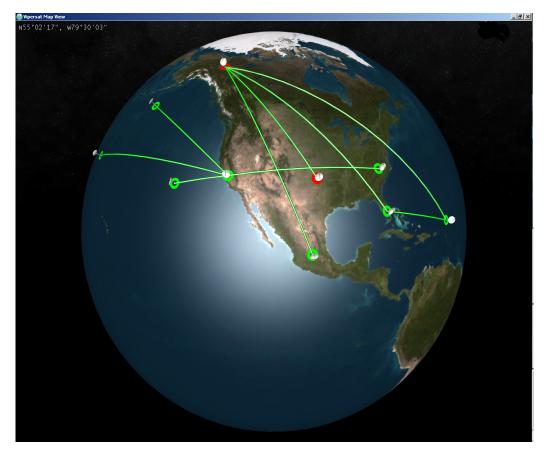


## VMS v3.6.x VIPERSAT Management System USER GUIDE



Part Number MN/22156 Revision 3

## VMS v3.6.x VIPERSAT Management System

## User Guide

Part Number MN/22156 Document Revision 3

Software version 3.6.x

August 30, 2008

#### 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: 3

Software Version: 3.6.x

©2008 by Comtech EF Data, Inc. All rights reserved. No part of this document may be copied or reproduced by any means without prior written permission of Comtech EF Data.

All products, names and services are trademarks or registered trademarks of their respective companies.

Comtech reserves the right to revise this publication at any time without obligation to provide notification of such revision. Comtech periodically revises and improves its products and therefore the information in this document is subject to change without prior notice. Comtech makes no warranty of any kind with regard to this material, including but limited to the implied warranties of merchantability and fitness for a particular purpose. No responsibility for any errors or omissions that may pertain to the material herein is assumed. Comtech makes no commitment to update nor to keep current the information contained in this document.

Printed in the United States of America

#### Document Revision History

Revision	Description
0	Initial Release. <i>Note</i> : This new document part number, MN/22156, supersedes the previous VMS User Guide part number, 22156.
1	<b>New functionality in v3.5.x:</b> VMS N:1 Redundancy; Site Distribution Lists; CDM-700 Out- of-Band Driver; CDD-564IF InBand Driver
2	New functionality in v3.6.0: VMS SOTM, VNO and Global Map View
3	<b>New functionality in v3.6.3:</b> 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.

{ This Page is Intentionally Blank }

#### Chapter 1 General

How to Use This Manual 1-1
Manual Organization
Chapter 1 — General
Chapter 2 — VMS Installation 1-1
Chapter 3 — VMS Configuration 1-2
Chapter 4 — Configuring Network
Modems
Chapter 5 — VMS Services
Chapter 6 — Out-of-Band Units 1-2
Appendix A — VMS Cross Banding 1-2 Appendix B — Antenna Visibility 1-2
Appendix B — Antenna Visibility 1-2
Appendix C — Redundancy 1-2
Appendix D — Domain Controller and
DNS
Appendix E — SNMP Traps 1-2
Appendix F — Automatic Switching 1-2
Appendix G — Entry Channel Mode
Switching
Appendix H — VMS Billing Log Translator
(VBLT)
Appendix I — Glossary
Conventions and References
Product Description 1-5
Introduction
VMS Features
VMS Operation
VMS Architecture
New in this Release
v3.6.3 Release
SLM-5650A Inband Device Driver 1-9
SLM-5650A Full MIB Out-Of-Band M&C 1-9
CDM-570/570L Full MIB OOB M&C 1-10
Satellite Advanced Switching (Remote
Roaming)
Generic VMS Installer
VNO Basic User Authorization 1-10
Antenna Mesh Compensation Factor . 1-10 ToS Value Control for Management
Messages
Customer Support
Contact Information 1-12

## Table of Contents

Return Material Authorization		1-12
Reader Comments / Corrections		1-12

#### Chapter 2 VMS Installation

General
Types of Installation
Upgrading Redundant Server Configuration 2-3
Preparing Server for VMS Installation 2-4
Limiting DEP (Data Execution Prevention) . 2-4
Enabling Global Catalog Caching (Redundant
Configurations)
Configuring Server as Domain Controller and/or
DNS
Backing Up VMS Database (Upgrade) 2-8
Stopping Previous VMS Version (Upgrade) 2-10 Uninstall Previous VMS Version (Upgrade) 2-11
VMS Server Installation
Setting Com Security for VMS
Verifying Successful Server Installation 2-27
VMS Client Installation
Creating Client Accounts
Verifying Successful Client Installation 2-37
ViperGlobe Install
Verifying ViperGlobe Installation 2-39
VNO Install
VNO Overview
Installation Procedure

#### Chapter 3 VMS Configuration

General
Hardware Configuration
VMS Network Configuration       3-5         VMS Initial Setup Procedure       3-5         Configure Server Connection       3-5         Activate the Server Processes       3-6         Configure Auto Activate       3-7

Configure Addresses and Assign ID 3-7
VMS Network Build Procedure 3-11
Subnet Manager Configuration 3-11
Setting the Alarm Masks
Enabling Auto Home State 3-13
Bandwidth Manager Configuration 3-14
Create Satellite(s)
Create Transponders 3-15
Create Antennas 3-17
Create Antenna Devices 3-18
InBand Manager Configuration 3-21
Pool Management
Network Manager Configuration and
ViperGlobe
Basic Guaranteed Bandwidth 3-37
CIR Configuration
Enable CIR on the Satellite 3-39
CIR Policy Setting
Enable CIR on Remote Antennas 3-41
Adjust Bandwidth Allocation 3-42
N:M Device Redundancy
VMS Redundancy
SOTM (Satellite On The Move) 3-44

#### Chapter 4 Configuring Network Modems

General					4-1
Hardware Configuration					. 4-3
Configuring a Network Modem					4-4

#### Chapter 5 VMS Services

General											5-1
ViperView—Monitor a	and	I C	Co	nt	ro	I					5-2
Multiple Views											. 5-2
Error Detection .											. 5-6
Event Log											. 5-9
Clear											5-11
Twelve Hour .											5-11
Filters											5-11
Filters Tab .											5-11
Dates Tab .											5-12
Export											5-13
Refresh											5-13
Alarm Masks											5-13
Viewing/Settin	ig A	٩la	arr	n	M	as	sk	s			5-14

Unlock Alarm Masks			5-15
VMS Service Managers			5-17
Vipersat Manager			
InBand Manager			
Policy Tab			
Bitrate Limits			
Application Policies			
Туре			
Maximum Bitrate			
Minimum Bitrate			
Distribution Lists Tab			
Subnet Manager			
Subnet Manager Configuration			
Open			
InBand Management			
Soft Reset			
Resize Uplink Carrier			
Revert Uplink Carrier			
Reset Uplink Carrier			
Delete			
Properties			
General Tab			
In Band tab			
Policy tab			
Distribution Lists Tab			
ViperView			

#### Chapter 6 Out-of-Band Units

General	. 6-1
Controlling Non-IP Modems	. 6-1
SNMP Manager	
Parameter View	. 6-5
Configuring the RF Chain	. 6-7
Switching SNMP Out of Band Modems	6-10
Overview	6-10
Out of Band Circuit Manager (OBCM)	
Configuring the OBCM	
Vipersat Circuit Scheduler	6-14

#### Appendix A VMS Cross Banding

Vipersat Cross Banding Solution . . . . . . A-3

#### Appendix B Antenna Visibility

General	B-1
Using Antenna Visibility	B-2
Example — Blocking Spectrum Affected	by
Local Ground Frequency Interference.	B-5

#### Appendix C Redundancy

General	C-1
VMS Redundancy	C-2
Description	.C-2
Redundant Hot-Standby	.C-2
Protection Switch-over	.C-3
Active to Standby Switch	.C-3
Active Server Role	
Standby Server Role	
Automatic VMS Activation	
Server Synchronization	
Automatic Synchronization	
Manual Synchronization	
Server Contention	
Server Status	.C-6
Installing & Configuring VMS Server	
Redundancy	
Enabled	
Auto Activate	
Redundant Servers	
Priority	
Failover Time	
Manual Switching	
Clearing Server Contention	C-12
N:M Hub Modem Redundancy	C-13
Description	C-13
Installing N:M Redundancy	C-15
Hub N:M Redundancy Requirements .	C-15
Sample installation.	
	C-19
Setting up N:M redundancy	C-19
Redundancy Manager	C-20
Create Container	C-20
Adding Strips and Groups	C-20
Power Strips	C-21
Redundancy Groups	C-22
Enabling Heartbeats	C-23
Roles	C-25

Backup Configurations
Storing Spare Configurations in the
Primary Units
Preparing the repaired/replacement unit C-30
Restoring the acting primary unit spare
configuration C-31
Cleaning up
How N:M Redundancy Works C-32
Device failure detection
The Switch-over Process C-32
Vipersat Manager C-32
Redundancy Manager
Putting a Failed Unit Back into Service C-33
Setting Unit to Parked Configuration Mode . C-34

#### Appendix D Domain Controller and DNS

Setup	. D-1
Configuring a Domain Controller and DNS	D-3
Configuring a Secondary Domain Controller . Setup	
Installing Secondary DNS Server	

#### Appendix E SNMP Traps

Introduction					E-1
Using SNMP Traps					. E-2
SNMP Traps Available in VM	S				. E-2
Configuring SNMP Traps					E-3
Insert					
Modify					. E-4
Remove					. E-5
Summary					E-6

#### Appendix F Automatic Switching

General				. F-1
Bandwidth /	Allocatior	n and Load	Switching	. F-2

Load switching F-2
Bandwidth Allocation and Load Switching by
the STDMA Controller:
Load Switching Process
Load Switching by a Remote
Determining Need-for-Change
Load Switch Example
(SCPC)
Application switching
Type of Service (ToS) switching F-15

#### Appendix G Entry Channel Mode Switching

Entry Channel Mode (ECM)	G-1
Fail Safe Operation	G-2
Using Entry Channel mode	G-4
Switching an ECM Remote from SCPC	to
STDMA	G-5

#### Appendix H VMS Billing Log Translator (VBLT)

Description							H-9
Installation							. H-9
Operation							. H-9
Console Mode.							H-10
Examples							H-10
GUI Mode							H-11
Operation							H-11
3.3 Scheduled Task Mode	е						H-13
Billing Log Format							H-16
Billing Log Examples							H-16

#### Appendix I Glossary

#### Index

|--|

## List of Figures

#### **Chapter 1 Figures**

Figure	1-1	VMS ViperView display 1-	-6
Figure	1-2	ViperView Client, Server (VOS)	
	Rela	ationship1-	-8

#### **Chapter 2 Figures**

Figure 2-1 Automatic Updates window,
Recommended Setting
Figure 2-2 System Properties menu 2-5
Figure 2-3 Advanced tab2-5
Figure 2-4 DEP tab
Figure 2-5 NTDS Site Settings 2-7
Figure 2-6 Backup Command, VMS Server 2-9
Figure 2-7 VMS Backup Save As dialog2-9
Figure 2-8 Windows Task Manager, Processes tak
2-10
Figure 2-9 Task Manager Warning dialog 2-11
Figure 2-10 Add or Remove Programs Control
Panel
Figure 2-11 VMS, Remove Program2-13
Figure 2-12 Setup Wizard Welcome screen 2-14
Figure 2-13 License Agreement screen 2-15
Figure 2-14 Installation Type screen2-16
Figure 2-15 Service Configuration dialog 2-16
Figure 2-16 Choose Components dialog 2-17
Figure 2-17 Choose Install Location dialog 2-18
Figure 2-18 Choose Start Menu Folder dialog 2-18
Figure 2-19 Software Installation notice 2-19
Figure 2-20 Install Cypto-Box Key prompt 2-20
Figure 2-21 Found New Hardware Wizard 2-20
Figure 2-22 Hardware Installation2-21
Figure 2-23 Hardware Installation Completed
screen2-21
Figure 2-24 Installation Complete dialog 2-22
Figure 2-25 Control Panel 2-23
Figure 2-26 Administrative Tools 2-23
Figure 2-27 Component Services, My Computer
Menu
Figure 2-28 Com Security, Edit Limits 2-24
Figure 2-29 Launch Permissions 2-25
Figure 2-30 Select Users
Figure 2-31 Launch Permissions with New User .

2-26

2-20	
Figure 2-32 2-27	Services, Administrative Tools menu
	Vipersat Management System Service
	Successful Installation VinerView2 28
	Successful Installation, ViperView2-28
	Client Install
	Admistrative Tools menu2-32
	Create Group
Figure 2-38	Create Group Dialog
Figure 2-39	Create User Dialog2-33
Figure 2-40	Setting the User Password2-34
	Client Properties2-34
	Select Group Dialog2-35
Figure 2-43	My Computer Properties 2-35
Figure 2-44	Edit Limits
Figure 2-45	Launch Permissions2-37
Figure 2-46	Connect dialog2-37
Figure 2-47	ViperView window, VMS Client 2-38
Figure 2-48	Vipersat Network Globe Setup2-38
	Vipersat Map View window 2-39
	VNO Deployment with Redundant
	Servers
Figure 2-51	VNO-WS Installer2-42

#### **Chapter 3 Figures**

Figure 3-1 Sample Network Configuration 3-2
Figure 3-2 CDM-570/570L Telnet Vipersat
Configuration
Figure 3-3 Connect dialog3-6
Figure 3-4 Server Processes, Manual Activation .
3-6
Figure 3-5 Activated Server Notification 3-6
Figure 3-6 Server Properties, Auto Activate 3-7
Figure 3-7 Vipersat Manager, General tab 3-8
Figure 3-8 Vipersat Manager, Timeouts tab 3-9
Figure 3-9 Vipersat Manager, Registration tab3-11
Figure 3-10 Mask Unlock Alarm setting3-13
Figure 3-11 Auto Home State Timeout setting 3-14
Figure 3-12 Create Satellite menu command . 3-15
Figure 3-13 Create Satellite dialog 3-15
Figure 3-14 Create Transponder menu command
3-16

Figure 3-15 Create Transponder dialog . . . . 3-16 Figure 3-17 Antenna Visibility, Default Settings ... 3-18 Figure 3-18 Create Up Converter dialog .... 3-19 Figure 3-19 Create Down Converter dialog . . 3-19 Figure 3-20 Converter Icons on Antenna View3-20 Figure 3-21 New Devices Added to Converters . . 3-21 Figure 3-22 BC Carrier Flag Setting, CDM-570/ Figure 3-23 BC Carrier Flag Setting, SLM-5650A 3-22 Figure 3-24 InBand Settings for Remotes ... 3-23 Figure 3-25 Select Switching Modulator. .... 3-23 Figure 3-27 Subnet Properties, General tab. . 3-24 Figure 3-28 Subnet Properties, InBand tab ... 3-25 Figure 3-30 Properties Distribution List tab ... 3-27 Figure 3-32 S.A.S. tab with SOTM Enabled . . 3-28 Figure 3-33 Satellite Open menu command. . 3-29 Figure 3-37 Resize Uplink Carrier, Subnet. . . 3-31 Figure 3-38 Switched Carrier (Spectrum View)3-31 Figure 3-39 Switched Carrier (Subnet View) . 3-31 Figure 3-40 Switched Carrier (Hub Antenna View) 3-32 Figure 3-41 Vipersat Network, Global Map View . 3-33 Figure 3-43 Drag and Drop Satellite(s). . . . . 3-34 Figure 3-44 Globe View with Network Icon ... 3-35 Figure 3-45 Adding Sites, Network Manager and Figure 3-46 Map View with Linked Sites .... 3-37 Figure 3-47 Visualization of Basic Guaranteed Figure 3-48 CIR Enabled Command .....3-39 Figure 3-51 CIR Commands, Remote Antenna . . 3-41 

tion for SOTM
or SOTM .3-46
y, CDM-570/
tion, CDM-570/

#### **Chapter 4 Figures**

Figure 4-1	Modem E	Equipn	nent [	Drop-	Dow	vn Mer	าน,
Vipe	erView						.4-2

#### **Chapter 5 Figures**

Figure 5-1 Synchronize Command
Figure 5-2 ViperView, Multiple Window Views . 5-3
Figure 5-3 Subnet Manager View5-3
Figure 5-4 Antenna View
Figure 5-5 Event View
Figure 5-6 Spectrum View5-5
Figure 5-7 Parameter View
Figure 5-8 Unit Command Menu5-6
Figure 5-9 ViperView, Subnet Manager5-7
Figure 5-10 Drop-down menu
Figure 5-11 Modulator Properities dialog5-8
Figure 5-12 Modem tab, CDM modulator and
Demodulator only
Figure 5-13 Event Log View5-10
Figure 5-14 Event View Menu5-10
Figure 5-15 Event Log View, Filters tab5-11
Figure 5-16 Event Log Filter Selection 5-12
Figure 5-17 Event Log Dates tab5-13
Figure 5-18 Demodulator Alarm Masks5-14
Figure 5-19 Modulator Alarm Masks5-14
Figure 5-20 Mask Unlock Alarm Flag5-16
Figure 5-21 Server View
Figure 5-22 Vipersat Manager Network View . 5-18
Figure 5-23 InBand Manager Properties Command
5-19
Figure 5-24 InBand Manager, Policy tab5-19
Figure 5-25 Application Policy dialog5-21
Figure 5-26 Revised Policy Tab5-22
Figure 5-27 Remove Application Policy dialog5-22
Figure 5-28 InBand Manager, Distribution Lists tab
5-23 Figure 5-20, Distribution Lists, Insert Command
Figure 5-29 Distribution Lists, Insert Command

#### 5-23

3-23	
Figure 5-30 Distribution List Window 5-	
Figure 5-31 Add Site Dialog, Search Network 5-	
Figure 5-32 Add Site Dialog, Select Subnet 5-	
Figure 5-33 Distribution List Window, Configure	d
5-25	
Figure 5-34 Distribution List Created5-	-25
Figure 5-35 Subnet Manager	-26
Figure 5-36 Separate window5-	-27
Figure 5-37 Subnet Manager5	-27
Figure 5-38 Subnet Manager configuration 5-	-28
Figure 5-39 Subnet Mananger open command	
window5-	-29
Figure 5-40 Select modem dialog 5-	
Figure 5-41 Disable in-band extension warning	
5-30	
Figure 5-42 Resize uplink dialog5-	-30
Figure 5-43 Uplink Modem Extra dialog 5-	
Figure 5-44 Revert uplink carrier dialog 5	
Figure 5-45 Reset uplink warning5	
Figure 5-46 Properties general tab5-	
Figure 5-47 New subnet dialog	
Figure 5-48 In Band Tab, Subnet Properties . 5-	
Figure 5-49 Modem Extra dialog5	
Figure 5-50 Modify, Modem Extra5-	
Figure 5-51 Select Modem dialog5-	
Figure 5-52 Select demodulator dialog 5-	
Figure 5-53 Policy Tab, Subnet5-	
Figure 5-54 Distribution Lists Tab, Subnet 5-	
Figure 5-55 Distribution List Enabled for Site	
Modification	-38
Figure 5-56 Modify Site List5-	
Figure 5-57 Distribution List Window, Site	
Modification	-39
Figure 5-58 ViperView top view5-	-40
<b>G F F F F F F F F F F</b>	

#### Chapter 6 Figures

Figure 6-1	SNMP Modem Manager 6-2
Figure 6-2	Declaring a CDM-600L 6-3
Figure 6-3	CDM-600L IP address dialog6-3
Figure 6-4	New SNMP modem dialog6-4
Figure 6-5	CDM-600L properties screen 6-4
Figure 6-6	SNMP Modem Manager 6-5
Figure 6-7	Parameter View6-6
Figure 6-8	Configuring the RF Chain6-7
Figure 6-9	Out of Band Antenna Tab 6-8
Figure 6-10	O Selecting the Out of Band Modem 6-8

Figure 6-11	Out of Band Dialog Box6-9
Figure 6-12	Sample Overlay Network6-10
Figure 6-13	Out of Band Circuit Manager6-11
Figure 6-14	Channel Configuration 6-11
Figure 6-15	Setting up an OBVM Circuit6-12
Figure 6-16	
Figure 6-17	
Figure 6-18	

#### Appendix A Figures

Figure A-1 Cross Banded Transponders, C-band	&
Ku-band	-2
Figure A-2 A Cross Banded Satellite Network A-	.3
Figure A-3 VMS Cross Banded Network	
Configuration A-	4
Figure A-4 VMS Cross Banded Network Solution	
A-5	
Figure A-5 Transponder dialog, C to Ku A-	6
Figure A-6 Transponder dialog, Ku to C $\ldots$ A-	6

#### Appendix B Figures

0	B-2	Antenna Properties, Visibility Tab. Ku-band Visibility Ranges, Center/ dwidth	
Figure		Ku-band Visibility Ranges, Base/To	
Figure	B-4	Frequency Range dialogs	B-4
Figure	B-5	Merging Visibility Ranges	B-4
Figure	B-6	VMS Bandwidth Pool with Ground	
•	Inte	rference	B-5
Figure	B-7	Transmit Carriers, No Visibility Bloc	к.
-	B-5	-	
Figure	B-8	Visibility Subtract dialog	B-6
Figure	B-9	Visibility Ranges with Blocks	B-6
Figure	B-10	) Transmit Carriers Repositioned,	
-	Visil	bility Block	B-7

#### Appendix C Figures

Figure C-1 Active an	d Standby VMS Servers, N:1
Redundancy.	C-2
Figure C-2 Server S	tatus Pop-Up C-6
Figure C-3 ViperView	w, VMS Server Drop-down
Menu	C-7

Figure C-4 VMS Server Properties, General Tab. C-8 Figure C-5 VMS Server Properties, Traps Tab ... C-10 Figure C-6 Activate Command, VMS Server Menu C-11 Figure C-7 Synchronize Command, VMS Server Figure C-8 N:M redundancy logic diagram. . . C-14 Figure C-10 Typical N:M redundant installation . . C-18 Figure C-11 N:M Redundancy Hierarchy . . . . C-19 Figure C-12 Redunancy Manager Tree . . . . C-19 Figure C-13 Redundancy Manager Drop-Down Figure C-14 Create Container dialog. . . . . . C-20 Figure C-15 Group drop-down menu . . . . . . C-21 Figure C-16 Group drop-down menu. . . . . . C-21 Figure C-17 New power strip dialog .....C-22 Figure C-18 Drag-and-drop populating power strip C-22 Figure C-20 Dragging port to group sub-container C-23 Figure C-21 Enable hearbeat in VMS, left window CDM-570/570L, right window SLM-5650A C-24 Figure C-22 Enabling heatbeat in CDM-570/570L Figure C-23 Enabling HeartBeat in SLM-5650A Figure C-25 Configuration backup. . . . . . . . C-26 Figure C-27 New configuration dialog ..... C-28 Figure C-28 Creating a backup configuration file. C-28 Figure C-30 Importing file.....C-30 Figure C-32 Restoring configuration. . . . . . . C-31 Figure C-33 Feature configuration page, CDM-570/ 570L.....C-35 Figure C-34 Administration page, CDM-570/570L C-35 Figure C-35 Ethernet Interface page, CDM-570/ 570L.....C-36 Figure C-36 Vipersat configuration page,

#### **Appendix D Figures**

Figure D-1 Manage your server dialog . . . . . D-4 Figure D-2 Preliminary steps ..... D-5 Figure D-3 Configuration options ..... D-5 Figure D-4 Server role dialog ..... D-6 Figure D-5 Summary of selections dialog .... D-6 Figure D-6 Active directory installation wizard D-7 Figure D-7 Active directory installation wizard D-7 Figure D-8 Domain controller type dialog . . . . D-8 Figure D-9 Create new domain dialog ..... D-8 Figure D-10 New domain name dialog . . . . . D-9 Figure D-11 NetBIOS domain name..... D-9 Figure D-12 Database and log folders dialog D-10 Figure D-13 Shared system volume dialog. . D-10 Figure D-14 DNS registration diagnostics screen. D-11 Figure D-15 Permissions dialog ..... D-12 Figure D-16 Administrator password ..... D-12 Figure D-17 Summary screen. . . . . . . D-13 Figure D-18 Configuring primary domain controller D-13 Figure D-19 Complete installation screen. . . D-14 Figure D-20 Restart screen ..... D-14 Figure D-21 Manage your server dialog . . . D-16 Figure D-22 Preliminary steps ..... D-17 Figure D-23 Network detection wait screen . D-17 Figure D-24 Configuration options ..... D-18 Figure D-25 Server role dialog ..... D-18 Figure D-26 Summary of selections dialog. D-19 Figure D-27 Active directory installation wizard start D-19 Figure D-28 Active directory installation wizard ... D-20 Figure D-29 Domain controller type dialog . . D-20 Figure D-30 Network credentials ..... D-21 Figure D-31 Additional domain controller . . . D-21 Figure D-32 Browse for domain list ..... D-22

VMS User Guide

		Additional domain controller with
		n name
Figure D-3	34 I	Directory and log folders dialog .D-23
Figure D-3	35 \$	Shared system volumeD-23
Figure D-3	36 I	Directory services restore mode
ad	min	istrative passwordD-24
Figure D-	37 \$	Summary screenD-24
Figure D-3	38 /	Active directory installation wizard
SC	reer	n
Figure D-3	39 I	Domain Controller confirmation screen
D-	25	
Figure D-	40 I	Restart screenD-25
Figure D-	41	D-26
Figure D-	42	Manage your server dialog D-27
Figure D-4	43 I	Preliminary steps screenD-28
Figure D-	44	DNS server role dialogD-29
Figure D-	45 I	DNS Selection summaryD-29
Figure D-		Insert disk promptD-30
Figure D-	47	Configuring components status .D-30
Figure D-	48 I	DNS server wizard welcome screen.
D-	31	
Figure D-4	49 3	Select configuration action D-31
Figure D-	50 I	Primary server locationD-32
Figure D-	51 2	zone name dialogrD-32
Figure D-	52 I	Dynamic update dialogD-33
Figure D-	53 I	Forwarders
Figure D-	54	Completing the configure a DNS
		wizard
Figure D-	55 (	Completion screen
Figure D-	56 I	DNS error messageD-35

#### Appendix E Figures

Figure E-1	Server drop-down menuE-3
Figure E-2	Properties general tabE-3
Figure E-3	Server traps tabE-4
Figure E-4	Trap desitination

#### Appendix F Figures

Figure F-1 Hub switching menu, CDM-570/570L . F-5	
Figure F-2 Hub Load switching menu, SLM-56504 F-6	١
Figure F-3 Switching menu for a remote, CDM-570 570L	
Figure F-4 Load switching menu for remote, SLM-5650AF-8	3
Figure F-5 Example load switching diagramF-10 Figure F-6 Application switching diagram,	)
CDM-570/570LF-13	3

#### Appendix G Figures

Figure G-1 ECM switch recovery < 3 minutes	
Figure G-2 ECM switch recovery > 3 minutes	
Figure G-3 STDMA tab with ECM mode, CDM-	570/
570L	G-5
Figure G-4 STDMA remote list tab, CDM-570/5	570L
G-5	
Figure G-5 Remote bandwidth entry, CDM-570	)/
570L	G-6
Figure G-6 Revert uplink carrier command, VM	1S
controlled modem	G-6

#### Appendix H Figures

Figure H-1	VLBT graphic user interface H-12
Figure H-2	Scheduled tasks H-13
Figure H-3	Scheduled task wizard H-14
Figure H-4	VLBT task tab H-14

{ This Page is Intentionally Blank }

## List of Tables

#### **Chapter 4 Tables**

 Table 4-1 CDM-570/570L Modem/Router Manual

 Connection Options
 4-4

#### Chapter 5 Tables

Table 5-2 Alarm Masking in a Typical Network 5-15

{ This Page is Intentionally Blank }

#### **C H A P T E R**

## 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 — Out-of-Band 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 — VMS Billing Log Translator (VBLT)

Covers how to install and operate VBLT, an application that converts switch events into billing log format.

#### Appendix I — 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)

#### How to Use This Manual

- *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 Web Service ICD* (Document Number, ICD- VNO-WS)

#### Introduction

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

VMS receives, stores, and processes this data from the network's VMS controlled modems and uses the data to update and display current network status information. The network data is then displayed by 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.

VMS is customized at setup for each satellite network it controls recognizing the unique bandwidth resources and limitations available for each network. 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 VMS receives a switching request from a network VMS controlled 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 VMS controlled 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 VMS controlled modem will not make the switch until the necessary network resources become available.

The satellite network's VMS controlled modems detect, monitor and, when commanded by VMS, physically make network changes. The VMS collects, analyzes, and displays data, and commands the VMS controlled modems to make network changes. Refer to each VMS controlled modem's *User's 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.

A sample display, shown in figure 1-1, shows VMS **ViperView** display giving the operator a complete view of a network's configuration, the health of all network components, and current bandwidth usage. The VMS display is flexi-

#### Product Description

ble and can be modified by the operator at any time, as described in this *User's Guide*, to optimize network Management and Control.

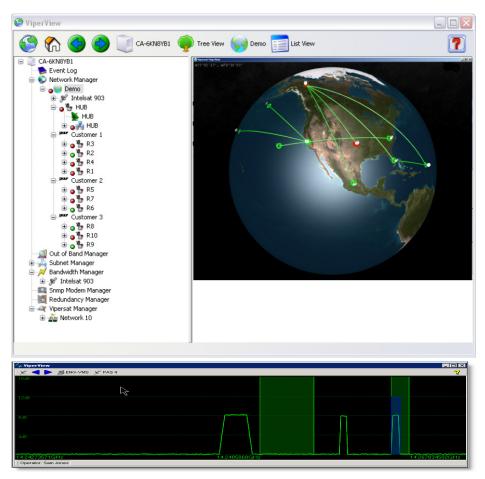


Figure 1-1 VMS ViperView display

Vipersat uses IP connections between network nodes, supporting UDP connectivity. The Vipersat VMS controlled modem, consisting 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.

VMS has a client/server architecture, as shown in diagram 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 VMS running on the central server, and the results are available to all clients across the network.

Through its client/server architecture, VMS supports centralized management, control, and distribution of data, alarms, and events. 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:

- Configuration Setup
- Network Status Displays (automatic and manual)
- Statistics Gathering (automatic and manual)
- Diagnostics Monitor and Control (automatic and manual)
- Dynamic Bandwidth Management
- Alarm Processing
- Optional VMS and Critical Hardware Redundancy
- Report Generation
- Network Administrator Mode
- Remote Access Capability via Local LAN or Internet/Intranet

#### **VMS** Operation

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

#### VMS Architecture

The VMS **Client** (ViperView) and **Server** (Vipersat Operating System) architecture figure 1-2 supports centralized management, control, and distribution of data, alarms, and events. Network units, such as a Vipersat VMS controlled modem while functioning as a modulator/demodulator, also detects, analyzes and reports to VMS details on network operation. VMS collects, stores,

#### **Product Description**

analyzes and acts on this information to intelligently control network operation to optimize bandwidth utilization and overall network performance.

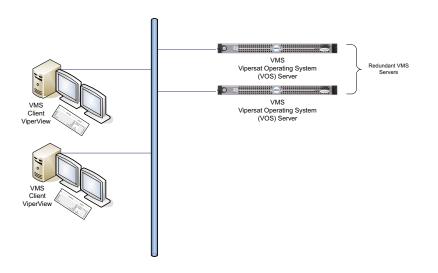


Figure 1-2 ViperView Client, Server (VOS) Relationship

The VMS management and monitoring system uses an intuitive graphic display, as illustrated in figure 1-1. 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 retrieves information from the VMS single, central server's database.

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

- System configuration
- Transmission configurations
- Satellite link Status
- QoS displayed as  $E_b N_o$  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 doubleclick 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 outstanding alarm condition of the network component or its sub-components:

- Green = online
- **Red** = alarm
- **Gray** = offline as the result of missing three consecutively PLDMs and not responding to the recovery process

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

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

#### New in this Release

#### v3.6.3 Release

#### SLM-5650A Inband Device Driver

This version now supports monitoring control and switching for SLM-5650A with Network Processor (NP) board. The Inband driver provides for full switching functionality backup and restore of hub device redundancy.

#### SLM-5650A Full MIB Out-Of-Band M&C

In addition to controlling the SLM-5650A as an inband device optioned with the Network Processor the base modem without the Network Processor will operate as manage OOB circuit controlled link.

#### CDM-570/570L Full MIB OOB M&C

The CDM-570/570L is supported as an OOB device operating without IP option card. This new device driver provides the monitoring and control of standard base modem control within and IP overlay network through SNMP.

#### Satellite Advanced Switching (Remote Roaming)

This new remote roaming feature provides advanced switching per remote to any given satellite. The advanced carrier switching from beam-to-beam in roaming applications allows for variable carrier characteristics between satellites per remote, whereby roaming from one satellite to another with different specifications, e.g. modulation, FEC Rate...

#### Generic VMS Installer

Changed installation authorization to remove serial number check. During the build authorization of VMS installation the packaging generation will not require serialization providing generic distributed install builds. Only key file updates (.vku) will be required to install latest versions of VMS as new or updates. Latest build versions will display on both Server and Client About Menus. This simplifies the distribution of release versions of VMS.

#### **VNO Basic User Authorization**

Supported in this release, the VNO server supports a new feature called Basic User Authentication. This feature provides a simple form of user access control to VNO resources and a limited set of privilege levels for specific VNO operations. It allows network operators to configure their VNO interface to expose a subset of all the networks on a per user basis. Users, passwords, and privilege levels are stored in VNO WS service.

#### Antenna Mesh Compensation Factor

This feature applies a power delta between any mesh remote sites. The hub is used as the reference value when calculating a power delta value between remote's with smaller antennas. This is accomplished through comparing its gain opposed to the gain differences between remotes. If multiple remotes are involved in a SHOD connection the VMS uses the lowest remote gain value for compensation control.

#### **ToS Value Control for Management Messages**

The management control messages can be stamped with a Type of Service (ToS) value providing for priority singling control through network routers. This priority control value increases reliability of management messages.

#### SLM-5650A Demodulator Only Support

The SLM-5650A optioned through FAST Codes produces a new device structure that masks all modulator functions. This new product is supported in this release by reading feature sets from the device providing for demodulator only.

#### **Contact Information**

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

Mail:	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 Vipersat 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 Vipersat Customer Support.
- 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.

#### **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.

#### СНАРТЕК

# 2

### VMS INSTALLATION

#### General

The Vipersat Management System software should be installed on a highperformance, industry-standard computer running the Microsoft Windows Server 2003 or later operating system.

For specifications for the minimum recommended VMS hardware configuration, 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:** The Automatic Updates function in Microsoft Windows must be properly set to avoid possible disruption of the VMS and the Vipersat network. Please see 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.

Automatic Updates 🛛 🗙		
Automatic Updates		
Help protect your PC		
Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.) How does Automatic Updates work?		
C Automatic (recommended)		
Automatically download recommended updates for my computer and install them:		
Every day 💌 at 3:00 AM 💌		
C Download updates for me, but let me choose when to install them.		
C Iurn off Automatic Updates.		
Your computer will be more vulnerable unless you install updates regularly. Install updates from the Windows Update Web site.		
Offer updates again that I've previously hidden		
OK Cancel Apply		

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 Operating System (VOS).
- **2.** On two or more (N:1) VMS servers in the optional fault-tolerant, redundant configuration; Vipersat Operating System (VOS).
- **3.** On a client workstation; Viperview User Interface.

Each of the first two configurations can be made as a:

- Clean Installation A clean installation is one done on a server that has not previously operated as a VMS server, or that has had its hard drive reformatted. With no existing network database, a full network configuration (Chapter 3, "VMS Configuration") must be performed following installation.
- Upgrade Installation An installation to be made on a server that has previously been installed as a VMS server in a Vipersat network, operating with a previous version of VMS. The existing network database will be automatically converted during installation, with minimal configuration changes required.

#### **Upgrading Redundant Server Configuration**

Perform the upgrade on the Standby server first. This will allow the installation of the new software and database conversion 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 deactive 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.

#### Preparing Server for VMS Installation

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.

#### Limiting 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.

System Properties	? ×
······	Automatic Updates Remote computer Name Hardware
Reference de la compacticación	System: Microsoft Windows Server 2003 Standard Edition Service Pack 1 Registered to:
	Negistered to: Viperlab2 Comtech Vipersat Networks Inc 69712-DEM-4211904-02010
	I by: Dell Server PE850 Intel(R) Pentium(R) D CPU 3.00GHz 3.00 GHz, 1.00 GB of RAM Physical Address Extension
	Support Information

Figure 2-2 System Properties menu

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

System Properties		? ×
General Advanced	Computer Name	Hardware   Remote
You must be logged	on as an Administrator to make mos	st of these changes.
	essor scheduling, memory usage, ar	nd virtual memory
		Settings
User Profiles		
Desktop settings re	lated to your logon	
		Settings
Startup and Recov	ery	
System startup, sys	tem failure, and debugging informati	ion
		Settings
	Enviro <u>n</u> ment Variables E	ror Reporting
-	OK Car	ncel <u>Apply</u>

Figure 2-3 Advanced tab

#### Preparing Server for VMS Installation

**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.

Performance Options	? ×
Visual Effects Advanced Data Execution Prevention	
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?	
$\textcircled{\begin{tabular}{ll} \bullet \\ only \end{tabular}}$ Turn on DEP for essential Windows programs and services only	
C Turn on DEP for all programs and services except those I select:	
	-
Add Remove	
OK Cancel App	ly

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.

## Enabling 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.

NTDS Site Settings Properties			? ×
Site Settings Object Security			1
NTDS Site Settin	gs		
Description:			
Change Schedule			
Inter-Site Topology Generator			
Server: VIPERLABBA	K		
Sit <u>e</u> : Default-First-Si	ite-Name		
Universal Group Membership	-	ching	
<u>R</u> efresh cache from:	Default-f	First-Site-Name	<b>_</b>
	OK	Cancel	Apply

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 switchover, 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.

## Configuring Server as Domain Controller and/or DNS



**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.

## Backing 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:** This database backup can only be restored on the current VMS version. It is not compatible with the new VMS version because a database conversion is performed during the installation process.

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

A successful installation of the new VMS will result in an automatic conversion of the current 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).

ViperView		1 뗽 Tree View 📄 List Vi	ew
UIPERLAB1	Open	Event Log	-
> Event Log ⊕S Network Manager Out of Band Manager	Backup Restore	Network Manager	
<ul> <li>⊕ Subnet Manager</li> <li>⊕ Ø Bandwidth Manager</li> <li>⊕ Ø Snmp Modem Manager</li> </ul>	Synchronize Deactivate	InBand Manager	
🕀 🔣 Redundancy Manager	Licensing	Out of Band Manager	
····· <b>*</b> Out of Band Circuit Mar ⊕ -≪ Vipersat Manager	Properties	Subnet Manager	Status connect
		Bandwidth Manager	
		Snmp Modem Manager	
		Redundancy Manager	
		Out of Band Circuit Manager	

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).

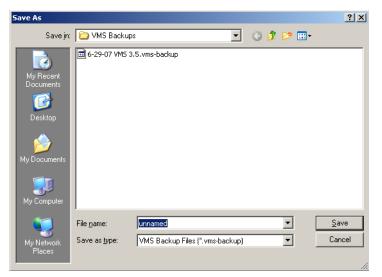


Figure 2-7 VMS Backup Save As dialog

# Stopping Previous VMS Version (Upgrade)

If you are installing VMS on a server which does not have a previous version of VMS installed, skip this "Stopping Previous VMS Version (Upgrade)" section and proceed with the instructions in 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 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.

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

- 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.

📕 Windows Task Mana	iger			- 🗆 🗵
<u>File Options View Hel</u>	p			
Applications Processes	Performance Netw	orking	Users	
Image Name	User Name	CPU	Mem Usage	
svchost.exe	SYSTEM	00	3,080 K	
svchost.exe svchost.exe	NETWORK SERVICE	00	4,160 K	
svchost.exe	LOCAL SERVICE	00 00	5,088 K	
svchost.exe			5,852 K	
svchost.exe	SYSTEM SYSTEM	00 00	28,724 K	
svchost.exe		00	2,196 K	
svchost.exe	SYSTEM	00	1,976 K 6,352 K	
svchost.exe	SYSTEM	00	6,352 K 4,592 K	
System	SYSTEM	00	4,592 K 244 K	
System Idle Process	SYSTEM	99	244 K 28 K	
taskmgr.exe		99	4.312 K	
TscHelp.exe	Administrator	00	2,828 K	
	Administrator	00	4,308 K	
	Administrator	00	13,524 K	
VOS.exe	Vms	00	11,440 K	
winlogon.exe	SYSTEM	00	6,264 K	
winvnc4.exe	SYSTEM	00	3,360 K	
wmiprvse.exe	SYSTEM	00	5,136 K	<b>_</b>
1 mile rooroxo		00	0,100 K	
Show processes fro	om all users		End Proce	ess
Processes: 36 CPU Us	sage: 0% Con	nmit Cha	arge: 211M / 2	:394M

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.

	📕 Windows	Task Mana	iger				<u>_     ×</u>
	<u>File</u> Options	⊻iew <u>H</u> el	p				
	Applications	Processes	Performan	nce Netw	orking	Users	
	Image N		User Name		CPU	Mem Usage	
	svchost.	exe	SYSTEM	CEDUICE	00	3,080 K	
Task Manager Warning			×	6ERVICE	00	4,160 K	
				VICE	00 00	5,088 K	
WARNING: Term	inating a proces	s can cause i	undesired	VICE	00	5,844 K 25,932 K	
results including					00	25,932 K 2,196 K	
process will not b				VICE	00	2,190 K 1,976 K	
data before it is		e you sure yo	iu want to	PICE	00	6,352 K	
terminate the pr	ocess?				00	4,600 K	
					00	244 K	
Yes	s No 00 28 /						
				br	00	2,188 K	
	TscHelp.	exe	Administra	tor	00	2,828 K	
	VConMg	r.exe	Administral	tor	00	4,308 K	
	vipervier		Administral	tor	00	13,524 K	
	VOS.exe	•	vms		00	11,432 K	
	winlogor	n.exe	SYSTEM		00	6,256 K	
	winvnc4	.exe	SYSTEM		00	3,360 K	
	wmiprvs	e.exe	SYSTEM		00	5,136 K	-
	🔽 Show	processes fro	om all users			End Proce	:55
	Processes: 36	CPU Us	age: 1%	Com	nmit Cha	arge: 210M / 2	394M //

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.

#### Preparing Server for VMS Installation



Figure 2-10 Add or Remove Programs Control Panel

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

### Preparing Server for VMS Installation

🐞 Add or Rem	ove Programs		
5	Currently installed programs and updates:	Sort by: Name	•
C <u>h</u> ange or Remove Programs	R Microsoft .NET Framework 2.0 Click here for support information.	Size Used Last Used On	88.50MB ▲ rarely 5/8/2007
Add <u>N</u> ew Programs	To change this program or remove it from your computer, click Change/Remove.	Chang	je/Remove
	闘 Microsoft .NET Framework 3.0	Size	57.73MB
<b>1</b>	BXML 6.0 Parser (KB927977)	Size	1.30MB
Add/Remove	Notepad++	Size	2.51MB
<u>W</u> indows Components	📸 Security Update for Windows Media Player 6.4 (KB925398)	Installed On	2/7/2007
	SnagIt 8	Size	20.21MB
	🛞 Vipersat Management System 🔫	Size	33.35MB
	WNC Free Edition 4.1.2	Size	1.27MB
	🥖 Windows Internet Explorer 7	Size	2.50MB
	🔗 Windows Internet Explorer 7 - Software Updates		
	🏉 Security Update for Windows Internet Explorer 7 (KB928090)	Installed On	3/8/2007
	🥖 Security Update for Windows Internet Explorer 7 (KB931768)	Installed On	5/8/2007
	🏉 Security Update for Windows Internet Explorer 7 (KB933566)	Installed On	6/25/2007
	🎥 Windows Server 2003 - Software Updates		
	🎥 Update for Windows Server 2003 (KB931836)	Installed On	3/8/2007
	🚵 Sacuvitu Hadata far Windows Sarvar 2002 (KD021704)	* • • • •	

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

- 1. Locate the file VMS 3.x Install.exe on the VMS distribution CD and doubleclick 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.** From the **Installation Type** screen shown in figure 2-14, select the radio button for the type of installation you will be making. The VMS software is comprised of two main components, the Server component and the Client component.
  - **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.

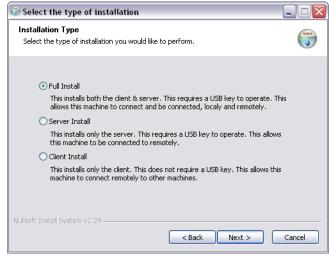


Figure 2-14 Installation Type screen

- 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.

Configure as Service     Configure as Service     Service Account     Enter service account, leas     field blank to use a local se     Username     VM5     Domain	
Password ••••••• Re-enter password •••••••	

Figure 2-15 Service Configuration dialog

7. Enter the User name for the account (e.g., VMS).

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, <u>vipersat</u>. 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.

Choose Components Choose which features of Vipe	rsat Management System you wa	nt to install.
	ant to install and uncheck the comp	oonents you don't want to
install. Click Next to continue.		
Select components to install:	System Network InBand Manager Subnet Manager Bandwidth Manager Snmp Modern Manager	Description Position your mouse over a component to see its description.
Space required: 21.9MB	Device Redundancy	
Julisoft Install System v2.29 —		

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 be interrupted with the notice shown in figure 2-19. Click on the **Continue Anyway** button to continue.



Figure 2-19 Software Installation notice

**16.** During installation, the **Waiting** dialog shown in figure 2-20 asking you to insert USB key will pop up and the installation progress bar will stop.

**Note**: This step will not occur if the key is already plugged in or when performing a Client Install, since a USB key is not required for this installation type.

Install the Vipersat Crypto-Box key by plugging it into an available USB port on the VMS server.

If this is an *Upgrade Installation*, proceed to step 19. If this is a *Clean Installation*, continue with the next step.

😽 Vipersat Management System Setup	_ 🗆 🗙
Installing Please wait while Vipersat Management System is being installed.	
Execute: "C:\DOCUME~1\brad\LOCAL5~1\Temp\nsw4C.tmp\update-vms-key.exe" C:\ Extract: C:\DOCUME~1\brad\LOCAL5~1\Temp\nsw4C.tmp\CbSetup.exe 100%	DOCU
Execute: "C:\DOCUME>1\brad\COCALS>1\Temp\nsw4C.tmp\CoSetup.exe" /Q /CRY. Extract: C:\DOCUME>1\brad\COCALS>1\Temp\nsw4C.tmp\u00edbeavems-key.exe" /Q /CRY. Extract: C:\DOCUME>1\brad\COCALS>1\Temp\nsw4C.tmp\u00edbeavems-key.exe: 1. Extract: C:\DOCUME>1\brad\LocALS>1\Temp\nsw4C.tmp\u00edbeavems-key.exe: 1.	
Please insert your USB key now	
Nullsoft Install System v2.14 <back next=""> Ca</back>	ncel

Figure 2-20 Install Cypto-Box Key prompt

17. The Found New Hardware Wizard will start.

Select the No, not this time radio button, then click Next to continue.



Figure 2-21 Found New Hardware Wizard

**18.** On the Hardware Installation notice shown in figure 2-22, click the **Continue Anyway** button to continue.



Figure 2-22 Hardware Installation

**19.** The installation process will continue and, when completed, the screen shown in figure 2-23 will be displayed. Click the **Finish** button to exit.

Found New Hardware Wizard	
	Completing the Found New Hardware Wizard
	The wizard has finished installing the software for:
	CBUSB Ver 1.3
	Click Finish to close the wizard.
	< Back. Finish Cancel

Figure 2-23 Hardware Installation Completed screen

**20.** Click the **OK** button in the **Waiting** dialog shown in figure 2-20 to complete the installation and updating of the Crypto-Box Key.

#### VMS Server Installation

**21.** After installing and/or updating the key, the installation will complete as shown in figure 2-24. Click the **Next** and then the **Finish** button to exit the installation wizard.

		(No.
Setup was completed successfully.		
Completed		
Extract: ParamEdit-CDM5XX-5.1.d		^
Extract: ParamEdit-CDM5XX-5.2.d		
Extract: ParamEdit-CDM5XX-5.3.d Extract: ParamEdit-CDM5XX-5.4.d		
Create folder: C:\Program Files\Vip		odapov
Execute: "C:\Program Files\Vipersa		
Output folder: C:\Documents and		
Create shortcut: C:\Documents an	nd Settings\rremillong.FREMONT\S	
	od Settings\rremilleng EDEMONT\S	itart MenulProgra
Create shortcut: C:\Documents an		
Create shortcut: C:\Documents an Create shortcut: C:\Documents an	nd Settings\rremillong.FREMONT\S	itart Menu\Progra
Create shortcut: C:\Documents an Create shortcut: C:\Documents an Created uninstaller: C:\Program Fi	nd Settings\rremillong.FREMONT\S	itart Menu\Progra
Create shortcut: C:\Documents an Create shortcut: C:\Documents an	nd Settings\rremillong.FREMONT\S	itart Menu\Progra

Figure 2-24 Installation Complete dialog



**Note:** If this is a standalone on a workgroup server, or an upgrade installation, move on to the section "Verifying Successful Server Installation" on page 2-27.

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

# Setting Com Security for VMS

1. From the Windows Start menu, select Settings and open up the Control Panel, as shown in figure 2-25 below.

🐓 Control Panel		
<u> </u>	s Iools Help	
🕒 Back 🝷 🕥 🝷 🏂	🔎 Search 🎼 Folders 🛛 🎲 🗙 🌠 🥅 -	
Address 📴 Control Panel		💌 🔁 Go
Name 🔶	Comments	<b></b>
🔥 Accessibility Options	Adjust your comput	
🕿 Add Hardware	Installs and trouble	
🔯 Add or Remove Programs	Install or remove pr	
Madministrative Tools	Configure administr	
🍓 Automatic Updates 💦	Set up Windows to	
Roadcom Control Suite 2	Broadcom Advance	
ADDAte and Time	Set the date, time,	
💁 Display	Change the appear	
Folder Options	Customize the displ	
C Fonts	Add, change, and	
🖙 Game Controllers	Add, remove, and c	
🔁 Internet Options	Configure your Inte	
aw Keyboard	Customize your key	
Sector Stress Sector Se	Changes licensing o	
Di Mouse	Customize your mo	
SNetwork Connections	Connects to other c	
by Phone and Modem Options	Configure your tele	
🗒 Portable Media Devices	View the portable m	
Captions 🇠	Configure energy-s	
Service and Faxes	Shows installed prin	

Figure 2-25 Control Panel

**2.** Select **Administrative Tools** and then **Component Services**, as shown in figure 2-26.

🌀 Back 🝷 🕥 🝷 秒 🔎	Search 📂 Folde	rs   🍃	» 🕑 🗙 🍤 🛄 •		
Address 🦏 Administrative Tools					
Name 🔺	Size	Туре	Date Modified	Attributes	
Active Directory Domains and	1 KB	5hortcut	1/29/2008 10:53 AM	A	
Active Directory Sites and Ser	1 KB	5hortcut	1/29/2008 10:53 AM	A	
Active Directory Users and Co	1 KB	5hortcut	1/29/2008 10:53 AM	A	
E Certification Authority	2 KB	5hortcut	5/2/2005 5:00 PM	A	
🗂 Cluster Administrator	2 KB	5hortcut	8/30/2007 9:39 AM	A	
Domponent Services	2 KB	5hortcut	5/2/2005 4:57 PM	A	
📕 Computer Management	2 KB	5hortcut	2/5/2008 2:12 PM	A	
🗿 Configure Your Server Wizard	2 KB	5hortcut	1/28/2008 11:42 AM	A	
避 Data Sources (ODBC)	2 KB	5hortcut	5/2/2005 5:00 PM	A	
🛃 Distributed File System	2 KB	5hortcut	5/2/2005 5:00 PM	A	
🛃 DNS	2 KB	5hortcut	1/29/2008 10:52 AM	A	
🚡 Domain Controller Security Pol	1 KB	5hortcut	1/29/2008 10:53 AM	A	
R Domain Security Policy	1 KB	Shortout	1/29/2008 10·53 AM	Δ	
	Figure	2-26	Administrative Tools		

**3.** Expand the Component Services tree until "My Computer" appears, and select **Properties**, as shown in figure 2-27.

#### Setting Com Security for VMS

🎒 Component Services	
🐌 Eile <u>A</u> ction <u>V</u> iew	<u>W</u> indow <u>H</u> elp
	S 🖉 😰 💷 🎽 🏊 🤃 🗰 🏛 🏥 🕮
Console Root	
Computers	COM+ DCOM Config Distributed Running
	Stop MS DTC Transacti Processes
⊕… 🔁 DCOM (     ⊕ Distribu	Refresh <u>a</u> ll components
🗄 🧰 Running	<u>V</u> iew
🗄 🎻 Active Directory Us	New <u>W</u> indow from Here
<ul> <li>⊕ ∰ Event Viewer (Loca</li> <li>⊕ ∰ Services (Local)</li> </ul>	P <u>r</u> operties
	Help

Figure 2-27 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 2-28.

	5	? >
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
	s allowed default access I plications that determine I	
	Edit <u>L</u> imits	Edit Default
	s allowed by default to lau	
activate objects. Yo determine their own	ou may also set limits on a permissions. Edit L <u>i</u> mits	pplications that Edit <u>D</u> efault
	n permissions.	

Figure 2-28 Com Security, Edit Limits

5. In the Launch Permissions window, select Add as shown in figure 2-29.

Launch Permission		? ×	
Security Limits			
Group or user names:			
Distributed COM Osels (VIII ETH     Domain Admins (VIPER-RACK)     Q Everyone			
venomroom (venomroom@Viper-Rack.com)			
	Add	<u>R</u> emove	
Permissions for Administrators	Allow	Deny	
Local Launch	V		
Remote Launch			
Local Activation	N N		
Remote Activation			
	OK	Cancel	

Figure 2-29 Launch Permissions

**6.** Ensure the Location is the domain, then type "VMS" in the object box and select **Check Names**. If the location was correct you should see the result shown in figure 2-30.

Select Users, Computers, or Groups	? ×
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
Viper-Rack.com	Locations
Enter the object names to select ( <u>examples</u> ):	
VMS (VMS@Viper-Rack.com)	Check Names
Advanced	Cancel //

Figure 2-30 Select Users

7. Click on **OK**. This will return you to the Launch Permissions window with the new user highlighted. Check **Allow** on any boxes that are blank as shown in figure 2-31, then click the **OK** button.

Launch Permission		? ×			
Security Limits	Security Limits				
Group or user names:					
🕵 Domain Admins (VIPER-RACK\Domain Admins)					
🕵 Everyone					
venomroom (venomroom@					
VMS (VMS@Viper-Rack.co	om)				
•					
	Add	<u>R</u> emove			
Permissions for VMS	Allow	Deny			
Local Launch					
Remote Launch	→ 🛛				
Local Activation Bemote Activation					
Remote Activation					
1					
	ОК	Cancel			

Figure 2-31 Launch Permissions with New User

This concludes setting the Component Securities on the Domain Controller.

# Verifying Successful Server Installation

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



Figure 2-32 Services, Administrative Tools menu

**2.** Select **Vipersat Management System** from the Services list as shown in figure 2-33, then click on **Start** the service.

This will start the VOS (Vipersat Operating System).

#### Verifying Successful Server Installation

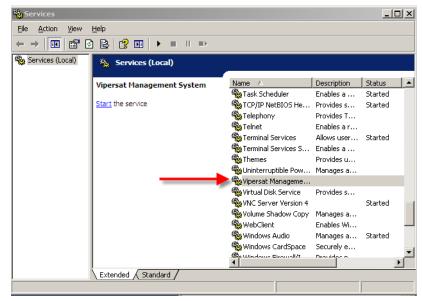


Figure 2-33 Vipersat Management System Service

**3.** From the Program File directory, find **VMS 3.x** and click the **Connection Manager**. Accept "localhost" and click on the **OK** button in the **Connect To** dialog. The **Viperview** window will appear, as shown in figure 2-34.

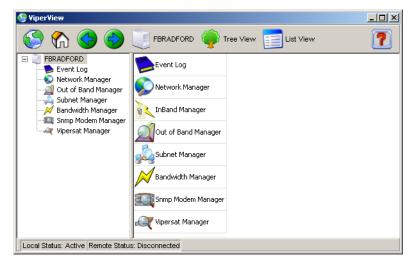


Figure 2-34 Successful Installation, ViperView

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.

**Note**: If this is an upgrade, the network database will already exist and configuration is not required.

• For *VMS Redundancy Server configurations*, proceed to Appendix C, "Redundancy", for instructions on configuring redundant servers.

The Vipersat Management System client software should be installed on a highperformance, industry-standard workstation computer running Microsoft Windows XP Professional with SP2. 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 view the Global Map 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<sup>TM</sup> 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 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, 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.



**Note:** The installation does not require the USB 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 VMS Client installation, follow the same procedure used for Server installation provided in the section "VMS Server Installation" on page 2-14. In step 4., select the radial button **Client Install**, as shown below in figure 2-35.

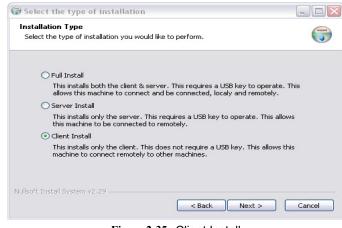


Figure 2-35 Client Install

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

## **Creating 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.

#### VMS Client Installation

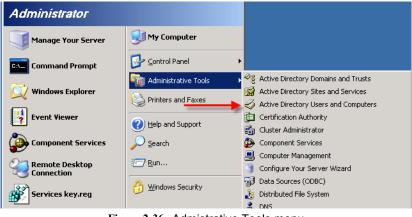


Figure 2-36 Admistrative Tools menu

**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.

	Y & Y     Y	Description Built-in account for admini Members of this group are DNS Administrators Group DNS clients who are permi Designated administrators All workstations and serve All domain controllers in th All domain guests
Saved Queries       Name         Viper-Rack.com       Administrator         Domain Controllers       Administrator         Computers       DonsAdmins         Domain Controllers       DonsUpdateProxy         Iteres       Domain Controllers         Delegate Control       Domain Controllers         Pind       Computers         Ocontact       Group         View       InetOrgPerson         New Window from Here       MSMQ Queue Alias	User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Built-in account for admini Members of this group are DNS Administrators Group DNS clients who are permi Designated administrators All workstations and serve All domain controllers in th
Builtin     Gomputers     Computers     Delegate Control     Find     Delegate Control     Find     Delegate Control     Find     Computer     All Tasks     View     New Window from Here     MSMQ Queue Alias	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Members of this group are., DNS Administrators Group DNS clients who are permi Designated administrators All workstations and serve All domain controllers in th
New         Computer           All Tasks         Contact           Yiew         InetOrgPerson           New Window from Here         MSMQ Queue Alias	Security Group Security Group	= =
Export List User Properties	Security Group User User User User User User Security Group	All domain users Designated administrators Members in this group can Built-in account for guest IIS Worker Process Group Built-in account for anony Built-in account for anony Built-in account for anony Servers in this group can

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.

New Object - Group	×
Create in: Viper-Rack.	com/Users
Group name:	
VMS Users	
Group name (pre- <u>W</u> indows 2000):	
VMS Users	
Group scope	Group type
C Domain local	Security
🖲 Global	C Distribution
C Universal	
	OK Cancel

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.

w Object - User	
Create in:	Viper-Rack.com/Users
<u>F</u> irst name:	VMS Initials:
Last name:	Client
Full name:	VMS Client
User logon name:	
VMS Client	@Viper-Rack.com
User logon name (pre	- <u>W</u> indows 2000):
VIPER-RACK\	VMS Client
	< Back Next > Cancel

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.

New Object - User 🛛 🗙
Create in: Viper-Rack.com/Users
Password:
User must change password at next logon
<ul> <li>User cannot change password</li> <li>Password never expires</li> </ul>
C Account is disabled
< <u>B</u> ack <u>N</u> ext > Cancel

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.

MS Client Properties	;	? ×
Remote control General Address Member 01 Member of:	Terminal Services Profile   Account Profile Telephones   Dial-in Environment	COM+ Organization Sessions
Name	Active Directory Folder	
Domain Users	Viper-Rack.com/Users	
<u>Add</u>	<u>B</u> emove	
Primary group: D	Iomain Users	
Set Primary Group	There is no need to change Primary you have Macintosh clients or POSI applications.	
	OK Cancel	Apply

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.

Select Group	? >	<
Select this object type:		
Group or Built-in security principal	Object Types	
From this location:		
Viper-Rack.com	Locations	
Enter the object name to select ( <u>examples</u> ):		
VMS Users	Check Names	
1		
Advanced	OK Cancel	
Advanced	OK Cancel	//.

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.

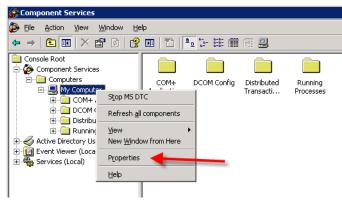


Figure 2-43 My Computer Properties

**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.

Computer Propertie	s	?
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
	s allowed default access t plications that determine t	
	E dit <u>L</u> imits	Edit Default
	s allowed by default to lau ou may also set limits on a permissions. Edit Limits	
	· · · · ·	

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.

Launch Permission		? ×			
Security Limits					
		1			
	Group or user names:				
	🗾 💯 Domain Admins (VIPER-RACK\Domain Admins) 🛛 🔳				
💯 Everyone					
	VMS (VMS@Viper-Rack.com)				
MS Users (VIPER-RACK/VMS Users)					
•					
	A <u>d</u> d	<u>R</u> emove			
Permissions for VMS Users	Allow	Deny			
Local Launch	$\checkmark$				
Remote Launch	→ 🗹				
Local Activation	—▶ 🗹				
Remote Activation	→ 🗹				
	OK	Cancel			

Figure 2-45 Launch Permissions

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

## Verifying Successful Client Installation

After installation, verify that the VMS Client installation was successful by running the program. The VMS Server must be running VOS.

- **1.** From the Program File directory, find VMS 3.x and click the **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).

Connect		×
Select server to connect to	_	OK
localhost		Cancel

Figure 2-46 Connect dialog

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

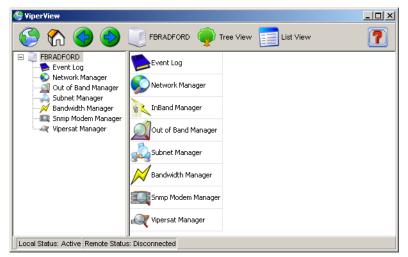


Figure 2-47 ViperView window, VMS Client

# ViperGlobe Install

ViperGlobe is a small separate installation and is installed only on a VMS Client workstation that has the necessary supporting video graphic hardware. Located on the VMS install disk, **VMS 3.6.x.xxx Globe View Setup** will install in the same directory as the VMS Client.

Double-click on the Setup file to install the application.

🕞 Vipersat Ne	twork Globe Setup: Completed	
	d	
Show details		
Cancel	Nullsoft Install System v2.29 < Back Close	; ;

Figure 2-48 Vipersat Network Globe Setup

## Verifying ViperGlobe Installation

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

- 1. From the Program File directory, find VMS 3.x and click the Vipersat Network Globe shortcut.
- **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 Vipersat Map View window will appear, as shown in figure 2-49.

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

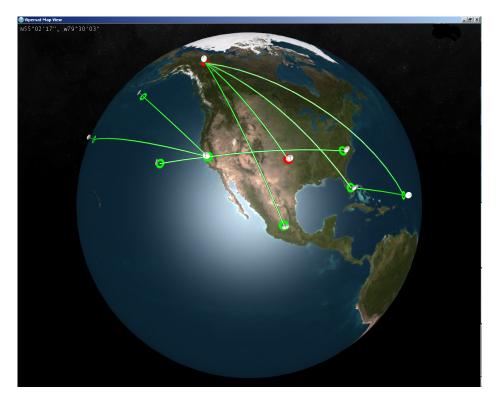


Figure 2-49 Vipersat Map View window

## **VNO** Install

## **VNO Overview**

Comtech EF Data - Vipersat Network Products Group VNO solution provides an interface into a defined subset of the actual network managed by VMS. This is exposed as a Web Services SOAP interface provided by the VNO-WS.exe service. The VNO web service supports both non-redundant stand-alone and redundant VMS deployments.

With redundant VMS servers, figure 2-50 depicts the VNO-WS.exe installed on a separate Windows workstation running the same service providing active awareness between the VMS Servers. It is recommended that this separate workstation be the same workstation running ViperView (Client PC workstation).

The VNO-WS service accepts requests from the VNO Web application running on an IIS server. Requests and responses transmitted between the web application on the IIS server and VNO-WS web service uses SOAP over HTTP protocol. The SOAP request is translated into an RPC call into VOS and the response is returned to the web application, which usually transforms into HTML and sends the HTML back to a web browser where a VNO user interface is presented to the VNO user.

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. Refer to the *VNO User Guide* for details.

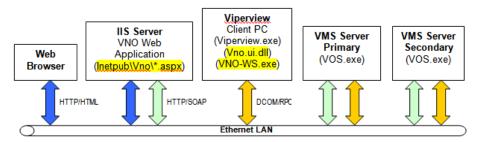


Figure 2-50 VNO Deployment with Redundant VMS Servers

## Installation Procedure

The VNO installation process consists of installing software, highlighted in yellow sections in figure 2-50, on the IIS Server and the Client PC. Although the VNO\_WS Server can run on the VMS server, it is recommended that it be installed only on the client PC running Viperview.

- **1.** If running, terminate the Viperview.exe and VConMgr.exe applications on the server. Use the Task Manager to end the applications and processes.
- **2.** Execute the VMS 3.6.x.xxx SOAP Proxy setup.exe application. This will install VNO-WS.exe and VNO.ui.dll in the default Vipersat\VMS\3.0\bin directory.
- **3.** As shown in figure 2-51, the Installer will present a dialog requesting VNO configuration parameters.

### • VNO Host IP

This parameter is the IP address for the network interface that the VNO web service will use for TCP/IP communications with VNO client applications. A value of 0.0.0 will use all network interfaces on the server. This is the recommended setting unless a specific network interface is required.

#### • VNO Host Port

This parameter specifies the TCP port used by VNO-WS. The default port is decimal 8080. Any available port can be specified provided that the client 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 VNO.admin.exe utility is used to configure the user database and privilege levels. This utility is located in the VMSinstalled directory 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 addresses. In a redundant VMS configuration, up to nine addresses can be entered (e.g., for all VMS servers in the same redundancy group).

🛱 VNO WS Installation	
IP 0.0.0.0 Port 8080	Basic User Authentication
VMS Server IP	
127.0.0.1	
Cancel Nullsoft Install System v2.29	Install

Figure 2-51 VNO-WS Installer

- **4.** Refresh the Service Control Manager and verify that the VMS VNO WS services entry is displayed in the list of services.
- **5.** Start the VMS VNO service. A single beep will indicate that the service started. Verify that the status has changed to *Running*. The vno-ws-log.txt log file in the Vipersat\VMS\3.0\Data directory will also show if the service started.

### СНАРТЕК

# 3

# VMS CONFIGURATION

# General



**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 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.

### General

- 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 sample network in figure 3-1.

Sever View				×
🚱 🏠 📀 🌍 🧾 CA-6KN8YB1 🍕	Tree View 🥎 Demo	List View	2	]
CA-6KN8YB1 CA-6KN8YB1 CA-6KN8YB1 Carlos Constraints Constraints Constraints Carlos Constraints Carlos Constraints Customer 1 Customer 1 Customer 1 Customer 1 Customer 1 Customer 1 Customer 2 Customer 2 Customer 3 Customer 4 Customer 3 Customer 3 Customer 3 Customer 4 Customer 3 Customer 3 Customer 4 Customer 3 Customer 4 Customer 3 Customer 4 Customer 4 Cust	HuB HuB FRau" Customer 1 FRau" Customer 2 FRau" Customer 3	Operator not specified		

Figure 3-1 Sample Network Configuration

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

# 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 3-2, 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.

🛃 Telnet 10.1.0.16	×
Vipersat Configuration	
STDMA Mode	
Automatic Switching	Ξ.,
Network IDE2]	
Receive Multicast Address[239.1.2.4]. Managing IP Address	
Dynamic Power Control Config	;
Vipersat Summary	)
UDP Fort Base Address[49152 [0xC000]]U	'
Save Parameters to permanent storage	
Telnet Logout	-

Figure 3-2 CDM-570/570L Telnet Vipersat Configuration

### Hardware 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.

This procedure assumes that the user is experienced with the VMS 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.

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



**Tip:** Watch the devices as they are discovered by the VMS, as viewed in the ViperView window. Be certain that all of the known units in the network have been discovered before proceeding. 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, the database can be restored to this point.

# VMS Initial Setup Procedure

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

### **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 "Verifying Successful Server Installation" on page 2-27.

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

2. On the VMS Client, 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 3-3). Enter the **IP address** of the active VMS Server and click the **OK** button.

Connect	×
Select server to connect to	OK
localhost	Cancel

Figure 3-3 Connect dialog

The ViperView window will open.

### **Activate the Server Processes**

In ViperView, right-click on the Server icon on the top menu bar and select **Activate** from the drop-down menu (figure 3-4) to manually initialize the VMS server processes.



Figure 3-4 Server Processes, Manual Activation

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



Figure 3-5 Activated Server Notification

### **Configure Auto Activate**

- **1.** Right-click on the Server icon and select **Properties** from the drop-down menu.
- **2.** In the **General** tab, check the box for **Auto Activate** as shown in figure 3-6. This will automatically activate the server processes the next time the VOS service is started.

CA-6KN8YB1	? 🔰
General Traps	
CServer Status	
Up Time : 0 days, 0 hours, 4 minutes, 5	i0 seconds
Version : 3.6.3.998	
Serial: {9DCB7CA2-500F-11D3-B0F	F-00105A202838}
Local Status: Active Enabled I Auto Activate Redundant Servers	Priority
Address	1
	Retry Delay
	1sec
	Retry Count
	5
	Failover Time
Add Modify Remove	10sec
OK Car	ncel Apply

Figure 3-6 Server Properties, Auto Activate

### **Configure Addresses and Assign ID**

- 1. Right click on Vipersat Manager from the ViperView tree view list and select **Properties**. The Vipersat Manager window will open.
- 2. Select the General tab shown in figure 3-7, and 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.

ieneral	Timeouts	Registratio	n		
		IP Setup			
	[	Management	Multica	et Address	
		239 . 1			
		Local VMS Ad	dress		
		192 . 168	3 . 15	0.188	
		Base Port	TOS	i Value	
		C000	0		
			Gua	rdband	
			-	1%	
	Str	eamload Data	ates -		
	T×	512Kbps	Rx	32Kbps	1
		Force Multi			5
		Legacy B			
		C Legacy L	loauc	ISC MODE	
		ОК		Cancel	Appl

Figure 3-7 Vipersat Manager, General tab

- **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.
- **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. 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 allow management/singling messages the highest passage level.
- 6. The **Guardband** is the center carrier-to-carrier frequency slot allocation setting. The default setting of 35% will place carriers within the bandwidth pools at 1.35 times the carrier symbol rate. Contact your satellite service provider for proper setting of carrier spacing.
- 7. The **Streamload Data Rate** values determine the amount of bandwidth required to GET and PUT modem configuration files. Set the rates not to exceeded 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.

8. The Force Multicast Port Restart check box provides the option to reset the port used by the VMS server for multicast transmissions. 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.

9. The Legacy Broadcast Mode check box provides support for the previous method of sending the active management IP address message using an acknowledged multi-command packet. This message updates the Managing IP Address field in all listening modems set to receive the management multicast message. The message interval is defaulted to send an update every 15 seconds. See Timeouts tab for timer interval setting.

If all modems are running CDM-570/570L, CDD-564/564L–v1.5.4, SLM-5650A–v1.3.2 or greater, uncheck this box to use the unsolicited message type.

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

🔍 Vipersat Manager 🛛 🔹 🕄
General Timeouts Registration Heartbeat Interval Timeout Debounce 2.5sec 10.25sec 10 Communications Retry Timeout Retry Count Ssec 3 Announcement Period 15sec Failure Threshold 3
OK Cancel Apply

Figure 3-8 Vipersat Manager, Timeouts tab

11. The **Heartbeat** timer values sets the <u>Interval</u>, <u>Timeout</u> and <u>Debounce</u> of hub device redundancy messaging. The **Interval** of 2.5 seconds updates the modem to send it's heartbeat message to the VMS at set rate. The **Timeout** 

is how long the VMS will wait before determining communications failure commanding a device redundancy switchover. The **Debounce** is a message count on how long the VMS will receive messages sent from the modem with alarm information set. This value is important to reduce the possible spurious alarm redundancy triggers.

**12.** The **Communications** timer values set timeouts for command messages. The **Retry Timeout** is the wait between messages which works in conjunction with **Retry Count**. The default setting with a 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.

**13.** The **Announcement Period** is a the interval at which 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.

- 14. The Failure Threshold parameter specifies the number of consecutive attempts that the VMS will make for a single remote unit to switch using an available demodulator before that demodulator is made unavailable.
- 15. Select the **Registration** tab shown in figure 3-9 and click the **Add** button to add the **Network ID** number (any number between 1 255) that will identify this network. This number must match the Network ID established in the modems for this network.

💐 Vipersat Mana	iger		? 🔀
General Timeouts	Registration		
Network ID's			
			Add
			Modify
			Remove
Add N	etwork ID		
Netwo	'k ID	Monitor Only	
10	(	Monitor & Cont	rol
	ОК	Cancel	
	ОК	Cancel	Apply

Figure 3-9 Vipersat Manager, Registration tab

- **16.** Select the **Monitor & Control** radio button if this network is to be managed by this VMS, otherwise select **Monitor Only**.
- **17.** Click the **OK** button to save these settings for the Vipersat Manager Properties.

# VMS Network Build Procedure

### **Subnet Manager Configuration**

Most of the work here will be done by VMS. The operator needs to verify that each subnet has all of the expected elements populated in the subnet.

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

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



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

### Setting the Alarm Masks

Network alarms must be set to insure an alarm alerts the operator to an actual problem. If there are spurious alarms, or alarms which have no operational meaning the operator will become desensitized and critical network failures can be missed. This section addresses masking alarms that represent normal network conditions. VMS allows the masking of these nuisance alarms. Do not skip this step if you want your operators to manage the network pro-actively and respond quickly to alarms.

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. <u>Perform the following procedure for all network</u> <u>units that function as either a Burst Controller or an Expansion unit</u>.



**Note:** On SLM-5650A modems, masking is pre-configured when set to Hub and Selective TDMA is enabled.

**1.** From the *Tree View*, select the unit and open the Properties window as shown in figure 3-10.

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

*For SLM-5650A units*, right-click on the demodulator icon and select **Properties** from the drop-down menu.

- 2. Select Mask Unlock Alarm, then click on OK.
- **3.** Right-click on the unit's icon again and select **Force Registration** to activate the flag.

🚅 Hub-51-G1-5₩	? ×	Demodulator ? ×
General Configurations Name		General Name
Lock Front Panel Mask Unlock Alarm Enable Heartbeat Auto Home State Timeout QOS Management Enable Rules Routes Right click on unit		☐ Burst Controller ✓ Allocatable ✓ Unlock Alarm Mask Right click on demodulator
OK Cancel	ply	OK Cancel Apply
CDM-570/570L. CDD-56X		SLM-5650A

Figure 3-10 Mask Unlock Alarm setting

### **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.

- 1. From the VMS Tree View, right-click on each remote data unit (*not expansion units and never any hub units*) and open the **Properties** window(figure 3-11).
- **2.** Enter a time in minutes for the **Auto Home State** to take effect, then click **OK**.



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

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.

🖛 Remote-3-Data 🔋	× = 10.1.129.50 ? ×
General Configurations Name Remote-3-Data	General Configurations Name Remote 2
Lock Front Panel Mask Unlock Alarm Enable Heartbeat Auto Home State Timeout 4 QOS Management Enable Rules Routes	IP Address 10 . 1 . 129 . 50 Subnet Mask 255 . 255 . 0 Auto Home State Timeout (min) 4 FIPS Blocks Per Frame 0 Heartbeat Enabled
OK Cancel Apply	OK Cancel Apply

CDM-570/570L

SLM-5650A

Figure 3-11 Auto Home State Timeout setting

### **Bandwidth Manager Configuration**

### Create Satellite(s)

The first step is to create the satellite for the network with the appropriate operating frequency information.

- **1.** Right-click on the Bandwidth Manager and select **Create Satellite** from the drop-down menu (figure 3-12).
- **2.** Enter the satellite **Name** and the **Center** and **Translation Frequency** settings in the Create Satellite dialog (figure 3-13).

Check with your service provider if unknown. Bandwidth Allocation and Location entries will be defined later, if necessary.

😚 ViperView		
🍪 🌀 🌍 🜍 🧾 CA-6KN8'	/B1 💮 Tree View 🗾 List View	
CA-6KN8YB1	Event Log	
Out of Band Manager     Subnet Manager	Network Manager	
Bandy Open	InBand Manager	≡
Somp Create Satellite     Redunuancy manager	Out of Band Manager	
	Subnet Manager Status 3 Alarmi	
	Bandwidth Manager	
	Somo Modem Manager	
Local Status: Active Remote Status: 0/0		

Figure 3-12 Create Satellite menu command

Create Satellite	? ×
General	
Name	
unnamed	
Bandwidth Allocation Policy	
Optimal Fit Threshold	Minimum Fragment Size
OHz	OHz
- DE Chana da si dina	
RF Characteristics Center Frequency	Translation Frequency
14.25GHz	2.3GHz
<u>.</u>	
Location Latitude	Longitude
0:0'0"	0:0'0"
ОК	Cancel Apply

Figure 3-13 Create Satellite dialog

- **3.** After a **Refresh** command, the newly created satellite will appear under Bandwidth Manager in the ViperView window.
- 4. Repeat the previous steps to create additional satellites, as required

### **Create Transponders**

The next step is to create transponders in the newly created satellite. Each transponder is entered with its center frequency and bandwidth.

- **1.** Right-click on the satellite icon and select **Create Transponder** from the drop-down menu (figure 3-14).
- **2.** Enter the transponder **Name**, **Center Frequency**, and **Bandwidth Span** in the Create Transponder dialog (figure 3-15).

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 crossbanded transponders (refer to Appendix A, "VMS Cross Banding" for more information).

😚 ViperView		- 0 🛛
🌍 💿 🌍 🐑 🧾 CA-6KN8	YB1 🏺 Tree View 🗾 List View	
CA-6KN8YB1	Event Log	<u>^</u>
Vetwork Manager     Out of Band Manager     Subnet Manager	Network Manager	
⊕ one Subnet Manager ⊖ M Bandwidth Manager ⊕ % Warnand	InBand Manager	≡
Snmp     Open     Redu     Create Antenna	Out of Band Manager	
Gut 0     Create Transponder     Vipers	Subnet Manager 7 Alarm	
Properties	Bandwidth Manager	
Local Status: Active Remote Status: 0/0	Somo Modem Manager	×

Figure 3-14 Create Transponder menu command

Create Transponder	? ×
General	
Name	Pad OdBm
Frequency Range Center Frequency OHz Bandwidth Span 36MHz	Translation Override OHz
ОК	Cancel Apply

Figure 3-15 Create Transponder dialog

**3.** Repeat the previous steps to create multiple transponders.

### 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 a Hub antenna, followed by the Remote antennas, as described below.

- 1. Right-click on the satellite icon and select Create Antenna from the dropdown menu.
- 2. In the General tab of the Create Antenna dialog (figure 3-16), enter the Name, Operator and Contact Information.

perator not specified	lame		Rx-Gain
not specified ontact Information	unnamed		OdB
ontact Information	perator		
	not specified		
not specified	ontact Information		

Figure 3-16 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 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 tab to configure the **Antenna Visibility** range, as shown in figure 3-17.



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

Center	Bandwidth
500GHz	1THz

Figure 3-17 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, and binding the modem modulators and demodulators to the converters.

**1.** Right-click on an Antenna icon and select **Create Up Converter**. The dialog box shown below(figure 3-18) will open.

It is important to ensure that the **Up Converter** frequencies are correct, as this is a very common 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.

Create Up Converter	? ×
General	,
E-Band Block Up Converter	
Local Oscillator 13.05GHz	Inversion
O 70MHz Up Converter	
Transponder Center	🗖 Inversion
O 140MHz Up Converter	
Transponder Center	Inversion
C Custom	
RF Reference 14.25GHz	Inversion
IF Reference 1.2GHz	
Bandwidth 500MHz	
Power Limit OdBm	
OK Cancel	Apply

Figure 3-18 Create Up Converter dialog

**2.** Right-click on the Antenna icon again and select **Create Down Converter** (figure 3-19). Ensure that the frequency settings here are correct.

Create Down Converter	? ×
General	
L-Band Low Noise Block Down Converter	
Local Oscillator 11.075GHz	Inversion
C 70MHz Down Converter	
Transponder Center	Inversion
C 140MHz Down Converter	
Transponder Center	Inversion
C Custom	
RF Reference 12.275GHz	Inversion
IF Reference 1.2GHz	
Bandwidth 500MHz	
OK Cancel	Apply

Figure 3-19 Create Down Converter dialog

**3.** Notice that the newly created Up and Down Converters appear in the Antenna View (figure 3-20).

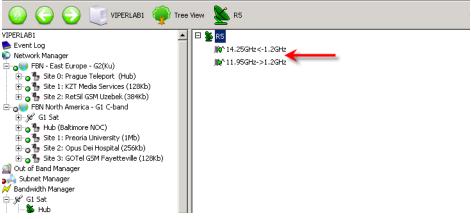
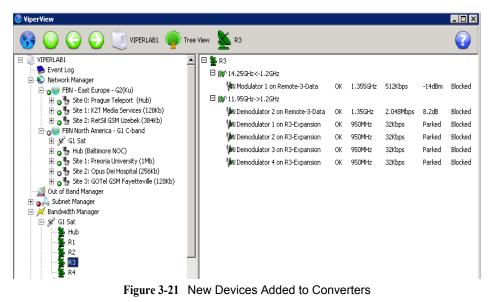


Figure 3-20 Converter Icons on Antenna View

- 4. Bind node Modulators and Demodulators to the Up and Down Converters:
  - Expand the Subnet Manager tree down to the Modulator and Demodulator level for those units that will utilize this Antenna.
  - Click on the Antenna icon in the left window panel to display the Converters in the Antenna View in the right window panel.
  - Click-hold on each modulator/demodulator device icon in the left panel, drag it to the right panel and drop it onto the desired converter.

The new devices appear under the Converters as shown in figure 3-21.



- **5.** Make the *Expansion Unit* Demodulators available by right-clicking on them in the Antenna View and selecting **Allocatable** from the drop-down menu.
- 6. Repeat the previous steps for each Antenna.

### InBand Manager Configuration

A precursor to configuring InBand management is to set the 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.

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.

Right-click on the BC demodulator and select **Properties** from the drop-down menu. The dialog appearance with the correct settings are shown in figure 3-22 (CDM-570/570L) and figure 3-23 (SLM-5650A).

Demodulator 2		? ×
General Modem		
Flags	Carrier Type C None C SCPC C STDMA	
	OK Cancel	Apply

Figure 3-22 BC Carrier Flag Setting, CDM-570/570L

Demodul	ator	? ×
General		
	Name  Permodulator  Burst Controller  Allocatable  Unlock Alarm Mask	
	OK Cancel	Apply

Figure 3-23 BC Carrier Flag Setting, SLM-5650A

1. Enable **InBand Management** on each remote subnet. On nodes which are part of the switched network, right-click on the Subnet icon from the Tree View and select **InBand Management**, as shown in figure 3-24.

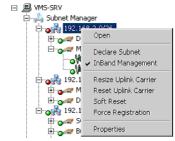


Figure 3-24 InBand Settings for Remotes

**2.** When **InBand Management** is selected, as shown in figure 3-24, a window will open prompting the operator to select the Modulator for switching from the **Name** list shown in figure 3-25.

elect Modem	Þ
Name Modulator 1 on R2 DATA	ОК
	Cancel

Figure 3-25 Select Switching Modulator

**3.** Select the remote's modulator, open the Subnet View, as shown in figure 3-26, and refresh the device view to verify that the VMS has picked up the home state.



**Tip:** If the list is empty, it is likely that the remote is not registered. Ensure that all sites are registered with the VMS before attempting InBand Management. Typically, if the device icon is illuminated (green or red), the modem has registered. To verify that the modem is registered with the managing VMS, secure a connection to the unit through either Telnet or Web interface.

ViperView						×
🚯 💑 G2 Remotes 🛅 List V	iew					0
-37-10.1.132.0/24	Address X 10.1.132.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1,133.0/24	atus Address 10.1.133.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
v InBand Managemen	Address	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1 Resize Uplink Carrie Revert Uplink Carrie	10 1 125 0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
Status: O Reset Uplink Carrier	r					
Soft Reset			Цог	no indicat	es succe	ooful
Delete					ies succes nown does	
Properties			inde		iowii uoo.	51100.

Figure 3-26 InBanding a Remote

4. Right-click on the Subnet and open the Properties page.

The **General** tab, which opens first, allows the operator to enter a **Subnet Name**, if desired, and add **External Subnets**. External Subnets are additional networks beyond the local area network of the modem.

If the remote site has a router, and applications you wish to switch on (voice, e.g.) reside on the other side, insert the **Subnet Address** and **Mask** here. See figure 3-27, below.

a 172.17.129.0/26
General In Band Policy Distribution Lists S.A.S.
Subnet Name can be entered here
External Subnets
Address Mask
Address         OK           Øl         0         0         0           Mask         0         0         0
Insert Modify Remove
OK Cancel Apply

Figure 3-27 Subnet Properties, General tab

**5.** The **InBand** tab on the Properties page (figure 3-28) displays the **Home State**, the **Remote Modulator**, the **Downlink Modulator** (if selected), and the **Uplink Demodulator**. If the initial InBand setting failed (did not show the correct Home State in the Subnet view), check to ensure these settings are correct.

This tab can be used to change Home State settings for a remote. Enter the desired settings and revert the uplink carrier. Remember to reset the Home State parameters in the modem and save them after doing this.

172.17	7.130.0	/26			? 🗙	
General	In Band	Policy	Distribution	Lists S.A.S.		
Home S	State					
Freque	ncy	cy Bitrate Power				
14.26	1GHz	512Kbps 17.5dBm			n 🚺	
	e Modulat					
Modu	Modulator 1 on Data Unit Select					
Downlin	nk Modula	itor —				
	Select					
-Uplink I	Demodula	tor				
Demo	dulator 2	on Burs	t Controller	S	elect	
		ОК	C	ancel	Apply	

Figure 3-28 Subnet Properties, InBand tab

**6.** The **Policy** tab (figure 3-29) allows the operator to modify policy settings for this remote site that are inherited from the global Policy tab (see the section "InBand Manager" on page 5-18).

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

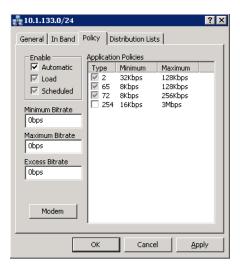


Figure 3-29 Properties Policy Tab

The check boxes have 3 states:

Clear — The policy or switch type is not allowed Clear with Check — The policy or switch type is controlled locally Gray with Check — The policy or switch type uses global settings

Application Policy Type numbers have the following convention:

- 1 Scheduled Switching and VFS
- 2 Voice
- 3 Video

4-64 — Reserved for the System

65-253 — User Defined

**254** — Uninterruptable Switch (used to ensure that additional applications will not generate a switch, thus preventing video glitches)

7. The **Distribution Lists** tab (figure 3-30) allows the operator to set up a list of sites to be included in a switch under defined circumstances. For example, this feature can be used to tune expansion demodulators at a list of sites to receive a multicast video stream.

To declare a distribution list, right-click on the white area in the tab box, then click on the **Insert** button that appears.

eneral   In Band	Policy Distribution Lists	? ×
Destination	Name	
	Insert	
	OK Cancel A	pply

Figure 3-30 Properties Distribution List tab

**8.** The **Distribution List** dialog (figure 3-31) provides a **Destination** box and a **Name** box, and allows the operator to select **Sites** to add to the list.

If the destination is left as 0.0.0.0 and the network is in *Entry Channel Mode* with switch type *Load*, the effect is to permanently PAMA the links in the list.

Distribution List	×		
Destination 0 . 0 . 0 . 0 Name	OK Cancel	Select Object Look in: G2 Remotes	×
Site List	Add Site	10.1.133.0/24 10.1.134.0/24 10.1.135.0/24	
		Object name: 10.1.135.0/24	ОК
		Objects of type: InBand Subnet	Cancel

Figure 3-31 Distribution List dialogs

The **Satellite Advanced Switching** (S.A.S.) tab (figure 3-32) is a remote roaming feature that provides advanced switching per remote to any given satellite. The advanced carrier switching from beam-to-beam in roaming applications allows for variable carrier characteristics between satellites per remote, whereby roaming from one satellite to another with different specifications, e.g. Modula-

tion and FEC Rate, can occur. Note, however, that Turbo mode should never be changed.

To configure a roaming remote and different specifications per satellite are required, perform the following steps. Otherwise, proceed to the next section, "Pool Management".

🕺 172.17.128.0/26 🛛 🔹 💽	🕺 172.17.128.0/26
General In Band Policy Distribution Lists S.A.S.	General In Band Policy Distribution Lists S.A.S.
Per Satellite Advanced Settings	Per Satellite Advanced Settings
Domain Settings	Domain         Settings           Vipersat         QPSK, 3/ 4, Turbo
Right Click to Insert	Modem Extra
Look in: 📈 Vipersat Bandwidth Manag 🗸	BFEC & Modulation Modulation OP5K
S Vipersat	FEC Rate 3/4 Rate
	FEC Type Turbo
Object name: OK	
Objects of type: Frequency Domain V Cancel	OK Cancel
OK Cancel Apply	OK Cancel Apply

Figure 3-32 S.A.S. tab with SOTM Enabled

- **9.** Right-click in the center of the S.A.S. tab and select **Insert** to open the Select Object dialog.
- **10.** Select the **Vipersat Bandwidth Manager Service** from the list of object names and click **OK**.
- **11.** Select the Satellite and click **OK**, then modify the Modulation and FEC Rate for the switched SCPC characteristics of this satellite service area.



**Note:** When switching between satellites, the Modem Extra values set within the SAS will override the Modem Extra block setting in the Policy tab. The Home State Extra block setting is **not** affected, as it is used for reverting to STDMA mode.

### **Pool Management**

The next step is to set up bandwidth pool(s) in the transponder(s) created earlier. Bandwidth pools are the heart of the switching engine. They are the only portion of the space segment actively controlled by the VMS.

1. Right-click on the satellite in the tree view and select **Open** (figure 3-33).



Figure 3-33 Satellite Open menu command

This opens the **Spectrum Analyzer** / **Bandwidth** ViperView window (figure 3-34).

**Tip:** At this point, the carriers should be visible. If not, double-click in the center of the window. If the carriers still do not appear, there is an error in the frequency settings on either the satellite, the transponder, or the converters.

per¥iew				
😚 🖋 G2 Sat				0
WER-G2				
2dB -	Zoom To			
⁴ →	Create Pool			
dB	Delete			
1.4211GHz	Properties	14.43128686	7GHz	14.460141039GHz
Operator: not specified				

Figure 3-34 Spectrum View

The gray edges in the Spectrum View represent the Guardband. The darker area is the Transponder, and the carriers shown are the TDM Outbound and STDMA carrier for the network associated with the opened satellite.

**2.** Right-click in the Transponder area and select **Create Pool** from the menu to open the Create Pool dialog shown in figure 3-35, below.

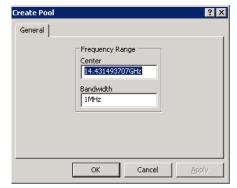


Figure 3-35 Create Pool dialog

**3.** The **Center Frequency** setting will reflect the Transponder frequency value corresponding to the point where the mouse was clicked to create the pool.

Correct this setting to the desired value for this pool, and adjust the **Bandwidth** to the correct width.

Click **OK** and the new pool will appear (figure 3-36).

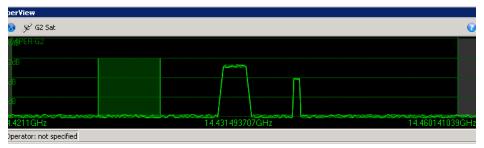


Figure 3-36 New Bandwidth Pool

- 4. Repeat the previous steps to create additional bandwidth pools.
- **5.** Right-click on the inbanded subnet in the Subnet Manager View and select **Resize Uplink Carrier** from the drop-down menu (figure 3-37).

The Resize Uplink dialog will open, allowing a **New Bitrate** to be specified. The bit rate shown is equal to the current bit rate; in this case, the STDMA channel rate.

6. Click on OK to close the dialog and initiate a switch.

ViperView							×
😚 🦂 G2 Rem	notes 🛅 List View						0
10.1.132.0	Da Status Open	Address .1.132.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1.133.	✓ InBand Management	Address 1.133.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1.134.0	Resize Uplink Carrier < Revert Uplink Carrier	1.134.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1.135.0	Reset Uplink Carrier Soft Reset	Address .1.135.0/24	Resize Uplink New Bitrate	X	Bit Rate 512Kbps	Frequency 14.445GHz	
Status: OK Add	Delete		512Kbps	Extra			
	Properties		ОК	Cancel			

Figure 3-37 Resize Uplink Carrier, Subnet

Returning to the Spectrum View, the blue shaded area represents the slot assigned by the VMS for the switch. Upon receipt of the next PLDM (Path Loss Data Message), a carrier will appear showing the current  $E_bN_0$  and bandwidth (figure 3-38).

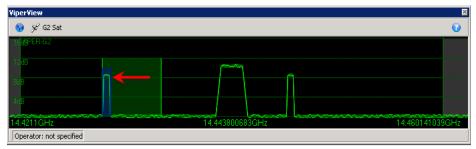


Figure 3-38 Switched Carrier (Spectrum View)

The Subnet View will show the site status as *Switched*, with a type of *Manual*, along with the current Bit Rate and Frequency (figure 3-39).

¥iper¥iew							
😵 💑 G2 Remotes [	📑 List View						6
10.1.132.0/24	Status OK	Address 10.1.132.0/24	Status Switched	Type Manual	Bit Rate 512Kbps	Frequency 14.42933504GHz	←
10.1.133.0/24	Status OK	Address 10.1.133.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1.134.0/24	Status OK	Address 10.1.134.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1.135.0/24	Status OK	Address 10.1.135.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
Status: OK Address: 10	.1.132.0/22						

Figure 3-39 Switched Carrier (Subnet View)

NOTE

7. From the Tree View, click on the Hub antenna under the Bandwidth Manager to display the Hub devices in the right window panel.

From this view, the operator can see the switched demodulator that the VMS selected, the carrier frequency in L-Band, the bit rate, the current  $E_bN_0$ , and the subnet/subnet mask (figure 3-40).

Blocked
Blocked
Blocked
Blocked
10.1.132.0/24
Available
Blocked
Blocked
Blocked

Figure 3-40 Switched Carrier (Hub Antenna View)

**Note:** After reaching this point and all indications are as noted above, the Subnet Manager, the Bandwidth Manager, and the InBand 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.

### Network Manager Configuration 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.

VMS version 3.6 introduces ViperGlobe, an optional global Map View application. 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 Map View.

The operator can now anchor sites to true geographic locations. In a SOTM (Satellite on the Move) network, moving sites are placed based on GPS infor-

mation received from the antenna ACU. An example of this type of network is depicted in figure 3-41, below.

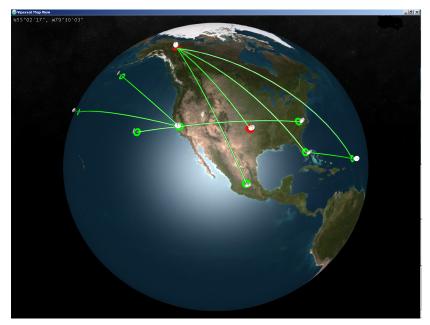


Figure 3-41 Vipersat Network, Global Map View

This section describes the procedure for configuring Network Manager in the VMS, and graphically displaying the network using ViperGlobe.

- 1. From the Tree View, right-click on the Network Manager icon and select Create Network (figure 3-42).
- 2. In the Network Properties dialog that opens, enter a Network Name.
- 3. Expand the Network Manager to expose the new Network icon.

😵 YiperYiew	
🚯 🙆 😋 🐑 🧾 VIPERLABI 🏟 Tre	ee View
VIPERLAB1     VIPERLAB1	ee view Eise Log  Event Log  Event Log  Network Manager  Out of Band Manager  Subnet Manager  Subnet Manager  Subnet Manager  Signing Modem Manager  Redundancy Manager  Vipersat Manager  Vipersat Manager

Figure 3-42 Creating the Network

**4.** Drag and Drop the satellite(s) for this network from the Bandwidth Manager onto the Network icon (figure 3-43).



Figure 3-43 Drag and Drop Satellite(s)



**Note:** References to ViperGlobe in the following steps apply to Client machines that have the optional ViperGlobe application installed.

5. Open the Vipersat Map View window by one of two methods:

• Double-click on the Network Map View icon (Desktop Shortcut).

• From the *Start* menu, select *Programs* then *VMS 3.6* followed by **Vipersat Network Globe**.

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

The Vipersat Map View window will open, displaying the globe (figure 3-44).



Figure 3-44 Globe View with Network Icon

**6.** In the upper right corner of the window, the Vipersat network will appear as an orange icon. 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 (figure 3-45):

• Right-click on the Network icon under Network Manager in the Tree View of the Viperview window and select the **Create Site** command from the drop-down menu.

This method requires that the site coordinates for latitude and longitude be specified after the site is created.

• Right-click on the desired geographic location on the globe in the Vipersat Map View window and select **Create Site**.

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 upper left corner of the window as a reference.

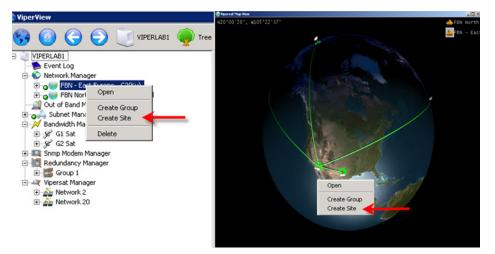


Figure 3-45 Adding Sites, Network Manager and ViperGlobe

- Execute the Create Site command and enter the Name to be used for the site.
   In the Tree View, expand the Network to expose the newly created site.
- 8. Right-click on the Site icon and select Properties.

The exact coordinates can be entered in the dialog that opens.

- **9.** After adding a site, 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 3-46), assuming that the sites are up and there is at least one active link.

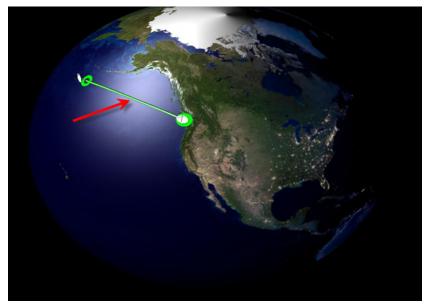


Figure 3-46 Map View with Linked Sites

In order to have the sites on the Map View indicate alarms, it is also necessary to drag and drop the subnet icons associated with each site into the Network Manager.

- **11.** 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 right corner of the map 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.

# Basic Guaranteed Bandwidth

Basic Guaranteed Bandwidth is a feature that provides the means for assigning a guaranteed minimum bandwidth on a per site basis. This bandwidth allocation is known as the **Committed Information Rate** (CIR). When properly configured, this feature ensures that there will always be sufficient bandwidth available to

## VMS Network Configuration

switch a terminal to its CIR. Requests for rates above the CIR are granted on a first-come, first-serve, best effort basis. A terminal that does not have an assigned CIR has no guarantee for any bandwidth, and is only granted bandwidth on a purely opportunistic basis.

The Basic Guaranteed Bandwidth / CIR function depends on the pre-allocation of system resources, namely RF spectrum and network hardware devices (demodulators). Overlaying frequency masks are utilized for the pre-allocation of bandwidth, as illustrated in figure 3-47.

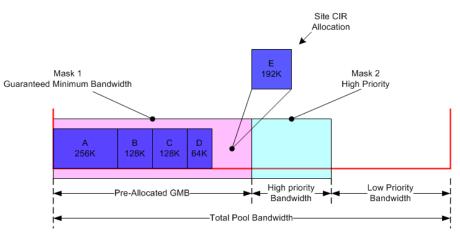


Figure 3-47 Visualization of Basic Guaranteed Bandwidth

Mask 1 designates the frequency spectrum that is reserved for sites with defined CIR bandwidth slots. The slot size is equal to the Minimum Bit Rate value that is defined by the site Policy parameter setting.

Mask 2 designates a separate spectrum allocation dedicated to sites that are selected to operate within this priority frequency segment. Creating this spectrum mask is optional when setting up the Basic Guaranteed Bandwidth feature.

## **CIR Configuration**

The configuration of CIR involves four steps:

- Enabling CIR on the Satellite
- Setting the CIR policies first the Global, then the Local Subnet
- Enabling CIR on the Remote Antenna(s)
- Defining the Priority Bandwidth allocation (optional)

## Enable CIR on the Satellite

Right-click on the Satellite appearance in the Tree View and select **CIR Enabled** from the drop-down menu (figure 3-48).

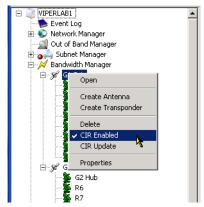


Figure 3-48 CIR Enabled Command

## **CIR Policy Setting**

The CIR assigned to a Remote is equal to the Minimum Bit Rate setting, which is determined by the local Subnet policy setting. Any Remote that has the local policy set to 0 bps (the default) will use the global policy setting as its CIR value. This relationship facilitates the configuration of CIR on a system-wide basis. A local policy, if set *above* 0 bps, will over-ride the global policy, in much the same manner as is used by the VMS to control switching policies.

In the example figures shown below, the global policy Minimum Bit Rate value is set to 256 Kbps. The remote with the subnet 172.16.128.0/27 has a minimum rate of 384 Kbps, which will be its assigned CIR.

To configure the CIR Policy settings, perform the following procedure.

- **1.** Click on the **VMS Server** appearance at the top of the Tree View to display the Service Managers in the right panel of the window.
- **2.** Right-click on the **InBand Manager** and select **Properties** from the dropdown menu. The window shown in figure 3-49 will open.

## VMS Network Configuration

Event Log		
Network Manager		
inBand Manager	🕵 InBand Manager	? 🗙
Out of Band Man	Policy Distribution Lists	
💑 Subnet Manager	Enable Application Policies           Image: Application Policies           Image: Automatic           Type           Minimum           Maximum	
Bandwidth Mana	✓ Load     ✓ 10 512Kbps 1Mbps     ✓ Scheduled	
🚉 Snmp Modem Ma	Minimum Bitrate 256Kbps	
Redundancy Mar	Maximum Bitrate	
Out of Band Circi	2Mbps Excess Bitrate	
减 Vipersat Manage	Obps	
	State	
	OK Cancel A	pply

Figure 3-49 Global CIR Setting

The **Minimum Bit Rate** setting on the Policy tab establishes the global CIR value for the Network.

Perform the following steps for all Remotes that will utilize a CIR that is different than the global value.

- **1.** Right-click on the local Subnet appearance for the Remote and select the **Properties** command.
- **2.** Open the **Policy** tab and set the **Minimum Bit Rate** for the Remote (figure 3-50).

172.16.128.0/	27	?×
General In Band Enable Automatic Cad Scheduled Minimum Bitrate 384Kbps Maximum Bitrate SMbps Excess Bitrate Obps QPSK, 3/ 4, Turbo Modem	Policy Distribution Lists S.A.S. Application Policies Type Minimum Maximum 7 10 512Kbps 1Mbps	
	OK Cancel A	pply

Figure 3-50 Remote CIR Setting

## **Enable CIR on Remote Antennas**

1. Right-click on the Antenna appearance for the desired Remote and enable CIR for either **Normal** or **Priority** bandwidth from the drop-down menu (figure 3-51).

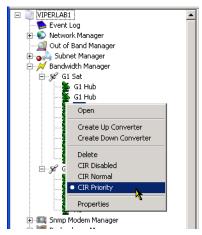


Figure 3-51 CIR Commands, Remote Antenna

Selecting **CIR Normal** will allow this Remote to access the *Low Priority Bandwidth* spectrum (see figure 3-47) when attempting to switch above its CIR.

Selecting **CIR Priority** will grant access to the *High Priority Bandwidth* spectrum for this Remote.

2. Repeat for each Antenna associated with a CIR Remote.



**Note:** An attempt to enable CIR for a remote that results in the available bandwidth (the sum of the Guaranteed, Normal, and Priority bandwidths) exceeding the Total Pool Bandwidth will be denied, and an error message will appear (figure 3-52).



Figure 3-52 Enable CIR Error

## **Adjust Bandwidth Allocation**

- 1. Right-click on the Satellite and open the Properties window.
- 2. Select the CIR tab, as shown in figure 3-53.

🖋 G1 Sat	? ×
General Transponders CIR	
Guaranteed Bandwidth	288KHz
Normal Bandwidth	2.712MHz
Priority Bandwidth	2MHz
	*
ОК	Cancel <u>Apply</u>

Figure 3-53 Satellite CIR tab

Because the Remote CIR policies have been configured previously, the available bandwidth for **Guaranteed** and **Normal** has been calculated by the VMS and is displayed here.

**3.** If **Priority Bandwidth** is required, enter the amount and click on the **Apply** button. Note that the Normal Bandwidth will be reduced by this amount.

It will be necessary to perform a **CIR Update** whenever any of the following occur:

- The Bandwidth Pools are changed
- The CIR (Minimum Bandwidth) for a Remote is changed
- A Remote Antenna is added or removed, with or without CIR



**Note:** An Update is not required when changing either a Remote priority or the Priority Bandwidth because the VMS will automatically adjust the available bandwidth.

The CIR Update command is selected from the Satellite drop-down menu (figure 3-48).

# 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 (Satellite On The Move)

This section applies only to those networks with mobile platforms, such as a maritime environment. VMS 3.6.x 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 3-54. Configuring this feature requires that sites are on-line.

## VMS Network Configuration

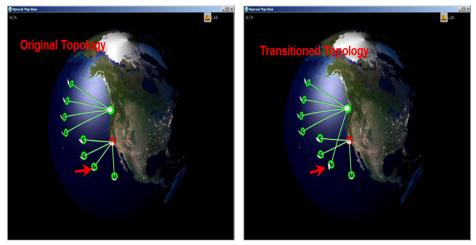


Figure 3-54 SOTM Transitioned Site

- 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 3-55).

General		<u>?</u> ×
	9	
Position Latitude 22.0°N Heading 1 0.0°	Longitude 130.4°W	
		<b>1</b> 2
	OK Can	cel <u>Apply</u>

Figure 3-55 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 subnet should appear (figure 3-56).

Note that, if the subnet icon was not copied into the Network Manager site as described in *Network Manager Configuration*, this box will be empty.

Select Object	Select Object
Look in: 🐴 R7 💽	Look in: 🙀 10.1.134.0/24
A 10.1.134.0/24	Remote7Mesh
	≪ Remote7OOB ≪ Remote-7-Data
	10.1.134.25 <b>ROSS</b>
Object name:	Object name: 10.1.134.25 OK
Objects of type: GPS Source Cancel	Objects of type: GPS Source Cancel

Figure 3-56 Selecting ROSS Unit for SOTM

- **4.** Select the **Subnet** and click **OK**. This will open up a dialog showing the subnet components.
- 5. Select the ROSS unit and click OK.

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.

6. 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).

- 7. Right-click on the Hub modem unit that represents the first TDM outbound and select the **Properties** page.
- 8. Click Routes. The Routes window will open (figure 3-57).

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**.

## VMS Network Configuration

Routes								×
Network	Mask	Gateway		Interface	Hdr Comp	Pld Comp	Encrypt	
10.1.128.0	255.255.255.0	0.0.0.0		Satellite	Disabled	Disabled	Disabled	
10.1.129.0	255.255.255.0	0.0.0.0		Satellite	Disabled	Disabled	Disabled	
<ul> <li>✓ 10.1.130.0</li> <li>✓ 10.1.131.0</li> </ul>	255.255.255.0 255.255.255.0	0.0.0.0 0.0.0.0		Satellite Satellite	Disabled Disabled	Disabled Disabled	Disabled Disabled	
Import	Export					<u></u> K		<u>C</u> ancel
	<b>\</b>	[	CDM57	OL C:\Docu	iments and	Settings\r	remillong.	? 🗙
			SMTF Acces Maint	s Admin	STDMA Compression Mngd Switch	Switching DES D Network	Vipersat PC   Home   QoS	VLAN IGMP Routing
			#	Route Name			Next Hop	L I
			0	DFG MMC 400	0.0.0//		10.1.0.1	<u>1</u>
			1 2	VMS,tt88 VMS,tt89	10.1.130 10.1.131	.0/24		P P
							DK	Cancel

Figure 3-57 Dynamic Routing Entry, CDM-570/570L

**9.** 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.

10. 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.

- **11.** Right-click on the Hub unit with the first TDM outbound and open the **Properties** page.
- **12. Enable** QOS Management by checking the box, then click on the **Rules** button (figure 3-58).

General Configurations	<				
General Configurations Name Hub-S1-G1-TDM/BC	1				
└── Lock Front Panel └── Mask Unlock Alarm └── Enable Heartbeat Auto Home State Timeout					
0 QOS Management C Enable Rules Routes					
OK Cancel Apply					
QOS Rules	1				×
Source         Port         Destination         Port           ✓         0.0.0.0/0         0/65535         0.0.0.0/0         0/65535	Protocol None	Priority Min BW 0 32Kbps	Max BW 9.999Mbps	Filter	WRED
Right Click to Ins					
Import Export				<u>о</u> к	<u>C</u> ancel

Figure 3-58 QOS Rules Configuration, CDM-570/570L

**13.** 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.

## VMS Network Configuration

This concludes the VMS Network Configuration.

# **C H** A **P T E R**

# 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.

## General

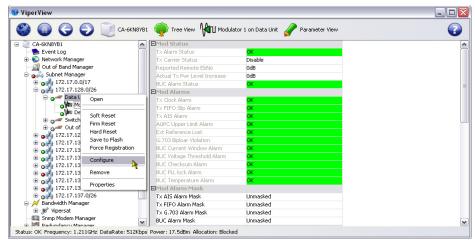


Figure 4-1 Modem Equipment Drop-Down Menu, ViperView

- **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:** 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.

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

 Table 4-1
 CDM-570/570L Modem/Router Manual Connection Options

D.1.4.J

# CHAPTER

# 5

# VMS SERVICES

# General

This section covers using the various Services that make up the VMS, a satellite network management system with an intuitive, user-friendly, graphical user interface which displays:

- · Continuously updated network health and status information
- Multiple networks managed from a single server
- · Centralized network configurations
- · Organized network layouts
- Automated equipment detection
- Large network management with intuitive drag-and-drop bandwidth management and configuration.

The following sections describe the system services which, working together, form 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 right-clicking on the Servers 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.

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.

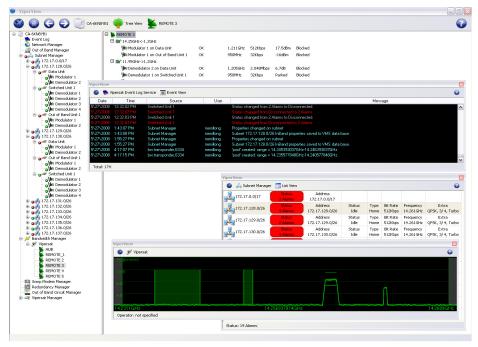


Figure 5-2 ViperView, Multiple Window Views

For example, the **Subnet Manager View** shown in figure 5-3 can be opened to display the current switch status, bit-rate, and RF frequency of all network remotes.

ViperView	52 Remotes ा List View						×
10.1.			Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1	133.0/24 Statu: Open	Address 10.1.133.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1	✓ InBand Management	Address 10.1.134.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
10.1	Resize Uplink Carrier Revert Uplink Carrier	Address 10.1.135.0/24	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.445GHz	
Status: O	Reset Uplink Carrier Soft Reset						
	Delete	_			and the second sec	tes succes 1own does	
	Properties			1115	and onn		

Figure 5-3 Subnet Manager 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.

🦻 🗕 нив					3
📡 НИВ					
□ ))@^ 14.25GHz<-70MHz					
🍿 Modulator 1	Unknown	N/A	N/A	Blocked	
日 顺14.25GHz<-1.2GHz					
🌾 Modulator 1	Unknown	N/A	N/A	Blocked	
🍿 Modulator 1	Unknown	N/A	N/A	Blocked	
🍿 Modulator 1	Unknown	N/A	N/A	Blocked	
🌾 Modulator Exp 1	Unknown	N/A	N/A	Blocked	
🖂 ∭^ 12.275GHz->70MHz					
🎾 Demodulator 2	Unknown	N/A	N/A	Unavailable	
🖻 🏬 11.95GHz->1.2GHz					
🎾 Demodulator 1-23	Unknown	N/A	N/A	10.1.130.0/24	
🎾 Demodulator 2-23	Unknown	N/A	N/A	10.1.131.0/24	
Mail Demodulator 3-23	Unknown	N/A	N/A	Available	
🎾 Demodulator 4-23	Unknown	N/A	N/A	Available	
Mail Demodulator 2-16	Unknown	N/A	N/A	Unavailable	
Mai Demodulator 2-18	Unknown	N/A	N/A	Unavailable	
MRI Demodulator 2-19	Unknown	N/A	N/A	Unavailable	
12-17 Hub-STDMA-2	Unknown	N/A	N/A	Blocked	

Figure 5-4 Antenna View



Note: The Antenna View shows L-Band frequencies.

Use the Event Log to stay current on recent network activity, as shown in the **Event View** window shown in figure 5-5.

ViperView					×
🌍 🛸 V	ipersat Event	Log Service 📃 Event	View	1	7
Date	Time	Source	User	Message	
4\28\2006	12:05:49am	Inband Manager		Automatic>>Home switch on 192.168.1.128/26 - 128Kbps, carrier @ 14.256GHz	
4\28\2006	12:06:01am	Inband Manager		Home>>Automatic switch on 192.168.1.128/26 - 800Kbps, 720KHz, carrier @ 14.284300215GHz	
4\28\2006	12:06:13am	Inband Manager		Automatic>>Home switch on 192.168.1.128/26 - 128Kbps, carrier @ 14.256GHz	
4\28\2006					
4\28\2006	12:06:49am	Inband Manager		Home>>Automatic switch on 192.168.1.128/26 - 800Kbps, 720KHz, carrier @ 14.284300215GHz	
4\28\2006	12:07:00am	Inband Manager		Automatic>>Home switch on 192.168.1.128/26 - 128Kbps, carrier @ 14.256GHz	
4\28\2006					
4\28\2006	12:07:35am	Inhand Manager		Home>>Automatic switch on 192 168 1 128/26 - 800Kbps_720KHz_carrier @ 14 2843002156Hz	-
Total: 2533					

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.

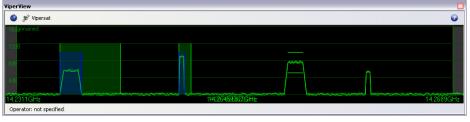


Figure 5-6 Spectrum View

The **Parameter View**, shown in figure 5-7, constantly supplies the operator with updated information for a selected unit.

😂 ViperView			_ 🗆 ×
🚱 🕜 🌍 🌍 🧾 EN	3-VMS 🌍 Tree View 🖅 H	IUB-STDMA-G1 🥜 Parameter View	2
🖻 🍌 Subnet Manager 🛛 🔺	□Unit Status		
0.1.0.0/17	Unit Model Number		
HUB-STDMA-G1	Unit Serial Number	0	
	Unit Software Version Number		
→ Demodulator 2-23	Unit Circuit ID		
Demodulator 3-23	Unit Alarm Status	ОК	
Mai Demodulator 4-23	Unit Temperature	0	
	Reference 2E7 option Installed	Not Installed	
Expansion 2	Reference 2E8 option Installed	Not Installed	
Expansion 3	Ext Reference Alarm Status	OK	
⊞…o≪ HUB-570 ⊞…o≪ Hub-Expansion	Unit Type	0	
10.1.128.0/24	⊡Unit Alarms		
€ of R1 DATA	+5V Alarm	OK	
E a 10.1.129.0/24	+12V Alarm	ок	
D 10.1.130.0/24	-5V Alarm	ОК	
E R3_MESH_564L	+23V Alarm	ок	
⊕ arr R3-Data	-12V Alarm	ОК	
	Tx Synthesizer Alarm	ок	
🖃 📈 Bandwidth Manager	Rx 1st LO synth Alarm	ОК	
🖉 PAS 10	Rx 2nd LO synth Alarm	ОК	
ँ — 🌺 Н∪В	Ext Ref PLL Alarm	ОК	
- 👺 Remote 1 🛛 🖵	EEPROM Checksum Alarm	ОК	
۱ <u>٬٬٬</u>	□Unit Config Store/Load		•
Status: Unknown Alarm State: Ok State: Disc		10.1.0.23	

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

## ViperView-Monitor and Control

• 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.

😼 ViperView		
🍪 💿 🌍 🌍 🚺 CA-6/	8YB1 🂮 Tree View 🕅 Modulator 1 on Data Unit	Parameter View
E 🧾 CA-6KN8YB1	Mod Status	
- 📂 Event Log	Tx Alarm Status OK	
🗉 😡 Network Manager	Tx Carrier Status Disable	
- 🧾 Out of Band Manager	Reported Remote EbNo OdB	
😑 👝 🍌 Subnet Manager	Actual Tx Pwr Level Increase OdB	
🕀 👩 💑 172.17.0.0/17	BUC Alarm Status OK	
a 🗐 a 🖓 172.17.128.0/26	Mod Alarms	
	Tx Clock Alarm OK	
OP 0	Tx FIFO Slip Alarm OK	
Soft Reset	Tx AIS Alarm OK	
DAMOC	AUPC Upper Limit Alarm OK	
Out Firm Reset     Arrow 172,17,1     Hard Reset	Ext Reference Lost OK	
	G.703 Biploar Violation OK	
172.17.1 Save to Hash	BUC Current Window Alarm OK	
+ 172.17.1 Force Registration	BUC Voltage Threshold Alarm     OK	
172.17.1 Configure	BUC Checksum Alarm OK	
	BUC PLL lock Alarm	
	BUC Temperature Alarm OK	
172.17.1 Properties	Mod Alarm Mask	
172.17.137.0/26	Tx AIS Alarm Mask Unmasked	
🖃 📈 Bandwidth Manager	Tx FIFO Alarm Mask Unmasked	
😟 🖋 Vipersat	Tx G.703 Alarm Mask Unmasked	
🔤 🔤 Snmp Modem Manager	BUC Alarm Mask Unmasked	
Status: OK Frequency: 1.211GHz DataRate: 5		

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 which are operating normally. Red, on both the map and for entries in the menu tree to the left of the map, indicates that there is an alarm condition. Gray indicates that no status multicast (PLDM) being received.

**Tip:** The red error condition indicator indicates that at least one of the devices in a site is reporting an alarm condition for a link.

At this point, no details are shown, but you can very quickly expand the display so you can scan the entire network and determine the condition of each of the network's components.

At the main screen level, you have a number of choices to examine and remedy the error conditions. The tools available are easily reached from the display.

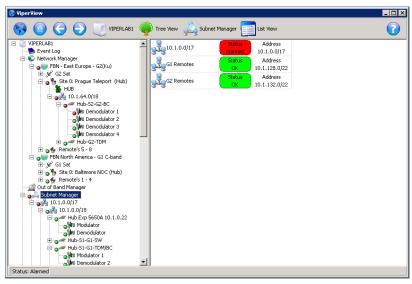


Figure 5-9 ViperView, Subnet Manager

Right-clicking on a point in the network (using either Network Manager or Subnet Manager) 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 data unit Modulator.

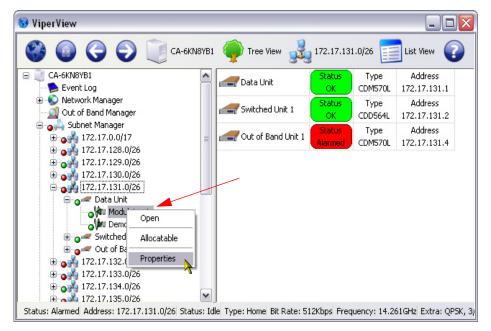


Figure 5-10 Drop-down menu

Right-clicking on the Modulator and selecting **Properties** opens the tabbed dialog shown in figure 5-11.

	🕼 Modulator	? ×
	General	
a Modulator 1	Name Modulator	
General Modem		
Modulator 1		
Type : ComTech CDM570 L-Band Modulator		
Address : 1		
OK Cancel Apply	OK Cancel	Apply
CDM-570/570L	SLM-5650A	

Figure 5-11 Modulator Properities dialog

The **General** tab displays the current name assigned to the modulator and allows renaming, if required.

Clicking the **Modem** tab (*CDM only*) displays the dialog shown in figure 5-12. This tab allows setting the **Flags** and the **Carrier Type** for the device.

Modulator 1		? ×
General Modem		
Flags In-Band Allocatable	Carrier Type C None C SCPC C STDMA	
	OK Cancel A	pply

Figure 5-12 Modem tab, CDM modulator and Demodulator only

These same settings also appear in the Demodulator Properties window for both the CDM-570/570L and CDD-56X.

## **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 5-13).

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.

## ViperView-Monitor and Control

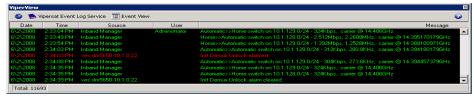


Figure 5-13 Event Log View

Each log entry is displayed using the standard VMS color scheme:

- Green the logged item was completed successfully
- Red The logged item failed and caused an alarm
- Grey The unit was not available
- White Items which do not have a status associated with them
- Yellow Command
- Blue Configuration change
- **Purple** Corrupted entry

Clicking on the **Event View** icon on the Object Bar, as shown in figure 5-13, displays a drop-down menu with five commands:

- Clear
- Twelve Hour
- Filters...
- Export...
- Refresh

۵ 🍋	/ipersat Event Log	g Service 🔳 Event View		6
Date	Time	Clear	User	
6\2\2008 6\2\2008 6\2\2008	11:34:13 AM 11:34:42 AM 11:35:53 AM	Inband Inband Subne Filters	rremillong rremillong rremillong	Inband Manager global policy saved to VMS data base Inband Manager global policy saved to VMS data base Properties changed on subnet
5\2\2008 5\2\2008 5\2\2008	11:35:53 AM 11:38:02 AM 11:38:02 AM	Subne Export Subne Refresh	rremillong rremillong rremillong	Subnet 172.17.131.0/26 InBand properties saved to VMS data base. Properties changed on subnet Remote 4 - 172.17.131.0 Subnet 172.17.131.0/26 InBand properties saved to VMS data base.
5\2\2008 5\2\2008 5\2\2008	12:06:35 PM 12:06:35 PM 2:30:17 PM	Subnet Manager Subnet Manager Inband Manager	rremillong rremillong rremillong	Properties changed on subnet Remote 4 - 172.17.131.0 Subnet 172.17.131.0/26 InBand properties saved to VMS data base. Home>>Manual switch on 172.17.131.0/26 - 512Kbps, 460.8KHz, carrier @ 1
\$\2\2008	2:30:36 PM	Inband Manager	rremillong	Home>>Manual switch on 172.17.132.0/26 - 1Mbps, 900KHz, carrier @ 14.23

Figure 5-14 Event View Menu

# Clear

Selecting **Clear** from the menu deletes all previously recorded events from the log.

# **Twelve Hour**

Selecting the **Twelve Hour** clock setting will toggle between 12 or 24 hour event time stamping.

## Filters...

Selecting the **Filters...** command from the menu opens the **Event Log View** dialog shown in figure 5-15. Here, the log entries appearance can be tailored to display either a particular type of event and/or a specified date range.

Insert
Remove
Properties
🗌 Invert Filte

Figure 5-15 Event Log View, Filters tab

## **Filters Tab**

Clicking the **Insert** button opens the **Insert Object Wizard** dialog, shown in figure 5-16, for selecting an event filter. From the list in the **Name** box, select the filter for the type of event to be displayed in the log.

Insert Object Wizard Select Object Type You must select the type of objec not you want to see additional co	x you wish to insert from the list below. And whether or infiguration pages.
Name Switch Event Filter Symp Modem Status	More Information Switch Event Filter Event filter to filter InBand switches
	< Back Finish Cancel

Figure 5-16 Event Log Filter Selection

**Note:** Currently, there is a set of predefined filters available for the Event Log. As additional filters become available, they can be added to the VMS program through an installer utility.

Clicking the **Finish** button adds the selected object type to the **Event Log View** Filters tab. Multiple filters can be inserted.

The *Display events not filtered by configured filters* check box provides an override to the filter list, allowing all events to be displayed in the log view.

## **Dates Tab**

Similarly, the **Dates** tab can be selected for specifying the date and time to start and stop viewing events, as shown in figure 5-17.

### ViperView-Monitor and Control

Event Log View	<u>? ×</u>
Filters Dates	
Start Date & Time	
	Time 12:00:00 AM
End Date & Time	
	Time 10:14:04.AM
	OK Cancel

Figure 5-17 Event Log Dates tab

The parameters entered on the **Filters** and **Dates** tabs work together to provide customized Event Views of network activity.



**Note:** A billing translation program is available in the VMS for processing the event log to extract billing information. This program, described in Appendix H, "VMS Billing Log Translator (VBLT)", filters entries in the event log into a format which can be used for billing purposes.

## 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 log with any pending events waiting in the event thread.

# 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 5-18 and figure 5-19.

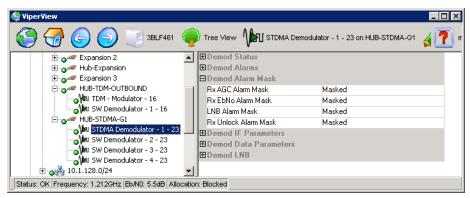


Figure 5-18 Demodulator Alarm Masks

🚭 YiperYiew		
🌍 分 🌀 🌍 🧾 3BLF461	Tree View Modulat	tor N/A on Hub-Expansion 🥜 Parameter ' 👔
3BLF461     Subnet Manager     HUB-570     HUB-570     Hub-Expansion 2     Hub-Expansion 3     HUB-TDM-OUTBOUND     HUB-STDMA-G1	Description:     D	Masked Masked Masked Masked
Status: OK Frequency: 950MHz Power: 30dBm Allo	cation: Blocked	

Figure 5-19 Modulator 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 5-2 are for a typical VMS network.

Device Type	Demodulator Lock Status	Demodulator Level Alarm	Demodulator Auto Gain Ctrl
TDM/ Burst Cont.	Х	Х	Х
Remote			
Hub Expansion	Х	Х	Х
Remote Expansion	Х	Х	Х

 Table 5-2
 Alarm Masking in a Typical Network

## 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, the unit will generate many unwanted alarms in the system during normal operations.

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.

The Unlock Alarm mask for a device is set from the Properties dialog.

*For a CDM-570/570L or a CDD-56X*, open the Properties window for the <u>unit</u>, as shown in figure 5-20.

For an SLM-5650A, open the Properties window for the demodulator.

## ViperView—Monitor and Control

	Demodulator ? 🗙
General Configurations	General
Name Http-S1=G1-SW	Name Demodulator
Lock Front Panel      Mask Unlock Alarm      Enable Heartbeat	
Auto Home State Timeout 0 QOS Management	Burst Controller      Allocatable      Unlock Alarm Mask
Enable     Rules       Routes	Right click on demodulator
Right click on unit	OK Cancel Apply
OK Cancel Apply	OK Cancel Apply
CDM-570/570L, CDD-56X	SLM-5650A

Figure 5-20 Mask Unlock Alarm Flag

# **VMS Service Managers**

When VMS is started on the server and ViperView is opened on the client workstation, the Server View, shown in figure 5-21, displays the installed VMS Services. Included in this display are the Network Manager, the InBand Manager, the Out-of-Band Manager, the Subnet Manager, the Bandwidth Manager (replaces the Upstream Manager in previous versions), the SNMP Modem Manager, the Redundancy Manager, the Out-of-Band Circuit Manager, and the Vipersat Manager.

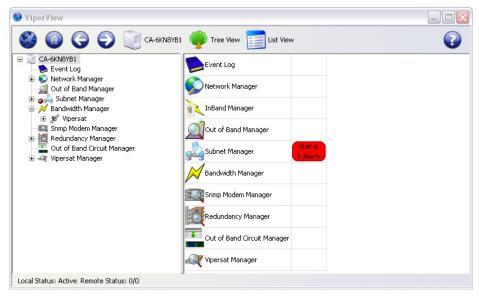


Figure 5-21 Server View

# Vipersat Manager

The Network View under the Vipersat Manager displays all of the units sharing the same network number, as shown in figure 5-22.

#### VMS Service Managers

	-6KN8YB1 🌍 Tree View 😤	Network 10	ist View		
CA-6KN8YB1	Hub Expansion 2	Status	Туре	Address	
n Event Log	mus Expansion 2	2 Alarms	CDD564L	172.17.0.10	
S Network Manager	Hub Expansion 3	Status Alarmed	Type CDD564L	Address 172.17.0.11	
<ul> <li>Jubnet Manager</li> <li>Jr2.17.0.0/17</li> <li>Jr2.17.128.0/26</li> </ul>	Hub Expansion 4	Status OK	Type CDD564L	Address 172.17.0.12	
Data Unit	Hub Expansion 1	Status Alarmed	Type CDD564L	Address 172.17.0.9	
Switched Unit 1	Switched Unit 1	Status 2 Alarms	Type CDD564L	Address 172.17.128.2	
URI Demodulator 1	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.129.2	
WII Demodulator 3	Switched Unit 1	Status 2 Alarms	Type CDD564L	Address 172.17.130.2	
Out of Band Unit 1	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.131.2	
	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.132.2	
	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.133.2	
Switched Unit 1     172.17.131.0/26	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.134.2	
<ul> <li>172.17.132.0/26</li> <li>172.17.133.0/26</li> </ul>	Switched Unit 1	Status 2 Alarms	Type CDD564L	Address 172,17,135,2	
<ul> <li>172.17.134.0/26</li> <li>172.17.135.0/26</li> </ul>	Switched Unit 1	Status OK	Type CDD564L	Address 172.17.136.2	
<ul> <li></li></ul>	Switched Unit 1	Status 2 Alarms	Type CDD564L	Address 172,17,137,2	
Mendwidth Manager     Sector Vipersat	Burst Controller	Status Alarmed	Type CDM570L	Address 172,17.0.5	
HUB REMOTE_1 REMOTE 2	Data Unit	Status 2 Alarms	Type CDM570L	Address 172,17,128,1	
REMOTE 3	Out of Band Unit 1	Status Alarmed	Type CDM570L	Address 172.17.128.4	
REMOTE 5	🚝 Data Unit	Status	Type CDM570L	Address 172,17,129,1	
Redundancy Manager	Out of Band Unit 1	Status OK	Type CDM570L	Address 172.17.129.4	
<ul> <li>Wipersat Manager</li> <li>Metwork 10</li> </ul>	Data Unit	Status	Type CDM570L	Address 172.17.129.4	

Figure 5-22 Vipersat Manager Network View

The health status of each unit in the Network View is indicated by the unit's status color and the supporting text.

# InBand Manager

Right-clicking on the **InBand Manager** icon displays the Properties command, shown in figure 5-23.

😚 ViperView	
🏈 💿 🌍 🐑 🧾 СА-6КN8YB1	🏟 Tree View 🧮 List View 😨
CA-6KN8YB1 Event Log Vetwork Manager Out of Band Manager Subnet Manager Subnet Manager Mandwidth Manager Supersat Redundancy Manager Out of Band Circuit Manager Vipersat Manager Vipersat Manager	Event Log Network Manager Network Manager Not of Band Manager Subnet Manager Bandwidth Manager Redundancy Manager Out of Band Circuit Manager Vipersat Manager
Local Status: Active Remote Status: 0/0	

Figure 5-23 InBand Manager Properties Command

Selecting the **Properties** command displays the **InBand Manager** window shown in figure 5-24.

Enable Automatic	Applicatio Type	Minimum	Maximum
Vinimum Bitrate 19Kbps Maximum Bitrate 10Mbps	<ul> <li>✓ 2</li> <li>✓ 65</li> <li>✓ 72</li> <li>✓ 254</li> </ul>	8Kbps	128Kbps 128Kbps 256Kbps 3Mbps
Obps		-	

Figure 5-24 InBand Manager, Policy tab

# **Policy Tab**

From the InBand Manager **Policy** tab you can set the global policies under which switching will occur in the Vipersat network. These policy settings are set globally for all networks and are propagated down to all remotes in the system. Independently each remote's policy will inherent the global policies, but the operator may choose the break the inherent settings and configure each site independently.

The check boxes at the top of the tab allow you to enable or disable the following functions:

- Automatic Switching
- Load Switching
- Scheduled Switching (Using VCS)

### **Bitrate Limits**

In the **Bit Rate Limits** box you can set the **Minimum**, **Maximum**, and **Excess** bit rate limits for the network. These values are used to determine the load switching bit rate trigger points.

Minimum - This is the minimum bit rate value for all circuits on the site.

Maximum - This is the maximum bit rate value for all circuits on the site.

**Excess** - This value is added to application switched circuits to accommodate momentary excess data flow.

### **Application Policies**

Application Policies are created here at the global system level, but can be either modified or disabled at the site level (Subnet Manager) to accommodate specific site requirements. In the **Application Policies** box you can **Insert**, **Modify**, and **Remove** policies for individual circuit types, then either select or de-select these policies once entered.

Right-clicking in the blank area of the Application Policies box displays a dropdown menu for Inserting a policy. Right-clicking on an existing policy displays a choice to Insert a new policy or Remove the existing policy. A policy can be modified by double-clicking on the policy to enter the edit mode which allows the Type, Minimum bitrate, and Maximum bitrate parameters to be changed.

Choosing Insert displays the Application Policy dialog shown in figure 5-25.

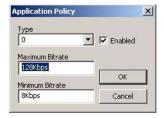


Figure 5-25 Application Policy dialog

Using this dialog, you can establish policy parameters for Type and Bitrate (Maximum and Minimum).

### Туре

Enter the type of circuit here. Application Policy Type numbers have the following convention:

1 — Scheduled Switching and VFS (Vipersat File Streamer)

2 — Voice

3 - Video

4-64 — Reserved for the System

65-253 — User Defined

**254** — Uninterruptable Switch (used to ensure that additional applications will not generate a switch, thus preventing video glitches)



**Caution:** Do not assign circuit types within the Vipersat reserved range as you may cause conflicts if a future VMS release uses that circuit type as a pre-assigned value.

### Maximum Bitrate

The **Maximum Bitrate** affects all circuits of the selected type for the site. This parameter is the rate that any single session of a policy type can not exceed. Once this bit rate is reached, no additional automatic switch requests (ASRs) will be accepted by the VMS.

### **Minimum Bitrate**

The **Minimum Bitrate** affects all circuits of the selected type for the site. This is an absolute minimum value that no selected-type transmission bit rate can be less than.

An **Enabled** check box is provided for specifying whether or not this policy is enabled.

Once an application policy is created, clicking on the **OK** button will display the Policy tab with the new policy appearance, as shown in figure 5-26.

Enable Automatic	Туре	on Policies Minimum	Maximum
Load     Scheduled inimum Bitrate 64Kbps aximum Bitrate	0 🕅	8Kbps	128Kbps
1.544Mbps xcess Bitrate 48Kbps			

Figure 5-26 Revised Policy Tab

Application policies can be modified by directly clicking on them and editing the parameters. To remove a policy, right-click on the policy and select **Remove** from the pull-down menu. A confirmation is required to execute this command.

2)	Remove Application Polic
4	Keniove Application Folic

Figure 5-27 Remove Application Policy dialog

# **Distribution Lists Tab**

**Distribution Lists** are used to define multiple target subnets for point-to-multipoint 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 created here at the global system level, but can also be created, modified, or disabled at the site level (Subnet Manager) to accommodate specific site requirements.

In the Distribution Lists box you can **Insert**, **Modify**, and **Remove** lists for individual subnets, then either select or de-select these lists once entered through the use of the check boxes.

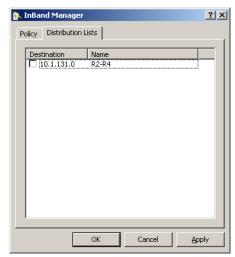


Figure 5-28 InBand Manager, Distribution Lists tab

**1.** Right-click in the blank area of the Distribution Lists box to display the **Insert** command for inserting a new list.

Right-click on an existing list to display a choice to **Insert** a new list, **Modify** the existing list, or **Remove** the existing list.

💽 InBand Manager		? ×
Policy Distribution L	ists	
	·	<u> </u>
Destination  10.1.131.0	Name R2-R4	
Ir	nsert	
	OK Cancel A	pply

Figure 5-29 Distribution Lists, Insert Command

2. Choose Insert to open the Distribution List window shown in figure 5-30.

istribution List	X
Destination 0 , 0 , 0 , 0	OK Cancel
Name	]
Site List Site	Add Site
	<u>R</u> emove Site

Figure 5-30 Distribution List Window

3. Enter the desired **Destination** IP address.

Typically, this will be a unique multicast address for a specific remote or remotes utilizing the same application. Note, however, that the destination address does not have to be a *valid* IP address; it can be a non-valid IP address that is used exclusively for a distribution list, for example.

- 4. Enter the Name for identifying this distribution list.
- **5.** Click on the **Add Site** button. A search dialog will open, allowing the desired subnet(s) to be selected from the VMS network.

Dialog		×
Look ir	n: 🙀 Real Network 💌	
REMOTES		
, Object name	:	ОК
Objects of type	InBand Subnet	Cancel

Figure 5-31 Add Site Dialog, Search Network

**6.** Double-click on the appropriate network element to navigate the network tree until the desired subnet address appears, as shown in figure 5-32. Select the subnet and click OK to add this site to the list.



Note: Only one selection at a time can be added to the list.

Dialog	×
Look in: 🛃 G1 💌	
10.1.128.0/24	
A 10.1.129.0/24	
A 10.1.130.0/24	
A 10.1.131.0/24	
Object name: 10.1.128.0/24	ОК
Objects of type: InBand Subnet	Cancel

Figure 5-32 Add Site Dialog, Select Subnet

7. Repeat this process until all of the desired subnets have been added to the list.

Distribution List		X
Destination 224 .010 .020	.025	ОК
Name Multi-Test		Cancel
Site List		
Site 10.1.128.0/24 10.1.130.0/24 10.1.131.0/24 10.1.132.0/24		Add Site

Figure 5-33 Distribution List Window, Configured

8. Click on the OK button to insert this list in the Distribution Lists tab.

🚺 InBand Manager	? ×
Policy Distribution Lists	
Destination Name	
10.1.131.0 R2-R4	_
✓ 224.10.20.25 Multi-Test	

Figure 5-34 Distribution List Created

9. The new list can be enabled or disabled by clicking in the check box.

### VMS Service Managers

InBand management allows Application Policies and Distribution Lists to be selected on a remote site-level basis and allows the system operator to enable and disable mesh and upstream switching or use policies/lists for selected remotes that differ from the global policies/lists. These site-level policies and lists are established using the Subnet Manager.

# Subnet Manager

The Subnet Manager provides a tree view from which the operator can drill down to investigate alarms. Device management can easily be performed from this view as it displays significant device parameters on the right side of the screen shown figure 5-37.

Clicking on the **Subnet Manager** icon in either the right or left column of ViperView displays a view of all subnets, the status of the switching modulator, the type of switch, if any, and the current transmitting bit rate and frequency.

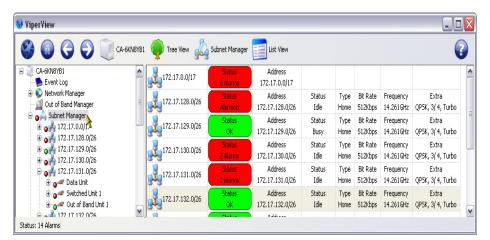


Figure 5-35 Subnet Manager

**Tip:** You can create a separate window, shown in figure 5-36, to display the information in the right panel of Viperview by right-clicking the icon, then selecting **Open** from the drop-down menu. This window can then be placed anywhere on your desktop and will continue to display its contents after you move on to other tasks.

172.17.0.0/17	Status 6 Alarms	Address 172.17.0.0/17					
172.17.128.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	Alarmed	172.17.128.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.129.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	OK	172.17.129.0/26	Busy	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.130.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	2 Alarms	172.17.130.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.131.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	2 Alarms	172.17.131.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.132.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	OK	172.17.132.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo

Figure 5-36 Separate window



**Note:** The same information is displayed in both the right-panel display in figure 5-35 and the separate window display shown in figure 5-36. Both of these displays are continually updated by VMS as new data is received from the network.

Clicking on an individual subnet displays all of the units associated with the subnet with their **Status**, **Alarm State**, current device **State**, unit **Type** and IP **Address** information displayed as shown in figure 5-37.

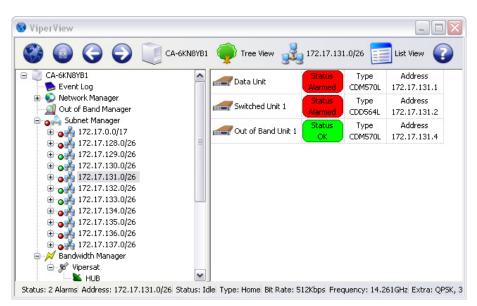


Figure 5-37 Subnet Manager

# Subnet Manager Configuration

Right clicking on an individual subnet displays a drop-down menu, as shown in figure 5-38, allowing the operator to:

- Open
- Soft Reset
- InBand Management
- Resize Uplink Carrier
- Revert Uplink Carrier
- Reset Uplink Carrier
- Delete
- Properties

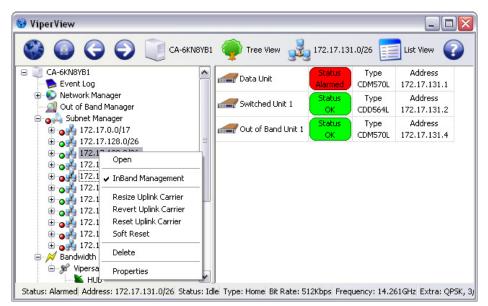


Figure 5-38 Subnet Manager configuration

### Open

Clicking the **Open** command creates an independent window with the data shown in the right portion of the screen in figure 5-38. The independent window appears as shown figure 5-39

172.17.0.0/17	Status 7 Alarms	Address					
172.17.128.0/26	Status OK	172.17.0.0/17 Address 172.17.128.0/26	Status Idle	Type Home	Bit Rate 512Kbps	Frequency 14.261GHz	Extra QPSK, 3/ 4, Turbo
172.17.129.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	OK	172.17.129.0/26	Busy	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.130.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	OK	172.17.130.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.131.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	4 Alarms	172.17.131.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo
172.17.132.0/26	Status	Address	Status	Type	Bit Rate	Frequency	Extra
	Alarmed	172.17.132.0/26	Idle	Home	512Kbps	14.261GHz	QPSK, 3/ 4, Turbo

Figure 5-39 Subnet Mananger open command window

The independent window can be placed anywhere on the screen and is constantly updated by VMS as new information is received from the network.

### InBand Management

Selecting the **InBand Management** command shown in figure 5-38 brings up the **Select Modem** dialog shown in figure 5-40. Selecting a modulator from the **Name** list and then clicking the **OK** button sets the Home State for the subnet to the current values assigned to the selected modulator.

Choose the modulator on the modem that is to be the designated switching modulator for the subnet.

ielect Modem	
Name Modulator 1 on R2 DATA	OK Cancel

Figure 5-40 Select modem dialog

If the drop-down menu in figure 5-38 was checked indicating that InBand Management was enabled, clicking the **Inband Management** checked InBand Management command brings up the **Disable In-Band Extension** warning shown in figure 5-41.



Figure 5-41 Disable in-band extension warning

Clicking the **Yes** button will disable in-band extension and you will lose the home state and policy settings set when In-Band Extensions were enabled.

### Soft Reset

Selecting the **Soft Reset** command from the drop-down menu causes an immediate soft reset of the selected unit.

### **Resize Uplink Carrier**

Selecting the **Resize Uplink Carrier** command from the drop-down menu in figure 5-38 displays the dialog shown in figure 5-42. You can enter a new bit rate value for the uplink in the **New Bitrate** window when manually switching to SCPC mode.



Figure 5-42 Resize uplink dialog

Clicking the **Extra** button brings up the dialog shown in figure 5-43. The items listed in the Modem Extra listing will vary depending on the modem types.

Modem Extra	X
FEC & Modula	tion
Modulation	QPSK
FEC Rate	3/4 Rate
FEC Type	Turbo
i ce type	19.00
	OK Cancel

Figure 5-43 Uplink Modem Extra dialog

Using this dialog you can change the FEC and Modulation characteristics of the uplink SCPC carrier when manually switched.

### **Revert Uplink Carrier**

The **Revert Uplink Carrier** 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.

Selecting the Revert Uplink Carrier command from the drop-down menu in figure 5-38 will display the **Revert Uplink** confirmation dialog shown in figure 5-44. Clicking the **Yes** button will cause the selected unit to revert to its home state.

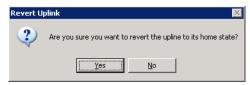


Figure 5-44 Revert uplink carrier dialog

### **Reset Uplink Carrier**

As with the Revert command (see above), the **Reset Uplink Carrier** 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 Reset Uplink Carrier command shown in figure 5-38 displays the **Reset Uplink** warning shown in figure 5-45.



Figure 5-45 Reset uplink warning

### VMS Service Managers



**Caution:** Read the Reset Uplink warning carefully, as performing this operation on a unknown transmitting unit may cause carrier interference on 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.

### Delete

Click the Delete command will delete the subnet from the network,

### Properties

The Subnet Properties page tabs are described below.

### General Tab

The **General** tab allows the operator to view or change the name of the subnet. Subnets declared are listed in the **External Subnets** list.



**Note:** External subnets apply when an application or ToS switch originates past a router at the remote.

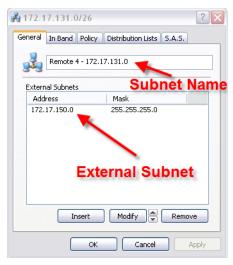


Figure 5-46 Properties general tab

• **Insert** - Clicking the **Insert** button brings up the New Subnet dialog shown in figure 5-47. Enter the IP address and subnet mask for the new subnet in the **Address** and **Mask** dialog boxes.

New Subnet	×
Address	ОК
3.0.0.0	Cancel
Mask	

Figure 5-47 New subnet dialog

- Modify Selecting an existing subnet from the External Subnet listing then clicking the Modify button brings up the New Subnet dialog displayed in figure 5-47. The existing subnet IP address and subnet mask will be displayed. Make the modifications required in this dialog then click the OK button to make the changes.
- **Remove** Selecting an existing subnet from the **External Subnet** listing then clicking the **Remove** button deletes the sunbet from the list.

### In Band tab

The **In Band** tab **Home State** box, shown in figure 5-48, shows the switching modulator device's home state:

- Frequency
- Bitrate
- Power

You can enter new values, as required, for each of these parameters in the dialog box associated with the parameter.

Home State		
Frequency	Bitrate	Power
14.261GHz	512Kbps	17.5dBm
Modulator 1 on [		Select
Downlink Modulati	or	
		Select
Uplink Demodulato	or	
	n Burst Controller	Select

Figure 5-48 In Band Tab, Subnet Properties

Clicking on the **Extra** tab displays the Modem Extra dialog shown in figure 5-49, allowing the operator to set the type of Modulation, FEC Rate, and Code Type for the unit's home state.

FEC & Modula	ation
Modulation	QPSK.
FEC Rate	3/4 Rate
FEC Type	Turbo

Figure 5-49 Modem Extra dialog

These settings can be modified by clicking on the desired parameter and choosing a new setting from the pull-down menu that appears.



Figure 5-50 Modify, Modem Extra



**Note:** During initial unit registration the set information in the modem is propagated to the VMS database which fills in the Home State values.

The **In Band** tab also identifies the switching **Modulator** (the remote data modulator) for the subnet, **Downlink Modulator** is the hub forwarding (outbound) TDM modulator to remote (used for Roaming applications) and the **Uplink Demodulator** is the Home State hub demodulator (typically is the STDMA demodulator). These associated devices set the known states for recovering remote data units.

Clicking the **Select** button brings up the **Select Modem** dialog shown in figure 5-51.

Select Modem	×
Name	OK
Modulator 1 on R2 DATA	Cancel

Figure 5-51 Select Modem dialog



**Note:** If the demodulator field is blank either the burst controller or remote flags are incorrect or the remote is not registered.

Clicking the **Select** button in the **Uplink Demodulator** box displays the **Select Demodulator** dialog shown in figure 5-52.



Figure 5-52 Select demodulator dialog.

Using this dialog you can select a different demodulator for the subnet to replace the existing demodulator. Clicking the **OK** button will change the selection.



**Note:** Home State Demodulators are associated and linked by transmission settings, frequency, data rate, modulation and FEC rate. If changing system selected unit to another will require manual tuning and realignment of remote unit configurations.

### Policy tab

The check boxes at the top of the **Policy** tab shown in figure 5-53 default to the InBand Manager settings, but can be locally enabled or disabled as follows:

- If the boxes are greyed and checked, global policies are in use.
- If the boxes are white and unchecked the feature is disabled.
- If the boxes are white and checked local policies are in use.

These policy states for each switching mode can be selected by clicking on the boxes until the desired policy state for that switching mode is displayed.

In the **Bitrate Limits** box, values for **Minimum**, **Maximum** and **Excess Bandwidth** can be defined based on a particular remote's link budget and requirements.

The application policies displayed in the **Application Policies** box are created using the **Insert** command. Refer to the section "Application Policies" on page 5-20 for more detailed information on setting policies.

eneral In Band	Policy	Distribution Lis	sts S.A.S.	
Enable	Applic	ation Policies		
🗹 Automatic	Тур	e Minimum	Maximum	
Coad	1 2 2 2 3	16Kbps	2Mbps 128Kbps 512Kbps	
Minimum Bitrate		ŝ.	3	
8Kbps				
Maximum Bitrate				
2Mbps				
Excess Bitrate				
16Kbps				
QP5K, 3/ 4, Turbo Modem	1			

Figure 5-53 Policy Tab, Subnet

Selecting an existing application policy, as shown in figure 5-53, and then clicking directly on one of the parameters allows you to modify the policy for the selected policy type. However, an existing policy cannot be removed from the Subnet site level; an application policy can only be removed from the InBand Manager global level.

Advanced modem settings for a switch type can be configured by clicking on the **Modem** button and modifying the Modem Extra parameters. These settings temporarily override the home state settings, and only apply when this switch occurs.

If the Modem button is inactive (greyed-out), it will be necessary to return to the In Band tab and open the Select Modem dialog (figure 5-51), then select the desired modem. The Modem button in the Policy tab will now be active.

### **Distribution Lists Tab**

**Distribution Lists** are used to define the target subnets for point-to-multipoint 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 created at the global system level (InBand Manager), but can be either modified or disabled here at the site level to accommodate specific site requirements.

Opening the Distribution Lists tab for a subnet will display the global lists that were created using InBand Manager, as shown in figure 5-54.



Figure 5-54 Distribution Lists Tab, Subnet

The enable/disable check boxes for the existing lists are greyed and checked, indicating that global settings are in effect. At the subnet level, these lists can be altered by clicking on the box until the desired state for that list is displayed:

- Click once to uncheck (disable) the list for this subnet.
- Click twice to check white box for list to be modified for this subnet.

The figure below shows that the second distribution list has been altered to allow its modification for this site.

,	10.1.128.0/24		? ×
G	eneral   In Band   P	olicy Distribution Lists	
	Destination	Name	-
	10.1.131.0	R2-R4	
	224.10.20.25	Multi-Test	

Figure 5-55 Distribution List Enabled for Site Modification

Right-clicking on an existing list displays a choice to either **Insert** a new list, **Modify** this list, or **Remove** this list.



Figure 5-56 Modify Site List

In this example, the Modify command is selected, opening the **Distribution** List window shown in figure 5-57.

224 . 10 . 20	, 25	_	ОК
Name			Cancel
Multi-Test			
Site List			
Site			Add Site
10.1.128.0/24			
10.1.130.0/24		<u>R</u> e	move Site
10.1.131.0/24			
10.1.132.0/24			

Figure 5-57 Distribution List Window, Site Modification

Here, the list can be modified by adding and/or removing sites from the list. To add a site, click on the **Add Site** button and follow the procedure outlined in section "Distribution Lists Tab" on page 5-22. To remove a site, select the desired site and click on the **Remove Site** button.

Once all modifications for the list have been completed, click on the **OK** button to save the changes.

When VMS ViperView starts, the top view displays the installed services as shown in figure 5-58. Each of these services is discussed in the following sections.

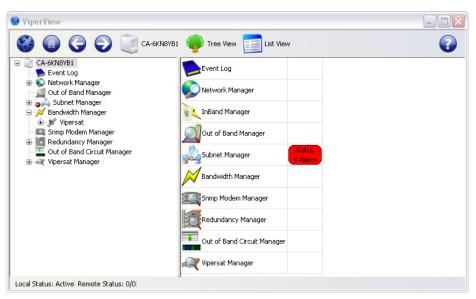


Figure 5-58 ViperView top view

- Vipersat Manager
- Subnet Manager
- SNPM Modem Manager
- Bandwidth Manager
- InBand Manager
- Network Manager.

{ This Page is Intentionally Blank }

ViperView

# **C H** A **P T E R**

# 6

# **OUT-OF-BAND UNITS**

# General

This chapter describes integrating out-of-band 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 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** Manager

The SNMP Modem Manager is the controlling service for all out-of-band modems. Right clicking on the manager icon opens a list which allows you to open the manager, declare modems, Save the entries and view the properties page. The properties page is shown below in figure 6-2.

📧 Snmp Modem Manager 🛛 💽 🗙
General
Polling Options Full Interval Status Interval Timeout 15s Status Interval Timeout 10s Switching Options Guardband 35%
OK Cancel Apply

Figure 6-1 SNMP Modem Manager

There are 4 settable parameters in the SNMP Modem Manager properties. They include the full interval poll, the status interval poll, the timeout and the allocation factor for carriers referred to as the guardband. 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.

• Timeout:

The time in seconds it will take before VMS times out on a command. Since 3 retries will be made before failing the timeout is actually the time listed multiplied by 3.

Guardband

The percent of allocation applied to carriers when switched by VMS. The default is 35% allowing for an allocation factor of 1.35.



**Note:** Currently this carrier guardband setting for OOB is separate from the inband setting under the <u>Vipersat Manager</u> and **must be** set to the same value.

The following procedure demonstrates using the SNMP Manager using a CDM-600L as an example.

1. From ViperView, right-click on the SNMP Manager to display the dropdown menu shown in figure 6-2.

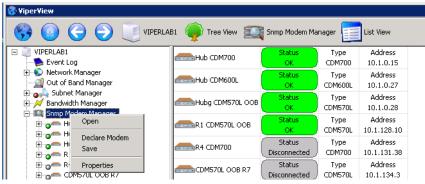


Figure 6-2 Declaring a CDM-600L

**2.** Select the **Declare Modem** command from the drop-down menu to display the **New SNMP Modem** dialog shown in figure 6-3.

New	CD	MG	001					×
IP	Add	lres	s					
Г	0	•	0	•	0		0	
	IΡ	Sub	net	Ma	sk			
	0	•	0	•	0		0	
	(	ЭК				Car	icel	

Figure 6-3 CDM-600L IP address dialog

- **3.** From the **Unit Type** drop-down menu select the modem type to be declared. In this example the CDM600L modem is selected.
- **4.** Enter the assigned IP address in the **IP Address** dialog box shown in figure 6-4.



Figure 6-4 New SNMP modem dialog

- **5.** The unit will now appear listed in the SNMP Modem Manager. Right click on the added unit and select **Properties** from the drop down menu to display the **General** tab shown in figure 6-5.
  - **a.** Assign a name to the CDM-600L in the top dialog box for reference.
  - **b.** The **IP Address** box is a read-only display of the IP address of the target CDM-600L. Add the Subnet Mask in the provided dialog
  - c. Insure the SNMP settings are correct. For a CDM600 the Read and Write communicties are **admin1234**. For all other devices the Read community is **Public** and the write community is **Private**.
  - **d.** If the CDM-600L is connected to a BUC, LNC or other device, select the **Enable Radio Devices** check-box to have this configuration recognized by VMS.

- Hub CDM600L ? 🗙
General
Hub CDM600L
IP Address
Subnet Mask 255 . 255 . 192 . 0
SNMP Settings
Read Community Write Community admin1234 admin1234
Enable Radio Devices
OK Cancel Apply

Figure 6-5 CDM-600L properties screen

Once a CDM-600L and its companion CiM-25 are configured and are connected to the network, the CDM-600L will appear in the SNMP Manager Manager as shown in figure 6-6.

😵 Yiper Yiew						
🚯 🙆 🤤 🕞 🧾 VIPER	RLAB1 🌍 Tree View 👝 H	ub CDM600L 🥜 Parameter View				
🖃 🥘 VIPERLAB1	System Information					
Event Log	Status	ок				
🕀 🌑 Network Manager	Equipment ID					
Out of Band Manager	Unit Serial Number					
🗄 👦 Subnet Manager	Software Version					
Bandwidth Manager	Device Time					
Snmp Modem Manager     Hub CDM700     Hub CDM500L     Hub CDM500L     G     G     Hub CDM50L OOB     R1 CDM570L OOB     G     R1 CDM570L OOB	Device Date					
	Circuit ID					
	Control	Local				
	Temperature	Oc				
	Interface Parameters					
CDM570L OOB R7     CDM570L OOB R7     CDM570 IF OOB	External Clock					
	Refrence Clock	Internal				
	Drop & Insert					
🗄 📶 Redundancy Manager	Drop Type					
Out of Band Circuit Manager	Drop Info	24 used timeslots				
🗄 🛶 🐺 Vipersat Manager	Insert Type					
	■Insert Info	24 used timeslots				
1	Tetereslisee					

Figure 6-6 SNMP Modem Manager

# **Parameter View**

The **Parameter View** display shown in figure 6-7, displays unit information and options available for the unit selected in the SNMP Modem Manager. The following discussion shows the type of information available, but you should refer to each unit's documentation for detailed information on setting or changing any of the parameters listed here.

The options available on the drop-down menu shown in figure 6-7 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. If you want the changes to be permanent, you must save the changes to the unit's flash memory.
- **Revert** If you make a change and want to revert to the previous setting, clicking the **Revert** command will revert the setting back to its original configuration.



Note: If you have marked the changed parameter by clicking the **Dirty Selected** command, the **Revert** command will not function.

- **Refresh** Clicking the **Refresh** command will read the current state of all parameters from the unit and display 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.

### General

😵 YiperYiew		
	AB1 🌍 Tree View 👝 Hu	ıb CDM600L 🥜 Parameter View
🖃 🤍 VIPERLAB1	System Information	Apply
- Event Log	Status	OK Revert
🗄 😒 Network Manager	Equipment ID	Refresh
Out of Band Manager	Unit Serial Number	
🗄 👦 Subnet Manager	Software Version	
🗄 📈 Bandwidth Manager	Device Time	
🖻 📖 Snmp Modern Manager	Device Date	
Hub CDM700	Circuit ID	
Hub CDM600L	Control	Local
Hubg CDM570L OOB	Temperature	Oc
R1 CDM570L OOB	□Interface Parameters	
	External Clock	
	Refrence Clock	Internal
	Drop & Insert	
	Drop Type	
Out of Band Circuit Manager	Drop Info	24 used timeslots
🗄 🛶 Vipersat Manager	Insert Type	

Figure 6-7 Parameter View

Before continuing with this process, you should click the **Refresh** button on the drop-down menu shown in. This will ensure that you have the most current information available for the unit before continuing.

The information available in the **Parameter View** contains both information you can edit and information which is hard-coded in the unit which cannot be changed.

This can be useful for out-of-band units allowing you to modify their configuration using the VMS.

# Configuring the RF Chain

The following procedure shows how to configure the SNMP Modem's RF chain and enable it for switching.

**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 6-8 below:

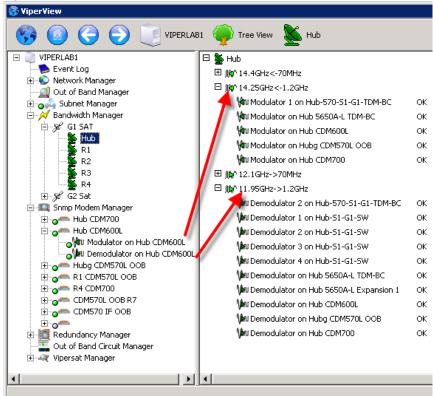


Figure 6-8 Configuring the RF Chain

- **2.** Drag and drop the modulator on to the up converter and the demodulator to the down converter.
- **3.** Right click on the antenna, click the properties page and select the Out of Band tab as shown in figure 6-9 below:

💁 Hub 🔹 🔋 🖸	×
Hub     Rx-Gain       General     Visibility     Out of band       Name     Rx-Gain       Hub     60dB       Operator     60dB       Operator     60dB       Contact Information     60 specified	
OK Cancel Apply	

Figure 6-9 Out of Band Antenna Tab

**4.** Highlight the Modulator for the new SNMP modem and click Enable as shown in figure 6-10 below:

Se Hub	? ×
General Visibility Out of band	
Name	Config
Modulator on Hub 5650A-IF Ex	Disabled
Modulator 1 on Hub-570-S1-G	Disabled
Modulator on Hub 5650A-L TD	Disabled
Modulator on Hub CDM600L	Disabled
Modulator on Hubg CDM570	-8dBm@512Kbps
Modulator on Hub CDM700	-15dBm@2Mbps
Enable Disable	Properties
ОК	Cancel <u>Apply</u>

Figure 6-10 Selecting	the	Out o	f Band	Modem
-----------------------	-----	-------	--------	-------

**5.** A dialog box will open prompting for a bit rate and power. VMS uses this to calculate correct power settings for any bit rate the out of band link will

switch to. Set them to a combination that will give an appropriate level. The dialog box is shown in figure 6-11. These two values set the base levels from which all SCPC switched modifications are referenced for this unit.

Example, if the set power of -28dBm was calibrated to represent a satellite link of 10dB  $E_b/N_o$  and the VMS modified (switched) the carrier bit rate from 256k to 512k the modulators power would change from -28dBm to -25dBm respectively.

Dialog	×
Bit Rate 256Kbps	ОК
Power	Cancel
-28dBm	Extra

Figure 6-11 Out of Band Dialog Box

# Overview

SNMP controlled modems are defined as Out-of-Band in the VMS. This means the traffic interface for these modems is not part of the IP infrastructure the Vipersat Network belongs to.

SNMP modems use either a serial traffic interface such as V.35 or G.703, a bridged GiGE interface (in the case of the CDM700s) or an IP interface which is isolated from the local area network native to the Vipersat Network (in the case of OOB CDM570 modems in managed switch mode).

VMS communicates with SNMP modems at remote sites through a TDM/ STDMA Vipersat overlay. A sample of this topology is shown below in figure 6-12

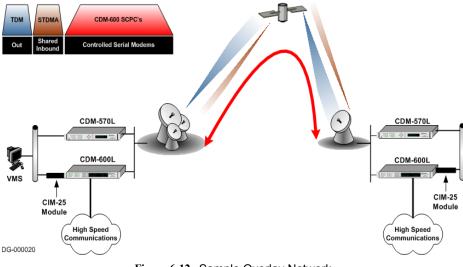


Figure 6-12 Sample Overlay Network

# Out of Band Circuit Manager (OBCM)

One of the methods available for switching out of band modems is the OBCM. Using the OBCM the operator can create channels with fixed modems and channel rates. These channels can currently be manually switched as will be illustrated below. In a future version of VMS this capability will be automated. SNMP traps will be passed by the SNMP modem manager to the Out-of-Band Manager to establish the predefined circuits.

# **Configuring the OBCM**

If the steps above for configuring the RF chain have been completed the following procedure can be used to configure the OBCM. This also assumes that each of the OOB units have been correctly declared and associated with there proper antenna components.

**1.** Open the Out of Band Circuit Manager by left clicking on the icon in the tree view as illustrated in figure 6-13.

🖏 YiperYiew									
😵 🙆 🤤 🌍 🧾 VIPERLA	81 🧃	🕐 Tree View 📰 Ou	it of Band Ciri	:uit Manager					
🖃 🧾 VIPERLAB1	Id	Name	Status		Hub Modem	Remote M	Bit Rate	Priority	Group
- 🛸 Event Log	1	CDM570 Channel	Idle		10.1.0.28	10.1.128.10	512Kbps	2	1
🗄 🌑 Network Manager	2	CDM700 Circuit 1	Idle		10.1.0.15	10.1.131.38	2.5Mbps	1	1
- 🛒 Out of Band Manager									
🗄 🚕 Subnet Manager			-						
🗄 📈 Bandwidth Manager				Create Ch	iannel				
🗄 📖 Snmp Modem Manager				Refresh					
🗉 📶 Redundancy Manager				Refresh					
Out of Band Circuit Manager		-							
🕀 💐 Vipersat Manager									
	Right Click on white area to bring up the tab to create a new channel								

Figure 6-13 Out of Band Circuit Manager

**2.** Select "Create Channel" to open up the dialog below.

Channel Settings	X
Id Name 0 New Channel	
First Modem 10 . 1 . 0 . 50	Second Modem 10 . 1 . 128 . 31
Channel Bit Rate 1024bps	Priority Group
	OK Cancel

Figure 6-14 Channel Configuration

**3.** The following parameters must be set:

- A channel ID. This must be unique within the system
- A channel name

### Switching SNMP Out of Band Modems

- IP address of the first modem
- IP address of the second modem
- A channel bit rate
- The channel priority (will be used in future release)
- The Group number (used in conjunction with the channel priority.
- **4.** Once the channel is configured it will be possible to manually switch it. Right click on the channel and select "Setup" from the drop down menu. This menu also allows the operator to revert an active channel, to edit the channel parameters and to delete the channel. figure 6-15 illustrates this.

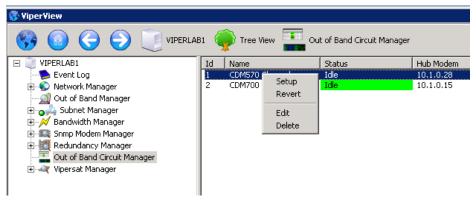


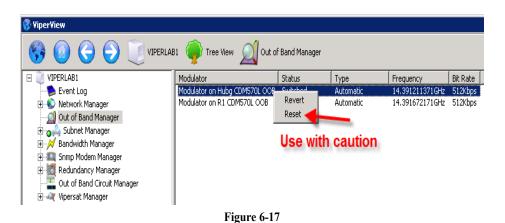
Figure 6-15 Setting up an OBVM Circuit

5. Once the channel sets up the channel will show an active status.

😵 YiperView				
😽 🙆 🤤 ラ 🧾 VIPERLAI	81 🤇	Tree View	Out of Band Circuit N	lanager
🖃 🧾 VIPERLAB1	Id	Name	Status	Hub Modem
Event Log	1	CDM570 Channel	Active 🚤	10.1.0.28
🗄 較 Network Manager	2	CDM700 Circuit 1	Idle	10.1.0.15
🛒 Out of Band Manager				
🗄 👝 Subnet Manager				
🗄 📈 Bandwidth Manager				
🗄 👹 Redundancy Manager				
Out of Band Circuit Manager				
🗄 🛶 Vipersat Manager				

Figure 6-16

**6.** While the circuit is active the switched modems will appear in the Out-of-Band Manager display. If, for some reason, communications is lost with the remote modem right clicking on the hub modem will allow the operator to free up the bandwidth resources by selecting Reset. Unless you are certain the remote modem is no longer transmitting do not free up its resources as it will then act as a foreign carrier in the network.



7. If you attempt to do an OBCM switch and it fails it is most probably a misconfiguration of the out of band modems (check the antennas to insure they are enabled), insufficient bandwidth or other errors in the RF chain.

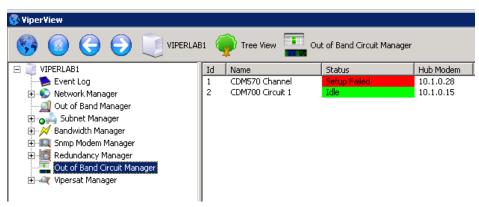


Figure 6-18

# Vipersat Circuit Scheduler

Another way of switching SNMP Out-of-Band modems is with the Vipersat Circuit Scheduler. If you have purchased this option see the manual for instructions on scheduling Out of Band switches.

You will still need to follow the instructions above through Configuring the RF chain for the VCS to work.

#### **A P P E N D I X**



# 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.

C-Band 24 36MHz transponders

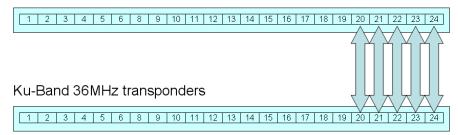


Figure A-1 Cross Banded Transponders, C-band & Ku-band

# Vipersat Cross Banding Solution

Figure A-2 illustrates a schematic representation of a cross banded satellite network.

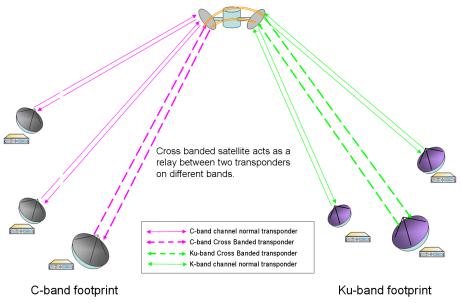


Figure A-2 A Cross Banded Satellite Network

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:** 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.

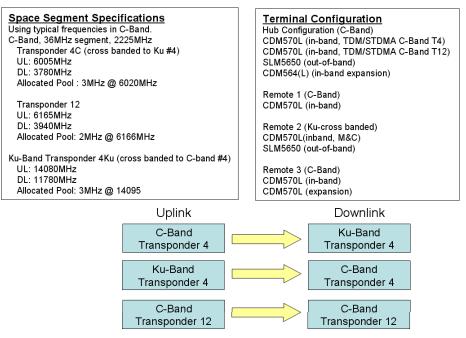


Figure A-3 VMS Cross Banded Network Configuration

- 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.

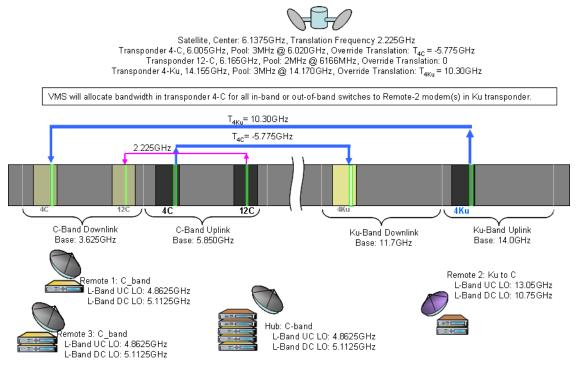


Figure A-4 VMS Cross Banded Network Solution

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.

Jame C to KU	Gain Variation OdBm
Frequency Range Center Frequency 6.2GHz Bandwidth Span 36MHz	Translation Override -5.775GHz

Figure A-5 Transponder dialog, C to Ku

lame	Gain Variation
KU to C	OdBm
Frequency Range	
Center Frequency	
14.36GHz	
Bandwidth Span	Translation Override
36MHz	10.3GHz
2	

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.

#### **A P P E N D I X**

# 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 bandwidth 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.

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.

	Bandwidt	h	- 6
500GHz	1THz		

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.

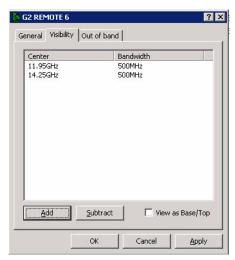


Figure B-2 Ku-band Visibility Ranges, Center/Bandwidth

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.

Base		Тор	
11.7GHz 14GHz		12.2GHz 14.5GHz	
	Subtract		iew as Base/Toj

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-

#### Using Antenna Visibility

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.

Frequency Range	×	Frequency Range	
Center		Base	
500GHz		OHz	
Bandwidth	Cancel	Ter	Cancel
1THz	View as Base/Top	Top 1THz	View as Base/Top

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.

Base	Top
11.7GHz 12.105GHz	12.1GHz 12.2GHz
14GHz	14.5GHz
Base 12.1GHz	Range X
Base 12.1GHz Top	OK Cancel
Base 12.1GHz	OK Cancel

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.

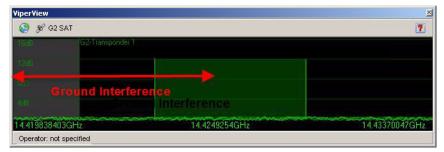


Figure B-6 VMS Bandwidth Pool with Ground Interference

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.

ViperView				j
🔇 🖋 G2 SAT				7
16dB				
	100			
14.423272465GHz	oon mari	14.426528143GHz	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	14.430369844GHz
Operator: not specified				

Figure B-7 Transmit Carriers, No Visibility Block

#### Using Antenna Visibility

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.

G2 REMOTE 5			? X
requency Range		×	
Base 12.1245GHz Top 12.1255GHz	— OK Cancel ✓ Miew as Base/Top		
Add	jubtract	□ View as Ba	se/Top
······			

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.

Base	Тор
11.7GHz 12.1255GHz 14GHz	12.1245GHz 12.2GHz 14.5GHz
Add Sul	btract

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.

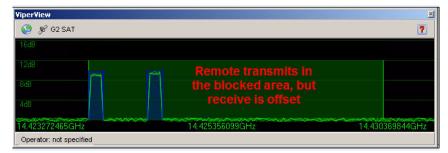


Figure B-10 Transmit Carriers Repositioned, Visibility Block

Using Antenna Visibility

{ This Page is Intentionally Blank }

#### **A P P E N D I X**



# 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) colocated 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.

# Description

VMS redundancy (protection) increases the system availability of a Vipersatenabled 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.

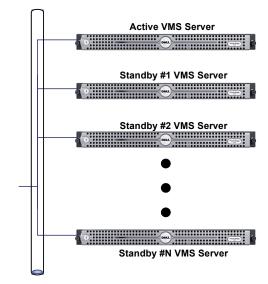


Figure C-1 Active and Standby VMS Servers, N:1 Redundancy

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-12.

#### **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 is lost and a manual synchronization is required to ensure that the standby receives the most current database from the active server.

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 clear-

ing server contention, refer to the section "Clearing Server Contention" on page C-12.

#### 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.

🍪 ¥iper¥iew		_ 🗆 ×
🇐 🏠 🔮 🤣	VIPERLAB1 👳 Tree View 🧮 List View	2
UIPERLAB1	Open idth Manager	
E Snmp Modem Manager ⊕ Snmp Modem Manager ⊕ S Network Manager	Backup Restore Modem Manager	
⊕Subnet Manager ⊕	Synchronize d Manager	
Out of Band Manager	Properties rk Manager	
	Subnet Manager	
	Received Wipersat Manager	
	Event Log	
	Out of Band Manager	
	Circuit Restoration Service	
	Redundancy Manager	
Local Status: Active Remote Statu	J Is: Connected	

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.

Server Up Time: 10 days, 1 hours, 23 min	iutes, 59 seconds
Redundancy	
Local Status: Standby Z Enabled IV Auto Activate	
Redundant Servers	Priority
Address	0
10.1.1.3 10.1.1.1	Retry Delay 500ms
	, Retry Count 10
Add Modify Remove	Failover Time

Figure C-4 VMS Server Properties, General Tab

4. Configure the redundancy settings for this server.

The **General** tab provides redundancy information on the server role and local status, and current server redundancy settings which can be edited as required.

#### 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.

#### **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.

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.

Failover Time

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 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.
- **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-5, 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.

6. When finished, click the OK button to save the server properties settings.

General Traps			? ×
SNMP Manager (TRAP	<b>D</b> .	<u> </u>	
Address 192.168.150.150 192.168.150.180	Port 162 162	Community public public	
<u>I</u> nsert	<u>M</u> o	odify	<u>R</u> emove
OK		Cancel	Apply

Figure C-5 VMS Server Properties, Traps Tab

- 7. Repeat steps 2 through 5 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.

😚 YiperYiew		
🚱 🏠 🄇 🤣	🗾 VIPERLAB1 🍕	Tree View
VIPERLAB1     Event Log     Event Log     Out of Band Manager     Subnet Manager     Subnet Manager     Manager     Snmp Modem Manager     Vipersat Manager     Channel Table Switching	Open	Event Log
	Backup Restore	Network Manager
	Activate	InBand Manager
	Licensing	
	Properties	Out of Band Manager
		Subnet Manager
		Bandwidth Manager
		Snmp Modem Manager
		Reg Vipersat Manager

Figure C-6 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.

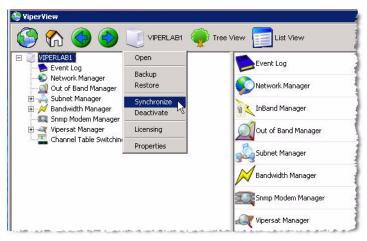


Figure C-7 Synchronize Command, VMS Server Menu

This concludes the procedure for installing and configuring the VMS redundancy servers.

#### VMS Redundancy

- 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.

## 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.

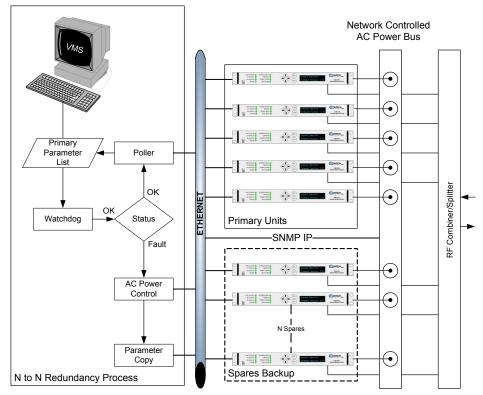


Figure C-8 N:M redundancy logic diagram

The switching control mechanism is completely monitored and controlled by the host master processing VMS as shown in the logic diagram in figure C-8. 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-34, 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-15, the VMS starts listening for heartbeat 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-8. 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 a Failed Unit Back into Service" on page C-33.

## 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<sup>™</sup> 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

#### N:M Hub Modem Redundancy

- 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-15, 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-9.

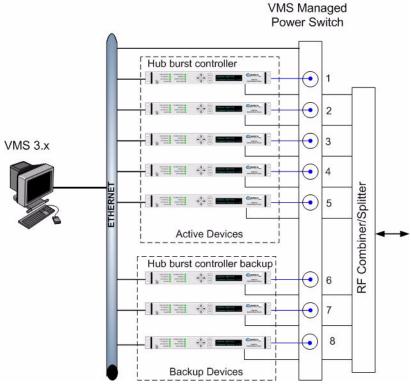


Figure C-9 N:M block diagram

#### Sample installation

Figure C-10 shows a diagram of a sample installation of an N:M redundant VMS installation. As shown in figure C-10, the units in the primary and secondary groups share a common Ethernet LAN with the IP controlled power switch.

#### N:M Hub Modem Redundancy

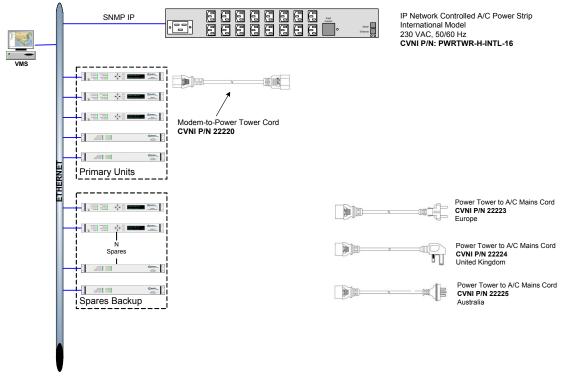


Figure C-10 Typical N:M redundant installation

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-10. Refer to these manuals for detailed information on this device.



**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-11. They are:

- 1. Redundancy Manager
- 2. Containers
- 3. Power Strips and Groups



Figure C-11 N:M Redundancy Hierarchy

Expanding the Redundancy Manager icon, shown in figure C-12, shows a typical N:M redundancy installation. Under the Redundancy Manager service icon are the icons for a container named Hub, in this example.

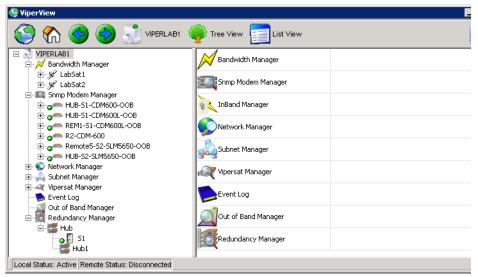


Figure C-12 Redunancy Manager Tree

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 rightclicking on it, as shown in figure C-13, the operator can enable device redundancy, create the main container for the site, and backup or restore the redundancy service.

🍪 ViperView			
🌍 🏠 🔇 🤣 🕺 VIPERLABI 🏺 Tree	View 🗾 List View		
VIPERLAB1     Bandwidth Manager	Bandwidth Manager		
Somp Modern Manager      Some Network Manager      Some Network Manager	Snmp Modem Manager		
🔁 🛁 Subnet Manager 🔁 🔐 Vipersat Manager — Devent Log	InBand Manager		
Out of Band Manager Redundancy Manager Open	Network Manager		
✓ Enabled	Subnet Manager		
Create Container	Vipersat Manager		
Backup Restore	Event Log		
	Out of Band Manager		
Local Status: Active Remote Status: Disconnected			

Figure C-13 Redundancy Manager Drop-Down Menu

#### **Create Container**

Selecting **Create Container** from the drop-down menu in figure C-13, brings up the **Create New Redundancy Group** dialog shown in figure C-14. Clicking the OK button creates a container with the name assigned in this dialog.



Figure C-14 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-15.

🅞 ViperView		
🌀 🏠 📀 🌏 📑 VIPERLAB1	Tree View 📰 List View	?
E VIPERLAB1	Bandwidth Manager	<b></b>
⊕ 🚉 Snmp Modem Manager ⊕ 🕥 Network Manager ⊕ 🚕 Subnet Manager	Snmp Modem Manager	
Wipersat Manager      Event Log	InBand Manager	
Out of Band Manager	Network Manager	
Dpen	Subnet Manager	
Create Group Create Strip	Vipersat Manager	
Create Container	Event Log	
Rename	Out of Band Manager	<u> </u>
Delete		Þ
Local Status: Active Remote Status: Disconnected		

Figure C-15 Group drop-down menu

Once the container is created, right-clicking on its icon brings up the drop-down menu shown in figure C-16.

🅞 ViperView		
🌍 🏠 🔇 🌍 式 VIPERLAB1	Tree View E	2
Bandwidth Manager	Bandwidth Manager	
Somp Modem Manager      Somp Modem Manager      Subnet Manager      Subnet Manager	Snmp Modem Manager	
<ul> <li>Briggs Subnet Manager</li> <li>Briggs Wipersat Manager</li> <li>Briggs Event Log</li> </ul>	InBand Manager	
Out of Band Manager	Network Manager	
Open	Subnet Manager	
Create Group Create Strip	Wipersat Manager	
Create Container	Event Log	
Rename 	Out of Band Manager	
Local Status: Active Remote Status: Disconnected		

Figure C-16 Group drop-down menu

#### Power Strips

Selecting **Create Strip** from the drop-down menu shown in figure C-16, displays the New Power Strip dialog shown in figure C-17.

New Power Strip
Name unnamed
Address Type
Read Community         Write Community           public         private
OK Cancel

Figure C-17 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-17. 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-18.

VIPERLAB1	Port	Role	Power	Activity	Device	Status
🗐 🔁 Event Log	1	None	Off	Idle	(none)	N/A
🗄 💿 Network Manager	2	None	Off	Idle	(none)	N/A
Out of Band Manager	3	None	On	Idle	(none)	N/A
Subnet Manager	4	None	On	Idle	(none)	N/A
	5	Primary	On	Idle	SPARE-564L #1 (.30)	Unkn.
	6	Backup	On	Idle	SPARE-570L #1 (.29)	Ok
🗇 👦 🖓 Group 1	7	Backup	On	Idle	SPARE-570L #2 (.28)	Ok
⊕ om HUB-S1-CDM600-OOB	8	None	On	Idle	(none)	N/A
⊕ om HUB-S1-CDM600L-OOB	9	None	On	Idle	(none)	N/A
🕀 👦 🛹 Hub S1-G1-Quad	10	None	Off	Idle	(none)	N/A
🗄 👝 🛹 SPARE-570L #1 (.29)	11	None	On	Idle	Hub-S2-G2-BC	Ok
E CDM-570-G1-OOB	12	None	On	Idle	(none)	N/A
Hub-S1-G1-TDM-BC	13	None	On	Idle	(none)	N/A
	14	Primary	On	Idle	Hub-S1-G1-TDM-BC	Ok
	15	None	Off	Idle	(none)	N/A
🗄 👷 Group 2	16	None	Off	Idle	(none)	N/A
🗄 💽 Remotes						
🔃 📈 Bandwidth Manager						
连 🚉 Snmp Modem Manager						
🖻 📶 Redundancy Manager						
🖻 🔛 Hub						
51-G1						
52-62						

Figure C-18 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-16 and select **Create Group** from the drop-down menu. This next group will represent the redundancy group for a given satellite or network.

reate New Re	dundancy Group	
Name		
E.		-
	OK	Cancel

Figure C-19 Create Group dialog

Once the group is created, drag the port to the group sub-container as shown in figure C-20. Group sub-containers can have entries from multiple strips.

VIPERLAB1	Port	Role	Power	Activity	Device	Stat
🚊 📈 Bandwidth Manager	1	None	Off	Idle	(none)	N/A
É % LabSat1	2	None	Off	Idle	(none)	N/A
± % LabSat2	3	None	Off	Idle	(none)	N/4
🕀 🔍 Snmp Modem Manager	4	None	Off	Idle	(none)	N/4
Network Manager	5	None	On	Idle	(none)	N/A
	6	Backup	On	Idle	SPARE-570L #1 (.29)	Ok
🖻 💑 Subnet Manager	7	Backup	On	Idle	SPARE-570L #2 (.28)	Fat
🖻 💁 Hub	8	None	On	Idle	(none)	N/A
🛱 👦 💑 Group 1	9	None	On	Idle	(none)	N/A
HUB-S1-CDM600-OOB	10	None	Off	Idle	(none)	N/A
HUB-S1-CDM600L-OOB	11	None	On	Idle	(none)	N/A
🕀 👝 🛲 Hub S1-G1-Quad	12	None	On	Idle	(none)	N/A
🕀 🚰 Hub-S1-G1-TDM/BC	13	None	On	Idle Idle	(none)	N/A
	14	Primary None	On Off	Idle Idle	Hub-S1-G1-TDM/BC (none)	Ok
🗄 🚰 SPARE-570L #1 (.29)	16	None	Off	Idle	(none)	N/A N/A
E of the state of	10	NONE	OIL.	TUIC	(none)	1474
E or Remotes						
🗄 📲 Vipersat Manager						
Event Log						
Out of Band Manager						
🖻 🔯 Redundancy Manager						
🖻 🔚 Hub						

Figure C-20 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-21. Check the **Enable Heart Beat** box.

#### N:M Hub Modem Redundancy

	HUB - SLM5650A	? ×
General Configurations Security	General Configurations Name HUB - SLM5650A IP Address 10 . 1 . 0 . 22 Subnet Mask 255 . 255 . 192 . 0 Auto Home State Timeout (min) 4 FIPS Blocks Per Frame 0 FIPS Blocks Per Frame	
OK Cancel Apply	OK Cancel	Apply

Figure C-21 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-22, check the **Primary Heartbeat** box. Click the **OK** button to continue.

CDM570L Configuration	<u>? ×</u>
Maintenance         Mngd Switch           Access         Admin         Compression           SMTP         SNMP         STDMA	Network QoS Routing DES DPC Home IGMP Switching Vipersat VLAN
Role Designation	Receive Multicast Address:
Expansion Unit	Hecetive Multicast Address: 239 . 1 . 2 . 4 Heart Beat  V Enable SOTM
Carrier Inhibit Timer: Osec	
Network Id: 2 Node name: Hub-570-S1-G1-T	Database: 1.5.4 DM-BC
	OK Cancel

Figure C-22 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-23 to enable HeartBeat messaging.

OMTEC	H Info	Admin	Modem	LAN	WAN	Routing	Stats	Vipersat		
EF DAT							<u>at   STDMA</u> ing   <u>DPC  </u>	<u>Stats</u>   Home State		
Vipersat Hub										
Vipersat	Hub									
		R	ole Hub	•						
General										
		Node Na	me Standar	d Vipersat					Network ID	2
	Receive M	ulticast Addre	ess 239.1.2.4	1				Managing	IP Address	10.1.
Hub Red	lundancy									
		HeartBe	eat C Disab	oled <ul> <li>Enable</li> </ul>	abled 🔶		_			
Same and the second second				an an chain an	and an all the state	Subr		a ann an an an		he have a

Figure C-23 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-33.

🅞 YiperYiew							_ 🗆 ×
🌍 🏠 📀 🌍 🧾 VIPE	ERLABBA	к 🌍	Tree Viev		Hub1		2
🖃 🚮 VIPERLABBAK	Port	Role	Power	Activity	Device	Status	8
⊕ - X Bandwidth Manager ⊕ - IIII Snmp Modem Manager	3 4	None None	On On	Idle Idle	(none) (none)	N/A N/A	
S Network Manager Subnet Manager C Subnet Manager C Subnet Manager C Stand Manager Redundancy Manager Hub S1 Hub S1	6 7 14	Pri	Config Back Config Rest Vone Primary Backup Clear Devic Switch On Switch Off		SPARÉ-570L #1 (.29) SPARE-570L #2 (.28) Hub-51-G1-TDM-BC	Ok Ok Ok	

Figure C-24 Role selection

Roles are either **None**, **Primary** or **Backup**. From this drop-down menu shown in figure C-33, 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-33.

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-25 stores these configuration files in the directory path: *C:\Program Files\Vipersat\VMS\3.0\bin\Device Redundancy*.

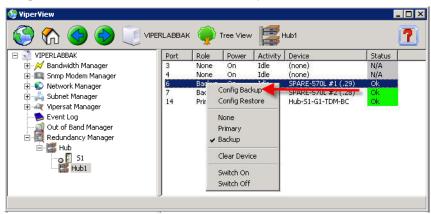


Figure C-25 Configuration backup

# **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-26.

<b>cdm570l-10.1</b>			? ×
	urations	and the second	
Name	Size	Modified	
New	Properties	Backup	Import
Delete	Edit	Restore	Export
	OK	Cancel	Apply

Figure C-26 Configuration tab

Click the **New** button, shown in figure C-27 which will open the **New Configuration** dialog shown in figure C-27.

me		ОК	
PARE#1 (.28)		Cancel	4/28/2
	/		
4	/		
New	Properties	Backup	Import
New     Delete	Properties Edit	Backup Restore	7

Figure C-27 New configuration dialog

Give the configuration file an appropriate name in the **New Configuration** dialog in figure C-27 and click the **OK** button. Then highlight the file name as shown in figure C-28 and click the **Backup** button.

HUB-TDM-S	TDMA-G1 (.16)	<u>Size</u> O	<u>Modifie</u> 5/10/2
d		-	
New	Properties	Backup	Import

Figure C-28 Creating a backup configuration file.

By default the file will be saved in the location shown in figure C-29.



Figure C-29 Saved file location

Storing Spare Configurations in the 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-30 and importing the file from the directory shown in figure C-31.

		Size	Modifie
HUB-TDM-S SPARE#1 (.2 SPARE#2 (.2		0 0 0	5/10/2 4/27/2 5/10/2
			1
<u>،  </u>			
∢   New	Properties	Backup	Import

Figure C-30 Importing file

Select the appropriate file from the list:

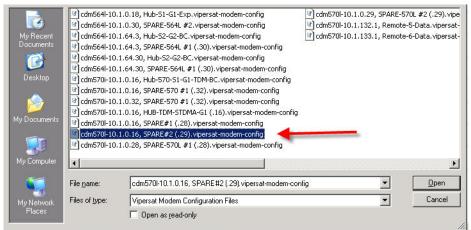


Figure C-31 Selecting file

# Preparing the 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 the 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.

	rdma-g1 (.16)	Size	Modifie 5/10/2
SPARE #1 (2 SPARE #2 (.2		0 0	4/27/2 5/10/2
I∎] New	Properties	Ватир	Import

Figure C-32 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 a 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.

#### N:M Hub Modem Redundancy



**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-33, enter the unit's features and unlock codes.

Feature Configuration					
Pinq Reply	.[Enabled]F				
Telnet	.[Enabled]				
SNMP	.[Disabled]				
	[Disabled]				
Downlink Route All Available Multicast.	[Disabled]				
	.[Enabled]				
	[Per Route]				
Receive 3xDES Decryption	[Available]				
Tx Header Compression	.[Per Route]				
Rx Header Compression	[Disabled]				
	.[Per Route]				
Rx Pauload Compression					
	.[341:C32C-8360-7342:5.02]F				
Vipersat Management					
	.[Enabled]				
	.[Enabled]				
Exit					

Figure C-33 Feature configuration page, CDM-570/570L

- 3. Disable STDMA
- **4.** On the **Administration** page shown in figure C-34, set the **Working Mode** to **Router Vipersat**.

Administration
Name/Password Configuration
Save Parameters to permanent storageS ExitX Telnet LogoutL

Figure C-34 Administration page, CDM-570/570L

**5.** Using the Internet Interface page shown in figure C-35, 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.

Ethernet Interface	
1AC Address	
אר Hudress	[
IF HUURESS	
Subnet Prefix Length[24 ]	1
ink Status[Auto - Neg Done For 100-Full Mode Link UP]	
Save Parameters to permanent storage	
xit	
[elnet Logout	
cance Logode	

Figure C-35 Ethernet Interface page, CDM-570/570L

- **6.** On the Vipersat Configuration page shown in figure C-36, set the **Unit Role** to **Hub Expansion**.
- 7. This completes setting the unit to the Passive 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.

Vipersat Configuration
STDMA ModeT
Automatic SwitchingA
Jnit Role
Expansion Unit
letwork ID
Jnit Name
Receive Multicast Address[239.4.5.6]
lanaqinq IP Address
Primāry Heart BeatPisabled]P
Dynamic Power Control Config
Set Home State Parameters
Jipersat SummaryD
Save Parameters to permanent storageS
xitX
[elnet LogoutL
-

Figure C-36 Vipersat configuration page, CDM-570/570L

8. On the Satellite Modem > Configuration > Configuration > Tx Configuration page shown in figure C-37, disable the unit's transmit capability by changing the Tx Carrier to [Off].

1

Tx Configuration
Tx Frequency
Tx Symbol Rate[0682.667] Tx FEC[Turbo]T
Tx Code Rate[3/4]
Tx Spectrum Inversion[Normal]U Tx Data Inversion[Normal]I Tx ScramblingB
Tx Power Level
Tx Clock Source[Internal]
Save Parameters to permanent storageS
ExitX Telnet LogoutL

Figure C-37 Transmit configuration page, CDM-570/570L

**9.** On the Satellite Modem > Configuration > Configuration > Rx Configuration page shown in figure C-38, set the **Rx Frequency** to the low end (50 or 950).

	Rx Configuration
Rx	Frequency
	Data Rate
Rx	Symbol Rate
Rx	FEC[Turbo]
Rx	Code Rate
Rx	Demodulation
Rx	Spectrum Inversion[Normal]
Rx	Data Inversion[Normal]I
Rx	Descrambling[On-Default]B
Rx	Acquisition Range[010]
	'No Alarm Point[02.0]P
Rx	Buffer Size[Disabled]F
Rec	enter Rx Buffer
Sav	e Parameters to permanent storageS
Exi	t
Tel	.net LogoutL

Figure C-38 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-39.

			Block Up	Convert	er (Bl	IC) Conf	igurati	.on	
	dress								
	Output								
BUC DC	Power			[Disabl	ed]				 
BUC 10	MHz Refere	nce		[Disabl	ed1				 
BUC Cur	rrent Alarm	Upper Lim	it (mA)	Î 3500	1				 
	rrent Alarm								
	Frequency								
				[ 00000	1				 
5 JUO P:	arameters to		t ctorado						
Save ra	arameters ti	, het manen	c scorage						 
CXIC									 
leinet	Logout								 

Figure C-39 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-40.

Low Nois	se Block Converter(LNB) Configuration
LNB 10MHz Reference LNB Current Alarm Upper Limit (m LNB Current Alarm Lower Limit (m	[0ff] [0ff] mA)[600] mA)[10]
Exit	orage

Figure C-40 LNB configuration, CDM-570/570L

- **12.** This completes the process of setting the VMS controlled modem to parked configuration mode and it 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.

# **A P P E N D I X**

# 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 you begin configuring your server as a domain controller, verify that:

- Make sure that the TCP/IP configuration settings for the server are correct, particularly those used for DNS name resolution.
- If a server is to be configured as the secondary server in a redundant VMS installation, the primary and secondary servers should have an active Ethernet connections between these two 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.
- Disable any extra Ethernet adapters on the server and ensure that only one gateway is assigned to the server.
- Disable the Windows Firewall.
- Verify that 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-along VMS server or as the Primary 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.

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.

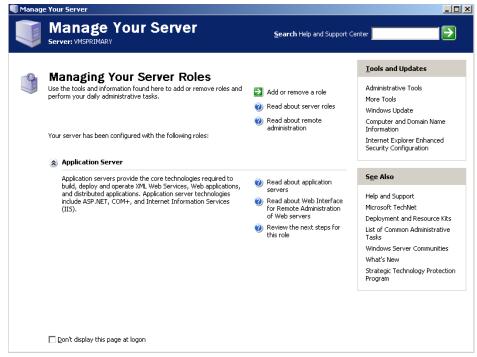


Figure D-1 Manage Your Server dialog

**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.

Configure Your Server Wizard	×
Preliminary Steps You can ensure that you successfully configure your server by completing the following steps before continuing.	No.
Before continuing, verify that the following steps have been completed.	
<ul> <li>Install all modems and network cards.</li> </ul>	
<ul> <li>Attach all necessary cables.</li> </ul>	
If you plan to use this server for Internet connectivity, connect to the Internet now.	
• Turn on all peripherals, such as printers and external drives.	
Have your Windows Server 2003 Setup CD available, or know your network installation path.	
When you click Next, the wizard will search for network connections.	
< Back Cancel	Help

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.

nfigure Your Server Wizard	X
<b>Configuration Options</b> You can add a common set of roles to this server, or you can customize this server by specifying the roles to add or remove.	No.
Configure this server using:	
O Iypical configuration for a first server	
Simplify the setup of a new network by adding a common set of roles for a first server. This option sets up this server as a domain controller by installing the Active Directory directory service; installs DNS server and DHCP server (if required) for IP address management; configures network routing; and activates a security firewall.	
Custom configuration	
Customize this server by adding the roles, such as file server, print server, or application server, that you want it to perform. You can also use this option to remove existing roles from this server.	
< <u>B</u> ack <u>N</u> ext > Cancel H	Help

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.

Server Role You can set up this server to perform one role to this server, you can run this wizard Select a role. If the role has not been add	d again. ed, you can add it. :	If it has already been added, you can
remove it. If the role you want to add or r Server Role File server	emove is not listed, Configured No	open <u>Add or Remove Programs</u> . Domain Controller (Active Directory)
Print server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DHCP server Streaming media server WINS server	No Yes No No No No No No No	Domain controllers store directory data and manage user logon processes and directory searches. <u>Read about domain controllers</u>
	< Back	Next > Cancel Help

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.

Summary:					
Run the Active Director	y Installation Wizard H	to set up this :	erver as a don	nain controller	

**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.

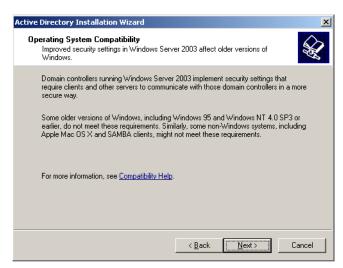


Figure D-7 Active directory installation wizard

- **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.

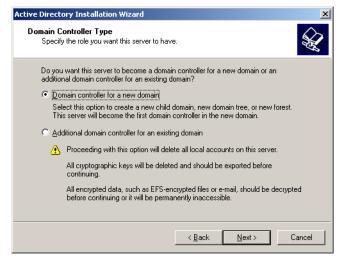


Figure D-8 Domain controller type dialog

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.

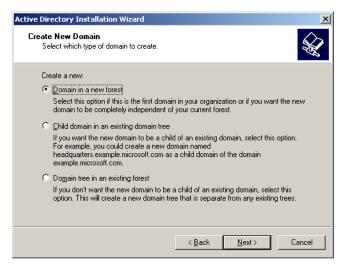


Figure D-9 Create new domain dialog

**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.

Active Directory Installation Wizard	x
New Domain Name Specify a name for the new domain.	<b>X</b>
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).	
Eull DNS name for new domain:	
taclab.vipersat.com	
< <u>B</u> ack <u>N</u> ext>	Cancel

Figure D-10 New domain name dialog

**13.** In the **NetBIOS Domain Name** dialog shown in figure D-11, enter the Net-BIOS 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.

Active Directory Installation Wizard	×
NetBIOS Domain Name Specify a NetBIOS name for the new domain.	Ż
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.	
Domain NetBIOS name: TACLABO	
< <u>B</u> ack <u>N</u> ext> Cancel	

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.

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log files.	<b>X</b>
For best performance and recoverability, store the database and the log on separate hard disks.	
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS Browse	
Where do you want to store the Active Directory log?	
Log folder:	
C:\WINDOWS\NTDS Browse	
	-
< <u>B</u> ack <u>N</u> ext > Car	cel

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.

Active Directory Installation Wizard
Shared System Volume Specify the folder to be shared as the system volume.
The SYSVDL folder stores the server's copy of the domain's public files. The contents of the SYSVDL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse
< <u>B</u> ack Next > Cancel

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:** 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.

ve Directory Installation Wizard	×
<b>DNS Registration Diagnostics</b> Verify DNS support, or install DNS on this computer.	<b>X</b>
Diagnostic Failed	<b></b>
The registration diagnostic has been run 2 times.	
Warning: Domain Controller functions like joining a domain, logging onto a domain and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.	
None of the DNS servers used by this computer responded within the timeout interval.	
For more information, including steps to correct this problem, see Help.	•
○ I have corrected the problem. <u>P</u> erform the DNS diagnostic test again.	
Install and configure the DNS server on this computer, and set this computer this DNS server as its preferred DNS server.	to use
$\bigcirc$ I will correct the problem later by configuring DNS manually. (Advanced)	
< <u>B</u> ack Next >	Cancel

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.

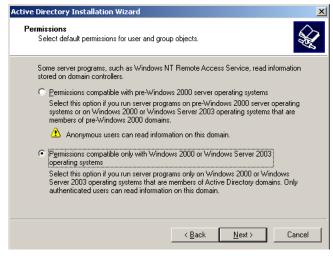


Figure D-15 Permissions dialog

**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.

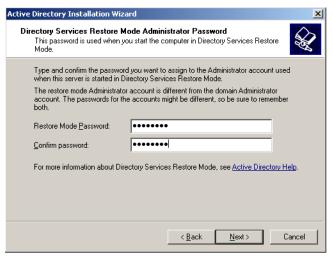


Figure D-16 Administrator password

**19.** Review the **Summary** screen shown in figure D-17, then click the **Next** button to continue.

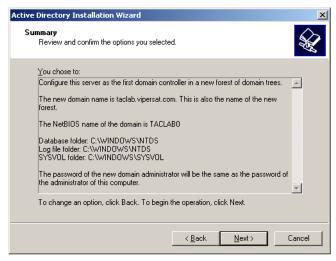
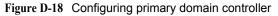


Figure D-17 Summary screen

**20.** The wizard will begin configuring the Primary domain controller as shown in figure D-18.

Active Directory Installation Wizard				
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.				
Starting				



**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.

#### Configuring a Secondary Domain Controller

💐 Manage	e Your Server			
	Manage Your Server	Search Help and Support Center		
•	Managing Your Server Roles Use the tools and information found here to add or remove roles and perform your daily administrative tasks. Your server has been configured with the following roles:	<ul> <li>Add or remove a role</li> <li>Read about server roles</li> <li>Read about remote administration</li> </ul>	<b>Lools and Updates</b> Administrative Tools More Tools Windows Update Computer and Domain Name Information Internet Explorer Enhanced Security Configuration	
	Application Server Application servers provide the core technologies required to build, deploy and operate XML Web Services, Web applications, and distributed applications. Applications server technologies include ASP.NET, COM+, and Internet Information Services (IIS).	<ul> <li>Read about application servers</li> <li>Read about Web Interface for Remote Administration of Web servers</li> <li>Review the next steps for this role</li> </ul>	See Also Help and Support Microsoft TechNet Deployment and Resource Kits List of Common Administrative Tasks Windows Server Communities What's New Strategic Technology Protection Program	
	Don't display this page at logon			

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.

Configure Your Server Wizard	×
Preliminary Steps You can ensure that you successfully configure your server by completing the following steps before continuing.	1 Alexandre
Before continuing, verify that the following steps have been completed.	
<ul> <li>Install all modems and network cards.</li> </ul>	
Attach all necessary cables.	
If you plan to use this server for Internet connectivity, connect to the Internet now.	
• Turn on all peripherals, such as printers and external drives.	
Have your Windows Server 2003 Setup CD available, or know your network installation path.	
When you click Next, the wizard will search for network connections.	
< Back Next > Cancel	Help

Figure D-22 Preliminary steps

**4.** The wait screen shown in figure D-23 will be displayed while your network settings are being detected.

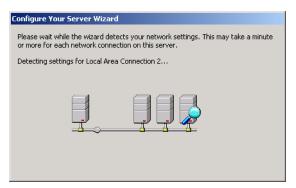


Figure D-23 Network detection wait screen

**5.** From the **Configuration Options** dialog shown in figure D-24, select the **Custom Configuration** radio button then click **Next** button.

#### Configuring a Secondary Domain Controller

nfigure Your Server Wizard		×
Configuration Options You can add a common set of roles to this server, or you can customize this server by roles to add or remove.	specifying the	Z
Configure this server using:		
O Typical configuration for a first server		
Simplify the setup of a new network by adding a common set of roles for a first server up this server as a domain controller by installing the Active Directory directory servic server and DHCP server (if required) for IP address management; configures network activates a security firewall.	e; installs DNS	5
Custom configuration		
Customize this server by adding the roles, such as file server, print server, or applicat you want it to perform. You can also use this option to remove existing roles from this		

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.

<b>Server Role</b> You can set up this server to perform one role to this server, you can run this wizar		es. If you want to add more than one
Select a role. If the role has not been add remove it. If the role you want to add or Server Role File server		
Print server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DHCP server Streaming media server WINS server	No Yes No No No No No No No	Domain controllers store directory data and manage user logon processes and directory searches. <u>Read about domain controllers</u>
	< <u>B</u> ack	Next > Cancel Help

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 Your Server Wizard				
Summary of Selections View and confirm the options you have sele	ected.			No.
<u>S</u> ummary:				
Run the Active Directory Installation Wiza	rd to set up this	server as a domair	o controller	
' To change your selections, click Back. To co	ontinue settina u	o this role. click Ne:	×t.	
		,		
	< <u>B</u> ack	( <u>N</u> ext >	Cancel	Help

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.

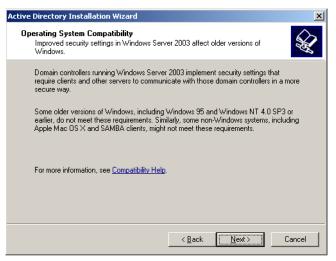


Figure D-28 Active directory installation wizard

- **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.

Active Directory Installation Wizard
Domain Controller Type Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain Proceeding with this option will delete all local accounts on this server.
<ul> <li>All cryptographic keys will be deleted and should be exported before continuing.</li> </ul>
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< <u>B</u> ack <u>N</u> ext> Cancel

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.

Active Directory Inst	allation Wizard
Network Credenti Provide a netwo	als Ik user name and password.
	ame, password, and user domain of an account with sufficient privileges Directory on this computer.
<u>U</u> ser name:	😰 administrator
Password:	•••••
<u>D</u> omain:	taclab0
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

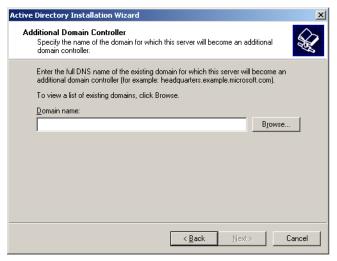


Figure D-31 Additional domain controller

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.

Browse for Domain	?×
Domains:	
1	
OK Car	icel

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.

tive Directory Installation Wizard			
Additional Domain Controller Specify the name of the domain for which the domain controller.	iis server will be	come an ad	ditional
Enter the full DNS name of the existing dom additional domain controller (for example: he			
To view a list of existing domains, click Brow	vse.		
Domain name:			
taclab.vipersat.com			Browse
,			
	( Deel	L No.45	Cancel
	< <u>B</u> ack	<u>N</u> ext>	Lancel

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.

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log files	
For best performance and recoverability, store the database and the log hard disks.	on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	Browse
Where do you want to store the Active Directory log?	
Log folder:	
C:\WINDOWS\NTDS	Browse
< <u>B</u> ack <u>N</u> ext>	Cancel

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.

Active Directory Installation Wizard	×
Shared System Volume Specify the folder to be shared as the system volume.	
The SYSVOL folder stores the server's copy of the do of the SYSVOL folder are replicated to all domain con	
The SYSVOL folder must be located on an NTFS vol	ume.
Enter a location for the SYSVOL folder.	
Eolder location:	
C:\WINDOWS\SYSVOL	Browse
< <u>B</u> a	ck <u>N</u> ext> Cancel

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.

Active Directory Installation Wize	ard 🔀
Directory Services Restore M This password is used when y Mode.	Iode Administrator Password ou start the computer in Directory Services Restore
	d you want to assign to the Administrator account used irectory Services Restore Mode.
	r account is different from the domain Administrator e accounts might be different, so be sure to remember
Restore Mode Password:	•••••
Confirm password:	•••••
For more information about Dire	ectory Services Restore Mode, see <u>Active Directory Help</u> .
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

Summary Review and confirm the options	you selected.	Se
You chose to:		
Configure this server as an addit taclab.vipersat.com.	tional domain controller for the domain	<u>^</u>
Database folder: C:\WINDOWS Log file folder: C:\WINDOWS\N SYSVOL folder: C:\WINDOWS'	ITDS	
		v
To change an option, click Bac	k. To begin the operation, click Next.	

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.

Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Stopping service NETLOGON
Cancel

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.

Active Directory Installation Wizard	x
Windows must be restarted before the changes made by the Active Directory Installation wizard take effect.	

Figure D-40 Restart screen

**24.** After reboot, Windows displays the confirmation screen shown in figure D-41.

id or

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.

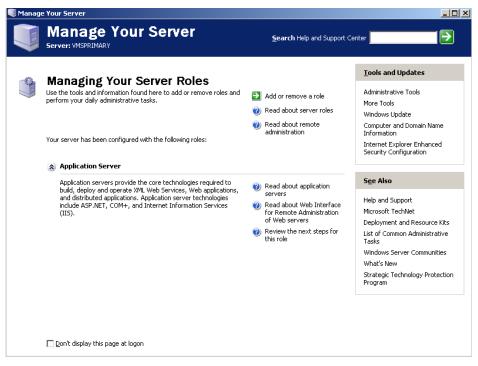


Figure D-42 Manage your server dialog

#### Installing Secondary DNS Server

**2.** Review the information in the **Preliminary Steps** screen shown in figure D-43 before proceeding and then click then **Next** button to proceed.

Configure Your Server Wizard	×
Preliminary Steps You can ensure that you successfully configure your server by completing the following steps before continuing.	No.
Before continuing, verify that the following steps have been completed.	
<ul> <li>Install all modems and network cards.</li> </ul>	
Attach all necessary cables.	
• If you plan to use this server for Internet connectivity, connect to the Internet now.	
<ul> <li>Turn on all peripherals, such as printers and external drives.</li> </ul>	
Have your Windows Server 2003 Setup CD available, or know your network installation path.	
When you click Next, the wizard will search for network connections.	
< Back Cancel	Help

Figure D-43 Preliminary steps screen

**3.** Highlight DNS server in the table shown in figure D-44 and then click **Next** button.

Configure Your Server Wizard		×
Server Role You can set up this server to perform one role to this server, you can run this wizar Select a role. If the role has not been add remove it. If the role you want to add or	d again. Ied, you can add it.	If it has already been added, you can
Server Role File server Print server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DHCP server Streaming media server WINS server	Configured No No No No No No No No No No No No	DNS (Domain Name System) servers translate domain and computer DNS names to IP addresses. If you plan to set up this server as a domain controller and it is the first domain controller in the domain, select the domain controller role. In this case, the domain controller role configures the server so that DNS and Active Directory work together. Read about DNS servers View the <u>Configure Your Server log</u> .
	< <u>B</u> ack	Next > Cancel Help

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.

Immary of Selections View and confirm the options you have	e selected.	
<u>S</u> ummary:		
Install DNS server Run the Configure a DNS Server Wiza	rd to configure DNS	
Run the Configure a Divo berver wiza	ira to configare Divo	
To change your celections, click Back, 1	To continue setting up this role, click No	ext.
To change your selections, click back.		

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.

Appendix D-Domain Controller and DNS



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.

Windows Setup	Installing DNS Server	×
Configuring Co Setup is mai	omponents king the configuration changes you requested.	Ē
	ease wait while Setup configures the components. This may take veral minutes, depending on the components selected.	
Status: Cop	ying files	
	< Back, Next >	

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.

Configure a DNS Server Wizard			
	Welcome to the Configure a DNS Server Wizard This wizard helps you configure a DNS server by creating forward and reverse lookup zones and by specifying root hints and forwarders. Before continuing, review the DNS checklists. DNS Checklists For more information about configuring DNS, click Help. To continue, click Next.		
	<back next=""> Cancel Help</back>		

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.

Configure a DNS Server Wizard	×
Select Configuration Action You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.	
Select the action you would like this wizard to perform: Create a forward lookup zone (recommended for small networks) This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.	
C Create forward and reverse lookup zones (recommended for large networks) This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers or both. The wizard will configure the root hints.	
C Configure root hints only (recommended for advanced users only) The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.	
< <u>B</u> ack <u>N</u> ext > Cancel He	alp

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.

#### Installing Secondary DNS Server

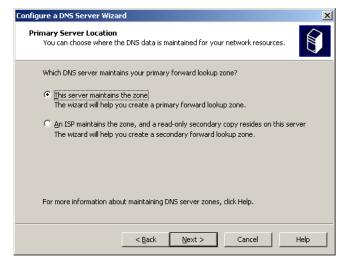


Figure D-50 Primary server location

**10.** Enter your DNS zone name in the **Zone name** dialog box shown in figure D-51. Click the **Next** button to continue.

w Zone Wizard				
Zone Name				6
What is the name of t	he new zone?			Ľ
The zone name specifi authoritative. It might or a portion of the dor not the name of the D	be your organizat main name (for exa	ion's domain nam	ne (for example, mi	icrosoft.com)
Zone name:				
ctaclab.vipersat.com	1			
For more information	about zone names	, click Help.		

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.

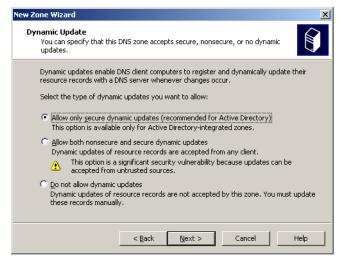


Figure D-52 Dynamic update dialog

**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.

Forw F	re a DNS Server Wizard  varders  Forwarders are DNS servers to which this server sends queries that it cannot  answer.
9	Should this DNS server forward queries?
1	C Yes, it should forward queries to DNS servers with the following IP addresses:
	(optional)
(	No. it should not forward queries
	If this server is not configured to use forwarders, it can still resolve names using root name servers.
F	For more information about forwarders, click Help.
	< <u>B</u> ack <u>N</u> ext > Cancel Help

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, dick 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 "Stopping Previous VMS Version (Upgrade)" on page 2-10 of Chapter 2, "VMS Installation" to complete the VMS installation.

Installing Secondary DNS Server

{ This Page is Intentionally Blank }

#### **A P P E N D I X**

# R

# **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 highorder 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.

🍓 ViperView		
	👰 Tree View 📰 List View	2
Event L Open	Event Log	<b>_</b>
End Setwor     Backup     Out of I     Restore	Network Manager	
Subnet     Rescure     Synchronize     Synchronize	i 🕻 InBand Manager	
E Redunc Licensing	Out of Band Manager	
Properties	Subnet Manager	
	Bandwidth Manager	
	Snmp Modem Manager	
Level Other Antice Density Other Consider		<u> </u>
Local Status: Active Remote Status: Connected		

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.

🎒 VIPERLAB1	? ×
General Traps Redundancy Role: Primary Local Status: Active Remote Status: Connected Remote Server 10. 1. 1. 3	
OK Cancel Apr	ly

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

#### Configuring SNMP Traps

• Community String

VIPERLAB1			? ×
SNMP Manager (TRAP			
Address	Port	Community	
192.168.150.150 192.168.150.180	162 162	public public	
132.100.130.100	102	public	
Insert	Mo	dify	Remove
OK		Cancel	Apply

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

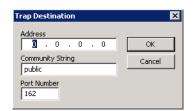


Figure E-4 Trap desitination

#### 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.

# 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.

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)

Table F-1STDMA ACK Message

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.

🚮 Telnet - 10	0.1.0.16					_ 🗆 🗵
Connect Edit	Terminal	Help				
			STDMA/SCPC Aut	o Switching		
Current WA CTS Switch Load Switc STDMA Slot STDMA Swit Percent AJ	N Trans Detect ching Capaci ch Dela llocatic	mit Mode. ion ity y	0 to disable)	[Continuous] [Disabled] [Disabled] [95%] [10 seconds] [10%]		 U W
EX1t			nt storage			 X

Figure F-1 Hub switching menu, CDM-570/570L

CON		Info Admin	Modem LA	N WAN	Routing	Stats	Vipersat		Copy Comt All R
Hub Swit	ching						iome State		All K
	Hub Load Switching	Load Switching:	O Disabled (	Enabled					
					Subm	iit			
		STDMA Slot Capacity:	valiu Ranye(0-	100%)			STDM	IA Switch Delay:	10 Valid Range(0
		Percent Allocation:	Valid Range(0-	100%)	Subm	iit			
									and with an extension

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.

#### Load switching

🚮 Telnet - 10	).1.128.1			_ 🗆 ×
Connect Edit	Terminal Help			
		STDMA/SCPC Auto	) Switching	
Current W Voice Swit Video Swit TOS Switch Load Switc SCPC Step SCPC Step SCPC Step SCPC Step	ch Detection ch Detection Detection Vp Threshold Down Threshold. Delay Pecess	[STDMA(Burst)] [Enabled] .[Disabled] .[Enabled] .[Enabled] .[5%] .[6%] .[10 seconds] [10%].		
Exit				 

Figure F-3 Switching menu for a remote, CDM-570/570L

	Info Admin	Modem L	AN WAN	Routing	Stats	Vipersat	Copyright © 2007
		g   <u>Monitor  </u> s   <u>Stats   Utility</u>	!				Contech EF Data All Rights Reserved
Remote Switching							
Remote Load Switching	3						
	Load Switching:	C Disabled	Enabled				
				Subr	nit		
SCPC	Step Down Threshold	65 Valid Range(0	)-100%)			SCPC Step Up Threshold:	90 Valid Range(0-100%)
٤	SCPC Step Up Excess	15 Valid Range(0	0-100%)			SCPC Switch Delay:	10 Valid Range(0-50 seconds).
				Subr		and the second second second	

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.

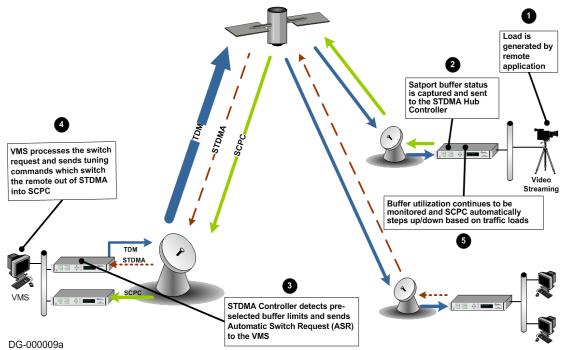


Figure F-5 Example load switching diagram

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 preselected 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.

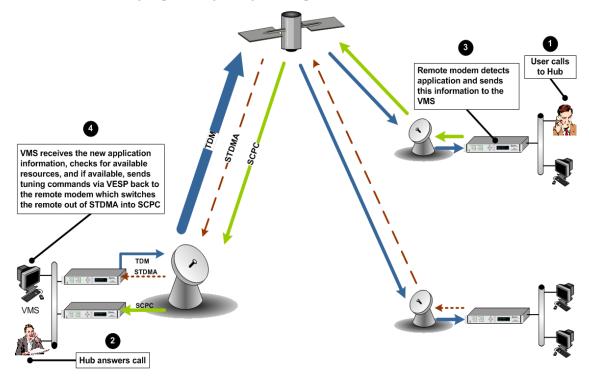
The home threshold is the bit rate set to trigger a return to the home threshold. This function is used when bandwidth has been allocated to meet load requirements, and the load has been either removed or partially removed. Since the channel's new load no longer requires the current bit rate, when the 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.



DG-000002a



# **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.

#### Application switching

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-basedswitching 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

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. Type of Service (ToS) Switching

{ This Page is Intentionally Blank }

# 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.

#### Entry Channel Mode (ECM)

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.

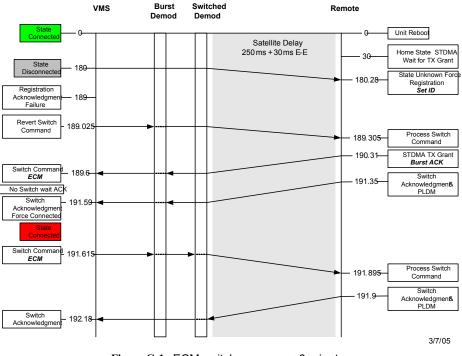
If the VMS loses communications with a switched remote for more than three minutes, it will attempt to return the remote to home state. If the revert-to-home state command succeeds (restoring communications) Entry Channel Mode will cause the remote to switch to its initial SCPC bit rate.

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.

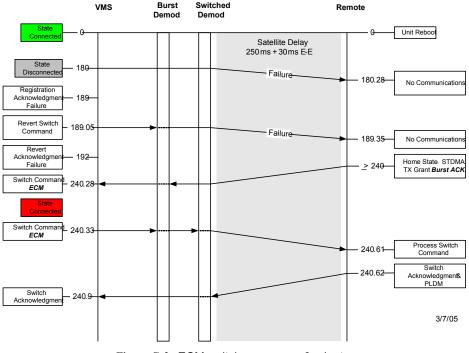
Since it is not possible to know which of the above scenarios caused the communications outage the VMS will not free the bandwidth slot except through operator intervention.

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.



#### ECM Switch Recovery 3min.

Figure G-1 ECM switch recovery < 3 minutes



#### ECM Switch Recovery 3min.

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.

dit Configuration	<u>? ×</u>
Features         Home         IGMP         Main           Access         Admin         Auto W.           SMTP         SNMP         STDMA	tenance Network Routing AN DES DPC Switching Vipersat
Enable STDMA Allocation Metho     Enable BFAT     Entry Channel	
	lot Maximum: Stats Collection: 00 msec 10 sec
	uard Band: i0 msec List Remotes
Automatic Remote Removal	Burst Map Multicast IP Address: 239 . 10 . 20 . 30 Dutbound IP Address for DPC: 0 . 0 . 0 . 0
	OK Cancel

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.

#	Name	Address	SCPC Rate	Туре
ÐO	Remote 1	192.168.151.1	0 bps	0
<b>D</b> 1	Remote 2	192.168.152.1	0 bps	0
2	Remote 3	192.168.153.1	0 bps	0
•3	Remote 4	192.168.154.1	0 bps	0

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.

#### Entry Channel Mode (ECM)

**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.

Remote Entry	×
Station Name: Remote 3	Disable
Address: 192 . 168 . 153 . 1	
SCPC Data Rate: Dbps	ОК
Switch Type: 0	Cancel

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: 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.

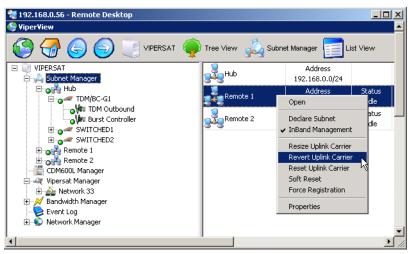


Figure G-6 Revert uplink carrier command, VMS controlled modem

**6.** This completes resetting the remote VMS controlled modem to operate in the STDMA mode.

{ This Page is Intentionally Blank }

Entry Channel Mode (ECM)

# H

# VMS BILLING LOG TRANSLATOR (VBLT)

# Description

VBLT is a windows console application that converts switch events, stored in the VMS 3.x event log, into a billing log format. VBLT can be run directly from the command line console, or using VBLT.ui, a graphical user interface frontend, or as a scheduled task using the windows task scheduler.



**Note:** If you have unique format requirements for your billing information, contact your Vipersat representative for details on having a format conversion program created to meet your needs.

#### Installation

Copy the two files, VBLT.EXE and VBLT.ui.EXE, into a directory (folder) where the user has valid *write* and *execute* privileges. These applications can be installed on a VMS server, or a remote Viperview client PC. Only users with Viperview privileges should run these applications.

#### Operation

VBLT can be executed in three modes: (1) console, (2) GUI frontend, or (3) schedule task. Before using VBLT in any mode, it is highly recommended that VMS 3.x service be active.

When specifying a remote VMS server, VBLT should be run from the same user account and PC that is hosting the remote Viperview client. This ensures that the correct security privileges are enabled before executing VBLT.

Consult your VMS or system administrator for more information on accessing a remote VMS server.

#### **Console Mode**

VBLT has the following command line options when used in console mode:

**-r days** - Number of days (24hr period) to retrieve starting from current time. Default is 1 day.

-v server - IP address, UNC, or DNS name of VMS 3.1 server. If this option is not specified, the local VMS server (localhost) is used.

-s session - Sets the starting session ID. Zero (0) is used as default.

-o "path" - Have billing log output to specified file path.

-I - localizes the time stamps to local time zone, default is UTC time.

-q - quiet mode, does not display output to console; used in conjunction with -o option

### Examples

In this example, the following command retrieves billing logs for the past two days from the local VMS server. The output is displayed on the console using local time zone.

vblt –r 2 –l

To retrieve billing logs for the past two days and save the results to a file call sample1.log, starting with a session id of 1467, use this command:

vblt –r 2 –s 1467 –o sample1.log

# GUI Mode

VBLT.ui provides a Windows user interface to the VBLT application. It also allows the user to specify start/end time & date range for billing log retrieval where as the console mode retrieves logs based on number of days from current time.

To use VBLT.ui, start the VBLT.ui application from the Windows Explorer by double clicking it. Verify that the VBLT.EXE application is in the same directory as VBLT.ui.EXE.

#### Operation

- **1.** Enter the start date and time in the **Start Date & Time** box shown in figure H-1.
- 2. Enter the s end date and time in the End Date & Time box shown in figure H-1. The end date and time must be greater than the start date and time.

🙅 VBLT.ui 1.2		
		Start Egit About
VMS Server	Output File	
localhost	Acme Corp	
Start Date & Time           Date         8/ 1/2005           Time         12:00:00 AM           Options	End Date & Time Date 8/ 5/2005 Time 12:00:00 AM	Regress Mode Retrieve events for past T day(s)
	re Sequential Home Events	Session ID 0
VBLT.ui 1.2		A 
1		Þ

Figure H-1 VLBT graphic user interface

- **3.** Selecting the Use Local Time option in the Options box determines whether to use local time zone references with respect to start and end time, and the time stamp on the output file. Selecting the Quiet Mode option will suppress any output to a VBLT console window.
- **4.** The **VMS Server** entry is optional. Leaving it empty, or entering **localhost** will retrieve the logs from the local VMS server running on the same PC as VBLT. To access a remote VMS server, enter its IP address (i.e. 212.10.0.1), UNC, or hostname. Any security privileges must be configured for remote access and name resolution.
- **5.** An **Output File** must be provided. If the file does not exist, it will be created. If it exists, it will be overwritten.
- 6. Click the OK button to start the retrieval. A dialog box will be displayed to indicate a successful or failed operation. Click Exit to quit VBLT.ui.

# 3.3 Scheduled Task Mode

The billing log retrieval process can be automated by using the Windows Task Scheduler. The Windows Task Scheduler will execute VBLT on a scheduled basis.

To create a scheduled VBLT task, use the Scheduled Task Wizard. Follow the steps below:

1. Open the Windows Task Scheduler, shown in figure H-2, by clicking Start, click All Programs, point to Accessories, point to System Tools, and then click Scheduled Tasks.

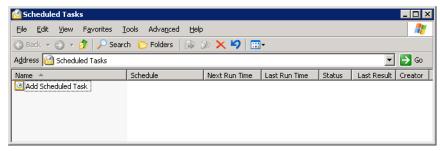


Figure H-2 Scheduled tasks

- 2. Click on the Add Scheduled Task item. This will open the "Scheduled Task Wizard"
- **3.** When prompted to select **Windows program to run**, click the **Browse** button, and select the VBLT.EXE from its install directory.
- **4.** Select a name for the task and scheduled period (Daily, Weekly, Monthly, etc.) from the dialog shown in figure H-3.

Scheduled Task Wizard		×
	<u>Lype a name for this task.</u> The task name can be the same name as the program name.	
Le contra	VBLT	
X	Perform this task:	
14	C <u>D</u> aily	
1000		
	C Monthly	
	O One time only	
	○ When my computer <u>s</u> tarts	
19 . C.	C When I log on	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Figure H-3 Scheduled task wizard

- 5. Set the start time, start date, and recurrence options.
- **6.** Enter your user and name password to confirm the new task entry. This username and password should be a valid VMS user.
- 7. In the last step, check the "Open advanced properties for this task ...." Option, then click Finish.
- **8.** The last step is to add the VLBT command options to the task. In the **Run** text box shown in figure H-4, go to the end of the VBLT.exe and add the desired options. The "-r" and "-o" options should be specified as shown in figure H-4.

VBLT		2 🛛
Task Sched	ule   Settings   Security	
C.M	NDOWS\Tasks\VBLT.job	
Bun	rce\system\VBLT@ebug\VB	LT.exe r 1 -o "dailylog.log"
		Browse
Start in:	C:\Projects\Vipersat\VMS3\s	source\system\VBLT\Debug
⊆omments:		
Ryn as:	COMTECHTEL/dkia	Set password
□ Run only if I Enabled (s	Jogged on cheduled task runs at specified t	ime)
	OK	Cancel Apply

Figure H-4 VLBT task tab

The VLBT application will now be run as a scheduled task by the Windows Task Scheduler.

#### 3.3 Scheduled Task Mode

An alternative method to running a scheduled VBLT task is to create a batch file that calls VBLT with the desired options. A scheduled task is created to run this batch file. This simplifies the maintenance as only the batch file needs to be modified if they are any changes to VBLT options.

The billing log format is created from switch events logged by the VMS. The billing log consists of eight (8) comma separated value fields as follows:

- **1. Satellite Name** name of satellite, as shown in VMS, that contains the subnet which generated the switch event.
- **2.** Antenna Name name of Antenna, as shown in VMS, associated with the Subnet which generated the switch event.
- 3. Date logged date of switch event in "dd/mm/yyyy" format
- 4. Time logged time of switch event in "hh:mm:ss.mss" format
- **5.** Session ID increasing counter that changes anytime a subnet switches back to its HOME state. This is an unsigned 32 bit counter.
- **6. Switch Type -** indicates the type of switch. This value can be "HOME", "MANUAL", "AUTOMATIC", "SCHEDULED", "UNKNOWN"
- 7. Bandwidth bandwidth of channel switch in Hertz (Hz)
- **8.** Bit Rate bit rate of channel switch in bits per second (bps)

## Billing Log Examples

"Galaxy 10R", "R1", 04/04/2005, 19:19:26:717, 996, HOME, 230400Hz, 512000bps "Galaxy 10R", "R1", 04/04/2005, 19:35:08:999, 997, MANUAL, 460800Hz, 512000bps "Galaxy 10R", "R1", 04/04/2005, 19:37:35:979, 997, HOME, 230400Hz, 512000bps "Galaxy 10R", "R1", 04/04/2005, 19:38:21:665, 998, MANUAL, 230400Hz, 256000bps "Galaxy 10R", "R1", 04/04/2005, 20:46:37:210, 998, MANUAL, 115200Hz, 128000bps

# GLOSSARY

## A

- ALC Automatic Limit Control A closed loop mechanism controlling the gain stabilization of the HPA's RF output power.
- APL Asynchronous Party Line A Vipersat term for RS-485 multi-drop bus used for control of indoor equipment. See also SPL.
- ARP Address Resolution Protocol A protocol for a LAN device to determine the MAC address of a locally connected device given its IP address. See also MAC.
- ASR Automatic Switch Request A switch request message generated by a Vipersat modem and forwarded to the VMS to establish a new satellite link or adjust bandwidth between source and destination IP addresses.
- ATM Asynchronous Transfer Mode

#### В

BER Bit Error Rate (sometimes Ratio) – A measure of the number of data bits received incorrectly compared to the total number of bits transmitted.

- BUC Block Up Converter An upconverter so called because it converts a whole band or "block" of frequencies to a higher band. IF is converted to final transmit frequency for satellite communications.
- BPS Bits Per Second A measure of transmission speed. See also Kb/s & Mb/s.
- BPSK Binary Phase Shift Keying A modulation technique in which the carrier is phase shifted +/-180 degrees. See also QPSK.

## С

- 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 Comtech Data Demodulator
  - CDM Comtech Data Modem
  - CIR Committed Information Rate The guaranteed minimum bandwidth assigned to a remote terminal.
  - CRC Cyclic Redundancy Check 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 Demand Assigned Multiple Access A process whereby communications links are only activated when there is an actual demand.
- dBm Decibel referenced to 1 milliwatt.
- DHCP Dynamic Host Configuration Protocol An Internet protocol for automating the configuration of computers that use TCP/IP.
  - DNA Dynamic Node Announcement A process in Vipersat satellite networks whereby remote sites periodically announce their presence to facilitate network setup and monitoring.
  - DPC Dynamic Power Control

- DRAM Dynamic Random Access Memory
- DSCP Differentiated Services Code Point 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.
  - DSP Digital Signal Processor A microprocessor chip optimized for signal processing applications.
  - DVB Digital Video Broadcast
  - DVP Digital Voice Processor Used in packet voice applications.

#### Ε

 $E_b/N_o$   $E_b/N_o$  is the ratio of  $E_b$  (energy per bit) and  $N_o$  (noise power density per Hz). The bit error rate (BER) for digital data is a decreasing function of this ratio.  $E_b$  is the energy of an information bit measured in Joules or, equivalently, in Watts per Hertz.

#### F

- FAST Code Fully Accessible System Topology 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.
  - FDMA Frequency Division Multiple Access A technique where multiple users can access a common resource (e.g., satellite) by each being allocated a distinct frequency for operation. See also TDMA.
    - FEC Forward Error Correction 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.
    - FIFO First In First Out A simple buffer or queue technique whereby data queued the longest is transmitted first.
    - FTP File Transfer Protocol An application for transferring computer files over the Internet. See also TFTP.

- G.729 ITU standard for LD-CELP (Low Delay Code Excited Linear Prediction) voice encoding at 8 kb/s.
  - GIR Guaranteed Information Rate
- Group ID A number assigned to equipment which defines it as a member of a group when addressed by the VMS burst controller.
  - GUI Graphical User Interface A form of graphical shell or user interface to a computer operating system or software application.

## Η

- HDLC High Level Data Link Control A standard defining how data may be transmitted down a synchronous serial link.
- HPA High Power Amplifier The amplifier used in satellite communications to raise the transmit signal to the correct power level prior to transmission to satellite.
- HTTP Hyper Text Transfer Protocol The Internet standard for World Wide Web (WWW) operation.
  - Hub The central site of a network which links to a number of satellite earth sites (remote's).

#### L

- ICMP Internet Control Message Protocol
  - IF Intermediate Frequency In satellite systems, IF frequencies are usually centered around 70 or 140 MHz (video/TV), or 1200 MHz (L-band).
  - IP Internet Protocol A format for data packets used on networks accessing the Internet.
  - ISP Internet Service Provider A company providing Internet access.
  - ITU International Telecommunications Union

- Kb/s Kilo bits per second 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 14.0–14.5 GHz. See also C-band.

## L

- L-Band A frequency band commonly used as an IF for satellite systems using block up/ down conversion. Usually 950–1450 MHz.
  - LAN Local Area Network
  - LLA Low Latency Application
  - LNA Low Noise Amplifier An amplifier with very low noise temperature used as the first amplifier in the receive chain of a satellite system.
  - LNB Low Noise Block A downconvertor so called because it converts a whole band or "block" of frequencies to a lower band. It is similar to LNA.
  - LNC Low Noise Converter A combined low noise amplifier and block down converter, typically with an L-band IF.
    - LO Local Oscillator

#### Μ

- M&C Monitor & Control
- MAC Media Access Control A protocol controlling access to the physical layer of an Ethernet network.
- Mb/s Mega Bits per Second 1 Million bits/second. A measure of transmission speed. See also bps & kb/s.
- Modem MODulator and DEModulator units combined.
- Multicast Transmitting a single message simultaneously to all recipients.

- NAT Network Address Translation 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 Network Interface Controller 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 Network Management System
- NOC Network Operation Center Has access to any earth station installed using the VIPERSAT Management System (VMS). A NOC can remotely interrogate, control, and log network activities.

#### Ο

- ODU Outdoor Unit 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.
- **OPEX** Operating Expenditure
- **OSPF** Open Shortest Path First A common routing algorithm.

#### Ρ

- PLDM Path Loss Data Multicast A message that is sent every sixty seconds and contains information on messages received or lost.
- PSTN Public Switched Telephone Network The world's public circuit-switched telephone network, digital and analog, and includes mobile as well as land-line voice and data communications.

- QPSK Quaternary Phase Shift Keying A modulation technique in which the carrier is phase shifted +/- 90 or +/-180 degrees. See also BPSK.
  - QoS Quality of Service

## R

- **Remote** Satellite earth site that links to a central network site (hub).
  - RF Radio Frequency A generic term for signals at frequencies above those used for baseband or IF.
  - **RFC** Request For Comment The de-facto Internet standards issued by the Internet Engineering Task Force (IETF).
  - **RIP** Routing Information Protocol
- **RS-232** A common electrical/physical standard issued by the IEEE used for point to point serial communications up to approximately 115 kb/s.
- **RS-485** A common electrical/physical standard issued by the IEEE used for multi-drop serial communications.
  - Rx Receive

## S

- SCPC Single Channel Per Carrier 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.
- SNMP Simple Network Management Protocol A protocol defining how devices from different vendors may be managed using a common network management system.
- SOTM Satellite On The Move
  - SPL Synchronous Party Line An electrically isolated interface between indoor and outdoor equipment used in Vipersat satellite systems. See also APL.

Star A network topology which, if drawn as a logical representation, resembles a star Topology with a hub at the center.

- STDMA Selective Time Division Multiple Access A multiple access technique where users time-share access to a common channel with variable-sized time slots allocated on usage.
- Streamload A proprietary Vipersat data streaming protocol. Protocol

### Т

- TCP/IP Transmission Control Protocol / Internet Protocol A standard for networking over unreliable transmission paths. See also UDP.
- TDMA Time Division Multiple Access A multiple access technique where users contend for access to a common channel on a time-shared basis. See also FDMA and STDMA.
- TFTP Trivial File Transfer Protocol A simple file transfer protocol used over reliable transmission paths. See also FTP.
  - ToS Type of Service
    - Tx Transmit.

## U

UDP User Datagram Protocol – A standard for networking over reliable transmission paths.

UDP A multicast transmission using the UDP protocol. multicast

#### V

VESP Vipersat External Switching Protocol – 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.

- VCS Vipersat Circuit Scheduler 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 broadcast-ing.
- VFS Vipersat File Streamer A file transfer application utilizing UDP and a proprietary Streamload protocol to transmit data across the Vipersat network.
- VMS Vipersat Management System A comprehensive M&C tool providing rapid and responsive control of Vipersat satellite networks.
- VoIP Voice over IP The routing of voice communications over the Internet or through any IP-based network.
- VOS Vipersat Object Service The main software service of the VMS application.

## W

- Wizard A specialized program which performs a specific function, such as installing an application.
- WRED Weighted Random Early Detection. A queue management algorithm with congestion avoidance capabilities and packet classification (QoS) providing prioritization.

{ This Page is Intentionally Blank }

# INDEX

#### A

automatic load switching F-2

В

basic guaranteed bandwidth 3-37

#### С

carrier type flag 3-21 CIR 3-37 committed information rate 3-37 Connection Manager 3-5, C-6

#### D

distribution lists global level 5-22 site level 5-37

#### Ε

Eb/No definition I-3 ECM to STDMA mode switch G-6 event log billing translator 5-13 filters 5-12 viewer 5-9

#### F

flags carrier type 3-21

#### Η

hardware requirements 2-1, 2-30 Heartbeat enable C-24 heartbeat C-32

#### L

load switching

automatic F-2 log event log viewer 5-9

#### Μ

main screen Monitor & Control Explorer 5-7 Monitor & Control Explorer main screen 5-7

#### Ρ

Passive Configuration C-34 policy global 5-20 setting states 5-36

#### R

redundancy configuration backup C-26 failover time C-9 group C-22 hub modem C-1 Hub Modem N:M description C-13 N:1 configuration C-8 N:1 installation 2-14, C-6 N:M configuration C-19 N:M installation C-15 N:M operation C-32 services C-1 VMS C-1 VMS N:1 description C-2 Redundancy Manager C-15, C-20, C-33

#### S

satellite on the move 3-44 Server activate 3-6 active role C-4 auto activate 3-7, C-4, C-8 connection 3-5 contention C-5, C-12 manual switching C-12 priority C-9 properties C-8 standby role C-4 status C-6 synchronization C-4 service installing F-2 SNMP Manager TRAP E-3 SOTM 3-44

Т

ToS

application type F-15 description F-15

#### V

VMS initial setup 3-5 installing services F-2 network build 3-11 redundancy C-1

#### W

WRED enabling I-9