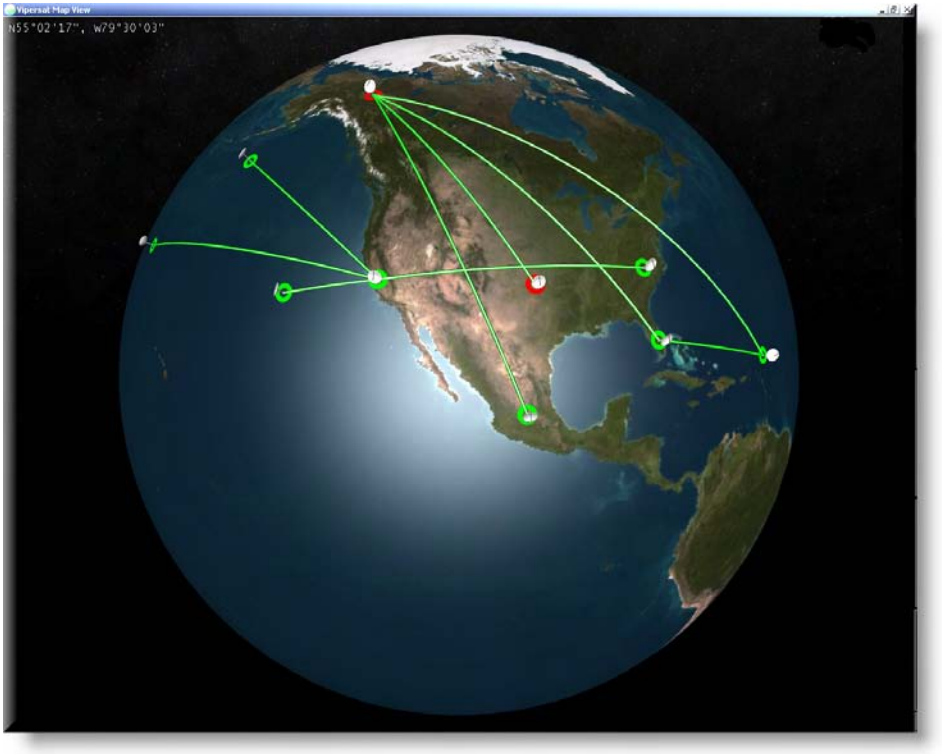
VMS v3.7.x

VIPERSAT Management System



User Guide

Part Number MN/22156 Revision 7

VMS v3.7.x

VIPERSAT Management System

User Guide

Part Number MN/22156
Document Revision 7

Software version 3.7.3

May 5, 2010

COMTECH EF DATA

VIPERSAT Network Products Group
3215 Skyway Court
Fremont, CA 94539
USA

Phone: (510) 252-1462
Fax: (510) 252-1695
www.comtechefdata.com

Part Number: MN/22156
Revision: 7

Software Version: 3.7.3

Printed in the United States of America

Document Revision History

Revision	Date	Description
0	7/03/07	**Initial Release**. *Note*: This new document part number, MN/22156, supersedes the previous VMS User Guide part number, 22156. **New functionality in v3.5.x:** VMS N:1 Redundancy; Site Distribution Lists; CDM-700 Out-of-Band Driver; CDD-564IF InBand Driver.
1	10/15/07	**New functionality in v3.6.0:** Roaming (SOTM), ROSS; Global Map View.
2	2/08/08	**New functionality in v3.6.2:** VMS Virtual Network Operator (VNO).
3	8/30/08	**New functionality in v3.6.3:** SLM-5650A Inband/OOB Driver; OBCM; CDM-570/570L Out-of-Band Driver; Satellite Advanced Switching for SOTM and Antenna Mesh Compensation Factor; Basic Guaranteed Bandwidth and CIR.
4	2/24/09	**New functionality in v3.6.4:** Event Log Filtering and VMS Event Conduit Service; VMS Redundancy Status and Auto Synchronize; Up/Down Converter Naming.
5	5/26/09	**New functionality in v3.7.1:** Guaranteed Bandwidth; Enhanced Switching; Integrated Circuit Scheduler. Not formally released.
6	10/30/09	**New functionality in v3.7.2:** Point-to-Point Switching; Remote Site Wizard; Application Image Manager; Application Policies Priority; Event Relay Server; Satellite Reservations Status; Antenna Visibility; Multi-Band LNB Roaming Support.
7	5/05/10	**New functionality in v3.7.3:** Database Protection and Hardening; SHOD/ Mesh Data Rate Limits; Independent Forward and Return Path Settings for Reservations and Advanced Switching ModCods; Site Reservation Control; Automatic Network Registration.

{ *This Page is Intentionally Blank* }

Table of Contents

Chapter 1
General

Chapter 2
VMS Installation

Chapter 3
VMS Configuration

Chapter 6
SNMP Managed Units

Appendix A
VMS Cross Banding

Appendix B
Antenna Visibility

Appendix C
Redundancy

Appendix D
Domain Controller and DNS

Appendix E
SNMP Traps

Appendix F
Automatic Switching

Appendix G
Entry Channel Mode Switching

Appendix H
Glossary

Index

List of Figures

Chapter 1 Figures

Chapter 2 Figures

Chapter 3 Figures

Chapter 4 Figures

Chapter 5 Figures

Chapter 6 Figures

Appendix A Figures

Appendix B Figures

Appendix C Figures

Appendix D Figures

Appendix E Figures

Appendix F Figures

Appendix G Figures

List of Tables

Chapter 4 Tables

Chapter 5 Tables

Appendix F Tables

{ *This Page is Intentionally Blank* }

CHAPTER

1

GENERAL

How to Use This Manual

This manual documents the features and functions of the Vipersat Management System (VMS), and guides the user in how to install, configure, and operate this product in a Vipersat network.

NOC administrators and operators responsible for the configuration and maintenance of the Vipersat network, as well as earth station engineers, are the intended audience for this document.

Manual Organization

This User Guide is organized into the following sections:

Chapter 1 — General

Contains VMS product description, customer support information, and manual conventions and references.

Chapter 2 — VMS Installation

Covers the steps for installing the VMS software application on a host server, in both standalone and redundant configurations.

Chapter 3 — VMS Configuration

Covers the Quick Configuration procedure as well as detailed steps for full System Configuration in building the Vipersat network.

Chapter 4 — Configuring Network Modems

Describes how VMS is used to configure modems in the Vipersat network.

Chapter 5 — VMS Services

Describes the various service managers that comprise VMS and how Viper-View is used to monitor and control the Vipersat network.

Chapter 6 — SNMP Managed Units

Describes the methods for integrating out-of-band modem units into a VMS-controlled satellite network.

Appendix A — VMS Cross Banding

An explanation of how VMS accommodates applications involving satellite cross strapping and cross banding.

Appendix B — Antenna Visibility

An explanation of how to use the VMS antenna visibility function to control the frequency spectrum used in VMS switching.

Appendix C — Redundancy

Describes the optional redundancy services available for VMS—N:1 Server redundancy and N:M Hub Modem redundancy.

Appendix D — Domain Controller and DNS

Describes the method of configuring VMS servers to perform the role of network Domain Controller and Domain Name Server for the VMS network.

Appendix E — SNMP Traps

Describes the use of SNMP traps by VMS.

Appendix F — Automatic Switching

Reference on how the VMS monitors and automatically responds to changing load, data type, and QoS requirements in the network.

Appendix G — Entry Channel Mode Switching

Supplement on how ECM provides a method for remotes to switch from STDMA to SCPC and back.

Appendix H — Glossary

A glossary of terms that pertain to Vipersat satellite network technology.

Conventions and References

The following conventions are utilized in this manual to assist the reader:

Note: Provides important information relevant to the accompanying text.

Tip: Provides complementary information that facilitates the associated actions or instructions.

Caution: Explanatory text that notifies the reader of possible consequences of an action.

Warning: Explanatory text that notifies the reader of potential harm as the result of an action.

The following documents are referenced in this manual, and provide supplementary information for the reader:

- *CDM-570/570L Modem Installation and Operation Manual* (Part Number MN/CDM570L.IOM)
- *Vipersat CDM-570/570L User Guide* (Part Number MN/22125)
- *CDD-562L/-564 Demodulator with IP Module Installation and Operation Manual* (Part Number MN/CDD562L-564.IOM)
- *Vipersat CDD-56X Series User Guide* (Part Number MN/22137)
- *SLM-5650A Installation & Operation* (Part Number MN-0000031)

- *Vipersat SLM-5650A User Guide* (Part Number MN-0000035)
- *Vipersat Circuit Scheduler User Guide* (Part Number MN/22135)
- *ROSS Getting Started Guide* (Part Number MN/13070)
- *Vload Utility User Guide* (Part Number MN/22117)
- *Vipersat CDM-570/L, CDD-56X Parameter Editor User Guide* (Part Number MN-0000038)
- *SLM-5650/A Parameter Editor User Guide* (Part Number MN-0000041)
- *VNO Quick Start Guide* (Document Number MN/VMS-VNOQSG)

Product Description

Introduction

The Vipersat Management System (VMS) is a server and client based network management system that gathers and processes information it receives from the modems that comprise a Vipersat satellite network. The modem's internal microprocessor-based input/output (I/O) controller measures, captures, and transmits real-time network operating parameters to the VMS via PLDM (Path Loss Data Message) packets.

The VMS receives, stores, and processes these messages and uses the data to update and display current network status information, and to manage bandwidth resources and switching operations . The network data is then displayed by the VMS in an easy-to-interpret, real-time graphic presentation. The result is a comprehensive, intuitive operator's network Management and Control tool for quick, responsive network control.

The VMS is customized at setup for each satellite network it controls, recognizing the unique bandwidth resources and limitations available for each network. The VMS has trigger points set defining the upper and lower limits for usage, type of service, and other network parameters defining bandwidth resource allocations for each traffic type. These triggers, or set-points, are easily modified at any time by a qualified operator whenever network resource allocations need to be reconfigured.

As the VMS receives a switching request from a network modem, it uses sophisticated algorithms to evaluate the request against available network resources and network policies before sending a switch command back to the requesting modem to make a switch to a given frequency and bit rate. If the switch request is denied—because of lack of available network resources, for example—the modem will not make the switch until the necessary resources become available.

The Vipersat satellite network modems detect, monitor and, when commanded by the VMS, physically or logically make network changes. The VMS collects, analyzes, and displays data, and commands the Vipersat modems to make these network changes. Refer to each *modem*'s *User Guide* for more details on each device's role in the satellite network.

Note: The Vipersat External Switching Protocol (VESP) is available to equipment manufactures, making it possible for them to smoothly integrate their products into a VMS controlled satellite network. Contact a Vipersat representative for details.

The VMS **ViperView** display (figure 1-1) gives the operator a complete view of a network's configuration, the health of all network components, and current

bandwidth usage. The VMS display is flexible and can be modified by the operator at any time, as described in this *User Guide*, to optimize network Management and Control.

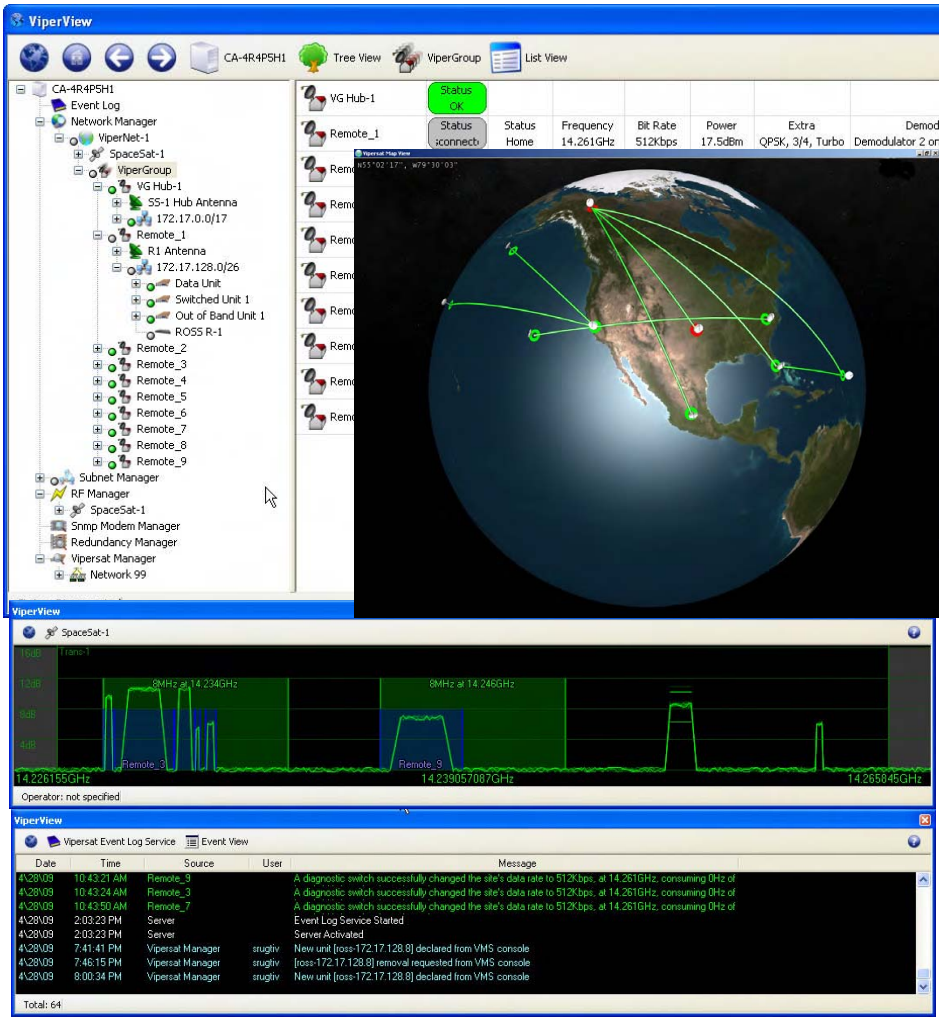


Figure 1-1 VMS ViperView display

Vipersat uses IP connections between network nodes, supporting UDP connectivity. The Vipersat modem consists of a satellite modem with an imbedded microprocessor router, which is the interface between LAN traffic and the satellite links that connect remote stations to the hub.

The VMS has a client/server architecture, as shown in figure 1-2, with rack servers communicating with remote client PC's. The client/server model has a number of advantages. The server maintains all databases in a central location accessible to all clients. Thus, all network status updates and performance data is stored in a single place, processed by the VMS running on the central server, and the results are available to all clients across the network.

Through its client/server architecture, the VMS supports centralized management, control, and distribution of data, alarms, and events. The VMS also simultaneously supports multiple clients, network management, and complete visibility of the entire network operation.

VMS Features

The VMS network management software has the following features:

- System Configuration
- Network Status Displays (automatic and manual)
- Dynamic Bandwidth Management
- Guaranteed Bandwidth Reservations
- Point-to-Point Switching
- Advanced Modulation/Code Switching
- Integrated Circuit Scheduler
- Diagnostics Monitor and Control (automatic and manual)
- Alarm Processing
- Optional Management Security
- Optional VMS and Critical Hardware Redundancy
- Statistics Gathering (automatic and manual)
- Report Generation
- Network Administrator Mode
- Remote Access via Local LAN or Internet/Intranet

VMS Operation & Architecture

A Vipersat network provides Internet Protocol (IP) connections between network nodes and supporting UDP and Multicast protocols. Vipersat satellite networks rely on Vipersat modems to provide the interface between LAN traffic and the satellite links that connect remote stations to the hub.

The VMS **Client** (ViperView) and **Server** (Vipersat Object Service) architecture (figure 1-2) supports centralized management, control, and distribution of data, alarms, and events. Network units, such as a Vipersat modem, while functioning as a modulator/demodulator, also detect, analyze, and report details on network operation to the VMS. The VMS collects, stores, analyzes, and acts on this information to intelligently control network operation to optimize bandwidth utilization and overall network performance.

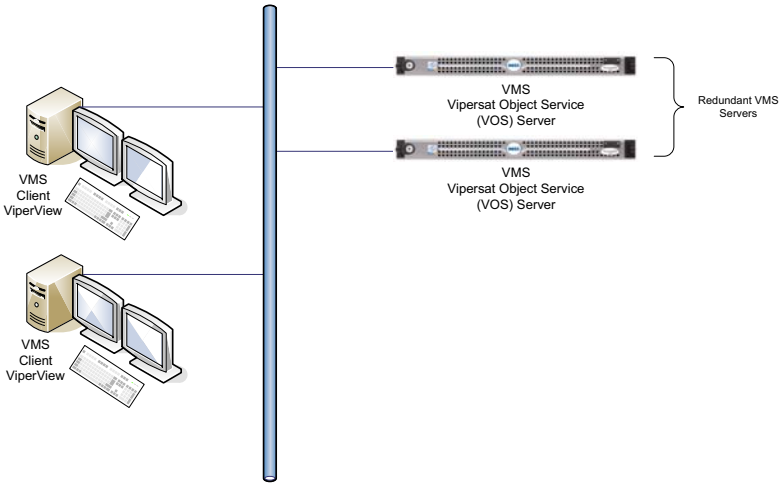


Figure 1-2 ViperView Client / Server (VOS) Relationship

The VMS management and monitoring system uses an intuitive graphic display, as illustrated in figure 1-1. The VMS makes visible the entire network's operation and performance. All network status and performance data is collected, processed, and stored at the server. Any client workstation can retrieve information from the VMS server's single, central database.

The VMS network management system displays the following information gathered from the network modems:

- System configuration
- Transmission configurations

- Satellite link Status
- QoS displayed as E_bN_o values for each circuit.
- Switching times and connection type and duration for each circuit.
- Network alarms showing health of network hardware IP and RF connections
- Bandwidth resource allocations
- Modem, RF equipment, and VSAT station management

The network map displays an integrated view of the entire network including all nets, subnets, equipment, and equipment interconnections. You can double-click on an icon to display its status information and/or sub-components. Right clicking on an icon displays a drop-down menu allowing the operator to issue commands, change configurations, or change the unit's state, as applicable.

The colors associated with each icon, as shown in the display illustrated in figure 1-1, reflect the current status condition of the network component or its sub-components:

- **Green** = Okay
- **Red** = Alarm
- **Gray** = Disconnected (offline) as the result of missing three consecutive PLDMs and not responding to the recovery process

All devices, networks, and carriers displayed by ViperView share the same color scheme for indicating their health in the network, giving the operator real-time at-a-glance network health status.

The VMS provides operator notification in the event of network alarms. This notification can be in the form of both visual and audible alerts. The VMS also maintains a log of all network activity, making use of analysis and network trouble-shooting information readily available.

New in this Release

v3.7.3 Release

Database Protection & Hardening

New resource management controls provide additional VMS server stability and protection for the switching database, thus minimizing the risk of corruption due to out-of-sync resources. During the configuration process, compatibility checking in combination with integrated warning messages alert the user/operator to potential conflicts with existing operating parameter selections. Attempts at inappropriate operations, such as deleting an assigned resource, are blocked and generate a notification to the user/operator.

SHOD/Mesh Data Rate Limits

The VMS InBand Management now offers a new SHOD Data Rate Limit feature for use in configuring Remote sites that utilize SHOD/Mesh applications. Minimum and Maximum bit rates can be specified for both directions, Transmit and Receive.

Satellite Reservations

Bandwidth reservations for the satellite that is utilized by a network or group have been enhanced with new features:

- **Tx & Rx Settings** — Reservations for a Remote site can now be established by defining separate CIRs for Transmit (return path switching) and Receive (forward path switching).
- **Site Reservation Control** — Once established, Reservations can be modified and controlled directly from the central Satellite Reservations window.

Advanced Switching—ModCods

Independent Advanced Switching tables—specifying modulation type and FEC code rate pairings with set data rates—are now provided for both Transmit (return path switching) and Receive (forward path switching) on a per Remote site basis.

Automatic Network Registration

As part of the registration process, the Vipersat Manager detects all of the Network IDs that are associated with the reporting modems and performs automatic Network Registration and grouping in ViperView. For each unique

Network ID that is detected, the Vipersat Manager creates a corresponding network container to hold all devices that register with that ID.

See the Release Notes for additional information on the VMS v3.7.3 product release.

Customer Support

Contact Information

Contact Comtech Vipersat Network Products Customer Support for information or assistance with product support, service, or training on any Vipersat product.

Mail: Attn: CTAC
Comtech EF Data – Vipersat Network Products
3215 Skyway Court
Fremont, CA 94539
USA

Phone: 1+510-252-1462

Fax: 1+510-252-1695

Email: supportcvni@comtechefdata.com

Web: www.comtechefdata.com

Return Material Authorization

Any equipment returned to CEFD (in-warranty and out-of-warranty) must have a Return Material Authorization (RMA) issued prior to return. To return a Comtech Vipersat Networks product for repair or replacement:

- Obtain an RMA form and number from either the CEFD Web Site, or via phone from a CTAC representative.
- Be prepared to supply the product model number and serial number of the unit.
- To ensure safe shipping of the product, pack the equipment in the original shipping carton/packaging.

Reader Comments / Corrections

If the reader would like to submit any comments or corrections regarding this manual and its contents, please forward them to a Vipersat Customer Support representative. All input is appreciated.

CHAPTER

2

VMS INSTALLATION

General

For specifications for the minimum recommended hardware and software platform configuration to host the VMS, please refer to the *VMS Release Notes* for the version of software that will be installed. Both Server and Client configurations are provided.

The VMS software is installed using an Installation Wizard. Depending on the desired setup, installation can be performed with the full set of files (both client and server), client-only files, or server-only files. The Wizard guides the installer through the installation process and provides all necessary information to complete typical, compact, and custom installations.

The same procedure for installation of the VMS on a server is used for both standalone and redundant configurations.

Caution: Installing VMS on non-recommended hardware or operating system will void the support warranty. Also, VMS must be installed on a dedicated server to retain support warranty.

Caution: Vipersat strongly recommends against running any kind of anti-virus program on the VMS server. Instead, all Microsoft Windows Updates should be installed as they become available. However, the Automatic Updates function in Microsoft Windows must be properly set to avoid possible disruption of the VMS and the Vipersat network. Please see the information below.

VMS Server - MS Automatic Updates Setting

The Microsoft Windows OS Automatic Updates feature provides a selection of configuration settings. The default setting, Automatic, will automatically download and install Windows updates. Typically, this process includes an automatic reboot of the server to implement the updates.

A VMS server with the default setting and an active connection to the Internet is susceptible to experiencing an automatic reboot that may adversely impact Vipersat network functions. This event can be especially damaging to redundant server configurations. When a redundant server reboots, the Primary or Secondary server (depending on which server was on-line) will require "activation" in order to restore proper functionality.

Vipersat therefore strongly recommends that the Automatic Updates configuration NOT be set to Automatic. This feature should be set to either of the two selections below:

- *Notify me, but don't automatically download or install them.*
- *Download updates for me, but let me choose when to install them.*

The Automatic Updates configuration window can be accessed from the **Start Menu** by choosing **Control Panel**, then opening it either directly or as a tab from the **System** panel.

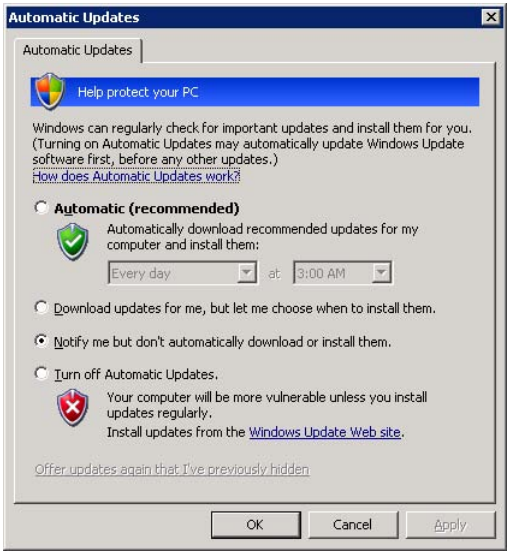


Figure 2-1 Automatic Updates window, Recommended Setting

Types of Installation

The VMS can be installed in three different configurations:

1. On a single VMS server; Vipersat Object Service (VOS).
2. On two or more (N:1) VMS servers in the optional fault-tolerant, redundant configuration; Vipersat Object Service (VOS).
3. On a client workstation; ViperView User Interface.

Server installations can be performed as either:

- **Clean Installation** - An installation on a server that has not previously operated as a VMS server, or that has had its hard drive re-formatted. With no existing network database, a full network configuration (Chapter 3, “VMS Configuration”) must be performed following installation.
- **Upgrade Installation** - An installation on a server that has previously been installed as a VMS server in a Vipersat network, operating with a previous version of VMS. An existing v3.7 network database will be automatically converted during installation.

Warning: When upgrading from v3.6.x, the existing network database is incompatible and will NOT be automatically converted during installation. Contact a service representative prior to attempting this type of upgrade. He/she will guide the operator in the necessary transition process to prevent loss of network configuration.

Note: It is NOT RECOMMENDED to run ViperView on the same machine as the VOS. Therefore, installing and running the VMS Client software component on a workstation that is separate from the VMS server is preferred.

Redundant Server Upgrade

For a redundant VMS configuration, perform the upgrade on the Standby server first. This will allow the installation of the new software and database creation to be verified without losing VMS service. If successful, continue the upgrade by doing the following:

- Deactivate the Active (Primary) server.
- Activate the Standby (Secondary) server.
- Perform upgrade installation on the now deactivated server.

This method provides a seamless upgrade with no VMS downtime.

The installation instructions in the following section include special instructions for each of these various installation types.

Caution: Failure to note and follow the instructions for the intended network configuration may cause the VMS installation to fail or to operate erratically.

Prepare Server for VMS Installation

The Vipersat Management System Server software should be installed on a high-performance, industry-standard computer running the Microsoft Windows Server 2008 or later operating system.

If not already done, perform the following tasks before proceeding with installation of VMS on the server:

- Limit DEP (Data Execution Prevention) — *see following section.*
- Create a user account in the Active Directory (example: VMS).
- Add the VMS user to the DCOM Limits.
- Reboot the server before continuing with the VMS installation.

Limit DEP (Data Execution Prevention)

DEP (Data Execution Prevention) is a service, available on some CPUs, which will actively block a virus or program which it determines acts like a virus. Without limiting the action of the DEP feature to essential Windows programs and services, this procedure will prevent DEP from blocking the actions associated with VMS.

Use the following procedure to make certain that this feature is limited to essential Windows programs only.

1. From the server's **Start** menu, go to the **System Properties** menu located at Start > Control Panel > System, as shown in figure 2-2.

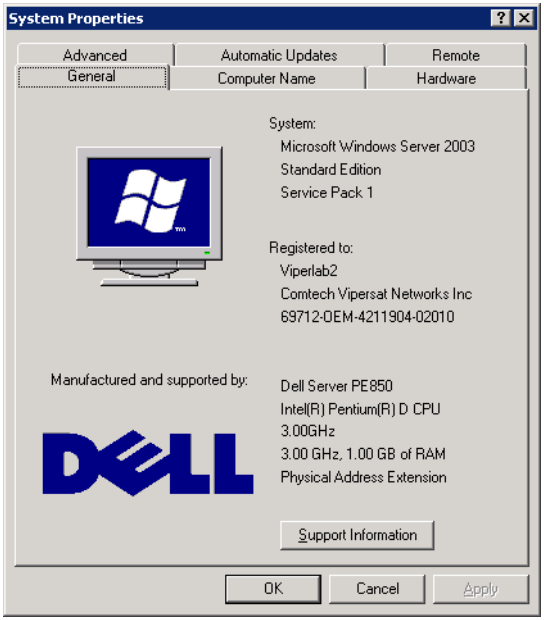


Figure 2-2 System Properties menu

2. Click the **Advanced** tab to display the dialog page shown in figure 2-3.

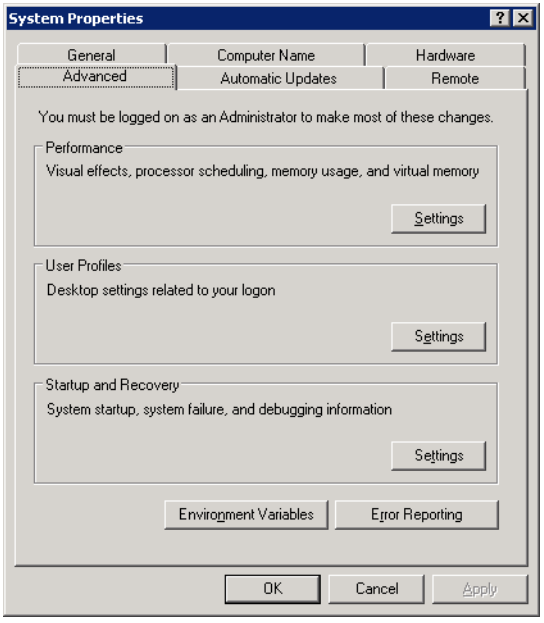


Figure 2-3 Advanced tab

3. In the **Performance** box on the **Advanced** tab, click the **Settings** button then click the Data Execution Prevention tab to show the dialog shown in figure 2-4.

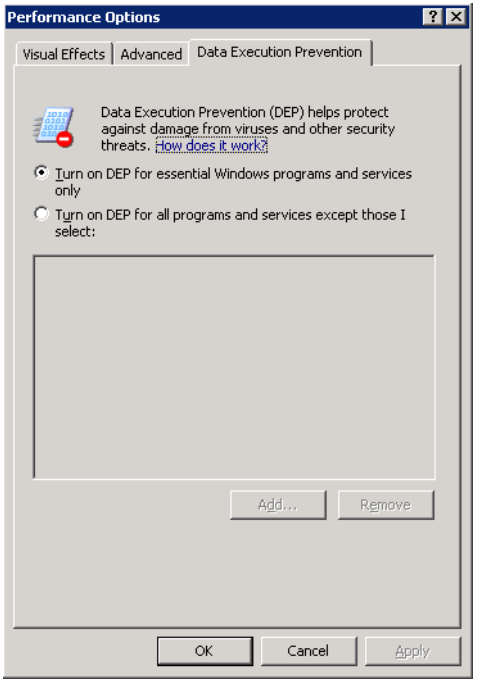


Figure 2-4 DEP tab

4. Select the **Turn on DEP for essential Windows Programs and services only** radio button. If the CPU processor does not support DEP, this radio button will be greyed out and unavailable.

5. Click the **OK** button to complete this procedure.

This action limits DEP to protecting only essential Windows programs without interfering with any other applications.

Enable Global Catalog Caching (Redundant Configurations)

Enabling Global Catalog Caching on the backup server(s) in a redundant configuration will ensure that the server will not fail on a subsequent boot after it has been brought online as the active server. Use the following procedure to enable Global Caching on backup servers.

1. From the Server **Start** menu, open the **NTDS Site Settings Properties** window from: Administrative Tools > Active Directory Sites and Services > Default-First-Site-Name.

2. From the **Site Settings** tab shown in figure 2-5, select the **Enable Universal Group Membership Caching** option to enable this function on the backup server.

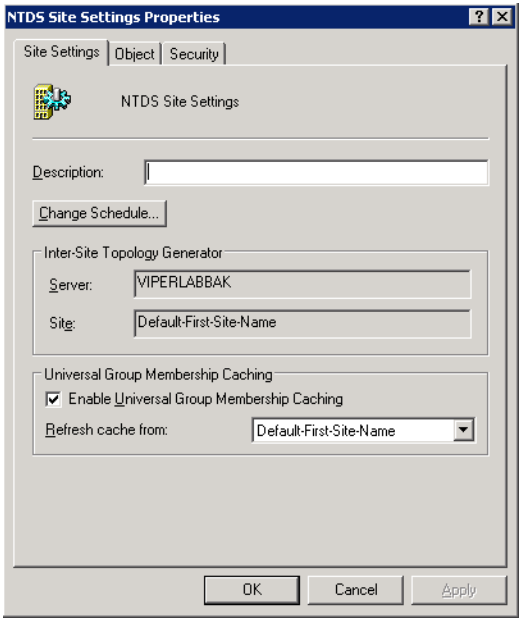


Figure 2-5 NTDS Site Settings

3. Click the **OK** button to complete this setting.

What this does is to cause the backup server to maintain its own global catalog in addition to the catalog resident on the active server. In the event of a switch-over, the backup server will operate until it is rebooted. At that time it will fail to run if it cannot find the Global Catalog on the active server, unless it has its own resident catalog, which this setting provides.

Configure Server as Domain Controller and/or DNS

NOTE

Note: If the server is to be used as a domain controller, it must be configured as a domain controller at this time before proceeding with the VMS installation.

In a redundant configuration, the servers must be configured as domain controllers and DNS.

If the VMS server is to be used as a Domain Controller and/or as a Domain Name Server (DNS), or if VMS is to be installed in an existing domain, follow the procedure outlined in Appendix D, “Domain Controller and DNS”, *Redundancy*, before starting the VMS installation.

Back Up VMS Database (Upgrade)

For VMS upgrades, it is recommended that the current VMS database be backed up prior to installing the new version of VMS. This precaution will allow for the current database to be restored in the event that the new install fails.

NOTE

Note: This database backup can only be restored on the current VMS version. It is not compatible with the new VMS version.

Should the new VMS installation fail, the fall-back procedure would be to re-install the previous version of VMS, then restore the database with the backup.

A successful installation of the new VMS will result in a new database. This new database should immediately be backed up, and any previous database backups should be removed from the server to avoid compatibility issues.

1. Right-click on the VMS Server icon and select **Backup** from the drop-down menu (figure 2-6).

Figure 2-6 Backup Command, VMS Server

2. Enter the **Name** for the backup file and select the directory location for saving the file from the **Save As** dialog window that opens (figure 2-7).

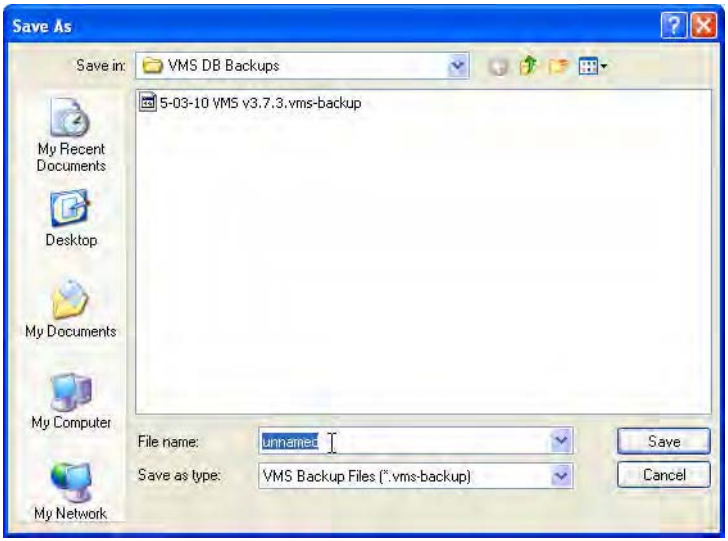


Figure 2-7 VMS Backup Save As dialog

Stop Previous VMS Version (Upgrade)

If there is an earlier version of VMS installed and running on the server, use the following procedure to stop VMS before proceeding with the new installation.

For VMS installation on a server that does NOT have a previous version of VMS installed, skip this section and proceed to the section “VMS Server Installation” on page 2-14.

Caution: If a prior version of VMS is installed and running on the server, you must first stop, then uninstall, this prior version as described in this and the following procedure.

Caution: Stopping VMS does not change the configuration of the server. Refer to Appendix D, “Domain Controller and DNS” for detailed instructions.

1. Right-click in the Windows status bar and select **Task Manager** from the pop-up menu. The Windows Task Manager window will appear.

2. From the **Processes** tab, scroll down the list to find the three VMS processes that are running—*VConMgr.exe*, *ViperView.exe*, and *VOS.exe*, as shown in figure 2-8.

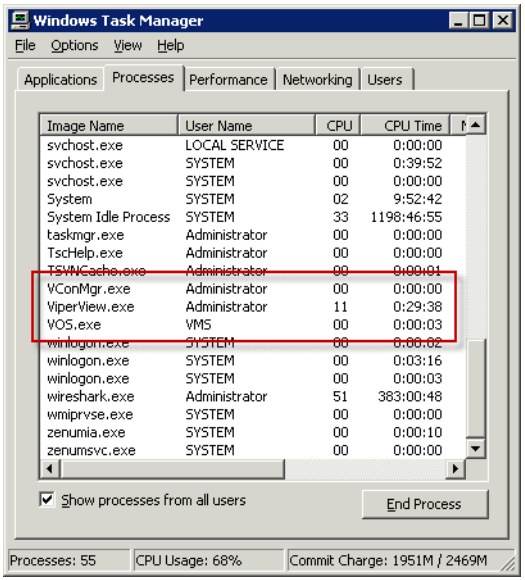


Figure 2-8 Windows Task Manager, Processes tab

3. Select each process and click on the **End Process** button. A Task Manager Warning dialog will appear (figure 2-9)—click on the **Yes** button to terminate the process.

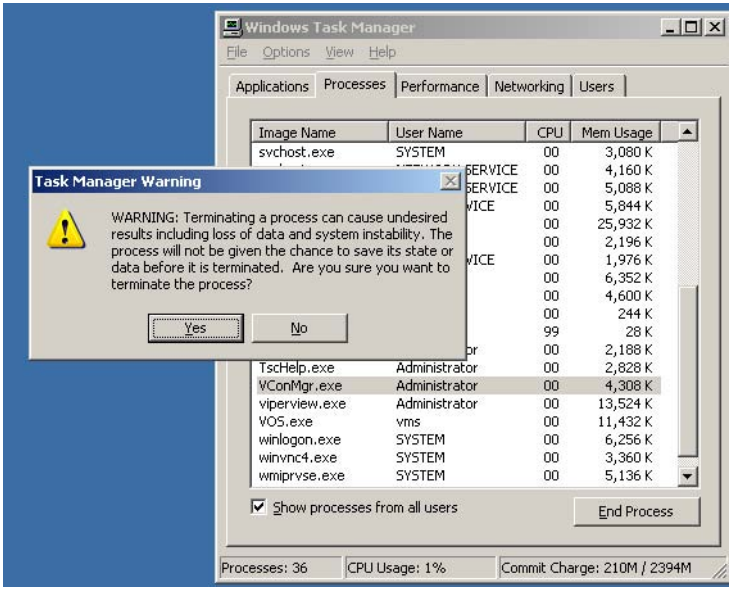


Figure 2-9 Task Manager Warning dialog

4. After each of the three processes have been terminated, close the Task Manager window then re-open it to confirm that the processes are no longer running.

5. Once the Vipersat Management System service has been stopped, uninstall the previous version of VMS from the server as described in the following section.

Uninstall Previous VMS Version (Upgrade)

1. Uninstall the previous version of VMS by selecting **Add or Remove Programs** from the server's **Control Panel**, as shown in figure 2-10.

Figure 2-10 Add or Remove Programs Control Panel

2. Select **Vipersat Management System** and click the **Remove** button (figure 2-11).

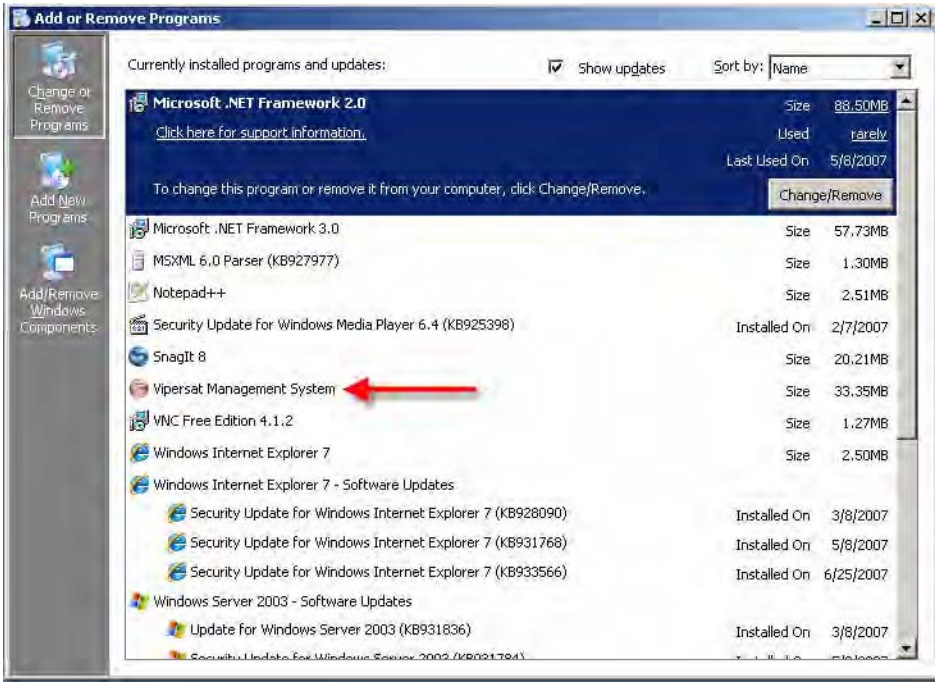


Figure 2-11 VMS, Remove Program

3. Close the **Add or Remove Programs** window.

VMS Server Installation

Note: For VMS Redundancy Server configurations, after installing VMS on each of the servers as described in this section, refer to Appendix C, “Redundancy”, for detailed instructions for configuring the redundant servers.

The installation process is automated and typically does not require manual intervention unless the installation is to be non-standard.

1. Locate the file **VMS 3.x Core Setup.exe** on the VMS distribution CD and double-click it to start the VMS Installer.

2. After starting the VMS installer, the **Vipersat Management System Setup Wizard** welcome screen, shown in figure 2-12, is displayed. Click the **Next** button to continue.

Figure 2-12 Setup Wizard Welcome screen

3. On the **License Agreement** screen, shown in figure 2-13, click the **I Agree** button to proceed.

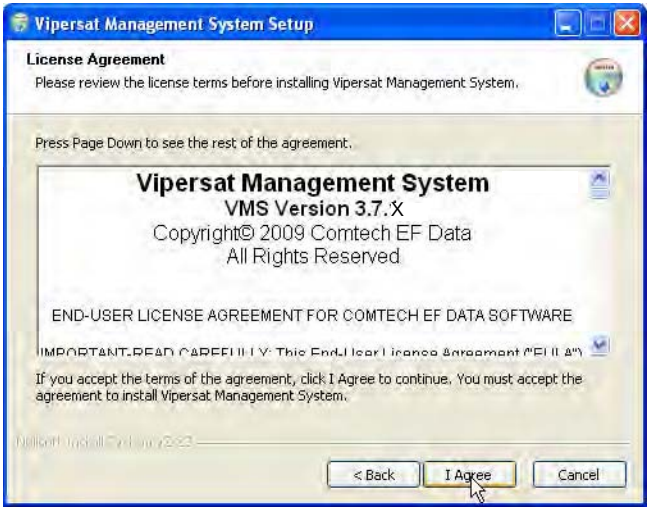


Figure 2-13 License Agreement screen

4. The VMS software is comprised of two main components, the Server component and the Client component. From the **Installation Type** screen shown in figure 2-14, select the radio button for the type of installation you will be making. For a VMS Server installation, select either *Full Install* or *Server Install*. (The *Client Install* selection is for a VMS Client workstation installation.)

- **Full Install** - This type of installation installs both components, and allows a local user to operate VMS locally on the server and also remotely. This installation type requires a USB key to operate VMS.
- **Server Install** - This type of installation only installs the Server component, and allows the VMS server to be operated through a remote connection by a client—the VMS can not be operated from the local server. This installation type requires a USB key to operate VMS.
- **Client Install** - This type of installation only installs the Client component, and is used to install the VMS client on a workstation that will be used to connect remotely to servers on the same LAN that are running the VMS. This installation type does not require a USB key to operate VMS.

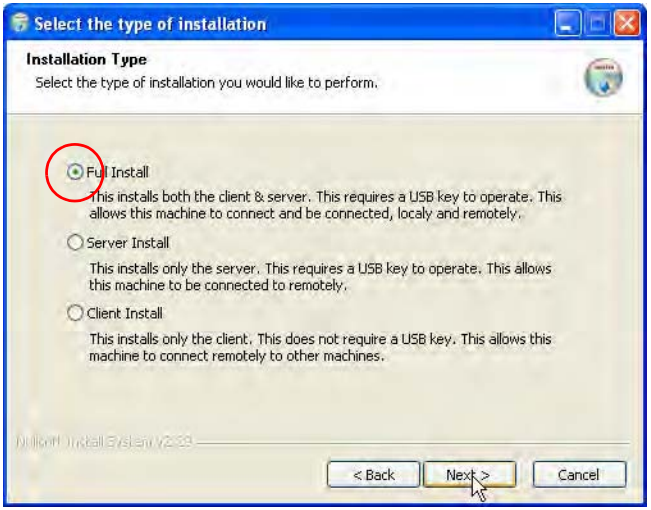


Figure 2-14 Installation Type screen

5. Click the **Next** button to proceed to the VMS Setup screen.

6. The Service Configuration defaults with all three boxes checked as shown in figure 2-15. It should be left this way.

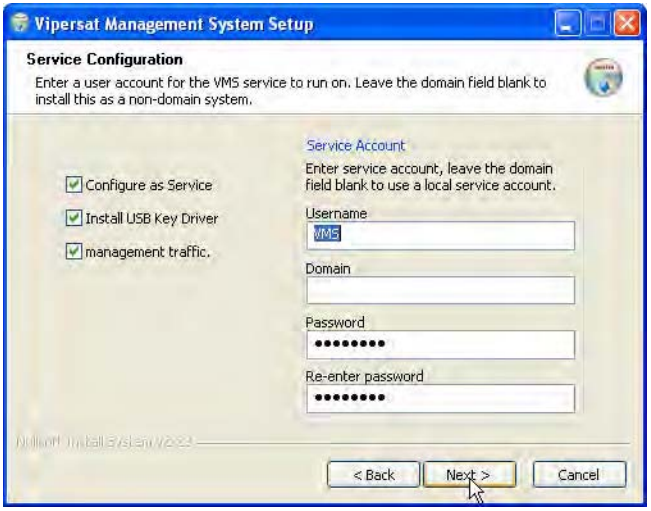


Figure 2-15 Service Configuration dialog

7. The **Username** for the account is auto-filled with the default entry (VMS). It is recommended not to change this setting.

Note: If this is an upgrade, use the same name as before.

8. If the VMS server is to operate in a Domain, enter the domain name in the Domain field exactly as the domain is named.

Caution: Failure to have an exact match between the assigned domain name and the domain name entered in this dialog will cause VMS to fail, requiring re-installation.

9. The **Password** field is auto-filled with the default password, V1persat. Enter a new password, if desired, to change the default setting.

Note: If this is an upgrade of a domain account, enter the password associated with this acount.

10. Click the **Next** button when this dialog is complete.

11. The **Choose Components** dialog appears, as shown in figure 2-16. All services are selected by default for a typical VMS installation. It is recommended that these settings not be changed, except for non-standard installations.

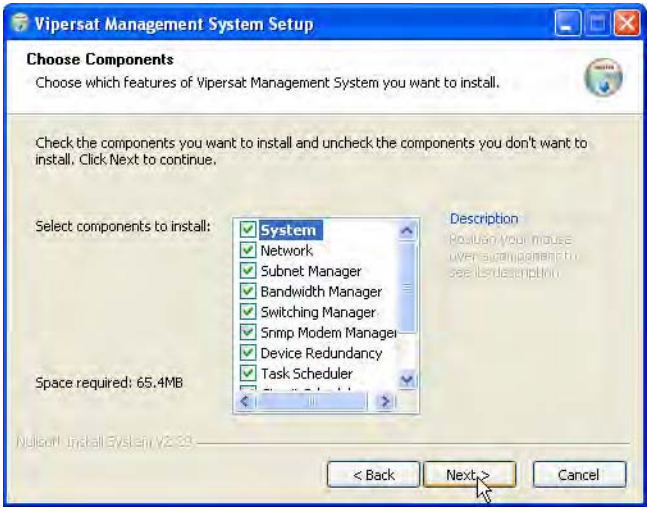


Figure 2-16 Choose Components dialog

12. Click the **Next** button to proceed.

13. In the **Choose Install Location** dialog shown in figure 2-17, it is recommended that the default file location be used. Click the **Next** button to continue.

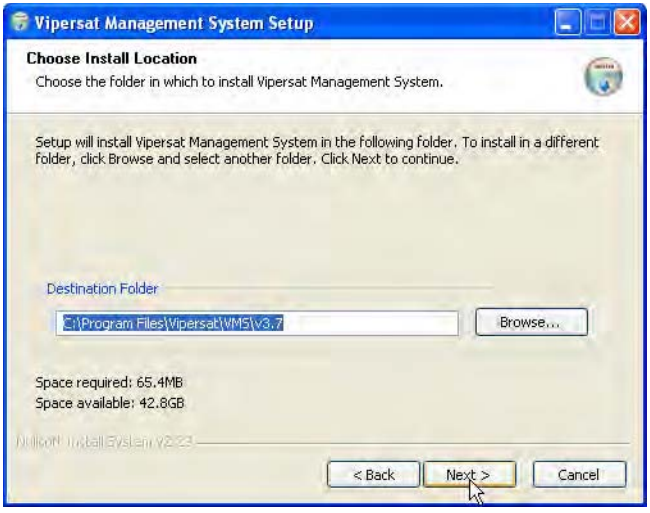


Figure 2-17 Choose Install Location dialog

14. From the **Choose Start Menu Folder** dialog shown in figure 2-18, accept the default folder name, VMS 3.x, and click the **Install** button to start the installation process.

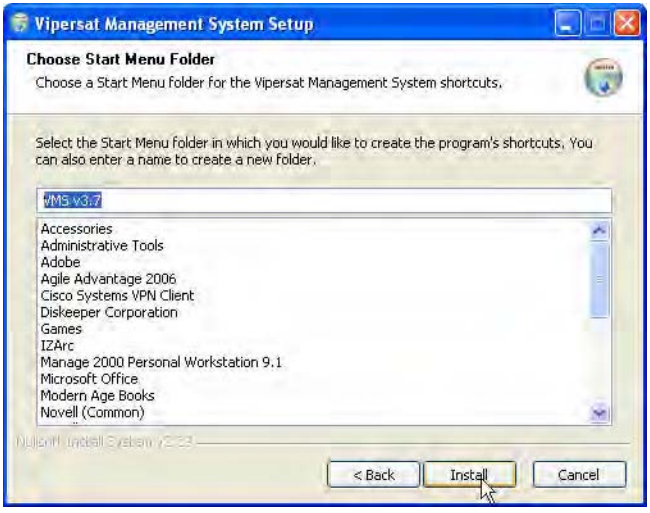


Figure 2-18 Choose Start Menu Folder dialog

15. The installation process will begin and a green progress bar will display.

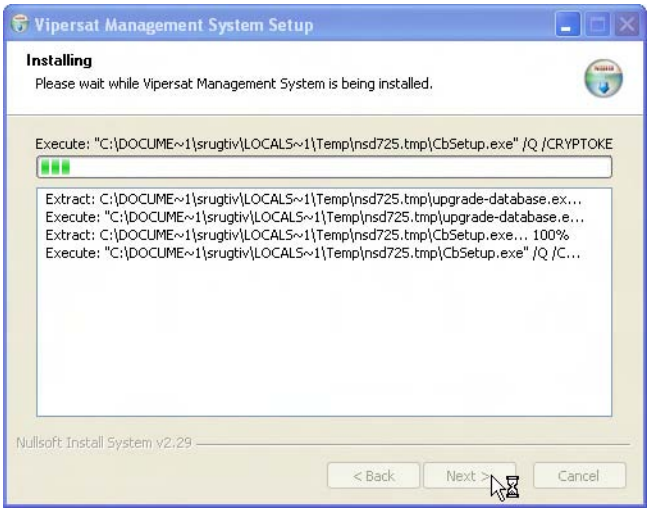


Figure 2-19 Installing dialog

16. The installation process will continue and, when completed, the screen shown in figure 2-20 will be displayed. Click the **Next** button.

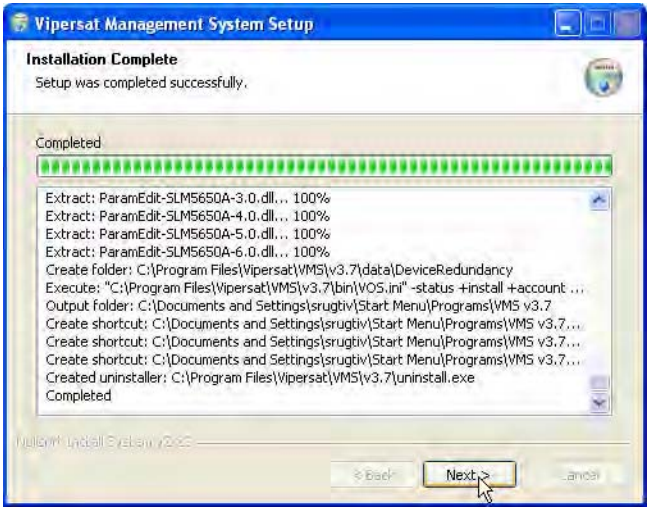


Figure 2-20 Installation Complete screen

17. Click the **Finish** button to exit the VMS Setup Wizard.

Figure 2-21 VMS Setup Wizard Finish dialog

Management Security Installation — Option

NOTE

Note: The Management Security feature is not provided with standard VMS installations, and is available only upon request and through an authorized agent.

This feature requires the use of a specially programmed Crypto-Key.

Management Security is an optional software module for the VMS that protects the M&C messages that pass between SLM-5650A modems and the VMS over exposed LAN/WAN segments within the network.

1. Execute the **VMS Management Encryption Option Setup.exe** application. This will open the Setup Wizard that will install the AES .dll file into the appropriate program file directory.

2. Complete the wizard setup to finish the installation.

This completes the installation of the VMS Management Security Option.

NOTE

Note: If this is a standalone installation on a workgroup server, or an upgrade installation, move on to the section “Verify Server Installation” on page 2-25.

If this is an installation on a new or completely rebuilt Domain Controller, continue with the following section, “Set Com Security for VMS”.

Set Com Security for VMS

1. From the Windows **Start** menu, select **Settings** and open up the **Control Panel**, as shown in figure 2-22 below.

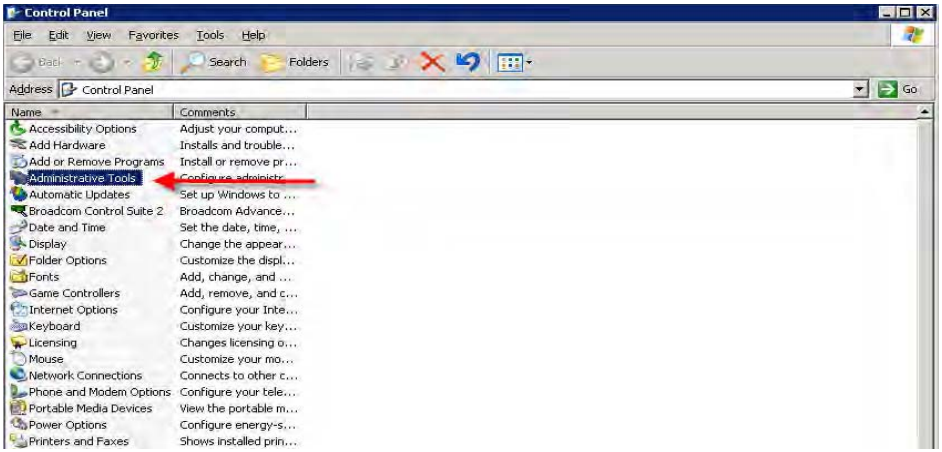


Figure 2-22 Control Panel

2. Select **Administrative Tools** and then **Component Services**, as shown in figure 2-23.

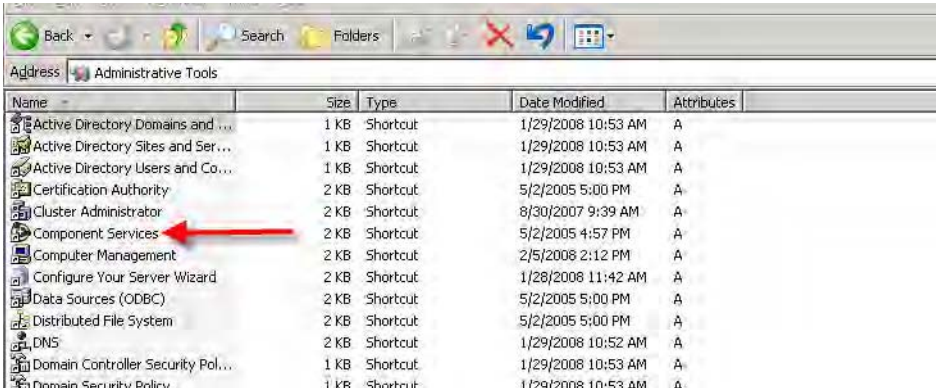


Figure 2-23 Administrative Tools

3. Expand the Component Services tree until “My Computer” appears. Right-click on My Computer and select **Properties**, as shown in figure 2-24.

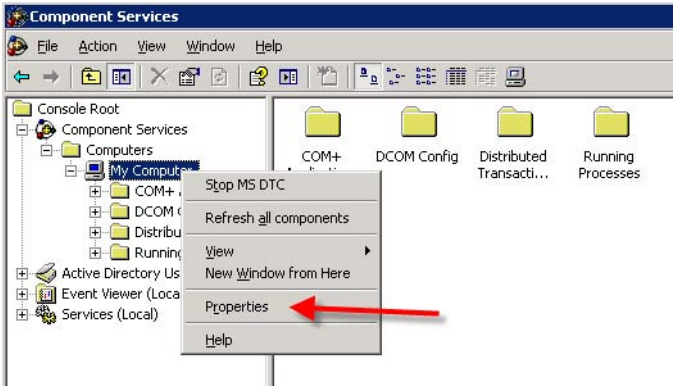


Figure 2-24 Component Services, My Computer Menu

4. Select the **COM Security** tab, then the **Edit Limits** button under *Launch and Activation Permissions*, as shown below in figure 2-25.

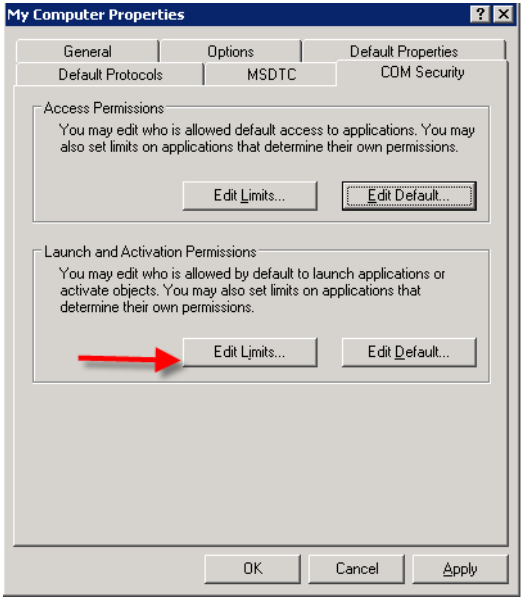


Figure 2-25 Com Security, Edit Limits

5. In the Launch Permissions window, select **Add** as shown in figure 2-26.

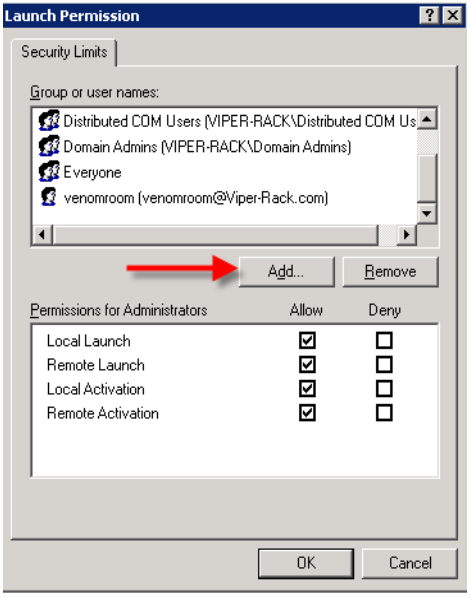


Figure 2-26 Launch Permissions

6. Ensure that the Location selection is the domain, then type “VMS” in the object names box and click the **Check Names** button. If the location is correct, the object name will be found and displayed underlined, as shown by the example in figure 2-27.

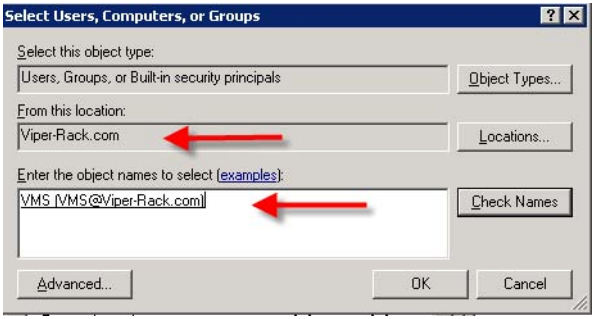


Figure 2-27 Select Users

7. Click on **OK**. The Launch Permissions window will display the new user highlighted. Check all of the **Allow** boxes as shown in figure 2-28, then click the **OK** button.

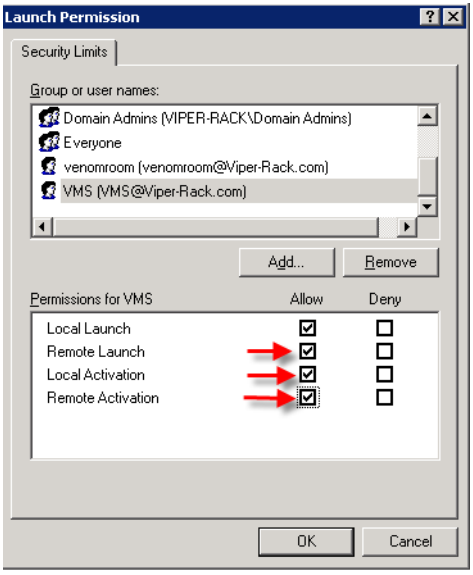


Figure 2-28 Launch Permissions with New User

This concludes setting the Component Securities on the Domain Controller.

Verify Server Installation

This verification process utilizes the ViperView Client, and thus can only be executed using just the server when a *Full Install* has been performed. For a *Server Install*, verification of successful installation requires the use of a Client workstation (see “Verify Client Installation” on page 2-37).

1. Insert the Vipersat Crypto-Key into an available USB port on the VMS server. This key is required to run the VOS.

2. Open the Services window on the server by selecting **Services** from the Start > Administrative Tools menu.

Figure 2-29 Services, Administrative Tools menu

3. Select **Vipersat Management System** from the Services list as shown in figure 2-30, then click on **Start** the service.

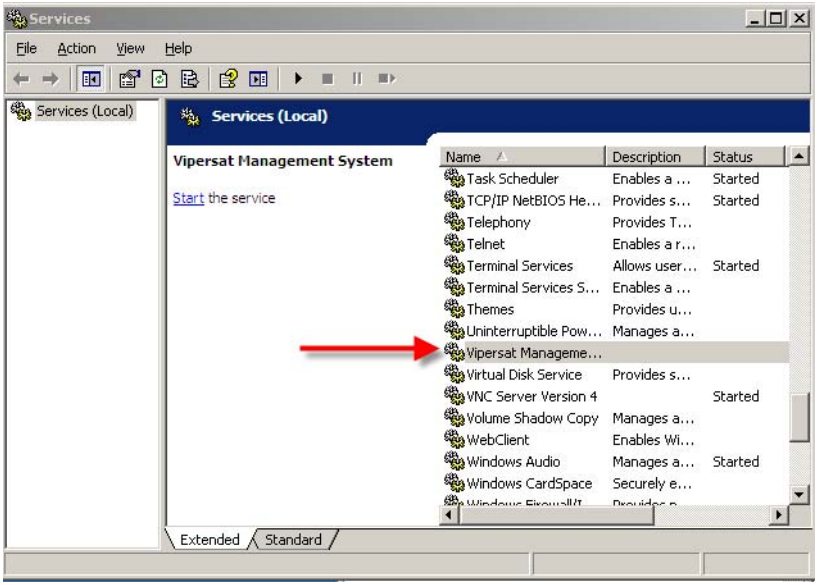


Figure 2-30 Vipersat Management System Service

This will start the VOS (Vipersat Object Service) process. VOS.exe will appear in the Processes tab of the *Windows Task Manager*.

NOTE

Note: The Vipersat Crypto-Key must be connected to the server's USB port. Otherwise, the attempt to start VMS will fail.

If the Start attempt fails, proceed to "VMS Service Start Failure" on page 2-27.

4. Open the **Connection Manager** from the path Start > Programs > VMS > Connection Manager.

The **Connect** dialog will appear.

Figure 2-31 Server Connect dialog

5. When using the server, accept “localhost” and click on the **OK** button. When using a client machine, enter the server IP address.

   The **ViperView** window will appear, as shown in figure 2-32.

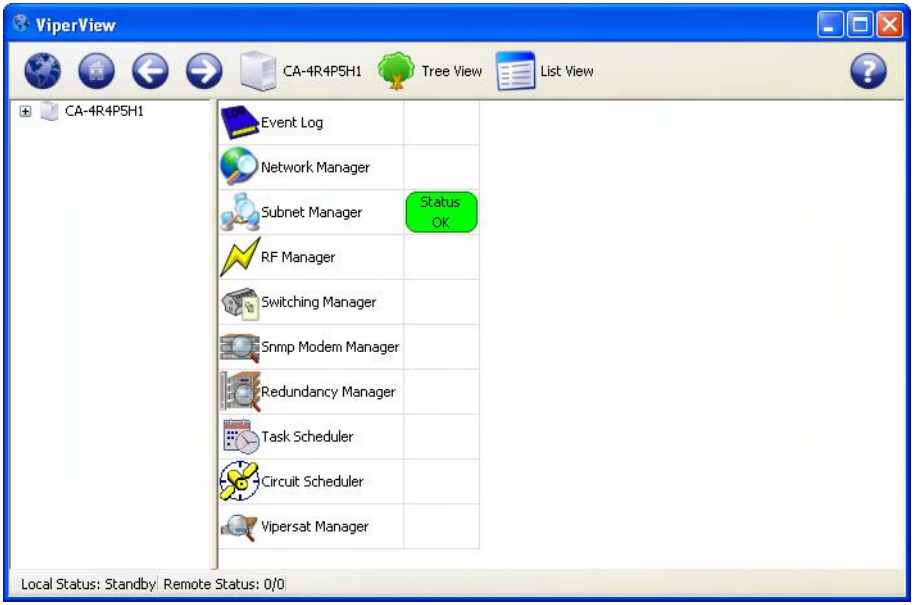


Figure 2-32 Successful Installation, ViperView

To verify the version of VMS that is installed, click on the  on the far right of the ViperView menu bar and select **About**.

For upgrade installations only, activate the server processes and verify that the network database configuration is accurately displayed.

VMS Service Start Failure

Should the attempt to start the VMS service fail, verify whether or not the Crypto-Key is the cause of the failure.

1. Open the Windows **Event Viewer**.
   [Start > Settings > Control Panel > Administrative Tools > Event Viewer]

2. Select **Applications** and look through the list for the appearance of an Error Type for Vipersat Management System, as shown in figure 2-33.

3. Double-click the event to open the **Properties** dialog (figure 2-34).

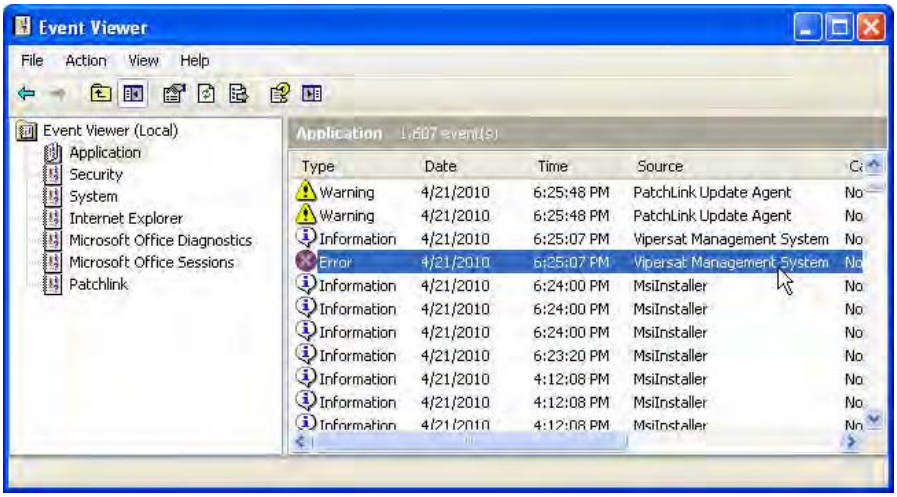


Figure 2-33 Application Error, Event Viewer

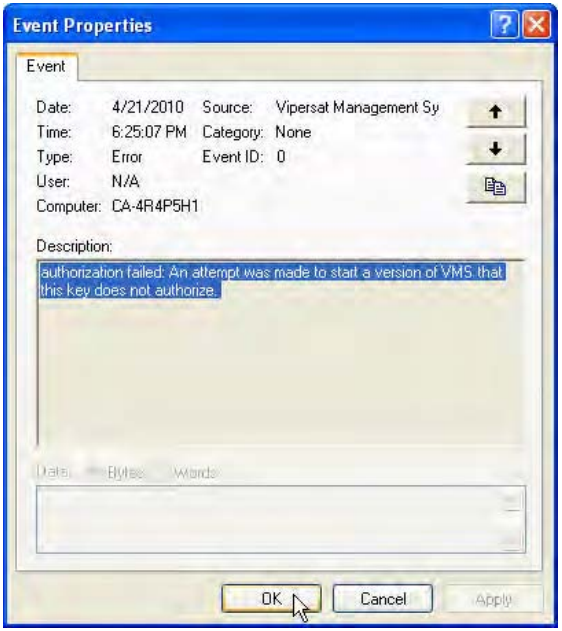


Figure 2-34 Event Properties window

If the key is the source of the problem, contact the network administrator or Comtech Vipersat Network Products Customer Support for replacement.

If the key is not the cause of the Start failure, repeat the installation procedure and try again. If still no success, contact Customer Support.

This completes the VMS Server installation procedure.

- For *VMS Standalone Server configurations*, proceed to Chapter 3, “VMS Configuration”, to configure the VMS database for the satellite network.
- For *VMS Redundancy Server configurations*, proceed to Appendix C, “Redundancy”, for instructions on configuring redundant servers.

VMS Client Installation

The Vipersat Management System Client software should be installed on a high-performance, industry-standard workstation computer running Microsoft Windows XP Professional with SP3. For specifications for the minimum recommended VMS platform configuration, please refer to the *VMS Release Notes* for the version of software that will be installed.

Note: To run the ViperGlobe application, it is necessary to have a video graphics card that supports a minimum of 256 MB of video memory and supports Pixel Shader Model 2.0 - 3.0 (reference NVIDIA™ Graphics Card family, 7000 series or equivalent).

Dual monitors are recommended for greater viewing of multiple windows.

The VMS Client software is installed using the same installation disk used for the Server installation. The Installation Wizard will prompt the user for Full Install, Server Install, or Client Install. Selection of the Client will only install the necessary files without prompting for USB key and password. This type of installation only installs the Client component on a workstation that will be used to connect remotely to the server(s) on the same LAN that are running the VMS. This installation type does not require a USB key to operate the software.

Note: The installation does not require the USB Crypto-Key as there are no services running on the client workstation. This machine will require network connections and proper security configurations to connect to the active VMS sever.

Note: The install must be done from an account with Administrator Privileges.

For the VMS Client installation, follow the same procedure used for the Server installation provided in the section “VMS Server Installation” on page 2-14. However, in step 4., select the radial button **Client Install**, as shown below in figure 2-35.

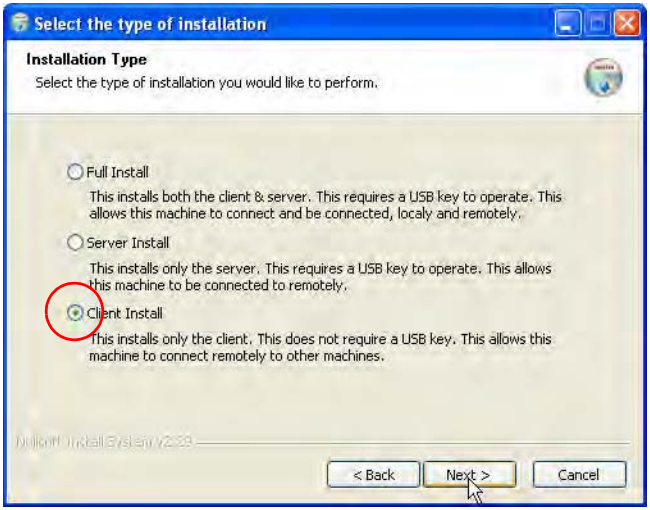


Figure 2-35 Client Installation Type

Once the installation wizard is finished, return here to continue with the following section.

Create Client Accounts

It is necessary to configure the appropriate security settings for the Client workstation to gain network access privileges to the VMS server.

If this is a client for a *standalone VMS*, an account must be created on the VMS server for the client to log into. The VMS account must also be added to the Client machine.

If this is a client for a *redundant VMS*, perform the following steps to create an account on the Primary VMS Domain Controller and set COM Security.

1. Open up Adminsitrative Tools and select **Active Directory Users and Computers**, as shown in figure 2-36 below.

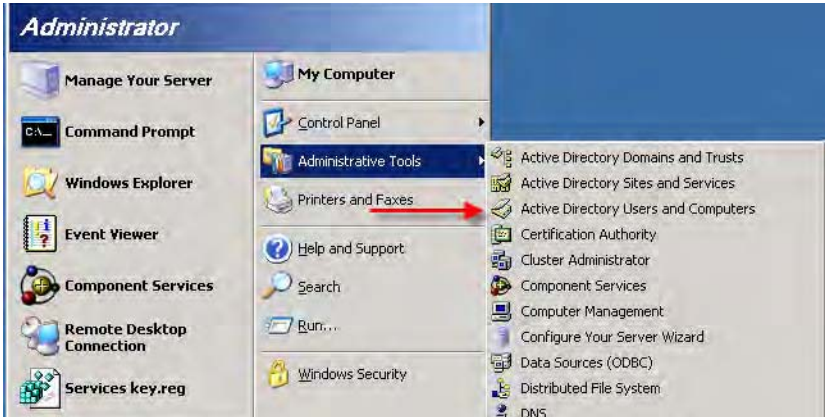


Figure 2-36 Admistrative Tools menu

2. Expand the Domain name tree, right-click on **Users** and select **New Group** from the drop-down menu, as shown below in figure 2-37.

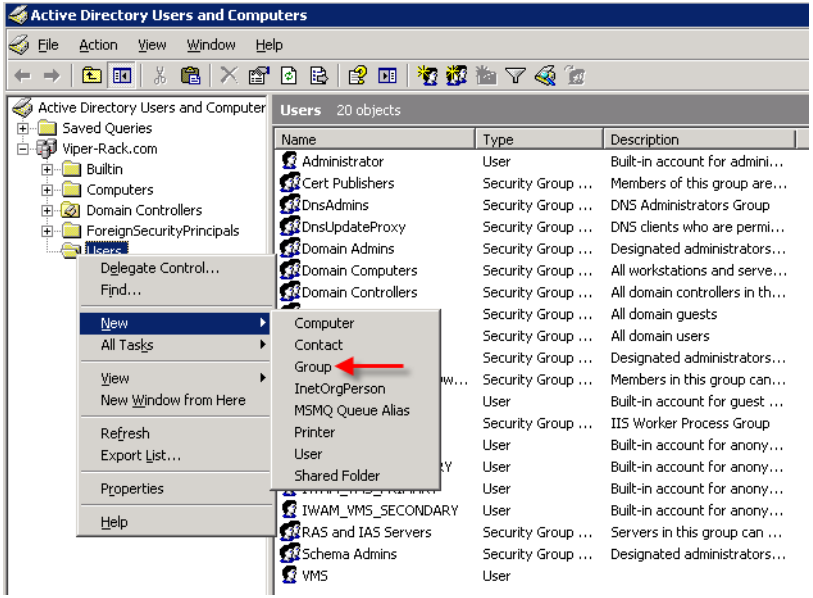


Figure 2-37 Create Group

3. The New Object–Group dialog will open. Under *Group Name*, enter **VMS Users** and ensure that the *Group Scope* and *Group Type* are set as shown in figure 2-38.

Click on the **OK** button to close the dialog.

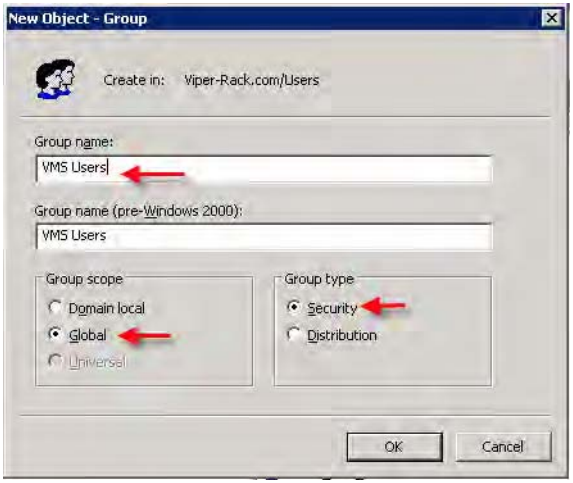


Figure 2-38 Create Group Dialog

4. Right-click on **Users** again in the Active Directory window and select **New User**. The New Object–User dialog will open (figure 2-39). The user name can be anything desired and will be used to log onto the server from the client machine.

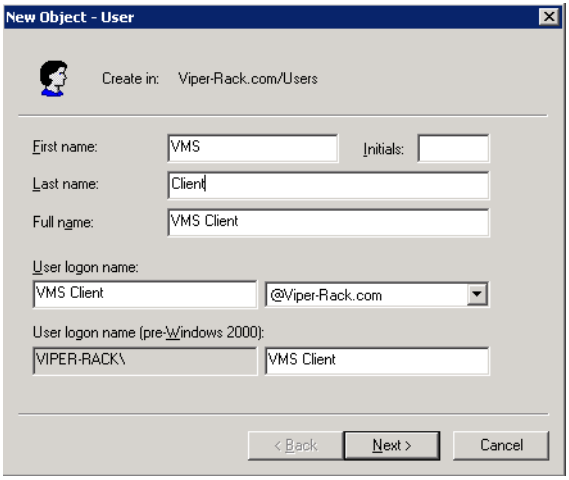


Figure 2-39 Create User Dialog

5. Click **Next** and the User Password dialog will open, as shown in figure 2-40. Create and confirm a password and set the properties as indicated.

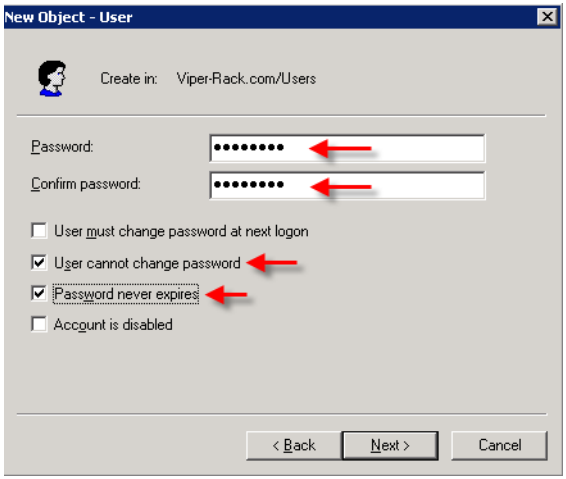


Figure 2-40 Setting the User Password

6. Move the new user to the VMS users group. Do this by right-clicking on the user that was just created and opening the **Client Properties** page shown below in figure 2-41. Open the **Member Of** tab.

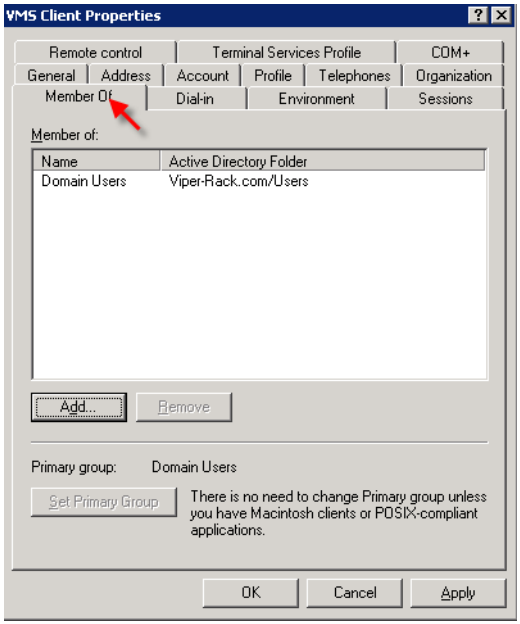


Figure 2-41 Client Properties

7. Click the **Add** button. The Select Group dialog will open, as shown in figure 2-42. Ensure that the location is the domain, then enter **VMS Users** as the object name and click **Check Names** to verify.

Click **OK** to close the dialog.

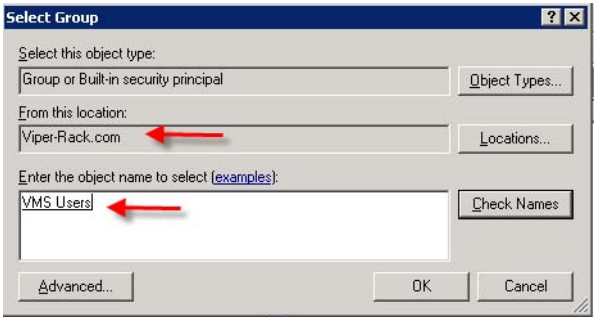


Figure 2-42 Select Group Dialog

8. Close the Active Directory window.

9. Open up Adminsitrative Tools and select **Component Services** to open the Component Services window, as shown below in figure 2-43.

10. Expand the Component Services tree and right-click on **My Computer**, then select **Properties** from the drop-down menu.

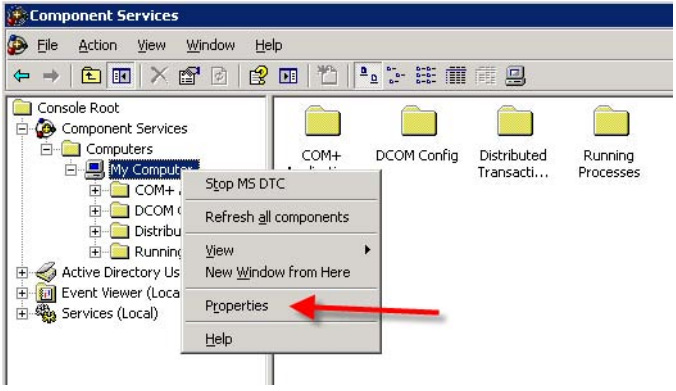


Figure 2-43 My Computer Properties

11. In the My Computer Properties window, open the **COM Security** tab as shown in figure 2-44. Under *Launch and Activation Permissions*, click on the **Edit Limits** button.

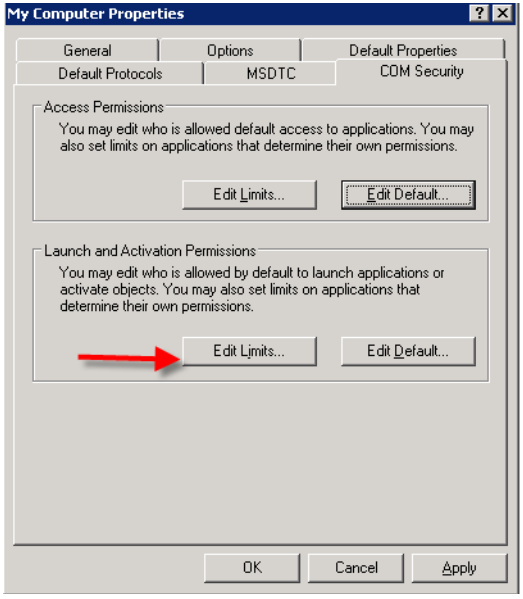


Figure 2-44 Edit Limits

12. From the Launch Permission dialog, click on the **Add** button.

- Enter **VMS Users** in the Select Users, Computers, or Groups dialog to add the group to the launch permissions.
- Check all of the **Allow** boxes for VMS Users, as shown in figure 2-45.

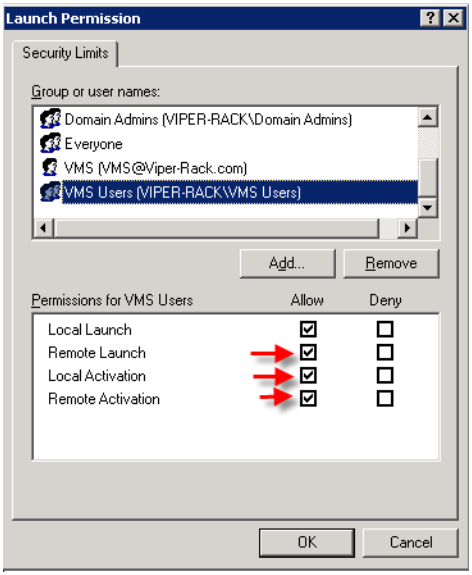


Figure 2-45 Launch Permissions

13. Click on the **OK** button to launch the selected permissions and close the dialog.

Verify Client Installation

After installation, verify that the VMS Client installation was successful by running the program. The VMS Server must be running VOS, the Vipersat Management System service (see “Verify Server Installation” on page 2-25 for the necessary steps to start the VMS service).

1. Open the **Connection Manager** using the path Start > Programs > VMS > Connection Manager.

2. At the connection prompt in the **Connect** dialog, enter the IP address of the VMS Server and click on the **OK** button (figure 2-46).

Figure 2-46 Connect dialog

3. The **ViperView** window will appear, as shown in figure 2-47.

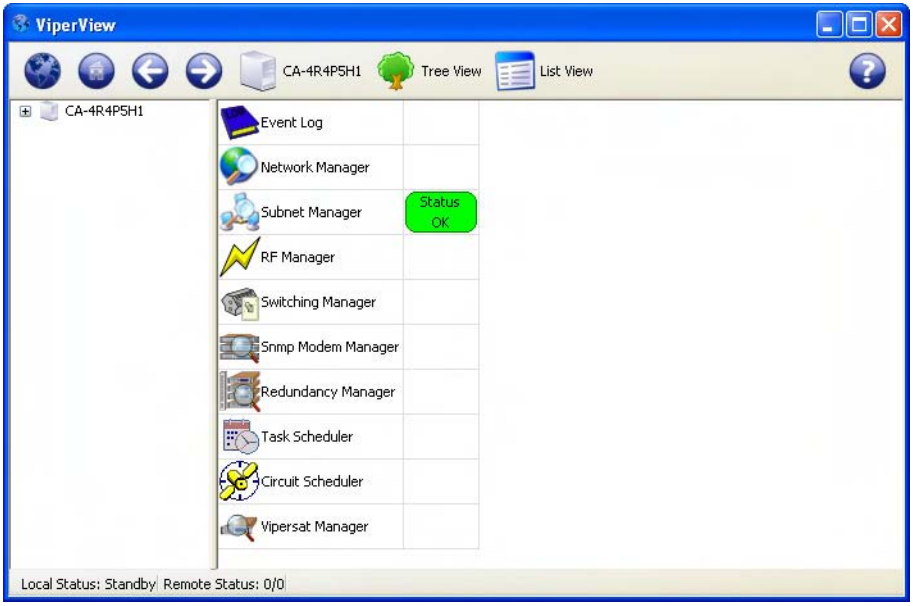


Figure 2-47 ViperView window, VMS Client

To verify the version of VMS that is installed, click on the  on the far right of the ViperView menu bar and select **About**.

This completes the VMS Client installation procedure.

ViperGlobe Installation

ViperGlobe is an optional VMS application program that is installed on the VMS Client workstation. This workstation must have the necessary supporting video graphic hardware that is required to run this application. ViperGlobe will install in the same directory as the VMS Client.

NOTE

Note: To run the ViperGlobe application, it is necessary to have a video graphics card that supports a minimum of 256 MB of video memory and supports Pixel Shader Model 2.0 - 3.0 (reference NVIDIA™ Graphics Card family, 7000 series or equivalent).

Installation Procedure

1. Locate the **VMS 3.7.x Globe Setup.exe** file on the VMS distribution CD and double-click on the file to start the installer.

   This will open the *Vipersat Network Globe Setup Wizard* (figure 2-48) that will install the ViperGlobe application.

Figure 2-48 Vipersat Network Globe Setup Wizard

2. Click the **Next** button to progress through the Setup process.

3. Specify the **Start Menu Folder** for locating the program shortcut. This folder defaults to the folder that was specified for the VMS Client installation.

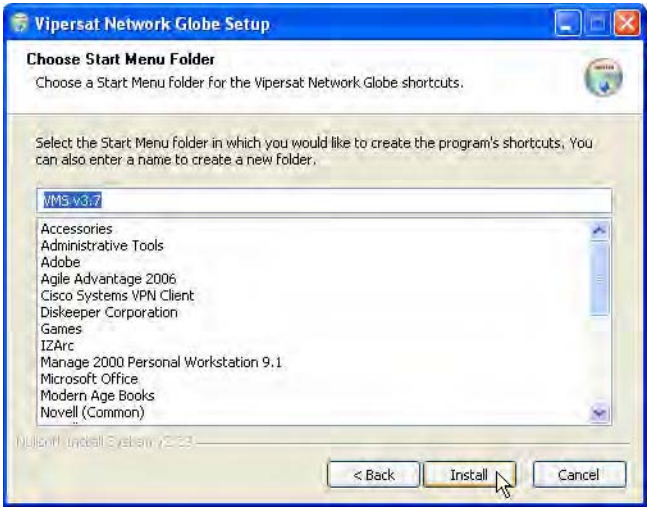


Figure 2-49 Choose Start Menu Folder

4. Click the **Install** button to begin the installation of the application files.

The installation progress will be displayed (figure 2-50), ending with the "Installation Complete" notification.

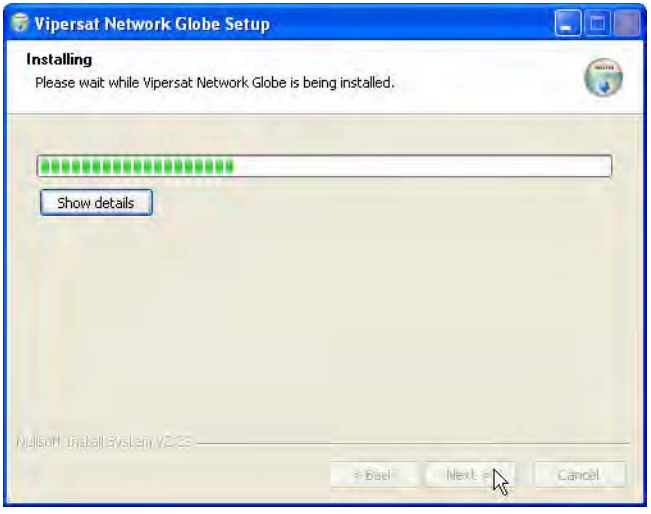


Figure 2-50 Installing Progress, Network Globe Setup

5. Click on the **Next** button, then **Finish** to close the setup wizard.

Figure 2-51 Completing Vipersat Network Globe Setup

Verify ViperGlobe Installation

After installation, and with all Client connections established to the VMS server, launch ViperGlobe:

1. Open ViperGlobe by selecting **Vipersat Network Globe** from the path Start > Programs > VMS > Vipersat Network Globe.

2. At the connection prompt, enter the IP address of the Active VMS server and click on the **OK** button in the **Connect To** dialog.

3. The **ViperGlobe** window will appear, as shown in figure 2-52.

   Note that this Globe View example shows an existing Vipersat network that has already been configured.

Figure 2-52 ViperGlobe window

This completes the ViperGlobe installation procedure.

VMS Web Services Installation & Configuration

Services Overview

The Comtech EF Data–Vipersat Network Products Group VMS Web Services SOAP (Simple Object Access Protocol) Server offering provides an interface for two VMS client applications and communications with the VMS (RPC server):

- **VNO** (Virtual Network Operator) – Allows satellite network operators to selectively extend network operation functions to individual customers for monitoring and controlling their own network(s).
- **ArrangeLink** (AL) – A satellite communications Circuit Scheduler interface allowing customers to schedule network resources for applications such as video conferencing and scheduled broadcasting.

The SOAP interface runs on a web services proxy server that hosts the web applications for VNO and AL using Internet Information Services (IIS). The user interface for these applications is accessed using a web browser from a client PC workstation.

The network component diagram shown in figure 2-53 reflects the recommended configuration for implementing the VMS Web Services. To minimize latency issues, the host platform for these services should be on the same LAN as the VMS Server. Should a network web server be locally available, it would serve as a logical platform for the SOAP server, as shown in the diagram.

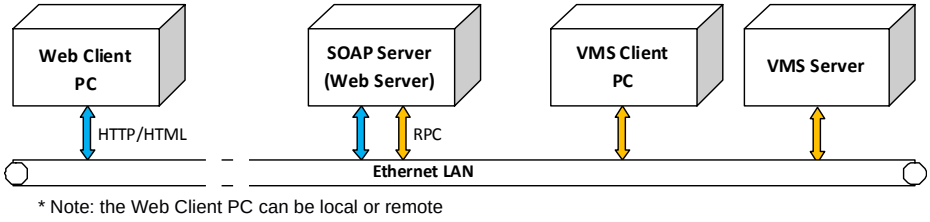


Figure 2-53 VMS Web Services Components

If there is no local web server available to host these services, then the following alternative configurations can be utilized:

- If the VMS is *standalone*, then the VMS Server can host the Web services and applications.
- If the VMS is *redundant*, then another local server must host the Web services and applications in order to retain true redundancy.

Requests and responses transmitted between the web application and the web service use SOAP over HTTP protocol. The SOAP request is translated into an RPC call into the VOS and the response is then returned to the web application. This response is transformed into HTML and sent back to a web browser that presents the user interface to the operator.

The ViperView client communicates directly with VOS using DCOM/RPC protocols. ViperView is used by the Central Network Operator for administrative functions, such as creating VNO networks and other resources in the network.

For additional information and details on the client applications, refer to the *VNO Quick Start Guide* and the *ArrangeLink User Guide*.

SOAP Server Prerequisites

The following items are required when installing the SOAP Services onto the server:

- Windows Server 2003 operating system, with current Service Pack.
- Microsoft Internet Information Services (IIS), current version, to provide Web server capabilities over an intranet, the Internet, or an extranet. This allows other PC workstations to access the web services remotely.
- Microsoft ASP.NET, current version.
- Full VMS Install.
- If a firewall is installed on the server, it must be turned off or set correctly to allow HTTP.
- The SOAP server must be on the same LAN and have either direct access or an Ethernet connection to the VMS server(s).
- The SOAP server must be on the same domain as the VMS server(s).
- The installer must have administrator privileges on the server.

Caution: Running SOAP Services on a machine enables that machine to act as an HTML server which may increase its vulnerability when connected to the Internet.

Server Preparation

Verify that Internet Information Services (IIS) and ASP.NET are installed and activated (checked):

1. From the Start menu, open the Add or Remove Programs control panel. Click on the **Add/Remove Windows Components** button in the left panel of the window.

The *Windows Components Wizard* window will open (figure 2-54).

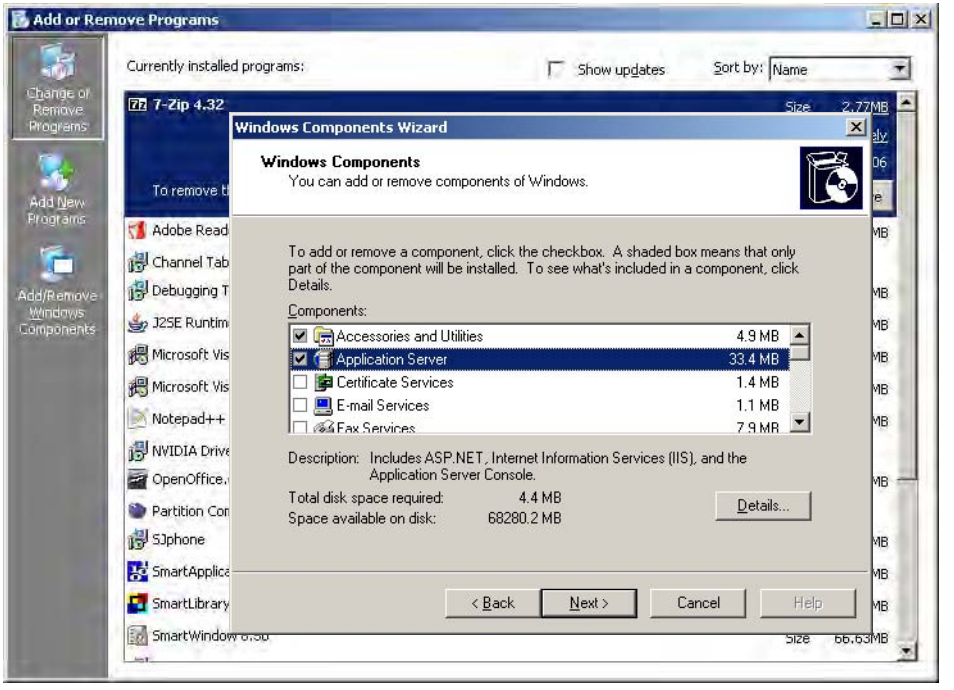


Figure 2-54 Add/Remove Windows Components

2. Click on **Application Server** and ensure that the check box is checked, then click on the Details button.

The *Application Server* window will open.

3. Ensure that the check boxes for ASP.NET and IIS are as shown in figure 2-55, below.

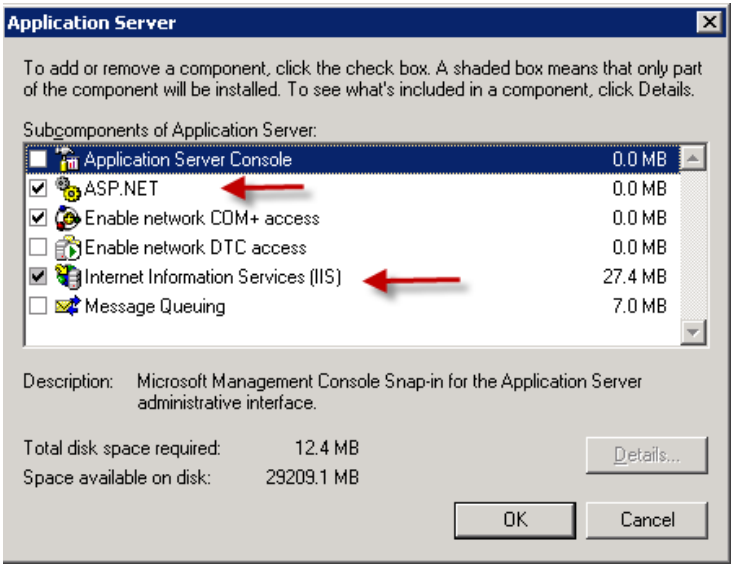


Figure 2-55 Configure Windows Application Server

4. Click on the **OK** button in the Application Server window to confirm the selections.

5. Click on the **Next** button in the Windows Components Wizard window to execute the component installations.

Set the IIS Default Application Pool Identity:

1. Open the **Internet Information Services (IIS) Manager** from Administrative Tools.

2. In the left window panel, expand the local computer tree view down to DefaultAppPool and select the **Properties** command from the drop-down menu (figure 2-56).

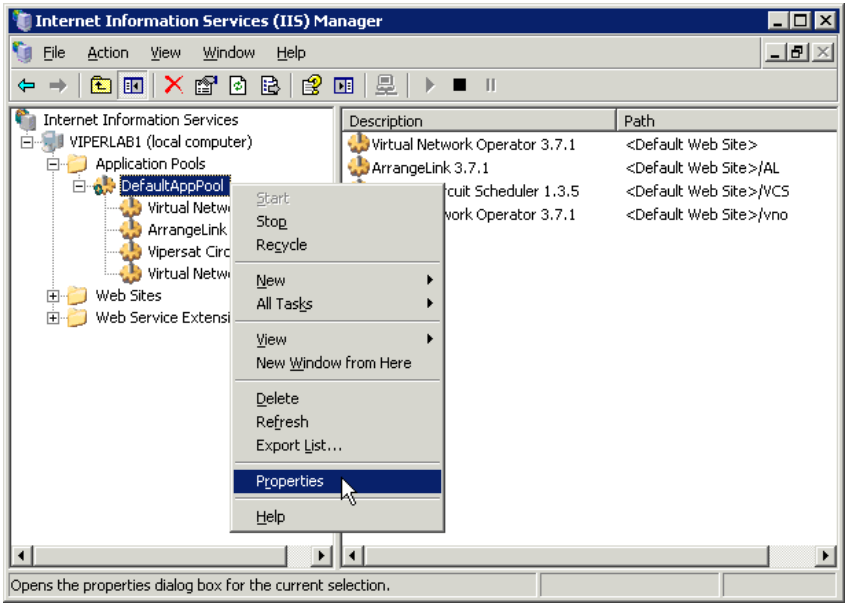


Figure 2-56 DefaultAppPool, IIS Manager

3. Open the Identity tab in the *Properties* dialog, select the **Predefined Network Service**, then click **OK**, as shown in figure 2-57.

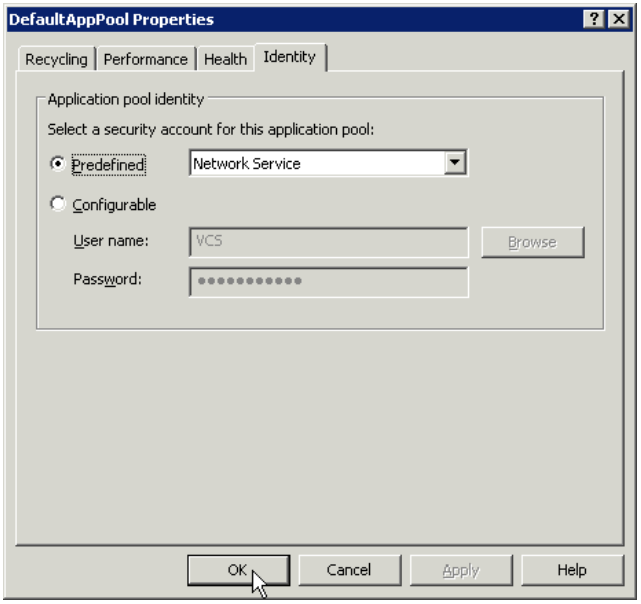


Figure 2-57 DefaultAppPool Identity

Remove Previous Version

If a previous version of VMS SOAP Services is installed on the server, that software should be removed prior to installing the new version.

1. From the Add or Remove Programs control panel, select the **VMS SOAP Server** program and click on the Remove button, as shown in figure 2-58.

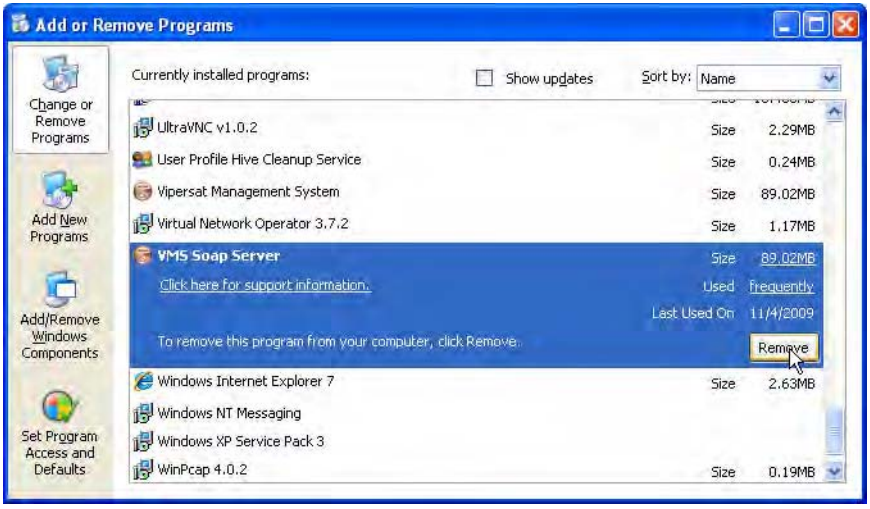


Figure 2-58 Remove VMS SOAP Server Program

2. A confirmation dialog window will appear. Click on the **Continue** button to remove the program.

Installation Procedure

Note that the installation and configuration must be done using an Administrator login.

Caution: This software must be installed on a platform that is running Windows Server 2003. Installing the SOAP Services on a computer that is not running Windows Server 2003 will void VMS product support.

VMS Installation

The VMS Web Services SOAP Server host machine must have a *VMS Full Install* performed; this is necessary in order to provide the required support files for proper operation of the SOAP interface. However, this copy of VMS is not used to manage the Vipersat network.

NOTE

Note: A VMS Crypto-Key is not required, and these files are not called upon to execute the client application.

Follow the installation procedure in the section “VMS Server Installation” on page 2-14 to perform the Full Install, then return here to continue with this procedure.

SOAP Services Installation

1. Locate the **VMS 3.x SOAP Setup.exe** file on the VMS distribution CD and double-click on the file to start the installer.

   This will open the *VMS SOAP Server Setup Wizard* (figure 2-59) that will install the SOAP services.

Figure 2-59 VMS SOAP Server Setup Wizard

2. Click the **Next** button to progress through the Setup process.

3. Specify the **Start Menu Folder** for locating the program shortcuts. This folder defaults to the folder that was specified for the VMS installation.

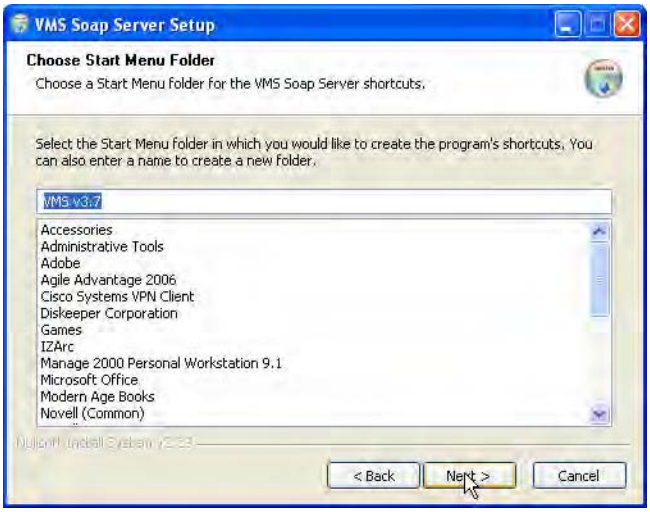


Figure 2-60 Choose Start Menu Folder

4. As shown in figure 2-61, the Installer will present a dialog requesting the VMS SOAP Server Configuration parameters.

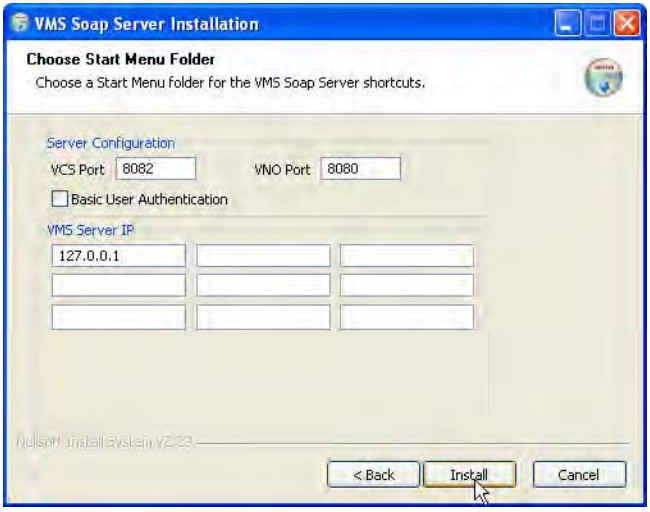


Figure 2-61 VMS SOAP Server Configuration

- **VCS Port**

  This parameter specifies the TCP port used by the SOAP Server for the VCS ArrangeLink application. The default port is decimal 8082. Any available port can be specified, provided that the client VCS applications send their request to this port.

- **VNO Port**

  This parameter specifies the TCP port used by the SOAP Server for the VNO application. The default port is decimal 8080. Any available port can be specified provided that the client VNO applications send their request to this port.

- **Basic User Authentication**

  This check box indicates whether the Basic User Authentication is enabled or not. If enabled, each client request contains a user name and password in the HTTP header. The SoapAdmin.exe utility is used to configure the user database and privilege levels. This utility is located in the VMS-installed directory Program Files\Vipersat\VMS\3.0\bin.

- **VMS Server IP**

  This parameter specifies the IP address(es) of the VMS server(s). In a standalone VMS configuration, enter the one VMS server IP address. In a redundant VMS configuration, up to nine addresses can be entered (e.g., for all VMS servers in the same redundancy group).

5. Enter the parameters described above, then click on the **Install** button.

The installation progress will be displayed, ending with the “Installation Complete” notification.

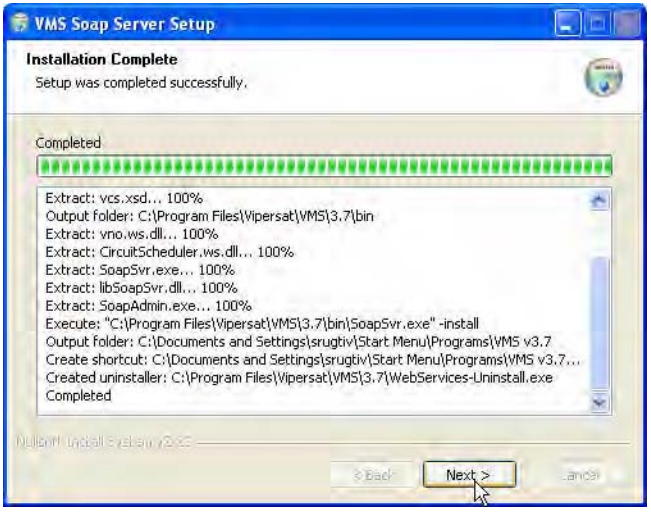


Figure 2-62 SOAP Server Installation Complete

6. Click on the **Next** button, then **Finish** to close the wizard.

7. Open the Services Control Manager and verify that the **VMS Web Services** appears in the list of services.

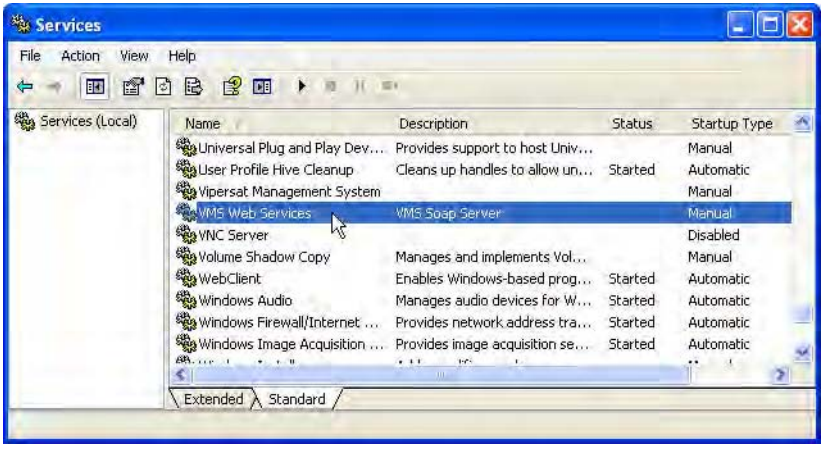


Figure 2-63 Services Control Manager, VMS Web Services

Web Applications Installation

For the installation procedure for VMS Web applications (e.g., ArrangeLink, VNO), refer to the specific Web application user guide.

Server Configuration

After successfully completing the installation of the SOAP Services, it is necessary to perform some configuration steps on the server to assure the proper operation of the VMS Web services and their communications with the VMS.

Set Up Log On Account

1. In the Services window, right-click on the VMS Web Services and select **Properties** from the drop-down menu.

2. In the Properties dialog, click on the **Log On** tab, as shown in figure 2-64.

Figure 2-64 Account Set Up, VMS Web Services

3. Enter an account user name and password that matches the user account that is running the VMS Server.

This account must be identical to (or be in the same user group as) that used for running the VMS Server in order for the Web Services to communicate with the VMS. If these user credentials do not match, an "*Access Denied*" error will result when attempting to connect.

4. Click on **OK** to save this account and close the Properties dialog.

5. Start the VMS Web Services.

A single beep will indicate that the service started. Verify that the status has changed to *Running*.

This completes the installation and configuration of the VMS Web Services.

This concludes the VMS Installation.

CHAPTER

3

VMS CONFIGURATION

General

The VMS configuration procedure assumes that the user is experienced with the VMS and/or has attended the System Operator training course, and gives summary instructions for configuring an installed VMS. If difficulties are experienced during configuration, contact Comtech EF Data's Vipersat CTAC for assistance.

This procedure must be executed in the order that is presented to ensure proper setup and configuration. After file installation and network hardware is in place and operational, the equipment should be communicating with the network management system. That is, the VMS has IP access to each unit either through a LAN or satellite connection.

Once the VMS is installed, started up, and the initial Vipersat Manager configuration is completed, the VMS immediately starts gathering and storing information from the units which make up the network.

Note: For a *Redundant VMS Server* configuration, perform the VMS configuration procedure on the **Active** server only. When completed, perform a server synchronization to synchronize the server databases.

Before proceeding with configuring the network using VMS, the *Administrator's Network Plan* and the following network information should be available, for reference.

- A list of all equipment used in the network, broken down by site.
- A schematic or other documentation of the network's topology.
- A Physical site map where each piece of equipment is located.

- IP addresses assigned to all network hardware.
- Documentation assigning IP address numbers and subnet masks to each site in the network, the multicast address(s) to be used, and the IP address of the VMS server's connection to the network.
- The functions each piece of equipment is to perform in the network (Hub, Remote, Expansion unit, etc.) and the equipment type (CDM-570/570L, CDD-564/564L, CDM-600L, SLM-5650A, ROSS, etc.).
- All frequencies and frequency allocations to be used by each site and each piece of equipment, and available pool frequencies.
- Types of traffic expected to be handled by each site and corresponding bandwidth allocations to accommodate the expected traffic volume and type.
- A list of the VMS licensing options that have been purchased. Details can be found on the Purchase Order, or a Vipersat representative can provide detailed information on licensing options and pricing for the VMS-managed network.
- A list of network modem equipment and the FAST features associated with each. This information can be obtained either via Telnet from the Main>Administration>Feature Configuration screen, or with Vload and the use of the Parameter Editor (Features tab).

The following sections describe configuring the VMS to the network topology, traffic type, and bandwidth requirements for the network. This information can then be compared to the physical network configuration displayed by the VMS, once it has completed its network analysis and displays the results, as shown in the network example, figure 3-1.

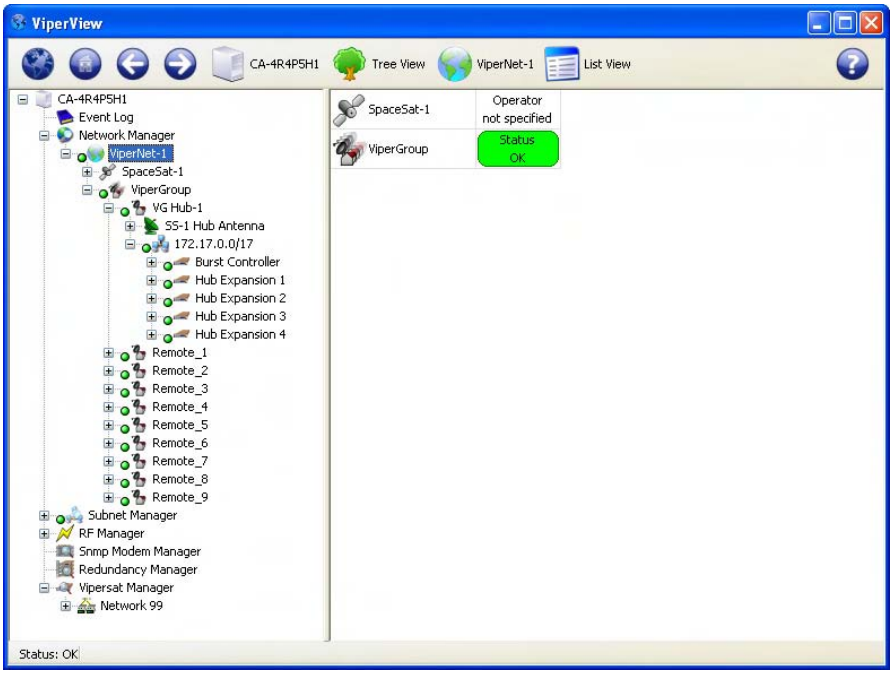


Figure 3-1 Network Configuration example

By comparing the planned network configuration with the actual network configuration, any missing nodes or potential trouble spots can be quickly identified. The tools described in this chapter can then be used to modify and optimize the network's configuration and operation.

NOTE

Note: An Out-of-Band network is displayed in the same manner as other elements in the network.

Configuration Alerts

The VMS performs a check of the configuration settings that are input by the user. If a setting is found to be in conflict, an alert message is generated to inform the user that an adjustment is necessary. When a conflicting parameter setting is entered into a dialog, an alert icon will appear next to the field in question. Clicking on the icon will display a pop-up info-tip that explains the conflict. The alert icon is also displayed in front of the menu item associated with that dialog.

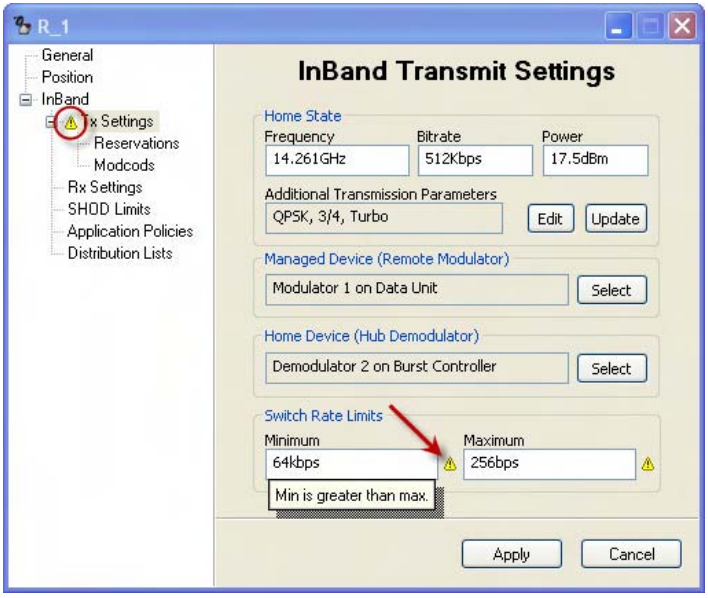


Figure 3-2 Alert, Parameter Conflict

Edit the setting to eliminate the conflict. Note that, once the setting is corrected, the alert icons will remain visible until another action is executed, such as selecting another menu item or exiting the dialog.

Hardware Configuration

Note: For VMS compatibility, see the product *Release Notes* for specific versions of each modem supported.

Once all of the needed information is obtained, configuration can begin. Before making the physical installation of hardware into a network, each modem/router must be pre-configured using either Telnet (CLI) or HTTP. Refer to the modem/router's documentation for details.

Comtech EF Data ships all modem/routers with FAST Codes pre-configured. The modem/routers are always configured at the factory as type Remote, with the Default Gateway pointed toward the Satellite, and with STDMA disabled.

At this point, VMS cannot discover the node. The operator can either use Telnet (CLI) or HTTP to set up these parameters as shown in the example CDM-570/570L CLI interface shown in figure 3-3, or flash a configuration file using VLoad.

As a minimum, the following items in the modem/router will have to be configured before it will be able to communicate with the VMS following installation in the network:

- Network ID
- Receive Multicast Address
- Managing IP address is set through reception of VMS announcement multicast message that is sent continuously on timed intervals.

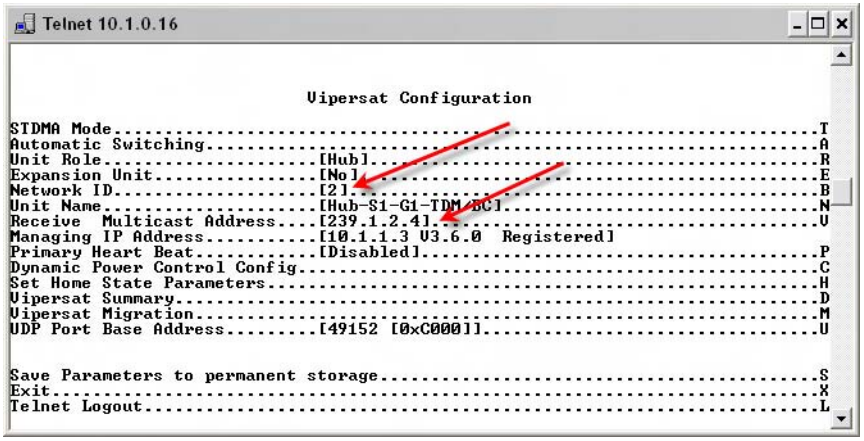


Figure 3-3 CDM-570/570L Telnet Vipersat Configuration

Once the modem/routers have the minumum required configuration and an installer successfully points the antenna at the satellite and establishes a receive link, the operator at the Hub site can push frequencies, bit rates, and FEC code rates to the units at remote sites using the VMS. The frequencies can be anywhere in the customer's frequency pool, allowing a thin-route SCPC connection to be established with the satellite network's modems.

For example, once communication is established, the Hub operator can set up the unit for STDMA using the instructions found in each modem manual. After a reset, the unit will come back online operating in STDMA mode with the desired configuration.

Once communication is established between VMS and all network devices, the network is ready to be configured.

VMS Quick Configuration Guide

This section is provided as a high-level guide for configuration of the VMS, and is intended for use by administrators and operators who are experienced with the configuration process. This material serves as a reference for what to do, and in what order.

For less experienced users, and for the comprehensive how-to configuration procedures, proceed to the section “VMS Initial Startup Procedure” on page 3-11.

A. Start VMS & ViperView

1. **Start** the Vipersat Management System service on the VMS Server.
2. **Connect** to the VMS Server from the VMS Client workstation to open ViperView.

B. Configure Vipersat Manager

1. Set the **Management** and **Local VMS** addresses.
2. Set the communications **Timeouts**.
3. **Activate** the Server processes.
4. Configure the server for **Auto Activate**.
5. Observe the **registration** of network units with the VMS and the population of the Vipersat Manager and the Subnet Manager.

   Verify with the *Administrator’s Network Plan.*
6. For missing units, use the **Scan Network** command to assist VMS registration.

C. Configure RF Manager

1. Create the network **Satellite**(s).
2. Create the satellite **Transponder**(s).
3. Create the bandwidth **Pools** for the satellite(s).
4. For Hub(s) and initial Remote(s):

- Create the network **Antennas**
- Create the antenna **Up Converters** and **Down Converters**
- **Bind** the Mods and Demods to the Converters for these sites

D. Configure Network Manager

1. Create the **Network**(s).
2. Copy the **Satellite**(s) from RF Manager to the network(s).
3. *Optional*: Create the **Groups** for the network(s).
4. Create the **Sites** for the network or group—Hub(s) and initial Remote(s).
5. Copy the site **Antennas** into the sites.
6. Copy the site **Subnets** into the sites.

Set Carrier Flags

1. Set the **STDMA** flag on the network Burst Controller.
2. Set the flags for the Allocatable Mods and Demods:
   - P2P Switching Modulators at the Hub
   - SCPC Switching Demodulators at the Hub
   - Mesh Demodulators at the Remotes

Mask Rx Unlock Alarms

Select **Mask Unlock Alarm** for all network units that function as either a Burst Controller or an Expansion unit.

Enable Auto Home State

Set the **Auto Home State Timeout** for Remote data units.

Configure InBand Management

1. Set the **InBand** flag for each Remote site.
2. Configure the **InBand Settings** and **Home State**.
   - InBand Transmit Settings
   - InBand Receive Settings
3. Set the **InBand Bandwidth Reservations**.

4. Set the **InBand Policies** for the Network level, Group level, and Site level.
   - InBand Policy Flags
   - InBand Application Policies
   - Define InBand Distribution Lists

Perform Switching Function Verification

Create Additional Remote Sites with Remote Site Wizard

Configure Advanced Switching

E. Configure Redundancy

Configure N:M Hub Device Redundancy

Configure VMS Redundancy

F. Configure SOTM

1. Set the **Dynamic** parameter for the mobile remote(s).
2. Select the **ROSS** unit for the remote(s).
3. Create the **Routes** for Hub TDM outbound units.
4. Configure the **QOS Rules** for Hub TDM.

G. Configure Encryption

Management Security Option

This feature option is NOT included with the standard VMS package, and is only available upon request from an authorized agent.

1. Enable **Management** and/or **Switching** encryption for the VMS server.
2. Enter the **Encryption Key**.

Modem TRANSEC Setting (SLM-5650A only)

Specify the number of **FIPS Blocks per Frame** for the modem.

VMS Initial Startup Procedure

Configure Server Connection

Start the Vipersat Management System service on the VMS Server and open the Connection Manager on the VMS Client.

1. On the VMS Server, select **Vipersat Management System** from Windows Services and **Start** the service, if it is not already running.

   Starting the service is described in Chapter 2, *VMS Installation*, in the section "Verify Server Installation" on page 2-25.

   Note: It is recommended that this service be configured for **Automatic** Startup.

2. On the VMS Client workstation, open the **Connection Manager**, using either the Desktop shortcut, or from the path Start > Programs > VMS > Connection Manager.

   Although the Connection Manager can be opened on the VMS Server, it is **NOT RECOMMENDED** to run ViperView on the same machine as the VOS.

3. The Connection Manager will prompt for the Server with which to connect (figure 3-4). Enter the **IP address** of the active VMS Server and click the **OK** button.

Figure 3-4 Connect to Server dialog

The **ViperView** window will open, as shown in figure 3-5.

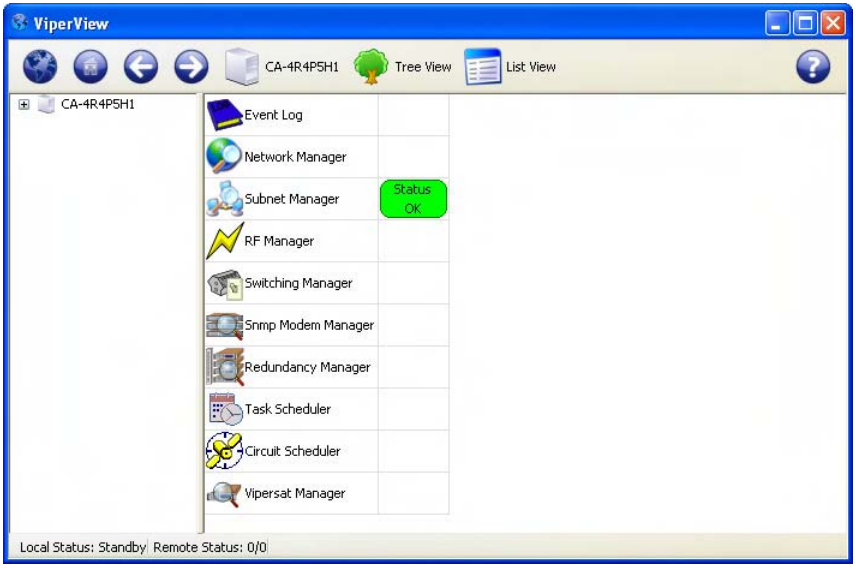


Figure 3-5 Initial ViperView Window

Vipersat Manager Configuration

In this section, Vipersat Manager is used to configure the necessary addresses and timeout parameters. Once the server is activated, this will allow the VMS to establish communications with, and register, the nodes in the network.

1. Expand the VMS server tree view in the left ViperView window panel. Right-click on **Vipersat Manager** (located at the bottom of the tree list) and select **Properties** from the drop-down menu, figure 3-6. The Vipersat Manager window will open.

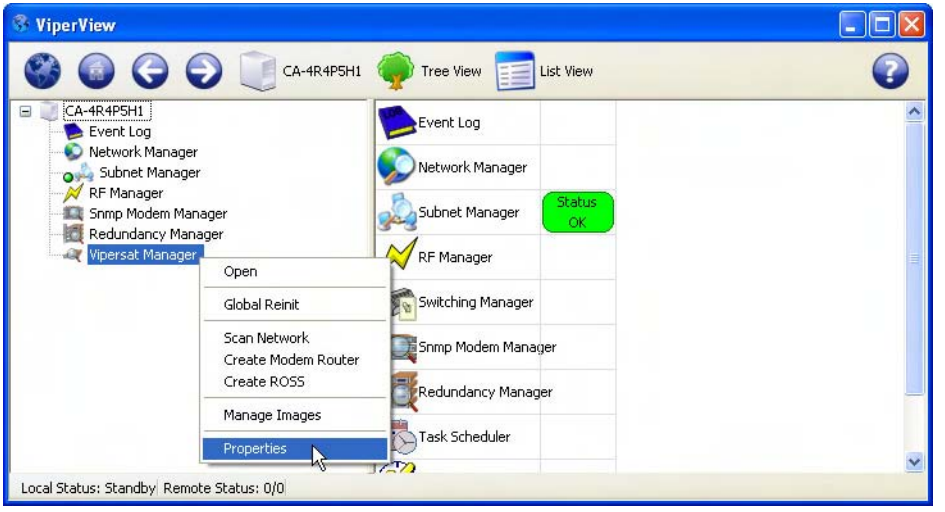


Figure 3-6 Vipersat Manager Properties menu command

2. In the **General** dialog shown in figure 3-7, make sure that the **Management Multicast Address** of the VMS matches the Receive Multicast Address for each modem in the network that is controlled by this VMS. This address is used to propagate managing multi-command messages from the VMS to all receiving IP network modems.

3. The **Local VMS Address** will default to 0.0.0.0 on new installations and must be changed to reflect the IP address of the NIC that connects the VMS server to the Vipersat Hub LAN. This address configuration is necessary because of multiple LAN ports on the server.

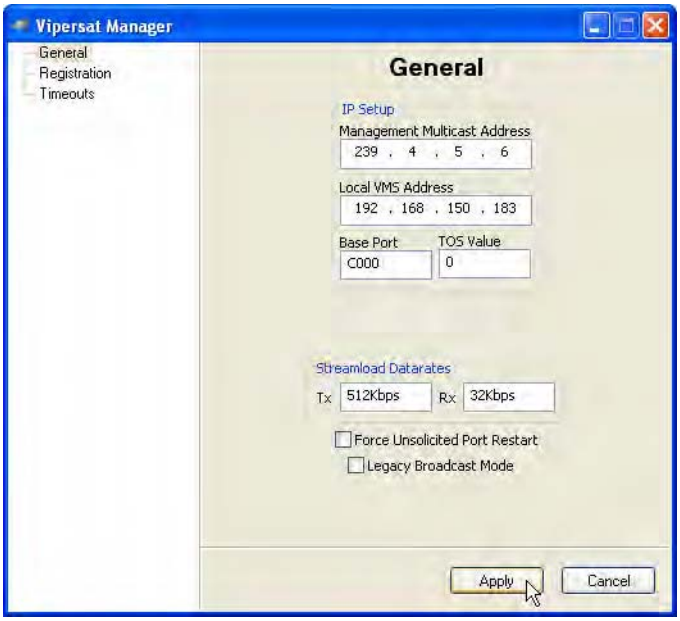


Figure 3-7 Vipersat Manager, General dialog

4. The **Base Port** sets the starting IP port addressing for all VMS messages. Changing this address base will affect the entire network requiring configuration changes to all modems. Leave this setting at default **C000** to avoid unnecessary configuration changes. Altering this setting is ONLY necessary if network port addressing is in contention.

5. The **TOS** (Type Of Service) **Value** provides prioritization of VMS messages in cases where the forwarding router is congested or overloaded. The value typically is set to Class Selector 6 or “192” for priority queuing to ensure management/signaling messages are granted the highest passage level.

6. The **Streamload Data Rate** values determine the amount of bandwidth required to GET and PUT modem configuration files. Set the rates not to exceed the network transmission bandwidths, forward and return channel rates. These values are typically set low as the file transferred is small and requires little overhead. Default settings are usually acceptable.

7. The **Force Unsolicited Port Restart** check box provides the option to reset the UDP port used by the VMS server for receiving status update messages sent by the network modems. This action is recommended whenever the Local VMS Address or base port setting is changed, especially for servers that have multiple NICs.

Activate the check box, then click on the **Apply** button to execute the restart.

8. The **Legacy Broadcast Mode** check box need only be activated for networks that consist of modems using the following firmware versions:

- CDM-570/570L—v1.5.3 and earlier
- CDD-564/564L—v1.5.3 and earlier
- SLM-5650A—v1.3.1 and earlier

This feature provides support for the previous method of sending the active management IP address message using a multi-command packet that requires acknowledgement. This multicast message updates the **Managing IP Address** field in all listening modems. The message interval is defaulted to send an update every 15 seconds. *See Timeouts dialog for timer interval setting.*

If all modems are running more recent firmware, then only the unacknowledged message type is used and this box can be left unchecked.

9. Select the **Timeouts** dialog shown in figure 3-8. The default timer settings are adjustable to accomodate communications that require additional time because of network congestion.

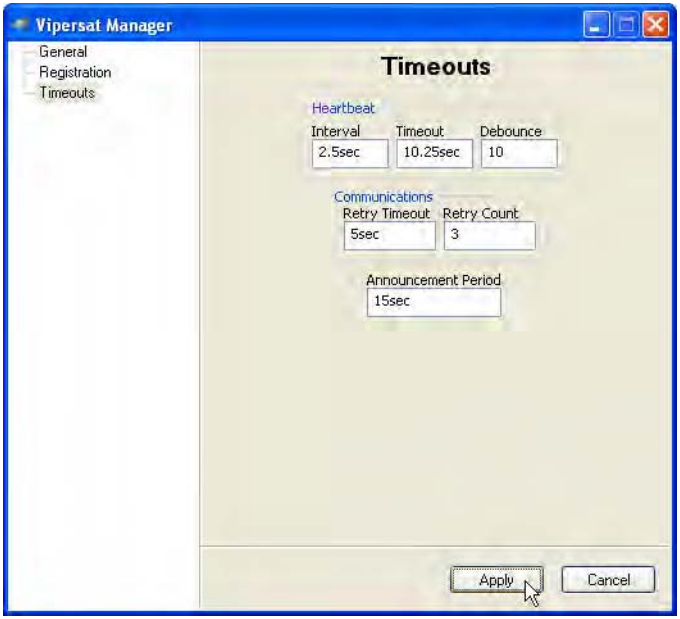


Figure 3-8 Vipersat Manager, Timeouts dialog

10. The **Heartbeat** timer settings include the Interval, Timeout and Debounce values for Hub device redundancy messaging.
    - The **Interval** parameter updates the modem to send it's heartbeat message to the VMS at the set rate.
    - The **Timeout** is how long the VMS will wait before determining communications failure and commanding a device redundancy switchover.
    - The **Debounce** is a counter setting for the number of consecutive alarmed messages the VMS will receive from a particular Hub unit before a redundancy switch is triggered. This parameter setting is useful for reducing or eliminating unnecessary redundancy triggers due to spurious alarms.

11. The **Communications** timer values set timeouts for command messages. The **Retry Timeout** is the wait between messages which works in conjunction with **Retry Count**. A retry count of 3 and a timeout of 5 seconds would set the message failure at a total timeout of 15 seconds with 3 attempts to command the modem.

    If communication latencies are greater than default settings (command communication failures), increase the **Retry Timeout** value.

12. The **Announcement Period** is the interval at which the VMS will multicast its management IP address to all listening modems within the network. This ensures, for example, that remotes that are not online during a redundancy switch will pick up the new managing address when they come back online.

    The default value (15 sec) enables the VMS to send the update message on a 15 second interval to establish the current managing address in all modems set to receive the message.

13. Click the **Apply** button to save these settings for the Vipersat Manager Properties, then **Close** the window.

Activate Server Processes

In ViperView, click on the Server icon on the top menu bar and select **Activate** from the drop-down menu (figure 3-9) to manually initialize the VMS server processes.

Figure 3-9 Server Processes, Manual Activation

The windows task bar will pop-up a text bubble indicating the activation.

Figure 3-10 Activated Server Notification

Open Event Log

At this point, it is helpful to open the Event Log window for observing VMS events as they occur during the configuration process. Right-click on the **Event Log** icon and select **Open**.

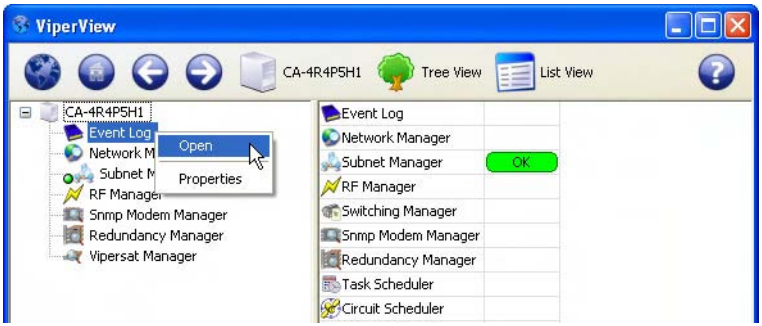


Figure 3-11 Event Log, Open

Resize and position the Event View window as desired for optimal viewing on the monitor.

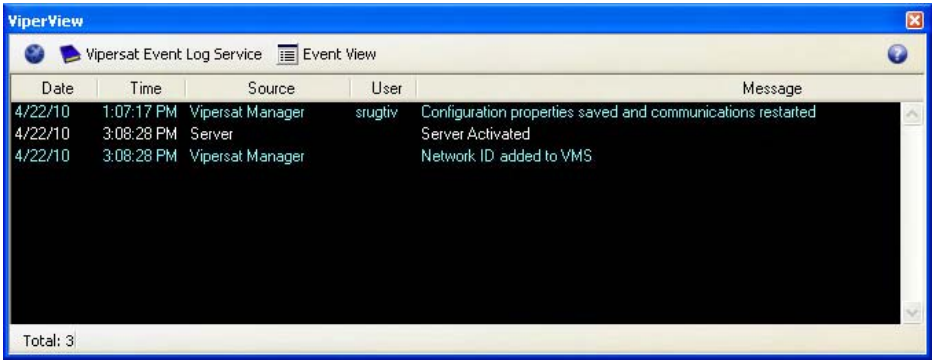


Figure 3-12 Event Log Window

More detailed information regarding the Event Log is provided in Chapter 5, “VMS Services”.

Configure Event Relay Server

This procedure configures the Event Relay function for network systems that will utilize external client software to receive VMS event information via TCP connection.

1. Open the Event Log **Properties** dialog.

Figure 3-13 Event Log Properties dialog

2. Enable (default) this function for use.

3. Set the **Port** number to be used (defaults to C008).

4. For changes, click the **Apply** button, then Close the window.

Configure Auto Activate

1. Click on the Server icon on the top menu bar and select **Properties** from the drop-down menu.

2. Select the **Redundancy** dialog, then check the box for **Auto Activate** as shown in figure 3-14. This will automatically activate the server processes whenever the Vipersat Management System service is started.

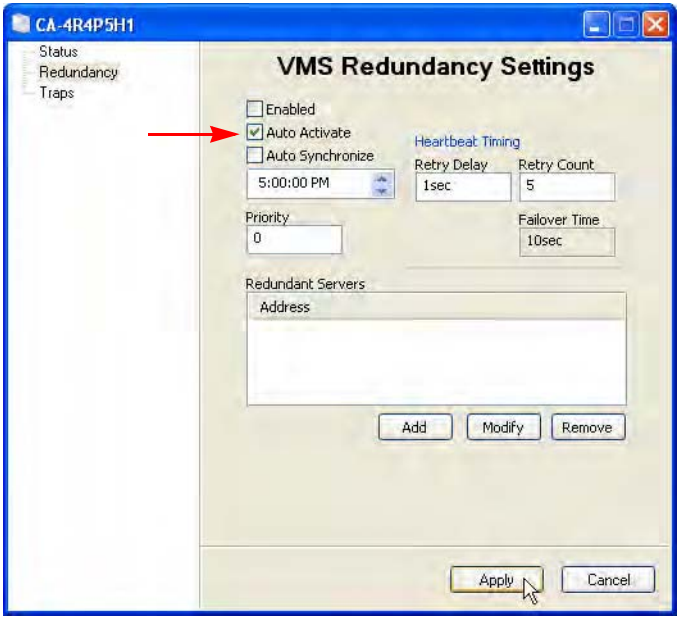


Figure 3-14 Server Properties, Auto Activate

The other parameters in this dialog pertain only to redundant server configurations which will be addressed later (see “VMS Redundancy” on page 3-105).

3. Click the **Apply** button to save this setting for the Server Properties, then **Close** the window.

Auto-Discovery Process

Once Vipersat Manager is configured and the server is activated, communications between the VMS and live network units at Hub and Remote sites is estab-

lished, and the auto-discovery process begins. As Hub and Remote units are identified, their appearance can be observed in ViperView under the Subnet Manager and the Vipersat Manager by expanding the tree view, as shown in figure 3-15.

Expand the tree view to display the list. If necessary, widen the left ViperView window panel by repositioning the vertical divider to the right.

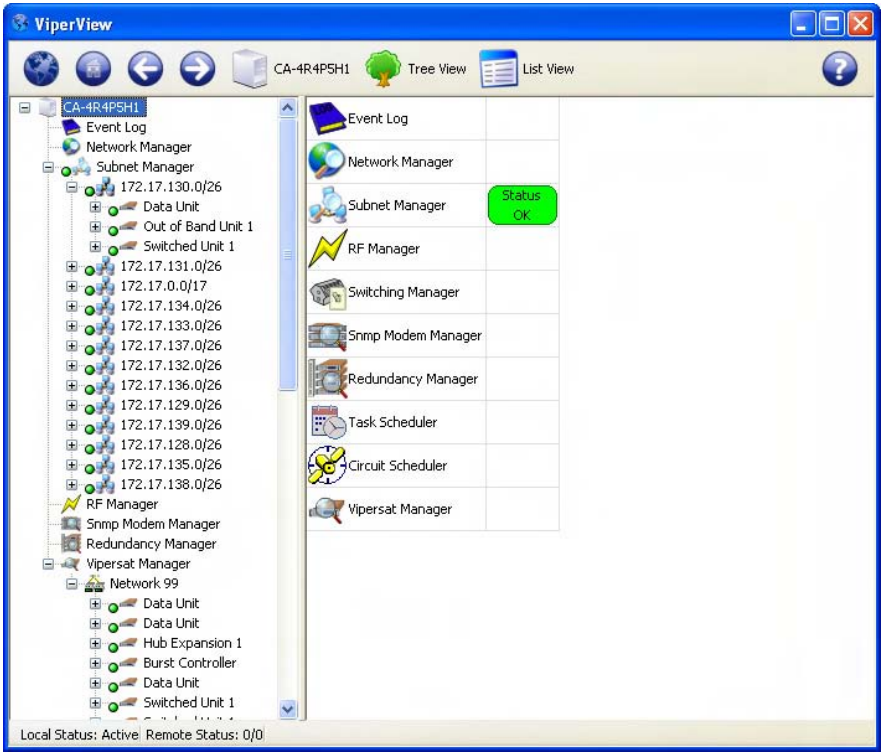


Figure 3-15 Registration of Network Units

Note that, as units are registered with the VMS, the Network ID parameter from each unit is automatically detected and used to create a corresponding network icon under the Vipersat Manager in which the units are registered and grouped. This action is recorded in the Event Log (figure 3-12).

Also observe the appearance of new events in the Event Log window that indicate unit registration with the VMS (figure 3-16).

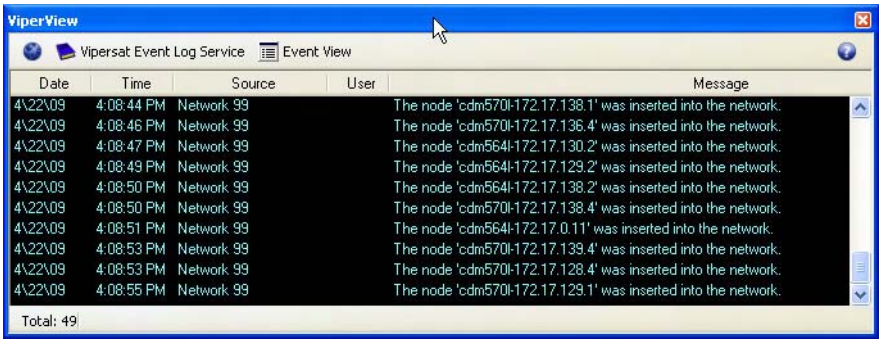


Figure 3-16 Event Log, Node Inserted into Network

Subnet Manager configuration is done automatically by the VMS. The operator should verify that each subnet has all of the expected elements populated in that subnet.

Once all of the management addresses are correct and communicating, the Subnet Manager will start to populate with the modem IP subnets. If some or all units are not populating, the managing VMS address (configured in each modem during the automatic registration) may not be correct.

After the subnet list population is complete, the VMS stores all listed subnets, and any reference to nodes within each subnet, in the VMS database.

Note: All Vipersat modems that have IP communications with the VMS will have their subnet address added to the VMS database.

Match up the units displayed in ViperView with the *Administrator's Network Plan* to verify that all devices have registered with the VMS. Allow sufficient time for registrations to occur; this will vary depending on the size of the network.

Tip: During the initial discovery/registration process, units and their subnets are displayed in the order that they are registered. Restarting the VMS Service will allow the *Subnet Manager* to display its elements sorted by IP address. The *Vipersat Manager* will display the elements belonging to each Network sorted by modem/unit type, then by IP address within each type.

If any devices or subnets are missing from view, perform the following command to assist the VMS in registering the unit(s).

- Scan Network — Right-click on the Vipersat Manager and select **Scan Network**.

For all units that remain missing from ViperView, do the following:

- Secure a connection to the unit through either Telnet or the Web interface to verify whether the unit is registered with the managing VMS or not.

Be certain that all of the known units in the network have been discovered before proceeding.

Backup Database

It is suggested that, once it has been verified that all known devices are present in the VMS database, a VMS backup be performed. Then, in the event that difficulties are encountered during the configuration process, the database can be restored to this point.

For the DB restoration procedure, see "Database Backup and Restore" on page 5-22.

1. Click on the VMS Server icon in the top tool bar and select **Backup** from the drop-down menu, figure 3-17.

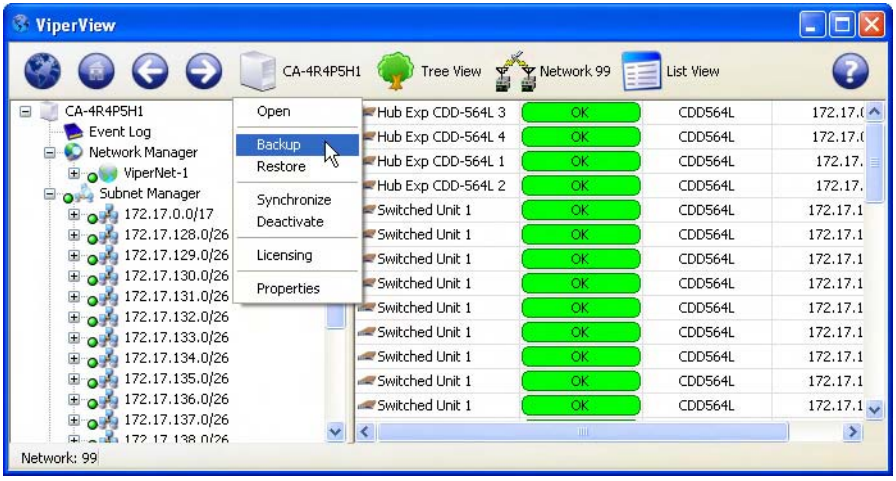


Figure 3-17 Backup VMS Database command

The Windows *Save As* dialog will appear

2. Name the backup file and save to the desired directory.

RF Manager Configuration

RF Manager configuration consists of creating the network satellite(s) with associated transponders and bandwidth pools, and the site antennas with associated Up converters and Down converters that the Vipersat network nodes will be using.

Create Satellite(s)

The first step is to create the satellite(s) for the network with the appropriate RF characteristics. Transponders are then defined, followed by the creation of bandwidth pools to accommodate SCPC carriers.

1. Right-click on the RF Manager and select **Create Satellite** from the drop-down menu (figure 3-18).

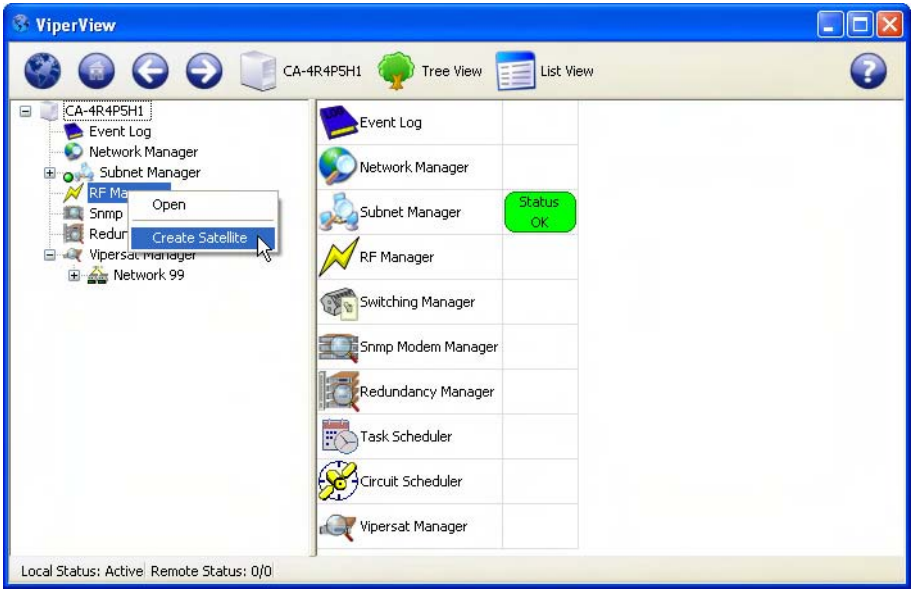


Figure 3-18 Create Satellite menu command

2. Enter the satellite **Name** and the **Center** and **Translation Frequency** settings in the Create Satellite dialog (figure 3-19).

   Check with the service provider if these settings are unknown.

   The default values (14.25 GHz and 2.3 GHz) are provided for Ku-Band applications.

3. An **Orbital Position** can be associated with this satellite by entering the longitudinal coordinate in degrees (decimal format), designated for **E**(ast) or **W**(est).

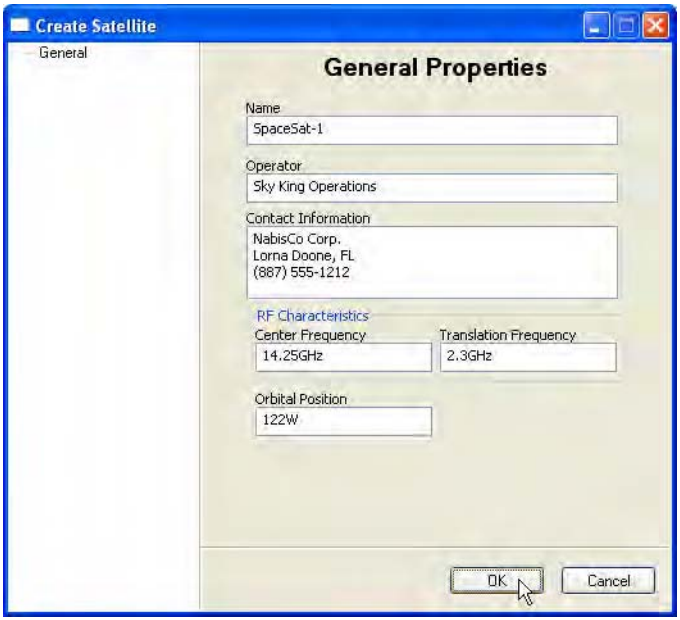


Figure 3-19 Create Satellite dialog

4. Optional information can be entered for the satellite **Operator** and **Contact Information**.

5. Click on **OK**. The newly created satellite will appear under the RF Manager in the ViperView window (see figure 3-20).

6. Repeat the previous steps to create additional satellites, as required.

Create Transponder(s)

The next step is to create the transponder(s) in the newly created satellite. Each transponder is defined with specified Frequency Range parameters.

1. Right-click on the Satellite icon that this transponder will be associated with and select **Create Transponder** from the drop-down menu (figure 3-20).

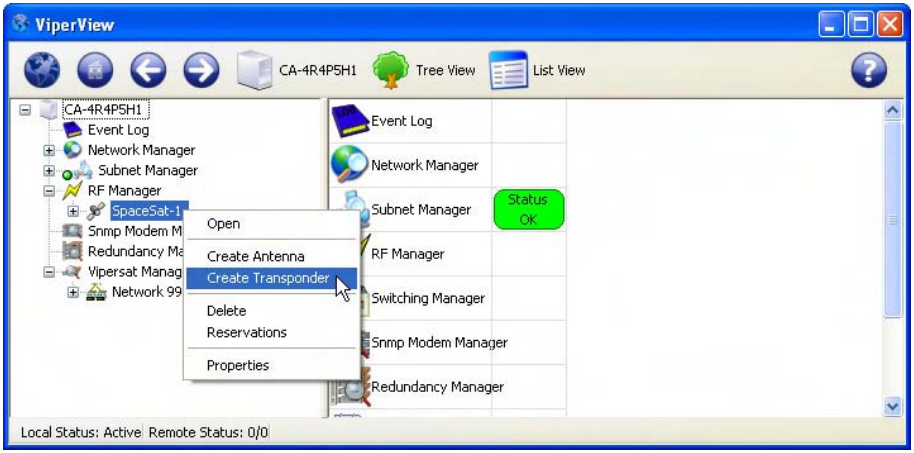


Figure 3-20 Create Transponder menu command

2. Enter the transponder **Name**, **Center Frequency**, and **Bandwidth Span** in the Create Transponder dialog (figure 3-21).

Frequency range settings can be specified using upper and lower limits by clicking the **View as Base/Top** checkbox.

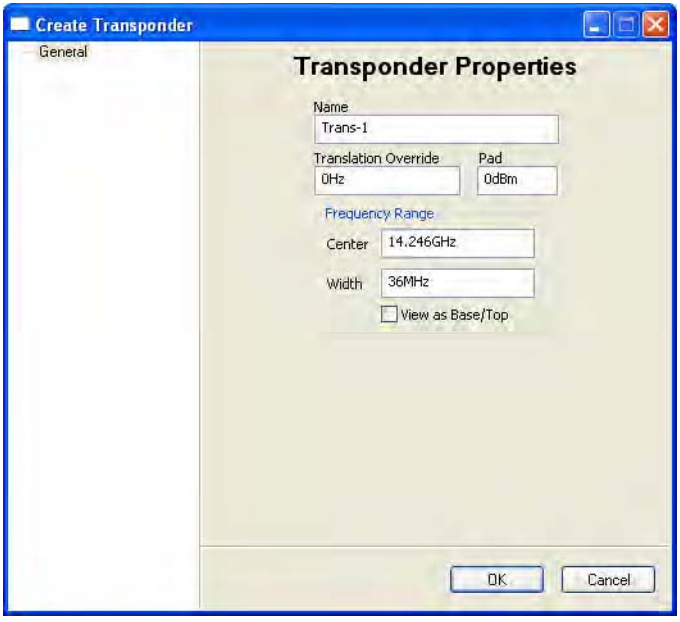


Figure 3-21 Create Transponder dialog

Leave the Pad and Translation Override entries at the default values, if unknown.

The Pad value sets the gain variation between transponders for automatic switching power calculations.

The Translation Override parameter is used for specific applications and represents a frequency offset for cross-banded transponders (refer to Appendix A, "VMS Cross Banding" for more information).

3. Click on **OK**.

4. Repeat the previous steps to create multiple transponders, as required.

Open Spectrum View

At this point, it is helpful to open the Satellite Spectrum window for observing usage of the transponder space segments during the configuration process. Right-click on the Satellite icon in the VMS server tree view list and select **Open**.

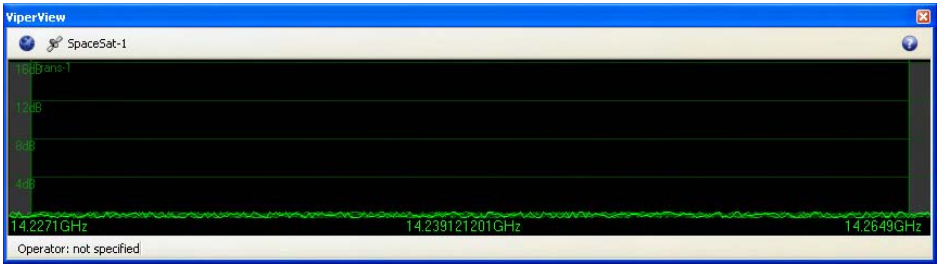


Figure 3-22 Satellite Transponder Spectrum View

Resize and position this window as desired for optimal viewing on the monitor. Use the following mouse techniques for adjusting the view:

- Focus the transponder width for optimal viewing by double-clicking in the window.
- Enlarge the view by rolling the scroll wheel downward.
  This displays a *narrower* frequency range.
- Diminish the view by rolling the scroll wheel upward.
  This displays a *wider* frequency range.
- Pan horizontally by click-holding the scroll wheel and mousing left or right.

The visible frequecy range is indicated by the frequency values displayed in the lower left and lower right corners of the window. The dark area represents the frequency range of the transponder that was created in the previous section, and is labeled with the transponder name (*Trans-1*, in figure 3-22) in the upper left corner. The gray areas are undefined satellite spectrum. The horizontal wavy green line in the lower portion of the window represents the noise floor. Note that the mouse pointer horizontal position within the window is displayed as a frequency value at the bottom center of the window.

More information regarding the Spectrum View is provided in Chapter 5, “VMS Services”.

Create Bandwidth Pools

The next step is to create the bandwidth pools that define the available spectrum for allocating to SCPC carriers.

1. Right-click on the Satellite icon and select **Properties** from the drop-down menu.

2. In the Satellite Properties window, select the **Pools** dialog, then click the **Create** button and specify the Pool Range settings, as shown in figure 3-23.

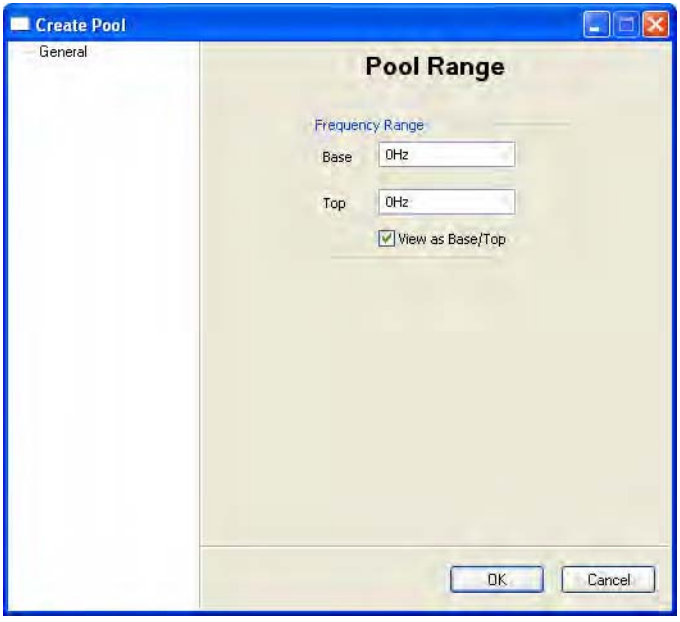


Figure 3-23 Create Pool dialog

3. Click **OK** to enter the new pool in the Allocatable Bandwidth table.

Figure 3-24 Satellite Pools dialog

4. Repeat the above steps to create additional pools, as required.

5. Enter the desired **Guardband** for the carriers that will be allocated bandwidth slots in the defined Pools. This value is entered as a percentage of the carrier bandwidth, and is divided equally for the left and right sides of the carrier.

For example, using the default Guardband setting of 30, a carrier using 3.3 MHz will be assigned to a 4.29 MHz slot, providing a guardband of 495 kHz on each side of the carrier.

6. Click **Apply** to save the settings, then Close the window.

The newly created pool(s) are displayed in the Spectrum View as shaded green areas, figure 3-25.

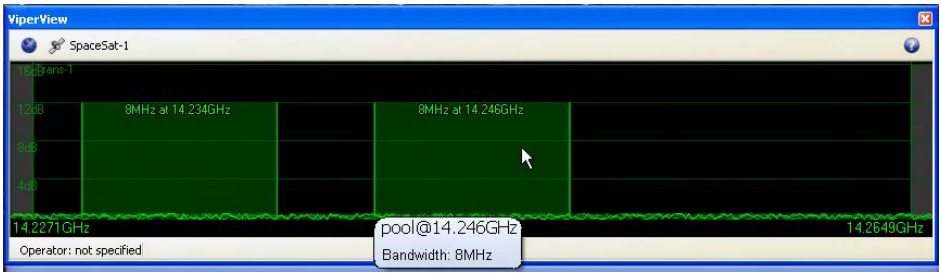


Figure 3-25 Bandwidth Pools, Spectrum View

Create Site Level RF Chain

Here, the Hub antenna(s) with associated converters and the initial Remote antenna(s) with associated converters will be created. The binding of the unit modulators and demodulators to their designated converters will then be performed. Later in the configuration process (Network Manager Configuration), the Vipersat *Remote Site Wizard* feature will be used to create the RF chain for the other Remotes.

Create Antennas

The following steps cover creation of the network antennas. Each antenna is a site container for upconversion/downconversion and modem devices. First create the Hub antenna(s), followed by the initial Remote antenna(s), as described below.

1. Right-click on the Satellite icon and select **Create Antenna** from the drop-down menu.

2. In the General dialog of the Create Antenna window (figure 3-26), enter the **Name** to be used for identifying this antenna. Entering the **Operator** and **Contact Information** is optional.

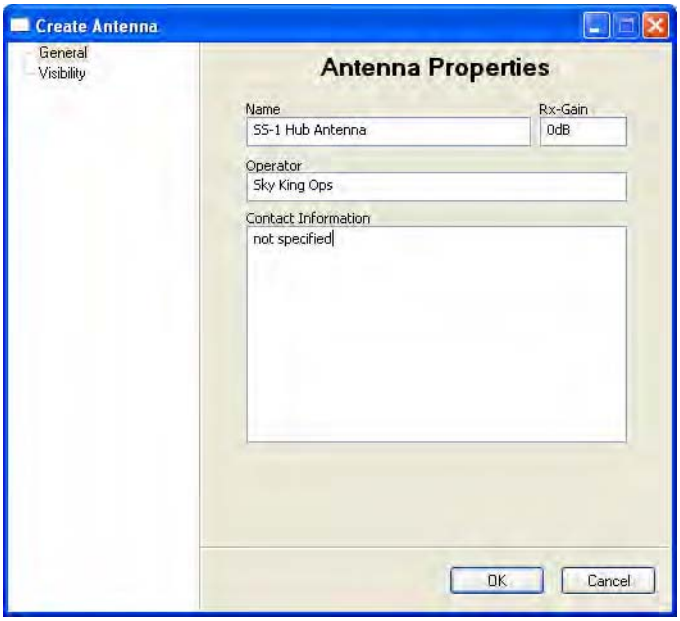


Figure 3-26 Create Antenna dialog

3. Set the Antenna **Receive-Gain** for the Mesh Compensation Factor.

Refer to link budgets and antenna manufacture specifications for gain settings. If meshing is not required, leave Rx-Gain at the default setting of 0 dB.

This feature applies a power delta between any meshed remote sites. The hub is used as the reference value when calculating a power delta value between remotes with smaller antennas. This is accomplished through comparing its receive gain to the gain differences between remotes.

During a mesh switch setup, the VMS compares the delta values and modifies the power adjustments at each remote site to compensate for differences in receive gain. If DPC is enabled, the system will then further fine tune power to the targeted configuration values.

If multiple remotes are involved in a SHOD connection, the VMS uses the lowest remote gain value for compensation control.

4. Select the Visibility dialog to configure the **Antenna Visibility** range, as shown in figure 3-27.

Caution: Unless specific limitations are required for the antenna range, the recommended (default) settings are 500 GHz center frequency and 1 THz bandwidth (or, the equivalent, 0 Hz Base and 1 THz Top). Refer to Appendix B, "Antenna Visibility", for more information on this feature.

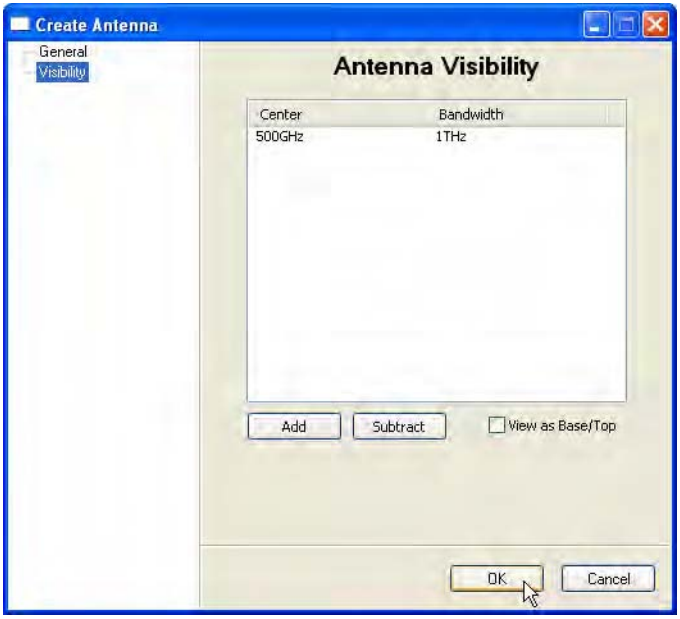


Figure 3-27 Antenna Visibility, Default Settings

5. Click on the **OK** button to complete the antenna creation.

   The new antenna will appear under the satellite in the ViperView window.

6. Repeat the previous steps to create additional antennas.

Create Antenna Devices

The following steps cover the creation of the antenna Up converters and Down converters.

1. Right-click on an Antenna icon and select **Create Up Converter** (figure 3-28).

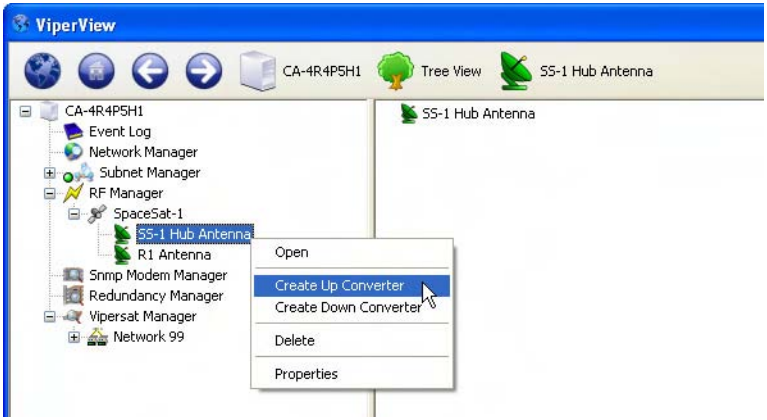


Figure 3-28 Create Up Converter menu command

2. The dialog box shown below (figure 3-29) will open. Specify a **Name** for this device.

It is important to ensure that the Up Converter **Frequency** setting is correct, as this is a very common source of error which breaks the switching engine.

Also, check the **Bandwidth** and **Power Limit** settings. If the RF hardware does not exactly match the satellite parameters, the Bandwidth setting may have to be changed.

Contact the Vipersat Network Product Group CTAC for further information.

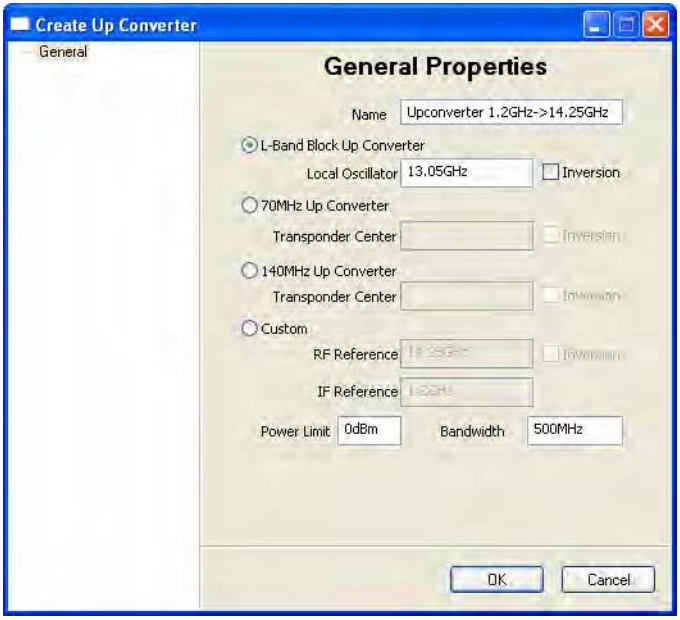


Figure 3-29 Create Up Converter dialog

3. Click on **OK** to enter this device as the Up converter for this antenna.

4. Right-click on the Antenna icon again and select **Create Down Converter**.

5. The dialog box shown below (figure 3-30) will open. Specify a **Name** for this device.

Ensure that the Frequency setting here also is correct.

6. Click on **OK** to enter this device as the Down converter for this antenna.

Figure 3-30 Create Down Converter dialog

7. Notice that the newly created Up and Down Converters appear in the Antenna View (figure 3-31).

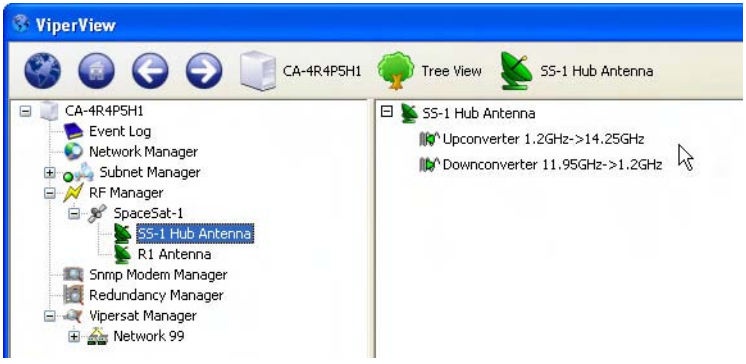


Figure 3-31 Converter Icons in Antenna View

8. Repeat the create converters process for all antennas.

Bind Modulators and Demodulators to Converters

The following procedure associates the Modulator for each unit at a site with the Up converter for that site's antenna, and associates the Demodulator(s) with the Down converter. This portion of the configuration is performed using the RF Manager in conjunction with either the Subnet Manager or the Vipersat Manager.

The method illustrated below uses the RF Manager with the Subnet Manager.

1. From the RF Manager tree view list in the left window panel, select the first site antenna for configuration (the Hub Antenna is used in this example).

   The antenna and its converters are displayed in the right window panel (figure 3-31).

2. Expand the Subnet Manager tree down to the Modulator and Demodulator level for the first unit that will utilize this Antenna (here, the Hub Burst Controller).

3. Click-hold on the Modulator device icon in the left panel, drag it to the right panel and drop it onto the Up Converter (figure 3-32).

   The device appears under the Converter as shown in figure 3-33.

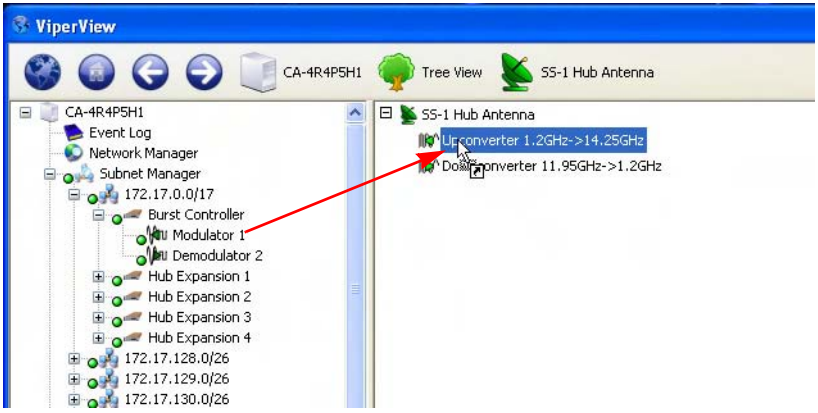


Figure 3-32 Binding Modulator to Up Converter

4. Click-hold on the Demodulator device icon, then drag-and-drop it onto the Down Converter.

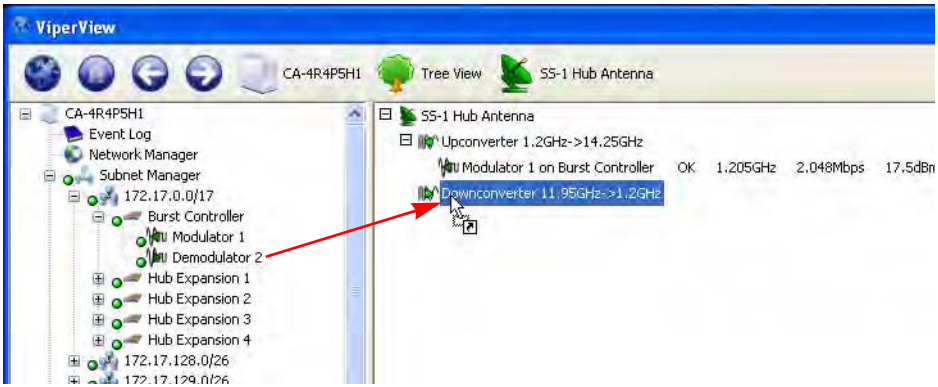


Figure 3-33 Binding Demodulator to Down Converter

As soon as the Hub BC binding is complete, the STDMA and the TDM carriers will appear in the Spectrum view. Note that the TDM carrier is displayed in red due to the fact that a power value has not yet been reported from a receiving Remote. The STDMA carrier appearance will vary between green and red, as the accuracy of the Eb/No values received by the BC may fluctuate due to the rapid locking/unlocking behavior.

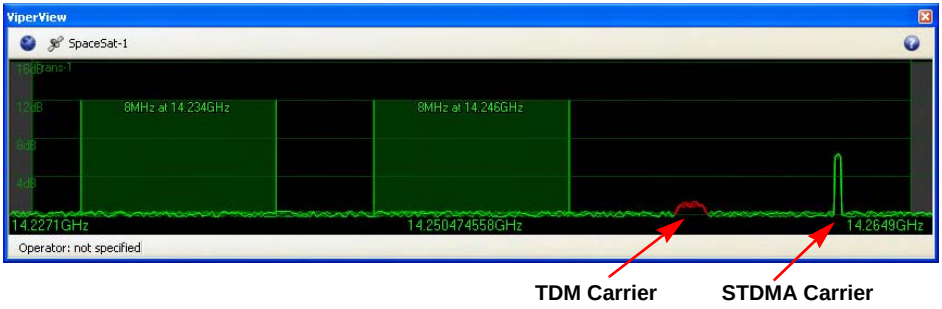


Figure 3-34 STDMA and TDM Carrier Appearance

5. Repeat the above steps for each additional unit at this site.

6. Select the next site antenna and perform the binding procedure for the mods and demods at that site.

Once at least one Remote site binding is completed, the TDM carrier display will change to green (figure 3-35).

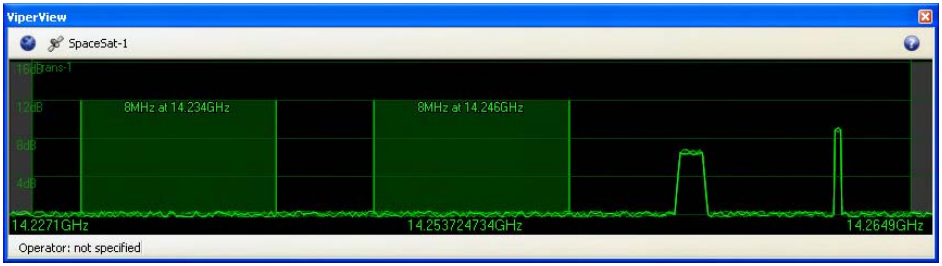


Figure 3-35 TDM Carrier Appearance Change

7. Continue the binding process until all site devices have been bound to their respective antenna's converters.

Network Manager Configuration

The remainder of the VMS configuration will involve the Network Manager, which will serve as the primary source within ViperView for managing network functions. The networks, and their associated elements, that are created in the Network Manager are *virtual*, and thus can be added and removed without affecting the actual networks upon which they are based. The source locations of the elements that are displayed in Network Manager originate from within the other VMS service managers.

A powerful feature that is provided for building the Remote sites is the *Remote Site Wizard*. Using this tool, a new Remote site can be configured very rapidly based on an existing reference site. The reference site and its associated settings serve as a template from which the new site will be built. In this way, a large number of remote sites can be easily generated.

In the first portion of this section, the method for creating and configuring sites using a manual procedure is covered. Although this method can be used for all network/group sites, it is recommended that only the Hub site(s) and the initial Remote site(s) be built this way. The remaining Remote sites should be generated using the automated method as described in the sub-section “Remote Site Wizard” on page 3-80.

Caution: Be aware that the two RF element types in Network Manager—satellites and antennas—can be taken out of Network Manager using two distinctly different methods:

- Using the **Delete** command – This deletes the element from Network Manager as well as from RF Manager, where it originated.
- Using the **Remove** command – This removes the element from Network Manager only.

The Network Manager also provides a means of exposing the satellite network(s) to customers via VNO (for network operations) and ViperGlobe (for geographical display).

Network Build Procedure

Create Network(s)

1. From the tree view list, right-click on the Network Manager icon and select **Create Network** (figure 3-36).

Figure 3-36 Create Network menu command

2. In the Create Nework dialog that opens (figure 3-37), enter a **Network Name** and click **OK**.

Figure 3-37 Create Network dialog

3. Expand the Network Manager view to expose the new Network container icon.

4. Repeat the above steps to create additional network containers, as required by the *Administrator's Network Plan.*

Create Groups

Group containers are optional and are used to help organize very large network structures, providing an intermediate level between the Network and its Site containers. For networks that will not utilize this feature, proceed to the following section, *Add Network/Group Satellite(s).*

1. Select **Create Group** from the Network drop-down menu, as shown in figure 3-38.

Figure 3-38 Create Group menu command

2. Enter a **Group Name** in the Create Group dialog, then click **OK**.

Figure 3-39 Create Group dialog

3. Repeat the above steps to create additional group containers, as required.

Add Network/Group Satellite(s)

Satellites can be associated with either a Network or a Group by dragging from RF Manager and dropping onto either element container. A satellite that is placed at the Network level will be available to all Groups and Sites under that network. A satellite that is placed at a Group level will only be available to the Sites under that group.

Note that once a satellite is dropped onto an element, it can not then be dragged out of that element and dropped onto another element, say from a Network to a Group. The satellite must be removed from the first element, then dragged from the RF Manager (the originating container) and dropped onto the other element.

1. Locate the satellite for this network/group in RF Manager and drag-and-drop it onto the network/group icon as shown in figure 3-40.

Figure 3-40 Drag Satellite to Network

2. If there are multiple satellites and/or networks/groups, repeat this drag-and-drop process as required.

3. Expand the network/group tree view to expose the satellite appearance(s).

Create Sites

Site containers are used to hold the antenna and subnet for a Hub or Remote site. This procedure follows the manual method for creating the Hub site(s) and the initial Remote site(s).

1. Select **Create Site** from the Network (or from the Group, if the site is to be a member of an existing group) drop-down menu, as shown in figure 3-41.

Figure 3-41 Create Site menu command

2. Enter a **Site Name** in the Create Site dialog, then click **OK**.

Figure 3-42 Create Site dialog

3. Repeat the above steps to create all necessary Hub and Remote site containers for this network.

NOTE

Note: It is recommended that, for each network, at least one Remote site container be created and configured as documented in the following sections. The remaining Remote sites can then be built as described in “Remote Site Wizard” on page 3-80.

Add Site Devices

1. Select the site antenna from the RF Manager satellite list and drag-and-drop it onto the appropriate site (figure 3-43).

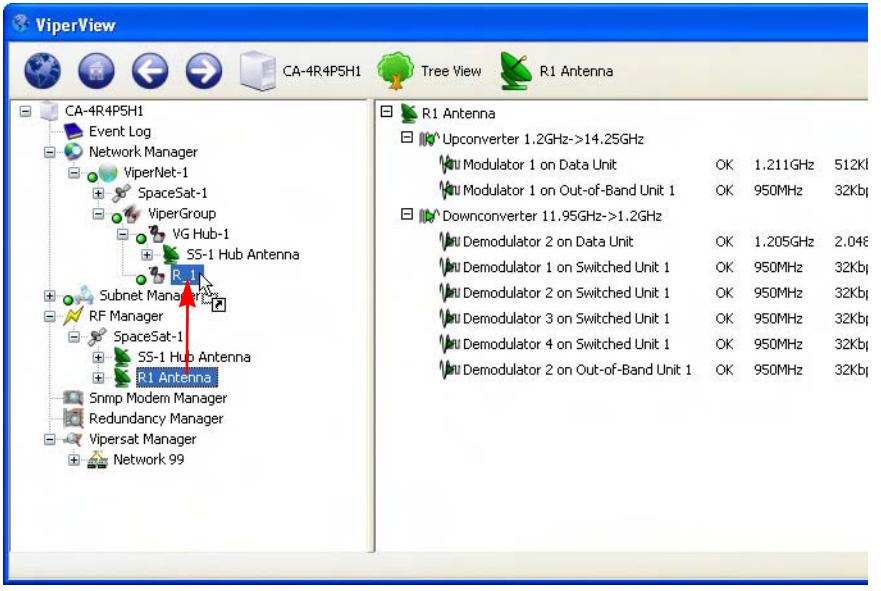


Figure 3-43 Drag Antenna onto Site

Alternative Method: Drag the antenna from under the satellite appearance in Network Manager.

2. Repeat this process for all antennas and sites.

3. Select the site subnet from the Subnet Manager list and drag-and-drop it onto the appropriate site (figure 3-44).

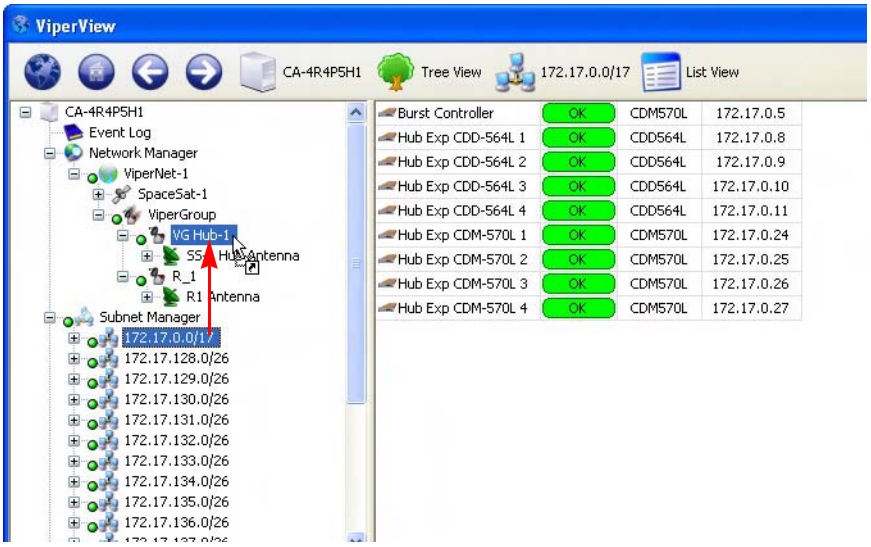


Figure 3-44 Drag Subnet onto Site

4. Repeat this process for all subnets and sites.

Set Carrier Flags

Carrier flags provide carrier type information to the system switching function. Each modem device (Modulator and Demodulator) is represented to the switching function as a transmission mode type (None, SCPC, or STDMA). These carrier flags set up the database for a starting point or home state condition. Additionally, there are flags to indicate availability of units for the switching resource manager.

Set STDMA Flag

It is important for the operator to set the STDMA flag on the network burst controller(s). The VMS sets the flags for the other network devices automatically.

1. Right-click on the BC demodulator and select **Properties** from the drop-down menu (figure 3-45).

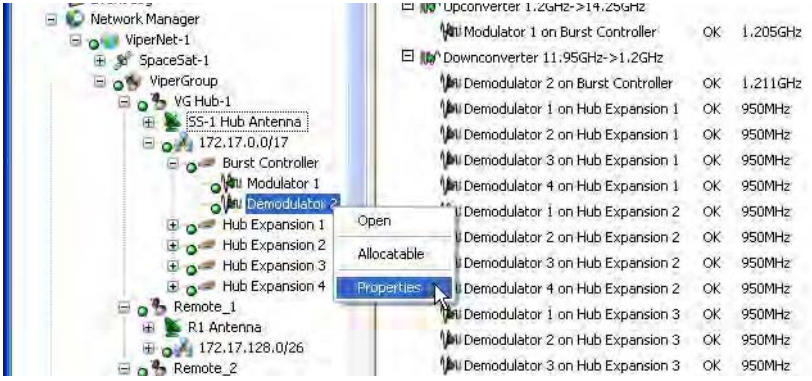


Figure 3-45 Hub BC Demodulator Properties menu command

2. The dialog appearance with the correct setting is shown in the figures below.
   - For a *CDM-570/570L Burst Controller*, select the **Modem** dialog, then select the **STDMA** radio button, figure 3-46.
   - For an *SLM-5650A Burst Controller*, select the **Burst Controller** check box, figure 3-47.

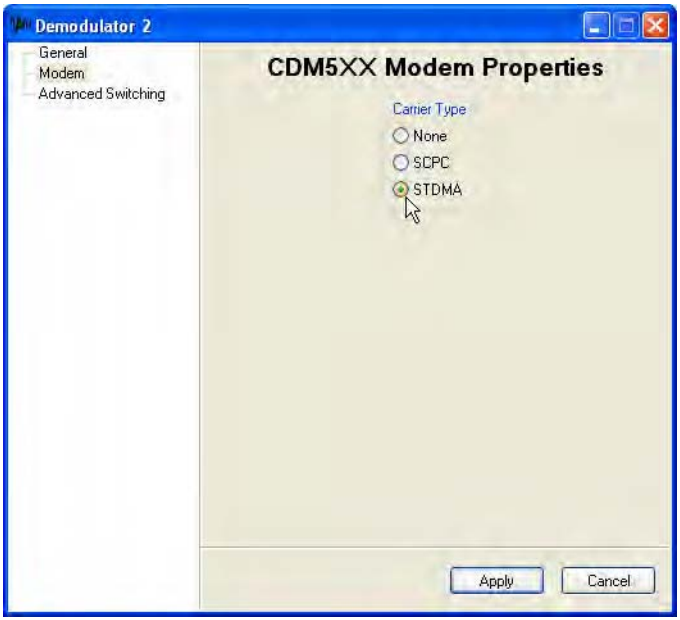


Figure 3-46 Carrier Flag Setting, Burst Controller—CDM-570/570L

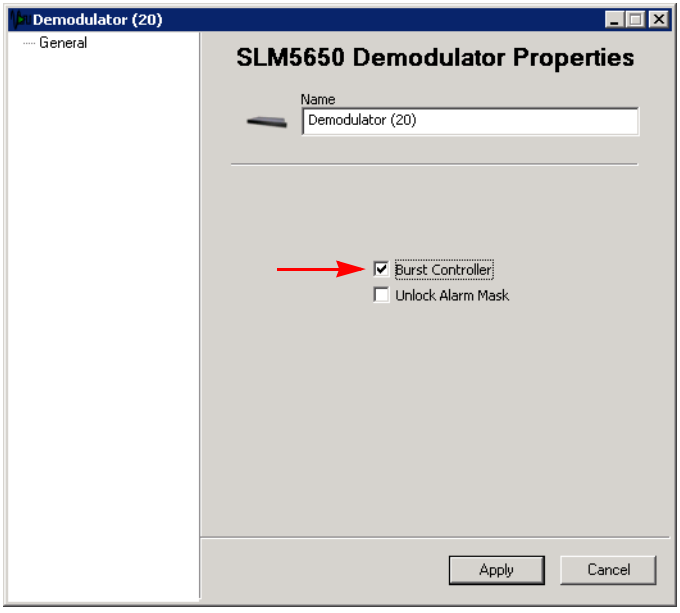


Figure 3-47 Carrier Flag Setting, Burst Controller—SLM-5650A

3. Click on the **Apply** button, then Close the window.

Set Mod and Demod Allocatable Flags

To make switching modulators and demodulators at the Hub and mesh demodulators at the Remotes available to the VMS for switching functions, the Allocatable flag for these devices must be set.

1. Expand the Network Manager tree to expose the Hub Antenna and select it.

2. In the right window panel, right-click on each allocatable modulator/demodulator and select **Allocatable** from the drop-down menu, as shown in figure 3-48.

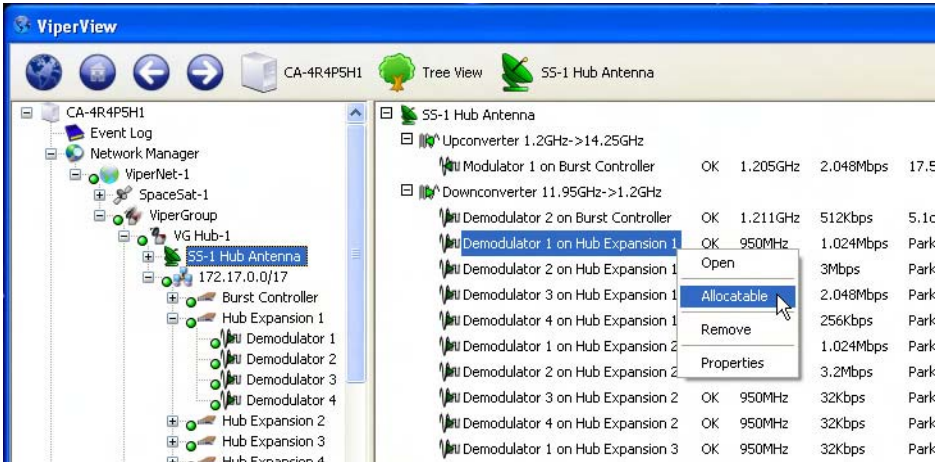


Figure 3-48 Allocatable Flag, Expansion Demod

3. Repeat the previous steps for each network Antenna (Hub and Remote) that supports allocatable modulators and/or demodulators.

Before a mod/demod is made allocatable, its status appears as *Blocked*. The status changes to *Available* after the device is made allocatable. Note that it may be necessary to perform a Refresh command in order for the status to be updated. Click on the Antenna View icon in the Menu Bar and select **Refresh**.

Mask Rx Unlock Alarms

Setting the Alarm Masks

The network alarm function must operate properly to ensure that, when an alarm condition is triggered, the generated alarm alerts the operator to an actual problem. If there are spurious alarms, or alarms which have no operational meaning, the operator may become desensitized and critical network failures can be missed. This section addresses masking alarms that represent normal network conditions. The VMS allows the masking of these nuisance alarms so that system operators can manage the network pro-actively and respond quickly to alarm indicators.

In a Vipersat network, there are burst controllers that are locking and unlocking multiple times per second, and expansion units whose normal parked or quiescent state is to be unlocked. Perform the following procedure for all network units that function as either a Burst Controller or an Expansion unit.

NOTE

Note: On SLM-5650A units, masking is automatically configured in the VMS when the modem is set to **Hub** type and configured as a **Burst Controller** (Selective TDMA is enabled).

1. From the *Tree View*, select the unit and open the Properties window.

For CDM-570/570L and CDD-56X units, right-click on the unit icon and select **Properties** from the drop-down menu (figure 3-49).

For SLM-5650A units, right-click on the modulator/demodulator icon and select **Properties** from the drop-down menu (figure 3-50).

2. In the General dialog, select **Mask Unlock Alarm**, then click on **Apply** and Close the window.

3. In the following sequence, right-click on the unit icon again and select:

- **Force Registration**
- then, **Soft Reset**

This will activate the flag in the modem and clear any latched alarms.

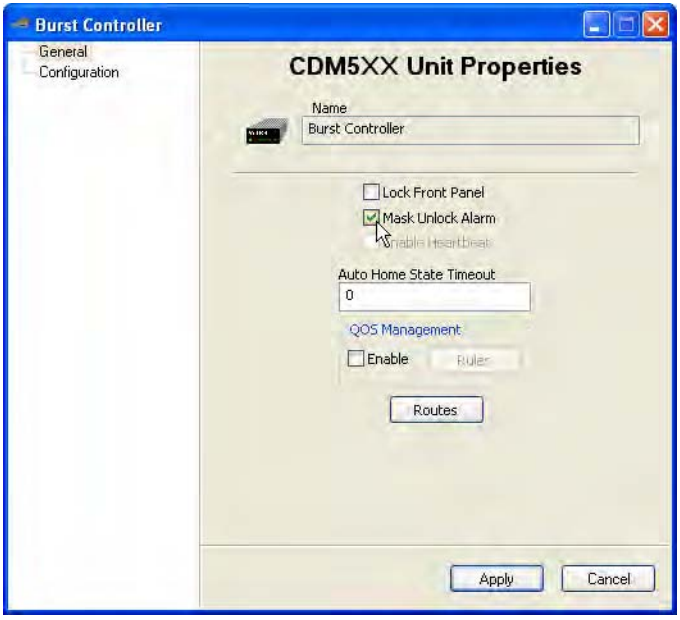


Figure 3-49 Mask Unlock Alarm, CDM-570/570L, CDD-56X

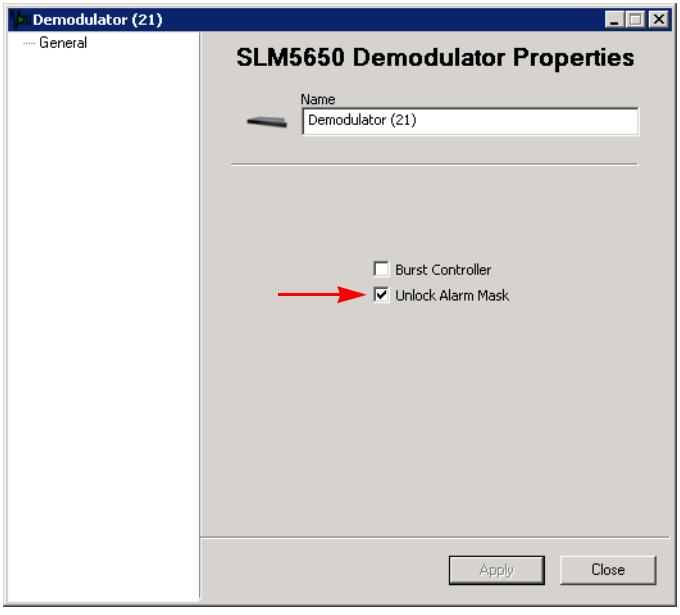


Figure 3-50 Mask Unlock Alarm, SLM-5650A

Enabling Auto Home State

A critical feature of Vipersat Networks is the modem Home State. Since the topology of the network is changing on the fly, it is necessary to ensure that Remote units will recover from a communications outage in a known state. If a Remote loses power, its home state parameters will cause it to boot up into its burst configuration, awaiting maps from the Hub. Knowing this, the VMS can free up assets (switched demodulators and bandwidth) if it loses communications with a Remote for a settable period of time. This is the Auto Home State concept.

The recovery cycle is automatic once the operator sets the Auto Home State parameter in the Remote unit.

Perform the following steps on each Remote data unit.

Do *not* perform this procedure on an Expansion unit, *nor* on a Hub unit.

1. From the *Tree View*, right-click on the Remote data unit and open the **Properties** window(figure 3-51 or figure 3-52).

2. In the General dialog, enter a time (in minutes) for the **Auto Home State** to take effect, then click on **Apply** and Close the window.

   The default value of **0** disables Auto Home State.

Caution: A Timeout of no less than 4 minutes is recommended; values less than 4 minutes may create undesirable recovery effects.

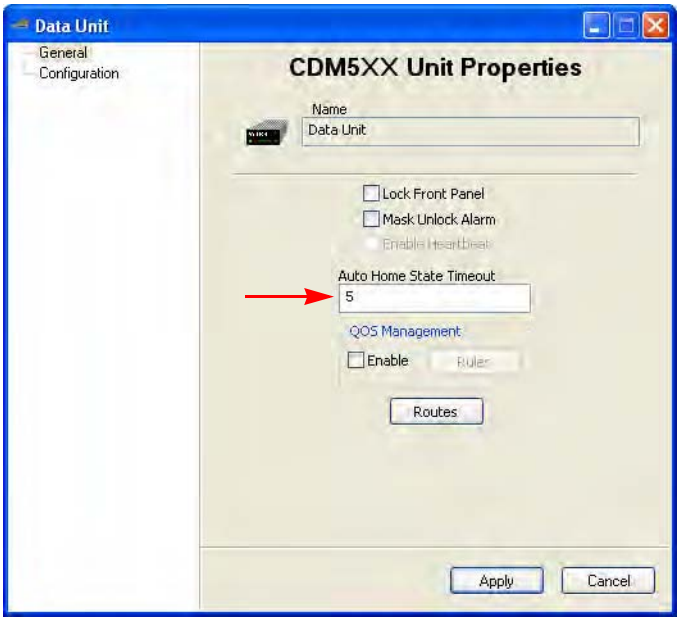


Figure 3-51 Auto Home State Timeout, CDM-570/570L

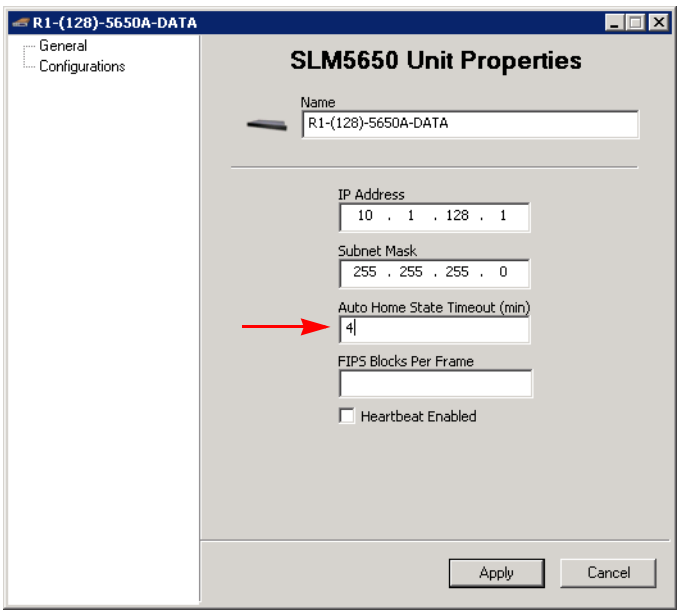


Figure 3-52 Auto Home State Timeout, SLM-5650A

3. Right-click on the unit icon again and select **Force Registration**.

This will force the parameter set in the modem. VMS will then set the parameter every time it registers the unit.

InBand Management Configuration

Dynamic carrier management is configured and controlled under the Network Manager, consolidating all operations per satellite within a specific network. Enabling InBand management activates VMS functionality for dynamic assignment of carriers, bandwidth pool management, and switching policies on a per Remote basis. InBand management is only configured for Remote sites, never for Hub sites.

Caution: Never set InBand management for a Hub site.

As described previously, all Remote sites in the network can be configured manually. However, the recommended practice is to manually create and configure one (or more) site(s) that will serve as a reference template for the remaining Remotes when using the Site Wizard tool.

The sequence for configuring InBand management is as follows:

- Activate InBand management, Tx and/or Rx
- Configure Home State and Switch Rate Limits
- Set Bandwidth Reservations
- Set Advanced Switching parameters—Data Rate and ModCods
- Set SHOD Limits
- Set Application Policies
- Define Distribution Lists

Note that all configuration settings for a Remote site are included in the reference template *except for the ModCods*. Therefore, the procedure for configuring the Advanced Switching table is presented after all of the Remotes have been created (see “Advanced Switching Configuration” on page 3-102).

Set InBand Management

For each Remote site in the network that will require dynamic control of their carriers (nodes which are part of the switched network), perform the following procedure.

1. Right-click on the site and open the site's Properties window, then select the **InBand General Settings** dialog (figure 3-53).

Figure 3-53 InBand General Settings dialog

2. Click on the **Enable InBand** button to activate the InBand parameter fields.

3. **Enable** the type of switching that this site will perform.

   return path switching — allows dynamic SCPC switching for establishing a Tx carrier from this Remote to the Hub. (Requires an expansion demodulator at the Hub.)

   Also allows this Remote to execute SHOD/mesh applications. (Requires an expansion demodulator at the receiving Remote(s), as well as one at the Hub.)

   forward path switching — allows dynamic SCPC switching for establishing a dedicated Tx carrier from the Hub to this Remote. Requires an allocatable modulator at the Hub.

   FPS must be enabled for:

   - A Remote that will perform Point-to-Point switching with the Hub.
   - An SOTM/roaming Remote—temporarily, for selection of the TDM modulator Home Device (it will subsequently be reset to disabled in a later step in this procedure).

4. If required, activate and specify the **Priority** for this site.

Priority levels can be assigned to sites as well as application policies. Resource allocation preference is based on the highest priority among contending sites and/or policies. Note that a *lower* number corresponds to a *higher* priority level. Priority **1** is the highest level (priority **0** equates to *No priority*). This setting defaults to the lowest level (2,147,483,646).

The site priority level determines the likelihood that:

- The requested bandwidth will be allocated, should there be contention with other Remote(s).
- A carrier that is assigned to this site will get resized based on bandwidth availability. Sites with higher priority levels are more likely to retain their requested bandwidth during periods of bandwidth contention than those sites that have lower priority levels.

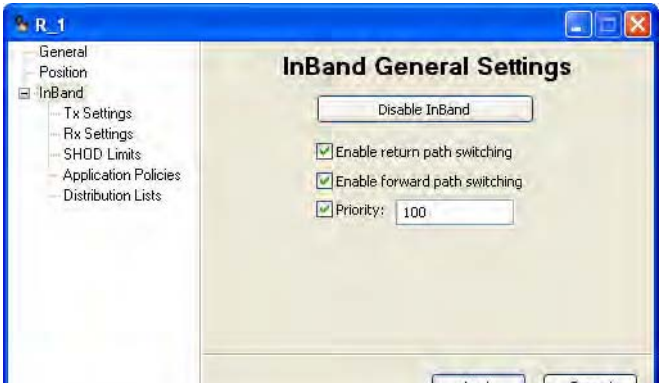


Figure 3-54 InBand Switching Enabled

5. If *return path switching* has been enabled, select the **Tx Settings** (Return Path) dialog (figure 3-55) for configuration of the transmit Home State.

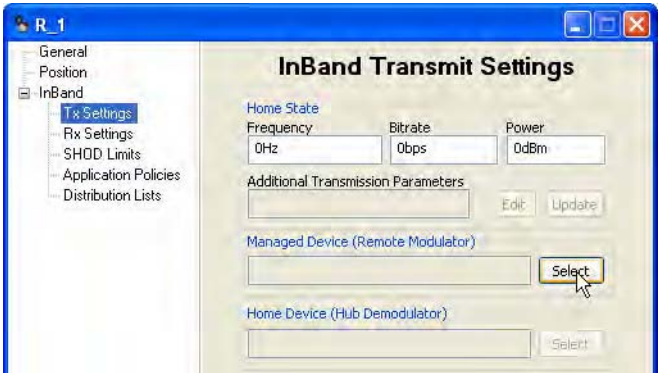


Figure 3-55 InBand Transmit Settings dialog

6. Select the *Remote Modulator* for this site by clicking on the **Select** button for Managed Device.

7. In the Select Object window that opens, double-click on the **Antenna** icon for this Remote site to view the associated mods (figure 3-56).

8. Select the **Modulator** for this site's data modem and click **OK** to enter it into the Tx Settings dialog.

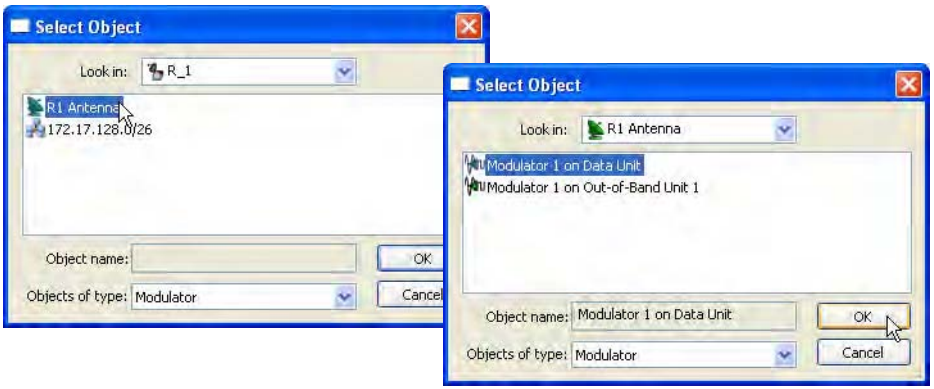


Figure 3-56 Select Remote Modulator

9. Next, select the *Hub Demodulator* for this site by clicking on the **Select** button for Home Device.

10. In the Select Object window that opens, double-click on the **Antenna** icon for the Hub site to view the associated demods (figure 3-57).

11. Select the **Demodulator** for this site's Burst Controller and click **OK** to enter it into the Tx Settings dialog.

NOTE

Note: As soon as the Home Device is chosen, an alert icon appears next to the *Additional Transmission Parameters* field in the Home State box, as well as the *Tx Settings* menu item. Clicking on the icon reveals a message warning that the current parmeters for this field (none) are not valid for the Home Device that has been selected.

This can be corrected by using the **Edit** button, if the settings for the selected device are known. However, the **Update** button will pull the correct settings for this field, as well as for the other Home State fields.

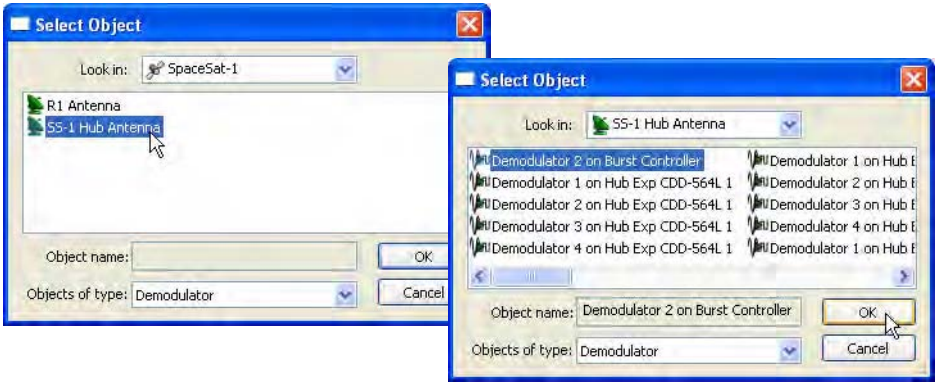


Figure 3-57 Select Uplink Demodulator

12. In the Home State box, click on the **Update** button, then click **Yes** to confirm the settings (figure 3-58).

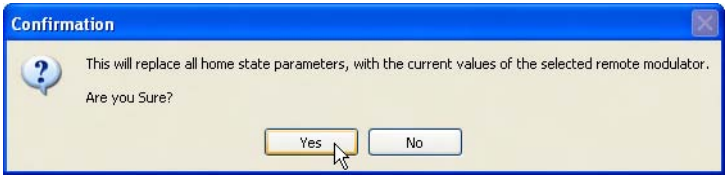


Figure 3-58 Confirmation, Home State Changes

The Frequency, Bitrate, Power, and Additional Transmission Parameters fields should populate with the values pulled from the chosen remote modulator, as shown in figure 3-59.

If the fields do not populate, communications with the Remote are impaired and will have to be restored before the site can be successfully InBanded for the return path.

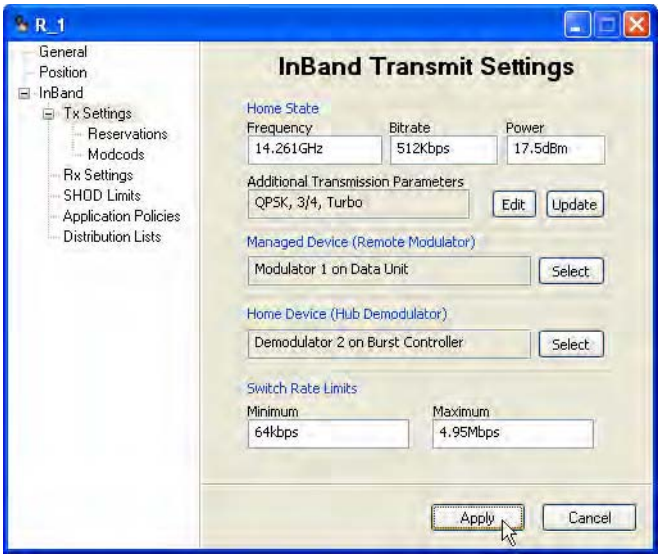


Figure 3-59 InBand Tx Settings dialog, populated

13. Set the **Minimum** and **Maximum** Transmit **Switch Rate Limits** for this site. These values set the transmission data rate range for governing the remote to operate within the budgeted switching constraints.

Units must be included in the entry—use bps, kbps, or Mbps.

If this Remote has forward path (P2P) switching enabled, or is used in a roaming application, continue with the next step.
If **not**, proceed to step 24.

14. Select the **Rx Settings** (Forward Path) dialog (figure 3-60) for configuration of the receive Home State.

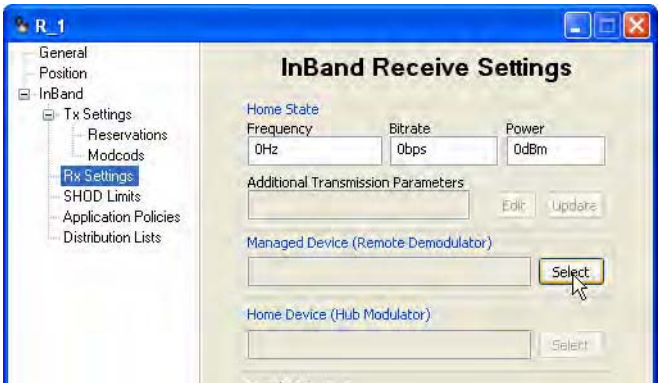


Figure 3-60 InBand Receive Settings dialog

15. Select the *Remote Demodulator* for this site by clicking on the **Select** button for Managed Device.

16. In the Select Object window that opens, double-click on the **Antenna** icon for this Remote site to view the associated demods (figure 3-61).

17. Select the **Demodulator** for this site's data modem and click **OK** to enter it into the Rx Settings dialog.

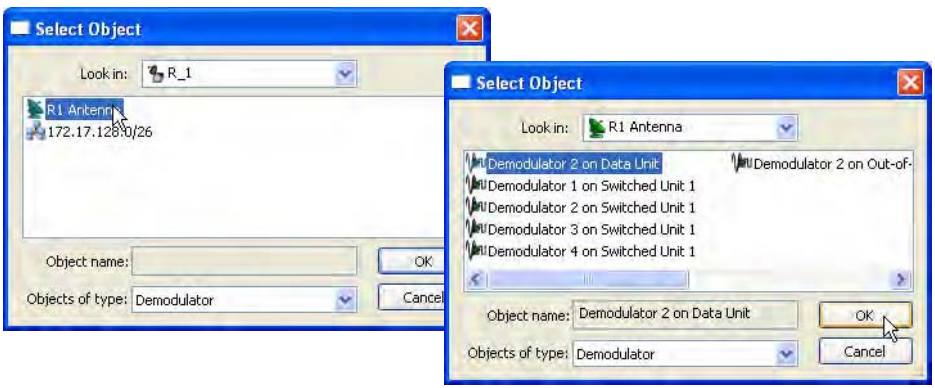


Figure 3-61 Select Remote Demodulator

18. Next, select the *Hub Modulator* for this site by clicking on the **Select** button for Home Device.

19. In the Select Object window that opens, double-click on the **Antenna** icon for the Hub site to view the associated mods (figure 3-62).

20. Select the **Modulator** for this site's TDM (typically the Burst Controller, unless another modem is designated for the TDM) and click **OK** to enter it into the Rx Settings dialog.

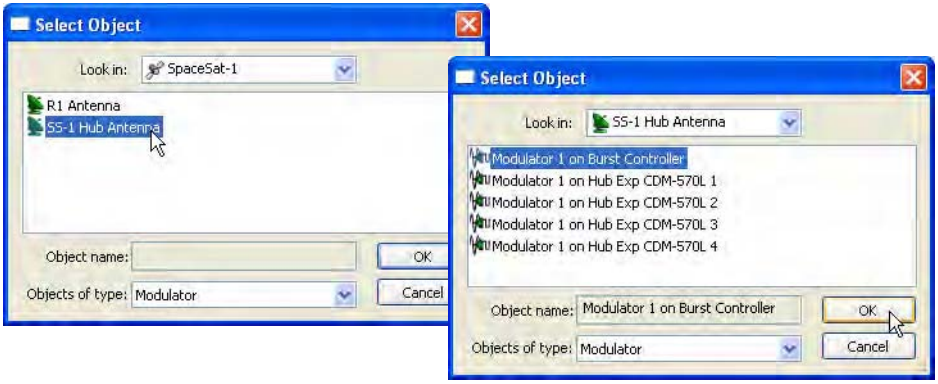


Figure 3-62 Select Downlink Modulator

21. In the Home State box, click on the **Update** button, then click **Yes** to confirm the settings.

The Frequency, Bitrate, Power, and Additional Transmission Parameters fields should populate with the values pulled from the chosen hub modulator, as shown in figure 3-63.

If the fields do not populate, communications with the Hub are impaired and will have to be restored before the site can be successfully InBanded for the forward path.

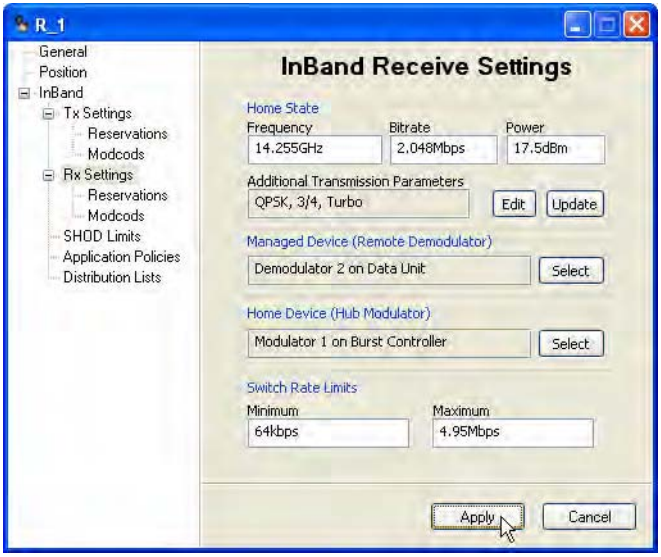


Figure 3-63 InBand Rx Settings dialog, populated

NOTE

Note: The value that appears in the **Power** field corresponds to the Hub TDM setting. Because this setting is determined based on ensuring a link with the weakest Remote in the group, the value may be excessive for what this Remote requires. It is recommended that this value be adjusted per Remote as necessary to provide sufficient power under clear sky conditions.

22. Set the **Minimum** and **Maximum** Receive **Switch Rate Limits** for this site. These values set the transmission data rate range for governing the remote to operate within the budgeted switching constraints

Units must be included in the entry—use bps, kbps, or Mbps.

For an SOTM/roaming Remote, continue with the next step.
Otherwise, proceed to step 24.

23. Select the InBand General Settings dialog and **disable** (un-check) the *forward path switching* (figure 3-64).

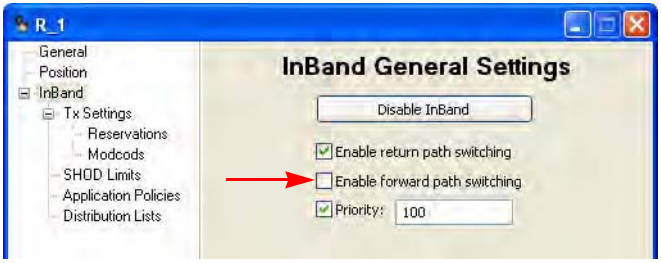


Figure 3-64 Disable Forward Path, Roaming Remote

24. Click on **Apply** to establish these new parameter settings in the VMS, then Close the window.

Repeat the above InBand procedure for all applicable Remotes.

Set InBand Reservations for Guaranteed Bandwidth

The InBand Bandwidth Reservation ensures that the Remote is always guaranteed bandwidth up to the rate that is specified. Beyond that, the Remote will only be granted additional bandwidth when it is available. Should system conditions occur that require some Remotes' data rates be reduced due to a shortage of bandwidth resources, those Remotes that own pre-allocated reservations will never be reduced below their guaranteed rate.

Reservations can be configured independently for the Transmit modulator and the Receive demodulator of a Remote data unit. Perform the following procedure for setting the InBand Tx Bandwidth (when return path switching is enabled) and/or the InBand Rx Bandwidth (when point-to-point forward path switching is enabled).

1. Open the Properties for the Remote site and select the **InBand Tx Reservations** menu item.

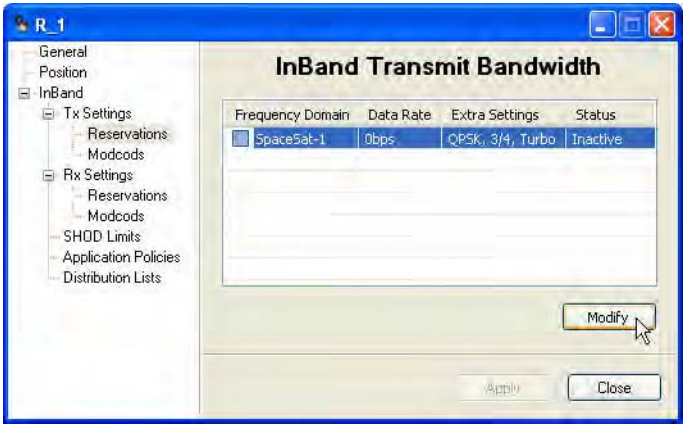


Figure 3-65 InBand Transmit Bandwidth dialog

Setting a data rate in this dialog will reserve a segment of bandwidth for the Remote ensuring that, at last resort (no additional bandwidth available), the Remote will be dropped to the rate specified here—its CIR—until excess bandwidth is once again available to be allocated.

Caution: Before enabling ANY Remote for Bandwidth Reservation, a Bandwidth Pool MUST have been created to allow the system to set guaranteed rates. See “Create Bandwidth Pools” on page 3-27.

Caution: Before enabling ANY Remote for Bandwidth Reservation, Hub expansion demodulators MUST have been made Allocatable to allow the system to set guaranteed rates (see “Set Mod and Demod Allocatable Flags” on page 3-46). To ensure that all reservations will be met, there must be a Hub expansion demodulator for each Remote site that has a CIR.

2. Click to highlight the satellite table entry, then click on the **Modify** button to open the Edit Reservation dialog.

Figure 3-66 Edit Reservation dialog

Enter the desired **Rate** for guaranteed bandwidth, making sure that the value entered does not exceed the *maximum switch rate* (InBand Bandwidth Policy setting). Note that the default setting is **0** bps.

Units must be included in the entry—use bps, kbps, or Mbps.

3. Select the Transmission Parameters **Extra** (**...**) button to set FEC & Modulation required for this CIR.

Clicking on a parameter will display the pull-down menu for that item. Set the parameters as required, then click on **OK**.

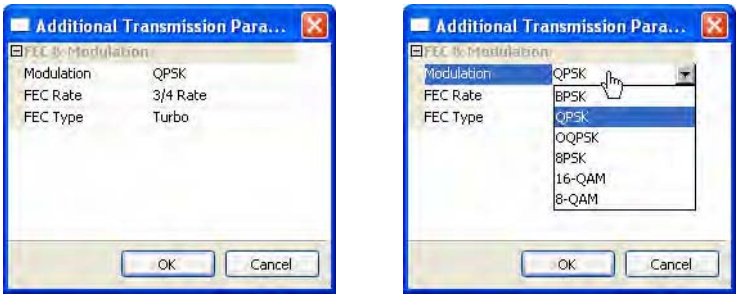


Figure 3-67 Edit, Additional Transmission Parameters

4. Click in the **Enable Reservation** check box to select the satellite for this bandwidth reservation, then click **OK**.

5. Click on **Apply** to define the guaranteed rate for this Remote.

Observe the **Status** of this reservation that is displayed in the far right column of the table; the Inactive label should change to Active, indicating that the reservation was accepted, as shown in figure 3-68.

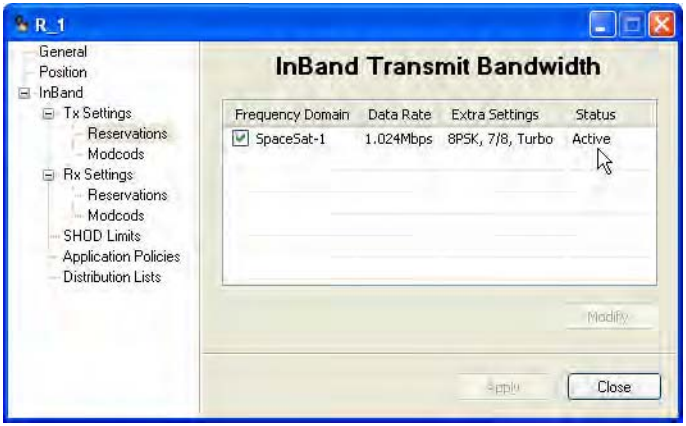


Figure 3-68 Bandwidth Reservation Applied

If the attempt was not accepted, the label Unavailable will be displayed, followed by information explaining the error—insufficient bandwidth available, or insufficient hardware (expansion demod) available.

6. Should an error occur with this reservation, correct the mis-configuration that caused the error, then re-apply the reservation.

7. Repeat steps 1 through 6 for configuring the **InBand Rx Reservations** for this Remote.

8. Close the Properties window for this Remote.

9. Open the **Satellite Reservations** window to view the currently assigned (per individual remote, and total) and available bandwidth for reservations on this satellite (figure 3-69 and figure 3-70).

Figure 3-69 Satellite Reservations menu command

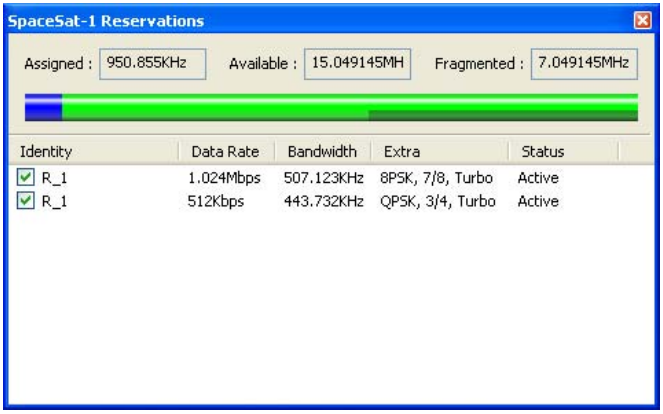


Figure 3-70 Satellite Reservations window

This window displays a table containing entries for each Remote site (both Tx and Rx, if so enabled) that has been assigned a CIR, and displays the following information:

- **Reservation Enable/Disable** — check box toggle. Status column display reflects this setting, either Active or Inactive.
- **Assigned, or Pre-Allocated, Bandwidth** — currently reserved for granting CIR when called for by the list of Remote sites presented in the table. This segment is displayed as a numerical frequency value, and is represented as the *dark blue* section of the bandwidth color bar. The Data Rate, Bandwidth, and Extra (mod/code) parameters for each site are also provided in the table.

- **Available Bandwidth** — currently unreserved and available for pre-allocation to Remote sites. This segment is displayed as a numerical frequency value, and is represented as the *light green* section (combined) of the bandwidth color bar. The largest continuous/ unfragmented block of available bandwidth is represented by the *light green* section that is not underlined with *dark green*.
- **Fragmented Bandwidth** — additional available bandwidth remaining that is separate from the largest continuous block. This segment is displayed as a numerical frequency value, and is represented as the *light green* section of the bandwidth color bar that is underlined with *dark green*.

The divisions shown in the color bar will vary depending on a number of factors, including the quantity and size(s) of the bandwidth pool(s), and the amount of pre-allocated bandwidth.

When Site reservations are assigned for both Tx and Rx (Point-to-Point), the first listing for a Remote represents the Tx bandwidth and the second listing is the Rx bandwidth.

From this window, individual reservations can be enabled/disabled via the check box in the Identity column. Reservation settings (Data Rate, Bandwidth, and Extra) can be edited by double-clicking on a table entry.

Note that the Satellite Reservations window can be left open to assist the user/operator in the reservation assignment process for other Remotes.

10. Continue to select Remotes as required and configure them for guaranteed bandwidth until either all resources are exhausted or network requirements are achieved.

11. To remove a bandwidth reservation for a Remote, click to uncheck the satellite check box in the site Reservations page, then click **Apply**.

Hub Allocatable Modulator & Demodulator Compatibility

Compatibility issues with allocatable mods and demods at the Hub may arise when implementing the Guaranteed Bandwidth feature in networks that include multiple modem types. When combining modem types, careful network design is essential to ensure that a compatible Hub mod/demod is available for establishing an SCPC link with a Remote. The following factors must be considered:

- **Transmission Rate** — The device must be capable of handling the data rate that will be allocated between the Remote and the Hub (e.g., SLM-5650A versus CDM-570/L or CDD-56X).

- **Encryption** — A Remote set for using TRANSEC requires the Hub device to use TRANSEC also.

Considerations for Using Guaranteed Bandwidth with Advanced Switching

Care should be taken when assigning Bandwidth Reservations to a Remote that also uses Advanced Switching (refer to “Advanced Switching Configuration” on page 3-102). The VMS does not guarantee a bit rate, *per se*. Rather, a bandwidth reservation (frequency value) is assigned. This is why the option for editing FEC and Modulation settings is provided in the Reservations dialog for a remote site.

The VMS attempts to assign the most efficient bandwidth utilization in an advanced switching environment. If Advanced Switching is configured for a Remote, a switch request that crosses the threshold where the higher-order modulation actually becomes more bandwidth efficient will result in a step up to the higher-order modulation at the lowest bit rate that exceeds the request.

For example, a site currently operating at QPSK 3/4 that generates a switch request for 192 kbps will be switched up to 256 kbps at 8PSK 7/8, provided this modulation code rate was specified in the Advanced Switching table entry for this switch point. This scenario is illustrated using the following equations:

QPSK 3/4 @192 kbps @1.3 spacing:

Allocated Bandwidth = 192 x (1/2) x (1/.75) x 1.3 = 166.4 kHz

8PSK 7/8 @256 kbps @1.3 spacing:

Allocated Bandwidth = 256 x (1/3) x (1/.875) x 1.3 = 126.781 kHz

However, when a bandwidth reservation is added to this scenario, the end result may differ. If the reservation specifies 192 kbps at QPSK 3/4, the VMS will perform the same calculation as shown in the first equation above and the reserved bandwidth will be 166.4 kHz. Since this falls within the range at which the VMS would step up to 8PSK, the bit rate available with an allocated bandwidth of 166.4 kHz would be provided, which is 336 kbps.

Thus, when a guarantee is set within the threshold range of advanced switching, unexpected results may result. In this example, the result is that the guaranteed data rate that is provided by the VMS (336 kbps) is actually greater than the expected CIR that was entered as the bandwidth reservation (192 kbps). In addition, the advanced switching performance will also differ, resulting in a higher data rate as well as higher bandwidth usage.

Effect of RF Changes on Reservations

Caution: The operator must be aware that changes made to bandwidth resources in the RF configuration *after* reservations have been defined may require re-evaluating these reservations and resetting pre-allocated bandwidth.

Reducing or moving a bandwidth pool, for example, may result in a failed attempt to grant the bandwidth necessary to meet a site's CIR requirement. Such a failure would cause the site to become unavailable for switching until reservations for that site are reset.

Any sites that become unavailable must be reset on an individual basis. However, for those sites with reservations that have not been made unavailable, resetting the reservations for one of those sites will result in all of them being reset. To reset site reservations, perform the following steps:

1. Open the Properties for the Remote site and select the InBand Reservations dialog.

2. Click on the check box to de-select the satellite for this bandwidth reservation, then click again to re-select the satellite.

3. Click on Apply, then Close the window.

   The VMS will reset the pre-allocated resources for this Remote, as well as all other Remotes with guaranteed bandwidth settings that are still available.

Set SHOD Limits

The VMS Single Hop On Demand (SHOD) operates in environments where variations in geographical location and Remote site hardware (antenna, power amplifier, etc.) can create link power inconsistencies when referenced to the Hub. Budgetary calculations may provide adequate link performance to the Hub, but will differ when establishing mesh connections to one or multiple Remote sites.

InBand management provides the SHOD Bit Rate Limit feature that can be used when configuring a Remote site that will be utilized in SHOD/Mesh applications. Use of this feature may be required to accommodate for varying link factors, such as disparity in antenna sizes and/or BUC specifications, which affect transmit power limitations.

For example, a given data rate that is achievable when establishing a link with the Hub may not be achievable when meshing with another Remote, due to differences in the respective link margins. The differences could be significant enough to prevent reliable communications for some mesh connections.

Both Transmit and Receive settings are presented for specifying minimum and maximum bit rates:

- The Tx setting defines the range limits for this Remote's modulator when this Remote is sending to another Remote or Remotes.
- The Rx setting defines the range limits for any Remote's modulator when this Remote is receiving from that Remote.
- When a Remote with a defined Tx limit is transmitting to a Remote with a defined Rx limit, the lesser of the two SHOD limit values will govern the transmission rate.

Figure 3-71 InBand SHOD Limitations dialog

NOTE

Note: These SHOD limitations may reduce and restrict application performance to the Hub during mesh connection allocations. There will be no provisions to block or notify applications that require greater bandwidth during mesh reductions.

Set InBand Application Policies

The establishment of Application Policies provides the rules and parameters that are utilized for application switching operations in the Vipersat network. Application switching is only available to those Remotes that have policy definitions associated with them, either directly (local policy) or via inheritance (from network and/or group).

Vipersat network InBand Application Policy settings can be established at three hierarchical levels within the Network Manager:

- The Network Level

- The Group Level
- The Site Level

This capability provides operators the ability to segregate application policies between these three levels in the network. Policies for one network, group, or site can be different from policies for another network, group, or site. Network policies are inherited by the groups and sites that belong to that network, and Group policies are inherited by the sites that belong to that group. Locally created Site policies apply only to that site.

Start by building policies at the Network level, then set the policies at the Group and/or Site levels.

1. Open the Network Properties and select the **InBand Application Policies** dialog, as shown in figure 3-72.

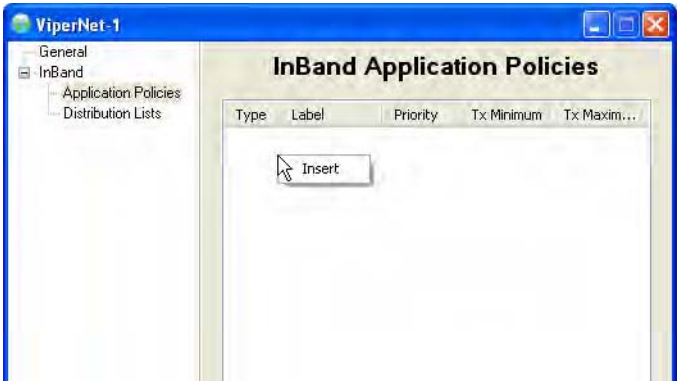


Figure 3-72 InBand Application Policies dialog, Network

2. To add a policy, right-click in the table space and select **Insert**.

3. Enter the Type value, Label, Priority, and Bitrate limits for this policy (figure 3-73), then click **OK** to enter this policy in the table .

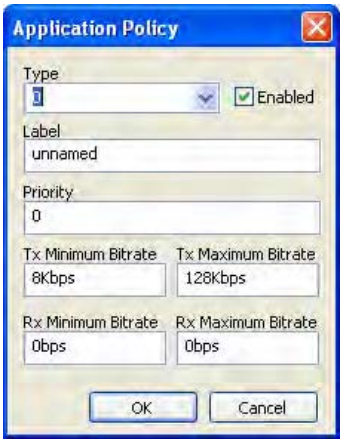


Figure 3-73 Application Policy Settings

Application Policy **Type** numbers have the following convention:

0 — ECM Load Switching
1 — Scheduled Switching and VFS
2 — Voice
3 — Video
4–63 — Reserved for the System
64–253 — User Defined
254 — Uninterruptable Switch / Immobile Carrier (such as for video; used to ensure that additional applications will not generate a switch, thus preventing video glitches)

Priority levels can be assigned to application policies as well as to sites. Resource allocation preference is based on the highest priority among contending sites and/or policies. Note that a *lower* number corresponds to a *higher* priority level. Priority **1** is the highest level. Priority **0** (default) equates to *No priority*.

The policy priority level determines the likelihood that:

- The requested bandwidth will be allocated, should there be contention with other policies.
- A carrier that is assigned to this policy will get resized based on bandwidth availability. Policies with higher priority levels are more likely to retain their requested bandwidth during periods of bandwidth contention than those policies that have lower priority levels.

Both Tx and Rx **Bit rate** parameters are presented, for accommodation of P2P configurations.

NOTE

Note: Note that the Rx settings default to the rate of **0 bps**. For P2P sites, take care to set these values appropriately to avoid undesirable results.

Setting the Rx values at the default rate will result in no carrier for the forward path, unless an Excess bit rate is specified (see step 6.).

4. Repeat this process of adding policies to build the policy table (figure 3-74).

It is recommended that a type 64 policy be defined at the Network level for general usage by all Remote sites. This policy would then, for example, be available for the Application Sessions feature which uses type 64 in its default settings.

5. By default, Automatic Switching is enabled for the network. However, this function can be disabled with the check box in the lower portion of the page.

6. An **Excess** bit rate can be specified here as well. This additional rate will be applied to all application switching and adds an extra margin of bandwidth to the carrier.

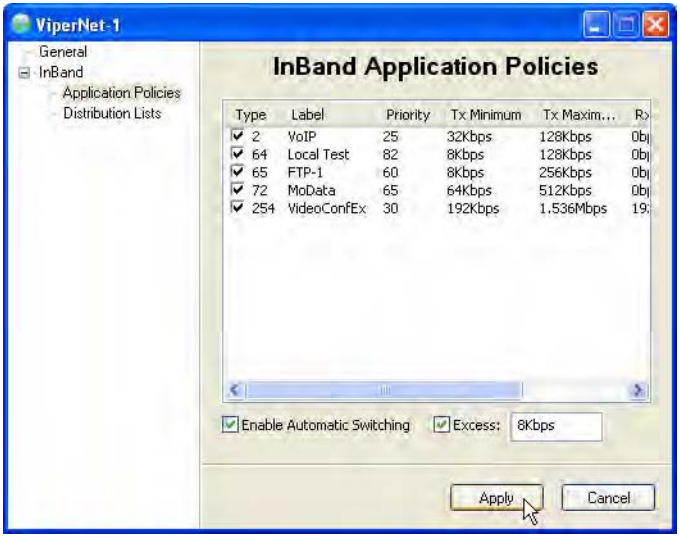


Figure 3-74 Application Policies Table, Network

7. Click on **Apply** to save these policy entries.

Repeat the above procedure to build *Group* policies, if required.

Inherited Policies

If policies were created for the network to which this group/site belongs, those policies will appear under the group/site as well (inherited).

At the group/site level, the operator can modify policy settings for this group/site that are inherited from the network/group policies.

Minimum, Maximum and *Excess Bit Rates* can be either left at 0 bps, which will cause this InBanded site to use the network settings, or set to the desired values for local control.

The check boxes have 3 states:

- **Clear** — The policy or switch type is not enabled (*Inherited–Disabled*)
- **Clear with Check** — The policy or switch type is enabled and can be edited (*Inherited–Editable*)
- **Gray with Check** — The policy or switch type is enabled and cannot be edited (*Inherited–Fixed*)

To edit an inherited policy, the check box must be set as **Clear with Check**. Then, the bit rates can be changed to the desired values for this group/site by clicking on the policy, then clicking on the parameter to be changed and entering a new value.

Local Policies

In addition to modifying existing inherited policies, local policies specific to a Remote site can be created, modified, and removed.

1. Open the Properties for an InBanded Remote site and select the InBand Application Policies dialog, figure 3-75.

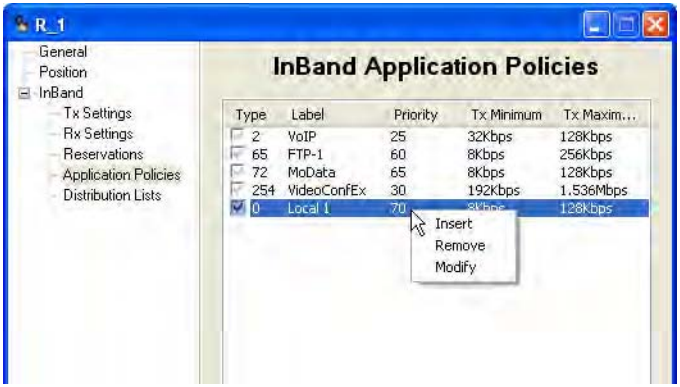


Figure 3-75 Application Policies Table, Remote Site

2. Right-click in the open table space to **Insert** a new policy just for this site.

3. To edit a local policy, the check box must be set as follows:

- **Clear** – the Label can be changed
- **Checked** – the Label and Bit Rates can be changed

Then, the parameters can be modified as required for this group/site by clicking on the policy, then clicking on the parameter to be changed and entering a new name or value.

4. To remove an existing local policy, right-click on the policy table entry and select **Remove**.

Note that only locally created policies can be removed, not inherited policies.

5. Click on **Apply** to save these policy entries.

Define InBand Distribution Lists

Distribution Lists allow the operator to set up a list of sites to be included in a switch under defined circumstances, such as meshing based on an ECM switch, multicast transmission from a remote to a group of remotes, or the setup of monitor remotes. For example, this feature can be used to tune expansion demodulators at a list of sites to receive a multicast video stream.

As with Application Policies, Distribution Lists can be established at the Network, Group, and Site levels. However, in the majority of applications, these lists are defined at the remote site level. Note that the InBand Policy flag must

be set for an element in order for the *Distribution Lists* dialog to appear under the Properties for that element

1. To declare a Distribution List, right-click on the white table area in the dialog, then click on the **Insert** button that appears (figure 3-76).

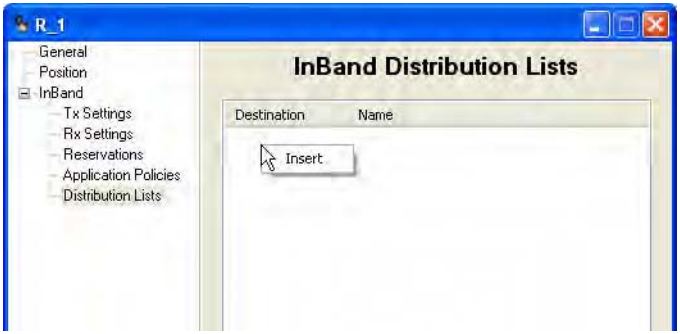


Figure 3-76 InBand Distribution Lists, Remote Site

The **Distribution List** dialog (figure 3-77) provides a **Target** address box and a **Label** name box, and allows the operator to add/remove subnet **Destinations** to the list.

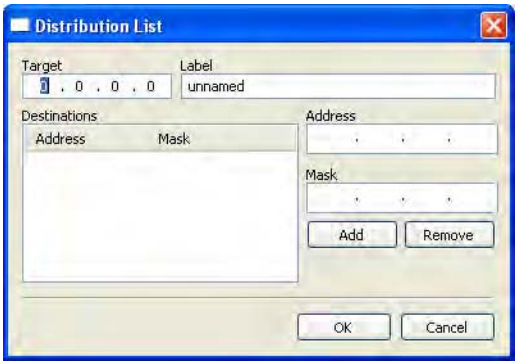


Figure 3-77 Distribution List dialog

2. Enter either a Target multicast or unicast address, or leave the address as all zeros, depending on the purpose for the list.

   For example, if the target is left as 0.0.0.0, ANY application switch for this site will cause the list to be activated.

3. Enter a Label to identify this list.

4. Enter the Address and Mask for the subnet to be added to this list, then click on the **Add** button.

5. Repeat the previous step to add multiple subnets.

   To prevent a routing loop from occurring, do NOT add the subnet for the remote site that owns this list.

6. When all desired subnets have been added, click **OK** to enter this list in the Distribution Lists table.

7. Repeat steps 1 through 6 to define additional lists.

8. A list entry is enabled/disabled with the use of the check box.

9. Click on **Apply** to save these list table entries.

Switching Function Verification

Once the InBand management configuration for a Remote is completed, the VMS switching functions will become active. At this point, manual switch commands can be used to verify that the switching function is operable. The following procedure will demonstrate a manual application switch operation from STDMA mode to SCPC mode utilizing a bandwidth slot assigned by the VMS from one of the pools that were created in the RF Manager configuration procedure.

1. Right-click on an InBanded Remote site in the Network Manager and select **Application Sessions** from the drop-down menu (figure 3-78).

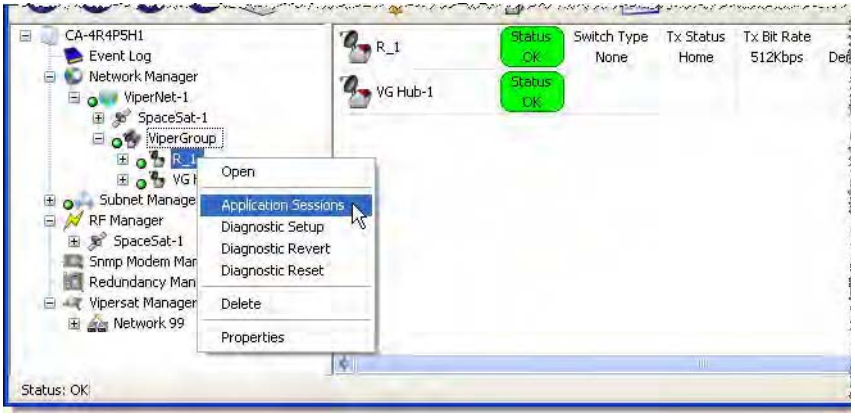


Figure 3-78 Application Sessions menu command

The InBand Sessions dialog will open, allowing a transmit **Datarate** and switch **Type** to be specified. The default data rate is 0 bps. This setting corresponds to the Tx Maximum; the resulting rate will be the lesser value between the Policy setting and the Site setting.

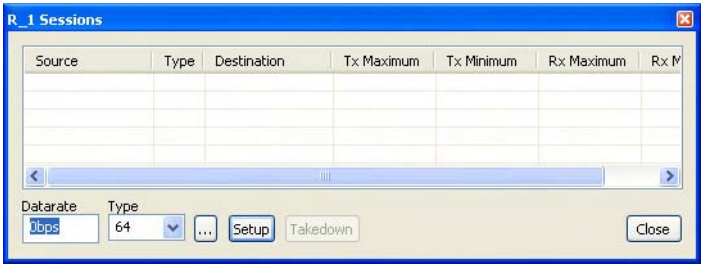


Figure 3-79 InBand Sessions dialog

2. Accept the default rate, select a valid switch type, and click on **Setup** to initiate an SCPC switch.

Note that the Type default is **64**; however, if Type 64 is not defined for this Remote, the switch attempt will fail, as shown in figure 3-80. Use the pull-down menu to view and select a valid policy for this Remote.

Figure 3-80 Switch Failed message

Note also that more switch options are available by clicking on the ellipses (**...**) button to open the **InBand Application Session** dialog
Refer to the section "Operator Switch Request" on page 5-33 *for more information on using the Application Sessions feature*.

The InBand Sessions table will record the new entry and the **Executing Switch** message will be temporarily displayed while the switch request is processed (figure 3-81).

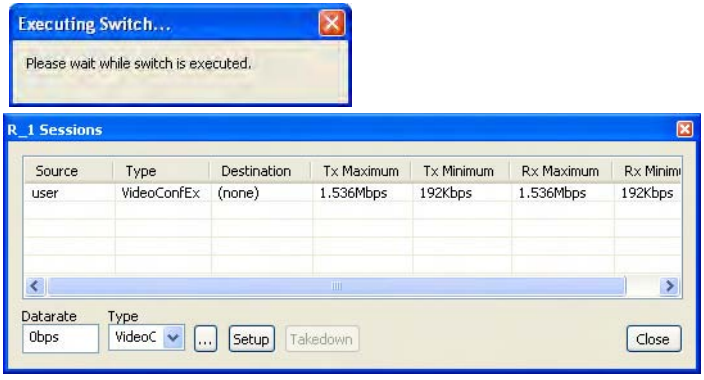


Figure 3-81 Manual Switch Execution

3. Click on the Group (or the Network, if no Group exists) to display the new site status for this Remote, figure 3-82. Note that the **Status** has changed from *None* to *Application*, and from *Home* to *Switched*. Also, the STDMA demod changed to the SCPC expansion demod.

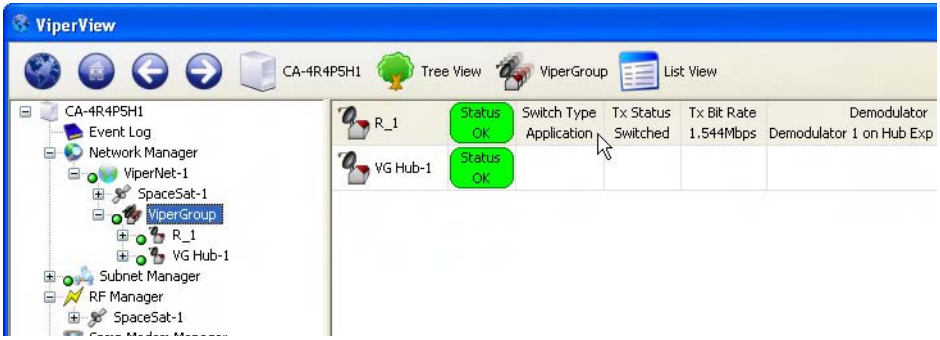


Figure 3-82 Remote Status in Group View

Tip: Turn on **Item Labels** using the command located under *List View* in the top menu bar.

If the switch attempt fails, then there is a network configuration error. The most likely reasons are:

- Invalid Policy Type
- Improper InBanding Configuration
- Incorrect Converter Frequency Settings
- Converters not Bound
- Incorrect Transponder and/or Bandwidth Pool Definition

Review the configuration procedure to identify and correct the mistake. If unable to resolve the situation, contact Comtech Vipersat Networks Customer Support for assistance (see “Customer Support” on page 1-12).

4. Observe the change in the Spectrum View (figure 3-83); a blue shaded area will appear representing the slot assigned by the VMS for the switch. Upon receipt of the next PLDM (Path Loss Data Message), the carrier(s) will appear showing the current E_bN_0 and bandwidth.

For P2P switching, two separate carriers (Tx and Rx) will appear for that site, as shown in this example.

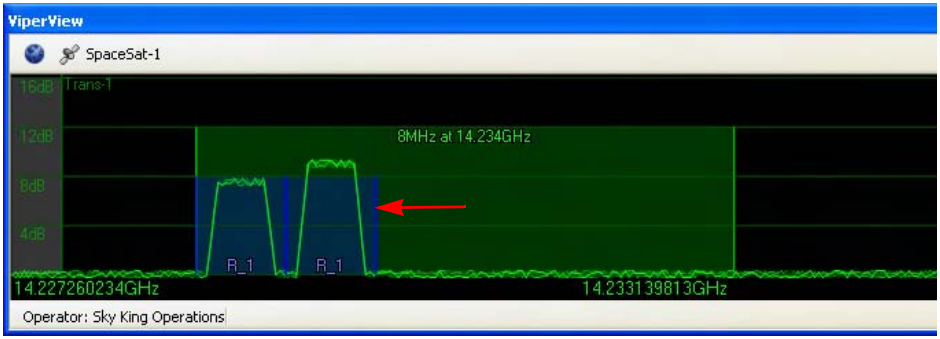


Figure 3-83 Switched Carrier, Spectrum View

5. Also, note the new entry in the Event View stating that the application switch was successful with the new data rate and frequency (figure 3-84).

For a Remote site that is configured for P2P switching, two entries will appear in the Event View: the first entry relates to the Remote modulator's Tx rate, and the following entry relates to the Remote demodulator's Rx rate.

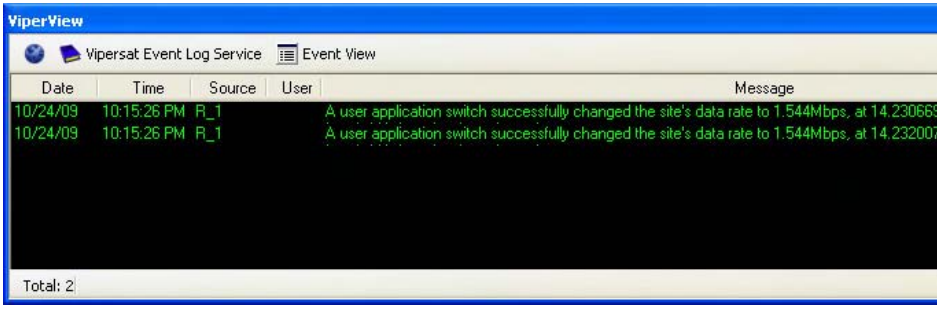


Figure 3-84 Switch Event, Event Log

6. From the *Tree View*, click on the Hub antenna under the Network Manager to display the Hub devices in the right window panel.

From this view, the operator can see the switched modulator and demodulator that the VMS selected for this session, the carrier frequency in L-Band, the bit rate, the current E_bN_0, and the identity of the Remote site (figure 3-85).

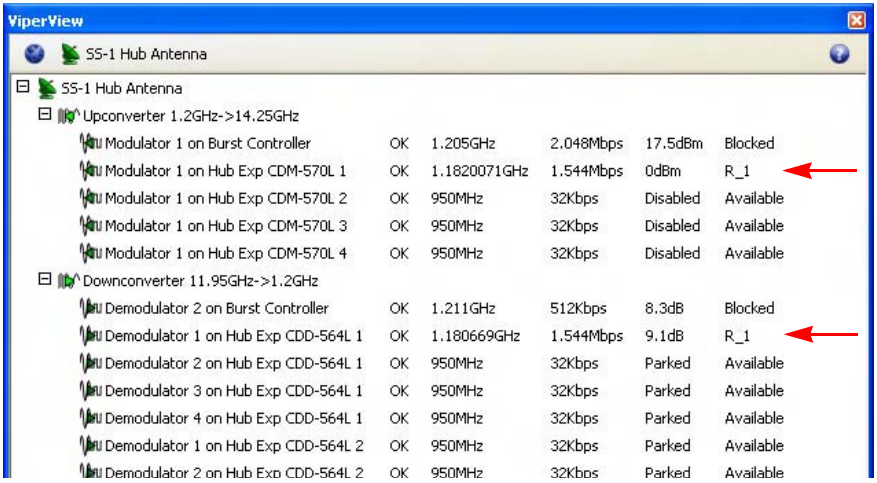


Figure 3-85 Switched Carrier, Hub Antenna View

7. End the session by selecting its appearance in the Application Sessions window and clicking on the **Takedown** button.

NOTE

Note: After reaching this point and all indications are as noted above, the Vipersat Manager, the RF Manager, and the Network Manager have been configured successfully. All frequencies and conversions are correct. To test the policies, it will be necessary to set up an application such as VoIP.

NOTE

Note: Additional (or all) Remote sites can be created and InBanded using the manual method described up to this point. However, it is recommended that, once the initial Remote site has been configured and can be used as a template reference, the remaining Remote sites be generated by utilizing the *Remote Site Wizard* feature as described below.

Remote Site Wizard

Creating and populating a Remote site with the use of the Remote Site Wizard tool greatly simplifies the process by directing the user with a scripted set of dialogs. And, by selecting an existing Remote site as a reference, a pre-defined default template is provided that automates the operation, allowing additional Remote sites to be generated rapidly.

Note: The procedure presented here utilizes the *reference site* feature. Although this is optional and a Remote site can be created without this step, the template approach is one of the most powerful features of the Site Wizard tool. Without it, additional operator/user input is required for configuration.

Caution: When specifying a Reference Site, be aware of the following restrictions:

Do not specify a reference site that utilizes a different *Network* and/or *Satellite* than the new site that is being created.

Although the reference site does not have to be in the same *Group* as the site that is being created, be aware that none of the reference site's inherited application policies will be copied to the new site in this situation.

1. Select **Create Remote...** from the Network (or from the Group, if the site is to be a member of an existing group within the network) drop-down menu, as shown in figure 3-86.

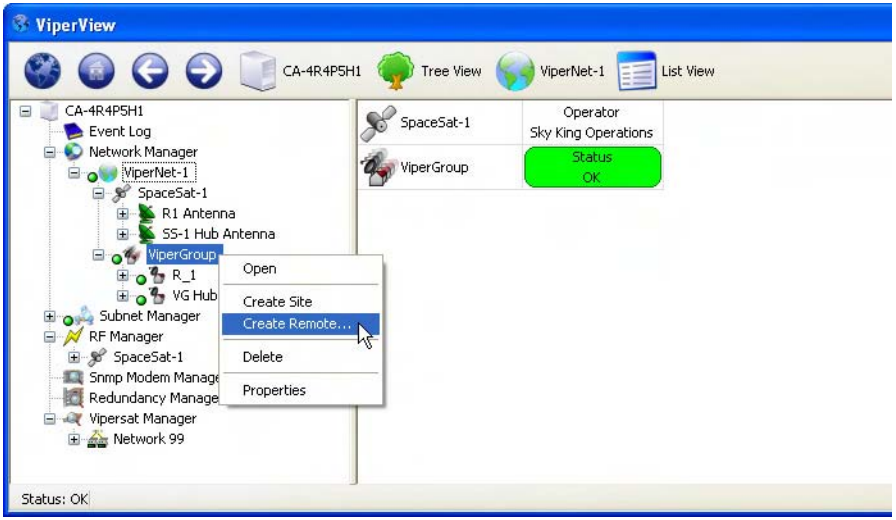


Figure 3-86 Create Remote... menu command

The **Remote Site Required Information** dialog will open, displaying a green pointer that guides the user to the fields which require input (figure 3-87).

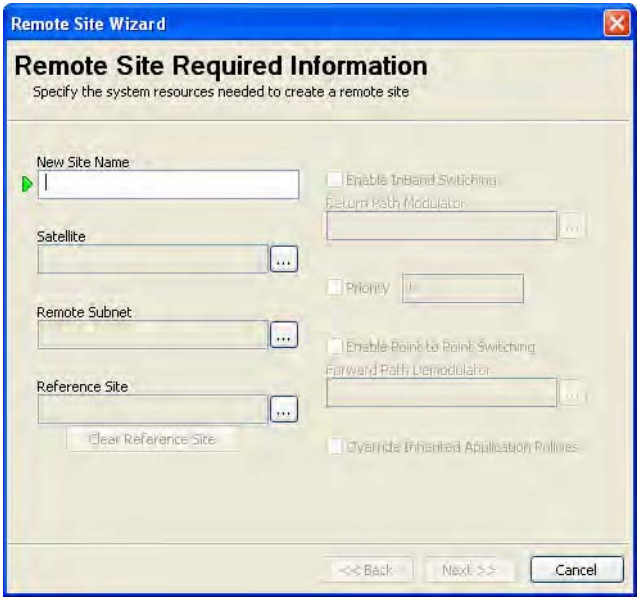


Figure 3-87 Remote Site Required Information, Create Remote...

2. Enter the **New Site Name**.

3. Select the **Satellite** to be used by this site (figure 3-88).

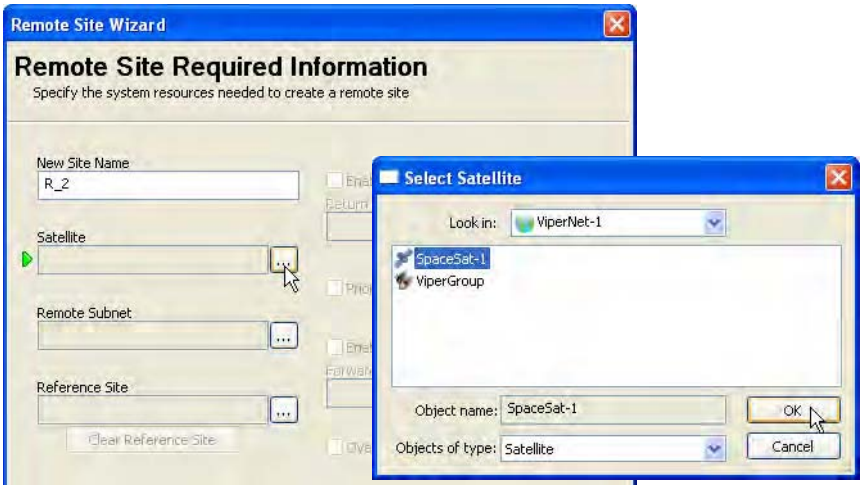


Figure 3-88 Select Satellite, Remote Site

4. Select the **Remote Subnet** for this site (figure 3-89).

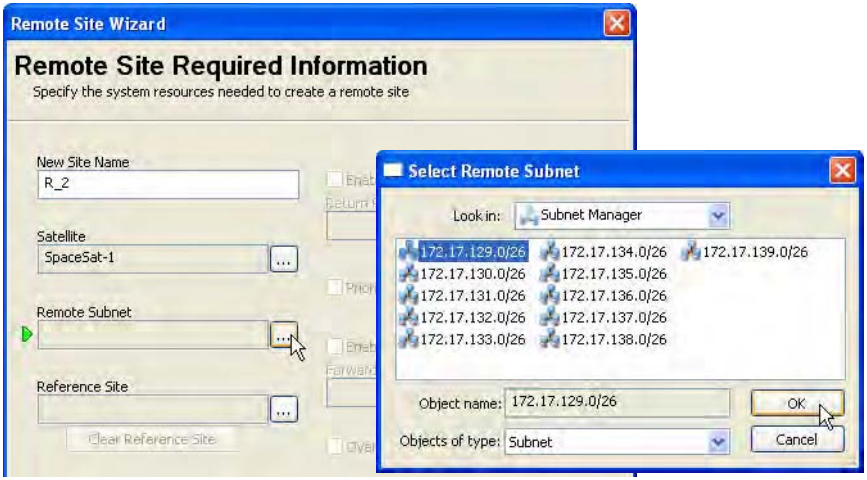


Figure 3-89 Select Remote Subnet

5. Select the **Reference Site** to be used as the template for building this Remote site (figure 3-90).

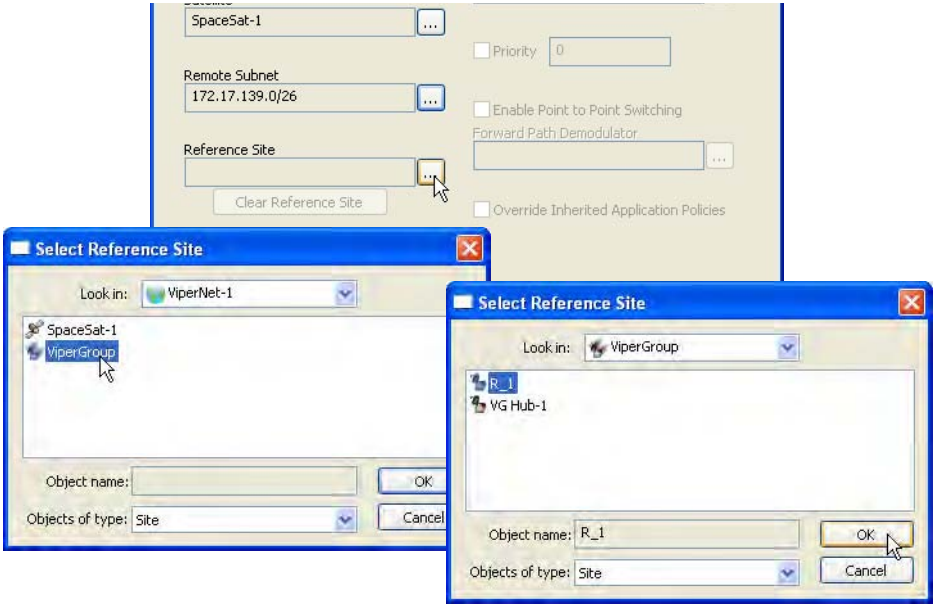


Figure 3-90 Select Reference Site

6. To InBand this site, **Enable InBand Switching**, then select the **Return Path Modulator** for this unit (figure 3-91). Continue with the next step.

If this site will *Not be InBanded*, proceed to step 9.

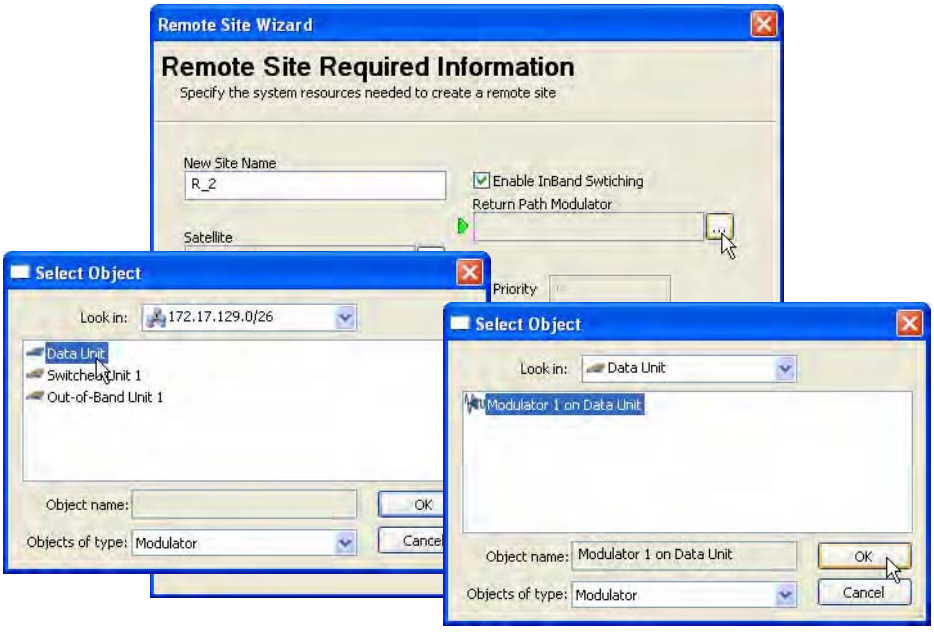


Figure 3-91 Select Return Path Modulator, InBand Switching

7. If required, set the **Priority** to be assigned to this site.

Note that a *lower* number corresponds to a *higher* priority level. The default value (0) equates to *No priority*.

8. To configure this site for **Point-to-Point Switching**, **Enable** the check box and then select the **Forward Path Demodulator** (the demod for this Remote data unit) to be used for this feature (figure 3-92).

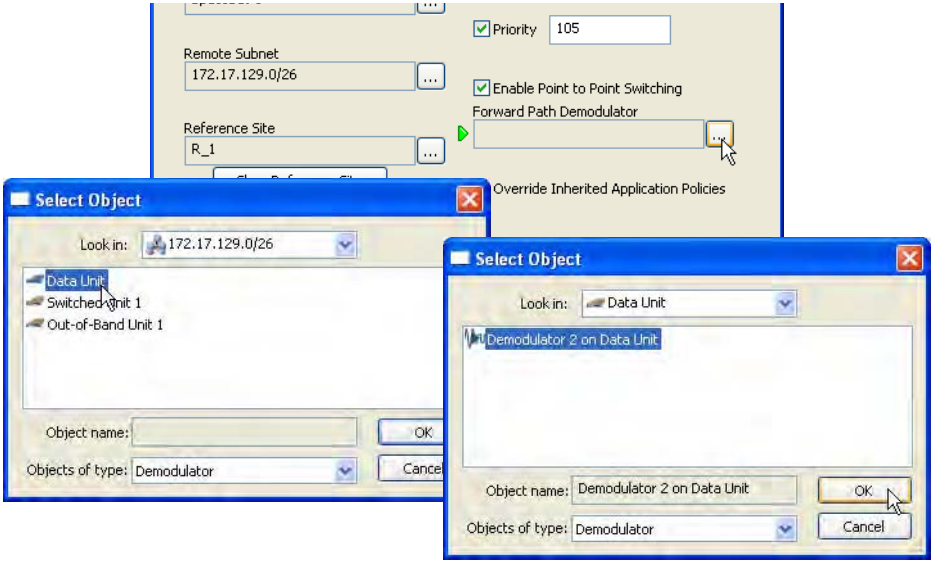


Figure 3-92 Select Forward Path Demodulator, P2P Switching

9. Click the **Next** button to proceed to the dialog for configuring the **Site RF Profile** (figure 3-93).

NOTE

Note: When a reference site has been specified, the template of that site's parameters will auto-fill these next dialogs, requiring modifications only to particular settings that differ for this new site.

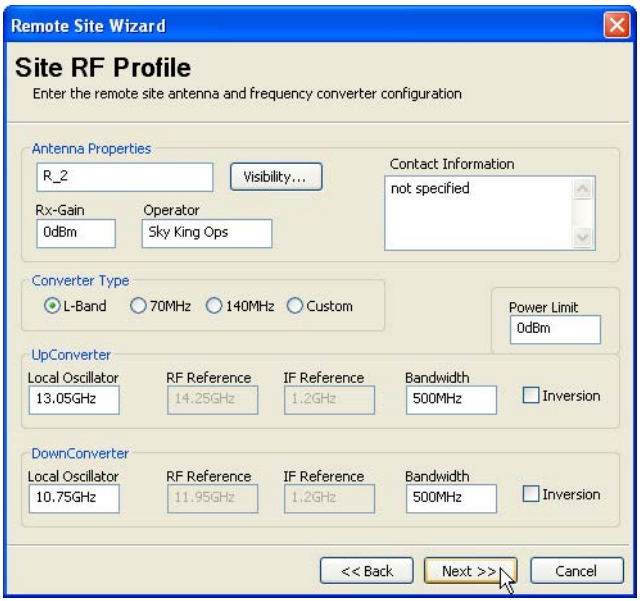


Figure 3-93 Site RF Profile, Create Remote...

10. Review the RF settings and edit this dialog if necessary, then click the **Next** button.

For *InBanded* sites, the **Return Path Home State Configuration** dialog will appear (figure 3-94). Continue with the next step.

For sites that are *not InBanded*, the **Ready To Create** window will appear (figure 3-99). Proceed to step 16.

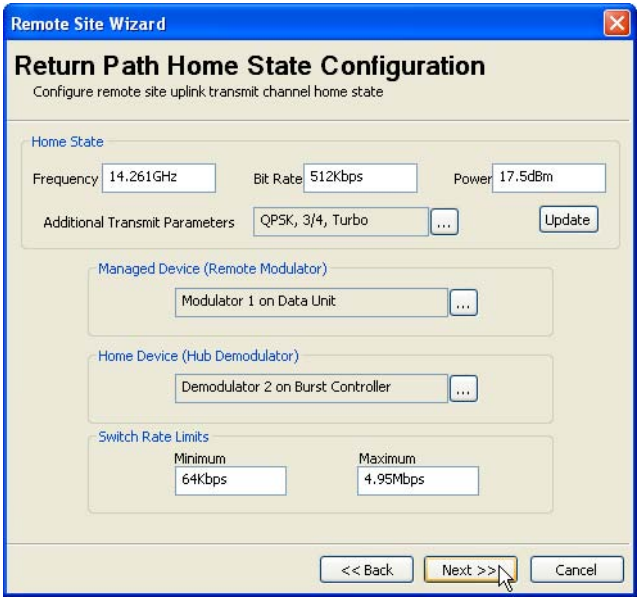


Figure 3-94 Return Path Home State Configuration, InBand

11. Again, this dialog is auto-filled from the reference site. Review and edit as necessary, then click **Next**.

For *Point-to-Point* sites, the **Forward Path Home State Configuration** dialog will appear (figure 3-95). Continue with the next step.

Otherwise, the **Return Channel Bandwidth** dialog will appear (figure 3-96). Proceed to step 13.

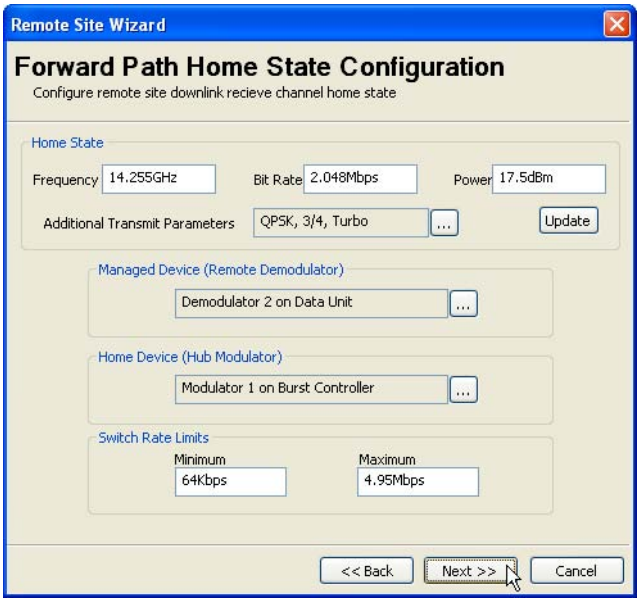


Figure 3-95 Forward Path Home State Configuration, P2P

12. Review and edit any fields as necessary, then click **Next**.

The **Return Channel Bandwidth** dialog will appear (figure 3-96), allowing guaranteed bandwidth reservations for this site to be specified.

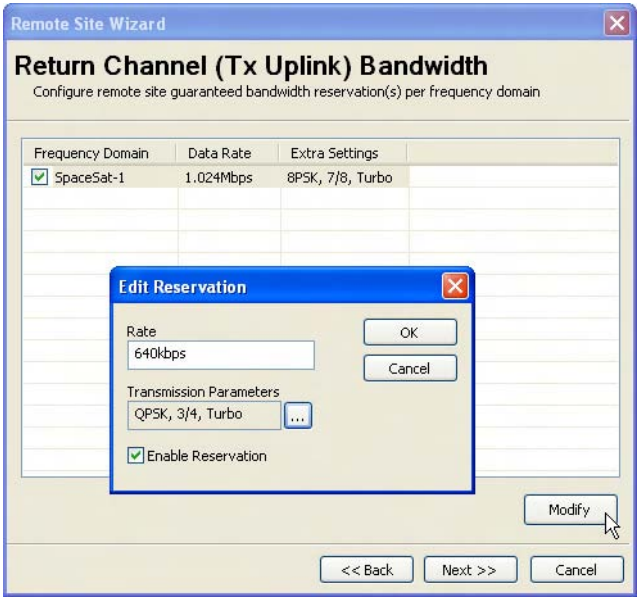


Figure 3-96 Return Channel Bandwidth, Create Remote...

13. By default, the guaranteed bandwidth reservations will match that of the reference site. Configure the reservations as required for this site, then click **Next**.

For *Point-to-Point* sites, the **Forward Channel Bandwidth** dialog will appear. Configure as required, then click **Next**.

The **Demodulator Settings** dialog will appear (figure 3-97), allowing the desired Demods at this Remote site to be flagged as allocatable.

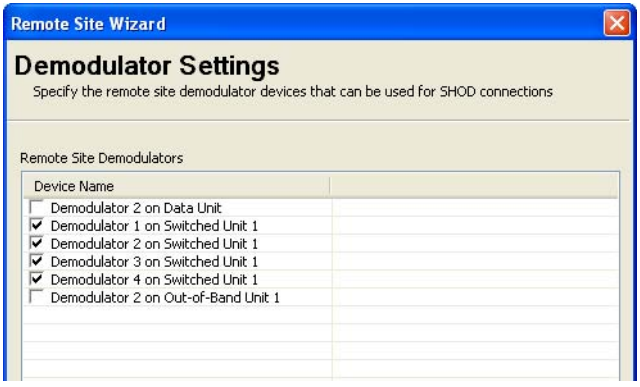


Figure 3-97 Demodulator Settings, Create Remote...

14. Specify any Demods to be used for SHOD/mesh connections, then click **Next**.

The next dialog to appear will be **Site Application Policy and Distribution List** (figure 3-98). Continue with the next step.

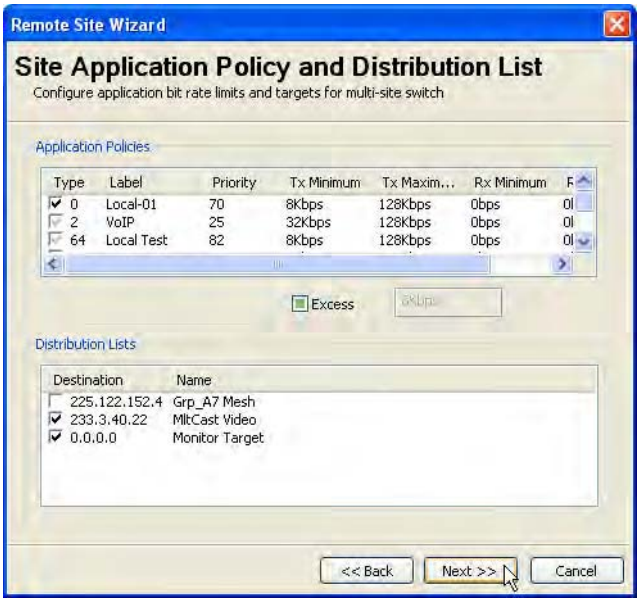


Figure 3-98 Site Application Policy and Distribution List, Create Remote...

15. Here, the user can modify any inherited policies or lists, or insert new local ones. Notice that the Local policies for the reference site will appear here also.

Proceed to the Site Wizard summary page (figure 3-99) by clicking **Next**.

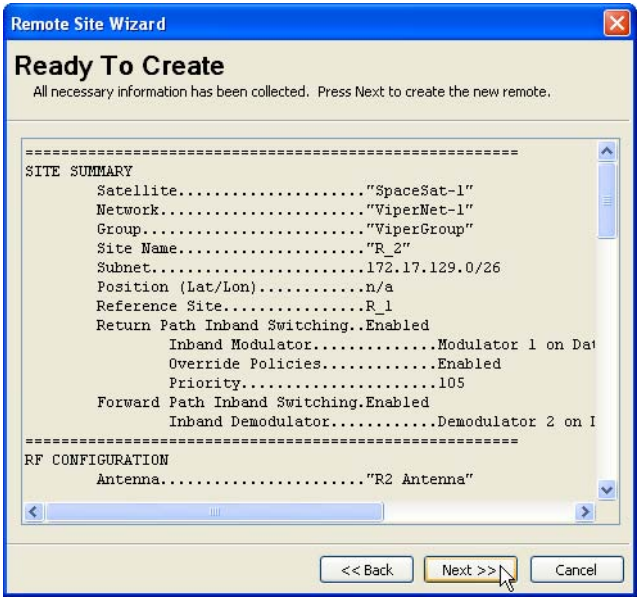


Figure 3-99 Ready to Create, Site Summary

16. With the **Ready To Create** summary page, the proposed configuration parameters for this site can be reviewed and, if necessary, the user can step **Back** to make changes prior to finalizing the creation process. After confirming the settings, click **Next** to create the new site.

If all settings are determined by the system to be acceptable, the **Site Creation Complete** window will appear (figure 3-100) with a *Site Creation Succeeded* message.

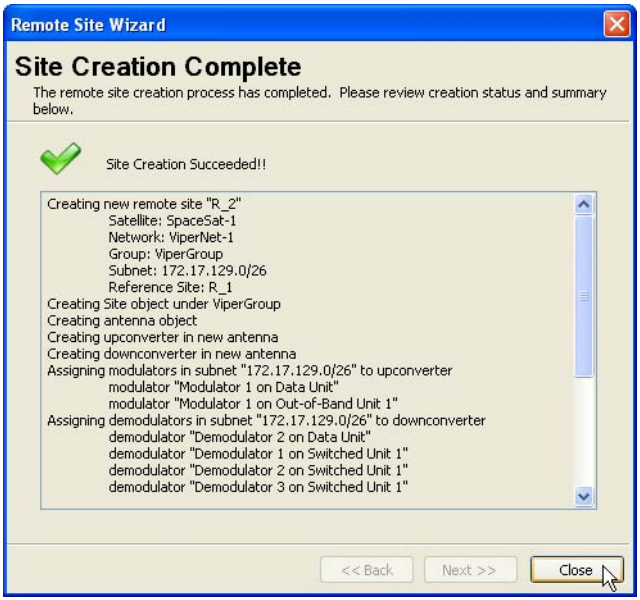


Figure 3-100 Site Creation Complete, Succeeded

Should some aspect of the proposed configuration not be accepted by the system, an error message will be displayed indicating that a reconfiguration is required before the site creation can be completed successfully.

Repeat the *Create Remote Site* procedure to generate additional network/group remote sites, as required.

Network Manager and ViperGlobe

The Network Manager provides a means of exposing the satellite network(s) to customers via VNO (for network operations) and ViperGlobe (for geographical display). The networks, and their associated elements, that are created in the Network Manager are *virtual*, and can thus be added and removed without affecting the actual networks upon which they are based.

ViperGlobe is an optional global network view application that is installed on VMS Client machines. The ViperGlobe option greatly enhances Network Manager by providing a geographical global representation of the Vipersat satellite network. ViperGlobe displays the networks that are created under the Network Manager and provides a visual global positioning of the network sites and the carrier links that exist between them. Network alarm status is also visually indicated in the globe view.

The operator can now anchor sites to true geographic locations. In an SOTM (Satcom On-The-Move) network, mobile sites are positioned based on GPS information received from the antenna ACU. An example of this type of network is depicted in figure 3-101, below.

Figure 3-101 Vipersat SOTM Network, Global Map View

This section describes the procedure for basic configuration of the Network Manager in the VMS, and graphically displaying the network using Viper-

Globe. For configuring an SOTM network, refer to the section “SOTM Configuration” on page 3-105.

1. From the Tree View, right-click on the Network Manager icon and select **Create Network** (figure 3-102).

2. In the Network Properties dialog that opens, enter a **Network Name** (*Vipersat Network* is used in this example).

3. Expand the Network Manager to expose the new Network icon.

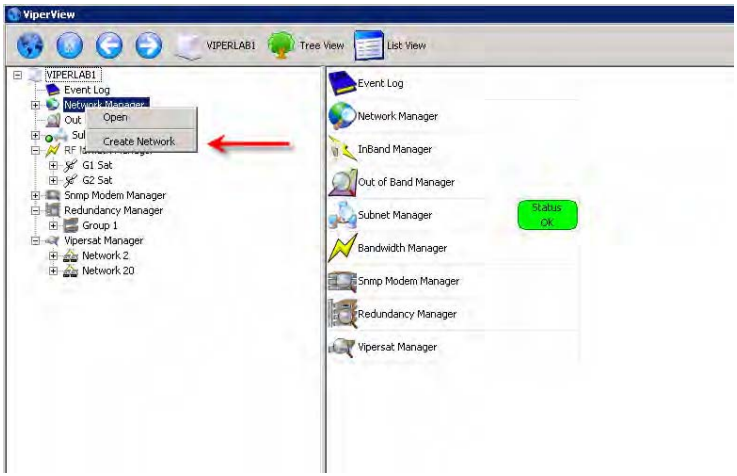


Figure 3-102 Creating the Network

4. Click-drag and drop the Satellite(s) for this network from the RF Manager onto the Network icon (figure 3-103).

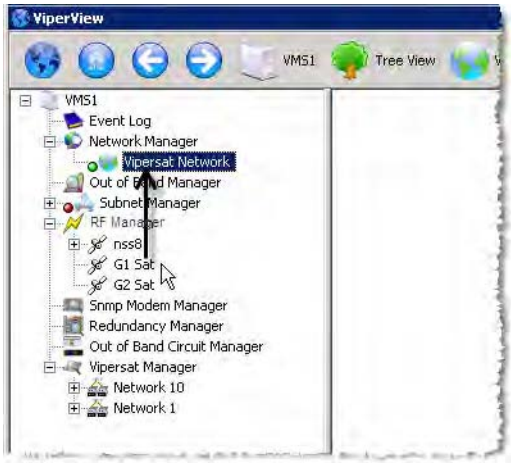


Figure 3-103 Click-Drag and Drop Satellite(s)

5. Open the ViperGlobe window from the *Start* menu, by selecting *Programs*, then *VMS*, followed by **Vipersat Network Globe**.

A Connect dialog will open, prompting for the **Server Name**. Enter the IP address of the VMS server and click **Connect**.

The ViperGlobe window will open, displaying the globe as seen in figure 3-104.

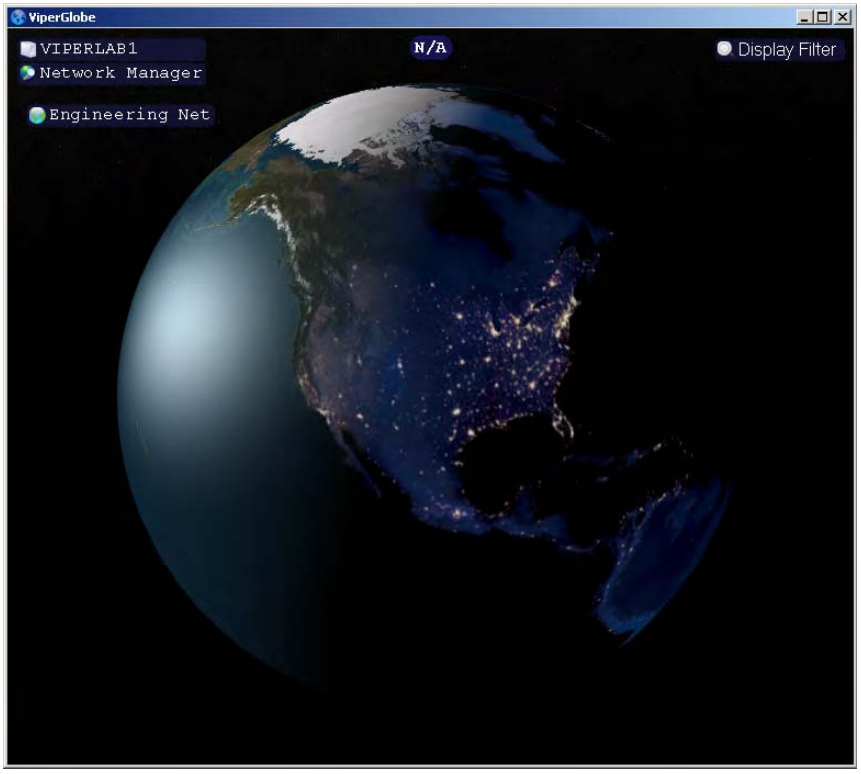


Figure 3-104 Globe View with Network Icon

Rotate the Globe by using the mouse to right-click-hold and drag to the desired position. Zoom in/out using the scroll wheel.

6. In the upper left corner of the window, the Vipersat network name will appear with a globe icon, just below the VMS Server name and Network Manager. Click on this icon to highlight it and make the network active.

The next step is to add the Sites, typically the Hub site and each of the Remote sites. This can be done by one of two methods:

- ViperView—Right-click on the Network icon under Network Manager in the tree view and select the **Create Site** command from the drop-down menu (figure 3-105).

  This method requires that the site coordinates for latitude and longitude be specified after the site is created, as described in a later step. Note that, if the Site coordinates are left at their default values (0.0N, 0.0E), the positioning of the Site as displayed in ViperGlobe will be arbitrarily assigned and will not be fixed.

- ViperGlobe—Right-click on the desired geographic location on the globe and select the **Create Site** command from the drop-down menu (figure 3-106).

  This method approximates the site coordinates for latitude and longitude based on the point where the mouse click occurs. The coordinates corresponding to the mouse position appear in the top center of the window as a reference.

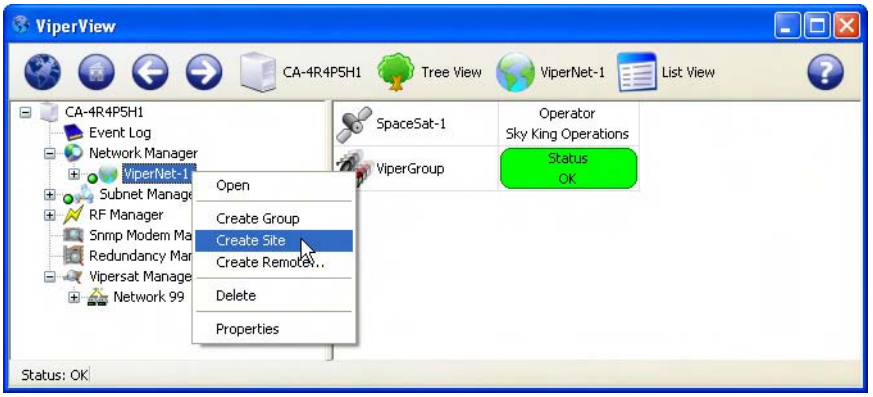


Figure 3-105 Adding Site, Network Manager

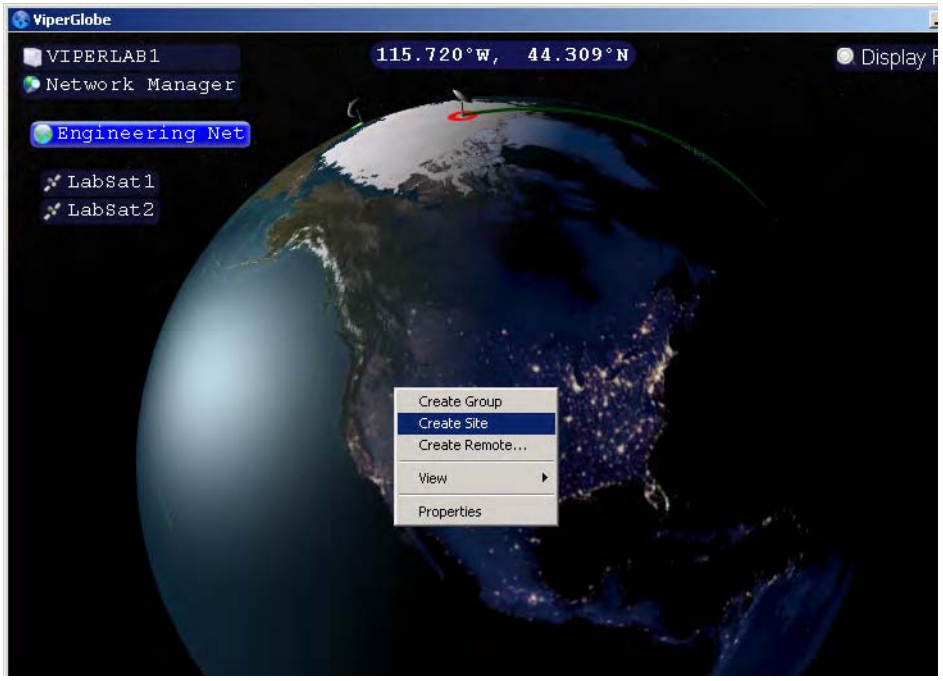


Figure 3-106 Adding Network Site, ViperGlobe

7. Execute the Create Site command and enter the **Name** to be used for this site.

In the Tree View, expand the Network to expose the newly created Site.

8. Right-click on the Site icon and select **Properties**.

Using the **Position** dialog, enter the exact coordinates for the Site.

9. After adding a site, click-drag and drop the associated **Antenna** from the Satellite Tree View onto the Site.

10. Once the Hub Site and at least one Remote Site have been added and populated with their antennas, a **Carrier Line** should appear between them (figure 3-107), assuming that the Sites are up and there is at least one active link.

Figure 3-107 Globe View with Linked Sites

In order to have the Sites in the Network Manager and on the Globe View indicate alarms, it is also necessary to drag and drop the subnet icons associated with each Site into the Network Manager.

11. Click-drag and drop the associated **Subnet** from the Subnet Manager onto the Site.

12. Repeat the above Create Site steps to create all desired sites for the Network.

Multiple Networks can be created under Network Manager by repeating the above procedure. Each of these Networks will appear as a separate network icon in the upper left corner of the globe window. When an icon is selected (click to highlight), the associated network element map will be displayed on the globe. All Sites created for the same Network will appear together in a single map.

Note that this procedure only covers a portion of what is required to configure the Network Manager, and is used to illustrate the functions in ViperGlobe. To perform the complete configuration, follow the sequence provided earlier in this chapter in *Network Manager Configuration*. The corresponding menu commands for ViperGlobe are displayed in the figures below.

Figure 3-108 Command Menu, VMS Server

Figure 3-109 Command Menu, Network Manager

Figure 3-110 Command Menu, Network

Figure 3-111 Command Menu, Satellite

As seen in figure 3-112, the command menu that appears when right-clicking on a globe Site includes these additional commands:

- **View**—displays a sub-menu that provides several viewing options that can be applied to the ViperGlobe window. The Show Names option displays the name for each site (figure 3-113). Other options include choice of Icon size, the geographic Detail level, and solar Lighting of the globe. View commands are accessible by right-clicking on any point on the globe.

- **Move Site**—provides a quick and easy means for coarsely repositioning an existing site. With this command, the operator simply clicks on the new location that is desired. For more accurate placement, the *Properties Position* page is used to define the specific coordinates for the Site.

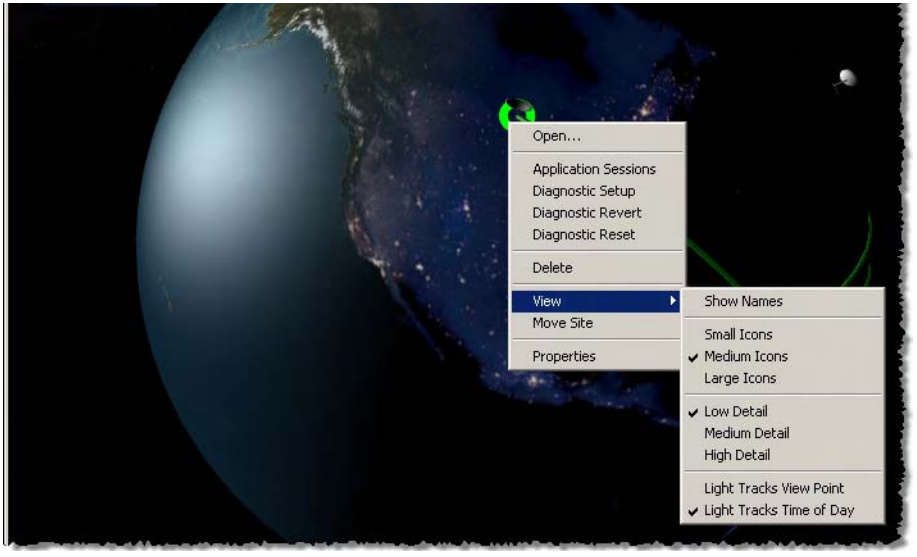


Figure 3-112 Command Menu, Network Site

Figure 3-113 Show Names Display

Advanced Switching Configuration

Overview

With the VMS Advanced Switching feature, the operator has the option of configuring multiple levels of modulation types and FEC code rates within the dynamic SCPC operation. Thus, more efficient bandwidth utilization can be realized.

An advanced switching table can be constructed for a remote modulator where specified modulation types and FEC code rates are paired with set data rates. Each data rate is associated with a Mod/Code and, as the system achieves the set rate, the transmission is modified to the new higher- or lower-order modulation setting specified for that rate. For each table entry, the VMS calculates an optimized switching threshold that the system uses to assign the most efficient bandwidth in an advanced switching environment.

As a switch request is processed, it is compared to the Advanced Switching table. If the requested data rate crosses a threshold where the higher-order modulation actually becomes more bandwidth efficient, the switch request will go up to the higher-order modulation at the lowest bit rate that exceeds the request. Thus, it is possible that a *higher* bit rate can be granted while actually utilizing *less* bandwidth resources.

For example, a site currently operating at QPSK 3/4 that generates a switch request for 192 kbps will be switched up to 256 kbps at 8PSK 7/8, provided this modulation and code rate was specified in the Advanced Switching table entry for this switch point.

The following equations illustrate this scenario:

QPSK 3/4 @192 kbps @1.3 spacing:

Allocated Bandwidth = 192 x (1/2) x (1/.75) x 1.3 = 166.4 kHz

8PSK 7/8 @256 kbps @1.3 spacing:

Allocated Bandwidth = 256 x (1/3) x (1/.875) x 1.3 = 126.781 kHz

Roaming with Advanced Switching

A roaming remote (SOTM) can take advantage of the Advanced Switching function when transitioning from one satellite beam to another. Switching tables for a remote can be configured on a per satellite region basis and, upon entering into a new service area, the remote forwards the designated table for that area to the VMS. This dynamically updates the modulator transmission settings on each transition.

Refer to the *ROSS User Guide* for additional details on the configuration and use of the Advanced Switching feature in a roaming application.

NOTE

Note: Site link power budgets must be in compliance to operate higher-order modulation/code rates.

When using Guaranteed Bandwidth in conjunction with Advanced Switching, there are important considerations which should be taken into account when performing the configuration of these features. Refer to the section "Considerations for Using Guaranteed Bandwidth with Advanced Switching" on page 3-66.

Configuration

Advanced Switching ModCods can be configured for Transmit (when return path switching is enabled) and/or Receive (when forward path switching is enabled) for a Remote site.

1. Open the Properties dialog for the Remote site and select **ModCods** from the tree menu (figure 3-114).

2. Click on the **Insert** button to create a new Advanced Switch table entry, and enter the requested **Bit Rate** for the switch.

3. To use new Mod/Code parameters (different from the default settings) for this switch, click on the **Additional Transmit Parameters** (**...**) button.

   This will open the dialog for entering the desired Modulation and FEC values for this entry (figure 3-115).

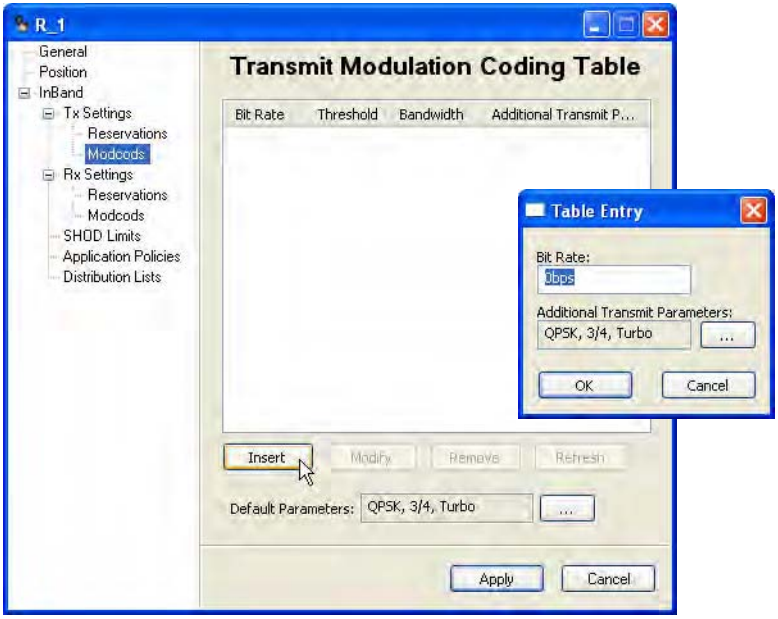


Figure 3-114 Advanced Switching dialog

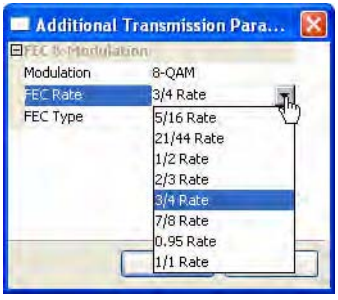


Figure 3-115 FEC & Modulation Parameters

4. Click on **OK** to record this entry in the table.

5. Repeat this process to create additional entries for this site, as required.

6. Entries can be revised by selecting the entry and using either the **Modify** button or the **Remove** button.

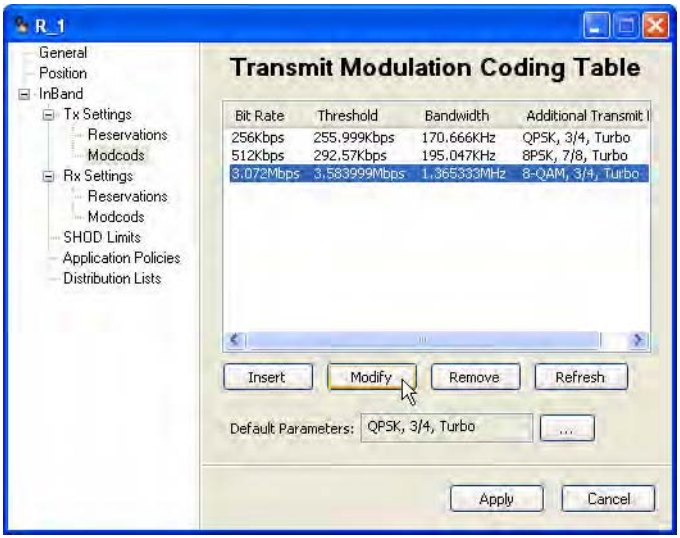


Figure 3-116 Revisions to AS Table Entries

Redundancy Configuration

N:M Device Redundancy

If device redundancy for hub primary modems is desired, it should be configured at this point. Complete instructions for configuring this feature can be found in Appendix C, "Redundancy".

VMS Redundancy

If VMS server redundancy is desired, it should be configured at this point. Complete instructions for configuring this feature can be found in Appendix C, "Redundancy".

SOTM Configuration

This section applies only to those networks with mobile platforms, such as a maritime environment, which are referred to as roaming or SOTM (Satcom On-

The-Move). The VMS incorporates automated features to seamlessly handle configuration changes inherent to a mobile environment. If a platform transitions to a new satellite, the VMS will automatically move the associated antenna, update the Inband Home State, and remove and rewrite the appropriate routes in the old and new TDM outbounds. QOS rules applying to the TDM outbound for the remote site will be moved as well. If the transition involves moving to a different hub, the modems will generate RIPv2 updates to the edge routers providing a path to the Internet.

This process is illustrated below, in figure 3-117. Configuring this feature requires that sites are on-line.

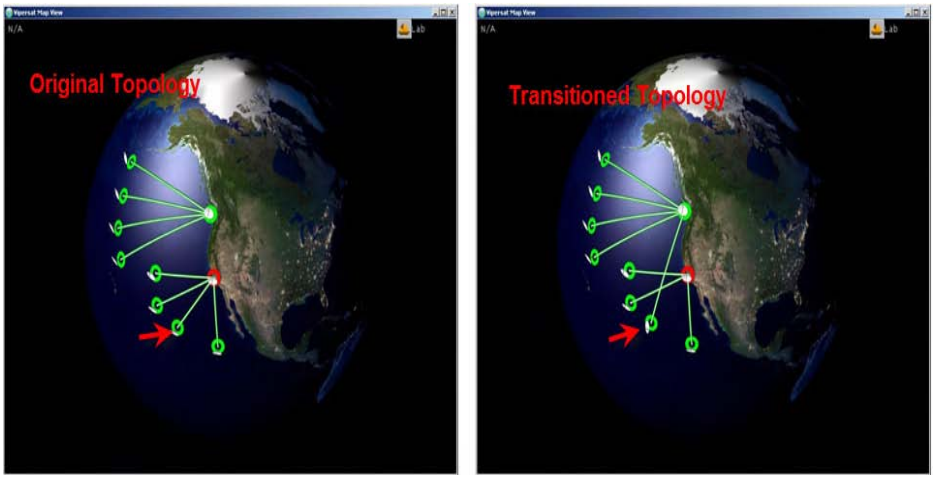


Figure 3-117 SOTM Transitioned Site

1. Open the Vipersat Map View and highlight the Network icon to make the network active.

2. Right-click on a mobile Remote site and open the **Properties** window (figure 3-118).

Figure 3-118 Enable Dynamic Function for SOTM Remote

3. Check the **Dynamic** box and select the browse button beneath it. This will open a dialog box in which the site antenna and subnet should appear (figure 3-119).

Note that, if the subnet icon was not copied into this site as described in *Network Manager Configuration*, it will not appear here.

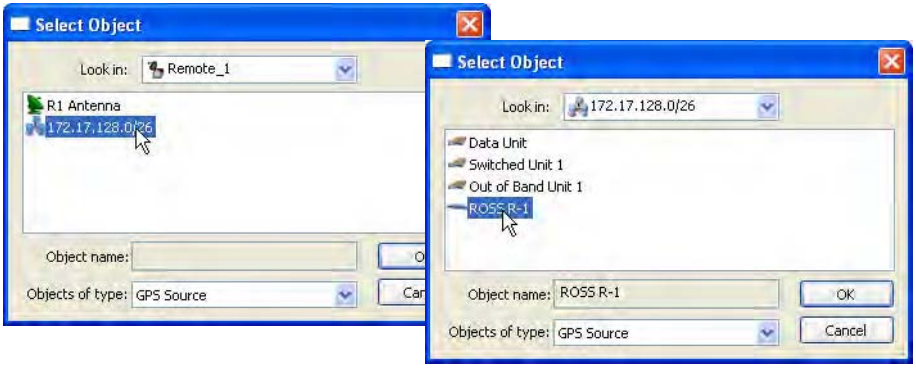


Figure 3-119 Selecting ROSS Unit for SOTM

4. Double-click on the **Subnet** to display the subnet components.

5. Select the **ROSS** unit and click **OK**.

6. The selected ROSS unit will appear in the remote's Properties dialog. Click **Apply** and Close the window.

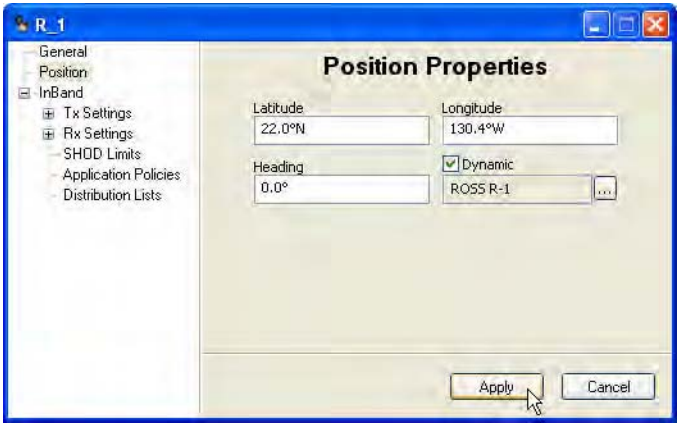


Figure 3-120 SOTM Remote Configured

At this point, the Remote site icon will snap to a location on the globe based on the GPS reading that the ROSS is receiving from the antenna.

7. Repeat the above procedure for all mobile remote sites.

The next step will be to set up the VMS to push the routes to the TDM outbounds. This step is necessary if there is more than one satellite–or satellite beam–being used in the network, or if multiple TDM outbounds are being used and the mobile sites will transition between them.

It will no longer be necessary to put static routes in the TDM modems. If any static routes exist, either telnet/console into the box(es) or use the Parameter Editor from the VMS and delete them. The only routes left in the TDM outbounds should be the Default Gateway to the edge router and any non-mobile remotes in the network (if desired, these routes can also be entered as *dynamic* VMS routes).

8. Right-click on the Hub modem unit that represents the first TDM outbound and select the **Properties** page.

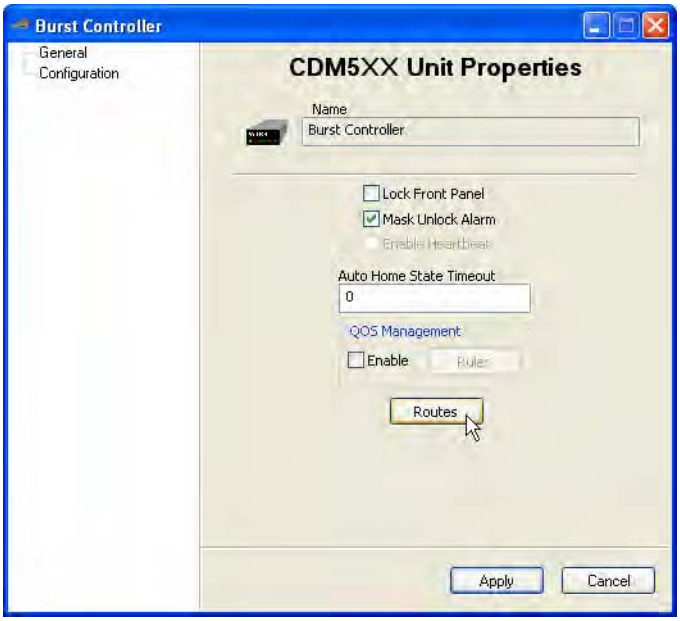


Figure 3-121 TDM Properties, Routes

9. Click the **Routes** button. The Routes window will open (figure 3-122).

Right-click in the window and select **Insert**.

A new route is added to the Route List. The operator can then edit the route settings, including the *Network* address, the *Mask*, the *Gateway*, and the *Interface* (next hop). For remotes, select **Satellite** as the interface.

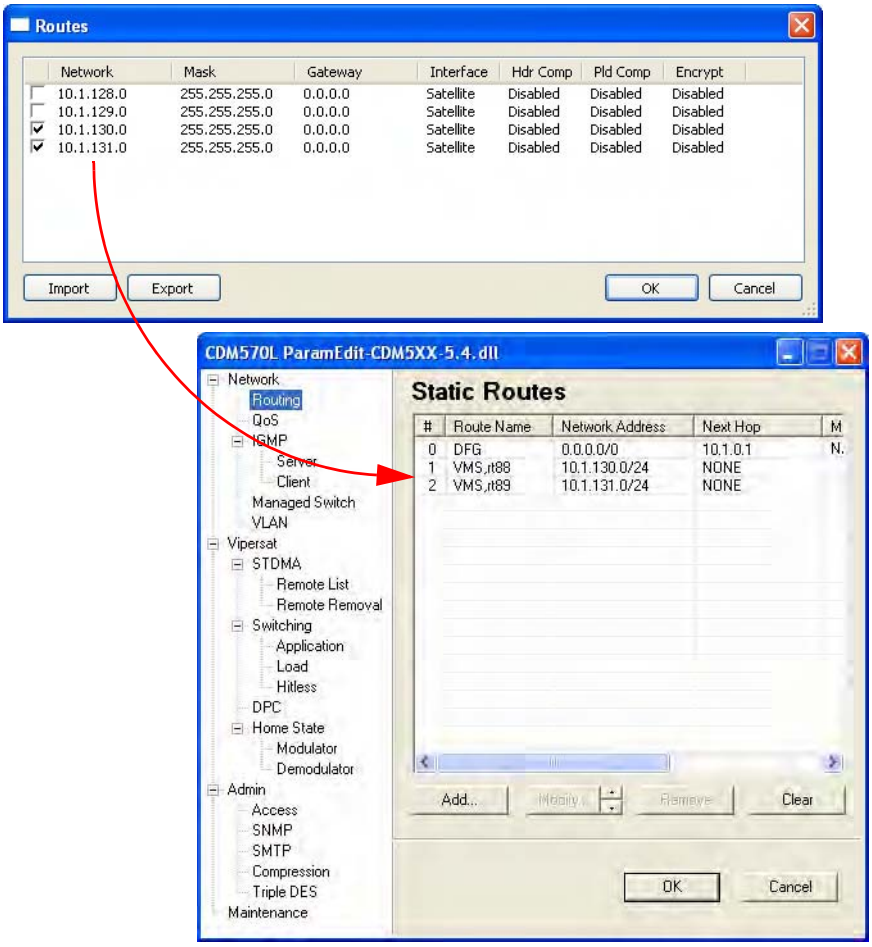


Figure 3-122 Dynamic Routing Entry, CDM-570/570L

10. Push the new route to the modem with a **Force Registration**. The modem will generate a RIPv2 update to the router identified as its default gateway.

This can be verified by right-clicking on the modem, selecting **Configure**, then opening the **Routing** tab as shown in the figure.

11. Repeat this route procedure for each TDM outbound modem.

If Quality of Service rules apply, configure them now. Typically, QOS rules in the TDM will be configured for Min/Max priority. This gives each remote a CIR (min rule) in the TDM outbound and a burstable rate (max rule). Since the number of rules per modem is limited to 32, these rules should be moved to the

currently active TDM outbound. Configure QOS rules for the remotes that use this modem as their “home” TDM.

12. Right-click on the Hub unit with the first TDM outbound and open the **Properties** page.

13. Enable QOS Management by checking the box, then click on the **Rules** button (figure 3-123).

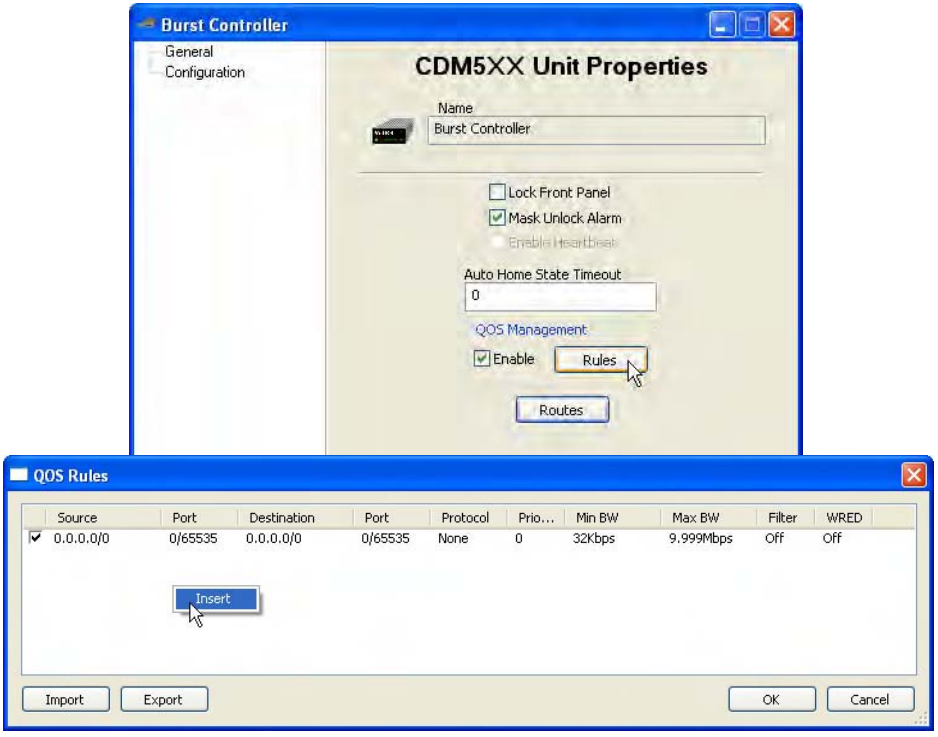


Figure 3-123 QOS Rules Configuration, CDM-570/570L

14. Right-click in the QOS Rules window to **Insert** a rule, then edit the rule settings that will apply to the remote.

When the remote transitions to a new TDM outbound, these rules will transition with it.

15. Apply these settings to save this configuration for the Hub TDM unit.

Encryption Configuration

Management Security Option

Note: The Management Security feature is not provided with standard VMS installations, and is available only upon request and through an authorized agent.

This feature requires the use of a specially programmed Crypto-Key.

Management Security is an optional software module for the VMS that protects the M&C messages that pass between SLM-5650A modems and the VMS over exposed LAN/WAN segments within the network. Encryption key management operates through manual key distribution, with M&C keys entered in the VMS and at each modem associated with the VMS.

A Switching encryption option for VESP is included in this security feature as well.

Encryption is based on the FIPS approved Advanced Encryption Standard (AES), a block cipher algorithm, using a 128-bit fixed block size and 256-bit keys.

1. Open the Properties window for the VMS Server and select the **Encryption** dialog, as shown in figure 3-124.

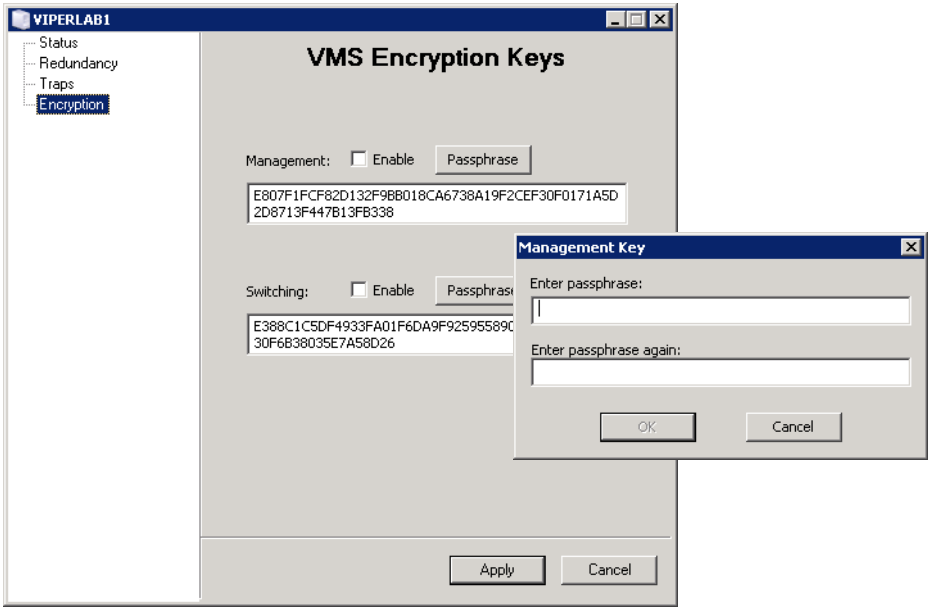


Figure 3-124 VMS Server Properties, General dialog

Here, Management and/or Switching encryption can be **Enabled**.

NOTE

Note: Take care with the sequence that is followed for enabling/activating the encryption feature. To minimize disruptions to network operations, enabling encryption in the VMS should be performed only after modem encryption has been enabled.

Refer to the *Vipersat SLM-5650A User Guide* for information on setting the Management Security feature in the modem.

2. Set the encryption key(s) by either entering a 64 character ASCII hex string (as depicted in the figure), or clicking on the **Passphrase** button and entering a passphrase in the pop-up dialog.

An MD5 cryptographic hash function translates the passphrase into a 128-bit hash value.

Note that the key entered here for Management must match the key that is entered for each modem that has encryption enabled.

The key for Switching is entered here only, and is automatically passed on to the modem by the VMS for VESP operations.

3. Click on **Apply** then Close the window.

Modem TRANSEC Setting

(*Applies to only Vipersat networks that use SLM-5650A modems*)

When using Transmission Security encryption, the VMS modem setting must be configured to match the setting used in the SLM-5650A modem itself. Perform the following procedure for each modem to be configured for encryption.

1. Open the **Properties** window for the SLM-5650A modem (figure 3-125).

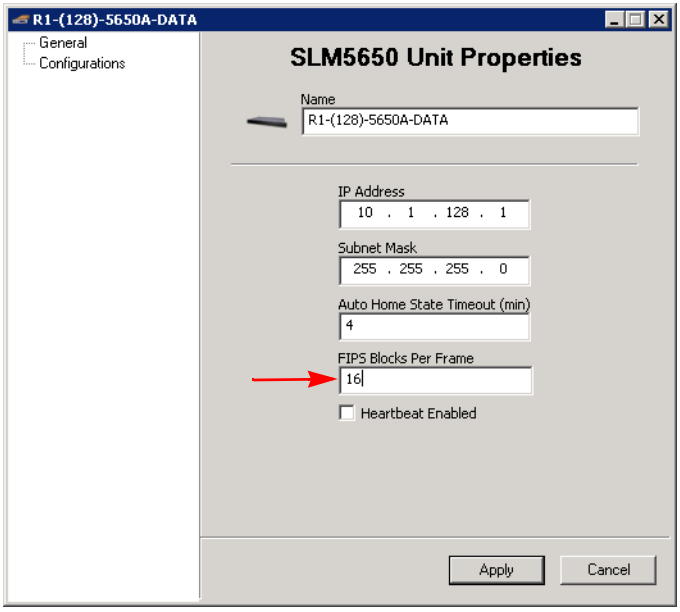


Figure 3-125 Properties Window, SLM-5650A Modem

2. Enter the number of blocks used for encryption in the **FIPS Blocks Per Frame** parameter field.

In the SLM-5650A modem, this parameter is specified on the Admin/Config page as the Encryption Frame Length in 16 Byte Blocks.

3. Click on **Apply** then Close the window.

This concludes the VMS Configuration.

CHAPTER

4

CONFIGURING NETWORK MODEMS

General

This section describes using VMS to configure Vipersat network modems. Configuration of modem parameter files is accomplished using the Parameter Editor. The Parameter Editor, as used from the VMS, performs the same functions as the Parameter Editor accessed via Vipersat's VLoad utility. The uses of the Parameter Editor in VMS and VLoad differ, however, in the way the edited parameters are stored and applied.

For example, once a modem/router parameter has been changed by the VMS, clicking the OK button on the edit screen causes the change to be implemented immediately in the modem. The same change made using VLoad will not be implemented in the modem until the modified parameter file is uploaded or "put" to the subject modem/router.

The parameter modifications may also be made directly to the modem using either a console, Telnet, or HTTP connection. Refer to the modem's documentation for details on configuring modem equipment using one of these methods.

The settings of any network modem/router can be configured or modified using the VMS. Right-clicking on a device icon will display a drop-down menu showing the options that can be exercised for the device (figure 4-1).

The following describes the actions for each item/command on the drop-down menu.

Note: Many of the parameters interact with each other. Before making a change to a parameter, carefully read the instructions and note any interaction with other parameters.

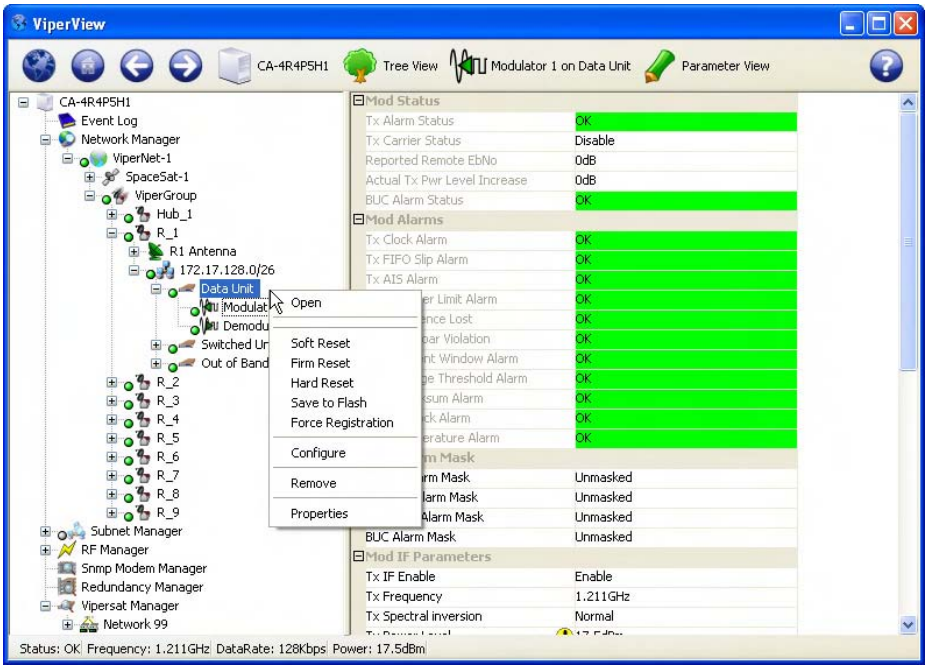


Figure 4-1 Modem Equipment Drop-Down Menu, ViperView

- **Open –** This item causes the selected modem/router to pop open a separate window displaying the device parameters for the unit.
- **Soft Reset –** This command causes the selected modem/router to perform a refresh of all latched alarms, clearing all internal table entries.
- **Firm Reset –** This command overwrites active memory in the modem/router with the contents of the unit's flash memory and executes it.
- **Hard Reset –** This command causes the modem/router to do a complete process reset. Performing a hard reset is similar to power cycling the unit.
- **Save to Flash –** This item will save all volatile configurations to the modem/router's flash memory. Anytime an operator makes a change to communication and operating parameters, it is necessary to save the changed information/configuration.

NOTE

Note: Save to Flash saves information in the selected modem/router, not in the VMS database.

- **Force Registration –** A modem/router is normally automatically registered on the network as part of the initial setup process. If this process fails, this command will force a registration attempt.

- **Configure –** This item will open the Parameter Editor, allowing configuration changes to the unit.
- **Remove –** This command deletes the device container from the VMS configuration database, removing it from selected view.
- **Properties –** This command allows access to the **General** and **Configuration** tabs for the selected unit.

Hardware Configuration

Refer to the user documentation for each modem/router in the satellite network for details on the physical installation of the device. The hardware documentation also has detailed information on using either the unit's front panel controls or a Telnet connection and the command line interface for directly configuring the target modem/router.

Configuring a Network Modem

A modem/router, when controlled by the VMS as part of a communications network, has its performance automatically controlled as VMS monitors the modem/router's role and performance in the network. VMS then commands the modem to modify its configuration, as needed, to optimize network performance.

In addition, the modem portion of each modem/router in a network can be controlled manually. Using the CDM-570/570L as an example, the listing in table 4-1 is typical of the information available in a modem/router's user documentation.

Each modem/router will have its own unique user interface and connection methods. Check the modem's documentation for details.

Note: Not all modem functions may be controlled by the VMS. Refer to the device's user documentation for instructions for using functions not available through the VMS.

Table 4-1 CDM-570/570L Modem/Router Manual Connection Options

User Interface	Connection	Modem Functions	CDM-570L Functions	Related Manual Chapters
Front Panel	Local - Keypad	ALL	IP Address/Subnet Mask only	Chapter 6
Serial Remote Control	Local - Serial RS-232 Remote Control Port	ALL	IP Address/Subnet Mask only	Chapter 14
Serial Command	Line Interface (CLI) Local - Serial RS-232 via Console Port	ALL	ALL	Chapter 17
Telnet	Local or Remote - Ethernet via 10/100 BaseT Traffic interface	ALL	ALL	Chapter 17
Web Server	Local or Remote - Ethernet via 10/100 BaseT Traffic interface	ALL	ALL	Chapter 18
SNMP	Local or Remote - Ethernet via 10/100 BaseT Traffic interface	ALL	ALL	Chapter 19

CHAPTER

5

VMS SERVICES

General

This section covers using the various Services that make up the VMS, the satellite network management system with an intuitive, user-friendly, graphical user interface which displays:

- Monitor and Control functions that ontinuously update network health and status
- Multiple networks managed from a single server
- Centralized network configurations
- Organized network layouts
- Automated equipment detection
- Intuitive drag-and-drop bandwidth management and configuration
- Roaming / Satcom-On-The-Move (SOTM)

The following sections describe the system services which, working together, form the VMS.

ViperView—Monitor and Control

ViperView and the VMS Services function to monitor and control network operations as well as to provide an interface for the administrator/operator to manage and perform modifications to the network.

Caution: In a redundant VMS configuration, when any changes are made to the VMS database, a **Synchronize** command should be executed (available by clicking on the Server icon, as shown in figure 5-1). This step is required to ensure that any changes made to the Active server are also made to the Standby server(s).

Figure 5-1 Synchronize Command

Multiple Views

VMS supports opening multiple ViperView window views, as shown on the sample screen in figure 5-2, allowing the operator to monitor several network services at once. These window views can be sized and positioned as desired.

The ViperGlobe and each of the ViperView child windows are constantly updated by the VMS, giving the operator real-time views of the current status of the network.

To open a child window, right-click on the Service or device appearance in the Tree View and select the **Open** command.

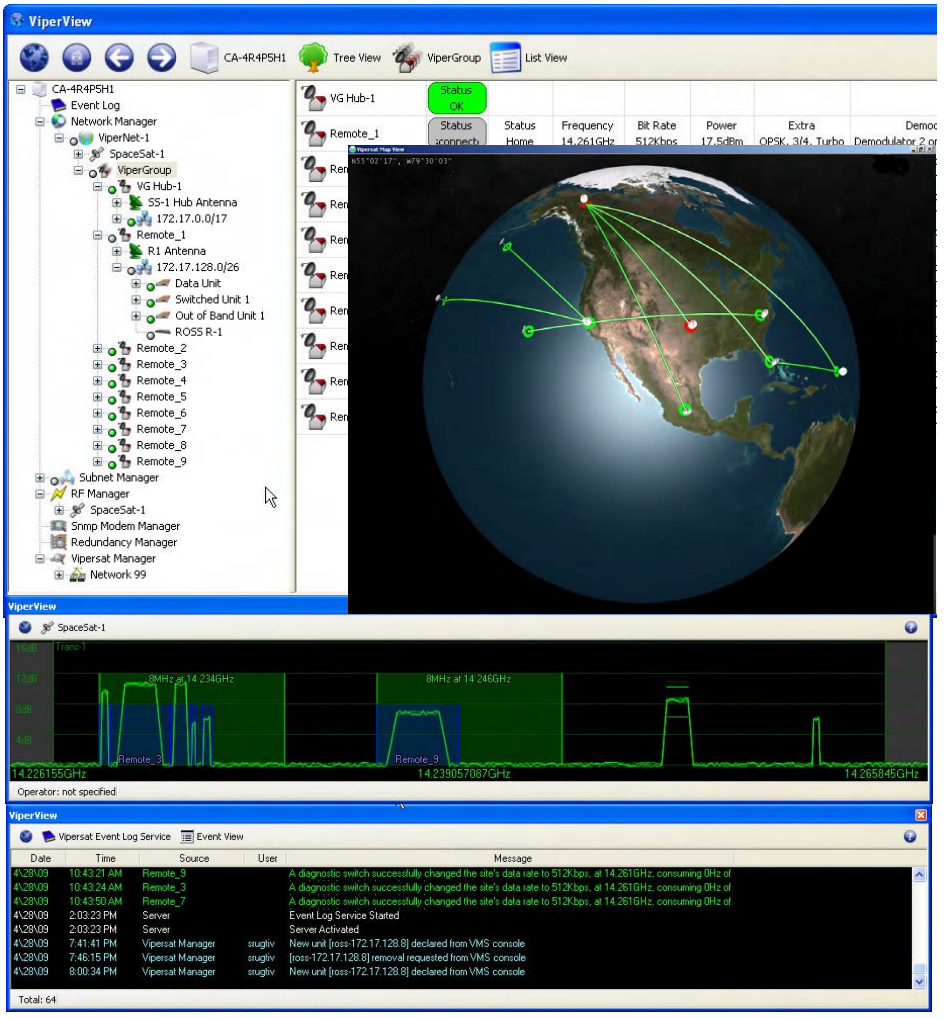


Figure 5-2 ViperView, Multiple Window Views

For example, the **Network Manager View** shown in figure 5-3 can be opened to display the current switch type, status and bit rate for both Tx and Rx, and the assigned Demods and Mods of all network remote members in a Group.

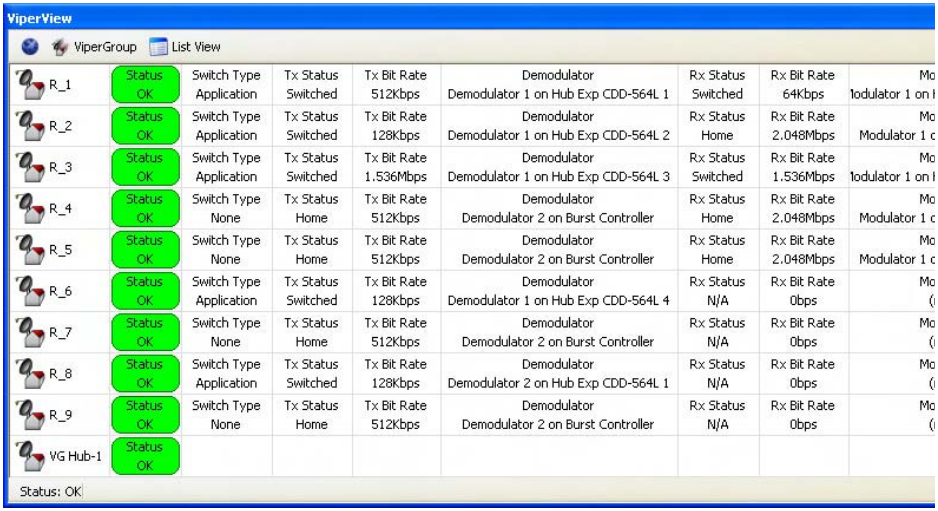


Figure 5-3 Network Manager, Group View

Similarly, the **Antenna View** displays the current status of a site's Modulators and Demodulators, as shown for the Hub site in figure 5-4.

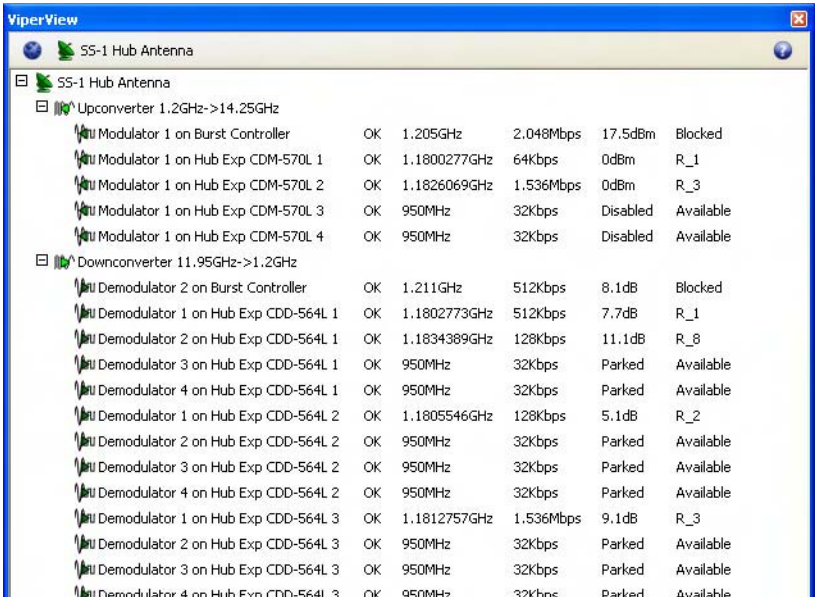


Figure 5-4 Antenna View, Hub

NOTE **Note:** The Antenna View shows L-Band frequencies.

Tip: Each List View within ViperView presents the option to turn **Item Labels** either On or Off via the the command located under *List View* in the top menu bar. When set to Off, smaller element icons and the absence of table cell labels result in a more compact view.

The Network Manager Group View example shown in figure 5-3, is displayed with Item Labels turned *On*.

Use the Event Log to stay current on recent network activity, as shown in the **Event View** window shown in figure 5-5.

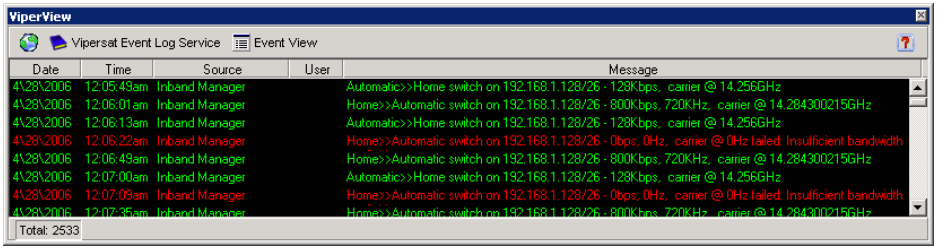


Figure 5-5 Event View

The Event View lists the details of network configuration changes, alarms, and switch events.

The **Spectrum View** displays a simulated spectrum analyzer, shown in figure 5-6, letting the operator monitor carriers and pools. The Spectrum View reports E_bN_o, space segment usage, and pool slots assigned by the VMS.

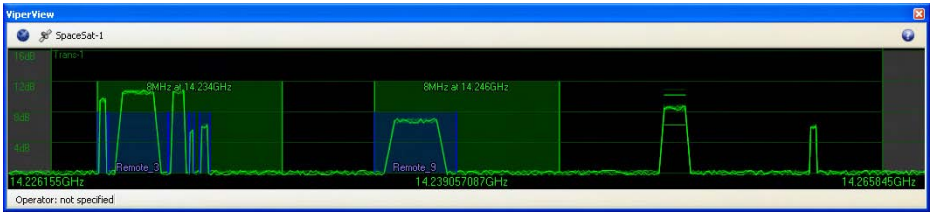


Figure 5-6 Spectrum View

The **Parameter View**, shown in figure 5-7, constantly supplies the operator with updated information for a selected unit.

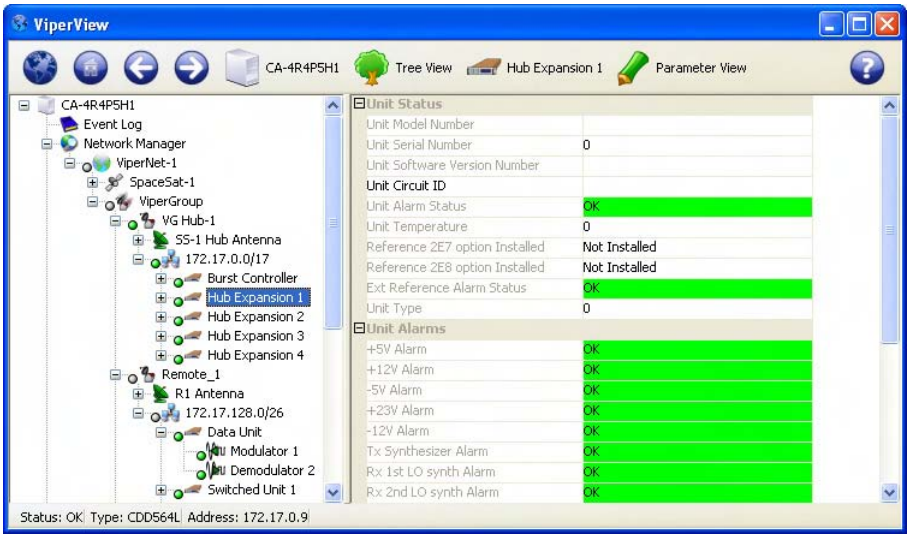


Figure 5-7 Parameter View

The **Parameter View** of a selected unit includes:

- Unit Status
- Unit Alarms
- Unit Config Store/Load
- Unit Events Log
- Unit Statistics Log
- Unit Reference
- Unit Ethernet

Right-clicking on a unit icon in the tree view displays the drop-down menu shown in figure 5-8. Use the commands from this menu to:

- **Open** a separate window for the unit's operating parameters
- Perform **Soft, Firm** and **Hard Resets**
- **Save to Flash**
- **Force Registration**
- **Remove**
- Manipulate router parameters with the **Configure** and **Properties** commands.

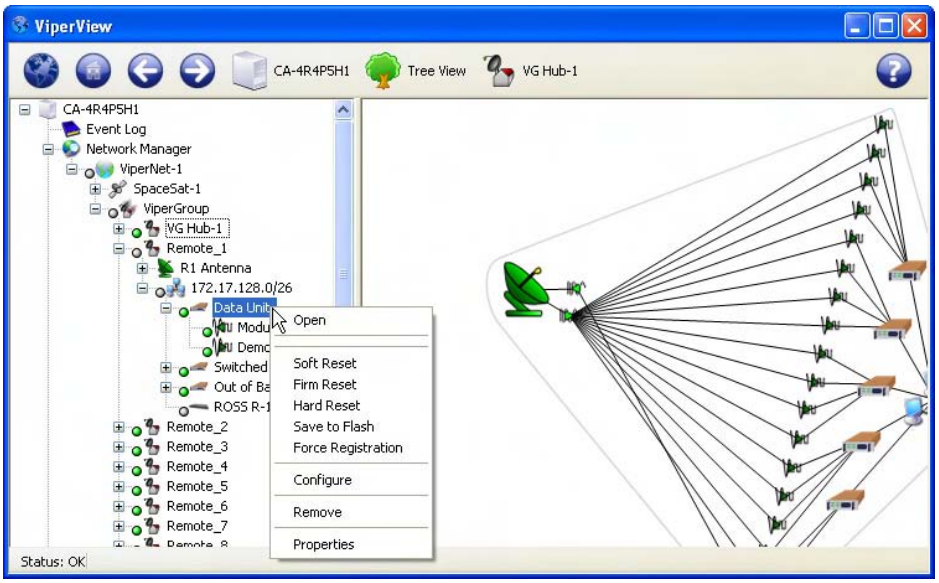


Figure 5-8 Unit Command Menu

Error Detection

Using the **ViperView** screen, you can quickly see which sites in the network are showing an error condition and which have all of the equipment and software operating normally.

Green is used, as shown in figure 5-9, to show which sites, links, and equipment are operating normally. *Red*, on both the right window panel and for devices in the tree view in the left panel, indicates that there is an alarm condition. *Gray* indicates that the status is unknown—no multicast (PLDM) is being received.

Tip: The red error condition indicator associated with a site indicates that at least one of the devices in a site is reporting an alarm condition for a link.

Utilizing the many display options of ViperView, the entire Vipersat network can be quickly and easily scanned to determine the condition of each of the components in the network.

At the main screen level, there are a number of choices to examine, isolate, and remedy the error conditions. The tools available are easily reached from the ViperView display. In figure 5-9, the presence of alarms can be seen reflected in

both the Network Manager service as well as the Subnet Manager service (selected in the figure).

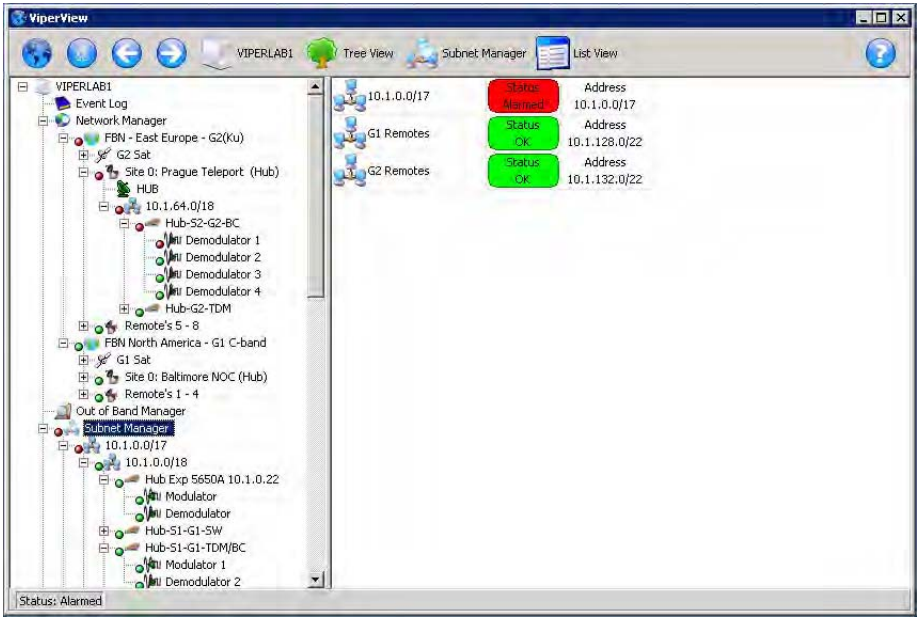


Figure 5-9 ViperView, Error Conditions

Using the Network Manager, right-clicking on a point in the network displays a drop-down menu which is specific to the selected point in the network. From this menu, the operator can perform any of the actions available on the list and instantly modify the parameters of that network element.

An example is shown in figure 5-10 for a Remote data unit that displays an alarm condition. Right-clicking on the modem and selecting **Configure** opens the Configuration dialog (CDM-570L) shown in figure 5-11. Here, the correct parameter settings can be verified and, if necessary, an image upgrade can be performed.

Another example, shown in figure 5-12, shows a Hub expansion demodulator in an alarm state due to reaching the maximum allocation failure count. Right-clicking on the demodulator allows the count to be **Reset** via the menu command that is presented.

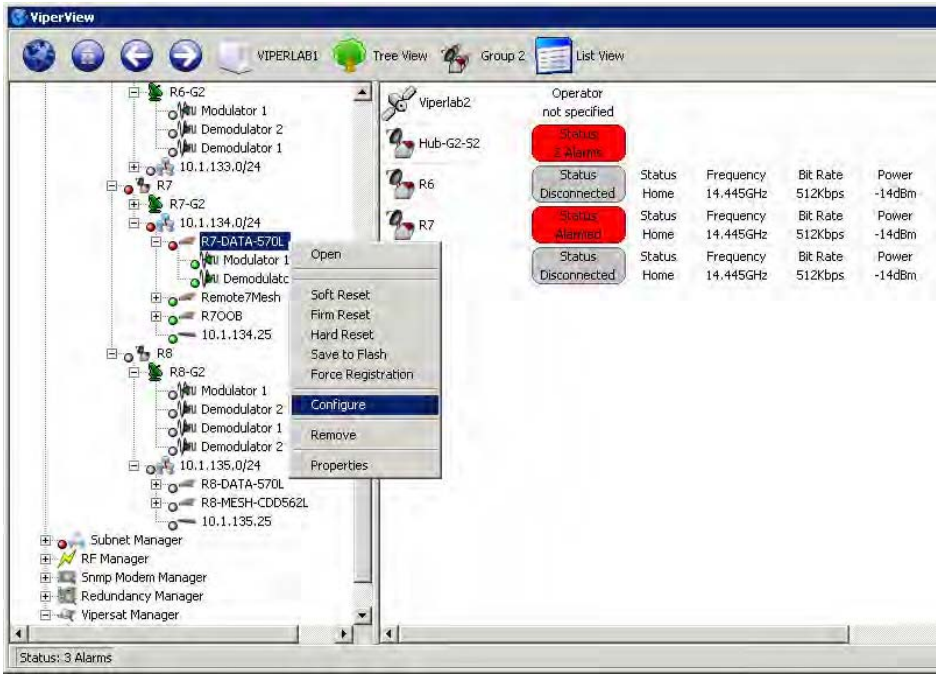


Figure 5-10 Modem Configure Command

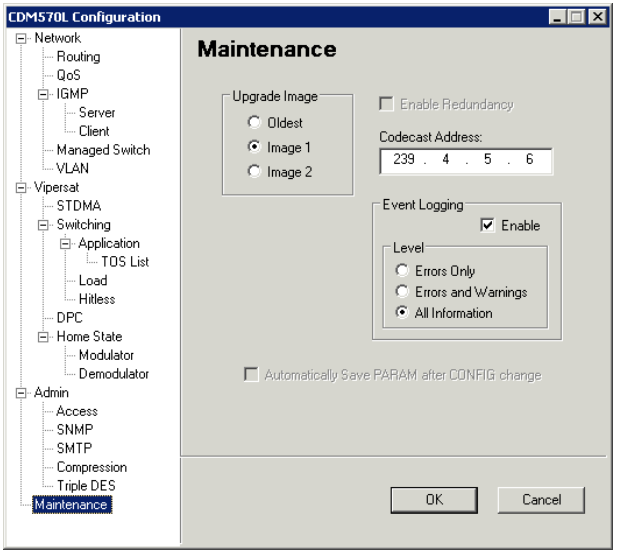


Figure 5-11 Modem Configuration dialog

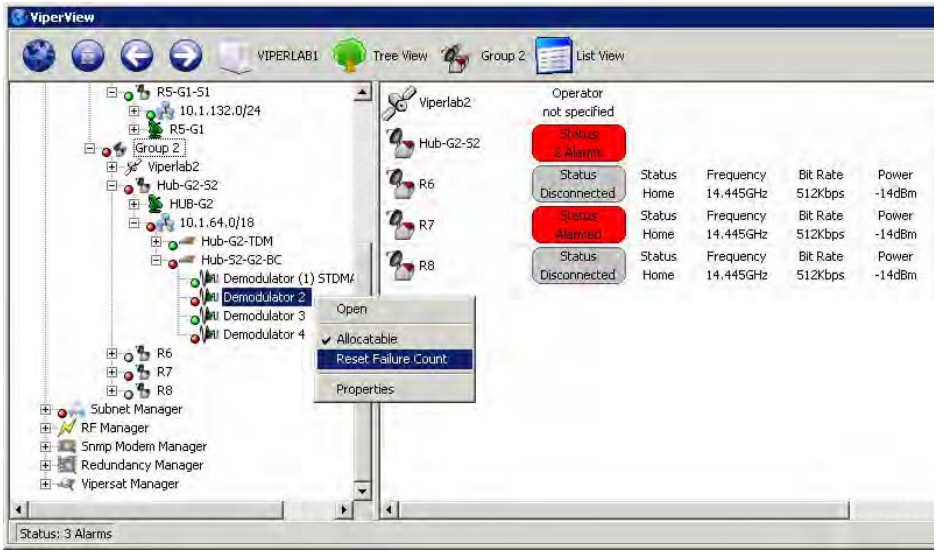


Figure 5-12 Reset Failure Count, Hub Demodulator

Event Log

The VMS **Event Log** displays a history of events occurring in the system and network. Anytime that there is a change in the current setting, status, resources, and configurations, the system ouputs an event message displaying information about the event. The displayed information is part of a complete database file of recorded network activity used for notifying the operator of possible errors or failures.

With the use of this information, the system administrator can quickly locate, identify, repair, or replace the network element that is associated with the error/failure.

Selecting the Event Log icon (directly below the Server icon) from the left panel of the ViperView window (figure 5-9) will display the Event Log view in the right panel. Alternatively, right-clicking on the icon allows the Event Log to be opened in a seperate ViperView child window (figure 5-5).

The Log lists all activity reported to the server. This is a useful tool when determining the functioning of the network. Each event listed is categorized by the date, time, source, and user. A message describing the activity which created the event is also provided.

Each log entry is displayed using the standard VMS color scheme:

- **Green** – Event completed successfully

- **Red** – Event failed and caused an alarm
- **Grey** – The unit was not available
- **White** – Items which do not have a status associated with them
- **Yellow** – Administrative command
- **Blue** – Configuration change
- **Purple** – Corrupted entry
- **Pink** – Server event

Clicking on the **Event View** icon on the Object Bar, as shown in figure 5-13, displays a drop-down menu with six commands:

- Clear
- Reset Filters
- Twelve Hour
- Filters...
- Export...
- Refresh

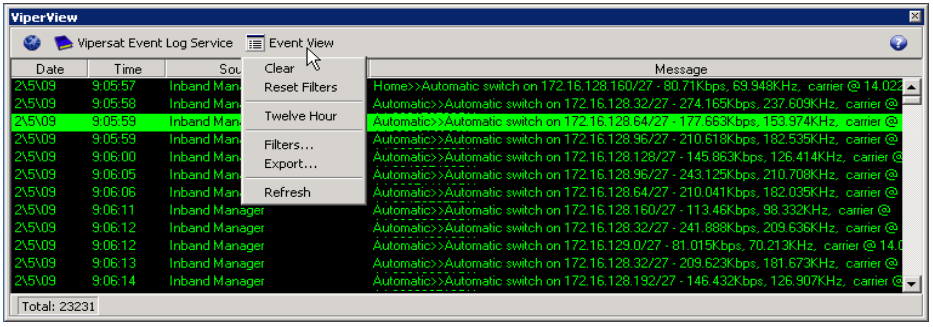


Figure 5-13 Event View Menu

Clear

Selecting **Clear** from the menu removes all log entries from the Event View display, and resets the Start Date/Time for recording new events to the present date and time. The removed entries are not deleted and remain in the vlog file.

Reset Filters

Selecting **Reset Filters** from the menu configures the Event Log filters to the default setting of displaying all events in this Event View window.

Twelve Hour

Selecting the **Twelve Hour** clock setting will toggle between 12 (checked) or 24 (unchecked) hour event time stamping.

Filters...

By default, the Event Log View is set to display all recorded events.

Selecting the **Filters...** command from the menu opens the **Event Log View** dialog shown in figure 5-14. Here, the log entries appearance can be tailored to display a specified *Date/Time* range, events associated with selected *VMS Sources*, and/or specific *Types* of events.

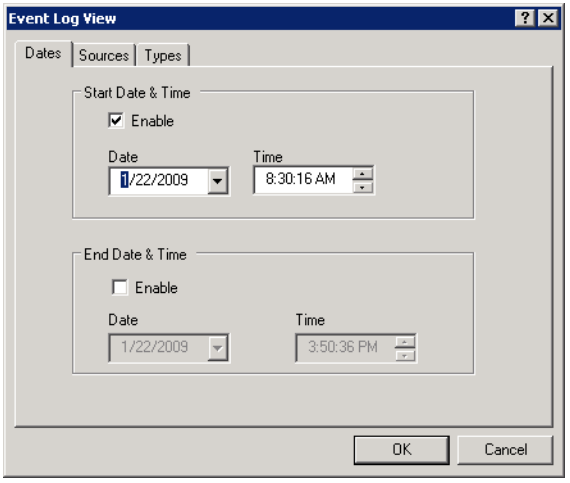


Figure 5-14 Event Log View, Dates tab

Caution: When using more than one Filters tab to create customized filtering, the resulting configuration is executed as an **AND** function, not as an OR function. Therefore, if an event does not match the conditions of the tab combination used, it will not be displayed.

NOTE

Note: Customized filtering settings are not saved and only apply to the current Event Log window that is displayed, whether it is from the main Viper-view window or a separately opened child window. Once the window is closed, re-opening the Event Log window will result in the display defaulting to show all events.

Dates Tab

The **Dates** tab can be selected for specifying the Date and Time to start and stop viewing events, as shown in figure 5-14.

Select the **Enable** check box to edit the current settings.

Sources Tab

The **Sources** tab (figure 5-15) can be selected for specifying a customized set of sources from the VMS Services tree from which all associated log events will be displayed.

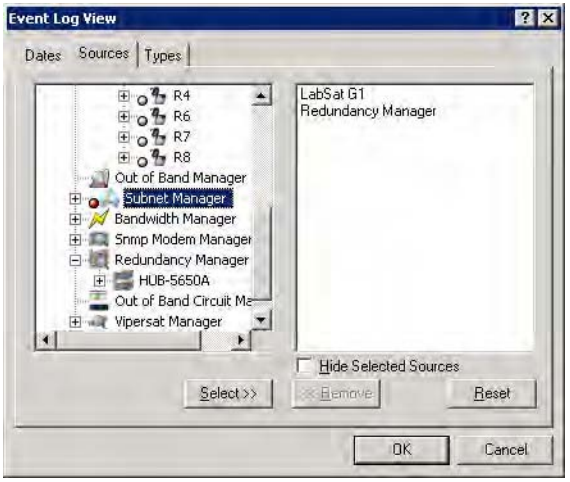


Figure 5-15 Event Log View, Sources tab

The VMS Server name appears in the left panel. Expand the tree to the level desired and click to highlight a source, then use the **Select** button to enter that source in the right panel. Repeat this process to create a cumulative customized source set.

Enabling the **Hide Selected Sources** check box will *prevent* these event sources from being displayed.

Types Tab

The **Types** tab can be selected for specifying a customized set of event types to be displayed.

Select the desired event types by clicking in the check boxes, as shown in figure 5-16.

Enabling the **Hide Selected Types** check box will *prevent* these event types from being displayed.

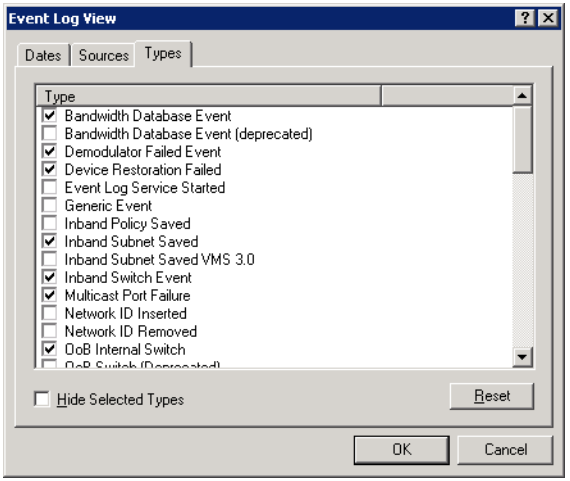


Figure 5-16 Event Log View, Types tab

Tip: The event Type for an Event Log entry can be identified by double-clicking on the given event listing to open the **Event Details** dialog. An example is shown in figure 5-17, below.

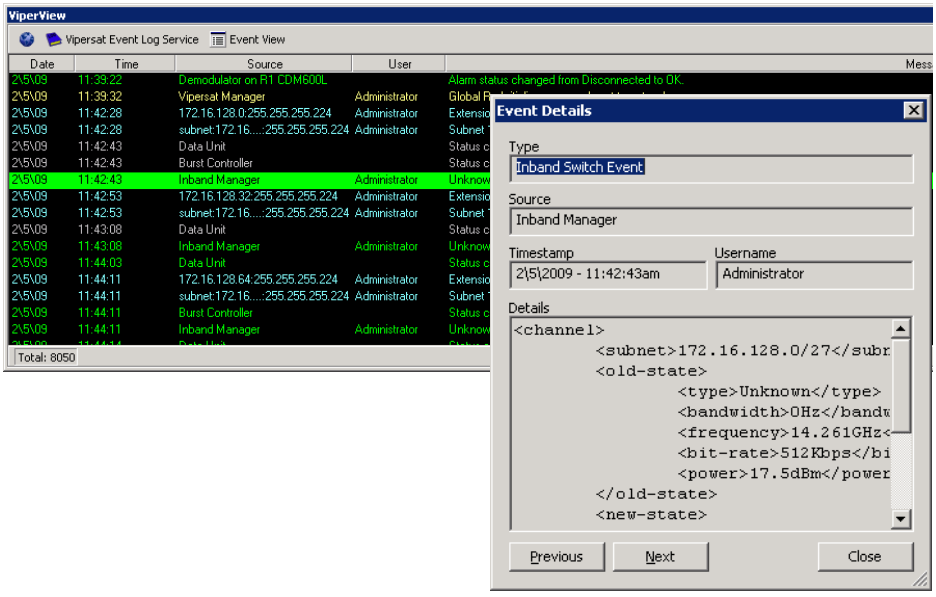


Figure 5-17 Event Details dialog

Once the desired filters have been defined, click on the **OK** button to execute the changes.

The parameters entered on the Dates, Sources, and Types tabs work together to provide customized Event Views of network activity.

Direct Event Filtering

The VMS Event Log also provides the means to configure event filtering directly from specific events.

Right-click on a logged event to display the drop-down menu shown in figure 5-18. The associated **Type** and/or **Source** for this event can be chosen to either *Show* or *Hide* this category in the Event View.

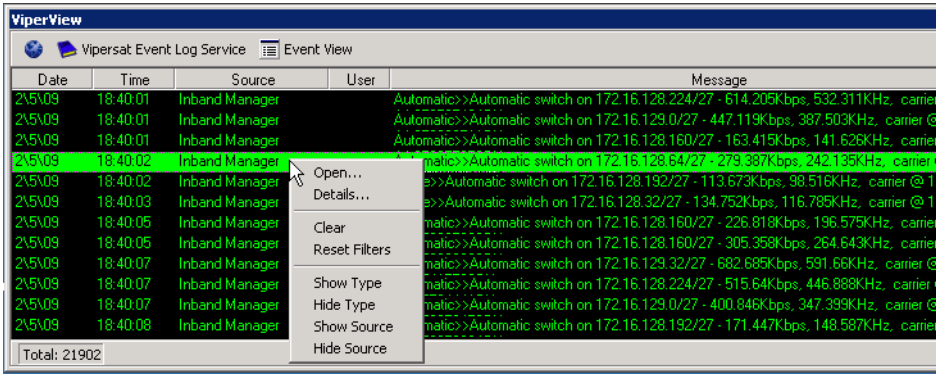


Figure 5-18 Menu, Selected Log Event

Select **Open...** from the menu to open the default ViperView window for the item in the Tree View (left panel) that corresponds to this event.

Selecting **Details...** will open the Event Details window for this event item.

Export

Selecting the **Export** command will open a windows file **Save As** dialog, prompting the operator to enter a file name and location to save the event log. The file is exported as an *Extensible Markup Language* (XML) file, which is a simple and very flexible text format for import into most database applications.

Refresh

Selecting the **Refresh** command will update the event view with any pending events waiting in the event thread.

Event Relay Server

The VMS Event Relay Server allows external client software to interact directly with the Event Log service, utilizing text messages over a TCP connection. Events generated by the VMS can be passed through the TCP/XML interface to a client application on any platform and from any location in the IP network. The events are transmitted in standard XML format.

With no dependency on the Windows Event Viewer and API, the Event Relay Server is more efficient and more reliable than the Event Conduit Service (VMS v3.6.4) that it replaces. And, because this server is directly integrated with the VMS, there is no need to install any additional software.

The Event Relay is configured from the Event Log Properties **General** dialog, and is set to **Enabled** by default, as shown in figure 5-19.

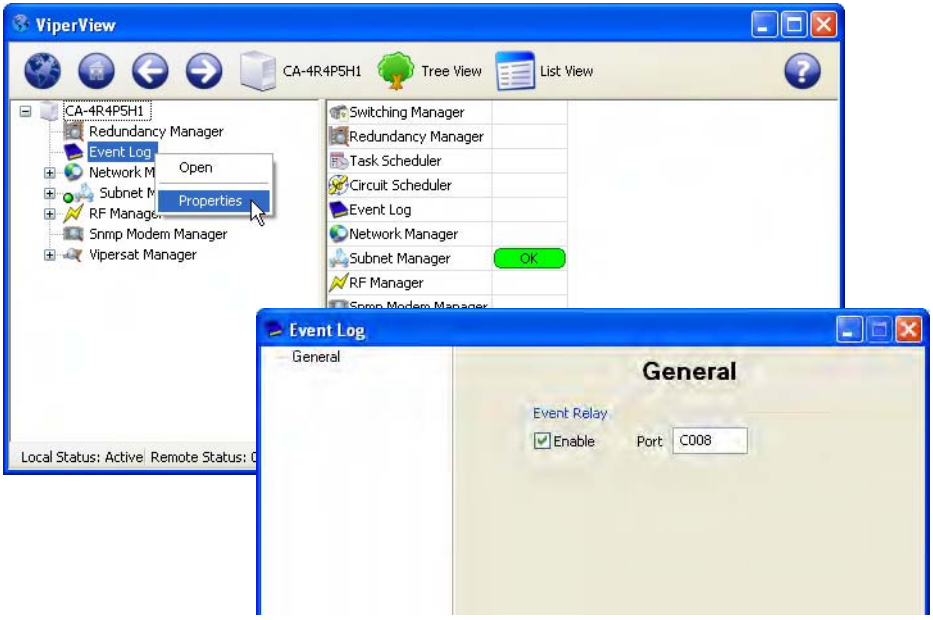


Figure 5-19 Event Relay Server Configuration

Alarm Masks

Alarm masks are a VMS tool that is used to limit false alarms generated by normal system operations.

Viewing/Setting Alarm Masks

Demodulators that are typically being locked and unlocked, such as switched demodulators/burst controllers, should have the Unlock Alarm masked. The setting of other alarm masks will depend on usage and whether or not a BUC is installed.

Alarms masks are viewed and set for the modem in the device view, as shown in figure 5-20 and figure 5-21.

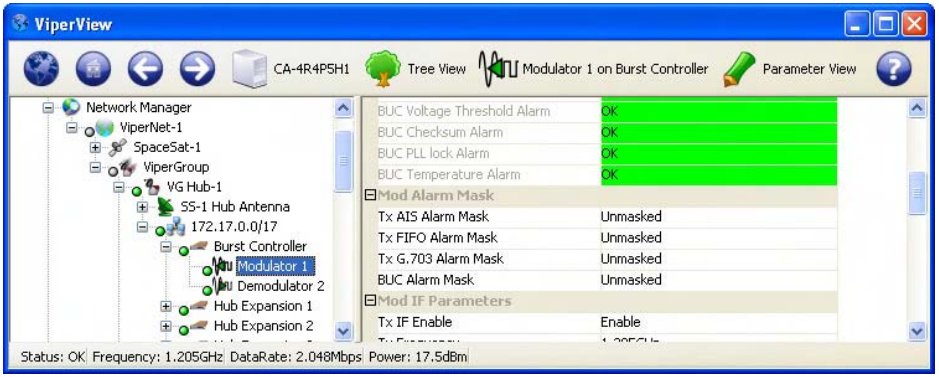


Figure 5-20 Modulator Alarm Masks

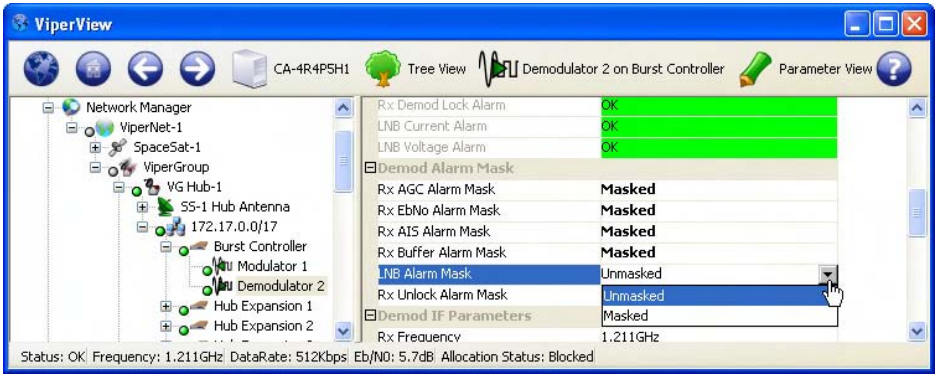


Figure 5-21 Demodulator Alarm Masks

To mask/unmask alarms for a device, select the device in the left panel tree view, then select an alarm from the Alarm Mask list in the right panel. Use the pull-down menu to select either **Unmasked** or **Masked**.

The alarm mask settings shown in table 5-1 are for a typical VMS network.

Table 5-1 Alarm Masking in a Typical Network

Device Type	Demodulator Lock Status	Demodulator Level Alarm	Demodulator Auto Gain Ctrl
TDM/ Burst Cont. Remote	X	X	X
Hub Expansion	X	X	X
Remote Expansion	X	X	X

Unlock Alarm Masks

InBand modem device **Mask Unlock Alarm** flags mask and set park states every time the modem registers with the VMS. These flags simplify and reduce the device item-by-item settings, making them persistent during active state. These flag settings are typically set on modems that are switched expansion units or hub burst demodulators. If these devices are not masked, many unwanted alarms will be generated in the system during normal operations due to their frequent locking/unlocking behavior.

Hub burst demodulators, when masked, only shutdown their link status alarms that are typically part of the carrier lock/unlock, leaving all other internal alarms unmasked.

The hub and remote expansion demodulator carrier alarm mask is cleared each time it is switched to receive a return carrier from a remote. This unmasking of alarms remains until the demodulator is returned to a parked state (unlock), where it is re-masked to prevent unwanted network alarms.

If the modem is rebooted, the alarm masks are cleared until the next VMS registration.

Note: It is not necessary to mask the SLM-5650A hub burst demodulator. If the alarm mask is set for this device type, the front panel carrier lock LED's WILL NOT illuminate.

See "Mask Rx Unlock Alarms" on page 3-47 for details on how to set unlock alarm masks.

Diagnostic Switching

A manual switch control feature called Diagnostic Switch allows an operator to perform maintenance testing or commission an antenna. All VMS automatic switching and carrier recovery mechanisms are disabled when a site is placed in diagnostic mode.

Caution: Diagnostic switching should only be used during maintenance periods; all guarantees are disabled for the affected network during this process..

Diagnostic Setup

To execute a diagnostic switch, right-click on the Remote site in Network Manager and select **Diagnostic Setup** from the drop-down menu, as shown in figure 5-22.

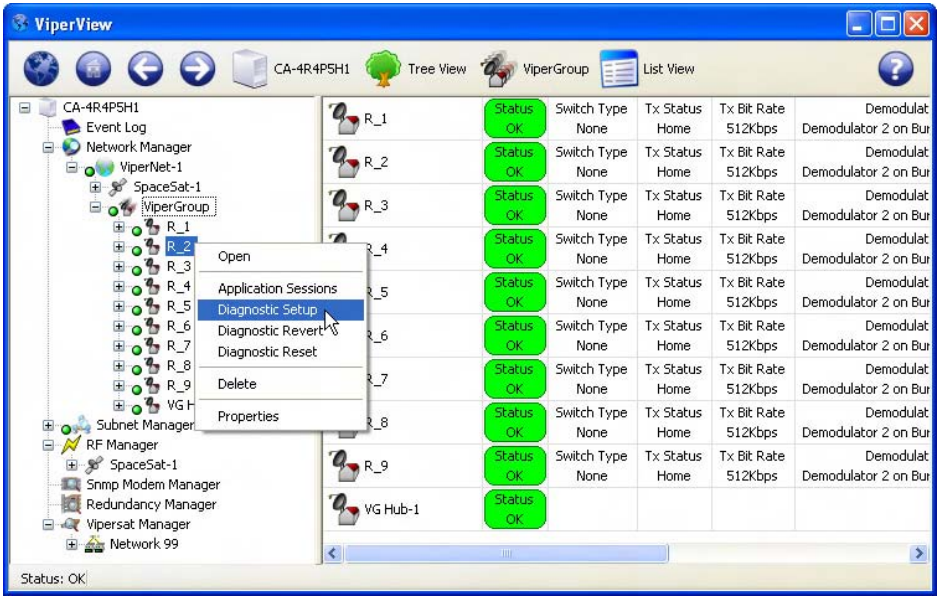


Figure 5-22 Diagnostic Setup command

A setup dialog will open for specifying the desired bit rate and transmission parameters for the SCPC switch (figure 5-23).

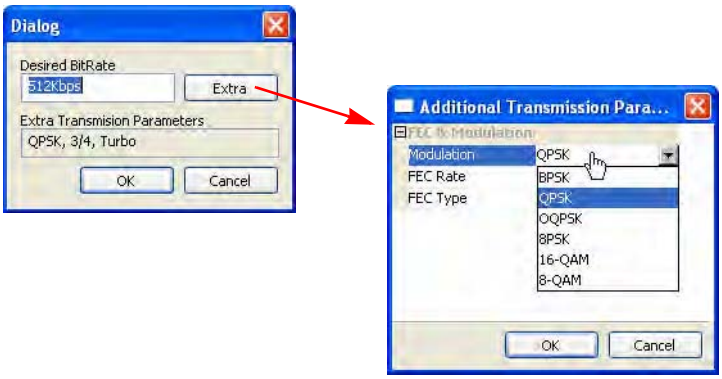


Figure 5-23 Diagnostic Setup dialogs

Click **OK** to initiate the switch. The **Executing Switch** message will be temporarily displayed while the switch request is processed.

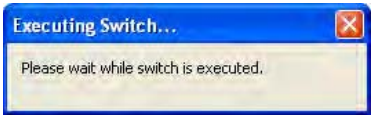


Figure 5-24 Executing Switch message

If successful, the new status for this remote will be displayed and the assigned carrier will appear in the spectrum view, as shown in figure 5-25 and figure 5-26.

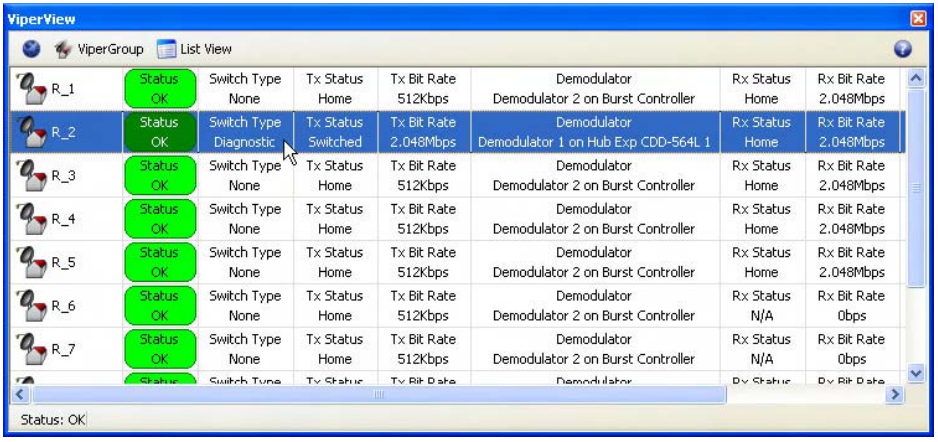


Figure 5-25 Remote Status, Diagnostic Switch

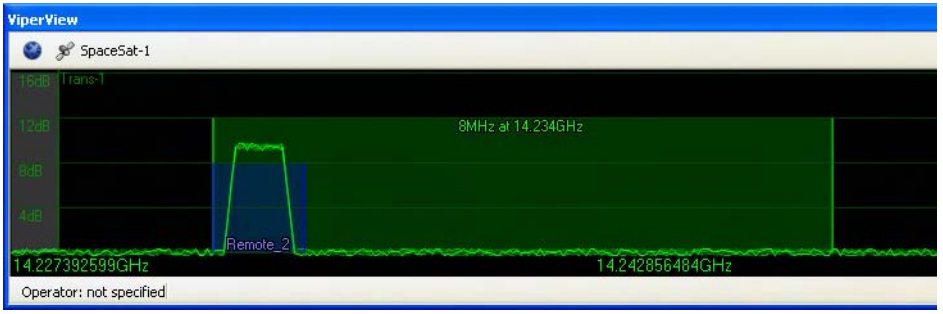


Figure 5-26 Carrier Appearance, Diagnostic Switch

If the diagnostic setup is not successful, a failed event will appear in the Event Log view.

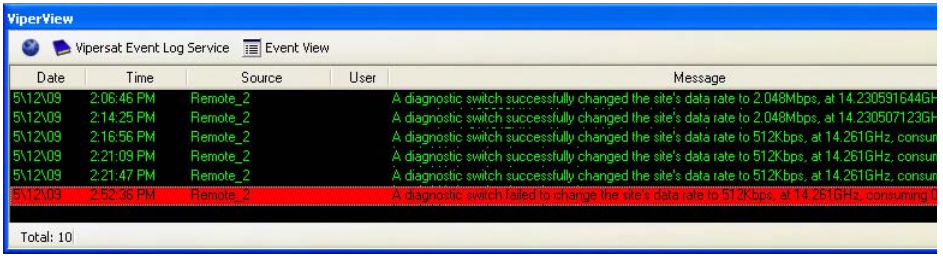


Figure 5-27 Failed Event, Diagnostic Switch

Diagnostic Revert

The **Diagnostic Revert** command returns the remote modem to its home state settings. This command is appropriate to use when SCPC transmission is no longer required, switching back to STDMA mode, or communications with the remote have been lost and it is *unknown* whether or not the modem is still transmitting. Unlike the Reset command (see below), the bandwidth slot is retained in case the modem communications are restored.

Diagnostic Reset

As with the Revert command (see above), the **Diagnostic Reset** command returns the remote modem to its home state settings. However, this command is appropriate to use when communications with the remote have been lost and it is *known* that the modem is not transmitting so as to prevent the occurrence of an interfering carrier. The bandwidth slot is freed for use by another network device.

Because of the possibility of an interfering carrier being created if the remote is still transmitting, selecting the Diagnostic Reset command displays the **reset uplink** warning shown in figure 5-28.

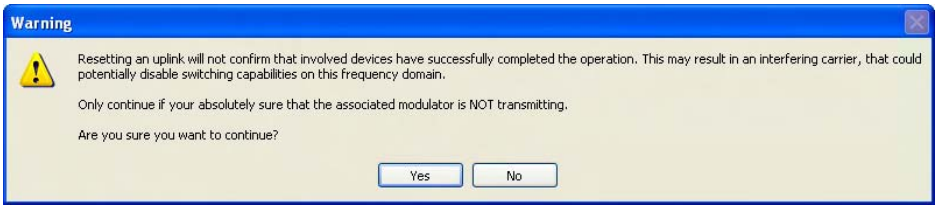


Figure 5-28 Reset Uplink warning

Caution: Read the Reset Uplink warning carefully, as performing this operation on an unknown transmitting unit may cause carrier interference on the operating network. It is safe to reset resources for a remote if it is known that the remote is not transmitting, powered down, or faulty.

Database Backup and Restore

It is recommended that periodic VMS database backups be performed on a regular basis. In addition, backups are necessary prior to installing a new version of VMS (upgrade) and whenever any significant changes are made to the network configuration. This precaution will allow for a current or recent database to be restored in the event that a failure—such as a file corruption—with the VMS occurs.

Backup Procedure

1. Right-click on the VMS Server icon in the ViperView main menu bar and select the **Backup** command from the drop-down menu (figure 5-29).

Figure 5-29 Backup Command, VMS Server Menu

2. Enter the **Name** for the backup file and select the directory location for saving the file from the **Save As** dialog window that opens (figure 5-30).

It is recommended that the file name include the VMS *version* and the *date* of the backup.

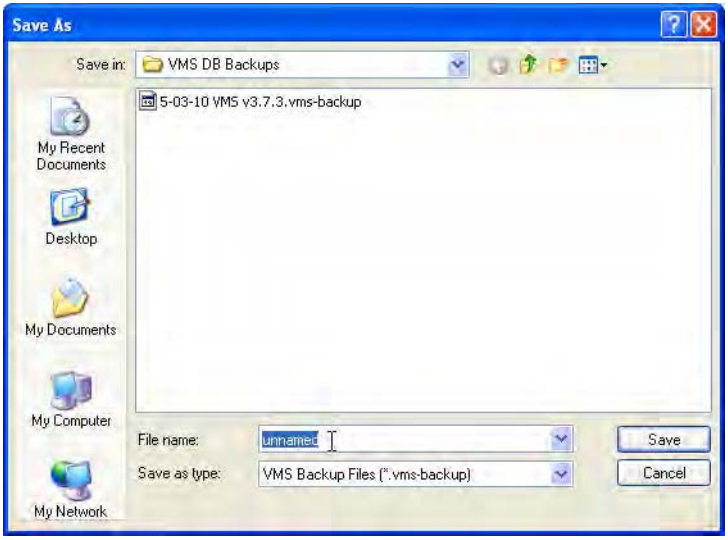


Figure 5-30 VMS Database Backup Save As dialog

Restore Procedure

NOTE

Note: The database backup can only be restored on the same VMS version. It is not compatible with a different VMS version.

1. Right-click on the VMS Server icon in the ViperView main menu bar and select the **Restore** command from the drop-down menu.

Figure 5-31 Restore Command, VMS Server Menu

2. Locate the backup file directory and select the desired database backup file for the currently running VMS version from the **Open** dialog.

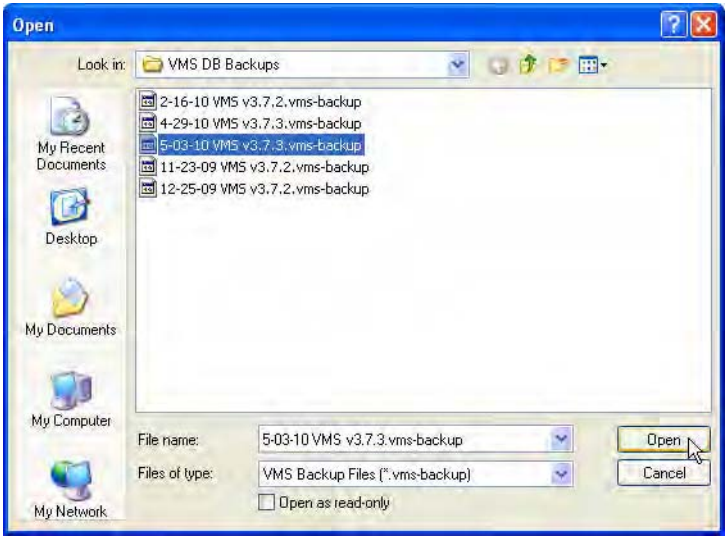


Figure 5-32 VMS Database Restore Open dialog

3. From the Tree View icon in the Viperview main menu bar, select the **Refresh** command.

4. Verify that the ViperView display is interactive and reflects network status correctly.

VMS Service Managers

When VMS is started on the server and ViperView is opened on the client workstation, the Server View, shown in figure 5-33, displays the installed VMS Service Managers. Included in this display are the Network Manager, the Subnet Manager, the RF Manager (formerly the Bandwidth Manager in previous versions), the Switching Manager, the SNMP Modem Manager, the Redundancy Manager, and the Vipersat Manager.

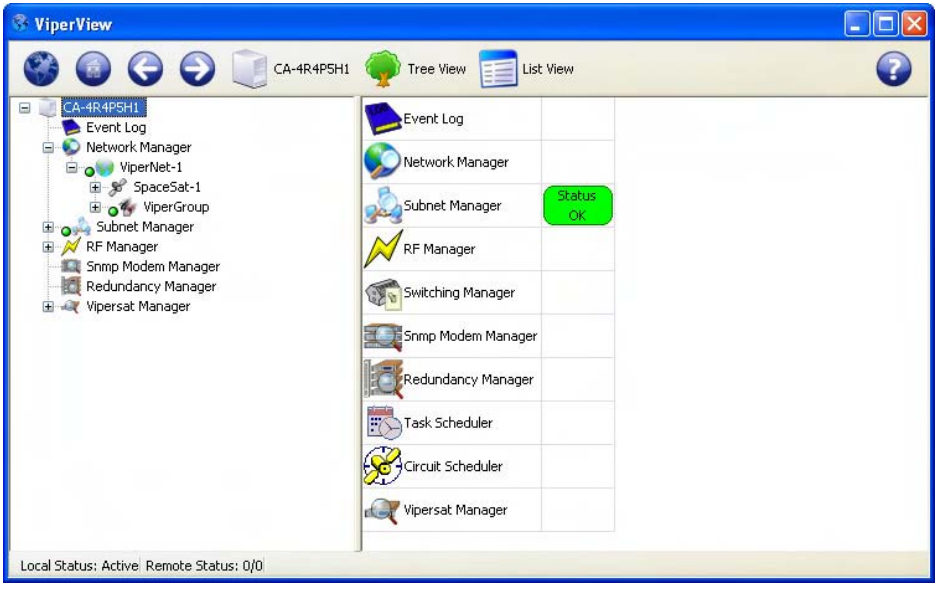


Figure 5-33 VMS Server View

Each of these services is discussed in the following sections.

Network Manager

The Network Manager is the heart of the VMS user interface, and serves as the primary source within ViperView for managing network functions. The networks, and their associated elements, that are created in the Network Manager are *virtual*, and thus can be added and removed without affecting the actual networks upon which they are based. The source locations of the elements that are displayed in Network Manager originate from within the other VMS service managers.

The Network Manager also provides a means of exposing the satellite network(s) to customers via VNO (for network operations) and ViperGlobe (for geographical display).

Operator networks are built and managed in the Network Manager by utilizing the Network, Group, and Site container structures. These hierarchical structures serve as a means of logically organizing all of the network elements for easy access. Configuration changes, InBanding of remotes, and switching and bandwidth policies are all controlled and monitored with this service manager.

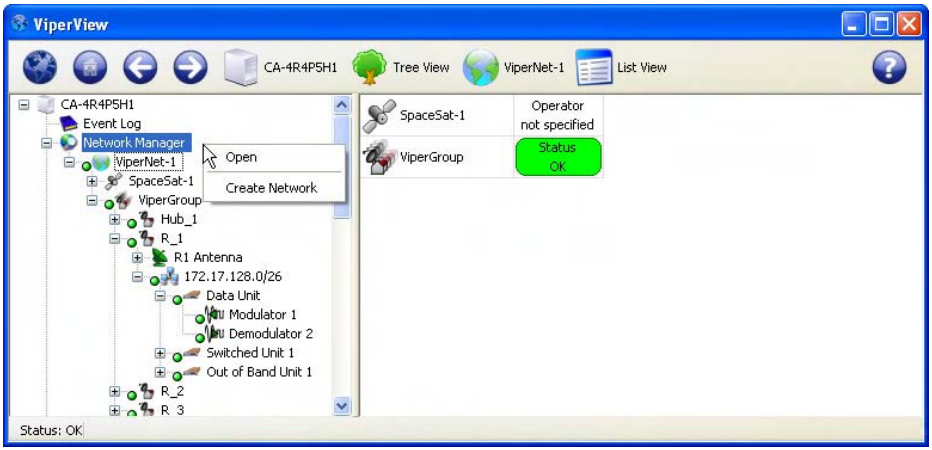


Figure 5-34 Network Manager, Drop-Down Menu

Site View

The Network Manager service in ViperView provides multiple displays that supply current status information for the network. The Site view is one such display, providing the status of each site component via a graphical representation of the interconnected devices, as shown in figure 5-35. Directing the mouse pointer to a component results in a status box pop-up. Additional status information for the site is provided in the window footer.

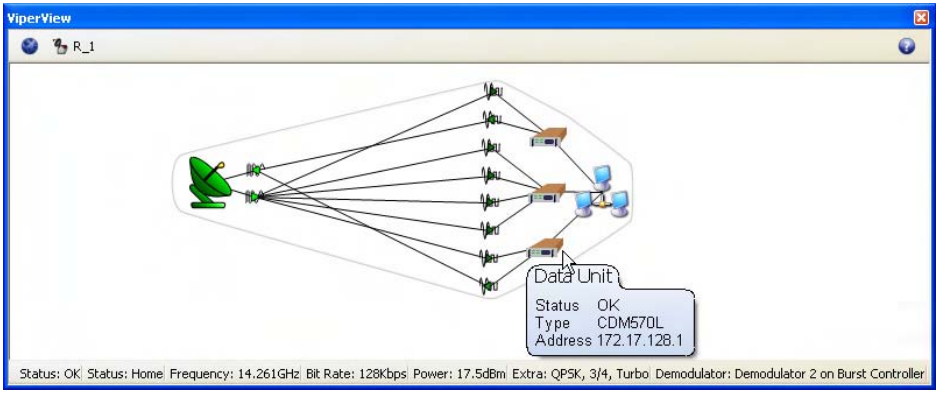


Figure 5-35 Network Manager, Remote Site View

InBand Management

InBand management allows Application Policies and Distribution Lists to be selected on a Network, Group, and Remote site-level basis and allows the system operator to enable and disable mesh, return path, and forward path (point-to-point) switching, or use policies/lists for selected remotes that differ from the network policies/lists. Bandwidth Reservations which provide a minimum guaranteed data rate (CIR) can also be established with this InBand feature. Each Remote site in the network that will require dynamic control of their carriers (nodes which are part of the switched network) must be InBanded.

Application Policies

From the Application Policies dialog that is accessible from the Network, Group, and Site Properties windows, the policies under which switching will occur in the Vipersat network can be defined. The policy settings that are defined on a per network and/or per group basis are propagated down to all remotes in the system. Each remote will inherit the policies from the network/group to which it is associated, but the operator may choose to break the inherited settings and configure each site independently. Locally created Site policies apply only to that site.

Along with an application type setting, each policy can specify a priority setting and min/max data rate settings for both transmit and receive.

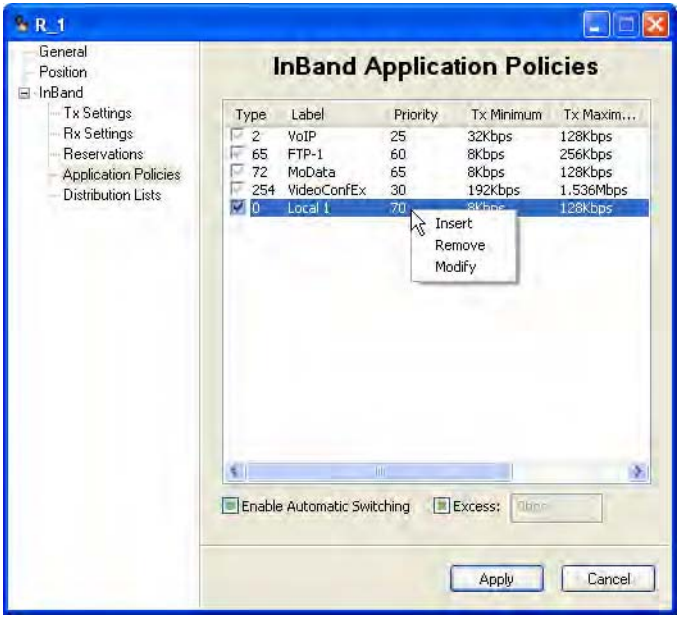


Figure 5-36 Application Policies, Remote Site

Distribution Lists

Distribution Lists are used to define multiple target subnets for point-to-multi-point distribution on an InBand service connection whenever an upstream switch to a specific destination IP address occurs, such as to a multicast address.

Distribution lists are typically created, modified, or disabled at the site level to accommodate specific site requirements. However, they can also be created at the group and network levels where they become inherited by the associated sites, just as with Application Policies.

In the Distribution Lists table, the user can **Insert**, **Modify**, and **Remove** lists, then either select or de-select these lists once entered through the use of the check boxes (figure 5-37).

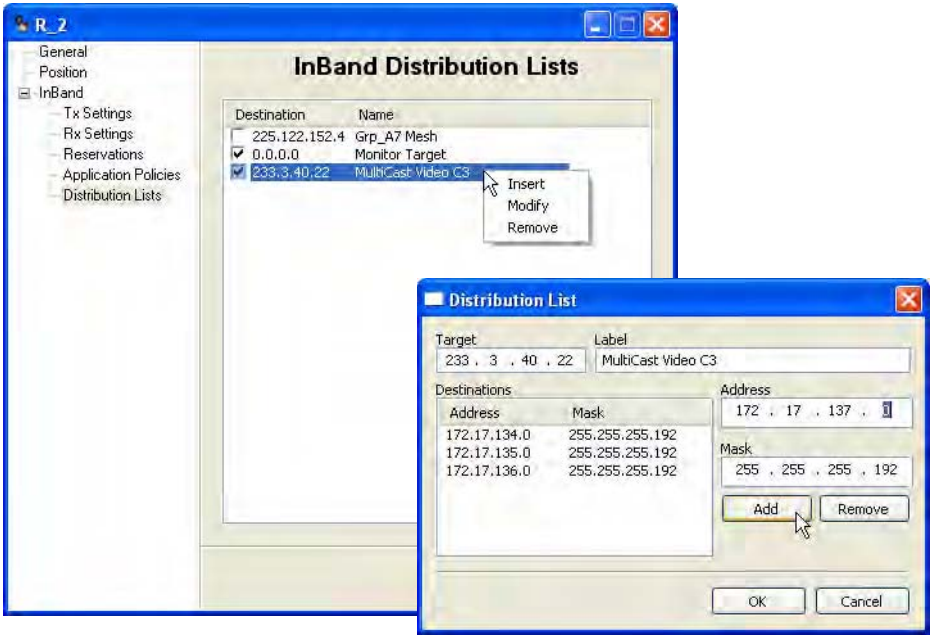


Figure 5-37 Distribution Lists, Remote Site

Guaranteed Bandwidth

The InBand Bandwidth Reservation ensures that the remote is always guaranteed bandwidth up to the rate that is specified, the committed information rate (CIR). Beyond that, the remote will only be granted additional bandwidth when it is available. This feature assures that, at minimum, all requests for SCPC bandwidth up to the CIR will be granted.

Setting a rate in the remote properties Reservations dialog (figure 5-38) will reserve a segment of bandwidth for the remote ensuring that, at last resort (no additional bandwidth available), the remote will be dropped to the rate specified here—its CIR—until excess bandwidth is once again available to be allocated.

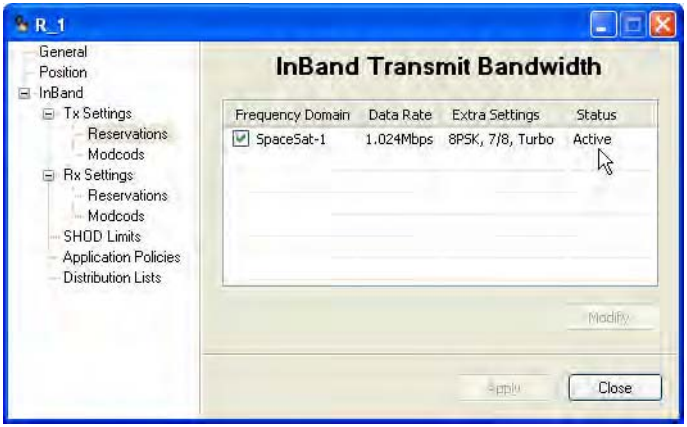


Figure 5-38 InBand Reservations Setting

Total bandwidth reservations for the satellite that is utilized by a network or group can be viewed by selecting **Reservations** from the satellite drop-down menu, as shown in figure 5-39 and figure 5-40.

Figure 5-39 Satellite Reservations command

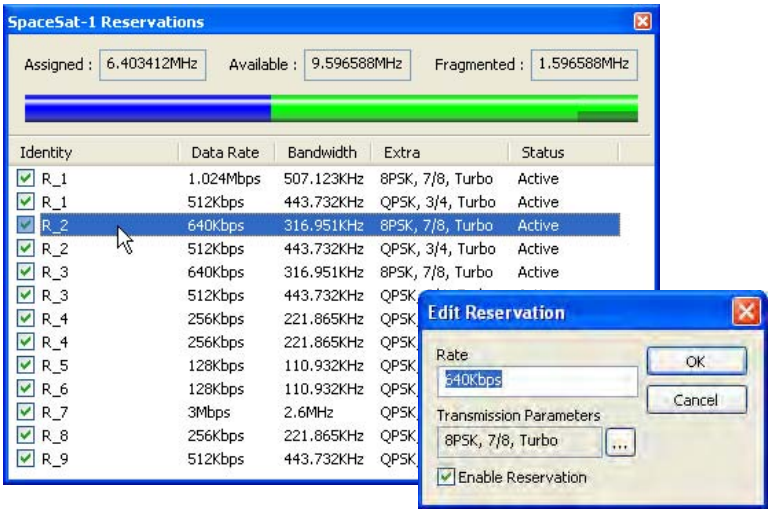


Figure 5-40 Satellite Bandwidth Reservations

The Satellite Reservations window displays a table containing entries for each Remote site (both Tx and Rx, if so enabled) that has been assigned a CIR, and displays the following information:

- **Reservation Enable/Disable** — check box toggle. Status column display reflects this setting, either *Active* or *Inactive*.
- **Assigned, or Pre-Allocated, Bandwidth** — currently reserved for granting CIR when called for by the list of Remote sites presented in the table. This segment is displayed as a numerical frequency value, and is represented as the *dark blue* section of the bandwidth color bar. The Data Rate, Bandwidth, and Extra (mod/code) parameters for each site is also provided in the table.
- **Available Bandwidth** — currently unreserved and available for pre-allocation to Remote sites. This segment is displayed as a numerical frequency value, and is represented as the *light green* section (combined) of the bandwidth color bar. The largest continuous/unfragmented block of available bandwidth is represented by the *light green* section that is not underlined with *dark green*.
- **Fragmented Bandwidth** — additional available bandwidth remaining that is separate from the largest continuous block. This segment is displayed as a numerical frequency value, and is represented as the *light green* section of the bandwidth color bar that is underlined with *dark green*.

The divisions shown in the color bar will vary depending on a number of factors, including the quantity and size(s) of the bandwidth pools, and the amount of pre-allocated bandwidth.

Individual reservations can be enabled/disabled via the check box in the Identity column. Reservation settings (Data Rate, Bandwidth, and Extra) can be edited directly from this window by double-clicking on a table entry, as shown in the figure.

Operator Switch Request

The Application Sessions switching control provides a means for the operator to view/change/remove any active InBand switch sessions for a site, as well as to manually set and execute a new application switch. The data rate, switch type, and distribution list selection can be specified with this feature, as illustrated in figure 5-41 and figure 5-42.

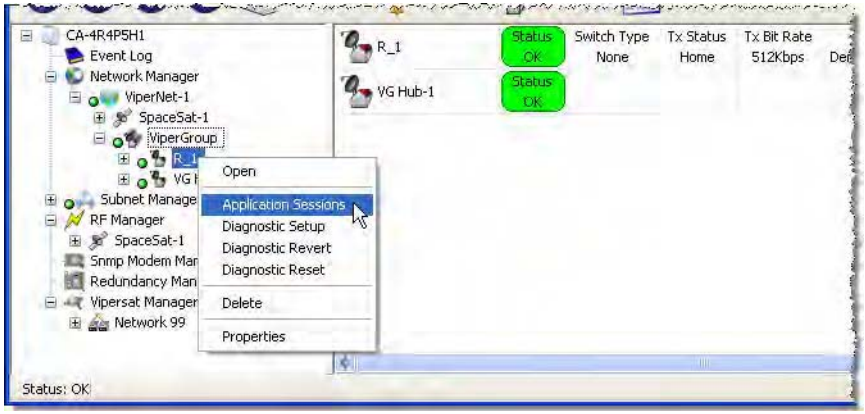


Figure 5-41 Application Sessions command

A session can be established quickly using the main InBand Sessions window by specifying just the application type. The default data rate setting (0 bps) will result in an attempt to switch using the pre-defined maximum and minimum data rates specified by this application policy. Changing the default will force a switch request using this new value for the Tx maximum (the ideal rate).

More options can be chosen by clicking on the ellipsis (**...**) button. Here, the ideal and minimum data rates—for both Tx and Rx (P2P)—can be modified from the defaults, as long as they fall within the defined range of the policy. And, if a distribution list has been configured for use by this site, a destination can be chosen from this list.

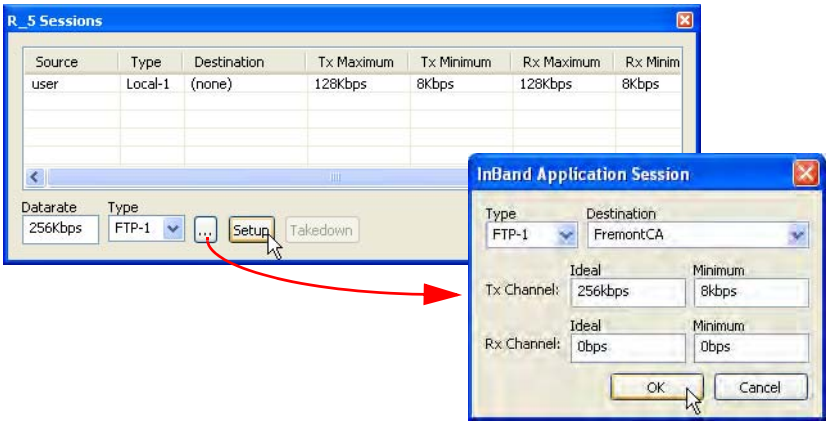


Figure 5-42 Application Session Setup

NOTE

Note: The Type default is 64; however, if Type 64 is not defined for this Remote, the switch attempt will fail and an alert will appear (figure 5-43). Use the Type pull-down menu to view and select a valid policy for this Remote.

Figure 5-43 Switch Failed, Invalid Policy Type

Once the desired parameters are set, the Setup button will initiate the switch request for the new SCPC carrier(s). The VMS will compare the requested application data rate to the maximum switch rate limit for this site; the resulting rate will be the lesser value between the Policy setting and the Site setting.

The new carrier(s) will appear in the Spectrum view, and the event is logged in the Event view.

Advanced Switching — ModCods

With the VMS Advanced Switching feature, the operator has the option of configuring multiple levels of modulation types and FEC code rates within the dynamic SCPC operation. Thus, more efficient bandwidth utilization can be realized.

An advanced switching table can be constructed for a remote modulator where specified modulation types and FEC code rates are paired with set data rates. Each data rate is associated with a Mod/Code and, as the system achieves the set rate, the transmission is modified to the new higher- or lower-order modulation setting specified for that rate. For each table entry, the VMS calculates an optimized switching threshold that the system uses to assign the most efficient bandwidth in an advanced switching environment.

As a switch request is processed, it is compared to the Advanced Switching table. If the requested data rate crosses a threshold where the higher-order modulation actually becomes more bandwidth efficient, the switch request will go up to the higher-order modulation at the lowest bit rate that exceeds the request. Thus, it is possible that a *higher* bit rate can be granted while actually utilizing *less* bandwidth resources.

For example, a site currently operating at QPSK 3/4 that generates a switch request for 192 kbps will be switched up to 256 kbps at 8PSK 7/8, provided this modulation and code rate was specified in the Advanced Switching table entry for this switch point, as shown in figure 5-44.

The following equations illustrate this scenario:

QPSK 3/4 @192 kbps @1.3 spacing:

Allocated Bandwidth = 192 x (1/2) x (1/.75) x 1.3 = 166.4 kHz

8PSK 7/8 @256 kbps @1.3 spacing:

Allocated Bandwidth = 256 x (1/3) x (1/.875) x 1.3 = 126.781 kHz

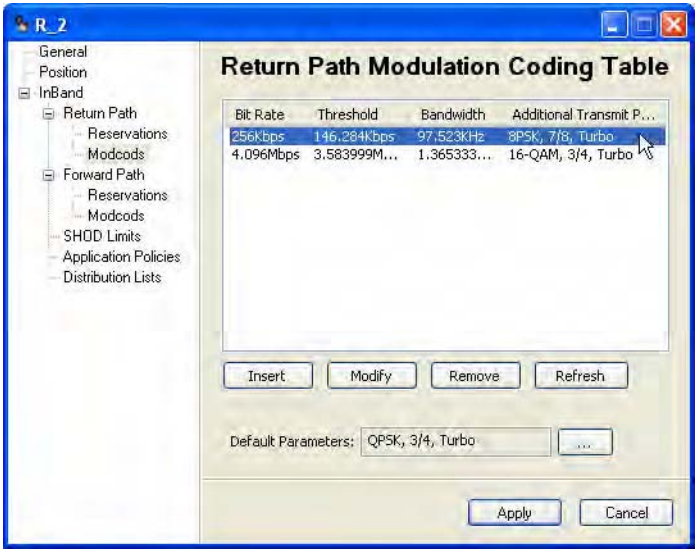


Figure 5-44 Advanced Switching Table for Remote (R_2)

Note that the calculated Bandwidth value for this table entry, 97.523 kHz, is for the carrier only. The bandwidth Slot that will be assigned for this carrier will include the additional guardband that is defined for the associated Pool. In this example, a guardband of 30% is used.

An InBand switching session for the Remote site (R_2) can be generated using the Application Sessions feature, with a specified data rate of 192 kbps at QPSK 3/4 (figure 5-45).

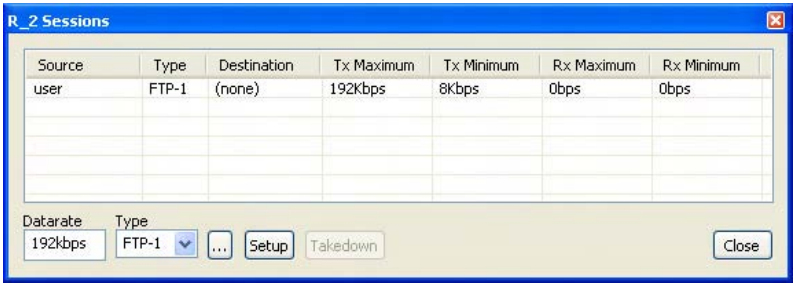


Figure 5-45 Manual Application Switch Session, R_2

Following the VMS switch, the site status for R_2 changes, indicating a new bit rate of 256 kbps at 8PSK 7/8 (figure 5-46).

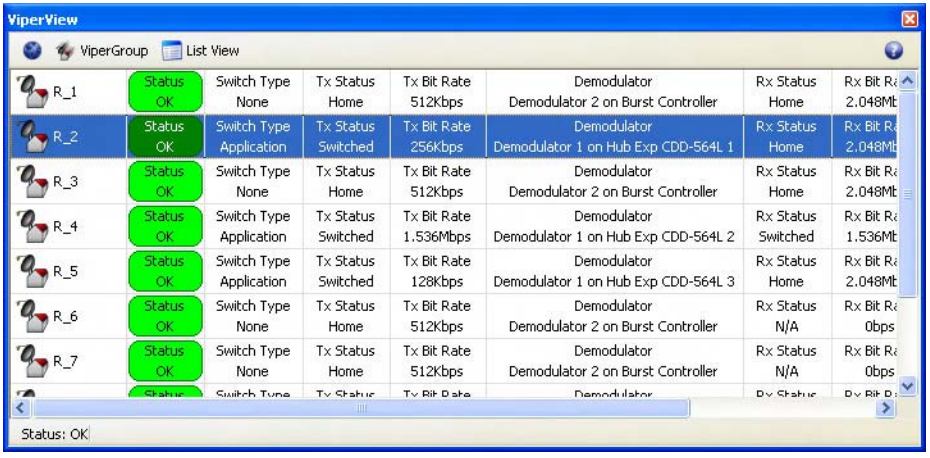


Figure 5-46 Updated Status View, R_2

The carrier appearance in the Spectrum view displays with an allocated bandwidth of 97.523 kHz (figure 5-47). When the guardband is added to this value, the assigned bandwidth slot becomes 126.781 kHz, just as was calculated in the example equation previously.

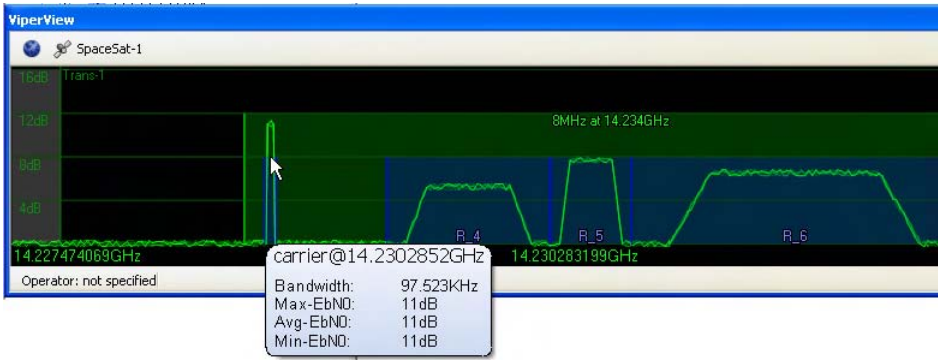


Figure 5-47 Allocated Carrier for Remote (R_2)

Roaming with Advanced Switching

A Roaming Remote (SOTM) can take advantage of the advanced switching function when transitioning from one satellite beam to another. Switching tables for a remote can be configured on a per satellite region basis and, upon entering into a new service area, the remote forwards the designated table for that area to the VMS. This dynamically updates the modulator transmission settings on each transition.

Refer to the *ROSS User Guide* for additional details on the configuration and use of the Advanced Switching feature in a roaming application.

Subnet Manager

All subnets for Hub sites and Remote sites are detected and displayed in the Subnet Manager, as well as the devices which are associated with these subnets. Upon VMS startup, the Subnet Manager sorts all of its elements by IP address. The subnets and devices can be exposed by expanding the tree view in the left window panel of ViperView. Clicking on the Subnet Manager displays the status and IP address of each subnet in the right window panel. Selecting a subnet will display a list of all of the modem/router units for that subnet, as well as their status, modem type, and address, as shown in figure 5-48.

Figure 5-48 Subnet Manager, Drop-Down Menu

The Parameter view for site devices, such as modems and their modulators and demodulators, can be displayed by selecting them from the tree.

Because the subnets also appear in the Network Manager, which serves as the primary operator interface for managing and controlling the VMS network(s), nearly all subnet features and functions are accessed from there. However, an important distinction between the two is that, although subnets can be *Removed* from the Network Manager, they can be *Deleted* from the Subnet Manager. This is because the Subnet Manager is the original container for the subnets, and the Network Manager contains virtual network elements.

Declare Subnet

Through the auto-discovery process in the VMS, existing subnets are detected and displayed by the Subnet Manager. The ability to add non-existing (or future) subnets to the network is provided by the Declare Subnet command, accessed from the Subnet Manager drop-down menu (figure 5-48). The new subnet is defined by its IP Address and Mask, as shown in figure 5-49.

Figure 5-49 Declare New Subnet dialog

Once defined, the new subnet will appear as a new icon under the Subnet Manager.

Populate Subnets

The Populate Subnets command instructs the VMS to query the Vipersat Manager for any network units that belong to a subnet and ensure that they are placed in the appropriate subnet.

RF Manager

The RF Manager is the controlling VMS service for all network satellites and site antennas. This is where the satellites are created and defined, along with the associated transponders and bandwidth pools that provide the allocatable spectrum for STDMA and SCPC carriers. This is also where the site antennas are created and defined, along with their associated converters that provide the RF interface for the network modems.

Once created and defined, the satellite(s) and the associated site antennas are copied into the Network Manager which provides the primary operator interface for these items. Opening a network satellite provides the Spectrum view which displays the transponder(s), pools, and the active carriers, as shown in figure 5-50.

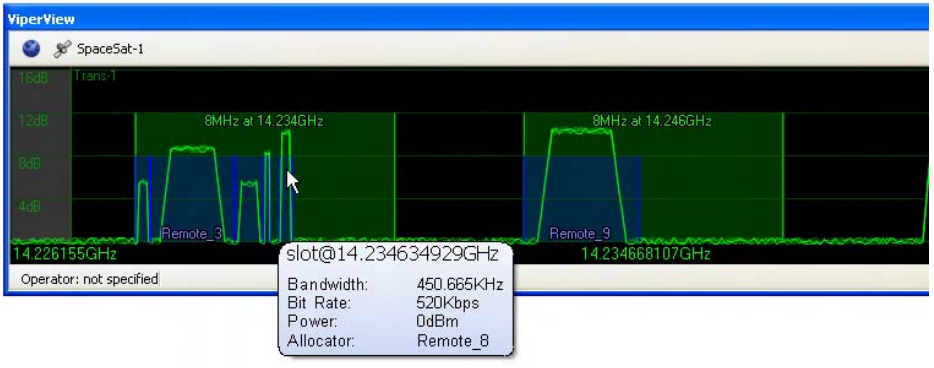


Figure 5-50 Satellite Spectrum View

Selecting an antenna from the RF Manager tree displays information relating to the associated Up converter and Down converter (figure 5-51).

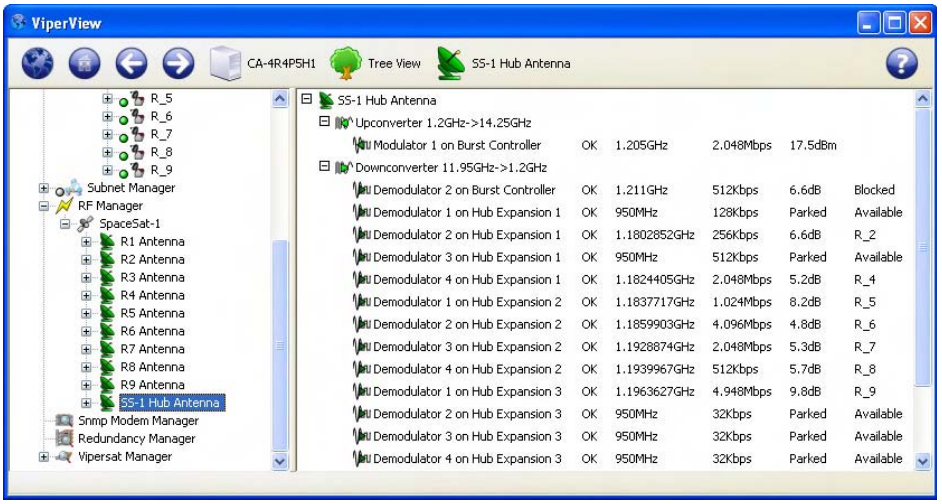


Figure 5-51 Antenna View, Hub Site

Switching Manager

The Switching Manager is the switching engine in the VMS, and manages all switching functions for both InBand and Out-of-Band modem units. Although this manager appears in the list of VMS service managers, there are no usable interfaces for the operator.

SNMP Modem Manager

The SNMP Modem Manager is the controlling VMS service for all non-Vipersat (Out-of-Band) modems. Modem units that do not have a Vipersat Network driver—and thus can not be configured for InBand management—are unable to utilize IP routing functions to communicate with the VMS, and instead utilize SNMP for these communications and are managed by the SNMP Modem Manager when functioning in a Vipersat satellite network.

For additional information on the SNMP Modem Manager, refer to Chapter 6, “SNMP Managed Units”.

Redundancy Manager

The VMS Redundancy Manager is the controlling service for N:M Hub modem redundancy. This service provides for the protection of critical VMS network modems operating in the Hub mode, and enhances overall network reliability by backing up primary components with standby backup units. The N:M redundant architecture is software driven utilizing IP packet control.

A representative block diagram of Hub modem redundancy is shown in figure 5-52, below.

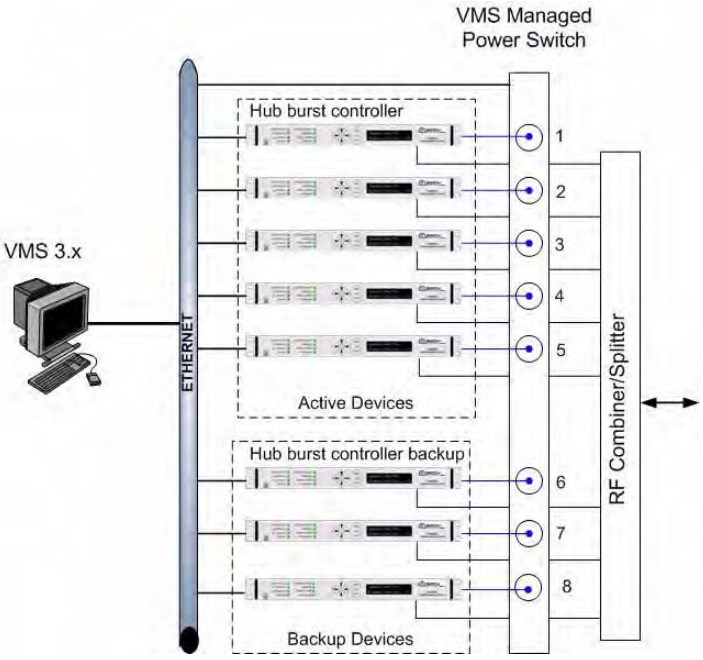


Figure 5-52 N:M Hub Modem Redundancy

For additional information on the Redundancy Manager and its usage, see Appendix C, "Redundancy".

Vipersat Manager

The Vipersat Manager is used to set the management addresses, register the Network IDs, and define the communications timeout parameters for the networks that will be managed and controlled by the VMS. This service manager maintains the comprehensive list of all registered network units, along

with their current health status—OK, Alarmed, or Disconnected. The units are identified and correlated with the network ID to which they are configured.

As new units are added and announce themselves to the network, the Vipersat Manager service processes and receives them. Once received, each unit is promoted to the Subnet Manager according to their addressing masks. Upon VMS startup, each network appearance under Vipersat Manager orders the units first by device type, then by IP address within the type.

The Network View under the Vipersat Manager displays all of the units sharing the same network number, as shown in figure 5-53.

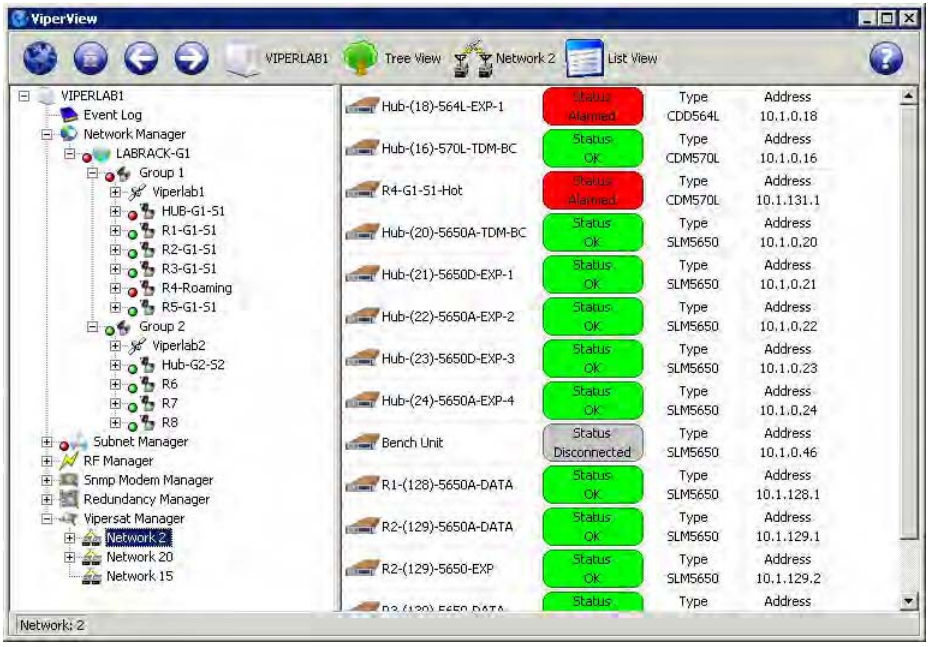


Figure 5-53 Vipersat Manager Network View

Global Reinit and Scan Network, commands to force the management system to poll for network device updates, are executed from the Vipersat Manager. Also, Vipersat network modem/routers and/or ROSS units can be created with this VMS service, allowing these units to be predefined prior to being placed into service in the network.

Application Image Manager

Firmware for Vipersat network modems can be upgraded using the Application Image Manager feature in the VMS. A library of binary (.bin) modem image

files can be created, from which a firmware version can be selected and Put (transmitted) to a network unit, as illustrated in figure 5-54 through figure 5-57.

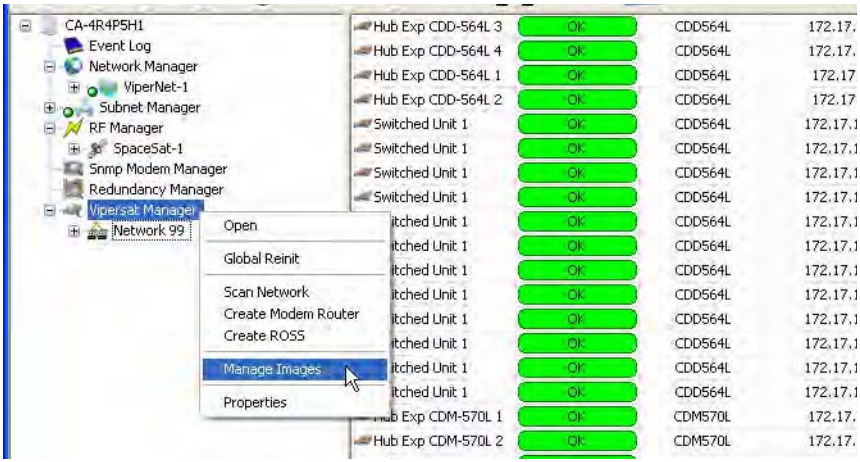


Figure 5-54 Manage Images command

Selecting the **Manage Images** command from the Vipersat Manager menu will open the Image Manager window, where the image library is held.

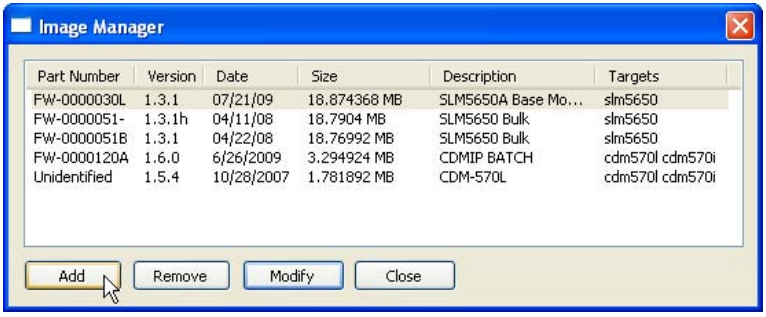


Figure 5-55 Image Manager, Library Setup

With Windows file selection, new images can be added to the list.

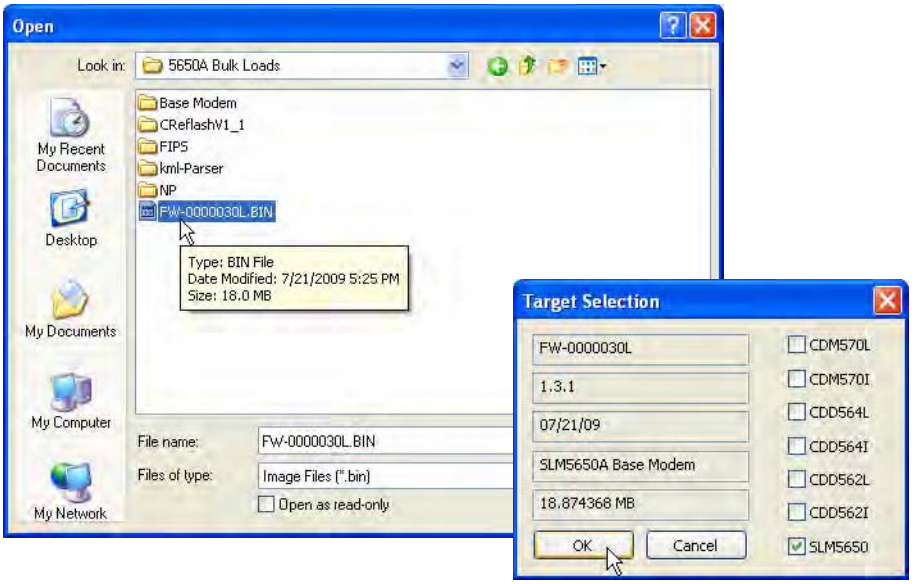


Figure 5-56 Image Manager, Add Selection

To upgrade the firmware image for a network unit, select the **Upgrade** command, then choose the required image from the library.

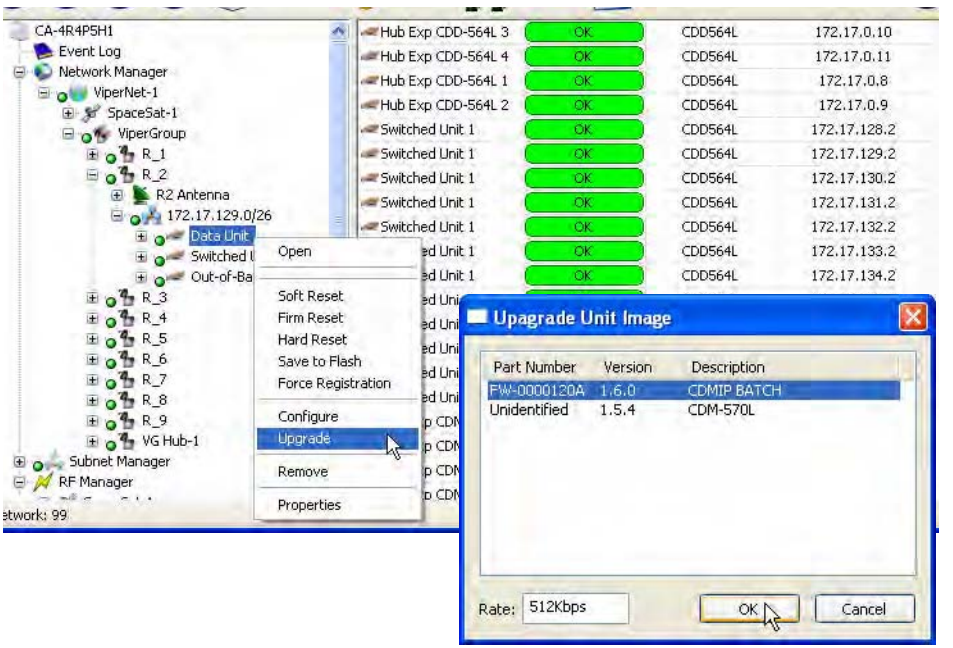


Figure 5-57 Upgrade Unit Image

CHAPTER

6

SNMP MANAGED UNITS

General

The SNMP Modem Manager is the controlling VMS service for all non-Vipersat (Out-of-Band) modems. Modem units that do not have a Vipersat Network driver—and thus can not be configured for InBand management—are unable to utilize IP routing functions to communicate with the VMS, and instead utilize SNMP for these communications and are managed by the SNMP Modem Manager when functioning in a Vipersat satellite network.

This chapter describes integrating non-Vipersat units into a VMS-controlled satellite network.

Controlling Non-IP Modems

Before VMS can communicate with a non-IP capable modem, the modem must have an IP-addressable unit, such as the Comtech CiM-25/600 or CiM-25/600L attached and assigned a valid IP address using procedures described in the appropriate product documentation, and described in the following procedure.

Modems such as the CDM-700, SLM-5650 or CDM-570 have a built-in Ethernet interface and do not require an external CiM unit. Refer to these unit's documentation for the procedure for assigning a valid IP address to the unit.

Note: Check the unit's documentation for specific, detailed procedures.

Once a valid IP address has been assigned to the target CiM-25, install the CiM-25 on its companion CDM-600L. The modem must then be declared in VMS using the following procedure.

1. Connect the target CiM-25 unit to your workstation and assign a valid IP address for the network where the CiM-25 and its companion CDM-600L are to be installed

2. Reconnect the CiM-25 to its companion CDM-600L, then connect the ethernet LAN and apply power as required.

Note: The CiM-25 must be plugged into an operating modem (except during setup) in order for it to operate reliably. A CiM-25 operating disconnected from a modem will exhibit erratic ethernet communications. Refer to the CiM-25 manual for additional information.

SNMP Modem Manager

The SNMP Modem Manager is the controlling service for all non-Vipersat modems. Right-clicking on the manager icon opens a menu with commands to Open the manager, Declare Modems, and view the manager Properties.

Set Polling Options

1. To set the manager **Polling Options**, right-click on the SNMP Modem Manager to display the drop-down menu shown in figure 6-1.

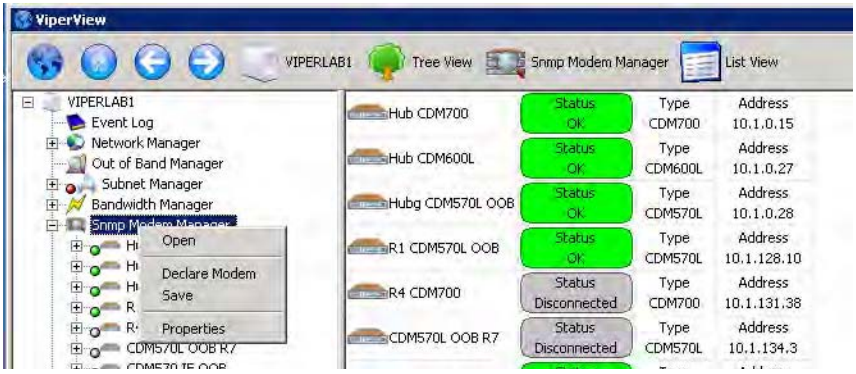


Figure 6-1 SNMP Modem Manager command menu

2. Select the **Properties** command to open the Properties page, shown below in figure 6-2.

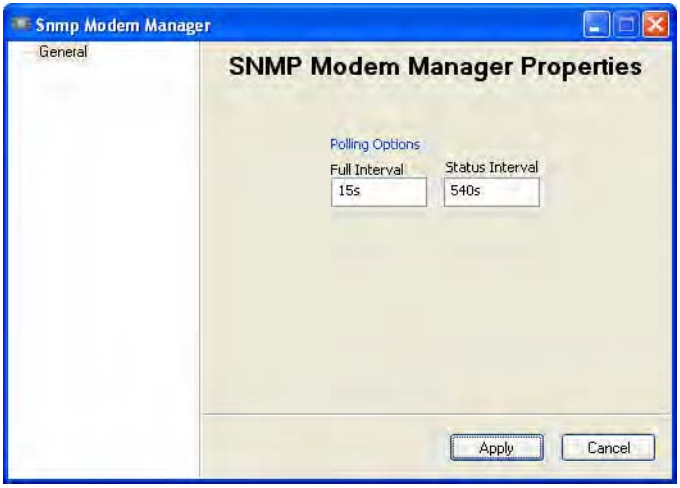


Figure 6-2 SNMP Modem Manager Properties

There are two settable parameters in the SNMP Modem Manager Properties—the Full Interval Poll and the Status Interval Poll. They are described below.

- **Full Interval** – The time in seconds, when connected to the device, that a full poll will occur for all parameters.
- **Status Interval** – The time in seconds between polls for unit status to detect alarm states.

Configure SNMP Modem

The following procedure demonstrates using the SNMP Modem Manager to configure a CDM-600L modem, as an example.

1. Right-click on the SNMP Modem Manager and select the **Declare Modem** command from the drop-down menu.

   The **New SNMP Modem** dialog will open, figure 6-3.

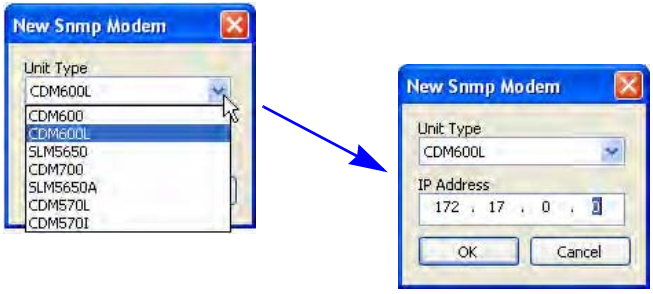


Figure 6-3 New SNMP Modem dialog

2. From the **Unit Type** pull-down menu, select the model that corresponds to this modem. In this example, the CDM600L modem is selected.

3. Enter the assigned **IP Address** for this modem (the CiM-25 address).

4. Click the **OK** button.

   The unit will now appear listed in the SNMP Modem Manager. Select the manager to see the modem appearance in the right panel of the ViperView window.

5. Right-click on the newly added unit and select **Properties** from the drop-down menu to display the **General** tab shown in figure 6-4.

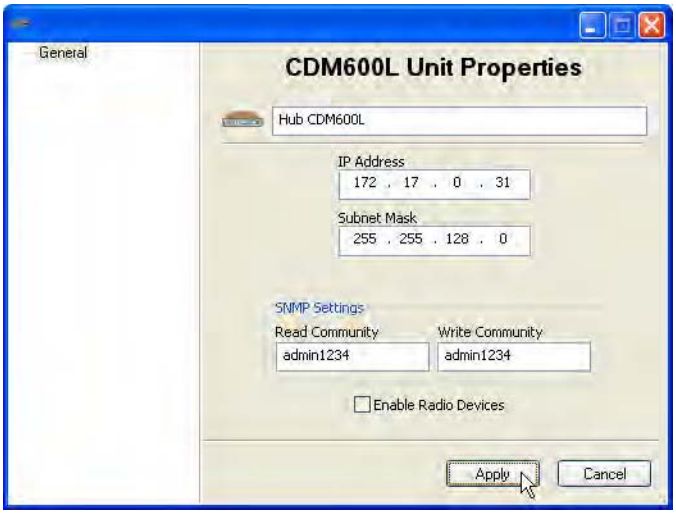


Figure 6-4 CDM-600L Unit Properties dialog

a. Assign a name to the modem in the first field for reference purposes and for identification in ViperView.

b. The **IP Address** field is a read-only display for the target modem.

c. Enter the **Subnet Mask** in the designated field.

d. Ensure the SNMP Settings are correct.

For a CDM-600/L, the Read and Write Communities are **admin1234**.

For all other units, the Read Community is **Public** and the Write Community is **Private.**

e. If the modem is connected to a BUC, LNB, or other device, select the **Enable Radio Devices** check-box to have this configuration recognized by the VMS.

f. Click on **Apply**, then Close the window.

Once the modem and its companion CiM-25 are configured and are connected to the network, the unit will appear under the SNMP Modem Manager, as shown in figure 6-5.

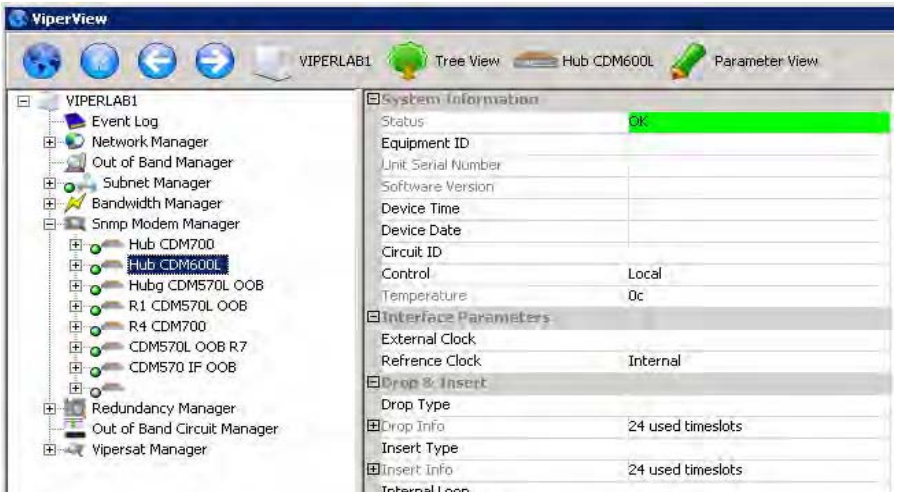


Figure 6-5 SNMP Modem Manager units

Parameter View

The **Parameter View** display shown in figure 6-6, displays unit information and options available for the unit selected in the SNMP Modem Manager. Refer to each unit's documentation for detailed information on setting or changing any of the parameters listed here.

The commands presented on the drop-down menu shown in figure 6-6 are:

- **Apply** – Clicking the **Apply** command writes any changes made to the unit's configuration in the **Parameter View** to the unit's active memory. In order to make the changes permanent, these changes must be saved to the unit's flash memory.
- **Revert** – To discard any changes and return the parameter(s) to the previous setting(s), click the **Revert** command to revert the setting(s) back to the original configuration.

NOTE

Note: If the changed parameter has been marked with the **Dirty Selected** command (see below), the **Revert** command will not function.

- **Refresh** – Clicking the **Refresh** command will read the current state of all parameters from the unit and update them in the Parameter View display.

- **Dirty Selected** – If you have made a change, selecting the changed item and then clicking the Dirty Selected command marks the item as changed and it will be changed in the unit's active memory.

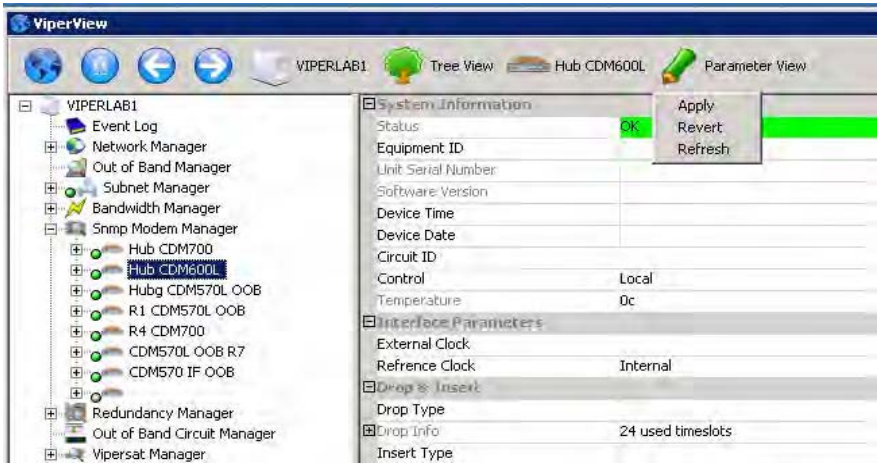


Figure 6-6 Parameter View

Before continuing with this process, select the **Refresh** command on the drop-down menu. This will ensure that the most current information is available for the unit.

The **Parameter View** contains both information that is hard-coded in the unit and cannot be changed, as well as information that can be edited. This is useful for out-of-band units, allowing their configurations to be modified with the VMS.

Configuring the RF Chain

The following procedure shows how to configure the SNMP Modem RF chain, thus enabling the carriers to be viewed and monitored with the VMS.

1. Expand the modem icon to show the Modulator and Demodulator. Select the appropriate antenna and expand the Up and Down converters, as shown in figure 6-7.

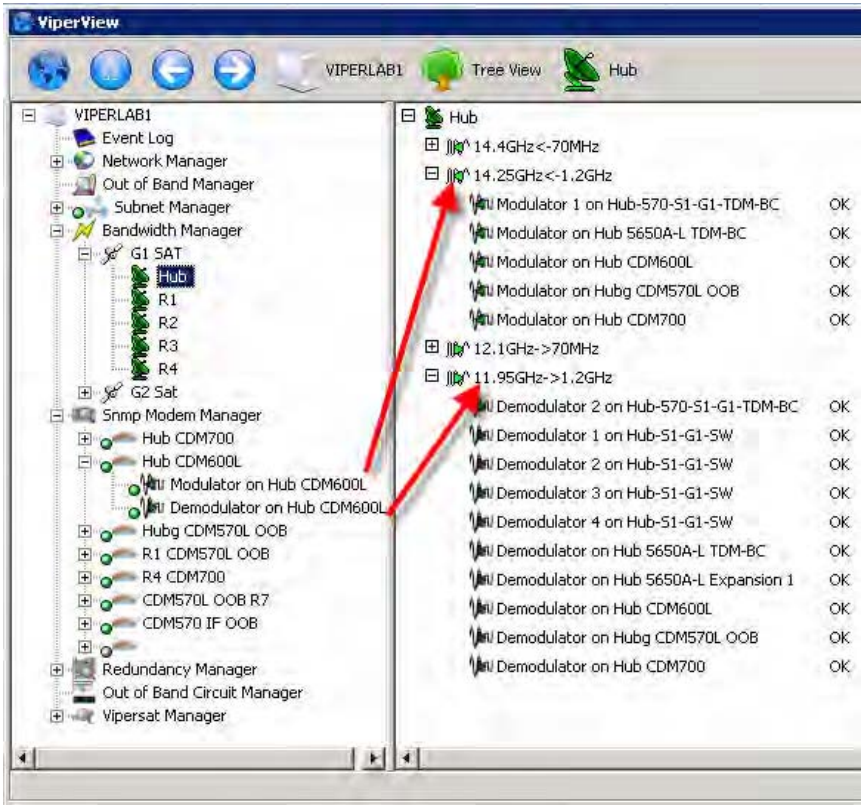


Figure 6-7 Configuring RF Chain, SNMP Modem

2. Drag-and-drop the modulator onto the up converter and the demodulator onto the down converter.

3. Right-click on the antenna, and select the **Properties** page.

4. Select the **Out of Band** tab, as shown in figure 6-8 below:

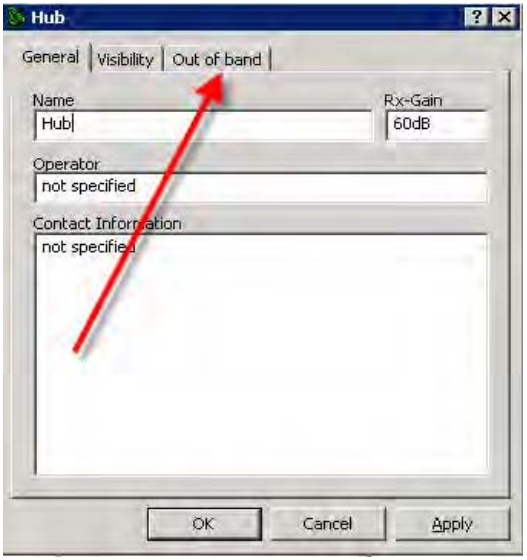


Figure 6-8 Out of Band Antenna Tab

5. Highlight the Modulator for the new SNMP modem and click **Enable**, as shown in figure 6-9.

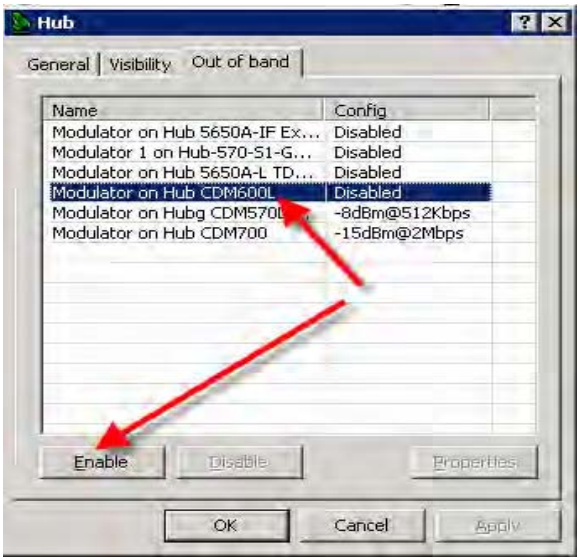


Figure 6-9 Selecting the Out-of-Band Modulator

6. A dialog box will open prompting for a **Bit Rate** and **Power** to be assigned to this unit.

Set them to a combination that will give an appropriate level.

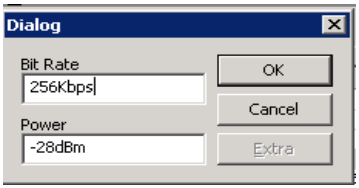


Figure 6-10 Out-of-Band Modulator dialog

APPENDIX

A

VMS CROSS BANDING

The VMS has the capability to accommodate applications involving satellite cross strapping and cross banding. The VMS is able to recognize, manage, and control satellite circuits which utilize more than one frequency. The typical satellite bands currently in use include:

- C-Band
  - Downlink 3.7 to 4.2GHz
  - Uplink 5.9 to 6.4GHz
  - 24 36MHz transponders
- Ku Band
  - Downlink 11.7 to 12.2 GHz
  - Uplink 14.0 to 14.5 GHz (FSS)
  - 24 36MHz or 12 72MHz transponders
- Ka Band
  - Downlink 17.7 – 21.2GHz
  - Uplink 27.5 – 31.0GHz

The VMS cross banding function allows VMS to manage and control the following satellite circuit configurations:

- Two remote terminals are in different antenna footprints on the same satellite where, for example, one antenna serves C-band users while another antenna serves Ku band users.

- The satellite has mapped the transponder from one antenna to a transponder on another antenna.
- The satellite serves as an RF inter-band relay which is also referred to as cross strapping

In the example shown in figure A-1 the C-band and Ku-band transponders 20 through 24 are cross banded.

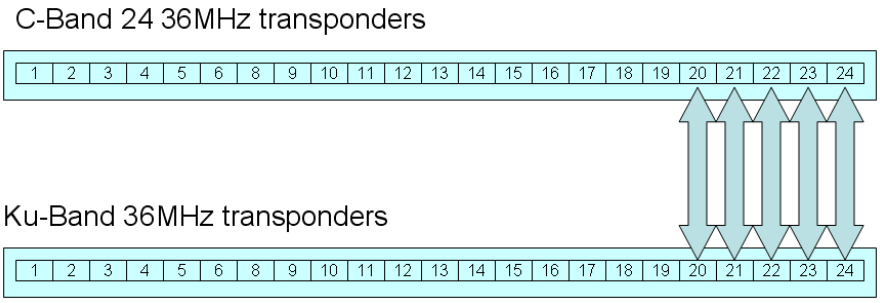


Figure A-1 Cross Banded Transponders, C-band & Ku-band

Vipersat Cross Banding Solution

Figure A-2 illustrates a schematic representation of a cross banded satellite network.

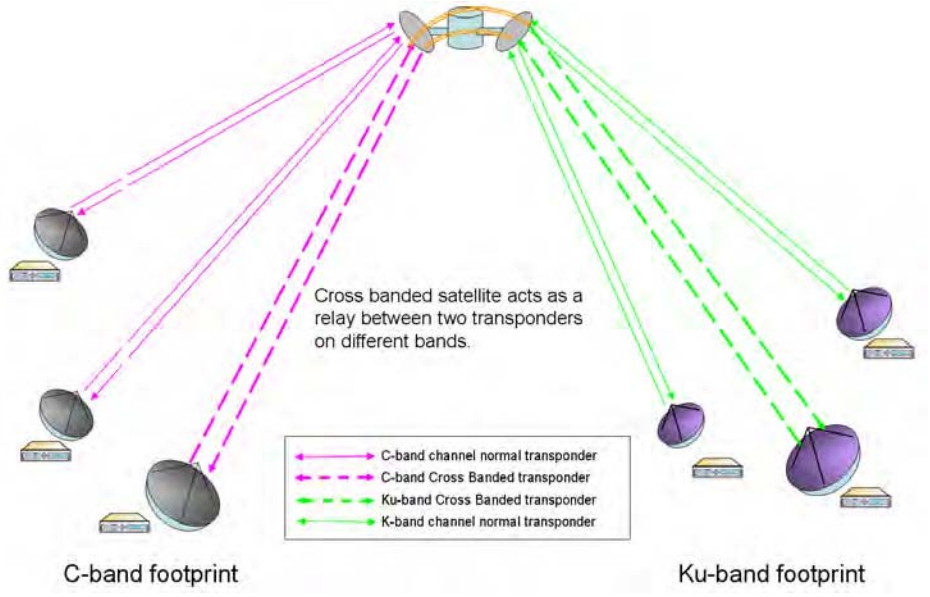


Figure A-2 A Cross Banded Satellite Network

The VMS does the following to allow a cross banded satellite network to be included in its management and control functions:

- VMS adds a translation override frequency to the transponder object which is used in place of the satellite's normal translation frequency
- The VMS bandwidth allocation logic then:
  - Selects demodulators first
  - Builds a collection of frequency limits based on available transponders
  - Selects modulators based on their intersecting limits

NOTE

Note: The VMS cross band function has no effect on non-cross banded configurations, and supports multiple transponders.

Figure A-3 shows a cross banded network configuration.

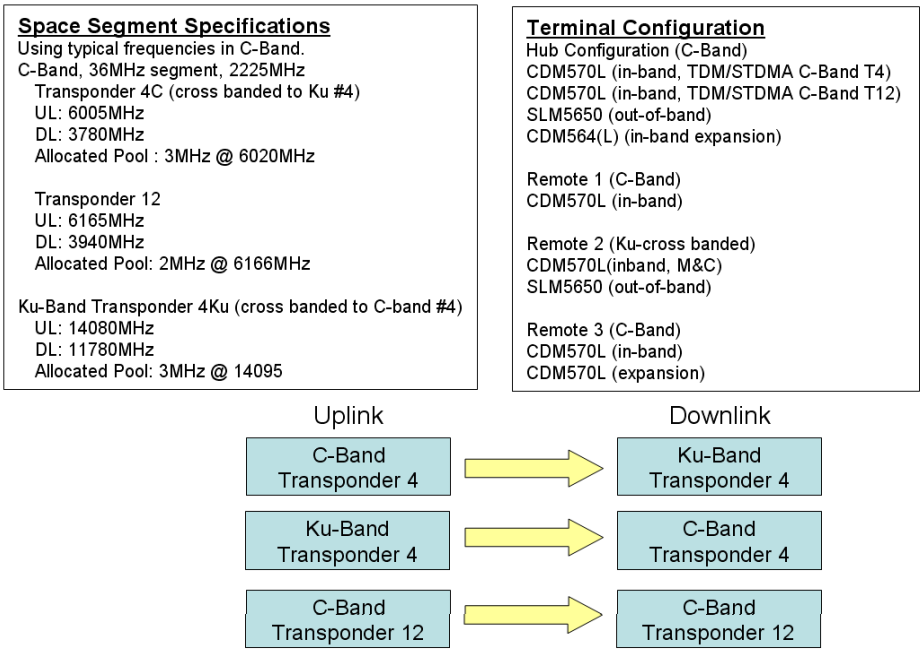


Figure A-3 VMS Cross Banded Network Configuration

In response to the network configuration shown in figure A-3 the VMS would:

1. Create Satellite - Set center frequency to 6.1375GHz and translation frequency to 2.225GHz

2. Create Transponder 4C (cross banded to Ku) - 6.005GHz, 36MHz

3. Perform a Translation Override = (6.005 – 11.78) = -5.775GHz

4. Create Pool, 3MHz at 6.020GHz

5. Create Transponder 12C - 6.165GHz, 36MHz

6. Create Pool 4, 2MHz at 6.166GHz

7. Create Transponder 4Ku - 14.155GHz, 36MHz

8. Perform a Translation Override = (14.08 – 3.78) = 10.30GHz

9. Create Pool 4, 3MHz at 14.170GHz

Figure A-4 illustrates the results of the VMS solution for managing and controlling the cross banded network described above.

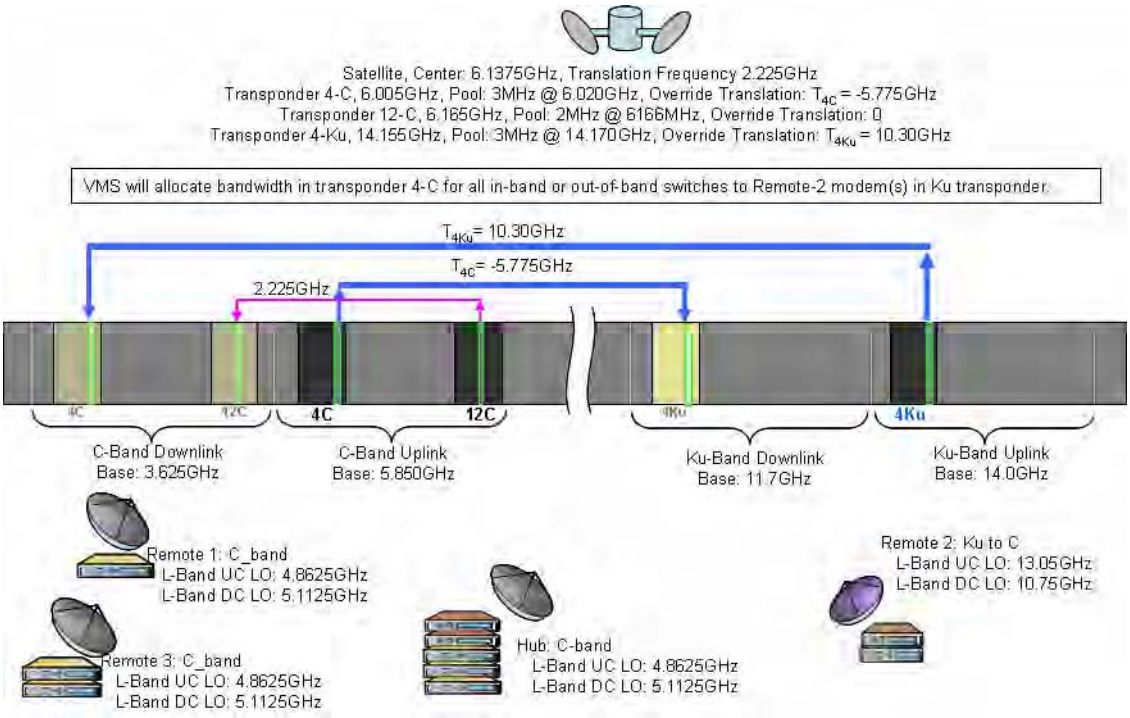


Figure A-4 VMS Cross Banded Network Solution

The VMS calculated Translation Override Frequency (TOF) is an integer value in Hertz that represents frequency offset of the cross banded transponders, mapping the modulator frequency to the demodulator frequency. When the TOF is set to a non-zero value, this value overrides the default satellite translation value and is calculated with respect to the Downlink (Rx) frequency.

The TOF value is positive if the cross banded downlink transponder frequency is lower than the Tx transponder band. The TOF value is negative if the cross banded downlink transponder frequency is higher than the Tx transponder band. Note that the VMS always subtracts the translation frequencies.

The figures below show the Create Transponder dialog for setting up VMS cross banding values. In this example, the cross banding is between C-band and Ku-band.

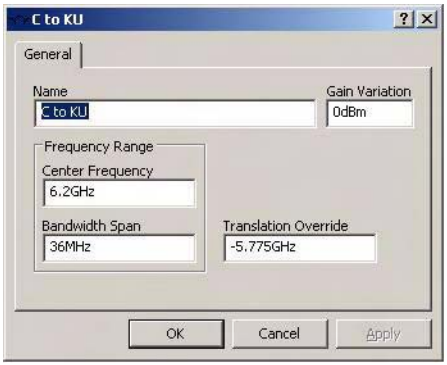


Figure A-5 Transponder dialog, C to Ku

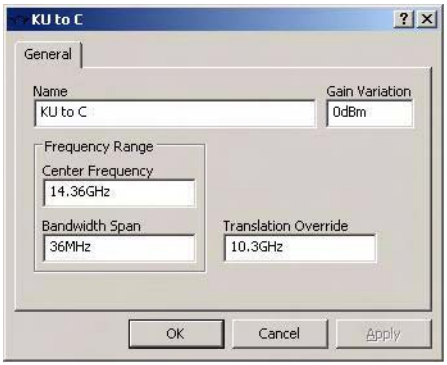


Figure A-6 Transponder dialog, Ku to C

To create a new transponder, right-click on the Satellite icon and choose **Create Transponder** from the pull-down menu that appears. On existing networks, right-click in the black portion of the satellite spectrum view, choose **Properties**, and the transponder window will open displaying the current settings. Alternatively, edits can be performed by displaying the antenna and transponder list.

In some instances, transponders may have different translation frequencies than others on the same band, thus requiring a translation override frequency configuration even without it being a cross banding or cross strapping application.

APPENDIX

B

ANTENNA VISIBILITY

General

Antenna Visibility is a powerful tool in the VMS that allows an operator to control the spectrum used by the VMS switching engine. Simply stated, it allows the operator on a site by site basis to block portions of the satellite or transponder bandwidth from being used by the RF manager, even if a defined bandwidth pool exists within the blocked portion.

Antenna visibility can be used in a variety of ways. However, great care must be taken when implementing this powerful tool in a Vipersat satellite network, or unexpected results will occur.

Warning: Do Not use antenna visibility without a thorough understanding of the mechanics involved. It is highly recommended that an operator complete the Vipersat Advanced VMS training course that includes coverage of Antenna Visibility prior to configuring a live network with this feature.

Using Antenna Visibility

Antenna Visibility is accessed by right-clicking on the desired satellite antenna and selecting Properties. The antenna properties window will open. Click on the **Visibility** tab to display the antenna visibility window. The figure below shows the antenna visibility flag as defaulted by the VMS. The default values ensure that the entire spectrum is available so that there are no limitations in effect when this feature is not used.

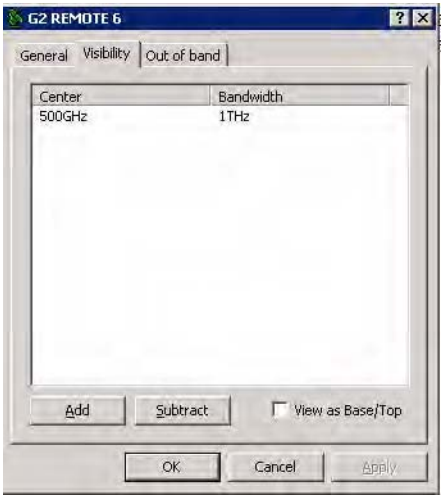


Figure B-1 Antenna Properties, Visibility Tab

An antenna with these settings is essentially clear for all satellite bands. Under most conditions, it is advisable to leave the visibility settings at the default values. Should a network application call for the use of antenna visibility, start by configuring the desired transmit and receive frequencies for the antenna to be able to use, as illustrated below using standard Ku Band.

Note: The VMS is not limited to any particular frequency band.

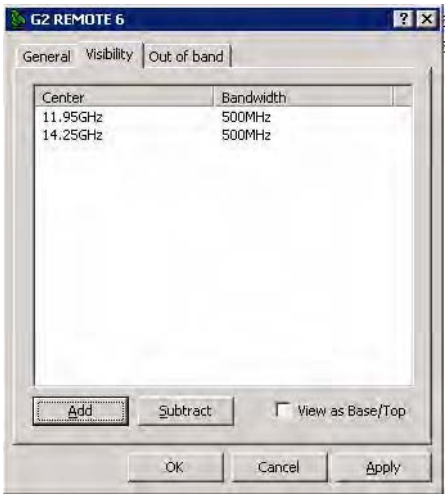


Figure B-2 Ku-band Visibility Ranges, Center/Bandwidth

The frequencies can be viewed, as above, with a center frequency and bandwidth, or as shown below with frequency ranges. Clicking in the **View as Base/Top** box will toggle between these two views.

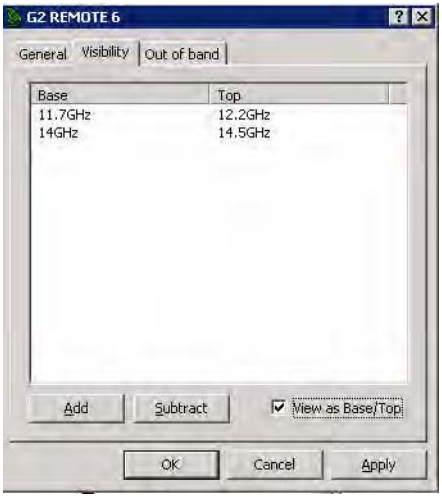


Figure B-3 Ku-band Visibility Ranges, Base/Top

The **Add** and **Subtract** buttons are used to modify the visibility by either adding or subtracting frequency ranges to/from the antenna. Clicking on either one of these buttons opens a **Frequency Range** dialog for specifying the new visibility range. Note that the appearance of this dialog reflects the appearance of the visi-

bility tab, showing either a center frequency with bandwidth, or a base frequency and top frequency. This appearance can be toggled using the **View as Base/Top** check box.

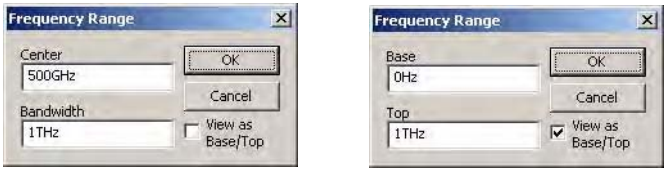


Figure B-4 Frequency Range dialogs

Enter the range of bandwidth to be added or subtracted and select **OK**.

Subtracting a frequency range from within visible bandwidth creates a visibility block, or mask, for that portion of the spectrum. To remove an existing visibility block and restore visibility for that bandwidth, select the two adjacent ranges and click **Add**. This will display the range of bandwidth blocked, as shown in the figure below. By selecting **OK**, the range will be added and the two ranges will become merged into one continuous range.

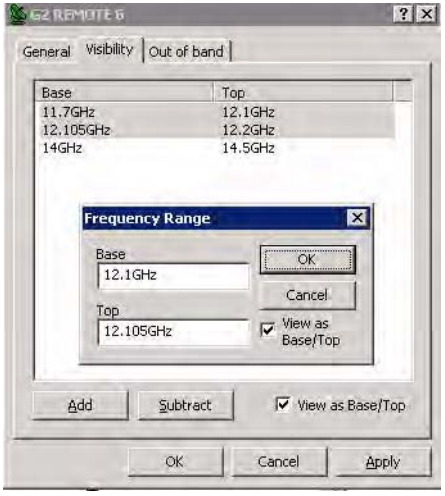


Figure B-5 Merging Visibility Ranges

Example — Blocking Spectrum Affected by Local Ground Frequency Interference

In the example shown here, Antenna Visibility is used to block off a portion of a bandwidth pool at a given remote site due to ground interference on the lower part of the transponder spectrum.

In this case, assume there is ground interference on the lower end of the transponder that overlaps into the bandwidth pool, as illustrated in the figure below.

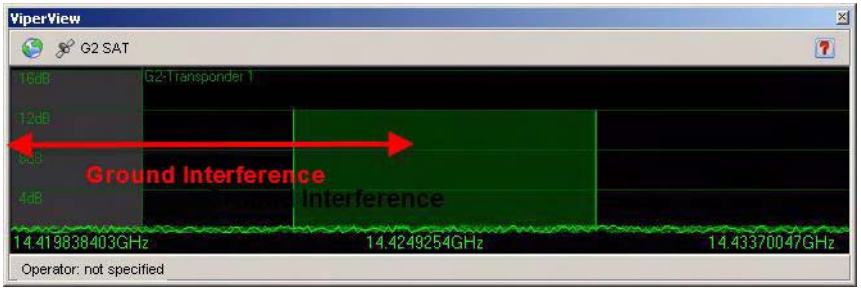


Figure B-6 VMS Bandwidth Pool with Ground Interference

Note: The satellite spectrum view provided by the VMS, as shown here, displays the transmit (uplink) carriers from the Hub and the remote sites. The corresponding receive (downlink) carriers are determined by the frequency offsets but are not visible.

This interference at the remote site may not affect the transmission path, but could prevent reception in the lower portion of the pool. With no antenna visibility block, the VMS would perform a switch with this remote, resulting in the carriers being placed as shown below. This places the corresponding receive carrier within the ground interference frequency range, and could cause a disruption in communications.

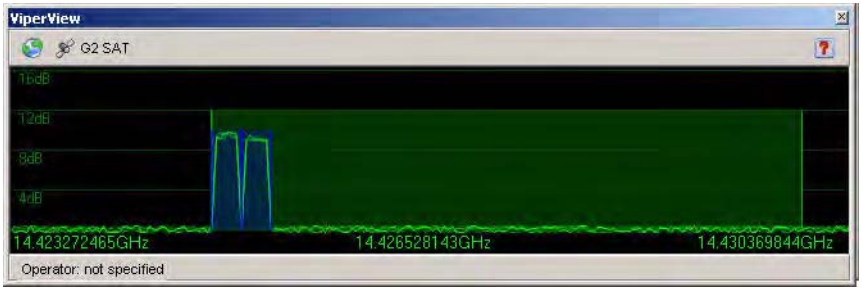


Figure B-7 Transmit Carriers, No Visibility Block

Using the visibility Subtract function, a new block for this area of interference can be created for the remote antenna, as shown in the figure below.

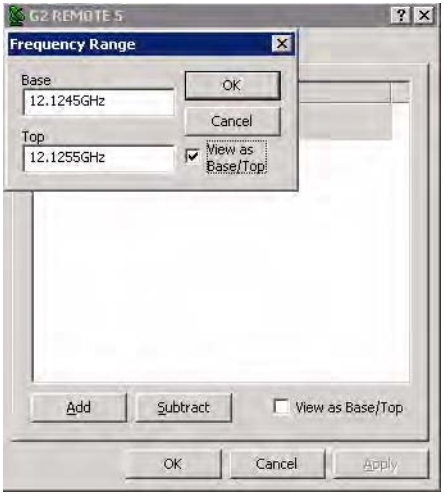


Figure B-8 Visibility Subtract dialog

The revised visibility map now shows a visibility block between 12.1245GHz and 12.1255GHz which represents the bottom 1MHz portion of the pool experiencing ground interference.

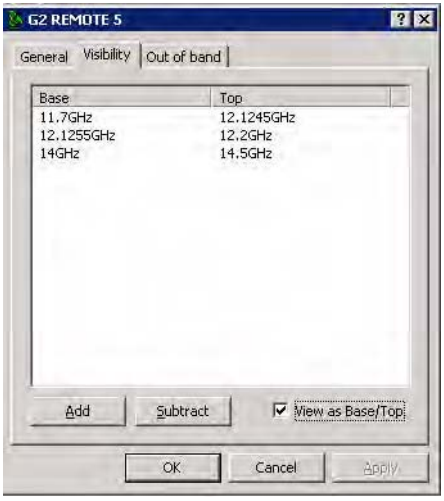


Figure B-9 Visibility Ranges with Blocks

This configuration results in the VMS switching as shown below. The receive carrier for the remote is now outside of the area of interference.

Figure B-10 Transmit Carriers Repositioned, Visibility Block

{ *This Page is Intentionally Blank* }

APPENDIX

C

REDUNDANCY

General

This appendix describes the optional redundancy services that protect critical Vipersat network equipment. The two main services offered are **VMS Redundancy** and **Hub Modem Redundancy**.

VMS Redundancy provides for N:1 redundant VMS server(s) (standby) co-located at the Hub alongside the active VMS server. This configuration provides for the automatic switch-over to a standby server in the event of a failure of the active server.

Hub Modem Redundancy provides for the operation of N:M multiple primary and multiple secondary modems installed at the Hub. If a protected device fails, its output is automatically removed from the satellite network. A replacement device, loaded with the failed device's configuration, is booted into service and its output is switched into the satellite network, replacing that of the failed device.

VMS Redundancy

Description

VMS redundancy (protection) increases the system availability of a Vipersat-enabled network by protecting the network from a VMS server failure. In the current release, N:1 redundancy is a monitored hot-standby configuration with N+1 VMS servers running in parallel.

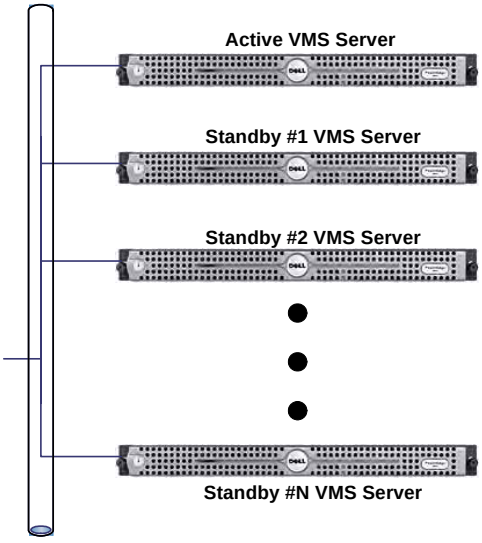


Figure C-1 Active and Standby VMS Servers, N:1 Redundancy

Each server can switch between two mutually exclusive modes of **active** or **standby**. The active/standby hierarchy is specified through the assignment of a priority level attribute. In the event that the active server fails, the backup server with the highest priority is hot-switched to assume control of the satellite network, replacing the failed server.

Note: The redundant VMS protection feature can only be activated with a valid license in the server(s) USB Crypto-Box key.

Redundant Hot-Standby

In a redundant configuration, the VMS servers run in parallel. The VMS database on the standby server(s) is continuously maintained, in real-time, as a mirror image of the VMS database running on the active server.

Note: It is recommended that all servers be co-located at the same site and be connected to the same Ethernet LAN. The monitoring workstation should also be co-located. This is to eliminate reliability issues that may be associated with the terrestrial data-link communications between a geographically remote server and NOC units. A data-link failure may result in contention of automatic switch-over control and interruption of restoral processing.

Protection Switch-over

If the active server fails, the VMS protected by N:1 redundancy immediately switches to a standby server. The VMS running on the standby server picks up and executes the ongoing network management tasks until the failure in the active VMS server is resolved by human intervention.

Both the active and standby servers operate in a query-peer mode to determine which server is to be the active VMS server in the network.

If, for example, the active VMS server fails causing a protection switch, a standby VMS server assumes control of the network. While the standby server is actively managing the live network, a previously active server that is being restarted cannot assume the active server role without first checking for the presence of an active VMS server already managing the network. The process for initiating and managing the transitions between active to standby modes is described below.

Active to Standby Switch

This transition occurs whenever:

- An automatic switch-over is triggered by the failure detection mechanism due to active VMS failure, or
- A manual switch-over is invoked from the active console by, for example, taking down the active server for maintenance.

A switch-over from the currently active server back to the server with higher priority (once recovered) is NOT automatic. An operator must manually perform the switch at the active server's console.

When a server with a higher priority is restarted, the VMS on the server detects an active peer on the network (a previous standby server) and automatically enters standby mode, and remains in standby mode until either an operator manually switches the server back to active mode, or a failure occurs causing an automatic switch-over.

For instructions on performing a manual switch-over, refer to the section "Manual Switching" on page C-13.

Active Server Role

The active VMS server has the following specific privileges that differ from a standby server:

- There can be only **one** (1) VMS server actively managing the network.
- The active server is considered the default VMS server for configuration and network topology purposes.
- The active server's database is considered the master copy. The standby server(s) receives a copy of the master database from the active server as a part of its start-up process and automatic synchronization.
- The first VMS server to come on-line assumes the active mode provided that all redundant servers are online and no other server is operating in active mode.
- The active server is the only unit that may initiate a manual protection switch-over (a transition from active-to-standby mode or standby-to-active mode). This is a two-step event controlled by the operator/administrator: the Active server is first *Deactivated*, then a Standby server is *Activated*.

Standby Server Role

A VMS standby server has the following specific functions that differ from the active VMS server:

- Upon startup, a standby VMS enters a query-peer mode where it attempts to discover a peer VMS in active mode. The VMS enters a standby mode when an active VMS is discovered.
- A standby VMS server's default mode is standby. It can only enter active as a result of a protection switch, either automatic or manual.

Automatic VMS Activation

An Auto Activate function is available to resolve any activation conflicts in the event that all servers go offline temporarily. Once the servers return to online status, the server that was the last active will automatically reactivate and assume the active role.

Server Synchronization

Server synchronization is always executed by/from the active VMS server, and is performed to ensure that all standby servers receive any necessary updates due to changes in the master database that resides in the active server. Two types of server synchronization occur with a redundant VMS configuration, automatic and manual.

Automatic Synchronization

As the name implies, automatic synchronization occurs automatically by the active VMS and is performed whenever any changes occur that are associated with automatic system functions, such as automatic switching, device redundancy, etc. The active server maintains a memory cache that holds the updates until they can be pushed out to the standby servers by an automatic synchronization that occurs during the VMS heartbeat. The updates are tagged onto the heartbeat message that is sent by the active server to the standby servers.

Manual Synchronization

Manual synchronization, also referred to as “full synchronization”, must be performed by administrator/user command for any changes not related to automatic VMS functions, such as whenever any database configuration changes are made to the server. Should a standby server be restarted, when it rejoins the redundancy group, the sequence of updates may be lost and a manual synchronization is required to ensure that the standby receives the most current database from the active server.

Note that this operation can be automated on a 24-hour basis with the *Auto Synchronize* feature. See the section, “Auto Synchronize” on page C-10, for how to configure this feature.

During a full synchronization, the active VMS service is temporarily taken down to avoid any changes occurring during the synchronization process. The active server sends the contents of the temp file holding the entire database backup to each standby server via simultaneous unicasts. If, for any reason, there is a failure with this update process, a notification will appear in the windows log.

Server Contention

Server contention is a built-in protection mechanism for redundant VMS operation. A situation may occur where the active server briefly loses network connectivity—a network cable is unintentionally pulled, for example—before communications are restored. The first priority standby will become active due to the lost heartbeat of the former active server. When the former active server returns, it will detect that there is another active server in operation, and will enter the contention state.

When this is sensed by the current active server, it also will enter the contention state. In such a situation, there is no way for the system to determine which server has the most current up-to-date database, and both servers will immediately de-activate to protect the current status of the network. A generated alarm,

both visual and audible activated, will appear on each server. In addition, an SNMP trap will be generated.

In this condition, VMS services are still running, but no changes of state can be executed in the network until the condition is cleared. For instructions on clearing server contention, refer to the section “Clearing Server Contention” on page C-14.

Server Status

The VMS Connection Manager provides the status of the VMS and each of the servers in a redundancy group. The Connection Manager, when running, will display its icon in the Windows Task bar at the bottom right of the screen. When the mouse is positioned over this icon, a status pop-up appears displaying information on the VMS and the servers, as shown in figure C-2, below.

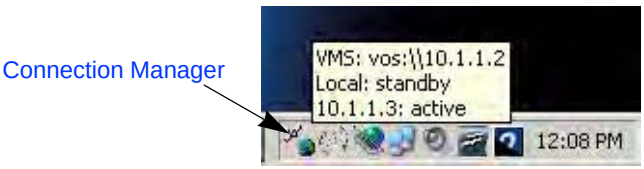


Figure C-2 Server Status Pop-Up

There are four possible server states:

- active
- standby
- contention
- disconnected

If no servers are connected, the status message will read “Vipersat Management System Disconnected”.

The server to which the console is currently connected (the local server) is identified by whatever was entered in the **Connect To** dialog; either its assigned name or its IP address (as appears in the first line of the example shown in figure C-2). The next server status that is displayed is that of the local server, followed by any remote servers listed by their IP address.

Installing & Configuring VMS Server Redundancy

Installation of a redundant VMS server configuration in a VMS controlled network requires the following:

- Two or more dedicated servers and a client workstation.

- The servers and the workstation should be co-located (in the same physical location) and connected to the same Ethernet LAN.
- A dedicated IP address for each VMS server.
- A common domain for the redundant servers and the client workstation. Refer to Appendix D, “Domain Controller and DNS”, in this document for details for establishing the VMS server as a domain server.

Starting a redundant VMS configuration requires bringing up the VMS servers and the workstation using the following procedure:

1. Install VMS on each of the servers following the instruction in Chapter 2, “VMS Installation”.

2. Start the Vipersat Management System service and ViperView.

   Select **Vipersat Management System** from Windows Services and **Start** the service, if it is not already running.
   Note: It is recommended that this service be configured for **Automatic** Startup.

   Click **Connection Manager** on the path:
   Start > All Programs > VMS 3.x> Connection Manager

   The Connection Manager will prompt for the server to connect to. Select the server that is to be the initial Active server; typically, this is the server with the highest priority setting.

   The ViperView window will appear as shown in figure C-3.

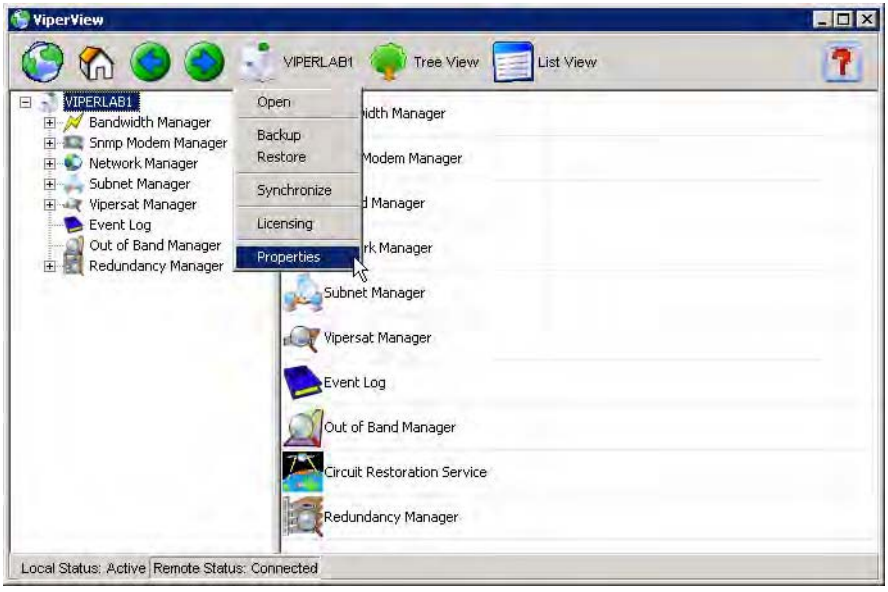


Figure C-3 ViperView, VMS Server Drop-down Menu

3. From the VMS Server drop-down menu, select the **Properties** command to display the VMS Server (VIPERLAB1 in this example) dialog window, shown in figure C-4.

The **Status** tab is displayed, providing the current status information for this server.

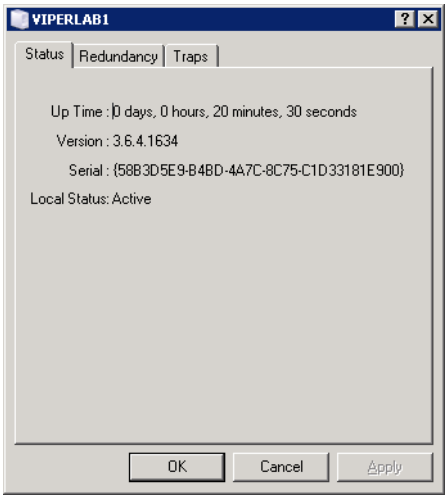


Figure C-4 VMS Server Properties, Status Tab

4. Click on the **Redundancy** tab to configure the redundancy settings for this server (figure C-5).

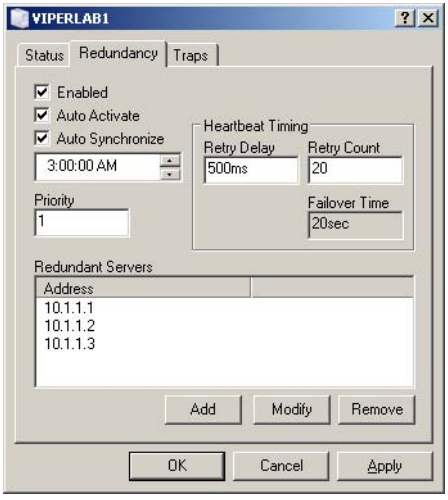


Figure C-5 VMS Server Properties, Redundancy Tab

Enabled

Clicking in the **Enabled** box selects/de-selects redundancy operation for this server. This setting must be enabled for each server that belongs to a redundancy group.

Auto Activate

Clicking in the **Auto Activate** box selects/de-selects this function. In the event that the redundant servers go offline temporarily, when the servers return to online status:

- with Auto Activate *selected*, the server that was the last active will automatically reactivate and resume the active role.
- with Auto Activate *de-selected*, a server will be activated only by an operator manually issuing an Activate command on one of the servers.

When choosing to use Auto Activate, each VMS server in the redundant group should be configured with the Auto Activate function selected.

Auto Synchronize

Clicking in the **Auto Synchronize** box selects/de-selects the periodic database synchronization operation for this server. It is recommended that this setting be enabled for each server that belongs to a redundancy group.

The daily time is generally set for when traffic is typically at a low level, such as early morning, for example.

Note that this feature provides a means of performing a full database synchronization *automatically*, that would otherwise have to be executed by the administrator/operator *manually*. Refer to the section, “Manual Synchronization” on page C-5, for more information.

Priority

The **Priority** setting identifies where this server ranks in the redundant server hierarchy for becoming active during a switch-over. The lower the number entered, the higher the priority.

Set the Priority to a unique number in the range 0 to 31.

Caution: No two servers in a redundancy group should ever be assigned the same priority; each server must have a unique number to prevent contention.

Heartbeat Timing

The Redundancy **Failover Time** is set by specifying the values for **Retry Delay** and **Retry Count**. The Failover Time is the amount of time that will pass prior to a switch-over to a Standby server following a failure in communications (heartbeat) with the Active server.

The Retry Delay represents how long the system waits before sending another heartbeat request. The Retry Count represents how many heartbeats are missed

before the device is determined to be offline. Failover Time is calculated by taking twice the Retry Delay value and multiplying it by the Retry Count value.

Generally, it is recommended to use the following values:

- For networks *with up to 100 nodes* — Retry Delay = 500 ms, Retry Count = 10.
- For networks *with over 100 nodes* — Retry Delay = 500 ms, Retry Count = 20.

Redundant Servers

The **Redundant Servers** box lists, by IP address, the other VMS servers that are in the redundancy group with this server. Each VMS server in the group must own a list that includes all of the other servers in that group.

Use the **Add**, **Modify**, and **Remove** buttons to create and maintain the list.

5. Configure the SNMP traps for this server. This may be required for relaying server status information/alarms to a primary management system at the NOC, for example.

Click the **Traps** tab, shown in figure C-6, to display the existing SNMP Manager traps. Use the **Insert**, **Modify**, and **Remove** buttons to add new traps and modify or remove existing traps. Refer to Appendix E, “SNMP Traps”, for detailed information on the SNMP Manager.

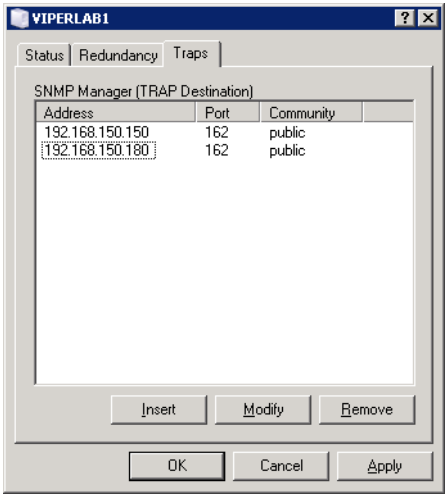


Figure C-6 VMS Server Properties, Traps Tab

6. When finished, click the **OK** button to save the server properties settings.

7. Repeat steps 2 through 6 for each VMS server in the redundancy group.

8. Place the VMS server with the highest redundancy priority into the *active* state:
Connect the console to the server with the highest priority and select the **Activate** command from the VMS Server drop-down menu.

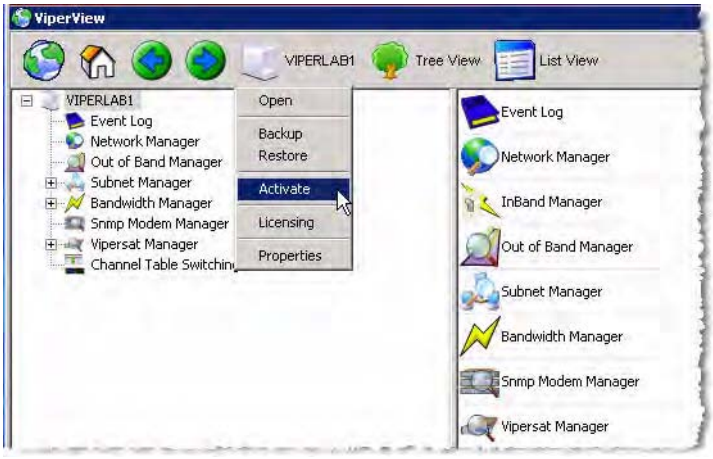


Figure C-7 Activate Command, VMS Server Menu

9. From the *Active* VMS server, select the **Synchronize** command from the Server drop-down menu to force the Standby server(s) to synchronize with the current status of the Active server.

This manual synchronization command must be executed whenever a Standby server is started or comes back into the group, as well as whenever any database changes are made to a unit. A synchronization can only be executed from the Active server.

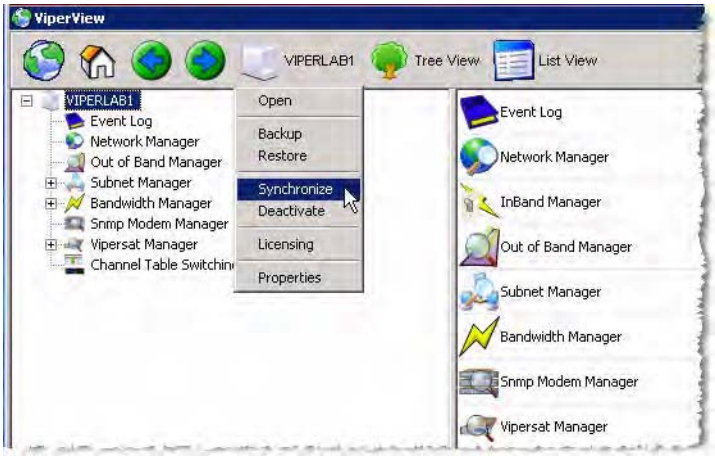


Figure C-8 Synchronize Command, VMS Server Menu

This concludes the procedure for installing and configuring the VMS redundancy servers.

- The next step is to configure the VMS database for the satellite network on the *Active* server. Refer to Chapter 3, “VMS Configuration”, for details on this procedure.
- Once the VMS configuration is completed on the Active server, perform a server synchronization to synch the Standby server database(s) with the Active server database.

Manual Switching

Manual switching can be used to designate a different server to be the active VMS server in the redundancy group.

1. From the currently active server, right-click on the server icon in Viperview to display the pull-down menu and select **Deactivate**.

2. From the standby server that will become the new active server, right-click on the server icon in Viperview and select **Activate**.

3. Verify the new server status using Connection Manager.

Clearing Server Contention

Should contention for active status between two VMS servers occur, use the following procedure to clear the condition.

1. From Viperview, right-click on the server icon and select **Clear Contention** from the pull-down menu that appears.

   A pop-up message will appear on the console indicating that the server will enter standby mode, and that the contention on the other server must also be cleared before this server status can be changed to active.

2. Repeat the previous step for the second server in contention.

3. Determine which server is to be made active (typically, the server with the highest priority) and select the **Activate** command.

   This server will become active and the other server will remain in standby mode.

N:M Hub Modem Redundancy

Description

The N:M Hub Modem Redundancy service provides for the protection of critical VMS network modems operating in Hub mode and enhances overall network reliability.

The N:M redundancy in VMS version 3.x has the following characteristics:

- Protects Vipersat Hub modems from equipment failure
- Is a VMS controlled feature
- Does not require any external switching hardware
- Preserves the satellite network configuration and state information during hardware failure
- Is scalable and flexible to satisfy the unique requirements of each network

N:M redundancy increases reliability by backing up critical primary central hub components with standby backup units. In a traditional 1:1 or 1:N redundancy, switching is handled by combining transmission equipment into logical mechanical switching units. These software/hardware units then interconnect the primary transmission units I/O through a physical mechanical maze of relays and cable jungles. They also become the next point of failure in the reliability hierarchy.

The Vipersat solution relies less on a mechanical backup system architecture, decreasing the single point of failure. The Vipersat software-driven N:M redundant architecture is completely IP packet controlled with the only hardware item being an IP controlled electrical power switch.

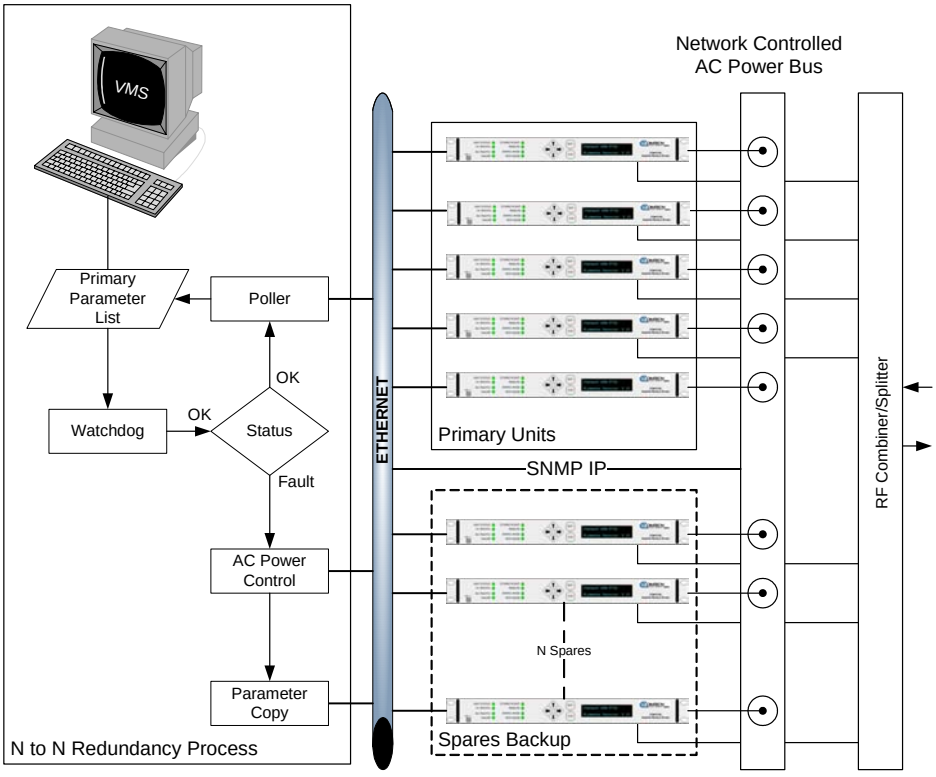


Figure C-9 N:M redundancy logic diagram

The switching control mechanism is completely monitored and controlled by the host master processing VMS as shown in the logic diagram in figure C-9. The VMS parameter backup and restore function is used to copy each primary units configuration database information which are then stored in a lookup list.

The stored primary unit's parameter files are used to put the image of a failed primary unit's parameters into a standby spare unit. The spare units should always be in the parked configuration described in the section "Setting Unit to Parked Configuration Mode" on page C-36, powered on, and listening and responding to the local LAN network.

After the N:M redundancy has been installed, as described in the section "Installing N:M Redundancy" on page C-17, the VMS starts listening for heart-beat messages from each of the primary and backup spare units for health and fault code response as shown in the logic diagram in figure C-9. If any primary unit fails (has an alarm set or misses three consecutive heartbeats) the VMS will invoke the backup procedure by sending a copy of the failed unit's database to the next available standby spare.

The spare unit is selected in order of IP address. If the spare unit fails to respond or process, it is marked as unavailable by VMS and the VMS repeats the process by selecting the next available unit in the list. Also, as part of the copy command, a separate message is sent to the IP remote controlled AC power bus removing power to the primary failed unit, shutting it down. This ensures that there is no possible contention between the failed unit and the spare unit being brought online.

As the spare unit receives the database configuration file it immediately copies the image over the stored offline state parameters and issues a firm rest to reinitialize the newly stored information without rebooting. Once the firm reset completes (approximately 1 second for non-STDMA mode or approximately 5 seconds for a unit operating in STDMA mode) the unit will announce itself by broadcasting an ARP message updating local routing tables.

The failed primary unit is readily identified by its powered down state. Once the cause of failure is identified and repaired, the primary unit can be reinstated and put back online using the procedure in the section “Putting Failed Unit Back into Service” on page C-35.

Installing N:M Redundancy

The installation of N:M redundancy in a satellite network involves the physical installation, interconnection, and grouping of the primary and secondary modems and the logical grouping of managed units using the VMS Redundancy Manager.

Hub N:M Redundancy Requirements

The following requirements must be met before you can do a successful installation of VMS N:M redundancy.

- N:M Redundancy is only applicable to Hub devices that are not expansion units
- The VMS version must be 3.x or later
- VMS controlled modems must have identical firmware version installed.
- A Server Technology horizontal Sentry™ PowerTower XL IP remote power control is required
- The active device and the backup device must be connected to the same Ethernet LAN
- The active and backup devices must be connected to the same RF output connection

- The VMS, managed power strip, and hub modems must be on the same LAN segment
- All modems must share the same RF infrastructure, such as combiners and splitters

Once devices have been installed in the satellite network as described in the section “Installing N:M Redundancy” on page C-17, a group of identical, active, primary devices functioning in the satellite network under VMS control and another group of N devices, identical to the active devices in a spare device pool are created.

Tip: The logical grouping should correspond to the physical device grouping and their connections to remote managed power controls.

The devices in the primary group are devices which are active in the network. These devices can be performing any function in the network, except expansion units. All of the devices in the backup group are turned on, but have not been configured to perform any network function and are assigned a different IP addresses than the active devices. All devices in both the active and spare groups are connected to the VMS managed power switch as shown in figure C-10.

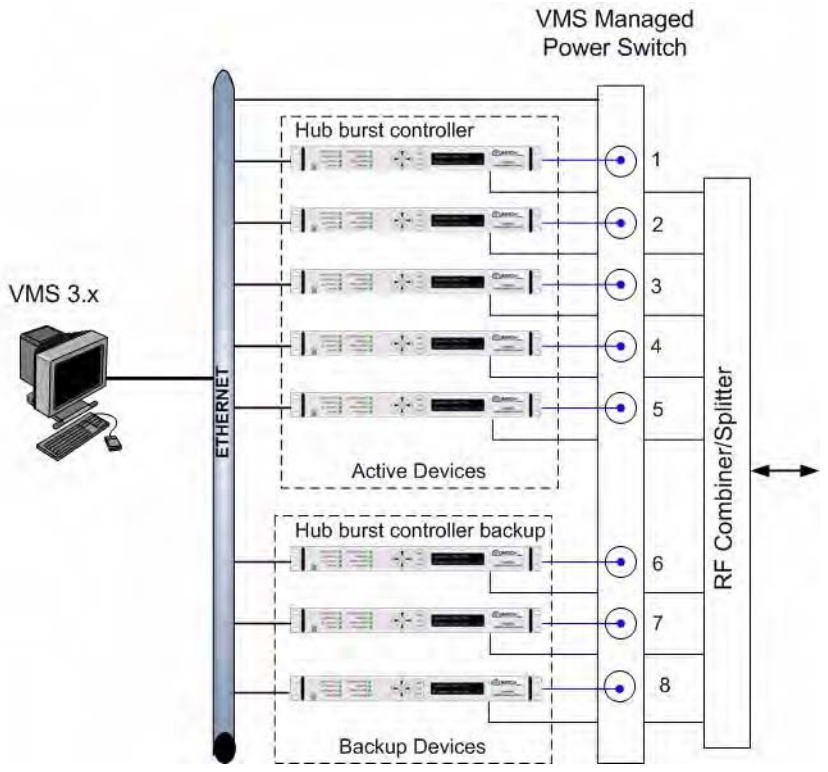


Figure C-10 N:M block diagram

Sample Installation

Figure C-11 shows a diagram of a sample installation of an N:M redundant VMS installation. As shown in figure C-11, the units in the primary and secondary groups share a common Ethernet LAN with the IP controlled power switch.

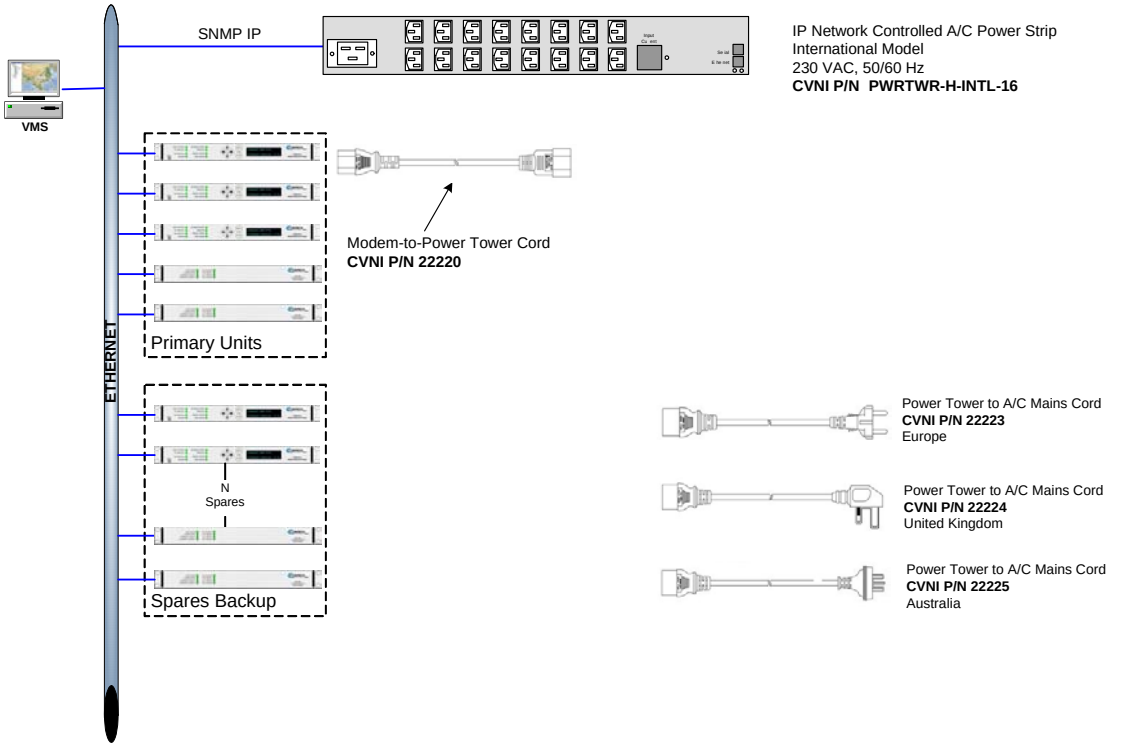


Figure C-11 Typical N:M redundant installation

The URL http://www.servertech.com/support/ProductManuals/ contains the *Power Tower XL/XM Installation and Operation* manuals for the network controlled power strip shown in figure C-11. Refer to these manuals for detailed information on this device.

NOTE

Note: All units in both the primary and secondary group must be identical, with exactly the same hardware configuration and accessories, and have identical firmware revision levels.

Use the following procedure to implement the optional N:M capability in a VMS network.

Setting Up N:M Redundancy

There are 3 hierarchal objects in N:M Redundancy, as shown in figure C-12. They are:

1. Redundancy Manager

2. Containers

3. Power Strips and Groups

Figure C-12 N:M Redundancy Hierarchy

Expanding the Redundancy Manager icon, shown in figure C-13, shows a typical N:M redundancy installation. Under the Redundancy Manager service icon are the icons for a container named Hub, in this example.

Figure C-13 Redunancy Manager Tree

Expanding the Hub icon shows additional icons such as the remote controllable switch labeled S1 in this example, and a group labeled Hub1.

Redundancy Manager

The Device Redundancy Manager is loaded as a service in ViperView. By right-clicking on it, as shown in figure C-14, the operator can enable device redun-

dancy, create the main container for the site, and backup or restore the redundancy service.

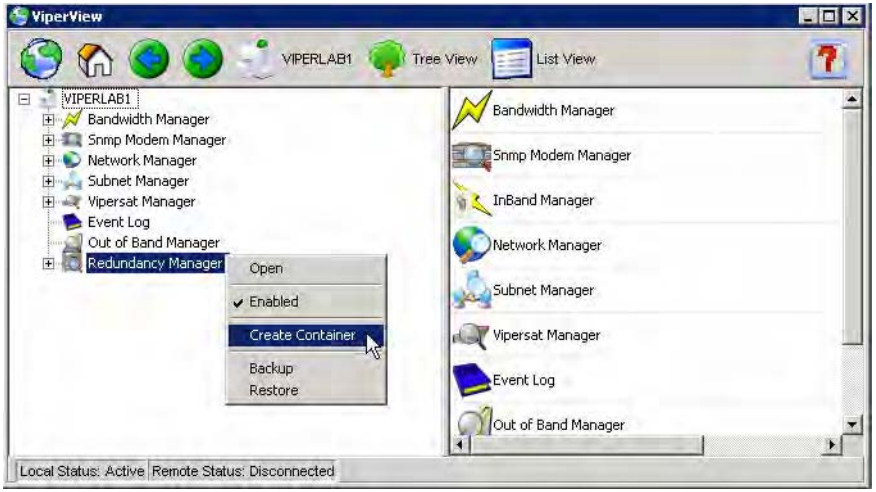


Figure C-14 Redundancy Manager Drop-Down Menu

Create Container

Selecting **Create Container** from the drop-down menu in figure C-14, brings up the **Create New Redundancy Group** dialog shown in figure C-15. Clicking the OK button creates a container with the name assigned in this dialog.

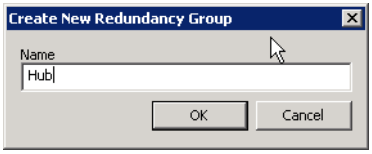


Figure C-15 Create Container dialog

Adding Strips and Groups

This top level container represents the main redundancy group. From it the operator can add Power strips and sub-groups by right clicking on the newly created group icon and selecting from the drop-down menu shown in figure C-16.

Figure C-16 Group drop-down menu

Once the container is created, right-clicking on its icon brings up the drop-down menu shown in figure C-17.

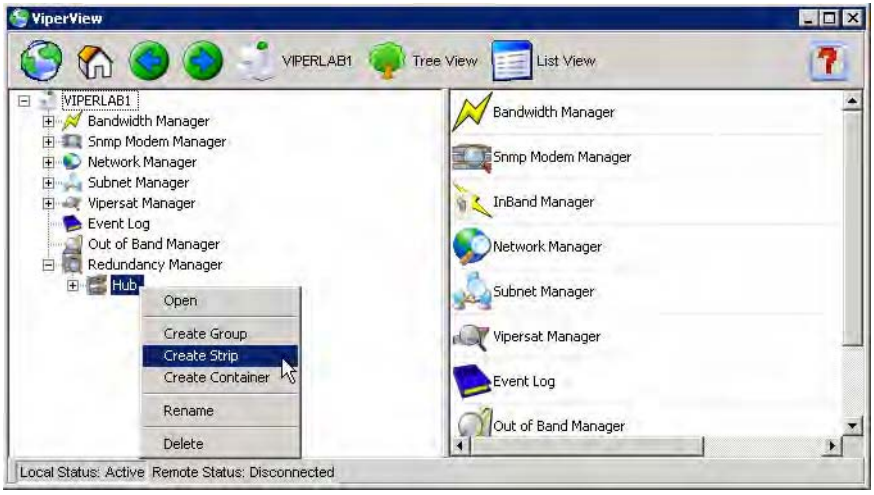


Figure C-17 Group drop-down menu

Power Strips

Selecting **Create Strip** from the drop-down menu shown in figure C-17, displays the New Power Strip dialog shown in figure C-18.

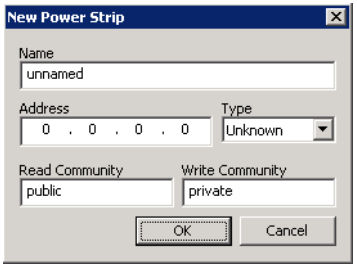


Figure C-18 New power strip dialog

The operator can name the strip (such as reference to a specific rack), enter the IP address, and select the type using the dialog in figure C-18. At this time VMS supports the Sentry 3 and 1 model of APC power strips. Vipersat recommends the Sentry 3. Leave the read and write communities public and private.

It will then be necessary to populate the strip with the primary and backup units. It is very important in this step to insure the association is made with the correct port. Populate the strip by dragging the unit from the subnet manager to the strip port as shown in figure C-19.

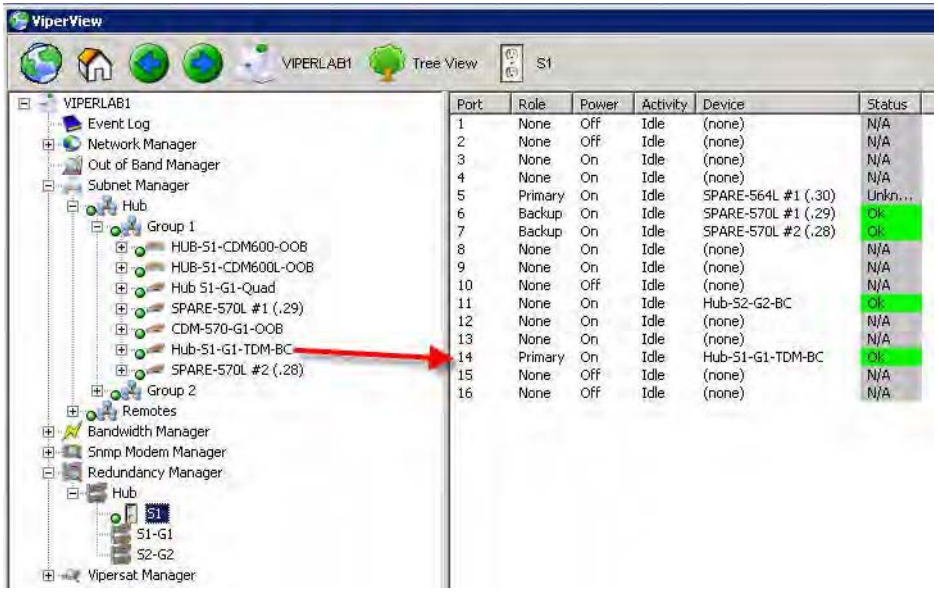


Figure C-19 Drag-and-drop populating power strip

Redundancy Groups

After declaring the strip(s), right-click on the main redundancy group as shown in figure C-17 and select **Create Group** from the drop-down menu. This next group will represent the redundancy group for a given satellite or network.

Figure C-20 Create Group dialog

Once the group is created, drag the port to the group sub-container as shown in figure C-21. Group sub-containers can have entries from multiple strips.

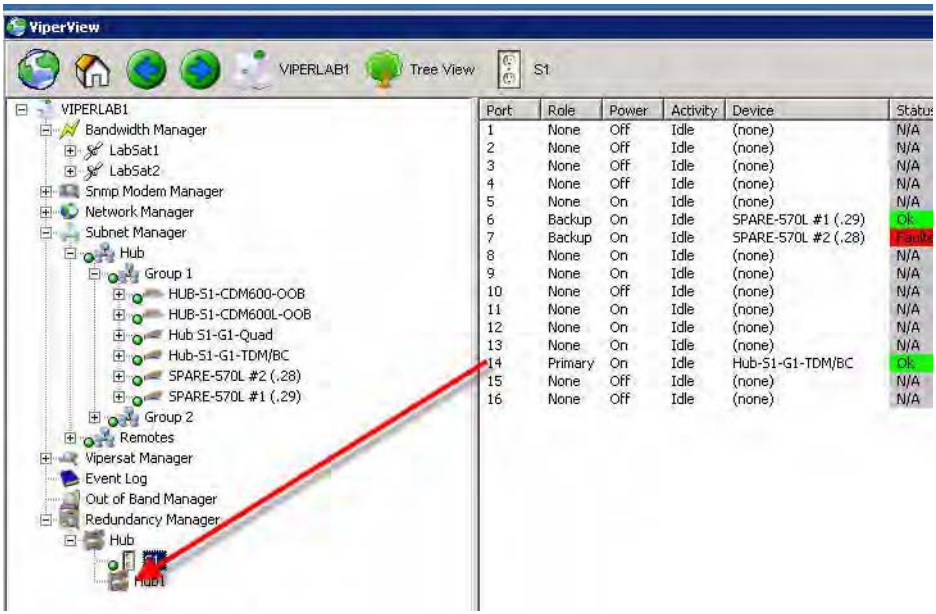


Figure C-21 Dragging port to group sub-container

Enabling Heartbeats

Next, enable heartbeats in the VMS and the devices.

From the Subnet Manager, right-click on the desired device and open the properties page shown in figure C-22. Check the **Enable Heart Beat** box.

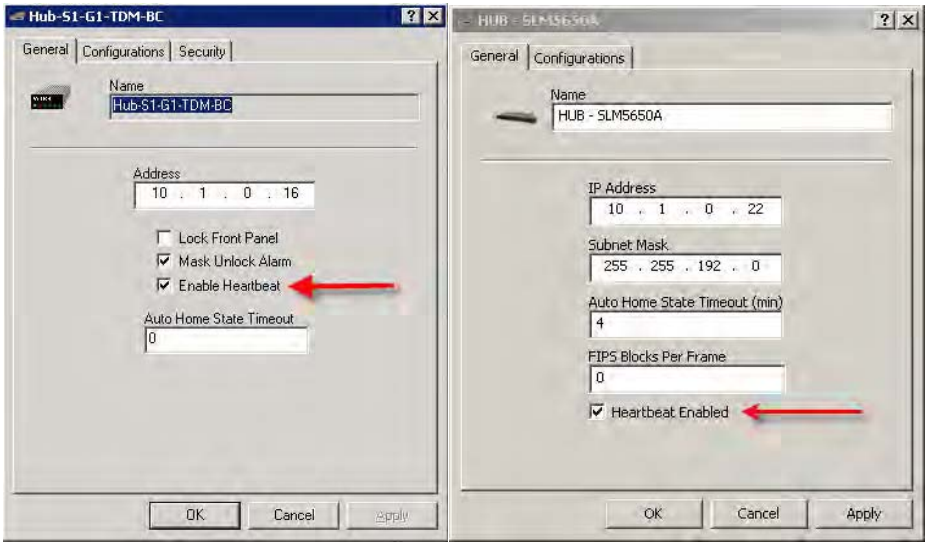


Figure C-22 Enable hearbeat in VMS, left window CDM-570/570L, right window SLM-5650A

Right-click on the device again from the drop-down menu select **Configure**. On the **Features** tab, shown in figure C-23, check the **Primary Heartbeat** box. Click the **OK** button to continue.

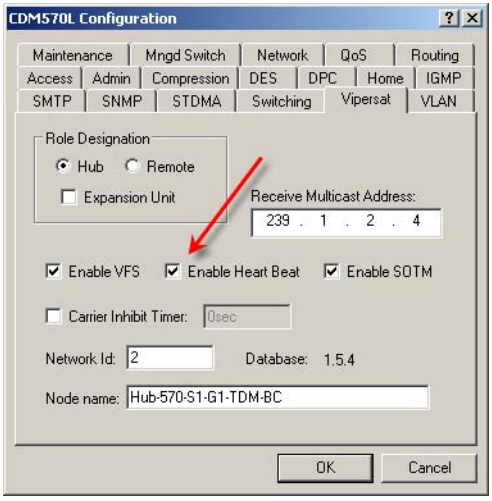


Figure C-23 Enabling heatbeat in CDM-570/570L modem

Force registration on the device. On the next PLDM the Status in the group window should turn green and change to OK.

Hub SLM-5650A Modem

Connect to the hub modem using Web interface, select the Vipersat page as shown on figure C-24 to enable HeartBeat messaging.

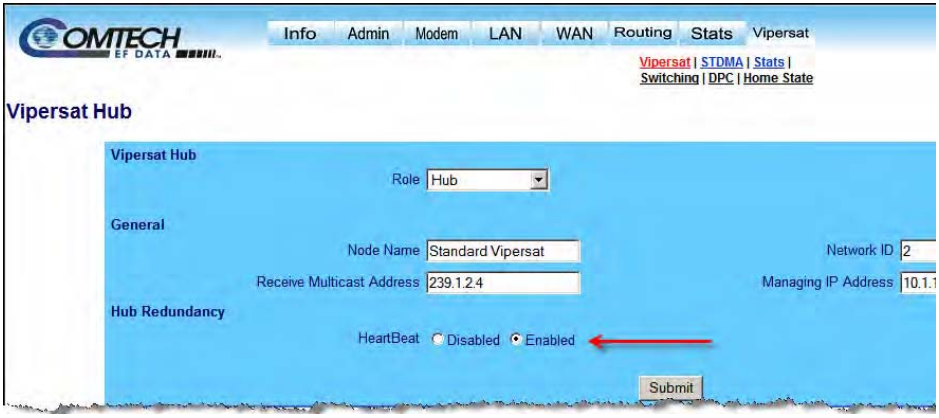


Figure C-24 Enabling HeartBeat in SLM-5650A Hub modem

Roles

Once the group sub-container is populated and heartbeats are enabled, roles can be defined for each of the ports by right-clicking on the device and selecting the appropriate role from the drop-down menu shown in figure C-34.

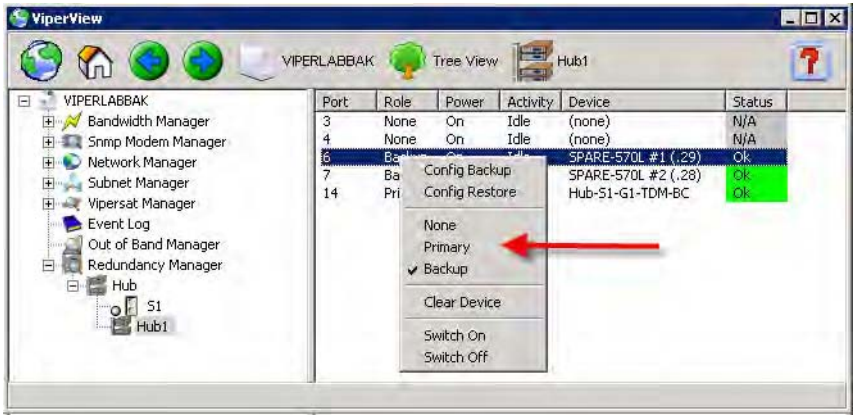


Figure C-25 Role selection

Roles are either **None**, **Primary** or **Backup**. From this drop-down menu shown in figure C-34, the operator can also Backup the device configuration (a very important step after populating the group), restore the device configuration, clear the device from the group or turn the port on or off. Before setting the roles ensure the Status for the device is Ok as shown in figure C-34.

There are four possible status indications:

1. **Ok** – Hearbeats are enabled in both VMS and the device, are being received by VMS and have no fault indications.

2. **Unknown** – Heartbeats are not enabled in VMS. May be enabled or not in the device.

3. **Faulted** – Hearbeats are enabled in VMS but not in the device or heartbeats are being received with a fault indication (non-zero status).

4. **N/A** – The port is not in use.

VMS will select only appropriate units from the list of backups. For example, only CDM570 backups will be used to backup a failed CDM570 even if there are CDD564 units designated as backup units earlier in the list.

Backup Configurations

At this point it is necessary to pull backup configuration files from each of the units. Clicking on the **Config Backup** command on the drop-down menu shown in figure C-26 stores these configuration files in the directory path: *C:\Program Files\Vipersat\VMS\3.0\bin\Device Redundancy*.

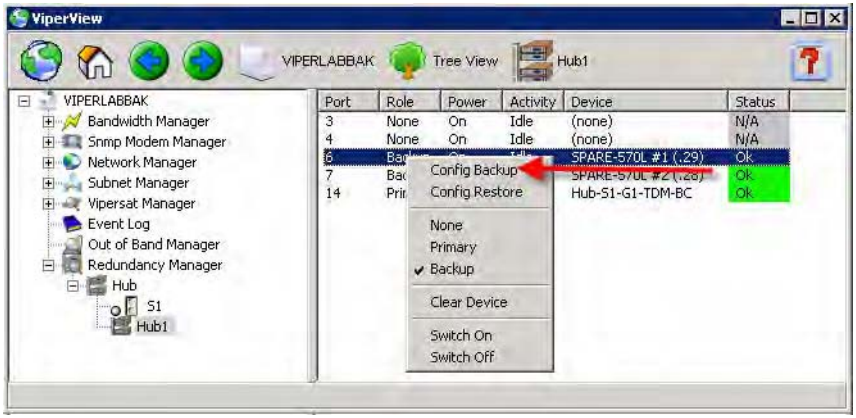


Figure C-26 Configuration backup

System Restoration

Once VMS performs a unit restoration, the backup unit will take on all the characteristics of the original unit that failed, including its IP address. Unless the operator wishes to maintain the original rack profile, the failed unit can either be repaired or replaced and designated as a backup to the unit which is now functioning as the primary.

Should the operator desire to return to the original rack profile the following steps are mandatory and will require a system/segment outage!

Pre-Configuring Backup Files

The files created in the preceding step are used by VMS for automatic redundancy and are not available to the operator for restoring device units to their original role. It will be necessary to create these files so they will be available for this purpose.

Creating Backup Configuration Files

From the Subnet Manager, right-click on the target unit, open the **Properties** page and select the **Configuration** tab shown in figure C-27.

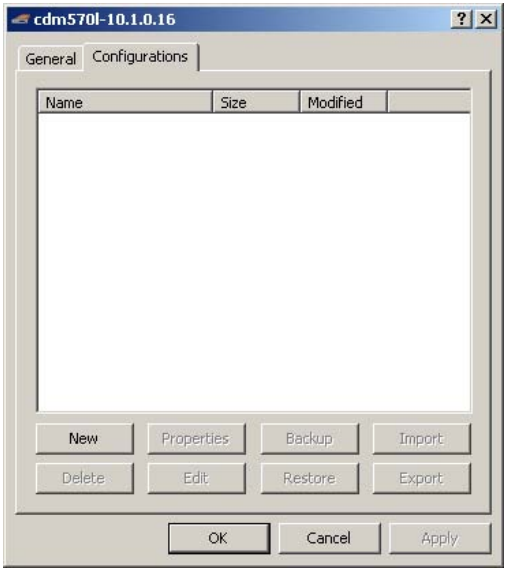


Figure C-27 Configuration tab

Click the **New** button, shown in figure C-28 which will open the **New Configuration** dialog shown in figure C-28.

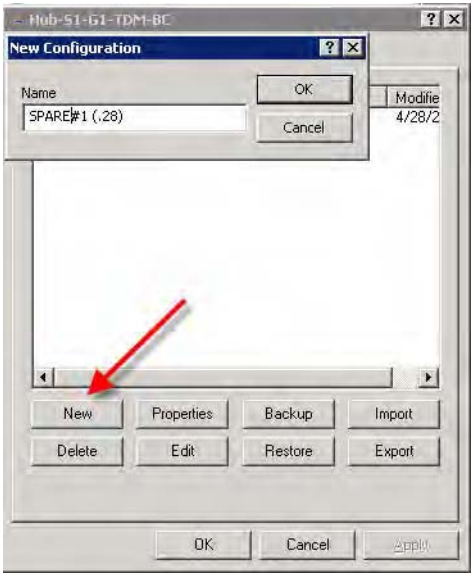


Figure C-28 New configuration dialog

Give the configuration file an appropriate name in the **New Configuration** dialog in figure C-28 and click the **OK** button. Then highlight the file name as shown in figure C-29 and click the **Backup** button.

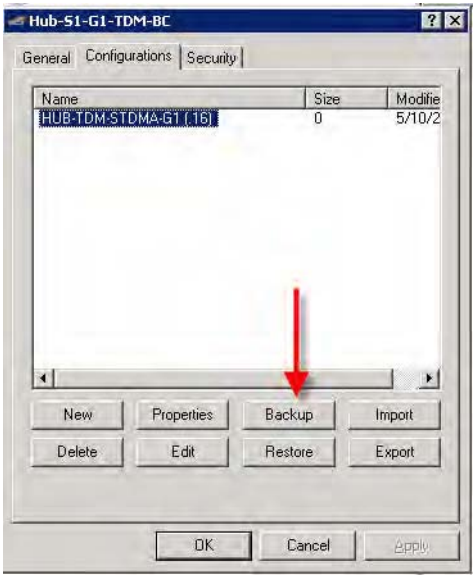


Figure C-29 Creating a backup configuration file.

By default the file will be saved in the location shown in figure C-30.

Figure C-30 Saved file location

Storing Spare Configurations in Primary Units

Once these backup files have been created, it is necessary to add all possible spare units to the **Configurations** tab for each of the primary units. This is done by creating a new configuration file name, highlighting it, then clicking the **Import** button as shown in figure C-31 and importing the file from the directory shown in figure C-32.

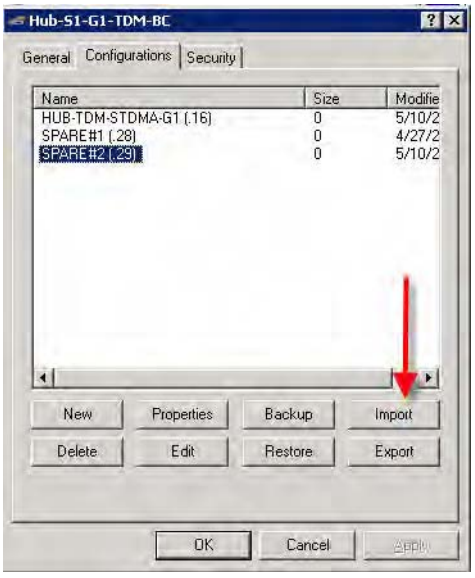


Figure C-31 Importing file

Select the appropriate file from the list:

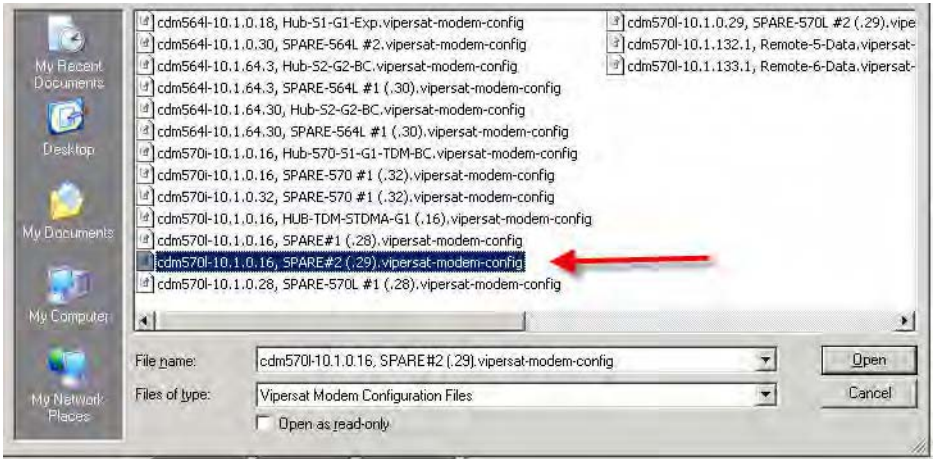


Figure C-32 Selecting file

Preparing Repaired/Replacement Unit

Pre-configure the repaired/replacement unit with the configuration of the primary unit being replaced. This step should be performed on a separate LAN segment from the satellite network to avoid conflicts. Vipersat strongly recommends using VLOAD to maintain backups of all network units. These backup files can be used for this purpose.

Install the replacement unit in the desired rack location and make all connections. The unit should be powered on, but insure the switch port is powered off.

Restoring Acting Primary Unit Spare Configuration

Since the backup unit assumed the identity of the failed primary unit during restoration, it will appear in the Subnet Manager as the original unit. Right-click on the unit and open the Properties page. Go to the Configuration tab and select the appropriate spare configuration imported in the preceding step. Be sure to select the proper configuration to avoid IP address conflicts.

Select Restore to load the configuration.

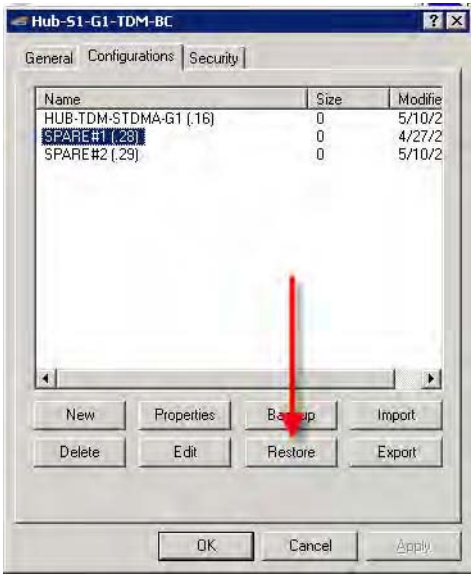


Figure C-33 Restoring configuration

At this point, the network segment controlled by this primary unit will go down. Power up the new primary unit using the drop down menu on the strip, or in the sub-group. If the configuration is correct, the network segment will automatically come back up after the unit reboots.

Cleaning up

Once the network has been restored, it will be necessary to create new configuration backups from the drop-down menus and to reset the system roles. Insure the status is OK. (It may be necessary to reset heartbeat flags)

How N:M Redundancy Works

In the event of failure of any active device, a unit from the spare device pool is configured with the configuration of the failed device, including its IP address, and re-initialized without a hard reset. VMS switches off power to the failed device immediately after detecting failure to ensure the failed device will not conflict with its replacement device when the replacement device is booted into service.

Note: The total elapsed time to detect a failed device, remove power, configure a device from the spare pool with the failed device's configuration, and reboot the replacement device into service in the satellite network is generally less than 5 seconds.

Device Failure Detection

Each device protected by N:M redundancy in a satellite network transmits a packet, called a heartbeat, at timed intervals whenever N:M redundancy is enabled on the device. During registration, VMS establishes the heartbeat interval for each protected device. The heartbeat packet contains the following information:

- The unit's IP address
- The unit's health/fault status
- The unit's receive and transmit health or fault status

The VMS monitors and analyzes each received heartbeat packet for information for a switch trigger such as:

- No heartbeat is detected for three (3) consecutive one-second intervals.
- The unit transmits a fault status indicating the unit's health, or loss of transmit or receive capability.

The Switch-Over Process

The switch-over process involves both the Vipersat Manager and the Redundancy Manager.

Vipersat Manager

Activity in the Vipersat Manager starts when the VMS N:M redundancy capability is enabled, then proceeds as follows:

1. VMS monitors error messages and heartbeat packets from protected units for an event indicating that a redundancy switch is required.

2. When an event is detected that requires a redundancy switch, VMS sends a notification event to the VMS Log service.

3. VMS sends notification to the Redundancy Manager that a switch-over is required.

Redundancy Manager

The Redundancy Manager receives the switch-over request from VMS which starts the following process:

1. The Redundancy Manager checks that the VMS notification is a for a valid switch condition. If the condition is not valid, the Redundancy Manager sends its action to the VMS log service and returns to waiting for the next event notification.

2. If the notification is a valid switch condition, the Redundancy Manager checks to see if there is a backup unit available. If no unit is available, the Redundancy Manager send this information to the VMS Log Service and returns to waiting for the next event notification.

3. If there is a backup unit available, the Redundancy Manager sends a command to the remote managed power control unit to turn off power to the plug used by the failed primary unit.

4. The Redundancy Manager saves (puts) the redundant configuration and base modem parameters to the backup unit.

5. The Redundancy Manager commands a firm reset of the backup unit.

6. After the switch, the backup unit is configured as the original primary unit and joins the network performing the same functions as the failed primary unit.

7. When the unit switch-over is completed, the Redundancy Manager sends the event to the VMS Log service completing the switch-over process.

8. The Redundancy Manager resumes waiting for the next event notification.

Putting Failed Unit Back into Service

This section describes the process of configuring a VMS controlled modem before connecting it to a VMS network as an N:M redundant backup unit.

Caution: A repaired failed unit will have the same IP address and function as its replacement unit which is currently online. Use the following procedure when returning the unit back into service as a backup. To avoid conflict with the online primary unit and possible loss or degradation of satellite network communications, use the following procedure.

Use the following procedure when putting a VMS controlled modem into service. The unit must have its IP address changed and its configuration modified to backup mode so that it can be connected to the network without conflicting with any ongoing communication or network control functions.

Warning: Do not apply power to the unmodified unit while it is still connected to the network. To do so may cause the network to behave unpredictably and possibly fail. A unit removed from service MUST be set to backup configuration before being placed back into service.

1. Disconnect the Ethernet connection between the unit and the LAN.

2. Remove all RF connections from the VMS controlled modem to the network.

Tip: To test a failed unit and then put it into backup configuration before putting it back into service, ideally it should be removed from the rack and the power cord removed from the unit's rear connector leaving the power cord connected to the remote managed power control unit.

Setting Unit to Parked Configuration Mode

You should configure all units you are installing into an existing VMS network to be in the parked configuration mode to ensure that:

- The unit will be recognized and respond to VMS commands
- The unit will not try to assume an active role in the network until it has been commanded to do so by VMS.

Connect to the unit using the serial console port as described in the unit's documentation available for download at:

http://www.comtechefdata.com/

Note: For the following configuration changes using a SLM-5650A refer to Vipersat version of modem manual. All referenced changes are similar in text descriptive terms.

1. Turn the unit on.

2. On the Administration > Feature Configuration page shown in figure C-34, enter the unit's features and unlock codes.

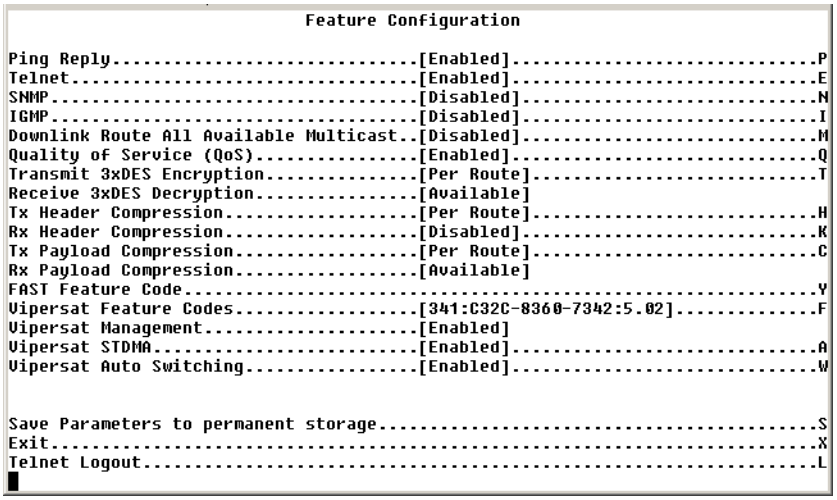


Figure C-34 Feature configuration page, CDM-570/570L

3. Disable STDMA.

4. On the **Administration** page shown in figure C-35, set the **Working Mode** to **Router - Vipersat**.

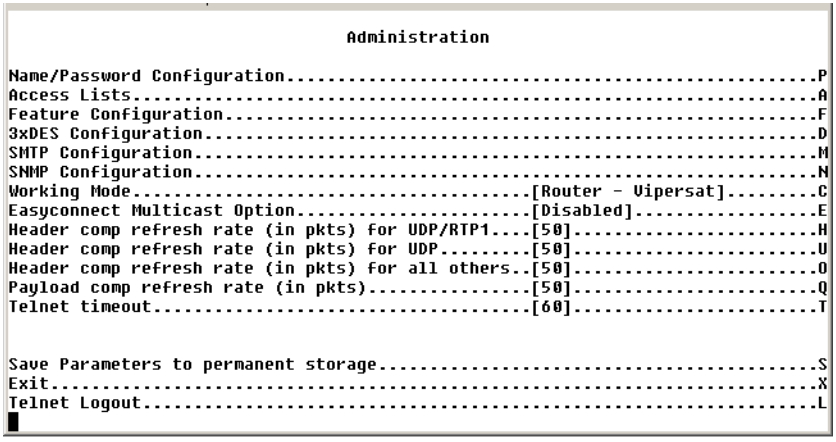


Figure C-35 Administration page, CDM-570/570L

5. Using the Internet Interface page shown in figure C-36, set the unit's IP address to the IP address of the backup unit which replaced it. If you do not use this IP address, make certain that the IP address is on the hub subnet and is not being used by any other active or backup unit.

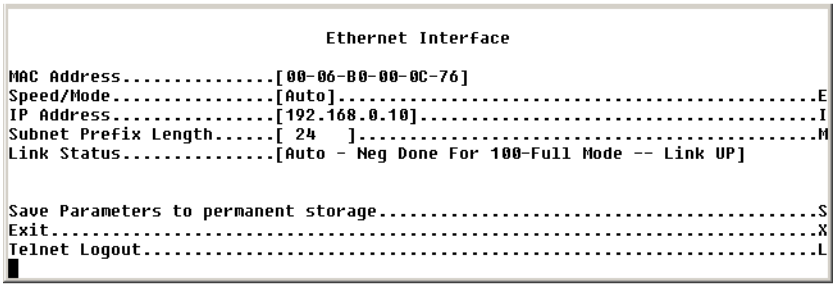


Figure C-36 Ethernet Interface page, CDM-570/570L

6. On the Vipersat Configuration page shown in figure C-37, set the **Unit Role** to **Hub Expansion**.

7. This completes setting the unit to the Parked Configuration mode if it is a CDM-564L. It is possible the unit was being used to supply voltage to a LNB, which is described below.

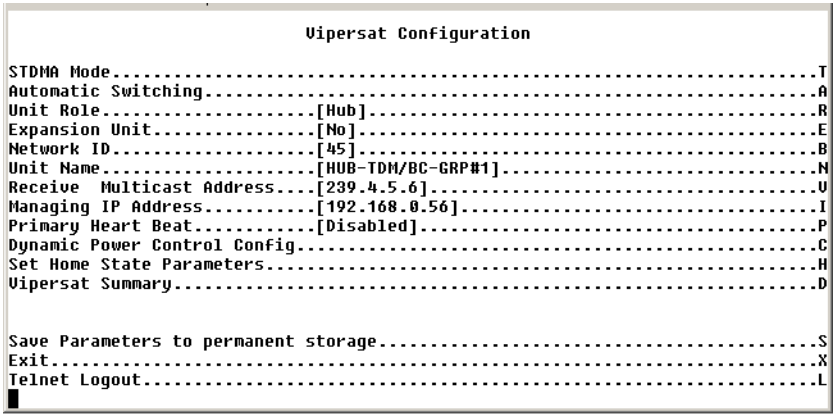


Figure C-37 Vipersat configuration page, CDM-570/570L

8. On the Satellite Modem > Configuration > Configuration > **Tx Configuration** page shown in figure C-38, disable the unit's transmit capability by changing the Tx Carrier to [Off].

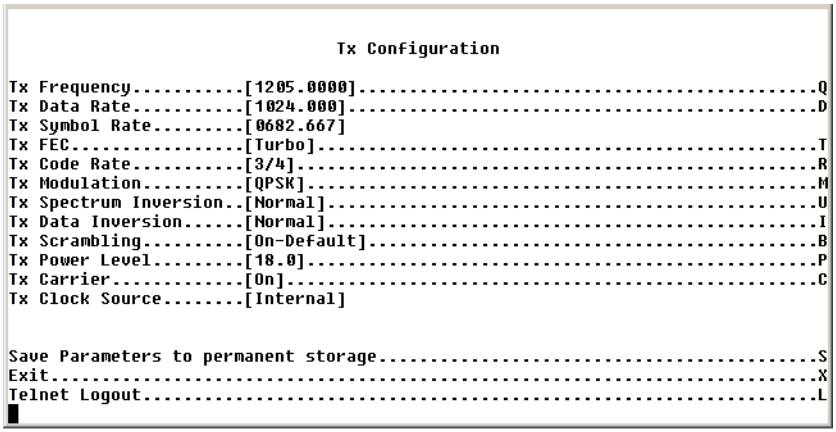


Figure C-38 Transmit configuration page, CDM-570/570L

9. On the Satellite Modem > Configuration > Configuration > Rx Configuration page shown in figure C-39, set the **Rx Frequency** to the low end (50 or 950).

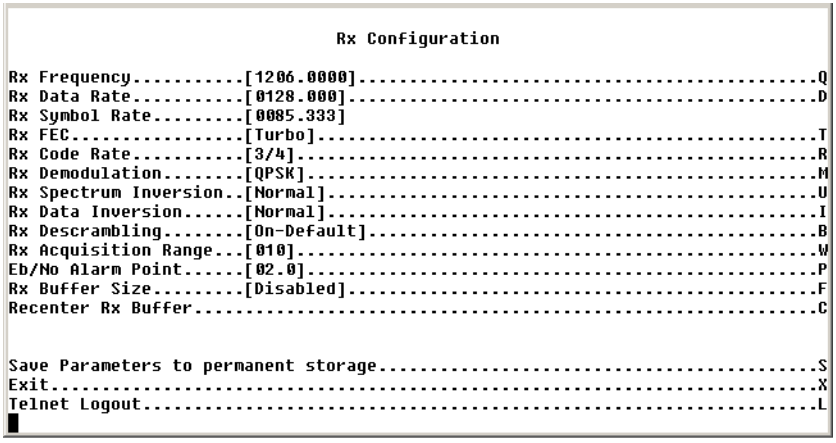


Figure C-39 Set receive frequency to low end, CDM-570/570L

10. Disable the Satellite Modem > Configuration > Configuration > Block Up Converter (BUC) > BUC DC Power as shown in figure C-40.

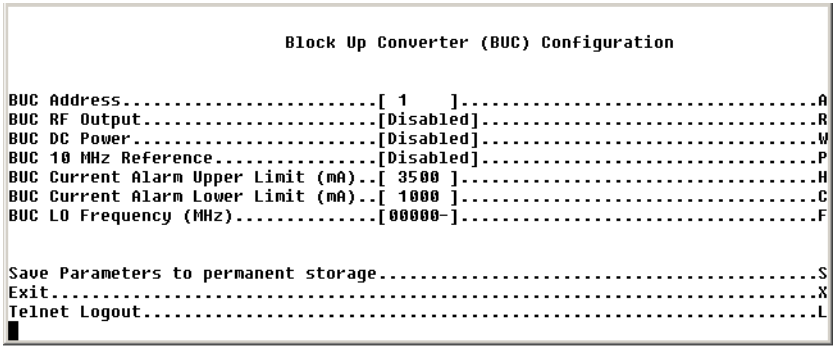


Figure C-40 BUC configuration, CDM-570/570L

11. Disable the Satellite Modem > Configuration > Configuration > Low Noise Block Converter (LNB) LNB DC Supply Voltage as shown in figure C-41.

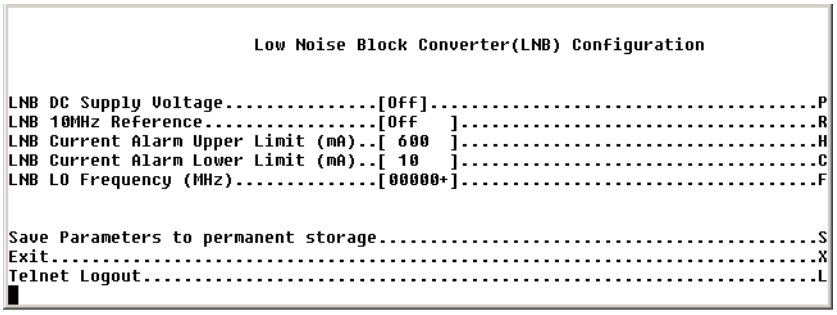


Figure C-41 LNB configuration, CDM-570/570L

12. This completes the process of setting the modem/router to parked configuration mode and it is now ready to be put back into service.

13. If the repaired unit is to be connected to the same plug, it will automatically reinstate the unit as a member of the backup group. VMS identifies the unit by its MAC address so if, for any reason, the failed unit is replaced with another unit, you will have to go to VMS and drag the newly installed unit to the appropriate plug on the power strip to complete its installation.

Caution: Failure to follow the discipline of connecting the repaired unit to the correct plug on the remote controlled power strip will result in the unit not being able to be turned off if it fails while acting as the primary unit, resulting in the possibility of having two active units trying to operate in the same role and consequently crashing the network.

APPENDIX

D

DOMAIN CONTROLLER AND DNS

This appendix describes configuring the VMS server or servers to perform the roles of network domain controller and DNS server for the VMS network. It is especially necessary that these functions be installed if the VMS installation is to be a redundant, fault-resistant installation.

Note: If you are not installing a redundant VMS configuration, use the instructions in this section and the section and ignore the instructions in the section “Configuring a Secondary Domain Controller” on page D-15.

Domain controllers store data and manage user and domain interactions, including user logon processes, authentication, and directory searches. If you plan to use this server to provide the Active Directory directory service to network users and computers, configure this server as a domain controller.

To configure a server as a domain controller, install Active Directory on the server. There are four options available in the Active Directory Installation Wizard. You can create an additional domain controller in an existing domain, a domain controller for a new child domain, a domain controller for a new domain tree, or a domain controller for a new forest.

Setup

Before configuring the server as a domain controller, verify that:

- The TCP/IP configuration settings for the server are correct, particularly those used for DNS name resolution.
- In a redundant VMS installation, there should be Ethernet connections between the active and backup servers.

- All existing disk volumes use the NTFS file system. Active Directory requires at least one NTFS volume in which to store the SYSVOL folder and its contents. FAT32 volumes are not secure, and they do not support file and folder compression, disk quotas, file encryption, or individual file permissions.
- Any extra Ethernet adapters on the server are disabled, and ensure that only one gateway is assigned to the server.
- The Windows Firewall is disabled.
- The Security Configuration Wizard is installed and enabled.

This Appendix is divided into two parts. The first part describes configuring a Domain Controller and Domain Name Server (DNS) on a single server which can then be used either as a stand-alone VMS server or as the Primary or Active VMS server in a redundant configuration.

The second part of this Appendix, starting with the section “Configuring a Secondary Domain Controller” on page D-15, describes configuring a secondary Domain Controller and Domain Name Server on the Secondary or Backup server in a redundant VMS installation.

Configuring a Domain Controller and DNS

Before you begin configuring your server as a domain controller, verify whether or not:

- TCP/IP configuration settings for the server are correct, particularly those used for DNS name resolution. The servers should have active Ethernet connections to each other.
- All existing disk volumes use the NTFS file system. Active Directory requires at least one NTFS volume in which to store the SYSVOL folder and its contents. FAT32 volumes are not secure, and they do not support file and folder compression, disk quotas, file encryption, or individual file permissions.
- Extra Ethernet adapters are disabled
- Ensure only one gateway is assigned to the server.
- Windows Firewall is disabled.
- The Security Configuration Wizard is installed and enabled.

To configure a stand-alone or Primary server as a domain controller, start the Configure Your Server Wizard by doing either of the following:

1. From **Manage Your Server** shown in figure D-1, click Add or remove a role. By default, Manage Your Server starts automatically when you log on. To open Manage Your Server, click Start, click Control Panel, double-click Administrative Tools, and then double-click Manage Your Server.

2. Open the Configure Your Server Wizard by clicking Start > Control Panel > Administrative Tools > Configure Your Server Wizard.

Figure D-1 Manage Your Server dialog

3. Review the **Preliminary Steps** shown in figure D-2 and then click the **Next** button to proceed once you have verified these steps have been completed.

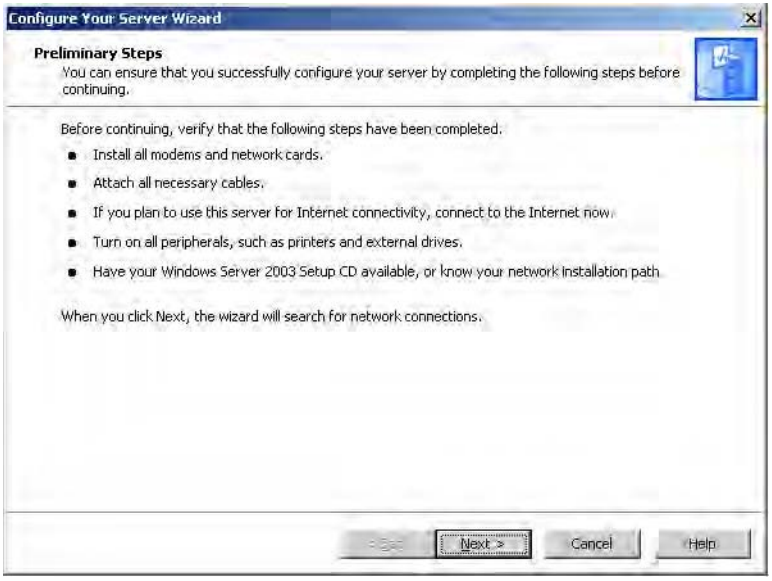


Figure D-2 Preliminary Steps

4. From the **Configuration Options** dialog shown in figure D-3, select the **Custom Configuration** radio button then click **Next** button.

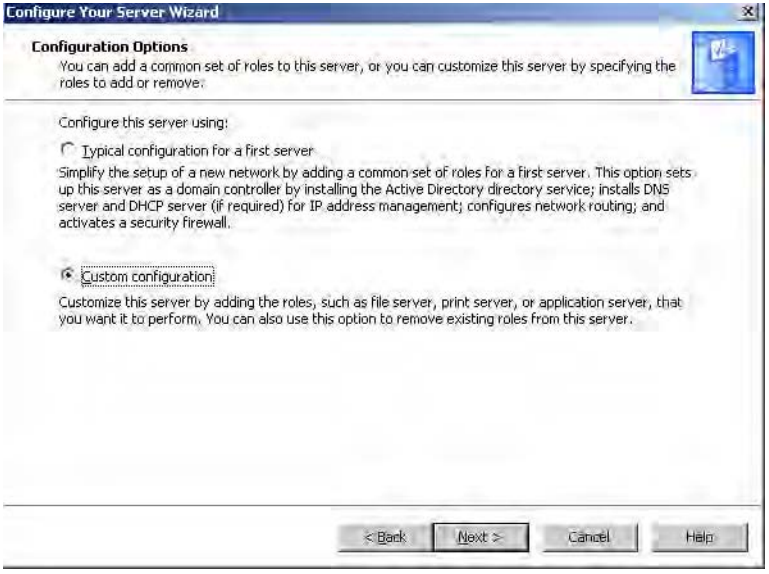


Figure D-3 Configuration Options

5. From the **Server Role** dialog shown in figure D-4, select the **Domain Controller (Active Directory)** item, then click the **Next** button.

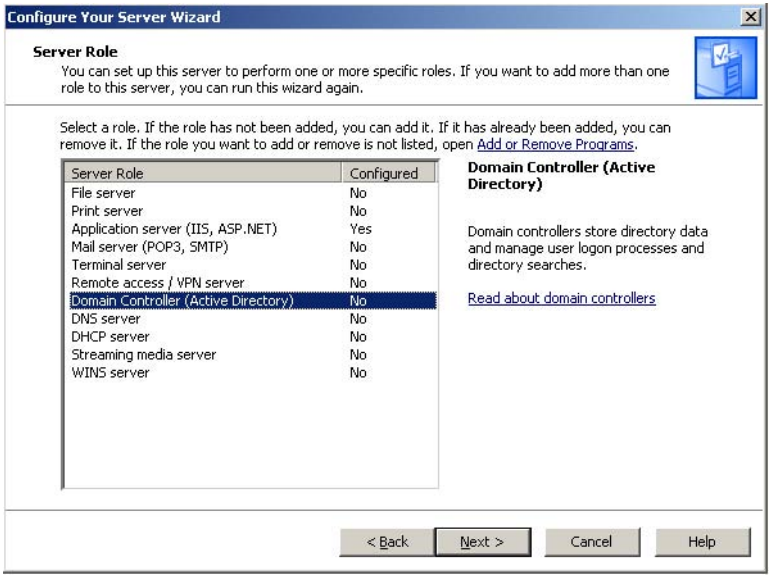


Figure D-4 Server Role dialog

6. Verify your selection displayed in the **Summary of Selections** listing shown in figure D-5, then click the **Next** button to proceed.

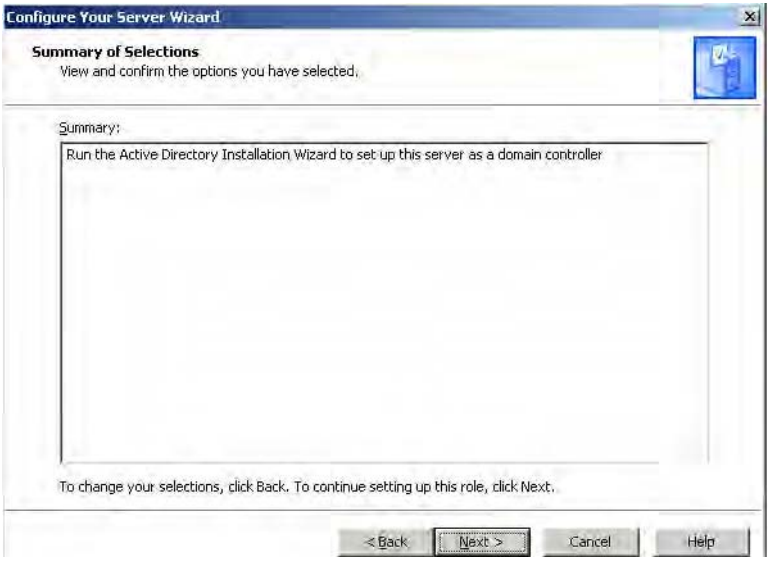


Figure D-5 Summary of Selections dialog

7. From the **Active Directory Installation Wizard** shown in figure D-7, click the **Next** button to begin the installation.

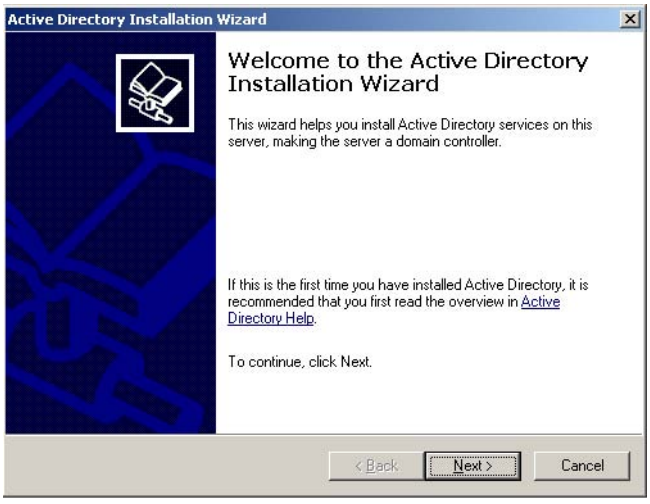


Figure D-6 Active Directory Installation Wizard

8. After reviewing the **Operating System Compatibility** information, shown in figure D-6, click the **Next** button.

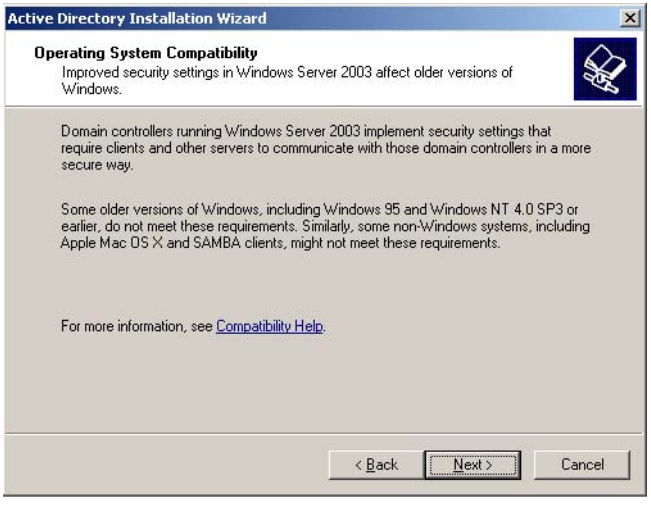


Figure D-7 Active directory installation wizard

9. After reviewing the **Operating System Compatibility** information, click the **Next** button.

10. From the dialog shown in figure D-8, select **Domain controller for a new domain** (default) radio button, and then click the **Next** button.

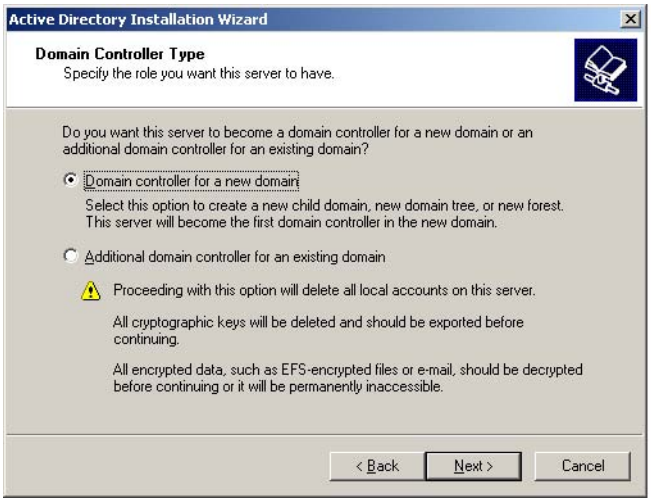


Figure D-8 Domain controller type dialog

11. From the **Create New Domain** dialog shown in figure D-9, select the **Domain in a new forest** (default) radio button, then click the **Next** button.

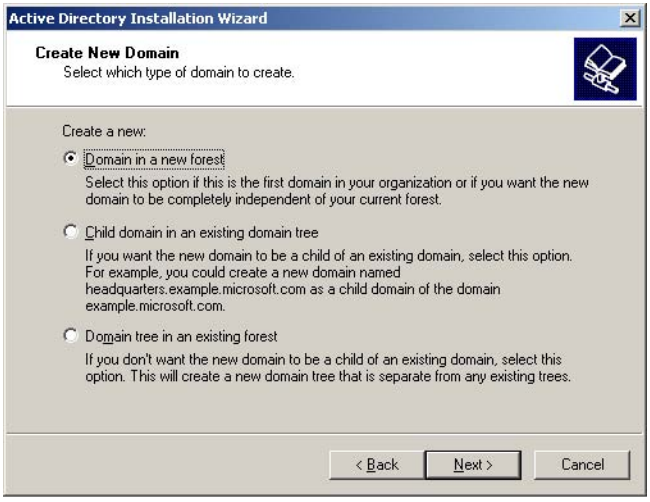


Figure D-9 Create new domain dialog

12. In the **New Domain Name** dialog, enter a fully qualified domain name in the **Full DNS name for the new domain** box. A full DNS name has the structure similar to *AnyName.company.com* as shown in the example in figure D-10. After entering the new domain name, click the **Next** button to proceed.

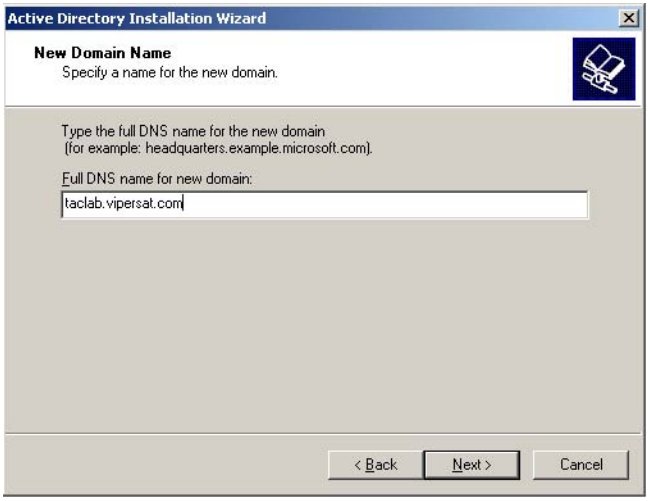


Figure D-10 New domain name dialog

13. In the **NetBIOS Domain Name** dialog shown in figure D-11, enter the NetBIOS name you have assigned to this domain. TACLAB0 is the NetBIOS name used in the example illustrated in figure D-11, but you should assign an appropriate name appropriate to your network. A NetBIOS name gives down-level compatibility.

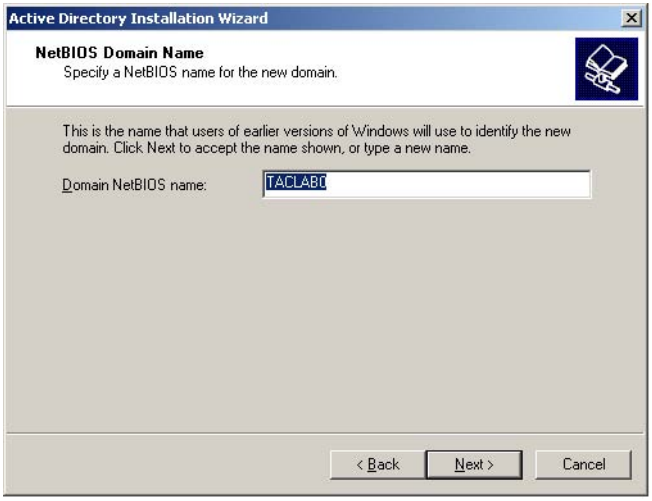


Figure D-11 NetBIOS domain name

14. In the **Database folder** dialogs shown in figure D-12, enter the path C:\Windows\NTDS for these folders. When you have verified these

entries, click the **Next** button to continue. This is the default location for Windows.

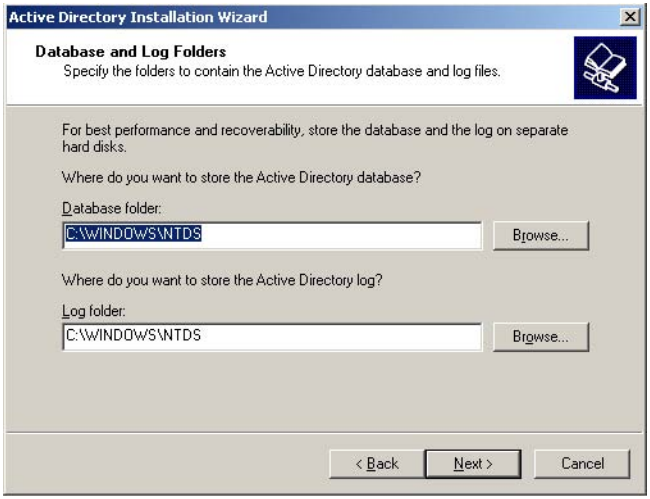


Figure D-12 Database and log folders dialog

15. Use the default folder location, C:\WINDOWS\SYSVOL as shown in figure D-13, for the Shared System Volume. Click the **Next** button to procede.

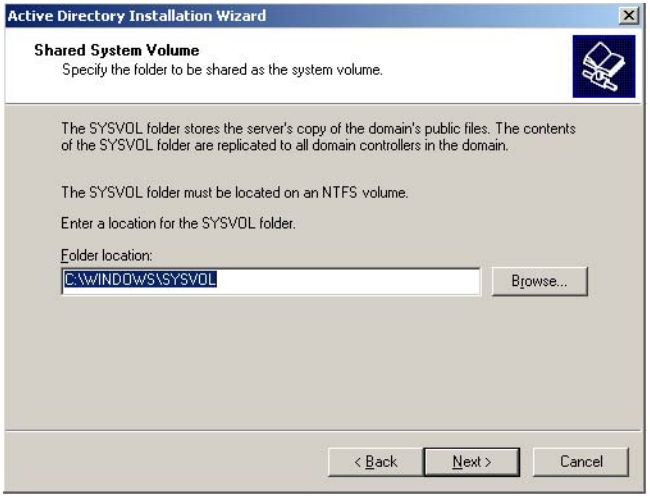


Figure D-13 Shared system volume dialog

16. If the **DNS Registration Diagnostics** screen is as shown in figure D-14, click **Install and configure the DNS server on this computer**. Click **Next**

to continue. The wizard will install and configure DNS support on the server.

NOTE

Note: The screen shown in figure D-14 will be displayed if you are configuring a server which has not had a previous DNS server installation. If you see a different screen at this point, check to make sure that the server has not been a previously configured as a DNS server.

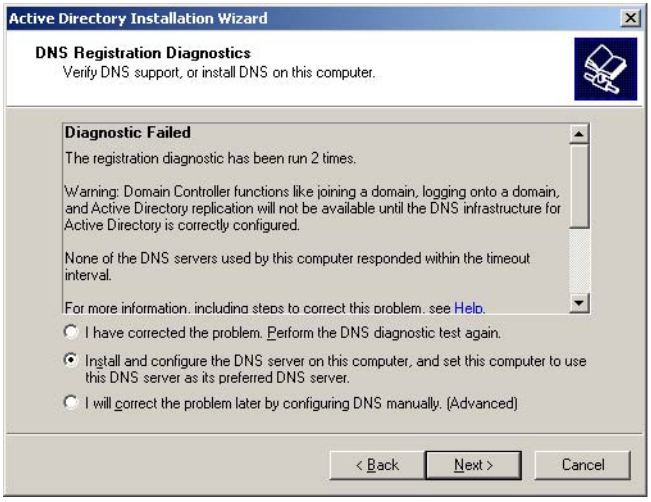


Figure D-14 DNS registration diagnostics screen

17. In the **Permissions** dialog shown in figure D-15, select the **Permissions compatible only with Windows 2000 or Windows Server 2003** (default) radio button, then click the **Next** button.

Figure D-15 Permissions dialog

18. In the **Directory Services Restore Mode Administrator Password** dialog shown in figure D-16, enter the password assigned to the Administrator account to be used when the server is started in the Directory Services Restore mode. You should use a complex password with at least 1 alpha and 1 numeric character, such as *V1persat*. When the password has been entered and verified, click the **Next** button to continue.

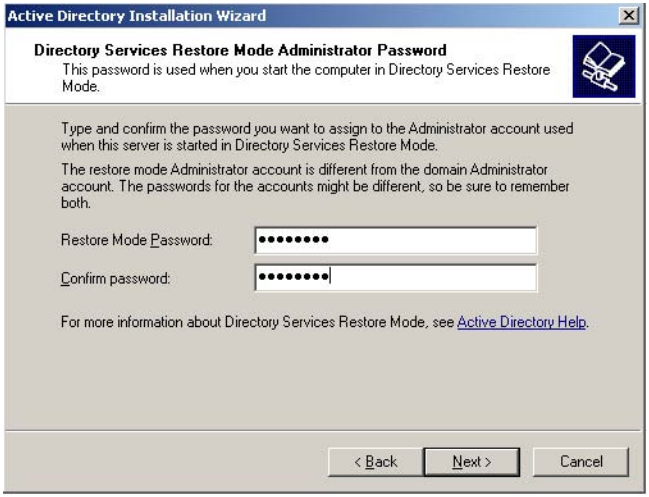


Figure D-16 Administrator password

19. Review the **Summary** screen shown in figure D-17, then click the **Next** button to continue.

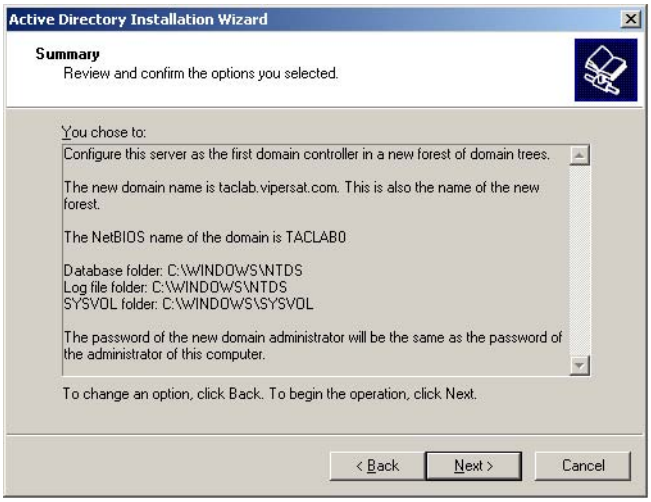


Figure D-17 Summary screen

20. The wizard will begin configuring the Primary domain controller as shown in figure D-18.

Figure D-18 Configuring primary domain controller

21. When prompted by the screen shown in figure D-19, click the **Finish** button to complete the setup.

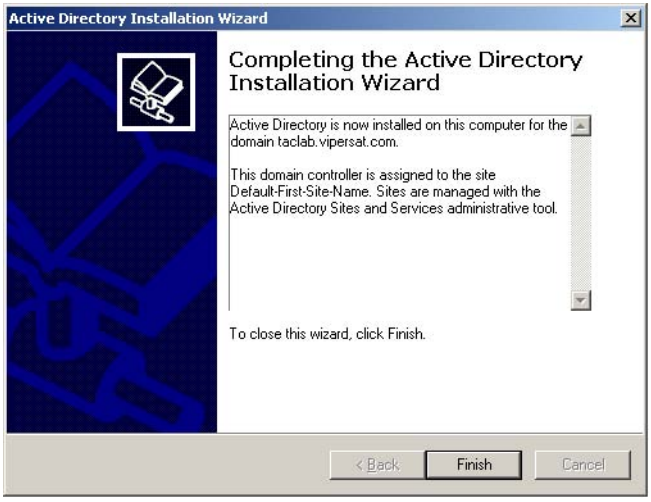


Figure D-19 Complete installation screen

22. Click the **Restart** button shown in Figure D-20 to reboot the server.

Figure D-20 Restart screen

This completes setting the primary server as a domain controller.

Configuring a Secondary Domain Controller

The procedure in the section describes configuring a Domain Controller on the Secondary VMS server in a redundant installation.

The following steps assume that the server is to be configured as the VMS Secondary Domain Controller (SDC) and has had a clean install of Windows 2003 server with service pack-1 and all updates. This procedure also assumes that the server's device drivers have been loaded and are fully functional.

Setup

The following steps make the assumption the server is to be configured as the VMS secondary domain controller (SDC) and assumes:

- There has not been a previous domain controller installation.
- There has been a clean install of Windows 2003 Server with service pack-1 and all updates.
- This procedure also assumes that the server's device drivers have been loaded and are fully functional.

On Local Area contention Properties, select TCP/IP and go to properties = > Make sure the DNS configured is the IP address of the Primary Domain Controller which has had DNS already as described in the section "Configuring a Domain Controller and DNS" on page D-3.

Note: This procedure relies on the secondary server being connected by an Ethernet link to the primary server and that the primary serve domain controller configuration is completed.

To configure a Domain Controller, start the **Configure Your Server Wizard** by doing either of the following:

1. Open the Configure Your Server Wizard by clicking Start > Control Panel > Administrative Tools > Configure Your Server Wizard.

2. From **Manage Your Server** shown in figure D-21, click Add or remove a role. By default, Manage Your Server starts automatically when you log on. To open Manage Your Server, click Start, click Control Panel, double-click Administrative Tools, and then double-click Manage Your Server.

Figure D-21 Manage your server dialog

3. Review the **Preliminary Steps** shown in figure D-22 and then click the **Next** button to proceed once you have verified these steps have been completed.

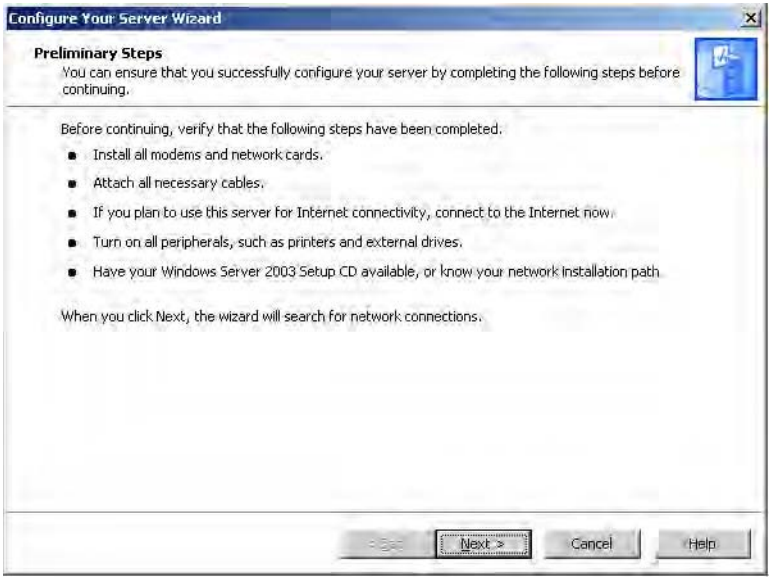


Figure D-22 Preliminary steps

4. The wait screen shown in figure D-23 will be displayed while your network settings are being detected.

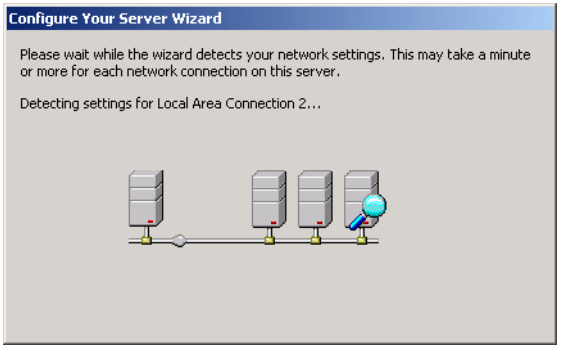


Figure D-23 Network detection wait screen

5. From the **Configuration Options** dialog shown in figure D-24, select the **Custom Configuration** radio button then click **Next** button.

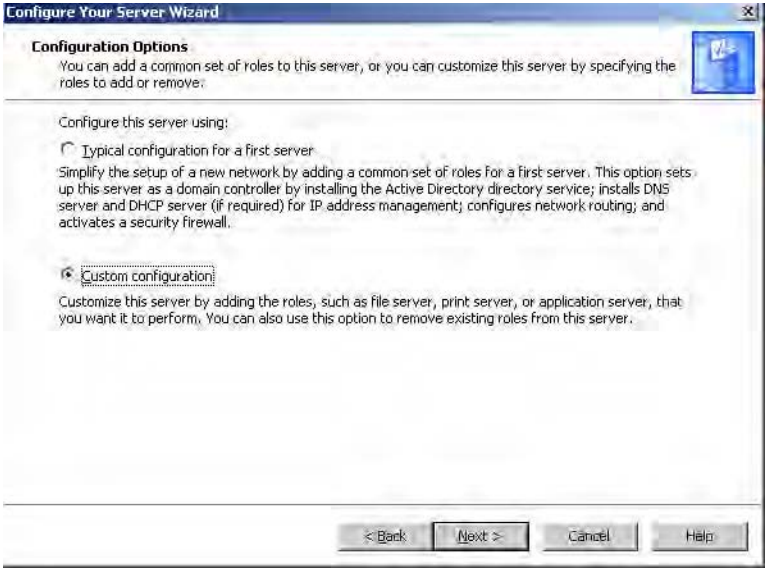


Figure D-24 Configuration options

6. From the **Server Role** dialog shown in figure D-25, select the **Domain Controller (Active Directory)** item, then click the **Next** button.

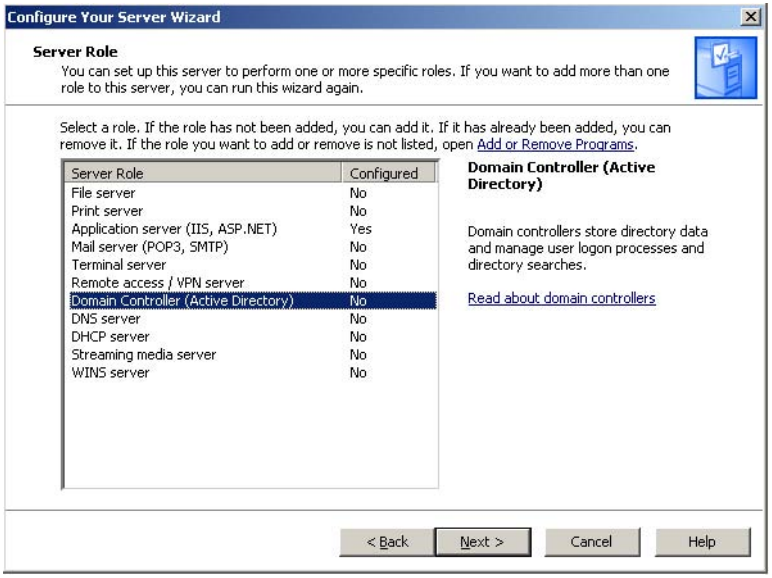


Figure D-25 Server role dialog

7. Verify your selection displayed in the **Summary of Selections** listing shown in figure D-26, then click the **Next** button to proceed.

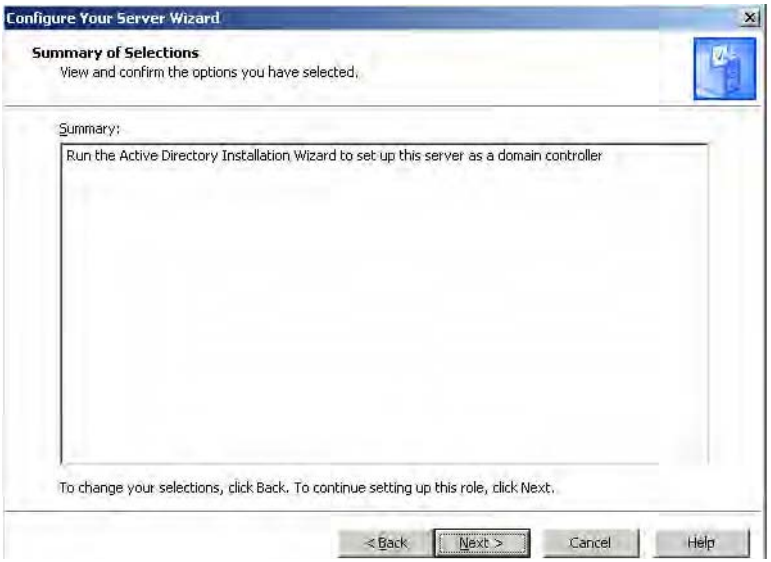


Figure D-26 Summary of selections dialog

8. From the **Active Directory Installation Wizard** shown in figure D-27, click the **Next** button to begin the installation.

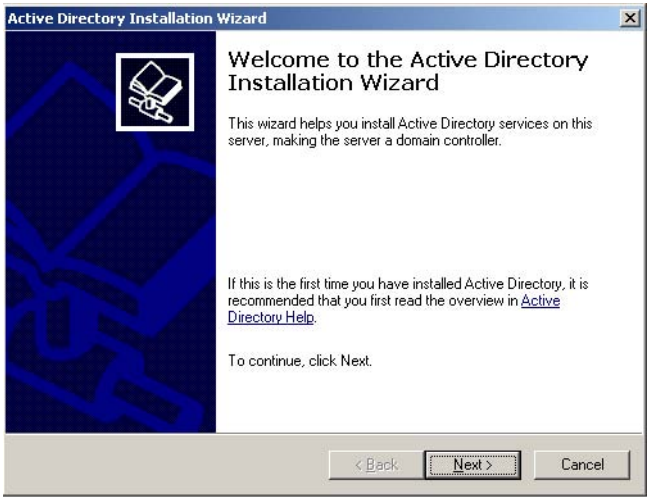


Figure D-27 Active directory installation wizard start

9. After reviewing the **Operating System Compatibility** information, shown in figure D-28, click the **Next** button.

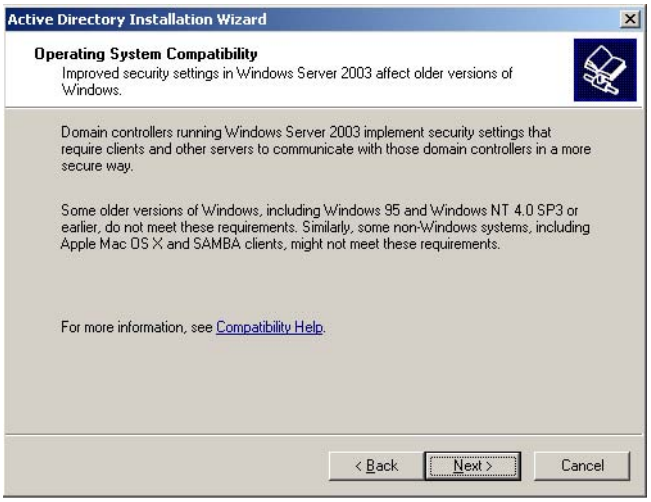


Figure D-28 Active directory installation wizard

10. After reviewing the **Operating System Compatibility** information, click the **Next** button.

11. From the dialog shown in figure D-29, select **Additional Domain controller for an existing domain** radio button, and then click the **Next** button.

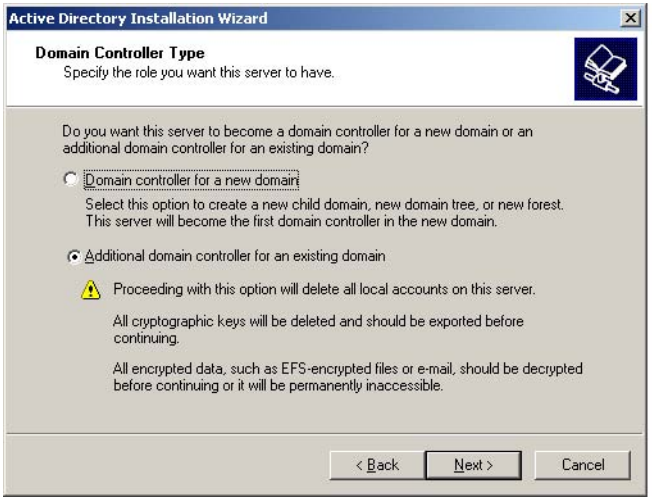


Figure D-29 Domain controller type dialog

12. In the **Network Credentials** dialog shown in figure D-30, enter the username, password and domain to be the administrator account for the domain

created above. When you have completed entering the data, click the Next button to continue.

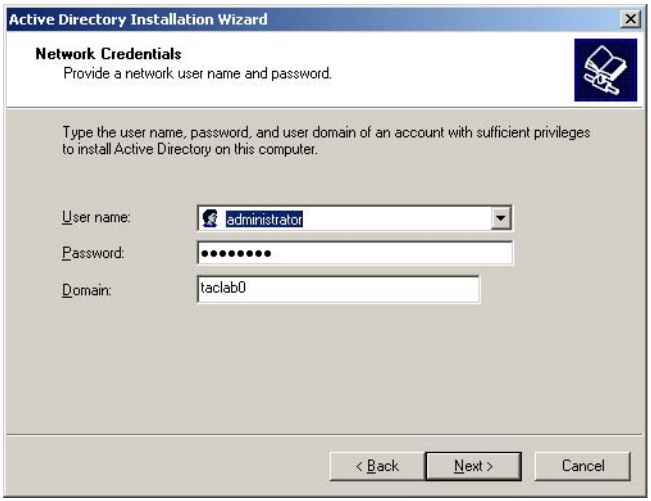


Figure D-30 Network credentials

13. from the **Additional Domain Controller** dialog shown in figure D-31, click the **Browse** button on the **Domain Name** dialog box.

14.

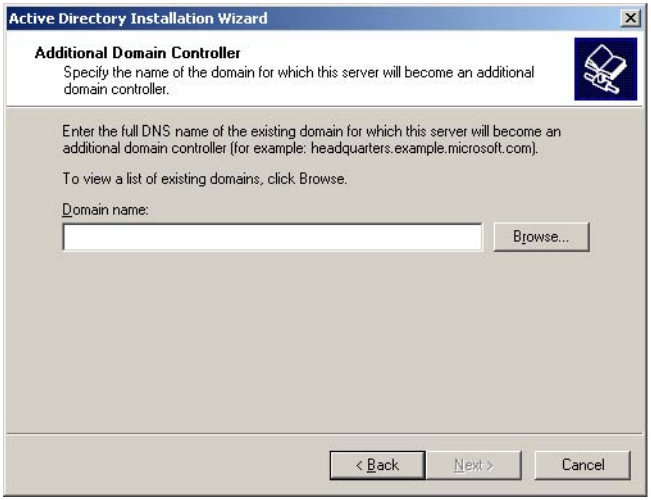


Figure D-31 Additional domain controller

15. Clicking the **Browse** button shown in figure D-31 brings up the **Browse for Domain** list shown in figure D-32. From the list of domains shown in the **Browse for Domain** list, select the Primary VMS server's domain, then click the **OK** button to proceed.

Figure D-32 Browse for domain list

16. The Additional Domain Controller screen shown in figure D-33 will be displayed the selected domain displayed. Click the **Next** button to continue.

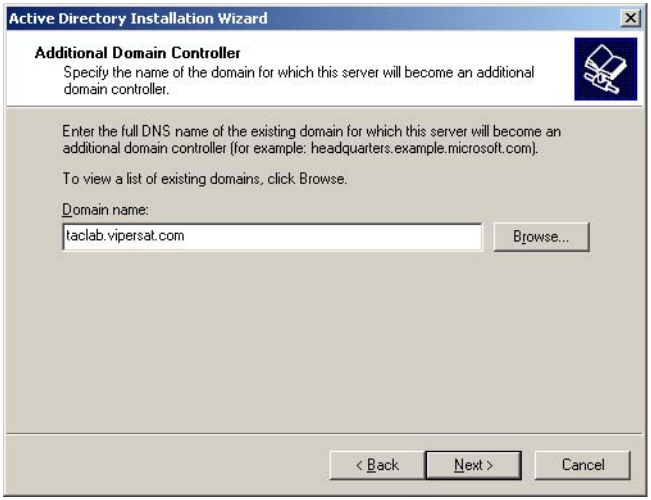


Figure D-33 Additional domain controller with domain name.

17. In the **Directory and Log Folders** dialog shown in figure D-34, enter C:\Windows\NTDS in the **Log Folder** dialog box as shown in figure D-34. This points the log folder to its default location in Microsoft Windows.

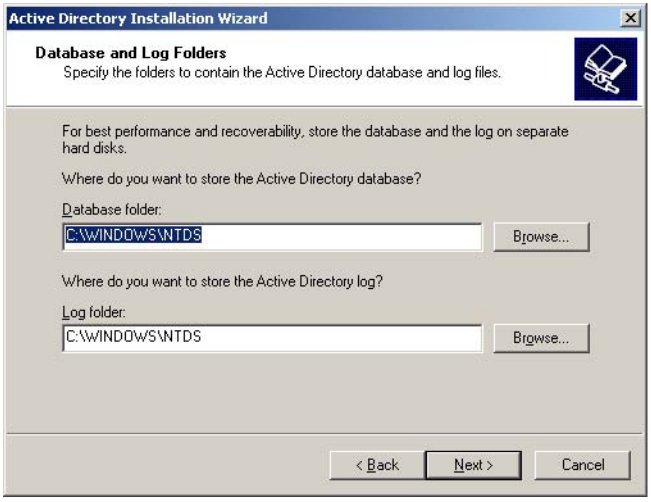


Figure D-34 Directory and log folders dialog

18. Leave the default folder location for the Shared System Volume, as shown in figure D-35, then click the **Next** button to continue.

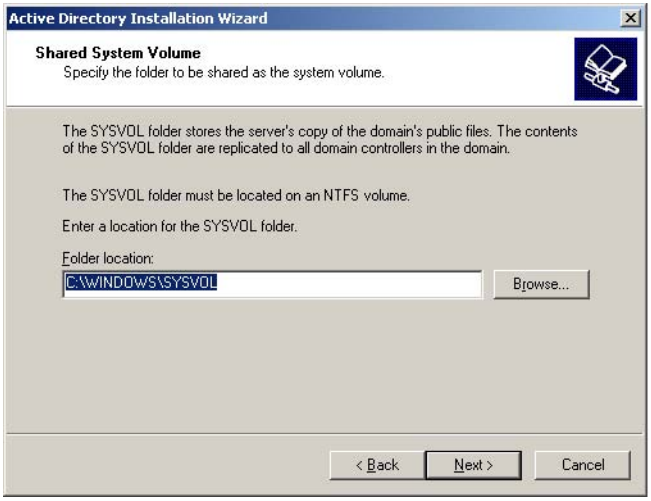


Figure D-35 Shared system volume

19. Type in the password for use by the Administrator account to be used when this server is started Directory Services Restore Mode. Enter the password in the **Restore Mode Password** and **Confirm** password dialog boxes as shown in figure D-36. Click the **Next** button when ready to proceed.

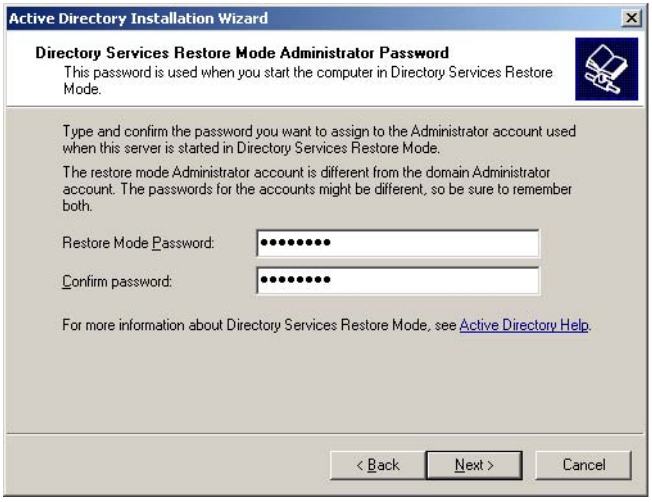


Figure D-36 Directory services restore mode administrative password

20. Review the **Summary** screen shown in figure D-37, then click the **Next** button to proceed.

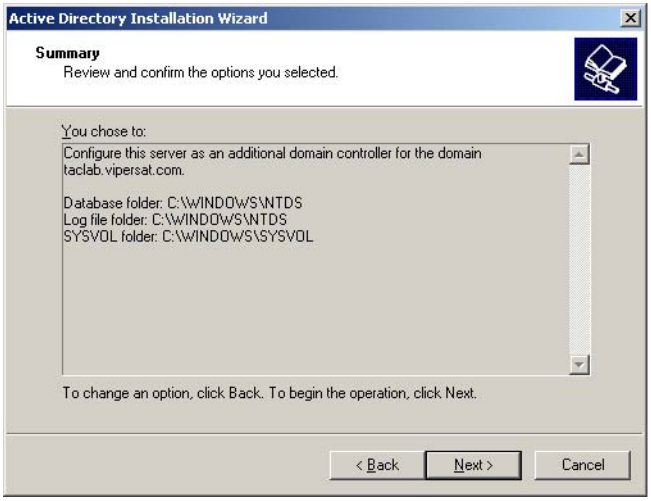


Figure D-37 Summary screen

21. The Active Directory Installation Wizard screen shown in figure D-38 will be displayed while Microsoft Windows configures your server.

Figure D-38 Active directory installation wizard screen

22. Review the screen shown in figure D-39 is displayed, then click the **Finish** button

Figure D-39 Domain Controller confirmation screen

23. From the screen shown in figure D-40, click the Restart Now button.

Figure D-40 Restart screen

24. After reboot, Windows displays the confirmation screen shown in figure D-41.

Figure D-41

This completes setting the secondary server as a domain controller.

Installing Secondary DNS Server

This procedure configures the secondary server to prepared take over the DNS function in the network if the primary server fails.

Setup

Before proceeding with setting the server to act as a secondary DNS server be sure that:

- You have successfully completed configuring the server as a Domain Controller
- Have your Server 2003 CD available
- Have Server 2003 Service Pack-1 installed

Use the following procedure to install the DNS server capability on the secondary server.

1. From the **Manage your server** dialog shown in figure D-42, click the **Add or remove a role** option.

Figure D-42 Manage your server dialog

2. Review the information in the **Preliminary Steps** screen shown in figure D-43 before proceeding and then click then **Next** button to proceed.

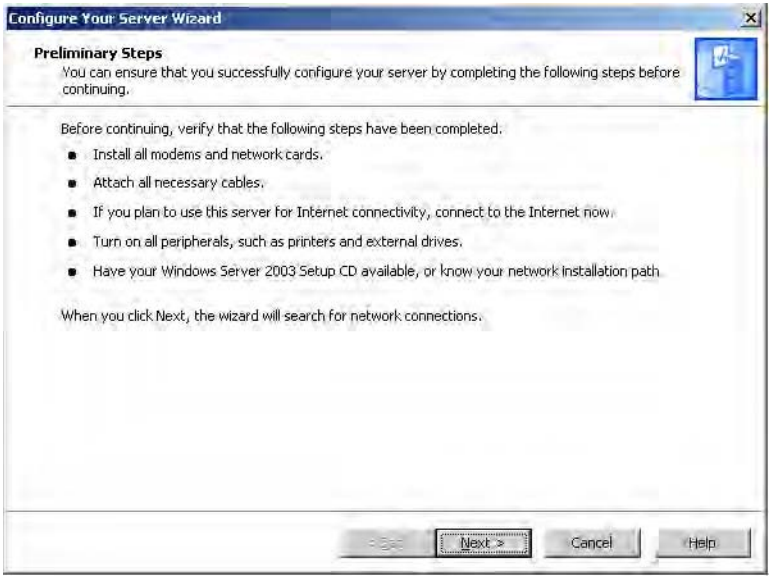


Figure D-43 Preliminary steps screen

3. Highlight DNS server in the table shown in figure D-44 and then click **Next** button.

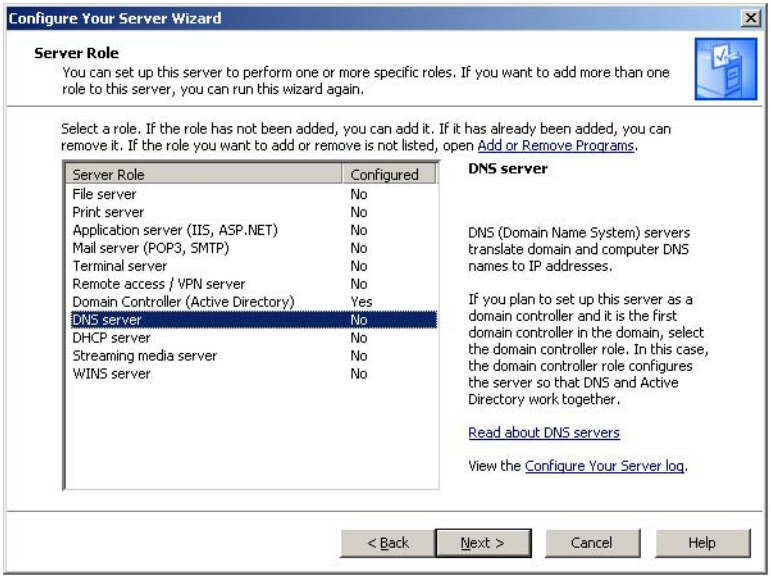


Figure D-44 DNS server role dialog

4. Review options selected as shown in figure D-45 and click the click the **Next** button to proceed.

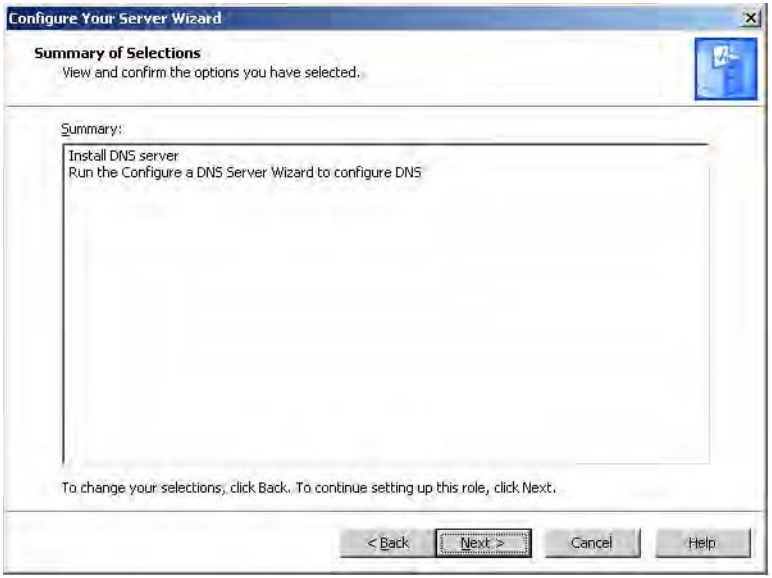


Figure D-45 DNS Selection summary

5. When prompted as shown in figure D-46, insert disc containing Service Pack 1 and click the **OK** button to start the installation process.

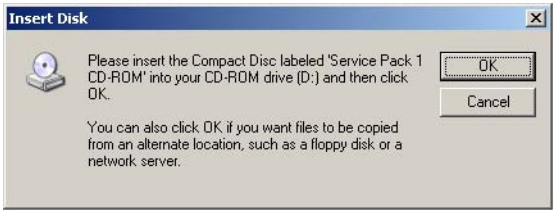


Figure D-46 Insert disk prompt

6. Setup will copy the required files and then proceed with configuring components as shown by progress bar in figure D-47.

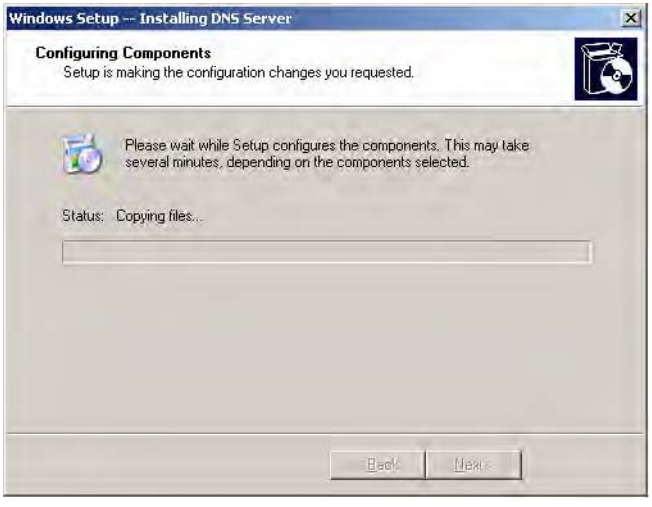


Figure D-47 Configuring components status

7. Click the **DNS Checklists** button shown in figure D-48 to display the checklist. After reviewing the DNS Checklist, click the **Next** button to continue.

Figure D-48 DNS server wizard welcome screen

8. Select the radio button **Forward Lookup Zone** as shown in **figure D-49**. Click the **Next** button to continue.

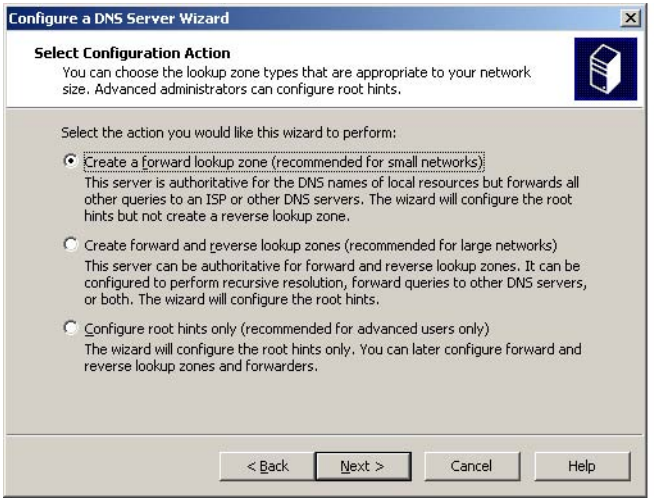


Figure D-49 Select configuration action

9. Select the radio button **This server maintains the zone** as shown in figure D-50. Click the **Next** button to continue.

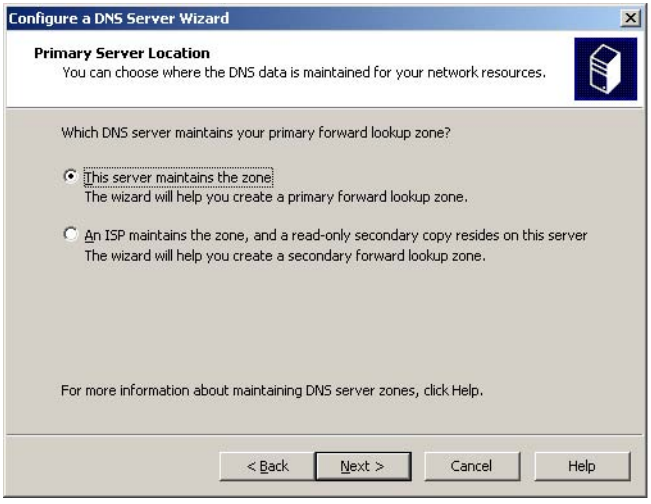


Figure D-50 Primary server location

10. Enter your DNS zone name in the **Zone name** dialog box shown in figure D-51. Click the **Next** button to continue.

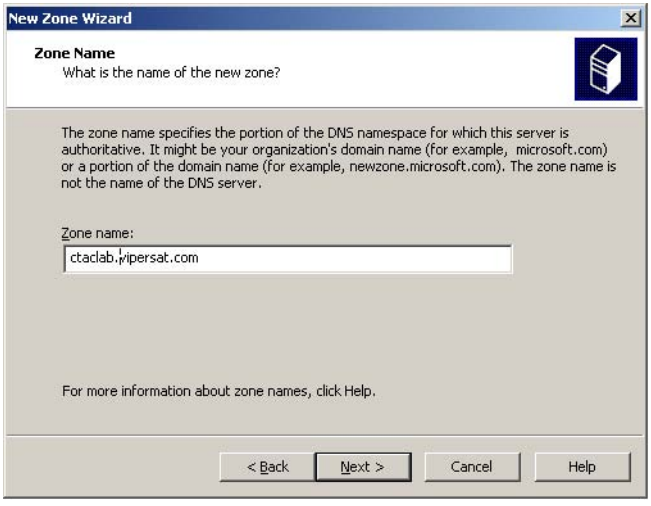


Figure D-51 zone name dialogr

11. Select the **Allow only secure dynamic updates** radio button shown in figure D-52. Click the **Next** button to continue.

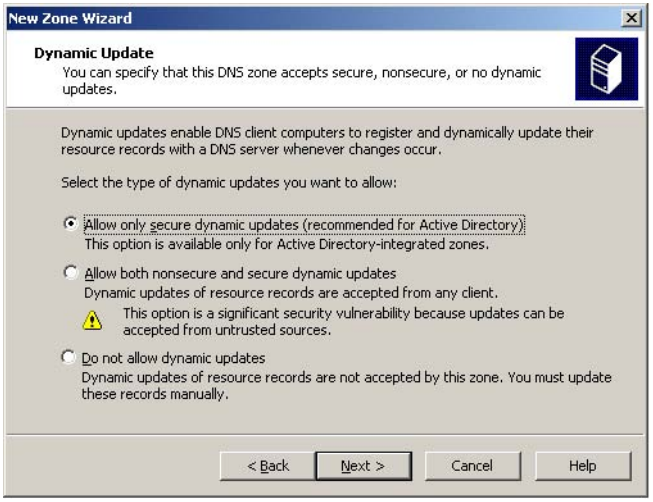


Figure D-52 Dynamic update dialog

12. Review the **Fowarders** dialog shown in figure D-53 and enter the IP address of DNS servers that this server will forward to if it is unable to resolve the request locally. Click the **Next** button when ready to continue.

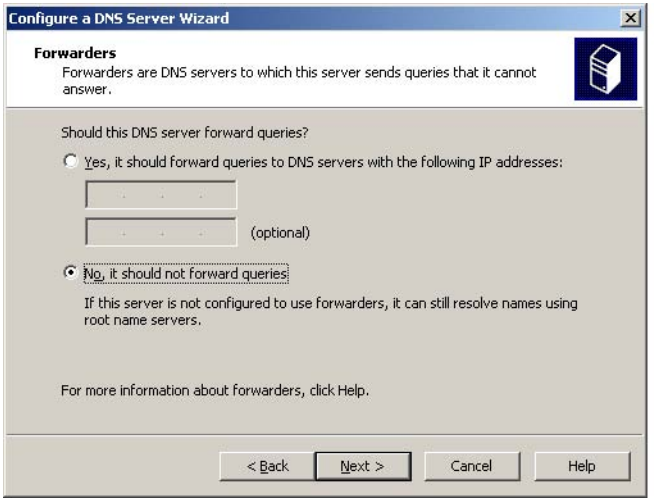


Figure D-53 Forwarders

13. After reviewing the **Completing the Active Directory Installation Wizard** screen shown in figure D-54, click the **Finish** button to continue.

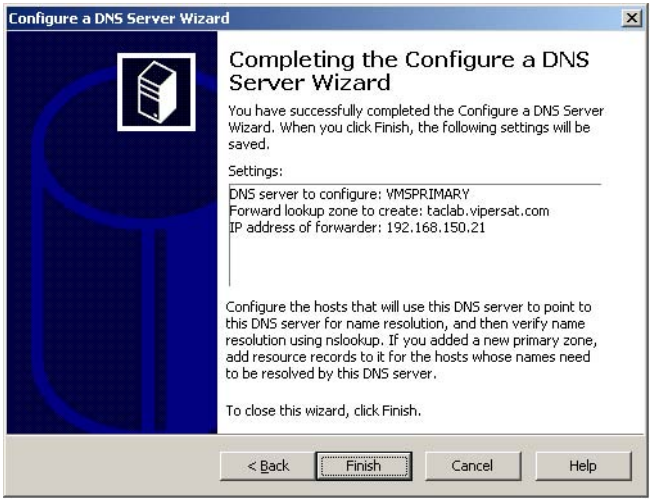


Figure D-54 Completing the configure a DNS server wizard

14. Carefully review the information in figure D-55 then click the **Finish** button.

Figure D-55 Completion screen

15. When the **DNS** error message shown in figure D-56 is displayed, click the **OK** button.

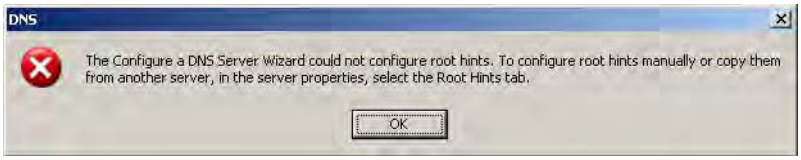


Figure D-56 DNS error message

This completes the installation of the DNS server on the Secondary VMS server in a redundant con figuration.

At this point return to section “Stop Previous VMS Version (Upgrade)” on page 2-10 of Chapter 2, “VMS Installation” to complete the VMS installation.

{ *This Page is Intentionally Blank* }

APPENDIX

E

SNMP TRAPS

Introduction

This appendix describes the use of SNMP traps by the Vipersat Management System (VMS). SNMP traps enable the VMS to capture significant network events, then generate an SNMP message reporting the event. In a VMS controlled satellite system, this configuration has several advantages:

- The VMS system, using its existing network monitoring capability, acts as a central collection point for all changes to the satellite network status and provides a single source for SNMP events reported for the satellite network. Individual network devices are not required to generate SNMP traps thereby reducing network overhead bandwidth.
- The VMS collects network changes and status as they occur and as they are reported by the satellite network's modem/routers as part of the normal VMS management and control function.
- Only events defined by the Vipersat MIB are sent as SNMP traps. This reduces the requirement to have each device transmit an SNMP trap as its status changes thereby reducing network overhead bandwidth requirements.

Note: Since VMS only collects and reports SNMP events from the satellite network and it is not the source of the event, you cannot query the VMS for additional information about an SNMP trapped event.

Using SNMP Traps

SNMP (Simple Network Management Protocol) along with the associated Vipersat Management Information Base (MIB), provides trap-directed notification of network changes.

VMS can be responsible for a large number of network parameters as defined in the Vipersat MIB. It is impractical for VMS to poll or request information from each device in a satellite network. Instead of each managed device generating its own SNMP traps, the VMS detects network status changes and when an event defined in the MIB occurs responds with a message called a trap.

After receiving a VMS generated trap, a high-level SNMP monitor can take action based on the trap type, and its parameters.

Using the VMS SNMP traps results in substantial savings of network bandwidth by eliminating the need for polling devices or having each device in the network generate its own SNMP traps. The primary purpose of and SNMP trap is high-order NMS notification.

SNMP Traps Available in VMS

The SNMP trap types available in VMS are:

- **Subnet Alarm Trap** - This trap is sent to the designated destinations whenever a subnet's alarm count or status in Subnet Manager is changed. This trap contains two values: 1) subnetLabel, 2) subnetAlarmCount
- **VMS Server Activated Trap** - This trap is sent to the designated destinations whenever a VMS server is activated (it's services are started). The IP address in the trap variable is the VMS server that has been activated. This trap contains one value: redundancyMode
- **VMS Active Server Failed** - This trap is sent by a VMS server operating in stand-by (non-active) mode whenever it has detected a failure of active server. A vmsServerActivatedTrap will follow when the stand-by is activated. This trap contains one value: redundancyMode
- **Redundant Device Restored Trap** - This trap is sent by VMS whenever the VMS Redundancy Manager has detected a failed device, has shut down the failed device, and has restored the failed unit with another device. This trap has four variables.

Note: SNMP Traps relative to the operation of servers in an N:1 redundant configuration only apply to a network which has the optional N:1 redundant capability available, installed, and configured.

Configuring SNMP Traps

To configure SNMP traps, from ViperView, shown in figure E-1, right click on the server's icon and select the Properties command from the drop-down menu.

Figure E-1 Server drop-down menu

Clicking the **Traps** tab on the server's properties screen displays the **Traps** dialog shown in figure E-3.

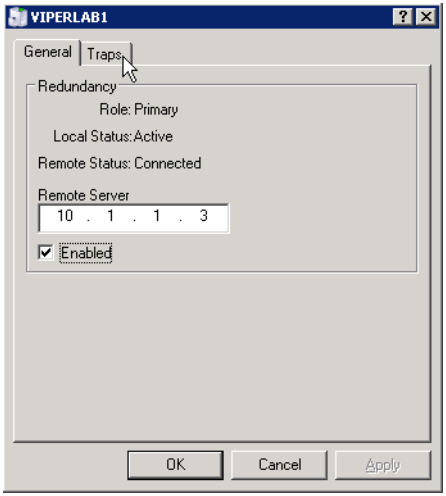


Figure E-2 Properties general tab

Select the **Traps** tab to display the **SNMP Manager TRAP** dialog shown in figure E-3. You can enter the Trap's destination information consisting of:

- IP address of SNMP manager receiving trap
- Port number

- Community String

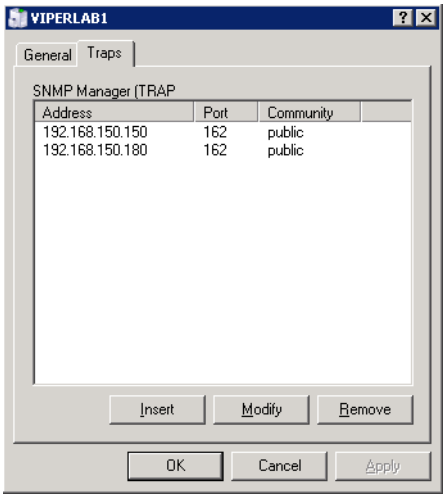


Figure E-3 Server traps tab

Insert

Clicking the **Insert** button displays the **Trap Destination** dialog shown in figure E-4 allowing you to enter the Trap's destination:

- IP Address
- Community String
- Port Number

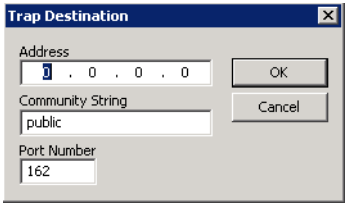


Figure E-4 Trap desitination

Modify

Selecting an existing Trap Destination from the list as shown in figure E-3 then clicking the **Modify** button will display the destination as shown in figure E-4 allowing you to change the Trap's destination as required.

Remove

Selecting a Trap Destination from the list shown in figure E-3 then clicking the **Remove** button will remove the Trap Destination.

Summary

You should keep in mind the following characteristics of an SNMP Trap.

- SNMP is not a “reliable” transport protocol. If the Trap message is lost due to network issues (congestion, noise, delays, etc.), the SNMP protocol will NOT retransmit the lost trap message.
- SNMP (v1&v2) is not a secure protocol. It is not difficult to eavesdrop or spoof messages. Isolating SNMP traffic from end-user channel is recommended.
- VMS will generate a trap message for each destination entered. Entering 10 trap destinations, for example, will generate 10 trap messages for each event.
- Only a VMS server in Active mode will generate trap messages. A redundant VMS server in stand-by mode will not generate or send a trap message until it is switched to Active mode for example the Primary server failure is detected.
- At this time there is no VMS SNMP agent in VMS. An SNMP Manager cannot poll VMS for status or configuration detail information.
- Current trap uses SNMP v1.

APPENDIX

F

AUTOMATIC SWITCHING

General

The basic signal topology in a Vipersat network is TDM (Time Division Multiplex) outbound and Vipersat's proprietary STDMA (Selected Time Division Multiple Access) inbound. The STDMA slots can have their duration and bandwidth allotments varied to tailor bandwidth allocation to meet the bursty traffic load of a typical data network.

When required, a network is switched from STDMA to SCPC. SCPC bandwidth is allocated from a bandwidth pool by VMS to meet QoS or other requirements for the duration of a connection. When the SCPC connection is no longer required, the bandwidth is returned to the pool for use by another client.

This basic structure gives the VMS controlled network its flexible, automated network utilization and optimization capability.

The VMS has the intelligence to interpret the constantly changing statistics gathered by the intelligent modem/routers and uses this data to issue commands back to the Vipersat Modem/Routers effectively managing the Vipersat network operation in real-time, optimizing each user's bandwidth usage to meet their QoS, and cost requirements, within their bandwidth allocation. The result is a stable satellite network connection automatically responding to customer's requirements while continuously monitoring and reacting to changing load, data type, and QoS requirements.

Bandwidth Allocation and Load Switching

Load Switching is the mechanism by which the Vipersat network switches a remote terminal from STDMA to SCPC mode or SCPC-to-SCPC dynamic based on traffic levels at the remote. There are two components of load switching in a Vipersat system: VMS (Vipersat Network Management), MODEM (CDM-570/570L, SLM-5650A). The VMS component receives switch requests from the MODEM based on policy settings and available resources, either grants or denies the request. Within the MODEM component, load switching is managed at either the Hub or the Remote, based on the current mode of operation. When a remote is in STDMA mode, load switching for that remote is managed by the Hub STDMA controller. After a Remote has been switched to SCPC mode it manages its own switching (or Step Up / Step Down) requests.

The basic concept for all load switching is that a running average of current utilization is maintained, and when that utilization exceeds a pre-set threshold, a switch is initiated. The data rate for the switch is computed by determining the current bandwidth requirement of the remote and adding some percentage of excess margin. The main difference between switching from STDMA to SCPC and adjusting within SCPC is that in STDMA mode, the current available bandwidth is constantly changing while in SCPC mode it is constant between switches. Furthermore, switches from STDMA to SCPC mode are always caused by the traffic level exceeding the switch threshold. Within SCPC mode, switches can be caused by traffic exceeding an upper threshold or dropping below a lower threshold. However, in both cases the new data rate is based on the actual traffic requirements adjusted up by the margin percentage. Also, based on policies set in the VMS, if a remote requests less than some threshold amount of bandwidth, the remote in put back into STDMA mode.

Note: If the Hub STDMA mode is GIR (Guaranteed Information Rate) or Entry Channel, normal load switching is automatically disabled. In GIR mode, the remote is switched to SCPC as soon as the GIR threshold is reached, if there is a switch rate defined. In Entry Channel mode, the remote is switched to SCPC as soon as the hub receives the first transmission from the remote.

Load switching

The next sections describe the principles behind Load Switching and Rate Adjustment (Step Up / Step Down).

Bandwidth Allocation and Load Switching by the STDMA Controller:

As part of normal STDMA processing, the hub monitors the traffic levels from each of the remotes for which it is allocating bandwidth. This is done using the STDMA ACK management message (Table 1) which is transmitted at the beginning of each burst from the remote. The STDMA ACK contains two metrics that are used by the hub:

1. The number of bytes received for transmission (Queued Bytes) since the last cycle.

2. The number of bytes currently waiting to be transmitted (Bytes In Queue).

These metrics are used by the hub for 3 purposes:

1. Determine the amount of STDMA bandwidth (slot size) to allocate in the next cycle.

2. Provide statistics of the amount of activity at each remote (Average Bytes Received).

3. Determine if a load switch is needed.

Table F-1 STDMA ACK Message

Data Type	Size in Bytes	Description	Unit of Measure	Notes
IP	4	IP address of Remote	N/A	Used by remote to identify itself
Unsigned	4	Queued Bytes	Bytes	Total number of bytes queued since last cycle (includes possible buffer overflow)
Unsigned	4	Bytes in Queue	Bytes	Number of bytes currently queued
Unsigned	1	Group Number	N/A	
Unsigned	1	Dropped Buffers	Packets	Number of packets dropped (due to limited bandwidth)

If there is adequate upstream bandwidth available, the values of these two metrics will be the same. However, if there is not enough bandwidth to satisfy the traffic requirements of the remote, or if the remote has exceeded the maximum allocation, some data will be held for the next cycle. In this case, the number of Bytes in Queue will start to grow and will exceed the Queued Bytes.

(In other words, the Bytes in Queue is the sum of the data not yet transmitted plus the new data received).

If the condition is due to a short burst of data, the backlogged data will eventually be transmitted and the system will return to a sustainable rate. However, if the overload condition is due to long term increased activity, then the backlog condition will continue to grow and eventually trigger an SCPC switch. If the overload condition lasts long enough, buffer capacity will eventually be exceeded and some data may have to be discarded.

Note: This is not necessarily bad, as it is often more effective to discard old data than transmit it after it has become 'stale.'

The "Bytes in Queue" metric is used to determine the STDMA bandwidth allocated (slot size) for the next cycle; the goal being to keep the data backlog to zero. The hub uses this metric to compute the slot size for each remote in the next cycle as follows:

- **Fixed Mode -** All remotes get the same slot regardless of need; in other words, the metric is not used.
- **Dynamic Cycle Mode -** Available bandwidth is allocated to remotes proportionally based on current need. The bandwidth allocation for remotes is calculated by dividing the Bytes in Queue for each remote by the total Bytes in Queue for all remotes to calculate the percentage bandwidth allocation to be given to each remote.
- **Dynamic Slot Mode -** The slot size for each remote is computed based on the time (at the current data rate) needed to transmit all the Bytes in Queue. If the result is less than the minimum slot size or more than the maximum slot size, the slot is adjusted accordingly.
- **GIR (Guaranteed Information Rate) Mode -** Initially computed the same as Dynamic Cycle except there is no maximum limit. After all remotes have been assigned slots, the burst map is checked to see if the total cycle length exceeds 1 second. If not, then all requirements are satisfied and the burst map is complete. However, if the cycle is greater than one second, then the slots are adjusted proportionally so that all remotes receive at least their guaranteed rate plus whatever excess is still available. (In the current design, when the 1 second restriction is exceeded, remotes without a specified GIR are reduced to the global minimum slot size and the remaining bandwidth is distributed amongst remotes that have been assigned a GIR rate. This approach is based on the assumption that remotes that have been assigned a GIR are paying a premium and should benefit from available excess bandwidth when needed. Note that the GIR allocations are restricted so that the assigned GIR totals cannot exceed available bandwidth. If this restriction is

somehow violated, then it will not be possible to properly allocate bandwidth when the network is overloaded.)

- **Entry Channel Mode -** This is the same as Dynamic Cycle, except that as soon as the Hub receives an STDMA ACK, it initiates a switch to SCPC mode based on the policy set for that remote.

The important thing to understand about “Bytes in Queue” is that any data that is not transmitted (i.e. does not fit) in the next slot will be reported again in the next STDMA ACK. Thus the “Bytes in Queue” is not necessarily an accurate measure of the actual traffic being passed through the remote.

The “Queued Bytes” on the other hand, reflects only the data that was received in the last cycle and thus is never duplicated (not including TCP retransmissions). This is the metric that is used for computing average load and initiating a load switch as needed.

Before discussing how load switching is determined, it is necessary to explain the user parameters that control the switch. The menu shown in figure F-1 and figure F-2 shows the entries in the automatic switching menu at the hub that are used to control load switching.

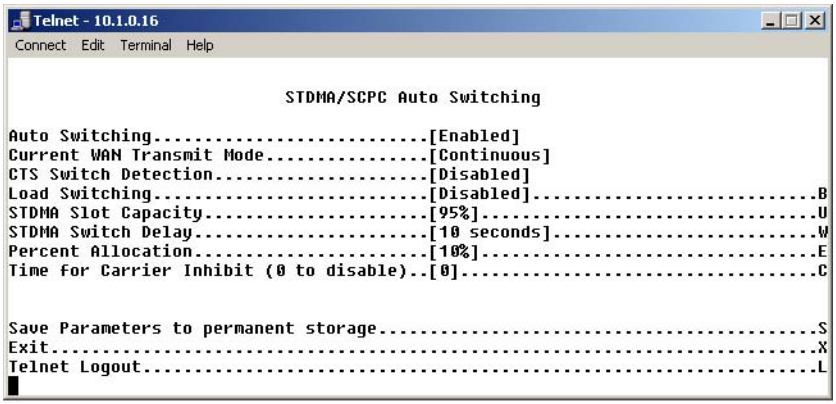


Figure F-1 Hub switching menu, CDM-570/570L

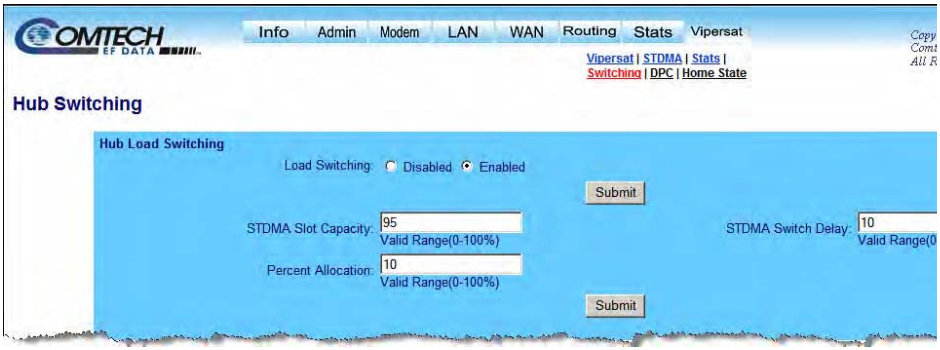


Figure F-2 Hub Load switching menu, SLM-5650A

- **Auto Switching -** This is a Vipersat feature which is enabled in the CDM-570/570L **Features** menu. If Auto Switching is not enabled, Load Switching will be ignored. There is no auto switching enable button in SLM-5650A modem configuration menus, the operator only needs to enable each switching function.
- **Load Switching -** This is a type of Automatic Switching that is based on the amount of traffic at a remote. If this mode is not set, then no remote will be switched based on load.
- **STDMA Slot Capacity -** This is a threshold value. When the amount of outbound traffic at a remote exceeds this percentage of the current STDMA slot capacity, a load switch is initiated. It is important to understand that in most STDMA modes, the amount of bandwidth allocated to a remote varies with need and thus from cycle to cycle. Thus the amount of traffic that constitutes X% will also vary from cycle to cycle.
- **STDMA Switch Delay-** This is a built in latency that forces a remote to maintain an average load over some number of seconds after reaching a switch condition before the switch is actually initiated. This prevents switches due to momentary traffic-bursts.
- **Percent Allocation -** This is an excess amount of bandwidth that is allocated beyond the current traffic rate when the switch to SCPC is made. For example, if the current average traffic at the time of the switch is 60K, and the **Percent Allocation** is 10%, then the allocation will be for 60K + 6K = 66K.

Note: Since the hub always allocates bandwidth in 16K blocks the 66K, when rounded up, would actually be 80K in this example.

Load Switching Process

Each time the hub receives an STDMA ACK, it computes the average load for that remote. This average is then compared to the bandwidth currently allocated to the remote.

For example, if a remote gets a 50 ms slot in an upstream that is running at 512000 bps then it can transmit 0.050 * 512000 = 25600 bits = 3200 bytes. If the Queued Bytes was 3000, then for that cycle, the remote was at 3000/3200 = 93.75% of capacity. (If the current cycle time is exactly 1 second, then the effective data rate of the remote is also 25600 bits per second.

However, if the cycle time is only 500 milliseconds, then the effective data rate is actually 25600 /.5 = 51200 bits per second. The effective data rate is important for calculating switch data rates. If the average bandwidth used exceeds the threshold percentage of available bandwidth, then a flag is set indicating a switch is pending. At this point, the statistics are reset and the traffic load is then computed for the time period specified by the switch delay. At the end of this delay, if the threshold is still exceeded, a switch is initiated. The data rate specified for the switch is determined by taking the current load, as indicated by the bytes queued during the delay period, multiplying it by the percent allocation and rounding up to the next 16Kbps.

A key point is that in most of the STDMA modes, the bandwidth allocated to each remote is constantly being adjusted to the needs of the network. As long as the network is running below capacity, most remotes will get the bandwidth they need and a switch will not be required.

Only when a remote requires more bandwidth than is available in STDMA will a switch occur.

Furthermore, in D2 mode, each remote will always appear to be running at near 100% capacity, even when there is actually excess bandwidth available. This is because in D2 mode, the remotes are almost never given more bandwidth than they need. As a result, the algorithm for D2 mode uses a maximum allowed slot size rather than the actual allocated slot size to calculate the effective data rate. This gives a more accurate estimate of the available STDMA bandwidth.

Load Switching by a Remote

Once a remote has been switched to SCPC mode, it checks its bandwidth requirements once per second to see if a change is needed. The menu for controlling the Step Up / Step Down switches are set in the menu shown in figure F-3.

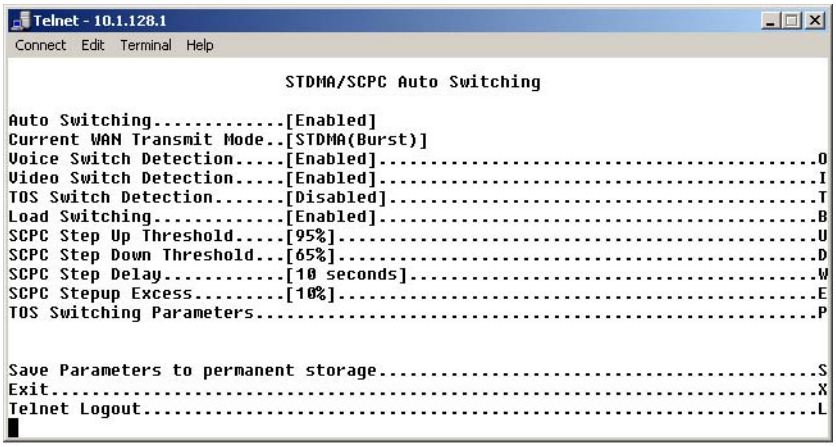


Figure F-3 Switching menu for a remote, CDM-570/570L

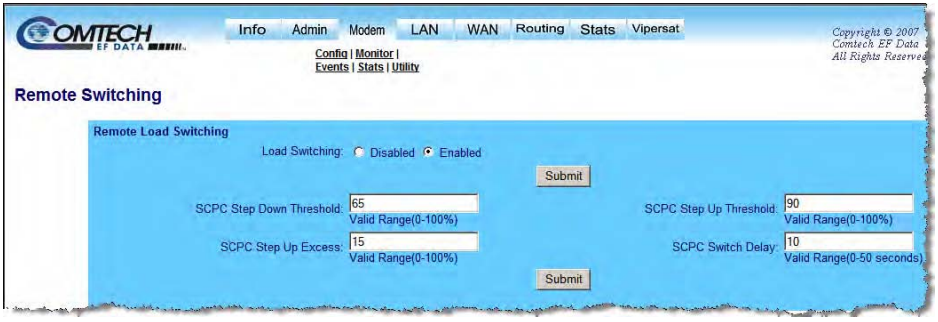


Figure F-4 Load switching menu for remote, SLM-5650A

- **Auto Switching -** Same as Hub
- **SCPC Step Up Threshold** - Same as **STDMA Slot Capacity** at hub.
- **SCPC Step Down Threshold** - Similar to **STDMA Slot Capacity** at hub except **Step Down** is used to trigger a switch if the average load falls below this value
- **SCPC Step Delay** - Same as **STDMA Switch Delay** at hub
- **SCPC Stepup Excess** - Same as **Percent Allocation** at hub. Note that the value applies to both **Step Up** and **Step Down** switches and if computed against the average traffic load at the time the switch is initiated.

Determining Need-for-Change

The following process is used to determine if bandwidth utilization warrants a need-for-change.

The user defines both a Step Up and Step Down threshold in terms of percent utilization, a bandwidth margin value, and a latency or averaging period. Once per second, the CDM router software determines the current percent utilization by dividing the bits transmitted by the current transmit data rate.

If the percent utilization exceeds the step up threshold or is less than the step down threshold for the entire latency period, then an ASR (Automatic Switch Request) is sent to the VMS. The bandwidth requirement for the ASR is computed by taking the average percent utilization over the latency period and multiplying that by the current data rate to determine the actual data rate used over the measured interval. This number is multiplied by the margin value and rounded up to the nearest 8K to determine the requested bandwidth.

Load Switch Example

An automatic load switching example, illustrated in the schematic diagram in figure F-5, illustrates how a network can respond to changes in traffic volume or load conditions. The network's capability and method of response to load changes is determined by the setting and capability of each of the components in the system such as the transmitter power output, the antenna capabilities for each of the sites in the network, and the policies set in VMS.

The elements for determining policies and their interactions are discussed in this section.

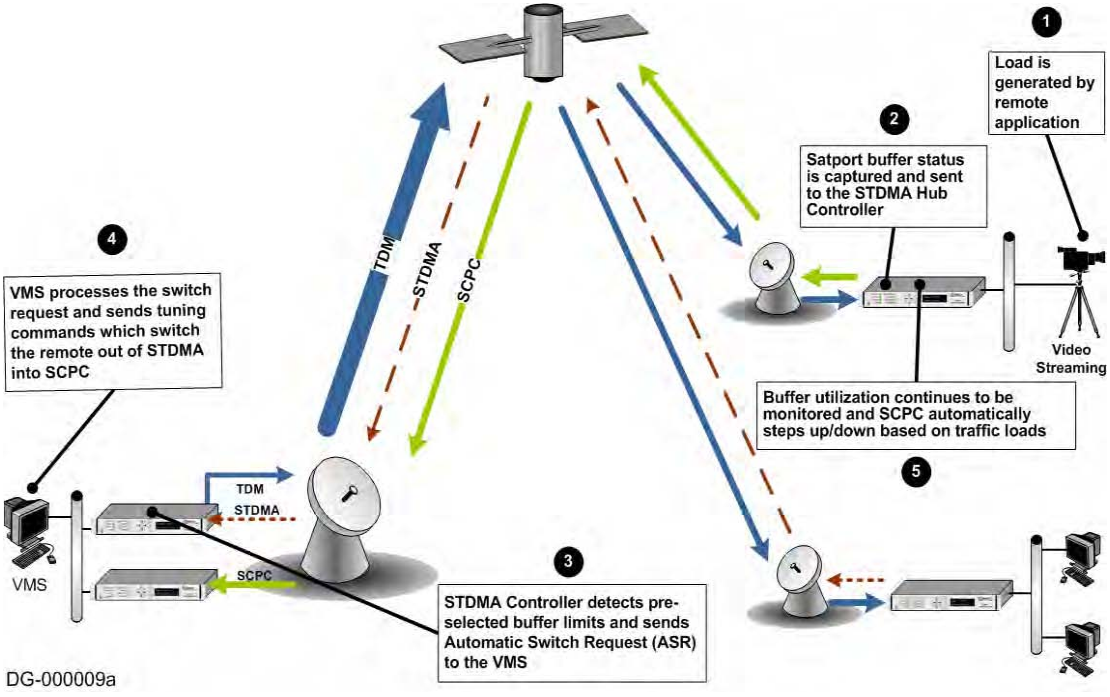


Figure F-5 Example load switching diagram

A load switch is illustrated in figure F-5 are using the following process.

1. A load is generated an application at a remote and the application is a video stream.

2. As an example the data is connected to the remote CDM-570/570L over an ethernet link for transmission to the satellite. While the data-stream transmission is in progress, the Satport buffer status is captured and the CDM-570/570L's buffer status is sent to the STDMA Hub Controller.

3. The STDMA Hub Controller compares the remote CDM-570/570L's pre-selected buffer limits with its buffer status and if the buffer status exceeds the preselected limits the STDMA Hub Controller increases the time-slot allocated to that channel. If this brings the buffer status within established limits no further changes are made.

4. If the buffer status continues to exceed the preselected limits, the STDMA Controller sends an Automatic Switch Request (ASR) to the VMS.

5. The VMS processes the switch request by checking for available resources by:

- Determining if there is a free demodulator.
- Determining the channel space (bandwidth) requirements to accommodate the data flow requested by the STDMA Hub Controller.

6. If the VMS finds available resources it processes the switch request and sends tuning commands which switches the remote CDM-570/570L out of STDMA into SCPC mode.

The ideal condition being looked for is that about 90% utilization of the channel be achieved striving to optimize the use of available bandwidth.

The CDM-570/570L continuously monitors traffic flow volume Whenever a preset upper or lower limit is exceeded, the CDM-570/570L sends a request to VMS to change bandwidth by the amount needed to meet the new requirement. By this process, the bandwidth is continuously optimized in real time, precisely accommodating circuit traffic volume.

The ability to actually accomplish this is limited by the currently available carrier bandwidth, and ultimately the power output and antenna size available at the transmitting remote site.

If the VMS does not have available bandwidth it will ignore the STDMA Hub Controller's request for increased bandwidth. The STDMA Hub Controller will continue to receive buffer status reports from the remote CDM-570/570L indicating that buffer flow is continuing. The STDMA Hub Controller will, in turn, continue to request additional bandwidth from the VMS. If at any time another service drops making bandwidth available, the next time the STDMA Hub Controller requests additional bandwidth the VMS will grant the request.

If the video data stream is completed before the switch in bandwidth is done, the channel is closed, the bandwidth which had been used is made available again to the pool, and no further action is taken.

Reduced data flow in switched mode (SCPC)

In the event the data flow is reduced, for example a streaming file transfer terminates, the SCPC switched demodulator detects the reduced flow and notifies the VMS. The VMS will then send a switch command to reduce the size of the carrier bandwidth to the new calculated bandwidth requirement.

This entire process is automatic following the policies established for the network. The network is dynamically modified changing its configuration to automatically respond to changes to the network's load.

The home threshold is the bit rate set to trigger a return to the home threshold. This function is used when bandwidth has been allocated to meet load requirements, and the load has been either removed or partially removed. Since the channel's new load no longer requires the current bit rate, when the bit rate falls below the preset Home Threshold the channel is switched back to its home condition, STDMA for example.

Note: The load switching example works exactly the same for the SLM-5650A modem.

Application switching

Application switching, diagramed in figure F-6, also is capable of changing bandwidth used, but the change is determined entirely by the type of application being requested ignoring load requirements.

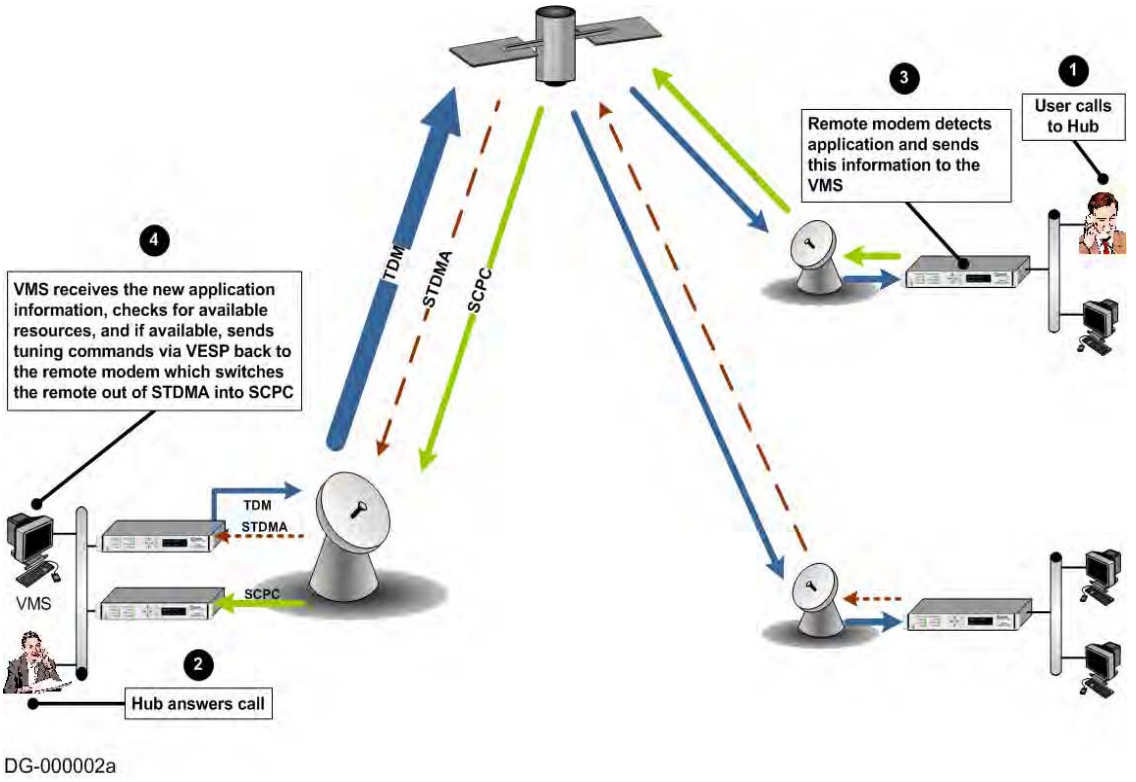


Figure F-6 Application switching diagram, CDM-570/570L

Note: Application switching is not available for SLM-5650A modems. The following application switching section refers to CDM-570/570L modems.

In a system configured for application switching, the remote site modem/router looks for a packet in the data stream coming from the LAN that is configured using the H.323 stack protocol and contains an H.225 signaling protocol. In the illustration shown in Figure F-6 the signal is a call initiated at the remote site.

The packet is then examined to determine the port number then, from the allocated port ranges, determines the type of application being sent.

The modem/router sends a switch request to the VMS requesting a carrier for the application type. Typical applications include:

- Video
- Voice over IP (VoIP)

Each application type will have been assigned a bandwidth allocation when the policy for the remote site is established. The voice application, for example, might have had the bandwidth set in the policy to handle three simultaneous voice connections. When a VoIP protocol is detected in the H.225 signaling protocol, the modem/router requests the VMS to switch the bandwidth to accommodate three voice circuits.

The same process applies if the protocol detected is Video.

When *both* VoIP and Video are requested, the bandwidth required for the Video is used and the VoIP, which has priority, shares the SCPC with the Video.

Once VMS receives the request to switch, it determines if there is a free demodulator and if there is bandwidth space available to handle the requested application. If the resources are available, the VMS then performs the switch.

Applications are streaming data. The remote modem/router looks at the streaming data flow until it sees a break in the data exceeding 10 seconds. Once a break is detected the modem/router presumes that the application is terminated (or has malfunctioned), drops the carrier, and makes the bandwidth resources available for another service.

Type of Service (ToS) Switching

Type of Service (ToS) switching is used on circuits carrying encrypted traffic where the packets cannot be examined to determine the type of traffic being carried. Normally, in a non-encrypted Vipersat network, packets are classified by the remote CDM-570/570L using protocol classification detection and the results are forwarded to VMS via Automatic Switch Request (ASR) messages. The VMS switch detector service then applies the required or requested bandwidth using policies which have been pre-configured in the VMS.

Type of Service switching can also be used in non-encrypted networks as well. One advantage is that each packet associated with the application will have ToS set. Therefore, ToS switching is extremely reliable. A drawback is that unless each application can set a different ToS value, resolution is lost.

For example, in a non-encrypted network if a voice application service connection is started, the CDM-570/570L's classifier analyzes signaling and data protocols (H.323, SIP, & Data RTP) being routed through the CDM-570/570L. After connection detection, the process waits for data (RTP). Data is normally sent after the receiving party answers, which then triggers the system to process an ASR.

Using the ToS classification, detection function allows application-based-switching in encrypted networks where the signaling protocols are encrypted or effectively hidden. ToS adds the type of service to the un-encrypted Quality of Service byte (QoS) in the IP header which then can be analyzed to determine the type of service being transmitted. Once the type of service is determined, VMS uses this information to perform switching following the policies established for the detected traffic type.

Note: Load switching by VMS is not affected by enabling ToS detection.

Refer to the Parameter Editor section of the modem manuals for detailed information on enabling and implementing ToS switching on your network.

Applying a ToS value to an application (VoIP, IPVC, or priority data) through either preservation or classification packet stamping, allows the VMS to function in an encrypted network.

{ *This Page is Intentionally Blank* }

APPENDIX

G

ENTRY CHANNEL MODE SWITCHING

Entry Channel Mode (ECM)

STDMA entry channel mode provides a method for remotes requiring SCPC access channels to enter/re-enter the network initially or after a power or other site outage. The switch time will be variable based on the burst rate (bps) of the STDMA group, the number of remotes with slots in the group, and where in the burst cycle the remote is when it acknowledges receipt of the burst map.

Initial SCPC rates are settable for each remote in the STDMA group(s). Upon detection of a burst map acknowledgement from a remote the STDMA burst controller will send a switch request to the VMS with the operator specified initial SCPC rate. Upon determining that there is an available demodulator and pool bandwidth the VMS will send a multi-command to remove the remote from the STDMA group, tune it and the switched demodulator to the specified initial bit rate and selected pool frequency. The remote will stay at this initial rate unless an application (such as VTC) or consistent load cause it to request additional bandwidth from the VMS.

Entry channel mode is not driven by the presence or absence of customer traffic. Once in ECM mode, the switched initial data rate becomes the new temporary home state. This temporary home state sets the low limit data load threshold, where the remote will stop sending load switch request commands. Remotes in ECM mode do not require burst maps to maintain SCPC transmission.

Note: Remotes in ECM mode toggle directly from STDMA to SCPC and back. The initial SCPC switch state is used instead of the modem's internal home state for modems operating in ECM mode.

After all remotes are processed into ECM, the Burst Controller drops into sanity mode sending a keep alive map to service remotes which may have their SCPC carrier inhibit flag set. The keep alive message is sent once every two seconds until re-entry is invoked.

Fail Safe Operation

For a detailed description of the features of VMS applications switching, refer to Appendix F, "Automatic Switching". As application switching relates to the ECM mode, it is useful to describe the fail-safe mechanism used for freeing pool bandwidth.

If the VMS loses communications with a switched remote for more than three minutes, it will attempt to return the remote to home state. If the revert-to-home state command succeeds (restoring communications) Entry Channel Mode will cause the remote to switch to its initial SCPC bit rate.

If the revert-to-home state command fails, the VMS will send a command to return the remote and the hub demodulator to the state where they were prior to losing communications, but leave the remote enabled in the STDMA burst controller. This provides the remote with 2 paths to rejoin the network:

1. If the outage was the result of power outage at the site, the remote CDM-570/570L or SLM-5650A will reboot in its home state (STDMA), acknowledge the receipt of the first burst map causing it to rejoin the network through ECM. The VMS will park the demodulator previously in use and free the bandwidth slot.

2. If the outage was due to an extended rain fade or other communications blockage with no loss of power, the remote will rejoin the network via the previously assigned SCPC channel. When VMS receives a PLDM it will send a revert-to-home state command and free the bandwidth slot and burst demodulator. The remote will then rejoin the network through ECM.

Since it is not possible to know which of the above scenarios caused the communications outage the VMS will not free the bandwidth slot except through operator intervention.

Figure G-1 and figure G-2 diagram the time state differences and the process of recovery. Note that the times referenced in the diagrams are approximate.

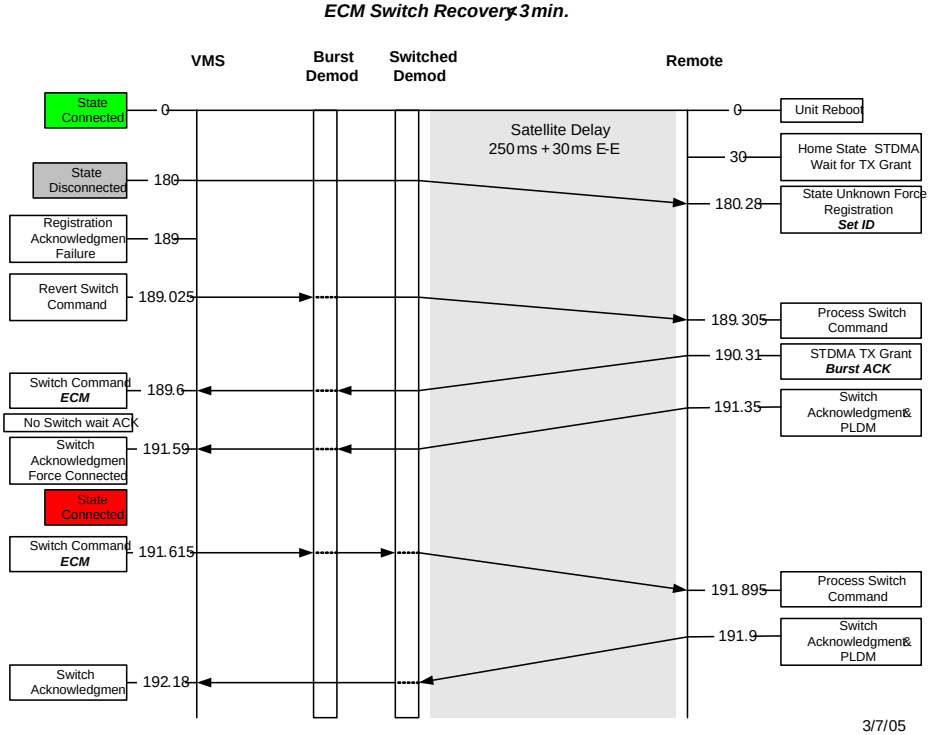


Figure G-1 ECM switch recovery < 3 minutes

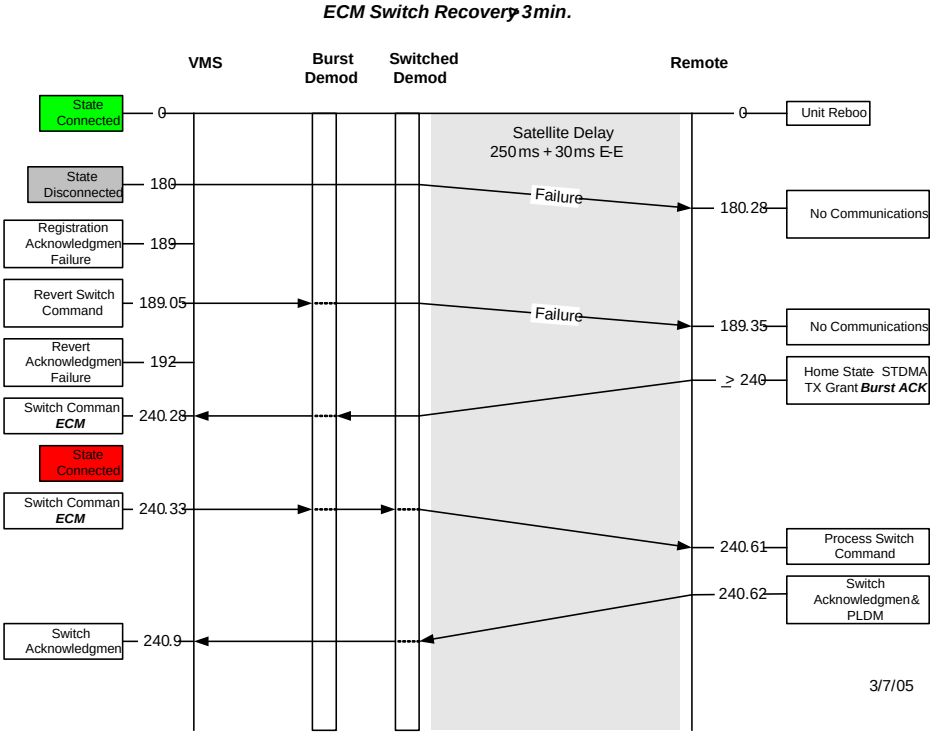


Figure G-2 ECM switch recovery > 3 minutes

Using Entry Channel mode

Entry Channel mode operates slightly differently from other VMS modes due to the STDMA burst controller losing the ability to automatically control once the CDM-570/570L or SLM-5650A is operating SCPC in ECM mode.

The following procedure illustrates this and demonstrates how to change the operation of a modem operating in SCPC ECM mode back to STDMA mode.

Figure G-3 shows the STDMA tab for the CDM-570/570L set up to run in Entry Channel mode. Once a switch has occurred in an ECM enabled VMS controlled modem the unit no longer sends switch requests so VMS does not have a switch request to respond to switch the VMS controlled modem back to STDMA from ECM mode.

The operator will have to manually intervene to switch the VMS controlled modem back to STDMA mode when the VMS controlled modem is no longer required to operate in ECM mode.

Note: Refer to the SLM-5650A modem manual for Entry Channel configuration setup. The text referenced within are similar between modems only the page layouts are different.

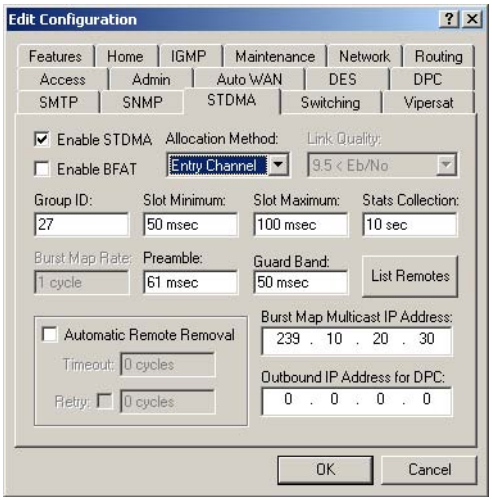


Figure G-3 STDMA tab with ECM mode, CDM-570/570L

Switching an ECM Remote from SCPC to STDMA

Use the following procedure to switch a remote operating in SCPC mode while in the ECM mode.

1. Click the **List Remotes** button on the **STDMA** tab shown in figure G-3 to display the pop-up **STDMA Remote List** shown in figure G-4.

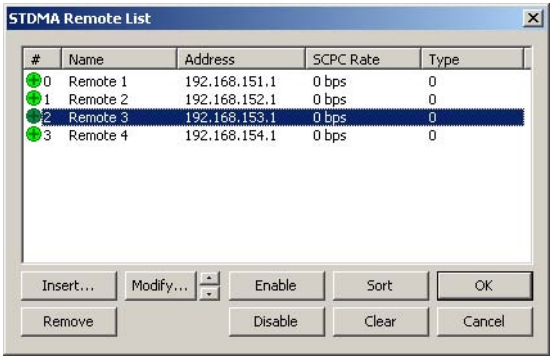


Figure G-4 STDMA remote list tab, CDM-570/570L

2. From the **STDMA Remote List**, select the CDM-570/570L you wish to switch from ECM mode running in SCPC to STDMA mode as shown in figure G-4.

3. Click the **Modify...** button to display the Remote Entry dialog shown in figure G-5. You can use the up and down arrows next to the button to change the selected remote.

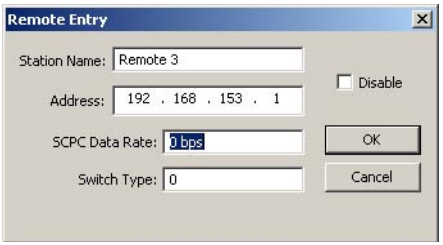


Figure G-5 Remote bandwidth entry, CDM-570/570L

4. To force a switch from ECM SCPC mode to STDMA mode, set the current value in the **SCPC Data Rate** dialog box to 0 (zero) as shown in figure G-5 then click the **OK** button.

NOTE

Note: This switch must be performed manually.

5. In VMS, right click on the remote from the drop-down menu shown in figure G-6 then click on the **Revert Uplink Carrier** command. This causes VMS to send the revert command to the target VMS controlled modem causing it to revert to its STDMA home state.

Figure G-6 Revert uplink carrier command, VMS controlled modem

This completes resetting the remote VMS controlled modem to operate in the STDMA mode.

APPENDIX

H

GLOSSARY

A

ACK A signal used in computing and other fields to indicate **ack**nowledgement, such as a packet message used in TCP to acknowledge the receipt of a packet.

ARP **A**ddress **R**esolution **P**rotocol – A protocol for a LAN device to determine the MAC address of a locally connected device given its IP address. See also MAC.

ASR **A**utomatic **S**witch **R**equest – A switch request message generated by older Vipersat modems (e.g., CDM-570/L) that is sent to the VMS to establish a new satellite link or adjust bandwidth between source and destination IP addresses.

B

Base Modem The main component in a satellite communications modem that consistes of a circuit board with the modem hardware and firmware and the associated interfaces.

BER **B**it **E**rror **R**ate (sometimes **R**atio) – A measure of the number of data bits received incorrectly compared to the total number of bits transmitted.

BPS **B**its **P**er **S**econd – A measure of transmission speed. See also Kb/s & Mb/s.

BPSK **B**inary **P**hase-**S**hift **K**eying – A digital modulation technique in which the carrier is phase shifted +/-180 degrees (two phases). The most robust of all PSKs, but unsuitable for high data-rate applications when bandwidth is limited due to encoding just one bit per symbol.

BUC **B**lock **U**p **C**onverter – An upconverter so called because it converts a whole band or "block" of frequencies to a higher band. The IF is converted to final transmit frequency for satellite communications. The BUC is part of the satellite ODU/transceiver.

C

C-Band A frequency band commonly used for satellite communications (and sometimes terrestrial microwave). For terrestrial earth stations, the receive frequency band is 3.7–4.2 GHz and the transmit band is 5.925–6.425 GHz. See also Ku-band.

CDD **C**omtech **D**ata **D**emodulator

CDM **C**omtech **D**ata **M**odem

CIR **C**ommitted **I**nformation **R**ate – The guaranteed minimum bandwidth assigned to a remote terminal.

CLI **C**ommand **L**ine **I**nterface – A mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks.

Codecast A network coding based ad hoc multicast protocol well-suited for multimedia applications with low-loss, low-latency constraints. Because data is streamed with no verification, high delivery ratios are obtained with very low overhead.

CRC **C**yclic **R**edundancy **C**heck – A method of applying a checksum to a block of data to determine if any errors occurred during transmission over communications links.

CXR Carrier – A radio frequency transmission linking points and over which information may be carried.

D

DAMA **D**emand **A**ssigned **M**ultiple **A**ccess – A process whereby communications links are only activated when there is an actual demand.

dBm **D**eci**b**el referenced to 1 **m**illiwatt.

DES **D**ata **E**ncryption **S**tandard – A federal standard method for encrypting information for secure transmission. The Vipersat system offers 3xDES (Triple DES) for encrypting traffic.

DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol – An Internet protocol for automating the configuration of computers that use TCP/IP.

DLL **D**ynamic **L**ink **L**ibrary – The implementation of the shared library concept in the Microsoft Windows system.

DPC **D**ynamic **P**ower **C**ontrol

DSCP **D**ifferentiated **S**ervices **C**ode **P**oint – The 6-bit field in an IP packet header that is used for packet classification purposes and is the portion of ToS that is detected by Vipersat modems.

DVB **D**igital **V**ideo **B**roadcast

DVP **D**igital **V**oice **P**rocessor – Used in packet voice applications.

E

E_b/N_o $\mathbf{E_b/N_o}$ is the ratio of $\mathbf{E_b}$ (energy per bit) and $\mathbf{N_o}$ (noise power density per Hz). The bit error rate (BER) for digital data is a decreasing function of this ratio. $\mathbf{E_b}$ is the energy of an information bit measured in Joules or, equivalently, in Watts per Hertz.

F

FAST Code **F**ully **A**ccessible **S**ystem **T**opology Code – Designation for feature code used by Comtech EF Data for their satellite modems. The FAST method makes it easy to quickly upgrade the feature options of a modem while it is running live in the network, either on site or remotely.

FEC **F**orward **E**rror **C**orrection – A process whereby data being transmitted over a communications link can have error correction bits added which may be used at the receiving end to determine/correct any transmission errors which may occur.

Flash Non-volatile computer memory that can be electrically erased and reprogrammed.

FTP **F**ile **T**ransfer **P**rotocol – An application for transferring computer files over the Internet. See also TFTP.

G

G.729 ITU standard for LD-CELP (**L**ow **D**elay – **C**ode **E**xcited **L**inear **P**rediction) voice encoding at 8 kb/s.

GIR **G**uaranteed **I**nformation **R**ate

Group ID A number assigned to equipment which defines it as a member of a group when addressed by the VMS burst controller.

GUI **G**raphical **U**ser **I**nterface – A form of graphical shell or user interface to a computer operating system or software application.

H

H.323 A protocol standard for multimedia communications designed to support real-time transfer of audio (such as voice over IP) and video data over packet networks. Quality of Service is a key feature of H.323. An alternative to SIP.

HDLC **H**igh **L**evel **D**ata **L**ink **C**ontrol – A standard defining how data may be transmitted down a synchronous serial link.

HPA **H**igh **P**ower **A**mplifier – The amplifier used in satellite communications to raise the transmit signal to the correct power level prior to transmission to satellite.

HTTP **H**yper **T**ext **T**ransfer **P**rotocol – The Internet standard for **W**orld **W**ide **W**eb (**WWW**) operation.

Hub The central site of a network which links to a number of satellite earth sites (remotes).

I

ICMP **I**nternet **C**ontrol **M**essage **P**rotocol

IDU **Id**oor **U**nit – In a VSAT system, the satellite modem is referred to as the IDU.

IF **I**ntermediate **F**requency – In satellite systems, IF frequencies are usually centered around 70 or 140 MHz (video/TV), or 1200 MHz (L-band).

IFL **I**ntra-**F**acility **L**ink – The coaxial cabling used to connect the satellite ODU to the IDU. Carries the inbound and the outbound signals, and the 24 VDC for the LNB.

Image A binary firmware file that provides the operational code for the processor(s) in a network unit.

IP **I**nternet **P**rotocol – A format for data packets used on networks accessing the Internet.

ISP **I**nternet **S**ervice **P**rovider – A company providing Internet access.

ITU **I**nternational **T**elecommunications **U**nion

K

Kb/s **K**ilo **b**its per **s**econd – 1000 bits/second. A measure of transmission speed. See also bps & Mb/s.

Ku-Band A frequency band used for satellite communications. For terrestrial earth stations the receive frequency band is in the range 10.95–12.75 GHz and the transmit frequency band is 13.75–14.5 GHz. See also C-band.

L

L-Band A frequency band commonly used as an IF for satellite systems using block up/down conversion. Typically 950–1450 MHz Rx, 1250–1750 MHz Tx.

LAN **L**ocal **A**rea **N**etwork

LLA **L**ow **L**atency **A**pplication

LNA **L**ow **N**oise **A**mplifier – An amplifier with very low noise temperature used as the first amplifier in the receive chain of a satellite system.

LNB **L**ow **N**oise **B**lock – A downconvertor so called because it converts a whole band or “block” of frequencies to a lower band. The LNB (similar to an LNA) is part of the satellite ODU/transceiver.

LNC **L**ow **N**oise **C**onverter – A combined low noise amplifier and block down converter, typically with an L-band IF.

LO **L**ocal **O**scillator – Component used in upconverters, downconverters, and transponders for frequency translation (heterodyne) of the carrier signal.

M

M&C	**M**onitor **& C**ontrol
MAC	**M**edia **A**ccess **C**ontrol – A protocol controlling access to the physical layer of an Ethernet network.
Mb/s	**M**ega **B**its per **S**econd – 1 Million bits/second. A measure of transmission speed. See also bps & kb/s.
Modem	**Mod**ulator and **Dem**odulator units combined.
Multicast	Transmitting a single message simultaneously to multiple destinations (group) on the IP network.
Multi-command	A command that allows multiple input choices in a single command execution..

N

NAT	**N**etwork **A**ddress **T**ranslation – An Internet standard that enables a LAN to use one set of IP addresses for internal (private) traffic and a second set of addresses for external (public) traffic.
NIC	**N**etwork **I**nterface **C**ontroller – The network interface for a PC/workstation that provides Ethernet connectivity. Depending on the computer, the NIC can either be built into the motherboard, or be an expansion card. Some computers (e.g., servers) have multiple NICs, each identified by a unique IP address.
NMS	**N**etwork **M**anagement **S**ystem
NOC	**N**etwork **O**peration **C**enter – Has access to any earth station installed using the VIPERSAT Management System (VMS). A NOC can remotely interrogate, control, and log network activities.
NP	**N**etwork **P**rocessor

O

ODU	**O**ut**d**oor **U**nit – In a VSAT system, the RF components (transceiver) are usually installed outdoors on the antenna structure itself and are thus referred to as an ODU. The ODU typically includes the BUC and LNB, and is connected to the IDU/modem by the IFL cabling.

P

PLDM **P**ath **L**oss **D**ata **M**essage – A packet message that is sent by older Vipersat modems (e.g., CDM-570/L) to the VMS every sixty seconds, providing status update and operating parameter information.

PSK **P**hase-**S**hift **K**eying – A digital modulation scheme that conveys data by changing the phase of a base reference signal, the carrier wave. Different PSKs are used, depending on the data rate required. Examples are binary phase-shift keying (BPSK or 2-PSK) which uses two phases, and quadrature phase-shift keying (QPSK) which uses four phases.

PSTN **P**ublic **S**witched **T**elephone **N**etwork – The world's public circuit-switched telephone network, digital and analog, and includes mobile as well as land-line voice and data communications.

Q

QAM **Q**uadrature **A**mplitude **M**odulation – A digital modulation technique in which the amplitude of two carrier waves is changed to represent the data signal. These two waves are 90 degrees out of phase with each other.

QoS **Q**uality **o**f **S**ervice

QPSK **Q**uadrature **P**hase-**S**hift **K**eying – A digital modulation technique in which the carrier is phase shifted +/- 90 or +/-180 degrees. With four phases, QPSK can encode two bits per symbol—twice the rate of BPSK. However, it also uses twice the power. Also known as 4-PSK or 4-QAM.

R

Remote Satellite earth site that links to a central network site (Hub).

RF **R**adio **F**requency – A generic term for signals at frequencies above those used for baseband or IF.

RFC **R**equest **F**or **C**omment – The official publication channel for Internet standards (such as communication protocols) issued by the Internet Engineering Task Force (IETF).

RIP **R**outing **I**nformation **P**rotocol

ROSS **R**oaming **O**ceanic **S**atellite **S**erver

RS-232 A common electrical/physical standard issued by the IEEE used for point to point serial communications up to approximately 115 kb/s.

RTP **R**eal-time **T**ransport **P**rotocol – A standardized packet format for delivering real-time applications such as audio and video over the Internet. Frequently used in streaming media systems, videoconferencing, and VoIP.

Rx **R**eceive

S

SCPC **S**ingle **C**hannel **P**er **C**arrier – A satellite communications technique where an individual channel is transmitted to the designated carrier frequency. Some applications use SCPC instead of burst transmissions because they require guaranteed, unrestricted bandwidth.

SIP **S**ession **I**nitiation **P**rotocol – A general purpose protocol for multimedia communications, commonly used for voice over IP (VoIP) signaling. An alternative to the H.323 protocol.

SNG **S**atellite **N**ews **G**athering – A satellite uplink van/truck with television crew on location conducting a live report for a newscast.

SNMP **S**imple **N**etwork **M**anagement **P**rotocol – A protocol defining how devices from different vendors may be managed using a common network management system.

SOTM **S**atcom **O**n-**T**he-**M**ove – The ability of a mobile remote terminal to roam across satellite beams to preserve link integrity and to automatically connect from one satellite and/or hub to another in a global network.

Star Topology A network topology which, if drawn as a logical representation, resembles a star with a hub at the center.

STDMA **S**elective **T**ime **D**ivision **M**ultiple **A**ccess – A multiple access technique where users time-share access to a common channel with variable-sized time slots allocated on usage.

Streamload Protocol A proprietary Vipersat data streaming protocol.

SUM **S**tatus **U**pdate **M**essage – A packet message that is sent by newer Vipersat modems (e.g., SLM-5650A) to the VMS every sixty seconds, providing status update and operating parameter information.

T

TCP/IP **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol – A standard for networking over unreliable transmission paths. See also UDP.

TDM **T**ime **D**ivision **M**ultiplexing – A method of multiplexing that provides the transmission of two or more signals on the same communication path or channel, but at different times by utilizing recurrent timeslots.

TFTP **T**rivial **F**ile **T**ransfer **P**rotocol – A simple file transfer protocol used over reliable transmission paths. See also FTP.

ToS **T**ype **o**f **S**ervice

Tx **T**ransmit.

U

UDP **U**ser **D**atagram **P**rotocol – A standard for networking over reliable transmission paths.

UDP multicast A multicast transmission using the UDP protocol.

Unicast Transmitting information/data packets to a single destination on the IP network.

V

VESP **V**ipersat **E**xternal **S**witching **P**rotocol – A switch-request protocol that allows external VPN equipment and Real-time proprietary applications to negotiate bandwidth requests between any two subnets on a Vipersat network. VESP is used by newer Vipersat modems (e.g., SLM-5650A) to send a switch request to the VMS to establish a new satellite link or adjust bandwidth for an existing link.

VCS **V**ipersat **C**ircuit **S**cheduler – A proprietary satellite communication scheduling system used to schedule Vipersat network resources in support of a variety of high-priority applications such as video conferencing and scheduled broadcasting.

VFS **V**ipersat **F**ile **S**treamer – A file transfer application utilizing UDP and a proprietary Streamload protocol to transmit data across the Vipersat network.

VLoad **V**ipersat **Load** Utility – A comprehensive tool for managing and distributing application, configuration, and identification information for the modem/routers in Vipersat satellite networks.

VMS **V**ipersat **M**anagement **S**ystem – A comprehensive M&C tool providing rapid and responsive control of Vipersat satellite networks. Comprised of client and server components.

VNO **V**irtual **N**etwork **O**perator – A provider of management services that does not own the telecommunication infrastructure. The Comtech Vipersat Network Products' VNO solution allows satellite space segment operators to selectively expose resources in their satellite network to other service providers, customers, or partners.

VoIP **V**oice **o**ver **IP –** The routing of voice communications over the Internet or through any IP-based network.

VOS **V**ipersat **O**bject **S**ervice – The main software service of the VMS application.

W

Wizard A specialized program which performs a specific function, such as installing an application.

WRED **W**eighted **R**andom **E**arly **D**etection – A queue management algorithm with congestion avoidance capabilities and packet classification (QoS) providing prioritization.

INDEX

T

U

V

W