might add the Digital certificate manager program to your AS/400 system.

To learn more about AS/400 security solutions that you can use when connecting to the Internet, review these topics:

- AS/400 Internet security solutions
- IBM Firewall for the AS/400
- AS/400 IP packet security

- AS/400 Digital Certificate Manager (DCM)
- AS/400 Virtual private networks (VPNs)

How TCP/IP security features compare to firewalls.

Generally, security solutions that protect your network from unauthorized access rely on firewall technologies to provide the protection. To protect your AS/400, you can choose whether to use a full-capability firewall product (IBM Firewall for AS/400). Or you can choose to put into effect specific firewall technologies as part of the OS/400 TCP/IP implementation. These specific firewall technologies are IP packet filtering and NAT (part of the IP Packet Security feature) and HTTP Proxy server.

Choosing to use either the new OS/400 TCP/IP security features or a firewall depends on your network environment, access requirements, and security needs. The following table provides information about each TCP/IP security feature and its contrasting firewall component. Use this table to determine whether you should use a firewall, TCP/IP security features, or a combination of both in providing your network protection.

Security technology	OS/400 TCP/IP implementation	Firewall implementation
IP packet filtering	• Provide additional protection for a single AS/400 system such as an Internet Web server or an intranet system with sensitive data. • Protect a subnetwork of a corporate **intranet** when the AS/400 is acting as a gateway (casual router) to the rest of the network. • Control communication with a somewhat trusted partner over a **private network** where the AS/400 is acting as a gateway.	• Protect an entire corporate network from the **Internet**. • Protect a large subnetwork with heavy traffic from the remainder of a corporate network.
Network Address Translation (NAT)	• Enable the connection of two **private networks** with incompatible addressing structures. • Hide addresses in a subnetwork from a less trusted network.	• Hide addresses of clients accessing the **Internet**. Use as an alternative to Proxy and SOCKS. • Make services of a system in a private network available to clients on the **Internet**.
Proxy server	• Proxy at **remote locations** in a corporate network when a central firewall provides access to the Internet.	• Proxy an entire corporate network when accessing the **Internet**.

You can find more information about using TCP/IP security features in the *TCP/IP Configuration and Reference*, SC41-5420. These articles will give you specific information on the firewall and procedures for configuring your IBM firewall for AS/400. *Getting Started with IBM Firewall for AS/400*, in the AS/400 Information Center.

Part 6. Appendixes

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator
3605 Highway 52 N
Rochester, MN 55901-7829
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

ADSM/400
Advanced 36
Advanced Peer-to-Peer Networking
AIX
AnyNet
Application System/400
APPN
AS/400
AS/400e
Client Access
CT
DATABASE 2
Distributed Relational Database Architecture
DRDA
Global Network
IBM
Net.Data
OfficeVision
Operating System/400
OS/2
OS/400
PowerPC AS
QMF
SAA
SecureWay
SmoothStart
System/36
System/38
S/390
Ultimedia
400

Lotus and Lotus Notes are registered trademarks of Lotus Development Corporation. Domino and Notes are trademarks of Lotus Development Corporation.

C-bus is a trademark of Corollary, Inc.

Microsoft, Windows, Windows NT, and the Windows 95 logo are registered trademarks of Microsoft Corporation.

Java and HotJava are trademarks of Sun Microsystems, Inc.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

PC Direct is a registered trademark of Ziff Communications Company and is used by IBM Corporation under license.

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

Where to Get More Information and Assistance

Many resources are available if you need more information about security or if you need assistance.

About IBM SecureWay

IBM SecureWay provides a common brand for IBM's broad portfolio of security offerings; hardware, software, consulting and services to help customers secure their information technology. Whether addressing an individual need or creating a total enterprise solution, IBM SecureWay offerings provide the expertise required to plan, design, implement and operate secure solutions for businesses. For more information about IBM SecureWay offerings, see "Where to Get More Information and Assistance" and visit the IBM I/T (Information Technology) Security home page:

`http://www.ibm.com/security`

Service Offerings

Following are descriptions of several offerings that are available from IBM to help you either with AS/400 security or with connecting to the Internet. For more information, please contact your IBM representative. In the U.S., you can contact your local Express Services marketing office, or you can call 1-800-IBM-4YOU. You can also find out current information about service offerings by visiting the following IBM Web site:

`http://www.as.ibm.com/asus`

Security Review for AS/400: Security Review for AS/400 is available from IBM Availability Services. The review includes the following:

- Use of security tools
- A customer questionnaire.
- An interview to gather information about security practices.

The result of the review is a report that summarizes your potential security exposures and makes preliminary recommendations for corrective action.

Security planning, implementation, and consulting services are also available from IBM Availability Services.

SmoothStart for Web Server/400 from I/Net: An IBM services specialist will install, configure, and tailor Web Server/400 from I/Net, to allow your business to have a presence on the World Wide Web.

At the completion of this service, you will have a prototype Web home page, Web Server/400 installed and operational, and AS/400 TCP/IP configured and ready to be connected to the Internet or your own internal intranet.

Planning for Internet Connection for AS/400: This service offering provides you with the information and guidance that you need to determine what AS/400 functions to offer to Internet users. The planning session will cover the functions of Internet Connection for AS/400 and compare it to Web Server/400 from I/Net.

At the completion of this service, you will be able to assess the applicability of Internet Connection for AS/400 to your environment.

SmoothStart for Internet Connection for AS/400–Anonymous FTP: Beginning with V3R2 of OS/400, you can now use `anonymous` as a valid user ID for users of file transfer protocol (FTP). With anonymous FTP, you can offer users on the Internet, or your own internal Intranet, access to files on your AS/400 without the need to distribute unique user IDs and passwords to the users.

The SmoothStart for Internet Connection for AS/400–Anonymous FTP service will provide you with a services specialist to help you do the following:

- Plan the use of anonymous FTP for your environment
- Set up an FTP user exit that will allow your users both to get files from one AS/400 library and to put files to another AS/400 library.

At the completion of this service, your AS/400 will be configured both to allow users to access files by using anonymous FTP and to prevent them from accessing files that you restrict. FTP users will also be able to upload files to one specific library.

SmoothStart for Internet Connection for AS/400–POP Mail Server: Beginning with V3R2, AS/400 can be a Post Office Protocol R3 (POP3) mail server and hold mail in mailboxes for users running a POP3 client. The users can pick up their mail whenever they are ready.

The SmoothStart for Internet Connection for AS/400–POP Mail Server offering provides you with a services specialist to configure the necessary objects to allow your AS/400 to be a POP3 mail server for your clients who are using mail programs like Eudora, Ultimail, and other POP3 clients running on AIX, Windows, OS/2, and MacIntosh.

At the completion of the service, your AS/400 will be configured as a POP3 mail server, with mailboxes created for ten mail clients to use for their mail. In addition, five non-AS/400 mail users will be defined on the AS/400 to allow you to send mail to them.

SmoothStart for Internet Connection for AS/400–Web provides you with a services specialist to install, configure, and customize the Internet Connection for AS/400 Web Server and HTML Workstation Gateway to allow your business to have a presence on the Web.

At the completion of this service, you will have a prototype Web home page and access to AS/400 applications from a Web browser. You will have AS/400 TCP/IP configured and ready for connection to the Internet or to your own internal intranet.

Security Analysis Lab: With the security analysis lab offering, IBM consultants attempt to infiltrate customers' networks. They assess network vulnerability and recommend security improvements.

Emergency Response Service: The emergency response service for commercial businesses provides swift, expert incident management skills during and after an electronic security emergency. In the event of a break-in, the emergency response team helps customers detect, isolate, contain, and recover from the unauthorized network infiltration.

Related Publications

Following are publications that provide more information about AS/400 security:

- *APPC Programming*, SC41-5443-00, describes the advanced program-to-program communications (APPC) support for the AS/400 system. This book guides in developing application programs that use APPC and defining the communications environment for APPC communications. It includes application program considerations, configuration requirements and commands, problem management for APPC, and general networking considerations.
- *Client Access Express for Windows Host Servers*, SC41-5740-03, provides information for the system administrator working with AS/400 server functions. The book includes server concepts, server functions, and exit program information.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet*, SG24-4929, discusses the security issues and risk associated with connecting your AS/400 to the Internet. It provides examples, recommendations, tips and techniques for TCP/IP applications.
- *AS/400 Wireless LAN Installation Planning Guide*, G571-0303-00, provides information about planning and installing a spread spectrum network. In addition to an overview of spread spectrum radio technology, this book also describes how to prepare for a site survey and ensure that antenna and cabling requirements are met for the areas to be covered.
- *Backup and Recovery*, SC41-5304-03, provides information about setting up and managing:
  - Journaling, access path protection, and commitment control
  - User auxiliary storage pools (ASPs)
  - Disk protection (device parity, mirrored, and checksum)
  - Plan a save strategy for your system.
  - Perform basic save operations.
  - Select which availability options are appropriate for you system.
  - Recover your system if a failure occurs.
- *DB2 UDB for AS/400 Database Programming*, SC41-5701-02, provides a detailed discussion of the AS/400 database organization, including information on how to create, describe, and update database files on the system. It also describes how to define files to the system using OS/400 data description specifications (DDS) keywords.
- *CL Programming*, SC41-5721-02, provides detailed descriptions for coding the data description specifications (DDS) for files that can be described externally. These files are physical, logical, display, print, and intersystem communication function (ICF) files.
- *Distributed Data Management*, SC41-5307-00, provides information about remote file processing. It describes how to define a remote file to OS/400 distributed data management (DDM), how to create a DDM file, what file utilities are supported through DDM, and the requirements of OS/400 DDM as related to other systems.
- *Distributed Database Programming*, SC41-5702-01, provides information on preparing and managing an AS/400system in a distributed relational database using the Distributed Relational Database Architecture (DRDA). The publication describes planning, setting up, programming, administering, and operating a distributed relational database on more than one AS/400 system in a like-system environment.

- *Getting Started with IBM Firewall for AS/400*, SC41-5424-02, describes how to set up, configure, and manage the Firewall for AS/400.
- *IBM Network Station Manager for AS/400*, SC41-0632-01, describes how to set up, configure, and manage the Network Station.
- *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200, provides practical suggestions and examples for many areas of AS/400 security.
- *Implementing AS/400 Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: Duke Press, a division of Duke Communications International, 1988. Provides guidance and practical suggestions for planning, setting up, and managing AS/400 security.

  ISBN Order Number:
  1-882419-78-2
- *HTTP Server for AS/400 Webmaster's Guide*, GC41-5434-04, provides the system administration with information for configuring and managing the Internet Connection Server and the Internet Connection Secure Server.
- *Managing OfficeVision/400*, SH21-0699-00, provides information about how to manage the day-to-day activities of OfficeVision. The book includes information on maintaining office enrollment and creating and managing office objects.
- *Planning for and Setting Up OfficeVision/400*, SH21-0695-00, provides information about planning for and setting up OfficeVision. The book includes information on planning for enrolling users, word processing, mail and calendar processing, using OfficeVision with IBM personal computers, and using OfficeVision in a communications network. The planning activities include filling out planning work sheets that are used to do the setup tasks.
- *Security - Basic*, SC41-5301-00, explains why security is necessary, defines major concepts, and provides information on planning, setting up, and monitoring basic security on the AS/400 system.
- *Security - Enabling for C2*, SC41-5303-00, describes how to customize your system to meet the requirements for C2 Security, as described in the *Department of Defense Trusted Computer Evaluation Criteria*
- *Security - Reference*, SC41-5302-03, provides complete information about security system values, user profiles, resource security, and security auditing. This manual does not describe security for specific licensed programs, languages, and utilities.
- *Basic System Operation, Administration, and Problem Handling*, SC41-5206-03, provides information about the system unit control panel, starting and stopping the system, using tapes and diskettes, working with program temporary fixes, as well as handling problems.
- *System API Reference*, SC41-5801-03, provides information on how to create, use, and delete objects that help manage system performance, use spooling efficiently, and maintain database files efficiently. This book also includes information on creating and maintaining the programs for system objects and retrieving OS/400 information by working with objects, database files, jobs, and spooling.
- *System/36 Environment Programming*, SC41-4730-00, provides information identifying the differences in the applications process in the System/36 environment on the AS/400 system. It helps the user understand the functional and operational differences (from a System/36 perspective) when processing in the System/36 environment on the AS/400 system. This includes an environment functional overview, considerations for migration, programming, communications, security, and coexistence.

- *TCP/IP Configuration and Reference*, SC41-5420-03, provides comprehensive information for configuring and using AS/400 TCP/IP support. It includes descriptions of all the TCP/IP server applications.

  Note: For V4R1, descriptions of the Internet Connection Server (formerly HTTP) and the Internet Connection Secure Server are in the *HTTP Server for AS/400 Webmaster's Guide* book.
- *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, provides introductory information, installation instructions, and setup procedures for the File Server Support licensed program offering. It explains the functions available with the product and includes examples and hints for using it with other systems.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, describes the criteria for levels of trust for computer systems. The TCSEC is a publication of the United States government. Copies may be obtained from:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- *The Whole Internet User's Guide and Catalog* by Ed Krol, O'Reilly & Associates, Inc., 1994, is a comprehensive introduction to the Internet. It includes a listing of information resources and an index of useful sites to visit.
- *Work Management*, SC41-5306-03, provides programmers with information about how to effectively manage their system work load by changing work management objects to meet their needs. The publication provides guidelines for performance tuning; descriptions of system values; and information on collecting performance data, gathering system use data, using work entries, and scheduling batch jobs.

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

AS/400e
Tips and Tools
for Securing Your AS/400
Version 4

Publication No. SC41-5300-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC41-5300-03

IBM®

Cu
Alc

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM CORPORATION
ATTN DEPT 542 CLERK
3605 Highway 52 N
ROCHESTER MN 55901-7829

Fold and Tape **Please do not staple** Fold and Tape

C
A

Readers' Comments — We'd Like to Hear from You

AS/400e
Tips and Tools
for Securing Your AS/400
Version 4

Publication No. SC41-5300-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
SC41-5300-03

IBM®

Cu
Alc

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM CORPORATION
ATTN DEPT 542 CLERK
3605 Highway 52 N
ROCHESTER MN 55901-7829

Fold and Tape | **Please do not staple** | Fold and Tape

C
A

Part Number: 43L1571

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

43L1571

SC41-5300-03