

Network Management

for Simulcast

Service Manual

Copyright © 1997 by the E.F. Johnson Company

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.

Viking Head/EF Johnson logo and Multi-Net® are registered trademarks of the E.F. Johnson Company. All other company and/or product names used in this manual are trademarks and/or registered trademarks of their respective manufacturer.

This software and documentation are based in part on HP OpenView® under license from Hewlett-Packard Company. HP OpenView is a registered trademark of the Hewlett-Packard Company.

Information in this manual is subject to change without notice.

Table of Contents

1. Introduction	1-1
1.1. Scope of manual.....	1-1
1.2. Conventions.....	1-1
1.3. Definition of terms.....	1-1
2. Network Structure	2-1
2.1. Network equipment	2-1
2.2. Site types.....	2-2
2.3. Logical addresses	2-9
2.3.1. IP address overview	2-9
2.3.2. E.F. Johnson method	2-10
2.3.3. IP addressing example	2-11
2.3.4. Subnet assignments	2-13
2.3.5. IP address assignments	2-15
2.4. Unique host names.....	2-17
2.5. Passwords.....	2-18
2.5.1. Router passwords.....	2-18
2.5.2. Windows® NT passwords	2-18
2.5.3. OpenView passwords.....	2-18
3. Router Configuration	3-1
3.1. Equipment setup.....	3-1
3.2. Configuration	3-1
4. Site/Channel Computer Configuration	4-1
4.1. Install Ethernet card	4-1
4.2. Equipment setup.....	4-1
4.3. Configure Windows NT 3.51	4-2
4.3.1. Mouse configuration	4-2
4.3.2. Enter a password.....	4-3
4.3.3. Install Windows networking	4-3
4.3.4. Edit the LMHOSTS file	4-4
4.3.5. Change the passwords.....	4-5
4.3.6. Change the system information through the Control Panel	4-6
4.3.7. Change the system information in Windows NT Registry	4-8
4.4. Install site controller application.....	4-10
4.4.1. Install the application	4-10
4.4.2. Set the start up application	4-10
4.4.3. Configure for no mouse	4-10

5. Host Computer Configuration	5-1
5.1. Install Ethernet card	5-1
5.2. Equipment setup.....	5-1
5.3. Configure Windows NT 4.0	5-2
5.3.1. Log on to Windows NT	5-2
5.3.2. Set CD properties	5-2
5.3.3. Install Windows networking	5-3
5.3.4. Edit the LMHOSTS file	5-4
5.3.5. Change the passwords.....	5-5
5.3.6. Change the system information through the Control Panel	5-6
5.3.7. Change the system information in Windows NT Registry	5-7
5.4. Install OpenView Professional Suite.....	5-9
5.5. Install host computer application	5-9
5.6. Create OpenView maps.....	5-11
5.6.1. Create a System map.....	5-11
5.6.2. Create a Site map.....	5-13
5.6.3. Create a Device map.....	5-14
5.6.4. Add lines and text	5-16
5.6.5. Set the default map	5-17
5.6.6. Protect the map	5-17
5.6.7. Format for background maps	5-17
5.6.8. Options for map creation	5-17
5.7. Edit site and system settings	5-18
5.8. Configure OpenView polling.....	5-19
5.8.1. Add devices to polling list	5-19
5.8.2. Set polling defaults	5-20
5.8.3. Verify polling settings.....	5-20
5.9. Configure OpenView traps.....	5-20
5.10. Set OpenView passwords.....	5-21
5.10.1. Log in passwords.....	5-21
5.10.2. Protect maps password	5-21
5.10.3. SNMP passwords	5-22
5.11. Service functions.....	5-22
5.12. Configure Windows NT 3.51	5-23
5.12.1. Enter a password.....	5-23
5.12.2. Install Windows networking	5-23
5.12.3. Edit the LMHOSTS file	5-25
5.12.4. Change the passwords.....	5-26
5.12.5. Change the system information through the Control Panel	5-27
5.12.6. Change the system information in Windows NT Registry	5-28
5.13. Install OpenView Work Group Node Manager.....	5-30
5.14. Other files.....	5-31
5.14.1. Install additional files	5-31
5.14.2. Modify DEVICES	5-31

6. Installation	6-1
6.1. MBC in repeaters	6-1
6.2. MBC in channel controllers	6-1
6.3. MBC configuration.....	6-4
6.3.1. Flash code into MBC	6-4
6.3.2. Configure MBC	6-4
6.4. Site computer to repeater	6-4
6.5. Channel computer to channel controller	6-5
6.6. Router to site/channel computer	6-5
6.7. Hub to site/channel computer	6-6
6.8. Hub to host computer	6-7
6.9. Router to host computer	6-8
6.10. Hub to router	6-8
6.11. Router to channel bank.....	6-9
7. Alignment and Calibration.....	7-1
7.1. Align threshold and timing tone gain	7-1
7.1.1. Alignment procedure	7-1
7.1.2. Alignment icons	7-2
7.2. Calibrate uni-directional, non-redundant systems	7-4
7.2.1. Data acquisition procedure (uni-directional)	7-5
7.2.2. Data acquisition icons for uni-directional	7-6
7.2.3. Write procedure (uni-directional)	7-8
7.3. Calibrate bi-directional, non-redundant systems	7-8
7.3.1. Phase 1 data acquisition (bi-directional)	7-9
7.3.2. Phase 2 data acquisition (bi-directional)	7-10
7.3.3. Data acquisition icons for bi-directional	7-10
7.3.4. Write procedure (bi-directional)	7-13
7.4. Determine and set overlap offset	7-13
7.4.1. Description of overlap offset	7-13
7.4.2. Determine overlap offset values	7-14
7.4.3. Set overlap offset values and recalibrate system	7-15
7.5. Set SMC parameters from OpenView	7-16
7.5.1. Read/Write parameters	7-17
7.5.2. Audio Gain.....	7-18
7.5.3. Data Gain	7-18
7.5.4. Pilot Tone Gain.....	7-18
7.5.5. Threshold	7-18
7.5.6. Timing Tone Gain	7-19
7.5.7. Buffer Delays section.....	7-19
8. Update Software	8-1
8.1. Update site controller application (Windows NT 4.0)	8-1

8.2. Uninstall host computer software (Windows NT 4.0)	8-2
8.3. Update site controller application (Windows NT 3.51)	8-3
8.4. Uninstall host computer software (Windows NT 3.51)	8-4
8.5. Install host computer software (Windows NT 3.51).....	8-5
8.6. Remove host computer software (Windows NT 3.51)	8-5
8.7. Install Windows NT 4.0.....	8-6
9. Troubleshooting	9-1
9.1. Ping troubleshooting techniques.....	9-1
9.2. Troubleshooting from a router	9-1
9.2.1. Show ARP - list of IP address in subnet	9-2
9.2.2. Show hosts - list of host names and IP addresses	9-2
9.2.3. Show IP route - list of known subnets and routes.....	9-2
9.2.4. Show int - information on ports	9-4
9.2.5. Ping from router.....	9-4
9.2.6. Telnet from router	9-5
9.3. Troubleshooting from a host computer.....	9-5
9.3.1. Ping from OpenView.....	9-5
9.3.2. Ping from Command Prompt	9-6
9.3.3. Telnet from computer	9-7
9.4. Recovery (Reverts) setup and actions.....	9-7
9.4.1. Consider interference problems.....	9-8
9.4.2. Consider status channel and home channel access.....	9-8
9.4.3. Configure automatic channel reverts	9-10
9.4.4. Manually unvert and revert channels.....	9-10
9.4.5. Channel unvert examples.....	9-11
9.4.6. Configure inputs for automatic site reverts	9-12
9.4.7. Configure actions for automatic site reverts	9-13
9.4.8. Manually unvert and revert sites.....	9-14
9.4.9. Site revert example.....	9-14
9.5. Perform manual repeater control	9-19
9.5.1. Repeater menu.....	9-20
9.6. Alarm list for E.F. Johnson components.....	9-20
9.6.1. Repeater generated alarms	9-20
9.6.2. Site/Channel computer generated alarms	9-22
9.6.3. Host Computer generated alarms (for the site/channel computers)	9-23
9.6.4. Host Computer generated alarms (for the repeaters)	9-23
9.6.5. Host Computer generated alarms (for a system).....	9-23
9.7. Mnemonics.....	9-24

Frequency Charts

SECTION

1. Introduction**1.1. Scope of manual**

This manual covers configuration and installation of network management equipment (devices).

The configuration process defines a logical network. Each port of each device is assigned a unique IP (Internet protocol) address, which is used to route information (messages). If IP addresses are not assigned properly, messages may not get to their destination and the purpose for the network could be adversely affected.

For information to get from one device to another, there must be a physical path (for example, a wire or an RF link). The layout of the physical paths between devices influences the assignment of addresses. This manual first covers the relationship between the logical and physical, then covers specific configuration and installation information.

1.2. Conventions

<Enter> refers to the enter or return key on the computer keyboard.

< > Other information in angle brackets is a definition of variable information. For example, <password> means to type a password, without the angle brackets.

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.

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 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.

SECTION

2. Network Structure

2.1. Network equipment

Network management equipment consists of

- routers
- computers
- hubs
- MBCs (message bridge cards)
- cables that wire these devices together

A router is installed at every site. (The master site may require more than one router.) The router is connected to the computer(s) at the site and to the channel bank(s). Routers keep track of how to forward messages to their destinations and either send the message to a computer at the site or send the message to another site by way of a channel bank.

Computer(s) are installed at every site. There are three types of computers in an E.F. Johnson network system - host, site, and channel. The host computer runs software that receives alarm messages from the system and displays them on the screen to inform the operator of the system's status. There is normally only one host computer in a system, although there could be more. Site computers send messages between the repeaters and the host computer. Each repeater site has a site computer. A channel computer sends messages between the channel controller and the host computer. There is one channel computer in a system.

Hubs act as signal splitters. If there is more than one computer or router at a site, a hub is needed.

MBCs are installed in repeaters and channel controllers. Each stack of repeaters or channel controllers has one MBC. An MBC reports repeater or channel controller status to the site or channel computer.

Several types of cables are used to connect these devices together. Null Ethernet® (crossover) cables connect routers and computers together. Standard (straight-through) Ethernet cables connect routers and computers to hubs. Serial cables connect MBCs to site and channel computers. RS-449 cables connect routers to channel banks.

The site and channel computers are rack mounted and do not have keyboards or monitors. (Keyboards and monitors are offered as options.) Routers are also rack mounted. The cables that connect the routers to the channel banks are only 10 feet long. The cables from the routers to the computers or hub can be up to 328 feet long. Cables between computers and MBCs can be up to 50 feet long. Adapters between cable connectors and device connectors may also be needed.

See Section 6 for installation information.

2.2. *Site types*

There are three basic types of sites, although variations will exist.

- **Master site:** The master site contains a router, a channel computer, and channel controllers. It may be collocated with a site computer and repeaters. In addition, it may also contain a host computer. If there is more than one computer or router, the master site also contains a hub. There is only one master site per system.
- **Remote site:** A remote site contains a router, a site computer, and repeaters. It may also contain a host computer, in which case a hub will be needed. There will normally be several remote sites.
- **Monitoring point site:** The monitoring point contains a router and a host computer. This site is remotely located; it is at a site without repeaters or a channel controller. This site does not always exist if a host computer is at a master or remote site.

Figure 2-1 shows a full master site and a typical remote site (although each site may have additional channel banks, routers, repeaters, and channel controllers).

Figure 2-2 shows a master site without a host computer. The host computer is shown at a typical monitoring point. A typical remote site is also shown.

Figure 2-3 shows a minimal master site and a remote site that also contains the host computer. Other remote sites in this system would be like the typical remote sites in Figures 2-1 and 2-2.

If there are several channel banks at a site, the router will be a multi-port router or there will be more than one router. Each channel bank is wired to a different port of a router, as shown in Figure 2-4. It is important that the correct ports are used. See Section 6.11 for router to channel bank cable installation.

Figure 2-1. Full master site with typical remote site

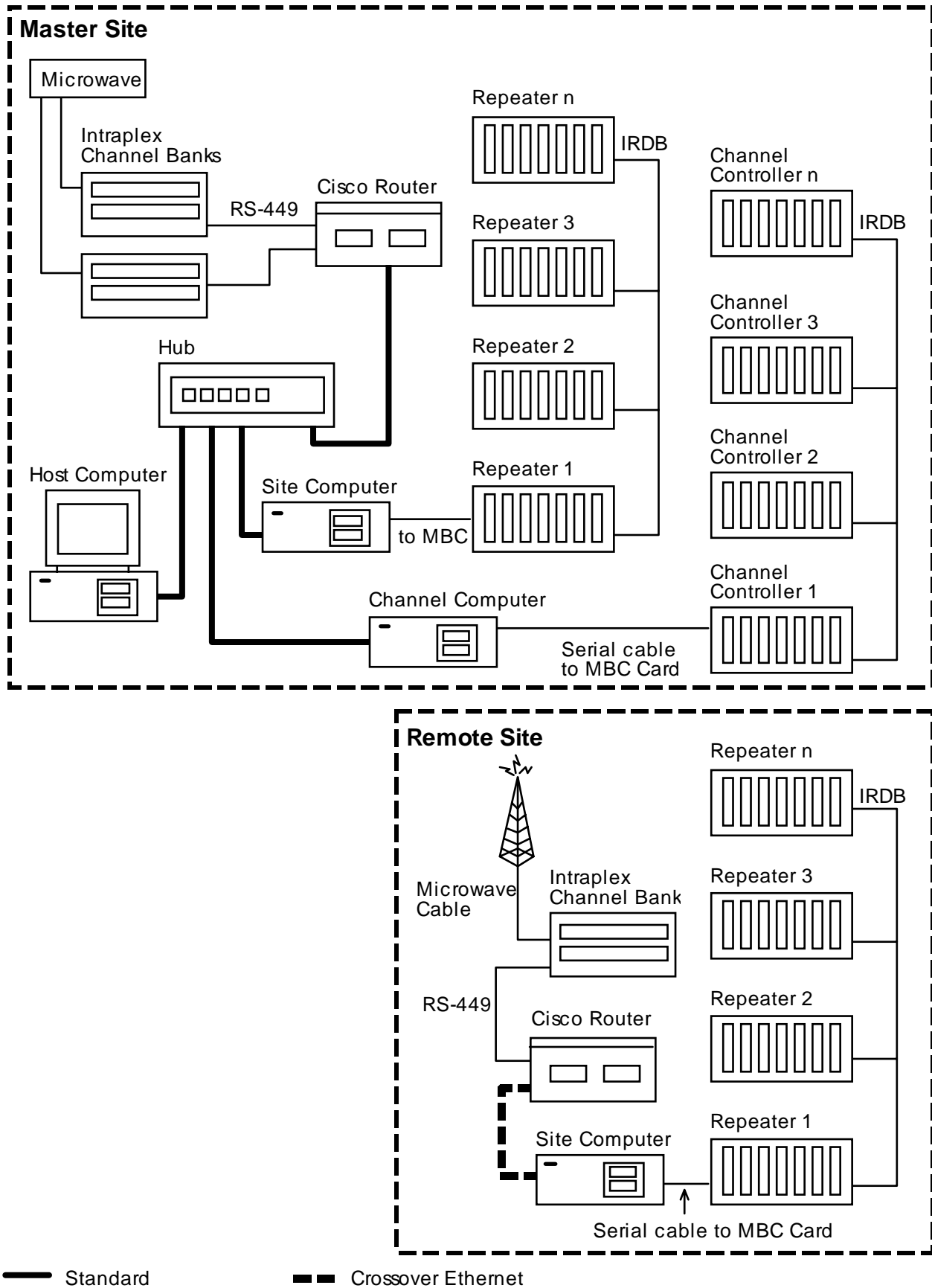


Figure 2-2. Master site, monitoring point, and remote site

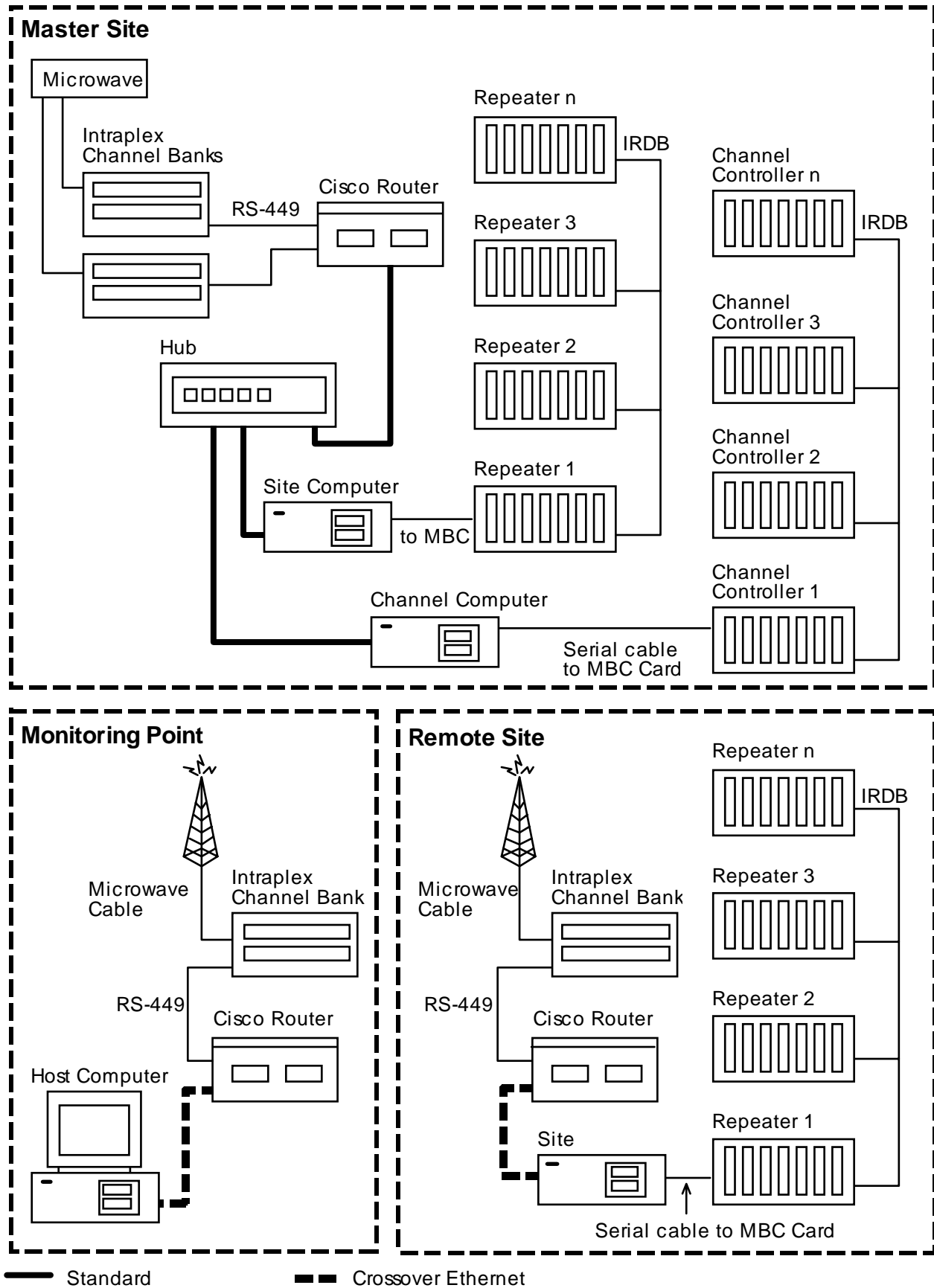


Figure 2-3. Minimal master site and remote site with host computer

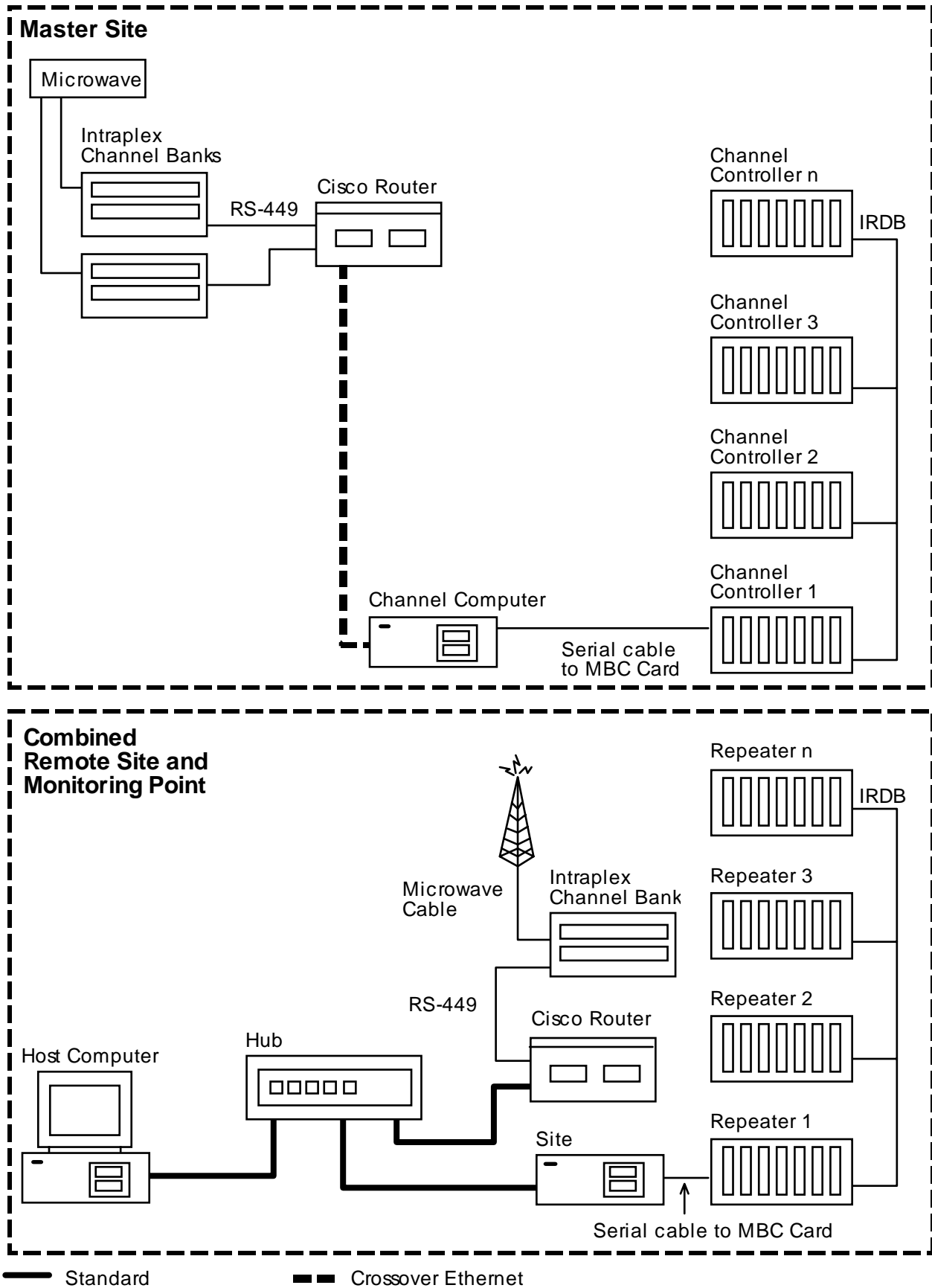
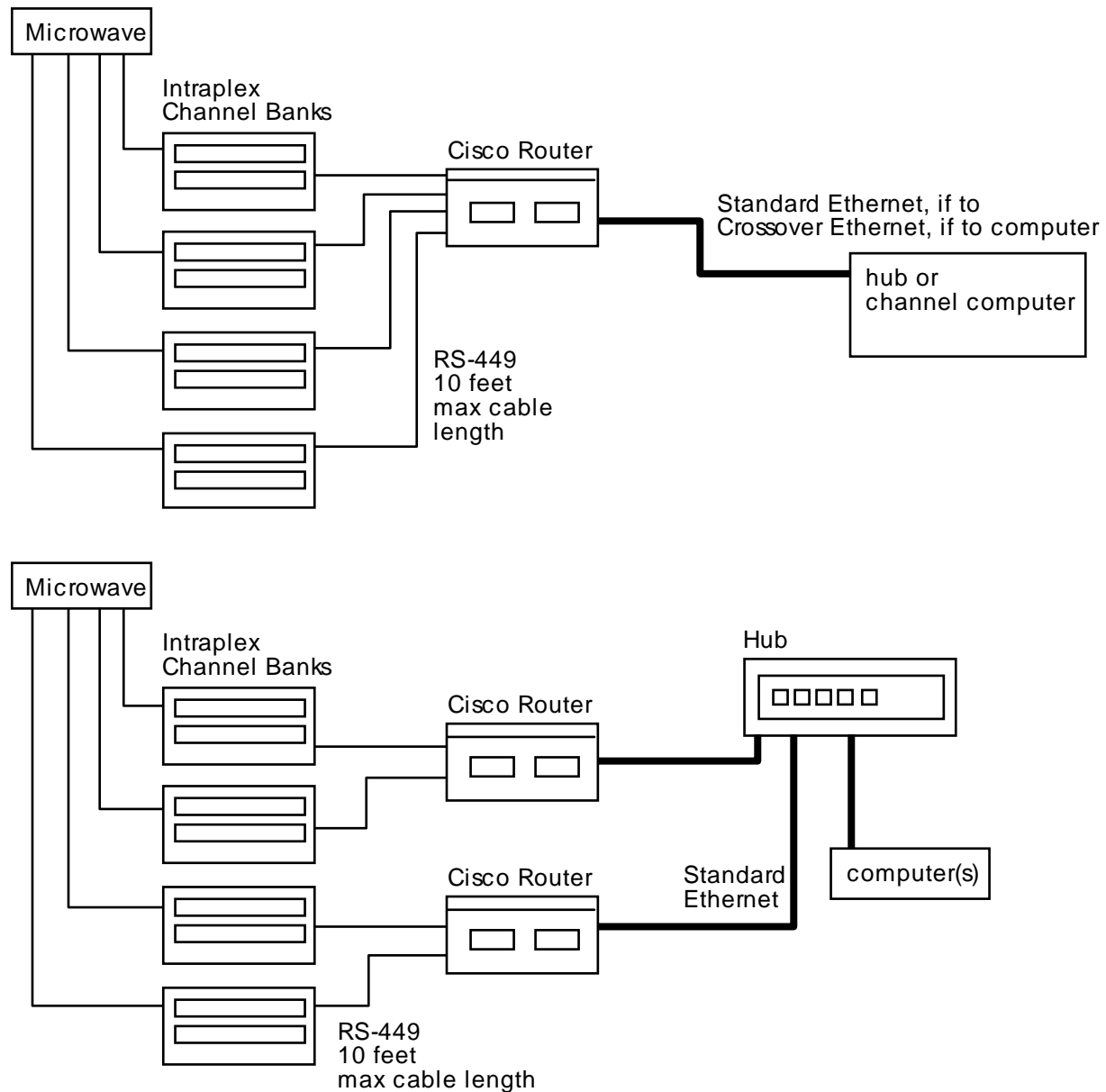


Figure 2-4. Each port of a router connects to a different channel bank

2.3. Logical addresses

2.3.1. IP address overview

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 must 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 must 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).

2.3.2. E.F. Johnson method

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 devices within a site 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 devices within a site. Inter-site backbone links are often microwave or some other long-distance carrier; links that connect site devices are typically connected by Ethernet cabling.

Standard subnet assignments:

Links within sites

200 - Monitoring Point subnet

201 - Master site subnet

202 - Remote site subnet

203 - Remote site subnet

etc.

If there are additional monitoring points, they are assigned remote site subnet numbers.

Links between sites (inter-site backbone links)

100 - Backbone between master site and monitoring point

102 - Backbone between master site and subnet 202

103 - Backbone between master site and subnet 203

etc.

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.

2.3.3. IP addressing example

Figure 2.5 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:

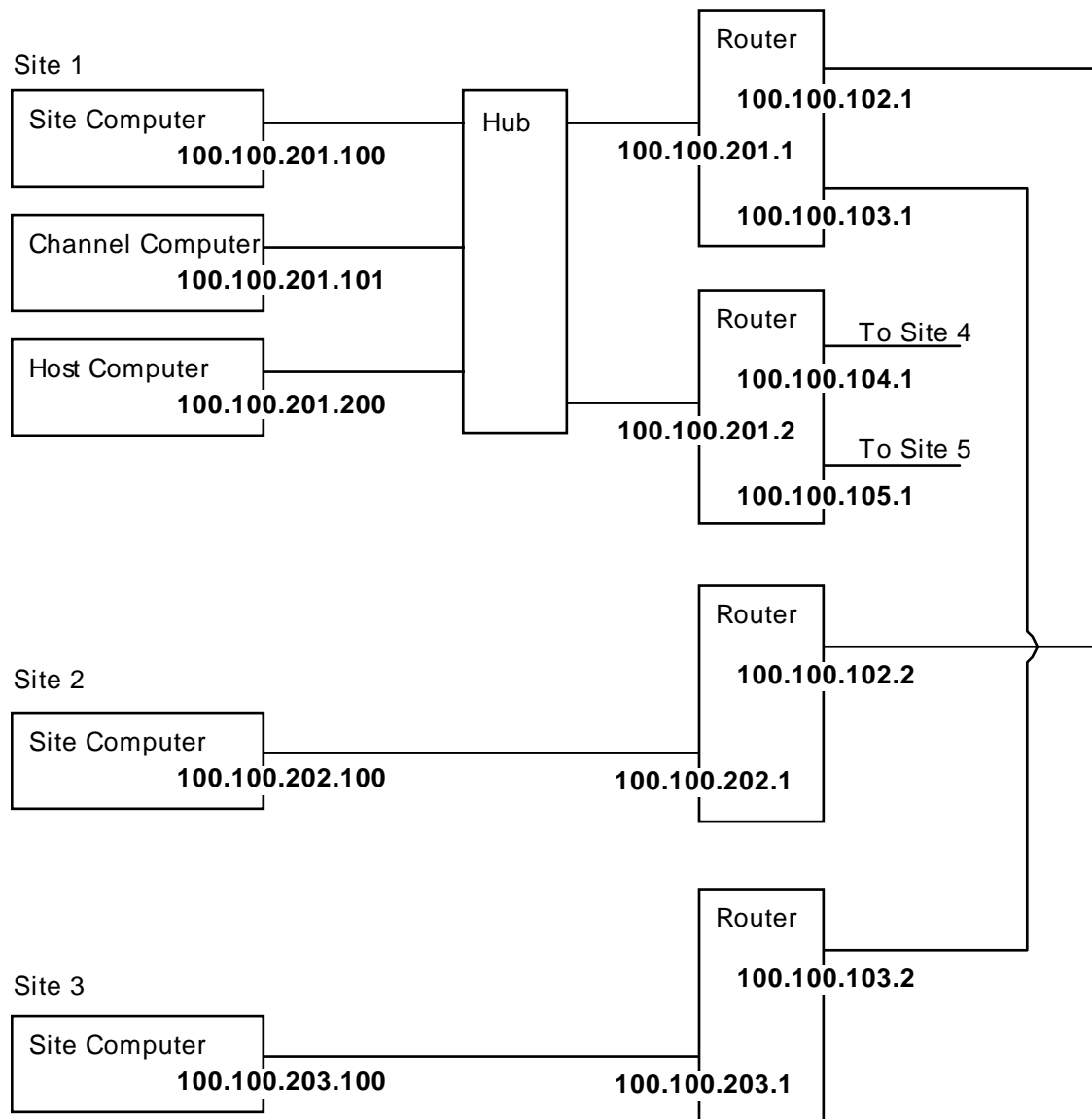
- 201 is the link within site 1
- 202 is the link within site 2
- 203 is the link within site 3
- 102 is the backbone link between site 1 and site 2
- 103 is the backbone link between site 1 and site 3
- 104 is the backbone link between site 1 and site 4
- 105 is the backbone link between site 1 and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

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.

Figure 2-5. IP addresses



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 addresses are 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 addresses unique. Expansion to site 4 and 5 would be the same.

2.3.4. Subnet assignments

Routers and computers communicate with each other by addressing messages to IP addresses. Before assigning IP addresses, determine which equipment has direct communications with other equipment. It is often helpful to draw a picture of the sites and the inter-site links (backbones); then, assign a subnet number to each site and to each backbone.

Begin by assigning subnet 201 to the master site (the site with the channel controllers). If there is a separate monitoring point, assign it subnet 200. Then, number the rest of the sites consecutively beginning with 202, 203, etc. Assign backbone links with a 100 series number that corresponds to the remote subnet. For example, assign subnet 102 to the link that is between the master site and subnet 202. Assign 103 to the link between the master site and subnet 203, etc.

Figure 2-6 shows a drawing for a 3-site system. This drawing represents the system in the example in Section 2.3.3. Figure 2-7 shows the same system with a remote monitoring point.

Figure 2-6. Three-site system

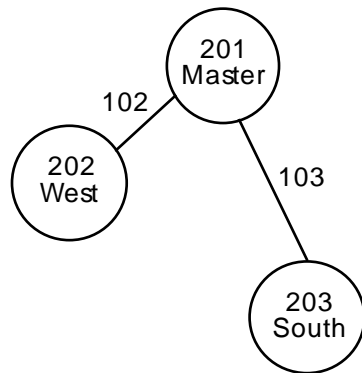
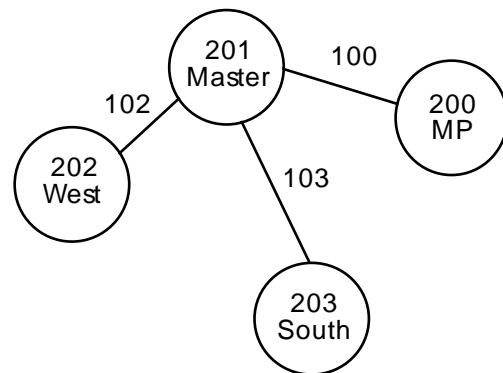


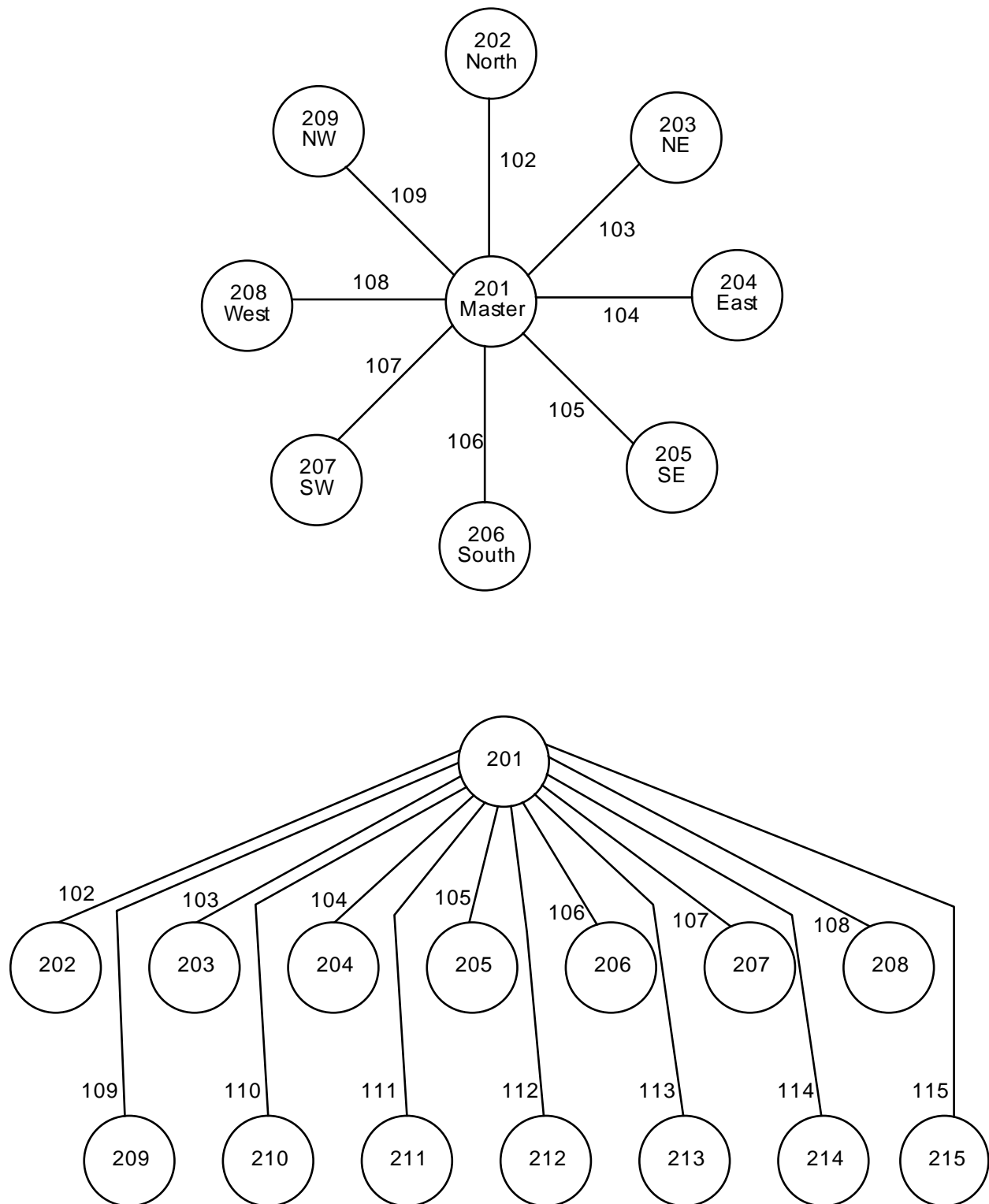
Figure 2-7. Three-site system with monitoring point



In these drawings, the sites have also been given names for human convenience. The network devices do not use the names, but people often remember names easier than numbers. In some situations the network devices will allow use of a name instead of a number, as long as the relationship between the name and number have been configured in the device.

Figure 2-8 shows examples of two systems with even more remote sites.

Figure 2-8. Subnet drawings



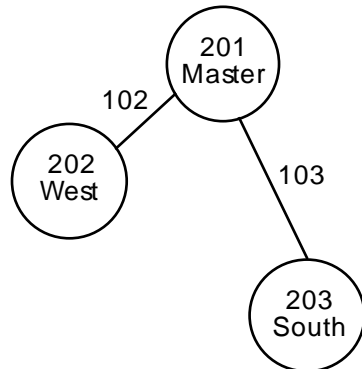
2.3.5. IP address assignments

After the subnets are assigned, then assign an IP address to each port of the routers and to each network port of the computers (using the method described in Section 2.3.2). The IP address is written as four numbers, such as 100.100.201.100. The first number should always be 100. The second number should be different for each system that E.F. Johnson installs. The third number is the subnet number that was assigned in Section 2.3.4 .

Within a subnet, the fourth number is assigned as follows:

- Router ports are assigned numbers sequentially starting with 1. (The Ethernet port of a router belongs to the subnet of the site. The serial ports of a router belong to subnets that are backbone links to other sites.)
- Site/Channel computers are assigned numbers sequentially starting with 100.
- Host computers are assigned numbers sequentially starting with 200.

The following chart shows the IP address for a three-site system.

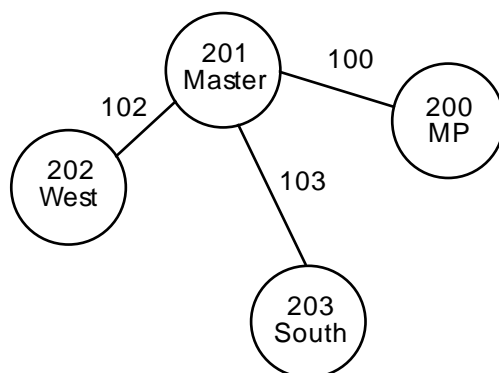


	IP address	Notes
Master Site		
Router serial 0	100.100.102.1	subnet to West Site subnet to South Site
Router serial 1	100.100.103.1	
Router Ethernet	100.100.201.1	
Site computer	100.100.201.100	
Channel computer	100.100.201.101	
Host computer	100.100.201.200	
West Site		
Router serial 0	100.100.102.2	subnet to Master Site
Router serial 1		
Router Ethernet	100.100.202.1	
Site Computer	100.100.202.100	
South Site		

NETWORK STRUCTURE

Router serial 0	100.100.103.2	subnet to Master Site
Router serial 1		
Router Ethernet	100.100.203.1	
Site Computer	100.100.203.100	

The following chart shows the IP addresses for a system with three sites plus a remote monitoring site.



	IP address		IP address
Master Site			
Router serial 0	100.100.102.1		
Router serial 1	100.100.103.1	South Site	
Router serial 2	100.100.100.1	Router serial 0	100.100.103.2
Router Ethernet	100.100.201.1	Router serial 1	
Site computer	100.100.201.100	Router Ethernet	100.100.203.1
Channel computer	100.100.201.101	Site Computer	100.100.203.100
West Site		Monitoring Point	
Router serial 0	100.100.102.2	Router serial 0	100.100.100.2
Router serial 1		Router serial 1	
Router Ethernet	100.100.202.1	Router Ethernet	100.100.200.1
Site Computer	100.100.202.100	Host computer	100.100.200.200

The master site router in the above chart has at least three serial ports. However, it could be done with two two-port routers, in which case the addresses would be as shown in the following chart.

	IP address	Notes
Master Site		
Router 1 serial 0	100.100.102.1	to West Site
Router 1 serial 1	100.100.103.1	to South Site
Router 2 serial 0	100.100.100.1	to Monitoring Point

Router 2 serial 1	
Router 1 Ethernet	100.100.201.1
Router 2 Ethernet	100.100.201.2
Site computer	100.100.201.100
Channel computer	100.100.201.101

2.4. Unique host names

Since it is often easier to remember names instead of numbers, the computers and routers allow the assignment of names to devices and to IP addresses. These names will be entered when asked for a host name, computer name, device name, or similar wording. The names can also be associated with IP addresses by using the router's ip host command and by editing the computer's files named lmhosts and hosts (stored in the \winnt\system32\drivers\etc\ directory). Then, the names can be used instead of IP addresses for commands like ping and telnet.

Each device is given a unique name. Names are normally based on the site's geographic location, such as city, section of county, etc. The following standard should be used to differentiate devices at a site, where "name" is the geographic location.

Name	Assigned to
name	Router
name-hub	Site computer
name-chn	Channel computer
name-hst	Host computer

If there are two routers at a site, add a number at the end of the name, for example, chicago1, chicago2, etc.

The maximum length of the entire name is 15 characters, that leaves 11 characters for the name portion in the above standard. For consistency, enter all names in lower case, since they are case sensitive.

Routers have several addresses, but only one name. If a device needs to have an address associated with a router's name, the router's address that communicates to the device should be used.

For example, if waseca is the name of a multi-port router using addresses:

100.100.102.1 to talk to the west site

100.100.103.1 to talk to the south site

100.100.201.1 to talk to the local subnet

Devices at the west site will associate the name waseca with address 100.100.102.1. Devices at the south site will associate the name waseca with the address 100.100.103.1. Devices that are part of the local subnet will associate waseca with address 100.100.201.1.

2.5. Passwords

Passwords are case sensitive. For consistency, enter all passwords in lower case unless specifically told otherwise. This section lists the passwords that will need to be entered during configuration.

2.5.1. Router passwords

Routers use several passwords for different purposes. Normally the passwords are all set the same. Except for SNMP community password ro, which is set to “public” and corresponds to the SNMP community password in OpenView.

- Enable secret (encrypted by the router)
- Enable password (provides security)
- Virtual terminal password (used when connecting from attached terminal)
- Line con password (used when telnetting from someplace on the network)
- SNMP community password ro (read only)
- SNMP community password rw (read/write)

2.5.2. Windows® NT passwords

Passwords for Windows NT have a maximum length of 14 characters and can not contain spaces.

- E.F. Johnson username and log-on password
- Administrator username and log-on password

2.5.3. OpenView passwords

- Observer log in password (access to very few functions)
- Operator log in password (access to functions in Operator Manual)
- Supervisor log in password (access to all functions)
- Protect maps password (makes maps read-only)
- SNMP Community password (read only)
- SNMP Set Community password (read/write)

SECTION

3. Router Configuration

3.1. Equipment setup

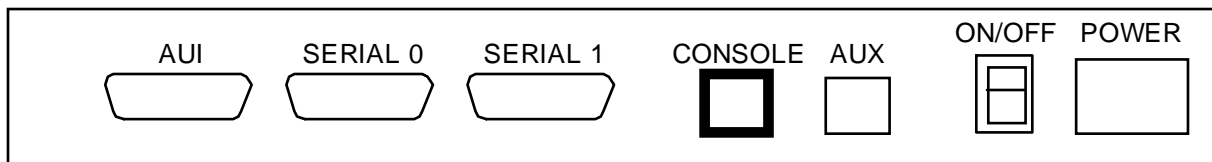
The router is configured by connecting a computer to the router and running a terminal (communications) program, such as Procomm Plus, on the computer.

Plug a serial cable into the computer's serial port and into the console port of the router (see Figure 3-1). The Auxiliary/Console Port Cable Kit (Cisco® Part No. 72-0803-02, E.F. Johnson Part No. 585-1156-053) contains an RJ-45 to RJ-45 rollover serial cable and DB adapters.

Start the terminal program on the computer before turning on the power to the router. Set the terminal program's communications parameters to 9600, N, 8, 1.

Turn the router's power on. The router will begin sending a sign-on message to the computer.

Figure 3-1. Router back panel (Cisco 2501)



3.2. Configuration

Router configuration involves answering questions that the router asks and then sending specific set-up commands to the router. Below is a sample configuration with explanations. (This sample is from the Cisco 2501 router, other routers may have different wording, but the commands should be the same.) The information that needs to be entered is shown as **bold**; information that the router displays is shown as lighter.

When **<Enter>** is shown, press the enter key to accept the default answer. Other information that is in angle brackets **< >** is a description of the information that needs to be entered. For example, **<ip address>** means to enter the required IP address, such as 100.100.103.1.

When the router is turned on, it sends several paragraphs of sign-on and legal information.

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
2500 processor with 1024 Kbytes of main memory
```

```
F3: 3072444+66260+202400 at 0x3000060
```

```
Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
```

ROUTER CONFIGURATION

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 10.3(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 30-Jan-96 20:37 by vatran
Image text-base: 0x0301B110, data-base: 0x00001000

cisco 2500 (68030) processor (revision D) with 1024K/1024K bytes of memory.
Processor board serial number 02348730
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY)

Notice: NVRAM invalid, possibly due to write erase.
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['.

Would you like to enter the initial configuration dialog? [yes]: **<Enter>**

First, would you like to see the current interface summary? [yes]: **<Enter>**

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	unassigned	NO	not set	up	down
Serial0	unassigned	NO	not set	down	down
Serial1	unassigned	NO	not set	down	down

Configuring global parameters:

Enter host name [Router]: **<unique name for this router>**

See Section 2.4. This name will also be used for the router's prompt.

The enable secret is a one-way cryptographic secret used instead of the enable password when it exists.

Enter enable secret: **<secret password>**

The enable password is used when there is no enable secret and when using older software and some boot images.

Enter enable password: **<enable password>**

% Please choose a password that is different from the enable secret

The router cautions that the same password for both secret and enable has been entered. Next, the router requests that the enable password be re-entered, in case the two passwords should not be the same.

Enter enable password: **<enable password>**

Enter virtual terminal password: **<virtual terminal password>**

Configure SNMP Network Management? [yes]: **<Enter>**

Community string [public]: **<Enter>**

Configure IP? [yes]: **<Enter>**

Configure IGRP routing? [yes]: **<Enter>**

Your IGRP autonomous system number [1]: **<Enter>**

Configuring interface parameters:

Configuring interface Ethernet0:

Is this interface in use? [yes]: **<Enter>**

Configure IP on this interface? [yes]: **<Enter>**

IP address for this interface: **<ip address>**

Number of bits in subnet field [0]: **16**

Class A network is 100.0.0.0, 16 subnet bits; mask is 255.255.255.0

Configuring interface Serial0:

Is this interface in use? [yes]: **<Enter>**

Configure IP on this interface? [yes]: **<Enter>**

Configure IP unnumbered on this interface? [no]: **<Enter>**

IP address for this interface: **<ip address>**

Number of bits in subnet field [16]: **<Enter>**

Class A network is 100.0.0.0, 16 subnet bits; mask is 255.255.255.0

Configuring interface Serial1:

Is this interface in use? [yes]:

If a device will be attached to this serial port, follow the same procedure as for serial port 0 above. If no device will be attached, enter No.

Note: If the router has additional serial ports, continue to enter the required information.

The following configuration command script was created:

```
hostname <unique name for this router>
enable secret 5 $1$uFlL$7l8EALcmq4KBmtwZtSetj/
enable password <enable password>
line vty 0 4
password <virtual terminal password>
snmp-server community public
!
ip routing
!
interface Ethernet0
ip address <ip address> 255.255.255.0
!
interface Serial0
ip address <ip address> 255.255.255.0
!
interface Serial1
ip address <ip address> 255.255.255.0
!
router igrp 1
network 100.0.0.0
!
end
```

Use this configuration? [yes/no]: **yes**

The enable password you have chosen is the same as your enable secret.

This is not recommended. Re-enter the enable password.

Building configuration...

Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down

ROUTER CONFIGURATION

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to down
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINK-3-UPDOWN: Interface Serial1, changed state to down
%SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 10.3(9), RELEASE SOFTWARE (fcl)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 30-Jan-96 20:37 by vatran <Enter>
```

```
oc-rtr>enable
```

```
Password: <enable password>
```

When this password is entered, it is not displayed on the screen.

```
oc-rtr#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
oc-rtr(config)#banner \<text>\
```

Example: banner \EF Johnson Operations Center Cisco Router\

The text defines a sign-on message for this router and should indicate the location of the router. A separator must be used before and after this text. In this example the backslash (\) character is the separator. The separator can be any character that is not used in the text and the same separator must be used at the beginning and ending of the text.

```
oc-rtr(config)#clock timezone <zone abbreviation> <hours from UTC>
```

Example: clock timezone CST -6

Enter the standard time zone for the location that the router will be installed and the offset from UTC (GMT, Zulu). Minutes may also be entered if necessary.

Eastern Standard Time: EST -5

Central Standard Time: CST -6

Mountain Standard Time: MST -7

Pacific Standard Time: PST -8

```
oc-rtr(config)#clock summer <zone> recurr <week> <day> <month> <hr:min> <week> <day>
<month> <hr:min> <offset>
```

Example: clock summer CDT recurr first Sunday April 02:00 last Sunday October 02:00 60

This command sets automatic adjustment for daylight savings time.

<zone> Time zone for summer time (for U.S.A., EDT, CDT, MDT, or PDT)

<week> Week of the month (first, last, or 1 to 5)

<day> Day of the week (Sunday, Monday, etc.)

<month> Name of month (January, February, etc.)

<hr:min> Hour and minutes in 24-hour format

<offset> Number of minutes to add during summer time

```
oc-rtr(config)#inter ether0
```

This command tells the router that the next three parameters will apply to the Ethernet port of the router.

```
oc-rtr(config-if)#band <kilobits per second>
```

Example: band 10000

Enter the bandwidth of the link connected to this port. For an Ethernet link, enter 10000.

```
oc-rtr(config-if)#delay 100
oc-rtr(config-if)#descript <path description>
```

Example: `descript oc-net`

Enter a description for the link. The example, `oc-net`, is short for operations center subnet. This description will display with some troubleshooting commands as a reminder of the link's location.

```
oc-rtr(config-if)#int s0
```

This command tells the router that the next three parameters will apply to the Serial 0 port of the router.

```
oc-rtr(config-if)#band <kilobits per second>
```

Example: `band 56`

Enter the bandwidth of the link connected to this port. For a microwave link, enter 56.

```
oc-rtr(config-if)#delay 100
oc-rtr(config-if)#descript <path description>
```

Example: `descript oc-west`

Enter a description for the link. The example, `oc-west`, is short for operations center to west site. This description will display with some troubleshooting commands as a reminder of the link's location.

Note: If there are additional serial ports, continue to enter these four commands for each port (`int s#`, `band 56`, `delay 100`, `descript <path description>`).

```
oc-rtr(config-if)#exit
oc-rtr(config)#ip host <name> <ip address>
```

Example:

```
ip host oc-hst 100.100.201.200
ip host west-hub 100.100.202.100
ip host south 100.100.103.2
```

This command associates a name with an IP address. An entry should be made for every computer and router in the system. See Section 2.4.

If a number needs to be corrected, just re-enter the host name and correct number. If an entry needs to be deleted, enter the command:

```
no ip host <name> <ip address>
```

```
oc-rtr(config)#line con 0
```

This command tells the router that the next two parameters will apply to a console (computer) that is attached to the router.

```
oc-rtr(config-line)#password <line password>
```

This password will be used to gain access to the router commands from a computer that is attached to the router.

```
oc-rtr(config-line)#login
```

Tells the router that a password is required at login.

ROUTER CONFIGURATION

```
oc-rtr(config-line)#line vty 0 4
```

This command tells the router that the next two parameters will apply to a virtual terminal for remote console access to the router.

```
oc-rtr(config-line)#password <virtual terminal password>
```

Enter the same password that was entered for the virtual terminal password at the beginning of configuration. When telnetting to the router, this password will be used to gain remote access to the router commands.

```
oc-rtr(config-line)#login
```

```
oc-rtr(config-line)#exit
```

```
oc-rtr(config)#ntp master
```

Enter the ntp master command in one router only. Normally, use a router at the site with the host computer. NTP stands for Network Time Protocol.

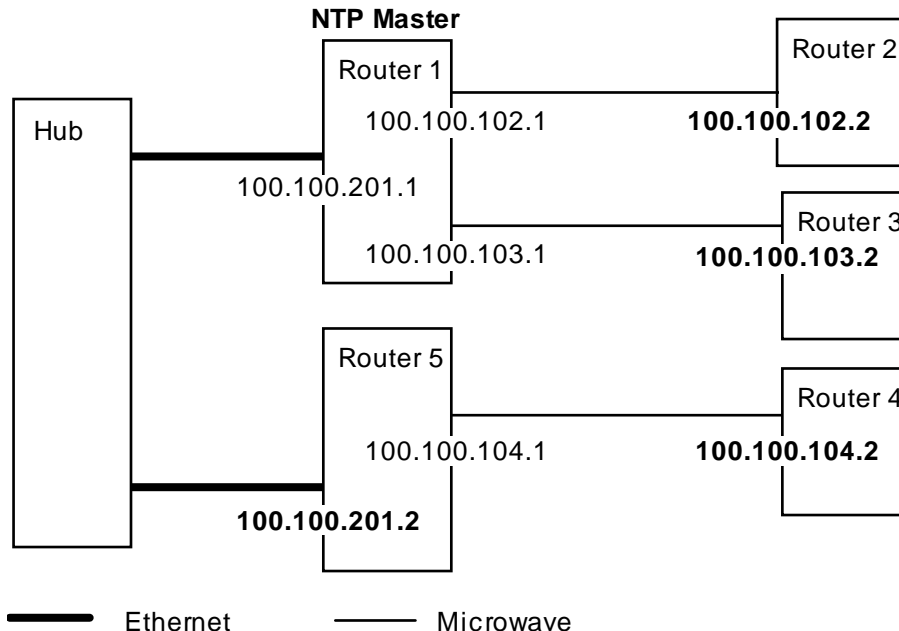
```
oc-rtr(config)#ntp peer <ip address>
```

Example: ntp peer 100.100.102.2

Example: ntp peer 100.100.103.2

This command is different if the router is the ntp master than if it is not the ntp master.

If the ntp master command has been given, enter an ntp peer command for each router in the system (except this router). Typically, use the IP address that is assigned to the serial 0 port of the router. If the router is connected to the ntp master's Ethernet port (via a hub), use the router's Ethernet port IP address. In the following diagram, the bold addresses would be used for the ntp peer commands.



If the ntp master command was not given, enter the IP address of the master that the router would use when communicating with the master. Using the above diagram, the following IP addresses would be used for the ntp peer command.

Router 2 - 100.100.102.1

Router 3 - 100.100.103.1

Router 4 - 100.100.201.1

Router 5 - 100.100.201.1

```
oc-rtr(config)#snmp community <password> ro
```

Example: snmp community public ro

Sets the ro (read only) snmp community password. This password is normally set to “public” and should be set the same as the snmp community password in OpenView.

```
oc-rtr(config)#snmp community <password> rw
```

Sets the rw (read/write) snmp community password. This password corresponds to the snmp set community password in OpenView.

```
oc-rtr(config)#snmp host <ip address or unique name> public snmp
```

Example: snmp host 100.100.201.200 public snmp

Example: snmp host waseca-hst public snmp

Enter the IP address or unique name of the host computer. This address is used for the destination of trap messages.

```
oc-rtr(config)#no service config
```

```
oc-rtr(config)#end
```

```
oc-rtr#
```

Wait for the next message; it can take a few seconds to appear.

```
%SYS-5-CONFIG_I: Configured from console by console <Enter>
```

```
oc-rtr#clock set <hour:min:sec> <date> <month> <year>
```

Example: clock set 8:46:00 11 Nov 1996

Sets the current time and date.

```
oc-rtr#wr mem
```

Writes the configuration to memory.

```
Building configuration...
```

```
[OK]
```

```
oc-rtr#
```

This ends configuration for the router. To verify that the router boots successfully, turn the router off and then back on. The following sign-on and legal messages should appear.

```
System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE  
Copyright (c) 1986-1995 by cisco Systems  
2500 processor with 1024 Kbytes of main memory
```

```
F3: 3072444+66260+202400 at 0x3000060
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

ROUTER CONFIGURATION

```
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 10.3(9), RELEASE SOFTWARE (fcl)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 30-Jan-96 20:37 by vatran
Image text-base: 0x0301B110, data-base: 0x00001000

cisco 2500 (68030) processor (revision D) with 1024K/1024K bytes of memory.
Processor board serial number 02348730
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY)

Press RETURN to get started!
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to down
%LINK-3-UPDOWN: Interface Ethernet0, changed state to up
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%LINK-3-UPDOWN: Interface Serial1, changed state to down
%SYS-5-CONFIG_I: Configured from memory by console
%SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 10.3(9), RELEASE SOFTWARE (fcl)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 30-Jan-96 20:37 by vatran
```

If <Enter> is pressed, the router will request a password.

The router can be turned off.

Mark the site name that this router was configured for on the outside of the router.

Routers are configured for a specific site and can not be moved to a new site without reconfiguration.

This page intentionally left blank.

SECTION

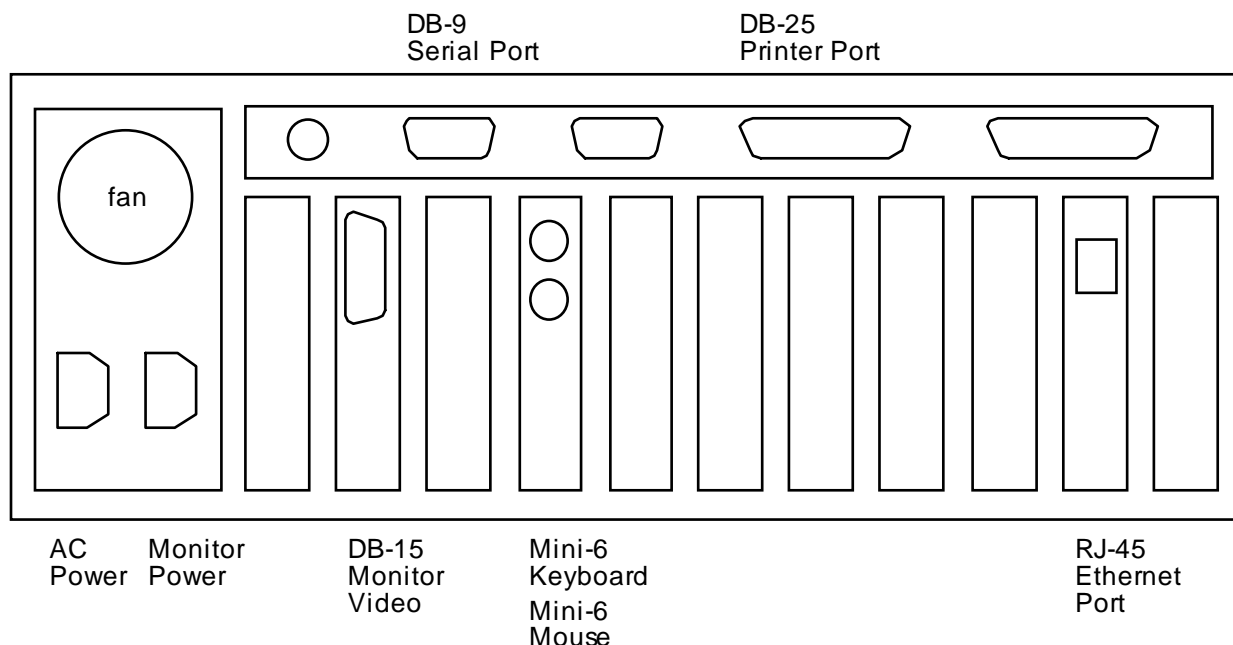
4. Site/Channel Computer Configuration**4.1. *Install Ethernet card***

1. Plug in the computer power cord.
2. Loosen the screws on the top cover of the computer.
3. Remove the cover by sliding it towards the back of the computer and lifting up.
4. Remove the blank cover from the next to last expansion slot (J11). Save the screw.
5. Insert the Ethernet card into expansion slot J11.
6. Using the screw saved in step 4, secure the Ethernet card in place.
7. Replace the computer cover.
8. Tighten the screws on the computer cover.

4.2. *Equipment setup*

A monitor, keyboard, and mouse need to be attached to the site and channel computers for configuring the computers. After configuration is complete, the monitor, keyboard, and mouse will be removed from the computers; they will not be attached to the computers when installed at the sites. When servicing a site, take along a monitor, keyboard, and mouse.

The site and channel computers have 3-1/2 inch floppy disk drives that are accessed by opening the cover on the right front of the computer. The front of the computer also has a reset button, power on/off switch, and a 5-pin DIN jack for attaching a keyboard that has a 5-pin DIN plug. Other peripherals are attached to the back of the computer as shown in the diagram below; however, the cards may be installed in different slots than shown.



Note: The monitor power cable may plug into a wall
 The keyboard cable may have a 5-pin DIN plug, which plugs into the front of the computer.
 The cards may be in a different order and have other connectors that are not used.

4.3. Configure Windows NT 3.51

Windows NT has been installed on the site and channel computers, however, it was probably not configured with the network information needed for the system. Configuring Windows involves opening several folders and entering information that includes the following.

- IP addresses (See Section 2.3 for information on assigning IP addresses.)
- Unique host names (See Section 2.4 for information on assigning host names.)
- Usernames and passwords (See Section 2.5.2.)
- Subnet mask: 255.255.255.0
- Default gateway: The IP address of the router port that will be connected to the Ethernet port of this computer.

4.3.1. Mouse configuration

1. Turn on the monitor and computer.
2. The screen displays:
 PS2-Mouse Configuration Change
 Press Any Key to Continue
3. Press a key. The setup screen appears.
4. Press F10 (Record and Exit).

5. The computer boots.

4.3.2. Enter a password

1. Press Ctrl+Alt+Del. A Welcome box appears.
2. Press the enter key (leaving the password box blank). The Log on Message box reports: "Your password has expired and must be changed".
3. Click OK. The Change Password box appears.
4. Enter the password for the computer in the Enter New Password box. Asterisks will appear on the screen as the characters are typed.
5. Verify the password by also entering it in the Confirm New Password box.
6. Click OK. A message confirms that the password has been changed.
7. Click OK.

4.3.3. Install Windows networking

1. The Program Manager and Main windows should be open. If not, open them.
2. Open the Control Panel.
3. Open the Network icon.
4. The Network Settings window displays a message that Windows NT Networking is not installed.

Note: If this window does not appear, click Cancel. Close the Control Panel and the Main program group; then skip to Section 4.3.4, Edit the LMHOSTS file.
5. Click Yes to install networking. The Windows NT Setup box appears.
6. Verify that the setup box displays: A:\i386
7. Click Continue. A Windows Installation message appears.

A. Verify network card installation

1. The Network Adapter Card Detection window appears.
2. Click Continue.
3. The computer detects the card that is installed and displays:

Setup has detected the following network adapter card in your computer:

3Com Etherlink III ISA/PCMCIA Adapter

If the message says that a network adapter card could not be detected, recheck the installation of the Ethernet card.

4. Click Continue.
5. A window displays the setup for the card:

I/O Port Address 0x300

Interrupt Number 10
Transceiver Type 10BaseT

6. Click Continue to accept the defaults.
7. A setup message reports that the parameters are not verifiably correct.
8. Click OK to use them anyway.

B. Installation options

1. A Windows NT setup box appears.
2. De-select "NWLink IPX/SPX Compatible Transport" (so that the check box is **not** checked).
3. Select "TCP/IP Transport" (so that the check box is checked).
4. Click Continue. A TCP/IP Installation Options box appears.
5. Select "Simple TCP/IP Services" (so that the check box is checked). Leave all other selections (boxes) as is.
6. Click Continue. Several messages appear.
7. Insert disks as requested, and click OK after inserting each disk.

C. Network settings

1. A Network Settings box appears.
2. Click OK.
3. Messages appear for configuring the network and setting up the protocol.
4. The TCP/IP Configuration box appears.
5. Enter the IP address for the computer.
6. Enter the Subnet Mask for the computer.
7. Enter the Default Gateway IP address for the computer.
8. Click OK. A Setup is Starting the Network message appears.
9. The Domain/Workgroup Settings box appears.
10. Click OK. A message reports that networking is now installed.
11. Click the Restart Computer button.
12. A message reports that shutdown is in progress and the computer reboots.

4.3.4. Edit the LMHOSTS file

Note: The LMHOSTS file needs to be edited once per system. The same file can be used for all computers within a system.

1. Insert the floppy disk named E.F. Johnson Site Controller (remote hub computer) into the A: drive. (The disk is Part No: 023-9998-406.)
2. Open the file named A:\LMHOSTS in an ASCII editor, such as Notepad.

3. Change the IP addresses and host names to those for this system. (See Section 2.3 for information about IP addresses and Section 2.4 for information about unique host names.)

Example:

```
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com      # source server
# 38.25.63.10  x.acme.com         # x client host
# 127.0.0.1    localhost
100.100.201.100 oc-hub
100.100.201.101 oc-chn
100.100.201.200 oc-hst
100.100.202.100 west-hub
100.100.203.100 south-hub
100.100.201.1  oc
100.100.102.2  west
100.100.103.2  south
```

4. Save the changes
5. Exit the editor

4.3.5. Change the passwords

1. Open the Administrative Tools program group.
2. Open the User Manager.

A. E.F. Johnson password

1. Open the efjohnson username properties by double clicking on the efjohnson username. If it does not exist, select menu item User -> New User and enter efjohnson in the Username field.
2. Enter the E. F. Johnson password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that the check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.

6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.

B. Administrator password

1. Open the Administrator username in the User Manager window.
2. Enter the Administrator password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that the check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.
6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.
9. Close the User Manager and Administrative Tools windows.

4.3.6. Change the system information through the Control Panel

1. Open the Main program group.
2. Open the Control Panel.
3. Open the Network icon.

A. Change the computer name

1. Click the Change button next to Computer Name.
2. Enter the unique host name for this computer (see Section 2.4).
3. Click OK

B. Change TCP/IP settings

1. Select TCP/IP Protocol in the scroll box.
2. Click on Configure.
3. Enter the IP Address, Subnet mask, and Default Gateway for this computer.
4. Click the DNS button.
5. Change the Host Name to match the computer name entered above (the unique host name for this computer).
6. Click OK.

Import the LMHOSTS file

1. Insert the floppy disk named E.F. Johnson Site Controller (remote hub computer) into the A: drive.
2. Click the Advanced button.
3. Click the Import LMHOSTS button.
4. Enter A:\ in the dialog box.
5. Click the Import button. The lmhosts file is imported.
6. Be sure the Enable LMHOSTS Lookup check box is checked in the Windows Networking Parameters section.
7. Click OK to close the Advanced window.
8. Click OK to close the TCP/IP Configuration window.
9. Click OK to close the Network Settings window.

C. Change system settings

1. Open the System icon in the Control Panel.
2. In the Operating System section, change the Show List For entry to 5 seconds.
3. In the Variable box, enter:

PATH

4. In the Value box, enter:

C:\UTILITY

5. Click the Set button.
6. In the Variable box, enter:

TZ

7. In the Value box, enter the standard time zone for the location that the computer will be installed, the offset from UTC (GMT, Zulu), and the daylight savings time zone.

Timezone	Entry
Eastern Standard Time	EST5EDT
Central Standard Time	CST6CDT
Mountain Standard Time	MST7MDT
Pacific Standard Time	PST8PDT

8. Click the Set button.
9. Click OK to close the System window.
10. Close the Control Panel.

D. Copy LMHOSTS to HOSTS

1. Open the File Manager.
2. Open the \WINNT\SYSTEM32\DRIVERS\ETC\ folder.

3. Select LMHOSTS.
4. Select menu item File -> Copy.
5. In the To box, enter HOSTS. Click OK.
6. A Confirm File Replace message box appears. Click Yes.
7. Close the File Manager.
8. Close the Main program group.

4.3.7. Change the system information in Windows NT Registry

1. From the Program Manager, select menu item File -> Run.
2. In the Command line field, enter:

regedt32

3. Click OK.
4. Select the window HKEY_LOCAL_MACHINE.

A. System folder

1. Open the System folder.

Note: The following steps (2-20) need to be repeated for several folders that are within the System folder. Return to this point until all folders have been modified.

2. Open one of these folders:
 - Clone
 - ControlSet001
 - ControlSet002
 - ControlSet003
 - ControlSet004
 - CurrentControlSet
3. Open the Control folder.
4. Open the ComputerName folder.
5. Select the ComputerName folder (which is in the ComputerName folder).
6. In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.
7. Select the ActiveComputerName folder (if present in the ComputerName folder). In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.
8. Close the Control folder.
9. Open the Services folder.
10. Open the Elnk31 folder.
11. Open the Parameters folder.
12. Select the Tcpip folder.

13. In the right window, change the following entries by double-clicking on the entry, changing the value, and clicking OK.

DefaultGateway

IPAddress

SubnetMask

14. Open the NETBT folder (in the Services folder).
15. Select the Parameters folder.
16. Verify the value of EnableLMHOSTS in the right window - it should be 0x1. If required, change the value by double-clicking on it, entering 1, setting Radix to Hex, and then clicking OK.
17. Open the Tcpip folder (in the Services folder).
18. Select the Parameters folder.
19. In the right window, double-click on Hostname, change the name to the unique host name for this computer, then click OK.
20. Close the folder that was opened in step 2.

Note: Return to step 2 under “A. System folder” until all folders have been modified.

Folders that require changes, if present and not dimmed:

Clone

ControlSet001

ControlSet002

ControlSet003

ControlSet004

CurrentControlSet

21. Close the System folder, after all folders have been modified.

B. Software folder

1. Open the Software folder.
2. Open the Microsoft folder.
3. Open the Windows NT folder.
4. Open the Current Version folder.
5. Select the Winlogon folder.
6. Verify the value of DefaultUserName in the right window - it should be efjohnson. If required, change the value by double-clicking on it, entering efjohnson, then clicking OK.
7. Look for AutoAdminLogon in the right window. If not present:

Select menu item Edit -> Add Value.

Enter AutoAdminLogon and click OK.

Enter 1 and click OK.

8. Look for DefaultPassword in the right window. If not present:

Select menu item Edit -> Add Value.

Enter DefaultPassword and click OK.

Enter the E.F. Johnson password and click OK.

9. Close the Registry Editor window.

4.4. Install site controller application

4.4.1. Install the application

1. Put the disk named E.F. Johnson Site Controller into the floppy drive.
2. From the Program Manager, select menu item File -> Run.
3. Click Browse.
4. In the drive section, select the floppy drive.
5. In the filename section, select setup.exe.
6. Click OK.
7. Click OK in the Run dialog box.
8. Follow the on-screen instructions. Accept the defaults in all dialog boxes.
9. When installation is completed, the Program Manager will appear with a new program group named Site Controller.

4.4.2. Set the start up application

1. Open the Site Controller program group.
2. While holding the Control key, drag the Site Controller icon on top of the Startup program group.
3. Close the Site Controller program group.
4. Minimize the Program Manager window.

4.4.3. Configure for no mouse

1. Select the Program Manager icon - a pop up menu appears.
2. Click on Shutdown.
3. Select Shutdown and Restart.
4. Click OK.
5. When the system restarts, the Program Manager and Site Controller icons should display on the screen. Next, the Site Controller application should appear.
6. Exit the Site Controller by selecting menu item File -> Exit.

7. Disconnect the mouse from the back of the computer.
8. Press ALT+F4 to shut down the computer.
9. Use the cursor (arrow) keys to select Shutdown and Restart.
10. Press the enter key.
11. When the system restarts, an error message will display indicating that the mouse configuration has changed.
12. Press any key - the setup screen will appear.
13. Press F10 - the system will reboot.
14. Wait for the Site Controller application window(s) to appear on the screen.
15. Press ALT+F, then X to exit the Site Controller application.
16. Press ALT+F4 to shutdown the computer.
17. Use the cursor (arrow) keys to select Shutdown (not restart).
18. Press the enter key.
19. When the message appears that it is safe to turn off the computer, do so.
20. Disconnect the keyboard and monitor from the computer.
21. Mark the site name that this computer was configured for on the outside of the computer. Computers are configured for a specific site and can not be moved to a new site without reconfiguration.

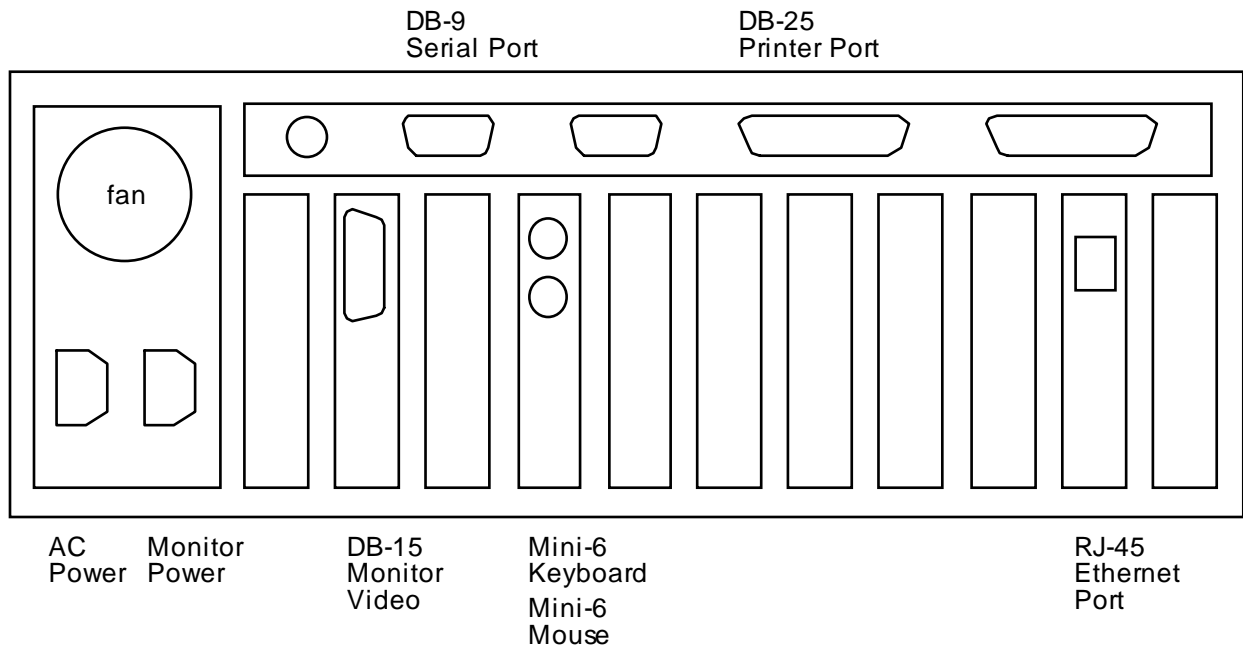
SECTION

5. Host Computer Configuration**5.1. Install Ethernet card**

1. Plug in the computer power cord.
2. Loosen the screws on the top cover of the computer.
3. Remove the cover by sliding it towards the back of the computer and lifting up.
4. Remove the blank cover from the next to last expansion slot (J11). Save the screw.
5. Insert the Ethernet card into expansion slot J11.
6. Using the screw saved in step 4, secure the Ethernet card in place.
7. Replace the computer cover.
8. Tighten the screws on the computer cover.

5.2. Equipment setup

The host computer has a 3-1/2 inch floppy disk drive and a CD-ROM drive that are accessed by removing the cover from the right front of the computer. The front of the computer also has a reset button, power on/off switch, and a 5-pin DIN jack for attaching a keyboard that has a 5-pin DIN plug. Other peripherals are attached to the back of the computer as shown in the diagram below; however, the cards may be installed in different slots than shown.



Note: The monitor power cable may plug into a wall outlet.
 The keyboard cable may have a 5-pin DIN plug, which plugs into the front of the computer.
 The cards may be in a different order and have other connectors that are not used.

5.3. **Configure Windows NT 4.0**

Windows NT has been installed on the host computer; however, it was probably not configured with the network information needed for the system. Configuring Windows involves opening several windows and folders and entering information that includes the following.

- IP addresses (See Section 2.3 for information on assigning IP addresses.)
- Unique host names (See Section 2.4 for information on assigning host names.)
- Usernames and passwords (See Section 2.5.2.)
- Subnet mask: 255.255.255.0
- Default gateway: The IP address of the router port that will be connected to the Ethernet port of this computer.

5.3.1. **Log on to Windows NT**

1. Press Ctrl+Alt+Del. A Welcome box appears.
2. Press the enter key (leaving the password box blank). The Log on message box reports: “You are required to change your password at first login”.
3. Click OK. The Change Password box appears.
4. Enter the password for the computer in the New Password box. Asterisks will appear on the screen as the characters are typed.
5. Verify the password by also entering it in the Confirm New Password box.
6. Click OK. A message confirms that the password has been changed.
7. Click OK.

5.3.2. **Set CD properties**

1. Click Start on the taskbar at the bottom of the screen. A menu appears.
2. Select menu item Run.
3. Enter regedt32.
4. Click OK. The Registry Editor window appears.
5. Click on the HKEY_LOCAL_MACHINE window.
6. Open the System folder.
7. Open the CurrentControlSet folder.
8. Open the Services folder.
9. Click once on the Cdrom folder.
10. In the right window, double-click on Autorun. The DWORD Editor window appears.
11. In the Data box, enter 0 (zero).

12. Click OK.
13. Close the Registry Editor.

5.3.3. Install Windows networking

1. Click Start on the taskbar.
2. Select menu item Settings -> Control Panel. The Control Panel window appears.
3. Open the Network icon.
4. The Network Configuration window displays a message that Windows NT Networking is not installed.

Note: If this window does not appear, click Cancel. Close the Control Panel and the Main program group; then skip to Section 5.3.4, Edit the LMHOSTS file.
5. Click Yes to install networking. The Network Setup Wizard window appears.
6. Select “Wired to the network”.
7. Click Next. The network adapters window appears.
8. Click Start Search. Network adapters are added to the list.

 If a message indicates that a network adapter card could not be detected, recheck the installation of the Ethernet card.
9. When the search is finished, click Next. The network protocols window appears.
10. Select “TCP/IP Protocol”.
11. Click Next. The network services window appears.
12. Click Next to accept the defaults. The install window appears.
13. Click Next to install files. A window asking for the CD drive letter appears.
14. Enter the CD drive letter and i386. For example,
 D:\i386
15. Click Continue.
16. A window displays the setup for the card:

I/O Port Address	0x300
Interrupt Number	10
Transceiver Type	10BaseT
17. Click Continue to accept the defaults.
18. A setup message reports that the parameters are not verifiably correct.
19. Click OK to use them anyway.
20. The DHCP server window appears.

21. Click No.
22. Network files are copied and installed onto the hard disk.

A. TCP/IP Properties

1. The Microsoft TCP/IP Properties window appears.
2. Enter the IP address, subnet mask, and default gateway for this computer.
3. Click the DNS tab.
4. Verify that the host name is correct for this computer. (It should be the same as the computer name.)
5. Click OK.
6. Click Yes or Next to accept the defaults on the remaining setup windows.
7. Click Finish.
8. Click Yes to restart the computer.

5.3.4. Edit the LMHOSTS file

Note: The LMHOSTS file needs to be edited once per system. The same file can be used for all computers within a system.

1. Insert the floppy disk named E.F. Johnson Site Controller (remote hub computer) into the A: drive.
2. Open the file named A:\LMHOSTS in an ASCII editor, such as Notepad.
3. Change the IP addresses and host names to those for this system. (See Section 2.3 for information about IP addresses and Section 2.4 for information about unique host names.)

Example:

```
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com      # source server
# 38.25.63.10  x.acme.com         # x client host
# 127.0.0.1    localhost
100.100.201.100 oc-hub
100.100.201.101 oc-chn
100.100.201.200 oc-hst
100.100.202.100 west-hub
```

100.100.203.100	south-hub
100.100.201.1	oc
100.100.102.2	west
100.100.103.2	south

4. Save the changes.
5. Exit the editor.

5.3.5. Change the passwords

1. Click Start on the taskbar.
2. Select menu item Programs -> Administrative Tools -> User Manager.

A. E.F. Johnson password

1. Open the efjohnson username properties by double clicking on the efjohnson username. If it does not exist, select menu item User -> New User and enter efjohnson in the Username field.
2. Enter the E. F. Johnson password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that a check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.
6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.

B. Administrator password

1. Open the Administrator username in the User Manager window.
2. Enter the Administrator password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that the check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.
6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.
9. Close the User Manager window.

5.3.6. Change the system information through the Control Panel

1. Click Start on the taskbar.
2. Select menu item Settings -> Control Panel.
3. Open the Network icon.

A. Identification tab

If the computer name is not correct, click the Change button. The Identification Changes window appears. Change the name and click OK.

B. Protocols tab

1. Select TCP/IP.
2. Click the Properties button. The Microsoft TCP/IP Properties window appears.
3. Click the WINS Address tab.
4. Be sure the Enable LMHOSTS Lookup check box is checked.
5. Click Import LMHOSTS. The Open box appears.
6. Put the floppy disk named E.F. Johnson Site Controller (remote hub computer) into the A: drive.
7. From the Look in drop down list, select 3-1/2 Floppy (A:).
8. Click Open.
9. Select the lmhosts file.
10. Click Open. The file is imported and the Open box closes.
11. Click OK in the Microsoft TCP/IP Properties window.
12. An empty WINS address warning appears.
13. Click Yes to continue.
14. Click Close in the Network window. A message box appears.
15. Remove the disk from the A drive.
16. Click Yes to restart the computer.

C. Change system settings

1. Click Start on the taskbar.
2. Select menu item Settings -> Control Panel.
3. Open the System icon. The System Properties window appears.
4. Click the Startup/Shutdown tab.
5. In the System Startup section, change the Show List For entry to 10 seconds.
6. Click the Environment tab.
7. In the Variable box, enter:

TZ

8. In the Value box, enter the standard time zone for the location that the computer will be installed, the offset from UTC (GMT, Zulu), and the daylight savings time zone.

Timezone	Entry
Eastern Standard Time	EST5EDT
Central Standard Time	CST6CDT
Mountain Standard Time	MST7MDT
Pacific Standard Time	PST8PDT

9. Click the Set button.
10. Click OK to close the System Properties window.
11. Close the Control Panel.

5.3.7. Change the system information in Windows NT Registry

1. Click Start on the taskbar.
2. Select menu item Run.
3. In the Open field, enter:
regedt32
4. Click OK. The Registry Editor appears.
5. Select the window HKEY_LOCAL_MACHINE.

A. System folder

1. Open the System folder.

Note: The following steps (2-20) need to be repeated for several folders that are within the System folder. Return to this point until all folders have been modified.

2. Open one of these folders:
 - Clone
 - ControlSet001
 - ControlSet002
 - ControlSet003
 - ControlSet004
 - CurrentControlSet
3. Open the Control folder.
4. Open the ComputerName folder.
5. Select the ComputerName folder (which is in the ComputerName folder).
6. In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.
7. Select the ActiveComputerName folder (if present in the ComputerName folder). In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.

8. Close the Control folder.
9. Open the Services folder.
10. Open the Elnk31 folder.
11. Open the Parameters folder.
12. Select the Tcpip folder
13. In the right window, change the following entries by double-clicking on the entry, changing the value, and clicking OK.

DefaultGateway

IPAddress

SubnetMask

14. Open the NETBT folder (in the Services folder).
15. Select the Parameters folder.
16. Verify the value of EnableLMHOSTS in the right window - it should be 0x1.
If required, change the value by double-clicking on it, entering 1, setting Radix to Hex, and then clicking OK.
17. Open the Tcpip folder (in the Services folder).
18. Select the Parameters folder.
19. In the right window, double-click on Hostname, change the name to the unique host name for this computer, then click OK.
20. Close the folder that was opened in step 2.

Note: Return to step 2 under “A. System folder” until all folders have been modified.

Folders that require changes, if present and not dimmed:

Clone

ControlSet001

ControlSet002

ControlSet003

ControlSet004

CurrentControlSet

21. Close the System folder, after all folders have been modified.

B. Software folder

1. Open the Software folder.
2. Open the Microsoft folder.
3. Open the Windows NT folder.
4. Open the Current Version folder.
5. Select the Winlogon folder.

6. Verify the value of DefaultUserName in the right window - it should be efjohnson. If required, change the value by double-clicking on it, entering efjohnson, then clicking OK.
7. Close the Registry Editor window.

C. Copy LMHOSTS to HOSTS

1. Click Start on the taskbar.
2. Select menu item Programs -> Command Prompt.
3. At the prompt, enter:

```
cd \winnt\system32\drivers\etc\  
copy lmhosts hosts  
exit
```

5.4. Install OpenView Professional Suite

1. Click Start on the taskbar.
2. Select menu item Settings -> Control Panel.
3. Open the Add/Remove Programs icon. The Add/Remove Programs Property window appears.
4. Click Install.
5. Follow the screen instructions, putting the HP OpenView Professional Suite CD in the drive and clicking Next and Finish.
6. OpenView's Setup program starts. Follow the screen instructions and accept the default values, except for the following items.

Do not install Internet Explorer.

Do not install Acrobat Reader. The license agreement will have to be agreed to, but select Cancel for the installer.

7. When finished, close the Control Panel.

• Modify DEVICES

1. Open the file named C:\OV\OVFILES\DEVICES in an ASCII editor, such as Notepad.
 2. Add the following line to the top of the list.
- | | | | |
|----------------|---------------|---------------|---|
| "Cisco Router" | 1.3.6.1.4.1.9 | 0x133a ROUTER | 0 |
|----------------|---------------|---------------|---|
3. Save the file.

5.5. Install host computer application

1. Click Start on the taskbar.
2. Select menu item Settings -> Control Panel.

3. Open the Add/Remove Programs icon. The Add/Remove Programs Property window appears.
4. Click Install.
5. Follow the screen instructions, putting the E.F. Johnson Host Computer disk 1 (Part No. 023-9998-405) in the drive and clicking Next and Finish.
6. The install program starts. Follow the screen instructions and accept the default values.
7. When finished, close the Control Panel.

A. Set taskbar properties

1. Click Start on the taskbar.
2. Select menu item Settings -> Taskbar. The Taskbar Properties window appears.
3. Select the Start Menu programs tab.
4. Click the Advanced button. The Exploring-Start Menu window appears.
5. Open the following folder hierarchy.

Winnt
Profiles
AllUsers
StartMenu
Programs

6. Click once on HP OpenView in the Programs folder.
7. In the right window, click once on the HP OpenView icon.
8. Select menu item Edit -> Copy.
9. Click once on the Startup folder (in the Programs folder of step 5).
10. Select menu item Edit -> Paste.
11. Close the Exploring-Start Menu window.
12. Select the Taskbar Options tab in the Taskbar Properties window.
13. Select Autohide.
14. Select Show small icons in start menu.
15. Click OK in the Taskbar Properties window.

B. Finish installing

1. Reboot the computer.
2. After logging on to Windows NT, OpenView should start.

5.6. Create 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.

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 5.6.7 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 5.6.1 Creating the System map, Section 5.6.2 Creating a Site map, and Section 5.6.3 Creating a Device map.

The OpenView program is used to create maps.

5.6.1. Create 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 5.6.8.)

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 9.4 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? When this check box is checked, 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 5.6.3 for adding a router instructions.
10. Save the map by selecting menu item File -> Save or by pressing Ctrl+S.

5.6.2. Create 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.

5.6.3. Create 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

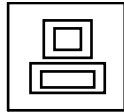


Router icon (generic)

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

• 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: When this check box is checked, 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.

- 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.

Note: For a bi-directional microwave system, the IAC 1 input for repeater 1 at each site should be configured so that the microwave default direction does not cause an alarm. See Section 5.7 for bi-directional configuration.

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

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

5.6.4. Add 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.

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

5.6.5. Set 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.

5.6.6. Protect 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.

5.6.7. 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).

5.6.8. 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.

5.7. *Edit site and system settings*

Note: This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

The Edit Offsets dialog box is used to configure several site and system settings. The Save System button will be enabled if changes have been made to the System Settings. The Save Site button will be enabled if changes have been made to the selected site's settings or if the selected site is not in the configuration file.

The site names are obtained from the OpenView map and the settings are obtained from a configuration file. During initial configuration and when a site is added to the system, a site must be saved even though no changes have been made to the settings. Saving the site adds it to the configuration file or modifies the settings in the file.

1. Select a System icon.
2. Select menu item System -> Calibration -> Edit Offsets. The Edit Offsets dialog box appears.

Site Settings

3. Select a site in the site list.
4. Enter the overlap offset value, if known. Enter a hyphen before negative numbers. This value can be from -100 to 100 microseconds. The simulcast system must be recalibrated if this value is changed. (See Sections 7.2 and 7.3 for information about calibration. See Section 7.4 for more information about overlap offsets.)
5. If a channel bank is used to transmit to the repeater site, select Channel Bank (so that the check box is checked). A channel bank is not used when a repeater site is collocated with a channel controller site. This setting affects the phase delay to be used for each site.
6. Click the Save Site button.
7. Repeat steps 3 through 6 for each site.

System Settings

8. The Buffer Delay Min value sets the lowest buffer delay in the system. This value can be from 250 to 2000 microseconds. Buffer delay is the amount of time the repeater delays after receiving a signal before transmitting the signal.
9. If the system has a bi-directional microwave, select Bi-Directional (so that the check box is checked). This change will take affect after OpenView is restarted and each Repeater 1 Describe dialog box is opened and saved.

After restarting OpenView, right-click on a repeater 1 icon and select Describe to open the EFJ Repeater Description dialog box. The IAC alarm 1 description will be updated automatically. Click OK. Repeat for the repeater 1 icon at every site in the system.

10. If the system has a redundant microwave, select Redundant (so that the check box is checked). A redundant system has two channel controllers that can control the system. Only one channel controller is in use at a time. This change will take affect after OpenView is restarted.
11. Click the Save System button.

5.8. Configure OpenView polling

Polling is configured from within the OpenView program.

5.8.1. Add devices to polling list

1. Select the map icons for all routers and computers in the system. Shift+click or Ctrl+click to select multiple icons.

2. Select menu item Monitor -> Polling -> Add Device(s). The IP addresses of the selected devices will be added to the polling list. If a device has more than one address, another dialog box will ask which address(es) to poll. Select the address that communicates with the host computer. If a device that does not have an IP address is selected, an error message will be displayed.

5.8.2. Set polling defaults

1. Select menu item Monitor -> Polling -> Configure System Defaults.
2. Set Interval to 1 minute.
3. From the Device Down Severity drop down list box, select Major.
4. Select Update Map Status, Sound Bell, and Log (so that the check box is checked).
5. From the Device Up Severity drop down list box, select Normal.
6. Select Update Map Status, Sound Bell, and Log (so that the check box is checked).
7. Click OK.
8. Select menu item Monitor -> Polling -> Start Polling.

If a system requires a different polling configuration, see the polling section of the Network Management online help or the System Manager Manual for additional polling information.

5.8.3. Verify polling settings

Select menu item Monitor -> Polling -> View Polling List.

A dialog box will show the name, interval, and IP address for each polled device. At the bottom of the dialog box, the total number of entries is displayed and also whether polling is on or off.

5.9. Configure OpenView traps

Traps are configured from within the OpenView program.

1. Select menu item Monitor -> Customize Traps.
2. Click the Add Device Class button.
3. From the list, select the entry with a Device Class Name of Cisco Router, and an Enterprise of 1.3.6.1.4.1.9.
4. Click OK.
5. Click the Add Trap button.
6. Select Specific in the Generic list.
7. Enter 0 in the Specific field.
8. Click OK.

9. In the Description field, enter:

Cisco Router Reloading

10. Select Update Map Status, Sound Bell, and Log (so that the check boxes are checked).

11. From the Severity drop down list, select Warning.

12. Click the Add Trap button.

13. Select Specific in the Generic list.

14. Enter 1 in the Specific field.

15. Click OK.

16. In the Description field, enter:

Telnet Connection Closed

17. De-select Update Map Status, Sound Bell, and Log (so that the check boxes are **not** checked).

18. From the Severity drop down list, select Informational.

19. Click OK.

5.10. Set OpenView passwords

These passwords are set from within the OpenView program.

5.10.1. Log in passwords

To set log in 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.

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.

5.10.2. Protect maps 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.

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.

5.10.3.SNMP passwords

Note: These passwords are not needed for normal day-to-day operation of the system. They are used by OpenView applications, such as the SNMP Manager and Autodiscovery.

Passwords to read and write information to SNMP devices are set by selecting menu item Options -> Customize Device Access.

To modify system defaults, select <System Default> from the Network Addresses list and then click the Modify button.

To modify information for a specific device, select the IP address of the device from the Network Addresses list and click the Modify button. Only devices that do not use system defaults will be listed in the Network Addresses list.

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 already be filled in.

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

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. (Corresponds to router password: SNMP community password ro.)

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. (Corresponds to router password: SNMP community password rw.)

5.11. Service functions

If the service.ini file is present when OpenView starts, extra functions are available for service personal. The service.ini file is stored on disk 1 of the E.F. Johnson Host Computer disk set.

To use service functions, exit OpenView and copy the service.ini file from the floppy disk to the hard disk directory C:\SITECTR\. When OpenView is started, the service.ini file will be read and then deleted from the hard disk.

Service.ini adds the following menu items to OpenView.

- System -> Calibration -> Edit Offsets. See Sections 5.7 and 7.4.3.

- System -> Calibration -> Threshold Alignment. See Section 7.1.
- System -> Calibration -> SMC Configuration. See Section 7.5.
- Repeater -> Setup State. See Section 9.5.1.
- Repeater -> Normal State. See Section 9.5.1.

5.12. Configure Windows NT 3.51

Note: This section is provided as a reference for systems using Windows NT version 3.51.

Windows NT has been installed on the host computer; however, it was probably not configured with the network information needed for the system. Configuring Windows involves opening several folders and entering information that includes the following.

- IP addresses (See Section 2.3 for information on assigning IP addresses.)
- Unique host names (See Section 2.4 for information on assigning host names.)
- Usernames and passwords (See Section 2.5.2.)
- Subnet mask: 255.255.255.0
- Default gateway: The IP address of the router port that will be connected to the Ethernet port of this computer.

5.12.1. Enter a password

1. Press Ctrl+Alt+Del. A Welcome box appears.
2. Press the enter key (leaving the password box blank). The Log on Message box reports: "Your password has expired and must be changed".
3. Click OK. The Change Password box appears.
4. Enter the password for the computer in the Enter New Password box. Asterisks will appear on the screen as the characters are typed.
5. Verify the password by also entering it in the Confirm New Password box.
6. Click OK. A message confirms that the password has been changed.
7. Click OK.

5.12.2. Install Windows networking

1. The Program Manager and Main windows should be open. If not, open them.
2. Open the Control Panel.
3. Open the Network icon.
4. The Network Settings window displays a message that Windows NT Networking is not installed.

Note: If this window does not appear, click Cancel. Close the Control Panel and the Main program group; then skip to Section 5.12.3, Edit the LMHOSTS file.

5. Click Yes to install networking. The Windows NT Setup box appears.
6. Verify that the setup box displays: A:\i386
7. Click Continue. A Windows Installation message appears.

A. Verify network card installation

1. The Network Adapter Card Detection window appears.
2. Click Continue.
3. The computer detects the card that is installed and displays:

Setup has detected the following network adapter card in your computer:

3Com Etherlink III ISA/PCMCIA Adapter

If the message says that a network adapter card could not be detected, recheck the installation of the Ethernet card.

4. Click Continue.
5. A window displays the setup for the card:

I/O Port Address	0x300
Interrupt Number	10
Transceiver Type	10BaseT

6. Click Continue to accept the defaults.
7. A setup message reports that the parameters are not verifiably correct.
8. Click OK to use them anyway.

B. Installation options

1. A Windows NT setup box appears.
2. De-select “NWLink IPX/SPX Compatible Transport” (so that the check box is **not** checked).
3. Select “TCP/IP Transport” (so that the check box is checked).
4. Click Continue. A TCP/IP Installation Options box appears.
5. Select “Simple TCP/IP Services” (so that the check box is checked). Leave all other selections (boxes) as is.
6. Click Continue. Several messages appear.
7. Insert disks as requested, and click OK after inserting each disk.

C. Network settings

1. A Network Settings box appears.

2. Click OK.
3. Messages appear for configuring the network and setting up the protocol.
4. The TCP/IP Configuration box appears.
5. Enter the IP address for the computer.
6. Enter the Subnet Mask for the computer.
7. Enter the Default Gateway IP address for the computer.
8. Click OK. A Setup is Starting the Network message appears.
9. The Domain/Workgroup Settings box appears.
10. Click OK. A message reports that networking is now installed.
11. Click the Restart Computer button.
12. A message reports that shutdown is in progress and the computer reboots.

5.12.3. Edit the LMHOSTS file

Note: The LMHOSTS file needs to be edited once per system. The same file can be used for all computers within a system.

1. Insert the floppy disk named SITECTRL (remote hub computer) into the A: drive.
2. Open the file named A:\LMHOSTS in an ASCII editor, such as Notepad.
3. Change the IP addresses and host names to those for this system. (See Section 2.3 for information about IP addresses and Section 2.4 for information about unique host names.)

Example:

```
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com      # source server
# 38.25.63.10  x.acme.com         # x client host
# 127.0.0.1    localhost
100.100.201.100 oc-hub
100.100.201.101 oc-chn
100.100.201.200 oc-hst
100.100.202.100 west-hub
100.100.203.100 south-hub
```

100.100.201.1	oc
100.100.102.2	west
100.100.103.2	south

4. Save the changes.
5. Exit the editor.

5.12.4.Change the passwords

1. Open the Administrative Tools program group.
2. Open the User Manager.

A. E.F. Johnson password

1. Open the efjohnson username properties by double clicking on the efjohnson username. If it does not exist, select menu item User -> New User and enter efjohnson in the Username field.
2. Enter the E. F. Johnson password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that the check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.
6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.

B. Administrator password

1. Open the Administrator username in the User Manager window.
2. Enter the Administrator password in the Password field and in the Confirm Password field.
3. Select Password Never Expires, so that the check box is checked.
4. Click the Groups button.
5. Verify that Administrators is listed in the Member Of box. If it is not listed, select Administrators in the Not Member Of box and click the Add button.
6. If anything other than Administrator is listed in the Member Of box, select them and click the Remove button.
7. Click OK.
8. Click OK in the User Properties window.
9. Close the User Manager and Administrative Tools windows.

5.12.5. Change the system information through the Control Panel

1. Open the Main program group.
2. Open the Control Panel.
3. Open the Network icon.

A. Change the computer name

1. Click the Change button next to Computer Name.
2. Enter the unique host name for this computer (see Section 2.4).
3. Click OK.

B. Change TCP/IP settings

1. Select TCP/IP Protocol in the scroll box.
2. Click on Configure.
3. Enter the IP Address, Subnet mask, and Default Gateway for this computer.
4. Click the DNS button.
5. Change the Host Name to match the computer name entered above (the unique host name for this computer).
6. Click OK.

Import the LMHOSTS file

1. Insert the floppy disk named SITECTRL (remote hub computer) into the A: drive.
2. Click the Advanced button.
3. Click the Import LMHOSTS button.
4. Enter A:\ in the dialog box.
5. Click the Import button. The lmhosts file is imported.
6. Be sure the Enable LMHOSTS Lookup check box is checked in the Windows Networking Parameters section.
7. Click OK to close the Advanced window.
8. Click OK to close the TCP/IP Configuration window.
9. Click OK to close the Network Settings window.

C. Change system settings

1. Open the System icon in the Control Panel.
2. In the Operating System section, change the Show List For entry to 10 seconds.
3. In the Variable box, enter:

PATH

4. In the Value box, enter:

C:\OV;C:\UTILITY

5. Click the Set button.

6. In the Variable box, enter:

TZ

7. In the Value box, enter the standard time zone for the location that the computer will be installed, the offset from UTC (GMT, Zulu), and the daylight savings time zone.

Timezone	Entry
Eastern Standard Time	EST5EDT
Central Standard Time	CST6CDT
Mountain Standard Time	MST7MDT
Pacific Standard Time	PST8PDT

8. Click the Set button.

9. Click OK to close the System window.

10. Close the Control Panel.

D. Copy LMHOSTS to HOSTS

1. Open the File Manager.

2. Open the \WINNT\SYSTEM32\DRIVERS\ETC\ folder.

3. Select LMHOSTS.

4. Select menu item File -> Copy.

5. In the To box, enter HOSTS. Click OK.

6. A Confirm File Replace message box appears. Click Yes.

7. Close the File Manager.

8. Close the Main program group.

5.12.6.Change the system information in Windows NT Registry

1. From the Program Manager, select menu item File -> Run.

2. In the Command line field, enter:

regedt32

3. Click OK.

4. Select the window HKEY_LOCAL_MACHINE.

A. System folder

1. Open the System folder.

Note: The following steps (2-20) need to be repeated for several folders that are within the System folder. Return to this point until all folders have been modified.

2. Open one of these folders:
 - Clone
 - ControlSet001
 - ControlSet002
 - ControlSet003
 - ControlSet004
 - CurrentControlSet
3. Open the Control folder.
4. Open the ComputerName folder.
5. Select the ComputerName folder (which is in the ComputerName folder).
6. In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.
7. Select the ActiveComputerName folder (if present in the ComputerName folder). In the right window, double-click on ComputerName, change the name to the unique host name for this computer, then click OK.
8. Close the Control folder.
9. Open the Services folder.
10. Open the Elnk31 folder.
11. Open the Parameters folder.
12. Select the Tcpip folder
13. In the right window, change the following entries by double-clicking on the entry, changing the value, and clicking OK.
 - DefaultGateway
 - IPAddress
 - SubnetMask
14. Open the NETBT folder (in the Services folder).
15. Select the Parameters folder.
16. Verify the value of EnableLMHOSTS in the right window - it should be 0x1. If required, change the value by double-clicking on it, entering 1, setting Radix to Hex, and then clicking OK.
17. Open the Tcpip folder (in the Services folder).
18. Select the Parameters folder.
19. In the right window, double-click on Hostname, change the name to the unique host name for this computer, then click OK.
20. Close the folder that was opened in step 2.

Note: Return to step 2 under “A. System folder” until all folders have been modified.

Folders that require changes, if present and not dimmed:

Clone
ControlSet001
ControlSet002
ControlSet003
ControlSet004
CurrentControlSet

21. Close the System folder, after all folders have been modified.

B. Software folder

1. Open the Software folder.
2. Open the Microsoft folder.
3. Open the Windows NT folder.
4. Open the Current Version folder.
5. Select the Winlogon folder.
6. Verify the value of DefaultUserName in the right window - it should be efjohnson. If required, change the value by double-clicking on it, entering efjohnson, then clicking OK.
7. Close the Registry Editor window.

5.13. Install OpenView Work Group Node Manager

Note: This section is provided as a reference for systems using Windows NT version 3.51 and HP OpenView Work Group Node Manager (not Professional Suite).

1. Insert the first installation disk into the floppy disk drive. (The name of the disk may be similar to HP OpenView for Windows Work Group Node Manager Disk 1.)
2. From the Program Manager, select menu item File-> Run.
3. In the Command line field, enter:
A:\SETUP
4. Click OK.
5. The HP OpenView for Windows Initializing Setup message box displays.
6. A Welcome box displays.
7. Click Continue.
8. The default path box displays.
9. Click Continue to accept the default Destination Path of C:\OV.
10. The HP OpenView Applications box displays.
11. Select SNMP over TCP/IP Communications, so that the check box is checked.
12. Click Continue.

13. Insert additional disks as requested.
14. The Setup Successful message box displays.
15. Click OK.

This completes installation and the HP OpenView program group has been placed in the Program Manager.

5.14. Other files

Note: This section is provided as a reference for systems using Windows NT version 3.51 and HP OpenView Work Group Node Manager (not Professional Suite).

5.14.1. Install additional files

1. Create the following directory on the hard disk.
C:\SITECTR\
2. Copy all files from the following disks/directories to the directory created in step 1.
Host Sitectr Disk 1 - all files
Host Sitectr Disk 2 - all files
Host Sitectr Disk 3 - files in the main directory
3. Create the following directory on the hard disk.
C:\SITECTR\SYMBOLS\
4. Copy all files from the following disk directory to the directory created in step 3.
Host Sitectr Disk 4 - files in the A:\SYMBOLS\ directory
5. Create the following directory on the hard disk.
C:\UTILITY\
6. Copy all files from the following disk directory to the directory created in step 5.
Host Sitectr Disk 3 - files in the A:\UTILITY\ directory
7. If background maps will be used, copy the graphics files (normally .bmp files) to the following directory. (See Section 5.6.7 for creating background maps.)
C:\OV\BKGROUND\

5.14.2. Modify DEVICES

1. Open the file named C:\OV\OVFILES\DEVICES in an ASCII editor, such as Notepad.
2. Add the following line to the top of the list.

HOST COMPUTER CONFIGURATION

“Cisco Router”	1.3.6.1.4.1.9	0x133a ROUTER	0
----------------	---------------	---------------	---

3. Save the file.

This page intentionally left blank.

SECTION

6. Installation

Figure 6-1 shows an overview of the cables to install Network Management equipment. See Section 2.2 for diagrams of different types of sites.

CAUTION: Flat and round cables with RJ-45 connectors are used for standard Ethernet cables, Ethernet crossover cables, and serial cables. Each type of cable is wired differently. Ethernet cables must be twisted-pair cables. Also, the colors of the wires in the cables may not always be the same or be used for the same function.

CAUTION: DB-9 to RJ-45 adapters are not all wired the same. The following two adapters can **not** be used interchangeably.

- The adapter at the computer end of the serial cable that is used to connect the computer to the router for configuration.
- The adapter at the computer end of the serial cable that is used to connect the computer to the repeater or channel controller MBC for installation. This adapter is also used (with a different cable) to connect the computer to the repeater or channel controller for programming.

Note: For a bi-directional microwave system, the IAC 1 input for repeater 1 at each site should be configured so that the microwave default direction does not cause an alarm.

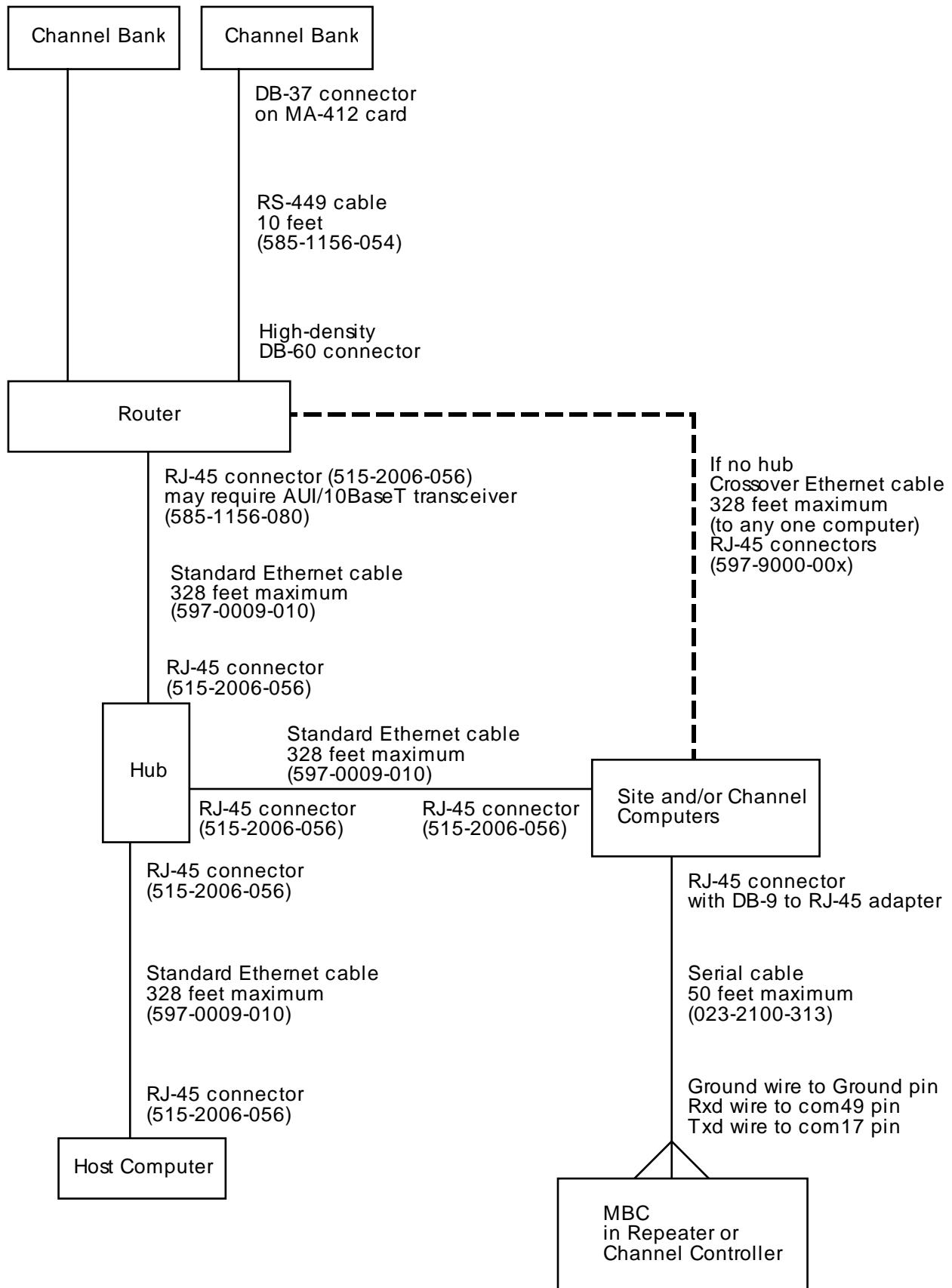
6.1. *MBC in repeaters*

One MBC (message bridge card) is installed at each repeater site. The MBC is normally installed in repeater 1 and can be placed in any slot except the last slot of the repeater. Configure the card as described in Section 6.3 and then wire it to the site computer as described in Section 6.4.

6.2. *MBC in channel controllers*

One MBC (message bridge card) is installed at a channel controller site. The MBC is normally installed in the first shelf and must be placed in the first set of cards. Configure the card as described in Section 6.3 and then wire it to the site computer as described in Section 6.5.

Figure 6-1. Cables for installing Network Management equipment



6.3. **MBC configuration**

Message Bridge Cards (MBCs) from stock need to be configured for Network Management functions. Serialization of the cards should have been performed by production, before the cards were sent to staging.

MBCs also need to have code flashed into them and need to be configured.

6.3.1. **Flash code into MBC**

The code in a file named MBC_ONLY.HEX is flashed into the MBCs using the DWN_BOSS.EXE program

1. Be sure the MBC rear panel connections (COM 17 and COM 49) are not connected to the site controller computer. If these are connected, unplug the cable from the site controller computer COM port.
2. Connect a computer to the MBC's laptop port.
3. Run the flash program with the command "dwn_boss mbc_only.hex". This loads the MBC code into the card.
4. When completed, the MBC card will display F on the front panel 7-segment display.

6.3.2. **Configure MBC**

1. Start the 2000pgmr software using the engineering test mode switch (2000pgmr -e).
2. Select the menu item Hardware -> Tools -> Raw Rx/Tx.
3. Be sure the MODE is set to 0.
4. Enter 34 00. Press Enter.

This configures the MBC card as a primary bridge card and the 7-segment display will show 0. Proper operation is indicated by rapid flashing of the green LED on the MBC card and a 0 on the display.

Although not currently supported, an MBC card may be configured as a secondary bridge card by entering 34 01 in step 4.

6.4. **Site computer to repeater**

The Message Bridge Cable Kit (E.F. Johnson part number 023-2100-313) contains a cable and adapter for connecting the site computer to a repeater that has an MBC installed. The DB-9 end of the adapter plugs into the DB-9 serial (COM) port of the computer. The RJ-45 cable connector plugs into the RJ-45 end of the adapter. At the repeater end, the receive, transmit, and ground wires are attached to the terminal block as shown in the following chart.

	DB-9 pin	RJ-45 pin	Repeater (with MBC) input
Receive	2	4	com49 (pin 10)

	DB-9 pin	RJ-45 pin	Repeater (with MBC) input
Transmit	3	3	com17 (pin 9)
Ground	5	2	ground (pins 21 or 22)

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connector with the cable towards you, the locking mechanism down, and the connector pins facing up.

This cable must not be more than 50 feet long.

6.5. **Channel computer to channel controller**

The Message Bridge Cable Kit (E.F. Johnson part number 023-2100-313) contains a cable and adapter for connecting the channel computer to the channel controller shelf that has an MBC installed. The DB-9 end of the adapter plugs into the DB-9 serial (COM) port of the computer. The RJ-45 cable connector plugs into the RJ-45 end of the adapter. At the channel controller end, the receive, transmit, and ground wires are attached to the top-left terminal block as shown in the following chart.

	DB-9 pin	RJ-45 pin	Channel Controller (with MBC) input
Receive	2	4	com49 (pin 32)
Transmit	3	3	com17 (pin 29)
Ground	5	2	ground (pins 21, 22, 23, or 24)

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connector with the cable towards you, the locking mechanism down, and the connector pins facing up.

This cable must not be more than 50 feet long.

6.6. **Router to site/channel computer**

When there is no hub, an Ethernet crossover cable is used to connect the router to the site computer or to the channel computer. The Ethernet crossover cable is E.F. Johnson part number 597-9000-00x Ethernet Cables - Anixter 10BaseT crossover. The x in the part number indicates cable lengths according to the following chart.

x	cable length	x	cable length
1	1 ft.	4	14 ft.
2	3 ft.	5	25 ft.
3	7 ft		

This cable connects to the RJ-45 port of the computer and to the RJ-45 (or AUI) port of the router. An AUI port requires an AUI to 10BaseT transceiver adapter (E.F. Johnson part number 585-1156-080 AUI/10BaseT Micro Transceiver).

The cable length may be up to 328 feet. Custom lengths may be made by crimping RJ-45 connectors to standard Ethernet cable.

Ethernet Crossover Cable Wiring Chart

RJ-45	Color	Twisted Pair				RJ-45
1	white-orange	x				3
2	orange	x				6
3	white-green		x			1
4	blue			x		4
5	white-blue			x		5
6	green		x			2
7	white-brown				x	7
8	brown				x	8

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connectors with the cables towards you, the locking mechanisms down, and the connector pins facing up.

6.7. Hub to site/channel computer

An Ethernet cable is used to connect the hub to the site/channel computer. This cable connects to the RJ-45 port of the computer and to any RJ-45 port of the hub. The cable length may be up to 328 feet and is made by crimping RJ-45 connectors to standard Ethernet cable.

Cable: E.F. Johnson part number 597-0009-010 - Ethernet Cable - 4 Twisted pair, Blk PVC jacket, 24 AWG solid wire

RJ-45 connectors: E.F. Johnson part number 515-2006-056 - RJ-45 Modular Connector, 8 wire x 8 position, keyed, 24 AWG solid wire

Ethernet Cable Wiring Chart

RJ-45	Color	Twisted Pairs				RJ-45
1	white-orange	x				1
2	orange	x				2
3	white-green		x			3
4	blue			x		4
5	white-blue			x		5
6	green		x			6
7	white-brown				x	7
8	brown				x	8

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connectors with the cables towards you, the locking mechanisms down, and the connector pins facing up.

6.8. Hub to host computer

An Ethernet cable is used to connect the hub to the host computer. This cable connects to the RJ-45 port of the computer and to any RJ-45 port of the hub. The cable length may be up to 328 feet and is made by crimping RJ-45 connectors to standard Ethernet cable.

Cable: E.F. Johnson part number 597-0009-010 - Ethernet Cable - 4 Twisted pair, Blk PVC jacket, 24 AWG solid wire

RJ-45 connectors: E.F. Johnson part number 515-2006-056 - RJ-45 Modular Connector, 8 wire x 8 position, keyed, 24 AWG solid wire

Ethernet Cable Wiring Chart

RJ-45	Color	Twisted Pairs				RJ-45
1	white-orange	x				1
2	orange	x				2
3	white-green		x			3
4	blue			x		4
5	white-blue			x		5
6	green		x			6
7	white-brown				x	7
8	brown				x	8

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connectors with the cables towards you, the locking mechanisms down, and the connector pins facing up.

6.9. Router to host computer

When there is no hub, an Ethernet crossover cable is used to connect the router to the site computer or to the channel computer. The Ethernet crossover cable is E.F. Johnson part number 597-9000-00x Ethernet Cables - Anixter 10BaseT crossover. The x in the part number indicates cable lengths according to the following chart.

x	cable length	x	cable length
1	1 ft.	4	14 ft.
2	3 ft.	5	25 ft.
3	7 ft		

This cable connects to the RJ-45 port of the computer and to the RJ-45 (or AUI) port of the router. An AUI port requires an AUI to 10BaseT transceiver adapter (E.F. Johnson part number 585-1156-080 AUI/10BaseT Micro Transceiver).

The cable length may be up to 328 feet. Custom lengths may be made by crimping RJ-45 connectors to standard Ethernet cable.

Ethernet Crossover Cable Wiring Chart

RJ-45	Color	Twisted Pair				RJ-45
1	white-orange	x				3
2	orange	x				6
3	white-green		x			1
4	blue			x		4
5	white-blue			x		5
6	green		x			2
7	white-brown				x	7
8	brown				x	8

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connectors with the cables towards you, the locking mechanisms down, and the connector pins facing up.

6.10. Hub to router

An Ethernet cable is used to connect the hub to the router. The cable length may be up to 328 feet and is made by crimping RJ-45 connectors to standard Ethernet cable.

This cable connects to any RJ-45 port of the hub and to the RJ-45 (or AUI) port of the router. An AUI port requires an AUI to 10BaseT transceiver adapter (E.F. Johnson part number 585-1156-080 AUI/10BaseT Micro Transceiver).

Cable: E.F. Johnson part number 597-0009-010 - Ethernet Cable - 4 Twisted pair, Blk PVC jacket, 24 AWG solid wire

RJ-45 connectors: E.F. Johnson part number 515-2006-056 - RJ-45 Modular Connector, 8 wire x 8 position, keyed, 24 AWG solid wire

Ethernet Cable Wiring Chart

RJ-45	Color	Twisted Pairs				RJ-45
1	white-orange	x				1
2	orange	x				2
3	white-green		x			3
4	blue			x		4
5	white-blue			x		5
6	green		x			6
7	white-brown				x	7
8	brown				x	8

RJ-45 pins are numbered 1 to 8 from left to right when looking at the connectors with the cables towards you, the locking mechanisms down, and the connector pins facing up.

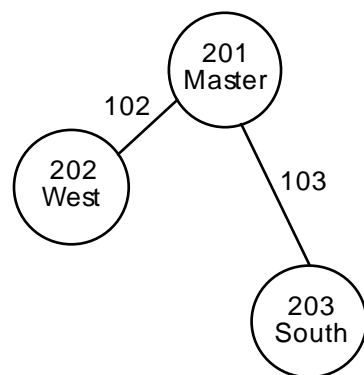
6.11. Router to channel bank

The cable from the router to the Intraplex channel bank is E.F. Johnson part number 585-1156-054 (Cable - RS-449 DTE, Male, 10 ft.). These cables are 10 feet long, so the router must be installed within 10 feet (cable distance) of all attached channel banks.

The high-density DB-60 connector plugs into a high-density DB-60 port of the router. The DB-37 connector plugs into the DB-37 port of the MA-412 card in the channel bank. It is important that the cable from a specific router port plugs into the correct channel bank.

Router ports were assigned IP addresses during configuration to create network subnets (backbones). The cable from a router port must go to the channel bank that transmits to the site at the other end of the network backbone link.

Using the following diagram as an example, at the master site, router serial 0 must attach to the channel bank that transmits to the west site. Router serial 1 must attach to the channel bank that transmits to the south site.



	IP address	Notes
--	------------	-------

INSTALLATION

Master Site		
Router serial 0	100.100.102.1	subnet to West Site
Router serial 1	100.100.103.1	subnet to South Site
Router Ethernet	100.100.201.1	
Site computer	100.100.201.100	
Channel computer	100.100.201.101	
Host computer	100.100.201.200	
West Site		
Router serial 0	100.100.102.2	subnet to Master Site
Router serial 1		
Router Ethernet	100.100.202.1	
Site Computer	100.100.202.100	
South Site		
Router serial 0	100.100.103.2	subnet to Master Site
Router serial 1		
Router Ethernet	100.100.203.1	
Site Computer	100.100.203.100	

This page intentionally left blank.

SECTION

7. Alignment and Calibration

Simulcast systems must be aligned and calibrated to avoid distorted signals in areas that have repeater coverage overlap. Alignment sets the threshold and timing tone gain values. 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).

7.1. Align threshold and timing tone gain

Note: This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

Threshold and timing tone gain must be aligned before calibrating the system. The following procedure will automatically align these values. Threshold and timing tone gain are described in Sections 7.5.5 and 7.5.6.

7.1.1. Alignment procedure

1. A channel defined as the status channel will not properly align. Therefore, if aligning the status channel:

- A. Select the System icon.
- B. Select menu item System -> Manual Repeater Control.
- C. Select the status channel in the channel controller site.
- D. In the Repeater Mode section, de-select Status Channel.
- E. Click the Set Mode button and close the dialog box.

The status channel in the repeater sites does not need to be changed.

- 2. Select a System icon.
- 3. Select menu item System -> Calibration -> Threshold Alignment. The Threshold Alignment dialog box appears.
- 4. Select a channel from the list.
- 5. Click the Start Alignment button.
- 6. Alignment requires some time. Icons to the left of the channel/repeater names will show the progress of the alignment procedure. The icons may change slowly.

If failure occurs, two icons will be displayed beside the repeater name. The left-most icon indicates the type of failure. The icon next to the repeater name indicates the stage of alignment when failure occurred. Repeater disable alarms do not indicate a failure.




For icon descriptions, see Section 7.1.2.

7. Repeat steps 4 through 6 for additional channels.
8. Alignment is complete. Close the dialog box.
9. If the status channel was aligned:
 - A. Select the System icon.
 - B. Select menu item System -> Manual Repeater Control.
 - C. Select the status channel in the channel controller site.
 - D. In the Repeater Mode section, select Status Channel.
 - E. Click the Set Mode button and close the dialog box.
10. If a repeater disable alarm occurred during alignment, enable the repeater:
 - A. Select the System icon.
 - B. Select menu item System -> Manual Repeater Control.
 - C. Select a repeater that has Disabled in the Mode column.
 - D. Select the appropriate mode in the Repeater Mode section.
 - E. Click the Set Mode button.
 - F. Repeat steps C through E as necessary.

7.1.2. Alignment icons

In the System -> Calibration -> Threshold Alignment dialog box, icons appear beside the channel and repeater names to indicate the progression of alignment. The following tables list the icons, their descriptions, and possible causes/remedies. To align, follow the instructions in Sections 7.1.1.

Table 7-1. Channel icons during threshold alignment

Channel Icons	Description	Possible Causes/Remedies
	Other icons will appear to the left of this icon as alignment proceeds. Clicking the box will collapse the repeater list.	To align, follow the instructions in Section 7.1.1.
	Other icons will appear to the left of this icon as alignment proceeds. Clicking the box will show the list of repeaters.	To align, follow the instructions in Section 7.1.1.
	Testing repeaters for zero values.	Alignment is progressing normally. The threshold value is being tested.















Channel Icons	Description	Possible Causes/Remedies
	Testing repeaters for valid values.	Alignment is progressing normally. The timing tone value is being tested.
	Unable to communicate with channel controller.	<ol style="list-style-type: none"> 1. Collisions may have occurred. Retry alignment procedure. 2. Channel controller may be turned off. 3. Determine if there are problems communicating with the site by trying other channels.
	Unknown failure.	<ol style="list-style-type: none"> 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 5.6.2. 3. System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Sections 5.6.1 and 5.6.2.
	Alignment is completed.	

Table 7-2. Repeater icons during threshold alignment

Repeater Icons	Description	Possible Causes/Remedies
	Alignment has not been started.	Align as described in Section 7.1.1.
	Testing repeater for zero values.	Alignment is progressing normally. The threshold value is being tested.
	Increasing threshold level.	Alignment is progressing normally. The threshold value is being adjusted.
	Zero values received successfully.	Alignment is progressing normally. The threshold value is properly set.

Repeater Icons	Description	Possible Causes/Remedies
	Could not get zero values.	Threshold value can not be set. 1. There may be too much noise on the signal. 2. The repeater may be mis-aligned. See the repeater manual for repeater alignment procedures.
	Testing repeater for valid values.	Alignment is progressing normally. The timing tone value is being tested.
	Could not get valid values.	The timing tone value can not be set. The repeater may be mis-aligned. See the repeater manual for repeater alignment procedures.
	Unable to communicate with repeater.	1. Collisions may have occurred. Retry alignment procedure. 2. Repeater may be turned off. 3. Determine if there are problems communicating with the site by trying other channels.
	Unknown failure.	1. IP address may be incorrect. Check assignment in EFJ Site Description dialog box. See Section 5.6.2. 2. System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Sections 5.6.1 and 5.6.2.
	This repeater is successfully aligned.	

7.2. Calibrate uni-directional, non-redundant systems

Note: This section is for calibrating uni-directional, non-redundant microwave systems. Section 7.3 is for bi-directional, non-redundant microwave systems. The program will display the appropriate dialog box and help for the system.

Note: The System -> Calibration -> Edit Offsets dialog box defines the type of system (uni- or bi-directional, and non-redundant or redundant). See Section 5.7.

If the system type is changed, OpenView must be restarted before changes take effect.

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 7.2.1.
2. Write procedure: The calculated values are written to the Simulcast Modulation Cards (SMCs) in the repeaters. See Section 7.2.3.

7.2.1. 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 7.2.2 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 7.2.3. 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.

7.2.2. 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 7-3. 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 7.2.1.
	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 7.2.1.
 flashing	Data acquisition is in progress.	Be patient until data acquisition has finished. Each repeater takes approximately 15 to 20 seconds.
	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 7.2.3.
	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.
	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
	Unknown failure.	<p>1. The channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller.</p> <p>2. IP address may be incorrect. Check assignment in EFJ Site Description dialog box. See Section 5.6.2.</p> <p>3. System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Sections 5.6.1 and 5.6.2.</p>

Table 7-4. 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 7.2.1.
OK	Data acquisition was successful.	If data is not to be acquired from other channels, continue with the write procedure in Section 7.2.3.
F	<p>Data acquisition failed.</p> <p>Possible causes:</p> <p>1. The repeater is reverted.</p> <p>2. The channel controller's timing tone gain is set too low.</p> <p>3. The repeater's threshold is set too high.</p>	<p>1. Fix the problems that have caused the repeater to revert. Unrevert the repeater. Recalibrate the channel.</p> <p>2. Perform the alignment described in Section 7.1.</p> <p>3. Perform the alignment described in Section 7.1.</p>

Repeater Icons	Description	Remedy
	<ol style="list-style-type: none"> Noise may have interfered with access to the repeater. The repeater's threshold value may be set incorrectly. 	<ol style="list-style-type: none"> Retry data acquisition. Perform the alignment described in Section 7.1.

7.2.3. 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.

7.3. Calibrate bi-directional, non-redundant systems

Note: This section is for calibrating bi-directional, non-redundant microwave systems. Section 7.2 is for uni-directional, non-redundant microwave systems. The program will display the appropriate dialog box and help for the system.

Note: The System -> Calibration -> Edit Offsets dialog box defines the type of system (uni- or bi-directional, and non-redundant or redundant). See Section 5.7. If the system type is changed, OpenView must be restarted before changes take effect.

Note: For a bi-directional microwave system, the IAC 1 input for repeater 1 at each site should be configured so that the microwave default direction does not cause an alarm.

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.

7.3.1. 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 7.3.3 for icon descriptions and remedies.

8. Repeat steps 4-7 for additional channels.

7.3.2. 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 7.3.3 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 7.3.4. 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.

7.3.3. 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 7-5. 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 7.3.1 and 7.3.2.
	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 7.3.1 and 7.3.2.
 flashing	Data acquisition is in progress.	Be patient until data acquisition has finished. Each repeater takes approximately 15 to 20 seconds.
	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 7.3.4.
	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.
	Data acquisition for the channel is half completed.	Continue to phase 2 data acquisition. See Section 7.3.2.
	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
	Unknown failure.	<p>1. The channel controller may be described incorrectly. In the channel controller's Describe dialog box, the Repeater Type should be Simulcast Controller.</p> <p>2. IP address may be incorrect. Check assignment in EFJ Site Description dialog box. See Section 5.6.2.</p> <p>3. System and/or Site numbers may be incorrect. Check assignments in EFJ System Description and EFJ Site Description dialog boxes. See Sections 5.6.1 and 5.6.2.</p>

Table 7-6. 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 7.3.1 and 7.3.2.
	Data acquisition was successful.	If data is not to be acquired from other channels, continue with the write procedure in Section 7.3.4.
	<p>Data acquisition failed.</p> <p>Possible causes:</p> <p>1. The repeater is reverted.</p> <p>2. The channel controller's timing tone gain is set too low.</p> <p>3. The repeater's threshold is set too high.</p>	<p>1. Fix the problems that have caused the revert. Unrevert the repeater. Recalibrate the channel.</p> <p>2. Perform the alignment described in Section 7.1.</p> <p>3. Perform the alignment described in Section 7.1.</p>
	<p>1. Noise may have interfered with access to the repeater.</p> <p>2. The repeater's threshold value may be set incorrectly.</p>	<p>1. Retry data acquisition.</p> <p>2. Perform the alignment described in Section 7.1.</p>

7.3.4. 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.

7.4. *Determine and set overlap offset*

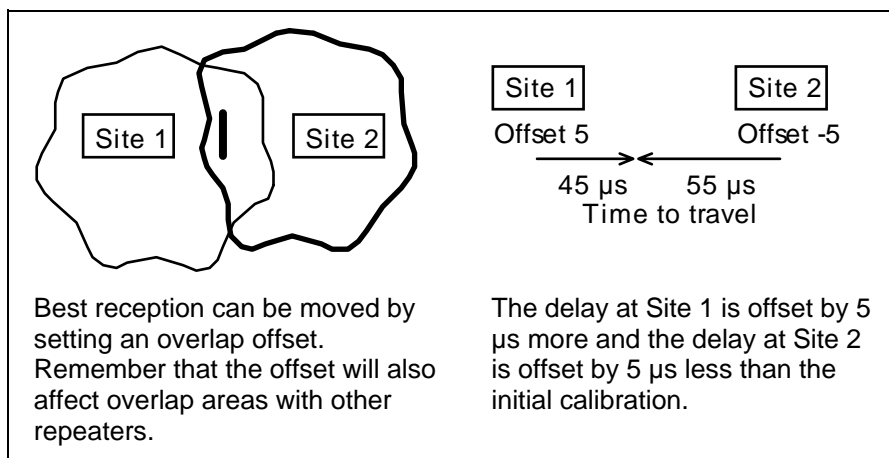
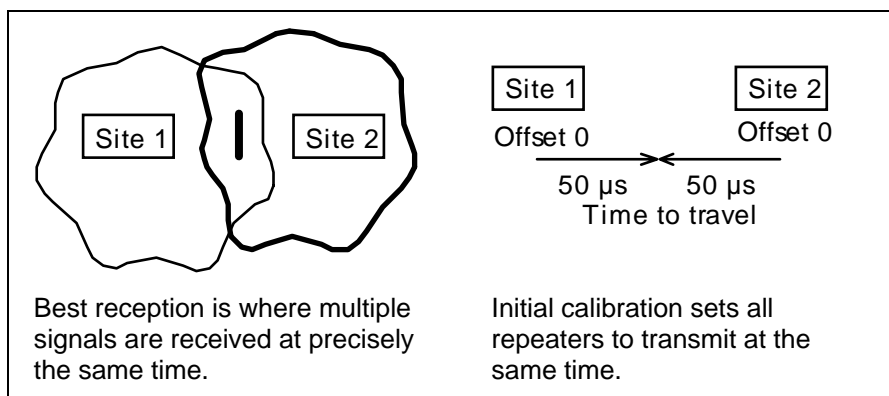
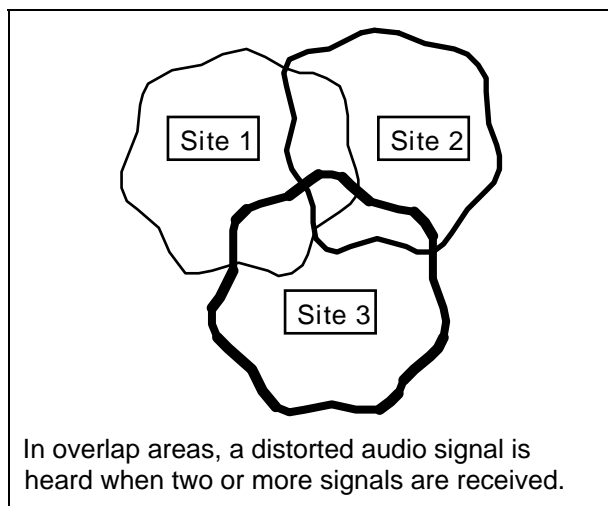
7.4.1. Description of overlap offset

In a simulcast system, repeater coverage areas overlap. A radio in the overlap area may receive two or more signals. If the signal strengths are similar, the radio's receive circuits will capture two or more signals. The signals often will not arrive at precisely the same time; therefore, the audio from the radio will be distorted. The amount of distortion will be more noticeable in some locations than in other locations, depending on the distance between the location and each site that is heard.

The distortion pattern of the overlap area can be changed with overlap offsets. Initially, repeaters are calibrated so that they all transmit at the same time. An overlap offset will cause a repeater to transmit a little earlier or a little later than the initial calibration time. A change in the time of transmission will change the time the signal arrives at the location and therefore change the amount of distortion at each location.

Overlap offset values are set in increments of 1 microsecond. For a rule of thumb: A radio signal travels at 0.186 mile per microsecond, so a setting of 5 microseconds will move the distortion pattern approximately 1 mile.

Figure 7-1 illustrates the overlap offset concept.

Figure 7-1. Overlap offset concept**7.4.2. Determine overlap offset values**

Note: Calibration must be completed first. Refer to Section 7.2 for uni-directional, non-redundant systems, or Section 7.3 for bi-directional, non-redundant systems.

Note: This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

Overlap offset values are determined by changing the buffer delay values from the SMC Configuration dialog box. The buffer delay values must then be returned to their original calibrated values and the overlap offset values are entered in the Edit Offsets dialog box. With this arrangement, the system can be periodically calibrated for minor propagation changes without affecting the overlap offset values.

Overlap offset values apply to a site; therefore, only one channel needs to be used to determine the values.

1. Select a System icon.
2. Select menu item System -> Calibration -> SMC Configuration.
3. Select a repeater from the list.
4. Click the Read button.
5. From the Buffer Delays section, make a note of the Buffer Delay value for the active User Defined Setting. This value will be needed for a calculation at the end of these instructions.
6. Modify the Buffer Delay value.

Each increment changes the transmit time 1 microsecond, which is the amount of time it takes the signal to travel approximately 0.186 mile. The signal travels approximately 1 mile in 5 increments of time.

Incrementing in a positive direction increases the delay before transmitting, which moves the point of minimum distortion closer to the repeater. Decrementing in a negative direction decreases the delay before transmitting, which moves the minimum distortion point farther from the repeater.

7. Click the Write button.
8. Repeat steps 3 through 7 for other repeaters on the channel that affect the overlap area.
9. Check the reception in the overlap area.
10. If necessary, repeat steps 3-4 and 6-9 until the overlap area distortion pattern is acceptable. Do not repeat step 5.
11. Make a note of the new Buffer Delay value for each repeater that was changed.
12. Subtract the values noted in step 5 from the values noted in step 11. Results may be negative or positive and will be entered in the Edit Offsets dialog box as described in Section 7.4.3.

7.4.3. Set overlap offset values and recalibrate system

Note: This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

1. Select a System icon.
2. Select menu item System -> Calibration -> Edit Offsets.

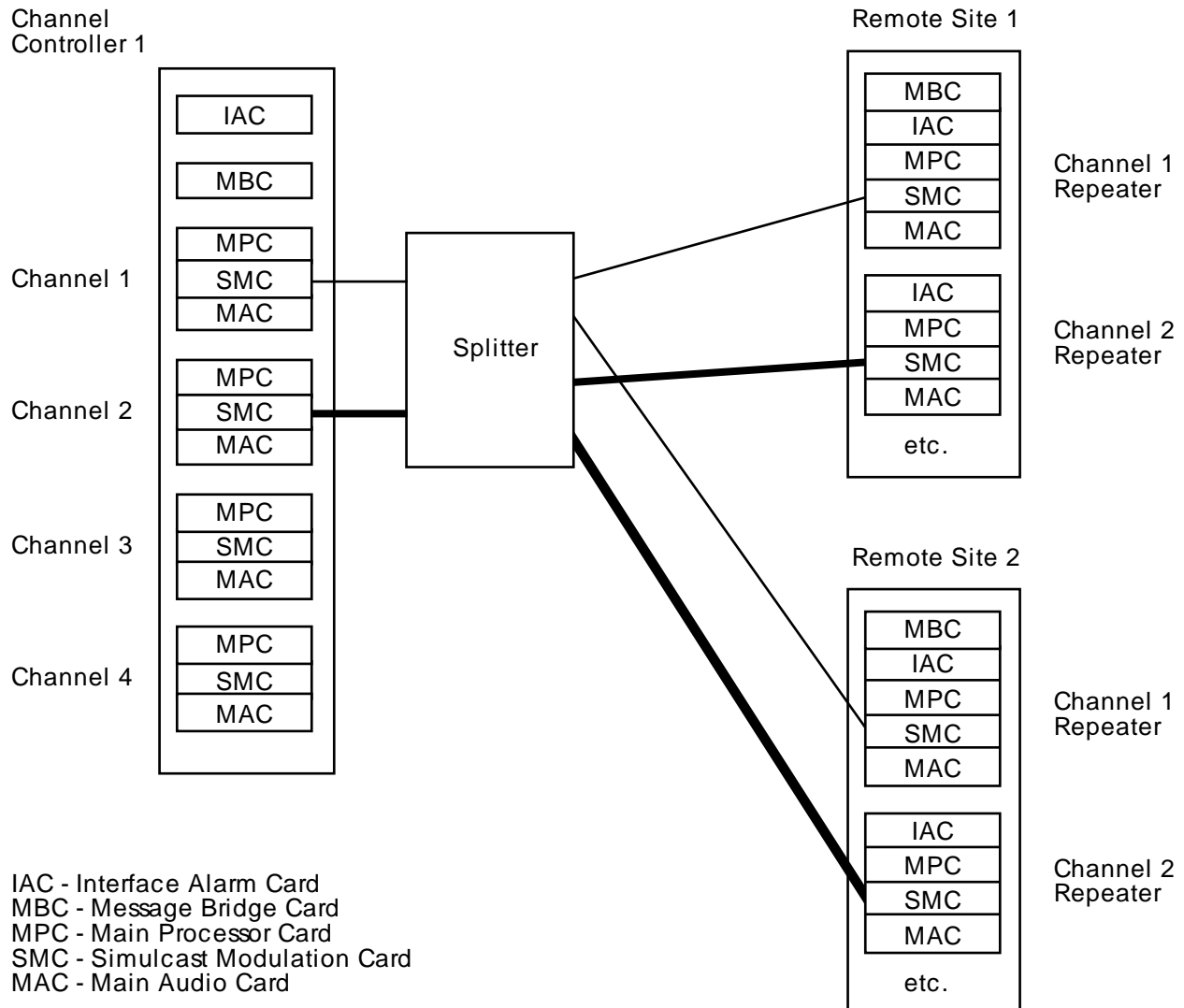
3. Select a site from the list.
4. Enter the offset value in the Overlap Offset box. Enter a hyphen before negative numbers. This value can be from -100 to 100 microseconds.
5. Click the Save Site button.
6. Repeat steps 3 through 5 for all sites.
7. Recalibrate all affected channels. See Section 7.2 for uni-directional, non-redundant systems, or Section 7.3 for bi-directional, non-redundant systems.

7.5. Set SMC parameters from OpenView

Note: Correct values are essential for proper simulcast reception in areas where repeater coverage overlaps. These values should only be changed by a trained simulcast technician.

Note: This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

Several parameters on the SMCs (Simulcast Modulation Cards) can be changed from OpenView. Each repeater has an SMC and each channel has an SMC in the channel controller, as shown in Figure 7-2.

Figure 7-2. SMC channel communication links

7.5.1. Read/Write parameters

SMC parameters are changed from the SMC Configuration dialog box, which is accessed by selecting a System icon and then selecting menu item System -> Calibration -> SMC Configuration.

The dialog box shows the system name and a list of sites and repeaters (including channel controllers). To change parameters, select a repeater in the list and then click the Read button. The program will read the current SMC parameters that are in the selected repeater and display them in the dialog box.

After changing the desired values, write the changes to the SMC by clicking the Write button.

7.5.2. Audio Gain

This value affects the gain or volume of the repeater's audio output signal. Changing the value in a repeater SMC will change the gain of the audio output of that repeater. Changing the value in a channel controller SMC will change the gain of the audio signal that is transmitted to all repeaters on the channel.

The output audio signal will be multiplied by the Audio Gain value. Values may be from 0.0000 to 2.0000. Values greater than 1 will increase the gain; values less than 1 will decrease the gain. A value of 0 will result in no signal and a value of 2.0000 may result in a clipped, distorted signal.

7.5.3. Data Gain

This value affects the gain or volume of the repeater's data output signal. Changing the value in a repeater SMC will change the gain of the data output of that repeater. Changing the value in a channel controller SMC will change the gain of the data signal that is transmitted to all repeaters on the channel.

The output data signal will be multiplied by the Data Gain value. Values may be from 0.0000 to 2.0000. Values greater than 1 will increase the gain; values less than 1 will decrease the gain. A value of 0 will result in no signal and a value of 2.0000 may result in a clipped, distorted signal.

7.5.4. Pilot Tone Gain

This value affects the gain or volume of the pilot tone sent by the channel controller SMC. The channel controller sends a pilot tone (of 2600 Hz) when no call is in progress. The absence of the pilot tone keys the remote repeaters push-to-talk circuit so that a call will be transmitted.

The output pilot tone signal will be multiplied by the Pilot Tone Gain value. Values may be from 0.0000 to 1.0000. A value of 0 will result in no signal and a value of 1.0000 will result in a clipped, distorted signal.

An SMC that is in a repeater does not use this value.

7.5.5. Threshold

A repeater SMC uses the threshold value to determine if the incoming signal is a timing tone or noise. During calibration, a timing tone is sent by the channel controller SMC. The repeater SMC detects when it starts receiving the timing tone. The difference between when the channel controller SMC sent the tone and the time the repeater SMC received the tone is the basis for buffer delays that are necessary for good reception in overlapping areas. To ensure that all SMCs are using the same time, the timing tone is sent once per second based on the 1 PPS (pulse per second) signal from the GPS (global positioning system).

The threshold value is a number from 0.0000 to 1.0000. A threshold value that is too low will cause noise to be detected as the timing tone and a value that is too high will cause a late detection of the beginning of the tone. If the SMC in the repeater detects a beginning of the timing tone that is not within one cycle time

(125 microseconds) of the real beginning of the tone, the buffer delays will not be calibrated correctly.

An SMC that is in a channel controller does not use this value.

7.5.6. Timing Tone Gain

This value affects the gain or volume of the timing tone sent by the channel controller SMC during calibration.

The output timing tone signal will be multiplied by the Timing Tone Gain value. Values may be from 0.0000 to 1.0000. A value of 0 will result in no signal and a value of 1.0000 will result in a clipped, distorted signal.

An SMC that is in a repeater does not use this value.

7.5.7. Buffer Delays section

Buffer delays and phase used to begin transmitting can be defined by the dip switch settings on the repeater's SMC or by values entered into set 0 or set 1. When parameters are read (with the Read button), the radio buttons show which setting is currently being used. To change settings, select a different radio button, change the values (if needed), and write the settings to the repeater's SMC with the Write button. Dip switch values cannot be changed from the program; they can only be changed by physically moving the switches on the SMC. (An SMC that is in a channel controller does not use these values.)

Buffer Delay: This value can be from 126 to 63,999 microseconds and is the amount of time the repeater needs to delay after receiving a signal before transmitting the signal.

It takes time for a signal to get from the channel controller to site 1. It takes a different amount of time for a signal to get from the channel controller to site 2. If site 1 and site 2 are going to transmit the signal at the same time, they must buffer the signal and wait a period of time until they can both transmit at the same time. Buffer Delay is the period of time the repeater must wait between the ending of signal processing and the beginning of transmitting the signal.

Phase: This value can be from 0 to 255. Each increment is approximately 1.4 degrees.

The signals from all sites must be transmitted with the same phase for best reception. The phase of the signals received at different sites will be different because of the different amount of time it takes to get to each site. The phase value should compensate for this difference so that all signals are transmitted with the same phase.

SECTION

8. Update Software**8.1. Update site controller application (Windows NT 4.0)**

Note: Follow these instructions if the host computer is running Windows NT 4.0. If the host computer is running Windows NT 3.51, follow the instructions in Section 8.3.

Updating the site controller application in the site and channel computers is done from the host computer. A connection will be made from the host computer to the site/channel computer. Then, the sitectl.exe file will be copied, or sent, to the remote computer.

A. Connect to the remote computer

1. Double-click on the Network Neighborhood icon. The Network Neighborhood window appears.
2. Click the Map Network Drive button (the second button on the toolbar). The Map Network Drive dialog box appears.
3. In the Path box, enter:

\\<computername>\c\$

where <computername> is the name of the remote site/channel computer.

For example: \\west-hub\c\$

Alternatively, the computer's IP address can be entered instead of computername.

4. In the Connect As box, enter:

efjohnson

5. Click OK. A window appears that shows the directory of the remote computer.

B. Copy the sitectl.exe file to the remote computer

1. Put the update disk into the A drive.
2. Click Start on the taskbar.
3. Select menu item Programs -> Windows NT Explorer. The Exploring window appears.
4. Click the plus sign to the left of

c\$ on <computername>

A list of folders appears under the computer name.

5. Click the plus sign to the left of the sitectr folder that is in the above list. The folder opens.
6. Click on the 3-1/2 Floppy (A:) icon. The right window shows the A directory.
7. In the right window, click once on sitectl.exe.

8. Select menu item Edit -> Copy.
9. In the left window, click on the tmp folder that is in the sitectr folder of step 5.
10. Select menu item Edit -> Paste. A Confirm File Replace message box appears.
11. Click Yes. The file is copied (sent) to the remote computer.
12. Close the Exploring window.

C. Reboot and disconnect from the remote computer

1. Click Start on the taskbar.
2. Select menu item Programs -> Command Prompt. The Command Prompt window appears.
3. At the C:\ prompt, enter:
`reboot <computername>`
4. Press Return.
5. Within 20 seconds:
 - A. Make the c\$ on <computername> window the active window.
 - B. Click the Disconnect Net Drive icon (the third icon in the toolbar). The Disconnect Network Drive dialog box appears.
 - C. Click OK. A warning message appears.
 - D. Click Yes. The directory window closes and the connection to the remote computer is disconnected.
6. To update additional site/channel computers, repeat steps A1 through C5. These instructions should be completed for each site/channel computer in the system.
7. Remove the update disk from drive A.

8.2. Uninstall host computer software (Windows NT 4.0)

Note: These instructions will uninstall the E.F. Johnson application, the Borland database engine, and will modify any necessary files.

1. Exit OpenView.
2. Click Start on the taskbar.
3. Select menu item Programs -> Host Computer -> Uninstall E.F. Johnson Host Computer. The Confirm File Deletion message box appears.
4. Click Yes.
5. The files are deleted and the Remove Programs From Your Computer dialog box appears. Additional files do **not** need to be removed manually.
6. Click OK.

To install software, see Section 5.5.

8.3. **Update site controller application (Windows NT 3.51)**

Note: Follow these instructions if the host computer is running Windows NT 3.51. If the host computer is running Windows NT 4.0, follow the instructions in Section 8.1.

Updating the site controller application in the site and channel computers is done from the host computer. A connection will be made from the host computer to the site/channel computer. Then, the sitectl.exe file will be copied, or sent, to the remote computer.

A. Setup

1. Open the Program Manager.
2. Open the Main Program Group.
3. Open the File Manager.
4. Make the Program Manager the active window. (Hold the Alt key. Press the Tab key repeatedly until the Program Manager name appears in the popup box. Release the Alt key.)
5. Open the Command Prompt. Move the Command Prompt window so that some part of the window will be visible when the File Manager is the active window.
6. Make the File Manager the active window.
7. Click on the Options menu.
8. Verify that "Open New Windows on Connect" has a check mark before it. If there is a check mark, click the Options menu so that the menu disappears. If there is no check mark, click on Open New Windows on Connect.
9. Put the update disk into the A drive.
10. Click on the A drive icon. The File Manager window displays the A drive information.

B. Connect to the remote computer

1. Select menu item Disk -> Connect Network Drive. A dialog box appears.
2. In the Path box, enter:
`\\<computername>\c$`
 where <computername> is the name of the remote site/channel computer.
 For example: `\\west-hub\c$`
3. In the Connect As box, enter:
`efjohnson`
4. Click OK. The Enter Network Password dialog box appears.
5. Enter the password of the remote site/channel computer.
6. Click OK. A box appears that shows the directory of the remote computer.
7. Select menu item Window -> Tile Horizontally.

C. Copy the sitectrl.exe file to the remote computer

1. In the directory of the remote computer, double-click on the sitectr directory name to open the directory. A tmp directory appears below and is indented from the sitectr directory.
2. Click once on the tmp directory name to select the tmp directory.
3. From the A directory, copy the sitectrl.exe file to the remote computer's \sitectr\tmp\ directory.
4. A Confirm Mouse Operation message box appears.
5. Click Yes.
6. A Confirm File Replace message box appears.
7. Click Yes.

D. Reboot and disconnect from the remote computer

1. Make the Command Prompt the active window.
2. Enter:


```
reboot <remote computer name>
```

where <remote computer name> is the name of the remote site/channel computer. For example: reboot west-hub
3. Press the Enter key.
4. Within 20 seconds, in the File Manager window, select menu item Disk -> Disconnect Network Drive. A dialog box appears.
5. Click OK.
6. To update additional site/channel computers, repeat these steps beginning with "B. Connect to the remote computer". These instructions should be completed for each site/channel computer in the system.
7. Remove the update disk from drive A.

8.4. Uninstall host computer software (Windows NT 3.51)

Note: These instructions will uninstall the E.F. Johnson application, the Borland database engine, and will modify any necessary files.

1. Exit OpenView.
2. Open the Program Manager.
3. Open the Host Computer program group. (If this program group does not exist, follow the instructions in Section 8.6.)
4. Open the Uninstall E.F. Johnson Host Computer program. The Confirm File Deletion message box appears.
5. Click Yes.

6. The files are deleted and the Remove Programs From Your Computer dialog box appears. Additional files do **not** need to be removed manually.
7. Click OK.

8.5. Install host computer software (Windows NT 3.51)

Note: These instructions will install the E.F. Johnson application, the Borland database engine, and will modify any necessary files.

1. Put the disk named E.F. Johnson Host Computer Disk 1 into the drive.
2. From the Program Manager, select menu item File -> Run.
3. Click Browse.
4. In the drive section, select the floppy drive.
5. In the filename section, select setup.exe.
6. Click OK.
7. Click OK in the Run dialog box.
8. Follow the on-screen instructions and insert disks as needed. Accept the defaults in all dialog boxes.
9. When installation is completed, the Program Manager will appear with a new program group named Host Computer.

8.6. Remove host computer software (Windows NT 3.51)

Note: These instructions should only be used on computers where the programs were not installed with the installation program. Look in the Program Manager for a program group called Host Computer. If it exists, see Section 8.4 for uninstalling the software.

The following instructions will remove the E.F. Johnson application from the hard disk.

1. Exit OpenView.
2. Open the File Manager
3. Select the sitectr directory.
4. Press the Del key. The Delete message box appears.
5. Click OK. The Confirm Directory Delete message box appears.
6. Click Yes to All.
7. The files are deleted.
8. In the File Manager, select the OV directory.
9. Open the OVWIN.INI file in an ASCII editor, such as Notepad.
10. In the [OpenViewApps] section, delete the following line:

SITECTR=C:\SITECTR\SITECTR.EXE

11. Save the file.
12. Close the File Manager.

8.7. Install Windows NT 4.0

Note: These instructions are for installing Windows NT 4.0 onto host computers that come without Windows installed or that need to have Windows re-installed.

Windows NT 4.0 installation files are on 3 floppy disks and 1 CD.

1. Put Setup Disk 1 (or Boot Disk) into the disk drive.
2. Reboot the computer. The Window's Setup program will be automatically started.
3. Follow the screen instructions. Press Enter to accept the defaults and insert floppy disks as requested.
4. When requested, put the CD disk in the drive and press Enter.
5. Page down through the License Agreement and press F8 to agree.
6. If a message says that Windows NT was found, press N to re-install Windows.
7. Except for the following, press Enter to accept defaults and continue.
 - Format the partition using the NTFS file system. (Use the up and down arrow keys to make a selection.)
 - Press ESC to skip examination for corruption, unless the computer has been having numerous disk errors.
8. Files are copied to the hard disk and this portion of the setup is completed. Take the CD and floppy disk out of the drive and restart the computer.
9. When asked, put the CD into the drive and click OK. More files are copied to the hard disk.
10. The Windows NT Setup wizard appears.
11. Click Next to gather information about the computer.

A. Gather information

1. In the Setup Options window, select Typical, and click Next.
2. In the Name and Organization window, enter the customer name and organization. Click Next.
3. In the Registration window, enter the CD key from the back of the CD folder, and click Next.
4. In the Computer Name window, enter the host name for the computer, and click Next.
5. In the Administrator Account window, enter the Windows NT administrator password in both the Password and the Confirm Password boxes. Click Next.
6. In the Emergency Repair Disk window, select Yes, and click Next.

7. In the Windows NT Components window, select “Install the most common components”. Click Next.
8. The Windows NT Setup window appears. Click Next to install Windows NT Networking.

B. Install Windows NT networking

1. A window appears that requests information on the method Windows NT should use to participate on a network.
2. Select “This computer will participate on a network”.
3. Select “Wired to the network”.
4. Click Next. The network adapters window appears.
5. Click Start Search. Network adapters are added to the list.
6. When the search is finished, click Next. The network protocols window appears.
7. Select “TCP/IP Protocol”.
8. Click Next. The network services window appears.
9. Click Next to accept the defaults. The install window appears.
10. Click Next to install files. A window asking for the CD drive letter appears.
11. Enter the CD drive letter and i386. For example,
D:\i386
12. Click Continue.
13. A window displays the setup for the card:

I/O Port Address	0x300
Interrupt Number	10
Transceiver Type	10BaseT
14. Click Continue to accept the defaults.
15. A setup message reports that the parameters are not verifiably correct.
16. Click OK to use them anyway.
17. The DHCP server window appears.
18. Click No.
19. Network files are copied and installed onto the hard disk.

C. TCP/IP Properties

1. The Microsoft TCP/IP Properties window appears.
2. Enter the IP address, subnet mask, and default gateway for this computer.
3. Click the DNS tab.

4. Verify that the host name is correct for this computer. (It should be the same as the computer name.)
5. Click OK.
6. Click Yes or Next to accept the defaults on the remaining networking setup windows.
7. The Windows NT Setup window appears. Click Finish to finish setup.

D. Finishing setup

1. The Date & Time Properties window appears.
2. Select the appropriate time zone from the drop down list.
3. If appropriate, select Automatically adjust clock for daylight savings changes.
4. Click the Date & Time tab.
5. Select the current date and time. Remember to account for the time zone.
6. Click Close.
7. The Detected Display message box appears. Click OK.
8. The Display Properties window appears.
9. In the Color Palette section, select 65,536 colors.
10. In the Desktop Area section, move the pixel slider to 1024 by 768 pixels. This may cause the palette section to change if the palette/pixel combination is not supported by the monitor.
11. Click Test. The testing mode message box appears.
12. Click OK. The test screen appears.
13. Click Yes if the bitmap appeared properly. The display settings message box appears.
14. Click OK.
15. Click OK in the Display Properties window.
16. Setup continues by copying files to the hard disk.
17. The Setup message box appears. Put a floppy in the drive to create the Emergency Repair Disk and click OK.
18. Files are copied to the floppy disk. When copying is finished, remove the disk from the drive.
19. The Windows NT Setup message box appears.
20. Click OK to reboot the computer.
21. This completes the installation of Windows NT. Remove any disks or CDs from the drives. See Section 5 for additional Windows NT setup and other host computer installations.

This page intentionally left blank.

SECTION

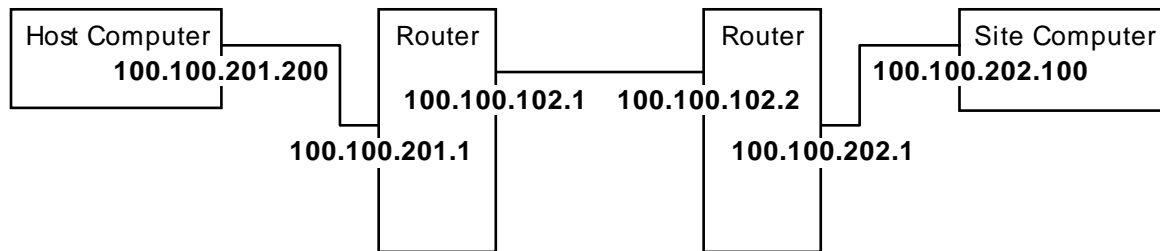
9. Troubleshooting

9.1. 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 9-1 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 9-1. 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.)

9.2. Troubleshooting from a router

Routers have several commands that can be used for troubleshooting. These commands can be accessed from a computer attached to the router (for attachment information see Section 3.1). Some of the commands can also be accessed after telnetting to the router from another router or computer. (To telnet from a router, see Section 9.2.6. To telnet from a computer, see Section 9.3.3.)

When a computer is attached to a running router, press <Enter> to gain access to the router. The router will then ask for a password. This is the <line password> entered during configuration for “line con 0”.

When telnetting to a router, the router will send a sign-on message and then ask for a password. This is the <virtual terminal password> entered during configuration for “line vty 0 4”.

The “config t” command needs to be entered before the router will accept most configuration commands (see Section 3.2).

When finished, the “logout” command will close the local or telnet connection. (If the “config t” command was entered, enter the “end” command before the “logout” command.)

9.2.1. Show ARP - list of IP address in subnet

This command will list the IP addresses of all devices that are on the same subnet as the router. If the router cannot communicate with a device, possibly because of device problems or incorrect connections, the IP address of that device will not be listed.

The example below shows the result of a show arp command that was given to a router named oc_rtr. The devices with IP addresses 100.100.201.200 and 100.100.201.1 are on the same subnet as the router named oc_rtr.

```
oc_rtr>show arp
Protocol Address          Age (min)    Hardware Addr  Type   Interface
Internet 100.100.201.200        5           00a0.24a3.7f1a  ARPA   Ethernet0
Internet 100.100.201.1          -           0000.0c5d.bb76  ARPA   Ethernet0
oc_rtr>
```

9.2.2. Show hosts - list of host names and IP addresses

This command will list the host names and IP addresses of network devices, as shown in the example below. The router was given this information during configuration with the “ip host <name> <ip address>” command.

```
oc_rtr>show hosts
Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Host                Flags      Age Type   Address(es)
west                (perm, OK) 44  IP      100.100.102.2
south              (perm, OK) 44  IP      100.100.103.2
oc_hub             (perm, OK) **  IP      100.100.201.100
oc_chan            (perm, OK) **  IP      100.100.201.101
west_hub           (perm, OK) **  IP      100.100.202.100
south_hub          (perm, OK) **  IP      100.100.203.100
oc_host            (perm, OK) **  IP      100.100.201.200
oc_rtr>
```

9.2.3. Show IP route - list of known subnets and routes

The show IP route command displays a list of all subnets and routes that the router knows about. If a remote router is working and the device(s) connected to it is (are) not working, the list will show that the subnet is possibly down.

The following example shows the result of a show ip route command. The line highlighted with a dashed box shows the network portion of the IP address (100.0.0.0), the subnet mask (255.255.255.0), and the number of known subnets (5 subnets).

Below the dashed box, the three lines beginning with “C” are the subnets that are attached to the router’s ports. For example, the subnet 100.100.102.0 includes the Serial0 port of the router.

The next two lines (that begin with “I”) show subnets that the router discovered by using IGRP (Interior Gateway Routing Protocol). This information includes the IP address of the remote router that is used to get to a subnet and the port of this router that is used to reach the remote router. For example, subnet 100.100.202.0 is reached by going to IP address 100.100.102.2, which can be reached through this router’s Serial0 port.

```

oc_rtr>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default

Gateway of last resort is not set

100.0.0.0 255.255.255.0 is subnetted, 5 subnets
C      100.100.102.0 is directly connected, Serial0
C      100.100.103.0 is directly connected, Serial1
C      100.100.201.0 is directly connected, Ethernet0
I      100.100.202.0 [100/178771] via 100.100.102.2, 00:00:56, Serial0
I      100.100.203.0 [100/178771] via 100.100.103.2, 00:00:47, Serial1
oc_rtr>

```

The example below shows a response that includes a subnet that has problems. The last line shows that subnet 100.100.203.0, subnet mask 255.255.255.0 is possibly down. The router knows that the route to subnet 100.100.203.0 is through IP address 100.100.103.2. The router can communicate with 100.100.103.2, but it cannot communicate with any devices on subnet 100.100.203.0.

```

oc_rtr#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default

Gateway of last resort is not set

100.0.0.0 255.255.255.0 is subnetted, 5 subnets
C      100.100.102.0 is directly connected, Serial0
C      100.100.103.0 is directly connected, Serial1
C      100.100.201.0 is directly connected, Ethernet0
I      100.100.202.0 [100/178771] via 100.100.102.2, 00:00:09, Serial0
I      100.100.203.0 255.255.255.0 is possibly down,
        routing via 100.100.103.2, Serial1

```

To further verify the problem, telnet to 100.100.103.2 and look at the response to its show ip route command. (Telnet is described in Section 9.2.6.)

```

oc_rtr#telnet south
Trying south (100.100.103.2)... Open

South Site Cisco 2501

User Access Verification

Password: <virtual terminal password>

```

As shown below, the show ip route command at the remote router only shows 4 subnets. The 100.100.203.0 subnet is not shown because there are no working routes to devices on the subnet; therefore, the subnet does not exist.

```

south_rtr>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

```

```

        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
Gateway of last resort is not set

    100.0.0.0 255.255.255.0 is subnetted, 4 subnets
I       100.100.102.0 [100/178771] via 100.100.103.1, 00:00:28, Serial0
C       100.100.103.0 is directly connected, Serial0
I       100.100.201.0 [100/178771] via 100.100.103.1, 00:00:28, Serial0
I       100.100.202.0 [100/178871] via 100.100.103.1, 00:00:28, Serial0
south_rtr> logout
oc_rtr>

```

When finished with the remote router, the logout command will return the prompt to the local router.

9.2.4. Show int - information on ports

Entering the show int command will display information about all serial and Ethernet ports of the router. At the end of each port's information, the router will pause and display: ---more---. To see the next port's information, press the space bar. To abort the command, press the letter n (for no).

To get information on a specific port, also enter the port name.

Examples:

show int - Displays information about all ports.

show int e0 - Displays information about the Ethernet0 port.

show int s0 - Displays information about the Serial0 port.

9.2.5. Ping from router

To ping a device (router or computer), enter the ping command and the unique host name or IP address of the device. (Host names were entered during configuration with the "ip host <name> <ip address>" command and can be viewed with the "show hosts" command described in Section 9.2.2.) See Section 9.1 for ping troubleshooting techniques.

Example:

```

oc_rtr> ping south
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.103.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/44 ms

```

To ping all routers with one command, enter:

```
ping 255.255.255.255 ?
```

Each router that receives the ping will respond with its IP address.

The escape sequence to abort ping is entered by simultaneously pressing the Ctrl, Shift, and 6 keys, releasing the keys, and then pressing the X key.

The chart below shows the possible responses when pinging a specific router.

!	Reply was received.
---	---------------------

.	Timed out while waiting for a reply.
U	Destination unreachable error was received.
C	Congestion experienced packet was received.
I	Test interrupted by user.
?	Unknown packet type.
&	Packet lifetime exceeded.

9.2.6. Telnet from router

Telnet (terminal emulation protocol) allows the local keyboard and monitor to act as though they were attached to a remote device. Once a telnet connection is made, the information typed on the local keyboard is sent to the remote device and the local monitor displays information from the remote device.

To establish a connection from a router's prompt, enter the telnet command and the unique host name or IP address of a remote router. (Host names were entered during configuration with the "ip host <name> <ip address>" command and can be viewed with the "show hosts" command described in Section 9.2.2.)

As shown in the following example, the router will show that it is trying to open the connection. When the connection is made, a sign-on message will display and the router will ask for a password. (This is the "virtual terminal password" entered during configuration of the remote router for "line vty 0 4".)

Next, enter the desired router commands. When finished, give the command "logout". The router will break the connection and display the local router's prompt.

```
oc_rtr#telnet south
Trying south (100.100.103.2)... Open

South Site Cisco 2501

User Access Verification

Password: <virtual terminal password>

south_rtr>. . . <entered desired commands>

south_rtr>#logout
oc_rtr#
```

9.3. Troubleshooting from a host computer

9.3.1. Ping from OpenView

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. Only routers and computers can be pinged. See Section 9.1 for ping troubleshooting techniques.

The Ping window is used to start/stop pings and to 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.

9.3.2. Ping from Command Prompt

Routers and computers can be pinged from the Command Prompt. The response will be displayed in the Command Prompt window. (In Windows NT 4.0, the Command Prompt is started from taskbar menu item Start -> Programs -> Command Prompt. In Windows NT 3.51, the Command Prompt is started from the Main program group.)

To ping a device, enter ping and the device's unique name or IP address. The unique name is the name that was entered in the lmhosts file. See Section 9.1 for ping troubleshooting techniques.

Example:

```
C:\> ping south
Pinging south [100.100.103.2] with 32 bytes of data:
Reply from 100.100.103.2: bytes=32 time=30ms TTL=254
Reply from 100.100.103.2: bytes=32 time=20ms TTL=254
Reply from 100.100.103.2: bytes=32 time=20ms TTL=254
Reply from 100.100.103.2: bytes=32 time=20ms TTL=254
4 times total
```

9.3.3. Telnet from computer

The Telnet program can be started from the Accessories group. (In Windows NT 4.0, use the taskbar menu item Start -> Programs -> Accessories -> Telnet. In Windows NT 3.51, open the Program Manager; then, open the Accessories group.)

Telnet (terminal emulation protocol) allows the local keyboard and monitor to act as though they were attached to a remote device. Once a telnet connection is made, the information typed on the local keyboard is sent to the remote device and the local monitor displays information from the remote device.

To telnet to a router, select the Connect menu. If the desired router is listed in the bottom section of the menu, select the listing. Otherwise, select menu item Remote System and a dialog box will display. In the Host Name field, enter the unique name or IP address of the desired router. Alternatively, select a name or address from the drop-down list, which lists the last few entries. In the dialog box, Port should be telnet and Term Type should be vt100. Click the Connect button to establish a telnet session with the router.

The router will (if able) send its sign-on message and ask for a password. This is the <virtual terminal password> entered during router configuration for “line vty 0 4”. After the password is entered, the router will send its prompt and then router commands can be entered. (See Section 9.2 for troubleshooting commands and Section 3.2 for configuration commands.)

To end the telnet session, enter logout at the router prompt, or select menu item Connect -> Disconnect. If logout is entered, a message box will show that the connection was lost.

9.4. *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.

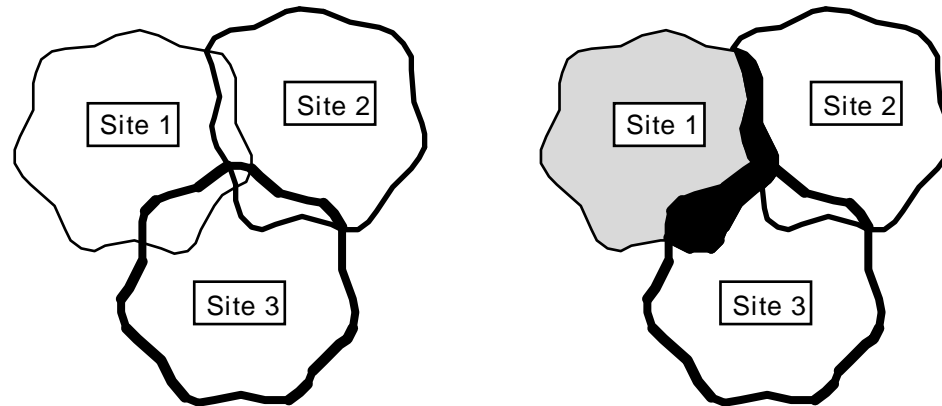
Channel reverts will shut down all repeaters on a channel. Site reverts will shut down individual sites or reconfigure individual sites to stand-alone sites. If a repeater failure can cause both reverts, both reverts will occur.

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 9.5).

9.4.1. 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 9-2.

Figure 9-2. 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 9-2) 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 9-2), 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.

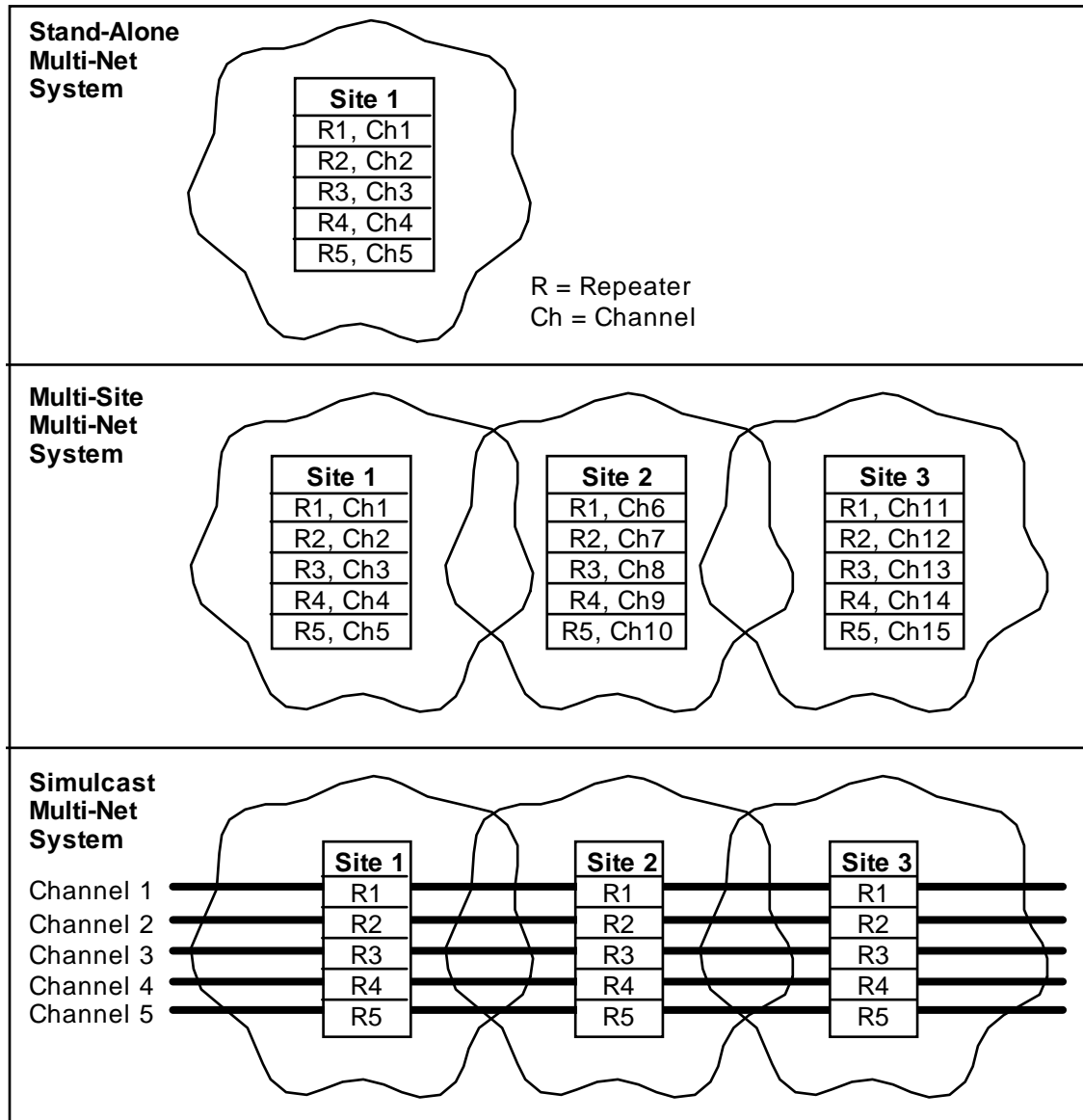
9.4.2. Consider status channel and home channel access

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 9-3 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 9-3. Relationship of repeaters, channels, and sites



9.4.3. 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? When this check box is checked, 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 9.6 shows the alarms that cause simulcast and repeater failures, which can result in channel reverts.

9.4.4. 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 9.5. The channel status will remain reverted and additional alarms on the channel will not revert the channel.

9.4.5. 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 9.4.4).

- **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.

9.4.6. 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 checking this check 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 9.6 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 9-4 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 9-4. 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											

9.4.7. 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)**

When this check box is checked, 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.

9.4.8. 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 9.5. The site status will remain reverted and additional alarms at the site will not revert the site.

9.4.9. 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.

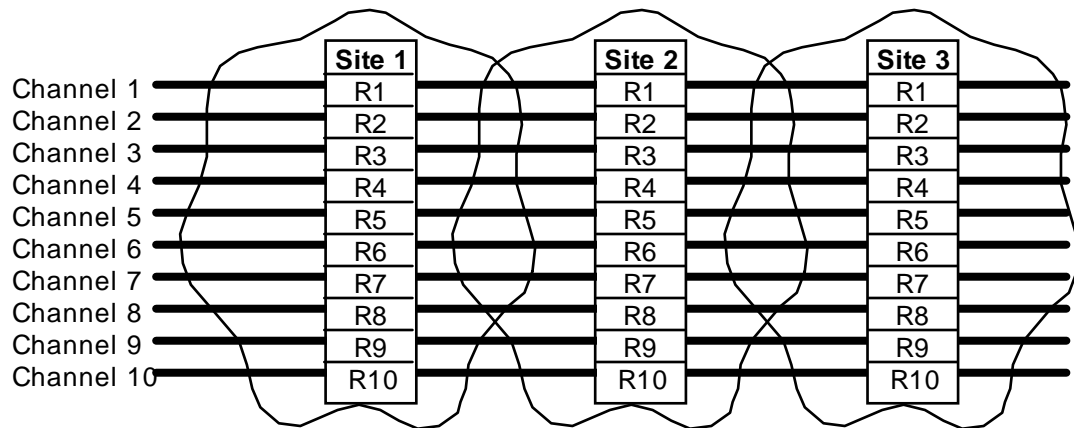
Refer to Figure 9-5. Site 3 has been configured to revert to a stand-alone Multi-Net site if repeaters 1 and 3 fail. In this system, repeater 1 is the status channel. Repeater 3 is the home channel for the group used by a high-priority collection of users. When repeaters 1 and 3 fail, groups that use 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.

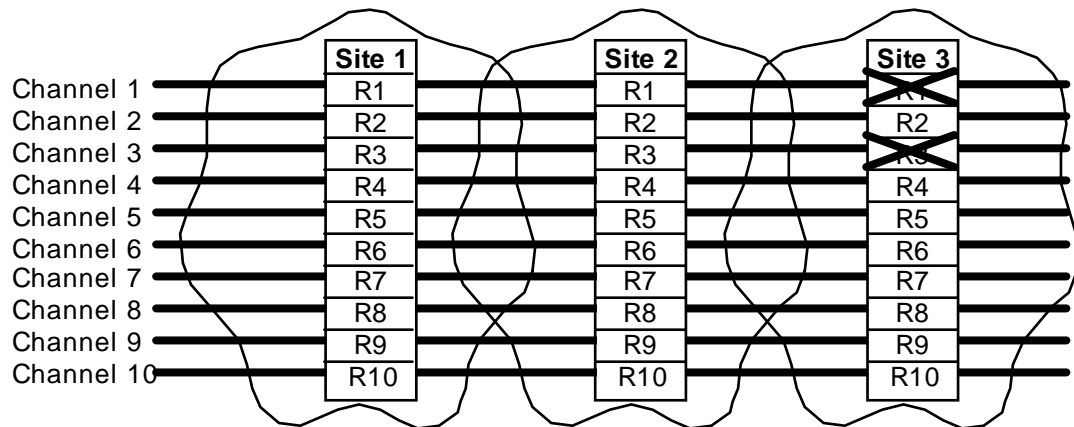
To configure the system for this type of revert involves two dialog boxes. The dialog box from menu item System -> Revert Input Configuration, is used to set up the input alarms (or conditions) that will cause a revert. Refer to Figure 9-6. For this example, a set of inputs is defined for site 3. Repeater 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 9-7. 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.

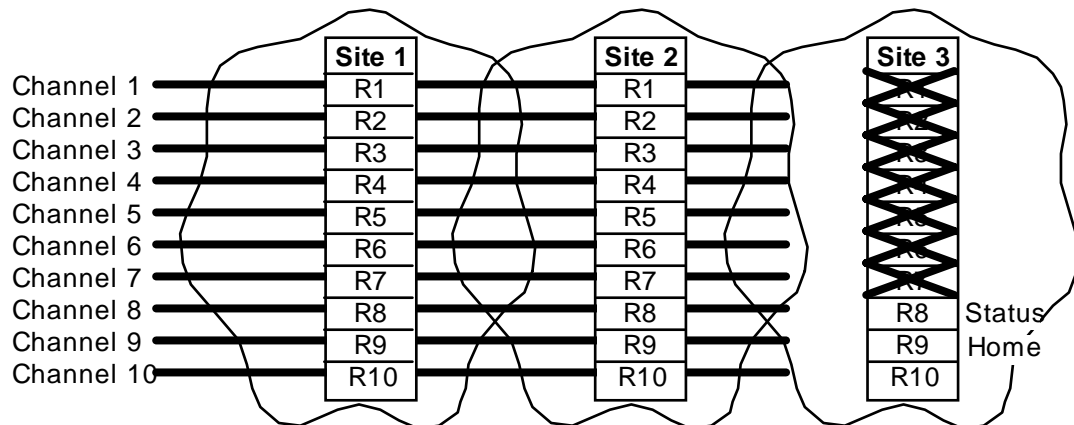
Figure 9-5. Site 3 is configured to revert to a stand-alone Multi-Net site.



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 9-6. Revert Input Configuration

Revert Input Configuration									
<p>System Name:</p> <p>Select Site to Configure:</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 40%;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Sites/Revert Input Sets</td></tr> <tr><td>CHANNELCTRL</td></tr> <tr><td>SITE1</td></tr> <tr><td>SITE2</td></tr> <tr><td>SITE3</td></tr> <tr style="background-color: black; color: white;"><td>Set #1</td></tr> <tr><td style="height: 150px;"></td></tr> </table> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Add Set Delete Set Duplicate Set </div> </div> <div style="width: 55%;"> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 60%;"> <input type="checkbox"/> Site Revert on HC Network Link Loss </div> <div style="width: 35%; text-align: right;"> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Alarm Set Type <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="radio"/> Simulcast Failure <input checked="" type="radio"/> Repeater Failure </div> </div> <div style="border: 1px solid black; padding: 5px;"> Repeaters With Active Alarms <div style="display: flex; flex-wrap: wrap; padding: 5px;"> <div style="margin: 2px;"><input checked="" type="checkbox"/> 1</div> <div style="margin: 2px;"><input type="checkbox"/> 2</div> <div style="margin: 2px;"><input checked="" type="checkbox"/> 3</div> <div style="margin: 2px;"><input type="checkbox"/> 4</div> <div style="margin: 2px;"><input type="checkbox"/> 5</div> <div style="margin: 2px;"><input type="checkbox"/> 6</div> <div style="margin: 2px;"><input type="checkbox"/> 7</div> <div style="margin: 2px;"><input type="checkbox"/> 8</div> <div style="margin: 2px;"><input type="checkbox"/> 9</div> <div style="margin: 2px;"><input type="checkbox"/> 10</div> <div style="margin: 2px;"><input type="checkbox"/> 11</div> <div style="margin: 2px;"><input type="checkbox"/> 12</div> <div style="margin: 2px;"><input type="checkbox"/> 13</div> <div style="margin: 2px;"><input type="checkbox"/> 14</div> <div style="margin: 2px;"><input type="checkbox"/> 15</div> <div style="margin: 2px;"><input type="checkbox"/> 16</div> <div style="margin: 2px;"><input type="checkbox"/> 17</div> <div style="margin: 2px;"><input type="checkbox"/> 18</div> <div style="margin: 2px;"><input type="checkbox"/> 19</div> <div style="margin: 2px;"><input type="checkbox"/> 20</div> <div style="margin: 2px;"><input type="checkbox"/> 21</div> <div style="margin: 2px;"><input type="checkbox"/> 22</div> <div style="margin: 2px;"><input type="checkbox"/> 23</div> <div style="margin: 2px;"><input type="checkbox"/> 24</div> <div style="margin: 2px;"><input type="checkbox"/> 25</div> <div style="margin: 2px;"><input type="checkbox"/> 26</div> <div style="margin: 2px;"><input type="checkbox"/> 27</div> <div style="margin: 2px;"><input type="checkbox"/> 28</div> <div style="margin: 2px;"><input type="checkbox"/> 29</div> <div style="margin: 2px;"><input type="checkbox"/> 30</div> </div> <div style="text-align: center; margin-top: 10px;"> <div style="border: 1px solid black; padding: 2px 10px;">Clear All</div> </div> </div> </div> </div> <div style="width: 40%; text-align: right;"> <div style="margin-bottom: 10px;"><div style="border: 1px solid black; padding: 2px 10px;">OK</div></div> <div style="margin-bottom: 10px;"><div style="border: 1px solid black; padding: 2px 10px;">Cancel</div></div> <div><div style="border: 1px solid black; padding: 2px 10px;">Help</div></div> </div> </div> </div>			Sites/Revert Input Sets	CHANNELCTRL	SITE1	SITE2	SITE3	Set #1	
Sites/Revert Input Sets									
CHANNELCTRL									
SITE1									
SITE2									
SITE3									
Set #1									

Figure 9-7. Revert Action Configuration

Revert Action Configuration																												
<p>System Name:</p> <p>Select Repeater to Configure:</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 60%;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Site/Repeater</th> <th style="width: 40%;">Revert Action</th> </tr> </thead> <tbody> <tr><td>SITE3</td><td></td></tr> <tr><td>R1</td><td>DIS-100%-SC</td></tr> <tr><td>R2</td><td>DIS-100%</td></tr> <tr><td>R3</td><td>DIS-100%</td></tr> <tr><td>R4</td><td>DIS-100%</td></tr> <tr><td>R5</td><td>DIS-100%</td></tr> <tr><td>R6</td><td>DIS-100%</td></tr> <tr><td>R7</td><td>DIS-100%</td></tr> <tr style="background-color: black; color: white;"><td>R8</td><td>MN-MIN-SC</td></tr> <tr><td>R9</td><td>MN-MIN</td></tr> <tr><td>R10</td><td>MN-MIN</td></tr> <tr><td> </td><td> </td></tr> </tbody> </table> </div> <div style="width: 35%; text-align: right;"> <div style="margin-bottom: 10px;"><div style="border: 1px solid black; padding: 2px 10px;">OK</div></div> <div style="margin-bottom: 10px;"><div style="border: 1px solid black; padding: 2px 10px;">Cancel</div></div> <div><div style="border: 1px solid black; padding: 2px 10px;">Help</div></div> </div> </div> <div style="width: 30%; padding-top: 20px;"> <div style="border: 1px solid black; padding: 5px;"> <p>Site Revert Action</p> <p>Repeater Mode:</p> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input checked="" type="radio"/> Stand-Alone Multi-Net (MN) <input type="radio"/> Disabled (DIS) </div> <p>Power Level:</p> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="radio"/> Full (100%) <input type="radio"/> 3/4 (75%) <input type="radio"/> 1/2 (50%) <input checked="" type="radio"/> Minimum (Min) </div> <div style="margin-top: 10px;"> <input checked="" type="checkbox"/> Status Channel (SC) </div> </div> </div>			Site/Repeater	Revert Action	SITE3		R1	DIS-100%-SC	R2	DIS-100%	R3	DIS-100%	R4	DIS-100%	R5	DIS-100%	R6	DIS-100%	R7	DIS-100%	R8	MN-MIN-SC	R9	MN-MIN	R10	MN-MIN		
Site/Repeater	Revert Action																											
SITE3																												
R1	DIS-100%-SC																											
R2	DIS-100%																											
R3	DIS-100%																											
R4	DIS-100%																											
R5	DIS-100%																											
R6	DIS-100%																											
R7	DIS-100%																											
R8	MN-MIN-SC																											
R9	MN-MIN																											
R10	MN-MIN																											

9.5. *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: When this check box is checked, 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.

9.5.1. 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 9.4.7).

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 5.6.3).

Setup State: To place a repeater in setup mode, select a repeater icon on a map, and then select menu item Repeater -> Setup State. **Note:** This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

Normal State: To take a repeater out of setup mode, select a repeater icon on a map, and then select menu item Repeater -> Normal State. **Note:** This menu item will only be available if the service.ini file was present in the C:\SITECTR\ directory when OpenView was started. See Section 5.11.

9.6. Alarm list for E.F. Johnson components

9.6.1. 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	X					Repeater put in test

Alrm ID	Disp	Led's	Alarm Description	Dig On/ Off	A/D Line	1/2 Pwr	Disable Simcst	RF Shut down	Causes For Alarm
			Mode						
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
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

TROUBLESHOOTING

Alrm ID	Disp	Led's	Alarm Description	Dig On/ Off	A/D Line	1/2 Pwr	Disable Simcst	RF Shut down	Causes For Alarm
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
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

9.6.2. 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

DBase ID	Alarm ID	Alarm Status	Alarm Description	Causes For Alarm
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

9.6.3. 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

9.6.4. 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

9.6.5. 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

9.7. *Mnemonics*

A/D - Analog to Digital
ARP - Address Resolution Protocol
CIM - Channel Interface Module
GPS - Global Positioning System
HC - Host Computer
HSDB - High-Speed Data Bus
IAC - Interface Alarm Card
IGRP - Interior Gateway Routing Protocol
IP - Internet Protocol
IRDB - Inter-Repeater Data Bus
MAC - Main Audio Card
MAC address - Media Access Control address
MBC - Message Bridge Card
NTP - Network Time Protocol
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

—A—

abbreviations, 9-23
 actions, site revert, 9-14
 active alarms, 9-20
 adapters, caution, 6-1
 add to polling, 5-20
 addresses, network, 2-6
 administrator username, windows,
 4-6, 5-5
 alarms
 descriptions, 9-20
 iac, 5-17
 log database id numbers, 9-20
 repeater, 9-20
 alignment, 7-1
 bi-directional, 7-9
 uni-directional, 7-5
 assign ip addresses, 2-7
 devices, 2-12
 subnet, 2-10
 assign subnets, 2-10
 audio gain, smc, 7-18
 auto logon, windows, 4-10
 automatic
 channel revert, 9-10
 site revert actions, 9-14
 site revert inputs, 9-12

—B—

backbone, 2-7
 background map, 5-12, 5-18
 bandwidth, router port, 3-5
 bi-directional
 calibration, 7-9
 configure, 5-20
 IAC1, 5-17
 buffer delay
 min, 5-20
 offset, 5-19, 7-14
 buffer delay, smc, 7-19

—C—

cable, 2-1
 caution, 6-1
 channel computer to channel
 controller, 6-4
 hub to host computer, 6-6
 hub to router, 6-7
 hub to site/channel computer, 6-
 5
 router to channel bank, 6-8
 router to host computer, 6-7
 router to site/channel computer,
 6-4
 site computer to repeater, 6-3

calibration, 7-1
 bi-directional, 7-9
 uni-directional, 7-5
 channel bank, 5-20
 channel bank cable to router, 6-8
 channel computer
 cable to channel controller, 6-4
 cable to hub, 6-5
 cable to router, 6-4
 configuration, 4-1
 channel controller
 cable to channel computer, 6-4
 channel revert configure, 5-13, 9-10
 channel revert status, 9-11
 channel unrevert, 9-11
 check maps, 5-18
 cisco. *See* router
 cisco router icon, 5-15
 clock
 computer, 4-8
 router, 3-4, 3-8
 community password, openview, 5-
 23
 computer, 2-1
 configuration, 4-1
 host names, 4-5, 5-4
 icon, 5-15
 name, 2-14, 4-6, 4-9, 5-6, 5-8
 passwords, 2-15
 computers. *See* host, site, or channel
 computer; or Windows
 configure
 channel computer, 4-1
 channel reverts, 9-10
 host computer, 5-1
 mbc, 6-3
 microwave type, 5-20
 mouse, 4-2
 offsets, 5-19
 polling, 5-20
 repeater control, 9-19
 reverts, 9-7
 router, 3-1
 site computer, 4-1
 site revert actions, 9-14
 site revert inputs, 9-12
 smc parameters, 7-17
 traps, 5-21
 windows, 4-1, 4-2
 windows 3.51, 5-24

—D—

data acquisition
 bi-directional, 7-9
 uni-directional, 7-5
 data gain, smc, 7-18
 daylight savings time
 router, 3-4

windows, 4-8
 default gateway, 4-2
 default, map, 5-18
 describe
 computer, 5-15
 repeater, 5-16
 router, 5-15
 site, 5-14
 system, 5-13
 describe objects as added, 5-19
 device map, 5-14
 disable. *See* revert
 distorted signals, 7-1, 7-5, 7-9, 7-14

—E—

e.f. johnson username, windows, 4-
 6, 5-5
 edit
 lmhosts file, 4-5, 5-4
 offsets, 5-19
 equipment location, 2-2
 ethernet cable, 6-6
 ethernet card, install, 4-1
 ethernet crossover cable, 6-5

—F—

filename, maps, 5-12
 flash code, mbc, 6-3

—H—

home channel, 9-9, 9-15
 host computer
 cable to hub, 6-6
 cable to router, 6-7
 configuration, 5-1
 ping, 9-6
 telnet, 9-7
 host names, 2-14
 computer, 4-5, 4-6, 4-9, 5-4, 5-6,
 5-8
 router, 3-5, 9-2
 hosts file, 4-8, 5-9
 hp openview. *See* openview
 hub, 2-1, 2-9
 cable to host computer, 6-6
 cable to router, 6-7
 cable to site/channel computer,
 6-5

—I—

iac alarm, 5-17
 icon
 alignment, 7-2
 computer, 5-15

- data acquisition, bi-directional, 7-11
- data acquisition, uni-directional, 7-6
- repeater, 5-16
- router, 5-15
- site, 5-14
- system, 5-12
- inputs, site revert, 9-12
- install, 6-1
 - ethernet card, 4-1
 - mbc, 6-1
 - openview, 5-9
 - openview (old), 5-32
 - sitectrl, 4-10
 - windows, 8-6
 - windows networking, 4-3
- install cable
 - channel computer to channel controller, 6-4
 - hub to host computer, 6-6
 - hub to router, 6-7
 - hub to site/channel computer, 6-5
 - router to channel bank, 6-8
 - router to host computer, 6-7
 - router to site/channel computer, 6-4
 - site computer to repeater, 6-3
- install software, 8-5
- install software updates. *See* update software. *See* update software
- installation, site types, 2-2
- ip addresses, 2-6, 9-2
- ip subnets, 2-10

—L—

- led on mbc, 6-3
- link loss, 9-13
- lmhosts file, 4-5, 4-7, 4-9, 5-4, 5-8
- location of equipment, 2-2
- log in openview password, 5-22
- logon windows, auto, 4-10

—M—

- ma-412 card, 6-8
- manual calibration, 7-1
 - bi-directional, 7-9
 - uni-directional, 7-5
- manual repeater control, 9-19
- map
 - automatic submaps, 5-19
 - background image, 5-18
 - computer, 5-15
 - create, 5-11
 - device, 5-14
 - filename, 5-12
 - lines, 5-17
 - options, 5-18

- protection, 5-18
- repeater, 5-16
- router, 5-15
- set default, 5-18
- site, 5-13
- system, 5-12
- text, 5-17
- map protection password, 5-22
- master site, 2-2
- mbc, 2-1
 - configure, 6-3
 - install, 6-1
 - led, 6-3
- message bridge cable kit, 6-3
- microwave
 - bi-directional, 5-20, 7-9
 - redundant, 5-20
 - uni-directional, 7-5
- mnemonics, 9-23
- modify
 - lmhosts file, 4-5, 5-4
 - offsets, 5-19
- monitoring point, 2-2, 5-13
- mouse configuration, 4-2
- multi-port router, 2-14

—N—

- names. *See* host names
- network addresses, 2-6
- network link loss, 9-13
- ntp, 3-6
- number of symbols, 5-18

—O—

- offset, overlap, 7-14
- openview
 - community password, 5-23
 - install, 5-9
 - passwords, 2-15, 5-22
 - ping, 9-6
 - polling, 5-20
 - set community password, 5-23
 - traps, 5-21
- openview (old), install, 5-32
- overlap offset, 5-19, 7-14

—P—

- passwords, 2-15
 - log in openview, 5-22
 - openview, 5-22
 - openview map protection, 5-22
 - openview snmp, 5-23
 - windows, 4-5
- path, windows, 4-7
- phase, smc, 7-20
- pilot tone gain, smc, 7-18
- ping, 9-1
 - from host computer, 9-6

- from router, 9-4
- polling, configure openview, 5-20
- power level, repeater, 5-17, 9-15, 9-20
- print object names, 5-18
- protect map, 5-18

—R—

- reconfigure repeater, 9-19
- recovery. *See* reverts
- redundant microwave, 5-20
- remote site, 2-2
- repeater
 - active alarms, 9-20
 - channel, 5-17
 - control, 9-19
 - describe, 5-16
 - failure, 9-13
 - icon, 5-16
 - mode, 9-19
 - power level, 5-17, 9-15, 9-20
 - restart, 9-20
 - revert, 9-20
 - setup mode, 9-20
 - unrevert, 9-20
- repeater cable to site computer, 6-3
- repeater controller. *See* channel controller
- restart repeater, 9-20
- revert, 9-7
 - channel, automatic, 5-13, 9-10
 - channel, manual, 9-11
 - repeaters, 9-20
 - site manual, 9-15
 - site, automatic actions, 9-14
 - site, inputs, 9-12
 - status channel, 5-13, 9-11
- revert action configuration, 9-14
- revert input configuration, 9-12
- round-trip time, 9-6
- router, 2-1
 - cable to channel bank, 6-8
 - cable to host computer, 6-7
 - cable to hub, 6-7
 - cable to site/channel computer, 6-4
 - clock, 3-8
 - configuration, 3-1
 - daylight savings time, 3-4
 - host names, 3-5, 9-2
 - icon, 5-15
 - multi-port, 2-14
 - name, 2-14
 - passwords, 2-15
 - ping, 9-4
 - port bandwidth, 3-5
 - snmp, 3-7
 - telnet, 9-5
 - timezone, 3-4
 - traps, 3-7

troubleshooting, 9-1
routes, 9-2

—S—

service functions, 5-23
service.ini, 5-23
set clock in router, 3-8
set community, openview password, 5-23
show, router commands, 9-2
shutdown. *See* revert
simulcast failure, 9-13
simulcast modulation card. *See* smc
site
 describe, 5-14
 icon, 5-14
site computer
 cable to hub, 6-5
 cable to repeater, 6-3
 cable to router, 6-4
 configuration, 4-1
site map, 5-13
site revert
 automatic actions, 9-14
 inputs, 9-12
 manual, 9-15
site settings, 5-19
site types, 2-2
sitectl.exe, 8-1, 8-3
smc configuration, 7-17
snmp
 openview, 5-23
 router, 3-7
software updates. *See* update
 software. *See* update software
status

active alarms, 9-20
 repeater, 9-19
 reverted channel, 9-11
 reverted sites, 9-15
status channel, 5-13, 5-17, 9-9, 9-11, 9-15, 9-19
submap. *See* maps
subnet, 2-7
subnet assignments, 2-10
subnet mask, 4-2
system
 describe, 5-13
 icon, 5-12
system map, 5-12
system settings, 5-19

—T—

tcp/ip parameters, windows, 4-7, 4-9, 5-6, 5-8
telnet
 from host computer, 9-7
 from router, 9-5
threshold alignment, 7-1
threshold, smc, 7-19
time
 ntp, 3-6
 router, 3-4, 3-8
timezone
 router, 3-4
 windows, 4-8
timing tone gain, 7-1
timing tone gain, smc, 7-19
traps
 router, 3-7
traps, configure openview, 5-21
troubleshooting, 9-1

alarm list, 9-20
 from computer, 9-6
 from router, 9-1

—U—

uni-directional calibration, 7-5
uninstall software, 8-2, 8-5
unique host names. *See* host names
unprotect
 map, 5-18
unrevert, 9-7
 channel, 5-13, 9-11
 repeaters, 9-20
 sites, 9-15
update software
 sitectl.exe, 8-1, 8-3
username, windows, 4-5, 4-10, 5-5, 5-9

—W—

windows
 configuration, 4-1, 4-2
 daylight savings time, 4-8
 install, 8-6
 install networking, 4-3
 passwords, 2-15, 4-5
 path, 4-7
 tcp/ip parameters, 4-7, 4-9, 5-6, 5-8
 timezone, 4-8
 username, 4-5, 4-10, 5-5, 5-9
windows 3.51
 configuration, 5-24
words on map, 5-17