AS/400 Advanced Series

Alerts Support

Version 4

IBM

AS/400 Advanced Series

Alerts Support

Version 4

First Edition (August 1997)

This edition applies to the licensed program IBM Operating System400 (Program 5769-SS1), Version 4 Release 1 Modification 0, and to all subsequent releases and modifications until otherwise indicated in new editions.

Make sure that you are using the proper edition for the level of the product.

Order publications through your IBM representative or the IBM branch serving your locality. If you live in the United States, Puerto Rico, or Guam, you can order publications through the IBM Software Manufacturing Solutions at 1-800-879-2755. Publications are not stocked at the address given below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication. You can also mail your comments to the following address:

> IBM Corporation
> Attention Department 542
> IDCLERK
> 3605 Highway 52 N
> Rochester, MN 55901-7829 USA

or you can fax your comments to:

> United States and Canada: 1-800-937-3430
> Other countries: 1-507-253-5192

If you have access to the Internet, you can send your comments electronically to IDCLERK@RCHVMW2.VNET.IBM.COM; IBMMAIL, to IBMMAIL(USIB56RZ).

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Part 1: Learning about Alerts

Part 2: Using Alerts

Appendixes

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. 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. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter 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
> 500 Columbus Avenue
> Thornwood, NY 10594
> U.S.A

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 the software interoperability coordinator. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee. Address your questions to:

> IBM Corporation
> Software Interoperability Coordinator
> 3605 Highway 52 N
> Rochester, MN 55901-7829
> U.S.A.

This publication could contain technical inaccuracies or typographical errors.

This publication may refer to products that are not currently available. IBM makes no commitment to make available any unannounced products

referred to herein. The final decision to announce any product is based on IBM's business and technical judgment.

This publication 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.

This publication contains small programs that are furnished by IBM as simple examples to provide an illustration. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. All programs contained herein are provided to you "as is." **The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.**

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

ACF/VTAM
AnyNet
Application System/400
AS/400
IBM
NetView
Operating System/400
Operational Assistant
OS/2
OS/400
SystemView
System/370
System/390
VTAM
400

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

v

About Alerts Support, SC41-5413

This book is intended for the programmer who needs to understand how to manage a system by using alerts support or for the programmer who wants to understand how to manage a network.

Who Should Read This Book

Using this book, the AS/400 programmer can:

- Configure the AS/400 system to use alert support.

- Allow end-user applications to create alerts and notify the OS/400alert manager of previously created alerts that need to be handled.

- Control the creating, sending, and logging of alert messages for problem management.

- Perform central site problem analysis for the AS/400 systems in a network.

You should be familiar with the following to use the information in this book:

- AS/400 programming terminology. You should also be familiar with the terminology of the host system

- Data communications concepts.

- Configuration and communications information that is provided in the books: *Communications Configuration*, SC41-5401, and *Communications Management*, SC41-5406

This book is divided into three parts:

- Part 1: Learning about Alerts
- Part 2: Using Alerts
- Part 3: Additional Information

Part 1 presents material that gives the user the opportunity to learn about alerts on a how-to level. Part 2 and Part 3 contain detailed reference material that was formerly contained in the *DSNX Support*, SC41-5409 book.

Prerequisite and Related Information

For information about Advanced 36 publications, see the *Advanced 36 Information Directory*, SC21-8292, in the AS/400 Softcopy Library.

For information about other AS/400 publications (except Advanced 36), see either of the following:

- The *Publications Reference*, SC41-5003, in the AS/400 Softcopy Library.

- The AS/400 Information Directory, a unique, multimedia interface to a searchable database that contains descriptions of titles available from IBM or from selected other publishers.

For a list of related publications, see the "Bibliography" on page X-1.

Information Available on the World Wide Web

More AS/400 information is available on the World Wide Web. You can access this information from the AS/400 home page, which is at the following universal resource locator (url) address:

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

Select the Information Desk, and you will be able to access a variety of AS/400 information topics from that page.

Chapter 1. How to Use Alerts to Simplify Your Network Management

This chapter provides an overview of alerts and how alerts can better serve your systems management needs. If alerts are new to you, this chapter gives you the opportunity to learn about them at a how-to level. If you are experienced in working with alerts, this chapter gives you the opportunity to learn about parts of alert management that you never knew existed.

What Are Alerts?

Alerts are specific types of system messages that are used to identify problems or impending problems. When you set up your system for alert support, you receive an alert system message whenever a problem has occurred or whenever a problem is about to occur. These alert messages help you to manage your systems and network more efficiently.

OS/400 alerts support provides you analysis data about the cause of a problem or impending problem. By summarizing the problem and giving the network or system operator guidance on corrective actions to the problem, alert support assists you in better managing both your network and the systems within your network.

Also, alerts support has both the flexibility to run on different machines and the rigidity to provide notification and analysis on specific problems.

Why Would I Want to Use Alerts?

You would want to use alert support because alert support helps you manage your network and systems more effectively. The following situations are examples of reasons to use alerts:

- If you need to have all your technical people at one location.

  By using alerts support, you can staff all of your technical support at one central site.

- If you run your own application on your system.

Alert support gives you the capability to define your own alertable messages so that your own applications has the same error reporting capabilities as the system functions.

- If you need the flexibility to choose where your technical support is located.

  With alert support, you can select which of your systems will receive technical support from your technical centers.

- If you manage a network with either homogeneous or heterogenous systems.

  Because alerts are designed to be independent of the system architecture, alerts from one system are readable on other systems.

- If you must monitor your network status.

  Alerts support information about specific network problems can help you track and monitor your system.

- If you must reduce your system and network costs.

  Because the system automatically controls the capabilities of alerts, you can automate common responses to system problems without operator intervention.

- If you have unattended remote systems.

  Alerts can notify a central site about a problem on a unattended system.

What Is Required to Set Up Alerts?

Alerts are set up in user applications by using message files for their messages and alert tables for their alert descriptions. If the message is alertable, the following is required:

- An alert message must be in the message file.

- An alert description must be in the alert table.

- The message file and the alert table must have the same name.

- The message file and the alert table must be in the library list of the job that generates the alerts.

Alerts implementation in this way removes some of the complexity in the ability to create unique alerts.

What Options Do I Have to Configure Alerts?

You can configure your alerts by setting up either a sphere of control or an alert controller session.

If you configure your AS/400 business computing system by using sphere of control, the system that serves as the focal point establishes a control point session with every system that is defined under the focal point sphere of control. An AS/400 **focal point** is an AS/400 system that is defined to receive alerts. A focal point **sphere of control** is a collection of nodes within your APPN network that sends alerts to the focal point. If you decide to use sphere of control, you must have advanced program-to-program communications (APPC) and Advanced Peer-to-Peer Networking (APPN) support on your AS/400 system.

If you configure your AS/400 system by using an alert controller session, you define the system to which alerts are sent as an alert controller. You can use an alert controller to configure your AS/400 system without the need for APPC support. This configuration does not support the sphere of control function and does not require you to define any focal points.

Where Do I Send My Alerts?

Actually, you do not send your alerts anywhere. Instead, the system determines where to send the alerts based on the focal point of that system. When you use APPC and APPN support, the focal point system establishes a management services session with other systems that are defined under the focal point's sphere of control. Alerts are sent through this management services session to a focal point.

Because the sphere of control function is such a powerful function, it is best that you use a man-

agement services session to configure your alerts and not alert controller sessions.

You should select the system that you want to use as the focal point for your network based on which system is the most centralized in your network. You can find out where the system is sending your alerts by using the Work with Alerts (WLKALR) command.

The AS/400 system also provides the capability to nest focal points. Nested focal points allows you to define a hierarchy of focal points where the high-level focal points accept alerts collected by low-level focal points.

The four types of focal points are:

- Primary focal point
- Default focal point
- Backup focal point
- Requested focal point

Primary Focal Point

A **primary focal point** is an AS/400 APPN node that defines all nodes under its sphere of control. Your primary focal point has two functions:

- Establish a management services session to your nodes.
- Reestablish the management services session whenever the link is lost or reconnected.

You can define your node as the primary focal point by using the Change Network Attribute (CHGNETA) command:

```
CHGNETA ALRSTS(*ON) ALRPRIFP(*YES) ALRDFTFP(*NO) ALRLOGSTS(*ALL)
    ALRCTLD(*NONE)
```

The alert primary focal point (ALRPRIFP) parameter defines whether the node is a primary alert focal point.

Default Focal Point

A **default focal point** is an AS/400 network node that acts as a focal point for all network nodes that are not under the sphere of control of an active primary focal point. A default focal contains only network nodes. The purpose of a default focal point is to ensure that all network nodes have a place to send their alerts.

You should define your focal point system as a primary focal point and not as a default focal point. However, if you need to define your system as a default focal point, you should have only a single default focal point.

You can define your node as the default focal point by using the following command:

```
CHGNETA ALRSTS(*ON) ALRPRIFP(*NO) ALRDFTFP(*YES) ALRLOGSTS(*ALL)
    ALRCTLD(*NONE)
```

The alert default focal point (ALRDFTFP) parameter defines whether your node is a default alert focal point.

Backup Focal Point

A **backup focal point** is an AS/400 system that is used as a focal point only when other nodes cannot communicate with their primary focal point. Your primary focal point identifies the system that will serve as the backup focal point.

You can define your node as the backup focal point by using the following command:

```
CHGNETA ALRBCKFP(netid id)
```

You must have the ALRPRIFP parameter set to *YES for the backup focal point system.

Requested Focal Point

A **requested focal point** is an AS/400 system that has been designated by a node as the focal point system to which data is sent. A node can request its focal point. You need to use a requested focal point when the entry point is the only node that knows when a link needs to be re-established.

You can define your node as the requested focal point by using the following command:

```
CHGNETA ALRRQSFP(network cp)
```

The following are requirements for setting up an AS/400 system as a requested focal point:

- You must use the alert requested focal point (ALRRQSFP) parameter to specify the focal point system to which alerts are to be sent.
- You must have the ALRPRIFP parameter set to *YES for the requested focal point system.

What Is Sphere of Control?

You can manage which systems are under whose control by setting up a sphere of control. The **sphere of control** specifies the systems within a network that send alerts to their primary focal point. The sphere of control allows you to better manage the complexity of a large and ever-growing network.

You can use the Work with Sphere of Control (WRKSOC) command to add systems to a sphere of control. Also, systems within the sphere of control can be automatically assigned to a default, requested, or backup focal point by the AS/400 system.

Removing Systems from the Sphere of Control

You can use the Remove Sphere of Control Entry (RMVSOCE) command to remove systems from a focal point's sphere of control. You should want to remove a system from a focal point sphere of control for the following reasons:

- A system is physically removed from a network.
- A system is replaced by another system that has a different name.
- A system no longer needs technical support.

A focal point in the sphere of control should not be removed from the sphere of control until another focal point has started focal point services to that system. This ensures that a system always has a focal point.

What Is the Best Way To Organize My Alerts?

The best way to organize your alerts is to build a hierarchical structure of focal points. A hierarchical structure of focal points is referred to as nested focal points. A **nested focal point** is a focal point that is defined within the sphere of control of another focal point. By nesting focal points, alerts that are collected by lower-level focal points are forwarded to their higher-level focal point.

The advantages of nesting focal points are that a focal point can be configured so that alerts are routed through fewer APPN nodes and that there can be fewer management services sessions on any given system. The disadvantage of nesting focal points is that the management for the sphere of control is performed on more than one system.

Make sure that the ability of your central site to handle alerts does not exceed the ability of your operator to handle those alerts. For example, if a single sphere of control manages 200 systems and each system generates five alerts each day, your operators will need to handle 1000 alerts every day.

Because system alerts are automatically sent to their APPN end node, APPN nodes do not have to be added to the sphere of control. This decreases the time spent on network configuration and reduces the number communication sessions needed.

Using Nested Focal Points on a System/370

In a System/370 host environment, NetView is usually the highest focal point that receives alerts from downstream AS/400 focal points. When using this approach, you need to consider the following:

- You may have AS/400 systems in the network that are not directly connected to System/370. Alerts gathered from these systems are forwarded on to NetView by using AS/400 focal point support.

- Other AS/400 systems may have the appropriate skills to manage the network in their own region. In this case, alerts are forwarded to NetView for statistical purposes, but the network management functions remain on their local AS/400 systems.

- You may have AS/400 systems that are dedicated only for one particular type of application. These systems could be the focal points that only track and resolve alerts for those particular application type.

- You may have network cost savings when you use nested focal points. This is especially true if the central site system is in a different geographic location. Typically, the more local a system is, the less expensive the network cost will be.

What Do I Need to Consider When I Configure My AS/400

You can configure your AS/400 system for alerts either with the configuration menus or with the control language commands. OS/400 network attributes are used to define your AS/400 system to be a focal point and to control other alert function. You can use the Change Network Attributes (CHGNETA) command to change the network attributes. The following alert functions are controlled by OS/400 network attributes:

- Alert status
- Alert logging status
- Alert primary focal point
- Alert default focal point
- Alert backup focal point
- Alert focal point to request
- Alert controller description
- Alert hold count
- Alert filter

Other Ways to Configure Your AS/400 System

You can use the Display Network Attributes (DSPNETA) command to display the current values of your network attributes.

Although you can configure your AS/400 system to provide focal point services, you can also configure your AS/400 system in the following ways:

- A system that is not a focal point but sends and forwards alerts to another system that is a focal point. For example, an AS/400 system that is not a focal point can still generate alerts and receive alerts from a 5494 controller. If this AS/400 system does not have an on-site operator handling these alerts, then the alerts can be forwarded to another system.

- A focal point in the network that is not attached to the host system. For example, an AS/400 system can be the host system and not need to forward any of its alerts to other systems.

- A nested focal point that forwards alerts to the NetView program from an APPN network. For example, you can reduce the number of management services sessions to your host system by designating an AS/400 system as a focal point. Any alert automatic handling can be done on the focal point. All other alerts can be handled by operators who use the NetView program to forward the alerts to a System/390.

What Ways Are There to Create Alerts?

When a problem or an impending problem occurs on an AS/400 system, alerts are created in the following ways:

- You can use the alert status control attribute to create alerts for the entire system.

- You can use the Change Message Queue (CHGMSGQ) command to determine whether the message queue is defined to accept alerts. If the message queue is defined to allow alerts, then alerts are created.

  Note: QSYSOPR message queue defaults to accept alerts. Also, QHST message queue is required to accept alerts.

- You can use the alert option on the message description to create alerts. This allows you to control exactly which messages can create an alert.

An Example of a Message Queue

The following is an example of how message queues are used to generate an alert.

- Given that the following is true:

  - Message ABC1234 has an alert option of *IMBED.

  - Message XYZ6789 has an alert option of *NO.

  - Message queue NOALERT does not allow alerts to be created.

  - Message queue ALERT allows alerts to be created.

- Then, the following is also true:

  - Alerts are not created on any message queue when the alert status is *OFF.

  - Alerts are not created on the NOALERT queue when the alert status is *ON. However, alerts are created for Message ABC1234 on the ALERT message queue.

Questions That Decide If a Message Should Be Alertable

When you are deciding whether a message should be alertable, you need to ask the following questions.

- Do you want your system to send any alerts?

  Set the alert status network attribute to *ON when you want to create alerts.

- Does your system have a local operator?

  Set the alert status network attribute to *UNATTEND when there is not a local operator. Set the alert status network attribute to *ON when there is a local operator.

- Is local problem analysis available for the problem?

  Set the alert option to *DEFER to run local problem analysis when it is available.

- Does problem analysis provide a local resolution to the problem?

  Create an alert to report that a problem occurred and was analyzed, but a local resolution was not found.

- Should the system message be forwarded to another location for handling?

  To forward the system message to another location for handling, set the alert status to *UNATTEND. When a system operator is present, set the alert status to *ON.

- Do you want to send an alert that reports the outcome of problem analysis?

  To send an alert that reports the outcome of problem analysis, set the alert status to *ON and set the alert option to *DEFER.

Where Can I Send My Alerts?

Alerts that are created on an AS/400 system can be sent to any other system in the network if the system is a focal point system. Also, alerts can be sent to a System/370 system if it has NetView support.

The sending and forwarding of alerts are basically the same. They both use the same sphere of control commands, they both are received by the focal point system in the same way, and they are both part of the OS/400 program.

The difference between sending an alert and forwarding an alert can be summarized as follows:

- The entry point system sends the alert to another system (the system that creates an alert).

- The focal point system forwards the alerts to another focal point system (the system that receives an alert).

The biggest benefit that forwarding alerts has over sending alerts is that the alert message can be sent to where the problem can best be handled.

You can use either the management services session or the alert controller session to forward alerts. If an AS/400 system is forwarding the alert to another AS/400, then a management services session should be used. If an AS/400 system is forwarding the alert to a system other than an AS/400system, then an alert controller session must be used. Because the management services session supports the sphere of control function, use the management services sessions whenever they are available.

Can I Save My Alerts?

You can save your alerts by logging them into the alert database. The main benefit to logging alerts into the alert database is to control the number of alerts that the operator is required to handle from one moment to the next. You can do this if you have created an alert on your local AS/400 system or have received alerts from another AS/400 system. You can control which alerts are logged into the database either by using the Change Network Attribute (CHGNETA) command or by

using an alert filter. An **alert filter** assigns each alert to a group and specifies the actions to take place for each group.

Alerts are also saved in the alert database when they cannot be sent to their designated focal point systems. These alerts are referred to as **held alerts**. Alerts become held alerts when either a network problem exists or if the number of alerts held is less than the value of the alert hold count (ALRHLDCNT) network attribute. ALRHLDCNT can assigned only when you use the alert controller description (ALRCTLD) network attribute.

When logged into the alert database, all held alerts are marked for sending at a later time. When you or the system resolves the network problem or when the number of held alerts equals the value specified in ALRHLDCNT parameter, the alerts are sent to their designated focal point.

You can display logged or held alerts by using the Work with Alerts (WRKALR) command.

Can I Delete My Alerts?

To delete unwanted alerts from the alert database you can use either the Work with Alerts (WRKALR) command or the Delete Alert (DLTALR) command. You delete alerts from the alert database when you want to control the size of the alert database and to free up needed disk storage. Use the QAALERT command to determine the size of your alert database.

Also, you can use Operational Assistant cleanup to automatically control the size of the alert database during system log cleanup.

Can I Define My Own Alertable Messages?

You can define any system messages as alertable just by changing the alert option (ALROPT) parameter in the message description. This allows your AS/400 system to make any message alertable whether it is a system or user message. For a list of current alertable messages, see Appendix B, IBM-Supplied Alertable Messages.

Being able to define your own alertable messages gives you greater flexibility in managing your

network and those systems within that network. By defining your own alertable messages, specific network and system conditions can be monitored.

Can I Use Alerts With NetView?

The NetView licensed program allows a System/370 host or a System/390 host to communicate with an AS/400 system. The NetView program provides the focal point capabilities so that the host system operator can display the alerts and perform the appropriate problem analysis based on the alert. All activities can be done from a System/370 or System/390 without the need of a AS/400 system.

To send your alerts over to NetView, you should use the NetView sphere of control commands. NetView sphere of control commands are similar to the sphere of control commands found on an AS/400 system. Another way to send alerts over to a System/370 or a System/390 is through the alert controller description. Because of its flexibility, use the NetView sphere of control commands instead of the alert controller description.

The NetView commands also provide the focal point capabilities so that the host system operator can display the alert and perform the appropriate problem analysis based on the alert.

Can I Display My Alerts?

You can display an alert by using the Work with Alerts (WRKALR) command. Besides displaying possible causes of the alert, the WRKALR command also displays any recommended actions that are associated with the alert. You can use a variety of WRKALR parameters to control which alert information is displayed and when it is displayed. This control is especially useful when you control alerts by an assigned user or an assigned group. (Assigning users and assigning groups are two ways to categorize alerts.)

When you display your alerts, the following information is displayed:

Resource hierarchy The lowest entry shows the resource name and the failing resource type. The resource hierarchy determines which hardware resource failed

when it is a hardware resource problem.

Date/Time The date and time that the problem occurred.

> **Note:** The System/36 and System/38 do not send the problem date and time information to the AS/400 system.

Alert type and description entry The alert type (permanent, temporary, performance, impending problem, or unknown) combined with the description entry assist the network operator in deciding the next appropriate step in problem analysis.

Probable causes The possible causes of the problem in descending order.

Alert detail Additional displays show the message ID, message text, hardware details, and software details to provide more information about the problem.

The following is an example of a Display Alert Detail display:

```
                      Display Alert Detail
                                             System:   ROCHESTR

----------Resource Hierarchy------
  Resource Name          Resource Type
    ROCHESTR               CP
    ATLANTA               CP
    CC03                  LC
    RCHLIN                LNK

Logged date/time . . . . . . :    02/15/88  15:18:04
Problem date/time  . . . . . :    02/15/88  15:18:01
Assigned user  . . . . . . . :
Group assigned . . . . . . . :
Filter . . . . . . . . . . . :
  Library . . . . . . . . . . :
Alert type . . . . . . . . . :    Permanent
Alert description  . . . . . :    Unable to communicate with remote node
Probable causes  . . . . . . :    Communications
                                  Communications/remote node
                                                                More...
Press Enter to continue.

F3=Exit   F11=Display detail menu   F12=Cancel   F18=Display actions
```

Alert support also has a refresh capability that automatically refreshes the display screen.

Can I Select Which Alerts to Display?

You can select which alerts to display and at what focal point that you want to display the alerts by using filters. You would want to use alert filtering for the following reasons:

- The volume of alerts is reasonable for the operators who are handling the alerts.

- The alerts are being sent to operators based on the expertise level of the operators.

Alert filtering is a function that assigns alerts into groups and specifies what actions to take for each group. Filtering is used at both the focal point system and the entry point system.

At the focal point system, the system can handle an incoming alert either by assigning the alert to a user or by notifying a user automated program to the alert.

At the entry point system, the system can use the alert filter to forward the alert either to a focal point system or to another entry point system. All filtering actions are valid at either the focal point system or entry point system.

A **filter** consists of both selection entries and action entries. A **selection entry** assigns each alert that is processed by the filter to a group. An **action entry** specifies what should be done to process each group of alerts.

Selection Entries:
The attributes that are contained in the selection entries describe what to look for in the alert. Each selection entry includes a logical expression that relates the alert attribute to a given value. Once an alert has satisfied a selection entry, the alert is assigned to a group. The group is a character value that the network administrator defines.

Use the Work with Filter Selection Entries (WRKFTRSLTE) command to access all the filter selection entry functions that are available. You can work with a list of filter selection entries to add, change, copy, remove, display, move, or print the selection entries.

Action Entries:
Actions entries are defined by the network administrator as part of the filter object. A **filter object** is an AS/400 object that can be saved and restored. Part of the filtering process defines how the groups that are specified by the selection entries are mapped to the actions that will be taken.

Use the Work with Filter Action Entries (WRKFTRACNE) command to access all the filter action entry functions that are available. You can work with a list of filter action entries to add,

change, copy, remove, display, move, or print the action entries.

Using the Data Queue for Automation: You can use data queues to help you automate responses to alerts. When an alert is created or received by a system, the filter that is used by the alert is set up to send an alert notification record to a data queue. Setting up a filter to send an alert notification message is controlled by the Send Data Queue (SNDDTAQ) parameter on the action entry.

The data queue can be monitored by your own system management application that is designed to automate responses to the alerts. When the alert notification is received by the data queue, the application can use the Retrieve Alert (QALRTVA) API to retrieve the alert from the alert database. Once the alert is retrieved, the application can do further processing that is required. Refer to the *System API Reference* book for more information on the QALRTVA API.

Are There Any Design Tips for Alerts?

The following are design tips that help you get the most out of alert support.

- Do not send alerts and high priority data on the same link because this causes alert throughput to decrease.

- Try to evenly distribute the number of alerts that are sent or received by a given system to prevent a delay in the logging of alerts.

- Because a large sphere of control requires significant processing time to re-establish a session, use nested focal points to reduce the size of the sphere of control of a focal point.

- Try not to use default focal points. Because the default focal point tries to oversee the entire network, additional processing time is needed whenever a node reenters the network because the default focal point tries to get a session to the reentered node.

- If a default focal point is needed, each network should only have one. More than one default focal point in the network provides no additional benefits and causes additional

system expense as default focal points compete for a new system.

- If you never want a message to be alertable, change the message descriptor so that the alert is not created rather than being filtered out. This saves processing time because the alert is never created and is therefore never filtered out. (Do this in a CL program the next time the operating system is installed so that the message descriptors are re-assigned their default values.)

- Try to automate alerts as much as possible at the entry point system so that the alerts do not have to flow to the central site.

What Are Some Ways to Use Alerts?

The following scenarios describe ways in which to use alerts.

Setting up a Simple Environment—Scenario

Figure 1-1 on page 1-10 shows an example of a simple alert environment. The simple alert environment has a primary focal point and two network nodes under the primary focal point's sphere of control.

NN1 is the primary focal point and has network nodes NN2 and NN3 under its sphere of control. NN1 is the primary focal point where all the skilled support people are located.

All end nodes (ENnn), by default, forward their alerts to their network node servers (NNn). The NNn forwards the alerts to NN1.

Because this is a simple alert environment, no backup focal point is needed.

Note: A network node server does not have to be defined as a focal point to receive alerts from an end node.

Expanded Example of Setting up a Simple Environment: Figure 1-2 on page 1-11 contains an expanded example of a simple environment.

In this example, the office system is at the central site because the central site has the expertise of City1. The central site has the lowest workload of all the systems. All other systems, except for some of the production systems, are under the office system's sphere of control. Only one production system is under the office system sphere of control. That production system is the focal point for all other production systems. The problems are handled by experts at the production site.

One of the shipping and distribution systems is the backup focal point. It is also the backup focal point for the rest of the system.

An end node needs to be defined under a focal point sphere of control when the end node network node server belongs to a different sphere of control. For example, if the shipping system is an end node at City3, then the shipping system needs to be added to the office system sphere of control.

Setting Up Alert Filters for a Network—Scenario

Figure 1-3 on page 1-12 shows an example network with four AS/400 systems. The STLOUIS system is the focal point, with SEATTLE, CHICAGO, and ATLANTA as entry point systems in the STLOUIS system sphere of control. The network administrator decides that all alerts for all systems should be sent to the focal point system. Because the operator who works on the CHICAGO system is an expert in resolving tape problems, however, all tape-related alerts for all systems should be sent to CHICAGO.

The network administrator uses the Change Network Attributes (CHGNETA) command to designate STLOUIS as the alert primary focal point system. The network administrator at STLOUIS uses the Work with Sphere of Control (WRKSOC) command to set up the sphere of control. The sphere of control includes the nodes from which STLOUIS receives alerts. In this example, the entry point systems SEATTLE, CHICAGO, and ATLANTA send their alerts to STLOUIS.

SEATTLE is an attended test system. All alerts are sent to the focal point STLOUIS. ATLANTA is an unattended system. As there is no operator
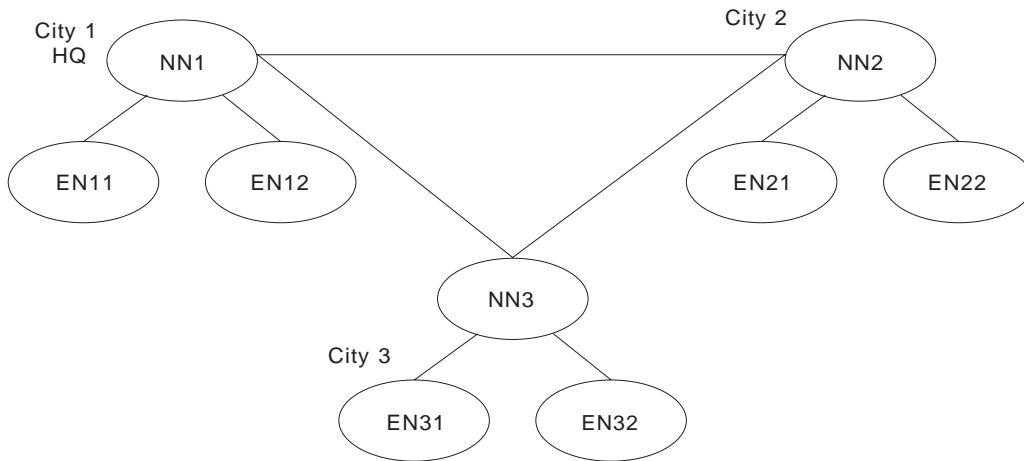
RV3W300-1

Figure 1-1. Example of a Simple Alert Environment

who works on the ATLANTA system, all alerts are sent to STLOUIS. Tape alerts from both SEATTLE and ATLANTA are sent to CHICAGO.

The CHICAGO system is attended by an operator who specializes in tape problems. Therefore, all tape-related alerts from SEATTLE, ATLANTA, and STLOUIS are received by CHICAGO. The operator most qualified to handle the tape errors can work on all tape problems for the network. All CHICAGO alerts are sent to the focal point STLOUIS for processing.

The operators at STLOUIS work on all alerts from all systems in the network, except for tape alerts. All tape alerts are sent to CHICAGO where they are processed.

To set up the most efficient way to route and process the alerts, the network administrator decides to add filters to the network.

Simple Monitoring—Scenario

The following scenario provides an example on how valuable alerts can be. Suppose that you want to monitor a remote system without depending on a remote system operator. The following example sends a message from a remote site to your central site every 15 minutes:

```
PGM

LOOP:   SNDPGMMSG  MSGID(CPI9805) MSGF(QCPFMSG) TOUSR(*SYSOPR)
        DLYJOB     DLY(900)
        GOTO LOOP

ENDPGM
```

By adding a few more lines of code, this program can become a more sophisticated program that can report on current performance and other critical system information.

For example, you can create an automation program that sends an alert 30 minutes with the processing unit utilization embedded in the message.

City 1
HQ
accounting
systems

City 2
accounting system

office
system

shipping and distribution
system

shiipping and distribution
system

City 3
shipping
system
production systems
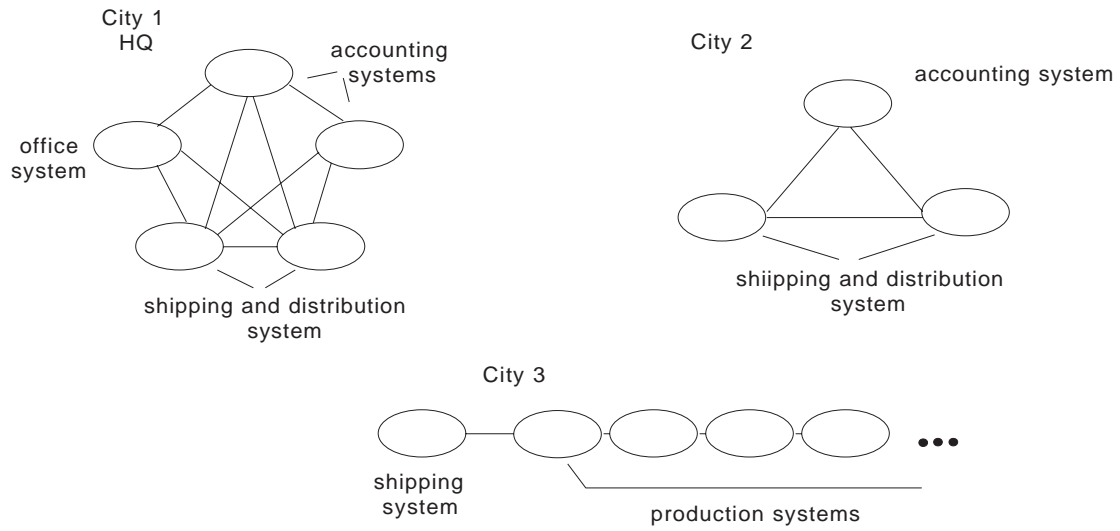
RV3W301-1

Figure   1-2. Expanded Example of a Simple Alert Environment.   This example shows the network nodes because the end nodes always send their alerts to their network node server.

Sphere of
Control

SEATTLE
CHICAGO
ATLANTA

STLOUIS
AS/400 System

Focal Point

ALRSTS(*ON)

ALRLOGSTS(*ALL)

SEATTLE
AS/400 System

Entry
Point

ALRSTS(*ON)

ALRLOGSTS(*LOCAL)

Test System

CHICAGO
AS/400 System

Entry
Point

ALRSTS(*ON)

ALRLOGSTS(*ALL)

Tape Operator
(TAPEOPR)

ATLANTA
AS/400 System

Entry
Point

ALRSTS(*UNATTEND)

ALRLOGSTS(*NONE)

Legend:

———————▶   All Alerts

- - - - - ▶   TAP* Alerts Only
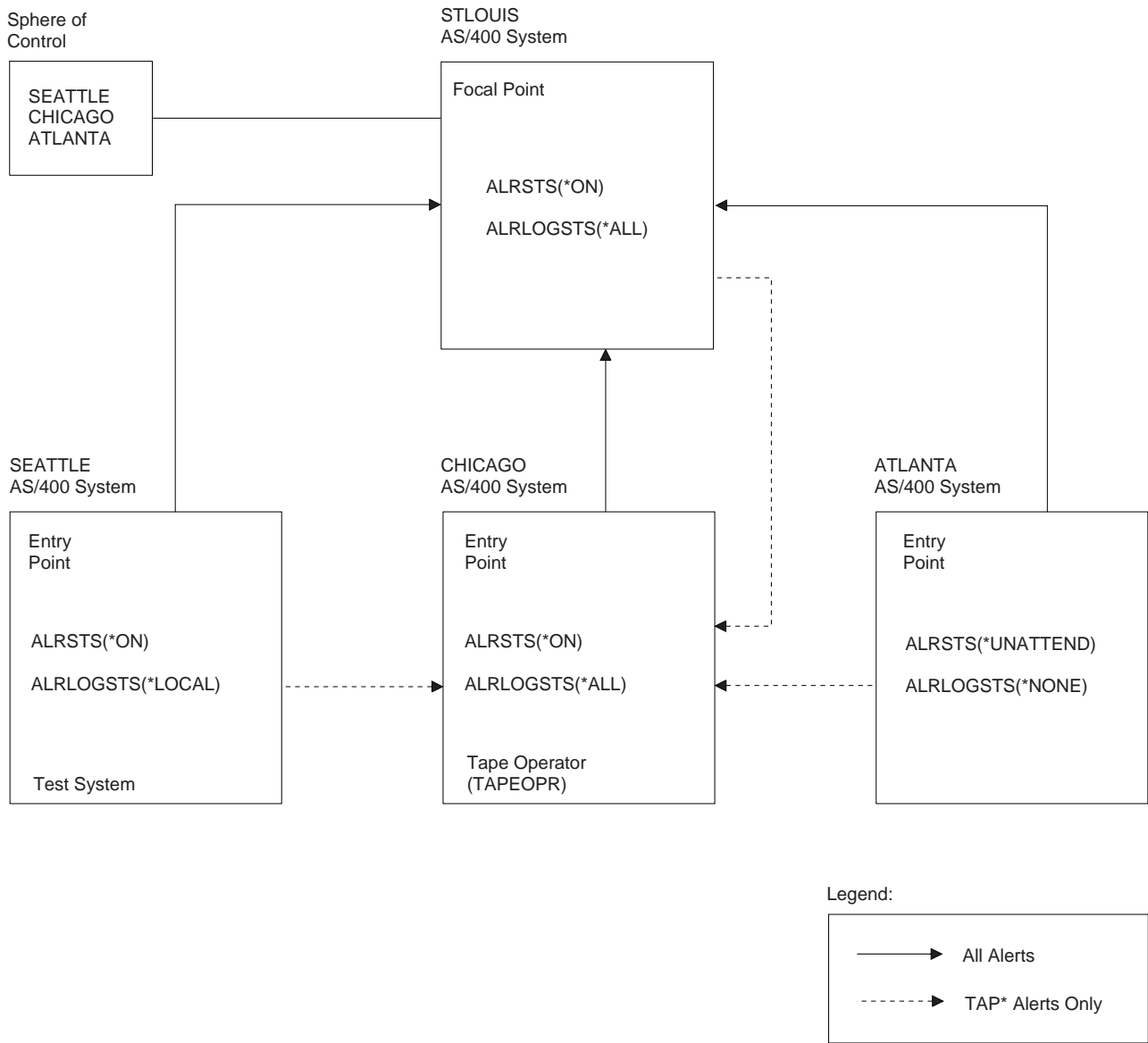
RV2P905-1

Figure   1-3. Example of an Alert Network with an Alert Filter

```
PGM

        /* VARIABLES FOR QWCRSSTS API */
        DCL        VAR(&RCVLENGTH); TYPE(*CHAR) LEN(4)
        DCL        VAR(&RECEIVER); TYPE(*CHAR) LEN(36)
        DCL        VAR(&FORMAT);    TYPE(*CHAR) LEN(8)
        DCL        VAR(&RESET);     TYPE(*CHAR) LEN(10)
        DCL        VAR(&ERRORCODE); TYPE(*CHAR) LEN(4)

        /* WORKING VARIABLES */
        DCL        VAR(&CPU);       TYPE(*DEC)  LEN(4 0)
        DCL        VAR(&CPUTEXT);   TYPE(*CHAR) LEN(4)
        DCL        VAR(&MSGDATA);   TYPE(*CHAR) LEN(30)

        /* SETUP FOR CALLING QWCRSSTS */
        CHGVAR     VAR(&RCVLENGTH); VALUE(X'00000024')
        CHGVAR     VAR(&FORMAT);    VALUE('SSTS0200')
        CHGVAR     VAR(&ERRORCODE); VALUE(X'00000000')

        /* FIRST CALL RESETS STATISTICS TO ZERO */
LOOP:   CHGVAR     VAR(&RESET);     VALUE('*YES     ')
        CALL       PGM(QWCRSSTS)  PARM(&RECEIVER +
                                  &RCVLENGTH +
                                  &FORMAT    +
                                  &RESET     +
                                  &ERRORCODE);

        /* WAIT FOR 5 SECOND INTERVAL */
        DLYJOB     DLY(5)

        /* GET THE CURRENT SYSTEM STATISTICS */
        CHGVAR     VAR(&RESET);     VALUE(*NO)
        CALL       PGM(QWCRSSTS)  PARM(&RECEIVER +
                                  &RCVLENGTH +
                                  &FORMAT    +
                                  &RESET     +
                                  &ERRORCODE);

        /* PULL OUT THE CPU UTILIZATION, RETURNED AS A BINARY */
        /* NUMBER IN TENTHS                                   */
        CHGVAR     VAR(&CPUTEXT);   VALUE(%SUBSTRING(&RECEIVER 33 4))
        CHGVAR     VAR(&CPU);       VALUE(%BINARY(&CPUTEXT));
        CHGVAR     VAR(&CPUTEXT);   VALUE(&CPU);
        CHGVAR     VAR(&MSGDATA);   VALUE('      CPU at: '    +
                                  *CAT %SUBSTRING(&CPUTEXT 1 3) +
                                  *CAT '.'                     +
                                  *CAT %SUBSTRING(&CPUTEXT 4 1))

        /* SEND THE ALERTABLE MESSAGE */
        SNDPGMMSG MSGID(CPI9805) MSGF(QCPFMSG)   +
                                  MSGDTA(&MSGDATA); +
                                  TOMSGQ(*SYSOPR)

        /* WAIT 30 MINUTES AND DO IT AGAIN */
        DLYJOB     DLY(1800)
        GOTO       CMDLBL(LOOP)

ENDPGM
```

What Do I Need to Consider When I Configure My System/36 or System/38 for Alerts?

You can configure your System/36 or System/38 for alerts by using an alert controller session. When you use the alert controller session, the OS/400 alert support establishes the switched connection and sends the alert to the alert's focal point. You must make sure that the controller description has been varied on and that an APPC device exists for that controller description. The alert support attempts to establish the switched connection by using the first APPC device that is found for the controller description. The APPC device is used to establish the switch connection. The APPC device is not used to establish an APPC conversation.

Other Alert Support Issues for a System/36 or a System/38

The following are other issues that you need to know when you are supporting alerts on either a System/36 or a System/38:

- You can use your System/36 and System/38 for alert forwarding. Although System/36, System/38, or AS/400 can be downstream systems, forward your alerts to an AS/400 system where possible to take advantage of the management services sessions capabilities.

- System/36 alert support uses an APPC or APPN subsystem to send alerts either to a host system or to another system that is capable of receiving alerts.

  System/38 alert support uses a system services control point-physical unit (SSCP-PU) session to send alerts either to a host system or to another system that is capable of receiving alerts.

- On the System/36, you can use the ALERT procedure to create a predefined subset of system messages that control the creation of alerts. You can also use the SETALERT procedure to create alerts for any System/36 user-defined error message.

  On the System/38, you can use the alert status (ALRSTS) network attribute to control the creation of alerts.

- On the System/36, you can use the disk file (ALERTFIL) to log any received alerts or locally generated alerts.

  On the System/38, you can use the journal (QALERT in library QUSRSYS) to log any received alerts or locally generated alerts.

- To start System/36 alert support, you must use the ENABLE procedure command to enable the APPC or APPN subsystem. Alert generation is started once the subsystem that specifies the alert location is enabled.

- An alertable message on System/38 is any message with an alert ID other than *NONE. System/38 sends an alert when such a message is sent to the QSYSOPR message queue.

Are There Other Ways to Analyze My Alerts?

The system operator is made aware of problems locally by messages that are sent to the QSYSOPR message queue. Some of these messages have problem analysis procedures associated with them that are run locally by the system operator. You can set up your network so that you can perform problem analysis in the following ways:

- At the reporting location.

- At the problem management focal point. The **problem management focal point** is the management services session responsible for the problem analysis and diagnosis for a sphere of control.

You can also analyze your alerts by using the following commands:

- Work with Problems (WRKPRB)

- Work with Alerts (WRKALR)

- Analyze Problem

Work with Problems Command

After viewing the message and any associated messages found in QSYSOPR, the system operator runs the WRKPRB command. This command provides a list of possible causes and the percentage probability of the causes. Based on this information, the operator can create a service request if required.

Work with Alerts Command

The central site operator can use the Work with Alerts (WRKALR) command to display problems at remote sites. The information that is provided in the alert may be sufficient to solve the problem. However, there may be occasions when additional

problem analysis is needed. One possible action is to use problem analysis at the site that is experiencing the problem. Messages that have problem analysis procedures shipped with the system have the log problem (LOGPRB) parameter in the message description that is set to *YES. Problem analysis for this message is started by pressing F14 when the cursor is on the message.

Analyze Problem Command

Use the Analyze Problem (ANZPRB) command for those problems that are not supported by problem analysis. Besides problem analysis, the ANZPRB command is also used to report on a problem. ANZPRB is used to analyze or report:

- Job or programming problems

- Equipment or communications problems

- Problems that made it necessary to do an initial program load (IPL) of the system again

- Problems on a device or system that is not attached to the local system

The ANZPRB command takes an operator through a series of questions and checklists to isolate the problem. During analysis, additional testing that uses the Verify Communications (VFYCMN) command may be performed. At the end of ANZPRB command, either an alert is generated or a service request is prepared.

Where Can I Find More Information?

You can find additional information in Part 2 and Part 3 of this book. More specifically, the Table 1-1 on page 1-15 points you to the next level of information on subjects that are covered in this part of the *Alerts Support* book.

Table 1-1. References to More Information.

Subject	Where to Find More Information
Implementing examples	Appendix A, "Sample Procedures for OS/400 Alerts" on page A-1
Focal points	"Alert Network Attributes" on page 2-4
Sphere of control	"The Sphere of Control" on page 2-7
Nested focal point	"Nested Focal Points" on page 2-11
Configuring your AS/400 system for alerts	"AS/400 Configuration" on page 2-3
Creating alerts	"OS/400 Alerts" on page 3-1
Displaying alerts	"Working with Alerts" on page 3-13
Management services session or alert controller session	"Configuring Your Network for Alerts" on page 2-1
Defining your own alerts	"Application-Generated Alerts" on page 3-7
Filtering	Chapter 4, "OS/400 Alert Filter Support" on page 4-1
Selection entries	"Selection Entries" on page 4-1
Action entries	"Action Entries" on page 4-1
Differences in System/36 and System/38 alert support	Appendix C, " Alerts Differences" on page C-1.

Chapter 2. Setting Up OS/400 Alert Support

This chapter describes how to set up your network and your system to use OS/400 alert support.

Configuring Your Network for Alerts

You can configure your network for problem management using the advanced program-to-program communications/advanced peer-to-peer networking (APPC/APPN) support on the AS/400 system.

If you use APPC/APPN support, you can control your system as an alert focal point using the sphere ofcontrol functions. An **alert focal point** is the system in a network that receives and processes alerts. Optional alert focal point functions include logging, displaying, and forwarding alerts. See "The Sphere of Control" on page 2-7 for information about the sphere of control. See "Management Services Session" for information about alerts with APPC/APPN support.

If you do not choose to use the APPC/APPN support, or if you are connecting your AS/400 system to a system that does not support APPC/APPN for alerts, you cannot use the sphere of control functions. See "Alert Controller Session" on page 2-2 for information about alerts without APPC/APPN support.

The sphere of control specifies the systems from which your AS/400 system receives alerts. If you are sending your alerts to a system that does not provide APPC/APPN support for alerts, you can specify a focal point system to which your AS/400 system sends alerts using the network attributes. See "Network Attributes for Alerts" on page 2-4 for information about network attributes.

See the *APPC Programming* and *APPN Support* books for more information about APPC and APPN support.

Sessions Used for Alert Support

When you use the alert support, sessions are established between an alert focal point and systems that create and send alerts. The type of session that is used depends on whether APPC/APPN support is used. If you use APPC/APPN support, then use the management services session. If you do not use APPC/APPN support, then use the alert controller session.

Management Services Session: If you use APPC/APPN support, the focal point system establishes a control point session with systems defined in the focal point's sphere of control. This session is used to exchange data known as **management services capabilities**. These capabilities are needed for the sphere of control functions. In this book, these sessions are called **management services sessions**. The management services session is also used for sending alerts to a focal point.

Alerts flow between network nodes on the SNASVCMG reserved mode session. Alerts flow between a network node and an end node on the CPSVCMG reserved mode session.

The AS/400, System/390, and System/370 systems support management services sessions. These sessions can be configured to any system in an APPN network.

Systems that do not support management services capabilities include:

- System/38
- System/36

You cannot define these systems in your sphere of control. If you want these systems to send alerts to your AS/400 system, you must configure those systems to send their alerts to your AS/400 system. Refer to the alerts chapter of the *C & SM User's Book* for the System/36 and to the *Data Communications Programmer's* book for the System/38. After this configuration has been done, then the System/36 or the System/38 can send alerts to your AS/400 system.

Note: Your AS/400 system does not have to be defined as a focal point to receive alerts from systems that do not support management services sessions for alerts. This is because these systems cannot be added to the sphere of control. If the alert logging status (ALRLOGSTS) network attribute is set to *RCV or *ALL, all alerts that are received by the AS/400 system are logged in the alert database.

Alert Controller Session:

If you want your AS/400 system to send alerts without using APPC/APPN support (management services sessions), you can define a system to which your AS/400 system sends alerts using the **alert controller description** (ALRCTLD)network attribute. This description defines the system to which alerts will be sent on an alert controller session. In this book, the session using the alert controller description is called the **alert controller session**.

This session does not support the management services capabilities, so you cannot use the sphere of control functions. You define the name of a controller description on your AS/400 system to be used for sending alerts. It is the responsibility of the receiving system to be able to handle the alerts that are received from the sending system.

Note: It is recommended that you use the APPC/APPN support with the sphere of control in a network of AS/400 systems. You should only use the alert controller session when the receiving system does not support management services sessions (for example, on a System/38 system or when using a switched link).

Transporting Alert Data:

Alerts move through a network to the focal point as a control point management services unit (CP-MSU) on a management services session. CP-MSUs are also used to exchange management services capabilities for sphere of control support.

Alerts flow as a network management vector transport (NMVT) on the alert controller session. The *SNA Formats* book has more information on the alert architecture and the alert transport.

Record-formatted maintenance statistics (RECFMS) is an alert format that has been

replaced by the NMVT and CP-MSU formats. The AS/400 system discards any alerts that it receives in RECFMS format.

Table 2-1 shows the ability of some of the systems eligible to send and receive alerts during a session.

Table 2-1. Systems that Support Alerts

	Receive		Send	
System	**CP-MSU**	**NMVT**	**CP-MSU**	**NMVT**
AS/400 system	X	X	X	X
System/36		X		X
System/38		X		X
System/370	X	X	X	
System/390	X	X	X	
OS/2* system	X		X	
3174				X

An Example Network

Figure 2-1 on page 2-3 shows an example network with AS/400 systems, a System/36, a System/38, and a System/370 or System/390 system.

The primary focal point system for this network is CHICAGO. By specifying *YES for the alert primary focal point parameter (ALRPRIFP=*YES) on the Change Network Attributes (CHGNETA) command, CHICAGO has been defined to be a primary focal point. The network operator at CHICAGO sets up the sphere of control using the Work with Sphere of Control (WRKSOC) command to include the nodes from which CHICAGO receives alerts. In this example, MILWKEE and DENVER have been included in CHICAGO's sphere of control. Both of these systems send their alerts to CHICAGO.

System/36 and System/38 do not support management services sessions for sending alerts. System/36 ATLANTA has been configured to send its alerts to CHICAGO. See the System/36 cit*C & S M User's Book* for more information about using alerts on the System/36. System/38 STPAUL has been configured to send its alerts to MILWKEE. MILWKEE then forwards alerts received from STPAUL to the focal point at CHICAGO. See the System/38 *Data Communications Programmer's*

book for more information about using alerts on the System/38.

In this example, OMAHA is an APPN end node. End nodes may participate in an APPN network by using the services of an attached network node (the serving network node). DENVER is the serving network node for OMAHA. An end node sends its alerts to its focal point through its serving network node. The alerts sent by OMAHA are forwarded by DENVER to the focal point at CHICAGO.

CHICAGO has been configured to send alerts to a higher level focal point, which is the NetView program running on a System/370 NEWYORK system. CHICAGO has also been configured to use an alert controller session by specifying NEWYORK for the alert controller description (ALRCTLD) parameter on the CHGNETA command.

AS/400 Configuration

You configure your system communications capabilities for network problem management with the configuration menus or the control language commands supplied with the AS/400 system. The configuration requirements are discussed in the *APPN Support* and the *Communications Configuration* book.
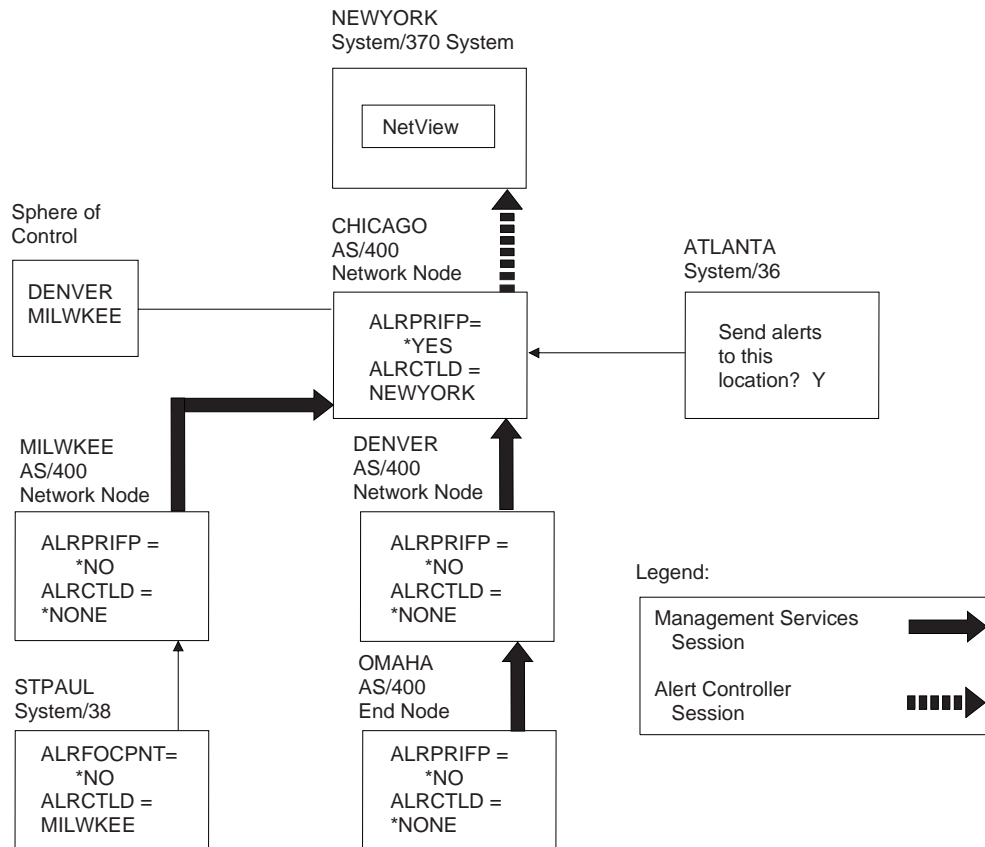
The following commands are used to create or change line descriptions:

To display the current create or change line description commands, execute the following command:

go cmdlin

To display the current create or change controller description commands, execute the following command:

go cmdctl

Figure 2-1. An Example Network for Alerts

If you rename a controller description, you should verify that it matches the controller name in the ALRCTLD parameter in the Change Network Attribute (CHGNETA) command.

If you are creating a controller description to use for management services sessions, the controller must support control point-to-control point sessions (CPSSN(*YES) on the create controller command).

To display the current create or change device description commands, execute the following command:

go cmddev

Note: You may not need to create a device description if you are using APPN. See the *APPN Support* for details on when APPN automatically creates a device description.

Network Attributes for Alerts

You can define your AS/400 system to be a focal point using the OS/400 network attributes. You can also control other alert functions using the network attributes.

You change the network attributes using the Change Network Attributes (CHGNETA) command. You can display the current values of the network attributes using the Display Network Attributes (DSPNETA) command.

Alert Network Attributes: The following alert functions are controlled by network attributes:

- Alert status
- Alert logging status
- Alert primary focal point
- Alert default focal point
- Alert backup focal point
- Alert focal point to request
- Alert controller description
- Alert hold count
- Alert filter

The following parameters for OS/400 alert support are supported by the Change Network Attributes (CHGNETA) command.

ALRSTS Parameter
Specifies whether local alerts are generated by the system.

*ON: The system generates alerts for all alert conditions except unattended conditions.

*UNATTEND: The system generates alerts for all alert conditions including those that have the alert type in the alert option parameter of the message description set to *UNATTEND.

*OFF: Alerts are not generated by the system.

See "OS/400 Alerts" on page 3-1 for more information about the alert options and the OS/400 message description.

ALRLOGSTS Parameter
Specifies how alerts are logged by the AS/400 system.

<u>*SAME:</u> The status of alert logging does not change.

*NONE: No alerts are logged.

*LOCAL: Only locally generated alerts are logged.

*RCV: Only alerts from other systems are logged.

*ALL: Both locally generated alerts and alerts received from other systems are logged.

ALRPRIFP Parameter
Specifies whether the system is an alert primary focal point. If the system is defined as a primary focal point, alerts are received from all nodes explicitly defined in the sphere of control. This parameter also allows the system to be a backup or requested focal point.

<u>*SAME:</u> The status of the alert primary focal point does not change.

*NO: The system is not an alert primary focal point.

*YES: The system is defined as an alert primary focal point and it provides focal point services to all systems in the network that are explicitly defined in the sphere of control. If a system is defined as a focal point, ALRLOGSTS(*ALL) or ALRLOGSTS(*RCV) should be specified to ensure that alerts coming in from nodes in the sphere of control are logged.

ALRDFTFP Parameter

Specifies whether the system is a default alert focal point. If the system is defined as a default alert focal point, alerts are received from all network systems not explicitly defined in the sphere of control of some other focal point system within the network.

*SAME: The default alert focal point does not change.

*NO: The system is not a default alert focal point.

*YES: The system is a default alert focal point and it provides focal point services to all network systems that are not being serviced by either a primary focal point or another default focal point. If a system is defined as a default focal point, the NODETYPE(*NETNODE) must be specified.

ALRBCKFP Parameter

Specifies the name of the system that pro-vides alert focal point services to the nodes in the sphere of control if the local system is unavailable.

*SAME: The backup focal point definition does not change.

*NONE: The backup focal point is not defined.

Element 1: Network ID

*LCLNETID: The network ID of the backup focal point is the same as that of the local system.

network-ID: Specify the network ID of the system that provides backup focal point ser-vices for alerts.

Element 2: Control Point Name

control-point-name: Specify the control point name of the system that provides backup focal point services for alerts.

This parameter is used on focal point systems (ALRPRIFP=*YES). The parameter is shipped with an initial value of *NONE. The validation rules are the same as that of the local network ID and control point name. If *LCLNETID is specified, the current value for LCLNETID will be stored in network attributes. Network IDs and control point names are CHAR(8) vari-ables.

ALRRQSFP Parameter

Specifies the name of the system that is requested to provide focal point services. If a focal point is already defined for the entry point, it will be revoked when the new focal point is requested.

*SAME: Do not change focal point to request.

*NONE: A focal point is not requested.

Element 1: Network ID

*LCLNETID: The network ID of the requested focal point is the same as that of the local system.

network-ID: Specify the network ID of the system that is requested to provide focal point services for alerts.

Element 2: Control Point Name

control-point-name: Specify the control point name of the system that is requested to provide focal point services for alerts.

This parameter is used on entry point systems. The parameter is shipped with an initial value of *NONE. The validation rules are the same as that of the local network ID and control point name. If *LCLNETID is specified, the current value for LCLNETID will be stored in network attributes. Network IDs and control point names are CHAR(8) variables.

ALRCTLD Parameter

Specifies the name of the controller through which alerts are sent on the alert controller session. Only a host or APPC controller may be specified. The controller must be varied on for alert processing to be operational on the alert controller session, although it does not need to be varied on when the CHGNETA command is used.

*SAME: The name of the alert controller does not change.

*NONE: No alert controller is described. Spec-ifying ALRSTS(*ON) with *NONE for the con-troller description means that local alerts are created, but are not sent out on the alert con-troller session.

controller-description: Specify the name of the controller being used for alerts on the alert controller session. This controller is ignored if the system has a focal point (for example, if

the system is in another system's sphere of control).

ALRHLDCNT Parameter

Specifies the maximum number of alerts that are created before the alerts are sent over the alert controller session.

*SAME: The hold alert count network attribute does not change.

*NOMAX: The current alert hold count is the maximum value. All alerts are held indefinitely until the ALRHLDCNT alert hold count value is changed to a lower value.

alert-hold-count: Specify the maximum number of alerts that can be created before being sent. Alerts are held until the threshold number is reached.

ALRFTR Parameter

Specifies the alert filter that is used when alerts are processed.

*SAME: The alert filter does not change.

*NONE: No alert filter is active.

Element 1: Filter Name

name: Specify the name of the alert filter that is used when alerts are processed.

Element 2: Library

*LIBL: The library list is used to locate the filter name.

*CURLIB: The current library for the job is used to locate the filter name.

library-name: Specify the name of the library where the alert filter is located.

Note: You should only use the ALRCTLD network attribute to send alerts to systems that do not support management services sessions for alerts. These systems include:

- System/36
- System/38

If an AS/400 system is a primary focal point, it is implicitly in its own sphere of control if it does not have a higher level primary focal point of its own. A primary focal point never sends its alerts to a default focal point.

See the *APPN Support* for information on the node type (NODETYPE) network attribute.

Primary Focal Point: When the ALRPRIFP parameter is changed from *NO to *YES, the system receives alerts from nodes that are defined in this system's sphere of control.

To specify your system as a primary focal point, type the following:

```
CHGNETA ALRPRIFP(*YES) ALRLOGSTS(*ALL)
```

This indicates you want your system to be a primary focal point, and you want the system to log all alerts.

The ALRPRIFP parameter can be changed from *YES to *NO even if there are systems in the sphere of control that are currently sending alerts to your focal point system. Focal point services will still be provided for the systems; however, no new services will be added and retries will not be done. This is to ensure that all systems in the network are served by a focal point at all times.

The recommended method of changing the ALRPRIFP network attribute from *YES to *NO is as follows:

1. Define another system in the network to be a primary focal point.

2. The network operator at the new focal point should add all of the systems named in your focal point's sphere of control into the new focal point's sphere of control.

3. The new focal point takes over as focal point for the systems defined in your sphere of control.

4. Change the ALRPRIFP parameter from *YES to *NO.

See "The Sphere of Control" on page 2-7 for more details.

Requested Focal Point: When the ALRRQSFP parameter is changed to a network ID and a control point name, the system requests that that control point provide focal point services. This parameter should be used whenever the entry point is responsible for retries. For example, your system could have a switched line to the

focal point, and you want the line connected only when you have data to send.

The system can request focal point services from any control point with which it can communicate. However, the requested focal point must specify ALRPRIFP(*YES) if it is an AS/400 system. You can end focal point services by changing the ALRRQSFP parameter for that system to *NONE.

See "The Sphere of Control" for more details.

Backup Focal Point: When the ALRBCKFP parameter is changed from *NONE to a network ID and a control point name, the system specifies that that control point provide focal point services if the primary focal point is unavailable.

Only a focal point system, ALRPRIFP(*YES), can specify a backup focal point. However, the specified backup focal point must specify ALRPRIFP(*YES) if it is an AS/400 system. The backup focal point does not need to specify any nodes in the sphere of control.

See "The Sphere of Control" for more details.

Default Focal Point: When the ALRDFTFP parameter is changed from *NO to *YES, the system receives alerts from network nodes in the network that are not already sending alerts to another focal point, or network nodes currently sending alerts to a default focal point.

The ALRDFTFP parameter can be changed from *YES to *NO even if there are systems in the sphere of control that are currently sending alerts to your focal point system. Focal point services will still be provided for the systems; however, no new services will be added and retries will not be done. This is to ensure that all systems in the network are served by a focal point at all times.

The recommended method of changing the ALRDFTFP network attribute from *YES to *NO is as follows:

1. Define another system in the network to be a primary focal point.

2. The network operator at the new focal point should add all of the systems named in your focal point's sphere of control into the new focal point's sphere of control.

3. The new primary focal point takes over as focal point for the systems defined in your sphere of control.

4. Change the ALRDFTFP parameter from *YES to *NO.

See The Sphere of Control for more details.

Serving Network Node for an End Node: An end node sends its alerts to the same focal point as its serving network node. To determine the serving network node:

- The network node must be specified as a serving network node in the network attributes of the end node.

- As many as five serving network nodes can be set up in the network attributes of the end node, but the first link to a serving network node that is activated determines the actual serving network node.

Since end nodes learn their focal point from their network node, end nodes do not have to be in a sphere of control. If an end node is in the sphere of control of a focal point, it sends alerts to that node instead of to the focal point learned from the serving network node.

Note: The serving network node cannot be a System/36 network node. To send alerts to System/36, the alert controller session must be defined (using the ALRCTLD network attribute).

See the *APPN Support* for more information.

The Sphere of Control

The sphere of control defines the set of control points that send alerts to your system as a focal point.

When your system is defined to be a primary focal point, you must explicitly define the control points that will be in your sphere of control. This set of control points is defined using the Work with Sphere of Control (WRKSOC) command. You can work with this command by doing one of the following:

- Type the Work with Sphere of Control (WRKSOC) command from the command line.

- Choose option 6 (Communications) from the AS/400 Main Menu, option 5 (Network management) from the Communications menu, and option 4 (Work with sphere of control (SOC)) from the Network Management menu.

When your system is defined to be a default focal point, the AS/400 system automatically adds network node control points to the sphere of control using the APPN network **topology**[1] database. When the AS/400system detects that a network node system with the same network ID as the local system has entered the network, the system sends management services capabilities to the new control point so that the control point sends alerts to your system.

A default focal point becomes a focal point only for systems that do not already have a non-default focal point. If a system already has an active non-default focal point, then your request to be a default focal point is rejected.

The purpose of a default focal point is to prevent the situation where a system in the network does not have any focal point at all. You should define your focal point systems as primary focal points. It is recommended that if you define a default focal point, you define only one system in the network to be a default focal point.

You can use the Add Sphere of Control Entry (ADDSOCE) command to add systems to the alert sphere of control. You can use the Remove Sphere of Control Entry (RMVSOCE) command to delete systems from the alert sphere of control. The systems are specified by network ID and control point name.

The Display Sphere of Control Status (DSPSOCSTS) command shows the current status of all systems in your sphere of control. This includes systems that you have defined using the Work with Sphere of Control (WRKSOC) command (if your system is defined as a primary focal point), and systems that the AS/400system has added for you (if your system is defined as a requested, backup, or default focal point). You can work with this command by doing one of the following:

- Type the Display Sphere of Control Status (DSPSOCSTS) command from the command line.
- Choose option 6 (Communications) from the AS/400 Main Menu, option 5 (Network management) from the Communications menu, and option 3 (Display sphere of control (SOC) status) from the Network Management menu.

Working with the Sphere of Control

The Work with Sphere of Control (WRKSOC) command allows you to add control point systems to the sphere of control and to remove existing control points.

Note: Products, such as the System/38 or System/36, that do not support management services for sending alerts, should not be defined in the sphere of control. For information on sending alerts from System/36, refer to the alerts chapter of the System/36 *C & S M User's* book. For information on sending alerts from System/38, refer to the System/38 *Data Communications Programmer's* book.

```
                Work with Sphere of Control (SOC)
                              System:   ROCHESTR  Position to
. . . . . . . .          Control Point    Network ID . . . . . . . .
              Type options, press Enter.   1=Add  4=Remove        Control
Opt  Point     Network ID  Current Status            *NETATR_   
CHICAGO1  APPN       Remove pending  _   CHICAGO2   APPN       Revoked
  _  MILWKEE    APPN      Active   _  MPLS      MINNSTA    Add pending
  _  STLOUIS    MINNSTA   Active

                                    Bottom  F3=Exit   F4=Prompt   F5=Refresh
  F9=Command    F10=Display SOC status  F11=Display new focal points
F12=Cancel    F16=Repeat position to
```

Figure   2-2. Work with Sphere of Control

The following values are possible for `Current Status`:

Active
　Your system is actively providing focal point services for the indicated control point.

Add pending
　When a control point has been added, there is a delay while focal point services are started for that control point. Your system is currently trying to establish a session with the control

---

[1] In the Systems Network Architecture concept, the schematic arrangement of the links and nodes of a network.

point so that it can provide focal point services.

Inactive

Your system is not currently providing focal point services for the indicated control point. The control point cannot communicate with your system now because of a lost connection. If a control point with this status is removed from your system's sphere of control, it is not displayed.

Never active

Your system has never provided focal point services for the indicated control point. The control point has never sent alerts to your system. If a control point with this status is removed from your system's sphere of control, it is not displayed.

Rejected

The indicated control point does not require focal point services from your system. It is likely that the control point has a different focal point. If a control point with this status is removed from your system's sphere of control, it is not displayed.

Remove pending

Your system is providing focal point services, but a user has removed the control point from the sphere of control. The control point is removed from the sphere of control when another system starts focal point services for the control point or the session is lost.

Revoked

The indicated control point is no longer in your system's sphere of control. A new focal point is now providing focal point services for the control point. The new focal point is identified in the *New Focal Point* column. Press F11 to display new focal points. If a control point with this status is removed from your system's sphere of control, it is not displayed.

The *CL Reference* book contains more information about the WRKSOC command.

Adding a System to the Sphere of Control: On the Work with Sphere of Control (SOC) display, you can use option 1 (Add) to add a system to your sphere of control.

You can also use the Add Sphere of Control Entry (ADDSOCE) command to add systems to the alert sphere of control.

To add a system to the sphere of control, type the **control point name** and the **network ID** of the system. For the AS/400 system, these are the local control point name (LCLCPNAME), and the local network ID (LCLNETID) network attributes of the system you wish to add to the sphere of control.

When you add a control point to the sphere of control, and your system is defined to be a primary focal point, the AS/400 system sends management services capabilities to the new control point so your AS/400 system can be a focal point for that system. This results in one of the statuses described in "Working with the Sphere of Control" on page 2-8 being displayed.

If you use option 1 (to add a control point name), but do not enter the name, you will see the following display. If you use option 1 and enter the name on the Work with Sphere of Control display, the system is added.

```
                    Add Sphere of Control Entry
                                              System:   ROCHESTR
   Type choices, press Enter

      Network ID . . . . . . . .     *NETATR_
      Control point  . . . . . .     _____
```

Removing Systems from the Sphere of Control: Use option 4 (Remove) from the Work with Sphere of Control display to remove a control point from your sphere of control.

You can also use the Remove Sphere of Control Entry (RMVSOCE) command to remove systems from the alert sphere of control.

A control point in the sphere of control should not be removed from the sphere of control until another focal point has started focal point services to that system. This ensures that a system always has a focal point. When a control point is removed, it goes into a remove pending condition

until an operator at another focal point system adds the control point to its sphere of control, allowing it to act as the focal point for the removed control point, or until the connection to that system is lost.

The recommended method of removing a system from the sphere of control is as follows:

1. Define another system in the network to be a primary focal point.

2. The network operator at the new focal point should add the system you want removed from your sphere of control into the new focal point's sphere of control.

3. The new focal point takes over as focal point for the system that you want to be removed.

4. Wait until the system that you want to remove has a status of `Revoked`.

5. The system can now be removed from your sphere of control.

Displaying the Sphere of Control Status

The Display Sphere of Control Status (DSPSOCSTS) command displays the status of all systems that are currently in your system's sphere of control. This display shows systems you have defined in your sphere of control using the WRKSOC command and also systems the AS/400 system has defined in your sphere of control because your system is a default, requested, and backup focal point for those systems.

```
                                        System:   ROCHESTR
   Position to  . . . . . . . .  _____   Control Point
     Network ID . . . . . . . .  _____

   Type options, press Enter.
     5=Display

        Control               Type of
   Opt  Point    Network ID   Services       Current Status
    _   CHICAGO1  APPN         Primary        Remove pending
    _   CHICAGO2  APPN         Primary        Revoked
    _   MILWKEE   APPN         Primary        Active
    _   MPLS      MINNSTA      Requested      Active
    _   GRNBAY1   NRTHWI       Default        Active
    _   GRNBAY2   NRTHWI       Default        Active
    _   GRNBAY3   NRTHWI       Default        Active
    _   GRNBAY4   NRTHWI       Default        Active
    _   GRNBAY5   NRTHWI       Default        Add pending

   F3=Exit    F5=Refresh     F6=Print    F11=Display new focal points
   F12=Cancel  F16=Repeat position to
```

If the system is currently defined as a focal point (either primary or default), the following values are possible for `Current Status`:

Active
Your system is actively providing focal point services for the indicated control point.

Add pending
When a control point has been added, there is a delay while focal point services are started for that control point. Your system is currently trying to establish a session with the control point so that it can provide focal point services.

Inactive
Your system is not currently providing focal point services for the indicated control point. The control point cannot communicate with your system now because of a lost connection.

Never active
Your system has never provided focal point services for the indicated control point. The control point has never sent alerts to your system.

Rejected
The indicated control point does not require focal point services from your system. It is likely that the control point has a different focal point.

Remove pending
Your system is providing focal point services, but a user has removed the control point from the sphere of control. The control point is removed from the sphere of control when another system starts focal point services for the control point or the session is lost.

Revoked
The indicated control point is no longer in your system's sphere of control. A new focal point is now providing focal point services for the control point. The new focal point is identified in the *New Focal Point* column. Press F11 to display new focal points.

The *CL Reference* book contains more information about the DSPSOCSTS command.

Additional Considerations

The following topics are discussed:

- Nested focal points
- Looping considerations
- Held alerts
- Switched line considerations
- Management services sessions
- Alert controller session
- Alert support through an SNA subarea network
- Interconnected network considerations
- Performance considerations

Nested Focal Points

A nested focal point is a focal point that is defined in the sphere of control of another focal point. A nested focal point forwards all received alerts to its focal point. By nesting focal points, alerts can be concentrated into one system in part of an APPN network and then forwarded.

There are advantages and disadvantages to nesting focal points.

- Advantages
  - A focal point can be configured so that alerts are routed through fewer APPN network nodes between that focal point and the systems in its sphere of control.
  - There are fewer management services sessions at any given system. This distributes focal point processing, such as session establishment and retries among more systems.
- Disadvantages
  - The management for the sphere of control is performed at more than one system.

Looping Considerations

When configuring a network for sending alerts, it is possible to create a looping condition. Figure 2-3 on page 2-12 shows a network where alerts will loop.

SYSA is in the sphere of control of SYSB, SYSB is in the sphere of control of SYSC, and SYSC is in the sphere of control of SYSA. SYSA sends alerts to SYSB, SYSB sends alerts to SYSC, and SYSC sends alerts to SYSA. An alert created at SYSA would be sent through SYSB and SYSC, and would eventually be sent back to SYSA. This alert would be forwarded continuously through these three systems.

The OS/400 alert support provides a way to prevent a looping condition. When a loop is detected, a focal point is revoked to dissolve the loop. The last focal point established, which resulted in the loop, is revoked. For migration concerns about looping conditions, refer to Appendix D, Migration Concerns.

Held Alerts

Held alerts are alerts that could not be sent because of network conditions or the ALRHLDCNT network attribute and are being logged until they can be sent later. Alerts are held only when one of the following is true:

- A focal point has added this system to its sphere of control (a message is sent to this system's QSYSOPR message queue) and contact is established and lost with that focal point since the last initial program load (IPL).
- The NODETYPE network attribute is set to *ENDNODE and contact is established and lost with the serving network node since the last IPL.
- The ALRCTLD network attribute is not set to *NONE and contact is established and lost with this controller since the last IPL.
- The ALRHLDCNT network attribute is set to a value that is greater than 0 and the number of alerts processed is set to a value that is less than the alert hold count. The ALRHLDCNT only applies if the alerts are being sent using an alert controller session.

A message is sent to the QSYSOPR message queue when the system starts to hold alerts. Another message is sent when contact is established again and alerts can be sent. For migration concerns about held alerts, refer to Appendix D, Migration Concerns.
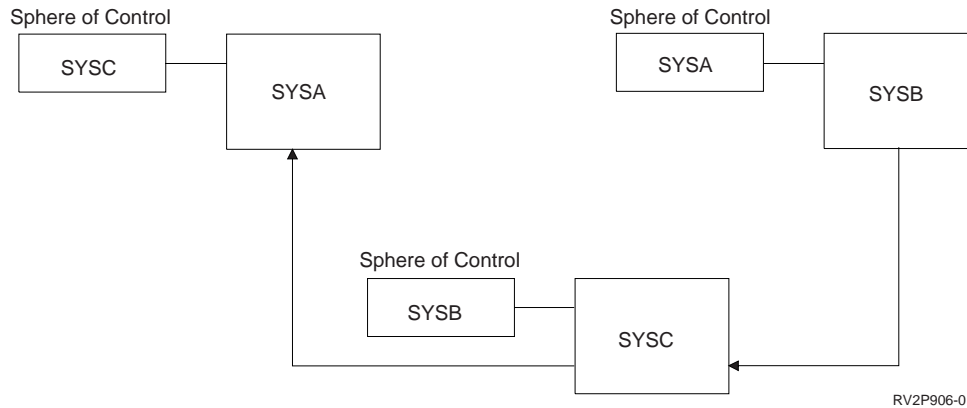
Figure 2-3. Looping Condition Created When Sending Alert

You can use the Work with Alerts (WRKALR) command and specify *HELD for the display option parameter to see the alerts that are currently held:

`WRKALR DSPOPT(*HELD)`

After the held alerts are sent, they are no longer shown when you specify *HELD for the display option parameter. Alerts that are held are logged even if the ALRLOGSTS network attribute would otherwise prevent them from being logged. See "Logging Held Alerts" on page 3-13 for more for information about logging held alerts.

When the held alert is sent, it remains logged only if the ALRLOGSTS network attribute indicates it should.

There is also a `Held alert` flag on the Alert Detail display. This flag is `Yes` if the alert has ever been held. This flag remains `Yes` even after the held alert has been sent. You can compare the `Problem date/time` with the `Logged date/time` on the Alert Detail display to estimate how long the alert was held.

See "Working with Logged Alerts" on page 3-14 for more information about the Alert Detail displays.

Switched Line Considerations

How the AS/400 system handles switched lines for alerts depends on the type of session used (management services session or alert controller session).

Management Services Session

Alert support on a switched line is dependent on the way APPN uses switched lines. A switched line is not activated for the sole purpose of sending an alert.

Alerts flow between an end node and its serving network node on the CPSVCMG reserved mode session. If this session is active on a switched line, the switched line does not automatically disconnect. If this session is not active, alerts cannot be sent.

Alerts flow between a network node and its focal point on the SNASVCMG reserved mode session. The SNASVCMG session normally passes through **transmission groups (TGs)**, groups of links between directly attached nodes appearing as a single logical link for routing messages, that are control point session capable (CPSSN(*YES) on the controller description). If there is no path that passes through only control point session capable TGs, then alerts cannot be sent to the focal point. A switched transmission group between two network nodes that is control point session capable does not automatically disconnect.

The *APPN Support* book contains more information about transmission groups.

Management Services Session
Retries: If the management services session between a node and its focal point goes down, the focal point changes the status of that node to `Inactive`. Whenever the status of a transmission group (TG) changes in the APPN network, the focal point tries to establish sessions again with all

network nodes in the sphere of control that have a status of `Inactive`.

Note: Many retries may occur if your system is a default focal point or as a primary focal point with many systems in the sphere of control.

If the system is a primary focal point, you may force a retry for systems in the sphere of control by removing the system from the sphere of control and then adding it back. You can do this using the Work with Sphere of Control (WRKSOC) command or with the Remove Sphere of Control Entry (RMVSOCE) and the Add Sphere of Control Entry (ADDSOCE) commands.

If the system is a default focal point, you cannot force a retry.

Focal points automatically attempt to retry primary and default focal point services. However, this does not include primary focal point services for end nodes and nodes in an Interconnect network. End points automatically retry requested focal point services. Nodes as end points in an Interconnect network retry primary focal point services.

Note: The CPSVCMG reserved mode session is used by APPN to notify other systems of changes in status. If no CPSVCMG reserved mode session is present, no retries can be done.

Alert Controller Session

When using the alert controller session (ALRCTLD network attribute) over a switched line, the OS/400 alert support will establish the switched connection and send alerts when the alert hold count (ALRHLDCNT) network attribute value is exceeded. The controller description must have been varied on for the connection to be established. Also, there must be an APPC device for the controller description that has been varied on. The alert support will attempt to establish the switched connection using the first APPC device found for the controller description that is varied on.

The APPC device is not used to establish an APPC conversation. It is only needed to establish the switched connection. You do not need to configure an APPC device at the remote system. Once the connection is established, the alert support will send all of the held alerts. It is important to note that the alert controller session does not use an APPC session, and will not automatically drop the switched connection when all of the alerts have been sent. The only control over dropping the switched connection is through use of the switched disconnect (SWTDSC) and disconnect timer (DSCTMR) values in the ALRCTLD controller description.

The Switched Disconnect (SWTDSC) value should be *YES. Once the connection is made, the link will remain active for the number of seconds specified by the disconnect timer (DSCTMR) value. The DSCTMR value should be large enough to allow alert support to send all of the held alerts. There is a relationship between the alert hold count network attribute and the disconnect timer value. If the alert hold count value is large, the disconnect timer value should also be large. The disconnect timer value should not be 0 or the connection will never drop, unless another application is using the connection and unbinds a session. Alert support does not bind or unbind a session when the alert controller session is used for sending alerts.

After the switched connection has been active for the number of seconds specified by the disconnect timer value, the connection is dropped, even if all of the alerts have not been sent. The remaining alerts and all new alerts are held until the alert hold count value is again exceeded. The actual time required to send one alert depends on several factors such as system load, and modem and link characteristics. You may want to experiment with disconnect timer values to get the smallest value possible while still sending the held alerts.

Alerts are sent without regard to the ALRHLDCNT attribute if the switched line is active for some other reason. If the switched line is not active, alerts are held until the specified alert hold count is reached or until the switched line connection is made by another application. If the control of the switched line by the ALRCTLD controller description does not meet your needs, you may want to consider writing your own application to control the switched line connection and disconnection. Other applications could be:

- Display station pass-through
- Distributed data management (DDM)

- SNA distribution services (SNADS) timed distributions

For example, starting display station pass-through over a switched line will cause the switched connection to be made, and held alerts will be sent. You should set the alert hold count network attribute to *NOMAX in this case, so the alert support will not establish the switched connection.

Alert Support through an SNA Subarea Network

Figure 2-4 shows an advanced peer-to-peer networking (APPN) network interacting with a subarea network where the host support includes:

- Virtual Telecommunications Access Method (VTAM*) Version 3, Release 2 program

    Note: If releases of the VTAM program before Version 3, Release 2 are used, the AS/400 system is configured as a dependent logical unit and the sphere of control support does not function correctly.

- Advanced Communications Facility/Network Control Program (ACF/NCP) Version 4, Release 3

The alerts SNASVCMG reserved mode session is supported through the SNA subarea network for this configuration.

There is no CPSVCMG reserved mode session between network node A (NNA) and network node B (NNB). Therefore, for NNB to find NNA in its sphere of control, NNB must define a remote location list entry showing that NNA can be accessed through VTAM/NCP. Also, NNA must define a remote location list entry for NNB.

NNB must be defined as the *primary focal point* for NNA.

Since there is no CPSVCMG reserved mode session between NNA and NNB, retries are performed by the entry point, NNA. NNA must be added to the sphere of control when connection is possible. Once active, NNA performs the retry.

Note: The alert controller session is not supported across the subarea (ALRCTLD parameter of the CHGNETA command).
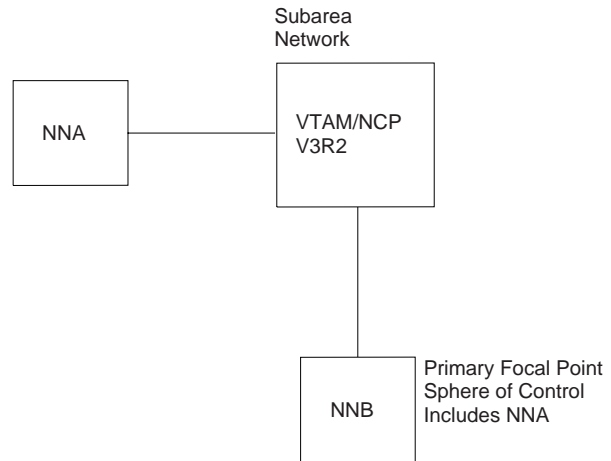
Figure 2-4. APPN Subarea Network

Interconnected Network Considerations

If you are using APPN, it is possible to connect networks that have different network IDs.

Nodes with network IDs that are different from the local node will not have retry performed by the focal point when placed in the sphere of control. Retries are performed by entry point systems. If you have a configuration similar to Figure 2-5 on page 2-15 where the nodes have different network IDs, it is recommended that you nest focal points. For example, in Figure 2-5 on page 2-15, it is recommended that NET2.D be nested with NET2.E and NET2.F in the sphere of control. In this example, NET1.A is a focal point, with NET1.B, NET1.C, and NET2.D in the sphere of control.

Performance Considerations

Alert throughput on the alert controller session decreases if high priority data is sent on the same link.

If many alerts are sent on a system or received from other systems, there may be a delay in the logging of the alerts.

A primary focal point with a large sphere of control may require significant processing to try to establish sessions again. This is especially true if there is much link activation/deactivation occurring in the network. By using nested focal points, the size of any particular sphere of control can be reduced.
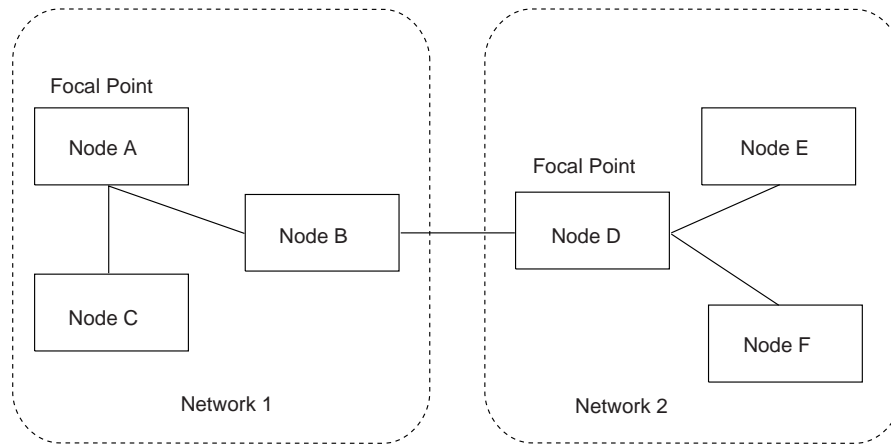
RV2P901-1

Figure 2-5. Interconnected Network

Each network should have only one default focal point. A default focal point serves as a focal point for systems in the network that do not already have a primary focal point. Having more than one default focal point in the network does not provide any additional benefit.

Chapter 3. Using OS/400 Alert Support

This chapter describes how to use OS/400 alert support for working with message descriptions, alert tables, and alert descriptions.

OS/400 Alerts

The AS/400 system creates an alert when an **alertable message** is sent to the local system operator. An alertable message is any message with the alert option field, located in the message description, set to a value other than *NO. You can change this value using the Change Message Description (CHGMSGD) command. In this way, you can select the messages for which you want alerts sent to a network operator at a focal point. IBM-supplied OS/400 messages are shipped with the system in the QCPFMSG message file.

A subset of OS/400 messages are defined as alertable. Most OS/400 messages are not alertable. For a list of which QCPFMSG messages are alertable, see Appendix B, IBM-Supplied Alertable Messages.

Besides changing the alert option field for IBM-supplied messages, you can:

- Create your own messages.

- Define your own messages as alertable.

- Create your own alerts using the QALGENA API. Refer to the *System API Reference* book for information about the QALGENA API.

For more information on defining your own messages, see the *CL Programming* book. To define alerts for your messages by creating alert tables and alert descriptions, see Appendix A, Sample Procedures for OS/400 Alerts.

The following application program interfaces (APIs) allow alerts to be created, sent, and retrieved:

- Generate Alert (QALGENA) API creates an alert for a message ID and returns it to the calling program.

- Send Alert (QALSNDA) API sends a Systems Network Architecture (SNA) generic alert to the OS/400 alert manager for processing.

- Retrieve Alert (QALRTVA) API retrieves an alert from the alert database for processing by the application.

Refer to the *System API Reference* book for more information about alert APIs.

There are several factors to consider when deciding whether a message should be alertable. You should consider the following questions when deciding whether an alert should be sent for a particular error:

- Do you want the system to send any alerts?

- Is the system running attended or unattended?

- Is local problem analysis available for the problem?

- Does problem analysis provide a local resolution to the problem?

- Do you want to send an alert to report the outcome of problem analysis?

Working with OS/400 Message Descriptions

The Add Message Description (ADDMSGD) command or the Change Message Description (CHGMSGD) command is used to specify whether a message will cause an alert to be created. All OS/400 messages contain an alert option. The system is shipped with the alert options in all system messages set to a specific default that you can change. You can also specify the alert option on messages that you create.

Alert Option: The alert option (ALROPT) parameter in the message description is made up of two parts, the **alert type** and the **resource name variable**. These two parts are separated by a blank when the parameter is specified in the Change Message Description (CHGMSGD) command.

Alert Type: The alert type is the value in the message description that determines if the message is alertable or not. The following values can be specified for the alert type:

3-1

*IMMED

This value causes an alert to be created immediately, at the same time that the message is sent to the local system operator.

Most messages defined as *IMMED are caused by a program failure.

*DEFER

This value causes an alert to be created after local problem analysis. *DEFER is specified only for messages that are qualified for problem analysis. This is determined by the log problem (LOGPRB) parameter in the message description.

Messages that are qualified for problem analysis are caused by equipment failures such as:

- Tape or diskette
- Display stations
- Printers
- Lines or modems

If you specify this value for a message for which problem analysis is not available, this value is treated as if you had specified *IMMED. When the system is operating in unattended mode, all alerts set to *DEFER are treated as *IMMED.

*UNATTEND

This value causes an alert to be created at the time that the message is sent to the local system operator message queue, but only when the system is unattended. The system is unattended when the alert status (ALRSTS) network attribute is set to *UNATTEND.

For all *operator intervention messages*, the normal setting of the alert type is *UNATTEND. This includes but is not limited to the following:

- Device door or cover open
- Printer out of paper or paper jammed
- Tape or diskette required
- Power for local device turned off

*NO

This value specifies that no alert is to be created for the message.

Note: The alert type in the message description is not related to the alert type on the Work with Alerts displays. See "Working with Logged Alerts" on page 3-14 for information about working with alerts.

Resource Name Variable: The resource name variable identifies the name of the failing resource in the message. The failing resource is the lowest level (most remote) resource that is common to all resources whose actual or impending loss is the cause of the alert. It is identified as the last entry displayed in the resource hierarchy in the Display Alert Detail and Display Recommended Action displays of the Work with Alerts (WRKALR) command. The resource hierarchy identifies the names of all the resources that provide a connection to the failing resource, plus the name of the failing resource itself.

The resource name variable is a number from 1 to 99 that is the number of the substitution variable in the message data containing the name of the failing resource. The name of the resource is placed in the substitution variable by the system when the message is sent to the QSYSOPR message queue.

There are certain values for the resource name variable that are defined by the system to identify specific resource types that the system knows. These reserved values are identified in Table 3-1 on page 3-3, along with the resource types that can be associated with each particular reserved value.

An example of a message that uses a resource name variable of 23 is:

```
Line &23 failed.  Recovery stopped.
```

In this example, the name of the resource passed in the message data for substitution is the name of a line description defined on the system. This name is sent in the alert as the name of the failing resource. The resource type displayed with the name is link (LNK).

Substitution Variables: The resource types that can be associated with each substitution variable shown in Table 3-1 on page 3-3 are defined as follows:

Line description This is the name of a line description created by a create line description command. See the *Communications Configuration* book for the create line description commands.

Controller description This is the name of a controller description created by a create controller description command. See the *Communications Configuration* book for the create controller description commands.

Device description This is the name of a device description created by a create device description command. See the *Communications Configuration* book for the create device description commands.

First level resource This is the name of the physical resource (usually an input/output processor) that is associated with the failing resource and closest to the system processor.

Second level resource This is the name of the physical resource that is associated with the failing resource and second

closest to the system processor. The type of resource named by this variable depends on the type of subsystem as shown in Table 3-1.

Third level resource This is the name of the physical resource that is associated with the failing resource and third closest to the system processor. The type of resource named by this variable depends on the type of subsystem as shown in Table 3-1.

Fourth level resource This is the name of the physical resource that is associated with the failing resource and is the fourth closest to the system processor. The type of resource named by this variable depends on the type of subsystem as shown in Table 3-1.

Network interface description This is the name of a network interface description created by the Create Network Interface Description (CRTNWIISDN) command. Refer to the *ISDN Support* book for more information.

Table 3-1. Resource Name Variables Defined by the System

Variable	Description	Resource Type Communications Subsystem	Resource Type Storage Subsystem	Resource Type Work Station Subsystem
23	Line description	LNK, BCH	N/A	N/A
24	Controller description	CTL	N/A	CTL, LC
25	Device description	N/A	TAP, DKT	DSP, PRT
26	First level resource	LC	LC	LC
27	Second level resource	ADP	ADP	DSP, PRT
28	Third level resource	POR	DSK, DKT, TAP	N/A
29	Fourth level resource	BCH	N/A	N/A
30	Network interface description	DCH	N/A	N/A
30	Network server description	SVR	N/A	N/A

Note: See Table 3-5 on page 3-16 for a list of the resource type abbreviations.

Alert Hierarchy: Only one number is defined for the resource name variable, but if this number is known by the system, a complete hierarchy, which includes an entry for each resource in the hierarchy, is built by the system, starting from the name of the failing resource up through the name of the system itself. For example, if the resource name variable is defined in the message

description as 28, and the failing resource is a communications port, the resource hierarchy provided by the system has the following entries:

System name This is the name of the system that detected the problem. The resource type is control point (CP).

> **Note:** The name that the AS/400 system uses for the system name is the local control point

name (LCLCPNAME) network attribute.

Input/output processor This is the name of the I/O processor on which the failing port is located. The resource type is local controller (LC).

Input/output adapter This is the name of the adapter card on which the failing port is located. The resource type is adapter (ADP).

Port This is the resource name for the failing port. The resource type is port (POR).

If a resource name variable is outside the range of values defined by the system, the name specified as the substitution data for the identified variable is sent in the alert as the failing resource, and is identified with a resource type of **unknown** (UNK) when the resource hierarchy is displayed. For example, if the message text for the alertable message is:

```
Error detected for tape &1.
```

and the name of the resource passed in the message data for substitution variable 1 is TAPE1, the name of the failing resource in the alert is TAPE1 and the resource type is UNK.

If there is no value specified for the resource name variable, or if the value is 0, the system local control point name is sent in the alert as the name of the failing resource.

Changing the Alert Options: The following example shows changing the alert options for message CPA5339 so that an alert is always created by the system when this message is sent to the local system operator.

```
CHGMSGD  MSGID(CPA5339) MSGF(QSYS/QCPFMSG)  ALROPT(*IMMED 1)
```

The name specified for substitution variable &1; will be used as the failing resource.

The *CL Reference* book contains additional information about the Change Message Description (CHGMSGD) command.

Alerts and Local Problem Analysis

Problems detected by the system are reported locally by messages sent to the QSYSOPR message queue. Some of these messages have problem analysis procedures associated with them that can be run locally by the system operator. Messages that have problem analysis procedures shipped with the system have the log problem (LOGPRB) parameter in the message description set to *YES. These messages can be identified when they are displayed at the QSYSOPR message queue by the asterisk (*) preceding them. When you see a message preceded by an asterisk, you can do local problem analysis by pressing F14 (Run problem analysis) with the cursor positioned on the message. You can also run the problem analysis routines using the Work with Problems (WRKPRB) command.

In a network, you can report problems by sending alerts to a focal point. The network operator at the focal point is responsible for handling the reported problems. This focal point system may not be at the same location as the system that originally detected and reported the problem.

You can set up your network so that you can do the appropriate problem analysis either at the reporting location or at a central site that is the problem management focal point. The **problem management focal point** is the management services responsible for the problem analysis and diagnosis for a sphere of control. At times, you may want problem analysis done at the failing location but the service call or repair action controlled by a central site. In other cases, because of the type of problem or the ability to handle the problem at a particular location, you may want both the problem analysis and the repair action controlled by a single location.

By appropriately setting the alert status (ALRSTS) network attribute for the system and the alert option (ALROPT) parameter of the message description for the message that reports the problem, you can tailor your network to use alerts in any of the following ways:

- Handle the problem at the system with the problem.

- Analyze the problem at the system with the problem but start recovery procedures at the focal point system.
- Handle the problem at the focal point system.
- Handle the problem at the focal point system only when the system with the problem is unattended.
- Handle problems differently depending on the type of problem.

Table 3-2 shows the relationship between the alert option (ALROPT) parameter in the message description and the alert status (ALRSTS) network attribute. In this figure, the messages defined as *DEFER have the log problem (LOGPRB) parameter in the message description set to *YES; setting the LOGPRB parameter to *NO in a message causes all alerts for that message to be treated as *IMMED.

Table 3-2. Relationship between Alert Status Network Attribute and Alert Option Parameter

Network Attribute	ALROPT Parameter in Message Description			
	*IMMED	*DEFER	*UNATTEND	*NO
ALRSTS(*ON)	Alert	Alert after local problem analysis	No alert	No alert
ALRSTS(*UNATTEND)	Alert	Alert	Alert	No alert
ALRSTS(*OFF)	No alert	No alert	No alert	No alert

In this figure, **Alert** means an alert is created immediately, **No alert** means that no alert is created, and **Alert after local problem analysis** means that an alert is created after problem analysis is attempted for the problem.

When there are local problem analysis routines available for a problem that has been reported to a remote problem management focal point with an alert, you can run problem analysis remotely using host command facility (HCF) or display station pass-through. You can use the `Problem date/time` on the Display Alert Detail display to locate the problem in the problem log at the reporting site with the same date and time. You can use the Work with Problems (WRKPRB) command to find problems in the problem log. You can also use SystemView* System Manager/400, an optional licensed program, to work with the problem log.

See "Working with Logged Alerts" on page 3-14 for more information about the Display Alert Detail displays.

When you work with problems, you can tell if an alert has been sent or will be sent by looking at the Problem Detail display for the problem you are working with. A problem that is alertable is displayed with `Alertable condition` set to `Yes`. If `Alert pending` is `Yes`, an alert is sent automatically after problem analysis has been run, unless it is determined that the problem no longer exists.

If `Alertable condition` is `Yes`, and `Alert pending` is `No`, an alert has already been sent because the problem analysis routines have already been run.

If an alert has been sent by the system after problem analysis, you may choose to send another alert before exiting problem analysis by pressing F9 (Send alert). You may want to do this if you have obtained different results by running the problem analysis routines the second time.

Use the Analyze Problem (ANZPRB) command for problems that you detect, but that the system has not reported. From the following displays, you can prepare service requests, send an alert, or both.

Refer to online information for more details on working with problems and local problem analysis.

Alert Messages for General Use

Message CPI9806 is a predefined alertable message in the QCPFMSG message file. This message is sent using the Send Program Message (SNDPGMMSG) command. Message CPI9806 is an operator-generated alert in the QCPFMSG alert table.

Message CPI9806 contains two substitution variables. The first 8 bytes contain the user-defined name that identifies the alert when the alert is

generated. This name can be the name for your system. In the following example, ROCHESTR is used as the user-defined name. The second variable is the message text, which can be up to 100 characters. Use the message text to describe the condition that the alert is reporting.

The following is an example of the command used to send CPI9806 with an operator-defined message text:

```
SNDPGMMSG MSGID(CPI9806) MSGF(QCPFMSG) MSGDTA('ROCHESTR We are +
          experiencing performance problems in Rochester')
          TOMSGQ(QSYSOPR)
```

The Send Program Message (SNDPGMMSG) command can be used only from a CL program. The following is an example of a batch job to create a CL program and a command called SNDALR. The SNDALR command, when issued by the operator, is processed by the SNDALR program (which issues the SNDPGMMSG command).

To submit the job, use the Submit Database Job (SBMDBJOB) command.

```
//BCHJOB CRTSNDALR LOG(4 00 *SECLVL)

 CRTCLPGM QGPL/SNDALR SRCFILE(FILE0001)
//DATA FILE(FILE0001) FILETYPE(*SRC)
 PGM  (&RESOURCE &MSGTEXT);
   DCL &RESOURCE *CHAR 8
   DCL &MSGTEXT  *CHAR 100
   DCL &MSGDATA  *CHAR 108
   CHGVAR &MSGDATA (&RESOURCE || &MSGTEXT);
   SNDPGMMSG MSGID(CPI9806) MSGF(QCPFMSG) MSGDTA(&MSGDATA); +
            TOMSGQ(QSYSOPR)
 ENDPGM
//

 CRTCMD QGPL/SNDALR PGM(QGPL/SNDALR) SRCFILE(FILE0002)   +
                TEXT('Send Operator Generated Alert')
//DATA FILE(FILE0002) FILETYPE(*SRC)
 CMD PROMPT('Send Operator Generated Alert')
    PARM KWD(RESOURCE) EXPR(*YES) MIN(1) MAX(1)  +
         TYPE(*CHAR) LEN(8) PROMPT('Resource name')
    PARM KWD(TEXT) EXPR(*YES) MIN(1) MAX(1)  +
         TYPE(*CHAR) LEN(100) PROMPT('Alert message text')
//

//ENDBCHJOB
```

Message CPI9805 (in the QCPFMSG message file) is also reserved for your use. CPI9805 is a user application alert in the QCPFMSG alert table. CPI9805 has the same message format as CPI9806.

Message CPI9804 (in the QCPFMSG message file) is reserved for use by IBM applications. CPI9804 is an IBM application alert in the QCPFMSG alert table. CPI9804 has the same format as CPI9806.

The alert option parameter for these messages is:

```
ALROPT(*IMMED 1)
```

Operator-Generated Alerts

Operator-generated alerts can be sent to report problems that you detect, but that the system has not reported. They can also be used to report additional information about a problem detected by the system.

Operator-generated alerts are created by using the Analyze Problem (ANZPRB) command or by selecting option 2 (Work with problems) on the Problem Handling menu, and then pressing F14 (Analyze new problem) on the Work with Problems display.

You can analyze the problem and place a call for service in addition to sending an alert for the problem.

If you just want to send an operator-generated alert, do the following:

1. Enter the ANZPRB command.

2. From the Analyze a Problem display, select the option that is most appropriate.

3. The system shows a number of displays for you to define the problem. Select the option for each display that is most appropriate for your problem.

4. After you enter the options to define the problem, a Report Problem display is shown.

5. Select option 1 (Send alert) to send an alert. Another display allows you to enter the message that you want to send in the alert.

6. If you are sending an alert to provide more information about a problem that the system detected, include the date, time, and the message code (if available) that are shown in the problem record for the problem. See "Alerts and Local Problem Analysis" on page 3-4 for information on how to find this information.

7. After you have entered your message, press the Enter key.

8. The alert is created and you are returned to the display that was shown before the ANZPRB command was entered.

Application-Generated Alerts

Application created alerts can be created either by:

- Sending an alertable application message to the QSYSOPR message queue or to the QHST log. Refer to Appendix A, Sample Procedures for OS/400 Alerts for more information.

- Or using the alert APIs (QALGENA and QALSNDA) to allow your application to create alerts and notify the OS/400 alert manager of previously created alerts that need to be handled. Refer to the *System API Reference* book for information about the alert APIs.

Creating an Alert Table

To create your own OS/400 alerts, you must first create an alert table for the alert descriptions. Use the Create Alert Table (CRTALRTBL) command to create the alert table. You then use the Add Alert Description (ADDALRD) command to describe your alerts and place them in the alert table, as described in "Adding Alert Descriptions to an Alert Table" on page 3-8.

The following parameters are supported by the Create Alert Table (CRTALRTBL) command:

ALRTBL Parameter

Specifies the name of the alert table that is created. An alert table has a one-to-one correspondence with a message file. To define an alert for a particular message, the name of the alert table must be the same as the name of the message file.

The alert table and message file do not have to be in the same library. However, the alert table library must be in the library list of the job that causes the alert to be created.

*CURLIB: The current library is used to locate the alert table. If no library is specified as the current library for the job, the QGPL library is used.

library-name: Specify the library where the alert table is to be created.

alert-table-name: Specify the name of the alert table that is created.

AUT Parameter

Specifies the authority granted to users who do not have specific authority to the object, are not on the authorization list, or whose group has no specific authority to the object.

*LIBCRTAUT: The public authority for the object is taken from the CRTAUT keyword of the target library. The CRTAUT value is determined when the object is created. If the CRTAUT value for the library changes after the object is created, the new value does not affect any existing objects.

*CHANGE: The user performs all operations on the object except those limited to the owner or controlled by object existence authority and object management authority. The user can change the object and perform basic functions on the object. Change authority provides object operational authority and all data authorities.

*ALL: The user performs all operations on the object except those limited to the owner or controlled by authorization list management authority. The user can control the object's existence, specify the security for the object, change the object, and perform basic functions on the object. If the object is an authorization list, the user cannot add, change, or remove users.

*USE: The user performs basic operations on the object, such as running a program or reading a file. The user is prevented from changing the object. Use authority provides object operational and read authority.

*EXCLUDE: The user is prevented from retrieving the object.

authorization-list-name: Specify the authority of the named authorization list.

LICPGM Parameter

Specifies the licensed program for which this alert table is used. The program, if specified, is included for the alert.

5716SS1: The licensed program for the OS/400 system is used.

*NONE: There is no licensed program for this alert table. This value is allowed for products that do not have a licensed program.

licensed program: Specify a 7-character ID for the program.

The program does not have to be an IBM licensed program. Any 7-character ID that is significant for the network operator viewing the alerts can be specified. If the value specified is defined to the system, then the ID, release, and level information are included in the alert. If the value specified is not known, then the release and level information are not included in the alert and only the ID and the program text in the LICPGMTXT parameter are included.

LICPGMTXT Parameter

Specifies text for the alert table licensed program (for example, the OS/400 program). The text is included in the alert.

*NONE: There is no text.

licensed program text: Specify up to 30 characters of text describing the program.

TEXT Parameter

User-entered text that explains the alert table and its descriptions.

*BLANK: No text is specified.

description: Specify up to 50 characters of text, enclosed in apostrophes.

Additional Alert Table Commands

The following commands are also available for alert tables:

- Delete Alert Table (DLTALRTBL)
- Change Alert Table (CHGALRTBL)
- Work with Alert Tables (WRKALRTBL)

Adding Alert Descriptions to an Alert Table

The alert table contains alert descriptions. Alert descriptions define the code points to use in an alert for a particular message. For more information on code points, see "SNA Generic Alerts" on page 3-24.

There is a one-to-one correspondence between a message description, which defines an error, and an alert description, which defines a network problem notification. An alert description for a message being added to an alert table must have the same name as the message file for that

message. For example, for message USR1234 in message file USRMSGS, alert description USR1234 must be added to an alert table named USRMSGS.

The alert table and message file do not have to be in the same library. However, the alert table library must be in the library list of the job that causes the alert to be created.

To add alert descriptions to an alert table, use the Add Alert Description (ADDALRD) command.

The following parameters are supported by the ADDALRD command:

MSGID Parameter

Specifies the message ID to which this alert description corresponds.

ALRTBL Parameter

Specifies the alert table in which this alert description is created. The name should be the same as the message file in which the specified message was created.

*LIBL: The library specified in the library list.

*CURLIB: The current library.

library name: Specify a library name.

ALRTYPE Parameter

Specifies the code point for the type of alert. The code point is 2 hexadecimal digits.

*NONE: No code point is specified.

alert type code point: Specify the code point for the severity of the problem.

ALRD Parameter

Specifies the code point for the description of the alert. The code point is 4 hexadecimal digits.

*NONE: No code point is specified.

alert description code point: Specify the code point that describes the alert condition.

PBLCAUSE Parameter

Specifies the code point for the most likely causes of the condition described.

*NONE: No code point is specified.

probable cause code point: Specify up to 99 code points for probable causes. The code points are listed in order of decreasing probability. Each code point is 4 hexadecimal digits.

CAUSE Parameter

Specifies the causes for the alert description. A cause consists of the following:

- Cause type

  *USER

  These code points describe the conditions caused by a user and defined as conditions that can be resolved by the operator without contacting any service organization.

  *INSTALL

  These code points describe conditions resulting from the initial installation or setup of equipment.

  *FAILURE

  These code points describe conditions caused by the failure of a resource.

  Note: You can specify *NONE if there are no causes. The *NONE cause keyword must be associated with the *UNKNOWN action keyword.

- Cause code point (4 hexadecimal characters)

- Detailed data (up to 3 qualifiers for detailed data)

  Detailed data ID code point

  The code point specifying the data (2 hexadecimal digits).

  Detailed data

  Up to 40 characters of detailed data. The default is *NODATA. A substitution variable (for example, &1) from the corresponding message description can be specified. The message data is substituted into the alert when the alert is created.

  For a code point that requires detailed data, see "Detailed Data for Causes and Actions" on page 3-10.

- Product identifier

  For a code point that requires a product identifier, see "Product Identifiers for Causes and Actions" on page 3-10.

  Note: The cause parameter specifies either detailed data or a product identifier.

ACTION Parameter

Specifies the actions for the alert description. An action consists of the following:

- Action type

  *USER

  These code points describe the actions recommended to correct the conditions caused by a user.

  *INSTALL

  These code points describe the actions recommended to correct conditions resulting from the initial installation or setup of equipment.

  *FAILURE

  These code points describe the actions recommended to correct conditions caused by the failure of a resource.

  *UNKNOWN

  The code point that follows is for a recommended action when the cause of the error is undetermined. This keyword can only be specified if CAUSE is *NONE.

  Note: You can specify *NONE if there are no actions.

- Action code point (4 hexadecimal characters)

- Detailed data (up to 3 qualifiers for detailed data)

  Detailed data ID code point

  The code point specifying the data (2 hexadecimal digits).

  Detailed data

  Up to 40 characters of detailed data. The default is *NODATA. A substitution variable (for example, &1) from the corresponding message description can be specified. The message data is substituted into the alert when the alert is created.

  For a code point that requires detailed data, see "Detailed Data for Causes and Actions" on page 3-10.

- Product identifier

For a code point that requires a product identifier, see "Product Identifiers for Causes and Actions" on page 3-10.

Note: The action parameter specifies either detailed data or a product identifier.

Detailed Data for Causes and Actions

Each user, install, or failure cause code point and each recommended action code point can have up to three detailed data qualifiers with the code point text. Detailed data qualifiers are substituted into the code point text. The number of detailed data qualifiers needed for a particular code point is determined by the third digit of the code point, as summarized below:

Third Digit	Number of Detailed Data Qualifiers
X'xx0x'–X'xx9x'	No detailed qualifiers
X'xxAx'–X'xxBx'	One detailed data qualifier
X'xxCx'	Two detailed data qualifiers
X'xxDx'	Three detailed data qualifiers
X'xxEx'	One product identifier qualifier

If *NODATA is specified for the detailed data for a code point, then the code point is not included in the alert.

If the data is not known when the alert description is defined, message substitution variables can be specified as detailed data. Message data is used from the message that caused the alert. Any substitution variables that match variables in the message description are filled in later.

The following data types are supported as substitution data for detailed data qualifiers:

Data Types	Name	Description
*CHAR	Character data	*VARY for varying length data is supported.
*CCHAR	Converted character data	*VARY for varying length data is supported.
*BIN	Binary data	*BIN 2 and *BIN 4 are supported.

Data Types	Name	Description
*DEC	Packed decimal data	*DEC x y where x is the total digits, and y is a fraction of any remaining digits.
*HEX	Hexadecimal data	*VARY for varying length data is supported.
*DTS	Date/time stamp	The date/time stamp is converted according to system values to a form that can be displayed.
*ITV	Time interval	The time interval is converted to a value that can be displayed.
*SYP	System pointer	The name of the object pointed to is substituted as the detailed data.

Each detailed data qualifier can substitute up to 44 bytes from the message data. If the message data is longer than 44 bytes, it is truncated.

Product Identifiers for Causes and Actions

If the third character of the code point is E (for example, X'00E1'), the code point requires a product identifier. The OS/400 alert support provides the following product identifiers:

*SNDHDW The sender hardware responsible for the alert (for example, the AS/400 system).

*SNDSFW The sender software code responsible for the alert (for example, the OS/400 licensed program). This is determined from the LICPGM parameter of the CRTALRTBL command.

*RSCHDW The resource hardware that failed (for example, I/O processor cards, tape units, or diskette units). This is determined from one of the following:

- Information in the problem log for hardware errors

• Information in the substitution variables of the message description for other errors

A code point requiring a product identifier must be associated with one of these products. This is specified for the code point on the ADDALRD and CHGALRD commands.

For example, recommended action X'00E1' is:

```
Perform [product-ID] problem analysis procedures
```

If the product identifier for this code point is defined as the sender hardware (in this example, the AS/400 system), the code point appears as the following at the alert focal point:

```
Perform AS/400 problem analysis procedures.
```

Following is an example of a command to add a code point with a product identifier:

```
ADDALRD MSGID(USR1234) ACT(USER/USRMSGS)
        ALRTYPE(01) ALRD(FE00)
        PBLCAUSE(6000 0030 0500)
        CAUSE(*NONE)
        ACTION((*UNKNOWN 00E1 *NONE *NODATA
                             *NONE *NODATA
                             *NONE *NODATA
                             *SNDHDW))
```

Additional Alert Description Commands

The following commands are also available for alert descriptions.

• Change Alert Description (CHGALRD)

• Remove Alert Description (RMVALRD)

• Work with Alert Descriptions (WRKALRD)

Working with Alert Descriptions

Using the alert description created in the previous example, when you enter the WRKALRD command, a display similar to the following is shown:

```
                                            System:  ROCHSTR
  Alert table . . . . . . :   CAPPL1
    Library . . . . . . . :     CAPPL1LIB
    Product . . . . . . . :     CAPPL10 (Customer Application - 0001)

  Position to  . . . . .  _____    Message ID

  Type options, press Enter.
    1=Add  2=Change  4=Remove  5=Display recommended actions 6=Print
    8=Display alert detail

  Opt    Message ID    Alert Description: Probable Cause

   8       APP1000       Software program error:  Software program
```

Displaying Alert Details: To display alert details, select option 8 (Display alert detail) from the Work with Alert Descriptions display. A Display Alert Detail display similar to the following appears.

```
                                            System:  ROCHSTR
  Message ID . . . . . . . . . :   APP1000
  Message text . . . . . . . . :   Application program &1; failed while writing t
                                   o file &2; library &3; with reason code &4;
  Alert type . . . . . . . . . :   (01) Permanent
  Alert description  . . . . . :   (2100) Software program error
  Alert option . . . . . . . . :   *IMMED
  Alert ID . . . . . . . . . . :   6774 AD43


  Probable
   Cause        Probable Cause Text
    1000        Software program
    7004        User
    7001        Local system operator
```

This display can show the following information:

Alert type
The alert type code point defines the severity of the problem. Possible values are:

Permanent
This is a loss of availability to the user that requires some action by the focal point operator.

Temporary
This is a momentary loss of availability that can affect the user, but does not require any action by the focal point operator.

Performance
The alerted condition may be causing an unacceptable level of performance.

Impending Problem
This is a potential loss of availability to the user that has not yet happened.

Unknown
The severity of the alert condition cannot be determined.

Permanently affected resource
The originator of this alert has determined that the target resource is lost because of a persistent error in a resource other than the target.

Alert description
The alert description code point defines the condition that caused the alert.

Alert option

The alert option field displays the ALROPT parameter from the message description for the given message. This is for information only.

Alert ID

The alert identifier field displays the alert identifier that is displayed with the specific information for an alert in the Work with Alerts (WRKALR) command displays. The alert ID is calculated for the alert using the cause code points when the alert is created. It can be used to identify a particular error condition (set of causes) at a problem management focal point.

It is possible that the alert identifier created when the alert was created does not match the alert identifier shown for this display. This is because of differences in the methods used to display the alert description and to create the alert. For example, the WRKALRD command shows duplicate code points, but the system removes duplicate code points when it creates the alert.

Probable Cause

The probable cause field lists the causes that are determined by the alert sender to be the most probable causes for the alert condition. These causes are listed in order of decreasing probability.

Notice that there is a difference between the probable cause and the user, install, or failure causes listed on the Display Recommended Actions display. The probable causes specify what has failed, while the others specify what is wrong for a probable cause.

For example, a probable cause may indicate a cable, while the user cause for the same alert might indicate that this cable is unplugged.

Displaying Recommended Actions: To
display recommended actions, select option 5 (Display recommended actions) from the Work with Alert Descriptions display. A Display Recommended Actions display similar to the following appears.

```
                                          System:  ROCHSTR
 Message ID . . . . . . . . . :    APP1000
 Message text . . . . . . . . :    Application program &1; failed while writing t
                                   o file &2; library &3; with reason code &4;

 Type options, press Enter.
   5=Display detailed qualifiers

                              Cause or
 Opt    Type                  Action     Text
        User cause            73A0       File full: &2;
   _    User cause            73A1       File needs reorganization: &2;
   _    User action           32C0       Report the following
   _    User action           1300       Correct then retry
   _    Failure cause         10E1       Software program &4;
   _    Failure action        32C0       Report the following
   _    Failure action        F0A0       For &1;
   _    Failure action        F008       Recurrence indicates media
```

This display can show the following information:

Type

The type defines whether this is a cause or an action and what type of cause or action. The types are:

- User cause
- User action
- Install cause
- Install action
- Failure cause
- Failure action

Cause or action

The cause or action defines the code point that explains the actual cause or action.

Text

The associated text for the code point.

Displaying Detailed Qualifiers: To
display detailed qualifiers, select option 5 (Display detailed qualifiers) from the Display Recommended Actions display. If the third hexadecimal digit is 0 through D, a Display Detailed Qualifiers display similar to the following appears.

```
                                          System:  ROCHSTR
 Message ID . . . . . . . . . :    APP1000
 Message text . . . . . . . . :    Application program &1; failed while writing t
                                   o file &2; library &3; with reason code &4;
 Cause or action type . . . . :    User cause
 Cause or action. . . . . . . :    (73A0) File full: &2;
 Number of qualifiers . . . . :    1 detailed data qualifier

 Detailed data ID . . . . . . :    (00D0) File name
 Detailed data  . . . . . . . :    &2;
```

The number of detailed qualifiers shown depends on the number needed for a particular code point. The detailed data can contain text or a message substitution variable.

This example shows substitution variables for code point text (&1) and detailed data (&2). Substi-

tution variable &1; in the code point text `File full: &1` specifies where the detailed data is displayed in the code point. The code point text is taken from the message description for message ALU73A0 in the QALRMSG message file. The ALU prefix in the message ALU73A0 indicates a user cause. For more information on substitution variables, see "Adding Code Points to the OS/400 Alert Message File" on page 3-25.

Substitution variable &2; specifies that the message data from message APP1000 is in message file CAPPL1. Message file CAPPL1 contains the data used for the detailed data qualifiers for this code point.

In the following example, the detailed data `APP1000` was defined at the time that the alert description was added:

```
                                        System:   ROCHSTR
Message ID . . . . . . . . . :    APP1000
Message text . . . . . . . . :    Application program &1; failed while writing t
                                  o file &2; library &3; with reason code &4;
Cause or action type . . . . :    Failure action
Cause or action. . . . . . . :    (F0A0) For &1;
Number of qualifiers . . . . :    1 detailed data qualifier

Detailed data ID . . . . . . :    (00D0) Message code
Detailed data  . . . . . . . :    APP1000
```

To display detailed qualifiers, select option 5 (Display detailed qualifiers) from the Display Recommended Actions display. If the third hexadecimal digit is E, a Display Detailed Qualifiers display similar to the following appears.

```
                                        System:   ROCHSTR
Message ID . . . . . . . . . :    APP1000
Message text . . . . . . . . :    Application program &1; failed while writing t
                                  o file &2; library &3; with reason code &4;
Cause or action type . . . . :    Failure cause
Cause or action. . . . . . . :    (10E1) Software program &4;

Product identifier . . . . . :    Sender software
```

In this example, the code point `10E1` specifies a product identifier qualifier. The substitution variable &4 specifies the placement of the product identifier in the code point text. The code point text is taken from the message description for message ALF10E1 in the QALRMSG message file. The ALF prefix in the message ALF10E1 indicates a failure cause.

Working with Alerts

The OS/400 alert support allows you to log and display alerts that have either been locally created on your system, or have been received from other systems in the network if your AS/400 system is a focal point.

The Alert Database

Alerts that have either been created locally by the system or that have been received by other systems are logged in the alert database. You can control the logging of alerts using the alert logging status (ALRLOGSTS) network attribute.

Logging Alerts: Table 3-3 shows whether an alert is logged in the alert database, depending on:

1. The ALRLOGSTS network attribute (*ALL, *LOCAL, *RCV, or *NONE)

2. Whether the alert is locally created or received from another system

Table   3-3. When Alerts Are Logged in the Alert Database

	*ALL	*LOCAL	*RCV	*NONE
Local	Logged	Logged	Not logged	Not logged
Received	Logged	Not logged	Logged	Not logged

Logging Held Alerts: If the AS/400 system cannot send or forward an alert to a focal point because of network conditions or because of the specified count in the Alert Hold Count (ALRHLDCNT) network attribute has not been reached, the system holds the alert by logging it in the alert database. The alert is marked in the database as held for sending at a later time.

Held alerts can be displayed by using the display option parameter of the Work with Alerts (WRKALR) command, or by pressing F15 (Subset) from the Work with Alerts main display. If you do not want the AS/400 system to send these held alerts once it can do so, you can delete these alerts from the alert database.

When a held alert is successfully sent, the alert logging status network attribute controls whether

the alert remains in the alert database. If the conditions shown in Table 3-3 indicate that the alert should not be logged, it is deleted from the alert database. If the conditions indicate that the alert should be logged, it remains in the alert database, but it is no longer displayed as a held alert.

Maintaining the Alert Database: The alert databases on the AS/400 system are a physical file named QAALERT and a logical file named QAALHSN in library QUSRSYS. Other logical files in the QUSRSYS library are used by the OS/400 Query support to improve performance while working with the logged alerts. The files used for alerts are shown in Table 3-4.

Table 3-4. Database Files for OS/400 Alert Support

File Name	Description
QAALERT	Physical file for alerts
QAALHLSN	Logical file keyed on held alerts
QAALRCLC	Logical file keyed on received/local alerts
QAALRSCN	Logical file keyed on resource name
QAALRSCT	Logical file keyed on resource type
QAALALTP	Logical file keyed on alert type
QAALPBID	Logical file keyed on problem ID
QAALUSER	Logical file keyed on assigned user
QAALGRP	Logical file keyed on assigned group

The automatic cleanup features of the Operational Assistant* program will automatically delete alerts that are older than a specified number of days and reorganize the alert database. Type GO ASSIST to specify cleanup options.

Following are the cleanup options available:

Database Backup and Recovery: To save the QUSRSYS library, specify *NONSYS for the LIB parameter on the Save Library (SAVLIB) command. The *Backup and Recovery* contains information about saving the system.

Database Reorganization: If you want to reduce the amount of space that the alert physical file takes up, you can use the Reorganize Physical File Member (RGZPFM) command to reorganize the alert database. This frees any space taken up

by deleted alert records. The *CL Reference* book contains more information about this command.

Deleting Alerts: You can delete one or more alerts from the alert database with the Delete Alert (DLTALR) command. You can use the RGZPFM command to reorganize the alert database after deleting alerts.

Clearing the Database: You can delete all of the alerts logged in the alert database by using the Clear Physical File Member (CLRPFM) command. This clears all alert records currently in the physical file. The *CL Reference* book contains more information about this command.

Working with Logged Alerts

The Work with Alerts (WRKALR) command displays logged alerts, with the most recent alert displayed first. Logged alerts can include alerts created locally and alerts received from other systems in the network, depending on the current setting of the ALRLOGSTS network attribute. Alerts that cannot be sent and are marked as held can also be displayed. Alerts can be deleted using the WRKALR command.

Note: Your system does not have to be actively processing alerts to work with alerts. Whatever is logged in the alert database is displayed.

Specifying Which Alerts to Display: When working with the logged alerts, you can select a subset of alerts to be displayed. You do this by specifying parameters on the Work with Alerts (WRKALR) command, or by pressing F15 (Subset) on the Work with Alerts display.

When you press F15, or request prompting for the Work with Alerts command, the following prompts are displayed:

```
  Type choices, press Enter.

  Display option . . . . . . . . .   *ALL__      *ALL, *RCV, *LOCAL, *HELD
  Period
    Start time and date
    Start time . . . . . . . . . .   *AVAIL__    Time, *AVAIL
    Start date . . . . . . . . . .   *BEGIN__    Date, *BEGIN, *CURRENT
    End time and date
    End time . . . . . . . . . . .   *AVAIL__    Time, *AVAIL
    End date . . . . . . . . . . .   *END___     Date, *END
  Alert type . . . . . . . . . . .   *ALL____    *ALL, *PERM, *TEMP, *PERF...
              + for more values      _____
  Alert resource . . . . . . . . .   *ALL____    Name, *ALL
              + for more values      _____
  Alert resource type  . . . . . .   *ALL        Character value, *ALL
              + for more values      _____
  Assigned user  . . . . . . . . .   *NONE_____  Name, *NONE, *ALL
              + for more values      _____
                                                              More...
```

```
                    + for more values
   Output . . . . . . . . . . . . .   *PRINT      *, *PRINT
                                                                    Bottom
   F3=Exit   F4=Prompt    F5=Refresh   F12=Cancel   F13=How to use this display
   F24=More keys
```

You can select one of the following subsets of the list of alerts to be displayed.

Local alerts

Alerts that have been created locally.

Received alerts

Alerts that have been received from other systems.

Held alerts

Alerts that the system has currently marked as held because they cannot be sent or for-warded to a focal point. When the alerts dis-played in this category are sent, they are no longer displayed for this category.

Date/time

You can select a subset of the alerts to be displayed by a range of dates and times.

Alert types

You can select a subset of the alerts to be displayed depending on the severity of the alert.

Resource names

Alerts that have been sent or received for a particular named resource.

Resource types

Alerts that have been sent or received for a particular type of resource.

Assigned user

Alerts that have been assigned to a particular user through an alert filter.

Group

Alerts that have been assigned to a particular group through an alert filter.

Output

You can display the output at the requesting work station or print the output with the job's spooled output.

Note: If you do not specify any parameters on the WRKALR command, then all alerts in the database are displayed.

The *CL Reference* book contains more information on the WRKALR command and the parameters listed above.

Work with Alerts Main Display: You can look at the Work with Alerts main display by doing one of the following:

- Typing the Work with Alerts (WRKALR) command on the command line.

- Choosing option 6 (Communications) from the AS/400 Main menu, then option 5 (Network management) from the Communications menu, option 5 (Network problem handling) from the Network Management menu, and option 2 (Work with alerts) from the Network Problem Handling menu.

```
                                                   System:   ROCHESTR
   Type options, press Enter.
     2= Change   4=Delete   5=Display recommended actions   6=Print details
     8=Display alert detail

        Resource
   Opt  Name      Type  Date   Time   Alert Description: Probable Cause
        CHCAGO7*  TAP   01/20  13:15  Storage subsystem failure: Tape drive
    _   TAP01     TAP   01/20  13:13  Tape operation error: Tape
    _   ATLANTA*  LNK   01/20  09:30  DCE interface error: Communications inte
    _   ATLANTA*  PRT   01/19  16:43  Operator intervention required: Printer
    _   ATLANTA*  LNK   01/19  15:18  Unable to communicate with remote node:




                                                             Bottom
   F3=Exit    F10=Show new alerts    F11=Display user/group    F12=Cancel
   F13=Change attributes   F20=Right    F21=Automatic refresh   F24=More keys
```

This display supplies the following information:

Resource name

This field identifies the failing resource (for example, TAP01).

If the resource name is followed by an asterisk (*), the resource name displayed is not associated with the resource type dis-played next to it. This is based on information in the alert itself. This allows an alert sender to have its name displayed on the main display, while also showing what kind of resource the alert is about (for example, a printer located at system ATLANTA).

Type

This field identifies the type of resource that detected the error condition (for example, TAP to indicate the resource is a tape). Table 3-5 on page 3-16 shows the types of resources and their abbreviations.

Date

This is the date the alert was logged on the system.

Time

This is the time the alert was logged on the system.

Alert description

This field supplies you with a brief description of the alert.

Probable cause

This field indicates the most likely cause for the alert. Although there can be several probable causes in the alert, only the first (and most likely) is shown on this display.

If the entire text for the alert description and probable cause is not displayed, press F20 (Right) to shift to another view, which shows only the alert description and probable cause.

Press F21 to start the automatic refresh of the list of alerts. The Work with Alerts display is periodically refreshed to show new alerts, so that the network status can be monitored. The refresh rate can be set or changed by pressing F13.

Table 3-5 (Page 1 of 2). Resource Type Abbreviations

Resource Type	Abbreviation
Access Unit	ACU
Adapter	ADP
Application	APP
Boundary function physical unit	BPU
Central processing unit	CPU
Communications controller	CMC
Computerized branch exchange	CBX
Controller	CTL
Control point	CP
CSMA/CD bus	BUS
DACC	DAC
Disk	DSK
Diskette	DKT
Display	DSP
Domain	DMN
Earth Station	EST
Facsimile Device	FAX
Focal point	FP
Frame relay line	FRL
IC controller	ICC
ISDN B-Channel	BCH
ISDN D-Channel	DCH

Table 3-5 (Page 1 of 2). Resource Type Abbreviations

Resource Type	Abbreviation
Keyboard	KBD
LAN bridge	BRG
Line	LIN
Line group	LG
Link	LNK
Link station	LS
Local area network	LAN
Local controller	LC
Logical link connection	LLC
Logical unit	LU
Loop	LP
Management server	MSV
Microwave station	MWS
Modem	MDM
Multiplexer	MUX
Multipoint line	MPL
Network ID	NID
Operating system	OS
OSI managed object	OMO
OSI management server	OSI
Personal banking machine	PBM
Physical unit	PU
Plotter	PLT
Point of sale unit	POS
Port	POR
Printer	PRT
Printer server	PSV
Private branch exchange	PBX
Program	PGM
Programmable work station	PWS
Protocol converter	PCV
PU T2 gateway	GW
PU T2 gateway application	GWA
Relational database	DB
Requester	RQS
Router	RTR
Satellite	SAT
Self-service terminal	SST
Serial line switch	SLS
Server	SVR
Service point	SP
SNA channel	CHL
SNA gateway	SNG
SNMP agent	SPA
SNMP device	SDV
Statistical multiplexer	STM
Storage device	STG
Switch	SWT
Tape	TAP
Teller assist unit	TAU
Token bus	TB
Token ring	RNG

Table 3-5 (Page 2 of 2). Resource Type Abbreviations

Resource Type	Abbreviation
Transaction program name	TPN
Transmission group	TG
T1 resource manager	T1M
Unknown	UNK

Display Recommended Actions

Display: To look at additional information about a particular alert, select option 5 (Display recommended actions) to show the Display Recommended Actions display.

```
                                          System:   ROCHESTR
       ----------Resource Hierarchy----------
       Resource Name          Resource Type
         ROCHESTR               CP
         ATLANTA                CP
         CC03                   LC
         RCHLIN                 LNK

       Failure causes  . . . . :  Communications/remote node
       Actions . . . . . . . . :  Run the following at the reporting location
                                    Command DSPLOG QHST
                                  For System message code CPA58CC
                                  Perform problem determination procedure at the
                                    reporting location for Log record number
                                    89254087E1
                                  Contact appropriate service representative
                                                                        Bottom
       Press Enter to continue.

       F3=Exit   F12=Cancel   F17=Display detail
```

This display supplies the following information:

Resource hierarchy
This field shows the configuration hierarchy for the alert. The bottom or lowest entry of the hierarchy shows the resource name and type of the resource that detected the error condition. Up to four more resource names and types can be displayed, which identify any resources involved with the alert up to the system that last processed the alert. If the detecting resource is not known, the system that sent the alert is displayed as the lowest entry.

User causes
This is a list of possible causes for a problem that is the result of a user action.

Install causes
This is a list of possible causes for a problem that is the result of the installation of new or upgraded hardware or software.

Failure causes
This is a list of possible causes for a problem that is the result of failures in the hardware, software, or a combination of these.

Actions
These are recommended actions to further isolate the problem or correct the condition which caused the problem.

Note: Not all of these fields are displayed for every alert. The information displayed for each alert depends on information contained in the alert itself. The *SNA Formats* book contains more information on all the alert fields.

Specific Actions for Problem Analysis on the AS/400 System: The OS/400 alert support creates alerts with recommended actions that are specific to problem analysis on the AS/400 system.

Analyze Problem: The recommended action

```
Run the following at the reporting location
  Command ANZPRB
```

indicates that you should use the Analyze Problem (ANZPRB) command at the AS/400 system that created the alert. The system message ID that you should use is also provided in the alert.

Display the History Log: The recommended action

```
Run the following at the reporting location
  Command DSPLOG QHST
```

indicates that you should display the history log of the AS/400 system that created the alert. The history log provides the complete message that caused the alert to be created. The message ID of the message that you should look at is also provided in the alert.

Use the `Problem date/time` on the Display Alert Detail display to locate the message in the history log. The times may not match exactly.

Run Problem Analysis Procedures: The recommended action

```
Perform problem analysis procedure at the
  reporting location for Log record number
  89254087E1
```

indicates that you should perform local problem analysis at the AS/400 system that created the

alert. The `Log record number` identifies the problem ID.

See "Alerts and Local Problem Analysis" on page 3-4 for information about local problem analysis.

Print Details: Print details (option 6) prints the details of the selected alert to a spooled file.

Display Alert Detail Display: The Display Alert Detail display supplies further details about the selected alert. You can look at this display by pressing F17 (Display detail) from the Display Recommended Actions display or typing option 8 (Display alert detail) next to the alert on the Work with Alerts display. This display may consist of more than one display of data.

```
                                             System:   ROCHESTR
----------Resource Hierarchy-----------
  Resource Name        Resource Type
   ROCHESTR              CP
   ATLANTA              CP
   CC03                  LC
   RCHLIN                LNK

Logged date/time . . . . . . :   02/15/88  15:18:04
Problem date/time  . . . . . :   02/15/88  15:18:01
Assigned user  . . . . . . . :
Group assigned . . . . . . . :
Filter . . . . . . . . . . . :
  Library . . . . . . . . . :
Alert type . . . . . . . . . :   Permanent
Alert description  . . . . . :   Unable to communicate with remote node
Probable causes  . . . . . . :   Communications
                                 Communications/remote node
                                                           More...
Press Enter to continue.

F3=Exit  F11=Display detail menu  F12=Cancel  F18=Display actions
```

This display can show the following information:

Logged date/time
This is the date and time that the alert was logged. This is the same date and time that appear on the Work with Alerts display.

Problem date/time
This is the date and time that the alert was created and reflects the time that the alertable condition was detected.

Assigned user
This is the user assigned to the alert. The user is assigned through the alert filter.

Group assigned
This is the group into which the alert is filtered.

Filter
This is the filter that was active when this alert was processed. This field is only shown if a user and group are not changed.

Library
This is the library where the active filter is. This field is only shown if a user and group are not changed.

Alert type
The alert type defines the severity of the problem. Possible values are:

Permanent
This is a loss of availability to the user that requires the focal point operator to intervene.

Temporary
This is a momentary loss of availability that can affect the user, but does not require the focal point operator to intervene.

Performance
The alerted condition may be causing an unacceptable level of performance.

Impending problem
This is a potential loss of availability to the user that has not yet happened.

Permanently affected resource
The originator of this alert has determined that the target resource is lost because of a persistent error in a resource other than the target.

Unknown
The severity of the alert condition cannot be determined.

Alert description
The alert description defines the condition that caused the alert.

Probable causes
Lists the causes that, in the alert sender's view, are the most probable causes for the alert condition. These causes are listed in order of decreasing probability.

Notice that there is a difference between the probable cause, and the user, install, or failure causes listed on the Display Recommended Actions display. The probable causes specify

what it is that has failed, while the others specify what is wrong with a probable cause.

For example, a probable cause may indicate a cable, while the user cause for the same alert might indicate that this cable is unplugged.

```
                                              System:   ROCHESTR
   ----------Resource Hierarchy----------
     Resource Name        Resource Type
       ROCHESTR             CP
       ATLANTA              CP
       CC03                 LC
       RCHLIN               LNK

   Qualifiers . . . . . . . . . :   AS/400 Message code CPA58CC
                                    AS/400 Message severity 99
   Text message:
     Sender ID  . . . . . . . . :   Control program
     Message  . . . . . . . . . :   Line RCHLIN failed. Recovery stopped.(C G R)
                                    Reason code: X'54002050'
                                                               More...


   Press Enter to continue.

   F3=Exit   F11=Display detail menu   F12=Cancel   F18=Display actions
```

Qualifiers

Lists product-specific detailed data about the alert condition.

Detailed data qualifiers can appear in several different places on the alerts displays:

- As part of a user, install, or failure cause on the Display Recommended Actions display.

- As part of an action on the Display Recommended Actions display.

- In the Qualifiers section of the Display Alert Detail display.

A detailed data qualifier is made up of three parts:

Product identification
Identifies the product associated with this detailed data qualifier. This part does not have to be present.

Data identification
Identifies the type of detailed data present in this qualifier.

Detailed data
The detailed data itself, in either character, hexadecimal, or decimal form.

Following is an example of a detailed data qualifier with two of the above three parts:

Command DSPLOG QHST

where Command is the data identification, and DSPLOG QHST is the detailed data.

Following is an example of a detailed data qualifier with all of the parts:

AS/400 Message code CPA58CC

where AS/400 is the product identification, Message code is the data identification, and CPA58CC is the detailed data.

Text message

Provides a text message from the alert sender about the problem. For alerts from an AS/400 system, the text message is the first level text for the message that caused the alert to be sent.

This section is made up of one or more of the following fields. The exact fields present depend on what is present in the alert. The possible fields are:

Sender ID Identifies the alert sender. The following values are possible:

> **Display station user** A person who is only a user of system resources (not an operator).

> **Operator** A person who is responsible for managing system resources.

> **Application program** A program written by or for a user.

> **Control program** A program that controls the system resources.

Message The actual message text. Notice that this text is displayed in the language in which the message was created at the alert sender.

You can press F11 to use the Display Detail Menu display. This display allows you to select the functions shown.

```
                                                  System:  ROCHESTR
         ----------Resource Hierarchy----------
         Resource Name        Resource Type
           ROCHESTR              CP
           ATLANTA               CP
           CC03                  LC
           RCHLIN                LNK


         Select one of the following:

             1. Display flags
             2. Display product identification


             5. Display LAN data
             6. Display alert in hexadecimal

         Selection or command
         ===> _____

         F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

```
                                                  System:  ROCHESTR
         ----------Resource Hierarchy----------
         Resource Name        Resource Type
           ROCHESTR              CP
           ATLANTA               CP
           CC03                  LC
           RCHLIN                LNK


         Sender hardware identification:
           Product classification . . :  IBM hardware
           Machine type . . . . . . . :  9406
           Model number . . . . . . . :  A40
           Plant of manufacture . . . :  10
           Sequence number  . . . . . :  01234
           Common name  . . . . . . . :  AS/400
                                                      More...


         Press Enter to continue.

         F3=Exit   F12=Cancel
```

```
                                                  System:  ROCHESTR
         ----------Resource Hierarchy----------
         Resource Name        Resource Type
           ROCHESTR              CP
           ATLANTA               CP
           CC03                  LC
           RCHLIN                LNK


         Flags:
           Local/Received . . . . . . :   Received
           Operator generated . . . . :   No
           Held alert . . . . . . . . :   No
           Delayed alert  . . . . . . :   No
           Analysis available . . . . :   Yes

                                                      More...

         Press Enter to continue.

         F3=Exit   F12=Cancel
```

Sender hardware identification

Provides information to identify the hardware product for the alert sender.

This section is made up of one or more of the following fields. The exact fields present depend on what is present in the alert. The possible fields are:

Product classification What type of product this is:

- IBM hardware

- IBM or non-IBM hardware (not distinguished)

- Non-IBM hardware

Machine type A 4-digit descriptor of the machine type.

Model number The model number of the machine.

Plant of manufacture The IBM plant of manufacture.

Sequence number The sequence number of the machine originating the error record.

Common name The hardware common name as given in the product announcement.

Microcode EC level Engineering Change (EC) level of the failing microcode component.

Emulated machine type Type of the hardware product being emulated, if emulation is being done.

Emulated model number The model number of the product being emulated, if emulation is being done.

Flags

Lists flags associated with the alert. The flags displayed are:

Local/Received Specifies whether the alert was created locally or received from another system.

Operator generated Specifies if this alert was generated by a network operator.

Held alert Specifies if this alert has at any time been held at the sending system or an intermediate system because of problems with sending the alert.

Delayed alert Specifies if this is a delayed alert. A delayed alert reports the error condition that resulted in any held alerts.

Analysis available The analysis indicator is set to Yes if you can run problem analysis procedures on the problem.

Resource hardware identification

Provides information to identify the hardware product for the failing resource.

This section has the same fields possible as the Sender hardware identification section.

```
                                                    System:   ROCHESTR
    ----------Resource Hierarchy-----------
    Resource Name           Resource Type
     ROCHESTR                CP
     ATLANTA                 CP
     CC03                    LC
     RCHLIN                  LNK


    Sender software identification:
     Product classification . . :   IBM software
     Program product number . . :   5716SS1
     Version  . . . . . . . . . :   02
     Release  . . . . . . . . . :   01
     Level  . . . . . . . . . . :   00
     Common name  . . . . . . . :   OS/400


                                                         Bottom
    Press Enter to continue.

    F3=Exit   F12=Cancel
```

Sender software identification

Provides information to identify the software product for the alert sender.

This section is made up of one or more of the following fields. The exact fields present depend on what is present in the alert. The possible fields are:

Product classification Identifies what type of product this is.

- IBM software
- IBM or non-IBM software (not distinguished)
- Non-IBM software

Program product number The product number of the program.

Serviceable component ID Component identification of a serviceable component, as assigned by service personnel.

Serviceable component level The release level as assigned by service personnel.

Version The version of the program.

Release The release level of the program.

Level The level of the program.

Common name Common name of software.

Customization date Date when a set of instructions was customized to a user's environment.

Customization time Time when a set of instructions was customized to a user's environment.

Customization identifier Identification of a set of instructions, customized to a user's environment.

Resource software identification

Provides information to identify the software product for the failing resource.

This section has the same fields possible as the Sender software identification section.

```
                                                    System:   ROCHESTR
    ----------Resource Hierarchy-----------
    Resource Name           Resource Type
     ROCHESTR                CP
     ATLANTA                 CP
     CC03                    LC
     RCHLIN                  LNK


    LAN data
     Ring or bus ID . . . . . . :   0001
     Fault domain description . :   400014100000 400000002101




                                                         Bottom
    Press Enter to continue.

    F3=Exit   F12=Cancel
```

LAN data

Provides information related to local area network (LAN) errors.

This section is made up of one or more of the following fields. The exact fields present depend on what is present in the alert. The possible fields are:

LAN identifier Identifies a local area network (LAN).

Ring or bus ID Identifies the ring number for a token-ring local area network or the bus number for an Ethernet network. This is displayed in hexadecimal format.

Local individual MAC address Identifies the address of the medium access control (MAC) within the node sending the alert. This is displayed in hexadecimal format.

Remote individual MAC address Identifies the address of the medium access control (MAC), which is part of the link connection, within the adjacent node. This is displayed in hexadecimal format.

LAN routing information Identifies the routing information used by a link.

Fault domain description Identifies the location on the network where an error is likely to be occurring, typically bounded by the address of two stations; for example, the upstream and the downstream local area network stations and the cable between them. This field contains:

- Individual medium access control (MAC) address of downstream station in hexadecimal format.

- Individual medium access control (MAC) address of upstream station in hexadecimal format.

Beaconing data Message or data sent by a station that detects a problem.

Single MAC address Specifies the address of the medium access control (MAC) element associated with the failure.

Fault domain error weight pair Indicates the severity of the problems reported by two medium access control (MAC) elements (the reporting station or the nearest active upstream neighbor).

Bridge identifier Identifies the bridge identifier of a local area network (LAN) bridge. The bridge identifier is composed of the following:

- Ring or bus number

- Bridge number

- Another ring or bus number

 This is displayed in hexadecimal format.

Local individual MAC name Identifies the name of the medium access control (MAC) element within the sending node.

Remote individual MAC name Identifies the name of the medium access control (MAC) element, which is part of the link connection, within the adjacent node.

Fault domain names Identifies the names of the upstream and the downstream local area network (LAN) stations that define the location on the network where the error is likely to be occurring.

Single MAC name Identifies the name of the medium access control (MAC) element related to the failure.

MAC Type Identifies the type of media access control (MAC) sub-layer to which the sender is attached. FDDI, Ethernet, and token bus are possible media access control (MAC) sub-layer types.

FDDI Station ID Contains a unique identifier for the fiber distributed data interface (FDDI) station transmitting the frame data.

Frame Counter The hexadecimal count of all frames received by this media access control (MAC).

Error Counter The hexadecimal count of complete frames received in error by this media access control (MAC) and no previous station.

Lost Counter The hexadecimal count of frames and tokens detected with a format error by this Media Access Control (MAC) and no previous MAC.

Not Copied Counter The hexadecimal count of all frames addressed to this media access control (MAC) that were not copied, but should have been. One possible cause could be local buffer congestion.

Copied Counter The hexadecimal count of all frames that were successfully received into the station's buffers by a media access control (MAC) sub-layer.

Local Station Condition This field indicates whether or not a duplicate address occurs at this station. Upstream neighbor condition - Help

Upstream Neighbor Condition This field indicates whether or not a duplicate address occurs at the upstream neighbor.

Upstream Neighbor Address Duplicate Address The Media Access Control (MAC) address of the upstream neighbor with a duplicate address.

Link Error Rate Cutoff When the link error rate is less than or equal to this value, a connection is flagged as faulty. Link error rate is the exponent (in hexadecimal) of the total bits per error bit.

Link Error Rate Alarm When the link error rate is less than or equal to this value, an alarm condition occurs. Link error rate is the exponent (in hexadecimal) of the total bits per error bit.

Link Error Rate Estimate An average, long-term link error rate. Link error rate is the exponent (in hexadecimal) of the total bits per error bit.

Link Error Monitor Reject Counter This hexadecimal number counts the number of times a link has been removed because it exceeded the link cutoff threshold.

Link Error Monitor Counter A hexadecimal number counting all link error monitor (LEM) errors. This value is zeroed only during station initialization.

Configuration State The configuration state after a configuration change has occurred at a station or concentrator.

Paths Available The paths available after a configuration change has occurred. The possible values are primary, secondary, and local.

Port Connector Type The type of port connector from which an undesired connection has been attempted.

Connect State Indicates the connection state of the port on this station with an undesired connection.

Port Connector Neighbor Indicates the other port in the undesired connection, which resides in the neighbor station.

Connection Accepted Indicates whether or not the undesired connection attempt was accepted.

FDDI Trace Status Contains the current trace status of the path. FDDI Elasticity Buffer Error Counter - Help

FDDI Elasticity Buffer Error Counter A hexadecimal count of the number of times an elasticity buffer error has occurred.

FDDI Hold State Indicates whether the primary or secondary rings are operational and the recovery enable flag is clear.

FDDI MAC Index Contains the hexadecimal identifier for a particular media access control (MAC) sub-layer within a station.

FDDI Port Index A hexadecimal identifier of the communication port for the station

FDDI Path Index A hexadecimal identifier of the communication path for the station

FDDI Station Name Contains the name of the originating station.

Address Format This identifies the format or bit ordering of the media access control (MAC) addresses in this subvector. The possible values are canonical format and most significant bit first.

FDDI Peer Wrap Data A dual-attachment mode creates this field while it is wrapped and in peer-connection mode.

FDDI Neighbor Change Data These values are created when the FDDI neighbor notification protocol detects a change in either an upstream or a downstream media access control (MAC).

FDDI MAC Path Change Data These values are created when the current path value changes for any media access control (MAC). The change could occur from primary to secondary or from secondary to primary.

FDDI Port Path Change Data These values are created when the current path value changes for any port in a station. The change could occur from primary to secondary or from secondary to primary.

Note: Not all of these fields are displayed for every alert. The information displayed for each alert depends on information contained in the alert itself. The *SNA Formats* book contains more information on all the alert fields.

SNA Generic Alerts

The AS/400 system supports the SNA generic alert architecture. The text that makes up an alert is represented by **code points**. A code point is a 1-byte (2 hexadecimal characters) or 2-byte (4 hexadecimal characters) code that designates a particular piece of text to be displayed at the focal point. Code points are sent by an alert sender to convey alert data and are used to get the units of text for displaying alert data at a focal point.

An example of a code point is probable cause X'6314'. The text for this code point is Tape drive. The code point X'6314' is sent in the alert. The text Tape drive is displayed by the AS/400 system on the alerts displays.

Generic Alert Code Points: Generic alert code points are used in the following fields of the alert display:

- **Alert type**. The alert type code point defines the severity of the problem.

- **Alert description**. The alert description code point describes the alert condition.

- **Probable causes**. These codes define the most likely causes of the condition being described.

- **User causes**. These codes describe the conditions caused by a user and defined as conditions that can be resolved by the operator without contacting any service organization.

- **Install causes**. These codes describe conditions resulting from the initial installation or set-up of equipment.

- **Failure causes**. These codes describe conditions caused by the failure of a resource.

- **Recommended actions**. These codes describe actions that the focal point operator can take to correct the problem that caused the alert or to complete the process of problem analysis.

- **Qualifiers**. Detail qualifiers can appear in user, install, or failure causes, and in the recommended actions. They can also appear alone in the Qualifiers section of the Display Alert Detail display. The code point used for detail qualifiers is a data ID that identifies the detail qualifier.

- **Resource type**. These codes describe the type of resources that detected the error condition.

The AS/400 system uses the generic alert architecture. The code points are converted to a message ID, which is used to retrieve the text that is to be displayed on the alert displays from the alert message file. The name of the OS/400 alert message file is QALRMSG in library QSYS.

Default Code Points: A code point is of the form xxxx, where x is any hexadecimal digit (a 1-byte code point is of the form xx).

A default code point is a code point of the form xx00. Default code points are special because if the AS/400 system cannot find a code point xxxx in the QALRMSG alert message file, the AS/400 system also tries the default code point xx00. A default code point is less specific than the original code point, but still provides useful information. For example, the text for probable cause code point X'6314' is Tape drive. Probable cause code point X'6300' is Input/output device.

Adding Code Points to the OS/400 Alert Message File: If the AS/400 system cannot find a code point or its default in the QALRMSG alert message file, the text *UNKNOWN(xxxx) is displayed where the code point text would have been displayed. xxxx is the unknown code point.

The following conditions can result in an *UNKNOWN code point:

- A code point that is not contained in the latest release level of the OS/400 alert message file.

- User application code point. Code points X'E000' to X'EFFF' are reserved for use by non-IBM products and customer applications.

- The sending system is in error.

A default code point may be displayed instead of the more specific one.

To add a code point to your AS/400 system, you must create a message in the alert message file.

To create a code point message, you need to know the code point (either the 2-digit or 4-digit value), the code point type, and the message text. More information is contained in the *SNA Formats* book.

Determining the Message ID: The message ID for a code point consists of the code point plus a 3-character prefix. Table 3-6 shows the message ID prefixes for the alert code points:

Table 3-6. Converting a Code Point to a Message ID

3-Character Prefix	Code Point
ALD	Alert description
ALP	Probable cause
ALU	User cause
ALI	Install cause
ALF	Failure cause
ALR	Recommended action
ALT	Alert type
ALX	Detail data ID
ALZ	Resource type

For example, the message ID for failure cause X'1234' is ALF1234.

The code point for the detail qualifier data ID is only 2 hexadecimal digits. It is represented as a message ID by ALXcc00 where cc is the 1-byte (2 hexadecimal characters) code point. For example,

the message ID for detail data ID X'12' is ALX1200.

The code point for the resource type consists of only 2 hexadecimal digits. It is represented as a message ID by ALZcc00 where cc is the 1-byte (2 hexadecimal character) code point. For example, the message ID for resource type X'25' is ALZ2500.

The code point for alert type consists of only 2 hexadecimal digits. It is represented as a message ID by ALTcc00 where cc is the 1-byte (2 hexadecimal character) code point. For example, the message ID for alert type X'03' is ALT0300.

Code Point Text Length Restrictions: The length restrictions for the alert code point messages are as follows:

- Alert description, probable cause: 90 characters

- User/install/failure causes, recommended actions: 132 characters

- Resource type: 2 or 3 character abbreviation (for example, TAP DKT)

If you create a code point message that is longer than the length specified, the last part of the code point message text is not shown on the alert displays.

Detailed Qualifiers: Some of the generic alert code points contain detailed qualifiers. A detailed qualifier is one of the following:

- Detailed data qualifier

- Product identifier qualifier

These detailed qualifiers are sent in the alert with the code point, and are put together by the AS/400 system on the alert displays. The following code point types can contain detailed qualifiers:

- User causes

- Install causes

- Failure causes

- Recommended actions

Each code point can contain from 0 to 3 detailed data qualifiers (for example, Command DSPLOG QHST), or a code point can contain a product identifier qualifier (for example, AS/400).

The number of detailed data qualifiers a code point contains is determined by the code point itself. The **third** hexadecimal digit of the code point determines the number of qualifiers present in the code point. For code point X'xxYx', Y determines the number. Table 3-7 lists the number of qualifiers required by a code point with the given third digit.

Table 3-7. Number of Detailed Qualifiers for a Code Point

Third Digit	Number of Qualifiers
X'xx0x' - X'xx9x'	No detailed qualifiers
X'xxAx' - X'xxBx'	One detailed data qualifier
X'xxCx'	Two detailed data qualifiers
X'xxDx'	Three detailed data qualifiers
X'xxEx'	One product identifier qualifier

Substitution Text for Detailed Qualifiers:
When you create a code point message that contains detailed qualifiers, you must specify where the qualifiers will be displayed. The *SNA Formats* book defines where in the code point text the qualifiers appear; you can control if they appear on the same line as all the remaining code point text, or on the line or lines following the code point text.

To specify detailed qualifiers that appear on the same line as the code point text, you use substitution variables to define the placement of the qualifiers. Table 3-8 shows the substitution variable numbers that should be used for each qualifier.

Table 3-8. Substitution Variables Used for Detailed Qualifiers

Variable	Description
1	First detailed data qualifier
2	Second detailed data qualifier
3	Third detailed data qualifier
4	Product identifier qualifier

If the detailed qualifier placement is defined at the end of the code point text, you can omit the substitution variable at the end of the text, and the system displays the detailed qualifier on the line following the code point text.

Note: Detailed qualifiers that are defined in the middle of the code point text must have a substitution variable.

Example 1

For example, recommended action X'F0A0' (one detailed data qualifier) is defined as follows:

```
For &1;
```

It might appear on the alert displays as:

```
For System message code CPA58CC
```

Example 2

Recommended action X'00B2' (one detailed data qualifier) is defined as follows:

```
Run the following at the reporting location
```

It might appear on the alert displays as:

```
Run the following at the reporting location
  Command DSPLOG QHST
```

Example 3

Recommended action X'00E1' requires one product identifier qualifier, and is defined as:

```
Perform &4; problem analysis.
```

It might appear on the alert displays as:

```
Perform AS/400 problem analysis.
```

Creating a Message Description: To add code point text, use the code point to create a message ID and add a message description to the alert message file. For example, to add probable cause X'6314', `Tape device`, the message ID is `ALP6314`.

The name of the OS/400 alert message file is QALRMSG in library QSYS. Use the Add Message Description (ADDMSGD) command to add the code point message.

```
ADDMSGD MSGF(QSYS/QALRMSG) MSGID(ALP6314)
      MSG('Tape device')
```

The following command adds the code point message for **Example 1** on page 3-26.

```
ADDMSGD MSGF(QSYS/QALRMSG) MSGID(ALRF0A0)
      MSG('For &1')
      FMT((*CHAR *VARY 2) (*CHAR 0) (*CHAR 0) (*CHAR 0))
```

The following command adds the code point message for **Example 2** on page 3-26.

```
ADDMSGD MSGF(QSYS/QALRMSG) MSGID(ALR00B2)
        MSG('Run the following at the reporting location')
```

Since the detail qualifier text is placed on the next line, no substitution variables are defined.

The following command adds the code point message for **Example 3** on page 3-26.

```
ADDMSGD MSGF(QSYS/QALRMSG) MSGID(ALR00B2)
        MSG('Perform &4; problem analysis.')
        FMT((*CHAR 0) (*CHAR 0) (*CHAR 0) (*CHAR *VARY 2))
```

Displaying the Contents of the Alert Message File: To display the code points that are currently in the alert message file, use the Work with Message Description (WRKMSGD) command:

```
WRKMSGD MSGF(QSYS/QALRMSG)
```

Chapter 4. OS/400 Alert Filter Support

This chapter describes the OS/400 alert filter support on the AS/400 system. It describes how alert filters can be used to route and process Systems Network Architecture (SNA) alerts in a network and how to automate operations for local alerts or received alerts within a network.

Filter Components

Selection entry and action entry are the two components that comprises a filter. They can either work together or be used individually by a systems management application. Figure 4-1 on page 4-2

illustrates the components of a filter.

A network administrator decides how the filter should process the alerts. For example, the network administrator might want all diskette, tape, and display alerts to be handled by Joe Miller. The network administrator creates an **alert filter object**, which consists of the selection and action entries. In this example, the administrator creates a selection entry that assigns all diskette, tape, and display alerts to the group HARDWJOE. Then, the administrator creates an action entry for the group HARDWJOE that logs the alerts and assigns them to user JMILLER.

Selection Entries

Selection entries assign each alert processed by a filter to a group. Each selection entry includes a logical expression that relates the alert attributes to values. Within these logical expressions, *AND has precedence over *OR or *IF. Selection entries are evaluated in the order in which they are sequenced. The first true expression determines the group to which each alert is assigned.

The attributes describe what to look for in the alert, for example, *RSCNAME and *ALERTID. The value specifies what the attribute should be to provide a match for that particular alert, for example, "CHICAGO" and "01235FB4." In this example, if the alert has an *RSCNAME value equal to CHICAGO and an *ALERTID equal to 01235FB4, the alert is assigned to the group TEMPORARY.

Once an alert has satisfied a selection entry, it is assigned to a group. The group is also a character value defined by the network administrator. The selection entry allows the administrator to group classes of alerts.

For example, an administrator may want all alerts that are for diskettes, tapes, or displays to be assigned to the HARDWJOE group. The HARDWJOE group in the administrator's alert filter policy means hardware problems for which Joe is responsible. In addition, the administrator wants all alerts that are for temporary or impending problems assigned to the group BITBUCKET. The BITBUCKET group in the administrator's alert filter policy is for alerts that should not be logged.

Action Entries

Action entries specify what should be done to process each group of alerts. The actions are defined by the network administrator as part of the filter object. Part of the policy defines how the groups specified by the selection entries should be mapped to the actions that can be taken. Possible actions include:

- Logging the alert. Alerts can be used for tracking purposes.

- Routing the alert to an assigned user. Alerts can be assigned to a specific user. Operators can then display alerts assigned to them. This allows operators to work with alerts that have been specifically routed to them.

- Routing notification of the alert to a data queue. This enables a systems management application to monitor the data queue and take action when alerts are received. For example, an application can automate the responses to several groups of alerts.

- Routing the alert to another system in the network. By routing the alerts from an unattended to an attended system in the network, you can ensure that the alerts for the unattended system are processed.

In the previous example, the actions for group HARDWJOE may be to log the alert and then

assign the alert to the user JOE. The group BITBUCKET is not logged, so there are no other actions to perform. The alert is discarded.

Working with Alert Filters

Before you can begin working with alert filters, you need to establish your alert filter policy. Once you have established your policy, you can create the filters and their components. Filters and their components are created and maintained through a series of commands and displays. "Working with Alert Selection Entries" on page 4-3 and "Working with Alert Action Entries" on page 4-4 describe how to work with alert filter components.

Use the ALRFTR parameter of the Change Network Attribute (CHGNETA) command to specify the active alert filter.

Figure 4-2 on page 4-3 shows how an administrator works with the filter components.

Use the Work with Filters (WRKFTR) command to access all the filter functions available. The WRKFTR command allows you to work with a list of filters, change and delete filters, work with selection entries and action entries that are contained in filters, create new filters, and print the contents (selection and action entries) of the filters.

Note: Only the libraries for which you have READ authority are searched.

Only the filters for which you have some authority are shown on the display.

To perform operations on the filters, you must have USE authority to the command used by the operation and the appropriate authority to the filters on which the operation is to be performed.

When you enter the WRKFTR command, a display similar to the following is shown:

```
                                                    System:   RCHAS209
 Type options, press Enter.
   1=Create   2=Change   4=Delete   5=Work with filter selection entries
   6=Print    8=Work with filter action entries

 Opt  Filter      Library    Type     Text
  _
  _   ALRBACKUP   BACKUP     *ALR     Backup filter for Alerts
  _   ORIGINAL    BACKUP     *ALR     Original Alert filter
  _   ALERTFTR    NETMGMT    *ALR     Filter for Alert processing
  _   TIMOTHY     TGFLIB     *ALR     Alert filter for TGF
```

To create a filter, select option 1 (Create) from the Work with Filters display. A Create Filter (CRTFTR) display similar to the following appears.

```
 Type choices, press Enter.

 Filter . . . . . . . . . . . .                Name
   Library . . . . . . . . . .   *CURLIB___    Name, *CURLIB
 Type . . . . . . . . . . . . .                *ALR, *PRB
 Text 'description' . . . . . . .  *BLANK_____

                       Additional Parameters

 Authority . . . . . . . . . . .   *LIBCRTAUT    Name, *LIBCRTAUT, *CHANGE...
```

The filter can also be created using the Create Filter (CRTFTR) command. The following is an example of a CRTFTR command:
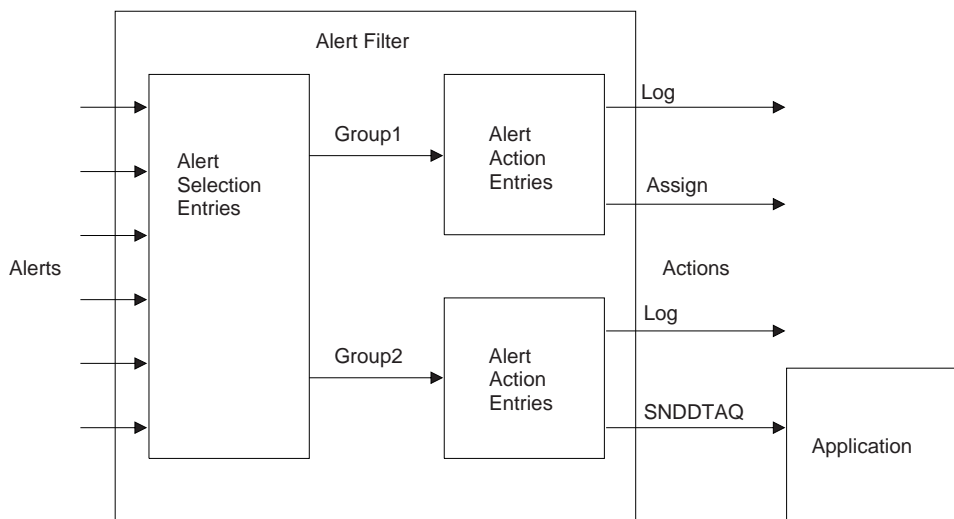
Figure 4-1. Example Filter Components

```
CRTFTR FILTER(MYLIB/MYFILTER)
      TYPE(*ALR)
      AUT(*CHANGE)
      TEXT('My filter')
```

This command creates an alert filter called
MYFILTER in the MYLIB library. The public has
*CHANGE authority to the filter. When a filter is
created, one selection entry and one action entry
are automatically added to the filter. For more
information about the CRTFTR command, see the
CL Reference book.

You can use the following options and commands
to change and delete filters:

Change   Select option 2 (Change) from the
             Work with Filters display, or use the
             Change Filter (CHGFTR) command.

Delete   Select option 4 (Delete) from the Work
             with Filters display, or use the Delete
             Filter (DLTFTR) command.

Working with Alert Selection Entries

Use the Work with Filter Selection Entries
(WRKFTRSLTE) command to access all the filter
selection entry functions available. The
WRKFTRSLTE command allows you to work with

a list of filter selection entries to add, change,
copy, remove, display, move, or print selection
entries. For information on printing selection
entries, see "Printing Alert Filters and Filter
Components" on page 4-5.

When you enter the WRKFTRSLTE command, a
display similar to the following is shown. You can
also access this display by selecting option 5
(Work with filter selection entries) on the Work
with Filters display.

```
                                          System:   RCHAS209
Filter . . . . . . . . :  TIMOTHY
  Library . . . . . . . :     TGFLIB
  Type  . . . . . . . . :     *ALR

Type options, press Enter.
  1=Add    2=Change   3=Copy    4=Remove   5=Display   7=Move

     Sequence
Opt  Number    Group        Selection data

_    0010      HARDWJOE     *IF *RSCTYPE *EQ DKT *OR *RSCTYPE *EQ TAP
_    0020      HARDWARE1    *IF *MSGID *CT 9999 *AND *MSGSEV *GT 40
_    0030      GROUP1       *IF *HARDWARE *CT '9406 ' *OR *HARDWARE *CT '9...
_    0040      BITBUCKET    *IF *RSCNAME *EQ CHI* *OR *RSCNAME *EQ DET*
_    0050      GROUP2       *IF *MSGID *EQ CPF1234 *OR *MSGID *EQ CPD8933 ...
_    0065      GROUP1       *IF *MSGID *NE CPF9999 *AND *MSGSEV *GE 40
_    0080      *DEFAULT     *IF *MSGID *NE CPF9999 *AND *MSGSEV *LT 40
_    *LAST     *DEFAULT     *ANY
```

To create an alert selection entry, select option 1
(Add) from the Work with Filter Selection Entries
display. An Add Alert Selection Entry
(ADDALRSLTE) display similar to the following
appears.
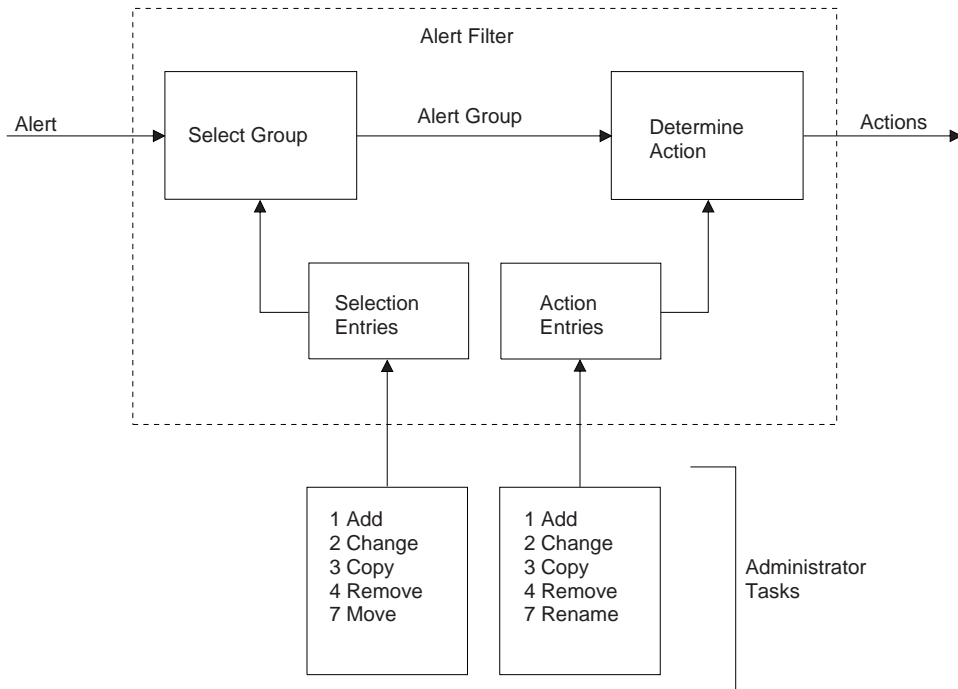
Figure   4-2. Maintaining Filter Components

```
┌──────────────────────────────────────────────────┐
│                                                  │
│  Type choices, press Enter.                      │
│                                                  │
│  Filter . . . . . . . . . . . . .  MYFILTER   Name │
│    Library . . . . . . . . . . .   MYLIB____  Name, *LIBL, *CURLIB │
│  Selection data:                                 │
│    Relationship . . . . . . . . _  *IF_____   *ANY, *IF, *AND, *OR │
│    Attribute  . . . . . . . . .    *RSCNAME__  *ORIGIN, *RSCNAME... │
│    Relational operator . . . . .   *EQ____    *EQ, *GT, *LT, *NE, *GE... │
│    Value  . . . . . . . . . . .    CHICAGO1_____ │
│               + for more values _                │
│  Sequence Number . . . . . . . .   *GEN       1-9999, *GEN │
│  Group . . . . . . . . . . . . .   CHICAGO___  Name, *DEFAULT │
│                                                  │
│                                                  │
└──────────────────────────────────────────────────┘
```

After the filter is created, specific selection and action entries can be added. Use the Add Alert Selection Entry (ADDALRSLTE) display to add specific selection entries to a filter. This display allows you to define selection criteria used to group alerts by categories. Selection entries can also be added using the Add Alert Selection Entry (ADDALRSLTE) command.

The following is an example of an ADDALRSLTE command:

```
ADDALRSLTE FILTER(MYLIB/MYFILTER)
           SELECT((*IF *RSCNAME *EQ CHICAGO1)
                  (*AND *RSCTYPE *EQ CP))
           SEQNBR(*GEN)
           GROUP(CHICAGO)
```

This command adds sequence number 10 to the MYFILTER filter in the MYLIB library. An entry with a position of 10 is created because this is the first entry that has been added to the filter. *GEN produces a sequence number greater than the highest available sequence number in increments of or within boundaries of 10. Any alerts that have a resource name of CHICAGO1 and a resource type of control point (CP) are assigned to the CHICAGO group. For more information about the ADDALRSLTE command, see the *CL Reference* book.

You can use the following options and commands to change and remove alert selection entries:

Change Select option 2 (Change) from the Work with Filter Selection Entries display, or use the Change Alert Selection Entry (CHGALRSLTE) command.

Remove Select option 4 (Remove) from the Work with Filter Selection Entries display, or use the Remove Alert Selection Entry (RMVFTRSLTE) command.

Working with Alert Action Entries

Use the Work with Filter Action Entries (WRKFTRACNE) command to access all the filter action entry functions available. The WRKFTRACNE command allows you to work with a list of filter action entries to add, change, copy, remove, display, rename, or print action entries. For information on printing action entries, see "Printing Alert Filters and Filter Components" on page 4-5.

When you enter the WRKFTRACNE command, a display similar to the following is shown. You can also access this display by selecting option 8 (Work with filter action entries) on the Work with Filters display.

```
┌──────────────────────────────────────────────────┐
│                                    System:  RCHAS209 │
│  Filter . . . . . . . . . :   TIMOTHY            │
│    Library . . . . . . . . :     TGFLIB          │
│    Type . . . . . . . . . :     *ALR             │
│                                                  │
│  Type options, press Enter.                      │
│   1=Add  2=Change  3=Copy   4=Remove  5=Display  7=Rename │
│                                                  │
│  Opt  Group       Actions                        │
│                                                  │
│   _   BITBUCKET   LOG(*NO) ASNUSER(*NONE) SEND (*NONE) SNDDTAQ(*NONE) │
│   _   GROUP1      LOG(*YES) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE) │
│   _   GROUP2      LOG(*NETATR) ASNUSER(THOMAS) SEND(APPN.DETROIT) SEND(*FOC... │
│   _   HARDWARE1   LOG(*YES) ASNUSER(*NONE) SEND(*FOCALPT) SEND(NORTHWST.STP... │
│   _   HARDWARE2   LOG(*YES) ASNUSER(*NONE) SEND(*NONE) SNDDTAQ(USERLIB/HARD... │
│   _   JOES        LOG(*NETATR) ASNUSER(CARL) SEND(*FOCALPT) SNDDTAQ(*NONE) │
│   _   TEMPLOOK    LOG(*YES) ASNUSER(JOSHUA) SEND(*NONE) SNDDTAQ(*NONE) │
│   _   TROUBLE     LOG(*YES) ASNUSER(DEBRA) SEND(*FOCALPT) SEND(EASTSEA.HEAD... │
│   _   *DEFAULT    LOG(*NETATR) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE) │
│                                                  │
└──────────────────────────────────────────────────┘
```

To add an alert action entry, select option 1 (Add) from the Work with Filter Action Entries display. An Add Alert Action Entry (ADDALRACNE) display similar to the following appears. This is the first part of a two-part display.

```
┌──────────────────────────────────────────────────┐
│                                                  │
│  Type choices, press Enter.                      │
│                                                  │
│  Filter . . . . . . . . . . . . .             Name │
│    Library . . . . . . . . . . .   *LIBL_____ Name, *LIBL, *CURLIB │
│  Group  . . . . . . . . . . . . .             Name │
│  Log alert . . . . . . . . . . .   *NETATR___ *YES, *NO, *NETATR │
│  User assigned . . . . . . . . .   *NONE_____ Name, *NONE │
│  Send to system:                                 │
│    Network ID . . . . . . . . .    *NONE_____ Name, *NETATR, *FOCALPT... │
│    Control Point . . . . . . . .   _____  Name │
│               + for more values _                │
│                                                  │
└──────────────────────────────────────────────────┘
```

You can page down to see the second part of the display. It is similar to the following:

```
┌──────────────────────────────────────────────────┐
│                                                  │
│  Type choices, press Enter.                      │
│                                                  │
│  Send to data queue:                             │
│    Data queue . . . . . . . . . _  *NONE_____ Name, *NONE │
│      Library . . . . . . . . . .   _____  Name, *LIBL, *CURLIB │
│    Data queue key . . . . . . . .  _____ │
│    _____ │
│    _____               │
│               + for more values _                │
│                                                  │
└──────────────────────────────────────────────────┘
```

After the selection entries are created, specific action entries can be added in any order. Use the Add Alert Action Entry (ADDALRACNE) display to add specific action entries to a filter. The action entries define the actions that should be taken for an alert that has been assigned to the specified group. This display allows you to define the actions for the specified group. Action entries can also be added using the Add Alert Action Entry (ADDALRACNE) command. The following is an example of an ADDALRACNE command:

```
ADDALRACNE FILTER(MYLIB/MYFILTER)
           GROUP(CHICAGO)
           LOG(*NETATR)
           ASNUSER(CHICAGOOPR)
           SEND(*FOCALPT) SEND(*NETATR.MILWKEE)
           SNDDTAQ(*LIBL/ALERTDTAQ)
```

This command adds the action entry which defines the actions for the group CHICAGO. The actions are:

- Log the alert based on the ALRLOGSTS network attribute.
- Send the alert to this system's focal point and send the alert to the system with the control point name MILWKEE.
- Send notification of the alert to the ALERTDTAQ data queue.
- Assign the alert to user CHICAGOOPR.

For more information about the ADDALRACNE command, see the *CL Reference* book.

You can use the following options and commands to change and remove alert action entries:

Change Select option 2 (Change) from the Work with Filter Action Entries display, or use the Change Alert Action Entry (CHGALRACNE) command.

Remove Select option 4 (Remove) from the Work with Filter Action Entries display, or use the Remove Alert Action Entry (RMVFTRACNE) command.

Printing Alert Filters and Filter Components

To print the selection and action entries for an alert filter, press F6 (Print) on the Work with Filter (WRKFTR) display. The print command creates a spool file. The spool file contains all selection entries in sequence followed by all action entries in sequence for the filter you select.

Figure 4-3 on page 4-6 is an example printout of a filter. The selection entries added using the ADDALRSLTE command and the action entries added using the ADDALRACNE command are shown. The default entries added when the filter was created are also included.

To print only the selection entries for a filter, press F6 (Print) from the Work with Selection Entries (WRKSLTE) display. To print only the action entries for a filter, press F6 (Print) from the Work with Action Entries (WRKACNE) display.

Setting Up Alert Filters for a Network

The following expands on the example that was initially presented in section " Setting Up Alert Filters for a Network—Scenario" on page 1-9.

Creating the Alert Filter for the ATLANTA System

To set up this alert routing, the network administrator uses alert filters. To create the filters, the Create Filter (CRTFTR) command is used. The CRTFTR command creates a filter with a default selection entry and a default action entry. In this example, the network administrator starts with the ATLANTA system. The filter for the ATLANTA system must send all alerts to STLOUIS and also send tape alerts to CHICAGO. The network administrator types the following command:

```
CRTFTR FILTER(ALRLIB/FILTER3)
       TYPE(*ALR)
       AUT(*EXCLUDE)
       TEXT('Alert filter for the ATLANTA system')
```

This command creates a filter called FILTER3 in library ALRLIB. The type is *ALR and the public has no authority to the filter.

Adding Alert Selection Entries: After the filter is created, the specific selection and action entries can be added. The Add Alert Selection Entry (ADDALRSLTE) command allows you to define selection criteria that will categorize a group of alerts. In this example, the filter policy states that all tape alerts are to be grouped. The network administrator types the following command:

```
ADDALRSLTE FILTER(ALRLIB/FILTER3)                          ADDALRACNE FILTER(ALRLIB/FILTER3)
           SELECT(*IF *RSCTYPE *EQ TAP)                                GROUP(TAPERROR)
           SEQNBR(10)                                                  LOG(*NETATR)
           GROUP(TAPERROR)                                             SEND(*NETATR.CHICAGO)
                                                                       SEND(*FOCALPT)
```

This command adds a selection entry 10 to the filter FILTER3 in library ALRLIB. A sequence number of 10 places this entry first in the filter. This is the first entry that is read by the filter. Any alerts that have a resource type of TAP are assigned to the group TAPERROR.

Adding Alert Action Entries: After the selection entries are added, the action entries can be added. The Add Alert Action Entry (ADDALRACNE) command adds an entry to the specified alert filter. The entry describes the actions that should be taken for an alert that has been assigned to the specified group.

In this example, the filter policy states that all tape alerts are sent to CHICAGO. The network administrator types the following command:

The actions defined for alerts in the group TAPERROR are:

1. Log the alert based on the ALRLOGSTS network attribute.

2. Send the alert to the system CHICAGO.

3. Send the alert to the focal point system.

Printing the Alert Filter: To check the entries, the network administrator uses a printout of the filter object. The network administrator can obtain a printout of the selection and action entries for a filter by option 6 (Print) on the Work with Filter (WRKFTR) display. The print command creates a spool file. The spool file contains all selection entries in sequence followed by all action entries in sequence. Figure 4-4 on page 4-7 is an example printout of the FILTER3 filter used on the ATLANTA system.

```
                                   Display Filter                         Page     1


Filter . . . . . . . . :    TIMOTHY
  Library . . . . . . . :     TGFLIB
  Type  . . . . . . . . :     *ALERT
  Text  . . . . . . . . :     Timothy's filter


-------------------------------Selection Entries---------------------


Sequence
Number      Group        Selection data


0010        HARDWARE1    *IF *MSGID *CT 9999 *AND *MSGSEV *GT 40
0020        GROUP1       *IF *HARDWARE *CT '9406 ' *OR *HARDWARE *CT '9404 '
0030        BITBUCKET    *IF *RSCNAME *EQ CHI* *OR *RSCNAME *EQ DET*
0040        GROUP2       *IF *MSGID *EQ CPF1234 *OR *MSGID *EQ CPD8933 *OR *MSGID *EQ CPI9807 *AND *RSCNAME *EQ DETROIT
0065        GROUP1       *IF *MSGID *NE CPF9999 *AND *MSGSEV *GE 40
0080        *DEFAULT     *IF *MSGID *NE CPF9999 *AND *MSGSEV *LT 40
0090        JOES         *IF *MSGSEV *LE 30 *AND *MSGID *LT CPF*
*LAST       *DEFAULT     *ANY


----------------------------------Action Entries---------------------


Group       Actions


BITBUCKET   LOG(*NO) ASNUSER(*NONE) SEND(*NONE) SNDDTAQ(*NONE)
GROUP1      LOG(*YES) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE)
GROUP2      LOG(*NETART) ASNUSER(THOMAS)SEND(APPN.DETROIT) SEND(*FOCALPT) SNDDTAQ(*NONE)
HARDWARE1   LOG(*YES) ASNUSER(*NONE) SEND(*FOCALPT) SEND(NORTHWST.STPAUL) SNDDTAQ(USERLIB/HARDWAREQ)
HARDWARE2   LOG(*YES) ASNUSER(*NONE) SEND(*NONE) SNDDTAQ(USERLIB/HARDWAREQ)
JOES        LOG(*NETART) ASNUSER(CARL) SEND(*FOCALPT) SNDDTAQ(*NONE)
TROUBLE     LOG(*YES) ASNUSER(DEBRA) SEND(*FOCALPT) SEND(EASTSEA.HEADQRTS) SNDDTAQ(*CURLIB/TROUBLEQ)
            SNDDTAQ(*LIBL/TEMP) SNDDTAQ(*CURLIB/TROUBLEQ)
TEMPLOOK    LOG(*YES) ASNUSER(JOSHUA) SEND(*NONE) SNDDTAQ(*NONE)
*DEFAULT    LOG(*NETATR) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE)
                                   * * * * *  E n d  O f  L i s t i n g  * * * * *
```

Figure   4-3. Example Alert Filter Printout

```
Filter  . . . . . . . . :     FILTER3
  Library . . . . . . . :      ALRLIB
  Type  . . . . . . . . :       *ALR
  Text  . . . . . . . . :       Alert filter for the ATLANTA system


-------------------------------Selection Entries---------------------


Sequence
Number        Group        Selection data

0010          TAPERROR     *IF *RSCTYPE *EQ TAP
*LAST         *DEFAULT     *ANY

-------------------------------Action Entries---------------------


Group          Actions

TAPERROR       LOG(*NETATR) ASNUSER(*NONE) SEND(*NETATR.CHICAGO) SEND(*FOCALPT) SNDDTAQ(*NONE)
*DEFAULT       LOG(*NETATR) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE)
                              * * * * *  E n d  O f  L i s t i n g  * * * * *
```

Figure   4-4. Example Alert Filter Used on the ATLANTA System

Creating the Alert Filter for the SEATTLE System

The alert filter for the SEATTLE system is the same as for the ATLANTA system.

Creating the Alert Filter for the CHICAGO System

To create the filter for the CHICAGO system, the network administrator reviews the filter policy for that system. All tape-related alerts from SEATTLE, ATLANTA, and STLOUIS are received by CHICAGO. All CHICAGO alerts are sent to the focal point STLOUIS for processing. Figure 4-5 on page 4-8 is an example printout of the FILTER4 filter used on the CHICAGO system.

Creating the Alert Filter for the STLOUIS System

The last filter to add is for the focal point system STLOUIS. To create the filter for the STLOUIS system, the network administrator reviews the filter policy for that system. All alerts from all systems are forwarded to STLOUIS. Tape alerts are sent to CHICAGO.

After creating the filter and adding the selection and action entries, the network administrator prints out a copy of the STLOUIS filter. Figure 4-6 on page 4-9 is an example printout of the FILTER1 filter used on the focal point STLOUIS system.

Figure 4-6 on page 4-9 shows that the local alerts and the received alerts are filtered through the FILTER1 filter. The filter definition states that all tape alerts originating at the local system are assigned to the TAPERROR group. The filter definition also sends a notification of all alerts from the TAPERROR group to the ALERTDTAQ data queue and sends them to the CHICAGO system. All other alerts are logged in the ALERTDTAQ data queue and remain on the STLOUIS system.

The complete alert routing for the network is shown in Figure 4-7 on page 4-10.

Using a Systems Management Application with Alert Filters

In addition to demonstrating alert routing, the network described in Figure 4-7 on page 4-10 shows how a systems management application can use filters.

The network administrator can track how many alerts of each type are created on each system in the network. To do this, the network administrator asks a systems programmer to write an accounting application that monitors the data queue. The network administrator designs the filters to forward notifications of alerts from all systems to the STLOUIS system and to add notification of those alerts to the ALERTDTAQ data queue. The systems management application monitors the data queue. Using the notification

```
                                        Display Filter                           Page    1

Filter  . . . . . . . . . :     FILTER4
  Library . . . . . . . . :       ALRLIB
  Type  . . . . . . . . :         *ALR
  Text  . . . . . . . . :         Alert filter for the CHICAGO system

-------------------------------Selection Entries---------------------

Sequence
Number         Group         Selection data

0010           LOCALTAPE     *IF *RSCTYPE *EQ TAP *AND *ORIGIN *EQ L
0010           REMOTETAPE    *IF *RSCTYPE *EQ TAP
*LAST          *DEFAULT      *ANY

---------------------------------Action Entries---------------------

Group          Actions

LOCALTAPE      LOG(*NETATR) ASNUSER(TAPEOPR) SEND(*FOCALPT) SNDDTAQ(*NONE)
REMOTETAPE     LOG(*NETATR) ASNUSER(TAPEOPR) SEND(*NONE) SNDDTAQ(*NONE)
*DEFAULT       LOG(*NETATR) ASNUSER(*NONE) SEND(*FOCALPT) SNDDTAQ(*NONE)
                                  * * * * *  E n d  O f  L i s t i n g  * * * * *
```

Figure 4-5. Example Alert Filter Used on the CHICAGO System

information in the data queue, the application produces a weekly report that shows the number of alerts of each type that were created on each system for the preceding week. You can use the QALRTVA API to retrieve the alerts from the alert database from notifications on the data queue.

```
Filter . . . . . . . . :    FILTER1
  Library . . . . . . . :    ALRLIB
  Type  . . . . . . . . :      *ALERT
  Text  . . . . . . . . :    Alert filter for the STLOUIS System

-------------------------------Selection Entries---------------------

Sequence
Number        Group        Selection data

0010          TAPERROR     *IF *RSCTYPE *EQ TAP *AND *ORIGIN *EQ L
*LAST         *DEFAULT     *ANY

----------------------------------Action Entries---------------------

Group          Actions

TAPERROR       LOG(*NETATR) ASNUSER(*NONE) SEND(*NETATR.CHICAGO) SNDDTAQ(*ALRLIB/ALERTDTAQ)
*DEFAULT       LOG(*NETATR) ASNUSER(*NONE) SEND(*NONE) SNDDTAQ(*ALRLIB/ALERTDTAQ)
                                 * * * * *  E n d  O f  L i s t i n g  * * * * *
```

Figure   4-6. Example Alert Filter Used on the STLOUIS System

Sphere of Control

SEATTLE
CHICAGO
ATLANTA

STLOUIS
AS/400 System

Focal Point

Local
Alerts

FILTER1

SEATTLE
AS/400 System

Entry
Point

FILTER2

Local
Alerts

Test System

CHICAGO
AS/400 System

Entry
Point

FILTER4

Tape
Alerts

Local
Alerts

Tape Operator
(TAPEOPR)

ATLANTA
AS/400 System

Entry
Point

FILTER3

Local
Alerts

Legend:

All Alerts

TAP* Alerts Only
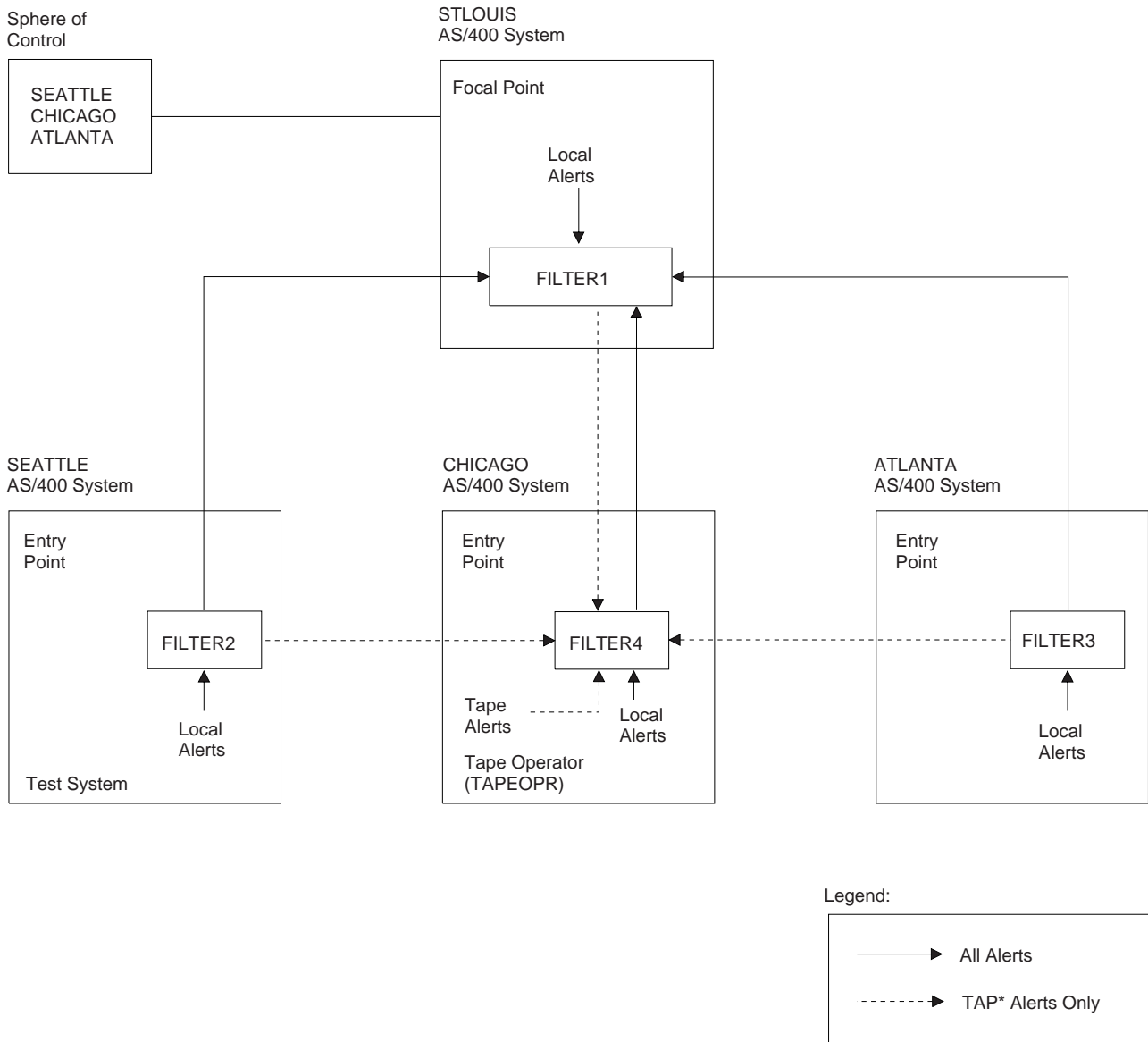
RV2P904-1

Figure   4-7. Example Alert Network Using Alert Filters

Appendixes

Appendix A. Sample Procedures for OS/400 Alerts

You may find it useful to add your own alert descriptions for user-defined messages or to change or add to the alert descriptions for IBM-supplied messages. For example, if you have an application program that sends messages to the network operator, by defining your own alert descriptions you can provide the operator with specific information about the cause of the problem and specify your own recovery procedure.

You need to create your own alert table to add alert descriptions for user-defined messages. To change or add to the alert descriptions for IBM-supplied messages, you need to change the IBM-supplied alert table (for example, QCPFMSG).

Examples of Creating an Alert Table

In the following example, the CRTALRTBL command is used to create alert table ALRTBLNBR1 in library ALRTBLLIB.

```
CRTALRTBL ALRTBL(ALRTBLLIB/ALRTBLNBR1)
          AUT(*CHANGE)
          LICPGM(5738SS1)
          LICPGMTXT('OS/400-Customer version')
          TEXT('This is the first ALRTBL created')
```

The public has *CHANGE authority to the table. The program associated with this alert table is the OS/400 licensed program. The alert includes the release and level information for the OS/400 program, along with the text, `OS/400-Customer version`.

In the following example, the CRTALRTBL command is used to create alert table CUSTALRTBL in library ALRTBLLIB.

```
CRTALRTBL ALRTBL(ALRTBLLIB/CUSTALRTBL)
          AUT(*CHANGE)
          LICPGM(CUST001)
          LICPGMTXT('Customer application 001')
          TEXT('Customer application alert table')
```

The public has *CHANGE authority to the table. The program associated with this alert table is CUST001. The licensed program ID CUST001 and the text `Customer application 001` are sent in the alert. Since CUST001 is not a recognized licensed program, no release or level information is sent in the alert.

An Example of Adding an Alert Description

Figure A-1 defines an alertable message and the alert for the message. The message APP1000 is in message file CAPPL1 in library CAPPL1LIB. The alert table name is CAPPL1, the same name as the message file.

In Figure A-1, the message file and the alert table are both in the CAPPL1LIB library. Although they must use the same name, they are not required to be in the same library. The alert table *does* have to be in the library list of the job that sends the message that causes the alert.

```
CRTLIB LIB(CAPPL1LIB) TEXT('Customer application 1 library')

ADDLIBLE LIB(CAPPL1LIB)

CRTMSGF MSGF(CAPPL1LIB/CAPPL1)
        TEXT('Customer application 1 - message file')

CRTALRTBL ALRTBL(CAPPL1LIB/CAPPL1) LICPGM(CAPPL10)
          LICPGMTXT('Customer Application 0001')
          TEXT('Customer Application 1 - alert table')

ADDMSGD MSGID(APP1000) MSGF(CAPPL1LIB/CAPPL1)
        MSG('Application program &1; failed while writing to
            file &2; library &3; with reason code &4;')
        SECLVL('The information could not be written to the file.
             The file is possibly full.')
        SEV(80)
        FMT((*CHAR 10) (*CHAR 10) (*CHAR 10) (*BIN 2))
        ALROPT(*IMMED)

ADDALRD MSGID(APP1000) ALRTBL(CAPPL1LIB/CAPPL1)
        ALRTYPE(01) ALRD(2100)
        PBLCAUSE(1000 7004 7001)
        CAUSE((*USER 73A0 D0 '&2');
              (*USER 73A1 D0 '&2');
              (*FAILURE 10E1 *NONE *NODATA
                              *NONE *NODATA
                              *NONE *NODATA
                              *SNDSFW))
        ACTION((*USER 32C0 D0 '&2'; 00 '&3');
               (*USER 1300)
               (*FAILURE 32C0 A6 '&1'; 0E '&4');
               (*FAILURE F0A0 20 'APP1000')
               (*FAILURE F008))
```

Figure A-1. Example Alertable Message Definition and Alert

Figure A-1 defines a recommended action 32C0, which requires 2 detailed data qualifiers. The detailed data ID A6 uses message substitution variable &1 as detailed data. The detailed data ID 0E uses message substitution variable &4 as detailed data.

Recommended action F0A0 specifies detailed data 'APP1000'.

Recommended action F008 specifies no detailed data.

Example of Alertable Message with Substitution Variables

When a message is sent using the Send Program Message (SNDPGMMSG) command, the alert description and message description can be displayed. Using the alert description and message description from the previous example, the following message is shown in the QSYSOPR message queue:

```
                                          System:   ROCHSTR
Queue . . . . . :  QSYSOPR      Program . . . . :  *DSPMSG
 Library . . . :    QSYS         Library . . . :
Severity . . . :  70            Delivery . . . :   *BREAK

Press Enter to continue.
 Application program CAPPL0001 failed while writing to file CSTFILA library
   DATALIBA with reason code 34.
```

The message is defined as alertable and a message is created. Using the WRKALR

command, and selecting option 5 (Display recommended actions), a display similar to the following is shown:

```
                    Display Recommended Actions
                                          System:   ROCHSTR
----------Resource Hierarchy-----------
Resource Name        Resource Type
 ROCHSTR              CP



User causes . . . . . . :   File full: File name CSTFILA
                            File needs reorganization: File name CSTFILA
Actions . . . . . . . . :   Report the following
                              File name CSTFILA
                                DATALIBA
                            Correct then retry
Failure causes  . . . . :   Software program Customer Application 0001
Actions . . . . . . . . :   Report the following
                              Program CAPPL0001
                                                        More...
```

The alert is created using the alert description for the message ID APP1000 in alert table CAPPL1. Substitution variables are filled in. The product identifier Customer Application 0001 is filled in.

Using the WRKALR command, and selecting option 8 (Display alert detail), the alert type, alert description, and probable cause are shown.

```
                                          System:   ROCHSTR
----------Resource Hierarchy-----------
 Resource Name        Resource Type
  ROCHSTR              CP



Logged date/time . . . . . . :   01/11/91  09:49:44
Problem date/time . . . . . :   01/11/91  09:49:44
Assigned user  . . . . . . . :
Group filter . . . . . . . . :
Alert type . . . . . . . . . :   Permanent
Alert description  . . . . . :   Software program error
Probable cause . . . . . . . :   Software program
```

Appendix B.   IBM-Supplied Alertable Messages

This appendix lists the alertable messages shipped with the OS/400 licensed program in the QCPFMSG message file. A message is alertable if the alert option (ALROPT) parameter is set to one of the following:

*IMMED   Send alert immediately

*DEFER   Send alert after local problem analysis

*UNATTEND Send alert for an unattended system

QCPFMSG Messages with ALROPT(*IMMED)

CPA57A1 Controller &24; contact not successful. (C R)

CPA57EB Controller &24; not found on token-ring network. (C G R)

CPA57EC Controller &24; failed. Probable remote station problem. (C G R)

CPA57EF Controller &24; contact not successful. Probable remote station problem. (C R)

CPA57E1 All sessions to controller &24; failed. Data may be lost. (C G R)

CPA57E4 Controller &24; contact not successful on line &23; (C R)

CPA5748 Controller &24; failed. Probable X.25 network problem. (C G R)

CPA5779 Controller &24; on line &23; not contacted. (C R)

CPA579A Controller &24; contact not successful. (C R)

CPA579B Controller &24; contact not successful. Probable X.25 network problem. (C G R)

CPA58AA Controller &24; failed. Data buffer exceeded (C G R)

CPA58AB Contact not successful for controller &24; Data buffer exceeded. (C G R)

CPA58AC Contact not successful for controller &24; Data buffer exceeded. (C R)

CPA58ED Controller &24; failed. Probable local system problem. (C G R)

CPA58EE Line &23; failed. Probable cabling or hardware problem. (C G R)

CPA58E4 Call on line &23; failed, packet mode connection not supported by the network (C N R).

CPA58F7 Line &23; failed while attached to network interface &30; Network is not ready. (C G R)

CPA58F8 Line &23; contact not successful on network interface &30; Network is not ready. (C N R)

CPA5808 Cannot communicate with device &25; Probable local system problem. (C R G)

CPA583A Controller &24; failed. Resources not sufficient. (C G R)

CPA5841 Controller &24; failed. Probable remote system problem. (C G R)

CPA5878 Internal system failure. Contact not successful on controller &24; (C R)

CPA5879 Contact not successful for controller &24; Internal system failure. (C G R)

CPA59DE Controller &24; contact not successful. Logical channel recovering from error. (C G R)

CPA59DF Controller &24; contact not successful. Probable local system problem. (C R)

CPA59D0 Line &23; failed. HDLC link disconnected. (C G R)

CPA59D5 Line &23; failed. HDLC link disconnected. (C G R)

CPA59F1 Internal system failure on line &23; (C G R)

CPA59F3 Controller &24; failed. Internal system failure. (C G R)

CPA59F8 Internal system failure on network interface &30; (C G R)

CPA596F Controller &24; contact not successful on line &23; (C R)

CPC3A34 Abnormal end of SNADS *SVDS sender &3/&2/&1; serving distribution queue &4;

CPC3A40 Abnormal end of SNADS *SVDS receiver &3/&2/&1; using distribution queue &4;

CPC8801 Job ended abnormally for SNADS sender &3/&2/&1,; serving *SNADS distribution queue &5;

CPC8803 SNADS router &3/&2/&1; ended abnormally.

CPC8805 SNADS receiver &3/&2/&1; ended abnormally.

CPC8821 Job ended abnormally for SNADS gateway sender &3/&2/&1,; serving &5; distribution queue &4;

CPC8858 Receive function for DSNX object distribution ended abnormally.

CPC8859 DSNX request processor ended.

CPC8860 DSNX host interface function ended abnormally.

CPC8870 DSNX cannot be received temporarily.

CPD0025 Internal error processing variable &2;

CPD2688 Mode not defined for device &25;

CPD27CD Line &23; vary on failed.

CPD27CE Controller &24; vary on failed.

CPD27CF Device &25; vary on failed.

CPD27D0 Line &23; vary on failed.

CPD27D1 Controller &24; vary on failed.

CPD27D2 Device &25; vary on failed.

CPD2740 Device &25; vary processing stopped.

CPD278A Line &23; vary on failed.

CPD278B Controller &24; vary on failed.

CPD278C Device &25; vary on failed.

CPD2896 Device &25; vary on stopped.

CPD2897 Controller &24; vary on stopped.

CPD3B64 Internal failure attempting to allocate conversation.

CPD8EB4 Device &25; vary on failed.

CPD8E47 Network interface &30; vary on failed.

CPD8E7C Network interface &30; vary on failed.

CPD8F79 Network server &30; vary on failed.

CPD9320 Error condition detected during analysis. Report error.

CPFAFA0 Errors detected on MSF internal message index.

CPFAFA1 Errors detected on MSF internal message queue.

CPFAF95 MSF job &4/&3/&2; ended. Reason code &1;

CPFAF98 Job &6/&5/&4; stopped processing MSF message.

CPF0907 Serious storage condition may exist. Press HELP.

CPF0908 Machine ineligible condition threshold reached.

CPF0909 Ineligible condition threshold reached for pool &1;

CPF0937 Machine check not recoverable. Error code &2;

CPF0957 System may not be able to start new jobs. Press HELP.

CPF0996 Storage usage reached critical point and must be reduced.

CPF111C System scheduled to power down.

CPF111D System is powering down.

CPF1816 System utility power failed at &1;

CPF1818 System ending. Power failure notification failed.

CPF1819 System ending. Power failure message not monitored.

CPF3B79 Internal system error has occurred.

CPF3E23 DDM data stream violates conversation capabilities.

CPF3E80 Syntax error detected in DDM data stream.

CPF3E81 The data descriptor received is not valid.

CPF3E82 Relational database already accessed.

CPF3E83 Data descriptor does not match data received.

CPF3E84 DDM conversational protocol error was detected.

CPF3E85 Relational database &4; not accessed.

CPF3E86 Error occurred during distributed database processing.

CPF3E87 Permanent error condition detected.

CPF3E88 The SQL cursor had been previously opened at the remote system.

CPF3E89 SQL cursor not open for an attempted remote operation.

CPF4168 Error on device or location &5; in file &2; in &3;

CPF4262 Feedback code not recognized on device &4;

CPF4509 Feedback code not recognized on device &4;

CPF4524 Error on device &4; Device response code is &6;

CPF4527 Error on device &4; Device response code is &6;

CPF4541 MODLUD reset ended request. Internal failure in system.

CPF4584 Transmit not allowed until previous response received.

CPF5105 Error on file &2; in library &3; on device &4;

CPF5406 Data passed on SNADS distribution not valid. Internal failure in system.

CPF5453 Input/Output error on device &4; Internal failure in system.

CPF594F The APPN congestion threshold has been reached for the system.

CPF8BC0 DDI MAC path change event occurred on line &23,; station &40;

CPF8B03 Excessive recoverable token-ring errors on line &23; for adapter &40; or &41;

CPF8B13 Excessive recoverable token-ring errors on line &23,; adapter &40;

CPF8B26 Receiver congestion reported by adapter &40; on line &23;

CPF8B27 Congested condition ended at adapter &40,; line &23;

CPF8B28 Token-ring line &23; beaconing. Recovery in process.

CPF8B29 Token-ring line &23; beaconing. Recovery in process.

CPF8B30 Token-ring line &23; beaconing. Recovery in process.

CPF8B31 Token-ring line &23; beaconing. Recovery procedures failed.

CPF8B32 Token-ring line &23; beaconing. Recovery procedures failed.

CPF8B33 Token-ring line &23; beaconing. Recovery procedures failed.

CPF8B35 Token-ring line &23; manually recovered. Adapters &40; and &41; removed.

CPF8B36 Token-ring line &23; manually recovered. Adapter &40; removed.

CPF8B85 MAC not-copied condition occurring on line &23,; station &40;

CPF8B90 DDI frame error ratio exceeds alarm threshold on line &23,; station &40;

CPF8B92 DDI link error rate on line &23,; adapter &40,; exceeds alarm threshold.

CPF8B97 DDI elasticity buffer error condition reported on line &23,; station &40;

CPF8804 Error occurred during distribution processing.

CPF8807 Error occurred while using QSNADS journal.

CPF8808 SNADS cannot allocate more queue space.

CPF8809 Errors detected on SNADS internal queues.

CPF8810 An unrecoverable error occurred in a SNADS module.

CPF8811 Errors occurred in SNADS receive distribution processor.

CPF8812 Error occurred while processing distribution queues.

CPF8824 Error occurred during inbound gateway distribute processing.

CPF8825 Data passed on SNADS inbound gateway distribution not valid. Internal failure in system.

CPF8861 Not able to establish communications with NetView Distribution Manager host.

CPF8862 DSNX host interface ended abnormally.

CPF8863 DSNX receive function ended abnormally.

CPF8864 Not able to open data base file &1; containing DSNX correlation table.

CPF8865 DSNX had a severe error while attempting to manage storage.

CPF8866 DSNX request exceeded system storage available.

CPF8871 SNADS object is damaged.

CPF9E15 Error in license management function.

CPF93C0 Software error logging not active.

CPIAFA7 Error occurred while using MSF log.

CPI0906 *ATTENTION* Controlling subsystem &1; should be started.

CPI0961 Uninterruptible power supply (UPS) no longer attached.

CPI0962 Uninterruptible power supply (UPS) now attached.

CPI0964 Weak battery condition exists.

CPI0965 Failure of battery backup feature in system unit.

CPI0966 Failure of the battery backup feature in expansion unit.

CPI0973 Weak battery condition no longer exists.

CPI0974 UPS has been bypassed.

CPI0975 UPS no longer bypassed.

CPI0976 Notification of message &1; failed.

CPI1E62 &1; backup not successful or not complete (&2);

CPI1117 Damaged job schedule &1; in library &2; deleted.

CPI1153 System password bypass period ended.

CPI1154 System password bypass period will end in &5; days.

CPI1165 One or more device parity protected units still not fully operational.

CPI1166 Units with device parity protection fully operational.

CPI1303 Insufficient storage in machine pool to start job &3/&2/&1;

CPI3A32 Recovery failed for SNADS *SVDS sender &3/&2/&1; serving distribution queue &4;

CPI3CEE QUSEXRGOBJ in QUSRSYS is damaged.

CPI3CEF Exit registration facility repository is full.

CPI573A This message is not used.

CPI573B Network server &30; failed.

CPI573D Network server &30; failed.

CPI573F Network server &30; failed.

CPI5807 Device &25; on controller &24; on line &23; failed.

CPI5808 Device &25; on controller &24; on line &23; failed.

CPI59A3 Connection on device &25; failed. Internal system failure.

CPI59A5 Unacknowledged service on device &25; failed. Internal system failure.

CPI59A7 Internal failure during automatic creation of controller description.

CPI59B1 Internal system failure while setting thresholds for line &23;

CPI59CA Internal system failure while setting counters for line &23;

CPI59C8 Internal system failure while setting counters for network interface &30;

CPI59D9 Internal operating system error in QLUS job.

CPI59E4 Line &23; failed. Resource already in use.

CPI59E5 Network interface &30; failed. Resource already in use.

CPI59F1 Line &23; failed. Internal system failure.

CPI59F3 Controller &24; failed. Internal system failure.

CPI59F8 Network interface &30; failed. Internal system failure.

CPI5903 Network password received for line &23; not valid.

CPI5904 No logical channel available for incoming call on line &23;

CPI591D Device &25; on controller &24; on line &23; failed.

CPI5914 Line &23; failed. Data received in Contention State.

CPI5915 Device &25; on controller &24; on line &23; failed.

CPI5928 Line &23; could not process an X.25 or local area network incoming call request.

CPI5932 Internal operating system error in QSYSARB job.

CPI598A Transmission priority mismatch between networks.

CPI7B40 Data received from &1;&2; not allowed.

CPI7E1A Cryptographic subsystem &26; failed

CPI7E1F Internal system error detected by resource &26;

CPI7E16 FAX adapter &27; failed.

CPI7E17 Communications error detected by fax adapter &27;

CPI7E2F Cryptographic subsystem &26; failed

CPI7E27 Line &23; has recovered from a wrapped configuration

CPI7E3B Fax adapter port &28; failed

CPI7E3C Fax adapter &27; failed

CPI7E42 Error with device &25; on workstation controller &24;

CPI7E43 Error with device &25; on workstation controller &26;

CPI7E44 Error with device &25; on workstation controller &24;

CPI7E5A Ethernet adapter &27; detected a recoverable error.

CPI7E5E Ethernet resource &27; status information

CPI7E5F Ethernet network adapter &27; detected recoverable error.

CPI7FC9 Network interface &30;; line &23; Threshold Information.

CPI7FF5 Network interface &30; threshold information. Loss of synchronization errors.

CPI7FF6 Short frame error limit reached on network interface &30;

CPI7FF7 Network interface &30; threshold information. DTSEIN error.

CPI7FF8 Network interface &30; threshold information. DTSEOUT error.

CPI7F0A Frame reject type X received on network interface &30;

CPI7F0C Network interface &30; information. Incoming calls rejected limit exceeded.

CPI7F07 Disconnect retry limit reached on line &23; network interface &30; during disconnect processing.

CPI7F08 Frame reject type W received on network interface &30;

CPI7F1A Frame reject type Y received on network interface &30;

CPI7F1C Frame reject type Z received on network interface &30;

CPI7F33 Network interface &30; threshold information. Far end code violation.

CPI7F34 Network interface &30; threshold information. Local end code violation.

CPI7F4A Network interface &30; line &23; threshold information. Send sequence counter (NS) error.

CPI7F45 Overrun error threshold limit reached on line &23,; network interface &30;

CPI7F46 Short frame error threshold limit reached on line &23,; network interface &30;

CPI7F47 Aborted frames threshold limit reached on network interface &30,; line &23;

CPI7F8B A disconnect-mode frame was received on network interface &30;

CPI7F8C An unsolicited disconnect-mode frame was received on network interface &30;

CPI7F8F Overrun errors threshold limit reached on network interface &30;

CPI7F84 Underrun errors threshold limit reached on network interface &30;

CPI7F85 Aborted frames threshold limit reached on network interface &30;

CPI7F86 Retransmitted frames limit reached on network interface &30;

CPI7F87 Send sequence errors threshold limit reached on network interface &30;

CPI7F9B Error on network interface &30;

CPI7F9D Line &23; attached to network interface &30,; underrun errors threshold reached.

CPI7F9E	Retransmitted frames limit reached on line &23,; network interface &30;	**CPI8E0A**	Line &23; threshold information.
		CPI8E0B	Line &23; threshold information.
CPI7F92	A set-asynchronous-balance-mode-extended frame was received on line &23,; network interface &30;	**CPI8E0C**	Line &23; threshold information.
		CPI8E0D	Line &23; threshold information.
		CPI8E0E	Line &23; threshold information.
CPI7F93	Disconnect-mode frame with final bit off received on line &23; attached to network interface &30;	**CPI8E0F**	Line &23; threshold information.
		CPI8E00	Line &23; threshold information.
CPI7F94	Disconnect-mode frame with final bit on received on line &23; attached to network interface &30;	**CPI8E01**	Line &23; threshold information.
		CPI8E02	Line &23; threshold information.
		CPI8E03	Line &23; threshold information.
CPI8A13	QDOC library nearing system object limit.	**CPI8E04**	Line &23; threshold information.
		CPI8E05	Line &23; threshold information.
CPI8A14	QDOC library has exceeded system object limit.	**CPI8E06**	Line &23; threshold information.
		CPI8E07	Line &23; threshold information.
CPI8EBA	Line &23; threshold information.	**CPI8E08**	Line &23; threshold information.
CPI8EBB	Line &23; threshold information.	**CPI8E09**	Line &23; threshold information.
CPI8EBC	Line &23; threshold information.	**CPI8E1A**	Line &23; threshold information.
CPI8EBE	Line &23; threshold information.	**CPI8E1B**	Line &23; threshold information.
CPI8EB0	Line &23; threshold information.	**CPI8E1C**	Line &23; threshold information.
CPI8EB1	Line &23; threshold information.	**CPI8E1D**	Line &23; threshold information.
CPI8EB2	Line &23; threshold information.	**CPI8E1E**	Line &23; threshold information.
CPI8EB3	Line &23; threshold information.	**CPI8E1F**	Line &23; threshold information.
CPI8EB4	Line &23; threshold information.	**CPI8E10**	Line &23; threshold information.
CPI8EB5	Line &23; threshold information.	**CPI8E11**	Line &23; threshold information.
CPI8EB6	Line &23; threshold information.	**CPI8E12**	Line &23; threshold information.
CPI8EB7	Line &23; threshold information.	**CPI8E13**	Line &23; threshold information.
CPI8EB8	Line &23; threshold information.	**CPI8E14**	Line &23; threshold information.
CPI8EB9	Line &23; threshold information.	**CPI8E15**	Line &23; threshold information.
CPI8EC0	Line &23; threshold information.	**CPI8E16**	Line &23; threshold information.
CPI8EC2	Line &23; threshold information.	**CPI8E17**	Line &23; threshold information.
CPI8EDE	Line &23; status information, the system workload may be too heavy.	**CPI8E18**	Line &23; threshold information.
		CPI8E19	Line &23; threshold information.
CPI8EF2	Line &23; threshold information.	**CPI8E2A**	Line &23; threshold information.
CPI8EF3	Line &23; threshold information.	**CPI8E2B**	Line &23; threshold information.
CPI8EF4	Line &23; threshold information.	**CPI8E2C**	Line &23; threshold information.
CPI8EF5	Line &23; threshold information.	**CPI8E2D**	Line &23; threshold information.
CPI8EF6	Line &23; threshold information.	**CPI8E2E**	Line &23; threshold information.
CPI8EF7	Line &23; threshold information.		
CPI8EF8	Line &23; threshold information.		

CPI8E2F	Call-Progress-Signal 00 threshold on line &23;
CPI8E20	Line &23; threshold information.
CPI8E21	Line &23; threshold information.
CPI8E22	Line &23; threshold information.
CPI8E23	Line &23; threshold information.
CPI8E24	Line &23; threshold information.
CPI8E25	Line &23; threshold information.
CPI8E26	Line &23; threshold information.
CPI8E27	Line &23; threshold information.
CPI8E28	Line &23; threshold information.
CPI8E29	Line &23; threshold information.
CPI8E3A	Line &23; threshold information.
CPI8E3B	Line &23; threshold information.
CPI8E3C	Line &23; threshold information.
CPI8E3D	Line &23; threshold information.
CPI8E3E	Line &23; threshold information.
CPI8E3F	Line &23; threshold information.
CPI8E30	Call-Progress-Signal 01 threshold on line &23;
CPI8E31	Call-Progress-Signal 02 threshold on line &23;
CPI8E32	Call-Progress-Signal 03 threshold on line &23;
CPI8E33	Call-Progress-Signal 04 threshold on line &23;
CPI8E34	Line &23; threshold information.
CPI8E35	Line &23; threshold information.
CPI8E36	Line &23; threshold information.
CPI8E37	Line &23; threshold information.
CPI8E38	Line &23; threshold information.
CPI8E39	Line &23; threshold information.
CPI8E40	Line &23; threshold information.
CPI8E41	Line &23; threshold information.
CPI8E42	Line &23; threshold information.
CPI8E43	Line &23; threshold information.
CPI8E44	Line &23; threshold information.
CPI8E45	Line &23; threshold information.

CPI8E46	Line &23; threshold information.
CPI8E7A	Line &23; threshold information.
CPI8E70	Line &23; threshold information.
CPI8E71	Line &23; threshold information.
CPI8E72	Line &23; threshold information.
CPI8E73	Line &23; threshold information.
CPI8E74	Line &23; threshold information.
CPI8E75	Line &23; threshold information.
CPI8E76	Line &23; threshold information.
CPI8E77	Line &23; threshold information.
CPI8E78	Line &23; threshold information.
CPI8E79	Line &23; threshold information.
CPI8E8B	Line &23; threshold information.
CPI8E8C	Line &23; threshold information.
CPI8E80	Line &23; threshold information.
CPI8E81	Line &23; threshold information.
CPI8E82	Line &23; threshold information.
CPI8E83	Line &23; threshold information.
CPI8E84	Line &23; threshold information.
CPI8E85	Line &23; threshold information.
CPI8E88	Line &23; threshold information.
CPI8FB2	Line &23; threshold information.
CPI8FB3	Line &23; threshold information.
CPI8FB4	Line &23; threshold information.
CPI8FC6	Line &23; status information, the system work load may be too heavy.
CPI8FDA	Line &23; threshold information.
CPI8FDB	Line &23; threshold information.
CPI8FDC	Line &23; threshold information.
CPI8FDD	Line &23; threshold information.
CPI8FDE	Line &23; threshold information.
CPI8FDF	Line &23; threshold information.
CPI8FD3	Line &23; threshold information.
CPI8FD4	Line &23; threshold information.
CPI8FD5	Line &23; threshold information.
CPI8FD6	Line &23; threshold information.
CPI8FD7	Line &23; threshold information.

CPI8FD8 Line &23; threshold information.

CPI8FD9 Line &23; threshold information.

CPI8FFF Line &23; threshold information.

CPI8FF2 Line &23; threshold information.

CPI8FF3 Line &23; threshold information.

CPI8FF4 Line &23; threshold information.

CPI8FF5 Line &23; threshold information.

CPI8FF6 Line &23; threshold information.

CPI8FF7 Line &23; threshold information.

CPI8FF8 Line &23; threshold information.

CPI8FF9 Line &23; threshold information.

CPI8F2D Line &23; status information, line is running.

CPI8F2E Line &23; status information, line is running.

CPI8F2F Line &23; status information, line is running.

CPI8F37 Line &23; status information, line is running.

CPI8F38 Line &23; status information, line is running.

CPI8F4A Line &23; threshold information.

CPI8F4B Line &23; threshold information.

CPI8F4C Line &23; threshold information.

CPI8F4D Line &23; threshold information.

CPI8F4E Line &23; threshold information.

CPI8F4F Line &23; threshold information.

CPI8F5F Line &23; threshold information.

CPI8F50 Line &23; threshold information.

CPI8F51 Line &23; threshold information.

CPI8F53 Line &23; threshold information.

CPI8F54 Error with device &25; on work station controller &24;

CPI8F55 Error with device &25; on work station controller &24;

CPI8F56 Error with device &25; on work station controller &24;

CPI8F58 Error with device &25; on work station controller &24;

CPI8802 Distribution queue &1; error held by sender job.

CPI8804 Error occurred while sending an entry on &1; &2; queue.

CPI8807 Error(s) logged by SNADS while a distribution request was being routed.

CPI8810 SNADS cannot allocate queue space.

CPI8811 Errors detected on SNADS internal queues.

CPI8813 Error occurred while using QSNADS journal.

CPI8816 Recovery failed for SNADS sender &3/&2/&1,; serving *SNADS distribution queue &5;

CPI8822 SNADS &5; distribution queue &4; error held by sender job.

CPI8826 Recovery failed for SNADS gateway sender &3/&2/&1,; serving &5; distribution queue &4;

CPI8854 DSNX error while journaling.

CPI93B0 Software problem data for &1; has been logged. Refer to help text for additional information.

CPI93B9 Software problem data for &1; has been logged. Refer to help text for additional information.

CPI9804 IBM application generated alert: &2;

CPI9805 User application generated alert: &2;

CPI9806 Operator generated alert: &2;

QCPFMSG Messages with ALROPT(*DEFER)

CPA5201 Hardware failure on device &3;

CPA57AA Call to controller on line &23; not answered. Probable remote problem. (C G R)

CPA57AB Call from controller on line &23; failed. Probable network or hardware problem. (C G R)

CPA57AD DCE or local hardware on line &23; failed. (C G R)

CPA57AE DCE on line &23; not turned on or not in data mode. (C G R)

CPA57AF Dialing digits for controller &24; not valid. (C R)

CPA57A0 Network interface &30; failed. Unable to detect power source from NT. (C G R)

CPA57A2 Incoming data on line &23; lost. (C G R)

CPA57A3 Controller &24; failed. Probable remote system or network problem. (C G R)

CPA57A4 Controller &24; failed. Remote system problem. (C G R)

CPA57A5 Call request on line &23; failed. Probable network failure. (C G R)

CPA57A6 Controller &24; failed. Remote system problem. (C G R)

CPA57A7 Controller &24; failed. Probable remote system problem. (C G R)

CPA57A8 Controller &24; failed. Probable remote system problem. (C G R)

CPA57A9 Controller &24; failed. Probable remote system or network problem. (C G R)

CPA57BA Call request on line &23; to controller &24; failed. Remote modem power may be off. (C R)

CPA57BB Network rejected call request to controller &24; on line &23; (C R)

CPA57BC Controller &24; contact not successful. Probable network problem. (C R)

CPA57BD Call request on line &23; failed. Notify network administrator. (C G R)

CPA57BE Network rejected call request to controller &24; on line &23; (C R)

CPA57BF Temporary network congestion while trying to contact controller &24; (C R)

CPA57B0 Call to controller &24; on line &23; rejected. Probable network or DCE problem. (C R)

CPA57B1 Call to controller &24; failed. X.21 station busy. (C R)

CPA57B2 Selection signals used to call controller &24; not correct. (C R)

CPA57B3 Parity error on line &23; (C G R)

CPA57B4 Not authorized to call controller &24; on line &23; (C R)

CPA57B5 Connection number to controller &24; has changed. (C R)

CPA57B6 Connection number for controller &24; failed. Probable connection number not valid. (C R)

CPA57B7 Call to controller &24; failed. Probable remote DCE problem. (C R)

CPA57B8 Controller &24; not ready. (C R)

CPA57B9 Controller &24; not ready. (C R)

CPA57CA Attempt to connect with controller &24; exceeded time limit. (C R)

CPA57CB Call to controller &24; on line &23; rejected. Probable network or DCE problem. (C G R)

CPA57CC Call to controller &24; failed. X.21 station busy. (C G R)

CPA57CD Selection signals used to call controller &24; not correct. (C G R)

CPA57CE Not authorized to call controller &24; on line &23; (C G R)

CPA57CF Connection number to controller &24; has changed. (C G R)

CPA57C0 Long term network congestion on line &23; (C G R)

CPA57C1 Network to controller &24; not operational. (C R)

CPA57C2 Controller &24; does not support X.21 SHM. (C R)

CPA57C3 Local system canceled call to remote system &24; (C R)

CPA57C4 Station address from controller &24; not configured. (C R)

CPA57C5 Controller &24; reconnection not expected. (C R)

CPA57C6 Controller &24; failed. No data received. (C G R)

CPA57C7 Attempt to connect with controller &24; exceeded time limit. (C G R)

CPA57C8 Controller &24; DCE cleared. (C G R)

CPA57C9 Station address from controller &24; not configured. (C G R)

CPA57DA Network to controller &24; not operational. (C G R)

CPA57DB Controller &24; failed. Local hardware problem. (C G R)

CPA57DD Controller &24; contact not successful. Remote system problem. (C R)

CPA57DE Controller &24; contact not successful. Probable remote system problem. (C R)

CPA57DF Controller &24; contact not successful. Probable remote system problem. (C R)

CPA57D1 Modem on line &23; not ready. (C G R)

CPA57D2 Line &23; failed. Probable hardware failure. (C G R)

CPA57D3 Connection number for controller &24; failed. Probable connection number not valid. (C G R)

CPA57D4 Call to controller &24; failed. Probable remote DCE problem. (C G R)

CPA57D5 Controller &24; not ready. (C G R)

CPA57D6 Controller &24; not ready. (C G R)

CPA57D7 Call request on line &23; to controller &24; failed. Remote modem power may be off. (C G R)

CPA57D8 Network rejected call request to controller &24; on line &23; (C G R)

CPA57D9 Network rejected call request to controller &24; on line &23; (C G R)

CPA57E2 Controller &24; failed. Remote system problem. (C G R)

CPA57E3 Controller &24; on line &23; not contacted. Remote time-out. (C R)

CPA57E8 Controller &24; failed. Not found on local area network. (C G R)

CPA57FA Call on line &23; failed. Too many dialing digits. (C N R)

CPA57FB Dialing digits for line &23; not valid. (C N R)

CPA57FC Time limit reached while trying to call using line &23; (C N R)

CPA57FD Line &23; not contacted. Call failed. (C N R)

CPA57FE Call on line &23; failed. Probable local hardware problem. (C N R)

CPA570A Controller &24; on line &23; not contacted. Received frame length too large. (C R)

CPA570B Controller &24; on line &23; not contacted. Received frame length too large. (C G R)

CPA570C Call to controller &24; failed. Too many dialing digits. (C R)

CPA570D Modem or local hardware error on line &23; (C G R)

CPA570E Line &23; HDLC data link reset. (C G R)

CPA5704 Controller &24; on line &23; not contacted. Link problem. (C R)

CPA5705 Controller &24; on line &23; not contacted. Link problem. (C G R)

CPA5706 Controller &24; on line &23; not contacted. Probable remote protocol error. (C R)

CPA5707 Controller &24; on line &23; not contacted. Probable remote protocol error. (C G R)

CPA5708 Controller &24; on line &23; not contacted. Remote station disconnected. (C R)

CPA5709 Controller &24; on line &23; not contacted. Remote station disconnected. (C G R)

CPA571D Controller &24; on line &23; not contacted. Remote disconnect. (C R)

CPA5710 Controller &24; on line &23; not contacted. No IOP storage available. (C R)

CPA5711 Controller &24; on line &23; not contacted. No IOP storage available. (C G R)

CPA5712 Time limit reached while trying to call controller &24; (C R)

CPA5713 Controller &24; on line &23; not contacted. Remote time-out. (C G R)

CPA5715 Controller &24; on line &23; not contacted. Call failed. (C R)

CPA5716 Controller &24; on line &23; not contacted. Remote disconnect. (C R)

CPA5717 Controller &24; on line &23; not contacted. Remote disconnect. (C G R)

CPA5718 Call to controller &24; on line &23; failed. Probable local hardware problem. (C R)

CPA5730 Controller &24; failed. Probable network problem. (C G R)

CPA5731 Temporary network congestion while communicating with controller &24; on line &23; (C G R)

CPA5751 Controller &24; failed. Recovery stopped. Probable remote system problem. (C G R)

CPA576A Controller &24; contact not successful. Probable remote system problem. (C R)

CPA576C Controller &24; contact not successful. Probable remote system problem. (C R)

CPA576F Controller &24; contact not successful. Probable remote system problem. (C G R)

CPA577E Call for line &23; on network interface &30; failed, probable configuration problem. (C N R)

CPA5775 Call on line &23; failed, semi-permanent connection not supported by the network (C N R).

CPA5777 The call for line &23; on network interface &30; failed, no response from the network. (C N R)

CPA578A Call to controller on line &23; failed. Network or hardware problem. (C G R)

CPA578B HDLC link establishment failed on line &23; (C G R)

CPA578C Controller &24; on line &23; failed. Probable insufficient resources. (C G R)

CPA578D Not enough resources for controller &24; (C G R)

CPA578E Controller &24; DCE cleared. (C R)

CPA578F Controller &24; failed. Remote system problem. (C G R)

CPA5781 Line &23; on Network Interface &30; not contacted. A protocol error has occurred. (C N R)

CPA5786 Line &23; on Network Interface &30; failed. A protocol error has occurred. (C G R)

CPA5787 Network interface &30; failed, retry limit reached. (C G R)

CPA5788 Network interface &30; failed, disconnect received from the network (C G R).

CPA5789 Network interface &30; failed, TEI assignment failed. (C G R)

CPA579C Controller &24; failed. No virtual circuits available. (C R)

CPA579F Controller &24; contact not successful. Probable remote system problem. (C G R)

CPA5790 Network interface &30; failed, TEI removed. (C G R)

CPA5791 Line &23; on network interface &30; failed, call cleared. (C G R)

CPA5792 Call for line &23; on network interface &30; failed, call cleared. (C N R)

CPA5793 Network interface &30; failed. No response from NT. (C G R)

CPA5794 Network interface &30; failed. Possible NT problem. (C G R)

CPA5795 Network interface &30; failed. Possible network problem. (C G R)

CPA5796 Network interface &30; failed. Possible NT problem. (C G R)

CPA5797 Network interface &30; failed. Loss of power from NT. (C G R)

CPA5798 Network interface &30; failed. Probable local wiring problem. (C G R)

CPA58A1 Call to controller on line &23; failed. Probable local hardware problem. (C G R)

CPA58A4 Line &23; failed. Probable configuration problem. (C G R)

CPA58A5 Line &23; failed. No IOP storage available. (C G R)

CPA58A6 Call to controller on line &23; failed. Probable local hardware problem. (C G R)

CPA58B1 Incoming data on line &23; lost. (C G R)

CPA58B2 Line &23; failed. Probable remote system problem. (C G R)

CPA58B3 Time-out on line &23; Probable remote system problem. (C G R)

CPA58B6 Call on line &23; failed. Time-out occurred. (C N R)

CPA58CC Line &23; failed. Probable local hardware problem. (C G R)

CPA58CD Controller &24; failed. Probable local system problem. (C G R)

CPA58D5 Line &23; failed. Probable modem problem. (C G R)

CPA58D6 Call to controller &24; on line &23; failed. Time-out occurred. (C R)

CPA58EA Line &23; failed while attached to network interface &30; Potential cabling problem. (C G R)

CPA58EB Line &23; contact not successful on network interface &30; Potential cabling problem. (C N R)

CPA58EF Line &23; contact not successful on network interface &30; Addressing problem encountered. (C N R)

CPA58E8 Line &23; failed while attached to network interface &30; Network no longer responding. (C G R)

CPA58E9 Line &23; contact not successful on network interface &30; Network not responding. (C N R)

CPA58FB Controller &24; failed. Maximum retry limit reached. (C G R)

CPA58FC Controller &24; not contacted, connect retry limit reached. (C G R)

CPA58FD Controller &24; contact not successful. Connect retry limit reached. (C R)

CPA58F5 Call for line &23; on network interface &30; failed, call cleared. (C N R)

CPA58F9 Line &23; failed while attached to network interface &30; Addressing problem encountered (C G R)

CPA580A Controller &24; contact unsuccessful. Probable remote system problem. (C R)

CPA580C Controller &24; contact not successful. Logical link protocol error detected.(C G R)

CPA580D Controller &24; contact not successful. Logical link protocol error detected. (C R)

CPA580E Controller &24; not contacted. Probable configuration problem. (C R)

CPA5801 Line &23; failed. Probable configuration problem. (C G R)

CPA5802 Line &23; not contacted. Internal system failure. (C N R)

CPA5811 Call for line &23; on network interface &30; failed, internal system failure. (C N R)

CPA5817 Line &23; failed. Probable local hardware problem. (C G R)

CPA5821 Line &23; failed. Probable local modem problem. (C G R)

CPA5826 Line &23; failed. Probable local modem problem. (C G R)

CPA5829 Controller &24; failed. Remote station disconnected. (C G R)

CPA5830 Controller &24; failed. Probable remote protocol error. (C G R)

CPA5835 Controller &24; failed. Link problem. (C G R)

CPA5838 Line &23; failed. Probable link problem. (C G R)

CPA5842 Controller &24; failed. Remote disconnect. (C G R)

CPA5843 Controller &24; failed. Configuration or remote system problem. (C G R)

CPA5847 Line &23; failed. Probable modem problem. (C G R)

CPA5848 Call on line &23; failed. Data link occupied error. (C N R)

CPA5849 Line &23; failed. (C G R)

CPA5851 Line &23; failed. Probable local hardware problem. (C G R)

CPA5852 Controller &24; failed. Logical link protocol error detected.(C G R)

CPA586A Line &23; response time limit reached. (C G R)

CPA586B Controller &24; response time limit reached. (C G R)

CPA5867 Line &23; failed. No polls from primary. (C G R)

CPA5868 Time between sync characters exceeded. (C G R)

CPA587A Contact not successful on controller &24; Internal system failure. (C R)

CPA587B Controller &24; contact not successful. (C R)

CPA5873 Data on line &23; lost. Probable line or modem failure. (C G R)

CPA5874 Controller &24; failed. Facility field too long. (C G R)

CPA5875 Controller &24; contact not successful. (C R)

CPA5876 Internal system failure while processing with controller &24; (C G R)

CPA5877 Contact not successful on controller &24; Internal system failure. (C R)

CPA589F Not enough resources for controller &24; (C R)

CPA59CB HDLC link establishment failed on line &23; (C N R)

CPA59CC HDLC link establishment failed on line &23; (C N R)

CPA59C1 Controller &24; failed. Probable internal system failure. (C G R)

CPA59C6 Controller &24; failed. Remote time-out. (C G R)

CPA59C8 Line &23; failed. HDLC frame retry limit exceeded. (C G R)

CPA59C9 Line &23; failed. HDLC frame retry limit exceeded. (C N R)

CPA59DA Controller &24; contact not successful. Not found on local area network. (C R)

CPA59D1 Line &23; HDLC data link reset. (C G R)

CPA59D6 Controller &24; failed. Probable remote system problem. (C G R)

CPA59D7 Controller &24; failed. Probable remote system problem. (C G R)

CPA59D8 Controller &24; failed. Probable remote system problem. (C G R)

CPA59D9 Controller &24; failed. Probable remote system problem. (C G R)

CPA59F2 Internal system failure on line &23; (C G R)

CPA59F4 Controller &24; failed. Internal system failure. (C G R)

CPA59F5 Internal system failure on line &23; (C G R)

CPA59F6 Controller &24; failed. Internal system failure. (C G R)

CPA59F7 Internal system failure on network interface &30; (C G R)

CPA591F Call to controller &24; failed. Dialing digit not valid. (C R)

CPA5917 Line &23; failed. Protocol mismatch. (C G R)

CPA595E Line &23; failed. Probable configuration problem. (C G R)

CPA595F Call for line &23; failed, possible network problem. (C G R)

CPA5953 Contact not successful for line &23; Protocol mismatch. (C G R)

CPA596A Line &23; failed. Protocol mismatch. (C G R)

CPA596B Contact not successful for line &23; Probable configuration problem. (C G R)

CPA596C Line &23; failed. Probable local hardware problem. (C G R)

CPA596D Line &23; failed. Probable modem problem. (C G R)

CPA94EA Tape controller &26; or tape device &25; failed.

CPA94F7 Tape device &25; not communicating with Tape I/O Processor.

CPA94F9 Tape device &25; returning a busy status.

CPD6348 Space pointer declare requires HLLPTR keyword to be specified or HLLPTR keyword not in proper order.

CPF4216 Hardware error on device &4;

CPF4583 Hardware error on device &4;

CPF4589 Hardware error on device &4;

CPF4590 Systems network architecture bind error on device &4;

CPF5201	Hardware failure on device &3;	**CPI1161**	Unit &1; with device parity protection not fully operational.
CPF5247	Feedback code on device &4; not recognized.	**CPI1167**	Temporary I/O processor error occurred.
CPF5253	Device &4; sent too much data.	**CPI2095**	Changing primary language not complete
CPF5265	Hardware error on device &4;		
CPF5266	Hardware error on device &4;	**CPI2098**	License information not processed during installation.
CPF5268	Hardware error on device &4;	**CPI5818**	Line &23; failed. Transmit complete timeout.
CPF6772	Volume on device &1; cannot be processed.		
CPF6782	Device &25; not operational.	**CPI59A2**	Connection on device &25; failed. Internal system failure.
CPF6783	Device &25; is not ready.	**CPI59A4**	Unacknowledged service on device &25; failed. Internal system failure.
CPF6784	Device &25; status changed from not ready to ready.	**CPI59B0**	Internal system failure while setting thresholds for line &23;
CPF6786	Interface check on the device.		
CPF6787	Equipment check while processing on device &25;	**CPI59CF**	Network interface &30; failed, channel error occurred.
CPF6788	Media error found on volume &1; on device &25;	**CPI59C7**	Internal system failure while setting counters for network interface &30;
CPF6793	Write error on volume &1; on device &25;	**CPI59C9**	Internal system failure while setting counters for line &23;
CPF6794	End of media was found on device &25;	**CPI59DF**	Network interface &30; failed, hardware error occurred.
CPF6795	Load failure occurred on device &25;	**CPI59D2**	Unacknowledged service on device &25; was not successful.
CPF6796	Device &25; was reset.		
CPF8BA8	Undesirable connection attempt on line &23,; adapter &40,; port &42;	**CPI59E0**	Network interface &30; failed, TEI assignment failed.
CPF8B9A	Line &23; in wrapped configuration at adapter &40;	**CPI59E1**	Network interface &30; failed, TEI removed.
CPIFFF8	Tape unit does not support synchronous data transfer	**CPI59E2**	Line &23; failed, channel error on network interface &30;
CPI0920	Error occurred on disk unit &1;	**CPI59E3**	Line &23; failed, hardware error occurred.
CPI0945	Mirrored protection is suspended on disk unit &1;	**CPI59F2**	Line &23; failed. Internal system failure.
CPI0956	Mirrored protection suspended on disk unit &1;	**CPI59F4**	Controller &24; failed. Internal system failure.
CPI0959	Mirrored protection suspended on disk unit &1;	**CPI59F5**	Line &23; failed. Internal system failure.
CPI0970	Disk unit &1; not operating.	**CPI59F6**	Controller &24; failed. Internal system failure.
CPI0992	Errors occurred on disk unit &1;	**CPI59F7**	Network interface &30; failed. Internal system failure.
CPI0996	Error occurred on disk unit &1;		
CPI1136	Mirrored protection still suspended.		

CPI591B Device &25; on controller &24; failed. Internal system failure.

CPI591F Resources for controller &24; not sufficient.

CPI592B Resources not sufficient for line &23;

CPI592D Line &23; failed. Local DCE problem.

CPI593D Line &23; failed. Automatic recovery started.

CPI593E Controller &24; failed. Automatic recovery started.

CPI5951 Network interface &30; failed. Automatic recovery started.

CPI7D10 Error on line &23; Unsolicited response received.

CPI7E0A I/O Attachment Processor resource &26; failed.

CPI7E0B Attachment I/O Processor resource &26; failed.

CPI7E0C Attachment I/O Processor resource &26; failed.

CPI7E0D Resource &26; failed.

CPI7E0E Attachment I/O Processor resource &26; failed.

CPI7E0F Attachment I/O Processor resource &26; failed.

CPI7E00 Communications I/O processor &26; removed or failed.

CPI7E01 Communications I/O adapter &27; removed or failed.

CPI7E02 High Speed Communications Adapter resource &27; failed.

CPI7E03 Communications I/O adapter &27; removed or failed.

CPI7E04 Workstation controller &26; removed or failed.

CPI7E05 High Speed Communications Adapter resource &27; failed.

CPI7E06 High Speed Communications Adapter resource &27; failed.

CPI7E07 High Speed Communications Adapter resource &27; failed.

CPI7E08 High Speed Communications Adapter resource &27; failed.

CPI7E09 High Speed Communications Adapter resource &27; failed.

CPI7E1B Cryptographic subsystem &26; failed

CPI7E1D Line &23; failed.

CPI7E1E Call failure. Active telephone line is not connected to port &28;

CPI7E10 Attachment I/O Processor resource &26; failed.

CPI7E11 Distributed Data Interface resource &27; failed.

CPI7E12 Distributed Data Interface resource &26; failed.

CPI7E13 Distributed Data Interface resource &27; failed.

CPI7E14 Distributed Data Interface resource &27; failed.

CPI7E15 Distributed Data Interface resource &27; failed.

CPI7E18 Internal system error in fax adapter &26;

CPI7E19 Distributed Data Interface resource &27; failed.

CPI7E2A Cryptographic subsystem &26; failed

CPI7E2B Cryptographic subsystem &26; failed

CPI7E2C Cryptographic subsystem &26; failed

CPI7E2D Cryptographic subsystem &26; failed

CPI7E2E Cryptographic subsystem &26; failed

CPI7E20 Wrong command value sent by OS/400 Licensed Program.

CPI7E21 Wrong command value sent by OS/400 Licensed Program.

CPI7E22 Controller on line &23; failed.

CPI7E23 Invalid M/Q bit sequence on logical channel on line &23;

CPI7E24 Error on line &23; Internal system failure.

CPI7E25 Error on line &23; Internal system failure.

CPI7E26 Line &23; has entered a wrapped configuration

CPI7E28 Line &23; on adapter &27; has switched active connection from primary port to backup port

CPI7E29	A test of the IOA internal data paths has failed	**CPI7E60**	File Server Input/Output Processor &26; failed.
CPI7E3A	Wireless Local Area Network adapter resource &27; failed.	**CPI7E61**	File Server Input/Output Processor &26; failed.
CPI7E3E	Fax adapter port &28; has detected a failed or missing coupler.	**CPI7E63**	File Server Input/Output Processor &26; failed.
CPI7E30	Error on network interface &30;	**CPI7E64**	File Server Input/Output Processor &26; failed.
CPI7E31	Optical Bypass Switch is stuck	**CPI7E66**	File Server resource &27; failed.
CPI7E32	Line &23; has entered an undesirable configuration	**CPI7E67**	File Server Input/Output Processor &26; failed.
CPI7E39	No dial tone detected by fax adapter &27; on port &28;	**CPI7E68**	File Server Input/Output Processor &26; failed.
CPI7E4A	Error on line &23; Unsolicited response received.	**CPI7E69**	File Server Input/Output Processor &26; failed.
CPI7E46	Token-ring resource &27; failed.	**CPI7E7A**	I/O Processor card &27; removed or failed.
CPI7E47	Token-ring resource &27; failed.	**CPI7E7B**	Local area network adapter port &28; failed.
CPI7E48	Ethernet resource &27; failed.		
CPI7E5B	Ethernet resource &27; failed.	**CPI7E7C**	Local area network adapter port &28; failed.
CPI7E5C	Ethernet resource &27; failed.		
CPI7E5D	Ethernet resource &27; failed.	**CPI7E7D**	Resource &27; failed.
CPI7E50	Ethernet resource &27; failed.	**CPI7E7E**	Resource &27; failed.
CPI7E52	Clear packet sent on logical channel on line &23;	**CPI7E7F**	External wrap test passed.
		CPI7E70	File Server Input/Output Processor &26; failed.
CPI7E53	Token-ring resource &27; failed.	**CPI7E71**	File Server resource &27; failed.
CPI7E54	Token-ring resource &27; failed.	**CPI7E72**	File Server Input/Output Processor &26; failed.
CPI7E55	Ethernet resource &27; failed.		
CPI7E56	Line &23; failed.	**CPI7E73**	File Server Input/Output Processor &26; failed.
CPI7E57	Line &23; failed.		
CPI7E58	Attachment I/O Processor resource &26; information.	**CPI7E74**	Resource &27; failed.
CPI7E59	Communications I/O adapter &27; removed or failed.	**CPI7E75**	File Server Input/Output Processor &26; failed.
CPI7E6B	File Server Input/Output Processor &26; failed.	**CPI7E76**	File Server Input/Output Processor &26; failed.
CPI7E6C	File Server Input/Output Processor &26; failed.	**CPI7E77**	File Server Input/Output Processor &26; failed.
		CPI7E78	Resource &27; failed.
CPI7E6E	File Server Input/Output Processor &26; failed.	**CPI7E79**	Local area network resource &27; failed.
CPI7E6F	File Server Input/Output Processor &26; failed.	**CPI7E80**	External wrap test failed.

CPI7E81 Resource &27; failed.

CPI7E82 External wrap test failed.

CPI7FAA Line &23; failed, recovery stopped.

CPI7FA7 Resource &27; failed.

CPI7FA8 Resource &26; failed

CPI7FA9 Resource &27; failed.

CPI7FCB Insufficient resource to start communications trace on network interface &30;

CPI7FCC Error on network interface &30; Internal system failure.

CPI7FCD Error on network interface &30; Internal system failure.

CPI7FCF Error on network interface &30; Internal system failure.

CPI7FDF Error on network interface &30; Internal system failure.

CPI7FD0 Line &23; on network interface &30; failed, recovery stopped. ISDN channel already in use.

CPI7FD1 Error on line &23; attached to network interface &30; Adapter card not installed.

CPI7FD2 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FD3 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FD4 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FD5 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FD6 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FD9 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FED Network interface &30; failed. Internal system failure.

CPI7FEE Error on network interface &30; Internal system failure.

CPI7FEF Network interface &30; failed. Internal system failure.

CPI7FE0 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FE1 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FE2 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FE3 Error on line &23; attached to network interface &30; Internal system failure.

CPI7FE5 Error on network interface &30; Internal system failure.

CPI7FE6 Error on network interface &30; Internal system failure.

CPI7FF2 Error on line &23; attached to network interface &30;

CPI7FF3 Error on &23; attached to network interface &30; Internal system failure.

CPI7F0D Lack of transmit buffers on network interface &30;

CPI7F0E Frame reject type X received on network interface &30,; line &23;

CPI7F0F ISDN message received on network interface &30; was not correct.

CPI7F00 Error on network interface &30; Internal system failure.

CPI7F04 Controller &26; detected a non-recoverable bus error.

CPI7F06 Disconnect retry limit reached on network interface &30;

CPI7F09 Frame reject type W received on network interface &30,; line &23;

CPI7F1B Frame reject type Y received on network interface &30,; line &23;

CPI7F1D Frame reject type Z, receive sequence count error, received on network interface &30,; line &23;

CPI7F1E Error on network interface &30; Internal system failure.

CPI7F10 Invalid call reference value detected on network interface &30;

CPI7F11 Error on network interface &30;

CPI7F13 No response from remote equipment on network interface &30;

CPI7F14 Protocol message received with an unexpected cause code on network interface &30;

CPI7F16 Error on network interface &30; Internal system failure.

CPI7F17 Error on network interface &30;

CPI7F18 Error on network interface &30; Internal system failure.

CPI7F19 Error on network interface &30; Internal system failure.

CPI7F2A Network interface &30; failed. Internal system failure.

CPI7F2B Error on network interface &30; during get configuration request.

CPI7F2C I/O card Licensed Internal Code for network interface &30; cannot start due to lack of resource.

CPI7F2D Network interface &30; failed.

CPI7F2E Protocol message received with unexpected or incorrect contents on network interface &30;

CPI7F2F Line &23; failed.

CPI7F20 Error on network interface &30; Internal system failure.

CPI7F21 Error on network interface &30; Internal system failure.

CPI7F25 Error on network interface &30; Internal system failure.

CPI7F26 Error on network interface &30; Internal system failure.

CPI7F27 Error on network interface &30; Internal system failure.

CPI7F28 Error on network interface &30; Internal system failure.

CPI7F29 Error on network interface &30; Internal system failure.

CPI7F3A Error on network interface &30; Internal system failure.

CPI7F3B Error on network interface &30; Internal system failure.

CPI7F3C Network interface &30; failed.

CPI7F3F Resource &27; failed.

CPI7F30 Error on network interface &30; I/O card Licensed Internal Code has ended abnormally

CPI7F37 Resource &27; failed.

CPI7F38 Resource &27; failed.

CPI7F39 Error on network interface &30; Internal system failure.

CPI7F4B Token ring resource &27; failed.

CPI7F4C Resource &27; failed.

CPI7F4E Error on line &23,; network interface &30; failed; insufficient resource.

CPI7F4F Error on network interface &30; Internal system failure.

CPI7F40 Error on line &23; attached to network interface &30; Internal system failure.

CPI7F42 Token-ring resource &27; failed.

CPI7F43 Resource &27; failed.

CPI7F48 Token-ring resource &27; failed.

CPI7F5A Error on line &23; attached to network interface &30; Internal system failure.

CPI7F5B Error on line &23; attached to network interface &30; Internal system failure.

CPI7F5C Error on line &23; attached to network interface &30; Internal system failure.

CPI7F5D Error on line &23; attached to network interface &30; Internal system failure.

CPI7F51 Error on line &23; attached to network interface &30; Internal system failure.

CPI7F55 Error on line &23; attached to network interface &30; Internal system failure.

CPI7F56 Error on line &23; attached to network interface &30; Internal system failure.

CPI7F6A Error on network interface &30; Internal system failure.

CPI7F6B Error on network interface &30; Internal system failure.

CPI7F6C Error on network interface &30; Internal system failure.

CPI7F6D Error on network interface &30; Internal system failure.

CPI7F6E Error on network interface &30; Internal system failure.

CPI7F60 Line &23; on network interface &30; failed. Internal system failure.

CPI7F61 Frame retry limit reached on network interface &30;

CPI7F62	Error on line &23; attached to network interface &30; Internal system failure.	**CPI7F90**	Error on line &23; attached to network interface &30; Internal system failure.
CPI7F64	Resource &27; detected a non-recoverable bus error.	**CPI7F91**	Error on network interface &30; Internal system failure.
CPI7F65	Token-ring resource &26; failed.	**CPI7F95**	Network interface &30,; line &23; failed. Frame with incorrect command field received
CPI7F67	Error on network interface &30; Internal system failure.		
CPI7F68	Error on line &23; attached to network interface &30; Internal system failure.	**CPI7F96**	Frame with incorrect format or response received on line &23; attached to network interface &30;
CPI7F7A	Controller &26; failed.	**CPI7F97**	A frame with an incorrect count was received on line &23; attached to network interface &30;
CPI7F7B	Error on network interface &30; Internal System Failure.		
CPI7F7C	Error on network interface &30; Received command field was not correct.	**CPI7F98**	Frame with oversized information field received on line &23; attached to network interface &30;
CPI7F7D	Error on network interface &30; A frame with an incorrect format or response was received.	**CPI7F99**	Line &23; on network interface &30; failed, recovery stopped. Internal system failure.
CPI7F7E	Error on network interface &30;	**CPI8EAA**	Line &23; failed
CPI7F7F	Error on Network interface &30; A frame with an oversized information field was received.	**CPI8EAB**	Line &23; failed.
		CPI8EAF	Line &23; failed
CPI7F70	Controller &26; failed.	**CPI8EA5**	Line &23; failed
CPI7F71	Controller &26; failed.	**CPI8EA6**	Line &23; failed
CPI7F72	Controller &26; failed.	**CPI8EA7**	Line &23; failed.
CPI7F73	Controller &26; failed.	**CPI8EA8**	Line &23; failed
CPI7F74	Controller &27; failed.	**CPI8EC3**	Device &25; failed, recovery stopped.
CPI7F75	Controller &26; failed.	**CPI8EC4**	Device &25; failed, recovery stopped.
CPI7F76	Controller &26; failed.	**CPI8EC5**	Device &25; failed.
CPI7F78	Controller &26; failed.	**CPI8EC6**	Device &25; failed, recovery stopped.
CPI7F8A	Set-asynchronous-balance-mode-extended (SABME) frame received on network interface &30;	**CPI8EDB**	HDLC frame retry limit reached on line &23;
CPI7F8D	Receive CRC threshold limit reached on network interface &30;	**CPI8EEA**	Resource &27; failed.
		CPI8EEB	Line &23;
CPI7F80	Controller &26; failed.	**CPI8EE0**	Error on port &28;
CPI7F82	Controller &26; failed.	**CPI8EE4**	Resource &27; failed.
CPI7F9A	Error on line &23; attached to network interface &30; Internal system failure.	**CPI8EE8**	Resource &27; failed.
		CPI8EE9	Resource &27; failed.
CPI7F9C	Receive CRC limit reached on line &23,; attached to network interface &30;	**CPI8EFA**	Line &23; failed.
		CPI8EFB	Line &23; failed.

CPI8EFC Port &28; status information. Line &23; is running.

CPI8EFE Port &28; status information. Line &23; is running.

CPI8EFF Line &23; failed because of configuration error.

CPI8EF0 Line &23; failed.

CPI8EF9 Line &23; failed.

CPI8E4F Line &23; status information, line is running.

CPI8E47 Error occurred on Line &23;

CPI8E48 Line &23; failed, recovery stopped.

CPI8E5A Line &23; failed.

CPI8E5C Line &23; failed.

CPI8E5E Line &23; error information.

CPI8E52 Port &28; failed to come up on line &23;

CPI8E53 Communication port &28; of line &26; is already being used.

CPI8E54 Communication port &28; of line &23; not installed.

CPI8E55 Line &23; failed, recovery stopped.

CPI8E56 Line &23; failed, recovery stopped.

CPI8E58 Line &23; error information.

CPI8E6A Line &23; error information.

CPI8E6B Error on line &23;

CPI8E6D Line &23; failed.

CPI8E6E Error on line &23;

CPI8E6F No cable was detected on communication port &28; of line &23;

CPI8E67 Communication port &28; of network interface &30; not installed.

CPI8E68 An error occurred on line &23;

CPI8E69 Line &23; failed.

CPI8E7B Error on line &23;; connection cleared by network equipment.

CPI8E7C Line &23; failed, recovery stopped.

CPI8E7D Line &23; failed, token-ring line is no longer connected to the ring.

CPI8E7F Line &23; failed during connection to the token-ring network.

CPI8E8A Line &23; failed during insertion into the token-ring network

CPI8E8D Line &23; failed.

CPI8E8E Line &23; failed.

CPI8E8F Line &23; failed.

CPI8E86 Network interface &30; failed.

CPI8E87 Network interface &30; error information.

CPI8E89 Line &23; failed during insertion into the token-ring network.

CPI8E9B Error on network interface &30;

CPI8E90 Line &23; failed during insertion into the token-ring network.

CPI8E91 Line &23; failed.

CPI8E92 Line &23; failed during insertion into the token-ring network.

CPI8E98 Line &23; failed.

CPI8FA1 Line &23; failed.

CPI8FA2 Line &23; failed.

CPI8FA5 Line &23; failed.

CPI8FA7 Line &23; failed.

CPI8FA8 Line &23; failed.

CPI8FA9 Line &23; failed.

CPI8FBA Resource &27; failed.

CPI8FBF Token-ring resource &27; failed.

CPI8FB1 Line &23; failed.

CPI8FB8 Token-ring resource &27; failed.

CPI8FCA Line &23; failed during insertion into the token-ring network.

CPI8FCB Line &23; failed during insertion into the token-ring network.

CPI8FCC Line &23; failed during insertion into the token-ring network.

CPI8FCD Line &23; failed during insertion into the token-ring network.

CPI8FCE Line &23; failed.

CPI8FC0 Line &23; failed.

CPI8FC1 DSR signal connection failed.

CPI8FC2 Line &23; failed.

CPI8FC3 Line &23; failed.

CPI8FC9	X.25 Network Layer Protocol Error Detected on line &23;	**CPI8F13**	Line &23; failed.
		CPI8F14	Line &23; failed.
CPI8FD1	Line &23; failed.	**CPI8F15**	Line &23; failed.
CPI8FED	Port &28; status information. Line &23; is running.	**CPI8F17**	Line &23; failed.
		CPI8F18	Error on Port &28;
CPI8FFA	Line &23; threshold information.	**CPI8F19**	Error on port &28;
CPI8FFD	Ethernet resource &27; failed.	**CPI8F2A**	Line &23; failed.
CPI8FFE	Ethernet resource &26; failed.	**CPI8F2B**	Line &23; failed.
CPI8FF0	Call cannot be received for line &23; No connections available.	**CPI8F20**	Line &23; failed.
		CPI8F21	Line &23; failed.
CPI8FF1	Line &23; cannot be varied on due to lack of IOP resources	**CPI8F22**	Line &23; failed.
		CPI8F23	Line &23; failed.
CPI8F0A	Resource &26; failed.	**CPI8F24**	Line &23; failed.
CPI8F0B	Resource &26; failed.	**CPI8F25**	Line &23; failed.
CPI8F0C	Resource &27; failed.	**CPI8F26**	Line &23; failed.
CPI8F0E	Resource &26; failed.	**CPI8F29**	Line &23; failed.
CPI8F0F	DCE on network interface &30; not ready.	**CPI8F3A**	Line &23; threshold information.
		CPI8F3B	Port &28; status information. Line &23; is running.
CPI8F00	Resource &27; failed.		
CPI8F02	Resource &27; failed.	**CPI8F3D**	Network time-out type 1 occurred on Port &28; Line &23; is running.
CPI8F03	Resource &26; failed.		
CPI8F04	Resource &26; failed.	**CPI8F3E**	Network time-out type 2 occurred on Port &28; Line &23; is running.
CPI8F05	Resource &26; failed.		
CPI8F06	Resource &26; failed.	**CPI8F3F**	Network time-out type 3A occurred on Port &28; Line &23; is running.
CPI8F07	Resource &26; failed.		
CPI8F08	Resource &26; failed.	**CPI8F30**	Line &23; failed.
CPI8F09	Resource &26; failed.	**CPI8F31**	Line &23; failed.
CPI8F1A	Error on line &23;	**CPI8F32**	Line &23; failed.
CPI8F1B	Network interface &30; failed.	**CPI8F34**	Line &23; status information, line is running.
CPI8F1C	Error on communication port name &28;		
		CPI8F35	Line &23; failed.
CPI8F1D	Probable local hardware failure on network interface &30;	**CPI8F36**	Line &23; failed.
		CPI8F39	Line &23; failed.
CPI8F1E	Probable local hardware failure on network interface &30;	**CPI8F40**	Line &23; failed.
		CPI8F42	Line &23; failed.
CPI8F1F	Line &23; failed.	**CPI8F43**	Line &23; failed.
CPI8F10	Resource &27; failed.	**CPI8F44**	Line &23; failed.
CPI8F11	Resource &27; failed.	**CPI8F46**	Line &23; failed.
CPI8F12	Resource &27; failed.		

CPI8F5A	Line &23; failed.	**CPI8F98**	Error on port &28;
CPI8F5B	Line &23; failed.	**CPI8F99**	Error on line &23;
CPI8F5E	No cable was detected on port &28; of network interface &30;	**CPI889A**	I/O Optical Bus failure is detected.
CPI8F52	Line &23; threshold information.	**CPI889C**	Processor cannot communicate with System Unit Expansion unit.
CPI8F6A	Line &23; failed.	**CPI889D**	Optical bus cable is connected incorrectly.
CPI8F6E	Line &23; failed, token-ring line is no longer connected to the ring.	**CPI8890**	Failure during an operation with I/O processor.
CPI8F6F	Line &23; failed, token-ring line no longer connected to the ring.	**CPI8891**	I/O processor with resource name &26; is not operational.
CPI8F61	Line &23; failed.	**CPI8892**	I/O Bus Failure during operation with I/O processor.
CPI8F62	Line &23; failed.		
CPI8F65	Line &23; failed.	**CPI8893**	The I/O Bus Encountered no IOPs During IPL.
CPI8F7A	Line &23; failed, recovery stopped.		
CPI8F7B	Line &23; failed.	**CPI8897**	Processor cannot communicate with bus extension unit
CPI8F7C	Line &23; failed.		
CPI8F7D	Network time-out type 3B on Port &28; Line &23; running.	**CPI8898**	Optical signal loss is detected on optical bus.
CPI8F71	Network call-progress-signal type 23 on port &28; Line &23; running.	**CPI9340**	Error with work station adapter &24;
		CPI9341	A LIC error occurred on work station adapter &24;
CPI8F73	Line &23; failed.	**CPI9342**	Too many devices attached to work station adapter &24;
CPI8F79	Line &23; failed.		
CPI8F80	Line &23; failed.	**CPI9350**	Error with device &25; on work station controller &24;
CPI8F81	Line &23; failed.		
CPI8F82	A network time-out type 7 occurred on line &23;	**CPI9351**	Error with device &25; on work station controller &24;
CPI8F83	An error occurred on Line &23;	**CPI9352**	Error with device &25; on work station controller &24;
CPI8F84	A network time-out type 6 occurred on line &23;	**CPI9353**	Too many devices attached to work station controller &24;
CPI8F85	Line &23; failed.	**CPI9354**	Error with work station controller &24;
CPI8F86	Line &23; failed.	**CPI9355**	A Licensed Internal Code error occurred on work station controller.
CPI8F87	Line &23; error information.		
CPI8F88	Line &23; failed.	**CPI9356**	Error with magnetic stripe reader on device &25;
CPI8F9A	Network interface &30; failed.		
CPI8F9B	Network interface &30; failed.	**CPI9357**	Error with magnetic stripe reader or selector light pen on device &25;
CPI8F9C	Network not active on network interface &30;	**CPI9358**	Too many devices varied on to work station controller &24;
CPI8F92	Line &23; failed.		
CPI8F94	Line &23; failed.	**CPI9359**	Device configuration error occurred on work station controller &24;

CPI9360   Error with workstation I/O processor &24;

CPI9369   Error with remote workstation controller

CPI937A   Device configuration error detected by storage device controller card &26;

CPI937B   Communication failure between system and storage device controller card &26;

CPI937C   Non-supported device detected by storage device controller card &26;

CPI9370   Failure on storage device controller card &26;

CPI9371   Device format error reported by storage device controller card &26;

CPI9373   Device communication error reported by storage device controller card &26;

CPI9374   Failure reported by storage device controller card &26;

CPI9375   Failure reported by storage device controller card &26;

CPI9376   Failure reported by storage device controller card &26;

CPI9377   Failure on storage device controller card &26;

CPI9378   Failure reported by storage device controller card &26;

CPI9379   Failure on storage device controller card &26;

CPI9380   Error on line &23;

CPI9381   Error on line &23;

CPI9384   Controller &24; status information.

CPI9386   Error on network interface &30; Internal system failure.

CPI9387   Error on line &23; attached to network interface &30; Internal system failure.

CPI9389   Error on network interface &30; Internal system failure.

CPI94A0   Disk error on device &25;

CPI94BA   Read error on device &25;

CPI94BB   Diskette write error on diskette device &25;

CPI94BC   Error on diskette device &25;

CPI94BD   Diskette on device &25; type is not correct.

CPI94BE   Error on diskette device &25;

CPI94BF   Controller card failed in diskette device &25;

CPI94CB   This service mode is not supported for diskette device &25;

CPI94CE   Error detected in bus expansion adapter, bus extension adapter, System Processor, or cables

CPI94CF   Main Storage card failure is detected.

CPI94C1   Diskette device &25; failed read or write buffer test.

CPI94C2   Diskette device &25; error.

CPI94C3   Failure on diskette device &25;

CPI94C4   Diskette device &25; failed and has recovered.

CPI94C5   Diskette device &25; exceeded error threshold.

CPI94C6   Diskette device &25; cannot respond.

CPI94C7   Parity error on diskette device &25;

CPI94C8   Error occurred on diskette device &25; during tests.

CPI94DB   Control panel display not operating properly.

CPI94D8   Control panel battery either discharged or not connected.

CPI94D9   Service processor card real time clock failed.

CPI94EA   Input/output processor &26; does not recognize the attached device.

CPI94EB   Read error on tape reel or cartridge, tape unit &25;

CPI94EC   Write error on tape reel or cartridge, tape unit &25;

CPI94ED   Asynchronous device not expected.

CPI94E0   A tape media or tape unit &25; failure was detected.

CPI94E1   The format of the data for the tape unit &25; is not compatible.

CPI94E2   Licensed Internal Code error, tape unit &25;

CPI94E3 Tape unit &25; failed.

CPI94E4 Tape unit &25; received incorrect command or command parameter.

CPI94E6 User detected a diskette unit &25; problem.

CPI94E8 Input/output processor &26; failed.

CPI94E9 Licensed Internal Code error, I/O processor resource &26;

CPI94FA Tape I/O Processor &26; detected non supported device configuration.

CPI94FC Disk error on device &28;

CPI94F0 Either tape controller &26; or tape unit &25; failed.

CPI94F2 Tape I/O Processor &26; failed.

CPI94F5 Either Tape I/O Processor &26; or tape device &25; failed.

CPI94F6 Tape I/O Processor &26; program failed.

CPI94F8 Tape I/O Processor &26,; tape device &25,; or S/370 interface failure.

CPI9400 Controller &26; failed.

CPI9401 Controller &26; indicates control panel problem.

CPI9402 Controller &26; indicates adapter &27; error.

CPI9403 Controller &26; indicates error on tape or disk unit.

CPI9404 Controller &26; indicates error on diskette unit &28;

CPI9405 Controller &26; failed.

CPI9406 Error on tape reel or cartridge, tape unit &25;

CPI9407 Controller &26; indicates error on device &28;

CPI9408 I/O processor &26; error log full.

CPI946A Interface error: Tape unit &25; (resource &28); or IOP &26;

CPI946B IOP resource &26; recovered from temporary error.

CPI947A Disk motor problem.

CPI947B Data decompression hardware failure on IOP &26; IOP &26; is still operational.

CPI947C Time-of-Day function has failed on IOP &26,; IOP &26; is operational

CPI947D IOP &26; indicates adapter &27; error.

CPI947E Data compression hardware failure on IOP &26; IOP &26; is still operational.

CPI947F IOP &26; failed.

CPI9470 I/O processor &26; failed.

CPI9471 A lack of resources was detected on I/O processor &26;

CPI9472 Partial I/O processor &26; failure occurred.

CPI9475 Partial I/O processor &26; failure occurred.

CPI9476 Temporary Device Error.

CPI9477 Disk subsystem configuration error.

CPI9478 Disk command timeout error.

CPI9479 Disk Media Error.

CPI9485 Address switch setting changed on tape device &25;

CPI9486 Address switch failed on tape device &25;

CPI9487 Error on tape device &25;

CPI9488 Error when power turned on to tape device &25;

CPI9489 Error while loading tape on tape device &25;

CPI9490 Disk error on device &28;

CPI95A3 Optical Library &25; I/O station failure.

CPI95A6 Optical Library &25; storage slot failure.

CPI95A8 Optical Library &25; optical drive failure.

CPI95BA Optical Library &25; optical drive write failure.

CPI95B0 Optical Library &25; optical drive read failure.

CPI95B1 Access panel open on Optical Library &25;

CPI95B3 Optical Library &25; SCSI bus error.

CPI95B7 Optical Library &25; optical drive failure.

CPI95B8 Optical Library &25; optical drive failure.

CPI95B9 Optical Library &25; media or drive failure.

CPI95CB Optical Library &25; optical drive failure.

CPI95CD Optical Library &25; media error.

CPI95C8 Optical Library &25; device error.

CPI95DB Optical Library &25; IOP LIC failure.

CPI95DD Optical Library &25; found an optical drive which is not supported.

CPI95D0 Optical Library &25; drive status not valid

CPI95D1 Optical Library &25; SCSI bus error.

CPI95D3 Optical Library &25; internal failure.

CPI95D5 Optical Library &25; failed to respond.

CPI95E4 Optical Library &25; internal disk unit failed.

CPI9502 Tape Unit &25; lost power before end-of-tape processing completed

CPI958A Optical Library &25; data cartridge could not be moved.

CPI958D Optical Library &25; data cartridge could not be moved.

CPI9580 Optical Library &25; error occurred.

CPI9581 Optical Library &25; did not become ready.

CPI9582 Optical Library &25; data cartridge could not be moved.

CPI9583 Optical Library &25; autochanger failure.

CPI9584 Optical Library &25; autochanger failure.

CPI9586 Optical Library &25; power supply error.

CPI9587 Optical Library &25; power supply error.

CPI9588 Optical Library &25; optical drive not responding.

QCPFMSG Messages with ALROPT(*UNATTEND)

CPA2C64 File &1; was not found on device &2; (C R)

CPA2601 Device &25; failed. Recovery ended. (C G R)

CPA2602 Device &25; failed. Recovery ended. (C G R)

CPA2603 Device &25; could not establish sessions. Recovery ended. (C G R)

CPA3701 Compression not available on all devices. (C I)

CPA3704 Load tape containing library &1; on device &2; (C G)

CPA3705 Load previous tape volume on device &2; (C G)

CPA3706 Load next tape volume on device &2; (C G)

CPA3707 Load correct tape volume on device &2; (C G)

CPA400A Volume &5; density is not correct. (C R INZ)

CPA400C File label &4; with creation date &5; already exists on diskette in &3; (C R)

CPA400D ASCII code of volume &5; on device &4; is not valid (C R).

CPA400E ASCII code of volume &5; on device &4; is not valid (C INZ R).

CPA400F Media error while writing to volume &5; on device &4; (C G)

CPA4001 End of forms on printer &3; (C I)

CPA4002 Verify alignment on printer &3; (I G N R E C)

CPA4003 Form feed attachment &4; required on printer &3; (C G H)

CPA4004 End of ribbon on printer &3; (C H I PAGE 1-9999999)

CPA4005 End of ribbon on printer &3; (C I)

CPA4006 Volume &5; density is not correct. (C R)

CPA4007 Paper jam on printer &3; (C R)

CPA4008 Open cover on printer &3; (C H PAGE 1-9999999)

CPA4009 Open cover on printer &3; (C R)

CPA401A Volume &5; is not usable. (C R)

CPA401B Volume on device &4; at end of data. (C G)

CPA4010 Character on printer &3; not printable. (H I PAGE 1-9999999)

CPA4011 Character on printer &3; not printable. (C R)

CPA4012 Print check on printer &3; (C H PAGE 1-9999999)

CPA4013 Print check on printer &3; (C R)

CPA4014 Forms error on printer &3; (C H PAGE 1-9999999)

CPA4015 Forms check on printer &3; (C R)

CPA4016 End of forms on printer &3; (C H I PAGE 1-9999999)

CPA4017 End of forms on printer &3; (C I)

CPA4018 Operator action required on device &1;

CPA4019 Paper jam on printer &3; (C H PAGE 1-9999999)

CPA4020 Volume &5; not last volume for file &6; (C I R).

CPA4021 Load failure occurred on device &4; (C R)

CPA4022 Error while reading labels on device &3; (C R)

CPA4023 Volume &4; damaged for file sequence &5; (C R)

CPA4024 Volume &5; density differs from other volumes (C R INZ).

CPA4025 Diskette in &1; different from first diskette in multivolume file. (C R INZ)

CPA4026 Diskette in device &2; not prepared correctly. (C R INZ)

CPA4027 Code on volume &5; differs from previous volumes (C R).

CPA4028 Diskette in device &2; not written in &4; (C R INZ)

CPA4029 Diskette in &3; has wrong format for save or restore. (C R INZ)

CPA403E Tape management information not available. (C I R)

CPA403F Storage extension information not available. (I R)

CPA4030 Volume identifier not standard for file &2; in library &3; on device &4; (C I R)

CPA4031 Expected volume &6,; found volume &5; in device &3; (C I R INZ)

CPA4032 Volume table of contents (VTOC) read error on device &3; (C R INZ)

CPA4033 Diskette volume identifier &2; at device &1; not valid for save or restore. (C I R)

CPA4034 Volume &5; not first for file sequence number &6; (C I R).

CPA4035 Labels on volume &5; device &4; are not valid (C R).

CPA4036 File expiration dates out of sequence (C I R).

CPA4037 Character &5; on printer &3; not printable. (H I PAGE 1-9999999)

CPA4038 Character &5; on printer &3; not printable. (C R)

CPA4039 End of forms on printer &3; (C H I PAGE 1-9999999)

CPA4040 End of forms on printer &3; (C I)

CPA4041 Problem on device &1; requires operator help.

CPA4042 Print head overheating on printer &3; (C H I PAGE 1-9999999)

CPA4043 Print head overheating on printer &3; (C R)

CPA4044 Verify alignment on printer &3; (I C G R)

CPA4045 Diskette volume identifier &2; in device &1; not valid for save or restore. (C R INZ)

CPA4046 Print check on printer &3; (C H I PAGE 1-9999999)

CPA4047 Either end of forms or forms check on printer &3; (C H I PAGE 1-9999999)

CPA4048 End of forms or forms check on printer &3; (C I)

CPA4049 Error on diskette volume &6; device &1; (C R)

CPA4050 Not authorized to data on diskette in device &1; volume &2; (C R)

CPA4051 Not authorized to data on diskette in device &1; volume &2; (C R INZ)

CPA4052 Diskette in device &2; out of sequence. (C R)

CPA4053 One-sided diskette required in device &1; (C R)

CPA4054 Error while reading labels on device &3; (C R INZ)

CPA4055 No authority to access data (C INZ R).

CPA4056 Code on volume &5; differs from previous volumes (C INZ R).

CPA4057 Labels on volume &5; device &4; are not valid (C INZ R).

CPA4058 Volume &5; on device &4; wrong type (C INZ R).

CPA4059 Found &5;; expected &6; on device &4; (C I INZ R)

CPA4060 Device &4; cannot process loaded volume. (C R INZ)

CPA4061 Cannot initialize tape on device &4; (C R)

CPA4063 Cannot access data file on volume &5; device &4; (C INZ R).

CPA4064 Diskette in &1; did not format correctly. (C R INZ)

CPA4065 Check status lights on printer &3; (C H PAGE 1-9999999)

CPA4066 Check status lights on printer &3; (C R)

CPA4068 Volume &5; density differs from previous volumes. (C R)

CPA407A Paper size changed on printer &3; (C H PAGE 1-99999)

CPA4070 Diskette in device &1; has extended label area. (C R)

CPA4071 Platen protection tape on device &2; needs replacement. (I C)

CPA4073 Data position check on printer &3; (C H PAGE 1-9999999)

CPA4074 Data position check on printer &3; (C R)

CPA4075 Not enough storage on printer &3; (C H PAGE 1-9999999)

CPA4076 Not enough storage on printer &3; (C G)

CPA4077 Load form type '&2'; on printer &3; (I C G)

CPA4078 Paper length error on printer &3; (C H PAGE 1-9999999)

CPA4081 File &7; will be written over. (C I R)

CPA4082 Diskette in device &1; is write-protected. (C R)

CPA4085 Insert next diskette to receive a copy. (C G)

CPA4086 Device &4; was not ready or next volume was not loaded. (C R)

CPA4087 Diskette inserted in device &3; is not correct. (C R)

CPA4088 Load next tape volume on device &4; (C G)

CPA4089 Load volume &5; on device &4; (C G)

CPA4090 Device &4; was not ready. (C R)

CPA4091 Wrong cartridge type in device &4; (C R).

CPA4114 File &6; not found on volume &5; device &4; (C R).

CPA4124 Found &5;; expected &6; on device &4; (C R)

CPA4134 Cannot access data on volume &5; device &4; (C R).

CPA4158 Volume &5; on device &4; wrong type (C R).

CPA4240 No authority to access data file on volume &5; (C R).

CPA4251 Change LPI switch on printer &1; to &2; (C G)

CPA4252 Diskette device &3; not ready. (C R)

CPA4253 Extensive error recovery is occurring on diskette in device &1; (C I)

CPA4254 &4; LPI not allowed on printer &3; (C G)

CPA4257 Creation date of file label &4; not matching. (C I)

CPA4258 File label &4; already exists on diskette in &3; (C R)

CPA4260 Diskette in device &1; is not correct format. (C R)

CPA4261 Diskette in device &3; full. (C R)

CPA4262 Volume &5; on device &4; is write protected. (C R)

CPA4263 Volume &5; not loaded or device &4; not ready. (C R)

CPA4264 Found &5;; expected &6; on device &4; (C I R)

CPA4265 Diskette in device &2; not prepared. (C R)

CPA4267 Diskette in device &2; not written in &4; (C R)

CPA4268 Wrong continuation volume loaded on device &4; (C R).

CPA4270 Expected creation date and found date not the same (C I R).

CPA4271 Diskette in &3; has wrong format for save or restore. (C R)

CPA4272 File &1; label &5; in device &3; overlapped. (C I)

CPA4273 Diskette in device &1; cannot be used for output. (C R INZ)

CPA4274 Insert next diskette in device &3; (C G)

CPA4275 Diskette in device &3; has volume identifier &4; Insert diskette volume &5; (C I R)

CPA4276 File label &5; not found on diskette in &3; (C R)

CPA4277 Diskette in &2; out of sequence. (C I R)

CPA4278 Active file found on this volume (C I R).

CPA4279 Data file label &7; not found (C R).

CPA4280 Volume table of contents (VTOC) read error on device &3; (C R)

CPA4281 Operation not allowed on diskette in device &1; (C R)

CPA4282 Device &4; cannot process loaded volume. (C R)

CPA4297 &4; characters per inch not allowed on printer &3; (C G)

CPA4317 Device &4; cannot write to loaded volume. (C R)

CPA5213 Volume sequence number exceeds length of field in diskette HDR1 label.

CPA5230 End of VOL list for file &2; in &3; (C I).

CPA5243 Press Ready, Start, or Start/Stop on printer &1;

CPA5301 Diskette device &3; not ready. (C G)

CPA5316 Verify alignment on printer &3; (I C G N R)

CPA5327 Diskette in &1; different from first diskette in multivolume file. (C R)

CPA5328 Files on diskette in device &3; are active. (C I R)

CPA5329 End of list for volume ID reached for file &5; (C I)

CPA5335 End of forms on printer &3; (C H I PAGE 1-9999999)

CPA5339 Character &5; on printer &3; not printable. (H I PAGE 1-9999999)

CPA5340 Character &5; on printer &3; not printable. (C R)

CPA5341 Print error on printer &3; (C R)

CPA5342 Print error on printer &3; (C H I PAGE 1-9999999)

CPA5343 Forms check on printer &3; (C R)

CPA5344 Forms error on printer &3; (C H I PAGE 1-9999999)

CPA5347 Ribbon error on printer &3; (C R)

CPA5348 Ribbon error on printer &3; (C H I PAGE 1-9999999)

CPA57AC Controller &24; failed. No virtual circuits available. (C R)

CPA57EA Contact not successful on controller &24; LPDA test in progress. (C R)

CPA57ED Contact not successful on controller &24; LPDA test in progress. (C G R)

CPA57E5 Controller &24; failed. Probable timing problem. (C G R)

CPA57FF Controller &24; on line &23; not contacted. (C R)

CPA57F7 HDLC connection time-out occurred on line &23; (C N R)

CPA570F Controller &24; failed. XID not supported. (C G R)

CPA571A Controller &24; on line &23; not contacted. XID retry limit reached. (C R)

CPA571B Controller &24; on line &23; not contacted. XID retry limit reached. (C G R)

CPA571C Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA571E Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA571F Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA5714 System cannot call controller &24; No lines available. (C R)

CPA5719 Controller &24; not contacted. Configuration problem. (C R)

CPA572A Controller &24; not contacted. Probable remote system problem. (C R)

CPA572B Controller &24; not contacted. Probable remote system problem. (C G R)

CPA572C Controller &24; not contacted. Probable configuration problem. (C R)

CPA572D Controller &24; not contacted. Probable configuration problem. (C G R)

CPA572E Controller &24; on line &23; not contacted. Protocol error. (C R)

CPA572F Controller &24; on line &23; not contacted. Protocol error. (C G R)

CPA5722 System cannot call out on line &23; Connection list entry is *ANY for the remote number (C N R).

CPA5723 System cannot call out on line &23; Connection list entry error. (C N R)

CPA5724 System cannot call controller &24; No lines available. (C R)

CPA5725 System cannot call out on line &23; No network interfaces available. (C N R)

CPA5726 System cannot call out on line &23; Connection list &40; does not exist. (C N R)

CPA5727 System cannot call out on line &23; Unable to use connection list &40; (C N R)

CPA5728 System cannot call out on line &23; Connection list entry &41; not found. (C N R)

CPA5729 System cannot call out on line &23; Line unusable at this time. (C N R)

CPA573A Controller &24; on line &23; not contacted. Probable application program problem. (C R)

CPA573B Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA573D Controller &24; on line &23; not contacted. Local configuration problem. (C R)

CPA5732 Call on controller &24; failed. Connection list entry is *ANY for the remote number. (C R)

CPA5733 System cannot call out on controller &24; Connection list entry error. (C R)

CPA5734 System cannot call out on controller &24; Unable to use connection list &40; (C R)

CPA5735 System cannot call out on controller &24; Unable to use connection list &40; (C R)

CPA5736 System cannot call out on controller &24; Connection list entry &41; not found. (C R)

CPA5737 Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA5738 Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA5739 Controller &24; on line &23; not contacted. Local configuration problem. (C R)

CPA574A Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA574B Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA574C Controller &24; on line &23; not contacted. (C R)

CPA574D Controller &24; on line &23; not contacted. Probable remote system problem. (C G R)

CPA574E Controller &24; on line &23; not contacted. (C R)

CPA574F Controller &24; on line &23; not contacted. (C G R)

CPA5742 Controller &24; on line &23; not contacted. (C R)

CPA5743 Controller &24; on line &23; not contacted. (C G R)

CPA5746 Line &23; failed. RESTART CONFIRM packet not received within required time. (C G R)

CPA5747 Controller &24; failed. Logical channel reset or cleared. (C G R)

CPA5749 Line &23; failed. Inactivity timeout. (C G R)

CPA575A Controller &24; on line &23; not contacted. (C R)

CPA575B Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA575C Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA575D Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA575E Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA575F Controller &24; on line &23; not contacted. (C R)

CPA5750 Controller &24; contact not successful. Remote system disconnected. (C G R)

CPA5753 Controller &24; failed. No virtual circuits available. (C G R)

CPA5754 Controller &24; on line &23; not contacted. (C R)

CPA5756 Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA5758 Controller &24; contact not successful. Probable remote system problem. (C R)

CPA5759 Controller &24; on line &23; not contacted. (C R)

CPA576B Controller &24; on line &23; not contacted. (C R)

CPA576D Controller &24; contact not successful. Logical channel reset or cleared. (C G R)

CPA576E Logical channel to controller &24; reset or cleared. (C R)

CPA5760 Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA5761 Controller &24; on line &23; not contacted. Probable configuration problem. (C R)

CPA5762 Controller &24; on line &23; not contacted. Configuration problem. (C G R)

CPA5763 Controller &24; on line &23; not contacted. Configuration problem. (C G R)

CPA5764 Controller &24; on line &23; not contacted. (C R)

CPA5765 Controller &24; on line &23; not contacted. Remote system problem. (C G R)

CPA5766 Controller &24; on line &23; not contacted. (C R)

CPA5767 Controller &24; on line &23; not contacted. (C G R)

CPA5768 Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA5769 Controller &24; on line &23; not contacted. Probable configuration problem. (C G R)

CPA577A Controller &24; on line &23; Probable configuration problem. (C G R)

CPA577B Insufficient resources for controller &24; (C G R)

CPA577C Line &23; on network interface &30; not contacted. (C N R)

CPA577D Queue full on controller &24; (C G R)

CPA577F Queue full on controller &24; (C G R)

CPA5770 Controller &24; on line &23; Probable configuration problem. (C G R)

CPA5771 Controller &24; on line &23; Probable configuration problem. (C G R)

CPA5772 The call for line &23; on network interface &30; failed, no channels available. (C N R)

CPA5773 The call for line &23; on network interface &30; failed, B channel is busy. (C N R)

CPA5778 Network interface &30; failed, possible network problem. (C G R)

CPA5780 Call for line &23; on network interface &30; failed, possible network problem. (C N R)

CPA5783 Line &23; not contacted, insufficient resources. (C N R)

CPA5784 Line &23; on network interface &30; failed, call cleared. (C G R)

CPA5785 Line &23; on network interface &30; failed, possible network problem. (C G R)

CPA579D Controller &24; failed. Duplicate user facilities (C G R).

CPA579E Controller &24; contact not successful. Duplicate user facilities. (C R)

CPA58BA Call on line &23; failed. Forbidden call. (C N R)

CPA58BB Call on line &23; failed. No answer tone. (C N R)

CPA58BC Call on line &23; failed. No answer. (C N R)

CPA58BD Call on line &23; failed. (C N R)

CPA58BE Call on line &23; failed. Modem command not valid. (C N R)

CPA58B7 Call on line &23; failed. Modem aborted call. (C N R)

CPA58B8 Call on line &23; failed. Dial tone error. (C N R)

CPA58B9 Call on line &23; failed. Remote busy. (C N R)

CPA58C1 Line &23; failed. Probable communication subsystem problem. (C G R)

CPA58C2 Line &23; failed. Local configuration problem. (C G R)

CPA58C3 Line &23; failed. Local configuration problem. (C G R)

CPA58C4 Line &23; failed. Local configuration problem. (C G R)

CPA58C6 Controller &24; failed. Probable remote system problem. (C G R)

CPA58DA Call to controller &24; on line &23; failed. Forbidden call. (C R)

CPA58DB Call to controller &24; on line &23; failed. No answer tone. (C R)

CPA58DC Call to controller &24; on line &23; failed. No answer. (C R)

CPA58DD Call to controller &24; on line &23; failed. (C R)

CPA58DE Call to controller &24; on line &23; failed. Modem command not valid. (C R)

CPA58D1 Controller &24; failed. Remote system failure. (C G R)

CPA58D7 Call to controller &24; on line &23; failed. Modem aborted call. (C R)

CPA58D8 Call to controller &24; on line &23; failed. Dial tone error. (C R)

CPA58D9 Call to controller &24; on line &23; failed. Remote busy. (C R)

CPA58E0 Controller &24; not replying. Remote system or configuration problem. (C R)

CPA58E1 Controller &24; failed. Remote station problem. (C G R)

CPA58E2 Controller &24; failed. Probable remote system problem. (C G R)

CPA58E3 Controller &24; failed. Probable remote system problem. (C G R)

CPA58FA Network interface &30; failed. Probable communication subsystem problem. (C G R)

CPA58FE Controller &24; on line &23; not contacted. Remote disconnect. (C G R)

CPA58FF Controller &24; on line &23; not contacted. Remote disconnect. (C R)

CPA58F0 Call for line &23; on network interface &30; failed, call cleared. (C N R)

CPA58F2 Network interface &30; failed. Local configuration problem. (C G R)

CPA58F3 Network interface &30; failed. Local configuration problem. (C G R)

CPA58F4 Network interface &30; failed. Local configuration problem. (C G R)

CPA580B Controller &24; contact not successful. Remote system disconnected. (C R)

CPA5803 Line &23; not contacted. Internal system failure. (C N R)

CPA5804 Line &23; contact not successful on network interface &30; Configuration error (C N)

CPA5805 Manually dial &40; for line &23; (C G N)

CPA5806 Manually dial &40; for controller &24; line &23; (C G)

CPA5807 Device &25; is not responding normally. (C G R)

CPA5809 Dial pending for line &23; (C G)

CPA581A Controller &24; failed. Logical channel reset or cleared. (C G R)

CPA581B Controller &24; contact not successful. Logical channel reset or cleared. (C G R)

CPA581C Controller &24; contact not successful. Logical channel reset or cleared. (C R)

CPA5810 Line &23; is ready to answer. (C G N)

CPA5812 Call for line &23; on network interface &30; failed, internal system failure. (C N R)

CPA5815 Line &23; is ready to answer. (C G N)

CPA5823 No activity on line &23; Line disconnected. (C G R)

CPA583B Controller &24; failed. Packet-level time-out. (C G R)

CPA583C Controller &24; contact not successful. (C R)

CPA583D Controller &24; contact not successful. Packet-level time-out.(C G R)

CPA583E Call from controller &24; not accepted during recovery. (C G R)

CPA583F Call from controller &24; not accepted during recovery. (C R)

CPA5836 Time-out on line &23; System may be over committed. (C G R)

CPA5880 Place modem for line &23; in data mode. (C G)

CPA59AA Controller &24; failed. Probable remote system problem. (C G R)

CPA59AC Controller &24; failed. Configuration problem. (C G R)

CPA59AE Controller &24; failed. Probable configuration problem. (C G R)

CPA59AF Controller &24; failed. Probable remote system problem. (C G R)

CPA59A1 Controller &24; failed. XID retry limit reached. (C G R)

CPA59A3 Controller &24; failed. Probable configuration problem. (C G R)

CPA59A4 Controller &24; failed. Probable remote system problem. (C G R)

CPA59A6 Controller &24; failed. Probable configuration problem. (C G R)

CPA59A7 Controller &24; failed. Protocol error. (C G R)

CPA59A9 Controller &24; failed. Remote system problem. (C G R)

CPA59B1 Controller &24; failed. Probable remote system problem. (C G R)

CPA59DB Controller &24; contact not successful. Remote system problem. (C R)

CPA59DC Controller &24; contact not successful. Remote system problem. (C R)

CPA59DD Controller &24; contact not successful. Remote system problem. (C R)

CPA59D3 Line &23; failed. HDLC data link not active. (C G R)

CPA59D4 Controller &24; failed. Probable network problem. (C G R)

CPA59FA Internal system failure on line &23; (C G R)

CPA59F9 Controller &24; failed. Internal system failure. (C G R)

CPA5902 Controller &24; not contacted. Call out request failed. (C R)

CPA592C Line &23; failed. Network configuration problem. (C G R)

CPA592E Network interface &30; failed. Cable or hardware problem. (C G R)

CPA592F Network interface &30; failed. Communication link problem. (C G R)

CPA593D Contact not successful on controller &24; Network interface is busy (C G R).

CPA593E Contact not successful on controller &24; Exceeded maximum controllers (C G R).

CPA596E Line &23; on network interface &30; failed. Probable configuration problem. (C G R)

CPA5968 Controller &24; contact not successful. Probable remote system problem. (C R)

CPA5969 Controller &24; contact not successful. Probable remote system problem. (C G R)

CPA6103 Sector size of diskette in &2; not valid. (C R INZ)

CPA6104 File label expiration date &5; on diskette in &3; has not been reached.(C I)

CPA6105 Creation date of file and creation date on command not same. (C I)

CPA6106 Cannot clear diskette in device &3; (C R)

CPA6111 Cannot process diskette in device &3; (C R)

CPA6113 Diskette in device &3; not correct. (C R)

CPA6114 Diskette format in device &2; not valid. (C R)

CPA6115 Code of diskette in &2; not valid. (C R INZ)

CPA6124 Format of diskette in device &2; not correct. (C R INZ)

CPA6162 Diskette in &1; will not be reorganized. (C I)

CPA6745 Volume on device &4; is write protected (C R).

CPA6746 Volume on device &4; cannot be processed (C R).

CPA6747 Volume on device &4; cannot be processed (C R INZ).

CPA6748 End of VOL list for device &4; (C I).

CPA6751 One-sided diskette in device &3; (C R)

CPA6752 Diskette in device &1; is write-protected. (C R)

CPA6755 Data on diskette in &1; not accessible for processing. (C R)

CPA6759 Defective diskette in device &5; (C R)

CPA6761 Active files on diskette in device &1; (C I R)

CPA6770 Data on diskette in device &1; cannot be accessed. (C I R)

CPA6773 VTOC indicates one-sided diskette in device &1; (C R)

CPA9E10 The usage limit for product &1,; feature &3; has been increased. (G)

CPA94EB Tape device &25; not ready.

CPA94EC Tape on tape device &25; is damaged.

CPA94ED Tape controller &26; error can be recovered.

CPA94EE Tape device &25; error can be recovered.

CPA94EF Tape device &25; busy.

CPA94FB Error log full in Tape I/O Processor &26;

CPA94F3 Tape device &25; not ready or not loaded.

CPA94F4 Tape on tape device &25; is damaged.

CPA9480 Top cover or front door not closed for tape device &25;

CPA9481 Tape reel missing for tape device &25;

CPA9482 Tape reel inverted for tape device &25;

CPA9483 Tape reel beginning-of-tape marker missing on tape device &25;

CPA9484 Tape reel not seated correctly on tape device &25; supply hub.

CPD26D4 Line resource name &1; not found.

CPD26D5 Controller resource name &1; not found.

CPD26D6 Device resource name &1; not found.

CPD2609 Device &25; configuration not valid. Reason code &1;

CPD2614 Device &25; vary request stopped.

CPD2615 Controller &24; vary configuration failed.

CPD2616 Device &25; vary failed. No recovery attempted.

CPD2619 Controller &24; not varied on. Reason code &1;

CPD2620 Line &23; Vary Configuration failed.

CPD2627 Automatic call line resource name &1; not found.

CPD2628 Controller &24; Vary Configuration failed.

CPD2629 Device &25; automatic vary on failed.

CPD2635 Line &23; vary on stopped.

CPD2641 Controller &24; class of resource conflict.

CPD2642 Controller &24; resource type conflict.

CPD2652 Device &25; resource type conflict.

CPD2653 Device &25; model number conflict.

CPD2656 Line &23; reset failed.

CPD2657 Controller &24; reset failed.

CPD2658 Device &25; reset failed.

CPD2659 Line &23; was not varied on.

CPD2674 Device &25; vary on failed. Reset required.

CPD2679 Device &25; vary on failed.

CPD2689 Device &25; vary configuration request stopped.

CPD2690 Line &23; vary configuration failed. Reset required.

CPD2691 Controller &24; vary failed. Reset required.

CPD2692 Device &25; vary on failed. Reset required.

CPD2693 Device &25; vary processing stopped.

CPD27F7 Device &25; vary processing stopped.

CPD27F8 Device &25; vary processing stopped.

CPD2712 Line &23; vary failed. No recovery attempted.

CPD2713 Controller &24; vary failed. No recovery attempted.

CPD2715 DBCS font table &1; not found.

CPD2716 Line &23; in test mode.

CPD2717 Controller &24; in test mode.

CPD2718 Device &25; in test mode.

CPD2731 Line &23; vary on failed.

CPD2739 Line &23; class of resource conflict.

CPD2747 Device &25; class of resource conflict.

CPD28B7 Line &23; resource names not on same IOP.

CPD28CB Controller &24; vary on stopped.

CPD28E7 Line &23; vary on stopped.

CPD28E8 Line &23; vary on stopped.

CPD28FE Controller &24; vary on stopped.

CPD2895 Line &23; vary on stopped.

CPD2898 Controller &24; vary on stopped.

CPD70E6 Service required on ASP &1; for access path protection.

CPD702F Internal system failure. System-managed access-path protection not started during IPL.

CPD703F System-managed access-path protection ended unexpectedly.

CPD8EC8 Line &23; vary configuration failed.

CPD8E4C Network interface &30; in test mode.

CPD8E40 Network interface resource name &1; not found.

CPD8E41 Network interface &30; vary configuration failed.

CPD8E43 Network interface description &30; reset failed.

CPD8E44 Network interface &30; class of resource conflict.

CPD8E46 NWI &30; vary configuration failed. Reset required.

CPD8E60 Controller &24; Vary Configuration failed.

CPD8F51 Line &23; vary on stopped.

CPD8F75 Network server &30; in test mode.

CPD8F76 Network server resource name &1; not found.

CPD8F77 Network server &30; class of resource conflict.

CPF410D Device &4; can not be assigned to system.

CPF410E Network interface &9; failed while opening file on device &4;

CPF4108 Media error on volume &8; device &4;

CPF4118 Device &4; was reset.

CPF4119 Device &4; cannot process loaded volume.

CPF4120 Device &4; equipment check.

CPF4121 Error on device &4;

CPF4141 SNA protocol violation for data received for remote location &5,; device description &4;

CPF4143 Internal system failure for remote location &5,; device description &4;

CPF4146 Line &9; failed while opening a file on device &4;

CPF4149 Session ended by a request from device &4;

CPF4178 TERM-SELF, UNBIND, or NOTIFY received for remote location name &5,; device description &4;

CPF4190 Error on device &4;

CPF4192 Error on device &4; Device response code is &6;

CPF4231 Negative response with sense data &7; received for remote location &5;

CPF4239 Device &4; dropped ready.

CPF4256 Diskette in device &4; is write-protected.

CPF4257 Diskette exchanged during processing.

CPF4258 Device &4; equipment check.

CPF4260 Session not established for remote location &5,; device description &4;

CPF4265 Error for remote location &5,; device description &4;

CPF4315 Device &4; no longer in ready status.

CPF4316 Volume loaded on device &4; is write protected.

CPF4371 Diskette or Tape device &4; is not operational.

CPF4372 Load failure encountered on device &4;

CPF4373 End of media on device &4;

CPF4388 Format of diskette in device &4; is not supported.

CPF450D Device &4; can not be assigned to system.

CPF450E Network interface &9; failed while closing file on device &4;

CPF4501 Equipment check on device &4;

CPF4515 Device no longer in ready status.

CPF4533 Error on device &4; Device response code is &6;

CPF4534 Diskette or Tape device &4; is not operational.

CPF4535 Load failure on device &4;

CPF4536 End of media on device &4;

CPF4538 Session stopped by request from device &4; Probable device error.

CPF4540 Device &4; dropped ready.

CPF4542 Line &9; failed while closing the file on the device &4;

CPF4544 Error on device &4;

CPF4545 Device &4; is not ready.

CPF4549 Format of diskette in device &4; is not supported.

CPF4553 Error on file &2; in library &3; device &4;

CPF4556 Volume on device &4; is write pro-tected.

CPF4569 Media error on volume &8; on device &4;

CPF4588 Device &4; cannot process loaded volume.

CPF4594 Device &4; was reset.

CPF4595 Diskette in device &4; is write-protected.

CPF4596 Diskette changed during processing.

CPF4597 Device &4; equipment check.

CPF5D62 Error occurred in translation routines.

CPF5047 Response received from device &4; not defined.

CPF510D Device &4; can not be assigned to system.

CPF510E Network interface &9; failed while doing a read or write to device &4;

CPF5101 Error on device &4;

CPF5103 Error on device &4; Device response code is &6;

CPF5106 Error on device &4; Device response code is &6;

CPF5110 Device &4; had an equipment check.

CPF5128 Line &9; failed while doing read or write to device &4;

CPF5135 Device &4; was reset.

CPF5140 Session stopped by a request from device &4;

CPF5143 Error on device &4; Device response code is &6;

CPF5162 Volume loaded on device &4; is protected.

CPF5167 SNA session for remote location &5,; device description &4; ended abnormally.

CPF5182 Relocated diskette sector detected.

CPF5197 Failure for remote location &5,; device description &4; for retail pass-through session.

CPF5198 Error on control unit &9; to which device &4; attached.

CPF5199 Error on device &4; Device response code is &6;

CPF5233 Device &4; cannot process loaded volume.

CPF5242 Device &4; dropped ready.

CPF5243 Operator action required on device &1;

CPF5244 Internal system failure for remote location &5,; device description &4;

CPF5248 SNA protocol violation for data received for remote location &5,; device description &4;

CPF5250 Negative response with sense data &7; received for remote location &5;

CPF5270 Device &4; no longer in ready status.

CPF5298 Internal system failure for retail pass-through program in job &7/&8/&9;

CPF5327 Diskette in device &4; is write-protected.

CPF5328 Diskette changed during processing.

CPF5329 Device &4; equipment check.

CPF5330 Format of diskette in device &4; is not supported.

CPF5331 Device &4; is not ready.

CPF5341 SNA session not established for remote location &5,; device description &4;

CPF5346 Error for remote location &5,; device description &4;

CPF5347 Error for remote location &5,; device description &4;

CPF5349 Media error on volume &8; on device &4;

CPF5384 Diskette or Tape device &4; is not operational.

CPF5385 Load failure on device &4;

CPF5386 End of media on device &25;

CPF5401 Interface error on device &4;

CPF5418 Transmit not allowed until previous response for device &4; is received.

CPF5419 Request from function manager not supported.

CPF5420 Signal code not correct for device &4;

CPF5422 Device &4; session is not active.

CPF5423 Not able to transmit to device &4; Session not in send condition.

CPF5427 SNA session to device &4; in error pending condition.

CPF5429 No response from the previous request on expedited flow.

CPF5430 Data stream sent to the device &4; not valid.

CPF5431 Too many or too few request descriptors requested.

CPF5433 Wait option not allowed on chain-and-one-half request.

CPF5434 Partial chain request to device &4; not allowed.

CPF5915 Line &23; not in a valid state for answering.

CPF5918 No valid entries in line list for controller &24;

CPF598D Incorrect network management data received.

CPF6151 Cannot duplicate diskette in device &1;

CPF6165 Device &1; is not ready.

CPF6702 Error processing volume on device &1;

CPF6751 Load failure occurred on device &4;

CPF6760 Device &1; not ready.

CPF6768 Volume on device &1; is write protected.

CPF6780 Defective cylinder on volume &1;

CPF6781 Defective cylinders on volume &1;

CPF6792 Device &25; needs to be cleaned.

CPF6797 Command did not complete on device &25;

CPF6798 Command for device &25; failed to complete.

CPF7A82 Error occurred while applying the problem filter.

CPF7A83 Problem filter &1/&2; not found.

CPF70F2 Service required for access path protection.

CPF702D System-managed access-path protection started using system default recovery times.

CPF702E Access path recovery times set or reset to system defaults.

CPF9E17 Usage limit exceeded for product &1; User added.

CPF9E18 Attempt made to exceed usage limit for product &1; User not added.

CPF9E70 Grace period expired. Requesting user already added.

CPF9E71 Grace period expired. Requesting user not added.

CPF9E72 Usage limit of &4; exceeded. Grace period will expire on &5;

CPF9E73 Expiration date &4; was reached.

CPF9E74 License key not valid.

CPF9E78 The license key for product &1,; license term &2,; feature &3; is no longer valid.

CPF90D8 Host printing of mail items ended; start QSNADS.

CPF91E8 Internal processing error occurred.

CPF9355 Controller for location &4; in network &5; is not available.

CPF9356 Logical connection not established for APPC device &25;

CPF9357 System detected an internal error on controller &24;

CPF9358 Sessions for all devices on controller &24; ended abnormally.

CPF9359 All work on controller &24; ended because of system error.

CPF9360 Connection attempt not accepted for controller description &24;

CPF94FC Type-ahead data stream not supported by controller.

CPF94FD Type-ahead option parameter value not valid.

CPI0946 Mirrored protection is suspended on disk unit &1;

CPI0947 Mirrored protection is suspended on disk unit &1;

CPI0948 Mirrored protection is suspended on disk unit &1;

CPI0949 Mirrored protection suspended on disk unit &1;

CPI0950 Storage unit now available.

CPI0957 Mirrored protection suspended on disk unit &1;

CPI0958 Mirrored protection suspended on disk unit &1;

CPI0988 Mirrored protection resuming on disk unit &1;

CPI0989 Mirrored protection resumed on disk unit &1;

CPI0998 Error occurred on disk unit &1;

CPI1144 Job scheduling function not active. Job schedule &1; in library &2; not available.

CPI1162 Unit &1; with device parity protection not fully operational.

CPI1466 Job holds large number of locks.

CPI1467 System lock table nearing capacity.

CPI3A31 Starting recovery for SNADS *SVDS sender &3/&2/&1; serving distribution queue &4;

CPI4015 Character cannot be printed on device &3; for file &1; in library &2;

CPI4016 Forms error on device &3; for file &1; in library &2;

CPI4017 Print check on device &3;

CPI4018 Cover open on device &3;

CPI4019 Ribbon error on device &3;

CPI4020 End of forms or forms jam on device &3;

CPI4024 Print head overheating on device &3;

CPI5730 Network server description &30; not usable at this time.

CPI58EA Session activation for device &25; and associated device &41; failed.

CPI58EB Session cannot be established for device &25;

CPI58EC Session for device &25; and associated device &41; ended abnormally.

CPI58ED Dial attempt for session for device &25; failed.

CPI58EE Downstream SNPT device &25; rejected activation.

CPI58E6 Error occurred on SNA pass-through session on control point &43;

CPI58E8 Group name &42; for device &25; does not exist.

CPI58E9 Associated device not configured for device &25;

CPI580B Attempt to lock device &25; during recovery failed.

CPI5800 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI5801 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI5802 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI5803 Incoming X.25 call for Controller &24; was rejected by the local system.

CPI5805 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI5806 An incoming call received on Network Interface &30; was rejected by the local system.

CPI5811 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI5812 An incoming-packet mode call received on Network Interface &30; was rejected by the local system.

CPI5813 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI5814 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI5815 An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI5816 Cannot retrieve configuration information.

CPI59AA The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59AE The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59AF The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59A1 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59A6 X.25 incoming call request on line &23; rejected.

CPI59BA The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59BB The local system rejected an incoming ISDN call received on network interface &30;

CPI59BC The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59BD The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59BE The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59BF The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59B3 Controller &24; failed. Maximum errors allowed exceeded.

CPI59B4 Device &25; failed. Maximum errors allowed exceeded.

CPI59B6 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59B7 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59B8 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59B9 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59CB Network interface &30; selected for line &23,; some network interfaces not chosen by the system.

CPI59CC The local system can no longer process incoming ISDN or X.25 calls.

CPI59C6 The local system rejected an incoming ISDN call received on Network Interface &30;

CPI59DD Resources for Network Interface &30; not sufficient.

CPI59D3 Unacknowledged service on device &25; was not successful.

CPI59D4 Controller &24; vary on failed while down loading PTFs.

CPI59D5 Automatic error recovery for network interface &30; canceled during IPL.

CPI59D6 Automatic error recovery for line &23; canceled during IPL.

CPI59D7 Automatic error recovery for controller &24; canceled during IPL.

CPI59D8 Automatic error recovery for device &25; canceled during IPL.

CPI59EA An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59EB An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59EC An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59ED An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59E6 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59E7 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59E8 An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI59FA Session activation for device &25; and associated device &41; failed.

CPI59FB Session cannot be established for device &25;

CPI59FC Session for device &25; and associated device &41; ended abnormally.

CPI59FD Dial attempt for session for device &25; failed.

CPI59FE Associated device &41; not compatible with activating device &25;

CPI59FF Internal system failure related to device &25;

CPI59F9 Associated device or group not configured for device &25;

CPI590A Line &23; failed. Configuration error or internal system failure.

CPI590B No keyboard translate table for device &25;

CPI590C Device &25; not contacted. Probable device failure.

CPI590D Local system rejected call from remote system on line &23;

CPI590E Local system rejected call from remote system on line &23;

CPI590F Local system rejected call from remote system on line &23;

CPI5902 Incoming call request on line &23; rejected.

CPI5905 Incoming call request on line &23; rejected.

CPI5908 Remote system trying to contact device &25; Device varied off or not responding.

CPI591A Controller on line &23; varied off or not recognized by local system.

CPI591E Resources for controller &24; not sufficient.

CPI5916 Incoming call request on line &23; rejected.

CPI5918 Line &23; has failed.

CPI5919 Customized table for device &25; not found.

CPI592A Resources for line &23; not sufficient.

CPI5920 Network interface description &30; not usable at this time.

CPI5922 Device description &25; is not usable at this time.

CPI5923 Controller description &24; in use.

CPI5924 Controller description &24; in use.

CPI5925 Controller description &24; in use.

CPI5927 Line description &23; in use.

CPI5929 Line description &23; in use. The switched connection may not have disconnected.

CPI593A Controller &24; failed. Probable network configuration problem.

CPI593B Controller &24; failed. Probable network configuration problem.

CPI593C Controller &24; failed. Probable network configuration problem.

CPI593F Controller &24; failed. Probable local configuration problem.

CPI594A LOCADR parameter for device &25; not correct.

CPI594B A networking device incompatible with device &25;

CPI594C A networking device incompatible SNGSSN parameter with device &25;

CPI594E Call from controller on line &23; not accepted.

CPI594F Call from controller on line &23; not accepted.

CPI5941 Controller description &24; not usable at this time.

CPI5942 Line description &23; not usable at this time.

CPI5943 Call from controller on line &23; not accepted.

CPI5944 Call from controller on IDLC line &23; rejected.

CPI5945 Automatic error recovery for network interface &30; canceled during IPL.

CPI5946 Automatic error recovery for line &23; canceled during IPL.

CPI5947 Automatic error recovery for controller &24; canceled during IPL.

CPI5948 Automatic error recovery for device &25; canceled during IPL.

CPI595A Call from controller on line &23; not accepted.

CPI595B Call from controller on line &23; not accepted.

CPI595C Call from controller on line &23; not accepted.

CPI5961 Device &25; cannot be used. Internal failure in system.

CPI597A An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI598B An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI598C An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI598D An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI598E An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI598F An incoming packet-mode call received on Network Interface &30; for Controller &24; was rejected.

CPI599A The local system rejected an incoming ISDN call received on Network Interface &30;

CPI599B An incoming call received on Network Interface &30; was rejected by the local system.

CPI599C An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI599D An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI599E An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI599F An incoming packet-mode call received on Network Interface &30; was rejected by the local system.

CPI7BC5 Alert filter &2/&1; not found.

CPI7BC6 Alert not sent to system &1;&2;

CPI7E51 Clear packet sent on logical channel on line &23;

CPI70EA QDBSRV01 system job abnormally ended.

CPI70E4 IPL required for internal system journal support.

CPI70FF Internal system journal function failed.

CPI8C45 Job for receiving PTFs has ended.

CPI8EBF Logical channel on line &23; was reset by the local system.

CPI8ECF Logical channel on line &23; was cleared by the local system.

CPI8EC7 All logical channels on line &23; were restarted by the local system.

CPI8EC8 Logical channel on line &23; was reset by the network.

CPI8EC9 Logical channel on line &23; was cleared by the network.

CPI8EDA HDLC frame sent on line &23; was rejected by the network

CPI8EDC HDLC data link has been disconnected on line &23;

CPI8EDD HDLC data link establishment failed on line &23;

CPI8EDF CLEAR CONFIRM packet not received on line &23; within required time.

CPI8ED0 All logical channels on line &23; were restarted by the network.

CPI8ED1 RESTART CONFIRM packet not received on line &23; within required time.

CPI8ED2 RESET CONFIRM packet not received on line &23; within required time.

CPI8ED3 Frame received on line &23; rejected by local system.

CPI8ED4 HDLC frame received on line &23; was rejected by the local system.

CPI8ED5 HDLC frame received on Line &23; was rejected by the local system.

CPI8ED6 HDLC frame received on line &23; was rejected by the local system.

CPI8ED7 Frame received on line &23; rejected by network.

CPI8ED8 HDLC frame sent on line &23; was rejected by the network.

CPI8ED9 HDLC frame sent on line &23; was rejected by the network.

CPI8EE2 The HDLC data link on line &23; was reset by the network.

CPI8EE3 Line &23; data link reset, disconnect mode (DM) frame received from network.

CPI8F96 Line &23; failed.

CPI8F97   Call not completed within specified time limit on line &23;

CPI8803   Library QUSRSYS not found.

CPI8805   Starting recovery for SNADS sender &5/&4/&3,; serving *SNADS distribution queue &1;

CPI8806   Error occurred while the QSNADS subsystem was being started.

CPI8812   Error occurred while SNADS processes were being submitted.

CPI8825   Starting recovery for SNADS gateway sender &3/&2/&1,; serving &5; distribution queue &4;

CPI9E19   Usage limit threshold exceeded for product &1;

CPI9E75   Grace period will expire on &4;

CPI9E76   Expiration date will be reached on &4;

CPI9E77   License key will not be valid in &8; days.

CPI9385   Line &23; status information.

CPI94C0   Address changed on diskette device &27;

Appendix C.   Alerts Differences

This appendix describes the differences in alert support between the AS/400 system and the System/36 and System/38.

Differences from System/36 Alert Support

The following is a list of differences between alert support on the AS/400 system and on System/36:

- System/36 alert support uses an APPC or APPN subsystem for sending alerts to a host system or to another system that is capable of receiving alerts. These alerts are sent on an SSCP-PU or PU-PU session. Management services sessions (as described in Management Services Session) are not supported. You define the alert support on System/36 when you use the CNFIGICF procedure to configure an APPC or APPN subsystem. For alert support, two items are specified in the subsystem configuration:

    - The remote location with which the subsystem is to communicate

    - That alerts are to be sent

    The AS/400 system uses APPC/APPN support and management services sessions for sending alerts to AS/400 systems or other systems that support management services capabilities. On a focal point AS/400 system, you specify the systems that will send alerts to your system by defining the sphere of control. You can define the destination of alerts for a system that does not support management services capabilities using the alert controller description for the ALRCTLD parameter of the Change Network Attributes (CHGNETA) command.

- To start System/36 alert support, you must enable the APPC or APPN subsystem using the ENABLE procedure command. Once the subsystem that specifies the alert location is enabled, alert generation is started.

    The creation of alerts on the AS/400 system is controlled by the alert status (ALRSTS) network attribute.

- Using System/36 alert support, you generate alerts from a predefined subset of system messages using the ALERT procedure. You can also generate alerts for any user-defined message for any error condition that can occur on System/36 using the SETALERT procedure.

    When an error condition occurs that causes an alertable message to be issued by the System/36, an alert corresponding to that error condition is generated and sent to the specified system. An alertable message on System/36 is any message with the alert generation status indicator set to Y (Yes).

    Alerts on the AS/400 system are controlled by OS/400 messages. When a message that is alertable is sent to the QSYSOPR message queue, an alert is created by the system. This message is marked as alertable using the alert options (ALROPT) parameter in the OS/400 message description. You change the message description using the Change Message Description (CHGMSGD) command.

- Any received alerts or locally generated alerts are logged to a disk file (ALERTFIL) on System/36. Alerts are only logged when they cannot be sent; for example, when the line becomes disconnected or when there is no active alert location to receive alerts.

    The AS/400 system logs alerts in a physical file (QAALERT in library QUSRSYS). The logging of alerts is controlled by the alert logging status (ALRLOGSTS) network attribute.

- You can send an operator-generated alert on System/36 using the ALERT NOTIFY procedure command.

    You can send an operator-generated alert on the AS/400 system using the Analyze Problem (ANZPRB) command. You can also use one of the alert messages defined for general use (CPI9804, CPI9805, and CPI9806).

- System/36 sends network management vector transport (NMVT) format pre-generic alerts. The AS/400 system supports the SNA generic alert architecture, either in NMVT format or control point management services unit

(CP-MSU) format. See the *SNA Formats* book for information on alert formats.

Differences from System/38 Alert Support

The following is a list of differences between the AS/400system and System/38:

- System/38 alert support uses an system services control point-physical unit (SSCP-PU) session for sending alerts to a host system or to another system that is capable of receiving alerts. You define the destination of alerts using the alert control unit (ALRCTLU) parameter of the Change Network Attributes (CHGNETA) command.

  The AS/400 system uses APPC/APPN support and management services sessions for sending alerts to AS/400 systems or other systems that support management services capabilities. On a focal point AS/400 system, you specify the systems that will send alerts to your system by defining the sphere of control. You can define the destination of alerts for a system that does not support management services capabilities using the alert controller description (ALRCTLD) parameter of the Change Network Attributes (CHGNETA) command.

- The generation of alerts is controlled on System/38 using the alert status (ALRSTS) network attribute.

  The creation of alerts on the AS/400 system is also controlled using the alert status (ALRSTS) network attribute. In addition to values of *ON and *OFF, the AS/400system supports a value of *UNATTEND for unattended operation.

- An alertable message on System/38 is any message with an alert ID other than *NONE. System/38 sends an alert when such a message is sent to the QSYSOPR message queue. You specify which messages are alertable using the alert ID (ALRID) parameter of the Change Message Description (CHGMSGD) command.

  You specify which messages are alertable on the AS/400 system using the alert options (ALROPT) parameter of the Change Message Description (CHGMSGD) command.

- Any received alerts or locally generated alerts are logged to a journal (QALERT in library QUSRSYS) on System/38. Alerts are logged in the journal when the alert focal point (ALRFOCPNT) network attribute is *YES.

  The AS/400 system logs alerts in a physical file (QAALERT in library QUSRSYS). The logging of alerts is controlled by the alert logging status (ALRLOGSTS) network attribute. The alert primary focal point (ALRPRIFP) and alert default focal point (ALRDFTFP) network attributes are used with the OS/400sphere of control support, and are not the same as the System/38 ALRFOCPNT network attribute.

- System/38 does not support held alerts. If System/38 cannot send an alert to the destination specified in the ALRCTLU network attribute, the alert is discarded.

- Messages CPI9804, CPI9805, and CPI9806 are defined as alertable for your use on System/38.

  Messages CPI9804, CPI9805, and CPI9806 are also defined on the AS/400 system. In addition, you can send an operator-generated alert using the Analyze Problem (ANZPRB) command.

- System/38 sends network management vector transport (NMVT) format pre-generic alerts. The AS/400 system supports the SNA generic alert architecture, either in NMVT format or control point management services unit (CP-MSU) format. See the *SNA Formats* book for information on alert formats.

Appendix D. Migration Concerns

This appendix discusses migration concerns that may appear in networks that are not exclusively comprised of Version 2 Release 2 systems.

Looping Considerations

When configuring a network for sending alerts, it is possible to create a looping condition. The OS/400 alert support provides a way to prevent a looping condition. In each alert, the AS/400 system remembers every focal point that has either created or forwarded the alert. When forwarding an alert, the focal point checks to see if it has already processed this alert. If it has, a message is sent to the system operator, and the alert is not forwarded. This applies if the network is comprised of Version 2 Release 2 systems.

Held Alerts

When a system is started, the alert manager attempts to find an alert focal point. If a focal point was assigned before the IPL, the alert manager attempts to use that system as a focal point. If a focal point is not available, the alerts are not held.

Bibliography

The following publications provide additional information about the topics described or referred to in this book. The books are listed with their full titles and order numbers. When AS/400 books are referred to in this book, a shortened version of the title is used.

IBM Publications

Communications and Programming

The following IBM AS/400 publications provide additional information about topics described or referred to in this book:

- *Backup and Recovery*, SC41-5304 provides information to help you become familiar with AS/400 functions, develop a backup plan, and recover from system failures.

- *APPN Support*, SC41-5407 provides information about the concepts of AS/400advanced peer-to-peer networking (APPN) and about planning APPN networks.

- *APPC Programming*, SC41-5443 describes the advanced program-to-program communications (APPC) support for the AS/400 system and provides the information necessary for developing communications application programs.

- *SNA Distribution Services*, SC41-5410 provides the information about using Systems Network Architecture distribution services (SNADS), object distribution, VM/MVS bridge, and the system distribution directory.

- *ISDN Support*, SC41-5403 contains information on AS/400 connectivity to an integrated services digital network (ISDN) using AS/400 integrated communications adapter.

- *LAN and Frame Relay Support*, SC41-5404 contains information on using an AS/400 system in a token-ring network, Ethernet network, or bridged network environment.

- *X.25 Network Support*, SC41-5405 contains information on using AS/400 systems in an X.25 network.

- *Communications Management*, SC41-5406 contains information about operating communications and handling communications errors.

- *Communications Configuration*, SC41-5401 contains general configuration information, including descriptions of network interface, line, controller, device, modes and class-of-service descriptions. Information about configuration lists and connection lists is also included.

- *SNA Upline Facility Programming*, SC41-5446 contains the programming information for using the system network architecture (SNA) upline facility with the AS/400 system. This book describes how to set up the upline facility, how to write application programs for the SNA upline facility, and the return codes that the SNA upline facility can send to a program.

- *OSI CS/400 Configuration*, SC41-3425 indicates how to gather information needed to identify the local node in the surrounding OSI environment, and communicate with the desired destination nodes, using relay nodes, if necessary. It provides worksheets for gathering this information, and instructs users on how to enter the information interactively using the Administrative Facility menu, list, and prompt panels, or using CL configuration commands.

- *OSI CS/400 Operations*, SC41-3426 provides information about using OSI alerts.

- *CL Programming*, SC41-5721 provides a discussion of AS/400 programming topics, such as a general discussion of objects and libraries, control language (CL) programming, messages and message handling, user-defined commands and menus, and application testing.

- *CL Reference*, SC41-5722 provides a description of the AS/400 control language (CL) and its commands.

- *Work Management*, SC41-5306 provides information on how to set up an initial work management environment and change work management objects.

- *System API Reference*, SC41-5801 provides a description of the OS/400 application programming interfaces (APIs). Included in this book is information about using the alerts APIs: QALGENA, QALSNDA, and QALRTVA.

NetView

- *Learning About NetView: Network Concepts*, SK2T-0292 (PC Diskette)

- *NetView Administration Reference*, SC30-3361

- *NetView Command Lists*, SC30-3423

- *NetView Command Summary*, SX27-3620

- *NetView Customization*, LY30-5586

- *NetView Diagnosis*, LY30-5587

- *NetView Hardware Problem Determination Reference*, SC30-3366
- *NetView Installation and Administration* book, SC30-3360
- *NetView Messages*, SC30-3365
- *NetView Operation*, SC30-3364
- *NetView Operation Primer*, SC30-3363
- *NetView Operation Scenarios*, SC30-3376
- *Network Program Products Bibliography and Master Index*, GC30-3353
- *Network Program Products General Information*, GC30-3350
- *Network Program Products Planning*, SC30-3351
- *Network Program Products Samples: NetView*, SC30-3352
- *Network Program Products Storage Estimates*, SC30-3403

NetView Distribution Manager

- *NetView Distribution Manager Application Programming*, SH19-6591
- *NetView Distribution Manager Diagnosis*, LY19-6293
- *NetView Distribution Manager General Information*, GH19-6587
- *NetView Distribution Manager Installation*, SH19-6590
- *NetView Distribution Manager Messages and Codes*, SH19-6595
- *NetView Distribution Manager Operation*, SH19-6592
- *NetView Distribution Manager Planning*, SH19-6589
- *NetView Distribution Manager User's* book, SH19-6602

Advanced Communications Function for Virtual Telecommunications Access Method (ACF/VTAM)

- *ACF/VTAM* General Information*, GC38-0254
- *ACF/VTAM System Programmer's*, SC38-0258

Systems Network Architecture (SNA)

- *Systems Network Architecture Technical Overview*, GC30-3072
- *Systems Network Architecture Formats*, GA27-3136
- *Systems Network Architecture Format and Protocol Reference*, SC30-3112
- *Systems Network Architecture–Sessions Between Logical Units*, GC20-1868

Data Link Control

- *IBM Synchronous Data Link Control Concepts*, GA27-3093

Communications Controllers

- *Book to Using the IBM 3704 Communications Controller Control Panel*, GA27-3086
- *Book to Using the IBM 3705 Communications Controller Control Panel*, GA27-3087
- *IBM 3704 and 3705 Control Program Generation and Utilities Guide and Reference*, GC30-3008
- *IBM 3704 and 3705 Program Reference Handbook*, GY30-3012
- *IBM 3725 Communications Controller, Principles of Operation*, GA33-0013
- *IBM 3725 Model 1 Communications Controller, Introduction*, GA33-0010
- *IBM 3725 Model 2 Communications Controller, Introduction*, GA33-0021
- *Introduction to the IBM 3704 and 3705 Communications Controllers*, GA27-3051

Personal Computer

- *Client Access/400 for DOS and OS/2 Technical Reference*, SC41-3563
- *Client Access/400 for DOS with Extended Memory Setup*, SC41-3500
- *Client Access/400 for OS/2 Setup*, SC41-3520
- *Personal Computer/Distributed System Node Executive Installation and Operation*, SH19-6585

System/36

- *Network and Systems Management*, SC21-8010

System/38

- *Data Communications Programmer's Book*, SC21-7825

Index

Communicating Your Comments to IBM

AS/400 Advanced Series
Alerts Support
Version 4

Publication No. SC41-5413-00

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

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.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:
    - United States and Canada: 1-800-937-3430
    - Other countries: 1-507-253-5192
- If you prefer to send comments electronically, use this network ID:
    - IBMMAIL(USIB56RZ)
    - IDCLERK@RCHVMW2.VNET.IBM.COM

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Readers' Comments — We'd Like to Hear from You

AS/400 Advanced Series
Alerts Support
Version 4

Publication No. SC41-5413-00

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

Name

Address

Company or Organization
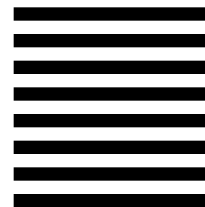
Phone No.

IBM®

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 245
3605 HWY 52 N
ROCHESTER MN 55901-7829

Fold and Tape   **Please do not staple**   Fold and Tape

IBM®

IBM   AS/400 Advanced Series   Alerts Support   *Version 4*