Network Management

for Simulcast

System Manager Manual

The E.F. Johnson Company, which was founded in 1923, designs, manufactures, and markets radio communication products, systems, and service worldwide. The company produces equipment for land mobile radio and mobiletelephone services which include business, industrial, government, public safety, and personal users.

June 1997
Part No: 004-0690-203

Table of Contents

SECTION

1. Introduction

1.1. Scope of manual

This manual covers all functions of HP OpenView and the E.F. Johnson application that together allow management of a networked radio systems. The manual is organized by management function.

- Security management - restrict access
- Configuration management - define the behavior of the network and customize functions
- Fault management - discover, isolate, and fix problems
- Performance management - monitor the network to determine if improvements are needed

Access to a computer running OpenView and the E.F. Johnson application as well as familiarity with Windows® NT and networks are assumed.

1.2. Conventions

Menu item selections are written similar to:

Monitor -> Status Legend

This example means to pull down the Monitor menu and select the Status Legend item.

Ctrl+click means to press the Control key (normally labeled Ctrl) while clicking the mouse on the desired location.

Keyboard shortcuts are written similar to:

Ctrl+Alt+Del
Ctrl+S

Press and hold the keys in the order written and then release all keys. Each keyboard key is separated by a + sign. Example: Ctrl+S means press and hold the Ctrl key, press the S key, then release both keys.

1.3. Definition of terms

Multi-Net Signaling - The format of the data messages that are used to control trunking. Data messages contain over-the-air instructions, or update information, about incoming calls and free channels. Multi-Net signaling also provides many enhanced operating features such as unique ID calls and access priority.

Multi-Net System - A trunked radio system that uses E.F. Johnson Multi-Net signaling. Other types of signaling can also be used. A Multi-Net system can be one site or multi-site. Each site uses a different set of channels and radios can be trunked between sites.

Network Management - A computer system that monitors the radio system for significant events. These events are sent to a host computer where they can be responded to manually, or in some cases automatically.

June 1997
Part No: 004-0690-203

Reverts - Actions that are automatically performed if failures occur. These actions are configured and performed through network management.

Simulcast - A transmission method where several sites that have overlapping coverage areas use the same channels. All sites have a repeater on each channel. All repeaters on the same channel are synchronized so they will transmit the same message at the same time and phase.

Simulcast System - A system whose transmission method is simulcast and whose trunking method is Multi-Net signaling. Simulcast systems are also monitored by network management.

Site - Repeaters and/or other network equipment that is physically located together. Each site includes one computer that is part of the network management system. Sites can be collocated.

Stand-Alone Multi-Net Site - A site that uses Multi-Net signaling, but will not trunk to other sites that use Multi-Net signaling. None of the enhanced operating features provided by Multi-Net signaling are available at these sites.

Trunking - The automatic sharing of channels in a multiple repeater system.

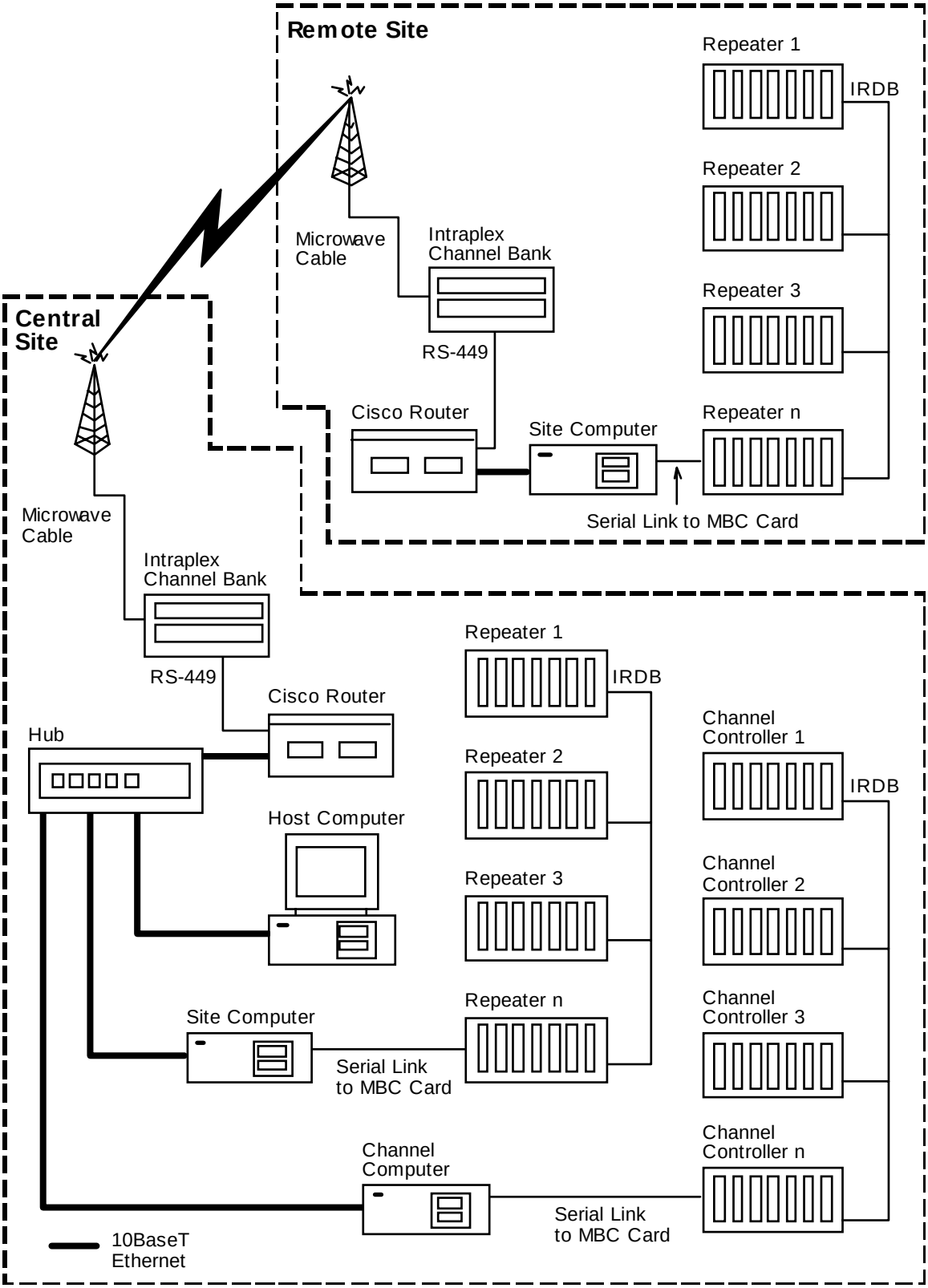
1.4. Overview of managing an E.F. Johnson Network

An E.F. Johnson Network is a system that enables remote repeater sites to report significant events to a host computer, where the events can be managed. The host computer runs the HP OpenView program and an E.F. Johnson proprietary application, which together use alarms to report significant events. The alarms are reported to the screen of the host computer by changing the color of map icons and by displaying an entry in an alarm log. The operator can then decide how to respond to the alarms. In addition, the system can be configured to automatically manage some alarms.

Figure 1-1 shows a typical central and remote site. There may be several other remote sites of similar configuration.

The remote sites communicate to the host computer (often located at the central site) via DS0 links (64 K bps). In this diagram, the DS0 link is part of the microwave link that carries other information between sites. Within a site, network components capable of TCP/IP are connected with 10BaseT Ethernet®. The site/channel computers are also connected by a serial link to MBCs (Message Bridge Cards) in the repeaters and channel controllers. E.F. Johnson proprietary software is used to communicate between the computer and MBC; then, the computers pass the information via TCP/IP to the host computer.

Figure 1-1. Block diagram of typical system



Alarms arrive at the host computer through several means. Computers and routers can be polled by the host computer on a regular basis to determine if the network link is functioning. Routers will send SNMP (Simple Network Management Protocol) trap messages to the host computer when a significant event occurs. The E.F. Johnson proprietary software will send messages to the host computer when significant events occur in repeaters and channel controllers. Repeaters and channel controllers also have IACs (Interface Alarm Cards) that can report external alarms, such as open doors. These alarms are also reported through the E.F. Johnson proprietary software.

Some alarms will correct themselves. For example, if a door opens, an alarm will be received that the door is open. When the door closes, an alarm will be received that the door has closed.

Some alarms can be configured to be managed automatically by the system. These are called Reverts. For example, if a critical alarm reports that one repeater is not working, the system could be configured to automatically shut down all repeaters on that channel. The problem is not corrected, but it is managed. It is not a perfect solution, but it may be the best solution for the circumstances. The critical alarm still exists, in fact more of them exist because more repeaters are not working. However, the system may be more useful without one channel, than with a large hole in the coverage of one channel.

Other alarms will have to be handled manually. If a door opens but does not close and no one is supposed to be at the site, the police may need to be called to go see who is there. If a storm takes out an entire site, some major work will need to be done.

SECTION

2. Security Management (Passwords)

2.1. Host computer passwords

2.1.1. Windows NT passwords

When the host computer is started (after shutdown or a power glitch), Windows NT will request a user name and password.

Administrators can add or delete user names and set passwords by using the Administrative Tools program group and selecting the User Manager program. See the Windows NT documentation for more information.

2.1.2. OpenView passwords

• Log in

Log in passwords are requested when OpenView is started and after someone has logged out. There are three levels of security. The supervisor password gives access to all OpenView functions. The operator password gives access to the functions described in the operator's manual and the observer password gives access to very few functions. Passwords are case sensitive.

To set passwords, select menu item Options -> Set Password. Select a security level from the drop down list box. Enter the password into the Password box. Verify the password by entering it again in the next box.

• Protect maps

The map password makes the maps read-only, which provides protection from accidental changes. When protected, the map can not be edited (for example, changing the layout of the icons or changing the background image). Alarms will still function normally and icon colors will be updated. When logged on with the operator password, maps can be opened but they cannot be edited.

Note: If operators are given the map password, they can change the map password.

To protect maps, select menu item Options -> Protect Map and enter a password. Verify the password by entering it again in the next box. This menu item is a toggle between protecting and unprotecting maps. To unprotect the maps, select menu item Options -> Unprotect Map and enter the required password.

If the password is lost, it can be deleted from the OVWIN.INI file and the maps will be unprotected (until a password is entered). A coded version of the password is stored in the Key entry of the [OpenView] section. OpenView must be restarted for the change to take affect.

• SNMP passwords

Note: These passwords are not needed for normal day-to-day operation of the system.

Passwords to read and write information to SNMP devices are set by selecting Options -> Customize Device Access. See Community and Set Community in Section 3.3 Device Access from OpenView.

2.2. Router SNMP passwords

Note: These passwords are not needed for normal day-to-day operation of the system.

Passwords that allow SNMP access to Cisco 2501 router information are set with the following router command.

snmp-server community *string* [RO | RW] [*number*]

where *string* is the password

RO is read only (corresponds to community password in OpenView)

RW is read-write (corresponds to set community password in OpenView)

number is a value from 1 to 99 used to specify an access list of IP addresses that can use the v.1 agent. (optional)

To delete a string, use the command:

no snmp-server community *string*

To set the corresponding passwords in OpenView, select menu item Options -> Customize Device Access. See Section 3.3 Device Access from OpenView.

SECTION

3. Configuration Management

Network components are devices (such as computers and routers) that are assigned IP addresses and talk to OpenView using TCP/IP and SNMP protocols. E.F. Johnson components (such as repeaters and channel controllers) talk to OpenView through specialized programming.

Equipment manuals may include additional configuration information that is part of installation and maintenance.

3.1. IP addresses

Network devices send messages to each other by addressing their messages to IP addresses. Each port of each device in a system must be assigned a unique address. An IP address is divided into three sub-addresses called network, subnet, and host.

A network is a system, or a collection of network devices, that need to communicate with each other. For example, all of the radio repeaters of a police department could be a network, while the radio repeaters of the cab company would be a separate network.

A subnet is a portion of the network, or a group of network devices, that share a common interest. For example, all the devices at one repeater site may need to talk to each other about that site, but other devices in the system do not need to hear the conversation. For another example, each backbone link relays only the messages for the sites on its link, and does not relay messages for sites that are on other backbone links.

A host is a unique network entity, in other words, anything that needs to be uniquely (or specifically) addressed within the network, for example, a computer or the port of a router.

Although there are three sub-addresses, an IP address is written as four numbers that are separated by periods. For example, 192.185.32.25 or 100.100.201.100. The range of each number is 0 to 255, with 0 and 255 reserved for special situations. A subnet mask defines which part of the IP address belongs to the network and subnet (also called a data link), and which part belongs to the host (also called a node).

E.F. Johnson has developed a method for assigning IP addresses that provides consistency in initial installation and future expansion. When using this method, the subnet mask is 255.255.255.0. This mask tells the equipment that the first three numbers define the network and subnet and the last number defines the host. An E.F. Johnson radio network system is a stand-alone network and therefore does not require coordination with the Internet world or existing networks (such as an in-house Novell® network).

Using the E.F. Johnson addressing method, the first two numbers will be unique to each system. The third number will be unique to each subnet within a system. The fourth number will be unique to each host within a subnet.

To provide for consistent future expansion, this addressing method further defines the third number. Inter-site backbone links will be assigned numbers between 100 and 199. Links that connect site devices will be assigned numbers between 200 and 255. Therefore, by looking at the third number, one can tell if the subnet is an inter-site backbone link or a link that connects site devices. Inter-site backbone links are often microwave or some other long-distance carrier; links that connect site devices are typically connected by Ethernet cabling.

The fourth number is also further defined. Within a backbone link (subnets between 100 and 199), the hosts will be assigned numbers sequentially starting with number 1. Within a site link (subnets between 200 and 255), there are three groups of devices. Routers will be assigned numbers sequentially starting with number 1. Site/Channel computers will be assigned numbers sequentially starting with number 100; and host computers will be assigned numbers sequentially starting with 200.

Figure 3-1 shows the IP addresses that would be assigned to a three-site system, as well as showing how expansion to a five-site system could begin. In this figure, 100.100 has been assigned for the system address.

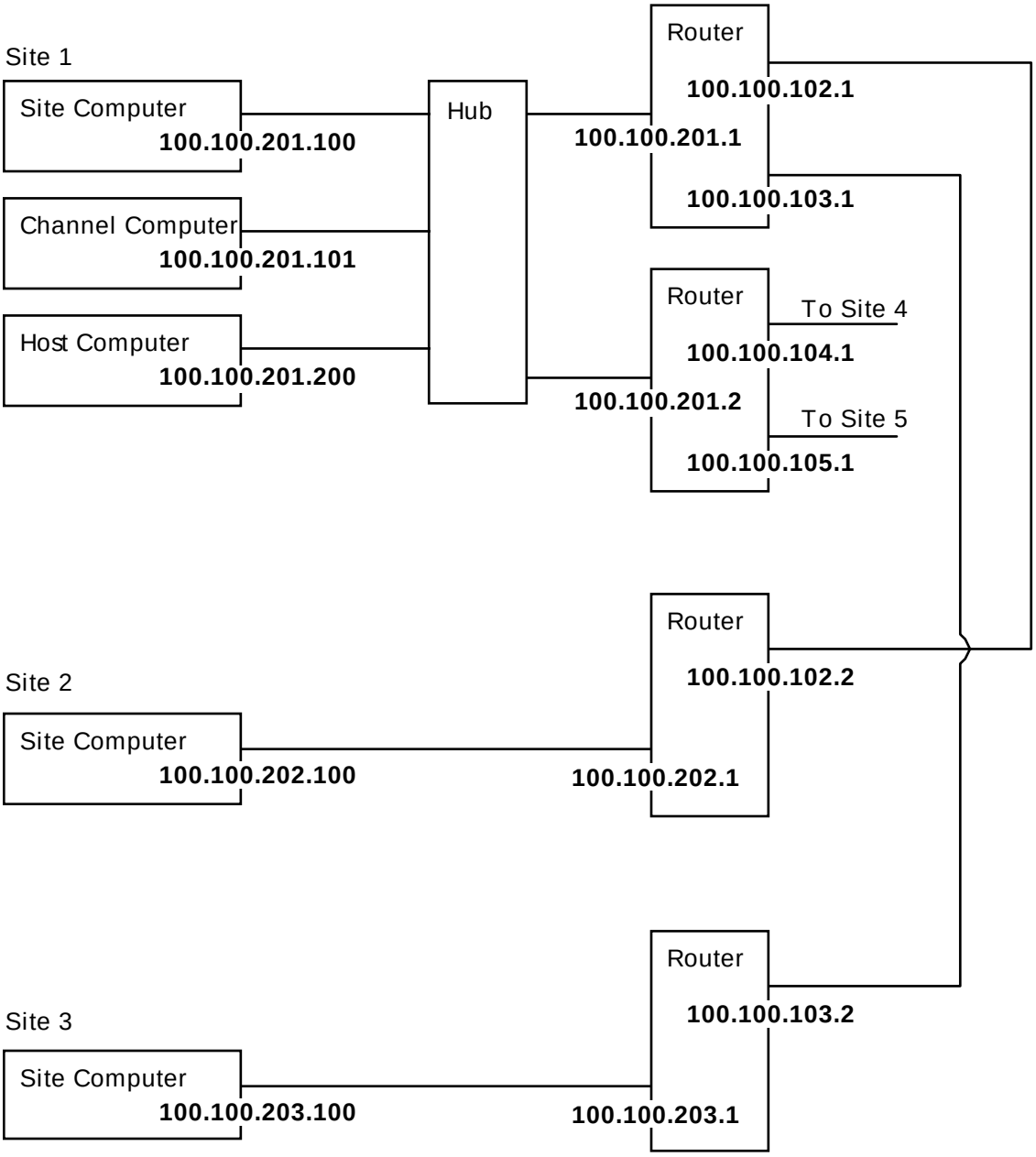
The subnet numbers (third number of the IP address) are assigned as follows:

- 201 is the link within site 1
- 202 is the link within site 2
- 203 is the link within site 3
- 102 is the backbone link between site 1 and site 2
- 103 is the backbone link between site 1 and site 3
- 104 is the backbone link between site 1 and site 4
- 105 is the backbone link between site 1 and site 5

Within site 1 (subnet 201) the host numbers (fourth number of the IP address) are assigned as follows:

- 1 is an Ethernet port on the first router
- 2 is an Ethernet port on the second router
- 100 is a network port on the site computer
- 101 is a network port on the channel computer
- 200 is a network port on the host computer

Figure 3-1 IP addresses



The hub is acting as a splitter. It does not need IP addresses because it does not send messages to and from specific hosts. Instead, the hub listens to all attached hosts. If a message comes in one port, the hub sends the message out all other ports.

Within site 2 (subnet 202) the host numbers (fourth number of the IP address) are assigned as follows:

- 1 is an Ethernet port on the router
- 100 is a network port on the site computer

Within site 3, the host numbers are the same as in site 2. However, since the subnet is 203, the IP address is unique. The same would be true for the expansion to a fourth site (subnet 204) and a fifth site (subnet 205).

Within the backbone link from site 1 to site 2 (subnet 102) the host number is 1 for the router at site 1, and 2 for the router at site 2. The link from site 1 to site 3 (subnet 103) is the same; 1 is for the router at site 1 and 2 is for the router at site 3. Again the different subnet makes the IP address unique. Expansion to site 4 and 5 would be the same.

3.2. OpenView maps

OpenView maps are created to show a visual representation of the network to the person using the map and to inform the program of the devices that are part of the network, as well as the information needed to communicate with the devices.

Note: Correct maps are essential for proper alarm notification. The E.F. Johnson company has provided maps with the system. Maps should be kept backed up and there should be a good understanding of the network system before making modifications.

Maps consist of:

- icons (symbols) representing network devices
- icons representing submaps
- lines showing communication links (optional)
- a background image showing geographic location (optional)

A map file is a collection of related submaps. The home submap (typically the System map) is the first map displayed when OpenView starts (or when the map file is opened). The System map contains icons for systems. Double-clicking on a System icon will display a submap that shows Site icons for each site within the system. Double-clicking on a Site icon will display a submap with icons for all monitored devices (routers, computers, repeaters, etc.) at that site.

The following information is needed to create maps.

- a list of devices at each site (routers, computers, repeaters, and channel controllers)
- a unique name (up to 64 characters) for each icon (systems, sites, routers, computers, repeaters, and channel controllers). OpenView calls this name an “Object Name”.
- a background image file (optional) and the geographic layout of the sites (to know where to place icons on the background image). See Section 3.2.7 for file formats.
- IP addresses for network components (routers and computers)
- information about E.F. Johnson components (repeaters, channel controllers, sites, and systems). In addition to a unique name, the descriptive information in the following sections will be needed: Section 3.2.1

Creating the System map, Section 3.2.2 Creating a Site map, and Section 3.2.3 Creating a Device map.

The OpenView program is used to create maps.

3.2.1. Creating a System map

Follow these steps to create a System map.

1. If an empty untitled window is not displayed, select menu item File -> New. An empty untitled window will appear.
2. Save the map by selecting menu item File -> Save As and enter a filename (append a directory name if necessary). OpenView will assign a .OVM extension to the filename. This filename will be part of the window title of each submap.
3. Name this submap by selecting menu item Edit -> Rename Submap. This name will be part of the window title for this submap. The maximum length of the name is 20 characters.
4. Make this submap the home submap by selecting menu item Edit -> Set Home Submap.
5. Add a background image (optional) for the map by selecting menu item Edit -> Set Background and then selecting the desired filename. (Background images are stored in the \OV\BKGROUND\ directory.)
6. Add a System icon by selecting menu item Edit -> Add. The Add toolbox will appear. Select Compound Object from the next to bottom drop down list box. Select EFJ System from the bottom drop down list box. Alternatively, to display icons, click the button to the left of the list; then, select the EFJ System icon.

EFJ System icon

Move the cursor to the desired map location for the icon and click the mouse button. The icon will be added to the map and the EFJ System Description dialog box will appear. (Unless displaying the dialog box has been disabled with menu item Options -> Customize HP OpenView, Describe Objects as Added, which is described in Section 3.2.8.)

7. In the EFJ System Description dialog box, enter the following information.

   - System Name: Enter a unique name for this system. The name will also appear under the icon on the map and in some dialog boxes.

   - System Number: Each system is assigned a unique number from 1 to 30. This number is arbitrary, but each system must be different.

   - Status Channel Repeater Number: Select the Repeater Number of the repeaters that are used on the Status Channel.

- Channel Revert MIN: Select the number of simulcast channels that will not automatically shut down if simulcast failure, repeater failure, or RNT/CIM Channel Problem alarms occur. This is the minimum number of channels that will stay operational, even if there are additional problems. To prevent any channels from automatically reverting, select the number of channels that exist in the system.

  Example: If the system has 10 channels and 8 channels are required to remain operational, select 8. If problems occur, up to 2 channels that have problems will be automatically shut down. The remaining 8 channels will stay operational, even if additional problems occur. Additional changes could be made manually. If automatic site reverts are configured, they may further automatically change the system.

  See Section 4.2 Recovery, for more information about channel reverts and other types of reverts.

  - Allow Status Channel Revert: If there are problems on the Status Channel, should the system automatically revert the Status Channel? An x in this box indicates that the system can automatically revert the Status Channel. If the Status Channel should not automatically revert, leave this box unchecked.

8. Repeat steps 6 and 7 to add additional System icons, if needed.
9. If the system's host computer is at a separate site (not collocated with the channel controller or repeaters), add the host computer's router to the System map. See Section 3.2.3 for adding a router instructions.
10. Save the map by selecting menu item File -> Save or by pressing Ctrl+S.

3.2.2. Creating a Site map

Follow these steps to create a Site map.

1. Double-click on a System icon (that was placed in the previous section) and a blank map will appear. The title bar will be named with the filename of the map and the name of the System icon that was double-clicked.
2. Add a background image (optional) for the map by selecting menu item Edit -> Set Background and then selecting the desired filename. (Background images are stored in the \OV\BKGROUND\ directory.)
3. Add a Site icon by selecting menu item Edit -> Add. The Add toolbox will appear. Select Compound Object from the next to bottom drop down list box. Select EFJ Site from the bottom drop down list box. Alternatively, to display icons, click the button to the left of the list; then, select the EFJ Site icon.

   EFJ Site icon

   Move the cursor to the desired map location for the icon and click the mouse button. The icon will be added to the map and the EFJ Site Description dialog box will appear.

4. In the EFJ Site dialog box, enter the following information.

   - Site Name: Enter a unique name for this site. The name will also appear under the icon on the map and in some dialog boxes.

   - System Number: Select the number that was assigned to the system that is associated with this site.

   - Site Number: Each site in a system is assigned a unique number from 0 to 31. Number 0 is reserved for the primary channel controller and number 31 is reserved for the secondary or backup channel controller. Otherwise, this number is arbitrary; however, each site in a system must be assigned a different number.

   - Site Type: Select “Primary Controller” for the site that has the primary channel controller. Select “Secondary Controller” for the site that has the secondary or backup channel controller. Select “Remote” for sites that have repeaters. A channel controller is a separate site, even if it is physically located with repeaters.

   - IP Address: Enter the IP address of the site or channel computer.

5. Repeat steps 3 and 4 to add additional Site icons. Remember that the Channel Controller is a site.

6. Save the map by selecting menu item File -> Save or by pressing Ctrl+S.

3.2.3. Creating a Device map

Follow these steps to create a Device map.

1. Double-click on a Site icon (that was placed in the previous section) and a blank map will appear. The title bar will be named with the filename of the map and the name of the Site icon that was double-clicked.

2. Add the devices that are at the site. Instructions for installing the most common devices are below.

3. Save the map by selecting menu item File -> Save or by pressing Ctrl+S.

4. Repeat as necessary to add devices to other sites.

• Router

1. Add a Router icon by selecting menu item Edit -> Add. The Add toolbox will appear.

2. Select Component from the next to bottom drop down list box.

3. Select Cisco 2501 or Router from the bottom drop down list box. Alternatively, to display icons, click the button to the left of the list; then, select the router icon.

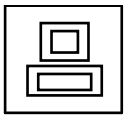
Cisco 2500-series router icon

Router icon (generic)

4. Move the cursor to the desired map location for the icon and click the mouse button. The icon will be added to the map and the Describe dialog box will appear.
5. In the Describe dialog box, enter a unique name for this router and enter a label that will appear as a name under the icon on the map. Also, click the Net Address button to enter the IP addresses of the router. The first IP address entry should be the IP address that talks to the host computer, because the first listed address will be used for pinging. MAC (Media Access Control) addresses are not required.

• Site or channel computer

1. Add an icon for the site or channel computer by selecting menu item Edit -> Add. The Add toolbox will appear.
2. Select Computer from the next to bottom drop down list box.
3. Select Personal Computer from the bottom drop down list box. Alternatively, to display icons, click the button to the left of the list; then, select the Personal Computer icon.



Site or Channel (Personal) computer icon

4. Move the cursor to the desired map location for the icon and click the mouse button. The Describe dialog box will appear.
5. In the Describe dialog box, enter a unique name for this computer and enter a label that will appear as a name under the icon on the map. Also, click the Net Address button to enter the IP address of the device. MAC (Media Access Control) addresses are not required.

• Repeater or channel controller

1. Add a Repeater icon by selecting menu item Edit -> Add. The Add toolbox will appear.
2. Select Component from the next to bottom drop down list box.
3. Select EFJ Repeater from the bottom drop down list box. Alternatively, to display icons, click the button to the left of the list; then, select the EFJ Repeater icon.

EFJ Repeater icon

4. Move the cursor to the desired map location for the icon and click the mouse button. The icon will be added to the map and the EFJ Repeater Description dialog box will appear.

5. In the EFJ Repeater dialog box, enter the following information.

   - Repeater Name: Enter a unique name for this repeater. The name will also appear under the icon on the map and in some dialog boxes.

   - System Number: Select the number that was assigned to the system that is associated with this site.

   - Site Number: Select the number that was assigned to the site that is associated with this repeater.

   - Repeater Number: Each repeater was programmed with a repeater number during installation/configuration. Each repeater at a site must be programmed with a different number from 1 to 30. The number entered in OpenView must be the same as the number programmed into the repeater. All repeaters on the same channel need to have the same repeater number.

   - Repeater Type: Select the mode for this repeater.

     Disabled: The repeater is not functioning.

     Multi-Net: (Not used in a simulcast system.) Multi-Net signaling is a trunked method that provides enhanced features. It can be multi-site, where each site has different channels and mobile stations are automatically switched to a different channel when they drive into the coverage of a different site.

     Simulcast Controller: The “repeater” is a channel controller, which makes several simulcast remote repeaters look like one repeater to the RNT (Radio Network Terminal, which controls the operating features of the radio system). Simulcast is a transmit method where each site in a system has the same channels and the channel audio is rebroadcast at each site.

     Simulcast Remote: A repeater that is part of a simulcast system.

   - Rptr Power Type: Low power repeaters have adjustable output from 25 to 75 watts. High power repeaters have adjustable output from 75 to 160 or 175 watts.

   - Channel: Select the channel number that represents the transmit and receive frequencies for the repeater. Each repeater was programmed with a channel number during installation/configuration. Refer to Appendix A for 800 MHz channel numbers and Appendix B for 900 MHz channel numbers.

   - Status Channel: An x in the box designates that this repeater is on the Status Channel. The Status Channel transmits update information for all calls. There is only one Status Channel in a simulcast system.

   - Power Level: Select the level of output power that the repeater uses for normal operation.

   - IAC Alarms Descriptions: Enter text to define custom Alarm Log descriptions for IAC alarms. IAC (Interface Alarm Card) alarms are external inputs on the IAC in repeaters and channel controllers. These alarms will be custom to each installation.

- Severity: Use the Severity drop down list boxes to select an alarm level for each IAC alarm.

3.2.4. Adding lines and text

Lines may be added to a map to show backbone links.

Lines and text are added from the Add toolbox (select menu item Edit -> Add). There are two types of lines. The button with a straight line will add a line that will stay where it was drawn even though icons are moved. The button with a line that has vertical end-pieces will draw a line that will move with the icon. Line weights can be selected from the drop down list box.

Text can be added with the text (T) button. The size of characters can be selected from the drop down list and bold or underline can be selected with the “B” and “U” buttons. OpenView uses the Windows system default font.

Clicking on the line and text buttons with Ctrl+click will allow multiple operations to be performed without reselecting the button.

3.2.5. Setting the default map

Define a default startup map by selecting Options -> Customize HP OpenView and entering the name of the map in the Default Map box. If a default map is not defined, OpenView will start with a blank untitled map.

3.2.6. Protecting the map

Maps should be protected to avoid accidental changes. To protect the map, select menu item Options -> Protect Map and enter the required password. Verify the password by entering it again in the next box. When maps are unprotected, they can be edited and an operator can open new maps by selecting menu item File -> Open. To unprotect maps, select menu item Options -> Unprotect Map and enter a password. This menu item is a toggle between unprotecting and protecting maps.

3.2.7. Format for background maps

Background maps are optional graphic files that normally show the outline of the county and major roads. Maps can be made in a graphics program, such as PC Paintbrush, and should be stored in the directory C:\OV\BKGROUND\.

Computer monitor size and the number of submaps normally displayed should be considered when deciding the size to create a background map. Maps can be reduced within OpenView, however, the icon names will not show on reduced maps. A typical size is approximately 375 pixels wide and 325 pixels high.

Background maps can be created in any program that will save a BMP (Windows 3.0 or later bitmap) graphics file or a TIFF graphics file (standard TIFF file format with .TIF file extension. TIFF version 5.0 or later are not supported). Typical resolutions are 72 or 96 pixels per inch (ppi).

3.2.8. Options for map creation

• **Check maps**: Selecting menu item File -> Check Map runs a test to see that all compound object icons (system and site) have corresponding maps. If there are no problems, this menu item is dimmed.

• **Print list of Object Names**: Selecting menu item File -> Print Object List will print a list of all Object Names assigned in the current map. Object names are names that were assigned to devices in the Describe dialog boxes. The list will be printed to the workstation printer.

• **Number of symbols**: The maximum number of symbols (icons, submaps, text blocks, and lines) can be set by selecting menu item Options -> Customize HP OpenView. The range is 8 to 32,760, with a default of 5000. OpenView rounds the entry to the next multiple of 8 and the change takes effect the next time OpenView is started.

• **Describe Objects as Added**: The Describe dialog box can be displayed after each icon is added to a map, or OpenView can be set to not display the dialog box each time. In which case, each icon will need to be described by right-clicking on the icon and selecting Describe, or by selecting the icon and selecting menu item Edit -> Describe. Describe Objects as Added can be changed by selecting menu item Options -> Customize HP OpenView.

• **Create Submaps Automatically**: OpenView can be set to automatically create submaps for Site and System icons when the icons are added to the maps, or submaps can be created manually by selecting menu item Edit -> New Submap. If created manually, give a map the same name as the icon that represents it. Create Submaps Automatically can be changed by selecting menu item Options -> Customize HP OpenView.

• Autodiscovery is another method of creating maps, but is not recommended for an E.F. Johnson radio network.

• **Maximum Number of Messages**: This option sets the size of OpenView's message queue. The range is 8 to 120, with a default of 8. A larger setting may be desired if there are normally many map status changes. The size can be changed by selecting menu item Options -> Customize HP OpenView. OpenView must then be restarted for the change to take effect.

3.3. Device Access from OpenView

Device Access information is used by OpenView applications, such as the SNMP Manager and Autodiscovery. System defaults and custom information for specific devices can be modified by selecting menu item Options -> Customize Device Access.

To modify information for a specific device, select the IP address of the device from the Network Addresses list and click the Modify button. To modify system defaults, select <System Default> from the Network Addresses list and then click the Modify button.

To change information for a device that is not listed, click the Add button and enter the IP address of the device. Alternatively, select a map icon, select menu item Options -> Customize Device Access, and click the Add button. The IP address of the selected map icon will be filled in.

To delete a device (or return it to system defaults), selected the device in the list and click the Delete button.

Only devices that do not use system defaults will be listed in the Network Addresses list.

Community: Enter the SNMP password that needs to be sent to read the MIB variables in a device. This password is case sensitive and must be the same as the password in the device.

Set Community: Enter the SNMP password that needs to be sent to write changes to the MIB variables in a device. This password is case sensitive and must be the same as the password in the device.

Retries: The number of times a request will be retried. This value must be greater than 0.

Timeout: Enter the time, in milliseconds, to wait for a response from a device.

Proxy Agent: A proxy agent is an SNMP device that communicates on behalf of a non-SNMP device. A proxy agent acts similarly to a translator. It communicates with OpenView using SNMP and communicates with a non-SNMP device using a different protocol.

SECTION

4. Fault Management - Setup

4.1. Alarm notification setup

OpenView receives solicited and unsolicited alarms. Solicited alarms happen when OpenView initiates a poll to a device and OpenView does not receive a response. If a response is received, no alarm occurs; however, if a critical status exists, it is changed to normal status. Unsolicited alarms happen when a device initiates a message to OpenView because the device has determined that a significant event occurred. If the device is an SNMP-capable device, the alarm is called a “trap”.

4.1.1. Polls

Some alarms are the result of polling. OpenView will periodically check all listed devices to see that the network connections are working properly. When a change in status occurs, an alarm is processed.

Polling is controlled through menu item Monitor -> Polling. Controls include stop/start polling, define a list of devices to poll, configure the time interval for polling, and configure the alarm level for notification.

View Polling List: Selecting menu item Monitor -> Polling -> View Polling List will display the View Polling List dialog box, which shows the list of devices that OpenView will poll. The list shows the name and address of the polled devices as well as the time interval between polls. At the bottom of the dialog box, the total number of entries is displayed and also whether polling is turned on or off. To remove a device from the list, select the device, and click the Remove button. The Configure button displays the Configure Device Parameters dialog box that allows default values to be overridden for the selected device (described later in this section).

Add Device(s) to polling list: First, select the map icons that represent the devices to be added. Shift+click or Ctrl+click to select multiple icons. Second, select menu item Monitor -> Polling -> Add Device(s). The IP addresses of the selected devices will be added to the list. If a device has more than one address, a dialog box will ask for the address(es) to be polled. If a device does not have an IP address, an error message will be displayed.

OpenView allows only one polling list. If different sets of devices are frequently polled, a “selection list” can be saved to avoid manually selecting the icons each time. To save or edit a selection list, select the desired icons, select menu item File -> Save Selection List As and enter a filename. To use a saved list, select menu item File -> Load Selection List and enter the filename of the saved list.

Remove Device(s) from polling list: First, select the map icons that represent the devices to be removed. Shift+click or Ctrl+click to select multiple icons. Second, select menu item Monitor -> Polling -> Remove Device(s). The selected device(s) will be removed from the list and a message will inform that polling was turned off for a number of devices. Alternatively, device(s) can be removed by selecting menu item Monitor -> Polling -> View Polling List, selecting the device(s) in the list, and clicking the Remove button.

Configure System Defaults: The polling interval and the alarm level for notification that apply to polled devices are controlled by polling defaults. Alarm notification happens when there is a change in alarm level (status), not each time the device is polled. (Note: Manually acknowledging an alarm is considered a change in status to normal level.) The defaults can be changed by selecting menu item Monitor -> Polling -> Configure System Defaults. (To override defaults for a specific device, see Configure Device Parameters below.)

In the Configure System Defaults dialog box, “Interval” defines how frequently a poll will be sent. Alarm Actions are set separately for notification of device down or device up. Device down means that the device polled did not send a response, which indicates a problem. Device up means the device did send a response, which indicates the network connection is working. Select the Severity or alarm level from the drop down list box. Also, select whether the color of the map icons will be updated, whether a sound will be played, and if the alarm should be reported in the log.

Configure Device Parameters: To override the default parameters for a specific device, select the map icon for the device and then select menu item Monitor -> Polling -> Configure Device Parameters. Alternatively, select menu item Monitor -> Polling -> Configure Device Parameters and then enter the IP address of the device. A device name is not required. A device must have an IP address to be polled. Some devices do not have addresses and therefore cannot be polled. <Default> will appear to the right of any section that is using system defaults.

In the Configure Device Parameters dialog box, “Interval” defines how frequently a poll will be sent. Alarm Actions are set separately for notification of device down or device up. Device down means that the device polled did not send a response, which indicates a problem. Device up means the device did send a response, which indicates the network connection is working. Select the Severity or alarm level from the drop down list box. Also, select whether the color of the map icons will be updated, whether a sound will be played, and if the alarm should be reported in the log.

Stop/Start Polling: This menu selection toggles to turn polling off and on. When polling is on, the HP OpenView for Windows Professional Suite version of OpenView animates a polling icon in the toolbar.

4.1.2. Traps

Traps are unsolicited messages from devices such as routers. These messages follow the SNMP protocol, which defines six standard messages. SNMP also allows manufacturers to define their own messages. OpenView recognizes the six

standard messages and can be customized to recognize other messages. Trap messages notify OpenView of a change of status for the device.

Traps are controlled through menu item Monitor -> Customize Traps. Selecting this menu item displays the Customize Trap Alarms dialog box. Controls include customize alarm notification for different trap messages, add devices and traps, and remove devices and traps.

The top-left part of the dialog box shows a list of device types. The “Device Class Name” column shows the device types, which are defined by class or type name. The “Flag” column contains the word “Ignore” if OpenView has been told to ignore traps from the device type. The “Enterprise” column shows the enterprise number for the device type. Devices have enterprise numbers so that different devices can send different non-standard messages.

The top-right part of the dialog box shows a list of traps for the device type (device class name) that is selected.

Traps from device types that are not listed will be processed as defined for the “Unconfigured/Default” device type. This device type has traps defined for the six standard SNMP messages as well as a default definition for any other message. The defaults can be customized by selecting the trap in the trap list and changing the Alarm Actions and Acknowledge Alarm on Matching Trap information in the bottom part of the dialog box.

The processing of traps from specific device types can be customized by selecting the device type in the device list, selecting the trap in the trap list, then changing the Alarm Actions and Acknowledge Alarm on Matching Trap information.

Alarm Actions: Select whether the color of the map icons will be updated, whether a sound will be played, and if the alarm should be reported in the log. Also, select the Severity or alarm level from the drop down list box. Enter the description for the Alarm Log in the Description box; and, if desired, enter an Extended Description that will be displayed when the More Info button in the Alarm Log is clicked. Variables can be used in the descriptions to extract specific information from the trap message.

Variables	Descriptions
\n	newline
\t	tab
$C	trap community string
$E	enterprise, represented as a text string if possible
$e	enterprise, represented as an object ID string of numbers
$A	name of device that sent the trap. If this device is not represented by a symbol in the map, this field defaults to “addressed:” concatenated with the device address.
$G	generic trap id number
$S	specific trap id number

$T	timestamp (time since device was last restarted)
$*	print all variables in the trap
$#	number of variables in the trap
$$	print the $ character
$n	print the value of the nth variable in the trap, where n is the variable sequence number starting at 1 used to reference subobjects in a device.
$-n	print the nth variable as a "name-type:value" string, where n is the variable sequence number starting at 1 used to reference subobjects in a device.
$+n	print the nth variable as a "name:value" string, where n is the variable sequence number starting at 1 used to reference subobjects in a device.

(Chart from "HP OpenView for Windows Workgroup Node Manager User's Guide")

Acknowledge Alarm on Matching Trap: For OpenView to clear a high-level alarm when it receives a low-level alarm, OpenView must be told which two alarms correspond to each other. To define which low-level alarm clears a high-level alarm, select the device type in the device list, select the trap that creates a high-level alarm in the trap list, then select the trap that creates the corresponding low-level alarm in the Acknowledge by Trap list. If the trap contains a variable that further defines the alarm, select the variable in the Must match on Variable box.

Add Device Class button: To add a device type to the device list, click on the Add Device Class button. The Add Device Class dialog box will appear. Select the desired device. The device type will be added to the device list. If the desired device type is not listed in the Add Device Class dialog box, it must be added to the OVFILES\DEVICES file.

Remove Device Class button: To remove a device type from the device list, select the device type, and click the Remove Device Class button. All customized traps for this device type will also be removed.

Ignore/Include Device Class button: To ignore traps from a device type in the device list, select the device type, and click the Ignore Device Class button. The word Ignore will be added in the Flag column. When a device type that has been ignored is selected, this button will toggle to say Include Device Class. The button can then be clicked to include the device type.

Add Trap button: To add a trap for a device type, select the device type from the device list and click the Add Trap button. The Add Trap dialog box will appear. Select a trap from the Generic drop down list. If Specific was chosen, also enter a trap number in the Specific box. The trap will be added to the trap list.

Delete Trap button: To delete a trap, select the device type from the device list, select the trap from the trap list, and click the Delete Trap button.

Load Traps button: If a trap definition file (.TDF) has been provided, pre-defined traps can be loaded by clicking on the Load Traps button and selecting the file.

Note: During installation, devices are configured to send their trap messages to a specific IP address, which in this case is the address of the host computer.

4.1.3. E.F. Johnson alarms

Alarms from E.F. Johnson components (such as repeaters) are unsolicited alarms that are initiated by the E.F. Johnson components when a change in status occurs.

OpenView will report these alarms at the frequency defined by selecting Options -> Customize Alarms.

Frequency: The default is 0 seconds. OpenView reports all alarms from E.F. Johnson components (such as repeaters) to the Alarm Log and updates the color of the icons. If set to a higher value, identical alarms that are received within the time frame will not be reported. After the time frame has expired, notification of the alarm resumes.

4.1.4. Alarm Log options

• The order that alarms are displayed can be changed by selecting menu item Options -> Customize Alarms. In the Alarms section, select sorted by Time or by Status.

The default is “Time”. The entries in the Alarm Log will be displayed in reverse chronological order (newest at the top of the list). Selecting “Status” will display the entries according to severity (most severe or highest status level at the top of the list) and according to time within each alarm level.

• Unacknowledged alarms will be moved from the Current log to the History log when OpenView is shut down and restarted. This can be changed by setting ReloadAutoAck to No in the OVAlarm section of OVWIN.INI.

4.1.5. Alarm Sound

From menu item Options -> Customize Alarms, select Disable Sounds, Sound Once, or Repeat.

Disable Sounds: No sounds will be heard when alarms occur.

Sound Once: The alarm sound will sound once when an alarm is displayed in the alarm log.

Repeat: The alarm sound will be repeated until the alarm clears. A time interval (Every __ minutes) between 0 and 999 can be set to define how often the sound is repeated. The “For status” entry sets which level of alarms will receive the repeated sound. For example if set to “Major”, only major and critical alarms will have repeated sounds; all other alarms will sound only once. (See Section 5.5 Color status legend.)

By default the alarm sound will be the system beep. For a system that is capable of playing sound files, sound files can be associated with each alarm through the Sound dialog in the Windows Control Panel.

4.1.6. Status Propagation

Maps are linked hierarchically. The top level is a System map, the middle level contains Site maps, and the bottom level contains Devices maps. The status propagation option defines if alarms are shown on maps that are at a higher hierarchical level than where the alarm occurred. Status propagation can be changed from menu item Options -> Customize Alarms.

The default is “Pass status up all levels”.

Pass status up all levels: With this setting, an alarm will be passed to all higher hierarchical maps to display a colored icon for alarm notification. For example, if a device reports an alarm, the following icons will change color 1) the Device icon, 2) the Site icon where the device is located, and 3) the System icon. (If there is already a higher level alarm at the site and system level, the icon will remain the color of the highest alarm.)

Pass status up one level: Alarms will only be passed up one level in the hierarchy. With this setting, a System level map will not show that a Device level map has an alarm.

Do not pass status up: The alarm will only show on the map where the alarm occurred.

4.1.7. Alarm Forwarding

Alarms can be forwarded to another console. To configure alarm forwarding, select menu item Options -> Customize Alarms. A dialog box appears for setting the following items.

Enable Forwarding to Address: An x in the box to the left (by clicking in the box) turns on alarm forwarding. Also enter the IP address of the console that is to receive the alarms.

Objects: Alarms can be forwarded based on which object (device) has reported the alarm. To forward all alarms, select “For any object”. To forward alarms only from specific objects, click the Select button. A dialog box will appear, where the desired objects can be selected.

Status: Alarms can be forwarded based on the alarm level of the alarm. From the drop down list box, select the lowest level of alarms to be forwarded. All alarms above, and including, the selected level will be forwarded.

4.2. Recovery (Reverts) setup and actions

CAUTION: Reverts require extreme caution and knowledge about the radio system. Otherwise, reverts could cause more problems than the initial failure. Setting up automatic reverts should be done with the assistance of the E.F. Johnson project manager.

Reverts are actions that are performed if failures occur. Automatic actions can be configured and performed through OpenView. If there is a failure, the remaining working pieces need to be reconfigured to provide the best possible coverage for the system's communications needs. By setting up channel reverts and site reverts, OpenView can provide automatic reconfiguration.

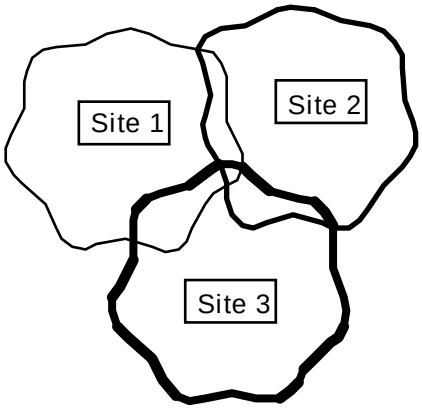
Channel reverts will shut down all repeaters on a channel. Site reverts will shut down individual sites or reconfigure individual sites to stand-alone sites. If a repeater failure can cause both reverts, both reverts will occur.

Some situations will be beyond the scope of automatic reverts. Therefore, it is possible to manually revert channels and sites. Channels and sites are always manually unreverted (returned to normal). Repeaters can also be individually controlled (see Section 4.3).

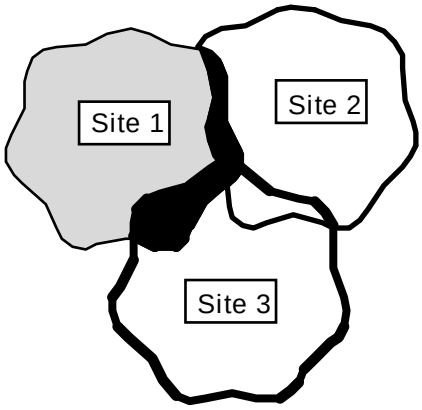
4.2.1. Consider interference problems

In a simulcast system, the repeaters in adjacent sites are on the same channel and purposely overlap to fill in weak coverage areas. If one site is reverted to a stand-alone Multi-Net site, the overlapping areas will have interference problems. See Figure 4-1.

Figure 4-1. Reverted sites can cause interference



In a simulcast system, all radios receive the same signal.



If Site 1 is reverted to a stand-alone Multi-Net site, radios in the black area will receive a signal from Site 1 and a different signal from Sites 2 and 3.

Interference problems could be minimized in several ways. Reducing the output power level of the repeaters in Site 1 (Figure 4-1) might decrease the area affected by interference; however, it may also create a hole in the coverage area of the system. Reduced power level may also put more stations in fringe areas.

If only one repeater is not working at Site 1 (Figure 4-1), the channel with the non-working repeater could be shut down. That is, the repeaters in sites 2 and 3 for that channel could be disabled. Except for having one less channel, the system would continue to function as a normal simulcast system.

If a system has enough channels, each site could use different channels and be reverted to a stand-alone Multi-Net site. The benefits of simulcast coverage would be lost, but the holes and fringe areas would be reduced.

There will be trade-off decisions that must be made when equipment fails. Knowing the coverage area of the working repeaters and considering the effects on the whole system will lead towards a configuration that minimizes the loss as much as possible.

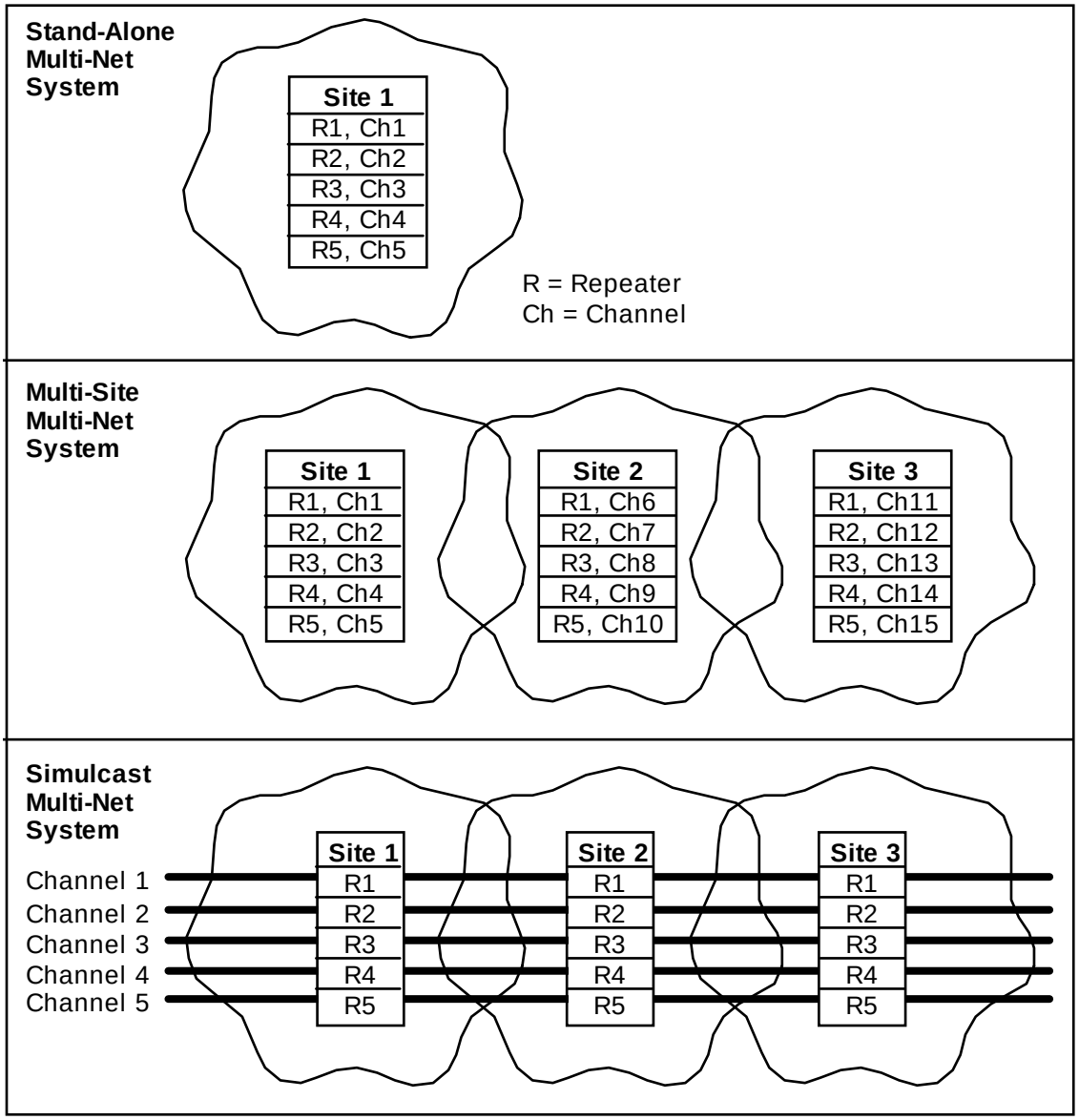
4.2.2. Consider status channel and home channel access

In simulcast systems, communications between radios and repeaters use Multi-Net signaling, as described in the Multi-Net Application Note (Part No. 009-3039-003).

Figure 4-2 shows the relationship between repeaters, channels, and sites in Simulcast and Multi-Net systems. Multi-Net descriptions often refer to a single repeater. In a simulcast system, the description would refer to all repeaters on the same channel.

CAUTION: Radios monitor their home channel and the status channel for over-the-air instructions. If there are problems on either channel, radios may not receive their instructions. Therefore, pay special attention to the status channel and home channels when configuring reverts.

Figure 4-2. Relationship of repeaters, channels, and sites



4.2.3. Configure automatic channel reverts

A simulcast system can be configured to automatically shut down all repeaters that are on a channel that has simulcast failure, repeater failure, or RNT/CIM Channel Problem alarms. If there are 10 channels, the loss of 1 channel may be better than a large hole in coverage on 1 channel. When the problem is fixed, the channel needs to be manually unreverted.

The number of channels that can not automatically shut down is selected when describing the System icon. This is done when the OpenView map is made, and can be changed by right clicking a System icon, selecting Describe, and changing the value under Channel Revert MIN. This dialog box is also used to select whether the Status Channel can be reverted.

Channel Revert MIN: Select the number of simulcast channels that will not automatically shut down if simulcast failure, repeater failure, or RNT/CIM Channel Problem alarms occur. This is the minimum number of channels that will stay operational, even if there are additional problems. To prevent any channels from automatically reverting, select the number of channels that exist in the system.

Example: If the system has 10 channels and 8 channels are required to remain operational, select 8. If problems occur, up to 2 channels that have problems will be automatically shut down. The remaining 8 channels will stay operational, even if additional problems occur. Additional changes could be made manually. If automatic site reverts are configured, they may further automatically change the system.

Allow Status Channel Revert: If the Status Channel has problems, should the system automatically revert the Status Channel? An x in this box indicates that the system can automatically revert the Status Channel. If the Status Channel should not automatically revert, leave this box unchecked.

The alarm description list in Section 7.2 shows the alarms that cause simulcast and repeater failures, which can result in channel reverts.

4.2.4. Manually unrevert and revert channels

The revert status of channels can be seen by selecting a System icon and then selecting menu item System -> Channel Revert. A dialog box shows the system name, the total number of channels in the system, and the number of reverted channels. There is also a list of repeater numbers, channel numbers, and their current revert status. If the system has automatically reverted a channel, its status will be Reverted, otherwise the status is Normal.

The system will not automatically unrevert a channel. To unrevert a channel, select the channel in the list and click the UnRevert button. If the problem(s) that caused the revert has not been repaired, the channel will again automatically revert. To manually revert a channel, select the channel in the list and click the Revert button.

To unrevert individual repeaters and keep the channel reverted, select a Repeater icon and then select menu item Repeater -> UnRevert. Repeaters can also be reconfigured by using the Manual Repeater Control dialog box covered in Section 4.3. The channel status will remain reverted and additional alarms on the channel will not revert the channel.

4.2.5. Channel unrevert examples

The information in this section is for example only and may or may not apply to a specific system. Each system should be analyzed for other situations that may benefit from automatic reverts.

Note: If a channel that has failed repeaters is unreverted, radios that receive data from the sites that have failed repeaters will not hear calls made on the unreverted

channel. Remember to consider the condition of home channels and the status channel when unreverting channels.

A simulcast system can be configured to automatically shut down all repeaters that are on a channel that has simulcast failure, repeater failure, or RNT/CIM Channel Problem alarms. Channel reverts are configured in the Channel Revert Configuration section of the system icon Describe dialog box. Channels are unreverted using menu item System -> Channel Revert (as described in Section 4.2.4).

• Low-usage area with failure

If a system has reverted a channel because of a failure at a site in a low-usage area, the channel may be unreverted to provide high-usage areas with all channels. Radios receiving data from the site with the failed repeater will not hear calls made on the unreverted channel.

• Status channel with failure

If the status channel is reverted, unreverting it will optimize system response at sites with no failures. Radios in coverage areas with status channel failures will still receive update information on their home channels. No calls will be heard on the status channel from sites with failed repeaters.

The status channel can be configured to never revert.

• More failures than Channel Revert MIN

If the system has reverted as many channels as it can (as defined by Channel Revert MIN), additional failures on other channels will not cause channel reverts. Channels are reverted in the order that OpenView receives the alarms; however, if Channel Revert MIN is reached and there are more problems, it may be wise to unrevert some channels and revert others.

For example, a system may revert a home channel; then, a non-home channel has problems but is not reverted because the system has already reverted the number of channels that it is automatically allowed to revert. In this case, the system may work more efficiently if the home channel is manually unreverted and the non-home channel is manually reverted. Radios on the unreverted home channel that receive data from the site with the failed repeater will not receive data from the home channel, but they will still receive data from the status channel.

4.2.6. Configure inputs for automatic site reverts

Configuring automatic site reverts requires two processes. One process is to set up the revert inputs (criteria or conditions) that will cause a revert; and the other process is to set up the revert actions. There can be several sets of revert inputs per site, but there is only one revert action per site. Reverts are on a site by site basis; if a revert input set is met for a site, only that site is reverted.

Two dialog boxes are used to set up site reverts. This section covers configuring the revert inputs and the next section covers configuring the revert actions.

CAUTION: Use extreme caution when setting up automatic site reverts. Consider the effects that changing one site will have on the entire system.

Selecting a System icon and then selecting menu item System -> Revert Input Configuration will display the site Revert Input Configuration dialog box.

A revert input set defines the type of alarms (simulcast or repeater failures) and the list of repeaters that must have these alarms before the system will automatically revert the site. Besides revert input sets, a site can also have a revert input that will cause the site to revert if the network link is lost.

Site Revert on HC Network Link Loss: Selecting a site from the Sites/Revert Input Sets list and putting an x in this box (by clicking in the box) will set up a revert input. This input will cause the site to revert if it can not communicate with the host computer, which runs OpenView.

Creating Revert Input Sets: Each site can have up to 16 other input sets that will cause the site to revert. To add a set, select a site from the Sites/Revert Input Sets list and then click the Add Set button. A new entry, such as Set #1, will be added to the list.

To define the type of alarms for the selected set, select either Simulcast Failure or Repeater Failure in the Alarm Set Type section. The alarm description list in Section 7.2 shows the alarms that will cause simulcast and repeater failures.

To define the repeaters that must have these alarms, select all of the desired numbers in the Repeaters With Active Alarms section. These numbers correspond to the numbers that have been programmed into the repeaters. Select/deselect repeaters by clicking in the box to the left of the number. A selected repeater number will show an x in the box.

Note: A channel controller site cannot be set to revert.

Changing Revert Input Sets: To change a set, first select the desired set from the Sites/Revert Input Sets list. Then, select or deselect items in the Alarm Set Type and Repeaters With Active Alarms sections. The Clear All button will deselect all repeater numbers.

To remove a set, select the set (from the Sites/Revert Input Sets list) and then click the Delete Set button.

Tip: When several sets are desired, it may be beneficial to first make a chart of the plan. Figure 4-3 shows an example chart for a site, which has 10 repeaters. In this example, the site will revert if any one of the following sets exists.

- Set #1: Repeaters numbered 5, 6, 7, 8, and 9 are reporting simulcast failure alarms.
- Set #2: Repeaters numbered 1, 2, and 3 are reporting simulcast failure alarms.
- Set #3: Repeaters numbered 3, 4, 5, and 6 are reporting repeater failure alarms.

• Set # 4: Repeaters numbered 7, 8, 9, and 10 are reporting repeater failure alarms.

Figure 4-3. Chart showing site revert conditions

	Type	1	2	3	4	5	6	7	8	9	10
Set #1	S					X	X	X	X	X	
Set #2	S	X	X	X							
Set #3	R			X	X	X	X				
Set #4	R							X	X	X	X
.....											
Set #16											

4.2.7. Configure actions for automatic site reverts

Two dialog boxes are used to set up site reverts. The previous section covers configuring revert inputs and this section covers configuring the revert actions.

CAUTION: Use extreme caution when setting up automatic site reverts. Consider the effects that changing one site will have on the entire system.

Selecting a System icon and then selecting menu item System -> Revert Action Configuration will display the site Revert Action Configuration dialog box. The dialog box lists each repeater and shows the repeater's current revert setup in the Revert Action column. Revert actions are set up for each repeater at a site. If the site automatically reverts, all repeaters at the site will revert according to their individual setup.

To change the setup for a repeater, select the repeater from the list and then select the desired actions from the Site Revert Action section.

• Repeater Mode

Stand-Alone Multi-Net (MN): The repeater will use Multi-Net signaling, but will not communicate with any other radio sites (Multi-Net sites or other sites) within the system.

Disabled (DIS): The repeater will be shut down. It will not transmit or receive in any mode.

• Power Level

Select the desired transmit power level.

• Status Channel (SC)

Put an x in the box (by clicking in the box) to designate that the repeater is on the Status Channel. The Status Channel transmits update information for all calls. There is only one Status Channel in a simulcast system. Although, a site configured as a separate stand-alone site may have a different status channel.

4.2.8. Manually unrevert and revert sites

To see the revert status of sites, select a System icon and then select menu item System -> Site Revert. A dialog box shows the system name, the total number of sites in the system, and the number of reverted sites. There is also a list of sites and their current revert status. If the system has automatically reverted a site, its status will be Reverted, otherwise the status is Normal.

The system will not automatically unrevert a site. To unrevert a site, select the site in the list and click the UnRevert button. If the problem(s) that caused the revert has not been repaired, the site will again automatically revert. To manually revert a site, select it from the list and click the Revert button. Alternatively, sites can be reverted and unreverted by selecting a Site icon and then selecting menu item Site -> Revert or Site -> UnRevert.

To unrevert individual repeaters and keep the site reverted, select a Repeater icon and then select menu item Repeater -> UnRevert. Repeaters can also be reconfigured by using the Manual Repeater Control dialog box covered in Section 4.3. The site status will remain reverted and additional alarms at the site will not revert the site.

4.2.9. Site revert example

The information in this section is for example only and may or may not apply to a specific system. Each system should be analyzed for other situations that may benefit from automatic reverts.

If the home channel of an important group of users and the status channel both fail at a site, the site can be automatically reverted and reconfigured to allow communications within the site. If a system has very large overlap areas, the affected site might be shut down without greatly degrading coverage. However, if shutting down the site would leave large areas inaccessible, reconfiguring the site to a stand-alone Multi-Net site may be a better alternative.

Note: Subscriber units on the system will need to have a “backup” system programmed for a stand-alone Multi-Net site. When the fleet map is produced for the subscriber units, the site revert actions and the backup system must be planned together.

CAUTION: Radios monitor their home channel and the status channel for over-the-air instructions. If there are problems on either channel, radios may not receive their instructions. Therefore, pay special attention to the status channel and home channels when configuring reverts.

The following example shows how a 3-site, 10-channel system could be configured for an automatic site revert.

Refer to Figure 4-4. Site 3 has been configured to revert to a stand-alone Multi-Net site if repeaters 1 and 3 fail. In this system, repeater 1 is the status channel. Repeater 3 is the home channel for the group used by a high-priority collection of users. When repeaters 1 and 3 fail, groups that use channel 3 as the home channel have no access to the radio system in the site 3 coverage area. When the system

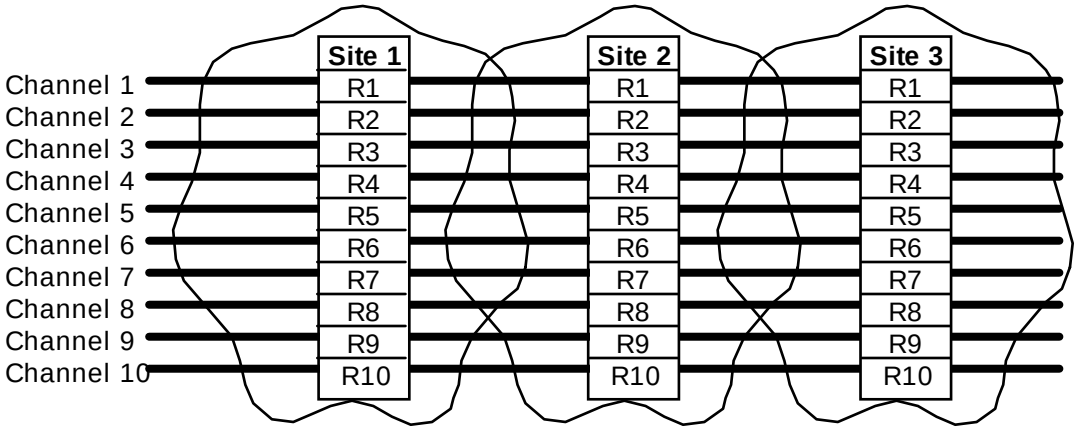
reverts, groups that use a backup subscriber unit system will have local access for site 3; other groups will have no access for site 3.

When the high-priority users need to use the repeater at site 3, they will need to change their radios to a backup system that is programmed (in this example) with repeater 8 as the status channel. Repeater 9 is the home channel for their group. Trunked communication will then be available to them within the site; however, no audio is sent back to the RNT. Therefore, there will be no consoles, unique ID calls, or telco calls from site 3.

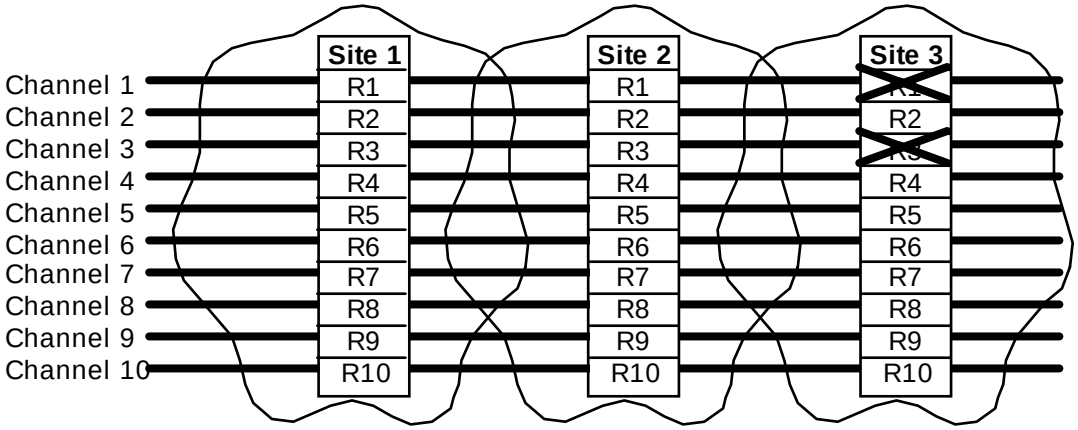
To configure the system for this type of revert involves two dialog boxes. The dialog box from menu item System -> Revert Input Configuration, is used to set up the input alarms (or conditions) that will cause a revert. Refer to Figure 4-5. For this example, a set of inputs is defined for site 3. Repeater Failure is selected in the Alarm Set Type section of the dialog box. Repeaters 1 and 3 are selected in the Repeaters With Active Alarms section of the dialog box.

The dialog box from menu item System -> Revert Action Configuration, is used to set up the actions that the system will take when the above inputs are met. (In this example, when repeaters 1 and 3 of site 3 fail, the system will take the actions defined for site 3.) Refer to Figure 4-6. In the dialog box, repeater 8 is configured to be a stand-alone Multi-Net repeater and to be the status channel. Repeaters 9 and 10 are configured to be stand-alone Multi-Net repeaters. Repeaters 1 to 7 are configured to be disabled. If desired, the power level can also be changed, possibly to reduce interference in an overlap area.

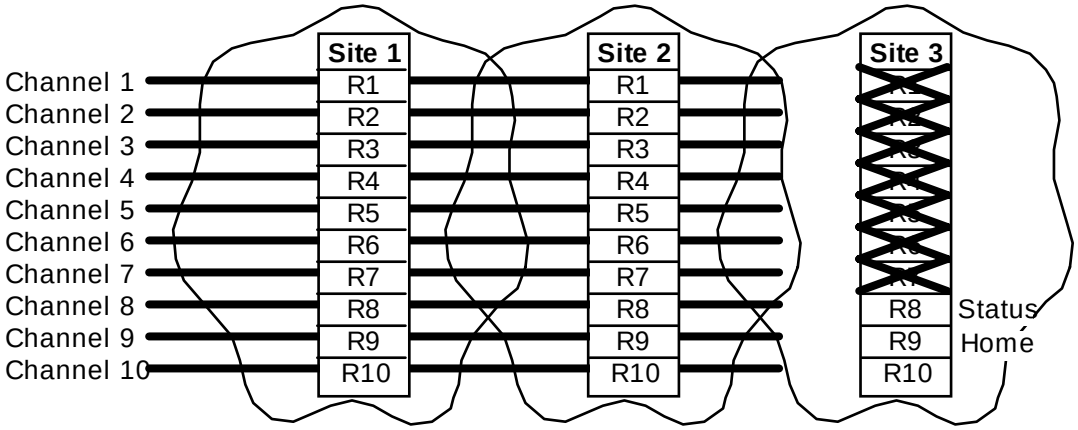
Figure 4-4. Site 3 is configured to revert to a stand-alone Multi-Net site.



Normal 3-site, 10-channel simulcast system.



At site 3, repeaters fail on the status channel (Channel 1) and on the home channel for a high-priority group (Channel 3).



The system was configured to automatically revert site 3 to a stand-alone Multi-Net site using repeaters 8, 9, and 10 and shutting down repeaters 1 through 7. To avoid interference, systems with large overlap areas may also need to manually shut down repeaters 8, 9, and 10 at sites 1 and 2.

Figure 4-5. Revert Input Configuration

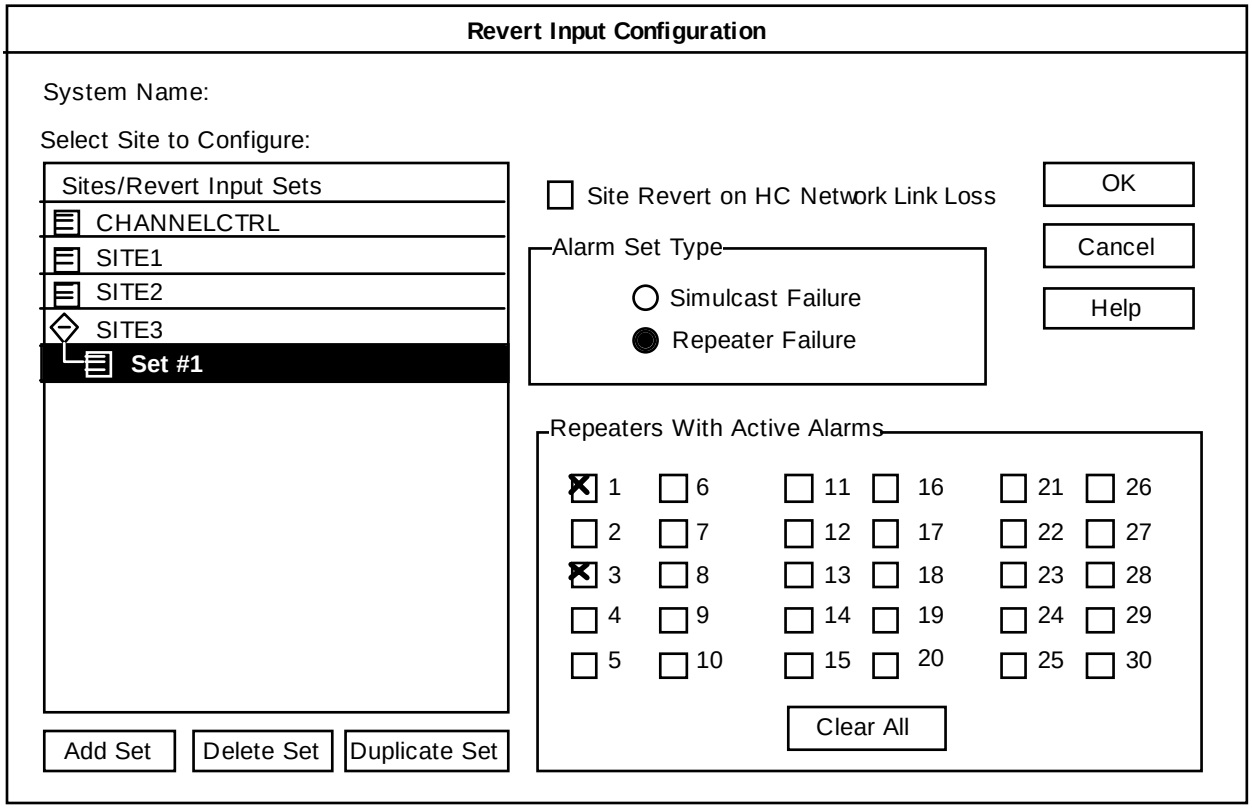
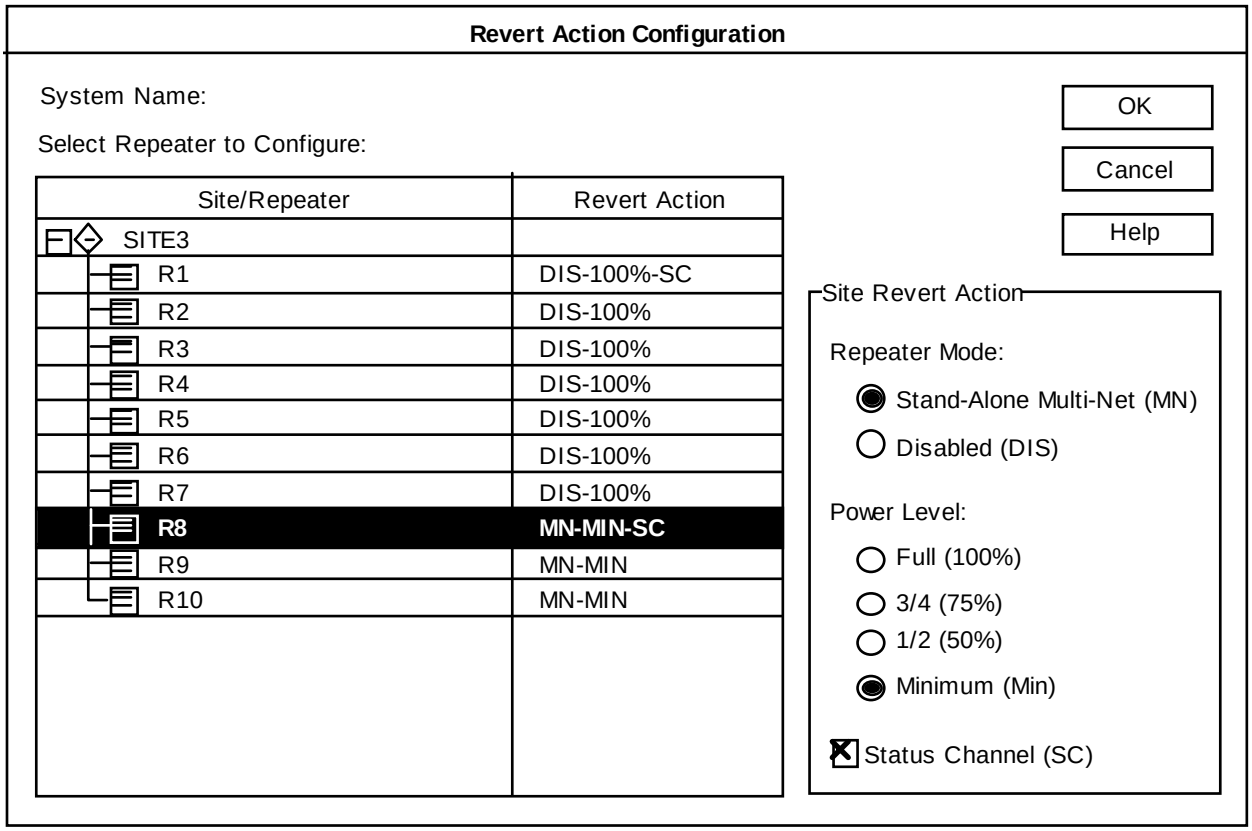


Figure 4-6. Revert Action Configuration



4.3. Perform manual repeater control

Since each system has a unique installation and unique propagation patterns, some situations will be beyond the scope of automatic reverts. Therefore, it is possible to manually set the repeater mode and power level for each repeater and also set if the repeater is on the Status Channel. Repeater control is done by selecting a System icon and then selecting menu item System -> Manual Repeater Control. The Manual Repeater Control dialog box will appear.

This dialog box shows the name of the system and a list of all sites/repeaters within the system. The repeaters can be shown/hidden by clicking the +/- button next to the site name or by double clicking the site name. For each repeater, the mode, power level, and whether the repeater is on the Status Channel are shown.

The Current column shows if the information is “True” or “False”. True indicates the conditions at the present time. False indicates that there is a communication problem with the repeater, so current information is unavailable.

To make changes, select the repeater to change, select the desired options, and then click either the Set Mode button, the Set Power button, or the Set Mode and Set Power button. The repeater will be reprogrammed and the dialog box will be updated accordingly.

- **Repeater Mode**

  This section is used to select the trunking method of the repeater and whether the repeater is on the Status Channel.

  Disabled: The repeater will be shut down. It will not transmit or receive in any mode.

  Stand-Alone Multi-Net: The repeater will use Multi-Net signaling, but will not communicate with any other radio sites (Multi-Net sites or other sites) within the system. The enhanced operating features provided by Multi-Net signaling will not be available.

  Simulcast Channel Control: Select this option if the “repeater” is part of the channel controller in a simulcast system. A channel controller makes several simulcast remote repeaters look like one repeater to the RNT (Radio Network Terminal, which controls the operating features of the radio system).

  Simulcast Remote Repeater: Select this option for any repeater that is part of a simulcast system. A simulcast system has several sites. Each site in a system has the same channels and the channel audio is rebroadcast at each site.

  Status Channel: An x in this box designates that the repeater is on the Status Channel. The Status Channel transmits update information for all calls. There is only one Status Channel in a simulcast system. Although, a site configured as a separate stand-alone site may have a different Status Channel.

- **Power Level**

  Select the desired transmit power level.

4.3.1. Repeater menu

Repeaters can also be controlled by selecting a repeater icon from the map and then selecting a function from the Repeater menu. The following functions are available.

Active Alarms: To view the active alarms for a repeater, select a repeater icon and then select menu item Repeater -> Active Alarms. A dialog box shows the repeater name and a list of active alarms, including active alarms that have been manually acknowledged from the Alarm Log.

Restart: A repeater can be restarted by selecting a repeater icon on a map, and then selecting menu item Repeater -> Restart.

Revert: To revert a repeater, select a repeater icon on a map, and then select menu item Repeater -> Revert. The repeater will be reverted to the configuration set in the Revert Action Configuration dialog box (see Section 4.2.7).

UnRevert: To unrevert a repeater, select a repeater icon on a map, and then select menu item Repeater -> UnRevert. Unrevert returns the repeater to the configuration set in the EFJ Repeater Description dialog box (see Section 3.2.3).

This page intentionally left blank.

SECTION

5. Fault Management - Operating

OpenView receives periodic status messages from devices. When a device reports a problem, the operator is notified of an alarm by the following events.

- A beep or sound file plays.
- The Alarm Bell in the toolbar changes color.
- Map icons change color.
- An entry is displayed in the Alarm Log.

5.1. A beep or sound file plays

Alarm sounds are configurable by the operator. (See Section 4.1.5 Alarm Sound.) Depending on configuration, when an alarm occurs there may be no sound, a simple beep, or a sound from a sound file. Each level of alarm may have a different sound. The sound may occur only once or it may repeat until alarms above a specified status level are acknowledged.

5.2. The Alarm Bell in the toolbar changes color

The Alarm Bell icon in the toolbar will change color to indicate the status of the alarm.

Note: If a higher-level alarm exists, the Alarm Bell will not change color, but will stay the color of the highest-level alarm.

To view the color legend, select menu item Monitor -> Status Legend.

Clicking on the Alarm Bell button will display the Alarm Log. The Alarm Log is described later in this section.

5.3. Map icons change color

When an alarm occurs, maps show the location of the alarm by changing the color of the icons where the alarm occurred. To view the color legend, select menu item Monitor -> Status Legend.

When OpenView starts, a map is displayed. This map is typically the home map and will show a System icon for each system. Double-clicking on a System icon will display a submap that shows Site icons for each site within the system. Double-clicking on a Site icon will display a submap with icons for all monitored devices (repeaters, routers, etc.) at that site.

When the status of a device changes, its icon changes color to indicate the current status. The System and Site icons associated with the device also change color, unless they are already colored for a higher-level alarm. (System and Site icons can be configured to not change color. See Section 4.1.6 Status Propagation.)

To display the Alarm Log for a specific icon, move the cursor over the desired icon, click the right mouse button, and select Alarms. The Alarm Log will show

only the alarms for that icon. To have the log show all alarms, click the Alarm Bell in the toolbar.

Note: Viewing the alarms of a System or Site icon will only show network-level alarms (not alarms for all devices at that location).

Maps can also be viewed by selecting menu item Window -> Home Submap or Window -> Locate Submap. Specific icons can be located by selecting menu item Window -> Locate Object.

The Home map and parent submap can also be viewed by using the Home and Previous buttons in the toolbar.

5.3.1. Map viewing options

The scale of a map can be changed from the View menu and by clicking the zoom buttons in the toolbar. When a map is first displayed, the default size is 1 to 1 (1:1). Maps can be zoomed to 1/2 normal size (1:2), 1/4 normal size (1:4), or 1/8 normal size (1:8). The zoomed size remains in effect until changed.

If an entire map is not displayed in its window, select menu item View -> Pan to choose the part of the map to view. In the Pan dialog box, a rectangle represents the part of the map that will show in the window. Click on the rectangle and drag it to the desired location. Click “OK” to view the selected area in the map window.

A grid (like graph paper) can be displayed on a map by selecting menu item View -> Show Grid. This menu item then changes to Hide Grid, which is used to turn off the grid display. The horizontal and vertical spacing of the grid lines can be changed by selecting menu item View -> Set Grid.

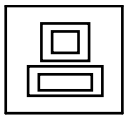
5.3.2. Icon descriptions

EFJ System Icon: This icon represents radio and network equipment that are inter-connected to provide communication capability to a single entity. Double clicking on this icon will display a map of sites within the system.

EFJ Site Icon: This icon represents a physical location that has network equipment. Double clicking on this icon will display a map of all network equipment and repeaters located at the site.

Cisco 2501: A Cisco 2500-series router is represented by this icon. A router is a network device that routes network traffic between sites (or subnets).

Router: This icon may be used for a router model that does not have its own icon. A router is a network device that routes network traffic between sites (or subnets).



Computer: Site computers and channel computers are represented with this icon. Generically, OpenView calls it a Personal Computer.

EFJ Repeater: This icon represents a single repeater. That is a piece of radio equipment that is capable of receiving and re-transmitting radio frequencies. This icon is also used to represent channel controllers.

5.4. An entry is displayed in the Alarm Log

The Alarm Log displays an entry for each alarm. This section describes:

- Accessing the Alarm Log
- Description of the Alarm Log
- Displaying Current or History list
- Acknowledging Alarms
- Displaying selected groups (Filter dialog box)
- Descriptions of the alarms

5.4.1. Accessing the Alarm Log

Alarm information is displayed in the Alarm Log, which can be accessed in several ways.

- Display all alarms by clicking the Alarm Bell button in the toolbar or selecting menu item Monitor -> Alarm Log.
- Display selected groups of alarms by displaying the Alarm Log, clicking Filter, and selecting desired criteria. (See Section 5.4.5 Displaying selected groups.)
- Display the alarms for a specific icon (system, site, or device) by moving the cursor over the desired icon, clicking the right mouse button, and selecting Alarms. (For displaying maps and icons, see Section 5.3 Map icons change color.) From the Alarm Log, the icon for the device or site that sent the alarm can be found by selecting the alarm entry and clicking the Go To button.

5.4.2. Description of the Alarm Log

The Alarm Log information is displayed in columns, as described below.

Status: A word that describes the alarm level. The alarm level is also indicated by the color of the entry. (See Section 5.5 Color status legend.)

Date: The date the alarm was reported.

Time: The time the alarm was reported.

Description: A description of the fault that caused the alarm. (See the alarm description list in Section 7.2.)

Object: The system, site, or device that reported the alarm. The map containing the icon for an entry can be located by selecting an entry and clicking the Go To button.

The widths of the displayed columns can be changed by clicking and dragging the vertical bars (|) in the column headings.

The Alarm Log displays alarm entries in the order they are reported, or by order of severity (as set under menu item Options -> Customize Alarms. See Section 4.1.4 Alarm Log options.).

5.4.3. Displaying Current or History list

The History/Current button at the bottom of the Alarm Log is a toggle button. When the Current list is displayed, the button will be named History and clicking it will display the History list. Likewise, when the History list is displayed, the button will be named Current and clicking it will display the Current list. The top-right area of the Alarm window will indicate if the Current or History list is being viewed by displaying “Current Display Options”, or “History Display Options”.

Alarm entries will stay in the Current list until they are acknowledged, then OpenView will move the entries to the History list.

5.4.4. Acknowledging Alarms

OpenView receives periodic status messages from devices. When the situation that created a high-level alarm has been corrected, the next status message from the affected device will update the Alarm Log by moving the old entry to the History list and displaying the new entry in the Current list. The color of the Alarm Log entry and the Device, Site, and System icons will also update accordingly.

If a repeater re-starts, its existing alarms will be moved from the Current list to the History list. After re-start, any new alarms will be displayed in the Current list.

To manually acknowledge or “clear” an alarm, click on the alarm entry in the Alarm Log, then click the Acknowledge button. Multiple non-consecutive entries can be selected with Ctrl+click. Multiple consecutive entries can be selected with Shift+click. All alarm entries can be acknowledged at one time by clicking the Acknowledge All button. Acknowledging an alarm moves the log entry from the Current list to the History list.

Note: Manually clearing an alarm is considered a change in status to normal level. In many cases, it may be advisable to not manually clear critical alarms, instead let them clear themselves when the problem is corrected (as described above). Manually clearing alarms will return icons to normal color, making the network appear to be working without problems.

5.4.5. Displaying selected groups (Filter dialog box)

The Filters button at the bottom of the Alarm Log will display the Alarm Log Filters dialog box, where the alarms to view can be selected. When OK is clicked, the Alarm Log displays only the alarms that were selected. To again display all current alarms, click the Alarm Bell in the toolbar or select menu item Monitor -> Alarm Log.

The top-right area of the Alarm window indicates which alarms are being viewed. When viewing all alarms, this area reads:

Current Display Options
Show All Alarms
All Objects

The first line will read “History Display Options” if the History list is displayed. When viewing alarms filtered with the Alarm drop-down box, the second line will change to the alarm selected to view. When viewing alarms filtered by the Object Type/Object Name drop down boxes, the bottom line will change to the type-name of the selected alarms.

The drop down boxes of the Alarm Log Filters dialog box are described below.

Alarm: Use this drop down box to select the alarm description to view. The Alarm Log will then display alarms that have the selected description. The descriptions listed are the same descriptions used in the Description column of the Alarm Log.

Object Type: Select the type of device from this drop down box. For example, if only alarms from routers are to be viewed, then select “router” from the list.

Object Name: To view only alarms that are from a specific device, select the device’s name in this drop down box. If a device has subcomponents, they can be selected by also entering the Sub(component) or Node numbers. Object names are shown in the Object column of the Alarm Log. The descriptive label that appears below a map icon is not necessarily the Object Name.

Object Status: Use this drop down box to select an alarm level. The Alarm Log will then display only alarms that are of the selected level. Alarm levels are shown in the Status column of the Alarm Log and also by selecting menu item Monitor -> Status Legend.

Note: When an icon is selected, its Object Type and Object Name are displayed in the status bar at the bottom of the OpenView window. The format is, object name (object type) in submap name. They also appear in the Describe dialog box (right click on an icon and select Describe). The Object Type is the title of the dialog box and the Object Name is in the Name box.

5.4.6. Descriptions of the alarms

Repeaters and channel controllers have IACs (Interface Alarm Cards) that can report external alarms, such as open doors. Each repeater can have different alarms. The descriptions of IAC alarms are found by right clicking a repeater or channel controller icon and then selecting Describe.

Other E.F. Johnson alarm descriptions are listed in Section 7.2.

5.5. Color status legend

A legend for icon colors can be seen by selecting menu item Monitor -> Status Legend. Colors for Alarm Log entries are similar. (Computer monitors will vary as to the exact colors seen on the screen.)

Alarm colors are described in Figure 2-1. The highest-level alarm is listed first.

Note: If a color for a higher priority alarm is already displayed, a lower priority alarm will not change the color of the icon or Alarm Bell.

Figure 5-1. Icon and map colors

Status	Map	Log	Description
Critical	Red	Red	The device is unavailable. It may have stopped operating.
Major	Dark Red	Red	A problem has been reported; there is some degradation of function.
Minor	Orange	Yellow	A condition has been reported that may be degrading functions.
Warning	Yellow	Yellow	An abnormal condition exists that is not causing degradation of function.
Marginal	Mustard	Yellow	A problem has not occurred, but a situation is close to being out of specifications.
Informational	Magenta	Magenta	Information about a situation that may be abnormal.
Disabled	Cyan	Cyan	The device is down.
Unmanaged	Wheat	White	OpenView does not manage the device.
Normal	Green	Green	The device is working properly.
Unknown	Blue	Cyan	OpenView has no information on the status of the device.

5.6. Active repeater alarms

To view the active alarms for a repeater, right click on a repeater icon and then select Active Alarms. Alternatively, select a repeater icon and then select menu item Repeater -> Active Alarms. A dialog box shows the repeater name and a list of active alarms, including active alarms that have been manually acknowledged from the Alarm Log.

This page intentionally left blank.

SECTION

6. Performance Management

6.1. Calibrate uni-directional, non-redundant systems

Note: This section is for calibrating uni-directional, non-redundant microwave systems. Section 6.2 is for bi-directional, non-redundant microwave systems. The program will display the appropriate dialog box and help for the system.

Simulcast systems must be calibrated to avoid distorted signals in areas that have repeater coverage overlap. During calibration the channel controller sends a timing tone that is used to determine the length of time it takes for a signal to reach each repeater. The repeaters' buffer and phase delays are then adjusted so that all repeaters will transmit at the same time and phase. The timing of the entire system is synchronized by GPS (global positioning system).

The manual uni-directional calibration process occurs in two steps.

1. Data Acquisition procedure: Information is collected that is used to automatically calculate the repeaters' buffer and phase delays. See Section 6.1.1.
2. Write procedure: The calculated values are written to the Simulcast Modulation Cards (SMCs) in the repeaters. See Section 6.1.3.

6.1.1. Data acquisition procedure (uni-directional)

1. Select a System icon.
2. Select menu item System -> Calibration -> Manual Calibration.
3. Select a channel from the list.
4. Click the Acquire Data button.

   If the channel is the status channel, a message box will appear. Clicking OK will continue the process for the status channel; clicking Cancel will cancel data acquisition for the status channel.

   If a "Channel cannot be calibrated" message appears, the channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller.
5. Data acquisition requires some time. A flashing icon next to the channel name indicates that data acquisition is in progress. Status messages will appear below the Write button.
6. When the data acquisition process for the selected channel finishes, the icons next to the channel and associated repeaters will change.
   - An OK icon indicates that data acquisition was successful for a repeater.
   - A W icon indicates that the channel is writeable (two or more repeaters have returned good data).

- Other icons indicate that the data acquisition process was not successful. See Section 6.1.2 for icon descriptions and remedies.

7. Repeat steps 3-6 to acquire data for additional channels.
8. When data has been acquired for all channels to be calibrated, continue with the write procedure in Section 6.1.3. Data will only be written to repeaters that display an OK icon.

   CAUTION: If all repeaters on a channel do not have OK icons, writing that channel's data may cause poor simulcast performance. The recommended procedure is to close the manual calibration dialog box, fix any unsuccessful repeaters, and recalibrate the associated channels. An exception can be made if a repeater is disabled and will remain disabled. When the disabled repeater is put back into service the associated channel should be recalibrated.

6.1.2. Data acquisition icons for uni-directional

In the System -> Calibration -> Manual Calibration dialog box, icons appear beside the channel and repeater names to indicate the status of data acquisition. The following tables list the icons, their descriptions, and possible remedies.

Table 6-1. Channel icons during uni-directional calibration

Channel Icons	Description	Remedy
⊟◈	Other icons will appear to the left of this icon as calibration proceeds. Clicking the box will collapse the repeater list.	To calibrate, follow the instructions in Section 6.1.1.
⊞◈	Other icons will appear to the left of this icon as calibration proceeds. Clicking the box will show the list of repeaters.	To calibrate, follow the instructions in Section 6.1.1.
■ flashing	Data acquisition is in progress.	Be patient until data acquisition has finished. Each repeater takes approximately 15 to 20 seconds.
W	The channel is writeable. Data acquisition for the channel is completed. Two or more repeaters returned good data that may be written to the SMC.	If data is not to be acquired from other channels, continue with the write procedure in Section 6.1.3.

Channel Icons	Description	Remedy
✓	Data acquisition for the channel was completed but not successful. No timing values will be written for this channel.	Fix any repeater problems and recalibrate the channel.
R	The channel is reverted; calibration could not be started.	Fix the problems that have caused the channel to revert. Unrevert the channel. Then, calibrate the channel.
X	Unknown failure.	1. The channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller. 2. IP address may be incorrect. Check assignment in EFJ Site Description dialog box. See Section 3.2.2. 3. . System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Section 3.2.1 and 3.2.2.

Table 6-2. Repeater icons during uni-directional calibration

Repeater Icons	Description	Remedy
	Data acquisition has not occurred for the repeater.	To calibrate, follow the instructions in Section 6.1.1.
OK	Data acquisition was successful.	If data is not to be acquired from other channels, continue with the write procedure in Section 6.1.3.

Repeater Icons	Description	Remedy
F	Data acquisition failed. Possible causes: 1. The repeater is reverted. 2. The channel controller's timing tone gain is set too low. 3. The repeater's threshold is set too high.	1. Fix the problems that have caused the repeater to revert. Unrevert the repeater. Recalibrate the channel. 2. Call an E.F. Johnson service representative. 3. Call an E.F. Johnson service representative.
Z	1. Noise may have interfered with access to the repeater. 2. The repeater's threshold value may be set incorrectly.	1. Retry data acquisition. 2. Call an E.F. Johnson service representative.

6.1.3. Write procedure (uni-directional)

CAUTION: If all repeaters on a channel do not have OK icons, writing that channel's data may cause poor simulcast performance. The recommended procedure is to close the manual calibration dialog box, fix any unsuccessful repeaters, and recalibrate the associated channels. An exception can be made if a repeater is disabled and will remain disabled. When the disabled repeater is put back into service the associated channel should be recalibrated.

Click the Write button to write the timing values to the repeaters' SMCs. Only repeaters that have OK icons will be written. If a channel has a check mark icon, none of that channel's repeaters will be written. A flashing icon next to the channel name indicates that writing is in progress. An information alarm will occur as each repeater is written.

The Write process will write the data for all channels that display the W icon every time the Write button is clicked. For example, if data has been acquired for Channel X and the button is clicked, the data will be written to all the repeaters that show OK and are associated with Channel X. If data is then acquired for Channel Y and the Write button is clicked, the data will be written to all the repeaters that show OK and are associated with Channels X and Y. To avoid rewriting data, close and reopen the Manual Calibration dialog box after clicking the Write button.

6.2. Calibrate bi-directional, non-redundant systems

Note: This section is for calibrating bi-directional, non-redundant microwave systems. Section 6.1 is for uni-directional, non-redundant microwave systems. The program will display the appropriate dialog box and help for the system.

Simulcast systems must be calibrated to avoid distorted signals in areas that have repeater coverage overlap. During calibration the channel controller sends a timing tone that is used to determine the length of time it takes for a signal to reach each repeater. The repeaters' buffer and phase delays are then adjusted so that all repeaters will transmit at the same time and phase. The timing of the entire system is synchronized by GPS (global positioning system).

The manual bi-directional calibration process occurs in three steps: phase 1 data acquisition, phase 2 data acquisition, and writing the values.

Phase 1 data acquisition requires that all sites receive data from the microwave direction that does not cause an alarm. Phase 2 requires that all sites receive data from the direction that does cause an alarm. IAC 1 (on Repeater 1 at each repeater site) produces an alarm when the microwave is in one data direction and no alarm when the microwave is in the opposite data direction.

The program checks for the proper alarm/no alarm condition before starting data acquisition. If the wrong direction is detected, a message will be displayed, and the microwave direction must be changed before data acquisition can occur.

Data acquisition collects information that is used to automatically calculate the repeaters' phase and buffer delays for both microwave directions. After data acquisition is completed, the calculated values are written to the Simulcast Modulation Cards (SMCs) in the repeaters. If an attempt is made to close the dialog box before values are written, a message box will give the option to return to the dialog box or to close the box and lose all unwritten data.

6.2.1. Phase 1 data acquisition (bi-directional)

1. Lock the microwave data direction at all sites in the no-alarm direction.
2. Select a System icon.
3. Select menu item System -> Calibration -> Manual Calibration.
4. Select a channel from the list.
5. Click the Acquire Data button.

   If the channel is the status channel, a message box will appear. Clicking OK will continue the process for the status channel; clicking Cancel will cancel data acquisition for the status channel.

   If a "Channel cannot be calibrated" message appears, the channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller.
6. Data acquisition requires some time. A flashing icon next to the channel name indicates that data acquisition is in progress. Status messages will appear below the Phase 2 button.

7. When the data acquisition process for the selected channel finishes, the icons next to the channel and associated repeaters will change.

   • An H indicates that data acquisition was successful for this microwave direction. Two or more repeaters on the channel are OK.

   • Other icons indicate that data acquisition was not successful. See Section 6.2.3 for icon descriptions and remedies.

8. Repeat steps 4-7 for additional channels.

6.2.2. Phase 2 data acquisition (bi-directional)

1. Lock the microwave data direction at all sites in the alarm direction.
2. Click the Phase 2 button.
3. Select a channel from the list. Only channels that have an H icon will be available for selection.
4. Click the Acquire Data button.
5. Data acquisition requires some time. A flashing icon next to the channel name indicates that data acquisition is in progress. Status messages will appear below the Phase 2 button.
6. When the data acquisition process for the selected channel finishes, the icons next to the channel and associated repeaters will change.

   • An OK icon indicates that data acquisition was successful for the repeater.

   • A W icon indicates that the channel is writeable (two or more repeaters have returned good data).

   • Other icons indicate that the data acquisition process was not successful. See Section 6.2.3 for icon descriptions and remedies.

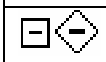
7. Repeat steps 3-6 for additional channels.
8. When data has been acquired for all channels to be calibrated, continue with the write procedure in Section 6.2.4. Data will only be written to the repeaters that display OK icons.

   CAUTION: If all repeaters on a channel do not have OK icons, writing that channel's data may cause poor simulcast performance. The recommended procedure is to close the manual calibration dialog box, fix any unsuccessful repeaters, and recalibrate the associated channels. An exception can be made if a repeater is disabled and will remain disabled. When the disabled repeater is put back into service the associated channel should be recalibrated.

6.2.3. Data acquisition icons for bi-directional

In the System -> Calibration -> Manual Calibration dialog box, icons appear beside the channel and repeater names to indicate the status of data acquisition. The following tables list the icons, their descriptions, and possible remedies.

Table 6-3. Channel icons during bi-directional calibration

Channel Icons	Description	Remedy
	Other icons will appear to the left of this icon as calibration proceeds. Clicking the box will collapse the repeater list.	To calibrate, follow the instructions in Sections 6.2.1 and 6.2.2.
	Other icons will appear to the left of this icon as calibration proceeds. Clicking the box will show the list of repeaters.	To calibrate, follow the instructions in Sections 6.2.1 and 6.2.2.
 flashing	Data acquisition is in progress.	Be patient until data acquisition has finished. Each repeater takes approximately 15 to 20 seconds.
W	The channel is writeable. Data acquisition for the channel is completed. Two or more repeaters returned good data that may be written to the SMC.	If data is not to be acquired from other channels, continue with the write procedure in Section 6.2.4.
✓	Data acquisition for the channel was completed but not successful. No timing values will be written for this channel.	Fix any repeater problems and recalibrate the channel.
H	Data acquisition for the channel is half completed.	Continue to phase 2 data acquisition. See Section 6.2.2.
R	The channel is reverted; calibration could not be started.	Fix the problems that have caused the channel to revert. Unrevert the channel. Then, calibrate the channel.

Channel Icons	Description	Remedy
X	Unknown failure.	1. The channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller. 2. IP address may be incorrect. Check assignment in EFJ Site Description dialog box. See Section 3.2.2. 3. System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Section 3.2.1 and 3.2.2.

Table 6-4. Repeater icons during bi-directional calibration

Repeater Icons	Description	Remedy
	Data acquisition has not occurred for the repeater.	To calibrate, follow the instructions in Sections 6.2.1 and 6.2.2.
OK	Data acquisition was successful.	If data is not to be acquired from other channels, continue with the write procedure in Section 6.2.4.
F	Data acquisition failed. Possible causes: 1. The repeater is reverted. 2. The channel controller's timing tone gain is set too low. 3. The repeater's threshold is set too high.	 1. Fix the problems that have caused the revert. Unrevert the repeater. Recalibrate the channel. 2. Call an E.F. Johnson service representative. 3. Call an E.F. Johnson service representative.
Z	1. Noise may have interfered with access to the repeater. 2. The repeater's threshold value may be set incorrectly.	1. Retry data acquisition. 2. Call an E.F. Johnson service representative.

6.2.4. Write procedure (bi-directional)

CAUTION: If all repeaters on a channel do not have OK icons, writing that channel's data may cause poor simulcast performance. The recommended procedure is to close the manual calibration dialog box, fix any unsuccessful repeaters, and recalibrate the associated channels. An exception can be made if a repeater is disabled and will remain disabled. When the disabled repeater is put back into service the associated channel should be recalibrated.

Click the Write button to write the timing values to the repeaters' SMCs. Only repeaters that have OK icons will be written. If a channel has a check mark icon, none of that channel's repeaters will be written. A flashing icon next to the channel name indicates that writing is in progress. An information alarm will occur as each repeater is written.

The Write process will write the data for all channels that display the W icon every time the Write button is clicked. For example, if data has been acquired for Channel X and the button is clicked, the data will be written to all the repeaters that show OK and are associated with Channel X. If data is then acquired for Channel Y and the Write button is clicked, the data will be written to all the repeaters that show OK and are associated with Channels X and Y.

6.3. E.F. Johnson alarm database

Alarms from E.F. Johnson repeaters and channel controllers are recorded in the E.F. Johnson log file, which is a Borland Paradox™ database file that can be used for trend and failure analysis.

The filename of the E.F. Johnson log is the name of the OpenView map with a db extension and is kept in the OV directory. If the file does not exist, it will be created the next time a log entry is written.

CAUTION: The E.F. Johnson log file will continue to grow to an unlimited size and should be backed up and maintained on a regular basis.

6.3.1. Format of log

The database fields are as follows.

DateTime: The date and time that the alarm was recorded. The format is: hours:minutes:seconds, month/date/year.

SystemNo: The number of the system that reported the alarm, as defined in the Describe dialog boxes when the map was created.

SiteNo: The number of the site that reported the alarm, as defined in the Describe dialog boxes when the map was created.

RptrNo: The number of the repeater that reported the alarm, as programmed in the repeater and entered in the Describe dialog boxes when the map was created.

AlarmID: The alarm's identification number. Refer to the alarm description list in Section 7.2.

6.4. OpenView alarm database

All alarms are recorded in the OpenView log file, unless they have been deleted from within the OpenView program. The OpenView log is a Borland Paradox database file that can be used for trend and failure analysis.

The OpenView log is in files named OVALINS.*, which are stored in the OV directory. The location of the log file can be changed by selecting menu item Options -> Customize HP OpenView and entering a new location in the Log File box. If the file does not exist, OpenView will create it the next time a log entry is written.

Note: Do not directly modify the OVALINS.* database files. If the files need to be used, copy them to another location before modifying. Modifying the files that OpenView is using can cause program operation problems.

6.4.1. Deleting items from the log

- Alarms can be deleted from the log file on a periodic basis by selecting menu item Options -> Customize Alarms and entering the number of days in the "Delete after" box of the Alarm section. The default is 7 days. The deletion will take place when OpenView is started or at midnight if OpenView is running.
- When viewing the History Alarm log, alarms can be selected and then deleted with the Delete button. Multiple non-consecutive entries can be selected with Ctrl+click. Multiple consecutive entries can be selected with Shift+click. All entries can be deleted by clicking the Delete All button.
- The maximum number of Alarm Log entries can be set with MaxRecords in OVWIN.INI under OVAlarm.

6.4.2. Format of log

The database fields are as follows.

atimekey: A Paradox database key.

adate: The date the alarm occurred, in date format.

ahours: The hour when the alarm occurred, in time format.

aminutes: The minute when the alarm occurred, in time format.

aseconds: The second when the alarm occurred, in time format.

aseverity: A number representing the severity of the alarm.

10 = Critical
9 = Major
8 = Minor
7 = Warning

6 = Marginal
5 = Informational
4 = Disabled
3 = Unmanaged
2 = Normal
1 = Unknown

aappid: A number representing the application that reported the alarm.

aclassid: The device class. For E.F. Johnson alarms, this is the same as AlarmID field of the E.F. Johnson log.

aorgclass: Not used

aflags: A number representing the alarm state. 0 = Open, 1 = Cleared.

aobjtyp: The device symbol number. These are stored in the OVSymbols section of the OVWIN.INI file. (The numbers in the log are in decimal format and the numbers in the INI file are in hex format.)

aobjname: The Object Name of the device, from the Describe dialog box (up to 64 characters).

asubobj: The subcomponent number, or -1 if not used. For E.F. Johnson alarms, this is the site number.

anode: The part number of the subcomponent, or -1 if not used. For E.F. Johnson alarms, this is the repeater number.

astatus: The current status.

adesc: The alarm description as it is displayed in the Alarm Log (up to 64 characters).

aextdesc: The extended alarm description as it is displayed by selecting the More Info button in the Alarm Log window. This field is in blob text format.

This page intentionally left blank.

SECTION

7. Troubleshooting

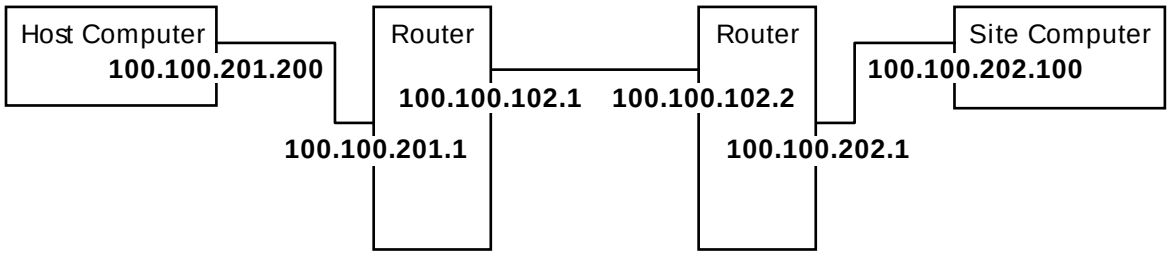
7.1. Ping

7.1.1. Ping troubleshooting techniques

Ping (packet Internet groper) sends a message to a device and waits for a response. The response will indicate that the network connection is working or that a problem was detected. The ping messages and responses are ICMP (Internet Control Message Protocol) echo messages and their replies.

If the device pinged does not respond, there could be a problem in several areas. Figure 7-1 shows the path of a ping from the host computer to a site computer. If the site computer does not respond, trying to ping the other addresses may show that the problem is somewhere between the host computer and the site computer.

Figure 7-1. Troubleshoot by pinging several IP addresses



To verify that the IP stack in the current device is functioning properly, ping address 127.0.0.1. (The current device is the device that sends the ping message.)

7.1.2. Ping program operation

Ping is controlled by moving the cursor over the desired map icon, clicking the right mouse button, and selecting Ping. Alternatively, select a map icon and then select menu item Monitor -> Ping.

The Ping window is used to start/stop pings and set ping options. The bottom of the window shows the number of pings sent, the number of pings received, and the percentage of data lost. These numbers are reset to zero when a ping is started.

Start/Stop pings: This is a toggle operation that is selected by clicking the menu item Start or Stop, in the Ping window. Alternatively, click on the hexagon (stop-sign shaped) red (for stop) or green (for start) button.

If a response is received from the device, a message similar to the following will appear in the Ping window.

reply from 100.100.103.2: sequence = 0 round-trip time = 30 ms

round-trip min/avg/max = 30/30/30 ms

The first line includes the network address of the pinged device (100.100.103.2), the number of the ping (sequence = 0), and the time it took between when the ping was sent and the response was received (round-trip time = 30 ms). If the continuous option has been selected, the sequence number will increase for each ping.

The second line shows the minimum, average, and maximum times for round-trip.

If a device is pinged and no response is received, a message similar to the following will appear in the Ping window.

1 packet transmitted, 0 packets received 100% packet loss

Ping Options: Customize pings by selecting Options in the Ping window menu. If Continuous Operation is unselected (default), selecting Start ping will ping the device once. If Continuous Operation is selected, selecting Start ping will repeatedly ping the device until Stop ping is selected. Ping time out is set in milliseconds and defines the amount of time OpenView will wait for a response from the pinged device.

7.2. Alarm list for E.F. Johnson components

7.2.1. Repeater generated alarms

Simulcast Failure alarms are caused by alarms listed in the “Disable Simcst” column. Repeater Failure alarms are caused by alarms listed in the “RF Shutdown” column.

DBase ID numbers are the same as the Alarm ID numbers for active alarms. For cleared alarms, add 200 to the Alarm ID to get the DBase ID. Descriptions for alarms 1 to 4 can be entered in the EFJ Repeater Description dialog box.

Alrm ID	Disp	Led's	Alarm Description	Dig On/ Off	A/D Line	1/2 Pwr	Disable Simcst	RF Shut down	Causes For Alarm
0	0	4	Repeater in Test Mode	X					Repeater put in test
1	1	4	IAC Input 1	X					Value opposite of configuration
2	2	4	IAC Input 2	X					Value opposite of configuration
3	3	4	IAC Input 3		29				A/D value outside of trip range
4	4	4	IAC Input 4		30				A/D value outside of trip range
5	5	4	Reserved (5)	X					Old IAC card (same as 1)
6	6	4	Reserved (6)	X					Old IAC card (same as 1)
7	7	4	Reserved (7)	X					Old IAC card (same as 1)
8	8	4	Reserved (8)	X					Old IAC card (same as 1)
9	9	4	MAC Processor	X				X	Have not communicated with MAC in 20 seconds
10	A	4	HSDB Processor	X					Problems with the bus

Alrm ID	Disp	Led's	Alarm Description	Dig On/ Off	A/D Line	1/2 Pwr	Disable Simcst	RF Shut down	Causes For Alarm
11	B	4	IRDB Cable	X					Problems with the bus
12	C	4	RNT/CIM Channel Problem	X					Have not heard from CIM in up to 2.5 minutes. Consoles will not receive audio from the affected channel. The channel will still be operating, unless it was shut down by an automatic channel revert.
13	D	4	TIC Processor	X					Have not communicated with TIC in 20 seconds
14	E	4	SMC Processor	X			X		Have not communicated with SMC in 20 seconds
15	F	4	VNC	X					Have not communicated with VNC in 30 seconds
16	0	5	AC Power Fail	X		X			Pin on latch goes low indicating AC fail
17	1	5	Battery Power Fail		14			X	A/D value less than 183
18	2	5	Power Supply Thermal		28				A/D value greater than trip point
19	3	5	Fan 1 Current		13				Fan current not within spec
20	4	5	Fan 2 Current		12				Fan current not within spec
21	5	5	IAC Mismatch	X					IAC and eeprom parameters don't match
22	6	5	GPS 1 PPS	X			X		SMC has indicated the 1 PPS is gone
23	7	5	SMC Link	X			X		SMC link is gone - no data and audio
24	8	5	No A/D Samples	X	X			X	Not able to sample any of the A/D values
25	9	5	GPS 10 MHz	X			X		10 MHz reference is gone
26	A	5	Repeater in Setup State	X					Repeater setup state - ignore all flags
27	B	5	Reserved						
28	C	5	Reserved						
29	D	5	Reserved						
30	E	5	Reserved						
31	F	5	Reserved						
32	0	4,5	RF Shutdown (several modes)	*X					See RF shutdown column
33	1	4,5	RF Half Power Mode	*X					See half power column
34	2	4,5	Thermal Sense in RF Portion		22	X		X	A/D value greater than trip point
35	3	4,5	RF Finals 1 and 2		17 & 18	X		X	Power values below 40 or spread is too far

Alrm ID	Disp	Led's	Alarm Description	Dig On/ Off	A/D Line	1/2 Pwr	Disable Simcst	RF Shut down	Causes For Alarm
36	4	4,5	RF Finals 3 and 4		19 & 20	X		X	Power values below 40 or spread is too far
37	5	4,5	RF VSWR		16 & 21	X			Fwd Power is < reflected or ratio is too much
38	6	4,5	Normal Synthesizer Tx Lock	X				X	Lock line is low 8 of 8 reads
39	7	4,5	Normal Synthesizer Rx Lock	X					Lock line is low 8 of 8 reads
40	8	4,5	HS Synthesizer Tx Lock	X				X	Lock line is low 8 of 8 reads
41	9	4,5	HS Synthesizer Rx Lock	X					Lock line is low 8 of 8 reads
42	A	4,5	RF Quarter Power	X					High Power only; 2 of the 4 finals are blown
43	B	4,5	Reserved						
44	C	4,5	Reserved						
45	D	4,5	Reserved						
46	E	4,5	Reserved						
47	F	4,5	Repeater Disabled						Op_mode flag in EE trig by columns 8&9

* Triggers based on other alarms

7.2.2. Site/Channel computer generated alarms

DBase ID	Alarm ID	Alarm Status	Alarm Description	Causes For Alarm
400	0	Active	SCS in Test Mode	Doesn’t have a repeater associated with it
401	1	Active	SIB Link Alarm	Has a repeater ID associated with it
402	2	Active	Simulcast Failure	Repeater can’t simulcast
403	3	Active	Repeater Failure	Repeater can’t operate
404	4	Active	Site Reverted	SCS performed a site revert
405	5	Active	Unable to configure repeater	Unable to configure a repeater
406	6	Active	Unconfigured Repeater	SCS knows of a repeater that wasn’t configured by the host computer
600	0	Cleared	SCS in Test Mode	Doesn’t have a repeater associated with it
601	1	Cleared	SIB Link Alarm	Has a repeater ID associated with it
602	2	Cleared	Simulcast Failure	Repeater can’t simulcast
603	3	Cleared	Repeater Failure	Repeater can’t operate
604	4	Cleared	Site Reverted	SCS performed a site revert
605	5	Cleared	Unable to configure repeater	Unable to configure a repeater
606	6	Cleared	Unconfigured Repeater	SCS knows of a repeater that wasn’t configured by the host computer

7.2.3. Host Computer generated alarms (for the Site/Channel computers)

DBase ID	Alarm ID	Alarm Status	Alarm Description	Causes For Alarm
800	NA	NA	HC-SCS Network Link Established	Site Computer connected
801	NA	NA	HC-SCS Network Link Lost	Site computer disconnected from the host computer
802	NA	NA	HC-SCS Connection Attempt Failed	Unable to connect to the site computer

7.2.4. Host Computer generated alarms (for the repeaters)

DBase ID	Alarm ID	Alarm Status	Alarm Description	Causes For Alarm
1000	NA	NA	Repeater Restarted	Received Opcode 37 (Repeater Restart Msg)
1001	NA	NA	SMC Configuration Finished	The SMC was successfully configured
1002	NA	NA	SMC Configuration Failed	The SMC could not be configured
1003	NA	NA	Repeater Configuration Finished	The repeater was successfully configured
1004	NA	NA	Calibration Write Failed	Unable to configure all repeaters
1005	NA	NA	Calibration Write Finished	All repeaters successfully configured

7.2.5. Host Computer generated alarms (for a system)

DBase ID	Alarm ID	Alarm Status	Alarm Description	Causes For Alarm
1200	NA	NA	Channel Reverted	A channel in this system was reverted
1201	NA	NA	Channel Unreverted	A channel in this system was unreverted

7.3. Mnemonics

A/D - Analog to Digital

CIM - Channel Interface Module

GPS - Global Positioning System

HC - Host Computer

HSDB - High-Speed Data Bus

IAC - Interface Alarm Card

IP - Internet Protocol

IRDB - Inter-Repeater Data Bus

MAC - Main Audio Card

MAC address - Media Access Control address

MBC - Message Bridge Card

PPS - Pulse Per Second

RNT - Radio Network Terminal

SCS - Site Controller Station or Site/Channel computer

SIB - Serial Interface Bus

SMC - Simulcast Modulation Card

SNMP - Simple Network Management Protocol

TCP - Transmission Control Protocol

TIC - Telephone Interface Card

VNC - Viking Network Controller

Index