grass valley

K2

10G Storage Area Network

Installation and Service Manual

Software Version 8.1

www.grassvalley.com

071-8779-01
February 2012

KEMA Quality

CERTIFICATE

Certificate Number: 510040.001

The Quality System of:

Grass Valley USA, LLC and its Grass Valley Affiliates

Headquarters:
400 Providence Mine Road
Nevada City, CA 95945
United States

15655 SW Greystone Ct.
Beaverton, OR 97006
United States

Brunnenweg 9
D-64331 Weiterstadt
Germany

Kapittelweg 10
4827 HG Breda
The Nederlands

2300 So. Decker Lake Blvd.
Salt Lake City, UT 84119
United States

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

Scope:
The design, manufacture and support of video and audio hardware and software products and related systems.

This Certificate is valid until: June 14, 2012
This Certificate is valid as of: December 23, 2010
Certified for the first time: June 14, 2000

H. Pierre Sallé
President
KEMA-Registered Quality

The method of operation for quality certification is defined in the KEMA General Terms And Conditions For Quality And Environmental Management Systems Certifications. Integral publication of this certificate is allowed.

KEMA-Registered Quality, Inc.
4377 County Line Road
Chalfont, PA 18914
Ph: (215)997-4519
Fax: (215)997-3809
CRT 001 042108

Accredited By:
ANAB

a DEKRA company

grass valley

K2

10G Storage Area Network

Installation and Service Manual

Software Version 8.1

www.grassvalley.com

071-8779-01
February 2012

Contacting Grass Valley

International Support Centers	**France 24 x 7**	+800 8080 2020 or +33 1 48 25 20 20	**United States/Canada 24 x 7**	+1 800 547 8949 or +1 530 478 4148
Local Support Centers (available during normal business hours)	**Asia**	**Hong Kong, Taiwan, Korea, Macau:** +852 2531 3058 **Indian Subcontinent:** +91 22 24933476 **Southeast Asia/Malaysia:** +603 7805 3884 **Southeast Asia/Singapore:** +65 6379 1313 **China:** +861 0660 159 450 **Japan:** +81 3 5484 6868		
	Australia and New Zealand: +61 1300 721 495		**Central/South America:** +55 11 5509 3443	
	Middle East: +971 4 299 64 40 **Near East and Africa:** +800 8080 2020 or +33 1 48 25 20 20			
	Europe	**Belarus, Russia, Tadzikistan, Ukraine, Uzbekistan:** +7 095 2580924 225 **Switzerland:** +41 1 487 80 02 **S. Europe/Italy-Roma:** +39 06 87 20 35 28 **-Milan:** +39 02 48 41 46 58 **S. Europe/Spain:** +34 91 512 03 50 **Benelux/Belgium:** +32 (0) 2 334 90 30 **Benelux/Netherlands:** +31 (0) 35 62 38 42 1 **N. Europe:** +45 45 96 88 70 **Germany, Austria, Eastern Europe:** +49 6150 104 444 **UK, Ireland, Israel:** +44 118 923 0499		

Copyright © Grass Valley USA, LLC. All rights reserved.
This product may be covered by one or more U.S. and foreign patents.

Grass Valley Web Site

The www.grassvalley.com web site offers the following:

Online User Documentation — Current versions of product catalogs, brochures, data sheets, ordering guides, planning guides, manuals, and release notes in .pdf format can be downloaded.

FAQ Database — Solutions to problems and troubleshooting efforts can be found by searching our Frequently Asked Questions (FAQ) database.

Software Downloads — Download software updates, drivers, and patches.

grass valley

END-OF-LIFE PRODUCT RECYCLING NOTICE

Grass Valley's innovation and excellence in product design also extends to the programs we've established to manage the recycling of our products. Grass Valley has developed a comprehensive end-of-life product take back program for recycle or disposal of end-of-life products. Our program meets the requirements of the European Union's WEEE Directive, the United States Environmental Protection Agency, and U.S. state and local agencies.

Grass Valley's end-of-life product take back program assures proper disposal by use of Best Available Technology. This program accepts any Grass Valley branded equipment. Upon request, a Certificate of Recycling or a Certificate of Destruction, depending on the ultimate disposition of the product, can be sent to the requester.

Grass Valley will be responsible for all costs associated with recycling and disposal, including freight. However, you are responsible for the removal of the equipment from your facility and packing the equipment to make it ready for pickup.

For further information on the Grass Valley product take back system please contact Grass Valley at + 800 80 80 20 20 or +33 1 48 25 20 20 from most other countries. In the U.S. and Canada please call 800-547-8949, and ask to be connected to the EH&S Department. Additional information concerning the program can be found at: www.grassvalley.com/about/environmental-policy

001187401

Contents

Safety Summaries....11

Preface....23

Chapter 1: Product description....29
- K2 SAN overview description....30
- K2 SAN key features....30
- What's new in the K2 10G SAN....31
- K2 Storage types and terms....32
- K2 SAN descriptions....32
  - Basic K2 SAN description....33
  - Redundant K2 SAN description....34
  - Basic Nearline K2 SAN description....35
  - Redundant Nearline K2 SAN description....36

Chapter 2: Preparing for installation....39
- K2 SAN installation checklists....40
  - Pre-installation planning checklist....40
  - Infrastructure checklist....40
  - Network setup and implementation checklist....40
  - Software update checklist....41
  - SAN configuration checklist....42
- Understanding system concepts....42
  - Control network description....42
  - Streaming/FTP network description....43
  - Media (iSCSI) network description....44
  - Networking tips....44
  - Network considerations and constraints....44
  - About host files....45
  - Host Table tips....45

Chapter 3: Cabling K2 SAN devices....47
- To follow cabling instructions....48
- Basic K2 SAN - Online or Production....48
- Redundant K2 SAN - Online or Production....49
- Basic Nearline K2 SAN....50
- Redundant Nearline K2 SAN....50
- Cable K2 Summit system....51
  - K2-XDP basic....51
  - K2-XDP redundant....51
- Cable Ethernet switch....52
  - K2-SWE basic online/production....52
  - K2-SWE redundant online/production....53
  - K2-SWE basic nearline....54
  - K2-SWE redundant nearline....54
- Cable K2 Media Server....55
  - K2-SVR basic....55
  - K2-SVR redundant....55
- Cable NH10GE K2 Media Server....56
  - K2-SVR-NH10GE online/production....56
  - K2-SVR-NH10GE basic nearline....57

K2-SVR-NH10GE redundant nearline....57
Cable K2 RAID....57
K2 RAID basic online/production....58
K2 RAID redundant online/production....59
K2 RAID basic nearline....59
K2 RAID redundant nearline....60

Chapter 4: Setting up the K2 SAN infrastructure....63
Setting up the Ethernet switch....64
Configuring the Ethernet switch via serial connection....64
Configuring the Ethernet switch via the Web interface....67
Configuring QOS on the GigE switch....73
Verify flow control setting on the GigE switch....74
Upgrading firmware on HP switch....75
Setting up the control point PC....76
To fix NetCentral screen resolution problem....77
Install SiteConfig on control point PC....77

Chapter 5: Planning and implementing a K2 SAN with SiteConfig....81
About developing a system description....82
Importing a system description....82
About device and host names....83
Modifying a device name....83
Modifying the control network....83
Modifying the FTP/streaming network....85
Modifying a media (iSCSI) network....87
About IP configuration of network interfaces on devices....89
Placeholder device IP configuration....90
Discovered device IP configuration....90
Modifying K2 client unassigned (unmanaged) interface....91
Modifying K2 Media Server unassigned (unmanaged) interface....93
About SiteConfig support on K2 devices....96
Discovering devices with SiteConfig....96
Assigning discovered devices....97
Modifying K2 client managed network interfaces....98
Modifying K2 Media Server managed network interfaces....103
Making the host name the same as the device name....108
Pinging devices from the PC that hosts SiteConfig....109
About hosts files and SiteConfig....109
Generating host tables using SiteConfig....110

Chapter 6: Managing K2 Software....113
Configuring K2 software deployment....114
Configuring deployment groups....114
Adding a software package to a deployment group....115
Checking all currently installed software on devices....115
About deploying software for the K2 SAN....116
Backup and Recovery Strategies....116
About the recovery disk image process....116
Recommended recovery process....117
Creating a recovery disk image for storing on E:....118
Restoring from a system-specific recovery disk image on E:....119
Restoring from the generic recovery disk image on E:....120
Installing the Discovery Agent on a K2 Media Server....122
Setting up Windows....123
Activating the Windows operating system....123

Chapter 7: Configuring and licensing the K2 SAN.....125
About K2 SAN licensing.....126
About QOS on the K2 SAN.....126
Importing a SiteConfig system description.....127
Configuring the basic K2 SAN - Online and Production.....127
Prerequisites for initial configuration - Basic K2 SAN.....127
Defining a new K2 SAN.....129
Configuring the server - Part 1.....132
Configuring RAID.....136
Configuring the server - Part 2.....142
Configuring optional NH servers.....147
Configuring the redundant K2 SAN - Online and Production.....151
Prerequisites for initial configuration - Redundant K2 SAN.....151
Defining a new K2 SAN.....153
Configuring server A - Part 1.....156
Configuring RAID.....160
Configuring server A - Part 2.....169
Configuring server B.....173
Configuring optional NH servers.....181
Configuring the basic nearline K2 SAN.....187
Prerequisites for initial configuration - Basic nearline K2 SAN.....187
Defining a new K2 SAN.....188
Configuring NH server - Part 1.....192
Configuring RAID.....196
Configuring NH server - Part 2.....203
Configuring the redundant nearline K2 SAN.....205
Prerequisites for initial configuration - Nearline K2 SAN.....205
Defining a new K2 SAN.....206
Configuring NH server A - Part 1.....210
Configuring RAID.....214
Configuring NH server A - Part 2.....221
Configuring NH server B.....223

Chapter 8: Configuring clients on the K2 SAN.....229
About iSCSI bandwidth.....230
Determining K2 client bandwidth requirements.....230
K2 SAN prerequisites for adding clients.....230
Verify license on K2 Media Server.....231
Preparing K2 clients.....231
Installing Multi-Path I/O Software.....232
Configuring a K2 client for the K2 Storage System.....233
Configure page 1 - K2 client.....234
Configure Software Configuration page - K2 client.....235
Configure Network Configuration page - K2 client.....236
Configure Database Client Configuration page - K2 client.....237
Configure File System Client Configuration page.....238
Configure iSCSI Initiator Configuration page - K2 client.....239
Adding a generic client device.....241
Assigning a SAN client to different FTP server.....241
Powering on/off a SAN client.....242
Taking a SAN client offline.....242

Chapter 9: Operating the K2 SAN.....243
Powering off the K2 SAN.....244
Power off K2 Media Servers.....244

Power off K2 RAID....245
Power off remaining K2 SAN devices....245
Powering on the K2 SAN....245
Basic K2 SAN power on procedure....246
Redundant K2 SAN power on procedure....247
Nearline K2 SAN power on procedure....249
Powering on the HP ProCurve switch....250
Powering on the control point PC....250
Failover behaviors....250
Pre-failover behavior....251
Control Team failover behavior....251
K2 client media (iSCSI) connection failover behavior....252
K2 Media Server failover behavior....254
K2 Media Server failover with Control team failover behavior....255

Chapter 10: Description of K2 SAN Devices....257
Device terminology....258
Control point PC description....258
K2 Ethernet switch description....259
K2 Ethernet switch specifications....259
K2 Media Server description....260
K2 Media Server specifications....260
NH K2 Media Server....261
NH K2 Media Server specifications....261
K2 RAID storage description....261

Chapter 11: Overview of K2 Storage Tools....263
About SiteConfig....264
Opening SiteConfig....264
SiteConfig main window....264
K2Config....265
Opening the K2Config application....266
Server Control Panel....267
Storage Utility for K2 SAN....268
About RANKs and LUNs in Storage Utility....269
NetCentral....269
Windows Remote Desktop Connection....270
Accessing Remote Desktop Connection....270

Chapter 12: Administering and maintaining the K2 SAN....271
Passwords and security on Grass Valley systems....272
About application security on the K2 SAN....272
Modifying K2 SAN settings....273
Accessing K2 SAN features....274
About SiteConfig and K2Config settings....274
Renaming a K2 SAN....276
Adding devices to a K2 SAN....276
Removing a K2 SAN....278
Accessing a K2 SAN from multiple PCs....278
Taking a K2 SAN offline....279
Bringing a K2 SAN online....279
Viewing iSCSI assignments....280
Using reference files....280
Managing redundancy on a K2 SAN....281
Identifying current primary/backup K2 Media Servers....281
Triggering an intentional failover....283

Recovering from a failover....284
Working with K2 Media Servers....284
Accessing K2 Media Server features in the K2Config application....285
Taking a K2 Media Server out of service....285
Using the Stop button in Server Control Panel....286
Placing a K2 Media Server in service....287
Shutting down or restarting a K2 Media Server....287
Identifying K2 Media Server software versions....287
Modifying K2 Media Server network settings....287
Configuring Server 2008 for domain....288
Restoring network configuration....289
Removing a K2 Media Server....293
Replacing a K2 Media Server....293
Replacing an iSCSI interface adapter (TOE card)....295
Installing the Fibre Channel card driver....296
Recovering from a failed K2 Media Server system battery....296
Checking K2 Media Server services....297
Licensing a K2 Media Server....299
Working with K2 clients....301
Accessing K2 client features in the K2Config application....301
Shutting down or restarting a K2 client....302
Taking a K2 client offline....302
Bringing a K2 client online....302
Adding a K2 client....302
Removing a K2 client....303
Identifying K2 client software versions....303
Modifying K2 client control network settings....304
Modifying K2 client media (iSCSI) network settings....304
Enabling and disabling the write filter using K2Config....305
Configure live streaming multicast using K2Config....306
Using Storage Utility....308
Accessing Storage Utility....308
Overview of Storage Utility....309
Working on the media file system and database....309
Checking the media file system....310
Cleaning unreferenced files and movies....310
Making a new media file system....311
Expanding the media file system by capacity....313
Expanding the media file system by bandwidth....314
Recovering the media database....319
Working with RAID storage....320
Checking RAID storage subsystem status....321
Checking controller microcode....321
Identifying disks....321
Get controller logs....323
Unbind RANK....324
About full/background bind....325
Bind RANK....325
Binding Hot Spare drives....327
Loading RAID controller and expansion chassis microcode....327
Downloading disk drive firmware....328
Replacing a disk module....329
Replacing a controller....330
Configuring RAID chassis network and SNMP settings....331
Working with Ethernet switches....333
Design considerations for Ethernet switches....333
Configuring a switch through the K2Config application....335
Verifying spanning tree settings....335

Upgrading firmware on HP switch....338

Appendix A: Custom K2 SAN systems....341
About custom K2 SAN systems....342
About custom K2 SAN information....342
System diagrams....342
iSCSI extended (redundant FSMs)....343
Fibre Channel connected clients (redundant FSMs)....344
Explanations and procedures....345
General guidelines....345
K2 RAID Fibre Channel port redundant configuration....345
Installing SANsurfer Switch Manager software....347
Uninstalling SANsurfer Switch Manager software....347
Fibre Channel switch domains....347
Fibre Channel switch zoning....347
Fibre Channel fabric cabling....352

Appendix B: Trademarks and Agreements....355

Safety Summaries

Safety Summary

Read and follow the important safety information below, noting especially those instructions related to risk of fire, electric shock or injury to persons. Additional specific warnings not listed here may be found throughout the manual.

⚠	***WARNING: Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.***

Safety terms and symbols

Terms in this manual

Safety-related statements may appear in this manual in the following form:

⚠	***WARNING: Warning statements identify conditions or practices that may result in personal injury or loss of life.***
⚠	***CAUTION: Caution statements identify conditions or practices that may result in damage to equipment or other property, or which may cause equipment crucial to your business environment to become temporarily non-operational.***

Terms on the product

These terms may appear on the product:

DANGER — A personal injury hazard is immediately accessible as you read the marking.

WARNING — A personal injury hazard exists but is not immediately accessible as you read the marking.

CAUTION — A hazard to property, product, and other equipment is present.

Symbols on the product

The following symbols may appear on the product:

⚠	Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
⚠	Indicates that user, operator or service technician should refer to product manual(s) for important operating, maintenance, or service instructions.
⚠	This is a prompt to note fuse rating when replacing fuse(s). The fuse referenced in the text must be replaced with one having the ratings indicated.

	Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.
	Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.
	Indicates that static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Warnings

The following warning statements identify conditions or practices that can result in personal injury or loss of life.

Dangerous voltage or current may be present — Disconnect power and remove battery (if applicable) before removing protective panels, soldering, or replacing components.

Do not service alone — Do not internally service this product unless another person capable of rendering first aid and resuscitation is present.

Remove jewelry — Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.

Avoid exposed circuitry — Do not touch exposed connections, components or circuitry when power is present.

Use proper power cord — Use only the power cord supplied or specified for this product.

Ground product — Connect the grounding conductor of the power cord to earth ground.

Operate only with covers and enclosure panels in place — Do not operate this product when covers or enclosure panels are removed.

Use correct fuse — Use only the fuse type and rating specified for this product.

Use only in dry environment — Do not operate in wet or damp conditions.

Use only in non-explosive environment — Do not operate this product in an explosive atmosphere.

High leakage current may be present — Earth connection of product is essential before connecting power.

Dual power supplies may be present — Be certain to plug each power supply cord into a separate branch circuit employing a separate service ground. Disconnect both power supply cords prior to servicing.

Double pole neutral fusing — Disconnect mains power prior to servicing.

Use proper lift points — Do not use door latches to lift or move equipment.

Avoid mechanical hazards — Allow all rotating devices to come to a stop before servicing.

Cautions

The following caution statements identify conditions or practices that can result in damage to equipment or other property

Use correct power source — Do not operate this product from a power source that applies more than the voltage specified for the product.

Use correct voltage setting — If this product lacks auto-ranging power supplies, before applying power ensure that the each power supply is set to match the power source.

Provide proper ventilation — To prevent product overheating, provide equipment ventilation in accordance with installation instructions.

Use anti-static procedures — Static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Do not operate with suspected equipment failure — If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.

Ensure mains disconnect — If mains switch is not provided, the power cord(s) of this equipment provide the means of disconnection. The socket outlet must be installed near the equipment and must be easily accessible. Verify that all mains power is disconnected before installing or removing power supplies and/or options.

Route cable properly — Route power cords and other cables so that they ar not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.

Use correct power supply cords — Power cords for this equipment, if provided, meet all North American electrical codes. Operation of this equipment at voltages exceeding 130 VAC requires power supply cords which comply with NEMA configurations. International power cords, if provided, have the approval of the country of use.

Use correct replacement battery — This product may contain batteries. To reduce the risk of explosion, check polarity and replace only with the same or equivalent type recommended by manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Troubleshoot only to board level — Circuit boards in this product are densely populated with surface mount technology (SMT) components and application specific integrated circuits (ASICS). As a result, circuit board repair at the component level is very difficult in the field, if not impossible. For warranty compliance, do not troubleshoot systems beyond the board level.

Sicherheit – Überblick

Lesen und befolgen Sie die wichtigen Sicherheitsinformationen dieses Abschnitts. Beachten Sie insbesondere die Anweisungen bez glich

Brand-, Stromschlag- und Verletzungsgefahren. Weitere spezifische, hier nicht aufgef hrte Warnungen finden Sie im gesamten Handbuch.

⚠ ***WARNUNG: Alle Anweisungen in diesem Handbuch, die das Abnehmen der Geräteabdeckung oder des Gerätegehäuses erfordern, dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Um die Stromschlaggefahr zu verringern, führen Sie keine Wartungsarbeiten außer den in den Bedienungsanleitungen genannten Arbeiten aus, es sei denn, Sie besitzen die entsprechende Qualifikationen für diese Arbeiten.***

Sicherheit – Begriffe und Symbole

In diesem Handbuch verwendete Begriffe

Sicherheitsrelevante Hinweise k nnen in diesem Handbuch in der folgenden Form auftauchen:

⚠	***WARNUNG: Warnungen weisen auf Situationen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen.***
⚠	***VORSICHT: Vorsichtshinweise weisen auf Situationen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen oder zum zeitweisen Ausfall wichtiger Komponenten in der Arbeitsumgebung führen können.***

Hinweise am Produkt

Die folgenden Hinweise k nnen sich am Produkt befinden:

GEFAHR – Wenn Sie diesen Begriff lesen, besteht ein unmittelbares Verletzungsrisiko.

WARNUNG – Wenn Sie diesen Begriff lesen, besteht ein mittelbares Verletzungsrisiko.

VORSICHT – Es besteht ein Risiko f r Objekte in der Umgebung, den Mixer selbst oder andere Ausr stungskomponenten.

Symbole am Produkt

Die folgenden Symbole k nnen sich am Produkt befinden:

⚠	Weist auf eine gef hrliche Hochspannung im Ger tegeh use hin, die stark genug sein kann, um eine Stromschlaggefahr darzustellen.
⚠	Weist darauf hin, dass der Benutzer, Bediener oder Servicetechniker wichtige Bedienungs-, Wartungs- oder Serviceanweisungen in den Produkthandb chern lesen sollte.
⚠	Dies ist eine Aufforderung, beim Wechsel von Sicherungen auf deren Nennwert zu achten. Die im Text angegebene Sicherung muss durch eine Sicherung ersetzt werden, die die angegebenen Nennwerte besitzt.
⏚	Weist auf eine Schutzerdungsklemme hin, die mit dem Erdungskontakt verbunden werden muss, bevor weitere Ausr stungskomponenten angeschlossen werden.
⏚	Weist auf eine externe Schutzerdungsklemme hin, die als Erg nzung zu einem internen Erdungskontakt an die Erde angeschlossen werden kann.
⚠	Weist darauf hin, dass es statisch empfindliche Komponenten gibt, die durch eine elektrostatische Entladung besch digt werden k nnen. Verwenden Sie antistatische Prozeduren, Ausr stung und Oberfl chen w hrend der Wartung.

Warnungen

Die folgenden Warnungen weisen auf Bedingungen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen:

Gefährliche Spannungen oder Ströme – Schalten Sie den Strom ab, und entfernen Sie ggf. die Batterie, bevor sie Schutzabdeckungen abnehmen, l ten oder Komponenten austauschen.

Servicearbeiten nicht alleine ausführen – F hren Sie interne Servicearbeiten nur aus, wenn eine weitere Person anwesend ist, die erste Hilfe leisten und Wiederbelebungsmaßnahmen einleiten kann.

Schmuck abnehmen – Legen Sie vor Servicearbeiten Schmuck wie Ringe, Uhren und andere metallische Objekte ab.

Keine offen liegenden Leiter berühren – Ber hren Sie bei eingeschalteter Stromzufuhr keine offen liegenden Leitungen, Komponenten oder Schaltungen.

Richtiges Netzkabel verwenden – Verwenden Sie nur das mitgelieferte Netzkabel oder ein Netzkabel, das den Spezifikationen f r dieses Produkt entspricht.

Gerät erden – Schließen Sie den Erdleiter des Netzkabels an den Erdungskontakt an.

Gerät nur mit angebrachten Abdeckungen und Gehäuseseiten betreiben – Schalten Sie dieses Ger t nicht ein, wenn die Abdeckungen oder Geh useseiten entfernt wurden.

Richtige Sicherung verwenden – Verwenden Sie nur Sicherungen, deren Typ und Nennwert den Spezifikationen f r dieses Produkt entsprechen.

Gerät nur in trockener Umgebung verwenden – Betreiben Sie das Ger t nicht in nassen oder feuchten Umgebungen.

Gerät nur verwenden, wenn keine Explosionsgefahr besteht – Verwenden Sie dieses Produkt nur in Umgebungen, in denen keinerlei Explosionsgefahr besteht.

Hohe Kriechströme – Das Ger t muss vor dem Einschalten unbedingt geerdet werden.

Doppelte Spannungsversorgung kann vorhanden sein – Schließen Sie die beiden Anschlußkabel an getrennte Stromkreise an. Vor Servicearbeiten sind beide Anschlußkabel vom Netz zu trennen.

Zweipolige, neutrale Sicherung – Schalten Sie den Netzstrom ab, bevor Sie mit den Servicearbeiten beginnen.

Fassen Sie das Gerät beim Transport richtig an – Halten Sie das Ger t beim Transport nicht an T ren oder anderen beweglichen Teilen fest.

Gefahr durch mechanische Teile – Warten Sie, bis der L fter vollst ndig zum Halt gekommen ist, bevor Sie mit den Servicearbeiten beginnen.

Vorsicht

Die folgenden Vorsichtshinweise weisen auf Bedingungen oder Vorgehensweisen hin, die zu Sch den an Ausr stungskomponenten oder anderen Gegenst nden f hren k nnen:

Gerät nicht öffnen – Durch das unbefugte ffnen wird die Garantie ung ltig.

Richtige Spannungsquelle verwenden – Betreiben Sie das Ger t nicht an einer Spannungsquelle, die eine h here Spannung liefert als in den Spezifikationen f r dieses Produkt angegeben.

Gerät ausreichend belüften – Um eine berhitzung des Ger ts zu vermeiden, m ssen die Ausr stungskomponenten entsprechend den Installationsanweisungen bel ftet werden. Legen Sie kein Papier unter das Ger t. Es k nnte die Bel ftung behindern. Platzieren Sie das Ger t auf einer ebenen Oberfl che.

Antistatische Vorkehrungen treffen – Es gibt statisch empfindliche Komponenten, die durch eine elektrostatische Entladung besch digt werden k nnen. Verwenden Sie antistatische Prozeduren, Ausr stung und Oberfl chen w hrend der Wartung.

CF-Karte nicht mit einem PC verwenden – Die CF-Karte ist speziell formatiert. Die auf der CF-Karte gespeicherte Software k nnte gel scht werden.

Gerät nicht bei eventuellem Ausrüstungsfehler betreiben – Wenn Sie einen Produktschaden oder Ausr stungsfehler vermuten, lassen Sie die Komponente von einem qualifizierten Servicetechniker untersuchen.

Kabel richtig verlegen – Verlegen Sie Netzkabel und andere Kabel so, dass Sie nicht besch digt werden. St tzen Sie schwere Kabelb ndel ordnungsgem ß ab, damit die Anschl sse nicht besch digt werden.

Richtige Netzkabel verwenden – Wenn Netzkabel mitgeliefert wurden, erf llen diese alle nationalen elektrischen Normen. Der Betrieb dieses Ger ts mit Spannungen ber 130 V AC erfordert Netzkabel, die NEMA-Konfigurationen entsprechen. Wenn internationale Netzkabel mitgeliefert wurden, sind diese f r das Verwendungsland zugelassen.

Richtige Ersatzbatterie verwenden – Dieses Ger t enth lt eine Batterie. Um die Explosionsgefahr zu verringern, pr fen Sie die Polarit t und tauschen die Batterie nur gegen eine Batterie desselben Typs oder eines gleichwertigen, vom Hersteller empfohlenen Typs aus. Entsorgen Sie gebrauchte Batterien entsprechend den Anweisungen des Batterieherstellers.

Das Ger t enth lt keine Teile, die vom Benutzer gewartet werden k nnen. Wenden Sie sich bei Problemen bitte an den n chsten H ndler.

Consignes desécurité

Il est recommand de lire, de bien comprendre et surtout de respecter les informations relatives la s curit qui sont expos es ci-apr s, notamment les consignes destin es pr venir les risques d'incendie, les d charges lectriques et les blessures aux personnes. Les avertissements compl mentaires, qui ne sont pas n cessairement repris ci-dessous, mais pr sents dans toutes les sections du manuel, sont galement prendre en consid ration.

⚠ ***AVERTISSEMENT: Toutes les instructions présentes dans ce manuel qui concernent l'ouverture des capots ou des logements de cet équipement sont destinées exclusivement à des membres qualifiés du personnel de maintenance. Afin de diminuer les risques de décharges électriques, ne procédez à aucune intervention d'entretien autre que celles contenues dans le manuel de l'utilisateur, à moins que vous ne soyez habilité pour le faire.***

Consignes et symboles de sécurité

Termes utilisés dans ce manuel

Les consignes de s curit pr sent es dans ce manuel peuvent appara tre sous les formes suivantes :

⚠ ***AVERTISSEMENT: Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales.***

⚠ ***MISE EN GARDE: Les mises en garde signalent des conditions ou des pratiques susceptibles d'occasionner un endommagement à l'équipement ou aux installations, ou de rendre l'équipement temporairement non opérationnel, ce qui peut porter préjudice à vos activités.***

Signalétique apposée sur le produit

La signal tique suivante peut tre appos e sur le produit :

DANGER — risque de danger imminent pour l'utilisateur.

AVERTISSEMENT — Risque de danger non imminent pour l'utilisateur.

MISE EN GARDE — Risque d'endommagement du produit, des installations ou des autres quipements.

Symboles apposés sur le produit

Les symboles suivants peut tre appos s sur le produit :

	Signale la pr sence d'une tension lev e et dangereuse dans le bo tier de l' quipement ; cette tension peut tre suffisante pour constituer un risque de d charge lectrique.
	Signale que l'utilisateur, l'op rateur ou le technicien de maintenance doit faire r f rence au(x) manuel(s) pour prendre connaissance des instructions d'utilisation, de maintenance ou d'entretien.
	Il s'agit d'une invite prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait r f rence dans le texte doit tre remplac par un fusible du m me calibre.
	Identifie une borne de protection de mise la masse qui doit tre raccord e correctement avant de proc der au raccordement des autres quipements.
	I dentifie une borne de protection de mise la masse qui peut tre connect e en tant que borne de mise la masse suppl mentaire.
	Signale la pr sence de composants sensibles l' lectricit statique et qui sont susceptibles d' tre endommag s par une d charge lectrostatique. Utilisez des proc dures, des quipements et des surfaces antistatiques durant les interventions d'entretien.

Avertissements

Les avertissements suivants signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire m me fatales :

Présence possible de tensions ou de courants dangereux — Mettez hors tension, d branchez et retirez la pile (le cas ch ant) avant de d poser les couvercles de protection, de d faire une soudure ou de remplacer des composants.

Ne procédez pas seul à une intervention d'entretien — Ne r alisez pas une intervention d'entretien interne sur ce produit si une personne n'est pas pr sente pour fournir les premiers soins en cas d'accident.

Retirez tous vos bijoux — Avant de proc der une intervention d'entretien, retirez tous vos bijoux, notamment les bagues, la montre ou tout autre objet m tallique.

Évitez tout contact avec les circuits exposés — vitez tout contact avec les connexions, les composants ou les circuits expos s s'ils sont sous tension.

Utilisez le cordon d'alimentation approprié — Utilisez exclusivement le cordon d'alimentation fourni avec ce produit ou sp cifi pour ce produit.

Raccordez le produit à la masse — Raccordez le conducteur de masse du cordon d'alimentation la borne de masse de la prise secteur.

Utilisez le produit lorsque les couvercles et les capots sont en place — N'utilisez pas ce produit si les couvercles et les capots sont d pos s.

Utilisez le bon fusible — Utilisez exclusivement un fusible du type et du calibre sp cifi s pour ce produit.

Utilisez ce produit exclusivement dans un environnement sec — N'utilisez pas ce produit dans un environnement humide.

Utilisez ce produit exclusivement dans un environnement non explosible — N'utilisez pas ce produit dans un environnement dont l'atmosph re est explosible.

Présence possible de courants de fuite — Un raccordement la masse est indispensable avant la mise sous tension.

Deux alimentations peuvent être présentes dans l'équipement — Assurez vous que chaque cordon d'alimentation est raccord des circuits de terre s par s. D branchez les deux cordons d'alimentation avant toute intervention.

Fusion neutre bipolaire — D branchez l'alimentation principale avant de proc der une intervention d'entretien.

Utilisez les points de levage appropriés — Ne pas utiliser les verrous de la porte pour lever ou d placer l' quipement.

Évitez les dangers mécaniques — Laissez le ventilateur s'arr ter avant de proc der une intervention d'entretien.

Mises en garde

Les mises en garde suivantes signalent les conditions et les pratiques susceptibles d'occasionner des endommagements l' quipement et aux installations :

N'ouvrez pas l'appareil — Toute ouverture prohib e de l'appareil aura pour effet d'annuler la garantie.

Utilisez la source d'alimentation adéquate — Ne branchez pas ce produit une source d'alimentation qui utilise une tension sup rieure la tension nominale sp cifi e pour ce produit.

Assurez une ventilation adéquate — Pour viter toute surchauffe du produit, assurez une ventilation de l' quipement conform ment aux instructions d'installation. Ne d posez aucun document sous l'appareil – ils peuvent g ner la ventilation. Placez l'appareil sur une surface plane.

Utilisez des procédures antistatiques - Les composants sensibles l' lectricit statique pr sents dans l' quipement sont susceptibles d' tre endommag s par une d charge lectrostatique. Utilisez des proc dures, des quipements et des surfaces antistatiques durant les interventions d'entretien.

N'utilisez pas la carte CF avec un PC — La carte CF a t sp cialement format e. Le logiciel enregistr sur la carte CF risque d' tre effac .

N'utilisez pas l'équipement si un dysfonctionnement est suspecté — Si vous suspectez un dysfonctionnement du produit, faites inspecter celui-ci par un membre qualifi du personnel d'entretien.

Acheminez les câbles correctement — Acheminez les c bles d'alimentation et les autres c bles de mani re ce qu'ils ne risquent pas d' tre endommag s. Supportez correctement les enroulements de c bles afin de ne pas endommager les connecteurs.

Utilisez les cordons d'alimentation adéquats — Les cordons d'alimentation de cet quipement, s'ils sont fournis, satisfont aux exigences de toutes les r glementations r gionales. L'utilisation de cet quipement des tensions d passant les 130 V en c.a. requiert des cordons d'alimentation qui satisfont aux exigences des configurations NEMA. Les cordons internationaux, s'ils sont fournis, ont re u l'approbation du pays dans lequel l' quipement est utilis .

Utilisez une pile de remplacement adéquate — Ce produit renferme une pile. Pour r duire le risque d'explosion, v rifiez la polarit et ne remplacez la pile que par une pile du m me type, recommand e par le fabricant. Mettez les piles usag es au rebut conform ment aux instructions du fabricant des piles.

Cette unit ne contient aucune partie qui peut faire l'objet d'un entretien par l'utilisateur. Si un probl me survient, veuillez contacter votre distributeur local.

Certifications and compliances

Canadian certified power cords

Canadian approval includes the products and power cords appropriate for use in the North America power network. All other power cords supplied are approved for the country of use.

FCC emission control

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by Grass Valley can affect emission compliance and could void the user's authority to operate this equipment.

Canadian EMC Notice of Compliance

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le pr sent appareil num rique n' met pas de bruits radio lectriques d passant les limites applicables aux appareils num riques de la classe A pr scrites dans le R glement sur le brouillage radio lectrique dict par le minist re des Communications du Canada.

EN55103 1/2 Class A warning

This product has been evaluated for Electromagnetic Compatibility under the EN 55103-1/2 standards for Emissions and Immunity and meets the requirements for E4 environment.

This product complies with Class A (E4 environment). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC emission limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

Laser compliance

Laser safety requirements

This product may contain a Class 1 certified laser device. Operating this product outside specifications or altering its original design may result in hazardous radiation exposure, and may be considered an act of modifying or new manufacturing of a laser product under U.S. regulations contained in 21CFR Chapter 1, subchapter J or CENELEC regulations in HD 482 S1. People performing such an act are required by law to recertify and reidentify this product in accordance with provisions of 21CFR subchapter J for distribution within the U.S.A., and in accordance with CENELEC HD 482 S1 for distribution within countries using the IEC 825 standard.

Laser safety

Laser safety in the United States is regulated by the Center for Devices and Radiological Health (CDRH). The laser safety regulations are published in the "Laser Product Performance Standard," Code of Federal Regulation (CFR), Title 21, Subchapter J.

The International Electrotechnical Commission (IEC) Standard 825, "Radiation of Laser Products, Equipment Classification, Requirements and User's Guide," governs laser products outside the United States. Europe and member nations of the European Free Trade Association fall under the jurisdiction of the Comit Europ en de Normalization Electrotechnique (CENELEC).

Safety certification

This product has been evaluated and meets the following Safety Certification Standards:

Standard	Designed/tested for compliance with:
ANSI/UL 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
IEC 60950-1 with CB cert.	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition, 2005).
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
BS EN 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment 2006.

ESD Protection

Electronics today are more susceptible to electrostatic discharge (ESD) damage than older equipment. Damage to equipment can occur by ESD fields that are smaller than you can feel. Implementing the information in this section will help you protect the investment that you have made in purchasing Grass Valley equipment. This section contains Grass Valley's recommended ESD guidelines that should be followed when handling electrostatic discharge sensitive (ESDS) items. These minimal recommendations are based on the information in the *Sources of ESD and Risks* on page 21 area. The information in *Grounding Requirements for Personnel* on page 22 is provided to assist you in selecting an appropriate grounding method.

Recommended ESD Guidelines

Follow these guidelines when handling Grass Valley equipment:

- Only trained personnel that are connected to a grounding system should handle ESDS items.
- Do not open any protective bag, box, or special shipping packaging until you have been grounded.

  NOTE: When a Personal Grounding strap is unavailable, as an absolute minimum, touch a metal object that is touching the floor (for example, a table, frame, or rack) to discharge any static energy before touching an ESDS item.
- Open the anti-static packaging by slitting any existing adhesive tapes. Do not tear the tapes off.
- Remove the ESDS item by holding it by its edges or by a metal panel.
- Do not touch the components of an ESDS item unless it is absolutely necessary to configure or repair the item.
- Keep the ESDS work area clear of all nonessential items such as coffee cups, pens, wrappers and personal items as these items can discharge static. If you need to set an ESDS item down, place it on an anti-static mat or on the anti-static packaging.

Sources of ESD and Risks

The following information identifies possible sources of electrostatic discharge and can be used to help establish an ESD policy.

Personnel

One of the largest sources of static is personnel. The static can be released from a person's clothing and shoes.

Environment

The environment includes the humidity and floors in a work area. The humidity level must be controlled and should not be allowed to fluctuate over a broad range. Relative humidity (RH) is a major part in determining the level of static that is being generated. For example, at 10% - 20% RH a person walking across a carpeted floor can develop 35kV; yet when the relative humidity is increased to 70% - 80%, the person can only generate 1.5kV.

Static is generated as personnel move (or as equipment is moved) across a floor's surface. Carpeted and waxed vinyl floors contribute to static build up.

Work Surfaces

Painted or vinyl-covered tables, chairs, conveyor belts, racks, carts, anodized surfaces, plexiglass covers, and shelving are all static generators.

Equipment

Any equipment commonly found in an ESD work area, such as solder guns, heat guns, blowers, etc., should be grounded.

Materials

Plastic work holders, foam, plastic tote boxes, pens, packaging containers and other items commonly found at workstations can generate static electricity.

Grounding Requirements for Personnel

The information in this section is provided to assist you in selecting a grounding method. This information is taken from ANSI/ESD S20.20-2007 (Revision of ANSI/ESD S20.20-1999).

Product Qualification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ANSI/ESD S1.1 (Section 5.11)	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ANSI/ESD STM97.1	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ANSI/ESD STM97. 1ANSI/ESD STM97.2	< 10^9 ohm
	ANSI/ESD STM97.2	< 100 V

Product qualification is normally conducted during the initial selection of ESD control products and materials. Any of the following methods can be used: product specification review, independent laboratory evaluation, or internal laboratory evaluation.

Compliance Verification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ESD TR53 Wrist Strap Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 1.0 x 10^9 ohm

* For situations where an ESD garment is used as part of the wrist strap grounding path, the total system resistance, including the person, garment, and grounding cord, must be less than 3.5 x 10^7 ohm.

Preface

About this document

This is a K2™ product manual. It describes the K2 10G Storage Area Network (SAN) and provides instructions for installing and using the product in a variety of applications. The manual contains information for K2 storage in both basic (non-redundant) and redundant configurations. Refer to the sections that apply your K2 SAN's configuration. For custom K2 SANs that do not fit one of these pre-defined levels, you must work with your Grass Valley representative for installation and operation.

The K2 10G SAN, as documented with this manual, is characterized by 10 Gig iSCSI connections and 8 Gig Fibre Channel connections. The K2 10G SAN requires K2 software version 7.3 and higher. Some devices and/or systems used with older K2 SANs are not compatible with the K2 10G SAN system. Consult "K2 Release Notes" for compatibility information.

For information on products that are compatible as clients to the K2 SAN, refer to those product's manuals, such as the "STRATUS Installation and Service Manual" and the "K2 FCP Connect Installation Manual".

For more information

The following sections help you find the information you need in product manuals and elsewhere.

For the installer of a standalone K2 product with internal storage

If you are installing a K2 system, such as a K2 Summit/Solo system, with standalone internal storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of a K2 product with direct connect storage

If you are installing a standalone K2 system, such as a K2 Summit system, with direct connect external RAID storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of K2 Summit systems with K2 SAN shared storage

If you are installing a K2 SAN with connected K2 Summit systems, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 SAN Installation and Service Manual	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
5	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

K2 Release Notes

Contains the latest information about the software shipped on your system, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

Quick Start Guides

The Quick Start Guide is a printed document, shipped in the product packaging with K2 Summit/Solo systems and K2 Dyno Replay Controllers. The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.

K2 Storage Cabling Guide

The K2 Storage Cabling Guide is a printed document, shipped in the product packaging with the primary RAID storage chassis. The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.

K2 Documentation Set

Except for the release notes, the full set of support documentation, including this manual, is available in the K2 or K2/STRATUS Documentation Set. You can find the Documentation Set on the Grass Valley website. The following URL allows you to browse by K2 software version:

http://www.grassvalley.com/dl/k2_summit

You can also find the Documentation Set on the USB Recovery Flash drive that ships with your K2 Summit/Solo system.

The Documentation Set includes the following K2 product documents:

K2 AppCenter User Manual	Provides instructions for configuring and operating the media channels of product.
Quick Start Guides	The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.
K2 System Guide	Contains the product specifications and instructions for modifying system settings.
K2 Service Manuals	Contains information on servicing and maintaining the K2 product.
K2 SAN Installation and Service Manual	Contains installation, configuration, and maintenance procedures for shared storage options.
K2 Storage Cabling Guide	The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.
RAID Instruction Manuals	There is an Instruction Manual for each type of RAID storage device that can be a part of a K2 SAN. These manuals contain procedures for configuring and servicing the device.
Fibre Channel Switch Installation Manual	Contains information on configuring and servicing the Fibre Channel switch.

SiteConfig User Manual	Contains information on using SiteConfig, Grass Valley's system management tool, for network configuration and software deployment.

On-line Help Systems

You can find documentation online with products as follows:

K2 AppCenter Help	Contains information on using K2 AppCenter. In the AppCenter user interface menu bar select **Help**, then choose **AppCenter Help Topics** from the drop-down menu.
NetCentral Help	Contains information on using NetCentral. From the NetCentral interface select **Help | NetCentral Help Topics**.
SiteConfig Help	Contains information on using SiteConfig. In the SiteConfig user interface menu bar select **Help**, then choose **SiteConfig Help Topics** from the drop-down menu.

K2 FCP Connect documentation

The K2 FCP Connect product has its own documentation set, described as follows:

GV Connect User Manual	Provides instructions for using GV Connect, which is a Final Cut Pro plugin, to access and work with K2 assets. GV Connect is part of the K2 FCP Connect product.
GV Browse User Manual	Provides instructions for using GV Browse, which is a Final Cut Pro plugin, to access and work with assets on a MediaFrame server in an Aurora Browse system. GV Connect is part of the K2 FCP Connect product.
K2 FCP Connect Installation Manual	Provides detailed instructions to install and configure the K2 FCP Connect product.
K2 FCP Connect Release Notes	Contains the latest information about the K2 FCP Connect product, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

NetCentral documentation

The NetCentral product has its own documentation set, described as follows:

NetCentral Quick Start Guide	Provides an overview of the installation process to quickly set up and run NetCentral.
NetCentral Installation Guide	Identifies requirements and procedures to correctly set up servers and devices, as well as provides detailed instructions to install and configure NetCentral software.
NetCentral User Guide	Describes how to use the NetCentral Manager to monitor devices.

NetCentral Help	Contains information on using NetCentral. From the NetCentral interface select **Help	NetCentral Help Topics**.

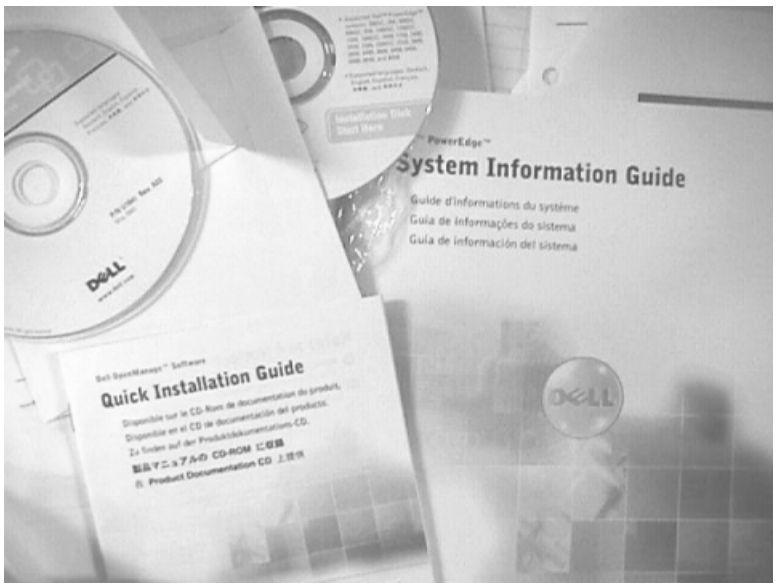
Grass Valley Website

This public Web site contains all the latest manuals and documentation, and additional support information. Use the following URL.

http://www.grassvalley.com.

Dell Server Documentation

If your system includes a Grass Valley product on a Dell server platform, refer to the applicable Grass Valley product manual for installation and configuration information. However, a full set of Dell server documentation has been provided on the *Dell Product Documentation* CD-ROM. Refer to the documents on this CD-ROM only as required by procedures in Grass Valley product manual.



Information referenced on the *Dell Product Documentation* CD-ROM includes, but is not limited to:

- Unpacking and rack-mounting
- Important safety and regulatory information
- Status indicators, messages, and error codes
- Troubleshooting help

⚠ ***CAUTION: Do not use the Dell Quick Installation Guide provided with the Dell CD-ROM package. This guide includes instructions for using the OpenManage software CD-ROM to install an operating system, which is not necessary on the Grass Valley product.***

Chapter 1

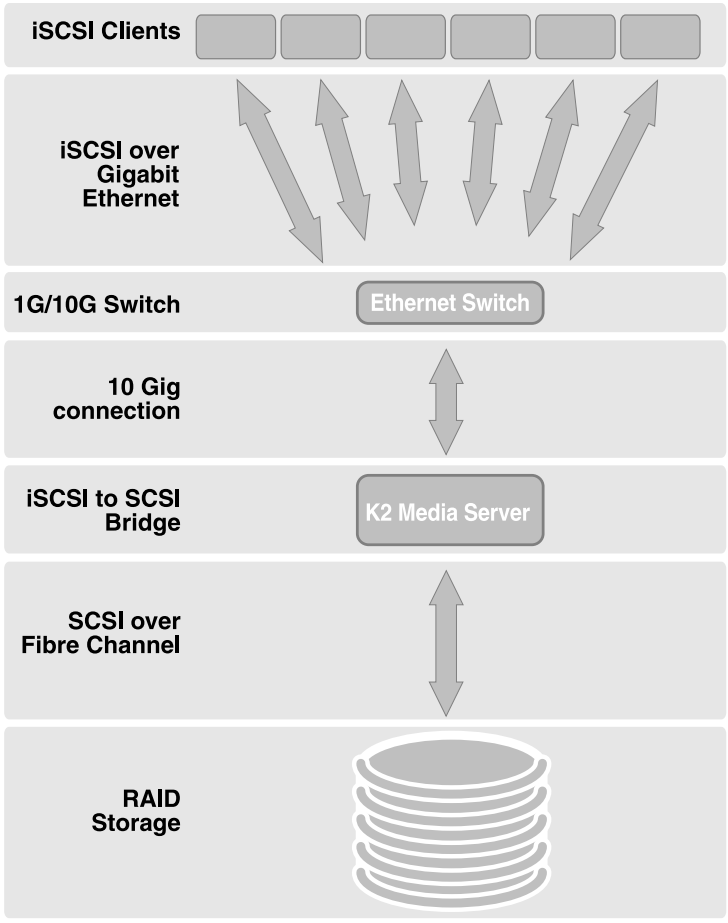
Product description

This section contains the following topics:

- *K2 SAN overview description*
- *K2 SAN key features*
- *What's new in the K2 10G SAN*
- *K2 Storage types and terms*
- *K2 SAN descriptions*

K2 SAN overview description

The K2 Storage Area Network (SAN) is Grass Valley's shared storage solution that gives multiple clients access to a common pool of media. In the iSCSI SAN, clients access the shared media storage via a Gigabit Ethernet network and a Fibre Channel connection. Data is communicated using the Small Computer System Interface (SCSI) data transfer interface and the Internet SCSI (iSCSI) protocol.



A custom-designed Fibre Channel SAN is also available in which clients access RAID storage via a Fibre Channel network, and the K2 Media Server connects via Ethernet for control functions only.

Refer to related topics in "K2 System Guide" for diagrams and explanations of the media file system and the media database.

K2 SAN key features

The key features of the iSCSI K2 SAN are as follows:

- iSCSI storage access protocol

- Gigabit Ethernet connectivity
- RAID 5 and RAID 6 storage
- FTP transfers
- Enhanced IT networked storage configurations to fit a wide variety of size and performance requirements.
- Scaling from 100 to < 5000 MB/s
- Redundancy and fault recovery with no single point of failure
- Tuned and optimized file system for reliable and robust transaction of media files
- Best in class storage management for high throughput, deterministic performance with load balancing, priority of service, and quality of service
- Best in class support for 3rd party editors

What's new in the K2 10G SAN

The primary differences between the K2 10G SAN and previous K2 SANs are as follows:

- 8 Gig Fibre Channel — An 8 Gig Fibre Channel card in the K2 Media Server and an 8 Gig controller in the K2 RAID support 8 Gig Fibre Channel connections. The K2 RAID chassis is unchanged. The previous K2 SANs supported 2 Gig or 4 Gig Fibre Channel connections.
- 10 Gig iSCSI — A 10 Gig iSCSI interface adapter (TOE) in the K2 Media Server and a 10 Gig SFP+ module in the Ethernet switch support a 10 Gig iSCSI connection. The 1 Gig iSCSI connections between SAN clients and the Ethernet switch remain unchanged. The previous K2 SANs used multiple 1 Gig interface adapters and 1 Gig Ethernet switch ports to provide iSCSI connections.
- K2 SAN simplification — The 10 Gig iSCSI connection allows most customer requirements to be met by a simple K2 SAN with one K2 Media Server, or two K2 Media Servers if redundant. The 1 Gig iSCSI connection of the previous K2 SANs needed multiple K2 Media Servers to meet customer requirements for higher bandwidth.
- K2 SAN license — A license enables bandwidth in increments for a single 10 Gig iSCSI interface adapter, rather than requiring multiple iSCSI interface adapters as in the previous K2 SANs.
- 64-bit K2 Media Server — The 64-bit operating system supports increased performance. The previous K2 Media Servers were 32-bit devices only.
- Third level of Quality of Service (QOS) — Editors and other generic file system clients can be assigned their own portion of K2 SAN bandwidth. The previous K2 SANs required additional iSCSI interface adapters to statically manage this type of bandwidth.

If you are familiar with previous K2 SANs, keep these differences in mind as you read about the K2 10G SAN in this manual. If you need information about previous K2 SANs, refer to previous versions of this manual.

Related Topics

K2 SAN descriptions on page 32

About K2 SAN licensing on page 126

K2 Media Server description on page 260

About QOS on the K2 SAN on page 126

K2 Storage types and terms

Grass Valley configures K2 storage to meet their customer's workflow needs. This topic describes some typical configurations and terminology.

Online – Online storage is considered "Tier 1" K2 storage in that it is suitable for both record and play. The purpose of an online SAN is to record and play media for broadcast or other on-air applications. Performance requirements are critical for online applications, so this type of SAN features high performance, low latency storage. Online storage can be iSCSI or Fibre Channel.

Production – Production storage is considered "Tier 2" K2 storage in that it is suitable for record (ingest) but not recommended for on-air playout. The purpose of production storage is to provide cost effective storage for production and editing applications. These applications require high performance but internal buffering in editing software puts less stress on the storage system, so performance requirements are lower than for online storage. Therefore, production storage can use low cost, high capacity drives, such as 7.2K SAS drives. In a typical workflow, production is finished on the production storage and then the content is pushed to an online K2 system for playout. Production storage is configured similar to Online storage, but with the 7.2K SAS RAID devices and drives. Production storage can be iSCSI or Fibre Channel.

Nearline – Nearline storage is considered "Tier 3" K2 storage in that it is suitable for media file transfer but does not support either record or play. The purpose of a nearline SAN is to provide a large pool of storage to which files can be saved. The nearline system is considered an "offline" system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system. The files on a nearline system can be readily available to an online K2 system via FTP or CIFS connections over Ethernet. Nearline storage has Fibre Channel connections between the K2 Media Server and the RAID storage devices.

Workgroup – Workgroup storage is a Fibre-Channel-only type of production storage intended for small workgroups. This type of storage is no longer recommended, as technology advances provide better value with standard iSCSI Production storage.

Live Production – In K2Config you can create a Live Production K2 SAN. This mode can be applied to online and production SANs. A K2 SAN with LIve Production mode has a shorter minimum delay between start record and start playout and is ideal for use with K2 Dyno. To support this mode, Grass Valley must design your K2 SAN for increased bandwidth.

Stand-alone – This is not shared storage. It is the local storage for a K2 Media Client, K2 Summit Production Client, or K2 Solo Media Server. Stand-alone storage can be internal media drives or direct-connect K2 RAID devices. Refer to the *K2 System Guide*.

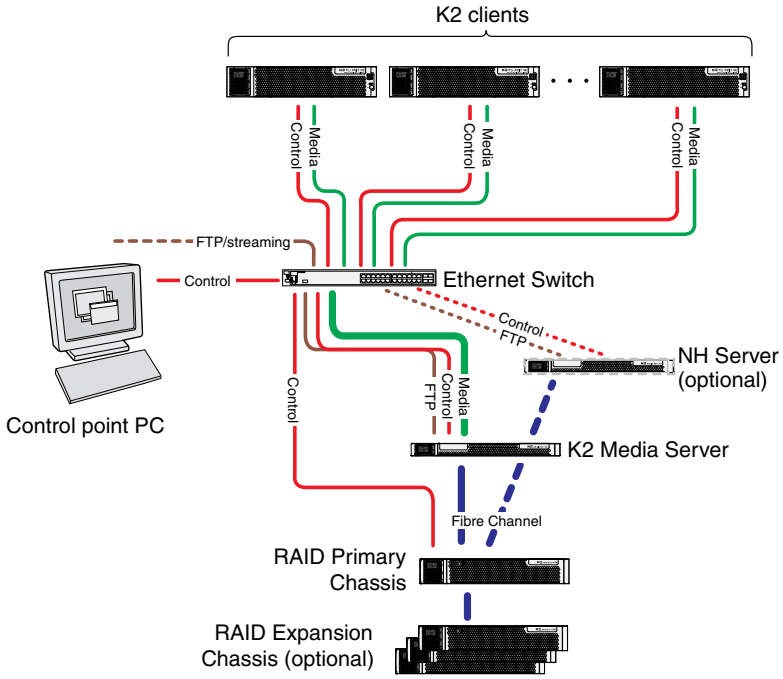
K2 SAN descriptions

The following sections describe the standard, pre-defined structures of the K2 SAN. Refer to related topics in this document for more information on custom K2 SAN systems.

Related Topics

About custom K2 SAN systems on page 342

Basic K2 SAN description



The basic (non-redundant) K2 SAN can be an online SAN or a production SAN. The SAN has one Ethernet switch, one K2 Media Server, and one basic K2 RAID chassis. Up to eleven RAID Expansion chassis are optional for increased storage capacity.

K2 clients and other iSCSI clients, such as Aurora Edits, are connected to the Ethernet switch. Each K2 client has one GigE connection for media and one GigE connection for control. The GigE switch is configured with V-LANs to keep the control/FTP traffic and the media (iSCSI) traffic separate.

The K2 Media Server has one 10 Gig connection for media (iSCSI), one GigE connection for control, one GigE connection for FTP, and one Fibre Channel connection to the RAID storage. The server hosts an iSCSI interface card for the 10 Gig media connection and a Fibre Channel card for the RAID storage connection. The iSCSI interface card provides a bridge between iSCSI and Fibre Channel SCSI. The server also hosts software components that allow it to function in various roles, including media file system manager, media database server, and FTP server.

The basic K2 RAID chassis is connected via a single Fibre Channel connection to the K2 Media Server. It is also connected to the GigE control network, which is required for SNMP (NetCentral) monitoring.

Optional 10 Gig NH K2 Media Servers are available to provide additional FTP bandwidth. If the optional NH server is used, all FTP traffic goes to this server, so the K2 Media Server is not cabled or configured for FTP.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

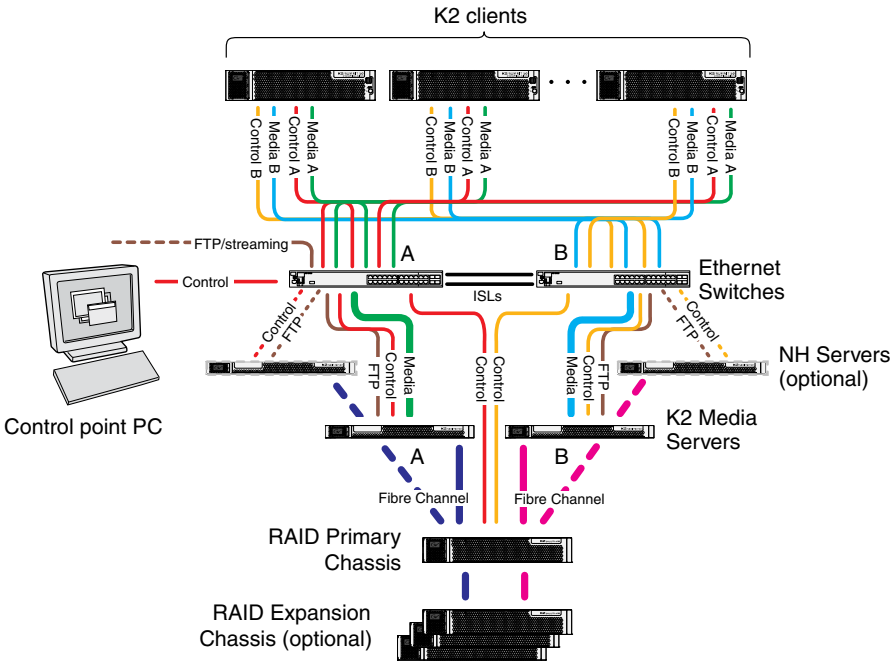
FTP/streaming traffic accesses the K2 SAN via the FTP GigE port on K2 Media Servers. FTP/streaming traffic does not go to K2 clients.

Related Topics

Description of K2 SAN Devices on page 257

Working with Ethernet switches on page 333

Redundant K2 SAN description



The redundant K2 SAN can be an online SAN or a production SAN. The SAN has two Ethernet switches connected by Inter-Switch Links (ISLs) to support a redundant Ethernet fabric. The SAN also has redundant K2 Media Servers. The servers are configured to have identical roles. This provides redundancy for database, file system, iSCSI bridge, and FTP roles. One K2 RAID supports redundant Fibre Channel connections. Up to eleven Expansion chassis are optional for increased storage capacity.

K2 clients have a pair of redundant (teamed) Gigabit Ethernet ports for control and two Gigabit Ethernet ports (A and B) for media (iSCSI). Each port of the control team is connected to a different switch. The A media port goes to the A switch and the B media port goes to the B switch. The switches are configured with V-LANs to keep the control/FTP and media (iSCSI) traffic separate.

Each K2 Media Server has one 10 Gig connection for media (iSCSI), one GigE connection for control, one GigE connection for FTP, and one Fibre Channel connection to the RAID storage. All GigE connections and the 10 Gig connection on a server go to the same GigE switch. The server hosts a 10 Gig iSCSI interface card for the 10 Gig media connections and a Fibre Channel card for the RAID storage connection. The iSCSI interface card provides a bridge between iSCSI and Fibre Channel SCSI. The server also hosts software components that allow it to function in its roles,

including media file system manager, media database server, and FTP server. Redundant K2 Media Servers are connected by a serial cable which supports the heartbeat signal required for automatic system recovery (failover) features.

The redundant K2 RAID chassis has redundant RAID controllers to support the Fibre Channel connections from the K2 Media Servers. The redundant K2 RAID chassis is also connected to the GigE control network, which is required for SNMP (NetCentral) monitoring.

On the redundant K2 RAID chassis there are two RAID 1 RANKs (also know as LUNs) for media file system metadata files and journal files. The remainder of the RAID storage is RAID 5 or RAID 6 for media.

Optional 10 Gig NH K2 Media Servers are available to provide additional FTP bandwidth. If the optional NH server is used, all FTP traffic goes to this server, so neither K2 Media Server is cabled or configured for FTP.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

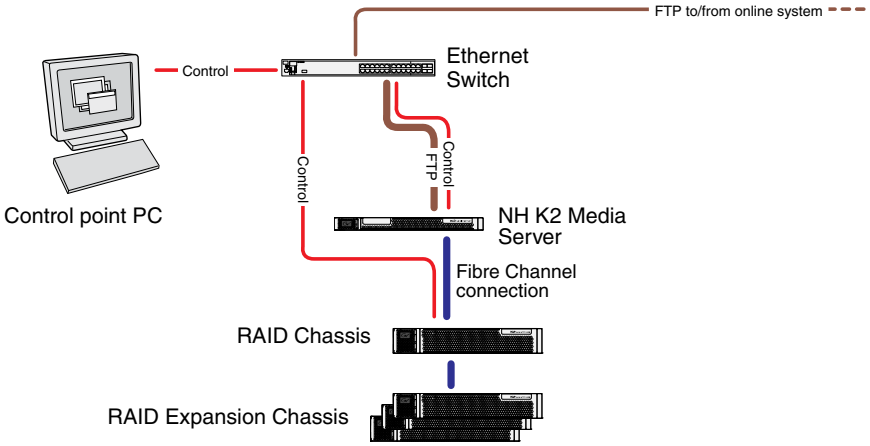
FTP/streaming traffic accesses the K2 SAN via the FTP GigE port on K2 Media Servers. FTP/streaming traffic does not go to K2 clients.

Related Topics

Description of K2 SAN Devices on page 257

Working with Ethernet switches on page 333

Basic Nearline K2 SAN description



The purpose of a Nearline SAN is to provide a large pool of storage to which files can be saved. The Nearline system is considered an “offline” system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system. This is because the Nearline system has no media database to support “movies” or “clips”, such as there is on an “online” K2 SAN. However, the files on a Nearline system can be readily available to an online K2 system via FTP transfer.

The basic Nearline SAN has one Ethernet switch.

The SAN also has one 10 Gig NH K2 Media Server. The NH server for a Nearline system has two ports for Fibre Channel connections. NH servers do not have media (iSCSI) ports.

A NH server on a Nearline system is configured with roles of FTP server and Media file system server.

In the Nearline system no K2 Media Servers take the role of iSCSI bridge or media database server.

No K2 clients or any other generic client are part of the Nearline system.

7.2K SAS drives provide the media file storage on a Nearline system. While these drives do not provide the high bandwidth of the drives required by an online K2 SAN, they offer larger capacity and lower cost. This makes these drives ideal for the Nearline SAN.

The primary RAID chassis has one controller. The primary RAID chassis is connected via Fibre Channel to the NH server. The controller in the RAID chassis is also connected to the GigE control network, which is required for SNMP (NetCentral) monitoring.

There must be one primary RAID chassis and may be up to eleven optional Expansion chassis. Primary chassis and Expansion chassis contain twelve drives. All disks in both primary and optional Expansion chassis are bound as RAID 6.

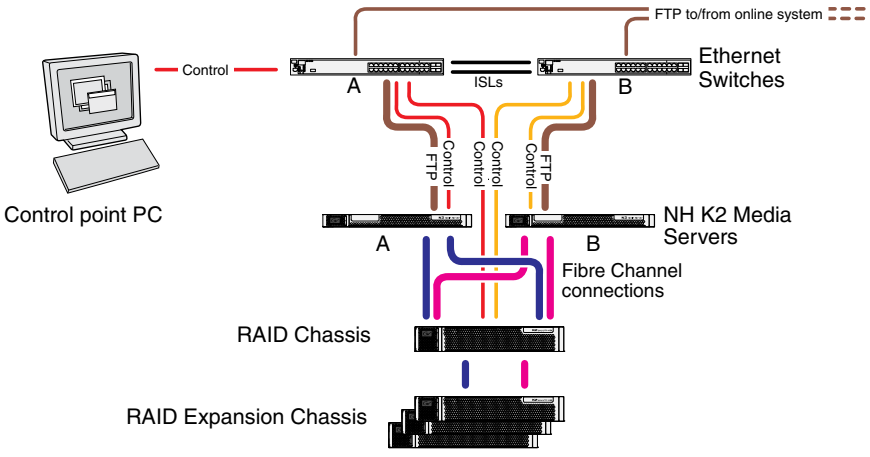
The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

Related Topics

Description of K2 SAN Devices on page 257

Working with Ethernet switches on page 333

Redundant Nearline K2 SAN description



The purpose of a Nearline SAN is to provide a large pool of storage to which files can be saved. The Nearline system is considered an “offline” system, which means the system stores files only, such GXF files or MXF files, with no ability to record or play those files directly on the system.

This is because the Nearline system has no media database to support “movies” or “clips”, such as there is on an “online” K2 SAN. However, the files on a Nearline system can be readily available to an online K2 system via FTP transfer.

The redundant Nearline SAN has two Ethernet switches, connected by Inter-Switch Links (ISLs) to support a redundant Ethernet fabric.

The SAN also has two 10 Gig NH K2 Media Servers. The NH server for a Nearline system has two ports for Fibre Channel connections. NH servers do not have media (iSCSI) ports.

A NH server on a Nearline system is configured with roles of FTP server and Media file system server. On a redundant system these roles are identical on both servers and provide redundancy as follows:

- FTP server — Both servers are active in this role simultaneously. To provide FTP redundancy in the event of a server failure, your facility’s FTP system must be able to access alternate FTP servers.
- Media file system server — Only one server is active at any one time in this role, and the media file system provides redundancy. If a fault occurs on the active server, one of the other servers automatically takes over as the active media file system server.

In the Nearline system no K2 Media Servers take the role of iSCSI bridge or media database server.

No K2 clients or any other generic client are part of the Nearline system.

7.2K SAS drives provide the media file storage on a Nearline system. While these drives do not provide the high bandwidth of the drives required by an online K2 SAN, they offer larger capacity and lower cost. This makes these drives ideal for the Nearline SAN.

The primary RAID chassis has two controllers. The primary RAID chassis is connected via Fibre Channel to the NH server. These Fibre Channel connections access the disks simultaneously for redundancy and increased bandwidth. Each controller in the RAID chassis is also connected to the GigE control network, which is required for SNMP (NetCentral) monitoring.

There must be one primary RAID chassis and may be up to eleven optional Expansion chassis. Primary chassis and Expansion chassis contain twelve drives. All disks in both primary and optional Expansion chassis are bound as RAID 6.

The K2Config control point PC is connected to the GigE control network. The K2Config application runs on this PC for configuring the SAN. The SiteConfig application also runs on this PC.

Related Topics

Description of K2 SAN Devices on page 257

Working with Ethernet switches on page 333

Chapter 2

Preparing for installation

This section contains the following topics:

- *K2 SAN installation checklists*
- *Understanding system concepts*

K2 SAN installation checklists

Use the following sequence of checklists to guide the overall task flow of installing and commissioning a K2 SAN.

Pre-installation planning checklist

	Task	Instructions	Comment
☐	Procure existing or create new SiteConfig system description	*About developing a system description* on page 82	You can do this before arriving at the customer site.
☐	Next: Infrastructure checklist		

Infrastructure checklist

	Task	Instructions	Comment
☐	Rack and cable	*Cabling K2 SAN devices* on page 47	—
☐	Configure Ethernet switch(es)	*Setting up the Ethernet switch* on page 64	—
☐	Install/update SiteConfig on control point PC	*Install SiteConfig on control point PC* on page 77	—
☐	For K2 Summit Production Clients, disable the write filter.	K2 System Guide	You must connect keyboard, monitor, and mouse and do this on each K2 Summit Production Client before managing with SiteConfig.
☐	Next: Network setup and implementation checklist		

Network setup and implementation checklist

	Task	Instructions	Comment
☐	Import or create the SiteConfig system description on the control point PC	*Importing a system description* on page 82	Select IP address range for each network and each device type.
☐	Modify names and networks in the SiteConfig system description.	*Modifying a device name* on page 83, *Modifying the control network* on page 83, *Modifying the FTP/streaming network* on page 85, *Modifying a media (iSCSI) network* on page 87	Set subnet mask and other settings.

	Task	Instructions	Comment
☐	Verify/modify device interfaces	*Modifying K2 client unassigned (unmanaged) interface* on page 91, *Modifying K2 Media Server unassigned (unmanaged) interface* on page 93	Do not proceed until the system description accurately represents all aspects of the actual system. Refer to SiteConfig Help Topics . Use procedures as appropriate for your site.
☐	Discover devices	*Discovering devices with SiteConfig* on page 96	Make sure the write filter is disabled (device is unlocked) on K2 Summit Production Clients.
☐	Assign placeholder devices to discovered devices	*Assigning discovered devices* on page 97	—
☐	Configure IP settings of network interfaces on discovered devices	*Modifying K2 client managed network interfaces* on page 98, *Modifying K2 Media Server managed network interfaces* on page 103	—
☐	Configure names	*Making the host name the same as the device name* on page 108	—
☐	Validate networks	*Pinging devices from the PC that hosts SiteConfig* on page 109	—
☐	Distribute host table information	*Generating host tables using SiteConfig* on page 110	—
☐	Next: Software update checklist		

Software update checklist

	Task	Instructions	Comment
☐	Create deployment groups	*Configuring deployment groups* on page 114	—
☐	Place software on control point PC	*Adding a software package to a deployment group* on page 115	—
☐	Check software on devices	*Checking all currently installed software on devices*	—
☐	Upgrade/install software to devices from control point PC	*About deploying software for the K2 SAN* on page 116	Refer to *K2 Release Notes*. Make sure the write filter is disabled (device is unlocked) on K2 Summit Production Clients.

	Task	Instructions	Comment
☐	Next: SAN configuration checklist		

SAN configuration checklist

	Task	Instructions	Comment
☐	Import SiteConfig system description into K2Config	*Importing a SiteConfig system description* on page 127	—
☐	Configure SAN in K2Config	*Configuring and licensing the K2 SAN* Use the appropriate instructions for your K2 SAN.	Make sure the write filter is disabled (device is unlocked) on K2 Summit Production Clients.
☐	Verify SAN license	*Verify license on K2 Media Server* on page 231	The K2 Media Server with role of file system server must be licensed for your SAN's design and bandwidth requirements.
☐	Add K2 clients to SAN	*Configuring a K2 client for the K2 Storage System* on page 233	—
☐	K2 SAN installation complete		

Understanding system concepts

Make sure you understand the following system concepts before planning or implementing a K2 SAN.

Control network description

The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network must be on a different subnet than the streaming/FTP network and the media (iSCSI) network. The control network and the streaming/FTP network may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the control network.

The control network applies to both online, production, and nearline K2 SANs.

All the devices of the K2 SAN are on the control network. Stand-alone K2 clients can also be on the same control network.

Redundant K2 SANs have one control network with hardware separated into an A side and a B side. There is an A Ethernet switch and a B Ethernet switch. Switches are connected by InterSwitch Links

(ISLs or trunks) to provide redundant paths for control network traffic. On a redundant K2 SAN, devices are on the control network as follows:

- Shared Storage K2 client - The two control GigE ports are configured as a team. The control team shares a single IP address. One port of the team is on the A side and the other port of the team is on the B side.
- K2 Media Server - Redundant K2 Media Servers with role of media file system/metadata server are balanced between the A and B sides. One server is on the A side and the other server is on the B side. K2 Media Servers with other roles, such as FTP server, are likewise balanced between A and B sides.
- K2 RAID - When a K2 RAID device has redundant controllers, controller 0 is on the A side and controller 1 is on the B side.
- Ethernet switch - For control and configuration, the A switch is on the A side and the B switch is on the B side

Streaming/FTP network description

The streaming/FTP network is for media transfers and FTP traffic. It must be on a different subnet than the control network and the media (iSCSI) network. The control network and the streaming/FTP network may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Hostnames of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the *_he0* suffix. This directs the streaming traffic to the correct port.

The streaming/FTP network applies to both online and nearline K2 SANs. For nearline systems, this is the primary network for moving media to and from the storage system.

Redundant K2 SANs have one streaming/FTP network with hardware separated into an A side and a B side. There is an A Ethernet switch and a B Ethernet switch. Switches are connected by InterSwitch Links (ISLs) to provide redundant paths for streaming/FTP traffic.

Only those K2 devices that host a K2 FTP interface are on the streaming/FTP network, as follows:

- K2 Media Servers - Those with the role of FTP server are connected via their dedicated FTP port. On a redundant K2 SAN, if you have multiple K2 Media Servers with role of FTP server, balance servers between the A and B sides.
- Stand-alone K2 clients - While not a part of a K2 SAN, stand-alone K2 clients can also be on the streaming/FTP network. Connect to the dedicated FTP port.

NOTE: Shared storage K2 clients are not on the streaming/FTP network. They do not have a FTP interface and they do not send or receive streaming/FTP traffic.

Automatic FTP server failover is not provided by the K2 SAN. If you require automatic failover to a redundant FTP server for your streaming/FTP traffic, you must provide it through your FTP application.

Media (iSCSI) network description

The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

The media network applies to online K2 SANs. Nearline K2 SANs do not have a media network.

Redundant K2 SANs have redundant media networks: an A media network and a B media network. The two networks are on separate subnets and are also physically separated onto the A Ethernet switch and the B Ethernet switch. InterSwitch Links (ISLs) between switches do not carry media (iSCSI) traffic. ISLs provide redundant paths for control network traffic and streaming/FTP network traffic only.

Devices are on the media network as follows:

- Shared Storage K2 client - On a non-redundant K2 SAN, the A media port connects to the media network. On a redundant K2 SAN, the A media port connects to the A media network and the B media port connects to the B media network.
- K2 Media Server - A server has one port available for connection to a media network. This is a 10 Gig iSCSI interface adapter, which supports the functionality of a TCP/IP Offload Engine (TOE). On a redundant K2 SAN, one server is on the A media network and one server is on the B media network.

Networking tips

- Before configuring any devices for networks, determine the full scope of IP addresses and names needed for the all the machines in your system. Work with the network administrator at your facility to have IP addresses and names available for your use.
- It is recommended that you use the patterns offered in SiteConfig by default to establish a consistent convention for machine names and IP addresses. You can plan, organize, and enter this information in SiteConfig as you develop a system description. You can do this even before you have devices installed and/or cabled.
- On 64-bit devices, configure IPv4 addresses. Disable the IPv6 interface of the Control and FTP interfaces. SiteConfig always configures IPv4 addresses for 64-bit devices.

Network considerations and constraints

- Do not use any 10.1.0.n IP addresses. These are used by the K2 RAID (NEC Condor) maintenance port and must be reserved for that purpose. If these addresses are otherwise used, maintenance port communication errors occur.

About host files

The hosts file is used by the control network and the streaming/FTP network for name resolution, which determines the IP address of a device on the network when only the device name (hostname) is given. The hosts file is located at *C:\Windows\system32\drivers\etc\hosts* on Windows XP and later operating systems. The hosts file must be the same on all network devices. It includes the names and addresses of all the devices on the network.

For FTP transfers on a K2 SAN, transfers go to/from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. To support FTP transfers, in the hosts file the K2 Media Server hostname must have the *_he0* extension added at the end of the name and that hostname must be associated with the K2 Media Server's FTP/streaming network IP address.

Here is an example of IP addresses and names associated in a hosts file:

```
192.168.100.11   root_server_1
192.168.101.11   root_server_1_he0
192.168.100.21   root_server_2
192.168.101.21   root_server_2_he0
192.168.100.31   root_server_3
192.168.101.31   root_server_3_he0
192.168.100.41   root_server_4
192.168.101.41   root_server_4_he0
192.168.100.51   root_raid_1
192.168.100.61   root_gige_1
```

In this example 192.168.100.xx is the control network and 192.168.101.xx is the streaming/FTP network. Each K2 Media Server has its hostname associated with its control network IP address. In addition, each K2 Media Server (that has the role of FTP server) has its *_he0* hostname associated with its streaming/FTP network address.

Use SiteConfig to define your networks and devices. When you do so, SiteConfig creates the correct hosts file and copies the hosts file to each network device. This enforces consistent hosts files across networks and reduces errors introduced by editing and copying hosts files on individual devices. You can also view hosts files from SiteConfig for troubleshooting purposes.

Host Table tips

- If transferring to or from a Profile XP or Open SAN system via UIM, the hosts file must also follow UIM naming conventions for those systems. Refer to the *UIM Instruction Manual*.
- Do not enable name resolutions for media (iSCSI) network IP addresses in the hosts file, as hostname resolution is not required for the media network. If desired, you can enter media network information in the hosts file as commented text as an aid to managing your networks.

- Use the following tip with care. While it can solve a problem, it also introduces a name resolution "anomaly" that might be confusing if not considered in future troubleshooting activities.

  For each SAN (shared storage) K2 client, add the "_he0" suffix to the hostname but then associate that hostname with the K2 Media Server's FTP/streaming network IP address, not the K2 client's IP address. Aliasing K2 client hostnames in this way would not be required if the transfer source/destination was always correctly specified as the K2 Media Server. However, a common mistake is to attempt a transfer in which the source/destination is incorrectly specified as the K2 client. The host file aliasing corrects this mistake and redirects to the K2 Media Server, which is the correct transfer source/destination.

  An example of a hosts file entry with this type of aliasing is as follows:

  ```
  192.168.101.11 server_1_he0 client_1_he0 client_2_he0
  ```

Chapter 3

Cabling K2 SAN devices

This section contains the following topics:

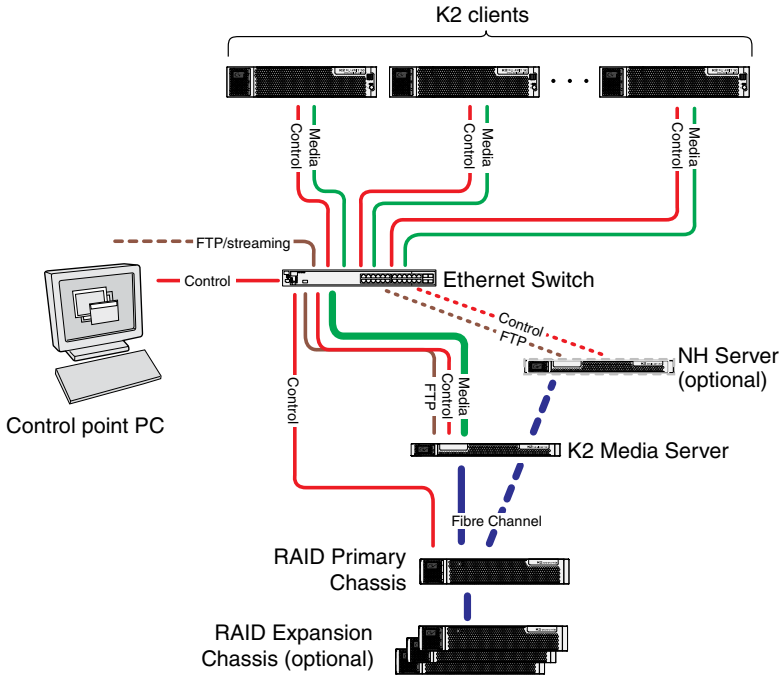
- *To follow cabling instructions*
- *Basic K2 SAN - Online or Production*
- *Redundant K2 SAN - Online or Production*
- *Basic Nearline K2 SAN*
- *Redundant Nearline K2 SAN*
- *Cable K2 Summit system*
- *Cable Ethernet switch*
- *Cable K2 Media Server*
- *Cable NH10GE K2 Media Server*
- *Cable K2 RAID*

To follow cabling instructions

To follow cabling instructions for your K2™ Storage Area Network (SAN), do the following:

1. Find the system cabling diagram that matches your K2 system.
2. Follow the references below the system diagram to locate cabling instructions for the individual devices of your K2 system.

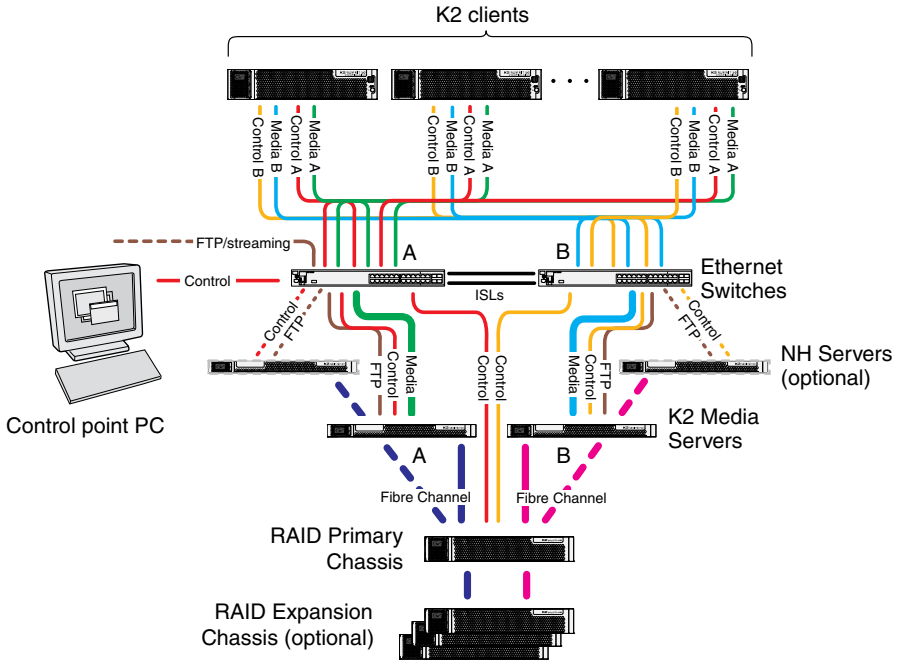
Basic K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Summit system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP basic* on page 51
Gigabit Ethernet Switch	HP 2910	*K2-SWE basic online/production* on page 52
K2 Media Server	Dell R610	*K2-SVR basic* on page 55
NH10GE K2 Media Server (optional)	Dell R610	*K2-SVR-NH10GE online/production* on page 56
K2 RAID	K2 RAID	*K2 RAID basic online/production* on page 58

This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

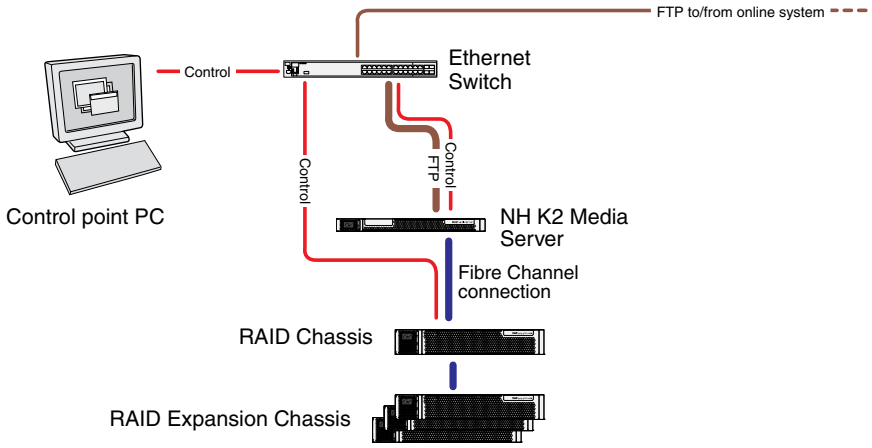
Redundant K2 SAN - Online or Production



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
K2 Summit system	K2 Summit 3G system or first generation K2 Summit system	*K2-XDP redundant* on page 51
Gigabit Ethernet Switch	HP 2910	*K2-SWE redundant online/production* on page 53
K2 Media Server	Dell R610	*K2-SVR redundant* on page 55
NH10GE K2 Media Server (optional)	Dell R610	*K2-SVR-NH10GE online/production* on page 56
K2 RAID	K2 RAID	*K2 RAID redundant online/production* on page 59

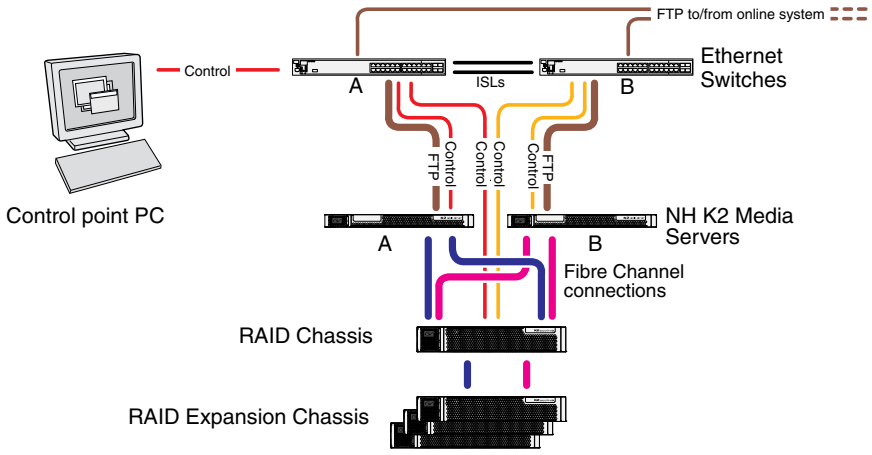
This manual documents the default GigE switch configuration. Other configurations are available, depending on your port count and FTP bandwidth requirements.

Basic Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 2910	*K2-SWE basic nearline* on page 54
NH10GE K2 Media Server	Dell R610	*K2-SVR-NH10GE basic nearline* on page 57
K2 RAID	K2 10G RAID	*K2 RAID basic nearline* on page 59

Redundant Nearline K2 SAN



To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
Gigabit Ethernet Switch	HP 2910	*K2-SWE redundant nearline* on page 54

To cable this K2 SAN device…	Of this model or platform…	Turn to these instructions:
NH10GE K2 Media Server	Dell R610	*K2-SVR-NH10GE redundant nearline* on page 57
K2 RAID	K2 10G RAID	*K2 RAID redundant nearline* on page 60

Cable K2 Summit system

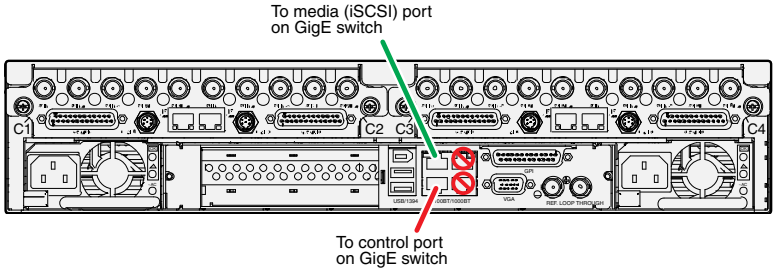
As directed by the system diagram for your K2 storage, cable the K2 Summit system using the instructions in this section.

K2-XDP basic

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a basic (non-redundant) online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.

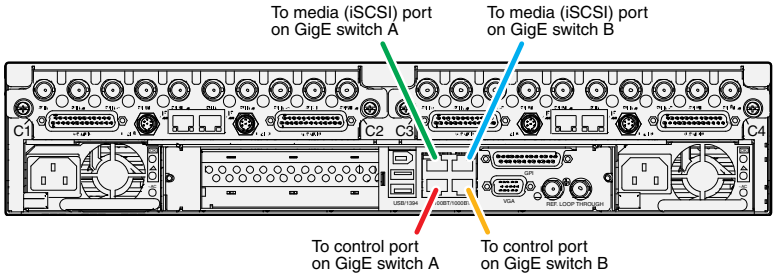


K2-XDP redundant

These cabling instructions apply to the following:

- K2 Summit 3G system or first generation K2 Summit system on a redundant online or production K2 SAN

Refer to "K2 Summit Production Client Quick Start Guide" for additional cabling details.



Cable Ethernet switch

As directed by the system diagram for your storage system, cable the switch or switches for your system using the instructions in this section.

These instructions are for the HP ProCurve switch 2900 and 2910 series. You must use this switch for iSCSI traffic.

For control and FTP/streaming traffic, it is allowed to use a different brand of switch, such as a Cisco Catalyst switch, if required by your site. If you are using a non-HP switch, apply the information in the following procedures accordingly. Refer to the documentation you received with the switch as necessary.

Install the switch in its permanent location. When installing in a video equipment rack, use 10-32 screws. Do not use HP's 12-24 screws, as they can cause thread damage.

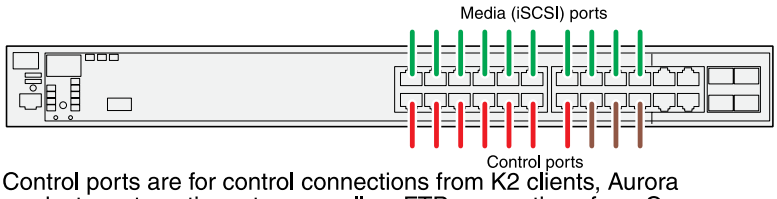
Provide power to the switch.

K2-SWE basic online/production

These cabling instructions apply to the following:

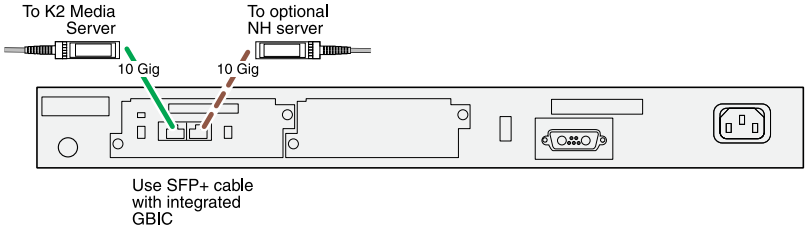
- HP 29xx series Gigabit Ethernet switch on a basic (non-redundant) online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

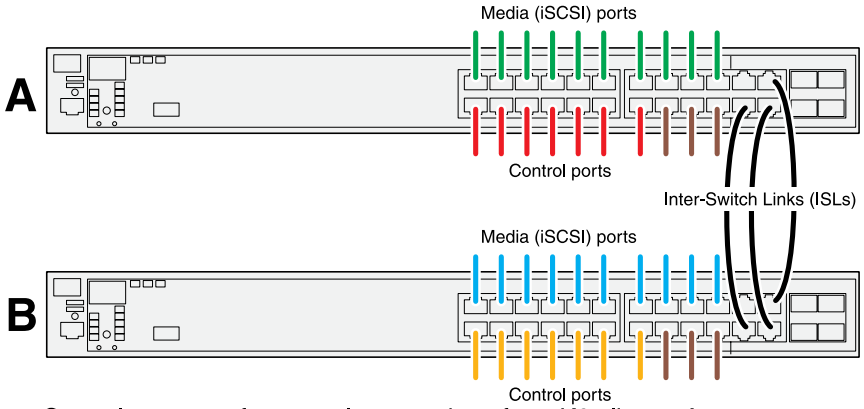


K2-SWE redundant online/production

These cabling instructions apply to the following:

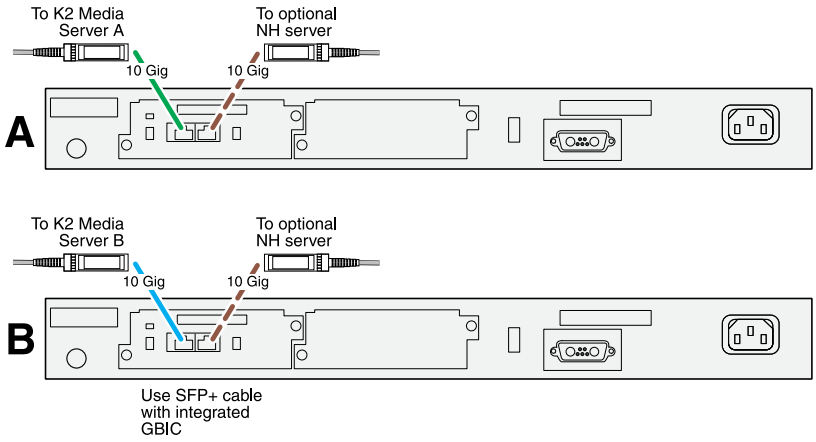
- HP 29xx series Gigabit Ethernet switch on a redundant online or production K2 SAN.

Front view



Control ports are for control connections from K2 clients, Aurora products, automation, etc., as well as FTP connections from Grass Valley and 3rd party systems.

Rear view



If you have other iSCSI clients, such as Aurora Edits, that have just one iSCSI connection and one control connection, approximately half of the clients should be connected to switch A and half of the clients should be connected to switch B. In a failover event, only the clients connected to one of the switches will remain operational, so make connections accordingly. Connect the client's iSCSI connection to one of the media ports on a switch and the client's control connection to one of the control ports on the same switch.

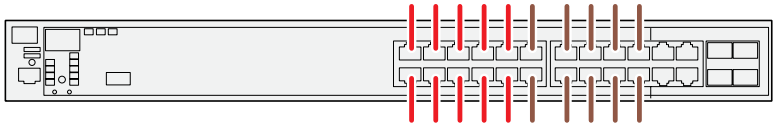
If you have more than one optional NH10GE K2 Media Servers, balance servers between switch A and switch B.

K2-SWE basic nearline

These cabling instructions apply to the following:

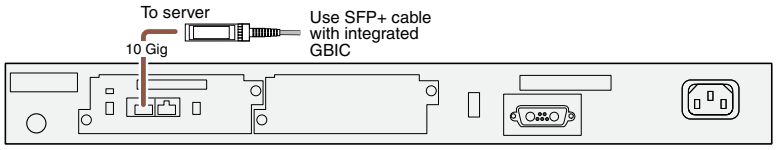
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN with one NH K2 Media Server.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view

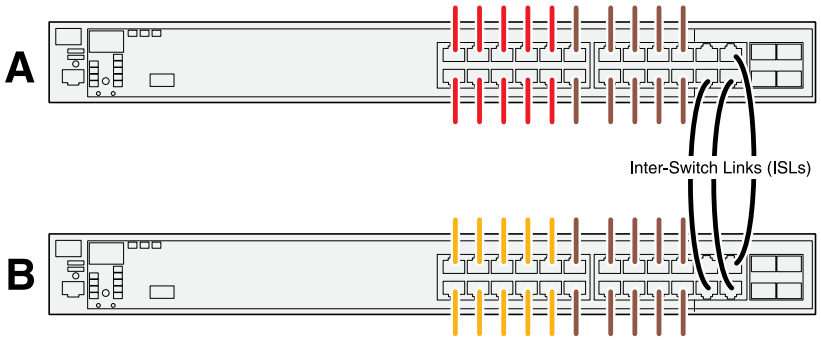


K2-SWE redundant nearline

These cabling instructions apply to the following:

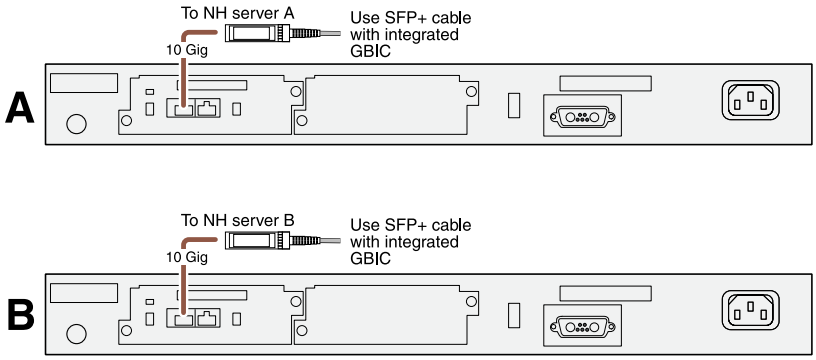
- HP 29xx series Gigabit Ethernet switch on a nearline K2 SAN.

Front view



Ports are for control connections as well as FTP connections from Grass Valley and 3rd party systems.

Rear view



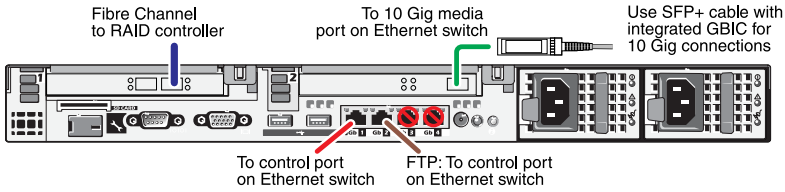
Cable K2 Media Server

As directed by the system diagram for your K2 SAN, cable the K2 Media Server or Servers for your K2 SAN using the instructions in this section.

K2-SVR basic

These cabling instructions apply to the following:

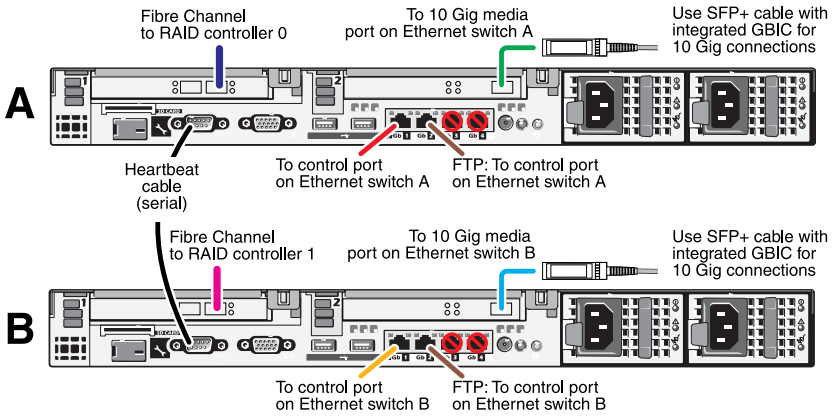
- Dell R610 PowerEdge Server on a basic (non-redundant) online or production K2 SAN.



K2-SVR redundant

These cabling instructions apply to the following:

- Dell 1950 PowerEdge Server on a redundant online or production K2 SAN.



Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

9 – No Connect

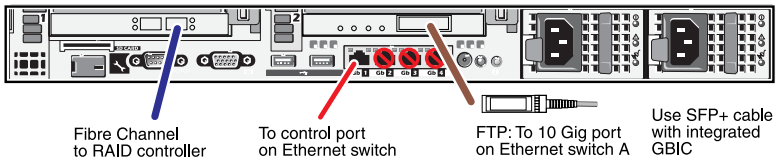
Cable NH10GE K2 Media Server

As directed by the system diagram for your K2 SAN, cable the NH10GE K2 Media Server or Servers for your K2 SAN using the instructions in this section

K2-SVR-NH10GE online/production

These cabling instructions apply to the following:

- Dell R610 PowerEdge Server NH10GE on an online or production K2 SAN.

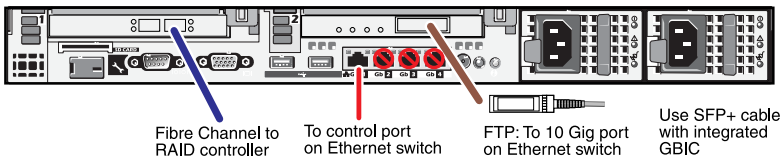


If you have more than one NH1 server, balance servers between controller 0 and controller 1.

K2-SVR-NH10GE basic nearline

These cabling instructions apply to the following:

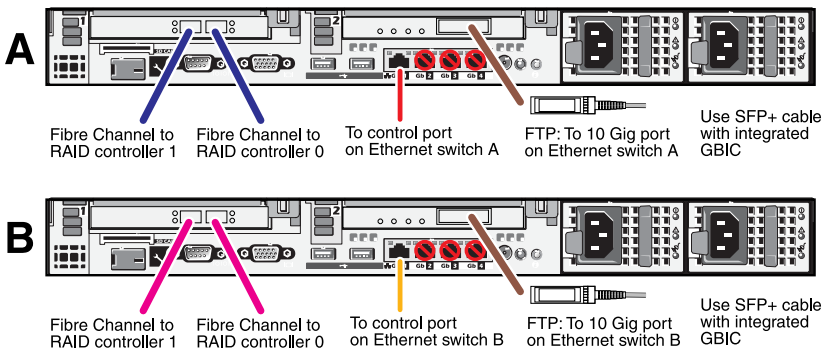
- Dell R610 PowerEdge Server NH10GE on a basic nearline K2 SAN.



K2-SVR-NH10GE redundant nearline

These cabling instructions apply to the following:

- Dell R610 PowerEdge Server NH10GE on a nearline K2 SAN.



Cable K2 RAID

Before cabling, install the K2 RAID chassis in its permanent location. After mounting the chassis in the rack, you must secure brackets to the front rail to support the Grass Valley bezel. Refer to related topics in this document for rack mount instructions.

On the 10G RAID, you do not need to manually set a Fibre Channel address ID on controllers or a chassis address on Expansion chassis.

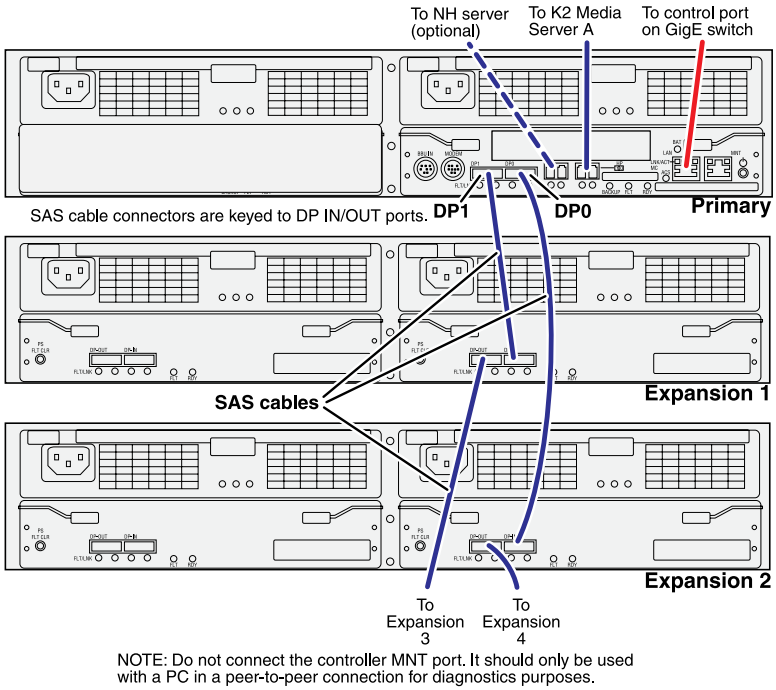
As directed by the system diagram for your storage system, cable the K2 RAID devices using the instructions in this section.

Once the RAID storage is connected and configured, do not swap Expansion chassis or otherwise reconfigure storage. If you connect an Expansion chassis in a different order or to the wrong controller, the controller will see a configuration mismatch and fault.

K2 RAID basic online/production

These cabling instructions apply to the following:

- K2 RAID (Condor with 10G controller) on a basic (non-redundant) online or production K2 SAN.

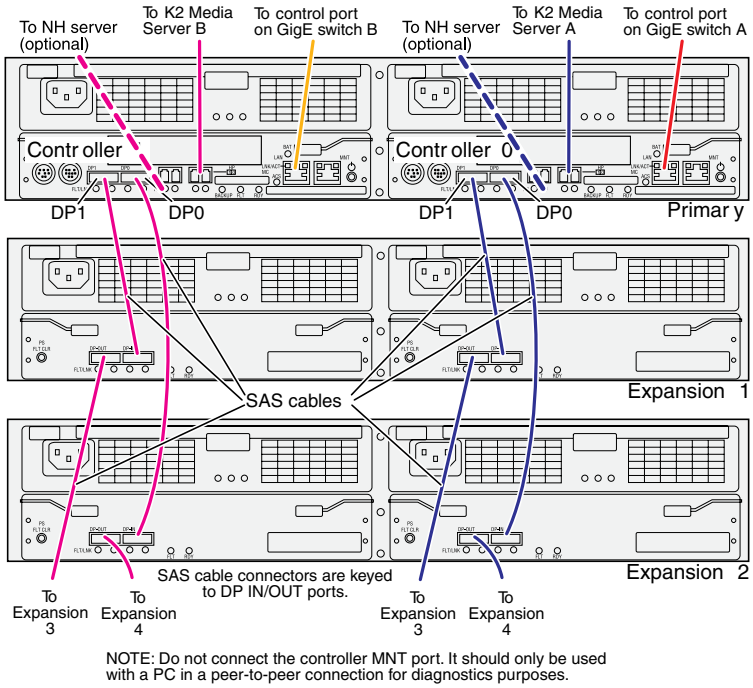


If you have more Expansion chassis than those illustrated, continue the indicated cabling pattern, alternating connections for additional Expansion chassis between DP1 and DP0. Expansion chassis 1, 3, 5, 7, etc. (odd numbers) connect to DP1. Expansion chassis 2, 4, 6, 8, etc. (even numbers) connect to DP0. For example, if you have four Expansion chassis (an even number), they are evenly balanced, so you have two connected to DP1 and two connected to DP0. If you have five Expansion chassis (an odd number), the “plus one” Expansion chassis is always connected to DP1, so you have three connected to DP1 and two connected to DP0.

K2 RAID redundant online/production

These cabling instructions apply to the following:

- K2 RAID (Condor with 10G controllers) on a redundant online or production K2 SAN.



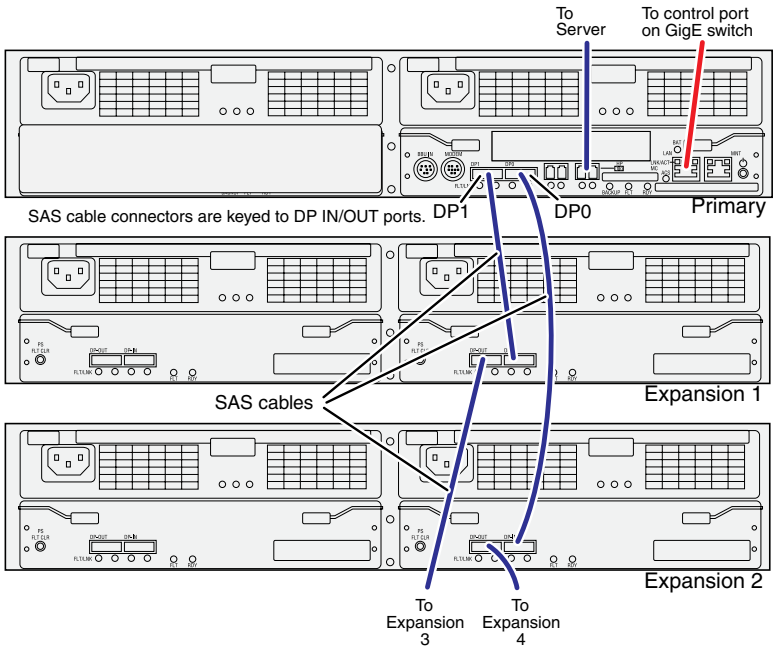
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

If you have more Expansion chassis than those illustrated, continue the indicated cabling pattern, alternating connections for additional Expansion chassis between DP1 and DP0. Expansion chassis 1, 3, 5, 7, etc. (odd numbers) connect to DP1. Expansion chassis 2, 4, 6, 8, etc. (even numbers) connect to DP0. For example, if you have four Expansion chassis (an even number), they are evenly balanced, so you have two connected to DP1 and two connected to DP0. If you have five Expansion chassis (an odd number), the "plus one" Expansion chassis is always connected to DP1, so you have three connected to DP1 and two connected to DP0.

K2 RAID basic nearline

These cabling instructions apply to the following:

- K2 RAID (Condor with 10G controllers) on a basic nearline K2 SAN.



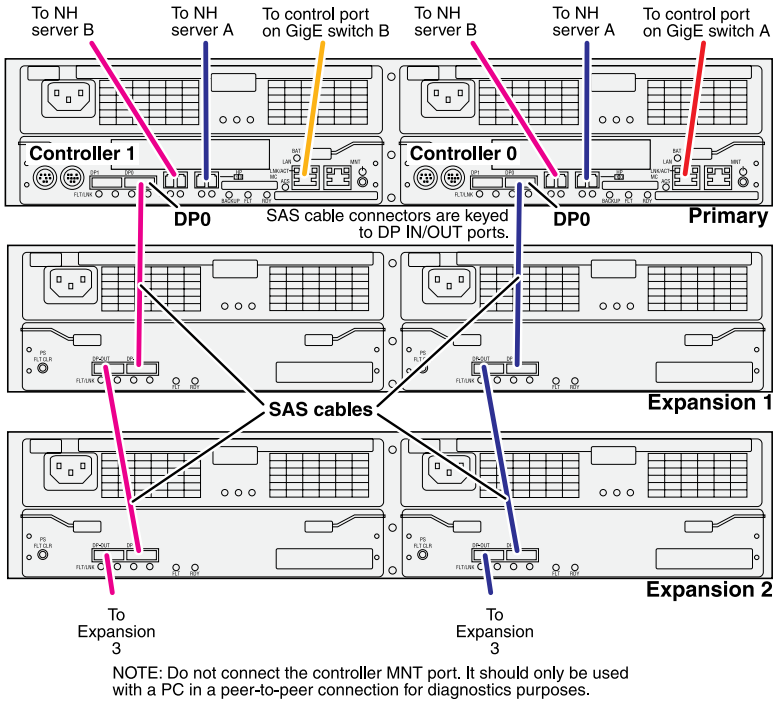
NOTE: Do not connect the controller MNT port. It should only be used with a PC in a peer-to-peer connection for diagnostics purposes.

If you have more Expansion chassis than those illustrated, continue the indicated cabling pattern, alternating connections for additional Expansion chassis between DP1 and DP0. Expansion chassis 1, 3, 5, 7, etc. (odd numbers) connect to DP1. Expansion chassis 2, 4, 6, 8, etc. (even numbers) connect to DP0. For example, if you have four Expansion chassis (an even number), they are evenly balanced, so you have two connected to DP1 and two connected to DP0. If you have five Expansion chassis (an odd number), the "plus one" Expansion chassis is always connected to DP1, so you have three connected to DP1 and two connected to DP0.

K2 RAID redundant nearline

These cabling instructions apply to the following:

- K2 RAID (Condor with 10G controllers) on a Nearline K2 SAN.



Continue this cable pattern for additional Expansion Chassis.

Chapter 4

Setting up the K2 SAN infrastructure

This section contains the following topics:

- *Setting up the Ethernet switch*
- *Setting up the control point PC*

Setting up the Ethernet switch

These procedures are for the HP ProCurve switch 2900 and 2910 series. You must use this switch for iSCSI traffic.

For control and FTP/streaming traffic, it is allowed to use a different brand of switch, such as a Cisco Catalyst switch, if required by your site. If you are using a non-HP switch, apply the information in the following procedures accordingly. Refer to the documentation you received with the switch as necessary.

It is not required that a GigE switch be dedicated to the Nearline system. If enough "control" ports (non-iSCSI ports) are available on a switch or switches configured for an online K2 SAN, the Nearline system can be connected to those control ports.

Configuring the Ethernet switch via serial connection

The following procedure is for the HP ProCurve switch 29xx series. Do not use this procedure on other switch models.

Use a direct console connection to the switch, start a console session, and access the Switch Setup screen to set the IP address.

1. Configure the PC terminal emulator on the control point PC or another PC as a DEC VT-100 (ANSI) terminal or use a VT-100 terminal, and configure either one to operate with these settings:
   - Baud rate 9600
   - 8 data bits, 1 stop bit, no parity, and flow control set to Xon/Xoff
   - Also disable (uncheck) the "Use Function, Arrow, and Ctrl Keys for Windows" option
2. Connect the PC to the switch's Console Port using the console cable included with the switch.

   If your PC or terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin straight-through adapter at one end of the console cable.
3. Turn on the PC's power and start the PC terminal program.
4. Press **Enter** two or three times and you will see the copyright page and the message "Press any key to continue". Press a key, and you will then see the switch console command (CLI) prompt.

   NOTE: If you press Enter too many times and get past the log in, enter the command EN to get into the command line.
5. Type the following, then press **Enter**:

   `menu`
6. If prompted to save the current configuration, answer no (press the n key) to proceed.

   The main menu opens.
7. On the main menu, choose **Switch Configuration**, then press **Enter**.
8. Select **IP Configuration**, then press **Enter**.

9. Press the right-arrow key to choose **Edit**, then press **Enter**. Tab to fields and enter information as follows:
   a) Change **Gateway** to be the default router.
   b) Tab to the **IP Config (DHCP/Bootp)** field and use the Space bar to select the **Manual** option.
   c) Tab to the **IP Address** field and enter the switch's control network IP address.
   d) Tab to the **Subnet Mask** field and enter the subnet mask used for your network.
10. Press **Enter**, then right-arrow to **Save**. Press **Enter** and revert to previous menu.
11. Select **Return to Main Menu** and press **Enter**.
12. From the main menu, chose **Console Passwords** and press **Enter**.

    The Set Password Menu opens.
13. Chose **Set Manager Password** and press **Enter**.
14. When prompted for the password, type a password of up to 16 ASCII characters with no spaces and press **Enter**.

    The password can be one that is used on other K2 devices, such as "adminGV!" or "GVAdmin", or it can be your site's administrator password.
15. When prompted to enter the password again, retype the password and press **Enter**.
16. Select **Return to Main Menu** and press **Enter**.
17. From the main menu, tab to **Command Line (CLI)** and press **Enter**.

    The command prompt appears.
18. Type the following, then press Enter:

    ```
    configure
    ```

    You are now in configuration mode.
19. Configure an administrator username.

    The username can be one that is used on other K2 devices, such as "Administrator" or "GVAdmin", or it can be your site's administrator username.

    For example, to set the username to "administrator" type the following, then press **Enter**:

    ```
    password manager user-name administrator
    ```
20. When prompted, enter and re-enter the password.
21. Set spanning tree to RSTP. To do this, type the following, then press **Enter**:

    ```
    spanning-tree force-version rstp-operation
    ```

    This configures spanning tree, but it does not turn spanning tree on. You must turn spanning tree on using the switch's Web interface.
22. Decide your SNMP community name as explained in the following options, then proceed with the next step:

    - If you decide to use a unique SNMP community name (not "public"), add the community and set its RW permissions. For example, if the community name is "K2", type the following, then press **Enter**:

      ```
      snmp-server community K2 unrestricted
      ```
    - If you decide to use the default SNMP community "public" for NetCentral monitoring, which already has RW permissions set as required by NetCentral, proceed to the next step.

23. Enter the SNMP community and IP address of the NetCentral server PC. The commands are slightly different on HP 2900 and HP 2910 switch models.

    For example, if the IP address is “192.168.40.11” and the community is “public”, you type one of the following as per your switch model, then press Enter:

    HP 2900: `snmp-server host public 192.168.40.11`

    HP 2910: `snmp-server host 192.168.40.11 public`

24. Enable Authentication traps. To do this, type the following, then press **Enter**:

    `snmp-server enable traps snmp-authentication standard`

    This allows NetCentral to test the switch to verify that it can send its SNMP trap messages to NetCentral.

25. Type the following, then press **Enter**:

    `menu`

    When prompted, save the configuration by pressing the y key.

    The main menu opens.

26. If you need a trunk for ISLs to gang switches together, use the following steps. These steps illustrate trunking the last three 1 Gig ports for three 1 Gig ISLs, which is the recommended configuration for ISLs on all multi-switch K2 SANs. Consult with your Grass Valley representative if your requirements deviate from the recommended policy:
    a) At the main menu, select **Switch Configuration** and press **Enter**.
    b) Choose selection **Port/Trunk Settings** and press **Enter**.
    c) Press the right-arrow key to choose **Edit**, then press **Enter**.
    d) Down arrow until at the bottom of the list of ports and select the last (highest port number) 1 Gig port in the list.
    e) Right-arrow over to the Group column.
    f) Use the Space bar and set the bottom 1 Gig port to **Trk1**.
    g) Set the next port up also to **Trk1**.
    h) Set the next port up also to **Trk1**.
    i) Press **Enter**, then right-arrow to **Save**. Press **Enter** and revert to previous menu.

27. Select **Return to Main Menu** and press **Enter**.

28. From the main menu, tab to **Command Line (CLI)** and press **Enter**. The command prompt appears.

29. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

    `show flash`

    Information is displayed similar to the following example:

```
HP_iSCSI_switch1# show flash
Image           Size(Bytes)   Date    Version
-----           ----------  --------  -------
Primary Image   : 6737518   07/25/08  T.13.23
Secondary Image : 5886358   10/26/06  T.11.12
Boot Rom Version: K.12.12
Current Boot    : Primary
```

30. Check the Primary Image Version and refer to related topics in "K2 Release Notes" for information about currently supported versions. If instructed to change the firmware on the switch, do so before continuing.

31. Type the following, then press **Enter**:

    `menu`

    The main menu opens.

32. From the main menu, choose **Reboot Switch** and press **Enter**.

    When prompted “Continue Reboot…?', answer yes (press the y key) to proceed.

    The switch restarts.

33. You can now use the switch’s web browser interface for further configuration.
34. Close the PC terminal program and disconnect the console cable.
35. if you have multiple switches, repeat this procedure on the other switches.

Next, configure the GigE switch via the Web interface.

Configuring the Ethernet switch via the Web interface

The following procedure is for the HP ProCurve switch 29xx series. Do not use this procedure on other switch models.

1. From the control point PC or another PC, make sure that you have a direct Ethernet cable connection to the switch, with no switches, routers, proxies, or other networking devices in between.
2. On the PC, open Internet Explorer and type the switch’s IP address in the Address field, as in the following example.

   `http://192.168.100.61`

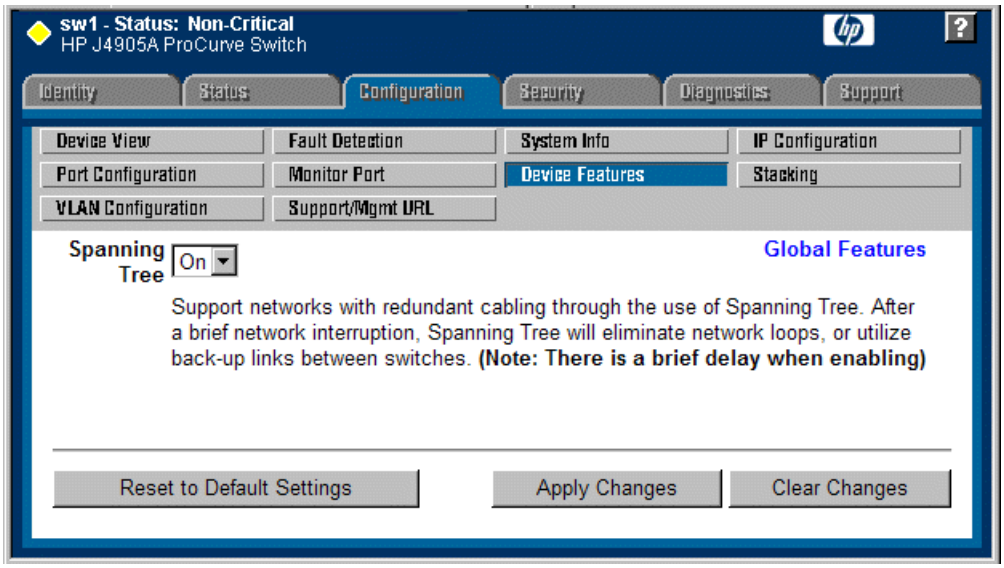
   This should be the name or IP address as currently configured on the switch.

3. Press **Enter** to open the switch’s configuration application.

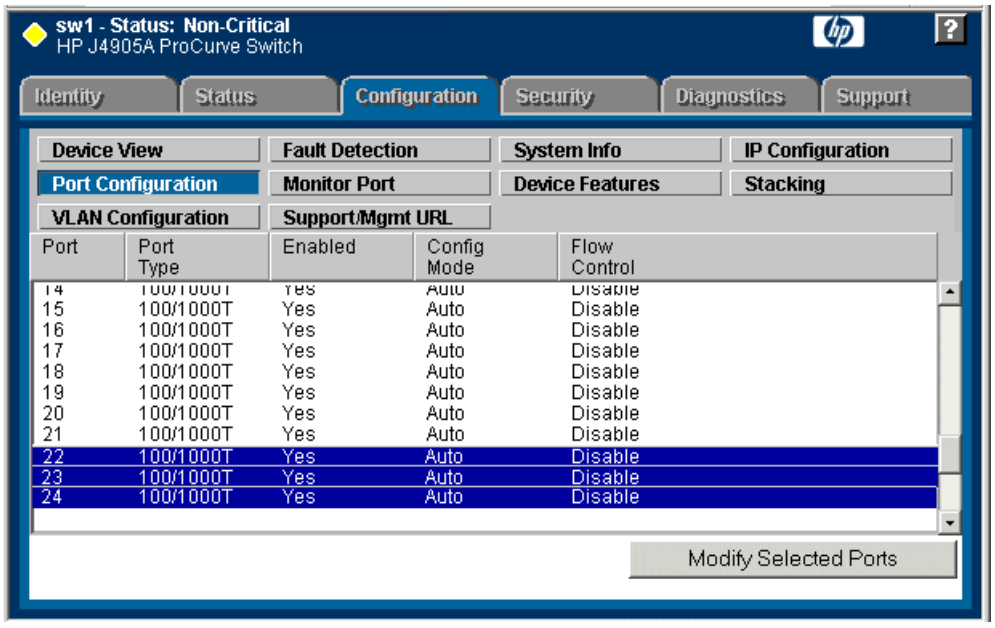
   NOTE: The configuration application for the HP ProCurve switch requires Java.

   You can also access the switch’s configuration application from the K2Config application.

4. In the switch's configuration application, choose **Configuration**, then **Device Features**.



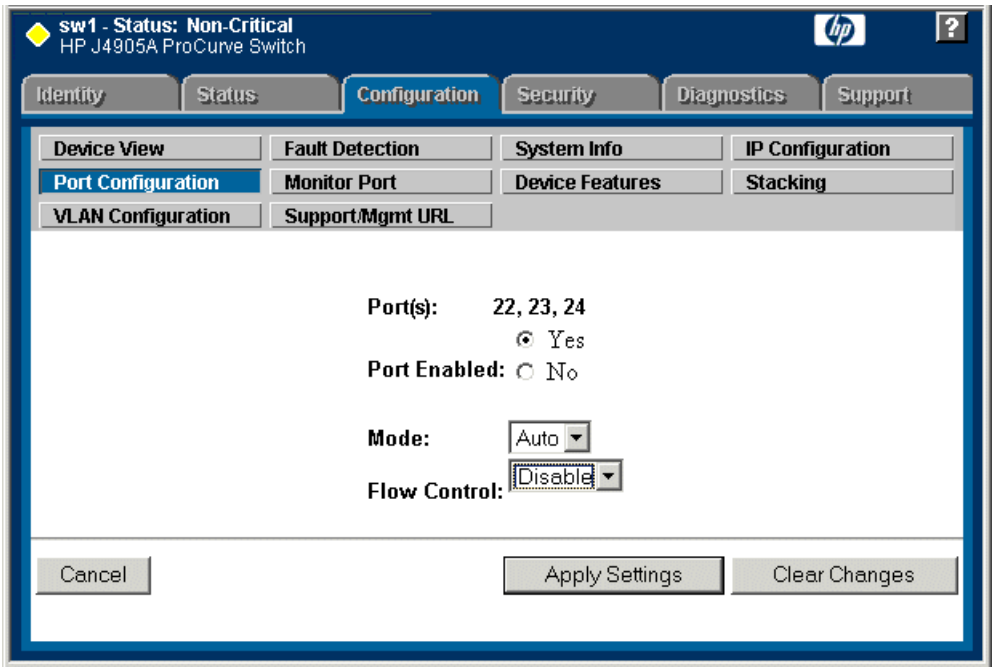
5. Set Spanning Tree to **On** and click **Apply Changes**.
   If prompted, log in with the switch's administrator username and password.
6. Click **Port Configuration**.



7. Scroll to the bottom of the list and verify that the SFP+ port is port A1.
   Re-cable if necessary to correct the SFP+ port.

8. If you do not need trunks, such as on a one-switch system, skip to the next step in this procedure. If you need trunks, such as on a two-switch system with ISLs, do the following:
   a) Select (Ctrl + Click) the trunked ports. Typically the trunked ports are at the bottom of the list and are labeled Trk1.
   b) Click **Modify Selected Ports**.

      If prompted, log in as administrator.

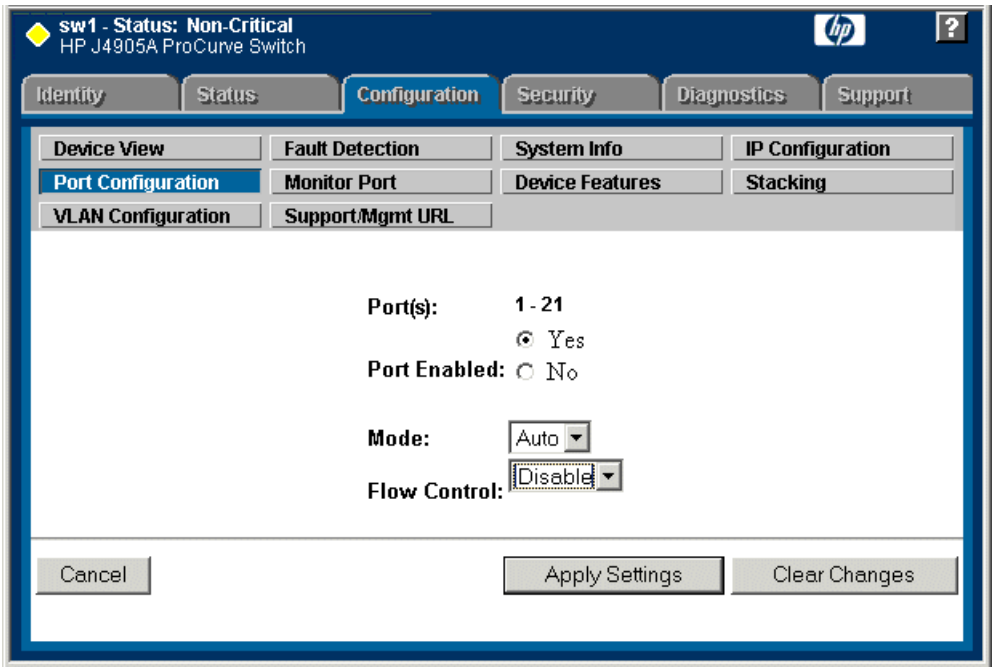


   c) For the trunked ports, set Port Enabled to **Yes**. On some switch models, some ports are disabled by default, so make sure you enable them. Leave Mode as default of **Auto**.
   d) Set Flow Control as follows:

      Set to **Disable**.

   e) Click **Apply Settings**.
9. On the Port Configuration page, do one of the following:
   - If you do not have trunks, select all ports.
   - If you have trunks, select the remaining ports (the ports not trunked).

10. Click **Modify Selected Ports**.



11. Make sure Port Enabled is set to **Yes**, leave Mode as default of **Auto**.
12. Set Flow Control as follows:

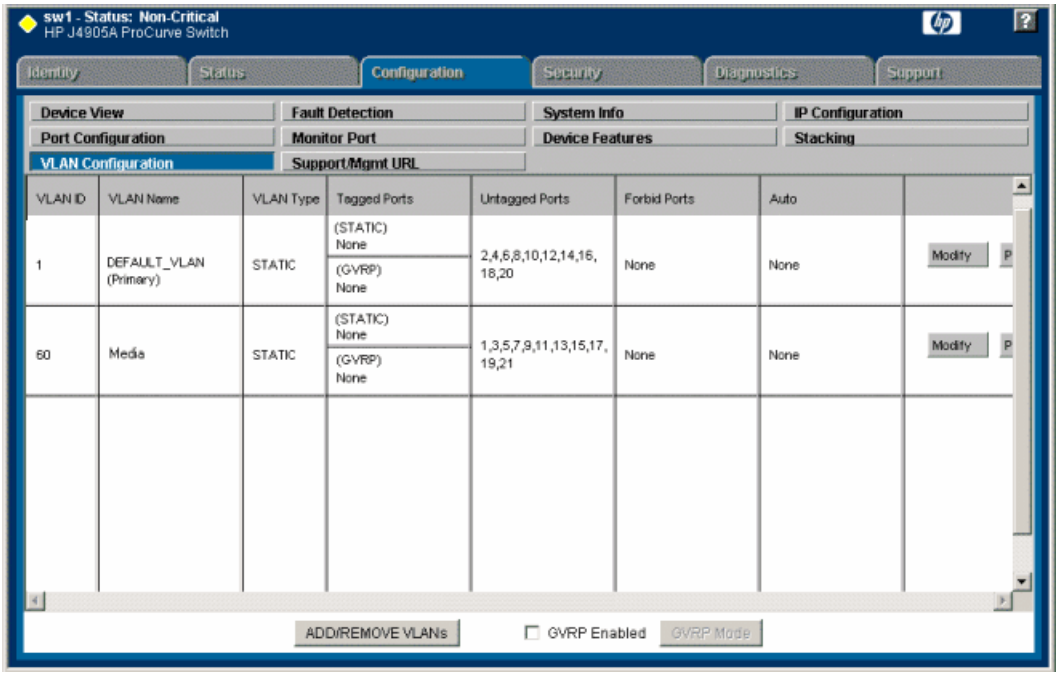
    Set to **Disable**.
13. Click **Apply Settings**.

    Wait until settings are applied and the Web interface becomes active.
14. Proceed as follows:

    - If the switch carries no media (iSCSI) traffic, such as for a Nearline system, there is no need to configure VLANs. Skip to the end of this procedure.
    - If the switch carries media (iSCSI) traffic, then it must have VLANs configured. Continue with the next step in this procedure.

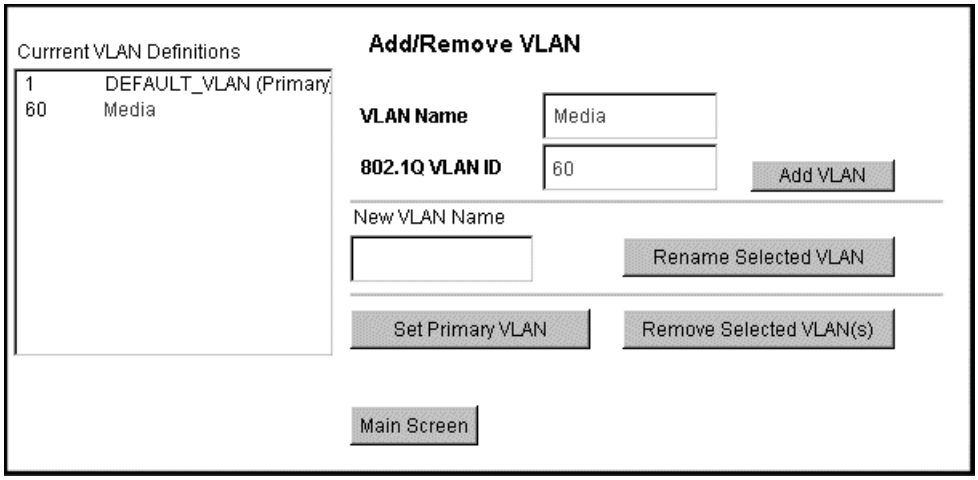
15. Choose **VLAN Configuration**.

    If prompted, log in with the switch's administrator username and password.



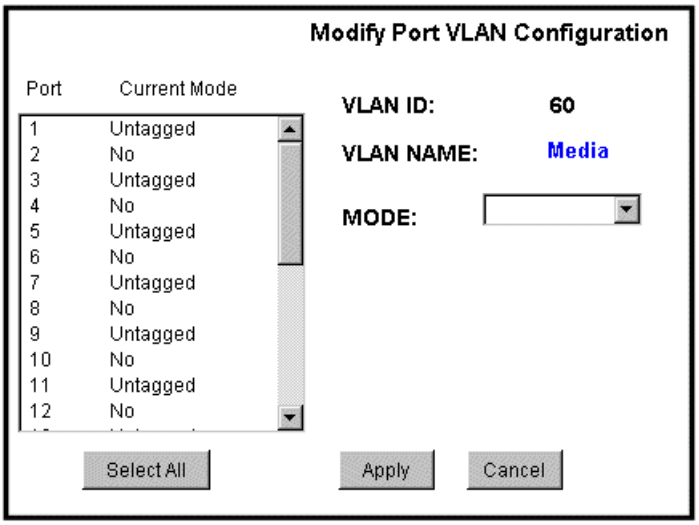
16. Create a new Media (iSCSI) VLAN as follows:

    a) Click **Add/Remove VLANs**.



    b) In the VLAN Name field enter `Media`.
    c) In the VLAN ID field enter `60`.
    d) Click **Add VLAN**.
    e) If prompted, log in as administrator.
    f) Click **Main Screen** to return to VLAN Configuration.

17. Configure the Media VLAN as follows:
    a) In the Media VLAN row, click **Modify**.



    b) Select all the odd numbered ports. (Tip: Use Ctrl + Click.)
    c) Also select port A1.

       This is the 10 Gig SFP+ port on the back of the switch that connects to the K2 Media Server for media (iSCSI) traffic.

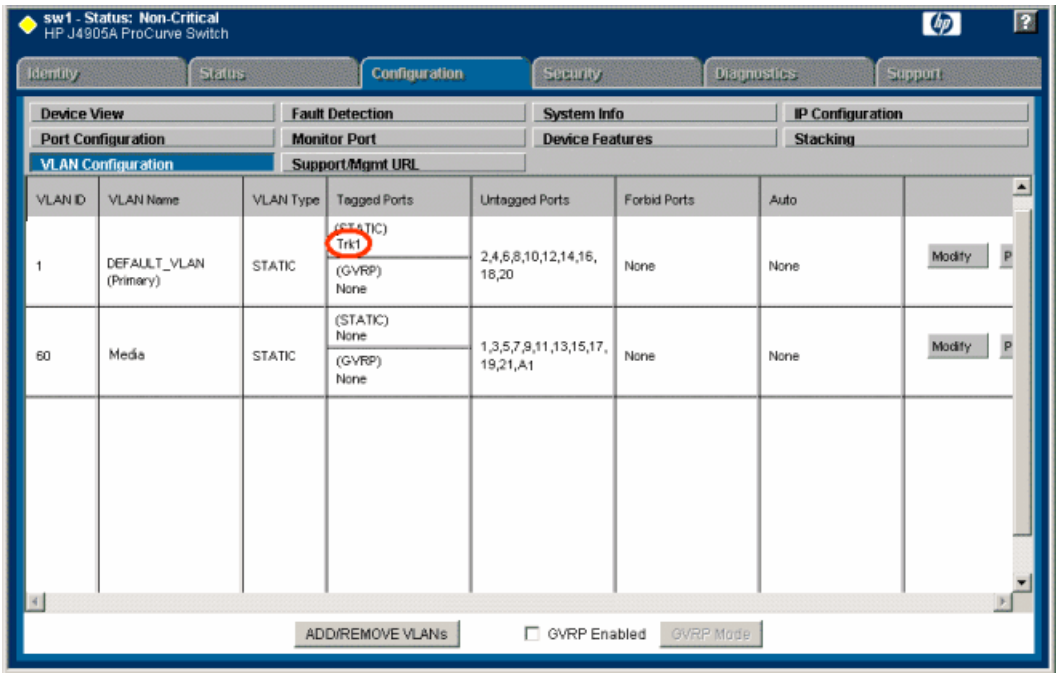
       If you have a NH10GE K2 Media Server for FTP traffic, the 10 Gig SFP+ port on the back of the switch that connects to this server does not go in the Media VLAN. This port stays in the default VLAN.

    d) In the Mode drop-down list, select **Untagged**, then click **Apply**. This removes the odd ports from the default (Control) VLAN.

       If you have a trunk, do not configure it as "Tagged". Media VLAN traffic (iSCSI) does not go over the trunk.

18. Click the **VLAN Configuration** tab.
19. If you have a trunk, configure the default (Control) VLAN as follows:
    a) In the DEFAULT_VLAN row, click **Modify**.
    b) In the Current Mode list box, scroll down and select the trunk.
    c) In the Mode drop-down list, select **Tagged**, then click **Apply**. This allows default VLAN traffic (non-iSCSI) to go over the trunk.

20. Click the **VLAN Configuration** tab.



21. If you have a trunk, verify that for the default VLAN the trunk is displayed in the Tagged Ports column.
22. If you have two switches, repeat this procedure for the other switch.
23. Close the switch configuration application.

Next, configure QOS on the GigE switch.

Configuring QOS on the GigE switch

Prerequisites for this procedure are as follows:

- The switch is HP ProCurve switch 29xx series.
- Trunks, VLANs and all other configuration is complete.
- The switch has an IP address
- You have network access to the switch

Use this procedure to make the Quality of Service (QOS) setting on the HP ProCurve switch 29xx series.

1. If you have not already done so, from a network connected PC open the MS-DOS command prompt and login to the switch as administrator, as follows:
   a) Telnet to the switch. For example, if the switch's IP address is 192.168.40.12, you type the following, then press **Enter**.

      ```
      telnet 192.168.40.12
      ```

   b) Press **Enter** one or more times until the switch's username prompt appears.
   c) Type the switch's administrator username and press **Enter**, then type the switch's administrator password and press **Enter**. The switch console command (CLI) prompt appears.

2. Type the following, then press **Enter**:

   `config`

   You are now in configuration mode.

3. Type the following, then press **Enter**:

   qos queue-config 2-queues

   This limits the number of active queues within the switch giving the most buffering to VLANs 1 and 60

4. Type the following, then press **Enter**:

   show qos vlan

   The screen displays VLAN information. Note the ID number of the Media (iSCSI) VLAN. It should be 60, as follows:

```
VLAN priorities

  VLAN ID Apply rule  | DSCP   Priority
  ------- ----------- + ------ -----------
  1       No-override |        No-override
  60      No-override |        No-override
```

5. a) Assign the Media VLAN the QOS priority of 3. For example, if the VLAN ID is 60, you type the following, then press **Enter**.

   `vlan 60 qos priority 3`

   b) Type the following, then press **Enter**:

   `show qos vlan`

   The screen displays VLAN information. Make sure that the Priority column reports that the Media VLAN has a value of 3.

Next, verify flow control settings.

Verify flow control setting on the GigE switch

Prerequisites for this procedure are as follows:

- The switch is HP ProCurve switch 29xx series.
- Trunks, VLANs, QOS, and all other configuration is complete.
- The switch has an IP address

- You have network access to the switch

Use this procedure to check flow control settings, and if necessary, configure flow control to "off" (disabled) for all ports.

1. If you have not already done so, from a network connected PC open the MS-DOS command prompt and login to the switch as administrator, as follows:
   a) Telnet to the switch. For example, if the switch's IP address is 192.168.40.12, you type the following, then press **Enter**.

      ```
      telnet 192.168.40.12
      ```

   b) Press **Enter** one or more times until the switch's username prompt appears.
   c) Type the switch's administrator username and press **Enter**, then type the switch's administrator password and press **Enter**. The switch console command (CLI) prompt appears.
2. Type the following, then press **Enter**:

   ```
   config
   ```

   You are now in configuration mode.
3. Type the following, then press **Enter**:

   ```
   show interface brief
   ```

   The screen displays setting for all ports. In the Flow Ctrl column (at the right) identify settings for ports and proceed as follows:

   - If all ports are set to "off", no further configuration is necessary. Do not proceed.
   - If one or more ports are set to "on", continue with this procedure.

4. Set ports to flow control "off" as necessary. You can set a range of ports. For example, to set ports 1 - 21 to off, you type the following, then press **Enter**.

   ```
   no int 1-21 flow-control
   ```

5. Type the following, then press **Enter**:

   ```
   show interface brief
   ```

   Verify that all ports have flow control set to off.

Upgrading firmware on HP switch

1. If you have not already done so, install a TFTP Server.

   For example, to install *tftpd32.exe*, go to *http://tftpd32.jounin.net/*.
2. Open the TFTP Server.
3. Make sure your current working directory includes the **.swi* file that you are using for the upgrade.

4. Execute the copy command with the following syntax:

   `copy tftp flash <ip-address> <remote-os-file> [ < primary | secondary > ]`

   Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

   For example, to download a software file named T_13_23.swi from a TFTP server with the IP address of 10.16.34.3 1, use the following:

   `ProCurve # copy tftp flash 10.16.34.3 T_13_23.swi`

5. When prompted `The primary OS image will be deleted. continue [y/n]?`, press **Y**.

   When the switch finishes downloading the software file from the server, it displays the progress message `Validating and Writing System Software to FLASH...`

6. Wait until the CLI prompt re-appears, then continue with the next step in this procedure.
7. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

   `show flash`

   Information is displayed similar to the following example:

```
HP_iSCSI_switch1# show flash
Image            Size(Bytes)   Date    Version
-----            ----------  --------  -------
Primary Image   : 6737518   07/25/08  T.13.23
Secondary Image : 5886358   10/26/06  T.11.12
Boot Rom Version: K.12.12
Current Boot    : Primary
```

8. Verify that the new software version is in the expected flash area (primary or secondary).
9. Restart the switch from the flash area that holds the new software (primary or secondary).

Setting up the control point PC

To set up the Control Point PC, you have the following options:

- Use the Grass Valley Control Point PC that comes from the factory with software pre-installed.
- Use a PC that you own and install the required software.

1. For either option, you must do the following for the Control Point PC that runs the K2 System Configuration application:
   a) Assign a control network IP address to the PC.
   b) Connect the PC to the GigE control network.
2. To use your own PC, you must additionally do the following:
   a) Verify that the PC meets system requirements.
   b) Install the K2 Control Point software.
   c) Install SiteConfig software.
   d) Install other supporting software.
   e) Install and license NetCentral server software. This can be on the K2 SAN control point PC or on a separate NetCentral server PC that monitors the K2 SAN.

To fix NetCentral screen resolution problem

To fix the screen resolution problem seen with NetCentral on the Grass Valley Control Point PC, do the following:

1. Go to Display properties (right mouse selection of properties on the display area)
2. Select Settings tab
3. Select the Advanced button
4. In the General tab, set the DPI setting to Normal size (96 DPI)
5. Restart the PC

Install SiteConfig on control point PC

NOTE: There might be a newer version of this document available. Check your product's release notes and the Grass Valley website at www.grassvalley.com/docs for references to an updated version that contains additional important information.

Work through the following topics to install the SiteConfig application on the control point PC.

About installing SiteConfig

SiteConfig uses a protocol that involves sending Ethernet broadcast messages to discover and configure devices. To enable this protocol to work correctly, there must be unrestricted network access between the PC that hosts SiteConfig and the devices to be discovered.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block SiteConfig protocols.

Also, do not install SiteConfig on a PC on which a drive from a managed device is mapped as an administrative share (C$). For example, if you have a PC set up to run anti-virus software and for this purpose you have network drives set up on the PC mapped to C$ shares on devices, then do not use that PC to host SiteConfig and manage those devices.

For a given system, there should be just one instance of SiteConfig managing the system.

System requirements for SiteConfig host PC

The PC on which SiteConfig is installed must meet the following requirements:

Requirements	Comments
Operating system	Microsoft Windows (Must be a U.S. version): • XP Professional Service Pack 2, Server 2003 • Vista Enterprise Service Pack 1
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory

Requirements	Comments
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 4.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs.
XML	Microsoft XML 4 Service Pack 2 is required.

Installing/upgrading SiteConfig

Prerequisites:

- The PC on which you are installing SiteConfg meets system requirements.
- The PC is connected to the LAN on which all the devices to be managed are connected.
- There are no routed paths to the devices to be managed.

1. Procure SiteConfig installation files from the Grass Valley website or via other distribution mechanisms.

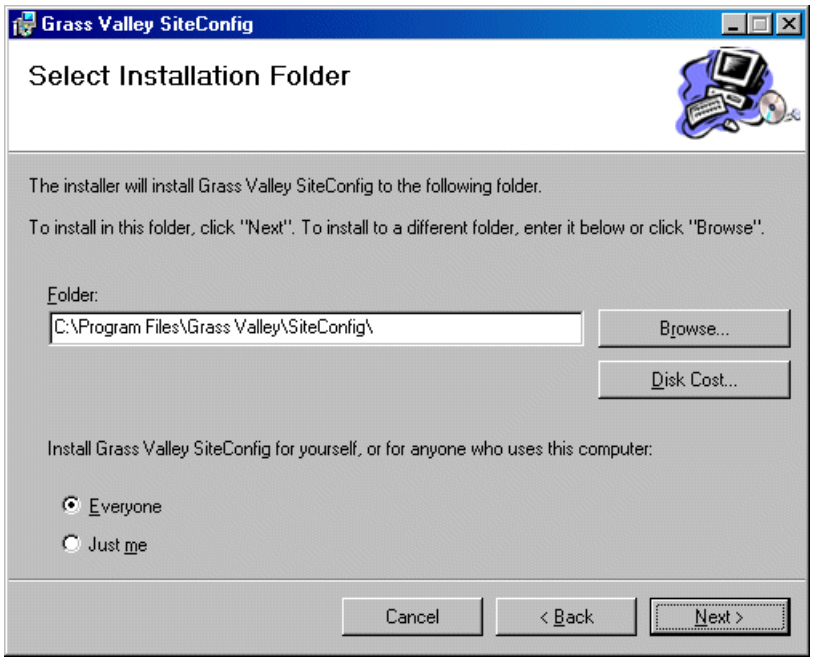
   The following directory and files are required to install SiteConfig:

   - `DotNetFx` directory
   - `ProductFrameUISetup.msi`
   - `setup.exe`

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click `setup.exe`.

   The installation wizard opens.

4. Work through the wizard pages, clicking **Next** and **Finish**.



   If the PC does not have the appropriate version of Microsoft .NET, the SiteConfig installation programs installs it.

5. Open the Windows operating system Services control panel on the PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent must be installed on the SiteConfig PC so that the PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

   The Discovery Agent is also known as the Network Configuration Connect Kit. For example, in Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.

6. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the `DiscoveryAgentServiceSetup.msi` file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

7. If not already configured, configure the SiteConfig PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the SiteConfig PC.

Install prerequisite files on the SiteConfig PC

Some software components share common prerequisite software. You must install a prerequisite software package on the SiteConfig PC to make the prerequisite software available for software deployment to devices.

1. Check release notes for the required version of prerequisite files, if any.
2. On the SiteConfig PC, open Windows Add/Remove programs and look for **Grass Valley Prerequisite Files**, then proceed as follows:
   - If the required version of prerequisite files is installed, do not proceed with this task.
   - If prerequisite files are not installed or are not at the required version, proceed with this task.
3. Procure the required prerequisite software installation file. The file name is *`Prerequisite Files.msi`*.
4. On the SiteConfig PC, run the installation file. The installation program copies prerequisite files to *`C:\Program Files\Grass Valley\Prerequisite Files`*.

Chapter 5

Planning and implementing a K2 SAN with SiteConfig

This section contains the following topics:

- *About developing a system description*
- *Importing a system description*
- *About device and host names*
- *Modifying a device name*
- *Modifying the control network*
- *Modifying the FTP/streaming network*
- *Modifying a media (iSCSI) network*
- *About IP configuration of network interfaces on devices*
- *Modifying K2 client unassigned (unmanaged) interface*
- *Modifying K2 Media Server unassigned (unmanaged) interface*
- *About SiteConfig support on K2 devices*
- *Discovering devices with SiteConfig*
- *Assigning discovered devices*
- *Modifying K2 client managed network interfaces*
- *Modifying K2 Media Server managed network interfaces*
- *Making the host name the same as the device name*
- *Pinging devices from the PC that hosts SiteConfig*
- *About hosts files and SiteConfig*
- *Generating host tables using SiteConfig*

About developing a system description

You use SiteConfig to create or modify a system description for the K2 SAN. You can do this in your planning phase, even before you have devices installed or cabled. Your goal is to have the SiteConfig system description accurately represent all aspects of your devices and networks before you begin actually implementing any networking or other configuration tasks.

There are several task flows you can take to develop a system description, as follows:

- Obtain the sales tool system description. This is the system description that was developed for your specific K2 SAN as part of the sales process. It should be a very accurate representation of the K2 SAN that is to be installed at the customer site. Import the system description into SiteConfig and then make final modifications.
- Obtain a similar K2 SAN's system description, import it into SiteConfig, and then modify it until it matches your K2 SAN.
- In SiteConfig, use the New Site Wizard to create a new system description. The wizard has models based on the pre-defined K2 SAN levels. You can enter much of your site-specific information as you work through the wizard, and then do final modifications using other SiteConfig features.

The topics in this manual follow the task flow for the sales tool system description. If you are using a different taskflow, use the topics in this manual as appropriate and refer to the *SiteConfig User Manual* or *SiteConfig Help Topics* for additional information.

Importing a system description

Prerequisites for this task are as follows:

- The SiteConfig PC has access to the system description file you are importing.
- Windows Explorer Folder Options must be set to Show hidden files and folders in order to see all the folders containing SiteConfig files.

1. Open SiteConfig and proceed as follows:

   - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Import**.
   - If the SiteConfig main window opens, click **File | Import**.

   The Import System Description dialog box opens.

2. Browse to and select a system description file (`*.scsd`) and click **Open**.

The current system description is closed and the system description you are importing is displayed in SiteConfig.

About device and host names

In SiteConfig, a device can have different names, as follows:

- Device name — This is a name for display in SiteConfig only. It is stored in the SiteConfig system description, but not written to the actual device. It is displayed in the device tree view and in the device list view. It can be a different name than the device's host name.
- Host name — This is the network name of the device. SiteConfig has a default naming convention for host names which you can use or override with your own host names.

In most cases it is recommended that the Device name and Host name be the same. This avoids confusion and aids troubleshooting.

The Device name can serve as a placeholder as a system is planned and implemented. During the install/commission process, when you reconcile a device's current and planned network interface settings, the Host name as configured in the system description can be overwritten by the host name on the actual device. However, the Device name configured in the system description is not affected. Therefore it is recommended that in the early planned stages, you configure the Device name to be the desired name for the device, but do not yet configure the Host name. Then, after you have applied network interface settings, you can change the Host name to be the same as the Device name. This changes the host name on the actual device so that then all names are in sync.

SiteConfig does not allow duplicate device names or host names.

Items in the tree view are automatically sorted alphabetically, so if you change a name the item might sort to a different position.

Modifying a device name

1. In the **Network Configuration | Devices** tree view, right-click a device and select **Rename**.
2. Type in the new name.

   Note that this does not change the hostname on the physical device. If you want the hostname to match the device name, you must also modify the hostname.

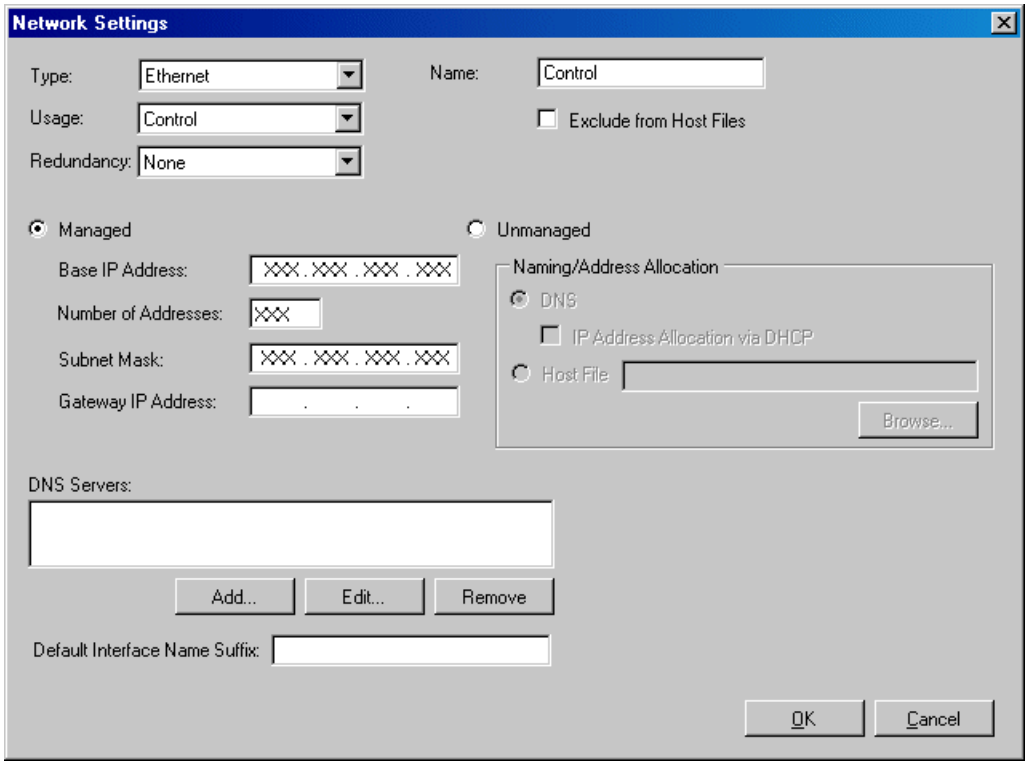
Modifying the control network

1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.

   The networks under that node are displayed in the list view.

2. Proceed as follows:
   - In the list view, right-click the Control network and select **Details**.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For control network
Type	*Ethernet* is required
Usage	*Control* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Control* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	Not allowed

4. Click **OK** to save settings and close.

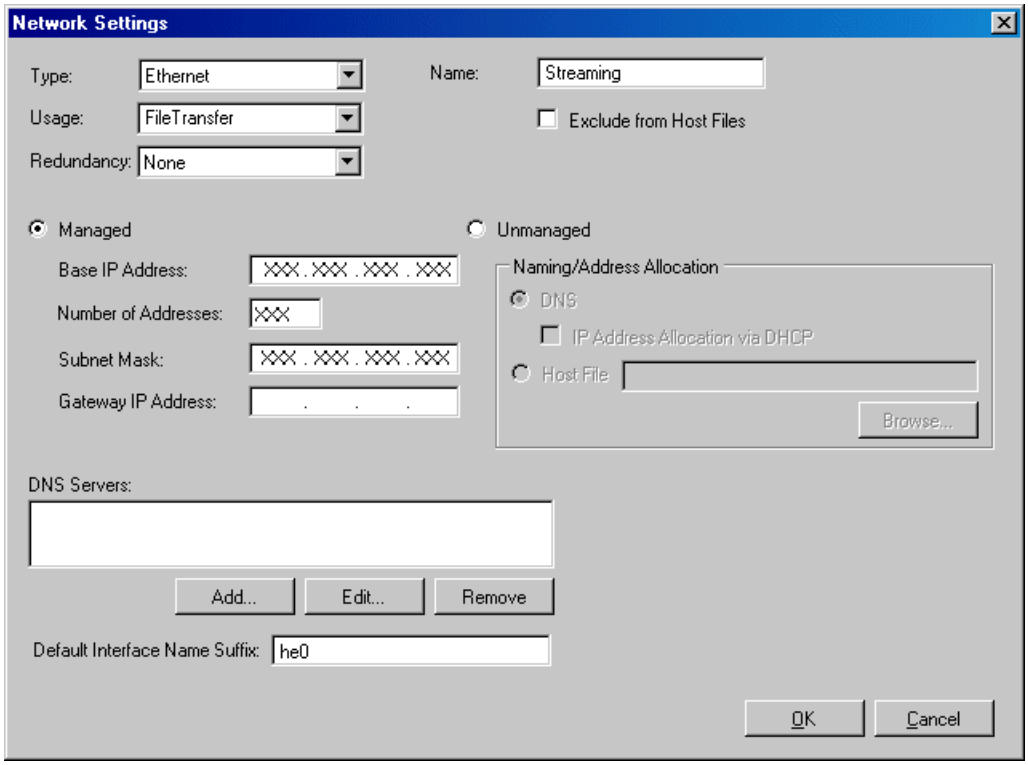
Modifying the FTP/streaming network

1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.
   The networks under that node are displayed in the list view.

2. Proceed as follows:

   - In the list view, right-click the Streaming network and select **Details**.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For FTP/streaming network
Type	*Ethernet* is required
Usage	*FileTransfer* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Streaming* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	*_he0* is required

4. Click **OK** to save settings and close.

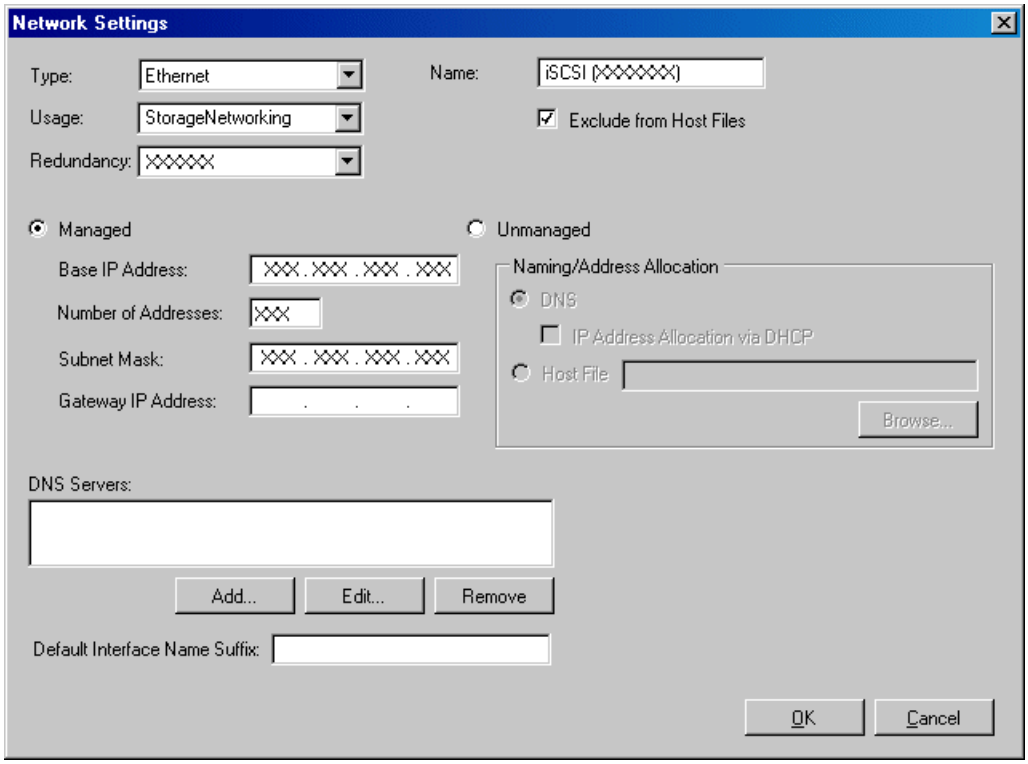
Modifying a media (iSCSI) network

1. In the **Network Configuration | Networks** tree view, select the K2 SAN's Site node.
   The networks under that node are displayed in the list view.

2. Proceed as follows:

   - If the K2 SAN is basic (non-redundant), in the list view, right-click the iSCSI network and select **Details**.
   - If the K2 SAN is redundant, in the list view, first right-click the primary iSCSI network and select **Details**. Then proceed to modify the primary iSCSI network. After the primary iSCSI network is modified, repeat these steps and modify the secondary iSCSI network.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For media (iSCSI) network
Type	*Ethernet* is required
Usage	*StorageNetworking* is required
Redundancy	*None* is required for a basic (non-redundant) K2 SAN
	Primary is required for a redundant K2 SAN media network A
	Secondary is required for a redundant K2 SAN media network B
Name	*iSCSI (non-Redundant)* is recommended for a basic (non-redundant) K2 SAN
	iSCSI (Primary Redundant) is recommended for a redundant K2 SAN media network A
	iSCSI (Secondary Redundant) is recommended for a redundant K2 SAN media network B
Exclude from Host Files	*Selected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Not allowed
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Not allowed
Default Interface Name Suffix	Not allowed

4. Click **OK** to save settings and close.

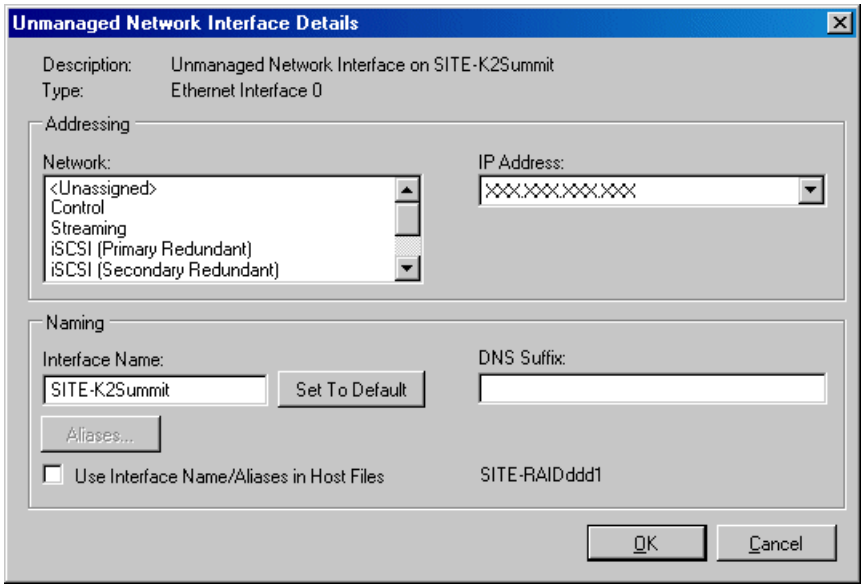
About IP configuration of network interfaces on devices

You can perform IP configuration of network interfaces when working with a placeholder device prior to discovery. When you add a device and choose a particular model, the model defines the number, type and usage characteristics of network interfaces to expect on such a device.

You can view and edit each network interface and set up IP configuration selecting an appropriate IP from the network to which each interface connects. The process for editing IP configuration varies, depending on the device's phase.

Placeholder device IP configuration

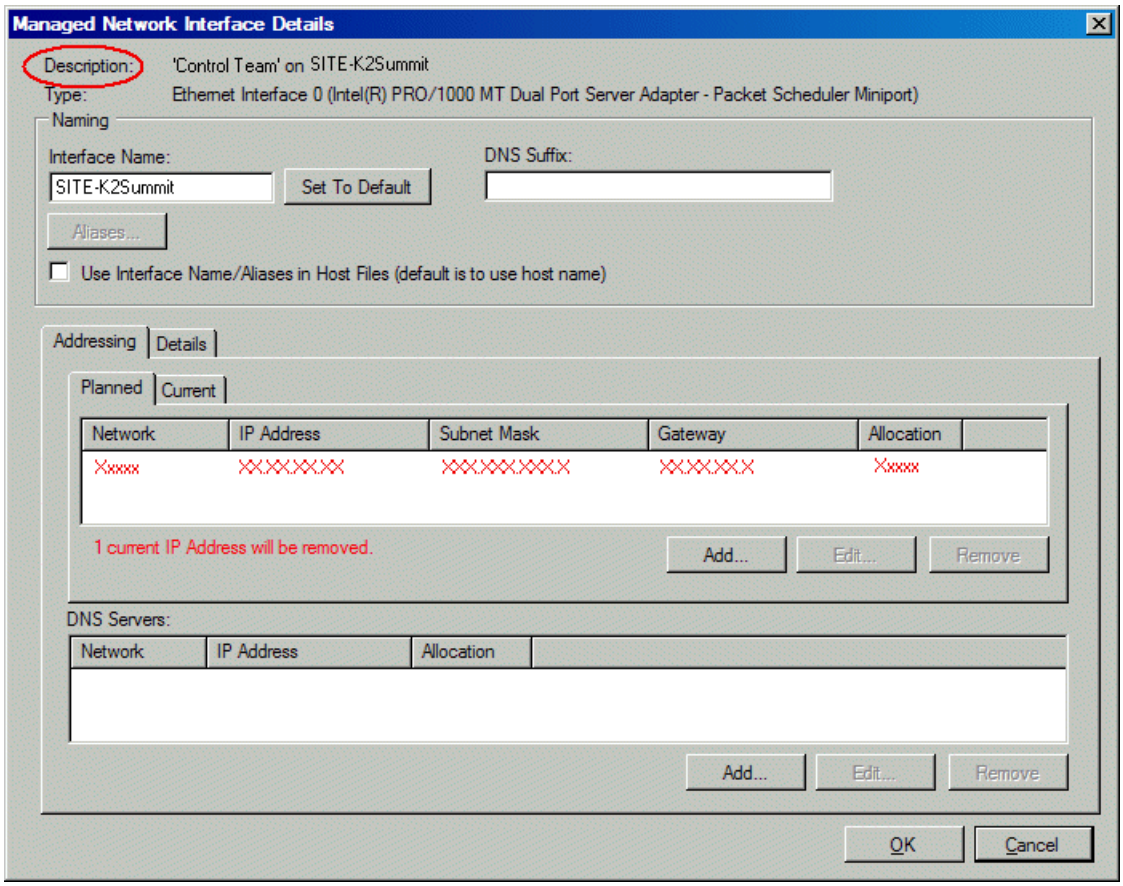
On a placeholder device, you edit network interfaces using the Unmanaged Network Interfaces dialog box.



The Unmanaged Network Interfaces dialog box allows you only to save changes to the system description.

Discovered device IP configuration

On a discovered device, you edit network interfaces using the Managed Network Interfaces dialog box.



The Managed Network Interfaces dialog box allows you to edit and save changes to the device.

Modifying K2 client unassigned (unmanaged) interface

Prerequisites for this task are as follows:

- The system description has a SAN K2 client that is a placeholder device.
- The placeholder device has a one or more unmanaged network interfaces.

Use this task to modify unmanaged network interfaces on a K2 SAN device as follows:

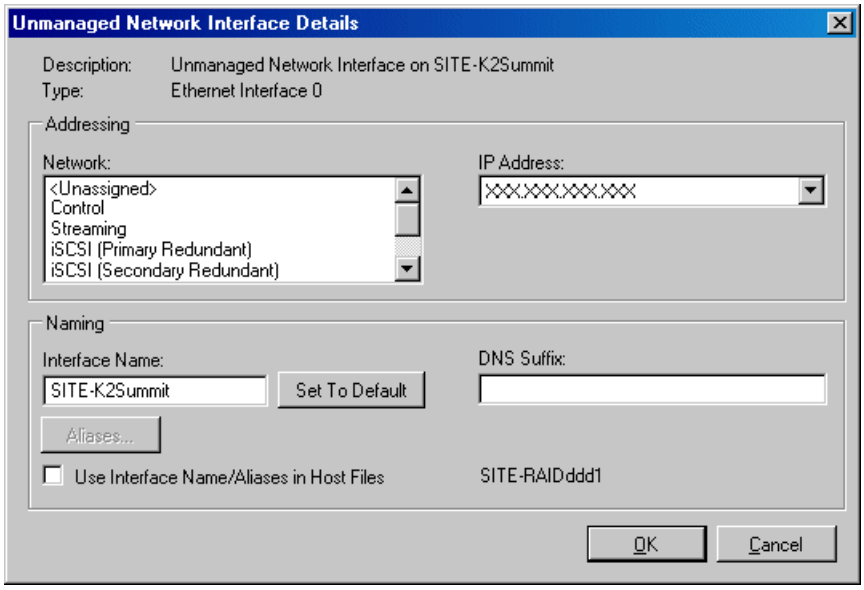
- K2 Summit Production Client

1. In the **Network Configuration | Devices** tree view, select a SAN K2 client placeholder device.

   The interfaces for that device are displayed in the interfaces list view.

2. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For media (iSCSI) network interface
Network	*iSCSI (non-Redundant)* is required for one iSCSI interface on a K2 client on a basic K2 SAN. The other iSCSI interface is unused.
	iSCSI (Primary Redundant) is required for one iSCSI interface on a K2 client on a redundant K2 SAN.
	iSCSI (Secondary Redundant) is required for the other iSCSI interface on a K2 client on a redundant K2 SAN
IP Address	The IP address for this interface on the network. Required.
Interface Name	Disabled, since names are excluded from the hosts file. Disregard.
Set to Default	Disabled, since names are excluded from the hosts file. Disregard.
...use Interface Name/Aliases in Host Files...	Disabled, since names are excluded from the hosts file. Disregard.
Aliases	Disabled, since names are excluded from the hosts file. Disregard.
DNS Suffix	Disabled, since names are excluded from the hosts file. Disregard.

NOTE: There is no FTP/streaming network for a SAN K2 client. On the K2 SAN, FTP/streaming goes to the K2 Media Server.

4. Click **OK** to save settings and close.

Modifying K2 Media Server unassigned (unmanaged) interface

Prerequisites for this task are as follows:

- The system description has a K2 Media Server that is a placeholder device.

- The placeholder device has a one or more unmanaged network interfaces.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

- 10G K2 Media Server
- NH K2 Media Server

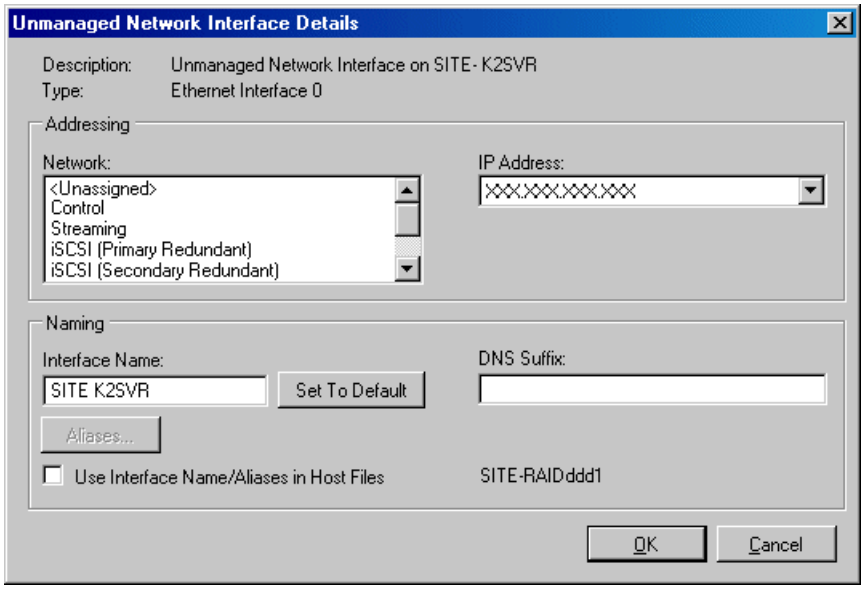
For the K2 Media Server, do not configure the Fibre Channel interface. SiteConfig does not manage this interface. It is represented in SiteConfig only to complete the description of the K2 Media Server.

1. In the **Network Configuration | Devices** tree view, select a K2 Media Server placeholder device.

   The interfaces for that device are displayed in the interfaces list view.

2. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For FTP/streaming network interface
Network	*Streaming* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name with the " _he0" suffix added is required. For example, if the host name is *K2prod01*, then *K2prod01_he0* is required here.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Selected* is required
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

Setting...	For media (iSCSI) network interface
Network	*iSCSI (non-Redundant)* is required on K2 Media Server for all interfaces of type iSCSI on basic K2 SAN.
	iSCSI (Primary Redundant) is required on K2 Media Server A for all interfaces of type iSCSI on redundant K2 SAN
	iSCSI (Secondary Redundant) is required on K2 Media Server B for interfaces of type iSCSI on redundant K2 SAN
IP Address	The IP address for this interface on the network. Required.
Interface Name	Disabled, since names are excluded from the hosts file. Disregard.

Setting...	For media (iSCSI) network interface
Set to Default	Disabled, since names are excluded from the hosts file. Disregard.
...use Interface Name/Aliases in Host Files...	Disabled, since names are excluded from the hosts file. Disregard.
Aliases	Disabled, since names are excluded from the hosts file. Disregard.
DNS Suffix	Disabled, since names are excluded from the hosts file. Disregard.

4. Click **OK** to save settings and close.

About SiteConfig support on K2 devices

Before SiteConfig can be used to discover or manage a device, the device must meet the following requirements:

- The device must be a Microsoft Windows operating system device.
- The device must have Microsoft .NET version 2.0 installed, as reported in the Windows Add/Remove Programs control panel.
- The SiteConfig Discovery Agent service must be running on the device, as reported in the Windows Services control panel.

For K2 clients and K2 Media Servers shipped new from Grass Valley with K2 software version 7.0 or higher, these requirements are pre-installed. These requirements are pre-installed on recovery images for these K2 systems as well. Therefore, if you suspect a problem with these requirements, do not attempt to install SiteConfig support requirements. If you must restore SiteConfig support requirements, re-image the K2 system.

Discovering devices with SiteConfig

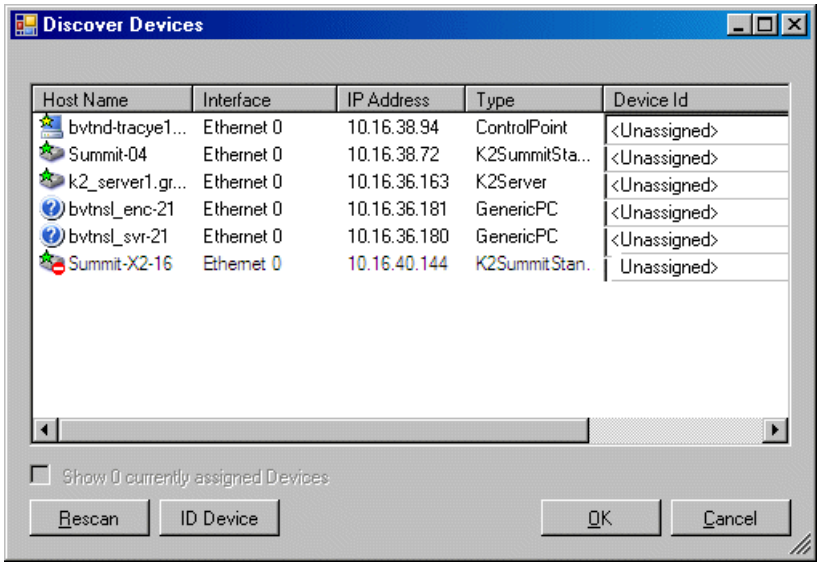
Prerequisites for this task are as follows:

- The Ethernet switch or switches that support the control network are configured and operational. If multiple switches, ISLs are connected and trunks configured.
- The PC that hosts SiteConfig is communicating on the control network.
- There are no routers between the PC that hosts SiteConfig and the devices to be discovered.
- Devices to be discovered are Windows operating system devices, with SiteConfig support installed.
- Devices are cabled for control network connections.
- If discovering a device with Microsoft Windows Server 2008 operating system, the device must have an IP address, either static or DHCP supplied.

1. Open SiteConfig.

2. In the toolbar, click the discover devices button.

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

Prerequisites for this task are as follows:

- Devices have been discovered by SiteConfig
- Discovered devices are not yet assigned to a device in the system description
- The system description has placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button .

   The Discover Devices dialog box opens.

2. Identify discovered devices.

   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.

3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.

4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:

   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.

5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.

6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying K2 client managed network interfaces

Prerequisites for this task are as follows:

- The physical device you are configuring has been discovered and is assigned to a device in the SiteConfig system description.
- SiteConfig has communication with the device.
- The device is defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

- K2 Summit Production Client

1. In the tree view select a K2 client, then in the Interfaces list view, identify interfaces as follows:

   - The SAN K2 client's control interface is a team. Modify the control team interface first. The control team is comprised of two individual interfaces, one for Control Connection #1 and one for Control Connection # 2. Do not modify these two individual interfaces.
   - For a SAN K2 client on a basic (non-redundant) K2 SAN, identify the iSCSI (non-Redundant) interface. After the control team, modify this interface as instructed in this procedure. Do not configure any other iSCSI interface, as only one iSCSI interface is used for a basic K2 SAN.
   - For a SAN K2 client on a redundant K2 SAN, identify the iSCSI (Primary Redundant) interface and the iSCSI (Primary Secondary) interface. After the control team, modify these interfaces as instructed in this procedure.
   - The SAN K2 client has no interface for FTP/streaming. All FTP/streaming goes to the K2 Media Server.

2. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - After you have successfully configured the control network interface, return to this step to configure each remaining interface.

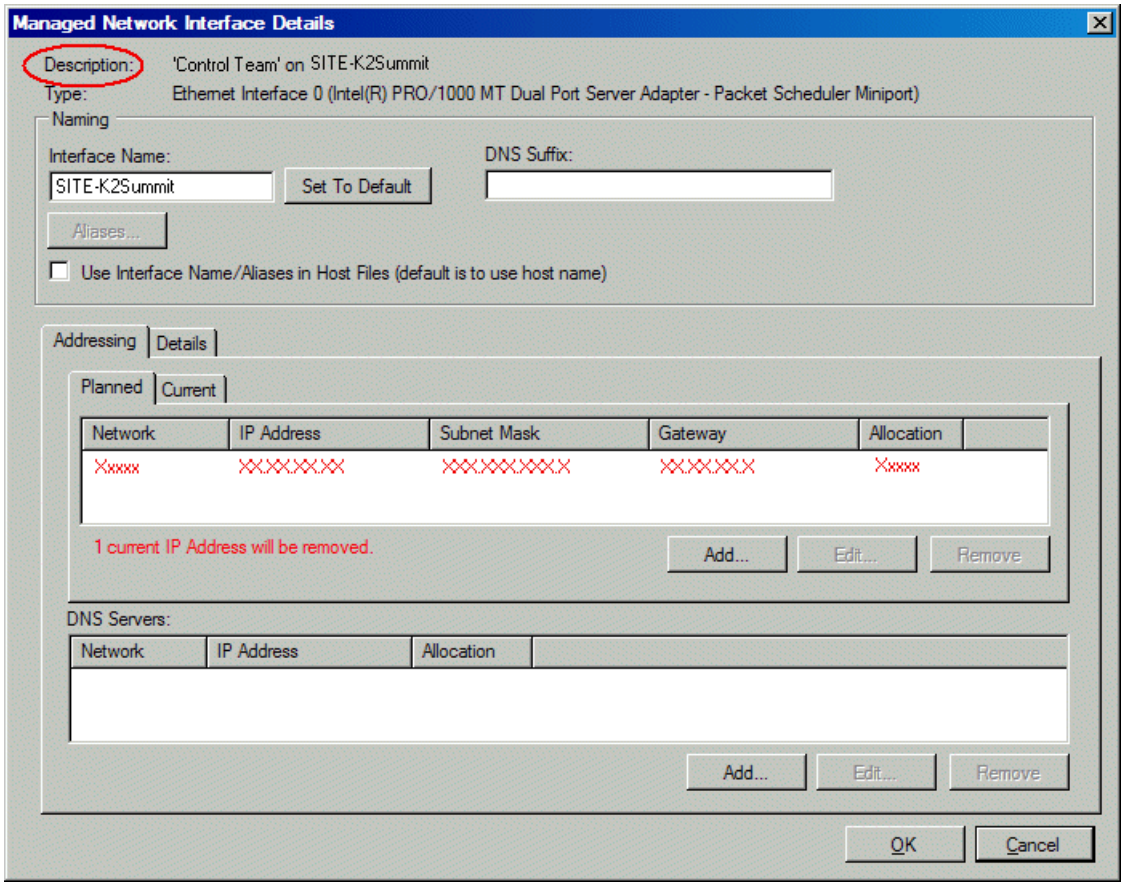
3. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

   NOTE: For the K2 Summit Production Client, make sure that the device is unlocked in SiteConfig before proceeding. This disables the write filter.

4. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

   The Managed Network Interface Details dialog box opens.



5. Identify the interface on the discovered device that you are configuring.

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.

6. Configure naming settings as follows:

Setting...	For network interface Control Team
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

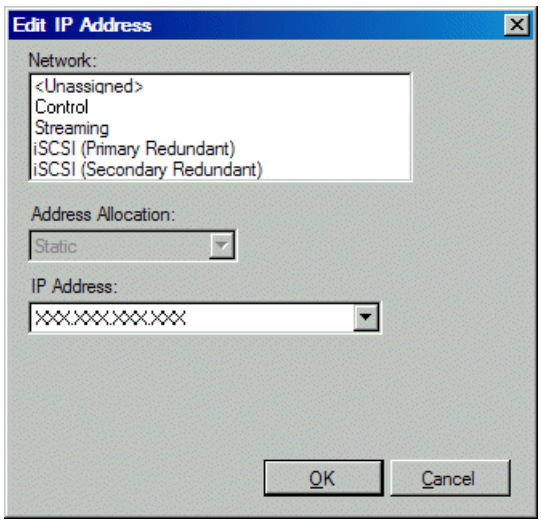
Setting...	For any network interface of type iSCSI
Interface Name	"Unused" is recommended. Displaying this text here serves as an aid in understanding SAN networks.The iSCSI network has no name resolution via the hosts file or otherwise, so the text you enter here is not actually use for name resolution.
Set To Default	Not recommended
DNS Suffix	Not allowed
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is recommended. Since this interface's network has its names excluded from the hosts file, this setting has no affect. The interface name is excluded from the hosts file, regardless of settings here.

NOTE: There is no FTP/streaming network for a SAN K2 client. On the K2 SAN, FTP/streaming goes to the K2 Media Server.

7. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

8. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	**For network interface Control Team**
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For basic SAN network interface Media Connection #1**
Network	*iSCSI (non-Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN network interface Media Connection #1**
Network	*iSCSI (Primary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN network interface Media Connection #2**
Network	*iSCSI (Secondary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

9. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

   A Contacting Device message box reports progress.

10. After configuring control network settings, do the following

    a) If a message informs you of a possible loss of communication, click **OK**.

       This message is normal, since this is the network over which you are currently communicating.

    b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

       The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

    c) In the Interface list view, right-click the interface and select **Ping**.

       The Ping Host dialog box opens.

       If ping status reports success, the interface is communicating on the control network.

       NOTE: For the K2 Summit Production Client, when configuration is complete, make sure you lock the device in SiteConfig. This enables the write filter.

Modifying K2 Media Server managed network interfaces

Prerequisites for this task are as follows:

- The physical device you are configuring has been discovered and is assigned to a device in the SiteConfig system description.
- SiteConfig has communication with the device.
- The device is defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on a K2 SAN device as follows:

- 10G K2 Media Server

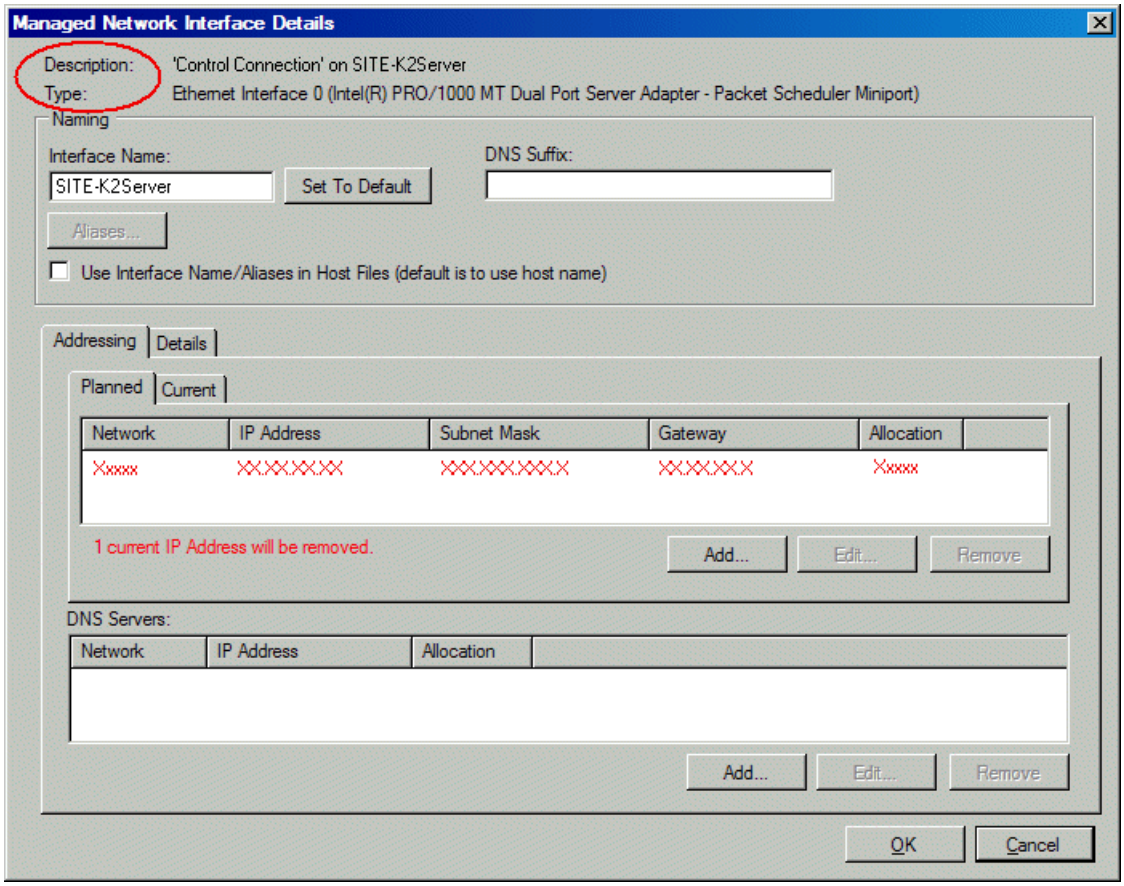
- NH K2 Media Server

1. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - After you have successfully configured the control network interface, return to this step to configure each remaining interface.
   - For the K2 Media Server, do not configure the Fibre Channel interface, which is a non-IP interface. SiteConfig does not manage this interface. It is represented in SiteConfig only to complete the description of the K2 Media Server.
2. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

3. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

   The Managed Network Interface Details dialog box opens.



4. Identify the interface on the discovered device that you are configuring.

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.
   - Identify iSCSI adapters by their "Type".

5. Configure naming settings as follows:

Setting...	For network interface Control Connection
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

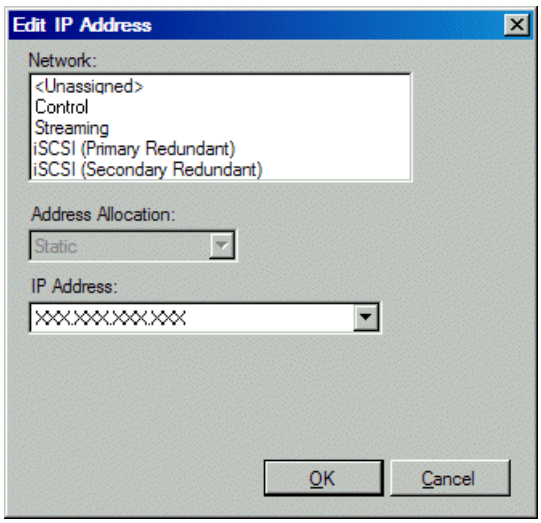
Setting...	For network interface FTP Connection
Interface Name	The device host name with the "_he0" suffix added is required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is required

Setting...	For any network interface of type iSCSI
Interface Name	The text "Unused" is recommended. Displaying this text here serves as an aid in understanding SAN networks.The iSCSI network has no name resolution via the hosts file or otherwise, so the text you enter here is not actually use for name resolution.
Set To Default	Not allowed
DNS Suffix	Not allowed
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is recommended. Since this interface's network has its names excluded from the hosts file, this setting has no affect. The interface name is excluded from the hosts file, regardless of settings here.

6. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.

7. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	**For network interface Control Connection**
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For network interface FTP Connection**
Network	*Streaming* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For basic SAN K2 Media Server any network interface of type iSCSI**
Network	*iSCSI (non-Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

Setting...	**For redundant SAN K2 Media Server A any network interface of type iSCSI**
Network	*iSCSI (Primary Redundant)* is required
Address Allocation	*Static* is required.

Setting...	For redundant SAN K2 Media Server A any network interface of type iSCSI
IP Address	The IP address for this interface on the network. Required.

Setting...	For redundant SAN K2 Media Server B any network interface of type iSCSI
Network	*iSCSI (Secondary Redundant)* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

8. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

   A Contacting Device message box reports progress.

9. After configuring control network settings, do the following
   a) If a message informs you of a possible loss of communication, click **OK**.

      This message is normal, since this is the network over which you are currently communicating.

   b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

      The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

   c) In the Interface list view, right-click the interface and select **Ping**.

      The Ping Host dialog box opens.

      If ping status reports success, the interface is communicating on the control network.

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.

3. Identify the state of buttons as follows:

   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.

4. If enabled, click **Set to Device Name**.

   This changes the host name to be the same as the device name.

5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

Prerequisites:

- The devices you are pinging are in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.

   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

About hosts files and SiteConfig

SiteConfig uses the network information in the system description to define a hosts file and allows you to view the hosts file. SiteConfig can manage this hosts file on Windows operating system devices that are in the system description and that are part of a SiteConfig managed network.

When you have successfully assigned devices and applied planned network settings to interfaces, it is an indication that host table information, as currently captured in the system description, is valid and that you are ready to have SiteConfig assemble the host table information into a hosts file. Your options for placing this host table information on devices are as follows:

- If you do not want SiteConfig to manage your host table information, you can manage it yourself. This is typically the case if your facility has an existing hosts file that contains host table information for devices that are not in the SiteConfig system description. In this case, you can have SiteConfig generate a single hosts file that contains the host table information for the devices in the system description. You can then copy the desired host table information out of the SiteConfig hosts file and copy it into your facility hosts file. You must then distribute your facility hosts file to devices using your own mechanisms.
- If you want SiteConfig to manage all information in hosts files on devices, you can have SiteConfig copy its hosts file to devices. In so doing, SiteConfig overwrites the existing hosts files on devices. Therefore, this requires that all devices that have name resolution through the hosts file be configured accordingly in the SiteConfig system description.

If you choose to have SiteConfig write hosts files to devices, the process consumes system resource and network bandwidth. Therefore you should wait until you have verified the information for all devices/interfaces in the host file, rather than updating hosts files incrementally as you discover/assign devices.

SiteConfig does not automatically deploy hosts files to managed devices as you add or remove devices. If you add or remove devices from the system description, you must re-deploy the modified hosts file to all devices.

Generating host tables using SiteConfig

Prerequisites for this task are as follows:

- Planned control network settings are applied to control network interfaces and devices are communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, have settings applied and are communicating.
- You have viewed host names, as currently defined in the system description, and determined that they are correct.
- The SiteConfig PC is added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.
3. Verify the information in the hosts file.

4. Do one of the following:

   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

   b) Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

Chapter 6

Managing K2 Software

This section contains the following topics:

- *Configuring K2 software deployment*
- *Backup and Recovery Strategies*

Configuring K2 software deployment

Take the following into consideration when using SiteConfig to deploy K2 SAN software.

- You typically configure one deployment group for K2 clients and one deployment group for K2 Media Servers. This allows you to target and sequence software deployment tasks to the different types of devices.
- You typically upgrade K2 Media Servers first, then K2 Media Clients.
- Always follow detailed steps in *K2 Release Notes* for the version of software to which you are upgrading.

Use the following topics to manage software deployment on a K2 SAN.

Configuring deployment groups

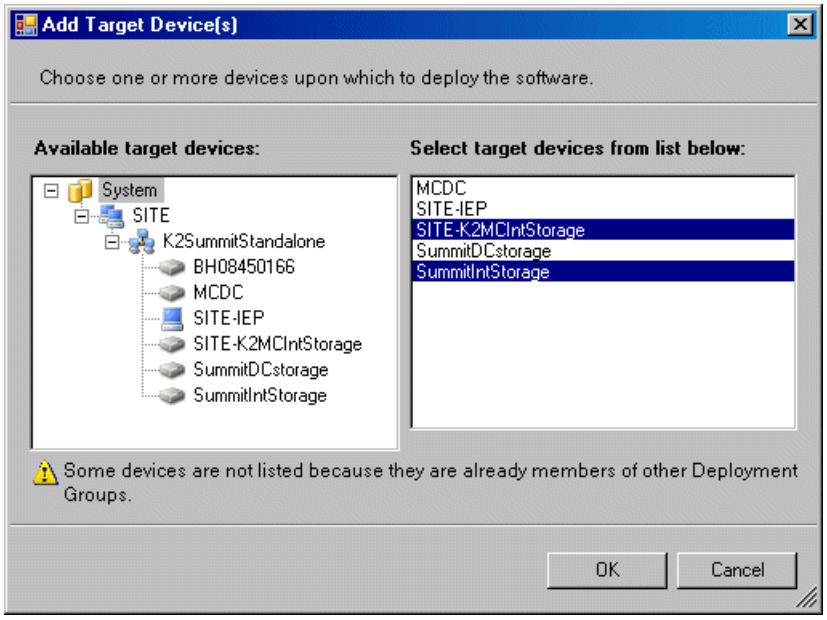
Prerequisites for this procedure are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.
2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.
3. Right-click the deployment group and select **Add Target Device**.

   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.

5. In the right-hand pane, select the devices that you are combining as a deployment group.

   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.

6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

Adding a software package to a deployment group

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.

   The Add Package(s) dialog box opens.

3. Do one of the following to select the software package:

   - Select from the list of packages then click **OK**.
   - Click **Browse**, browse to and select the package, then click **Open**.

4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

   SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

Checking all currently installed software on devices

Prerequisites for this task are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C$) on a device on which you are checking software.
- If the SiteConfig Network Configuration Kit and/or Discovery Agent at version lower than 1.1.0.185 is currently installed, it must be manually uninstalled and updated. For more information refer to *SiteConfig Migration Instructions*.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

   NOTE: If you have access problems, verify that the adminstrator account on the device has credentials as currently configured in SiteConfig.

   The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

About deploying software for the K2 SAN

You must control the sequence of software deployment tasks and device restarts as you upgrade software across the K2 SAN. The general sequence is to upgrade K2 Media Servers first then the SAN-attached K2 systems. The exact steps can vary from software version to version. Make sure you follow the task flow in the *K2 Release Notes* for the version of software to which you are upgrading.

Backup and Recovery Strategies

About the recovery disk image process

On the K2 Media Server, there are three partitions on the system drive to support backup and recovery strategies as follows:

- The C: drive is for the Windows operating system and applications.
- The D: drive is for the media file system (SNFS) and database. This allows you to restore the Windows operating system on the C: drive, yet keep the files on the D: drive intact. You can also restore the D: drive itself, however your backup and recovery strategy is different for non-redundant and redundant systems, as follows:
  - On non-redundant servers the media file system program, metadata, and journal files are on the D: drive. Also the media database program is on the D: drive. Therefore if you ever have a D: drive fault and you need to recover the data files (metadata, journal, and database), you can only restore them to the “snap-shot” contained in the most recent disk image you created. When you do this you restore the program files as well.
  - For redundant K2 SANs, the media file system program is on the D: drive, but the metadata and journal files are stored on the shared RAID storage. Also the media database program is on the D: drive, but the database data files are stored on the shared RAID storage. Therefore, if you ever have a D: drive fault, you can restore the media file system and database programs from a recovery disk image, and then access the data files (metadata, journal, database) from the shared RAID storage.
- The E: drive is for storing a system image of the other partitions. From the E: drive you can restore images to the C: and D: drives.

When you receive a K2 Media Server from the factory, the machine has a generic image on the E: drive. The generic image is not specific to the individual machine. It is generic for all machines of that type. Some K2 Media Servers also have a system-specific image on the E: drive.

You receive a recovery CD with your K2 Media Server. This recovery CD does not contain a disk image. Rather, the recovery CD is bootable and contains the Acronis True Image software necessary to create and restore a disk image. This recovery CD is specifically for the Windows server operating system which runs on the K2 Media Server. It is not for a desktop Windows operating system. Refer to "K2 Release Notes" for compatible versions of the recovery CD.

After your server is installed, configured, and running in your system environment, you should create new recovery disk images for the machine to capture settings changed from default. These "first birthday" images are the baseline recovery image for the machine in its life in your facility. You should likewise create new recovery disk images after completing any process that changes system software or data, such as a software upgrade. In this way you retain the ability to restore to a recent "last known good" state.

For the highest degree of safety, you should create a set of disk image recovery CDs, in addition to storing disk images on the E: partition. Since system drives are RAID protected, in most failure cases the disk images on the E: partition will still be accessible. But in the unlikely even of a catastrophic failure whereby you lose the entire RAID protected system drive, you can use your disk image recovery CDs to restore the system.

NOTE: Recovery disk images do not back up the media files themselves. You must implement other mechanisms, such as a redundant storage system or mirrored storage systems, to back up media files.

Recommended recovery process

The recommended recovery disk image process is summarized in the following steps.

At the K2 Media Server first birthday...

1. Boot from the Recovery CD.
2. Create a set of disk image recovery CDs. These CDs contain the C:, D:, and E: partitions.
3. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
4. Copy the disk image from the E: partition to another location, such as a network drive.

At milestones, such as after software upgrades…

1. Boot from the Recovery CD.
2. Create a disk image, writing the disk image to the E: partition. This disk image contains the C: and D: partitions.
3. Copy the disk image from the E: partition to another location, such as a network drive.

If you need to restore the K2 Media Server…

1. Boot from the Recovery CD.
2. If the E: partition is accessible, read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.
3. If the E: partition is not accessible, do the following:
    a. Read the disk image from your set of CDs and restore all three partitions
    b. Restart into Windows.
    c. Copy your most recent disk image to the E: partition.
    d. Boot from the Recovery CD.
    e. Read the image from the E: partition to restore the C: partition, restore the D: partition, or restore both partitions.

Plan a recovery strategy that is appropriate for your facility, then refer to procedures as necessary to implement your strategy.

Creating a recovery disk image for storing on E:

Do the following at the local K2 Media Server to create a disk image of the C: partition and the D: partition and store the image file on the E: partition:

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to forced a hard shutdown. The press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
4. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
5. In the Acronis main window, click **Backup**.

   The Create Backup Wizard opens.
6. On the Welcome page, click **Next**.
7. On the Partitions Selection page, do the following:
   a) Select the **(C:)** and the **(D:)** partitions and then click **Next**.
8. On the Backup Archive Location page, do the following:
   a) In the tree view select the **Backup (E:)** partition and enter the name of the image file you are creating.

      Create the file name using the machine hostname and the date. Name the file with the .tib extension.

      For example, if the hostname is MySystem1, in the File name field you enter *E:\MySystem1_20121027.tib*.

   b) Click **Next**.
9. On the Backup Options page, do not change any settings. Click **Next**.
10. On the Archive Comment page, if desired, enter image comments such as the date, time, and software versions contained in the image you are creating. Click **Next**.
11. On the "…ready to proceed…" page, do the following:
    a) Verify that you are creating images from the C: and D: partitions and writing to the E: partition, then click **Proceed**.
12. On the Operation Progress page, observe the progress report.
13. When a "Backup archive creation has been successfully completed" message appears, click **OK**.
14. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
15. Remove the recovery media while the machine is shutting down.

Restoring from a system-specific recovery disk image on E:

Use this task to restore a K2 Media Server using an image made from that particular K2 Media Server. If restoring from a generic factory default image, use the appropriate task.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. If you have not already done so, connect keyboard, monitor, and mouse.
3. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to forced a hard shutdown. The press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
4. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.
5. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.
6. On the Welcome page, click **Next**.
7. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
8. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
9. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
10. On the Restored Partition Location page, select **(C:)** and then click **Next**.
11. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
12. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
13. On the Next Selection page, depending on the partitions you are restoring, do one of the following:

    - If you are restoring only the C: partition, select **No, I do not** and then click **Next**.

      Skip ahead to the "…ready to proceed…" page in step 20.

    - If you are also restoring the D: partition, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.

      Continue with the next step in this procedure.

14. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
15. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.

16. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
17. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
18. On the Next Selection page, select **No, I do not** and then click **Next**.
19. On the Restoration Options page, do not make any selections. Click **Next**.
20. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
21. On the Operation Progress page, observe the progress report.
22. When a "The data was successfully restored" message appears, click **OK**.
23. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.
24. Remove the recovery media while the machine is shutting down.

Restoring from the generic recovery disk image on E:

There can be multiple versions of the generic recovery disk image on the server's E: partition. Refer to related topics in "K2 Release Notes" to determine which version you should use.

This procedure can be used on a server that needs to be restored to its factory default state. For example, if you neglected to make a first birthday image, you might need to use this procedure. If the image from which you are restoring was made from the specific machine, refer to the appropriate procedure.

NOTE: This procedure restores the server (both C: and D: partitions) to its factory default condition. Passwords and other site-specific configurations are reset to factory defaults.

1. Make sure that media access is stopped and that the system on which you are working is not being used.
2. Connect all motherboard NICs to LAN connections.
3. If the server has a 10 Gig connection, make sure it is connected to the 10 Gig connection on the Ethernet switch.

   If not connected to a switch, 10 Gig network adapter detection and ordering are unpredictable on the restored image.
4. If you have not already done so, connect keyboard, monitor, and mouse.
5. Do the following:
   a) Insert the Recovery CD.
   b) Restart the machine.

      If there is a problem restarting, hold the standby button down for five seconds to forced a hard shutdown. The press the standby button again to startup.

   The system boots from the Recovery CD.

   The Acronis program loads.
6. At the startup screen, select **True Image Server OEM (Full Version)**.

   The Acronis main window appears.

7. In the Acronis main window, click **Recovery**.

   The Restore Data Wizard opens.

8. On the Welcome page, click **Next**.
9. On the Backup Archive Selection page, in the tree view expand the node for the E: partition and select the image file, then click **Next**.
10. On the Restoration Type Selection page, select **Restore disks or partitions** and then click **Next**.
11. On the Partition or Disk to Restore page, select **(C:)** and then click **Next**.
12. On the Restored Partition Location page, select **(C:)** and then click **Next**.
13. On the Restored Partition Type page, leave the selection at **Active** and then click **Next**.
14. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual C: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
15. On the Next Selection page, select **Yes, I want to restore another partition or hard disk drive** and then click **Next**.
16. On the Partition or Disk to Restore page, select **(D:)** and then click **Next**.
17. On the Restored Partition Location page, select **(D:)** and then click **Next**.

    opens.

18. On the Restored Partition Type page, leave the selection at **Primary** and then click **Next**.
19. On the Restored Partition Size page, leave settings at their defaults. The size reported in the upper pane is the size detected of the actual D: partition. This should be the same as that reported in the Partition size field in the middle of the page. Free space before and Free space after should both be reported at 0 bytes. Click **Next**.
20. On the Next Selection page, select **No, I do not** and then click **Next**.
21. On the Restoration Options page, do not make any selections. Click **Next**.
22. On the "…ready to proceed…" page, verify that you are restoring the correct image to the correct location. Click **Proceed**.
23. On the Operation Progress page, observe the progress report.
24. When a "The data was successfully restored" message appears, click **OK**.
25. Click **Operations | Exit** to exit the Acronis True Image program.

    The machine restarts automatically.

26. Remove the recovery media while the machine is shutting down.

Next, do the following to restore the K2 Media Server to its factory-default state. Refer to related topics in this document or as otherwise indicated.

1. Set up Windows.
2. Restore network configuration.
3. Install K2 software and SNFS software. Refer to related topics in "K2 Release Notes".
4. Install the SiteConfig Discovery Agent.
5. Install Fibre Channel Card driver.
6. Activate Windows within 30 days.

Related Topics

Installing the Fibre Channel card driver on page 296

Activating the Windows operating system on page 123
Setting up Windows on page 123
Restoring network configuration on page 289
Installing the Discovery Agent on a K2 Media Server on page 122
Installing the Fibre Channel card driver on page 296
Activating the Windows operating system on page 123

Installing the Discovery Agent on a K2 Media Server

If the device that you plan to manage with SiteConfig does not have a SiteConfig Discovery agent installed, use this topic to verify and, if necessary, manually install SiteConfig support software. Doing so allows SiteConfig to discover and manage the device. If the device has any version of the SiteConfig Discovery Agent currently installed, you should use SiteConfig to upgrade the Discovery Agent, rather than installing it manually.

1. On the device you plan to manage with SiteConfig, open the Windows Services Control Panel and look for the following required item:
   - ProductFrame Discovery Agent
2. Proceed as follows:
   - If you find the required items, no further steps are necessary. SiteConfig support software is installed.
   - If a required item is not present, navigate to your SiteConfig files. If you do not already have these files in convenient location, you can find them on the PC that hosts SiteConfig, in the SiteConfig install location. Then continue with next steps as appropriate.
3. To launch the program that installs the ProductFrame Discovery Agent Service do the following:
   a) Copy the `Discovery Agent Setup` subdirectory to the device.
   b) In the `Discovery Agent Setup` directory, double-click the `DiscoveryAgentServiceSetup.msi` file.
   The setup program launches to install the SiteConfig Discovery Agent.
   c) Follow the setup wizard.
4. When presented with a list of device types, select the following:
   - K2Server
5. Complete the setup wizard and restart the device.
   The restart is required after the installation.

Setting up Windows

If a system is restored using the factory-default generic disk image or otherwise has the Windows operating system re-applied, a Windows set up process is required.

1. Upon first startup after reimage, a Windows Setup Wizard automatically opens. Work through the wizard as follows:
   a) Enter in the Windows Product Key and click **Next**.

      The Product Key is on a sticker on the top of the machine near the front right corner.

   b) Enter the name of the machine.

      To restore the factory-default name, enter the Serial Number (located at the right side and rear). The password is pre-set to the factory default. Leave the password as is.

   c) Click **Next**.
   d) Set Time and click **Next**.

   Windows loads components and restarts the K2 Media Server.
2. Upon restart, log in to Windows.
3. Rename the machine and set Windows clock as necessary.

Activating the Windows operating system

If a system is restored to its factory default state or otherwise has the Windows operating system re-applied, you might need to activate the operating system. This procedure provides instructions for doing this while the machine is connected to the Internet. The Activation wizard provides other options, which you can also choose if desired.

To active the Windows operating system, do the following:

1. Make sure the machine is connected to the Internet.
2. From the Windows desktop, in the system tray double-click on the key symbol icon. The Activate window opens.
3. Select **Yes, let's activate Windows over the Internet now** and click **Next**.
4. When prompted, "If you want to register with Microsoft right now.", select **No**.
5. Wait for the connection. If the system times out, you are prompted for entering information in the Internet Protocol Connection dialog. Enter the proxy address and port number as appropriate for your facility's connections.
6. Ensure that "You have successfully activated your copy of Windows" message appears in Activate Windows.
7. Click **OK** to close the Activate Windows.

Chapter 7

Configuring and licensing the K2 SAN

This section contains the following topics:

- *About K2 SAN licensing*
- *About QOS on the K2 SAN*
- *Importing a SiteConfig system description*
- *Configuring the basic K2 SAN - Online and Production*
- *Configuring the redundant K2 SAN - Online and Production*
- *Configuring the basic nearline K2 SAN*
- *Configuring the redundant nearline K2 SAN*

About K2 SAN licensing

When you purchase your K2 SAN, Grass Valley sizes the SAN according to your requirements for bandwidth and other considerations. Part of this sizing exercise is the application of the appropriate license for your SAN.

The K2 SAN license enables bandwidth in increments. A SAN with no license allows the lowest amount of bandwidth. With a license installed, additional bandwidth is allowed according to the bandwidth increment count embedded in the license.

The SAN license is a Sabretooth license. The license is installed on K2 Media Servers with role of iSCSI bridge. When you receive your SAN new from Grass Valley, the license is pre-installed. The K2Config application references the license on the K2 Media Server. When you add a client you specify its bandwidth and the K2Config application subtracts this bandwidth from the amount allowed by the license. The K2Config application reports when the total amount allowed is consumed and then does not allow you to add any more clients.

If you do not already have the highest bandwidth license on an existing system and you need more bandwidth and/or client connections, you can upgrade the license. You can replace your existing license with a license that has a higher bandwidth increment count embedded. You must consult with Grass Valley for a re-evaluation of your system design as part of the upgrade process. Some systems can require additional disks to support the increased bandwidth enabled by the license upgrade.

If you install K2 software version 7.3 or higher on K2 SAN with 1 GB iSCSI adapters (TOEs), no license is required. This is because the default amount of bandwidth allowed for a K2 SAN with no license is adequate for the maximum bandwidth needed for 1 GB iSCSI adapters.

About QOS on the K2 SAN

Grass Valley designs your system using Quality of Server (QOS) features for different categories of client Input/Output (I/O) traffic, as follows:

- Real Time Input Output (RTIO) — Clients supporting record/play operations are guaranteed I/Os with first priority.
- Non-Realtime Input Output — Clients that are not real-time, such as FTP servers, share an I/O pool that is separate from the real-time I/Os. The non-realtime clients can also temporarily use real-time I/Os when those I/Os are not being used by real-time clients.
- Reserved Input Output (RVIO) — Clients that have specific I/Os requirements are each assigned their own portion of the I/O pool. This guarantees the client has the I/Os it requires and also prevents the client from exceeding its designed amount. These I/Os are reserved only while the client is powered up. If the client is shutdown, the client's reserved I/Os become available in the I/O pool for use by other clients.

The exact QOS values for your K2 SAN are calculated by Grass Valley to meet your workflow requirements. When you operate your K2 SAN within the bounds of those requirements you should have no bandwidth problems, even during peak bandwidth events. If your workflow requirements change, allow Grass Valley to re-calculate your QOS values. Some versions of K2 software have a RVIO calculator in the K2Config application. Do not use the RVIO calculator to change your RVIO

value. The calculator is intended for use by qualified Grass Valley personnel only. Do not attempt to change any QOS values without guidance from Grass Valley. Doing so can result in unexpected performance problems.

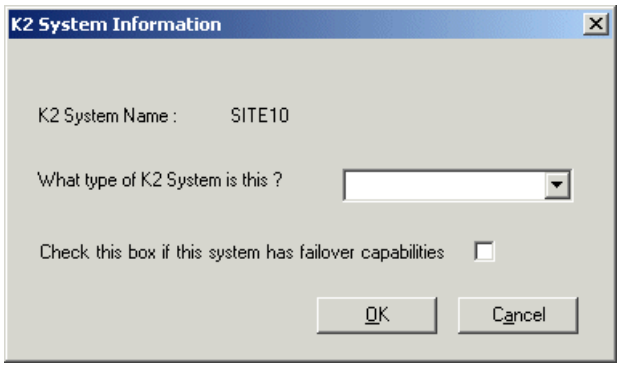
Importing a SiteConfig system description

You can import a SiteConfig system description that contains a K2 SAN into the K2Config application. You should do this only after the K2 SAN is fully complete and implemented in SiteConfig, as changes are not automatically synchronized between SiteConfig and K2Config after the import.

When you import a SiteConfig system description, K2Config identifies your SAN devices, defines the SAN, and displays the unconfigured SAN in the tree view. Therefore you do not need to define the K2 SAN in K2Config. You can skip this task and instead begin your work in K2Config by configuring the first K2 Media Server.

1. In the K2Config application, click **File | Import SiteConfig**.
2. Browse to and select the system configuration file.

   A K2 System Information dialog box opens.



3. In the drop-down list, select the type of K2 SAN that you are importing.
4. If a redundant K2 SAN, select "…**failover capabilities**…"
5. Click **OK**.
6. The SAN appears in the K2Config application.

Configuring the basic K2 SAN - Online and Production

Work through the topics in this section sequentially to configure an Online (Tier 1) or Production (Tier 2) basic, non-redundant K2 SAN.

Prerequisites for initial configuration - Basic K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software installed
- Control network IP address assigned
- Network communication over the control network with all other K2 devices
- Power on

Ethernet switch

- Ethernet cables connected
- Control network IP address assigned
- VLANs set up
- Trunks set up
- Power on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable connected
- Software installed, as from the factory, including QuickTime 7
- Control network IP address assigned
- Power on for all servers

K2 RAID chassis

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

K2 RAID Expansion chassis (optional)

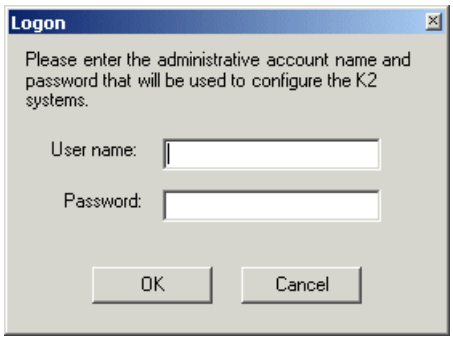
- Fibre channel cable(s) connected
- Power on

Defining a new K2 SAN

If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

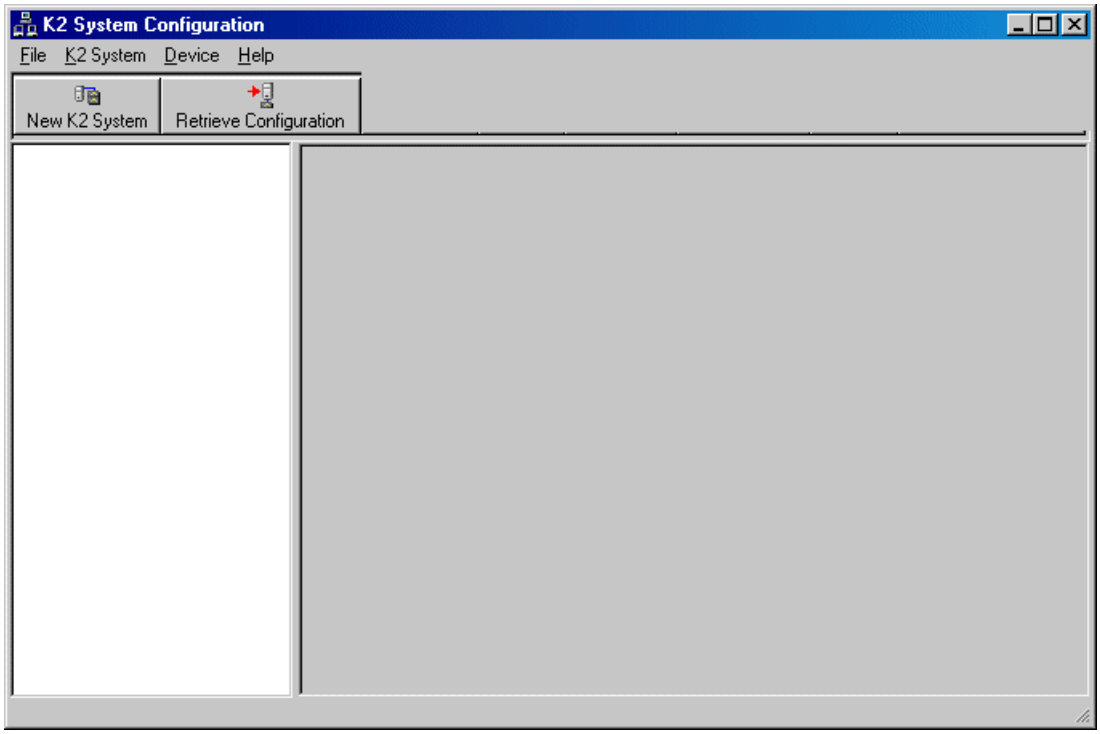
1. On the control point PC, open the K2Config application.

   A login dialog box opens.



2. Log in to the K2Config application with the Windows administrator account.

   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

Related Topics

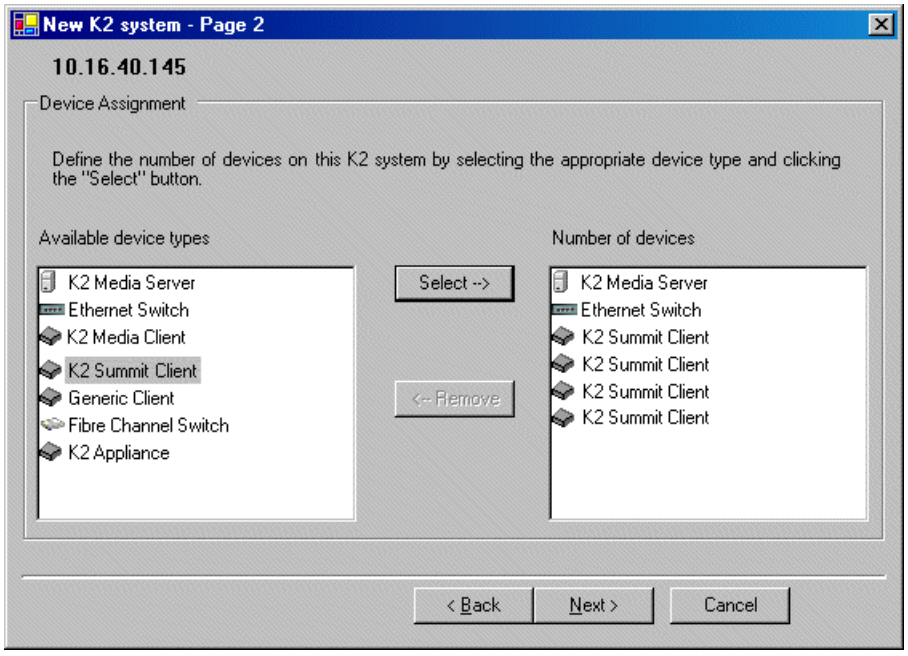
About application security on the K2 SAN on page 272

Configure New K2 System page 1 - Basic K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **L30**.
3. If so designed, select **Enable Live Production mode**.
   Do not select the Server redundancy option.
4. Click **Next**.

Page 2 opens.

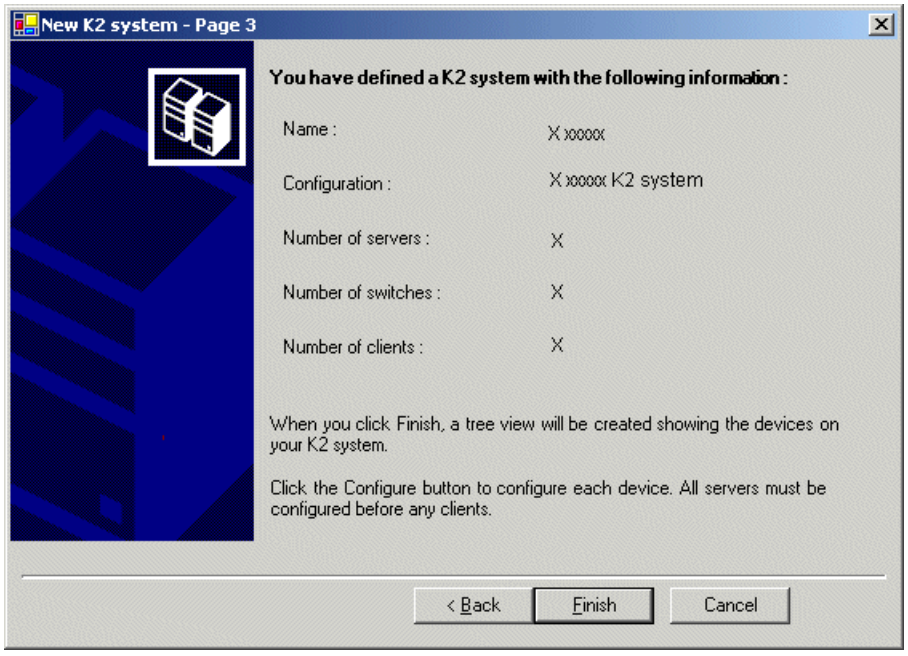
Configure New K2 System page 2 - Basic K2 SAN



1. Move the following into the Number of devices box:
   - One K2 Media Server
   - One Ethernet switch
   - K2 clients as appropriate for your system.
   - (Optional) One or more K2 Media Servers to represent each NH K2 Media Server on your system.
   - (Optional) Other devices as appropriate for your system.
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Basic K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a 10G basic K2 SAN you should have the following:
   - One Gigabit Ethernet switch
   - One K2 Media Server
   - Optionally, one or more NH K2 Media Servers
   - The number and type of clients appropriate for your system.
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

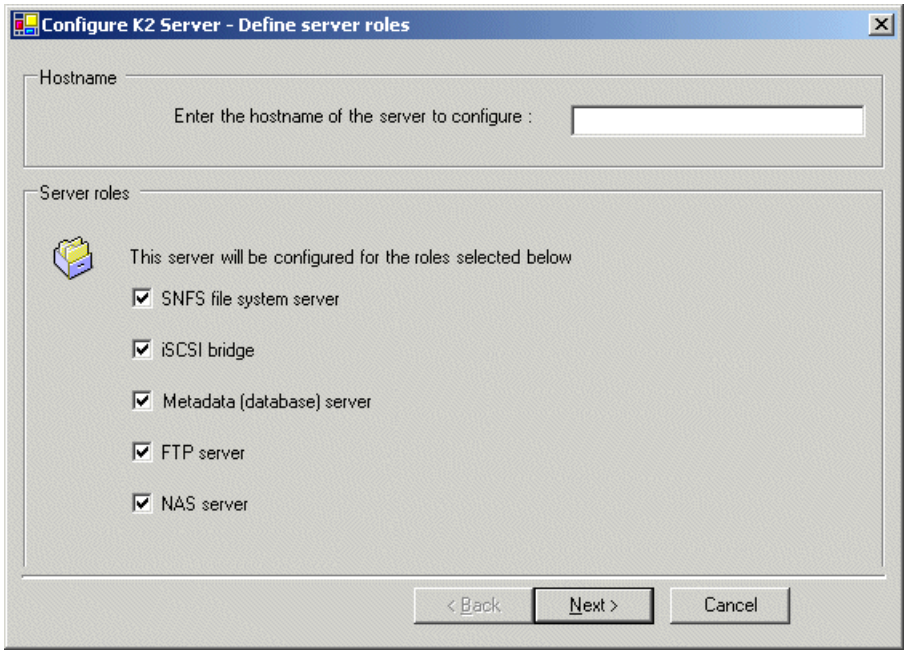
Next, configure the server.

Configuring the server - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Basic K2 SAN

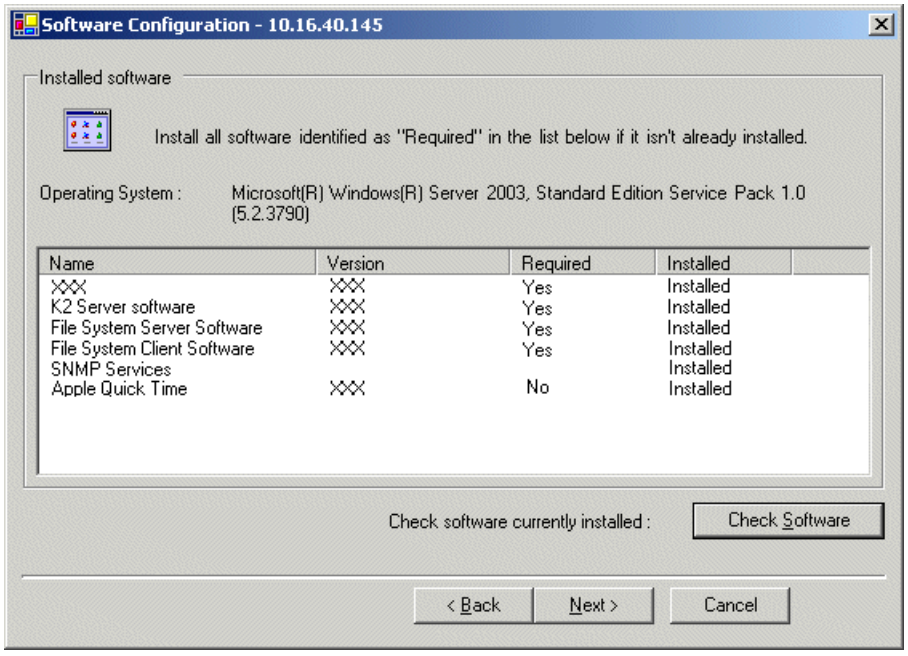


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Basic K2 SAN

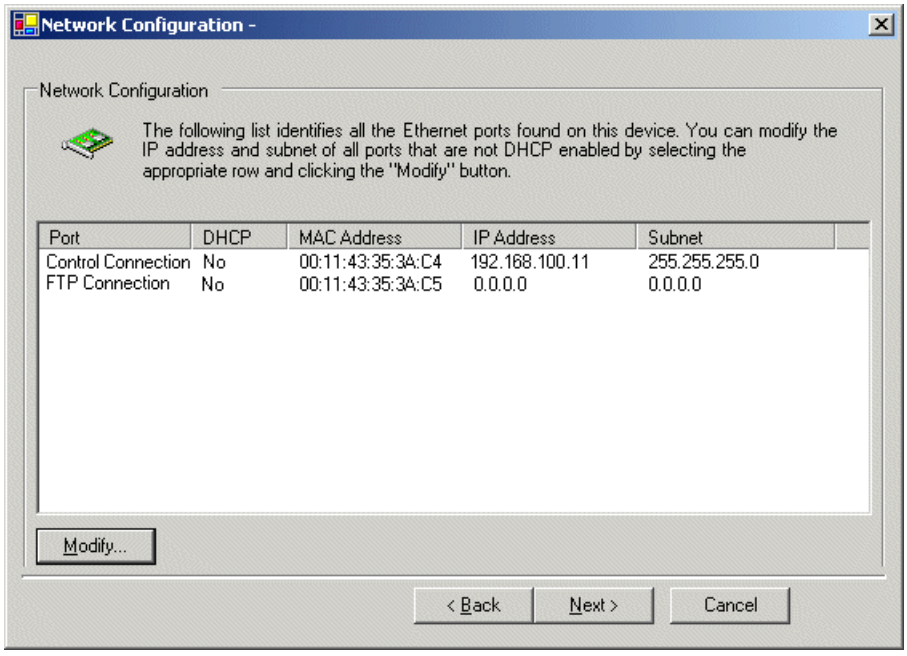


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Basic K2 SAN



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

      A network configuration dialog box opens.

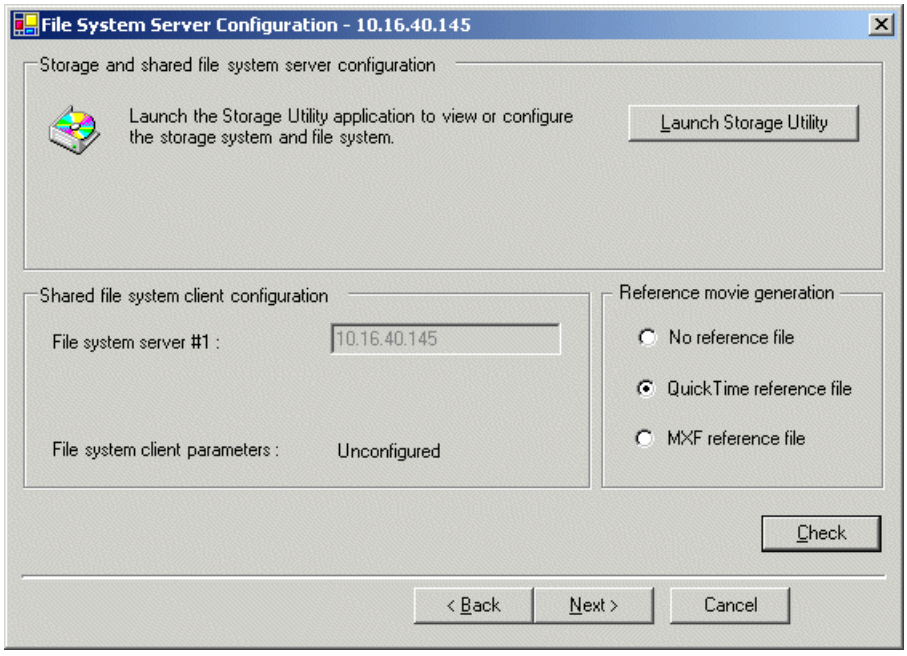
   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Basic K2 SAN



This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. Click **Launch Storage Manager**.

   Storage Utility opens.

2. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings - Basic

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected

- Power on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

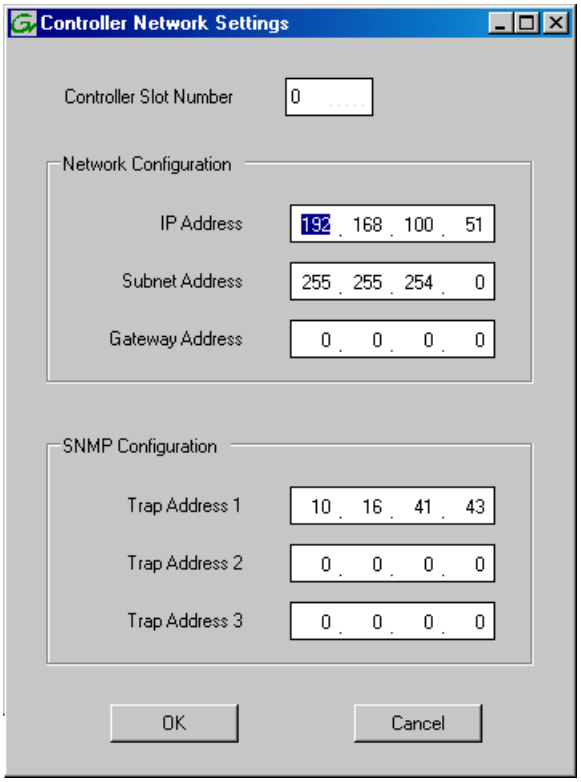
- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module, so the combined RAID storage devices, including the optional Expansion chassis, exist as a single entity on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.
6. For SNMP Configuration, enter the IP address of the NetCentral server PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.
7. Click **OK** to save settings and close.
8. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Basic K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

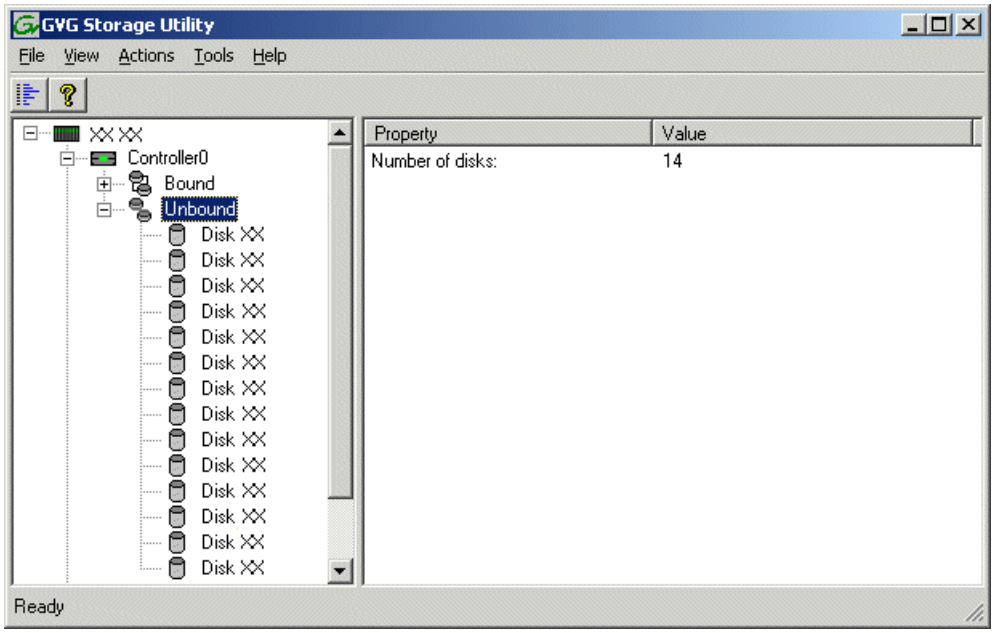
- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected
- Power on

NOTE: Binding destroys all user data on the disks.

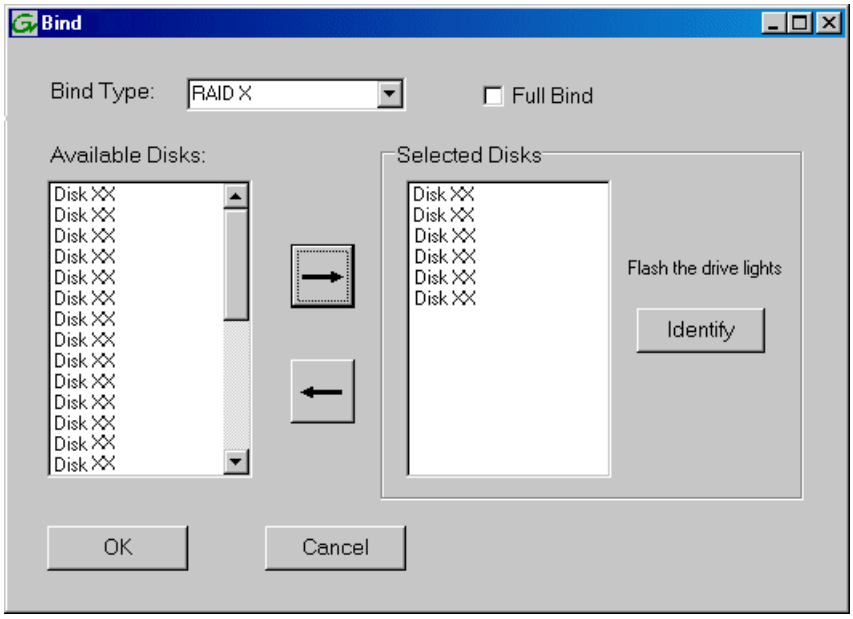
1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 5** or **RAID 6**, as specified by your system design.
7. In the Available Disks box, select six contiguous disks at the top of the list.

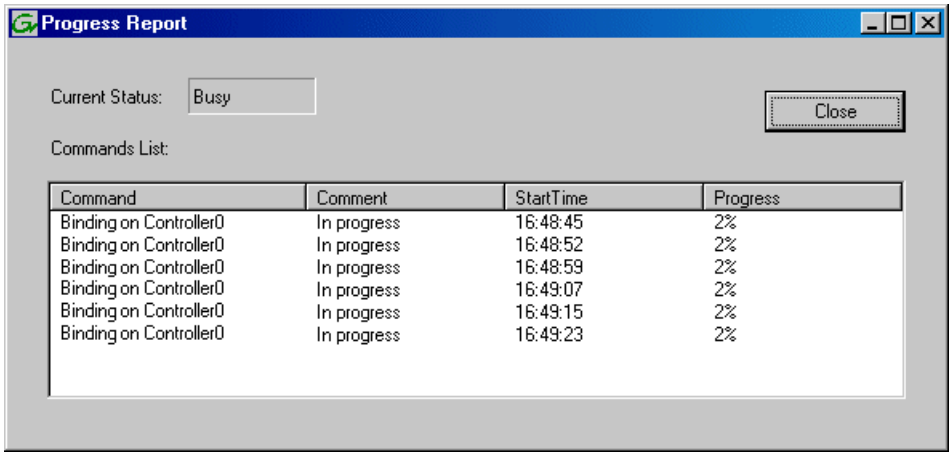
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    For basic storage you should have two RAID 5 or RAID 6 RANKs of six disks each on the primary RAID storage device. For each optional Expansion chassis, you would have an additional one or two RAID 5 or RAID 6 RANKs of six disks each.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

Related Topics

Identifying disks on page 321
About full/background bind on page 325
Binding Hot Spare drives on page 327

Creating a new file system - Basic K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

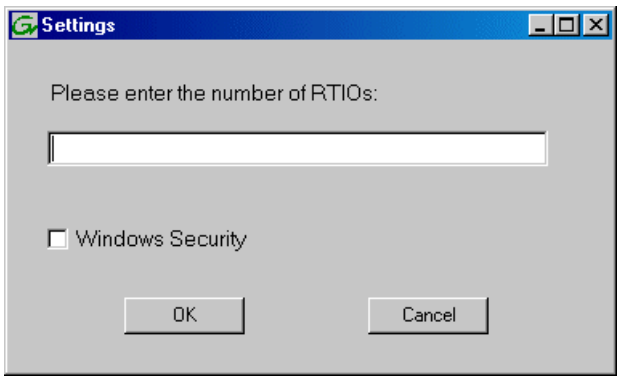
- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on
- Disks bound

Prerequisites for the optional K2 RAID Expansion chassis are as follows:

- Fibre channel cable(s) connected
- Power on

- Disks bound

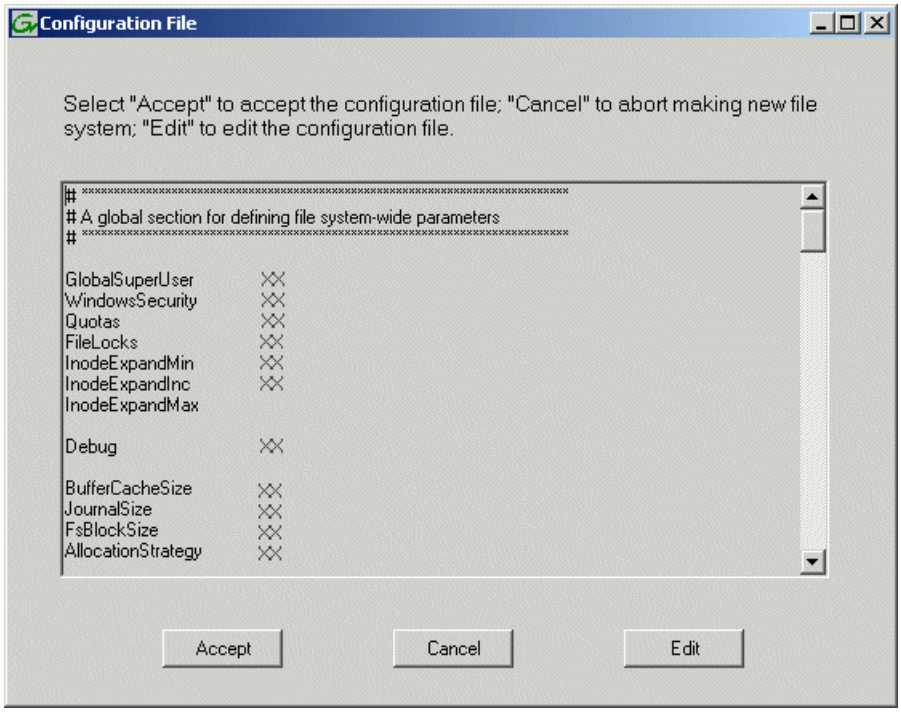
1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For the Real Time Input/Output (RTIO) rate, enter the value specified by your system design. If you do not know this value, contact your Grass Valley representative.
5. Configure Windows Security as follows:
   - If the K2 SAN is to be accessed by only K2 clients leave Windows Security unchecked.
   - If the K2 SAN is to be accessed by Aurora Edits, refer to the *Aurora Edit Installation and Configuration Guide* for instructions.

6. Click **OK**.

   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

7. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

Next, continue with configuring the server using the K2Config application.

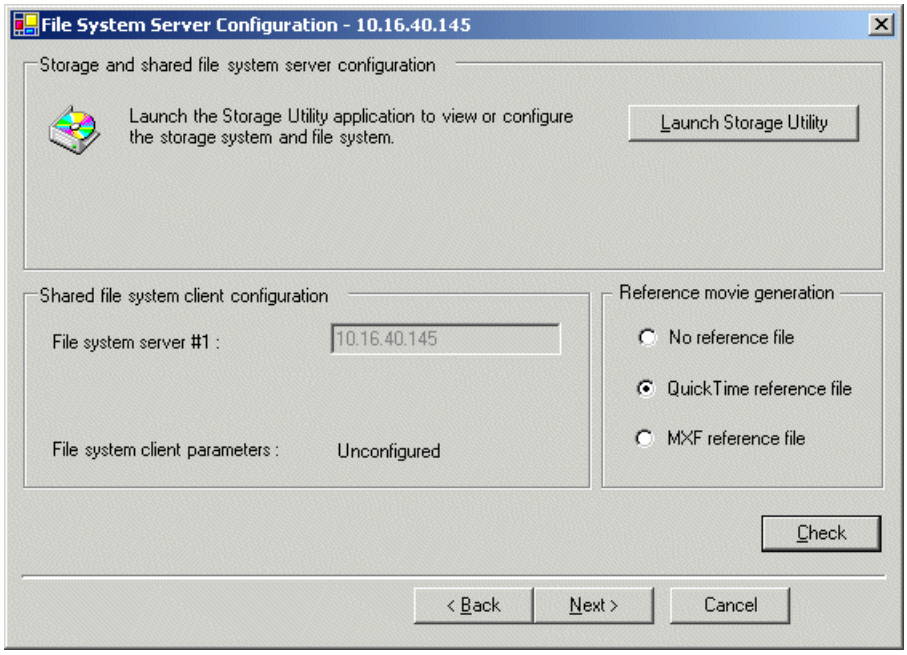
Configuring the server - Part 2

Configure File System Server Configuration page - Basic K2 SAN

Prerequisites for connected K2 RAID storage:

- Network and SNMP settings configured
- Disks bound

- New file system made



This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. In K2Config open the server's File System Server Configuration page, if the page is not already open.
2. If desired, configure reference file generation.
3. Click **Check**.
4. When the wizard reports that the configuration is correct, click **Next**.

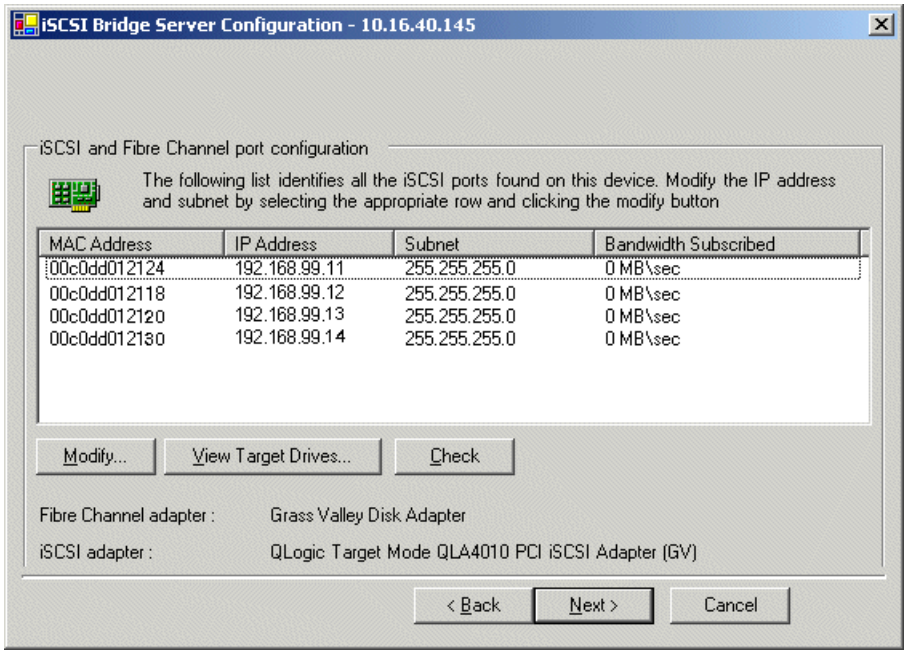
   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Related Topics

Configuring reference file type on a K2 SAN system on page 280

Configure iSCSI Bridge Server Configuration page - Basic K2 SAN



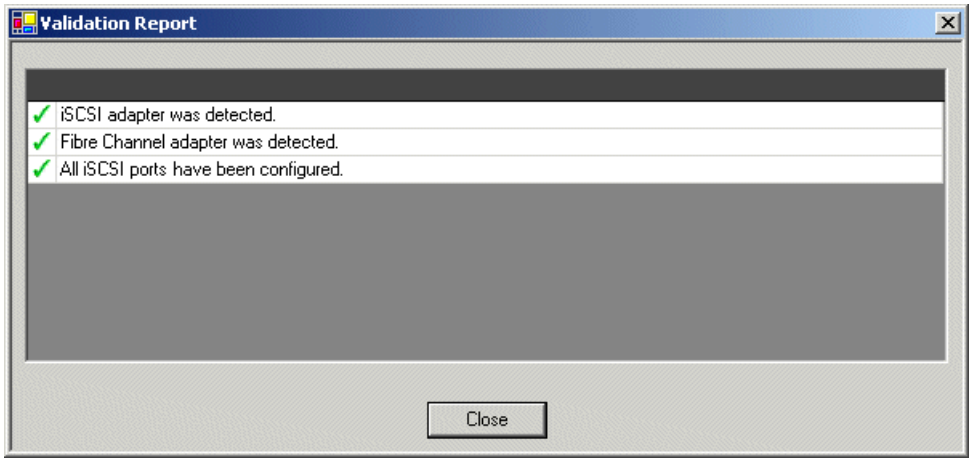
This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

1. Select an iSCSI adapter and do the following:
   a) Click **Modify**.

      A network configuration dialog box opens.

   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
2. Repeat the previous step for the other iSCSI adapters.

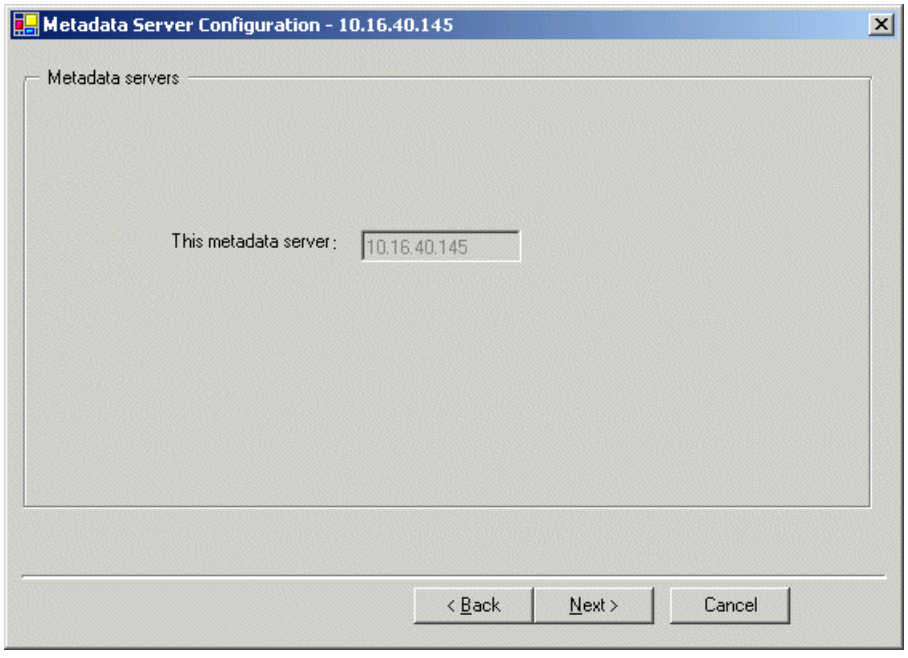
3. Click **Check**.
   The Validation Report opens.



4. Confirm that the iSCSI configuration is successful.
5. Close the Validation Report.
6. Click **Next**.

The Database Server Configuration page opens.

Configure Database Server Configuration page - Basic K2 SAN

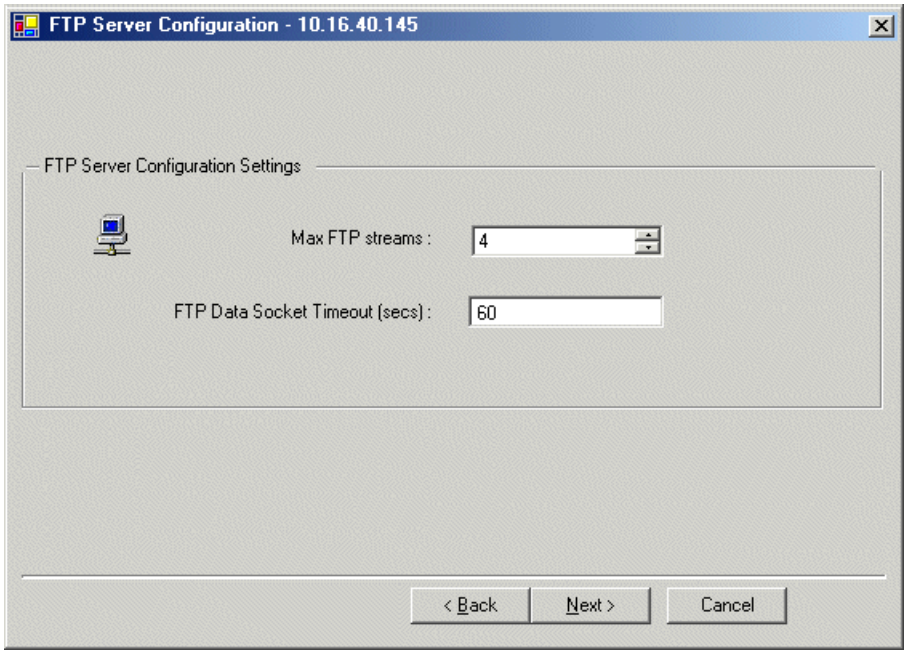


Click **Next**.

You do not need to enter or configure anything on this page.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Basic K2 SAN



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Proceed as follows:

- If you have NH servers, configure them next.
- If you do not have NH servers, configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring optional NH servers

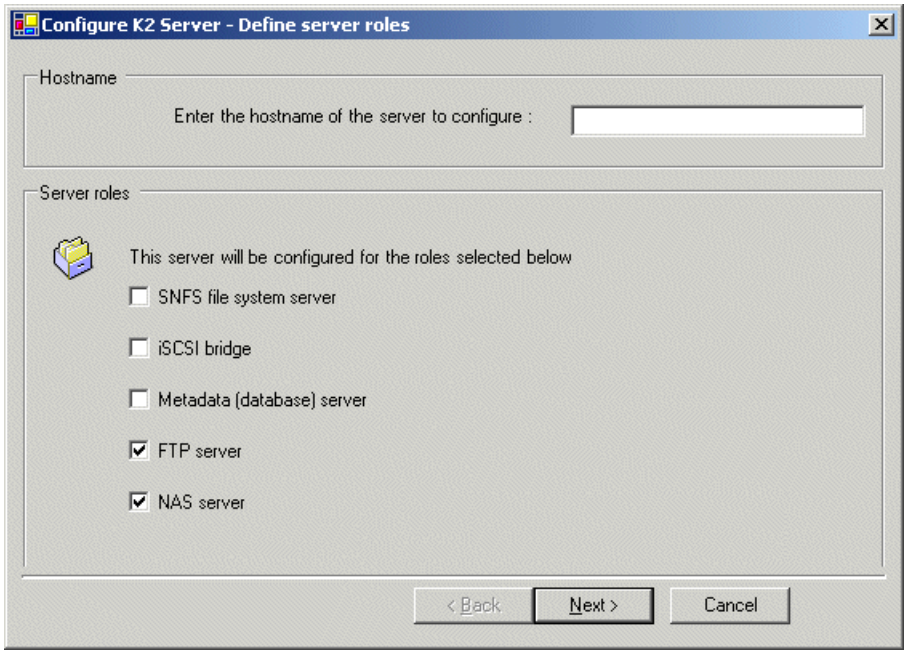
If you have one or more optional NH K2 Media Servers, you next configure those servers. This section applies to both NH1 (1 Gig FTP) servers and NH10GE (10 Gig FTP) servers.

NOTE: Multiple NH servers on a K2 SAN must be of the same type, either all NH1 or all NH10GE.

1. In the K2Config application tree view, select the K2 Media Server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

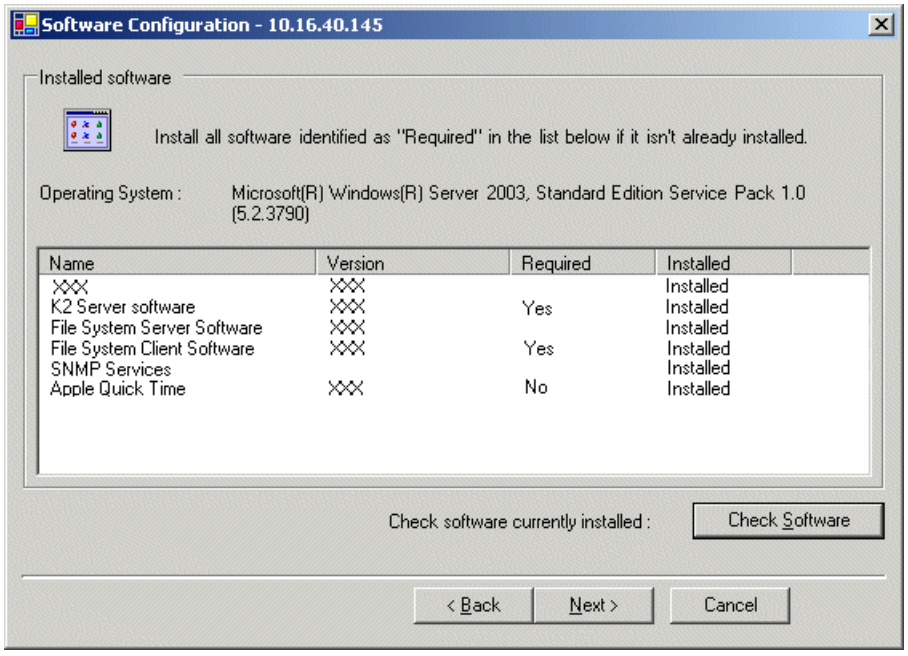
Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select **FTP server** and **NAS server**.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

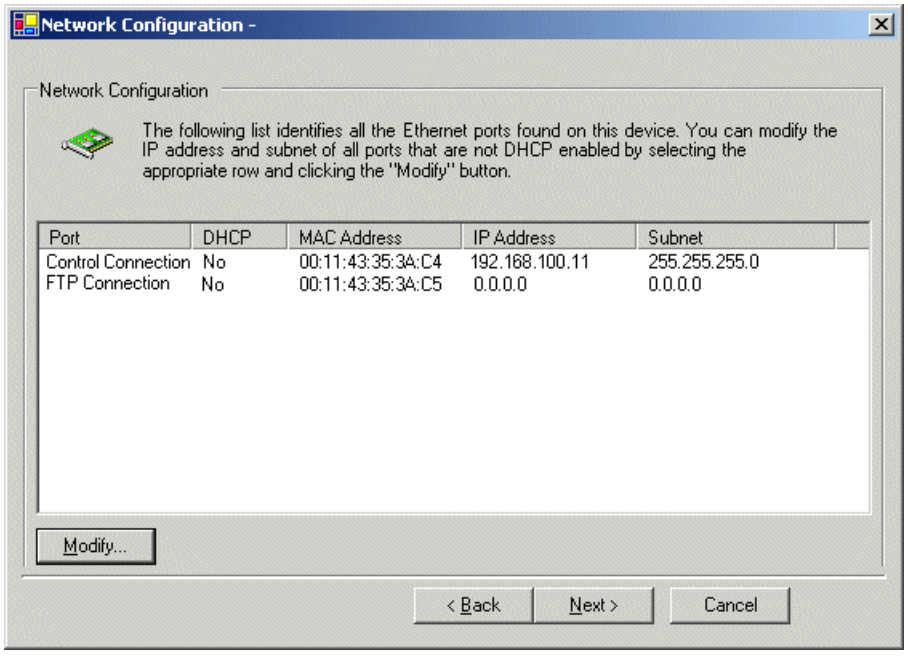


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

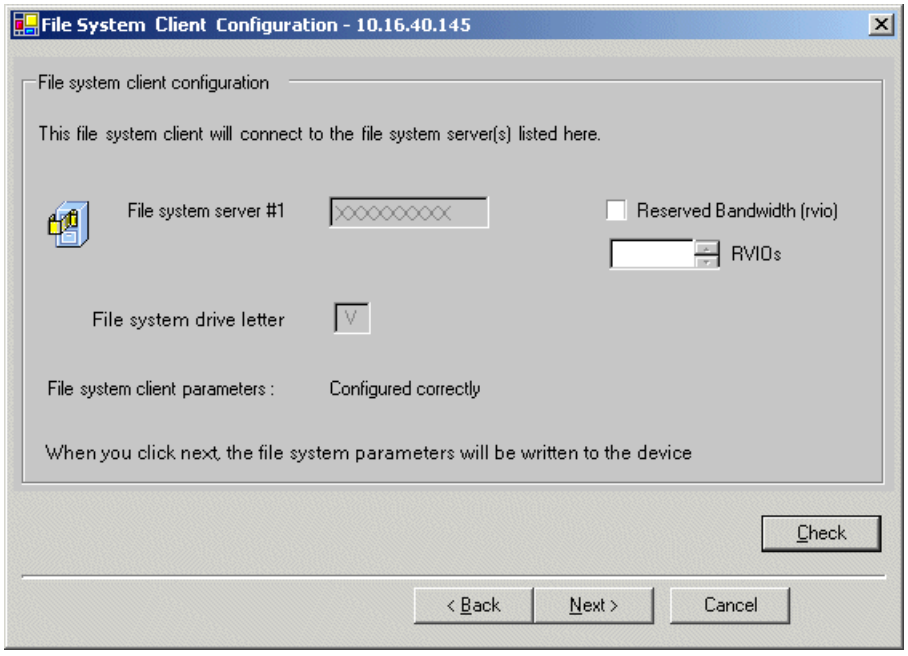
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Client Configuration page - NH server



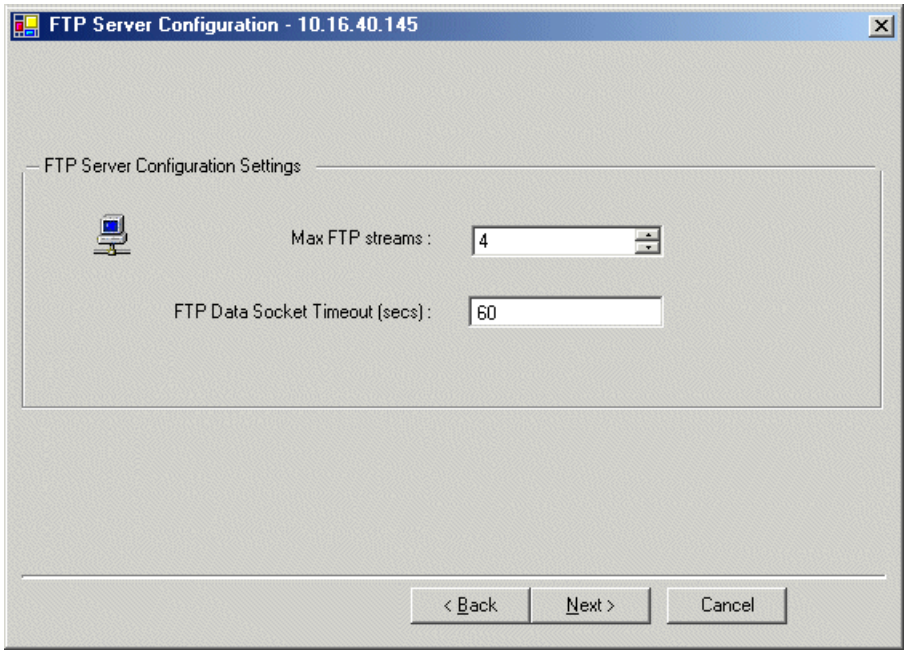
This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Basic SAN NH server



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

If you have other NH servers, configure them similarly, then configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring the redundant K2 SAN - Online and Production

Work through the topics in this section sequentially to configure an Online (Tier 1) or Production (Tier 2) redundant K2 SAN.

Prerequisites for initial configuration - Redundant K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software installed
- Control network IP address assigned
- Network communication over the control network with all other K2 devices
- Power on

Ethernet switch

- Ethernet cables connected
- Control network IP address assigned
- VLANs set up
- Trunks set up
- Power on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable connected
- Redundant servers connected by serial cable
- Software installed, as from the factory, including QuickTime 7
- Control network IP address assigned
- Power on for all servers

K2 RAID chassis

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

K2 RAID Expansion chassis (optional)

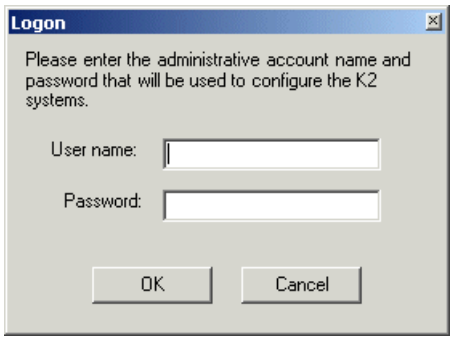
- Fibre channel cable(s) connected
- Power on

Defining a new K2 SAN

If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

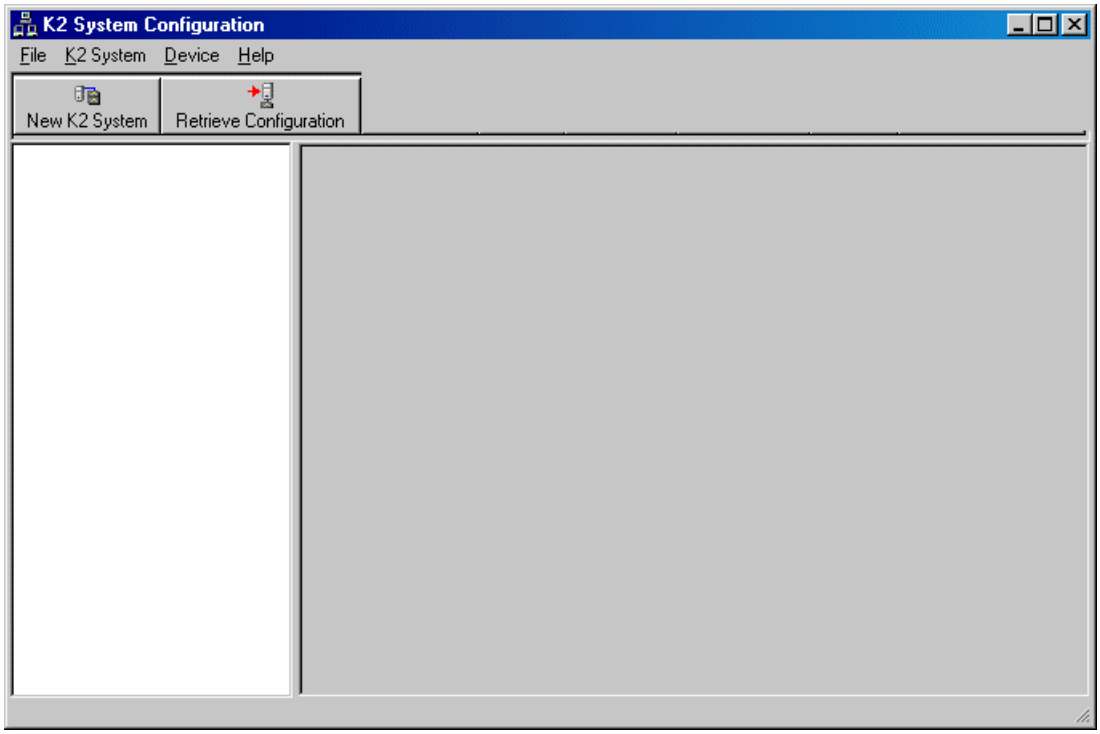
1. On the control point PC, open the K2Config application.

   A login dialog box opens.



2. Log in to the K2Config application with the Windows administrator account.

   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

Related Topics

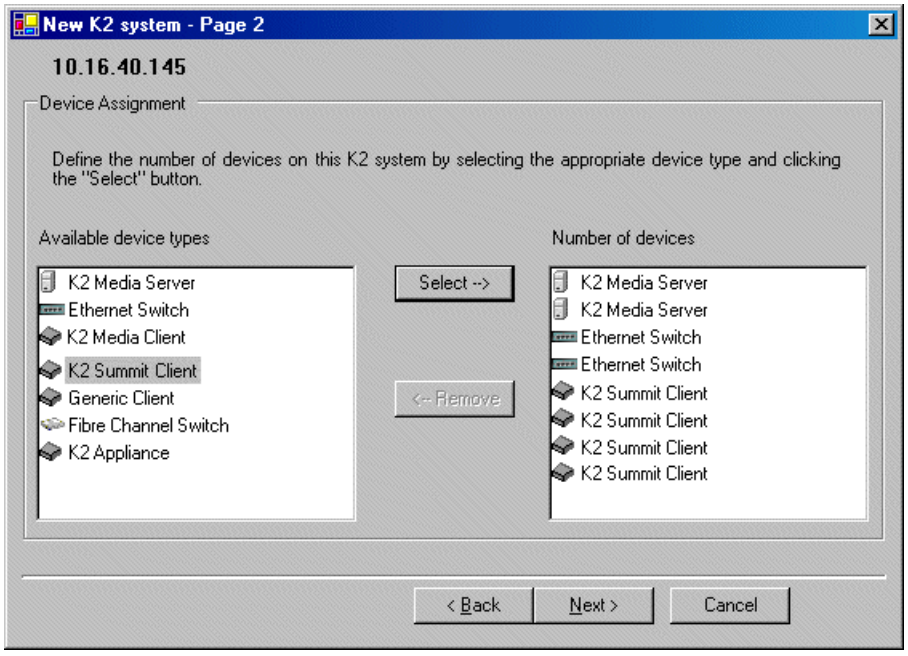
About application security on the K2 SAN on page 272

Configure New K2 System page 1 - Redundant K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **L30**.
3. If so designed, select **Enable Live Production mode**.
4. Select the Server redundancy option.
5. Click **Next**.

Page 2 opens.

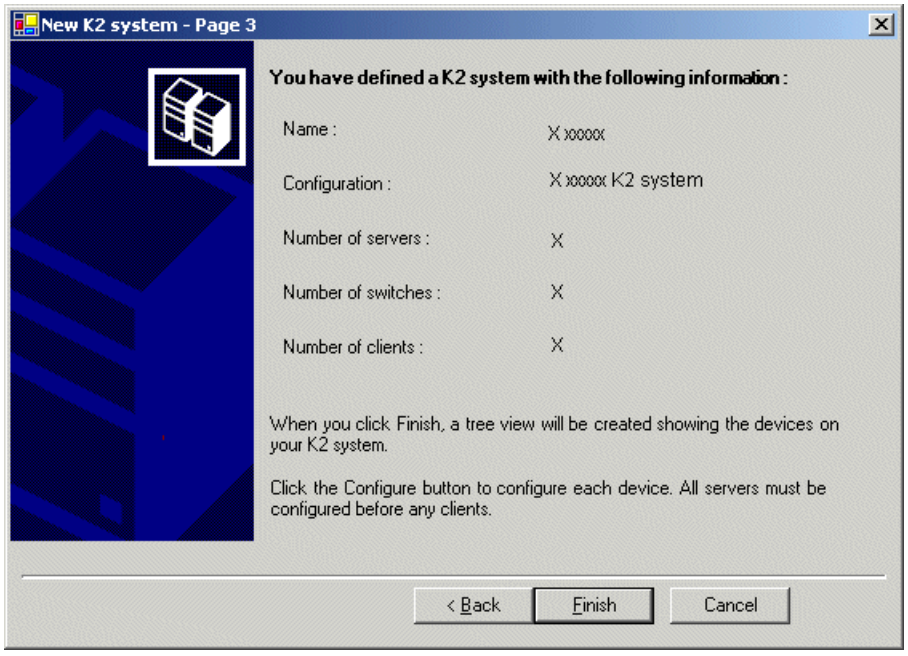
Configure New K2 System page 2 - Redundant K2 SAN



1. Move the following into the Number of devices box:
   - Two K2 Media Servers
   - Two Ethernet switches
   - K2 clients as appropriate for your system.
   - (Optional) One or more K2 Media Servers to represent each NH K2 Media Server on your system.
   - (Optional) Other devices as appropriate for your system.
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Redundant K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a 10G basic K2 SAN you should have the following:
   - One Gigabit Ethernet switch
   - One K2 Media Server
   - Optionally, one or more NH K2 Media Servers
   - The number and type of clients appropriate for your system.
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

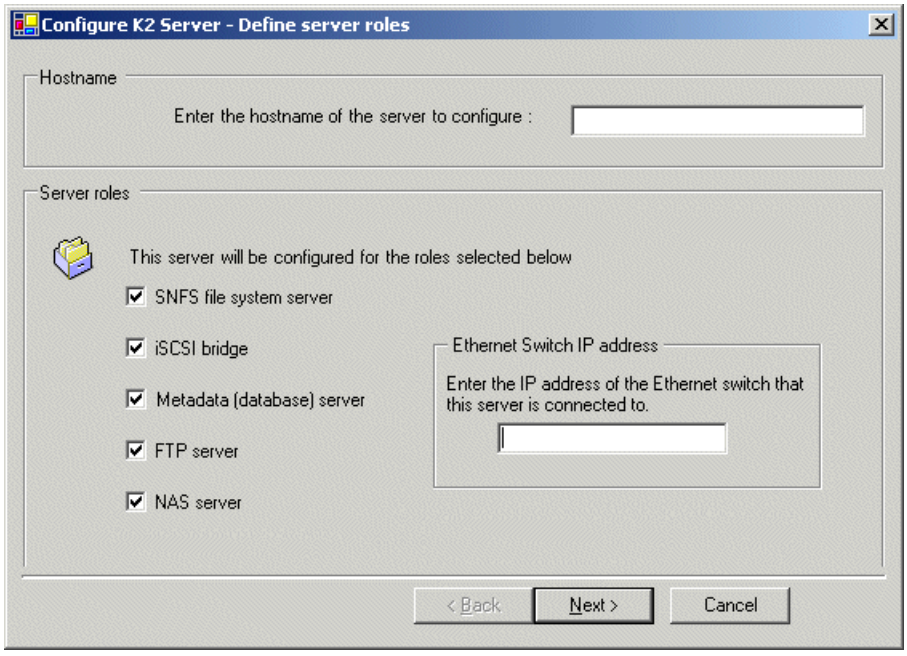
Next, configure the server.

Configuring server A - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Redundant K2 SAN server A and server B

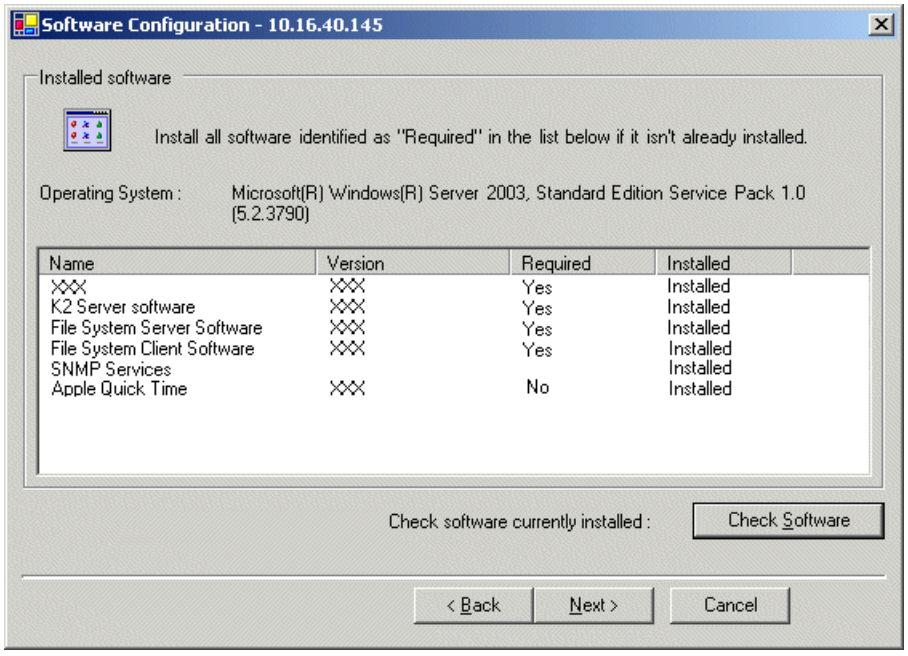


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Enter the name or IP address of the Ethernet switch, as currently configured on the switch, to which the K2 Media Server is connected.
3. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
4. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Redundant K2 SAN server A and server B

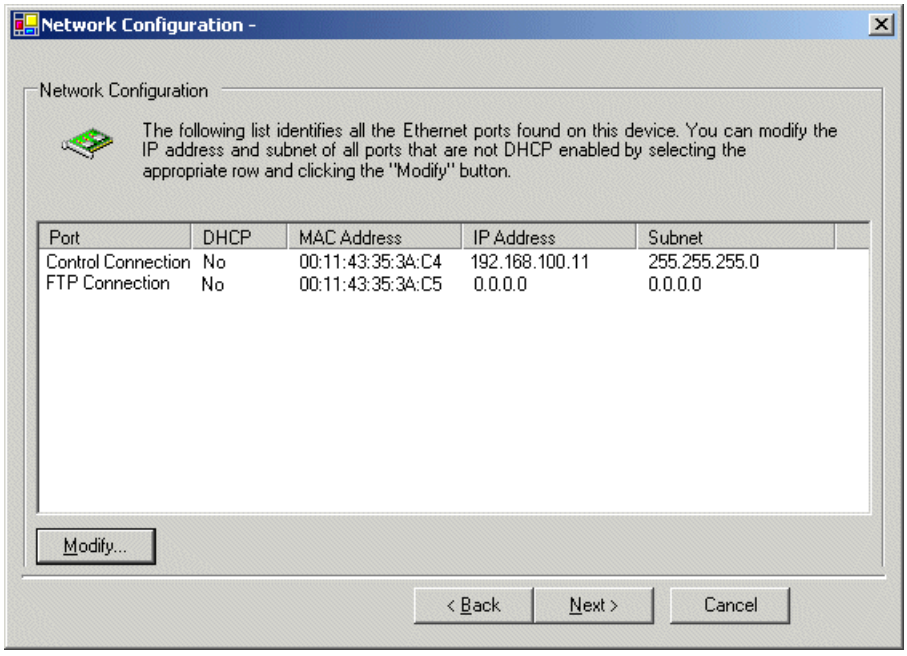


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Redundant K2 SAN server A and server B



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

   A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Redundant K2 SAN server A

1. Enter the name or IP address of the redundant K2 Media Server (server B).

   Do not yet enter anything in the File System Server #2 box.

2. Click **Launch Storage Manager**.

   Storage Utility opens.

3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected
- Power on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

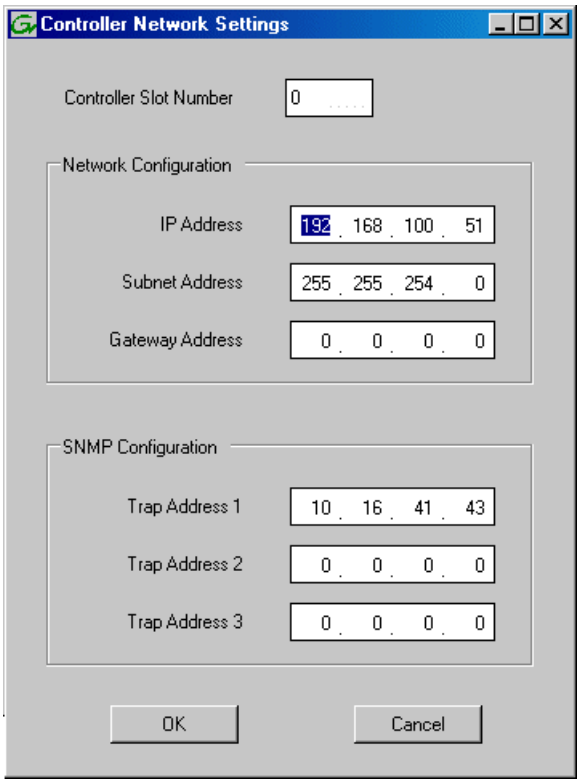
For K2 RAID, network and SNMP settings are set and stored on the RAID controller module. For the RAID chassis with two controllers, each controller has its own network settings and the RAID chassis exists as two entities on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.
6. For SNMP Configuration, enter the IP address of the NetCentral server PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.

7. For the RAID chassis with two controllers, in the Controller Slot Number field enter **1** and then press **Enter**.

   The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify.

8. Repeat the previous steps to configure controller 1.
9. Click **OK** to save settings and close.
10. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Redundant K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

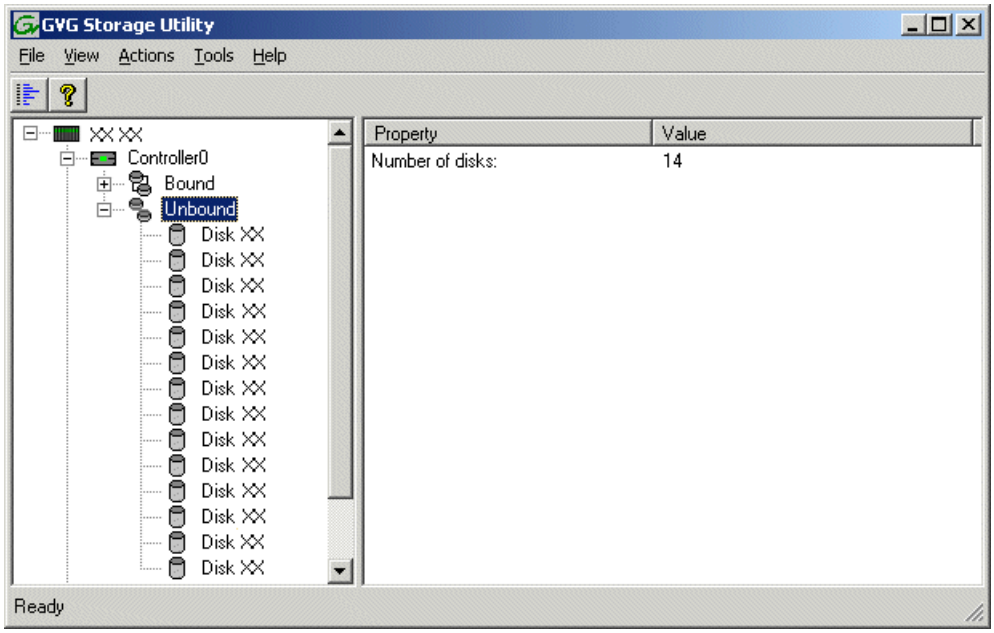
Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected
- Power on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".

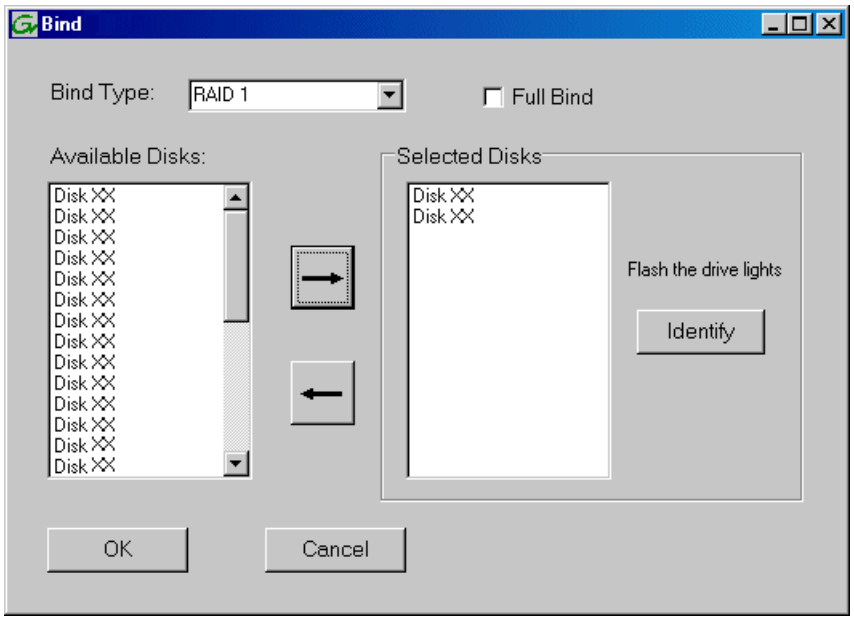


Redundant systems store file system metadata files and journal files on the primary RAID chassis. The first six disk slots in the chassis are dedicated for metadata/journal files. In the first five slots are five metadata/journal disks. The sixth slot is filled with a blank. Two disks are bound as a RAID 1 RANK for metadata storage and two disks are bound as a RAID 1 RANK for journal storage. The fifth disk is bound as a Hot Spare for the other four metadata/journal disks. The remaining six disks in the primary RAID chassis and all disks in Expansion chassis are for media storage. Media storage disks are bound as RAID 5 or RAID 6 in RANKs consisting of six disks each.

View disk properties and identify the four disks you will use for the metadata/journal RAID 1 RANKs, the one metadata/journal Hot Spare disk, any other disks that you intend to use for Hot Spares, and the remainder of the disks that are available for media storage. Make sure you select disks appropriately as you bind disks in the remainder of this procedure.

4. For systems that use RAID 1 RANKs, you must now create the separate RAID 1 storage for file system metadata files and journal files. To bind unbound disks for metadata and journal storage, do the following:
   a) Right-click the **Unbound** node for the controller, then select Bind in the context menu. (If the RAID chassis has two controllers, both controllers are represented by the single "Controller" node)

      The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



   b) Leave **Full Bind** unchecked.
   c) In the **Bind Type** drop down box, select **RAID 1**.
   d) In the Available Disks box, select two contiguous disks at the top of the list. These should be the first two disks in the primary RAID chassis. (TIP: Use 'shift-click' or 'control-click' to select disks.) This creates a RAID 1 RANK for file system metadata storage.
   e) Click the add (arrow) button to add disks to the Selected Disks list.

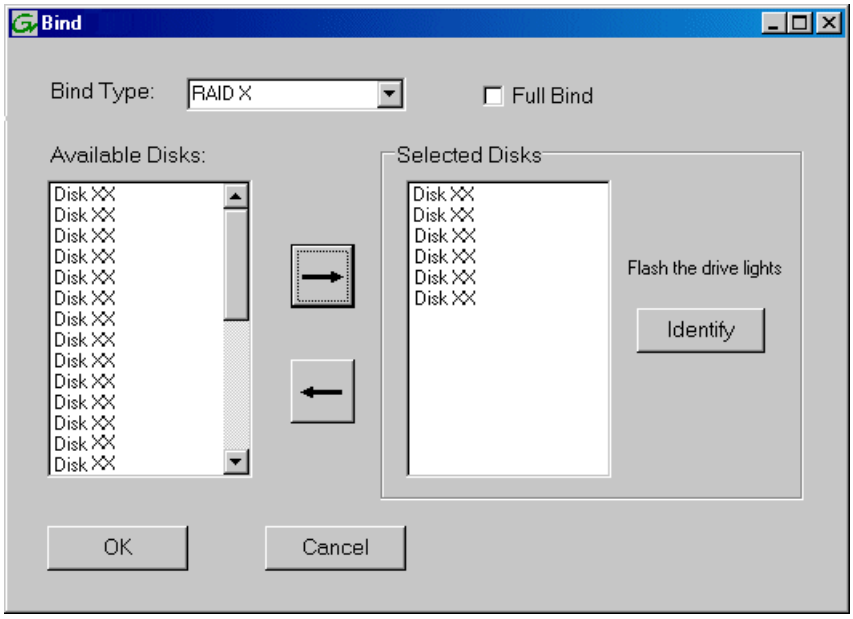
      NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

   f) Click **OK** to close the Bind dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
   g) Close the Progress Report and repeat the previous steps, selecting two more contiguous disks to create another RAID 1 RANK for journal storage. These should be the next two disks in the primary RAID chassis.
   h) Make the fifth disk in the primary RAID chassis a Hot Spare. In the **Bind Type** drop down box, select **Hot Spare**.
   i) In the Available Disks box, select the fifth disk in the primary RAID chassis.
   j) Click the add (arrow) button to add the disk to the Selected Disks list.
   k) Click **OK** to close the dialog box and begin the binding process.

5. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



6. Leave **Full Bind** unchecked.
7. In the **Bind Type** drop down box, select **RAID 5** or **RAID 6**, as specified by your system design.
8. In the Available Disks box, select six contiguous disks at the top of the list.

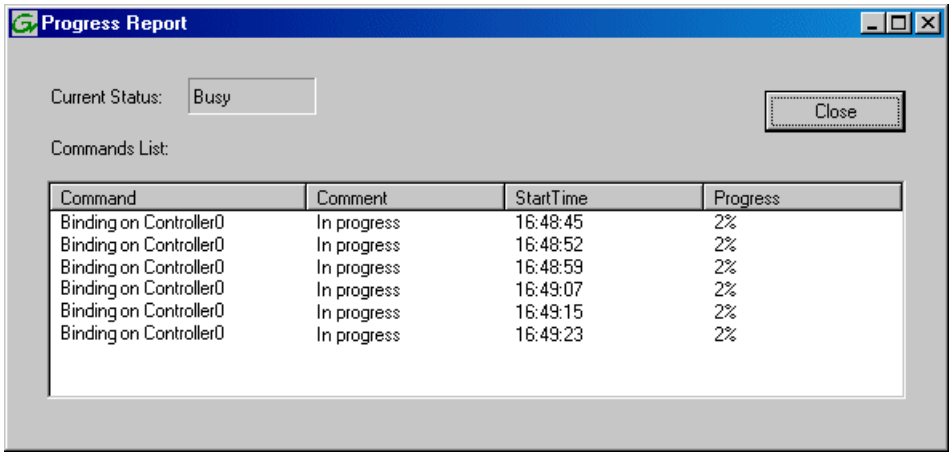
   Use ‘shift-click’ or ‘control-click’ to select disks.

9. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

10. Click **OK** to close the Bind dialog box and begin the binding process.

    The Progress Report dialog box opens, showing the status of the binding process.



11. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    For redundant storage, on the primary RAID chassis you should have two RAID 1 RANKs of two disks each, one Hot Spare Disk, and one RAID 5 or RAID 6 RANK of six disks. For each optional Expansion chassis, you would have an additional one or two RAID 5 or RAID 6 RANKs of six disks each.

12. Click **Close** in Progress Report window.
13. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

Related Topics

Identifying disks on page 321
About full/background bind on page 325
Binding Hot Spare drives on page 327

Creating a new file system - Redundant K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on
- Disks bound

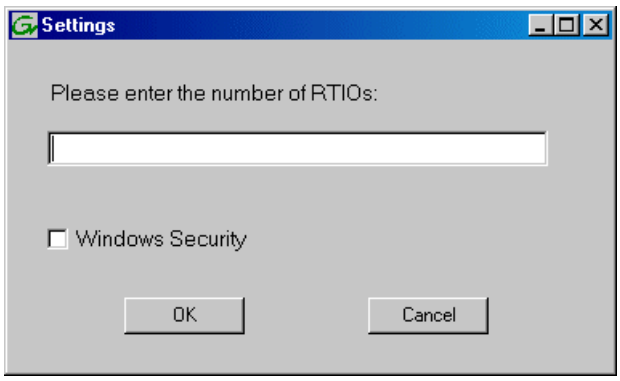
Prerequisites for the optional K2 RAID Expansion chassis are as follows:

- Fibre channel cable(s) connected

- Power on
- Disks bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility, click **Tools | Make New File System**.

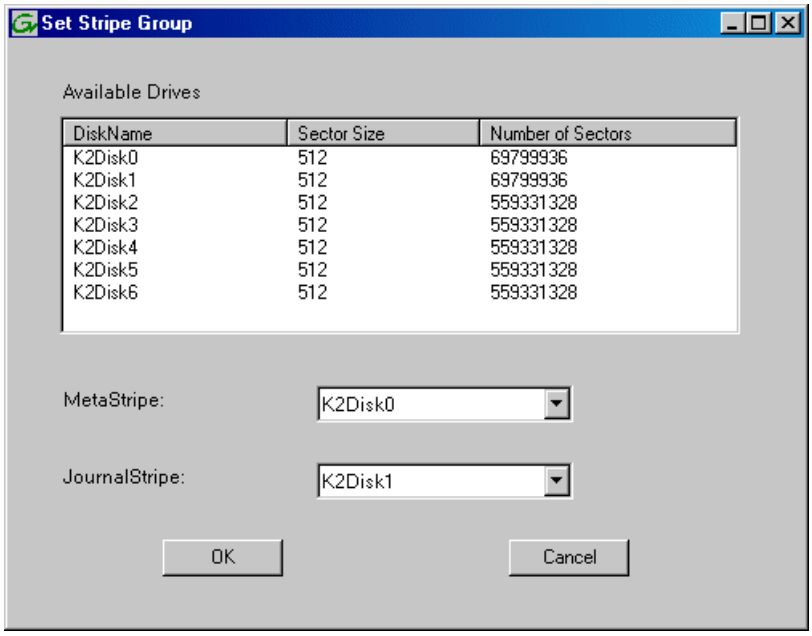
   The Setting dialog box opens.



4. For the Real Time Input/Output (RTIO) rate, enter the value specified by your system design. If you do not know this value, contact your Grass Valley representative.
5. Configure Windows Security as follows:
   - If the K2 SAN is to be accessed by only K2 clients leave Windows Security unchecked.
   - If the K2 SAN is to be accessed by Aurora Edits, refer to the *Aurora Edit Installation and Configuration Guide* for instructions.

6. Click **OK**.

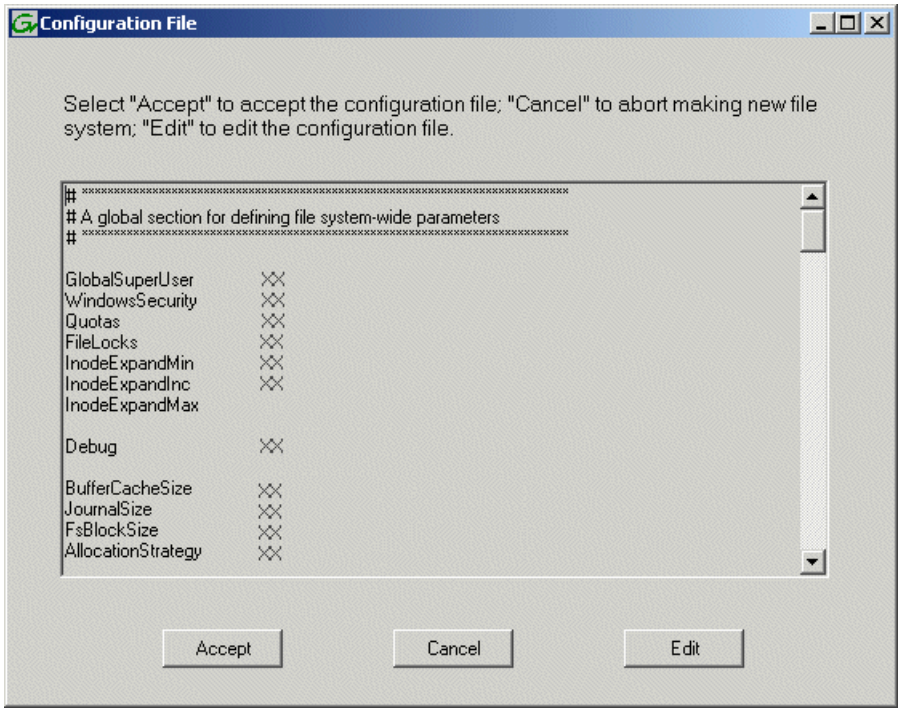
   The Set Stripe Group dialog box opens.



7. If you have RAID 1 RANKS, assign a RAID 1 RANK as a metadata stripe and another RAID 1 RANK as a journal stripe. You can distinguish RAID 1 RANKs from media RANKs by the value in the Number of Sectors column.

8. Click **OK**.

   The Configuration File dialog box opens.



   The configuration file for the media file system is displayed.

9. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

10. Click **Accept**.

    A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

    A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

11. Close the Storage Utility.

    NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

Next, continue with configuring the server using the K2Config application.

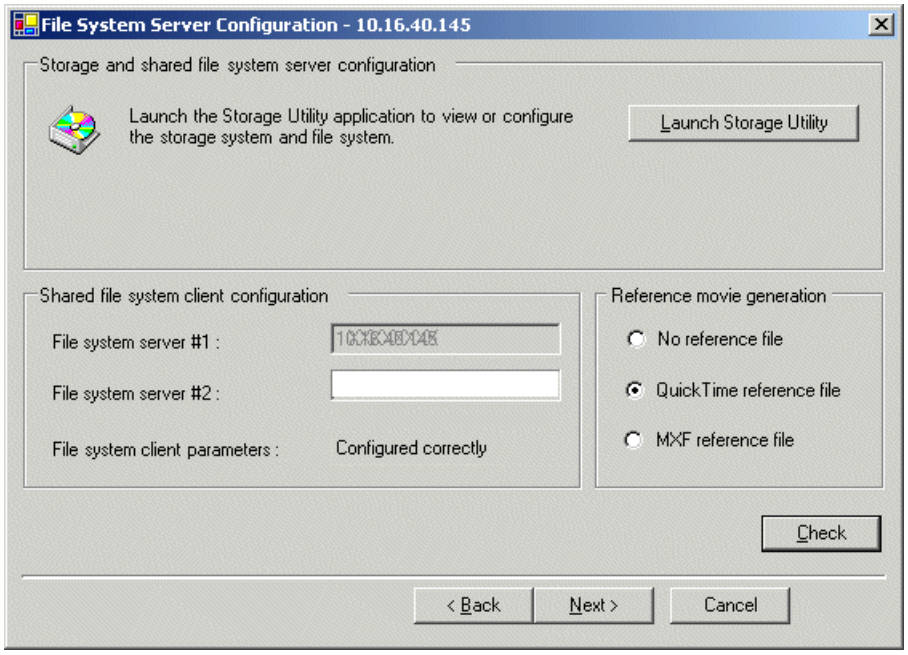
Configuring server A - Part 2

Configure File System Server Configuration page - Redundant K2 SAN server A

Prerequisites for connected K2 RAID storage:

- Network and SNMP settings configured
- Disks bound

- New file system made



This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page.

1. In Storage Utility open the server's File System Server Configuration page, if the page is not already open.
2. If you have not already done so, enter the name or IP address of the redundant K2 Media Server (server B).
3. If desired, configure reference file generation.
4. Click **Check**.
5. When the wizard reports that the configuration is correct, click **Next**.

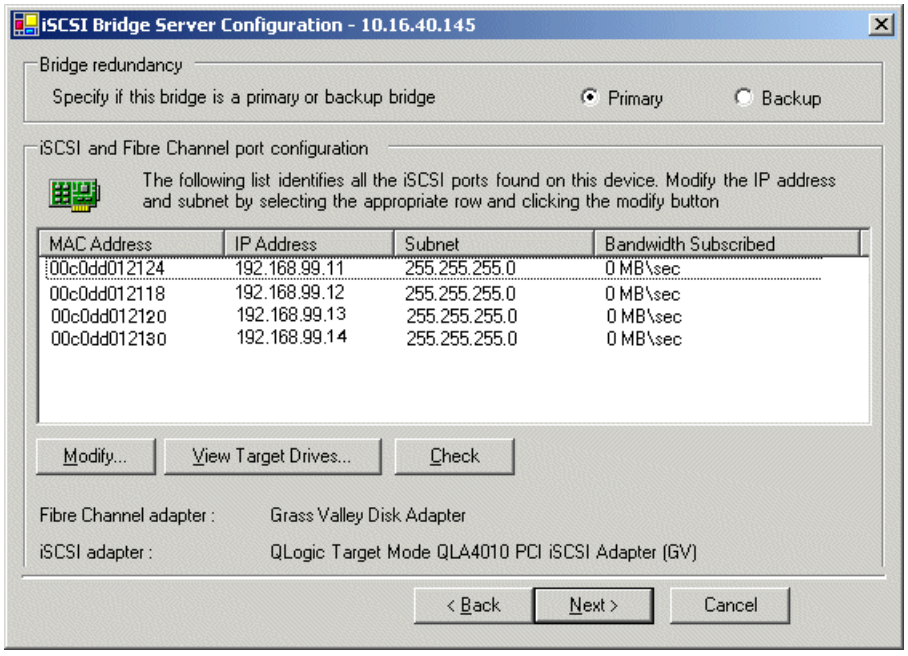
   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Related Topics

Configuring reference file type on a K2 SAN system on page 280

Configure iSCSI Bridge Server Configuration page - Redundant K2 SAN server A



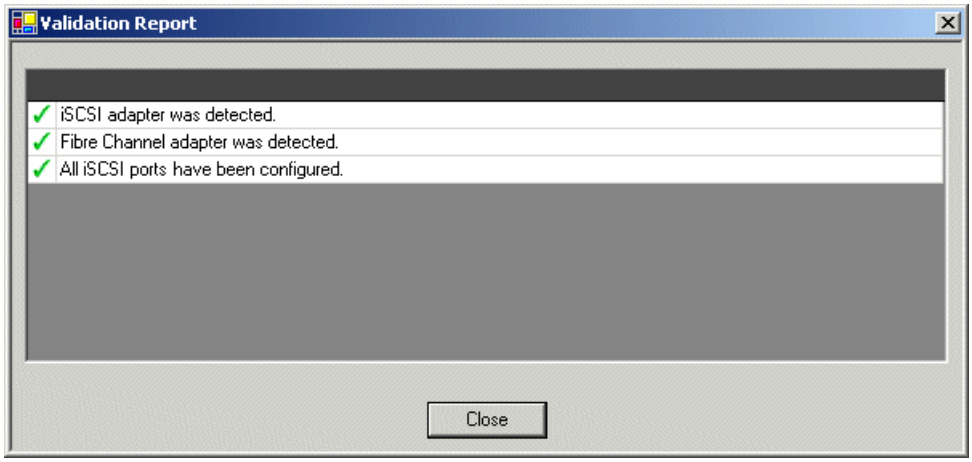
This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

1. Select **Primary**.
2. Select an iSCSI adapter and do the following:
   a) Click **Modify**.

      A network configuration dialog box opens.

   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
3. Repeat the previous step for the other iSCSI adapters.

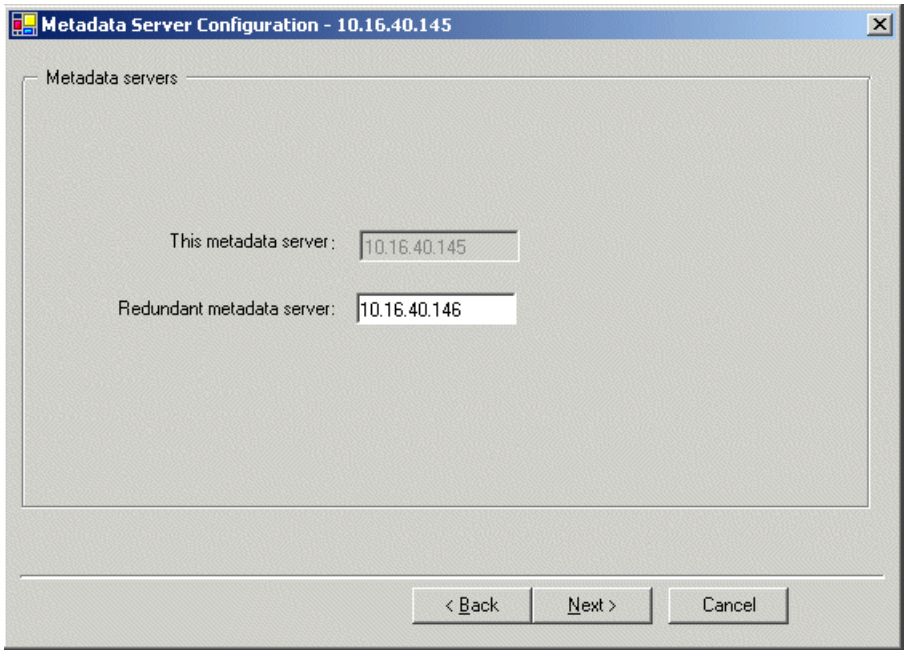
4. Click **Check**.
   The Validation Report opens.



5. Confirm that the iSCSI configuration is successful.
6. Close the Validation Report.
7. Click **Next**.

The Database Server Configuration page opens.

Configure Database Server Configuration page - Redundant K2 SAN server A

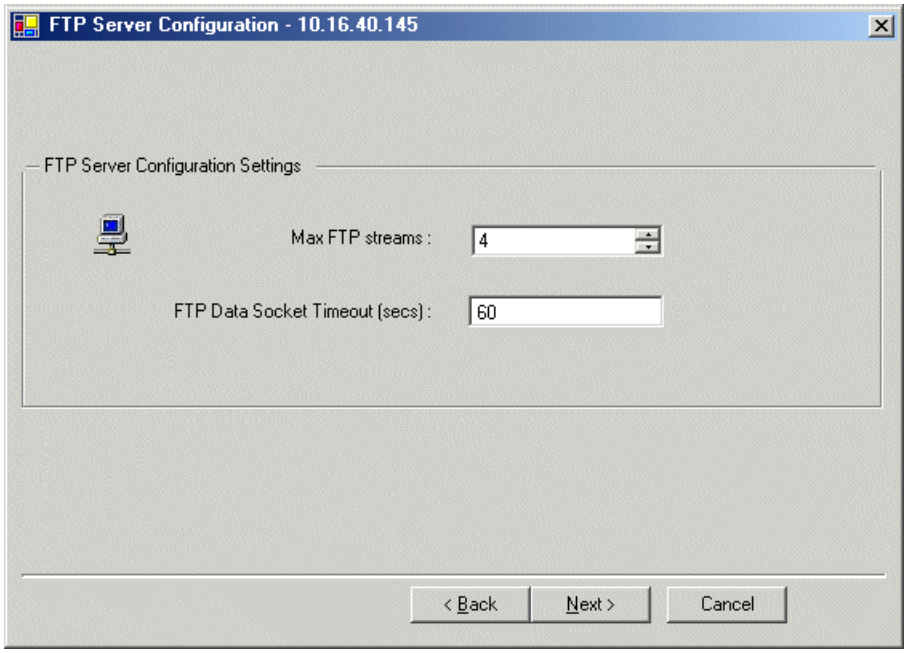


1. Enter the name or IP address of K2 Media server B. This is the redundant partner of the server you are now configuring.

2. Click **Next**.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Redundant K2 SAN server A



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, configure the redundant server.

Configuring server B

Prerequisites:

- Server A is configured

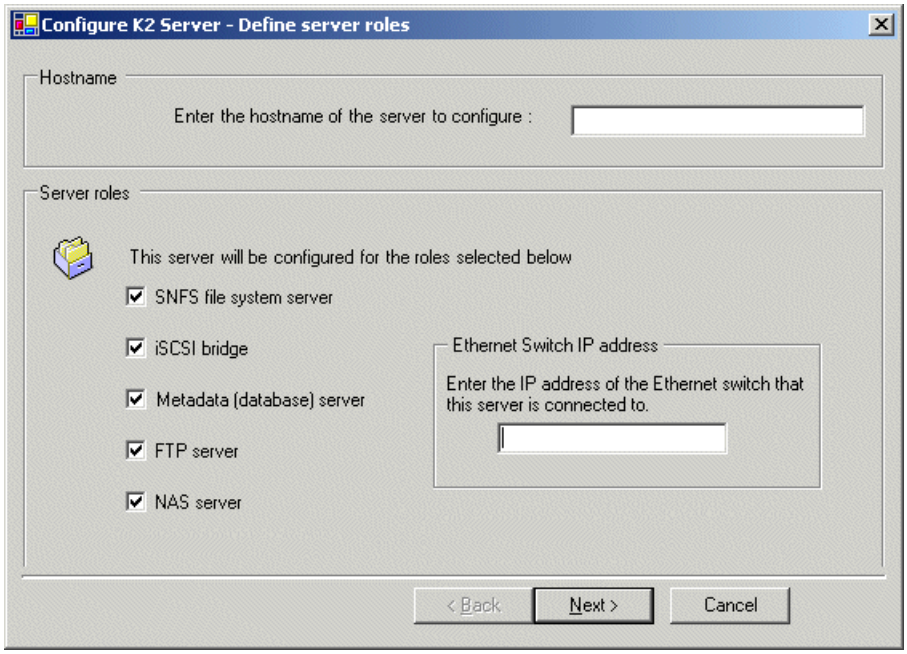
- The restart of server A after it is configured is complete

After you have configured the first K2 Media Server (server A) you next configure the redundant K2 Media Serer (server B).

1. Verify that server A has restarted by opening the MS-DOS command prompt and use the “ping” command.
2. In the K2 System Configuration application tree view, select the K2 Media Server you are configuring as server B.
3. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - Redundant K2 SAN server A and server B

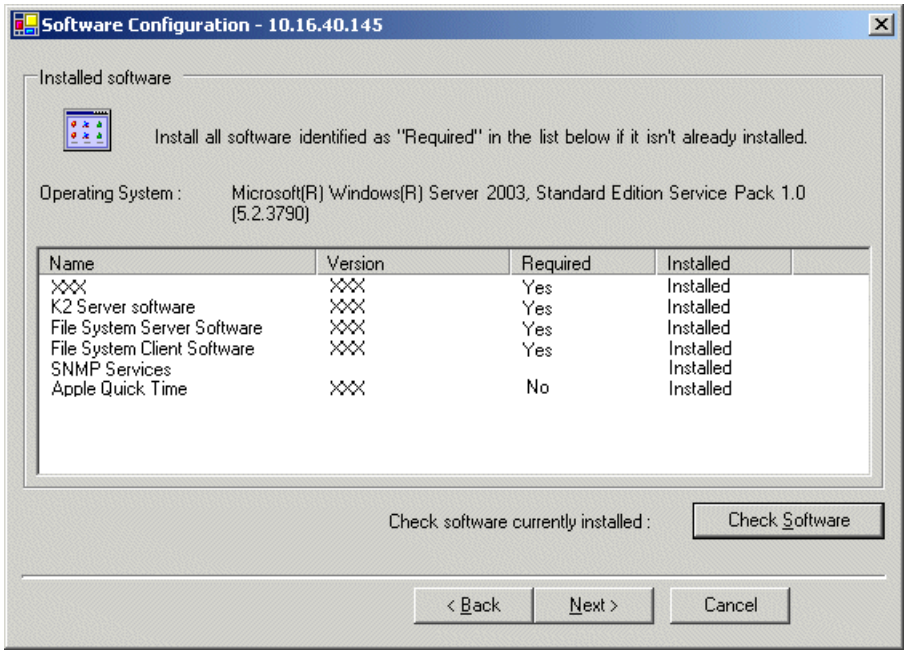


1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Enter the name or IP address of the Ethernet switch, as currently configured on the switch, to which the K2 Media Server is connected.
3. Select all roles, except as follows:

   If the K2 SAN has one or more optional NH servers, then FTP traffic should go to the NH server, not the K2 Media Server you are now configuring. In this case, do not select the FTP server role or the NAS server role
4. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - Redundant K2 SAN server A and server B

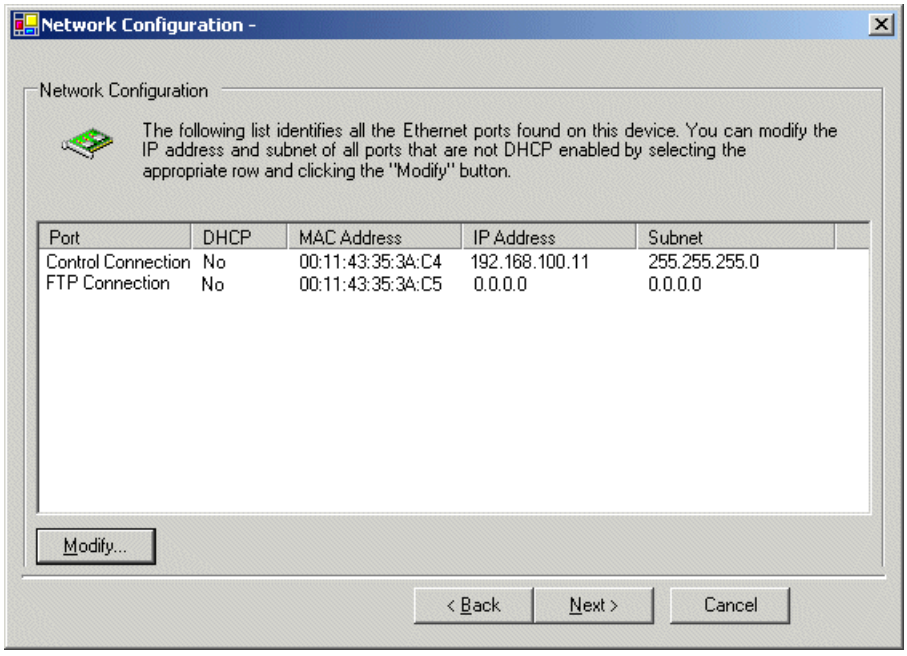


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - Redundant K2 SAN server A and server B



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

NOTE: This page does not configure the iSCSI interface (media network) ports.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. If the server has the role of FTP server, verify that the other port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

      A network configuration dialog box opens.

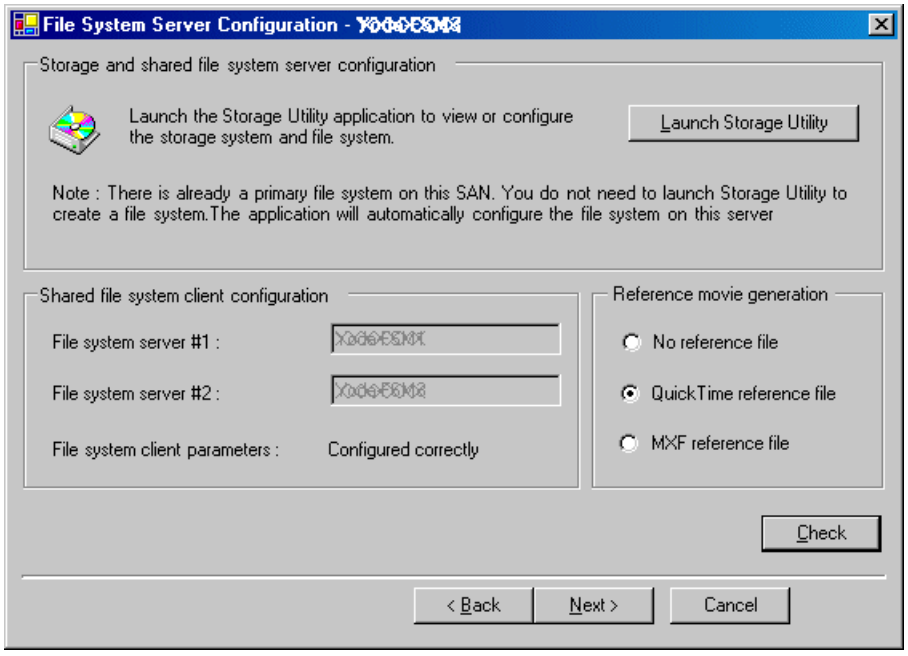
   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

   For systems with an optional NH (FTP) server, the server you are now configuring does not take the role of FTP server, so configuring the second port here for the FTP/streaming network is not required.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - Redundant K2 SAN server B



This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page. It is not necessary to bind RANKs or create a file system, since this task was completed when you configured the previous K2 Media Server.

1. If desired, configure reference file generation.
2. Click **Check**.
3. Confirm a "… file copied…" message.
4. When the wizard reports that the configuration is correct, click **Next**.
5. Confirm messages about copying the file system configuration file to the other server.

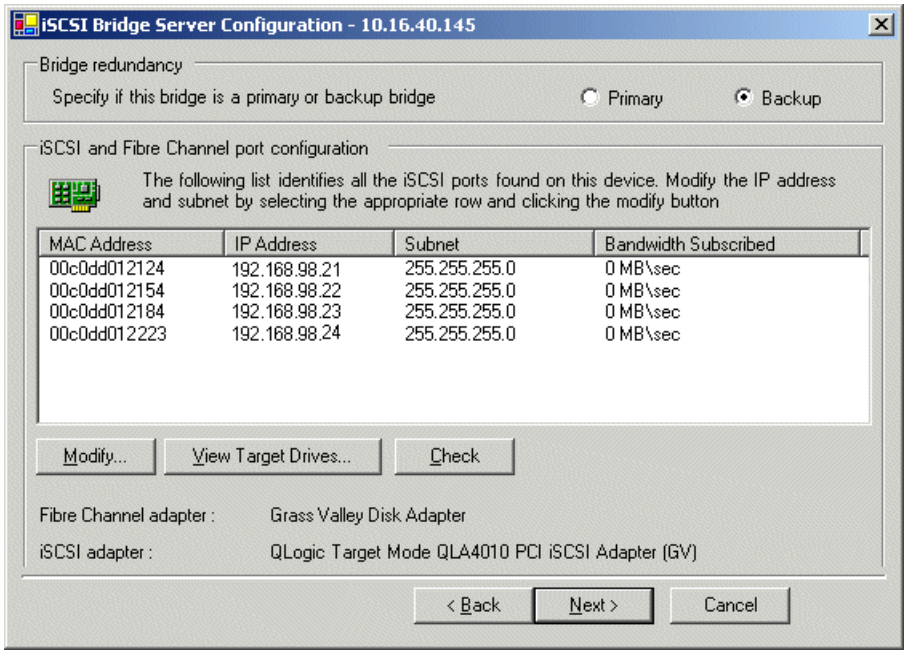
   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Related Topics

Configuring reference file type on a K2 SAN system on page 280

Configure iSCSI Bridge Server Configuration page - Redundant K2 SAN server B



This page manages the components that bridge between iSCSI (the GigE media network) and the Fibre Channel connection to the RAID storage. You configure network settings on the iSCSI adapters and the page validates that the Fibre Channel adapter is in place and that the media RANKs are visible as iSCSI targets.

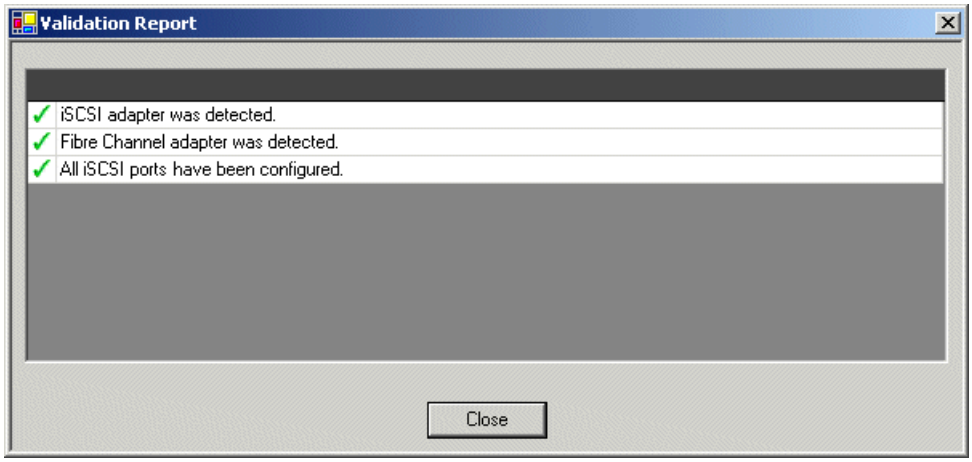
NOTE: The iSCSI adapters on this server must be on a different subnet than those on its redundant server partner.

1. Select **Backup**.
2. Select an iSCSI adapter and do the following:
   a) Click **Modify**.

      A network configuration dialog box opens.

   b) Verify or enter the media network IP address and the subnet mask.
   c) Click **Apply**.
   d) Click **View Target Drives**.
   e) Verify that all drives are shown in the **Drives exposed as iSCSI targets** field.
3. Repeat the previous step for the other iSCSI adapters.

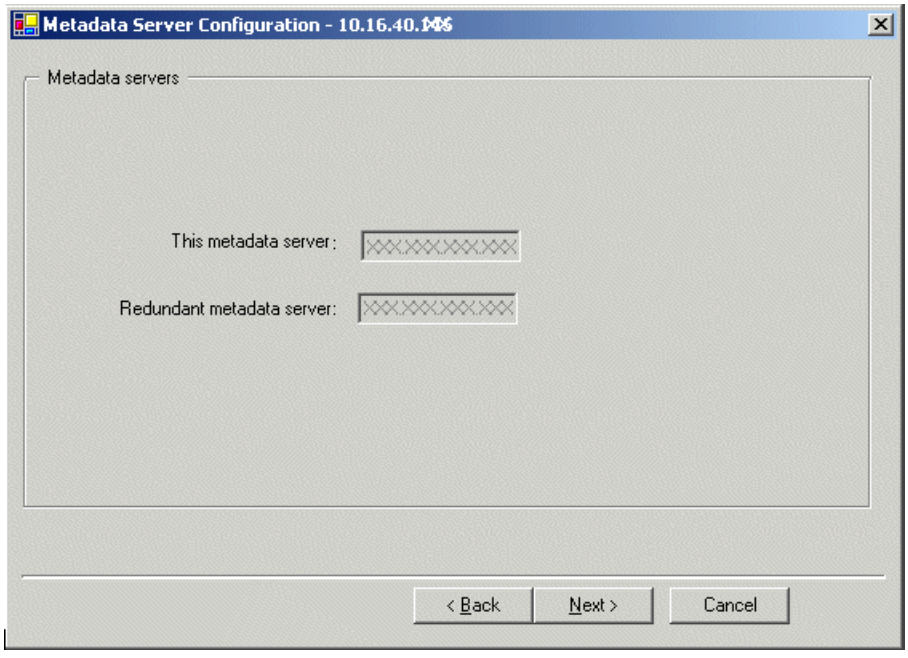
4. Click **Check**.
   The Validation Report opens.



5. Confirm that the iSCSI configuration is successful.
6. Close the Validation Report.
7. Click **Next**.

The Database Server Configuration page opens.

Configure Database Server Configuration page - Redundant K2 SAN server B

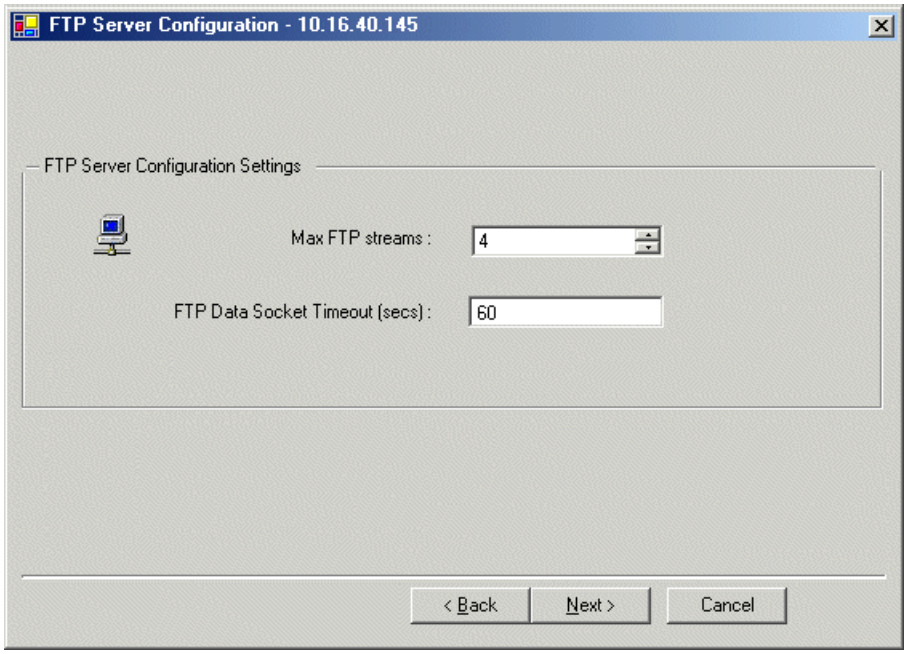


Click **Next**.

You do not need to enter or configure anything on this page.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - K2 SAN server B



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, check the V: drive

Check the V: drive

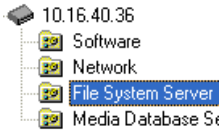
Prerequisites:

- The K2 Media Server is configured

- The restart of the K2 Media Server after it is configured is complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the "ping" command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

Proceed as follows:

- If you have NH servers, configure them next.
- If you do not have NH servers, configure K2 clients and/or other iSCSI clients on the K2 SAN next.

Configuring optional NH servers

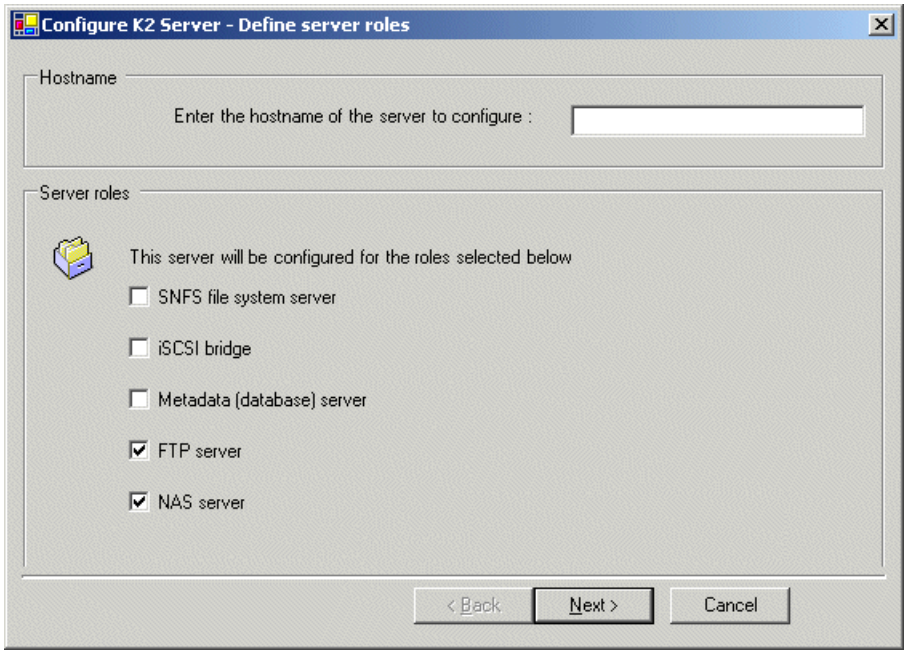
If you have one or more optional NH K2 Media Servers, you next configure those servers. This section applies to both NH1 (1 Gig FTP) servers and NH10GE (10 Gig FTP) servers.

NOTE: Multiple NH servers on a K2 SAN must be of the same type, either all NH1 or all NH10GE.

1. In the K2Config application tree view, select the K2 Media Server you are configuring.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

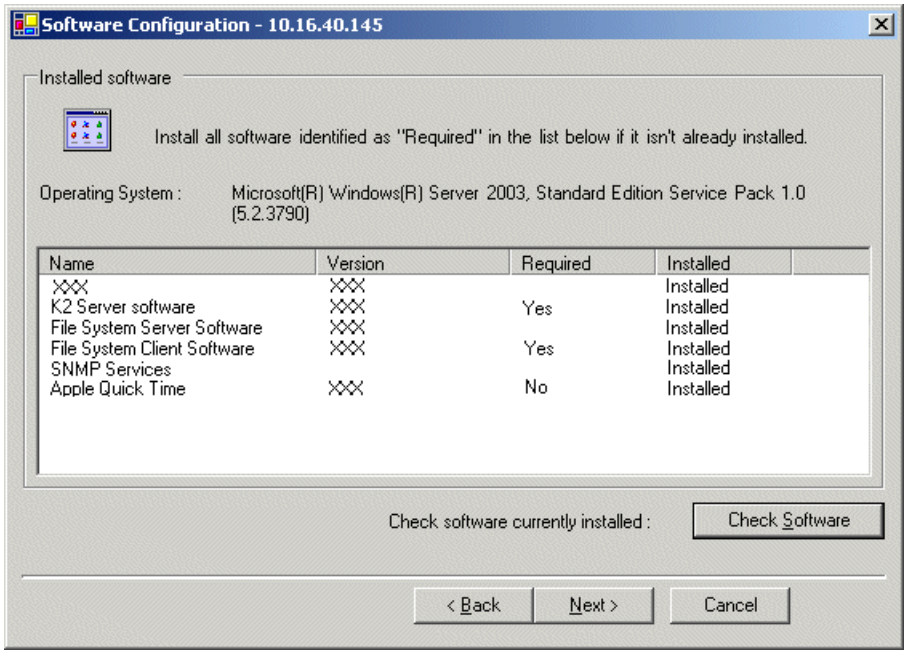
Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.
2. Select **FTP server** and **NAS server**.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

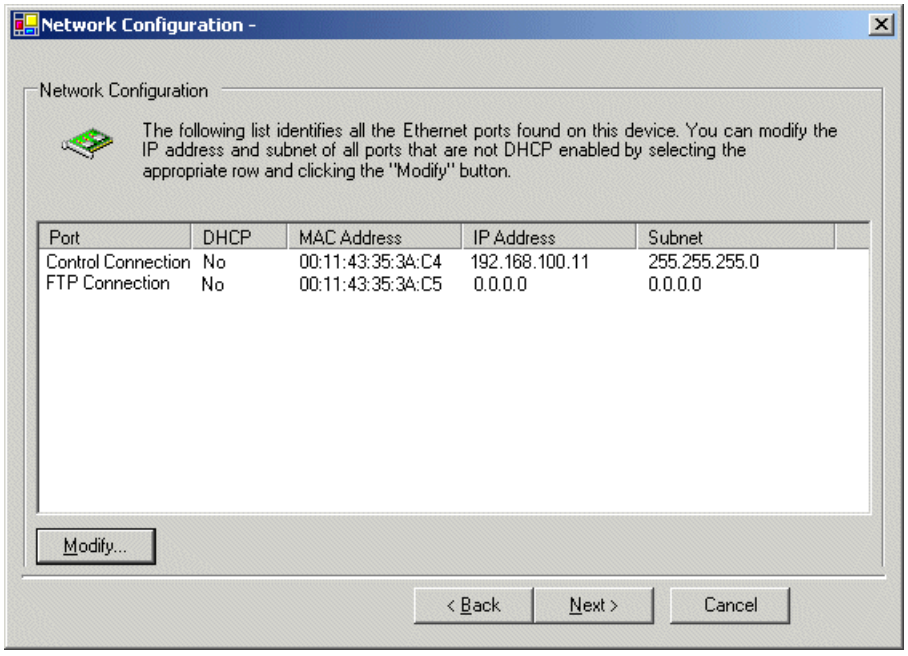


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

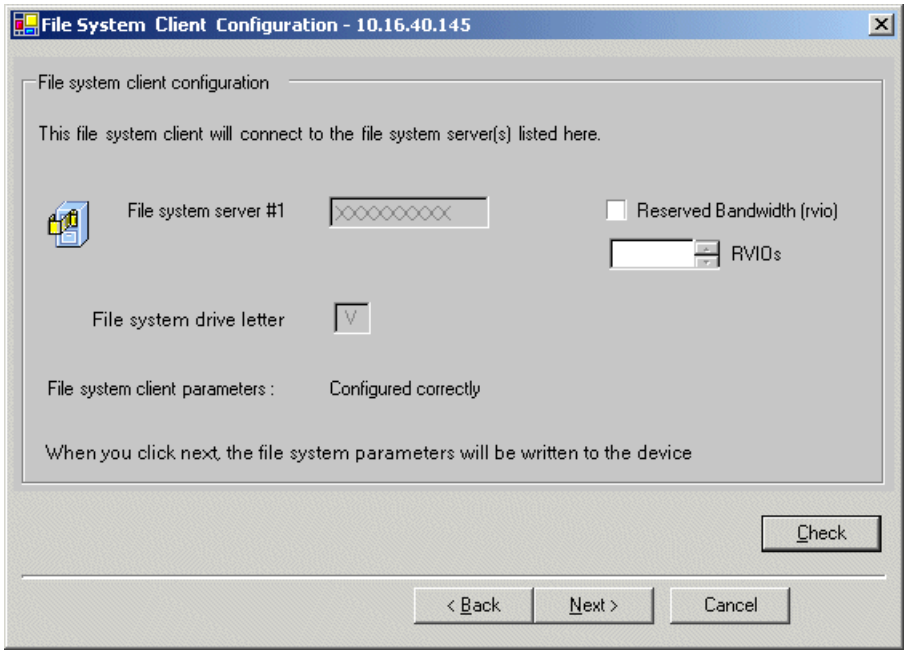
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Client Configuration page - NH server



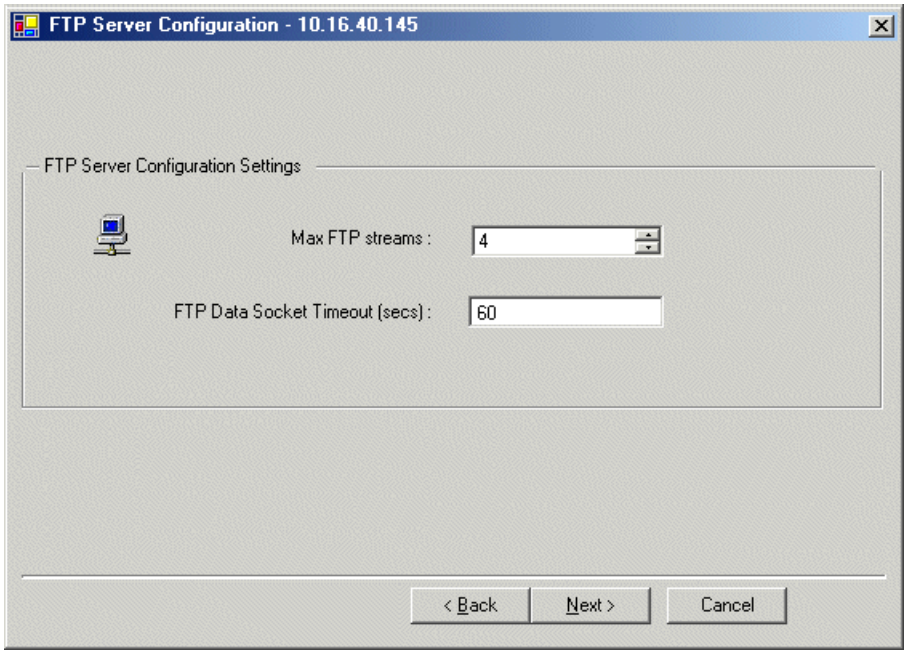
This system does not function as a file system server. It does function as a file system client, which is validated from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - Redundant K2 SAN NH server



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

If you have other NH servers, configure them similarly. Then check the V: drive on each of your NH servers.

Check the V: drive

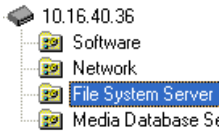
Prerequisites:

- The K2 Media Server is configured
- The restart of the K2 Media Server after it is configured is complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the “ping” command.

2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

Next, configure K2 clients and/or other iSCSI clients on the K2 SAN.

Configuring the basic nearline K2 SAN

Work through the topics in this section sequentially to configure a non-redundant nearline (Tier 3) K2 SAN.

Prerequisites for initial configuration - Basic nearline K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software installed
- Control network IP address assigned
- Network communication over the control network with all other K2 devices
- Power on

Ethernet switch

- Ethernet cables connected
- Control network IP address assigned
- VLANs set up
- Trunks set up
- Power on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable connected
- Software installed, as from the factory, including QuickTime 7
- Control network IP address assigned
- Power on for all servers

K2 RAID chassis

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected

- Power on

K2 RAID Expansion chassis (optional)

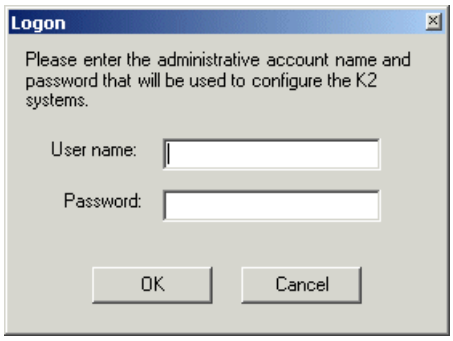
- Fibre channel cable(s) connected
- Power on

Defining a new K2 SAN

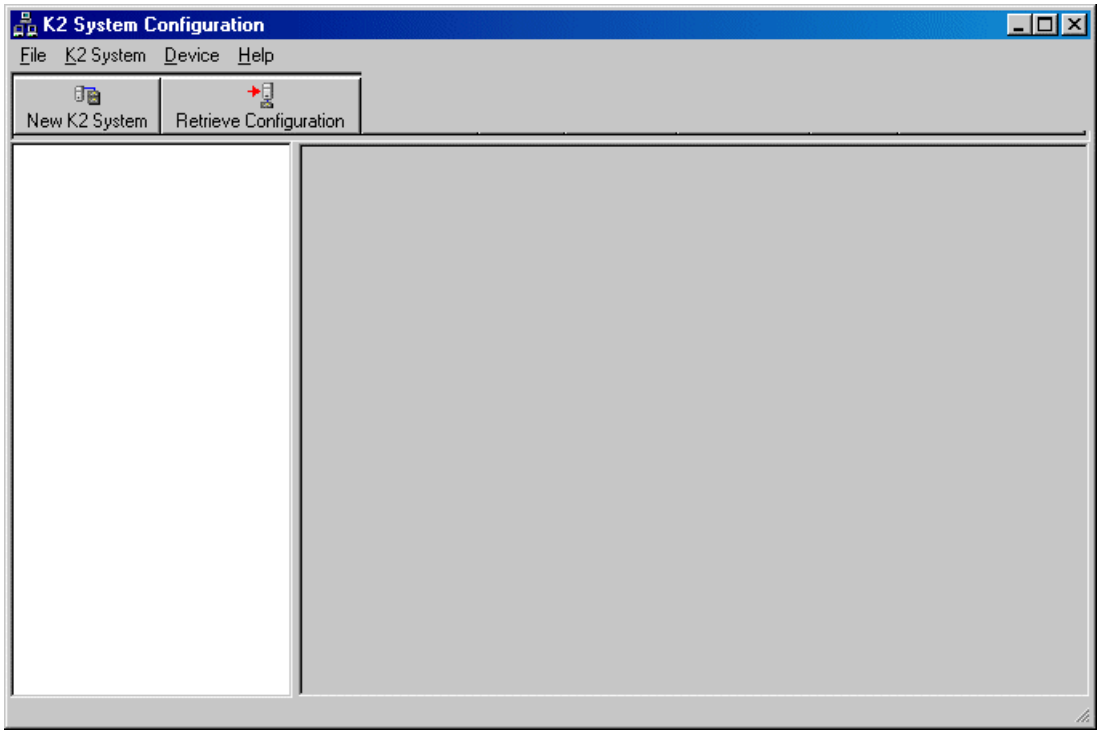
If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

1. On the control point PC, open the K2Config application.

   A login dialog box opens.



2. Log in to the K2Config application with the Windows administrator account.
   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

Related Topics

About application security on the K2 SAN on page 272

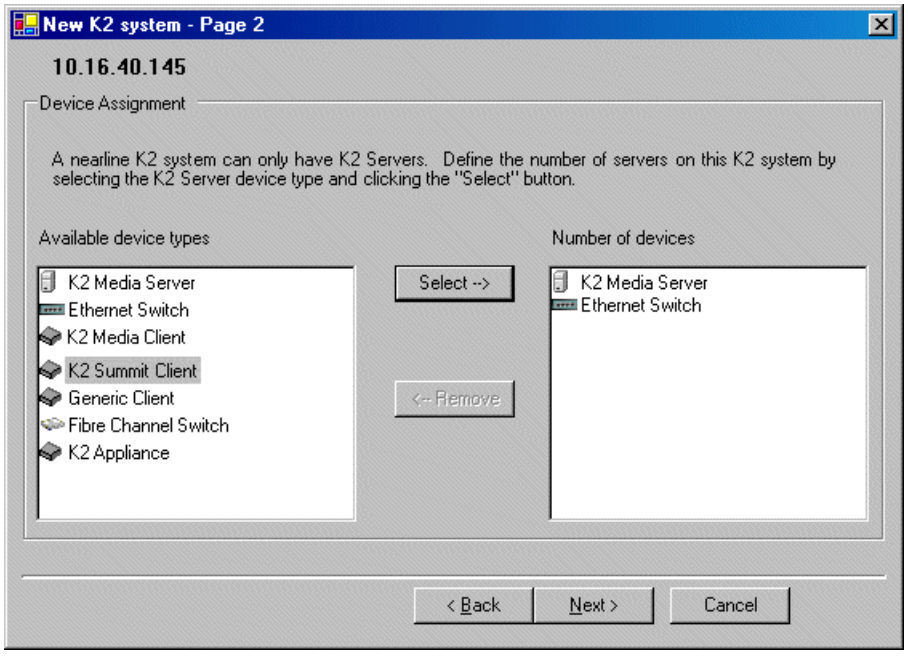
Configure New K2 System page 1 - Nearline K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **Nearline**.

   The Server redundancy option is not selected and is disabled. This option applies to media database redundancy. Since the Nearline system has no media database, this setting is correct for both redundant and non-redundant Nearline systems.
3. Click **Next**.

Page 2 opens.

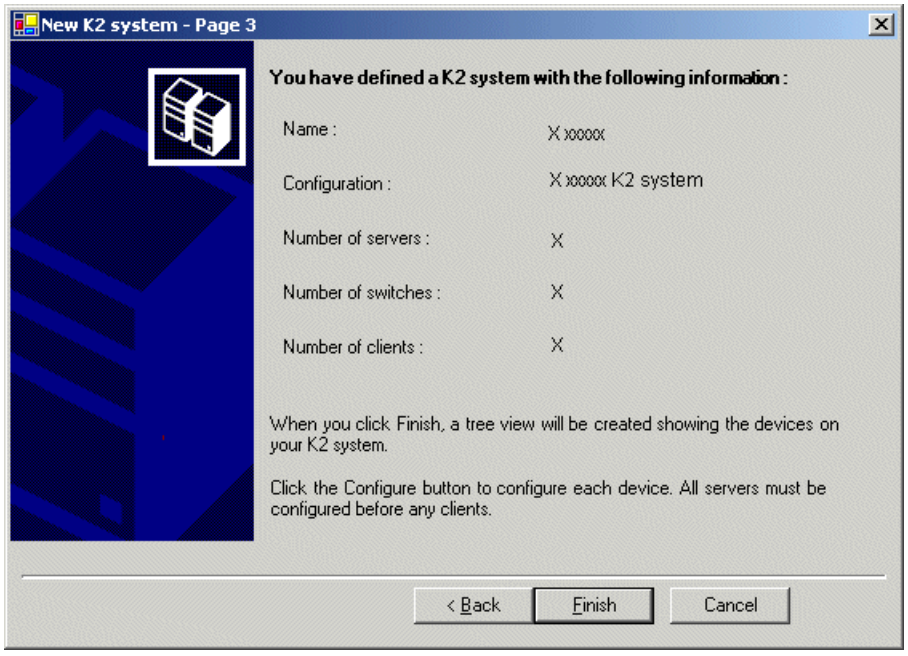
Configure New K2 System page 2 - Nearline K2 SAN



1. Move the following into the Number of devices box:
   - One K2 Media Server
   - One Ethernet switch
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Nearline K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a 10G redundant nearline K2 SAN you should have the following:
   - Two Gigabit Ethernet switches
   - Two K2 Media Servers
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

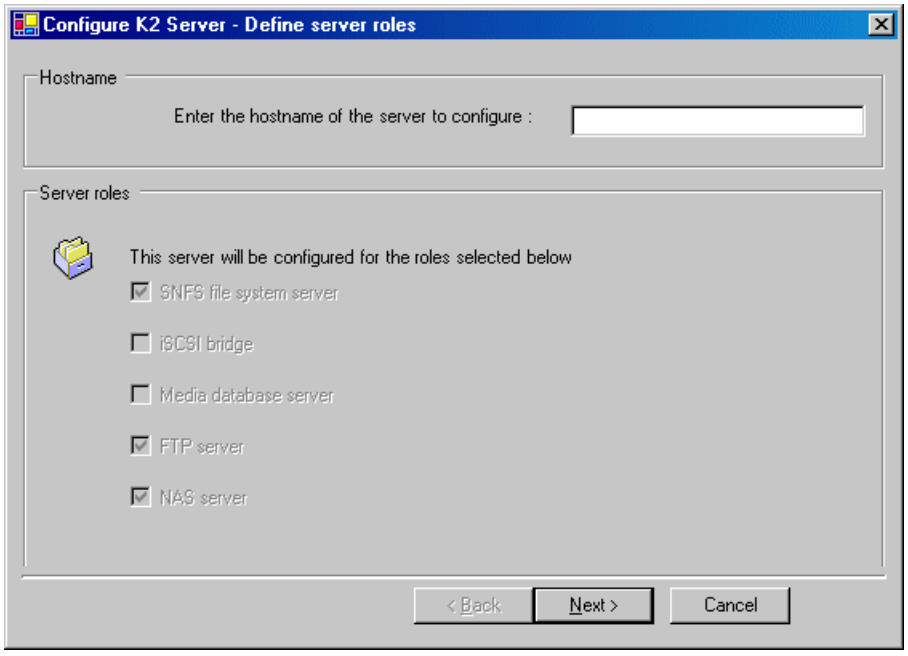
Next, configure the server.

Configuring NH server - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
   For the basic nearline K2 SAN, this is the only NH server.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

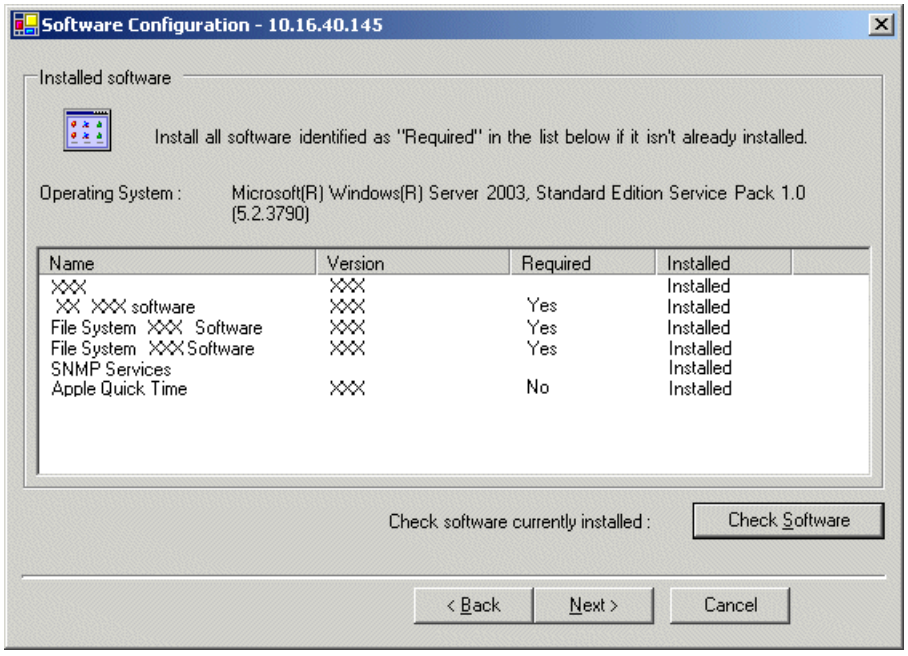
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server

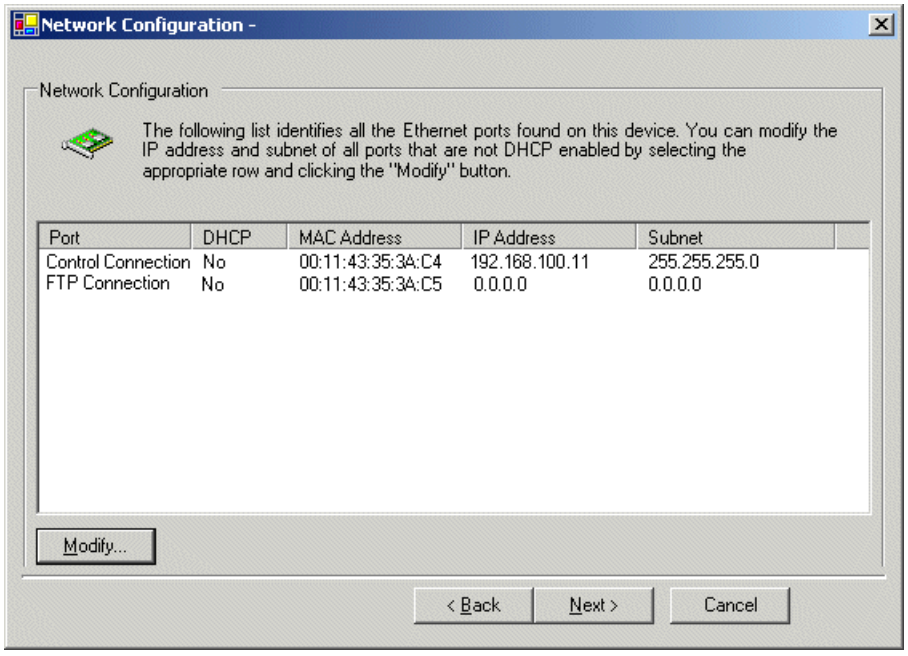


This page checks for the software required to support the roles you selected on the previous page.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

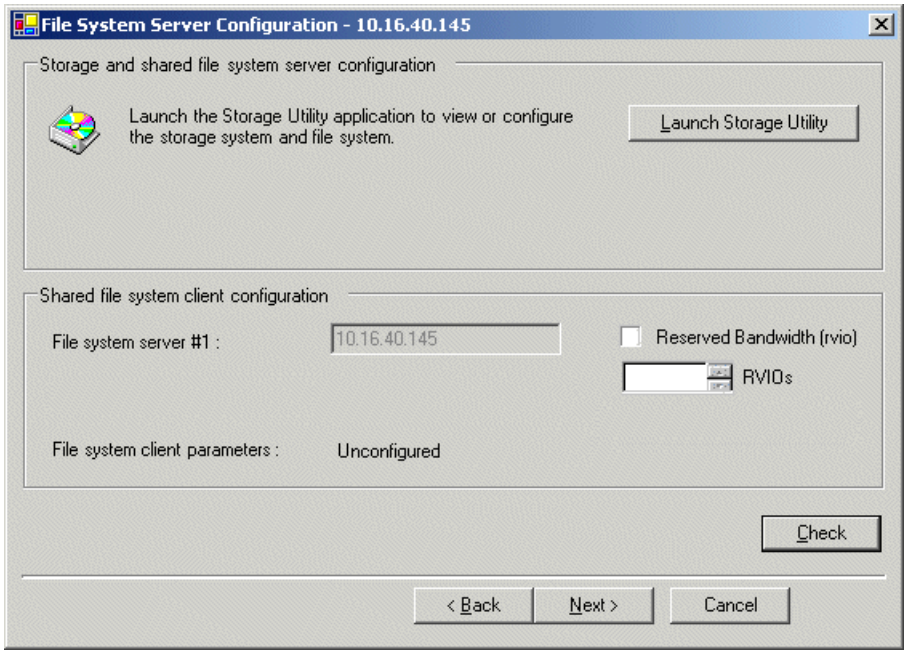
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Launch Storage Manager**.

   Storage Utility opens.
3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings - Basic

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected

- Power on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

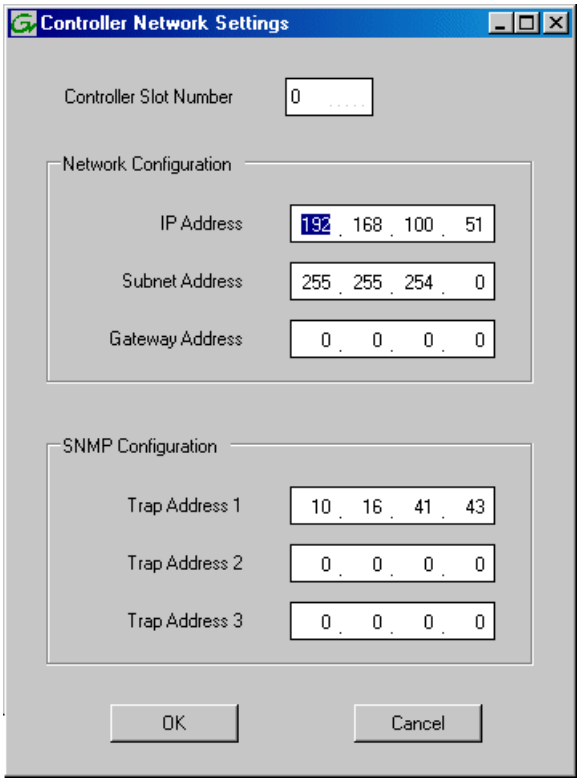
- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module, so the combined RAID storage devices, including the optional Expansion chassis, exist as a single entity on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.
6. For SNMP Configuration, enter the IP address of the NetCentral server PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.
7. Click **OK** to save settings and close.
8. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Nearline K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

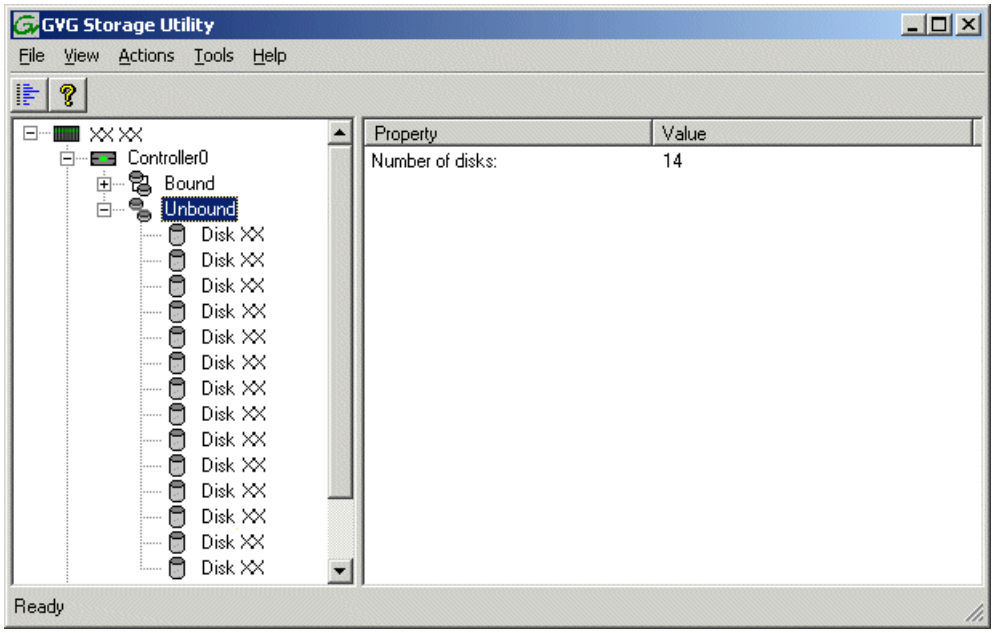
Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected
- Power on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



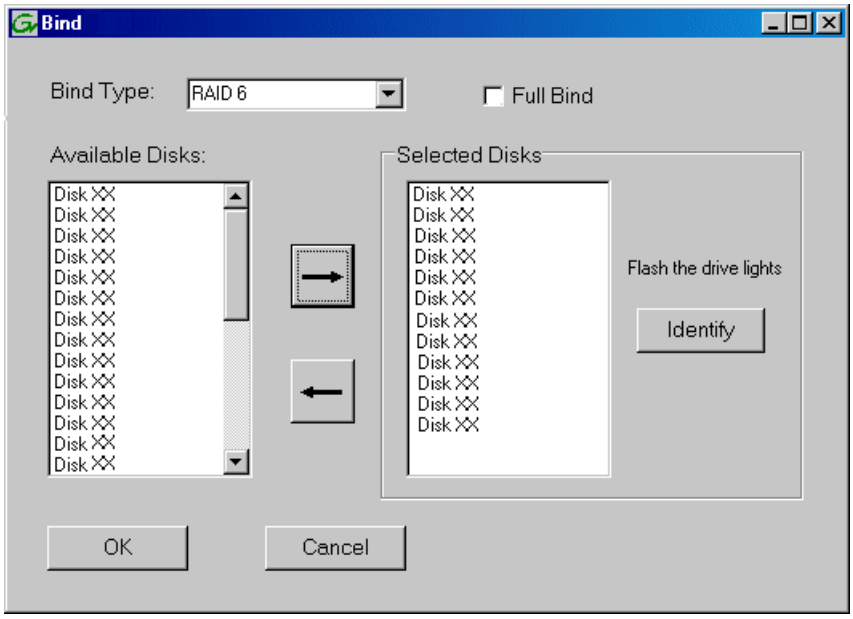
Nearline systems store media files across both the primary RAID chassis and the optional Expansion chassis. In addition, file system metadata files and journal files are mixed in with the media files.

The RAID configuration is the same on all chassis. Each chassis contains disks, which are bound as RAID 6 in a RANK of twelve disks. One twelve disk RANK fills one chassis.

4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 6**.
7. In the Available Disks box, select twelve contiguous disks at the top of the list.

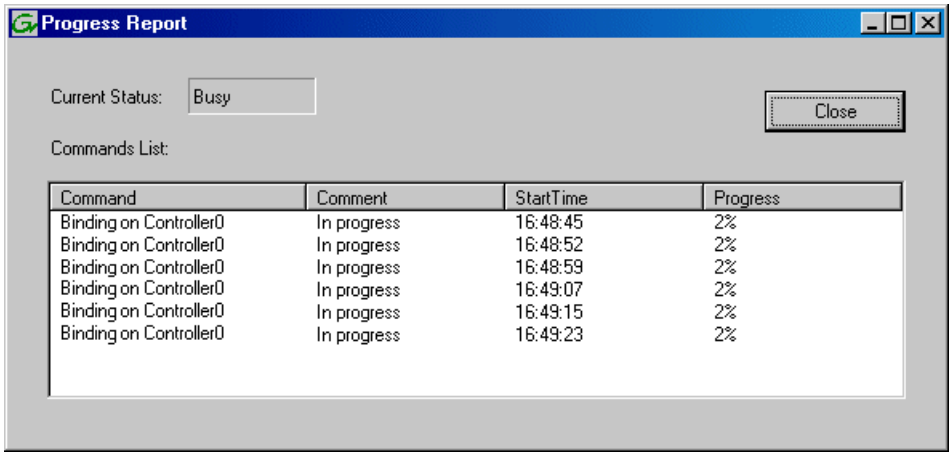
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    The disks in the primary RAID chassis and in optional Expansion chassis should be bound as RAID 6 RANKs, with twelve disks to a RANK.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

Related Topics

Identifying disks on page 321
About full/background bind on page 325
Binding Hot Spare drives on page 327

Creating a new file system - Nearline K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

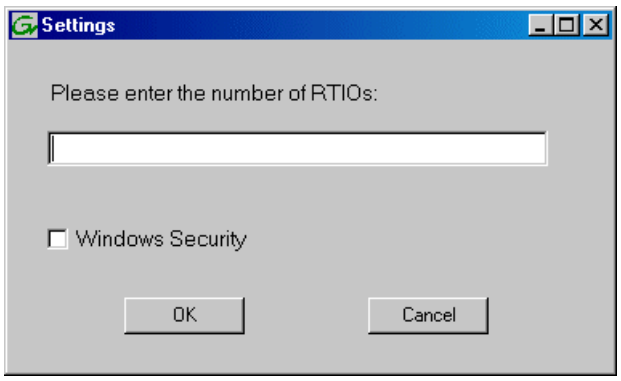
- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on
- Disks bound

Prerequisites for the optional K2 RAID Expansion chassis are as follows:

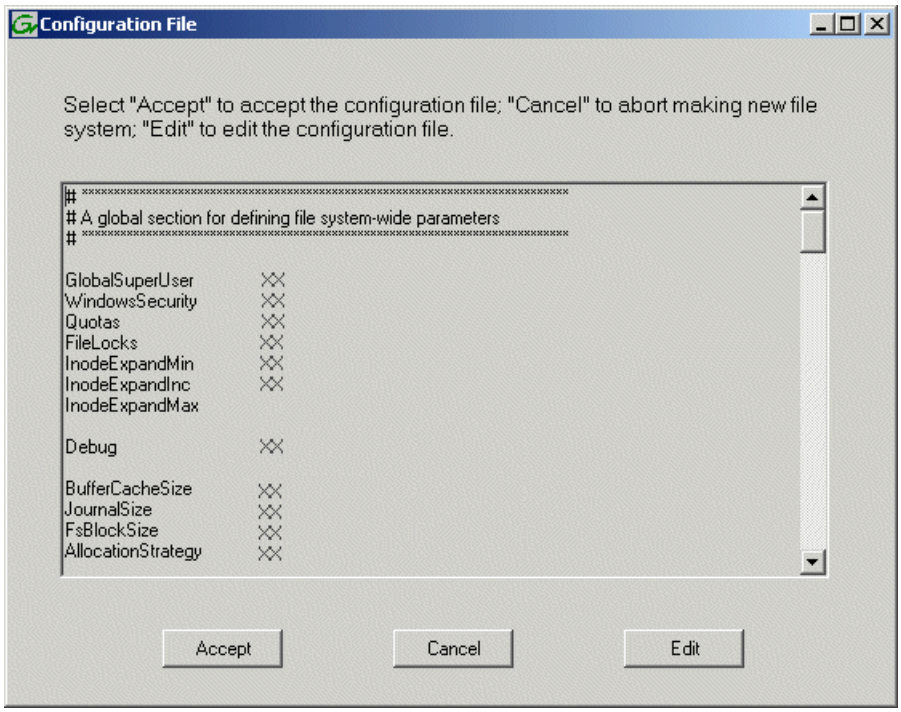
- Fibre channel cable(s) connected
- Power on

- Disks bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For a Nearline system, enter zero as the Real Time Input/Output (RTIO) rate.
5. Leave Windows Security unchecked.
6. Click **OK**.
   The Configuration File dialog box opens.



The configuration file for the media file system is displayed.

7. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

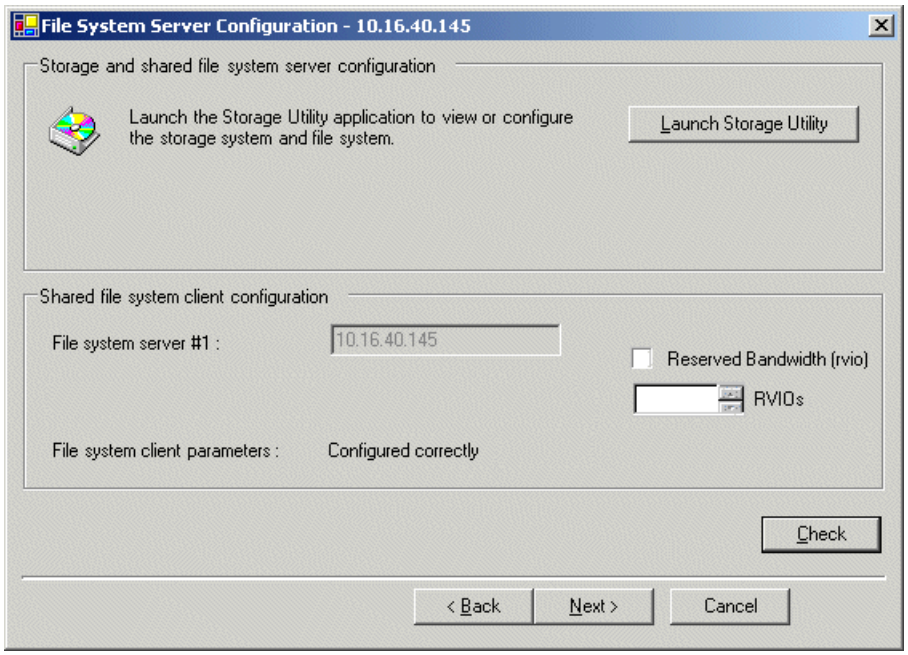
Next, continue with configuring the server using the K2Config application.

Configuring NH server - Part 2

Configure File System Server Configuration page - NH server

Prerequisites for connected K2 RAID storage:

- Network and SNMP settings configured
- Disks bound
- New file system made



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

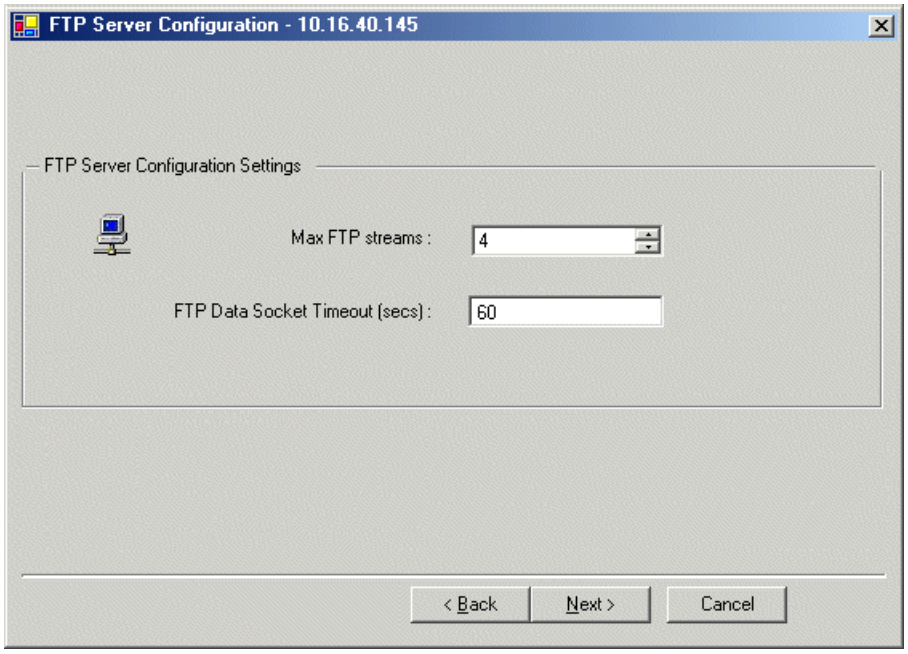
1. In K2Config open the server's File System Server Configuration page, if the page is not already open.

2. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
3. Click **Check**.
4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - NH server



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Check the V: drive

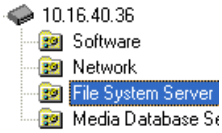
Prerequisites:

- The K2 Media Server is configured

- The restart of the K2 Media Server after it is configured is complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the "ping" command.
2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

The K2 Nearline SAN configuration is complete.

Configuring the redundant nearline K2 SAN

Work through the topics in this section sequentially to configure a redundant nearline (Tier 3) K2 SAN.

Prerequisites for initial configuration - Nearline K2 SAN

Before beginning your initial configuration, make sure the devices of the K2 SAN meet the following prerequisites.

Control point PC

- Ethernet cable connected
- Control Point software installed
- Control network IP address assigned
- Network communication over the control network with all other K2 devices
- Power on

Ethernet switch

- Ethernet cables connected
- Control network IP address assigned
- VLANs set up
- Trunks set up
- Power on

K2 Media Server

- Ethernet cables connected
- Fibre Channel cable connected
- Redundant servers connected by serial cable
- Software installed, as from the factory, including QuickTime 7

- MPIO software installed.
- Control network IP address assigned
- Power on for all servers

K2 RAID chassis

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

K2 RAID Expansion chassis (optional)

- Fibre channel cable(s) connected
- Power on

Related Topics

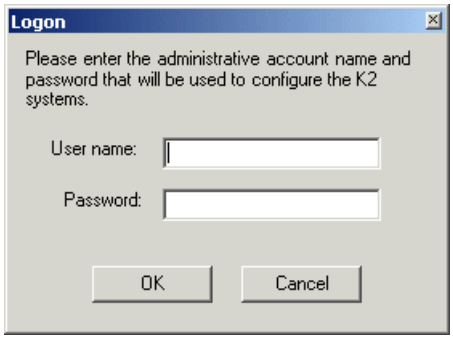
Installing Multi-Path I/O Software on page 232

Defining a new K2 SAN

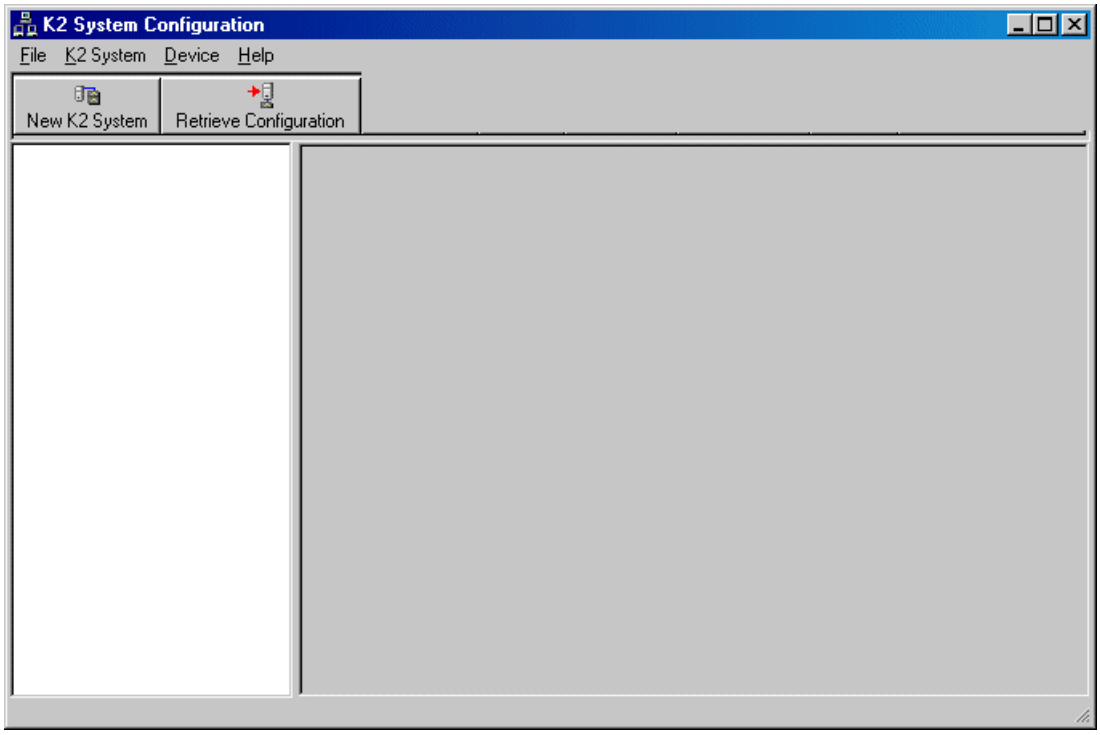
If you import a SiteConfig system description file in which the SAN is defined, you do not need to define a new SAN. You can skip this task and instead start by configuring the first K2 Media Server.

1. On the control point PC, open the K2Config application.

   A login dialog box opens.



2. Log in to the K2Config application with the Windows administrator account.
   The K2Config application opens.



3. Click **New K2 System**.

The New K2 System wizard opens to page 1.

Related Topics

About application security on the K2 SAN on page 272

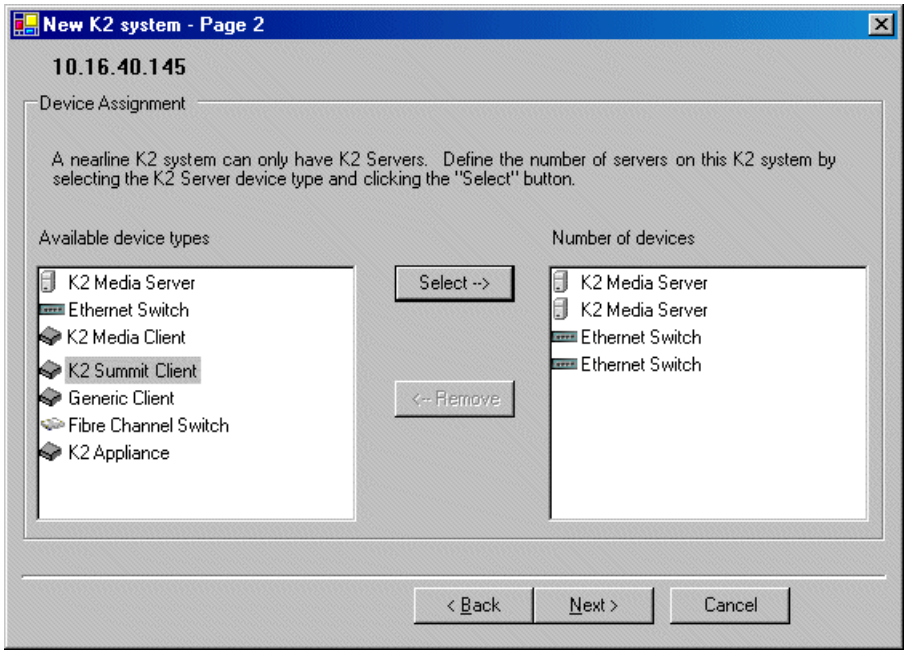
Configure New K2 System page 1 - Nearline K2 SAN

1. Create a name for your system and type it in the Name box.
2. Select **Nearline**.

   The Server redundancy option is not selected and is disabled. This option applies to media database redundancy. Since the Nearline system has no media database, this setting is correct for both redundant and non-redundant Nearline systems.
3. Click **Next**.

Page 2 opens.

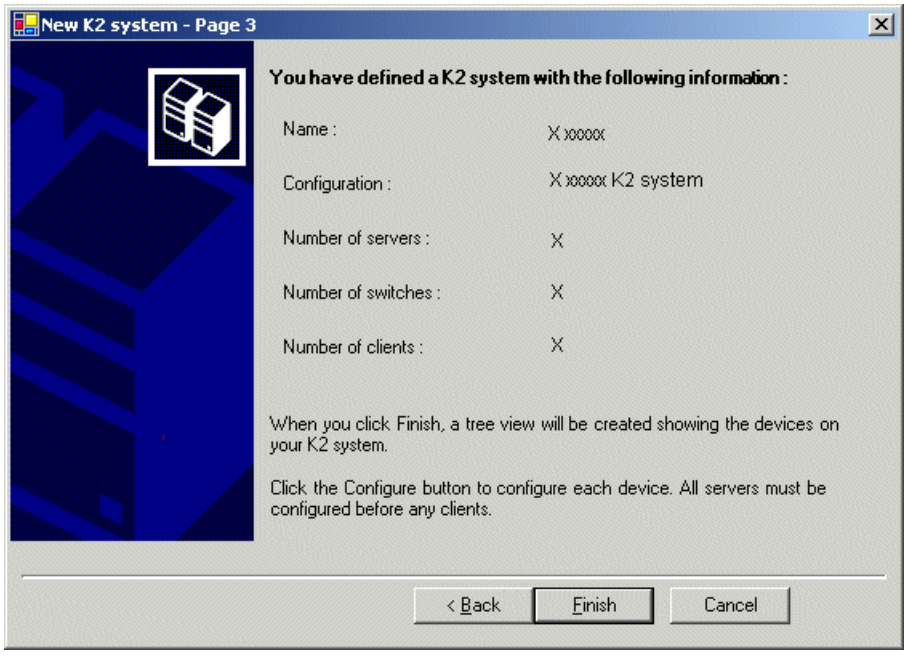
Configure New K2 System page 2 - Nearline K2 SAN



1. Move the following into the Number of devices box:
   - Two K2 Media Servers
   - Two Ethernet switches
2. Click **Next**.

Page 3 opens.

Configure New K2 System page 3 - Nearline K2 SAN



1. Review the information on this page and verify that you have correctly defined your K2 SAN.
   For a 10G redundant nearline K2 SAN you should have the following:
   - Two Gigabit Ethernet switches
   - Two K2 Media Servers
2. Click **Finish**.
   The Define New K2 Storage System wizard closes.

Your storage system appears in the tree view of the K2Config application.

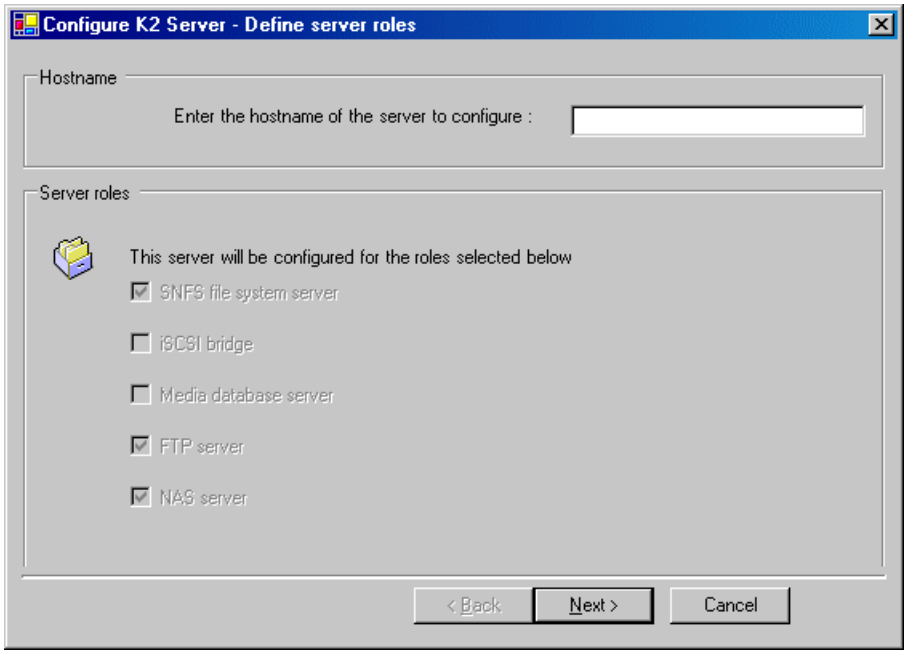
Next, configure the server.

Configuring NH server A - Part 1

1. In the K2Config application tree view, select **[K2Server1]**.
   For the nearline K2 SAN, this is NH server A.
2. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

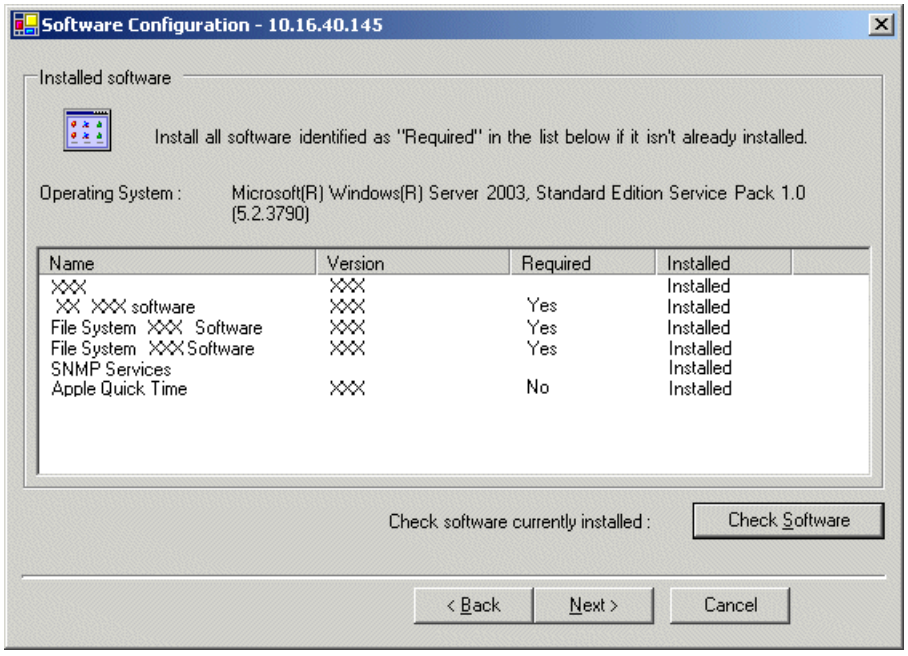
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server



This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on K2 Media Servers in nearline redundant systems.

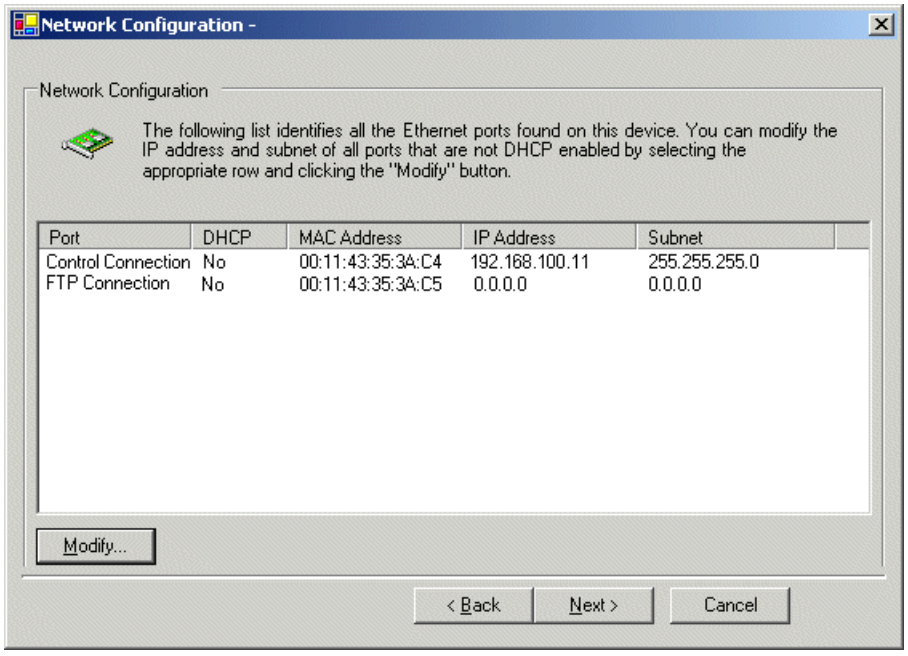
1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Related Topics

Installing Multi-Path I/O Software on page 232

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

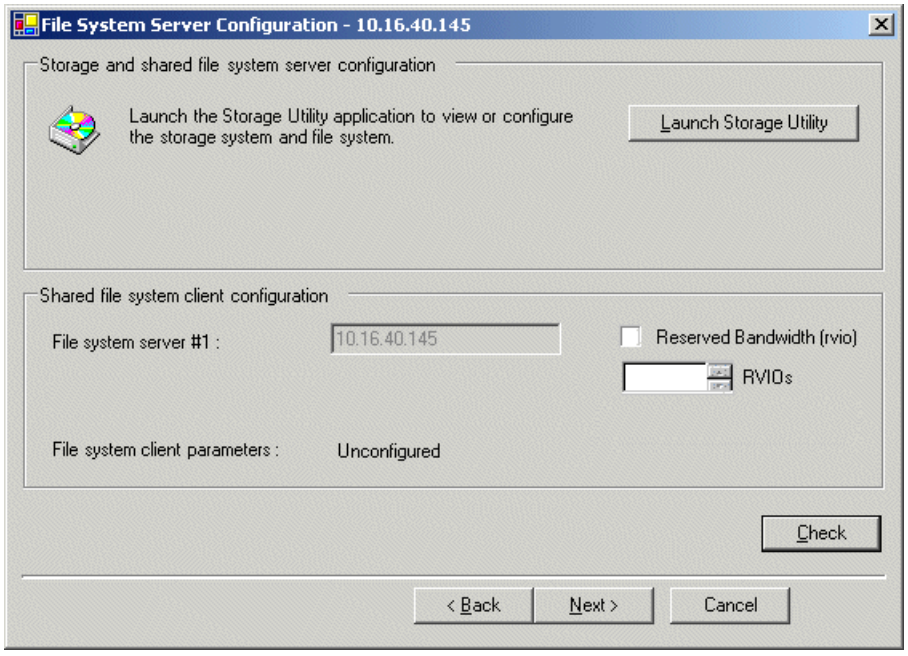
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Launch Storage Manager**.

   Storage Utility opens.
3. Leave the Configure K2 Server wizard open while you use Storage Utility.

   When you are done with Storage Utility, you continue with the wizard.

Next, use Storage Utility to configure the RAID storage and file system.

Configuring RAID

Use Storage Utility to complete the configuration of the K2 RAID storage devices, as explained in the following topics.

Configuring RAID network and SNMP settings

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected

- Power on

Use the Storage Utility to configure the following settings for the K2 RAID controller:

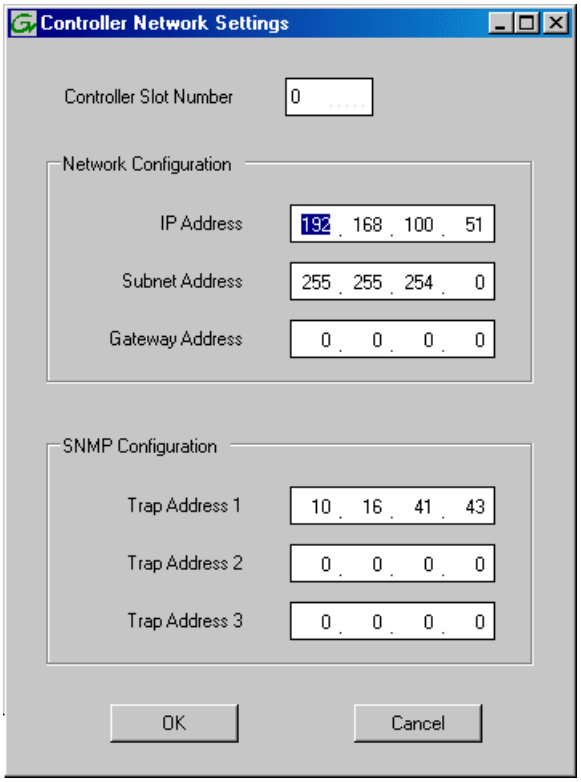
- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

For K2 RAID, network and SNMP settings are set and stored on the RAID controller module. For the RAID chassis with two controllers, each controller has its own network settings and the RAID chassis exists as two entities on the control network.

The RAID storage device is configured by default for the SNMP community name “public”. If your site’s policies require using a different SNMP community name, contact your Grass Valley representative.

1. Launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility tree view, expand the node for the K2 RAID, right-click the icon for a RAID controller, and select **Configuration | Network Properties**.

   The Controller Network Settings dialog box opens.



4. In the Controller Slot Number field enter **0** and then press **Enter**.

   The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.

5. Enter the control network IP address and other network settings.
6. For SNMP Configuration, enter the IP address of the NetCentral server PC.

   You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.
7. For the RAID chassis with two controllers, in the Controller Slot Number field enter **1** and then press **Enter**.

   The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify.
8. Repeat the previous steps to configure controller 1.
9. Click **OK** to save settings and close.
10. In Storage Utility click **View | Refresh**.

Next, bind disk modules.

Binding disk modules - Nearline K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on

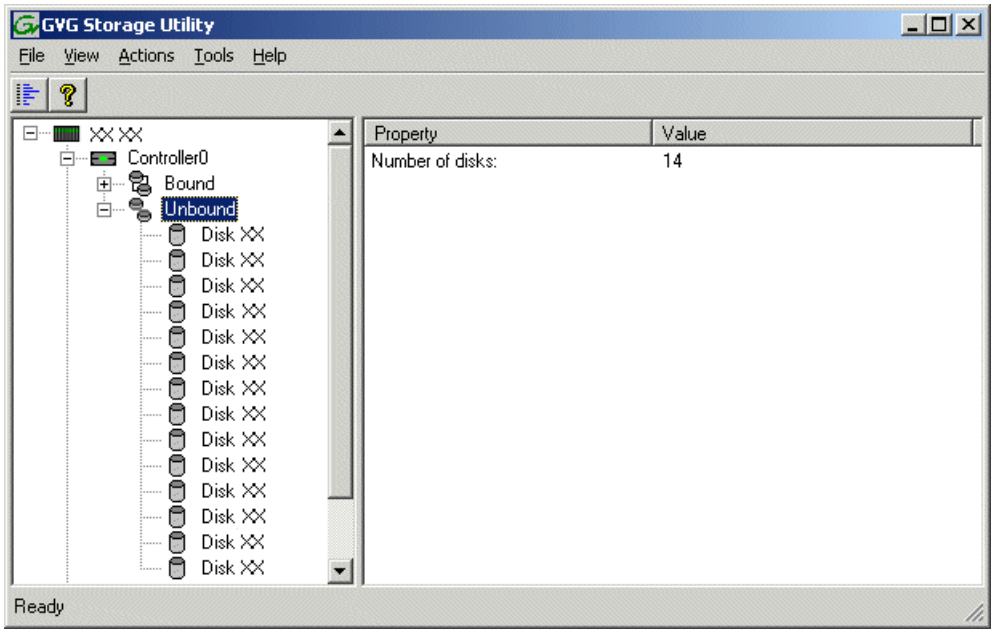
Prerequisites for the optional K2 RAID Expansion chassis (if present) are as follows:

- Fibre channel cable(s) connected
- Power on

NOTE: Binding destroys all user data on the disks.

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.

3. In the Storage Utility main window, identify bound RANKs and unbound disks by their placement in the hierarchy of the tree view. In the following illustration, disk numbers are represented by "XX".



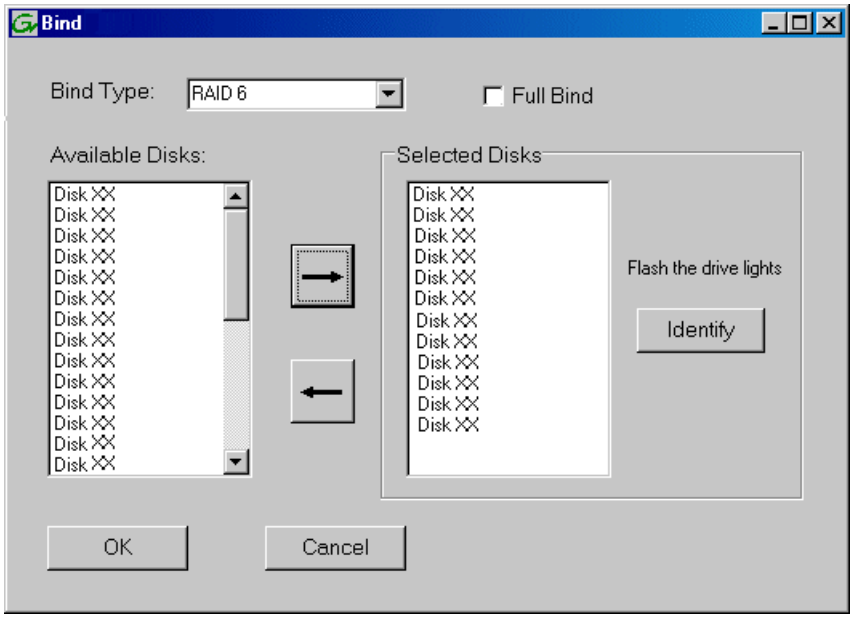
Nearline systems store media files across both the primary RAID chassis and the optional Expansion chassis. In addition, file system metadata files and journal files are mixed in with the media files.

The RAID configuration is the same on all chassis. Each chassis contains disks, which are bound as RAID 6 in a RANK of twelve disks. One twelve disk RANK fills one chassis.

4. Right-click the **Unbound** node for a controller, then select **Bind** in the context menu.

   If the RAID chassis has two controllers, both controllers are represented by the single “Controller” node.

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



5. Leave **Full Bind** unchecked.
6. In the **Bind Type** drop down box, select **RAID 6**.
7. In the Available Disks box, select twelve contiguous disks at the top of the list.

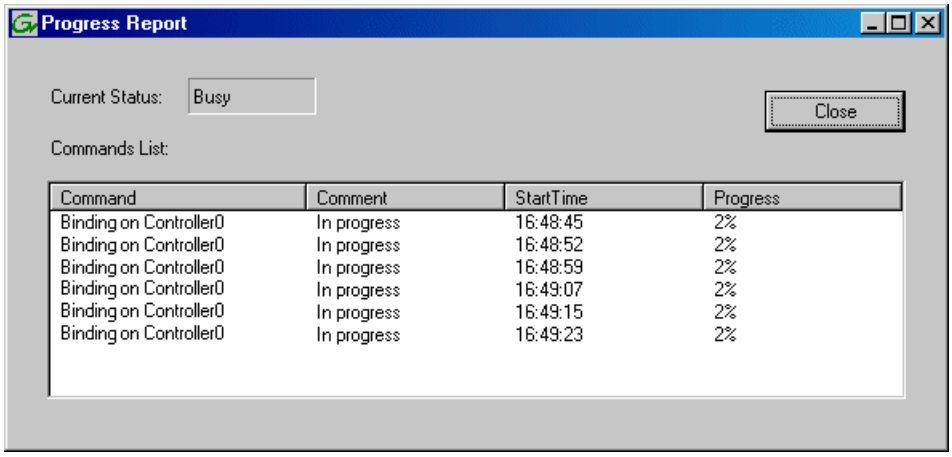
   Use ‘shift-click’ or ‘control-click’ to select disks.

8. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive light to flash.

9. Click **OK** to close the Bind dialog box and begin the binding process.

   The Progress Report dialog box opens, showing the status of the binding process.



10. Close the Progress Report and repeat these steps for other unbound disks.

    If specified by your system design, you can bind some disks as Hot Spares.

    When you are done, if you did not bind any extra Hot Spares, you should have the following results:

    The disks in the primary RAID chassis and in optional Expansion chassis should be bound as RAID 6 RANKs, with twelve disks to a RANK.

11. Click **Close** in Progress Report window.
12. Restart the K2 Media Server.

    NOTE: Make sure start up processes on the K2 Media Server are complete before proceeding.

Next, create a new file system.

Related Topics

Identifying disks on page 321
About full/background bind on page 325
Binding Hot Spare drives on page 327

Creating a new file system - Nearline K2 SAN

Prerequisites for the K2 RAID chassis are as follows:

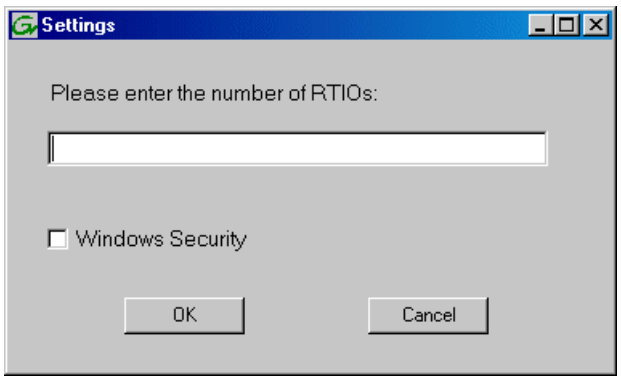
- Fibre Channel cable(s) connected
- Ethernet cable(s) connected
- Power on
- Disks bound

Prerequisites for the optional K2 RAID Expansion chassis are as follows:

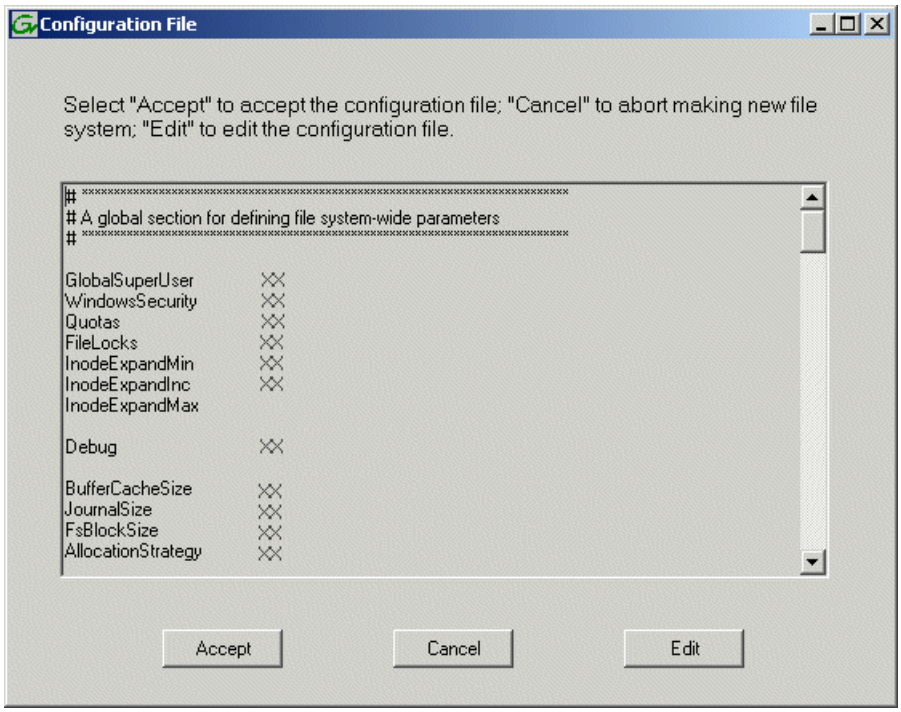
- Fibre channel cable(s) connected
- Power on

- Disks bound

1. If you have not already done so, launch Storage Utility from the K2Config application.
2. As prompted, wait while Storage Utility gathers system information, then Storage Utility opens.
3. In Storage Utility, click **Tools | Make New File System**.
   The Setting dialog box opens.



4. For a Nearline system, enter zero as the Real Time Input/Output (RTIO) rate.
5. Leave Windows Security unchecked.
6. Click **OK**.
   The Configuration File dialog box opens.



The configuration file for the media file system is displayed.

7. Verify media file system parameters.

   Do not edit the configuration file for the media file system.

8. Click **Accept**.

   A "…Please wait…" message box displays progress and a "…succeeded…" message confirms the process is complete.

   A message informs you that you must restart the server, however the restart at the end of the Configure K2 Server wizard suffices, so you do not need to restart now.

9. Close the Storage Utility.

   NOTE: Do not attempt to start SAN-attached systems or otherwise bring the SAN online until instructed to do so by the documented procedure.

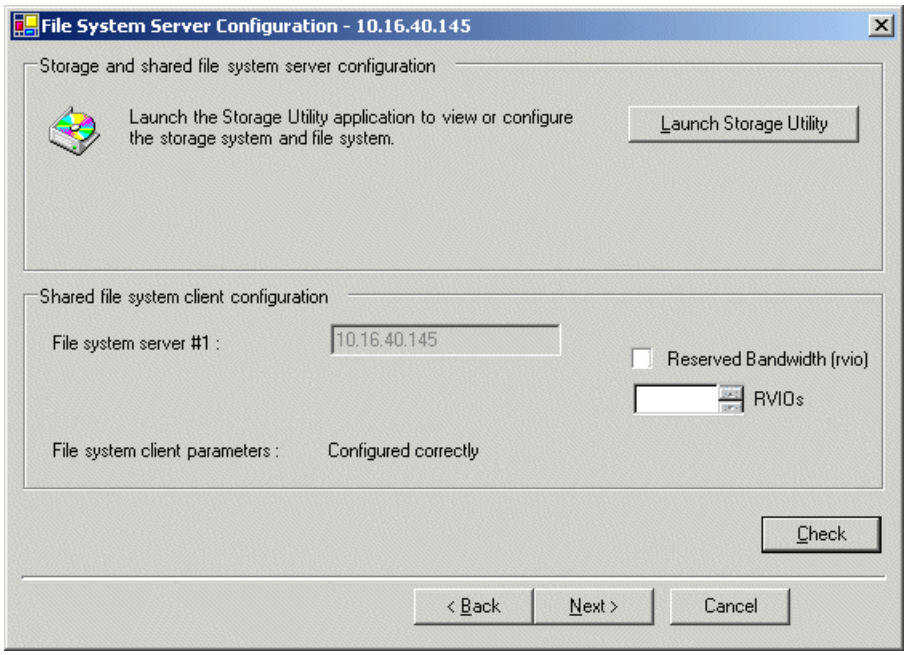
Next, continue with configuring the server using the K2Config application.

Configuring NH server A - Part 2

Configure File System Server Configuration page - NH server

Prerequisites for connected K2 RAID storage:

- Network and SNMP settings configured
- Disks bound
- New file system made



This page checks on the file system server role. The server also functions as a file system client, which is also checked from this page.

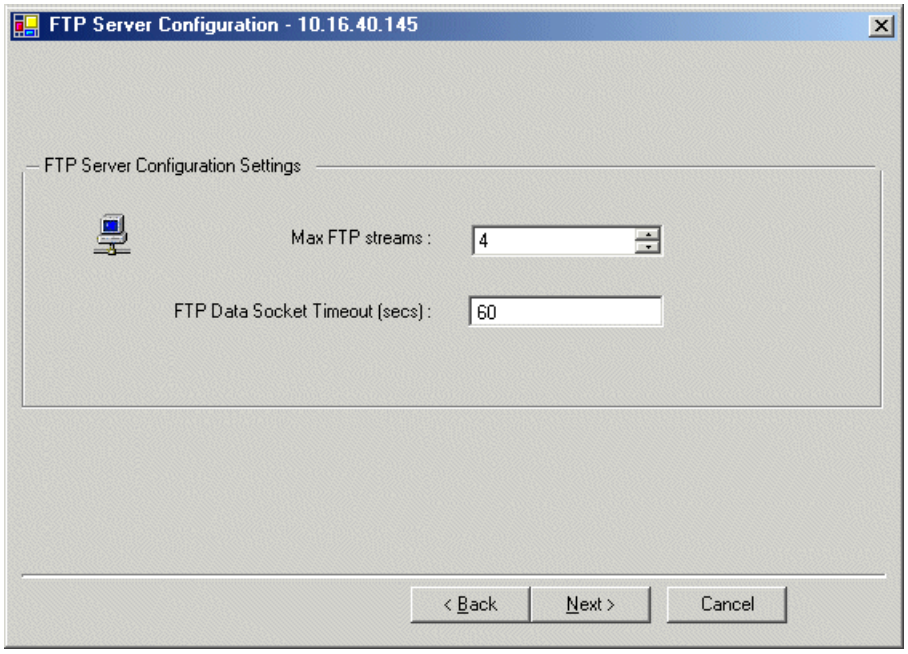
1. In K2Config open the server's File System Server Configuration page, if the page is not already open.

2. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
3. Click **Check**.
4. When the wizard reports that the configuration is correct, click **Next**.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The FTP Server Configuration page opens.

Configure FTP Server Configuration page - NH server A



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, configure the other NH server.

Configuring NH server B

Prerequisites:

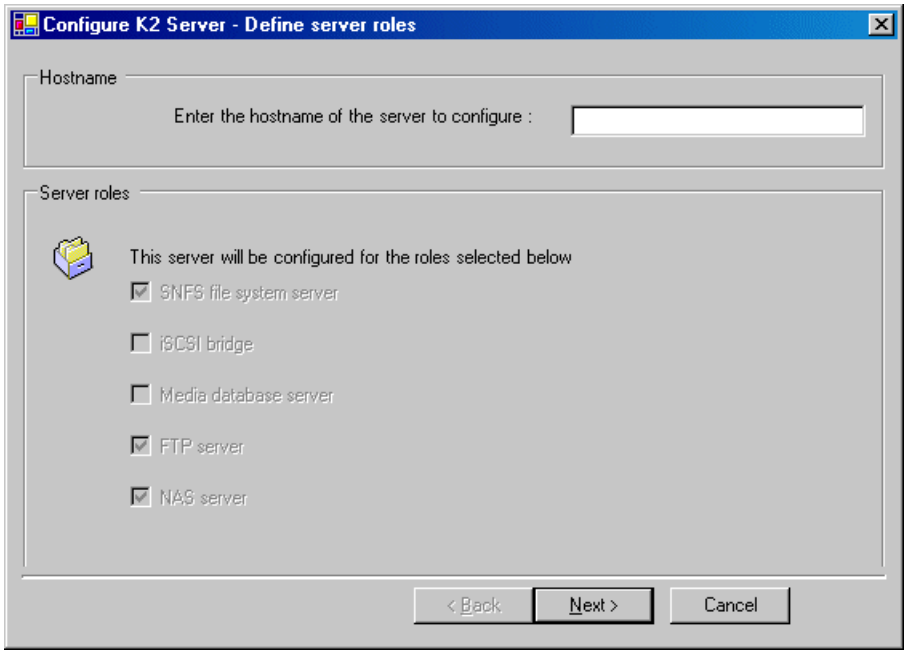
- Server A is configured
- The restart of server A after it is configured is complete

On nearline systems, both NH K2 Media Servers are identical, with the exception that only one server can be the active media file system server at any time. For this reason the K2Config application embeds the configuration and start of the media file system into the wizard when you configure the first NH K2 Media Server, as in the previous procedure. That server is now the acting media file system server. You can now configure the remaining server using the following procedure.

1. Verify that server A has restarted by opening the MS-DOS command prompt and use the "ping" command.
2. In the K2 System Configuration application tree view, select the K2 Media Server you are configuring as server B.
3. Click the **Configure** button.

The Configure K2 Server wizard opens to the Define server roles page.

Configure Define Server Roles page - NH server



1. Enter the name for the K2 Media Server, as currently configured on the machine.

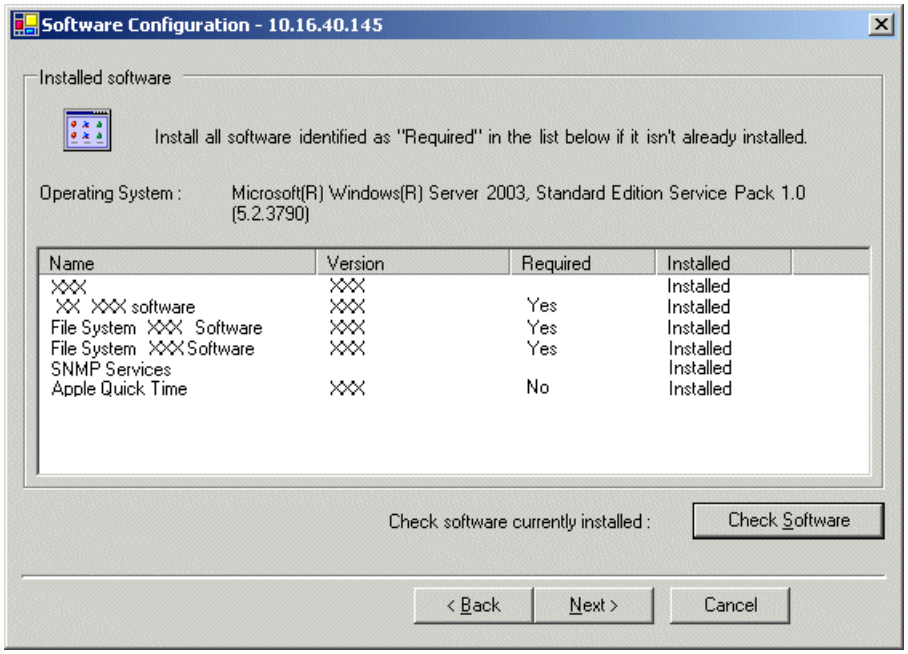
   For Nearline server roles, selections are disabled. Leave SNFS file system server, FTP server, and NAS server selected.

   The wizard does not allow you to select Media Database Server. There is no Media Database Server in a nearline system.

2. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - NH server



This page checks for the software required to support the roles you selected on the previous page.
NOTE: MPIO software is required on K2 Media Servers in nearline redundant systems.

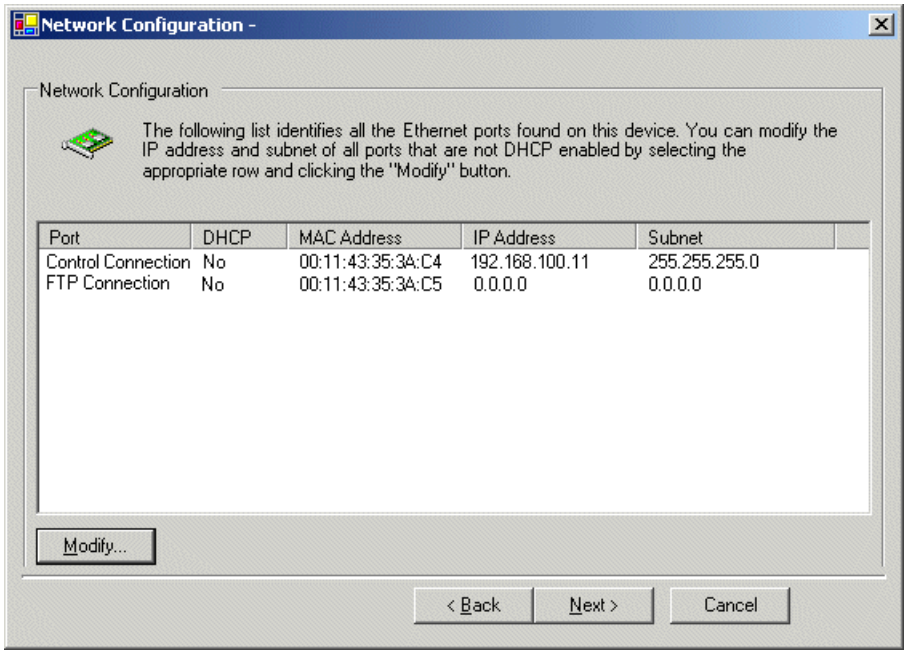
1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Related Topics

Installing Multi-Path I/O Software on page 232

Configure Network Configuration page - NH server



This page displays the control network Ethernet port, and allows you to configure the FTP/Streaming network Ethernet port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Verify that the FTP/Streaming port is configured correctly. If not configured correctly, do the following:

   a) Select the other port and click **Modify**.

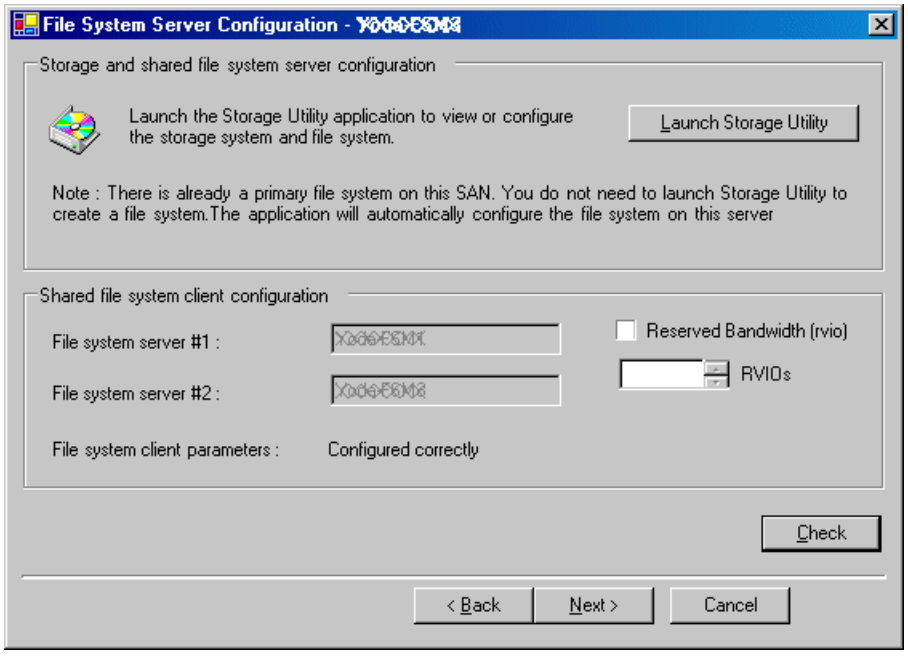
      A network configuration dialog box opens.

   b) Enter the FTP/Streaming IP address and the subnet mask and click **Apply**.

3. Click **Next**.

The File System Server Configuration page opens.

Configure File System Server Configuration page - NH server B



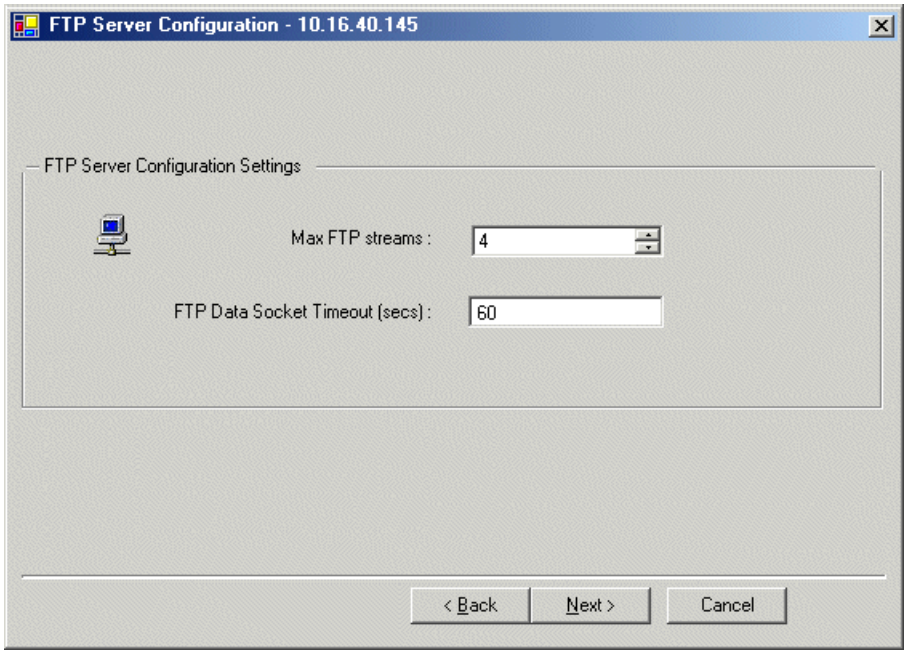
This page checks on the configuration of the K2 Media Server in one of its main roles as a file system server. The K2 Media Server also functions as a file system client, which is also checked from this page. It is not necessary to bind RANKs or create a file system, since this task was completed when you configured the previous K2 Media Server.

1. Do not select **Reserved Bandwidth** unless instructed to do so by Grass Valley. This system is usually not configured for RVIO.
2. Click **Check**.
3. Confirm a "… file copied…" message.
4. When the wizard reports that the configuration is correct, click **Next**.
5. Confirm messages about copying the file system configuration file to the other server.

   If you get a "The V: will not be available until this device is rebooted…" message, you can safely continue now and reboot later when instructed to do so.

The iSCSI Bridge Server Configuration page opens.

Configure FTP Server Configuration page - K2 SAN server B



This page appears only if the server has the role of FTP server.

Do not modify these settings. Leave at default values of Max FTP streams = 4 and FTP Data Socket Timeout = 60. Only qualified Grass Valley personnel should specify other values, as these settings are intended for use only with custom systems designed by Grass Valley.

1. Click **Next**.

   The Completing the Configuration Wizard page opens.

2. Click **Finish**.

   The wizard closes. The server restarts.

Wait until all startup processes have completed before continuing.

Next, check the V: drive

Check the V: drive

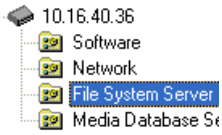
Prerequisites:

- The K2 Media Server is configured
- The restart of the K2 Media Server after it is configured is complete

This task is required for NAS server functionality.

1. Verify that the K2 Media Server has restarted by opening the MS-DOS command prompt and use the “ping” command.

2. In the K2Config application tree view, under the K2 Media Server select the File System Server node.



   The File System Server Configuration page appears.

3. Click **Check** and verify that the V: drive is shared.

The K2 Nearline SAN configuration is complete.

Chapter 8

Configuring clients on the K2 SAN

This section contains the following topics:

- *About iSCSI bandwidth*
- *Determining K2 client bandwidth requirements*
- *K2 SAN prerequisites for adding clients*
- *Configuring a K2 client for the K2 Storage System*
- *Adding a generic client device*
- *Assigning a SAN client to different FTP server*
- *Powering on/off a SAN client*
- *Taking a SAN client offline*

About iSCSI bandwidth

When you purchase a K2 SAN to provide the shared storage for your K2 clients, your Grass Valley representative sizes the storage system and recommends the appropriate license level and QOS level based on your bandwidth requirements. These bandwidth requirements are based on how you intend to use the channels of your K2 clients. The bit rates, media formats, and ratio of record channels to play channels all effect your bandwidth requirements.

As you add your K2 clients to the K2 SAN, you must assign a bandwidth value to each K2 client. This value is based on your intended use of the channels of that K2 client. There is a page in the K2Config application on which you enter parameters such as channel count, bit rate, and track count per channel to calculate the bandwidth value for a K2 client. The K2Config application takes that bandwidth value and assigns it to the total bandwidth available, so that the K2 client has adequate bandwidth for its intended media access operations. When the bandwidth values you enter in the K2Config application match the overall bandwidth requirements upon which your K2 shared storage is sized and licensed, you have sufficient bandwidth for all your K2 clients.

The K2 SAN uses a mechanism called a TCP/IP Offload Engine (TOE) as a bridge across which all media must travel between the iSCSI/Ethernet world and the SCSI/Fibre Channel world. A TOE is hosted by the iSCSI interface board, which also provides the connection to the Ethernet switch. In addition, the K2Config application restricts the amount of bandwidth available based on the level at which you have licensed your K2 SAN.

As you configure your K2 SAN, the K2Config application assigns a K2 client to a TOE and keeps track of the bandwidth so subscribed to each TOE. A single K2 client can only subscribe to a single TOE. However, a single TOE can have multiple K2 clients subscribed to it. It is important to realize that this does not adjust itself dynamically. If you change your intended use of a K2 client and increase its bandwidth requirements, you risk oversubscribing the TOE to which that K2 client is assigned.

The K2Config application provides a report of iSCSI assignments, which lists for each TOE the iSCSI clients assigned and their bandwidth subscription.

Determining K2 client bandwidth requirements

The K2Configapplication provides a page in the Configure K2 Client wizard that calculates the bandwidth requirement for a K2 client. On this page you enter information regarding the channel count, bit rate, and tracks per channel for your intended use of the K2 client. The page then calculates the bandwidth requirement and make it available for load balancing.

K2 SAN prerequisites for adding clients

The following K2 SAN preparations are required to support adding SAN clients:

- All K2 Media Servers and/or K2 RAID storage devices must be installed and cabled.
- The control network must be operational with K2 devices communicating. At the command prompt, use the ping command to verify.

- For basic, non-redundant K2 SANs, the media network must be operational. You can check this with the K2Config application.
- For redundant K2 SANs, media network A and media network B must be operational. You can check this with the K2Config application.
- K2 RAID devices must have disks bound and be configured as required for operation on the K2 SAN.
- K2 Media Servers must be configured such that an operational media file system is present.
- K2 Ethernet switches must be configured and have V-LANs set up.
- The SAN to which you are adding your clients must be defined with the appropriate number and type of clients. In other words, in the K2Config application tree view you should see the clients you are about to add represented as unconfigured devices.
- The K2 Media Server with role of file system server must be licensed as appropriate for the design of your K2 SAN.

NOTE: Do not run Storage Utility on a shared storage client. For shared storage, run Storage Utility only via the K2Config application.

Verify license on K2 Media Server

The K2 SAN license is installed on K2 Media Servers with role of iSCSI bridge. If a redundant system and/or a large system with multiple servers, the license must be installed on each K2 Media Server with role of iSCSI bridge. Use the following steps to verify the license on each K2 Media Server with role of iSCSI bridge.

1. On the K2 Media Server, open SabreTooth License Manager.
2. Verify that a license identified as K2-ISCSI-SVR is installed.

If the license for your K2 SAN license is not installed, you must install it before proceeding.

Related Topics

About K2 SAN licensing on page 126

Licensing a K2 Media Server on page 299

Preparing K2 clients

Do the following to each system in preparation for its addition as a client to the K2 SAN:

1. If you have not already done so, rack, cable, and provide power.
2. Power on the K2 client and log on to Windows as Windows administrator, which is username *Administrator* and password *adminK2* by default. Ignore startup messages referring to a missing media storage system.
3. Assign a control network IP address and configure other network settings for the K2 client. Use SiteConfig for this step. The two control ports are teamed, so even if are making a connection to port 1 only, you must configure network settings for the Control Team.
4. Optionally, use SiteConfig to configure media (iSCSI) networks at this time. You can use either SiteConfig or K2Config to configure media networks. If you use SiteConfig, then you must open the relevant page in K2Config so that K2Config reads the settings in from the system you are adding as a SAN client. This also allows you to verify the media network configuration in the context of K2Config.

5. Configure SNMP properties so the trap destination points to the NetCentral server PC. Use standard Windows procedures.
6. If the K2 client connects to the K2 SAN with a redundant Ethernet (iSCSI) fabric, install Multi-Path I/O software.
7. Copy the K2 SAN hosts file onto the system you are adding as a SAN client. You can use SiteConfig for this task.

Installing Multi-Path I/O Software

If a K2 Summit system, before doing this task make sure the write filter is disabled.

The following procedure is required for shared storage K2 clients that have their Gigabit Media ports connected to the two iSCSI Media networks. This configuration is used for redundant K2 SANs. The procedure is also required on K2 Media Servers on a redundant nearline SAN.

The files for the Multi-Path I/O software are copied on to the K2 client or K2 Media Server when the K2 software is installed.

1. Access the Windows desktop on the K2 system.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.
2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.
4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type one of the following at the command prompt:

   - For a K2 client or a 32-bit K2 Media Server, type the following:

     ```
     gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM
     ```
   - For a 64-bit K2 Media Server, type the following:

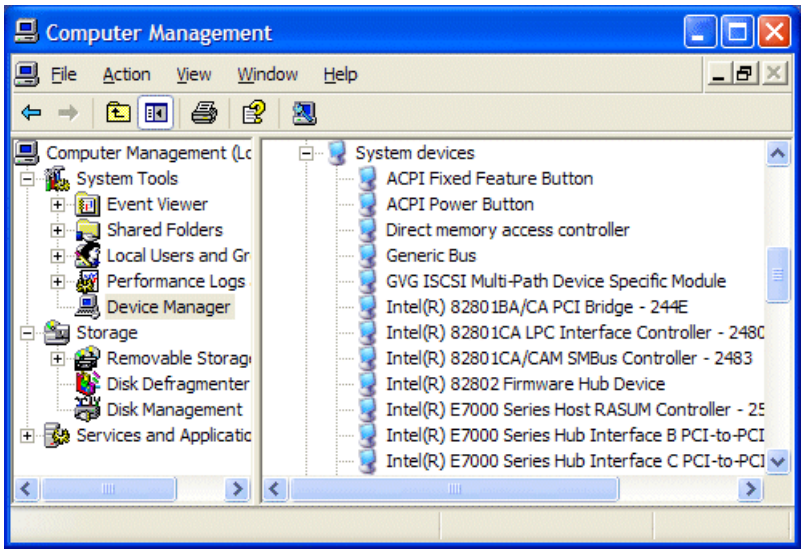
     ```
     gdsminstall64.exe -i
     ```
6. Type the following at the command prompt:

   - `gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM`
7. Press **Enter**.

   The software is installed. The command prompt window reports progress.
8. Restart the K2 system.

9. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

   The Computer Management window opens.



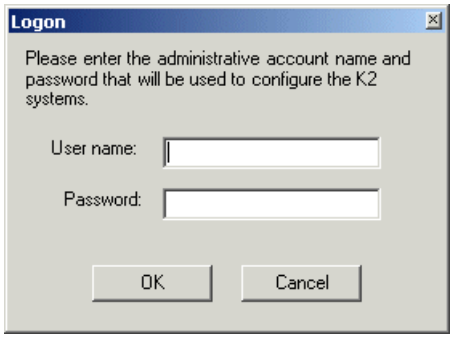
10. In the left pane select **Device Manager**.
11. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

Configuring a K2 client for the K2 Storage System

Before doing this task, make sure the write filter is disabled on the K2 Summit system you are adding to the K2 SAN.

1. On the PC that hosts K2Config, open the K2Config application.

   A login dialog box opens.



2. Log in to the K2Config application with the administrator account.

   The K2Config application opens.

3. In the K2Config application tree view, verify that the K2 SAN has the correct number of clients, according to your system design.

   If the correct number of clients is not currently added to the K2 SAN, you can add or remove clients now (before clients are configured), as follows:

   - To add a client, select the top node of the storage system and click the **Add Device** button.
   - To remove a client, select an unconfigured client and click the **Remove** button.

4. In the K2Config application tree view, select the system you are adding to the K2 SAN.
5. Select a client and click the **Configure** button.

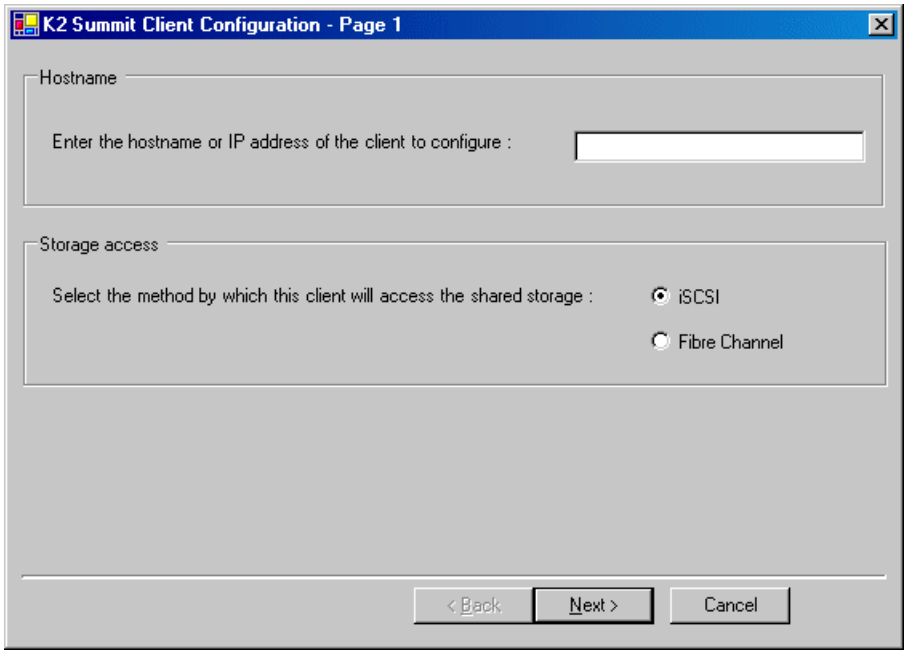
The configuration wizard opens to page 1.

NOTE: If your system has a large number of iSCSI clients, you are prompted to restart the server that has the role of SNFS file system server when you configure clients and cross the following thresholds: 64 clients; 80 clients; 96 clients.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Configure page 1 - K2 client



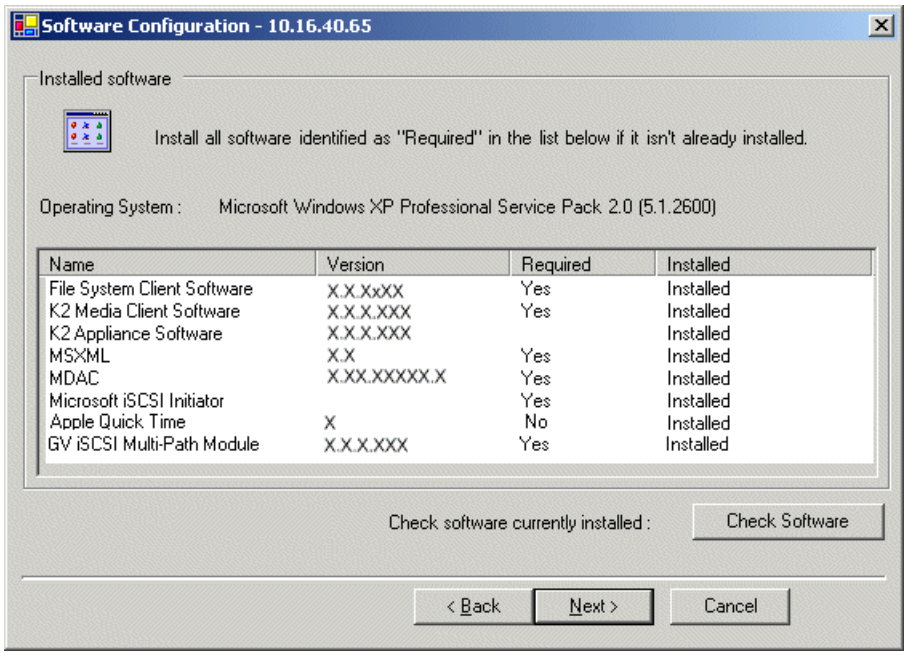
1. Enter the IP address or network name for a SAN client, as currently configured on the client system.

   You should configure your highest bandwidth SAN clients first, as this ensures load balancing is correct.

2. For the Storage Access settings, leave iSCSI selected.
3. Click **Next**.

The Software Configuration page opens.

Configure Software Configuration page - K2 client



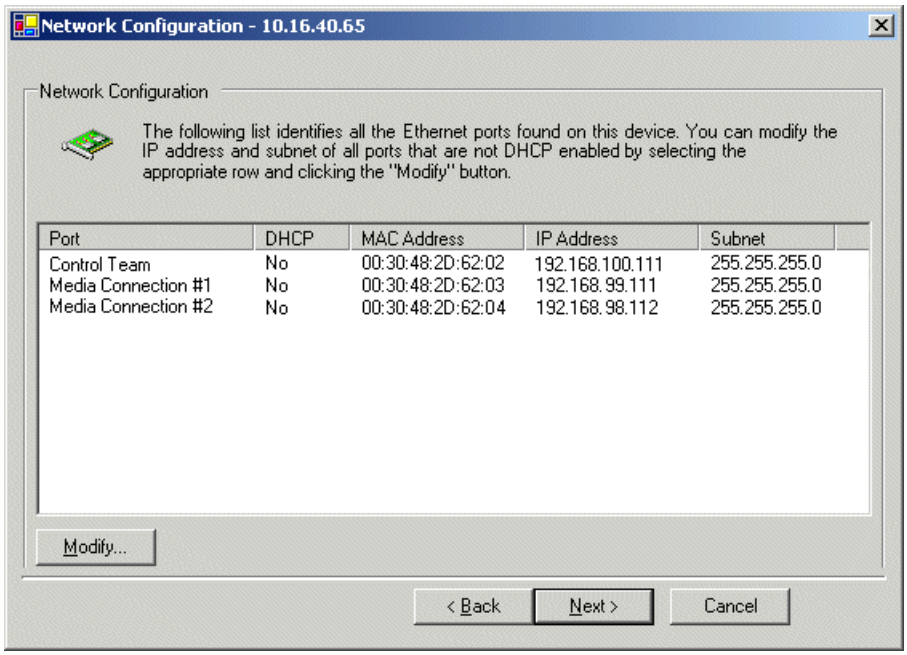
This page checks the client for required software.

NOTE: Multi-Path I/O software must be installed on K2 clients connected to a redundant K2 SAN.

1. If software with **Yes** in the Required column reports as **Not Installed**, install the software.
2. Click **Check Software**.
3. When all required software reports as **Installed**, click **Next**.

The Network Configuration page opens.

Configure Network Configuration page - K2 client



This page configures both control and media (iSCSI) network connections.

The K2 client actually has four Gigabit Ethernet ports, but two ports are configured as a teamed pair (the control team), while the other two ports (the media connections) are individual. The teamed pair shares an IP address and appears on this page as a single port.

1. Verify that the top port is configured correctly.

   The top port is the port over which the K2Config application is communicating. If correctly configured, it is already assigned the control network IP address, as displayed on this page.

2. Select **Media Connection #1** and then click **Modify**.

   A network configuration dialog box opens.

3. Verify or configure Media Connection #1 as follows:

   - If a basic (non-redundant) K2 SAN, verify or enter the media network IP address. Also enter the subnet mask.
   - If a redundant K2 SAN, verify or enter an IP address for the “A” media (iSCSI) network. Also enter the subnet mask.

4. Do one of the following:

   - If a basic (non-redundant) K2 SAN, skip to the last step in this procedure. Do not configure Media Connection #2.
   - If a redundant K2 SAN, proceed with the next step and configure Media Connection #2.

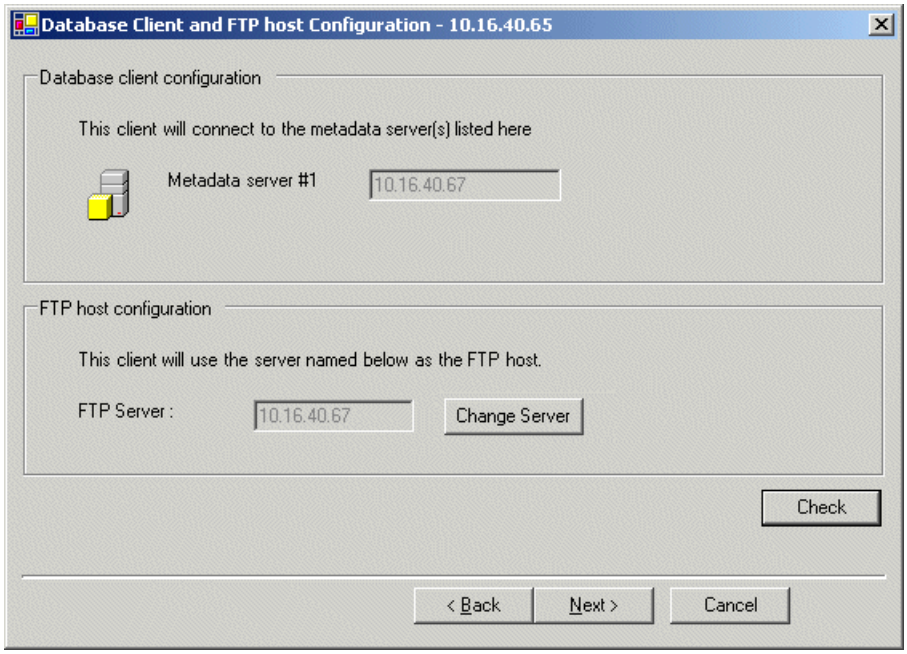
5. Select **Media Connection #2** and then click **Modify**.

   A network configuration dialog box opens.

6. Verify or enter an IP address for the "B" media (iSCSI) network. Also enter the subnet mask.
7. Click **Next**.

The Database Client Configuration page opens.

Configure Database Client Configuration page - K2 client



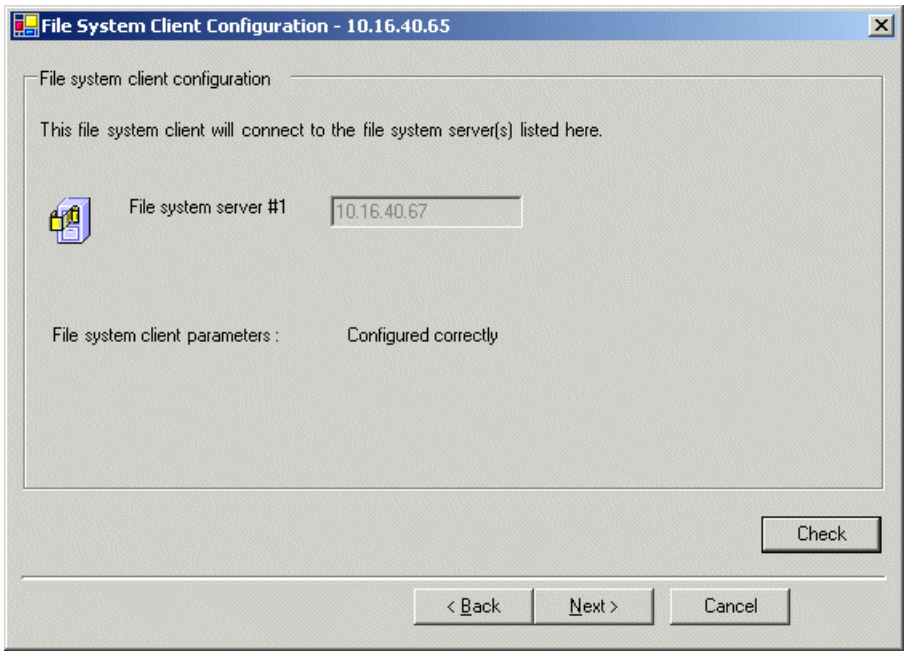
This page connects the SAN client as a media database client to the K2 Media Server taking the role of metadata (database) server. If there are redundant K2 Media Servers, both are listed on this page as database servers.

1. Verify that the K2 client is connecting to the correct K2 Media Server or Servers, as follows:
   - For a basic (non-redundant) K2 SAN, the client connects to the only server.
   - For a redundant K2 SAN, the client connects to server A as database server 1 and server B as database server 2.

   If there are multiple FTP servers (such as the optional NH servers), the K2Config application automatically assigns the SAN client to an FTP server to provide optimum FTP bandwidth across the system. Do not attempt to change the assignment to a different FTP server while you are doing this initial configuration.
2. Click **Check**.
3. When the wizard reports that the configuration check is successful, click **Next**.

The File System Client Configuration page opens.

Configure File System Client Configuration page

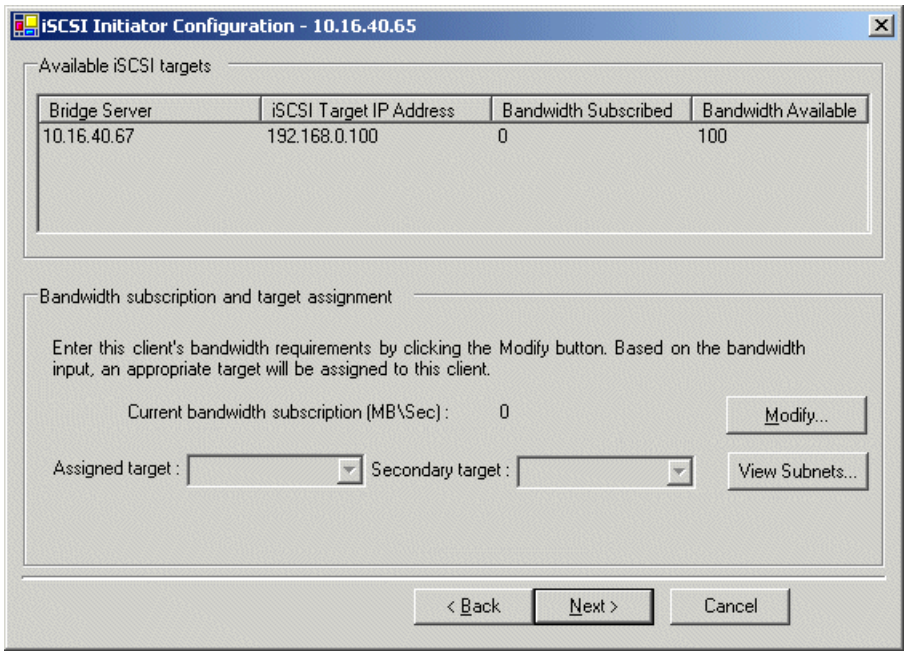


This page connects the SAN client as a media file system client to the K2 Media Server taking the role of media file system server. If there are redundant K2 Media Servers, both are listed on this page as file system servers.

1. Verify that the K2 client is connecting to the correct K2 Media Server or Servers, as follows:
   - For a basic (non-redundant) K2 SAN, the client connects to the only server.
   - For a redundant K2 SAN, the client connects to server A as file system server 1 and server B as file system server 2.
2. Click **Check**.
3. When the wizard reports that the configuration check is successful, click **Next**.

The iSCSI Initiator Configuration page opens.

Configure iSCSI Initiator Configuration page - K2 client

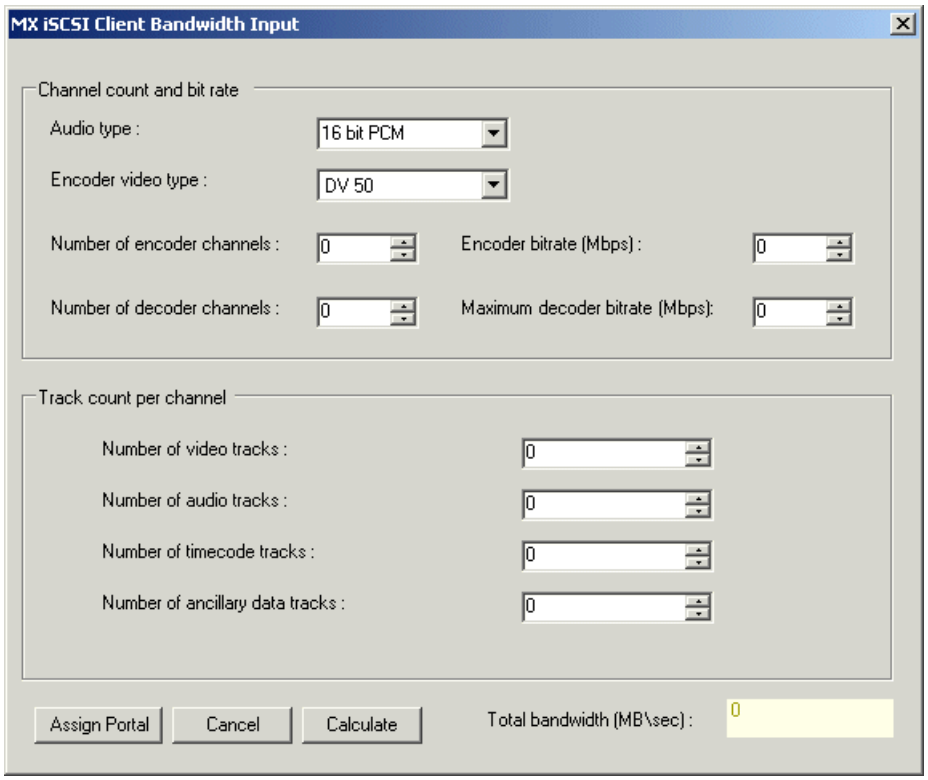


This page lists the iSCSI adapter on your K2 Media Server as an iSCSI target. The K2Config application subscribes the SAN client to the iSCSI target and allocates bandwidth, based on the bandwidth values that you enter. The K2Config application keeps track of each SAN client's bandwidth, and when the total amount allowed by the K2 SAN license is consumed, the K2Config application displays an informative message and then disables your ability to add more SAN clients. For large systems the K2Config application can load balance SAN clients across multiple iSCSI targets.

If a custom K2 SAN, qualified system designers can view subnets to help assign iSCSI targets.

1. Click **Modify**.

   The Bandwidth Input dialog box opens.



2. Enter the channel count, bit rate, and track count per channel information according to your intended use of the K2 client.

   If using ChannelFlex Suite with multiple inputs and/or outputs per channel, do not enter the number of channels. Instead do the following:

   - For **Number of encoder channels** enter the total number of inputs.
   - For **Number of recorder channels** enter the total number of outputs.

3. Click **Calculate**.
4. Click **Assign Portal**, then **OK** to confirm.

   If you have a redundant K2 SAN, the K2Config application makes the appropriate assignment to the redundant server, as reported in the Secondary target box.

5. Click **Next**.

   The Completing the Configuration Wizard page opens.

6. Click **Finish**.

   The wizard closes. The SAN client restarts.

Repeat these tasks to add remaining SAN clients to the K2 SAN.

Adding a generic client device

Prerequisites for adding a generic client to an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.

1. In SiteConfig, add the client device to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the type of client you are adding.
5. Click **OK**. The new client appears in the tree view.
6. Configure the client as appropriate. Refer to the documentation for the device.

   Enter the RVIO value as provided by Grass Valley. Do not attempt to calculate the RVIO value on your own.

   When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.

Assigning a SAN client to different FTP server

Before doing this task on a K2 Summit system, make sure the write filter is disabled on the K2 Summit system.

If your K2 SAN has multiple K2 Media Servers that take the role of FTP server, such as when you have one or more options NH servers, you can change the FTP assignment of a SAN client so that it uses a different FTP server. This is helpful if one of the FTP servers requires service work or otherwise becomes unavailable. In this case, you might want a SAN client assigned to that FTP server to use a different FTP server, so that its FTP access can continue.

1. From the Control Point PC, open the K2Config application.
2. For each SAN client, open the Media Database page.
3. Identify the SAN clients assigned to the FTP server that is about to become unavailable.
4. For those K2 clients, click **Change Server**.

   A message box appears that asks if you are sure you want to change the FTP server.

5. In the message box, click **Yes**.

   The K2Config application finds the FTP server with the most available FTP bandwidth and re-assigns the K2 client to that FTP server.

6. On each SAN client for which you changed the FTP server assignment, restart the client. This puts the change into effect, so that the next time the SAN client needs FTP access, it uses the newly assigned FTP server.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Powering on/off a SAN client

As long as the K2 SAN remains operational, you can use the standard power on and power off procedures appropriate for the SAN client. When a SAN client goes offline or comes online it does not disrupt the K2 SAN.

However, if you are powering down or otherwise taking the K2 SAN itself out of service, you must follow the correct SAN power down procedure. You must first stop all media access on your SAN clients to ensure that they do not cause error conditions. You can power off the SAN clients or take them offline using the K2Config application.

When powering up the K2 SAN, power on the SAN clients last so that they can verify their media storage as part of their start up processes.

Taking a SAN client offline

1. Stop all media operations on the device. This includes, play, record, and transfer operations.
2. Shut down the SAN client.

Chapter 9

Operating the K2 SAN

This section contains the following topics:

- *Powering off the K2 SAN*
- *Powering on the K2 SAN*
- *Failover behaviors*

Powering off the K2 SAN

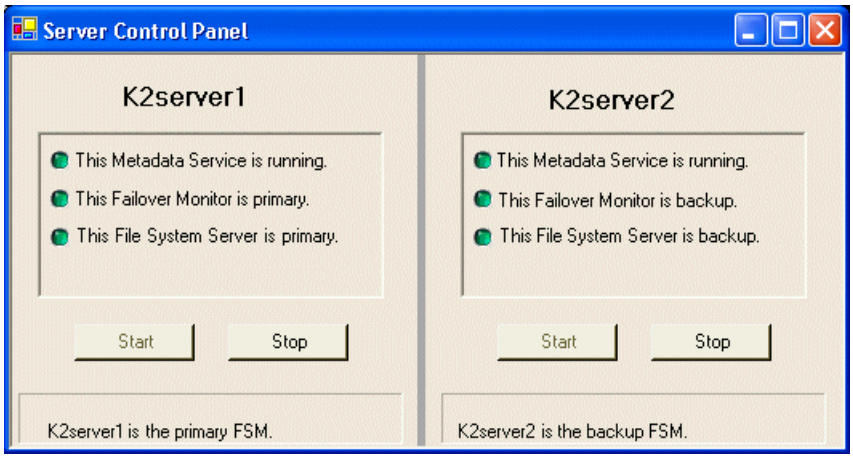
Use the following procedures to do an orderly power off of the complete K2 SAN.

Power off K2 Media Servers

1. Stop all media access as follows:
   - For nearline systems, stop all FTP streams or other media operations.
   - For online systems, power-off all K2 clients or other iSCSI clients.
2. Shut down K2 Media Servers as follows:
   - For nearline systems, shut down all K2 Media Servers.
   - For basic (non-redundant) online or production systems, shut down the K2 Media server that is the media file system and metadata server.
   - For redundant online or production systems, manage redundant server shutdown as follows:

   a) From the K2 System Configuration application, in the tree view select the name of the K2 SAN, which is the top node of the storage system tree. Then click the **Server Control Panel** button.

   The Server Control Panel opens.



   b) Take note of which is the primary K2 Media Server and which is the backup K2 Media Server.
   c) For the backup K2 Media Server, click **Stop**. This takes the server out of service.
   d) Shut down the backup K2 Media Server, if it does not shut down automatically.
   e) For the primary K2 Media Server, click **Stop**. This takes the server out of service.
   f) Shut down the primary K2 Media Server, if it does not shut down automatically.
3. Shut down any remaining K2 Media Servers, such as NH FTP servers.

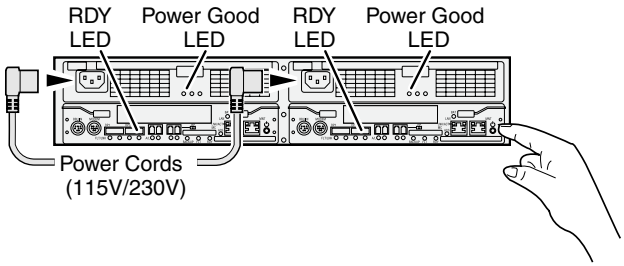
Next, power off K2 RAID devices.

Power off K2 RAID

Prerequisites for this task are as follows:

- K2 Media Servers are powered off

1. On the primary RAID chassis controller, identify the RDY LED. It blinks at a rate of 1 blink per second during normal operation.



2. Press and hold down the power button on a RAID controller. If you have two controllers, you can press the power button on either RAID controller 0 or RAID controller 1.
3. Release the power button in about 5 seconds, when the RDY LED blinks more quickly, at a rate of about 2 blinks per second. Do not hold down the power button for longer than 15 seconds.

   The power button on the RAID controller turns off power for the primary RAID chassis and any connected Expansion chassis. Power-off normally occurs within 20 seconds and is indicated when LEDs other than those on the power supplies go off and the fans stop rotating.
4. Wait for RAID power-off to complete before proceeding.
5. Power-off all Ethernet switches.
6. Power-off the control point PC and/or the NetCentral server PC, if necessary.

Next, power off remaining SAN devices.

Power off remaining K2 SAN devices

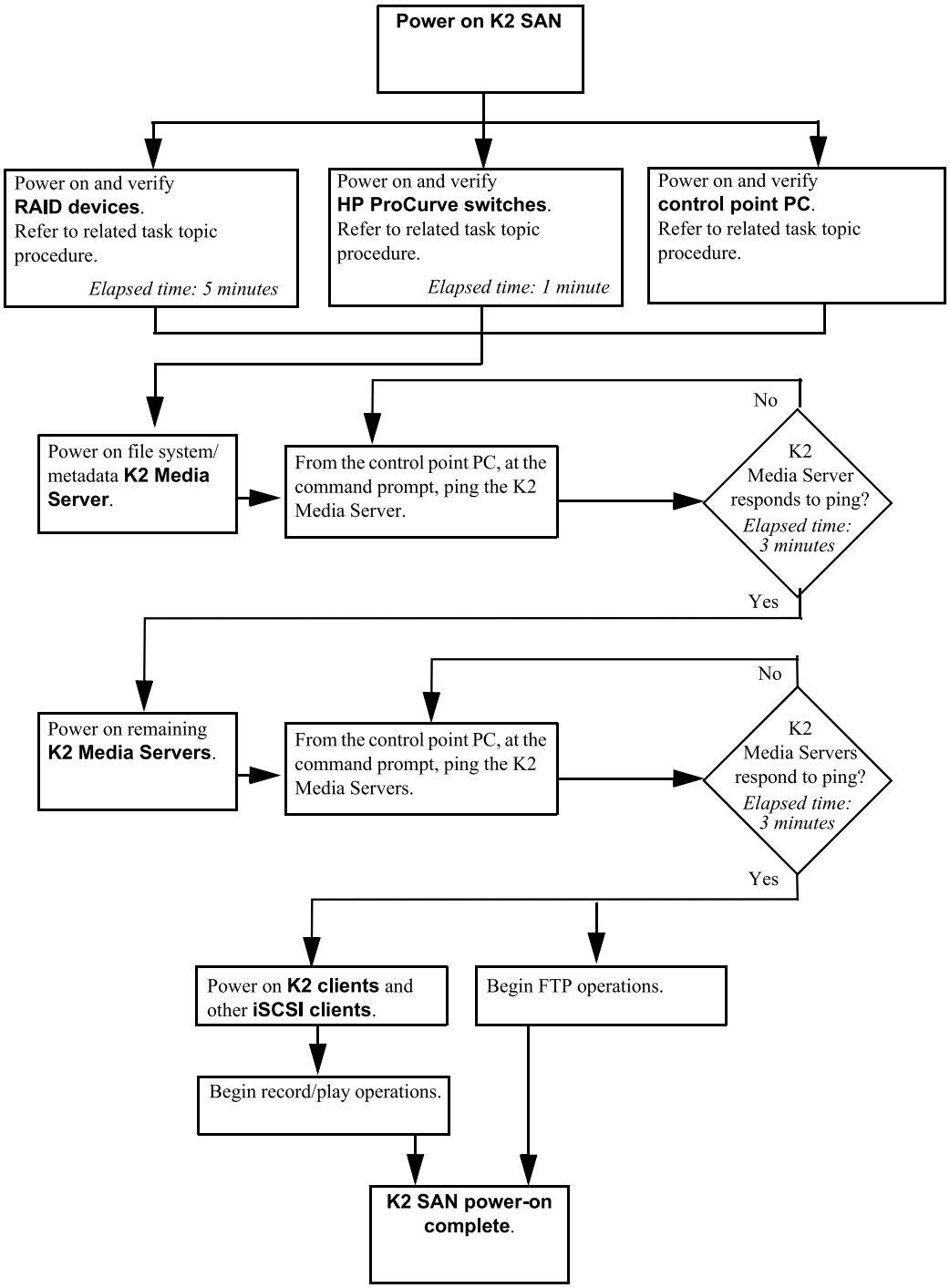
1. Power-off all Ethernet switches.
2. Power-off the control point PC and/or the NetCentral server PC, if necessary.

The K2 SAN is powered off.

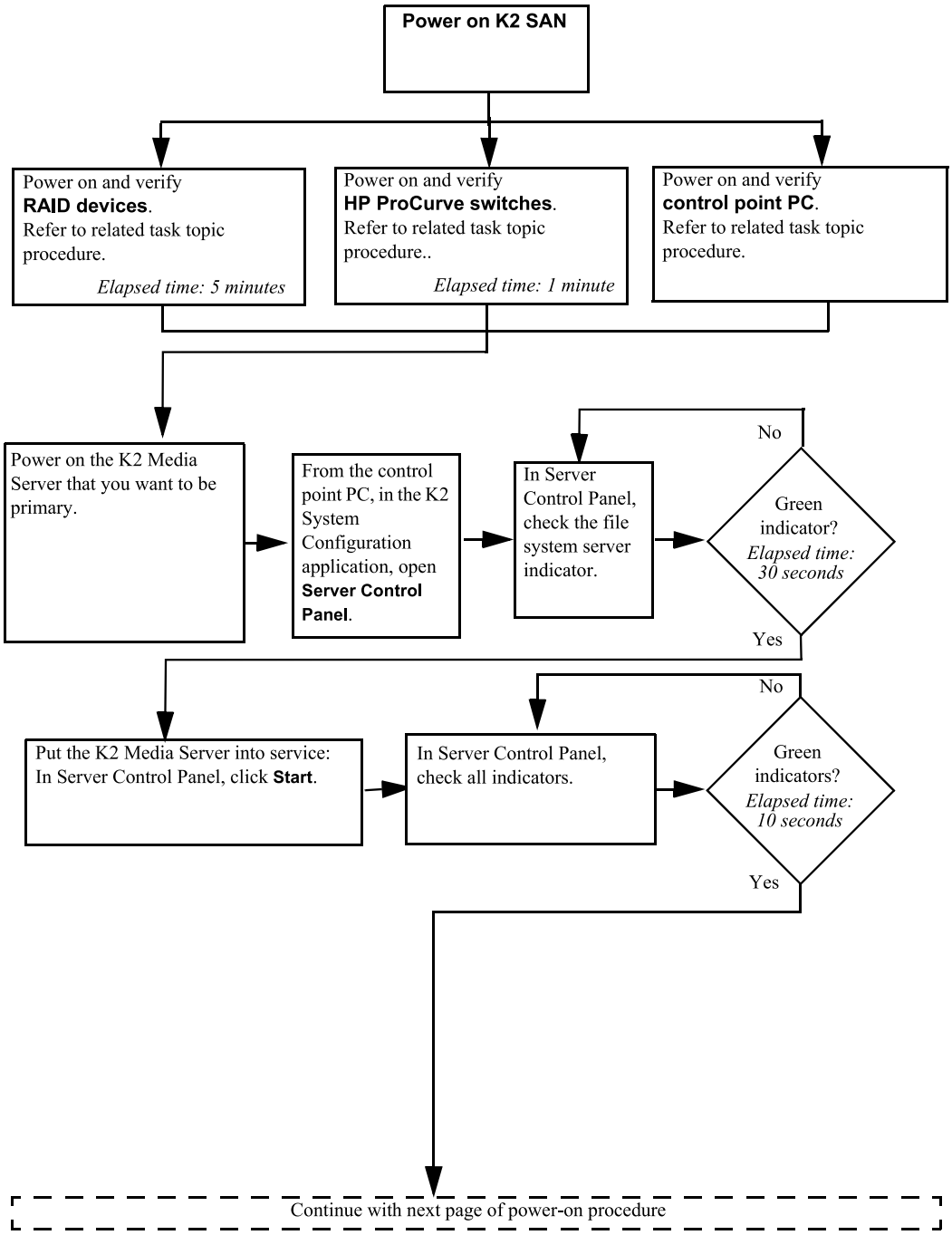
Powering on the K2 SAN

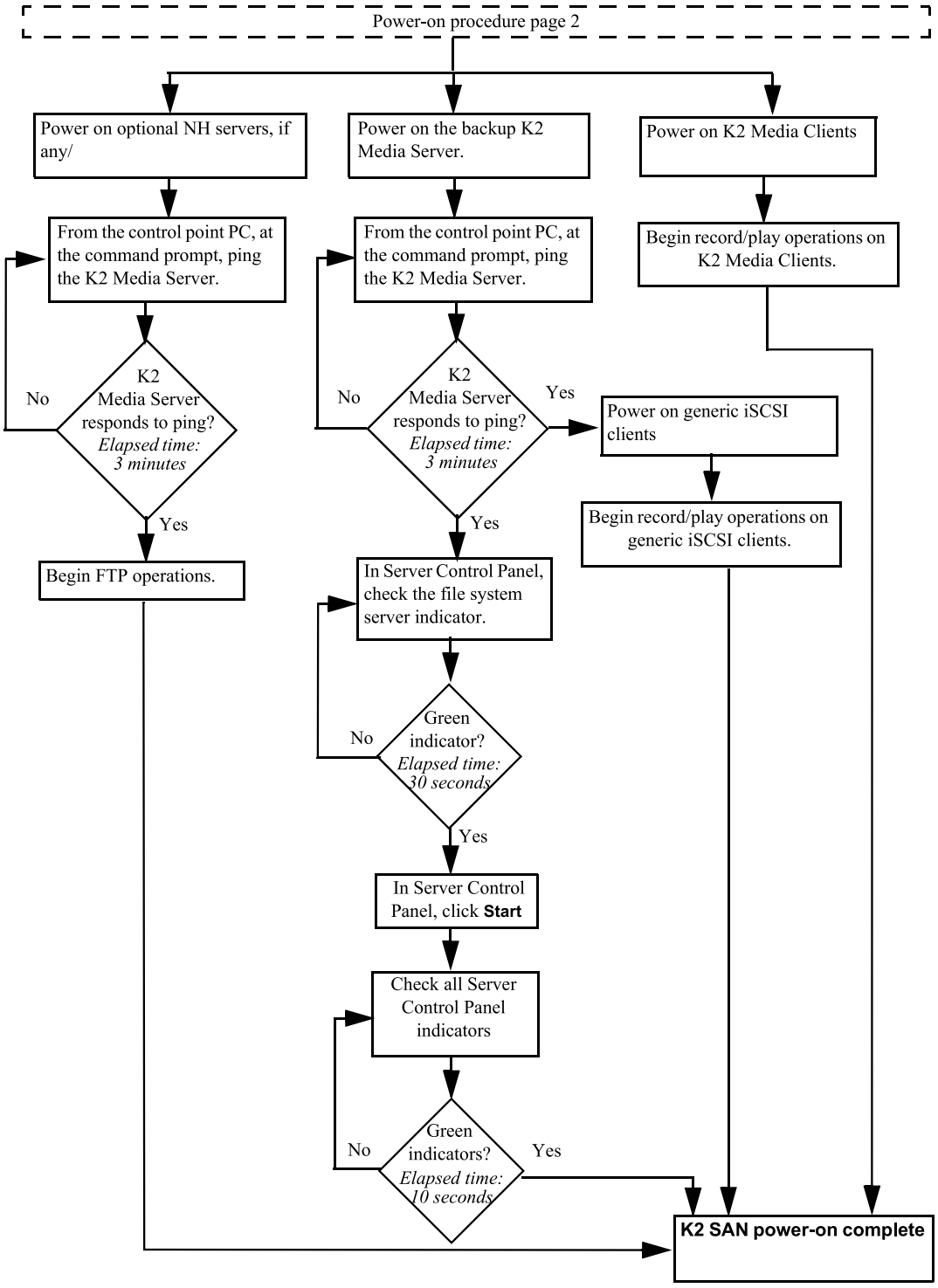
Use the following procedures to do an orderly power on of the complete K2 SAN.

Basic K2 SAN power on procedure

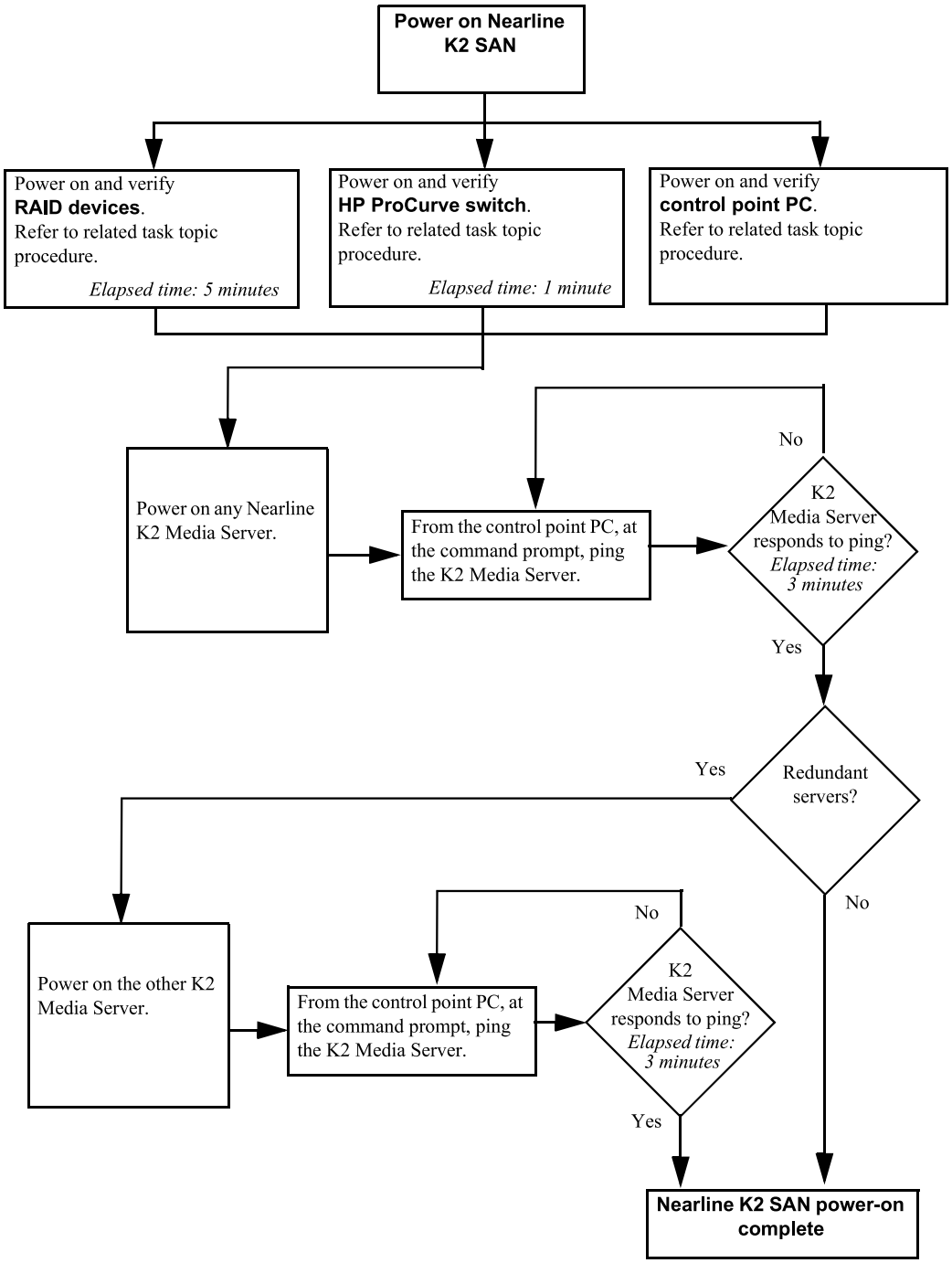


Redundant K2 SAN power on procedure




Power-on procedure page 2
Power on optional NH servers, if any/
Power on the backup K2 Media Server.
Power on K2 Media Clients
From the control point PC, at the command prompt, ping the K2 Media Server.
From the control point PC, at the command prompt, ping the K2 Media Server.
Begin record/play operations on K2 Media Clients.
No
K2 Media Server responds to ping?
Elapsed time: 3 minutes
Yes
No
K2 Media Server responds to ping?
Elapsed time: 3 minutes
Yes
Power on generic iSCSI clients
Yes
Begin FTP operations.
In Server Control Panel, check the file system server indicator.
Begin record/play operations on generic iSCSI clients.
No
Green indicator?
Elapsed time: 30 seconds
Yes
In Server Control Panel, click Start
Check all Server Control Panel indicators
No
Green indicators?
Elapsed time: 10 seconds
Yes
K2 SAN power-on complete

Nearline K2 SAN power on procedure



Powering on the HP ProCurve switch

Use the following procedure to power on and verify proper operation of the HP ProCurve switch.

1. Power up the switch.
2. Watch LEDs to verify proper operation.

   The diagnostic self test LED Behavior is as follows:

   - Initially, all the status, LED Mode and port LEDs are on for most of the duration of the test.
   - Most of the LEDs go off and then may come on again during phases of the self test. For the duration of the self test, the Test LED stays on.

   If the ports are connected to active network devices, the LEDs behave according to the LED Mode selected. In the default view mode (Link), the LEDs should be on.

   If the ports are not connected to active network devices, the LEDs will stay off.

Powering on the control point PC

Use the following procedure to power on K2 SAN's control point PC and verify proper operation during power up of the system.

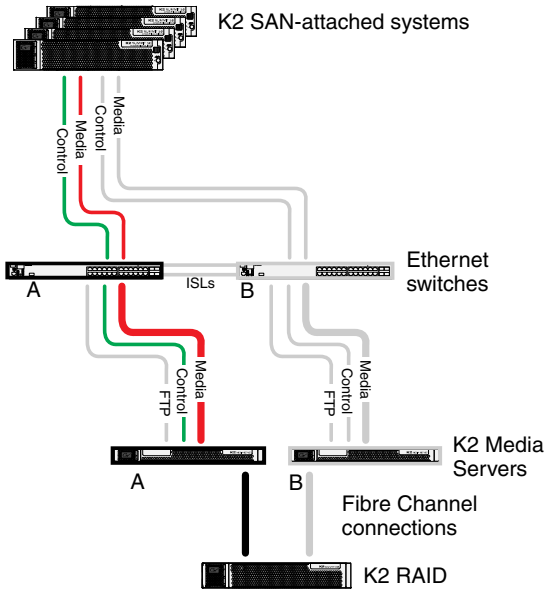
1. Power up and log on to the PC using standard Windows procedures.
2. Start and log on to NetCentral.
3. NetCentral reports devices as offline. As each device of the K2 SAN is powered on, check NetCentral to verify the device's status.

Failover behaviors

If a fault occurs and one of the failover mechanisms is triggered, an online redundant iSCSI K2 SAN behaves as explained in the following sections.

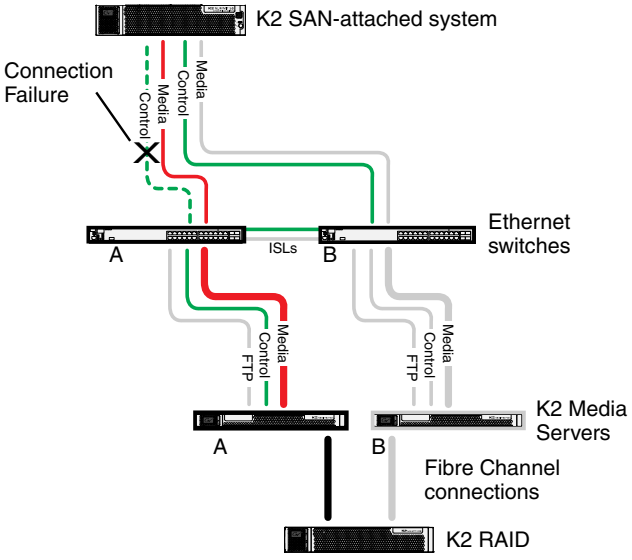
The diagrams that follow are representative of a generic redundant K2 SAN. Some details, such as the number of media connections, might not be the same as your K2 SAN. These diagrams illustrate the media (iSCSI) and control paths as they interact with the redundant K2 Media Servers in their role of media file system/metadata server and iSCSI bridge. Interactions of FTP traffic and/or paths involving K2 Media Servers with other roles are not illustrated.

Pre-failover behavior



The system operates initially with both media and control traffic on GigE switch "A" and K2 Media Server "A". Media (iSCSI) traffic is using media network "A". The iSCSI adapters (TOEs) on the "A" K2 Media Server provide access to the Fibre Channel connected RAID storage. K2 Media Server "A" is the media file system/metadata server.

Control Team failover behavior



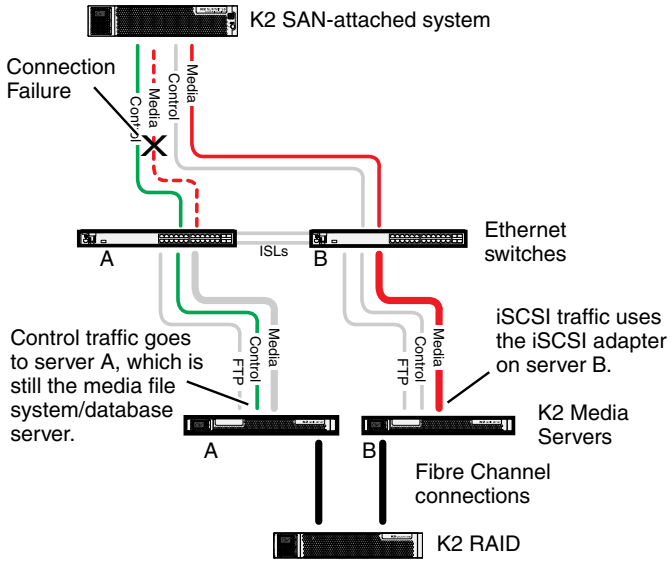
If the following system connection or component fails to respond to network communication:

- The control connection between a K2 SAN-attached system and GigE switch “A”.

Then the following failover behavior occurs:

1. The control team on the K2 SAN-attached system fails over and communication begins on the other control port.
2. The control communication finds a path through GigE “B” switch and across an ISL to GigE switch “A” to reach the same control port on the same K2 Media Server.
3. Media (iSCSI) traffic keeps using the same path.
4. K2 Media Server “A” is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.
5. The other K2 SAN-attached systems (not affected by the connection failure) keep using the same paths for media and control, as in pre-failover behavior.

K2 client media (iSCSI) connection failover behavior



If the following system connection or component fails to respond to network communication:

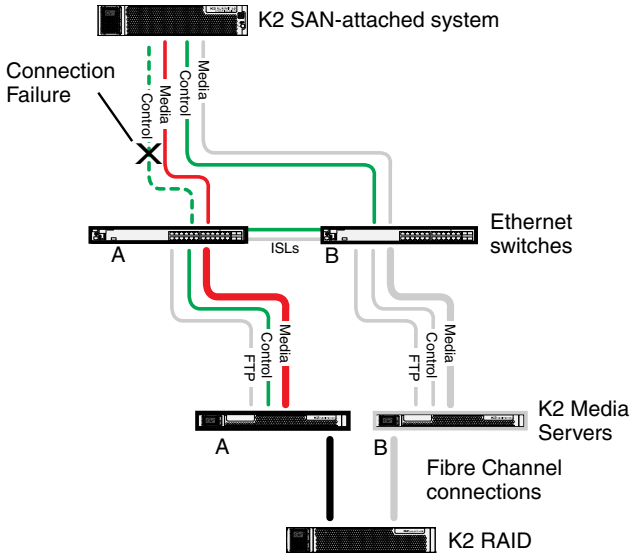
- Media (iSCSI) network “A” connection between a K2 SAN-attached system and the GigE switch

Then the following failover behavior occurs:

1. The K2 SAN-attached system drops communication on its “A” media port and begins using its “B” media port and the “B” media (iSCSI) network. The iSCSI adapter (TOE) on the “B” K2 Media Server provides access to the Fibre Channel connected RAID storage.
2. Control traffic keeps using the same path to K2 Media Server “A”.
3. K2 Media Server “A” is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.

4. The other K2 SAN-attached systems (not affected by the component failure) keep using the same paths for media and control, as in pre-failover behavior. This means the K2 SAN-attached systems unaffected by the failover are using the iSCSI adapter (TOE) on the "A" K2 Media Server to provide access to the Fibre Channel connected RAID storage, while at the same time the affected K2 SAN-attached systems are using the iSCSI adapter (TOE) on the "B" K2 Media Server to provide access to the Fibre Channel connected RAID storage. In this case both RAID controller are simultaneously providing disk access.

Control Team failover behavior



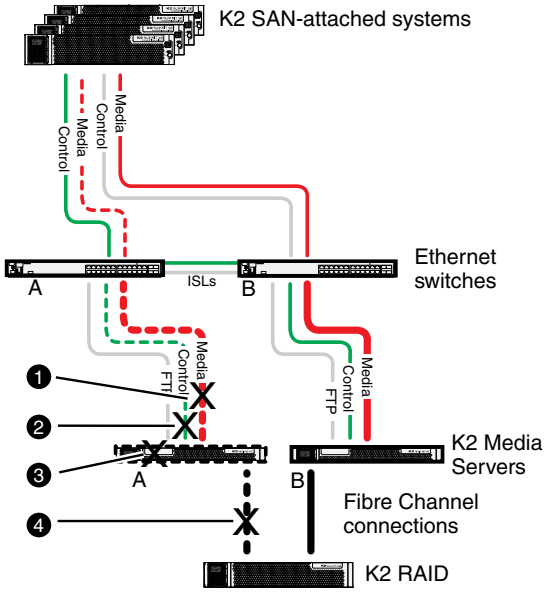
If the following system connection or component fails to respond to network communication:

- The control connection between a K2 SAN-attached system and GigE switch "A".

Then the following failover behavior occurs:

1. The control team on the K2 SAN-attached system fails over and communication begins on the other control port.
2. The control communication finds a path through GigE "B" switch and across an ISL to GigE switch "A" to reach the same control port on the same K2 Media Server.
3. Media (iSCSI) traffic keeps using the same path.
4. K2 Media Server "A" is still the media file system/metadata server. The media file system (SNFS) and media database do not fail over.
5. The other K2 SAN-attached systems (not affected by the connection failure) keep using the same paths for media and control, as in pre-failover behavior.

K2 Media Server failover behavior



If the following system connection or component fails to respond to network communication:

❶ Either of the Media (iSCSI) network “A” connections between the GigE switch and the K2 Media Server

❷ The control connection between GigE switch “A” and K2 Media Server “A”

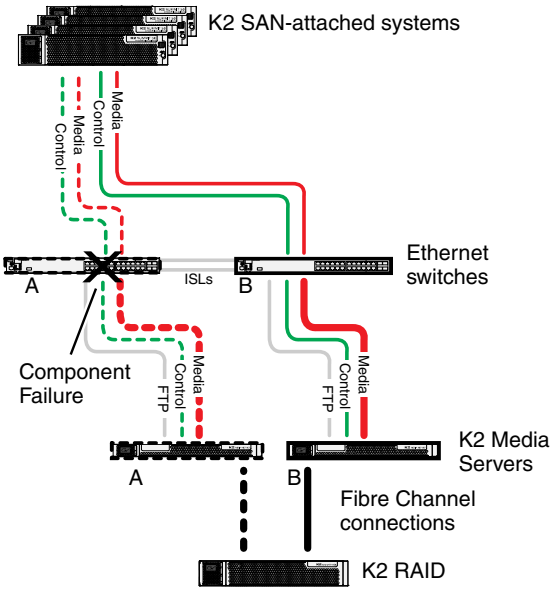
❸ K2 Media Server “A”

❹ The Fibre Channel connection between K2 Media Server “A” and RAID controller “A”

Then the following failover behavior occurs:

1. The media file system (SNFS) and media database on K2 Media Server “A” fail over and K2 Media Server “B” becomes the active media file system/metadata server.
2. All K2 SAN-attached systems drop communication on the “A” media port and begin using the “B” media port, finding a path through GigE switch “B” to K2 Media Server “B”. All K2 SAN-attached systems use an iSCSI adapter (TOE) on the “B” K2 Media Server to provide access to the Fibre Channel connected RAID storage.
3. All K2 SAN-attached systems keep communicating on the same control port, finding a new path through GigE switch “A” and across an ISL to GigE switch “B” to reach K2 Media Server “B”.

K2 Media Server failover with Control team failover behavior



If the following system connection or component fails to respond to network communication:

- The “A” GigE switch

Then the following failover behavior occurs:

1. The media file system (SNFS) and media database on K2 Media Server “A” fail over and K2 Media Server “B” becomes the active media file system/metadata server.
2. All K2 SAN-attached systems drop communication on the “A” media port and begin using the “B” media port, finding a path through GigE switch “B” to K2 Media Server “B”. All K2 SAN-attached systems use an iSCSI adapter (TOE) on the “B” K2 Media Server to provide access to the Fibre Channel connected RAID storage.
3. For all K2 SAN-attached systems, communication fails on the control port, so the control team fails over and communication begins on the other control port.
4. For all K2 SAN-attached systems, control communication finds a path through GigE switch “B” to K2 Media Server “B”.

Chapter 10

Description of K2 SAN Devices

This section contains the following topics:

- *Device terminology*
- *Control point PC description*
- *K2 Ethernet switch description*
- *K2 Media Server description*
- *NH K2 Media Server*
- *K2 RAID storage description*

Device terminology

K2 Media Client

The K2 product originally released with version 3.x K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

First generation K2 Summit system

The K2 Summit Production Client product originally release with version 7.x K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

K2 Summit 3G system

The K2 Summit 3G Production Client product originally release with version 8.1 K2 software. It can have internal storage, direct-connect storage, or shared (SAN) storage.

K2 client

Either a K2 Media Client or a K2 Summit Production Client. This term is used for K2 clients with internal storage, direct-connect storage, or shared (SAN) storage.

K2 SAN client

A device that is an iSCSI or Fibre Channel client to the K2 SAN.

Control point PC description

A control point PC runs applications from which you operate, configure, and monitor the K2 SAN. You can have one or more PCs that provide control point functionality. You must have at least one control point PC on which you install and run the K2Config application.

The primary applications that run on a control point PC are as follows:

- The K2 System Configuration application
- SiteConfig
- Storage Utility
- AppCenter
- NetCentral

In addition, you can use the control point PC for the following applications:

- QuickTime
- Adobe Acrobat Reader
- Windows Remote Desktop Connection

You can purchase a control point PC from Grass Valley. In this case the PC has all the above software pre-installed at the factory. When you receive the PC it is ready to install on the K2 SAN control network and begin using with minimal configuration.

You can also build your own control point PC by installing and configuring software on an existing PC. Refer to the *K2 System Guide* for specifications and instructions.

Related Topics

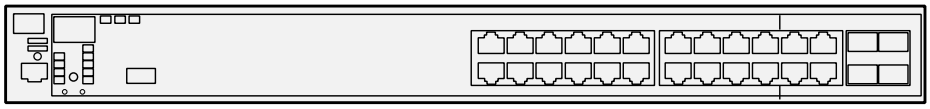
Overview of K2 Storage Tools on page 263

K2 Ethernet switch description

The K2 Ethernet switch provides the primary network fabric of the K2 SAN. The switch supports Gigabit Ethernet connections, which provides the bandwidth required for the iSCSI media traffic.

The HP ProCurve switch is qualified as the K2 Ethernet switch.

The 2900 and 2910 series switch is qualified for all K2 SANs. This section provides information on the 2900 and 2910 series switch.



The HP ProCurve switch is a store-and-forward device offering low latency for high-speed networking. In addition, the switch offers full network management capabilities.

You must use the HP ProCurve switch for iSCSI traffic. You can use a Cisco switch, such as the Cisco Catalyst 3750 Gigabit Ethernet switch, for control and FTP/streaming traffic, if required by your site.

Refer to the manuals that you receive with the switch for more information.

K2 Ethernet switch specifications

The K2 Ethernet switch is a HP ProCurve switch, with specifications as follows:

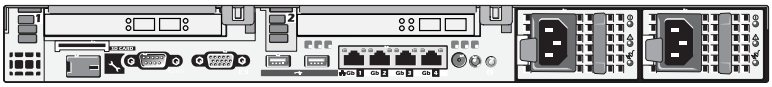
ProCurve switch 2910al-24G

Characteristic	Specification
Ports	20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T) 2 SFP+ 10-GbE ports 1 RS-232C DB-9 console port 4 dual-personality ports
Dimensions	14.4(d) x 17.4(w) x 1.73(h) in. (36.58 x 44.2 x 4.4 cm) (1U height)
Weight	10.92 lb. (4.95 kg)
Voltage	100-127 / 200-240 VAC

Characteristic	Specification
Power consumption	Idle power: 49 W; Maximum power rating: 82 W
Temperature	Operating: 32ºF to 131ºF (0ºC to 55ºC); Non-operating: -40ºF to 158ºF (-40ºC to 70ºC)
Relative humidity: (non-condensing)	Operating: 15% to 95% @ 104ºF (40ºC) 15% to 95% @ 149ºF (65ºC)
Maximum altitude	Up to 10,000 ft. (3 km)

K2 Media Server description

The central component of the K2 SAN is the K2 Media Server. The Dell PowerEdge R610 is qualified as the platform for the K2 Media Server.



The following interfaces provide K2 SAN functionality:

- Two GigE ports on the motherboard. The R610 has four GigE ports, but only two are used.
- One iSCSI interface card. A port on this card is also referred to as a TOE (TCP/IP Offload Engine).
- One Fibre Channel card.

K2 Media Server specifications

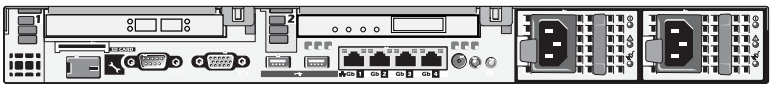
The K2 Media Server is built on a Dell PowerEdge R610 server platform. Specifications that are unique to it purpose as a K2 Media Server are listed in the following table. For a complete list of specifications, refer to Dell documentation.

Dell R610 PowerEdge server

Characteristic	Specification
Operating System	Microsoft® Windows® Server 2008 R2
Fibre Channel Adapter	ATTO Celerity FC-81ENSingle-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter
iSCSI Adapter	QLogic QLE8240 Single Port 10-Gbps iSCSI TOE to PCI Express HBA
Communications	Two dual port embedded Broadcom NetXtreme II 5709c Gigabit Ethernet NIC
Form Factor	1U

NH K2 Media Server

The NH K2 Media Server is an optional server. The Dell PowerEdge R610 is qualified as the platform for the NH K2 Media Server.



The NH K2 Media Server provides 10 Gig FTP bandwidth. The following interfaces provide K2 SAN functionality:

- One GigE port on the motherboard. The R610 has four GigE ports, but the additional ports are not used.
- One 10 Gig port.
- One Fibre Channel card.

NH K2 Media Server specifications

The NH K2 Media Server is built on a Dell PowerEdge R610 server platform. Specifications that are unique to it purpose as a K2 Media Server are listed in the following table. For a complete list of specifications, refer to Dell documentation.

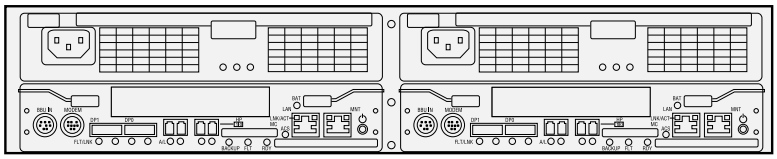
Dell R610 PowerEdge server

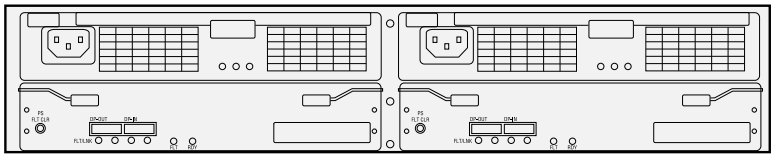
Characteristic	Specification
Operating System	Microsoft® Windows® Server 2003, Standard Edition
Fibre Channel Adapter	ATTO Celerity FC-81ENSingle-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter for online systems ATTO Celerity FC-82EN Dual-Channel 8Gb/s Fibre Channel PCIe 2.0 Host Adapter for nearline systems.
Communications	Two dual port embedded Broadcom NetXtreme II 5709c Gigabit Ethernet NIC Intel® Single-port 10 Gigabit SFP+ Ethernet Server Adapter x520
Form Factor	1U

K2 RAID storage description

This section refers to K2 10G RAID storage devices.

The K2 RAID storage device is a high performance, high availability mass storage system. The RAID chassis 8Gb/s host interface supports industry standard Fibre Channel technology. K2 RAID is available with either SAS drives for online storage or SATA drives for nearline storage.





The RAID Expansion Chassis provides additional storage capacity. The Expansion Chassis has two Expansion Adapters installed.

Refer to the installation chapters earlier in this manual for connection and configuration instructions.

The K2 RAID is NEC model D4-30 with D4 controller(s). For specifications and servicing information, refer to the *K2 RAID Storage Instruction Manual*.

Chapter 11

Overview of K2 Storage Tools

This section contains the following topics:

- *About SiteConfig*
- *K2Config*
- *Server Control Panel*
- *Storage Utility for K2 SAN*
- *NetCentral*
- *Windows Remote Desktop Connection*

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

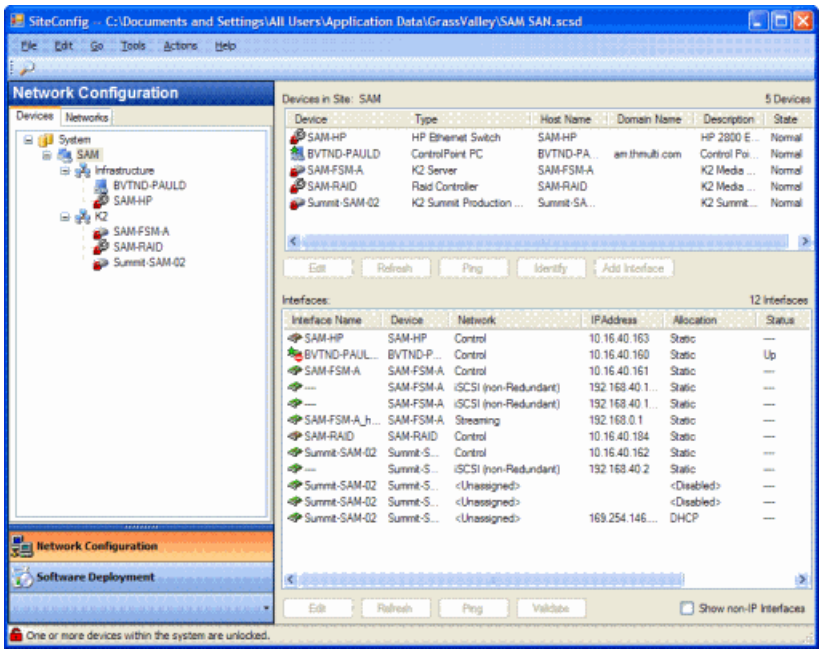
SiteConfig displays information from a system description file, which is an XML file.

Opening SiteConfig

1. Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

SiteConfig main window

The SiteConfig main window is as follows:



The left side of the screen shows the tree view of the currently loaded system description. The Network Configuration and Software Deployment buttons at the bottom of the tree view activate either the network configuration workspace or the software deployment workspace.

The network configuration workspace on the left has two tabs: a Devices tab to display the tree of devices in the system and a Networks tab to show the hierarchy of networks defined in the system.

The software deployment workspace also has two tabs: a Devices tab that displays the same tree view of devices but provides information about the software roles assigned to the devices and the software currently installed on devices. The Deployment Groups tab provides the interface to manage software deployment tasks.

Select an item in the tree and the view on the right side of the screen shows details about the item selected. Select a site or group to show information about all the items that fall under the selected item.

Right-click an item to access a context menu of operations.

Icon overlays on items and tooltips provide status and warning feedback.

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you

can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch's web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

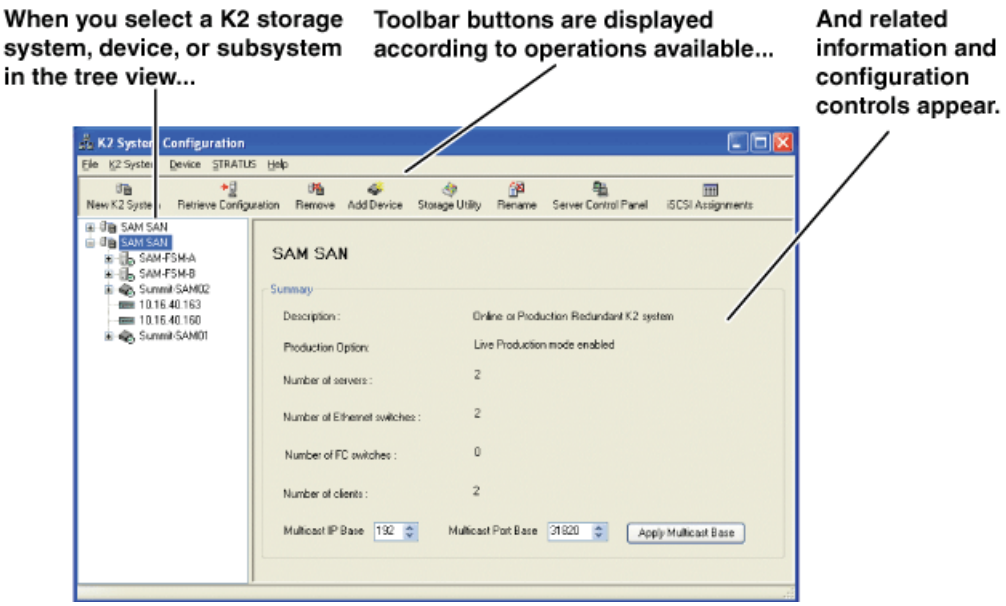
Related Topics

Accessing a K2 SAN from multiple PCs on page 278

Opening the K2Config application

1. On the control point PC open the K2Config application shortcut on the desktop. The K2Config application log in dialog box opens.
2. Log in using the designated administrator account for configuring K2 SAN devices.

3. The K2Config application opens.



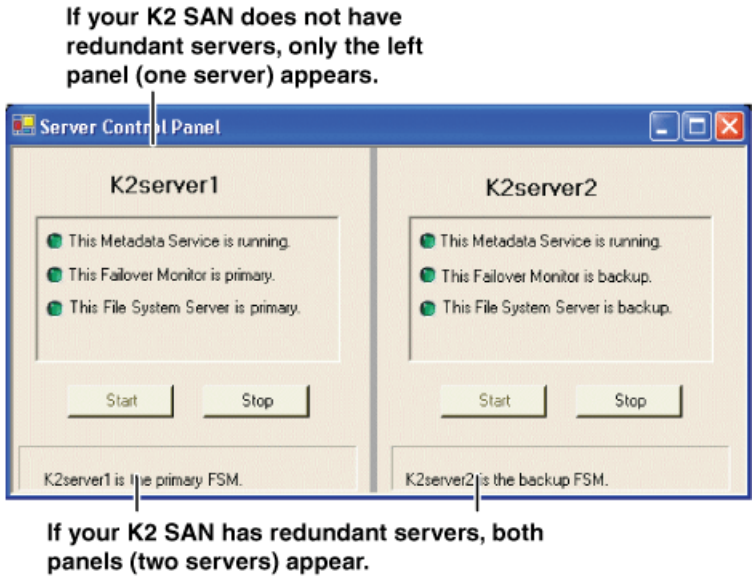
If you have one or more K2 SANs currently configured, the K2Config application displays the systems in the tree view.

If you have not yet configured a K2 SAN, the K2Config application opens with the tree view blank.

Server Control Panel

Server Control Panel allows you to monitor and control the current status of a K2 Media Server in its roles as the media file system server and the metadata server. This is especially useful for redundant K2 SANs, as you must know if a server is currently acting as primary or as backup before attempting any troubleshooting or service work.

Server Control Panel displays information about the metadata service and the media file system server primary/redundant roles.



NOTE: Do not click Stop or Start unless you intend to manually control the current primary/redundant roles. Using these buttons can trigger an automatic system recovery (failover) event.

To launch Server Control Panel, in the K2Config application, click the **Server Control Panel** button.

On the local K2 Media Server, you must log in with administrator-level privileges in order to use Server Control Panel.

Storage Utility for K2 SAN

There are two versions of Storage Utility:

- Storage Utility for the K2 SAN
- Storage Utility for stand-alone K2 systems

This section explains Storage Utility for the K2 SAN. Refer to the *K2 System Guide* to learn about Storage Utility for stand-alone K2 Summit/Solo system.

NOTE: For shared storage, run Storage Utility only via the* K2Config *application.

The Storage Utility is your primary access to the media file system, the media database, and media disks of the K2 SAN for configuration, maintenance, and repair. It is launched from the K2Config application.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

The Storage Utility's primary functionality is hosted by the K2 Media Server. The Storage Utility uses the Fibre Channel connection between the K2 Media Server and the RAID storage device for access and configuration. When you launch Storage Utility from the K2Config application on the control point PC, you use a Storage Utility remote interface to control the main application as it runs on the K2 Media Server.

The Storage Utility requires that the storage system be in an offline operating mode before it allows any configuration to take place. Take your K2 SAN devices offline before configuring with Storage Utility. This means all media access operations are disabled while you are using the Storage Utility.

NOTE: Do not run Storage Utility as a stand-alone application, separate from the* K2Config *application. To maintain a valid K2 SAN all configuration must be controlled and tracked through the* K2Config *application.

NOTE: Do not use the MegaRAID utility on a K2 system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

About RANKs and LUNs in Storage Utility

With Storage Utility you bind disks into a group. This group is a logical unit recognized by the Windows operating system, the media file system, and other software.

Storage Utility for K2 SAN labels this group of disks a RANK. This is different than previous versions of Storage Utility for K2 SAN which labeled the group of disks a LUN. In contrast, Storage Utility for stand-alone K2 storage still labels the group of disks a LUN.

This name change is necessary because the maximum disk size recognized by some Windows operating systems is relatively low, and in a K2 SAN with large capacity disks, a group of disks can exceed this maximum size. To solve the problem, Storage Utility binds disks as smaller size LUNs which can be recognized by the Windows operating system as a logical disk. Then multiple LUNs are combined into a RANK, as required to support the K2 SAN.

In Storage Utility, there is no operational difference between what is currently labeled a RANK and what was previously labeled a LUN. The tasks you perform are identical. However, Storage Utility reports the number of LUNs in each RANK, which is useful information if you need to view disks from Windows operating system administrative tools.

Storage Utility binds LUNs per RANK as follows:

Drives	RAID 5	RAID 6
500 GB 7.2K	2 LUNs/RANK	1 LUN/RANK
600 GB 15K	4 LUNs/RANK	4 LUNs/RANK
1 TB 7.2K	4 LUNS/RANK	2 LUNS/RANK

NetCentral

NetCentral is Grass Valley's monitoring application. The NetCentral server component runs on a NetCentral server PC, which could also be a K2 system control point PC. Devices report status,

primarily via Simple Network Management Protocol (SNMP), to NetCentral on the NetCentral server PC.

Refer to NetCentral manuals get the NetCentral system installed and operating. You must install a NetCentral device provider on the NetCentral server PC for each type of device you are monitoring.

Take the following into consideration when monitoring K2 systems with NetCentral:

- NetCentral is optional if you are using a standalone K2 system only. NetCentral is required if you are using a K2 SAN.

Windows Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.

Accessing Remote Desktop Connection

1. Do one of the following:
   - Click the **Start** button on the Windows task bar
   - Press the Windows key on the keyboard.
2. Select **Programs | Accessories | Communications | Remote Desktop Connection**.

   The Remote Desktop dialog box opens.
3. Enter the name or IP address of the system to which you are making the remote connection and click **Connect**.

Chapter 12

Administering and maintaining the K2 SAN

This section contains the following topics:

- *Passwords and security on Grass Valley systems*
- *Modifying K2 SAN settings*
- *Managing redundancy on a K2 SAN*
- *Working with K2 Media Servers*
- *Working with K2 clients*
- *Using Storage Utility*
- *Working on the media file system and database*
- *Working with RAID storage*
- *Working with Ethernet switches*

Passwords and security on Grass Valley systems

To provide a basic level of security, Grass Valley systems recognize three different security levels based on Windows users and groups, and the systems ship from the factory with accounts pre-configured accordingly. To access the system you must login with the username and password for one of the pre-configured accounts.

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	Grass Valley product user
Login	Administrator	GVAdmin	GVUser
Password	adminGV!	adminGV!	userGV!
AppCenter Configuration Manager	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Can't access
K2Config	Full access	Full access	Can't access
Server Control Panel	Full access	Can view	Can view
Windows Operating System	Full access	Limited access (based on Windows login privileges). Not a member of the Administrators group.	Limited access (based on Windows login privileges)

To support legacy FTP and security features, K2 systems also have *movie*, *mxfmovie*, *mpgmovie*, and *video_fs* accounts. Do not use these accounts to log in to the Windows operating system on K2 systems.

About application security on the K2 SAN

The K2Config application and the Storage Utility application both require that you be logged in to the application with administrator privileges in order to modify any settings. These privileges are based on the Windows account that you use when you log in to the K2Config application. When you open Storage Utility from within the K2Config application, the account information is passed to Storage Utility, so you do not need to log in separately to Storage Utility.

In SiteConfig you configure global and/or device-type credentials for device access. These credentials are likewise based on Windows accounts.

You must use a Windows account that has local administrator privileges on the machine to be configured. For example, when you are on a control point PC and you run the K2Config application

for the purpose of configuring a K2 Media Server, the account with which you log in to the K2Config application must be present on the K2 Media Server and must have administrator privileges on the K2 Media Server.

For initial setup and configuration, you can use the default Windows Administrator username and password to log in to applications and machines as you work on your K2 SAN. However, for ongoing security you should change the username/password and/or create unique accounts with similar privileges. When you do this, you must ensure that the accounts are present locally on all K2 SAN machines, including control point PCs, K2 Media Servers, K2 Media Clients, K2 Summit Production Clients, and other iSCSI clients.

NetCentral also has accounts for security levels, as follows:

- NetCentral Administrator
- NetCentral Technician
- NetCentral User

Grass Valley recommends mapping the NetCentral administrator with product administrator accounts for your K2 and other Grass Valley products. This allows you to log on to NetCentral as administrator using the product administrator logon. You can also assign other NetCentral groups to users, as necessary for your site's security policies. You need Windows administrator privileges to add or modify a user's privileges. For more on NetCentral security, see NetCentral documentation.

About credentials in SiteConfig

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. For known devices types, SiteConfig has a default administrator login and password. These default credential depend on the SiteConfig version, so check your SiteConfig Release Notes for any changes. When you add a device based on a known device type, SiteConfig references the default administrator login and password. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

You can choose to override the default credentials for a given device type. For example, if you have specified a different administrator account or a different password on the devices when commissioning the system, then you want SiteConfig to use these modified credentials.

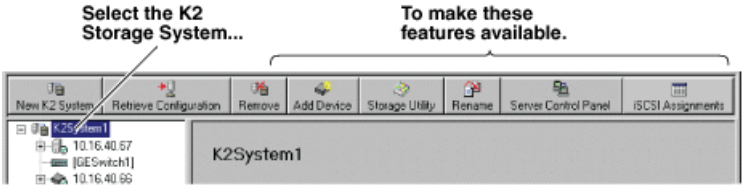
It is possible to also override the default credentials for a single device.

Modifying K2 SAN settings

Use the topics in this section when changing or viewing settings on an existing K2 SAN. These are the settings that define the K2 SAN.

Accessing K2 SAN features

In the K2Config, use the following features to K2 SAN settings:



About SiteConfig and K2Config settings

Many settings and operations, such as network settings, adding/removing devices, and software versions, are managed by both the SiteConfig application and the K2Config application. Each application has its own XML file in which information is stored. You can keep the applications in synch by using an orderly task flow as you configure the K2 SAN.

When doing initial installation and configuration tasks, you can export/import system information from one application's XML file to the other application's XML file. You can also merge from K2Config into an existing SiteConfig system description. These export/import/merge features support a one-time process in which a system as described in the XML file of one application is imported into the XML file in the other application. The target XML must not already contain the system being imported.

When you change a setting in one application, it is not automatically updated directly in the other application. The applications do not communicate dynamically with one another. However, both applications can read settings as currently configured on the actual physical device and update their XML file accordingly. This is the method you must use to keep the applications in synch.

When you change a setting that is managed by both applications, you should change it first in SiteConfig, as a general rule. This application gives you the best context for the system as a whole and provides features to identify and verify changes. Once the change is implemented on the actual physical device, you must then open the relevant page in the K2Config application. This causes the K2Config application to refresh its settings from the device and write the change to its XML file. It also allows you to verify your change within the context of the K2Config application.

The following table summarizes operations that involve interaction between SiteConfig and K2Config.

Operation	Task flow context and policies	Additional information
Import SiteConfig system description file into K2Config	Use this operation for initial install/commission (greenfield) sites. First define the site topology using SiteConfig and complete network configuration and software deployment. Then import the SiteConfig system description into K2Config and complete the K2 SAN configuration.	This operation creates a K2 SAN in K2Config with SiteConfig defined devices. Uses the site name to check if the K2 SAN already exists. The operation will not import if the K2 SAN exists with the same name. The operation can import all sites which are K2 SANs from a single system description file in a single import step.
Import K2Config XML into SiteConfig	Use this operation when you're running SiteConfig for the first time at a site with existing K2 SANs that have already been configured with K2Config. This allows you to seed the SiteConfig system description with device information that is already in the K2Config XML file. After you have done this operation for the first time, do not do it again.	This operation creates a SiteConfig site with K2Config defined devices. The operation removes all other sites.
Merge K2Config XML into SiteConfig system description	Use this operation when you've already defined some sites using SiteConfig and you later want to bring in another K2Config defined K2 SAN that doesn't exist in SiteConfig. Do not merge a K2Config XML that you've already merged. If you do so, it is likely that SiteConfig will create a new site with the same devices.	This operation creates a SiteConfig site with K2Config defined devices but leaves existing sites as is.
Rename Site\SAN	Rename first in SiteConfig. Then rename in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove Site\SAN	Remove first in SiteConfig. Then remove in K2Config. Do not import\merge into SiteConfig or K2Config.	—
Remove device	Remove from both SiteConfig and K2Config.	—
Add device	Add in SiteConfig first, do network configuration and software deployment. Then, add in K2Config and configure using K2Config.	—
Create a new site\SAN	Use SiteConfig to create site, add devices, configure network and deploy software, then import into K2Config and configure each device	—
Change hostname	Perform hostname change using SiteConfig. Remove and re-add to K2Config. If changing the hostname of a media file system/metadata K2 Media Server, re-configure all clients on the K2 SAN using K2Config	—

Operation	Task flow context and policies	Additional information
Change IP address (except address of TOE on K2 Media Server)	Use SiteConfig for IP address changes. Then in K2Config, click on the changed device's network configuration node. This refreshes the K2Config view of IPs from the device.	—
Change IP address of TOE on K2 Media Server	For TOE IP changes and/or TOE card removal, use K2Config.	—
Modify K2 SAN redundancy - redundant to non-redundant or vice versa	Use SiteConfig to recreate the site using the appropriate redundancy models and configure network and deploy software. Remove K2 SAN from K2Config. Import site into K2Config. Configure using K2Config.	—

Renaming a K2 SAN

Prerequisites for renaming an existing K2 SAN are as follows:

- You must be logged in to the K2 System Configuration application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.

1. In the K2 System Configuration application tree view, select the current name of the K2 SAN, which is the top node of the storage system tree.
2. Click **Rename**. The Rename dialog box opens.
3. Enter the new name of the SAN and click **Apply**.
4. If the SAN name is used similarly in SiteConfig, make the appropriate change in SiteConfig.

Adding devices to a K2 SAN

Refer to the topics in this section to add devices to an existing K2 SAN.

Adding a generic client device

Prerequisites for adding a generic client to an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.

1. In SiteConfig, add the client device to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the type of client you are adding.
5. Click **OK**. The new client appears in the tree view.

6. Configure the client as appropriate. Refer to the documentation for the device.

   Enter the RVIO value as provided by Grass Valley. Do not attempt to calculate the RVIO value on your own.

   When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.

Adding an Ethernet switch

Prerequisites for adding a Gigabit Ethernet switch to an existing K2 SAN are as follows:

- You must be logged in to the K2 System Configuration application with permissions equivalent to K2 administrator or higher.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.

1. In SiteConfig, add the switch to the appropriate group.
2. In the K2 System Configuration application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select **Ethernet Switch**.
5. Click **OK**. The new switch appears in the tree view.
6. Configure the switch as appropriate.

Adding a K2 Media Server

With online and production K2 SANs, the K2Config application enforces the number of K2 Media Servers, as pre-defined for the system. The application does not allow you to add K2 Media Servers. Refer to the installation chapter for each type of SAN for more information.

For all system levels and designs, adding a K2 Media Server with the role of media file system/metadata server to an existing K2 SAN is not supported as a customer procedure. Adding a server with these roles fundamentally changes the baseline design of the system, which means you must dismantle one or more pieces of the existing system and create a new system. This requires custom design and implementation services that should only be attempted by qualified Grass Valley personnel.

On some K2 SANs, the system design supports adding an optional NH K2 Media Server, as follows:

1. If you have not already done so, in SiteConfig, add the server to the appropriate group and verify that it is communicating correctly on networks.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select **K2 Media Server**.
5. Click **OK**. The new server appears in the tree view.

Next, configure the server as instructed in the installation chapter for the level of the K2 SAN.

Related Topics

Replacing a K2 Media Server on page 293

Removing a K2 SAN

Prerequisites for removing a K2 SAN from the K2Config application and/or the SiteConfig application are as follows:

- You must be logged in to the K2Config application with permissions equivalent to GV administrator or higher.
- The K2 SAN can continue operations while it is removed from the K2Config application. As long as you are removing only the complete K2 SAN and not removing any individual devices, there is no need to put devices offline or restart devices.
- For ongoing maintenance and support, you must always have at least one control point from which you can access the K2 SAN with the SiteConfig application and with the K2Config application. If you have installations of these applications on multiple control point PCs, do not remove the K2 SAN from all control point PCs at the same time.

1. In the SiteConfig application, remove the devices of the K2 SAN.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Remove**. The SAN is removed from the tree view.

Accessing a K2 SAN from multiple PCs

It is recommended that you install the SiteConfig application and the K2 System Configuration (K2Config) application on one PC only in your facility. This eliminates potential problems in the installation, configuration, and maintenance of your K2 SAN.

If you run SiteConfig and/or the K2Config application on multiple PCs in your facility, you must enforce an operational policy whereby you constrain your use of the applications as follows:

- Designate a control point PC as the configuration PC and then make changes from that PC only.
- On the other control point PCs, limit operations to view-only when accessing the K2 SAN. Do not make changes. With the K2Config application there is some basic protection, in that the first instance of the application in essence “locks out” any other instances. However, SiteConfig has no such protection and making changes on devices from multiple SiteConfig instances can result in configuration and software deployment errors.

SiteConfig has no features that are designed to support access from multiple instances. If you access systems from multiple instances of SiteConfig, you must define and enforce your own policy. For example, you can import system descriptions or otherwise create systems and discover devices in each instance of SiteConfig and then enforce policy whereby instances are kept in synch.

1. Install Control Point software on the designated K2Config control point PC and complete the initial system configuration. Close the K2Config application on that PC.
2. Install Control Point software on another control point PC and open the K2Config application.

3. Select **Retrieve Configuration** and enter the name or IP address of the K2 Media Server for the K2 SAN. If the K2 SAN has multiple K2 Media Servers, you must enter the name or IP address of the server configured first.

   If there is another instance of the K2Config application on a different control point PC currently accessing the K2 SAN, a message informs you of this and you are not allowed to access the system.

   If access is allowed, a Retrieving Configuration message box shows progress. It can take over 30 seconds to retrieve the configuration. When the configuration is retrieved, the K2 SAN appears in the tree view. Make sure that you only attempt view-only operations from this PC. Do not configure the K2 SAN from this PC.

4. Repeat the previous steps for other control point PCs from which you need access to the K2 SAN.

When you expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings, the K2Config application displays information as found in a configuration file, rather than continuously polling devices to get their latest information. The configuration file is saved on the V: drive, along with the media files in the shared storage system. When you use the Retrieve Configuration feature, you are connecting to the configuration file.

Taking a K2 SAN offline

1. Stop all media access.
2. Shut down all K2 clients and all generic clients. You can do this via SiteConfig.
3. Take all K2 Media Servers out of service.

   If you have redundant servers, make sure that you know which server is the current primary and which server is the current backup, and that you take primary/backup servers out of service in the proper order.

Related Topics

Taking a K2 Media Server out of service on page 285

Bringing a K2 SAN online

1. Verify that RAID storage devices, Ethernet switches, and other supporting system are powered up. Refer to the section earlier in this manual for power on procedures.
2. If K2 Media Servers are powered down, power them up. Refer to the section earlier in this manual for power on procedures.
3. Place K2 Media servers in service.

   If you have redundant servers, make sure that you place primary/backup servers in service in the proper order.

4. Power on all K2 clients and all generic clients.

Related Topics

Placing a K2 Media Server in service on page 287

Viewing iSCSI assignments

You can review a report of clients and their iSCSI configuration on a K2 SAN as follows:

1. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
2. Click **iSCSI Assignments**.

   The iSCSI Port Assignments report opens.

   The report displays the following information.

   - K2 Media Servers with the role of iSCSI bridge
   - Each server's iSCSI ports, identified by IP address
   - For each iSCSI port, the iSCSI clients assigned and their bandwidth subscription.

Using reference files

When you create a simple K2 clip on a K2 system, K2 software can create a corresponding reference file. The reference file is stored in a directory in the clip's folder on the V: drive. You can configure the software to create QuickTime reference files, MXF reference files, or no reference files. The following topics provide information about reference files on K2 systems.

About QuickTime reference files

For QuickTime reference files, the K2 clip must be a DV, AVC-Intra, XDCAM-EX, XDCAM-HD, XDCAM-HD 422, or IMX format simple clip in order to create the reference file. With the QuickTime reference file you can open the K2 clip with QuickTime tools, such as Final Cut Pro, for playback and editing. The QuickTime tool must be run on another system. Running the QuickTime player or other QuickTime tools on the K2 system is not supported. You have options for connections, access, and software to support your workflow requirements.

About MXF reference files

For MXF reference files, the K2 clip can be any supported format simple clip. K2 software creates the MXF reference file when you create a new simple clip by recording, importing, or copying. K2 software does not create the MXF reference file when you create a playlist, a program with continuous-recorded material, or a clip with tracks having a duration less than the clip duration. The reference file is a MXF OP1b file with external essence. The reference file gives you options for connections, access, and software to support your workflow requirements.

Configuring reference file type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of file system server, access the File System Server Configuration page as follows:

   - On a SAN that is already configured, in the tree view click **File System Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the File System Server Configuration page.

2. On the File System Server Configuration page select one of the following:
   - No reference file — K2 software does not create reference files.
   - QuickTime reference file — K2 software creates QuickTime reference files.
   - MXF reference file — K2 software creates MXF reference files.
3. Click **Check** to apply the setting.
4. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

If a redundant K2 SAN, you must configure similarly and restart both K2 Media Servers with role of file system server.

Managing redundancy on a K2 SAN

If you have a redundant K2 SAN, use the procedures in this section to control the primary/redundant roles of the K2 Media Servers.

Identifying current primary/backup K2 Media Servers

Before attempting any configuration or service work on a redundant K2 Media Server, you must know if the server is the current primary server or the current backup server for the media file system and the metadata service. While most configuration and service work can be accomplished on a backup server without affecting the operation of the SAN, if you attempt configuration or service work on the operating primary server, it will likely result in record/play failures and/or a loss of media.

To identify the current primary/backup K2 Media Server, use one or more of the methods described in the following procedures.

Identifying primary/backup from NetCentral

While monitoring the K2 Media Server in NetCentral, do the following:

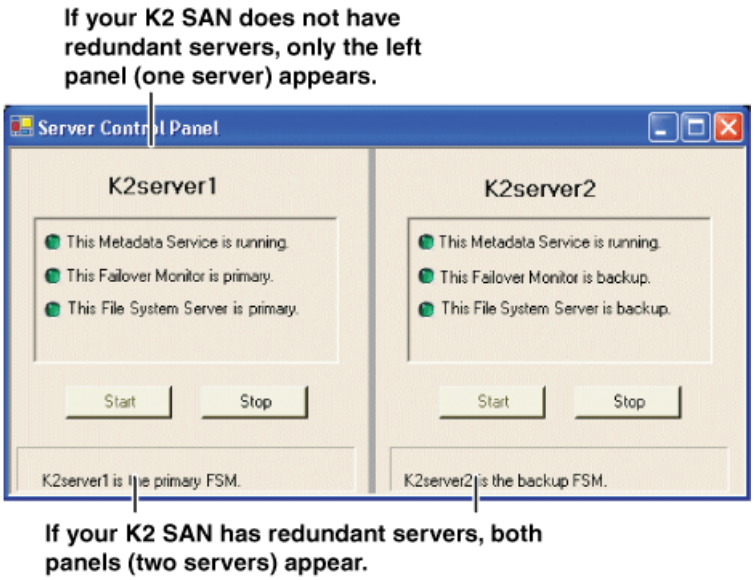
1. In the NetCentral tree view, select the K2 Media Server.
2. Click the **Facility** view control button
3. Open the **Roles** subsystem
4. Click the **Media Database Server** or **Metadata Server** link.

   The Media Database Server dialog box opens and reports the Failover Mode as either Primary or Backup.

Identifying primary/backup from the K2Config application

1. In the tree view, select the name of the K2 SAN, which is the top node of the storage system tree.

2. Click the **Server Control Panel** button. The Server Control Panel opens.



3. Identify the primary K2 Media Server and the backup K2 Media Server.

   If the K2 SAN does not have redundant servers, only one server (the left half of the Server Control Panel) is displayed.

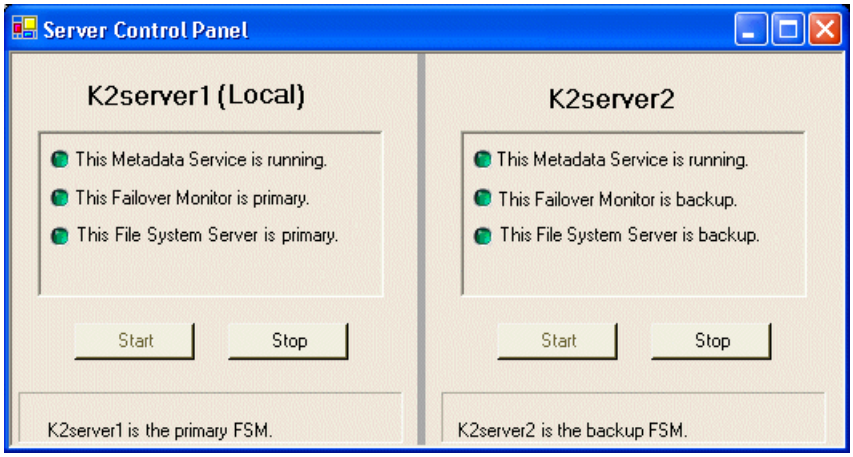
   For Nearline K2 SANs, the Server Control Panel is not available from the K2Config application.

Identifying primary/backup from the local K2 Media Server

The following procedure assumes that you are at the local K2 Media Server and you need to check its status in its role of media file system/metadata server, especially regarding redundancy. The recommended mode for local operation of a K2 Media Server is to use a connected keyboard, monitor, and mouse. You can also use Windows Remote Desktop Connection from a network-connected PC to access the Windows desktop for "local" operation, but this is not recommended if the system is currently online with media access underway. The additional load on network and local system resources could cause unpredictable results.

1. If you have not already done so, connect keyboard, monitor, and mouse to the K2 Media Server and log on to Windows.
2. If Server Control Panel is not already open, on the Windows desktop, click **Start | Grass Valley | Server Control Panel**.

3. Log on to Server Control panel with administrator-level permissions. The Server Control Panel opens.



4. Determine if the local machine is currently the primary K2 Media Server or the backup K2 Media Server.

   If the K2 SAN does not have redundant servers, only one server (the left half of the Server Control Panel) is displayed.

   For the K2 Media Servers of a Nearline K2 SAN, Server Control Panel on the local K2 Media Server reports if the server is the current active media file system (SNFS) server. No metadata information is displayed, since the Nearline system does not have a media database.

Triggering an intentional failover

⚠ ***WARNING: Do not attempt this procedure except under the supervision of qualified Grass Valley personnel.***

The following procedure renders the primary K2 Media Server unqualified to carry out its role in managing the K2 SAN. The backup K2 Media Server detects this condition and triggers a failover in which it takes the primary server out of service and takes control of the K2 SAN. Therefore, before using these procedures, verify that the backup K2 Media Server is fully operational and qualified to take control of the K2 SAN. Be aware that the failover capabilities of the -K2 SAN are degraded until you place the machine back into service as the backup K2 Media Server.

You should stop all media access before attempting this procedure. If media access is underway, there will be period of time in which media loss will occur.

In the following procedures, K2server1 and K2server2 represent your redundant K2 Media Servers. The procedure begins with K2server1 acting as the primary K2 Media Server.

1. Verify primary/backup roles and make sure K2server2 (the backup) is qualified and ready to become primary.
2. From the K2Config application, open **Server Control Panel**.
3. In Server Control Panel for K2server1 click **Stop**. This triggers the failover process.

   K2server1 shuts down. K2server2 detects (via the absence of the heartbeat signal on the serial cable) that K2server1 is gone, so K2server2 takes over as primary.

4. Allow the failover process to complete, until K2server2 is operating correctly in its new role as the primary K2 Media Server for the K2 SAN.
5. Verify K2server2 as primary.
6. Start up K2server1. It is now out of service. If you need to do service work on K2server1, you can do it now. After your work is complete, proceed with the next step.
7. If there are K2 Media Servers with role of iSCSI bridge or Fibre Channel switches on the same redundant "side" as K2server1, start or restart them.
8. In Server Control Panel, for K2server1, click **Start**. This notifies K2server2 (via a heartbeat signal on the serial cable) that K2server1 is coming online as backup.
9. Verify K2server1 as backup.
10. All failover processes are complete. All media management mechanisms are now running and K2server1 is now qualified and acting as the backup.

Recovering from a failover

⚠ ***WARNING: Do not attempt this procedure except under the supervision of qualified Grass Valley personnel.***

In the following procedures, K2server1 and K2server2 represent your redundant K2 Media Servers. The procedure begins with K2server1 being the server on the failed side of the SAN. K2server2 is acting as the primary K2 Media Server.

1. Verify primary/backup roles and make sure K2server2 is the primary.
2. Start up K2server1. It is now out of service.
3. Determine the cause of the failover and take corrective action as necessary. If you need to do service work on K2server1 or other devices on the failed side of the SAN, you can do it now. After your work is complete, proceed with the next step.
4. If there are K2 Media Servers with role of iSCSI bridge, Ethernet switches, or Fibre Channel switches on the same redundant "side" as K2server1, start or restart them. Make sure they have been started up at least once before putting K2server1 into service.
5. In Server Control Panel, for K2server1, click **Start**. This notifies K2server2 (via a heartbeat signal on the serial cable) that K2server1 is coming online as backup.
6. Verify K2server1 as backup.
7. All failover processes are complete. All media management mechanisms are now running and K2server1 is now qualified and acting as the backup.

Related Topics

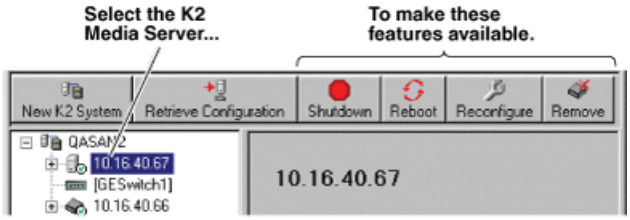
Powering on the K2 SAN on page 245

Working with K2 Media Servers

Use the procedures in this section when doing configuration or service work on a K2 Media Server that is part of an operational K2 SAN.

Accessing K2 Media Server features in the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a K2 Media Server are as follows:



Taking a K2 Media Server out of service

This procedure applies to K2 Media Servers that are taking the role of media file system and metadata server.

When you take a K2 Media Server out of service you stop services such that the K2 Media Server is prevented from functioning as a media file system and/or metadata server. In this state no media operations can take place.

If there is just one K2 Media Server in the role of media file system and metadata server, before you take the K2 Media Server out of service, you should stop all media access on the K2 SAN.

If there are redundant K2 Media Servers currently in service (both primary and backup) in the role of media file system and metadata server, take only the backup out of service. Do not take the primary out of service. If you take the primary out of service it will trigger a failover event. If the K2 Media Server that you want to take out of service is currently the primary, you have the following options:

- Make the current primary K2 Media Server the backup in an orderly fashion by triggering an intentional failover. Then, when the K2 Media Server is the backup, you can take it out of service.
- Take the current backup out of service (shutdown) so that the primary K2 Media Server is the only file system/metadata server currently in service. You can then take the primary K2 Media Server out of service without triggering a failover event.

1. Stop all media access on the K2 SAN.
2. In the K2Config application tree view, select the K2 SAN.
3. Select **Server Control Panel**. The Server Control Panel opens.
4. Identify the K2 Media Server you intend to take out of service. If there are redundant K2 Media Servers, consider that you might trigger a failover event.

   Use the Stop button in Server Control Panel as appropriate for the action that you want to take.
5. When you are sure that you understand the implications of taking the K2 Media Server out of service, click the **Stop** button for that server.

6. Proceed as follows:
   - If the server shuts down automatically, allow the shutdown processes to complete. Then start the server. When a redundant server restarts, it comes up in an out of service state.
   - If the server continues to run, it is in an out of service state.

Related Topics

Triggering an intentional failover on page 283
Using the Stop button in Server Control Panel on page 286

Using the Stop button in Server Control Panel

In Server Control Panel, the following behaviors occur when using the Stop button.

On a system with this configuration of media file system/metadata K2 Media Servers…	With server(s) in this state…	When you click the Stop button on this server…	The following behavior occurs.
Redundant servers	Both primary and backup are in service (online)	Primary	The server automatically powers itself down. This causes a failover event to occur and the backup server becomes primary. When you restart the former primary server, it comes up out of service.
		Backup	The server automatically powers itself down. When you restart the server, it comes up out of service.
Redundant servers	Only the primary is in service. The other server is either shut down or it is powered on but out of service.	Primary	The media file system services stop, but the server continues to run. It does not automatically shut down. The server is now out of service.
One (non-redundant) server	The server is in service	Primary (the only server)	The media file system services stop, but the server continues to run. It does not automatically shut down. The server is now out of service.

For Nearline K2 SANs, the Server Control Panel is not available from the K2Config application.

Placing a K2 Media Server in service

This procedure applies to K2 Media Servers that have the role of media file system and metadata server.

When you put a K2 Media Server in service it is capable of taking the role of media file system and metadata server.

1. In the K2 System Configuration application tree view, select the K2 SAN.
2. Select **Server Control Panel**. The Server Control Panel opens.
3. For the K2 Media Server that you want to place in service, click the **Start** button.

Shutting down or restarting a K2 Media Server

- To shut down or restart a K2 Media server that is in the role of media file system and metadata server, first put the server out of service, as explained in the procedures earlier in this section. Then you can shut down or restart the K2 Media Server.
- To shut down or restart a K2 Media server that is not in the role of media file system and metadata server, consider that the K2 Media Server can host the iSCSI interface adapters (TOEs) by which clients access the shared storage. You should stop all media access before shutting down or restarting any K2 Media Server that hosts an iSCSI interface adapter.

Identifying K2 Media Server software versions

Use one or more of the following options to identify K2 Media Server software versions:

- In NetCentral, select the **Facility** button, then in the tree view open the node for the K2 Media Server. This exposes the subsystems. You can find software version information on property pages for the **Software** subsystem and the **Roles** subsystem.
- In the K2Config application tree view, open the node for the K2 Media Server. This exposes the nodes for individual configuration pages. Select the **Software** configuration page to view software version information. To check for recent changes in software, click the **Check** button.
- Use SiteConfig software deployment features.

Modifying K2 Media Server network settings

Read the following sections for considerations and procedures for modifying network settings on a K2 Media Server.

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

Modifying K2 Media Server control network settings

If the K2 Media Server takes the role of media file system and metadata server, modifying its control network settings on an existing K2 SAN is not supported as a customer procedure. This is because the network identity of the K2 Media Server is embedded throughout the K2 SAN. To reconfigure

this network identity, you must reconfigure the entire system from the start. Contact your Grass Valley representative for assistance.

Modifying K2 Media Server FTP network settings

You can modify the FTP network settings using SiteConfig without directly affecting the media file system or metadata service. However, you must be aware of the requirements of your site's FTP, file transfer, and streaming system design, as the FTP network settings will likely need to be changed elsewhere.

After modifying FTP network settings using SiteConfig, open the Network Configuration page in the K2Config application. The settings should automatically update. Verify that the settings are correct.

Modifying K2 Media Server media network settings

Use this procedure if you must change the IP address assigned to an iSCSI interface board on a K2 Media Server. This should not be necessary for a normally operating system and in fact it should be avoided if possible.

1. Put all the devices of the K2 SAN in an offline or out of service state. Refer to the appropriate procedures in this chapter.
2. Open the K2 System Configuration (K2Config) application on the control point PC.
3. In K2Config, make sure you know the load balancing bandwidth parameters for each of the iSCSI clients, as you must re-enter these values later in this procedure.
4. In K2Config, remove all iSCSI clients from the K2 SAN. To do this, select each iSCSI client and click **Remove**.
5. Use SiteConfig to change the IP address. Make sure that the IP address is within the range designated for the network.
6. Restart the K2 Media Server.
7. In the K2Config tree view, expand the node for the media server that has the iSCSI interface adapter for which you need to change the IP address and click the **iSCSI Bridge** node. The iSCSI Bridge Server configuration page opens.
8. In K2Config, identify the iSCSI adapter for which you are changing the IP address. Since you changed it in SiteConfig, K2Config should now display the new IP address.
9. In K2Config, add each iSCSI client again and reconfigure. Make sure you add them in the correct order (highest bandwidth first) and enter the same bandwidth values (load balancing) for each client as the values originally configured.
10. Place the devices of the K2 SAN back online.

Configuring Server 2008 for domain

This topic applies to Grass Valley servers with a base disk image created prior to mid-2011. Server disk images created after that time do not require this special configuration.

Systems with the Microsoft Windows Server 2008 operating system require special configuration when on a domain. A server must have its firewall disabled for proper K2 system operation. This includes the Windows firewall that is only in effect for systems on a domain. On Microsoft Windows Server 2008 servers, the domain firewall setting does not appear in any configuration dialog box

until the server is on the domain. Therefore you must do the following steps after the server is operating on the domain.

1. Log in to the server with Windows administrator privileges.
2. From the Windows desktop click **Start | Control Panel | System and Security | Windows Firewall**.
3. On the left side, click **Turn Windows Firewall on or off**.
4. Under the new **Domain network location settings**, select the **Turn off Windows Firewall setting** and then click **OK**.

Restoring network configuration

When you restore a system from its system specific image, network configuration is also restored to the factory default settings. This is the recommended method of restoring network configuration. However, if for some other reason you must configure network settings manually, use the tasks in this section to restore the default network configuration.

Identify adapters

On some systems, it is possible that the Microsoft Windows operating system has enumerated network adapter names in an unpredictable sequence. You must identify adapters by their location rather than by the enumeration assigned by the Windows operating system and verify or modify the adapter name as necessary.

1. If not already open, open Network Connections as follows:
   a) From the Windows taskbar, click **Start | Network**.
      The Network window opens.
   b) Click **Network and Sharing Center**.
      Network and Sharing Center opens.
   c) Click **Change Adapter Settings**.
      Network Connections opens.
2. Verify that there are four similarly named adapters listed, with the first adapter having no enumerator at the end its name and the other adapters enumerated #2, #3, and #4 .
   If the system has a 10 Gig network interface card installed, is also listed.

3. For each adapter shown, identify its location, as follows:
   a) Right-click one of the adapters and select **Properties**.

      The Properties dialog box opens.

   b) Click **Configure**.
   c) On the **General** tab take note of Location displayed within the parentheses.

      You must make a written record of the enumerator that the Windows operating system has assigned to this location (PCI bus X, device 0, function X). Use the table below and fill in the blanks:

On this system, Windows has assigned the adapter enumerated…	To this location:
no enumerator	PCI bus ____, device 0, function ____
#2	PCI bus ____, device 0, function ____
#3	PCI bus ____, device 0, function ____
#4	PCI bus ____, device 0, function ____

4. Repeat the previous steps until you have determined which adapter name goes to which (PCI bus X, device 0, function X) location.

Next, name adapters.

Name adapters

Before doing this task, you must know the (PCI bus X, device 0, function X) location of adapters.

1. If not already open, open Network Connections as follows:
   a) From the Windows taskbar, click **Start | Network**.

      The Network window opens.

   b) Click **Network and Sharing Center**.

      Network and Sharing Center opens.

   c) Click **Change Adapter Settings**.

      Network Connections opens.

2. In Network Connections, click **View | Details**.
3. Determine which adapter names in the Device name column are assigned to which (PCI bus X, device 0, function X) location.

4. Reconcile the locations assigned to the adapter names with the names as currently configured in the Name column as follows:

   - On systems with no 10 Gig network interface card installed, the required mapping of names to locations is specified as follows:

The adapter name (as displayed in the Device Name column) that is assigned to this location…	Must be named as follows:
PCI bus 1, device 0, function 0	Control Connection
PCI bus 1, device 0, function 1	FTP-Streaming Connection
PCI bus 2, device 0, function 0	Unused Connection 1
PCI bus 2, device 0, function 1	Unused Connection 2

   - On systems with a 10 Gig network interface card installed, the required mapping of names to locations is specified as follows:

The adapter name (as displayed in the Device Name column) that is assigned to this location…	Must be named as follows:
PCI bus 1, device 0, function 0	Control Connection
PCI bus 1, device 0, function 1	Unused Connection 0
PCI bus 2, device 0, function 0	Unused Connection 1
PCI bus 2, device 0, function 1	Unused Connection 2
PCI bus 5, device 0, function 0	FTP 10G Connection

     The 10 Gig network interface adapter must be named `FTP 10G Connection`. If it has dual-ports, name the other connection `Unused Connection 3 10G`.

5. Proceed as follows:

   - If all the names on this system are configured correctly to locations, skip the rest of this procedure.
   - If names on this system are not configured correctly to locations, for each adapter name incorrectly configured, complete the remaining steps of this procedure.

6. Select the name in the Name column.
7. Select **File | Rename** to enter rename mode.
8. Type the name required for the location.

Next, reorder adapters.

Reorder adapters

Before beginning this task, make sure of the following:

- Adapters are named correctly according to their PCI bus location
- The control team is created

- The team and loopback are named

1. If not already open, open Network Connections as follows:
   a) From the Windows taskbar, click **Start | Network**.
   The Network window opens.
   b) Click **Network and Sharing Center**.
   Network and Sharing Center opens.
   c) Click **Change Adapter Settings**.
   Network Connections opens.
2. Select **Advanced**, then **Advanced Settings...**
3. On the **Adapters and Bindings** tab, order adapters as follows:
   - On systems with no 10 Gig network interface card installed, the specified order is as follows

Control Connection
FTP-Streaming Connection
Unused Connection 1
Unused Connection 2

   - On systems with a 10 Gig network interface card installed, the specified order is as follows

Control Connection
FTP 10G Connection
Unused Connection 1
Unused Connection 2
Unused Connection 3 10G

4. Click **OK** to close and accept the changes.
5. Close Network Connections.

If continuing with network configuration, next set power management settings.

Set power management settings

1. If not already open, open Network Connections as follows:
   a) From the Windows taskbar, click **Start | Network**.
   The Network window opens.
   b) Click **Network and Sharing Center**.
   Network and Sharing Center opens.
   c) Click **Change Adapter Settings**.
   Network Connections opens.

2. Right-click one of the adapters and select **Properties**.

   The Properties dialog box opens.

3. Click **Configure**.
4. On the **Power Management** tab, uncheck all checkboxes, if they are not already unchecked.
5. On the Properties dialog box, click **OK**.
6. If a "…lose connectivity…" message opens, click **Yes**.
7. Repeat these steps on the remaining network connection in the Network Connections window.

Configure static IP address on Server 2008

This task required on systems with Microsoft Windows Server 2008 operating system only.

SiteConfig cannot discover systems with the Microsoft Windows Server 2008 operating system that have no IP address, such as those that are configured for DHCP. Therefore you must configure the system with a static IP address. You can use any IP address.

Removing a K2 Media Server

In a functioning K2 SAN, you should not permanently remove a K2 Media Server that takes the role of media file system/metadata server, as this changes system capabilities and results in the failure of some or all of the media operations for which the system was designed. Remove a K2 Media Server only under the direct supervision of qualified Grass Valley personnel.

If you are replacing a faulty server with a replacement server, follow the documented procedure.

Replacing a K2 Media Server

The requirements for replacing a K2 Media Server on an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.

Use this procedure if a K2 Media Server in a working system is faulty or otherwise needs to be replaced with a new K2 Media Server.

NOTE: If you are replacing a non-redundant media file system/metadata server, you lose all media during the replacement process.

1. If the server hosts an iSCSI interface adapter, copy down iSCSI bandwidth settings for K2 clients and other iSCSI clients that use the faulty server as their iSCSI target, as follows:
   a) In the K2Config application, select the K2 SAN in the tree view and then click the button in the toolbar to view client iSCSI assignments. A page opens that displays each client's primary and secondary iSCSI targets.
   b) In the tree view, select one of the clients that have the faulty server as a primary or secondary iSCSI target.
   c) Open the client's iSCSI Initiator Configuration page and click **Modify**. The Bandwidth Input dialog box opens.
   d) Copy down the bandwidth settings configured for that client and then close the Bandwidth Input dialog box.
   e) Repeat these steps for each client that has the faulty server as a primary or secondary iSCSI target.

2. If the server hosts an iSCSI interface adapter, in the K2 System Configuration application, for the faulty K2 Media Server, open the iSCSI bridge page and make a note of the IP addresses.
3. Copy down network and hostname settings for the faulty K2 Media Server. You can do this from SiteConfig or from the K2Config application Network Configuration page.
4. Save a copy of the host table from the faulty K2 Media Server. You can use SiteConfig hosts file features or you can find the host table at the following location on the K2 Media Server:

   C:\WINDOWS\system32\drivers\etc\hosts
5. If the server hosts an iSCSI interface adapter, in the K2Config application, remove the K2 clients and other iSCSI clients that use the faulty server as their iSCSI target, as determined earlier in this procedure.
6. Stop all media access and power down all K2 clients and other iSCSI clients.
7. If the faulty server is a media file system/metadata server, take the K2 Media Server out of service. If it is a redundant server, it must be the backup before you take it out of service.
8. In the K2Config application, remove the faulty K2 Media Server as follows:
   a) In the tree view, select the K2 Media Server
   b) Click **Remove** and **Yes** to confirm. The K2 Media Server is removed from the tree view.
9. In SiteConfig, remove the K2 Media Server.
10. Physically remove the faulty K2 Media Server and put the replacement server in its place. Reconnect all cables to the replacement server as they were to the faulty server.

    NOTE: If the replacement server was previously configured on a K2 SAN, you must restart it before adding it to a K2 SAN or in any other way reconfiguring it for use.
11. In SiteConfig, add, discover, and assign the replacement server. Configure the hostname and all network settings on the replacement server to be the same as they were on the faulty server.
12. Copy the host table onto the replacement server. You can use SiteConfig for this task.
13. In the K2Config application, add and configure the replacement server. Refer to the installation chapter for the level of your system earlier in this manual for specific procedures, with the following special instructions:
    a) Add the server to the K2 SAN, using the **Add Device** button.
    b) Configure the replacement server so that its settings are all the same as they were on the faulty server.
       - On the Define Server Roles page, assign the same roles.
       - On the Network Configuration page, verify the same network settings for the FTP network.
       - If the server hosts an iSCSI interface adapter, on the iSCSI Bridge Server Configuration page, verify the same settings.

    c) After completing the configuration, restart the machine to put changes into effect.
14. If the server hosts an iSCSI interface adapter, in the K2 System Configuration application, add the clients that you removed in step 5 earlier in this procedure, with the following special instructions:
    a) Add the client with the highest iSCSI bandwidth first.
    b) On each client, configure iSCSI bandwidth settings so they are the same as they were before.
15. Power up all K2 clients and other iSCSI clients and test media access.

The replacing a server procedure is complete.

Related Topics

Taking a K2 Media Server out of service on page 285

Replacing an iSCSI interface adapter (TOE card)

Prerequisites are as follows:

- The K2 SAN must be at K2 system software version 3.2.7 or higher before you begin this procedure.
- K2 system software version must be the same on all K2 Media Servers, before and after you replace the iSCSI interface adapter or adapters.
- If the K2 Media Server has two single-port adapters and the replacement adapter is a dual port adapter, you must remove both single-port adapters, even though only one adapter is faulty, and replace them with the dual-port adapter.

1. In the K2Config application, for the K2 Media Server with the adapter or adapters you are replacing, open the iSCSI bridge page and identify the ports on the adapter or adapters.
2. For the ports on the adapter or adapters you are replacing, make a note of the IP addresses and subnet mask settings.

   Later in this procedure you must assign these same settings to ports on the replacement adapter.
3. Close the K2Config application.
4. Take the clients of the K2 SAN offline and take all K2 Media Servers out of service.
5. If you are replacing two single-port adapters with a dual-port adapter, uninstall K2 system software from the K2 Media Server.
6. Power down the K2 Media Server and replace the iSCSI interface adapter or adapters. Refer to the service documentation on the Dell Documentation CD for procedures. If you are replacing two single-port adapters with a dual-port adapter, install the dual-port adapter in slot 2. Leave slot 3 empty.
7. Power up the K2 Media Server.
8. If you are replacing two single-port adapters with a dual-port adapter, install the current versions of K2 system software (version 3.2.7 or higher is required) on the K2 Media Server and then restart the K2 Media Server.
9. In the K2Config application, open the iSCSI bridge page for that K2 Media Server. It displays iSCSI interface adapters on the K2 Media Server, identified by MAC address. Notice that on replacement adapter ports the MAC address is different than it was on the former adapter, the IP addresses is set to 0.0.0.0, and bandwidth subscription set to 0.
10. Do the following for the replacement iSCSI interface adapter or adapters on the K2 Media Server:
    a) Select each port and set it to the same IP addresses\subnet mask as formerly assigned.
    b) Apply the settings.

       When the IP address is set successfully, the K2Config application automatically applies the same bandwidth subscription that was previously assigned to that IP address. The iSCSI bridge page updates and displays the bandwidth subscription.

11. After making settings on the iSCSI interface adapter or adapters, on the iSCSI bridge page, click **Check**.

    A "…Replaced iSCSI port…" message and a "…Added iSCSI port…" message appears for each port on the adapter or adapters that you replaced.

12. If you are replacing iSCSI interface adapters on multiple K2 Media Servers, repeat this procedure on the remaining K2 Media Servers.
13. Place the devices of the K2 SAN back online.

Installing the Fibre Channel card driver

When you restore a K2 Media Server from the generic disk image, the 8Gb Fibre Channel card driver is not on the disk image. After restoring the disk image, you must install the Fibre Channel card driver as instructed in this procedure.

1. After restoring the disk image and restarting the K2 Media Server, a Found New Hardware wizard opens. Dismiss the wizard and continue with this procedure.
2. Navigate to the following directory:

   `C:\Profile\Drivers\Atto 8Gb HBA Drivers`

3. Open the directory for the K2 Media Server platform on which you are installing, as follows:

Directory	Platform type
x64	64 bit
x86	32 bit

4. Open `setup.exe`.

   An install wizard opens.

5. Restart the K2 Media Server

Recovering from a failed K2 Media Server system battery

The following procedure applies to K2 Media Servers based on the Dell 2850/2950 platform. K2 Media Servers on other Dell models can have similar procedures. Refer to the service documentation on the Dell Documentation CD for specific procedures.

When the system battery in a K2 Media Server fails (non rechargeable) the system configuration is lost, and the system will not complete startup processes when the battery is replaced.

1. Restart the K2 Media Server.

   A startup screen displays the message "Invalid configuration information - Please run setup program. Time of day not set - Please run setup program."

2. Press **F2** to enter setup.
3. Set the system date and time
4. Select **System Setup | Integrated Devices**
5. Select **RAID**. This also sets ChA and ChB to RAID

6. Restart the K2 Media Server.

   A startup screen displays the message "Warning: Detected mode change from SCSI to RAID on ChA of the embedded RAID system."

7. Select **Yes**.

   A startup screen displays the message "Warning: Detected mode change from SCSI to RAID on ChB of the embedded RAID system."

8. Select **Yes**.

   The K2 Media Server restarts as normal.

When startup completes, normal operation is restored.

Checking K2 Media Server services

The following table specifies the startup type of services for the different K2 Media Server roles. Depending on a K2 Media Server's roles, some services have different startup types. Unless otherwise noted, services with startup type Automatic are started, while services with startup type Manual or Disabled are not started. You can use this table to check services if you suspect that they have been tampered with or for any reason are not set correctly.

To reset services, reconfigure the server with the K2Config application, starting at the beginning of the configuration wizard. Do not manually change the way services run on a configured K2 Media Server.

Service	SNFS file system server	iSCSI bridge	Metadata server	FTP server	NAS server
*CvfsPM[1]	Automatic[2]	Automatic	Manual	Automatic	Automatic
Grass Valley AppService	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley Extent Manager Service	Manual	Manual	Manual	Manual	Manual
*Grass Valley FTP Dameon	Manual	Manual	Manual	Automatic[3]	Manual
Grass Valley Import Service	Manual	Manual	Manual	Manual	Manual
Grass Valley K2 Config	Automatic	Automatic	Automatic	Automatic	Automatic

[2] This startup type is top priority for servers with this role. In other words, if a server has this role, then this is always the service's startup type, regardless of other roles that specify a different startup type.

[1] With SNFS version 3.5, this is the only service. Previous versions had StorNext File System service and StorNext File System RPC Port Mapper service

[3] This startup type is top priority for servers with this role. In other words, if a server has this role, then this is always the service's startup type, regardless of other roles that specify a different startup type.

Service	SNFS file system server	iSCSI bridge	Metadata server	FTP server	NAS server
Grass Valley MegaRaid Server [4]	Manual	Manual	Manual	Manual	Manual
Grass Valley MetaDataService	Manual	Manual	Manual	Manual	Manual
Grass Valley Performance Status	Manual	Manual	Manual	Manual	Manual
Grass Valley Performance Status Maker	Manual	Manual	Manual	Manual	Manual
Grass Valley SabreToothWS	Manual	Manual	Manual	Manual	Manual
Grass Valley Server Monitor	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley SNFS SetRtio	Automatic	Automatic	Automatic	Automatic	Automatic
Grass Valley Storage Utility Host	Automatic	Automatic	Automatic	Automatic	Automatic
GV STRATUS Summit Services	Automatic	Automatic	Automatic	Automatic	Automatic
ProductFrame Discovery Agent Service	Automatic	Automatic	Automatic	Automatic	Automatic
SabreTooth License Server	Automatic	Automatic	Automatic	Automatic	Automatic
SabreTooth Protocol Service	Automatic	Automatic	Automatic	Automatic	Automatic
SNMP Service	Automatic	Automatic	Automatic	Automatic	Automatic
SNMP Trap Service[5]	Automatic	Automatic	Automatic	Automatic	Automatic
STRATUS K2 Configuration Service	Automatic	Automatic	Automatic	Automatic	Automatic

*Startup type set by the K2Config application.

[4] This service has no purpose on a K2 Media Server. It is only used on a K2 client.

[5] This service has no purpose on a K2 Media Server. It is only used for receiving traps on a SNMP manager.

Licensing a K2 Media Server

Licenses are requested through the License Wizard and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The License Wizard and SabreTooth License Manager must be located on the Grass Valley product.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. A floating license can be used on multiple machines, one at a time. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

Use these procedures to license a K2 Media Server for your K2 SAN as designed by Grass Valley. Consult with Grass Valley before attempting to add a license to an existing K2 SAN.

To license a K2 SAN, the license must be installed on the K2 Media Server with role of file system server.

Related Topics

About K2 SAN licensing on page 126

Requesting a license

This topic applies to Grass Valley Sabretooth licenses. For the system you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID to create your unique license.

1. Log on to the device that you want to license.

   You must log in as a Windows administrator with a local account, not a domain account.

2. Open the License Request Wizard.

   Find the License Request shortcut on the Windows desktop.

   The License Request Wizard displays.

3. Read the on-screen instructions, then click **Next**.

   The Customer dialog box displays.

4. Enter the information requested on this page then click **Next**.

   You must provide a valid email address to receive your license file.

   The Sales Number dialog box displays.

5. Enter the Sales Order Number in the field then click **Next**.

   Typically the Sales Order Number is found on the Software License sheet that you received from Grass Valley.

   The Summary dialog box displays.

6. Review the License Request information and click **Finish**.

   A License Request text file, `License_Request_<SalesNumber>.txt`, is generated and saved to the Windows Desktop.

   NOTE: If you are requesting licenses for more than one application, be sure to modify the name of the first License Request text file before saving it to your desktop. (In Notepad, use the Save As command.) Otherwise, the second License Request text file will overwrite it.

7. Do one of the following:

   - Attach the License Request text file to an email.
   - Paste the text directly into an email message.

   You might want to keep a copy of the message for your records.

8. Send the email as instructed by the License Request Wizard.

   An email will be sent from Grass Valley to the return email address you specified; your SabreTooth software license will be provided as a text file.

9. Save this email in case you ever need to re-image this machine.

Next add the license to the SabreTooth License Manager.

If you encounter difficulties when requesting a license

If you encounter difficulties running the License wizard, or the License wizard is not available, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
   a) Double click on the License Manager icon on the Windows Desktop.

      The SabreTooth License Manager opens.

   b) Choose **File | Generate Unique Id** the License Manager.
   c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
2. Prepare an email that includes the following information:

   - Customer Name
   - Customer Email
   - Sales Order Number
   - Unique ID of the device where you will install software.

3. Send the email to K2License@grassvalley.com.

The SabreTooth license number will be emailed to the email address you specified.

Adding a license

Your software license, `Licenses_<SalesNumber>.txt`, is provided as a text file. Use the License Manager to add this file to your system and enable the desired feature.

1. Double click on the License Manager icon on the Windows Desktop.

   The SabreTooth License Manager opens.

2. Do one of the following:

   - Choose **File | Import License** and navigate to the file location to open the text file.
   - Drag and drop the text file onto the License Manager.

   You will now see the permanent license in SabreTooth, as well as any other licenses, permanent or temporary, that have been installed on this machine.

You should archive the permanent license to a backup system.

Deleting licenses

Deleting a license disables the feature that it enabled. You might want to delete a temporary license prior to its expiry if you have decided not to purchase the feature. You can delete a temporary license after the permanent license has been installed without disabling the licensed product.

1. Select the license in the SabreTooth License Manager.
2. Use the Delete key on your keyboard or right click with your mouse and select **Delete**.

Archiving licenses

You can archive your licenses to a secure external location. This allows you to quickly re-install a license should it be deleted or should you have to downgrade and then re-license the software. You can archive multiple licenses at the same time.

NOTE: If you downgrade to an earlier version of the licensed software, make sure to archive the licenses first.

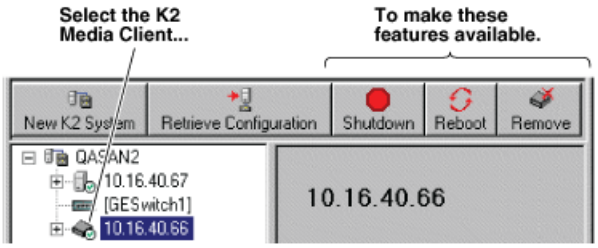
1. In the SabreTooth License Manager, select the license or licenses.
2. Choose **File | Export License** to open the Save As dialog box.
3. Assign a meaningful name to the file, and save it to the desired location. Grass Valley recommends saving the license file to a USB drive or other external location.

Working with K2 clients

Use the procedures in this section when doing configuration or service work on a shared storage K2 client that is part of an existing K2 SAN.

Accessing K2 client features in the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a shared storage K2 client are as follows:



Shutting down or restarting a K2 client

Prerequisites are as follows:

- Stop all media access on the K2 client.

Your options for shutting down a K2 client are as follows:

- Do a local shutdown/restart via AppCenter. Assuming a keyboard, monitor, and mouse is connected to the local K2 client, in AppCenter select **System | Shutdown**, then select **Shutdown** or **Restart** and **OK**. AppCenter exits, Windows shuts down and powers off the K2 client.
- Do a local shutdown/restart via Windows. Assuming a keyboard, monitor, and mouse is connected to the local K2 client, if AppCenter is not open, you can use the normal Windows procedure to shutdown. You can also do this type of shutdown/restart using the Windows Remote Desktop Connection.
- In the SiteConfig tree view right-click the K2 Client and select **Shutdown** or **Restart**.
- Do a remote shutdown/restart via the K2Config application. In the tree view select the K2 client and then click **Shutdown** or **Restart**.
- Do a local hard shutdown. Use this method only when there is a problem that prevents you from using one of the other methods for an orderly shutdown. To do a hard shutdown, hold down the standby button for approximately five seconds. To restart, press the standby button again.

Taking a K2 client offline

- To take a K2 client offline, simply stop all media access and then shut down the K2 client.

Bringing a K2 client online

- To bring a K2 client online, simply restart the K2 client. When the K2 client starts up, it is always in the online state.

Adding a K2 client

The prerequisites for adding a K2 client to an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- The K2 SAN must have adequate bandwidth available to meet the bandwidth needs of the K2 client you are adding.
- The devices of the K2 SAN do not need to be offline, and there is no restart of devices required.
- The K2 client must be connected to appropriate networks and be powered up.

- If a K2 Summit system, the write filter must be disabled.

1. In SiteConfig, add the K2 client to the SAN as follows:
   a) In the Network Configuration tree view, add the client as a placeholder device next to existing clients.
   b) Discover devices.
   c) Identify the K2 client you are adding.
   d) Assign the discovered K2 client to placeholder K2 client.
   e) Verify that networks are assigned and planned network interface settings applied.
2. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.
3. Click **Add Device**. The Add Device dialog box opens.
4. Select the appropriate type of client.
5. Click **OK**. The new client device appears in the tree view.
6. Configure the K2 client as appropriate.
7. If a K2 Summit Client, enable the write filter. In SiteConfig, you can do this using the Lock feature.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Removing a K2 client

The prerequisites for removing a K2 client from an existing K2 SAN are as follows:

- You must be logged in to the K2Config application with permissions equivalent to K2 administrator or higher.
- Media access must be stopped on the K2 client you are removing.
- You can remove a K2 client without disrupting the operation of the rest of the SAN.
- If a K2 Summit system, the write filter must be disabled.

1. Stop media access on the K2 client.
2. In SiteConfig, remove the K2 client.
3. In the K2Config application tree view, select K2 client.
4. Click **Remove** and **Yes** to confirm. The K2 client is removed from the tree view.
5. You must restart the K2 client before re-adding it to a K2 SAN or in any other way reconfiguring it for use. If a K2 Summit system, the write filter must be disabled before the restart.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Identifying K2 client software versions

Your options for identifying K2 client software version are as follows:

- In NetCentral, select the **Facility** button, then in the tree view open the node for the K2 client. This exposes the subsystems. You can find software version information on property pages for the **Software** subsystem.

- In the K2Config application tree view, open the node for the K2 client. This exposes the nodes for individual configuration pages. Select the **Software** configuration page to view software version information. To check for recent changes in software, click the **Check** button.
- Use SiteConfig software deployment features.

Modifying K2 client control network settings

To modify the hostname or IP address of a K2 client, use the following procedure. Refer to other procedures for the details of individual steps.

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

1. Make sure you know the load balancing (bandwidth) parameters currently set for the K2 client in the K2Config application. You must reconfigure these parameters later in this procedure.
2. If a K2 Summit system, disable the write filter. You can do this in K2Config or in K2Config.
3. In SiteConfig, remove the K2 client.
4. In the K2Config application, remove the K2 client from the K2 SAN.
5. In SiteConfig, add the K2 client to a K2 SAN as follows:
   a) In the Network Configuration tree view, add the client as a placeholder device next to existing clients.
   b) Discover devices.
   c) Identify the K2 client you are adding.
   d) Assign the discovered K2 client to placeholder K2 client.
   e) Verify that networks are assigned and planned network interface settings applied.
6. Edit hosts files or other name resolution mechanisms for all the devices of the K2 SAN. You can use SiteConfig for this task.
7. In the K2Config application, add the K2 client as a new device to the K2 SAN, load balancing the K2 client just as it was previously. This is important, as you want the K2Config application to assign it to the same available bandwidth on the same iSCSI target as previously.
8. If a K2 Summit system, enable the write filter. You can do this in K2Config or in K2Config.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Enabling and disabling the write filter using K2Config on page 305

Modifying K2 client media (iSCSI) network settings

If IP address to which you are changing is in a different subnet, do not use this procedure. Instead, remove, then add the K2 client.

If the iSCSI network address to which you are changing is within the same subnet and range as the current iSCSI network, use the following procedure.

1. Stop media access on the K2 client.
2. If a K2 Summit system, disable the write filter. You can do this in K2Config or in K2Config.
3. Use SiteConfig to change the IP address. Make sure that the IP address is within the subnet and range designated for the network.

4. In the K2 System Configuration application, open the Network configuration page for the K2 client.
5. Verify that the IP address updates correctly.
6. If a K2 Summit system, enable the write filter. You can do this in K2Config or in K2Config.
7. Restart the K2 client.

Related Topics

Enabling and disabling the write filter using K2Config on page 305

Enabling and disabling the write filter using K2Config on page 305

Enabling and disabling the write filter using K2Config

Before doing this task, make sure that your K2 Summit system is in a state as follows:

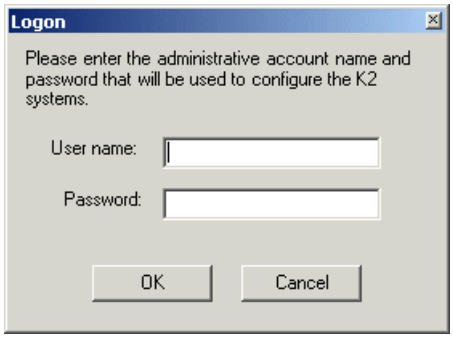
- Media access is stopped
- The K2 Summit system is not being used

This task required a restart.

You can use the K2Config application to enable and disable the writer filter on a SAN-attached K2 Summit system.

1. On the PC that hosts K2Config, open the K2Config application.

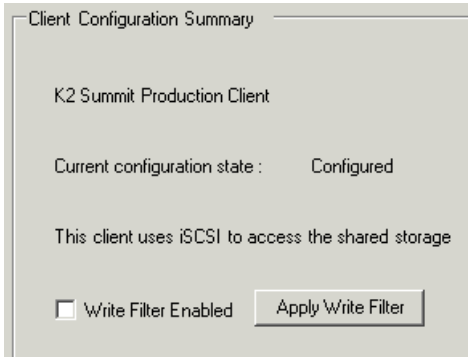
   A login dialog box opens.



2. Log in to the K2Config application with the administrator account.

   The K2Config application opens.

3. In the K2Config application tree view, select a K2 Summit system.
   The K2 Summit system's summary information is displayed.



4. Identify the **Write Filter Enabled** setting, which displays the current state of the write filter as follows:
   - If selected, the write filter is currently enabled on the K2 Summit system.
   - If not selected, the write filter is currently disabled on the K2 Summit system.
5. Configure the **Write Filter Enabled** setting to change the state of the write filter as follows:
   - Select the setting to enable the write filter.
   - Clear the setting to disable the write filter.
6. Click **Apply Write Filter** to put your change into effect.
7. When prompted, confirm your change and the restart of the K2 Summit system.

Configure live streaming multicast using K2Config

Before doing this task, make sure that the SAN-attached K2 Summit systems are in a state as follows:

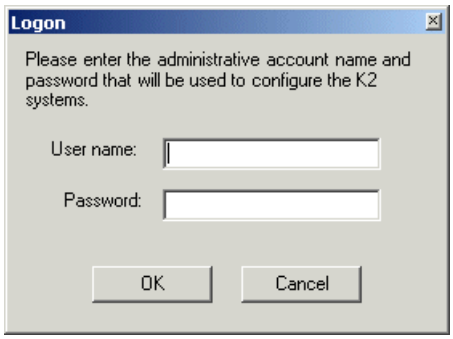
- Media access is stopped
- The K2 Summit system is not being used
- The write filter is disabled

This task required a restart.

You can use the K2Config application to configure multicast settings on all the K2 Summit systems attached to a K2 SAN. Refer to related topics in "K2 System Guide" for live streaming technical details.

1. On the PC that hosts K2Config, open the K2Config application.

   A login dialog box opens.

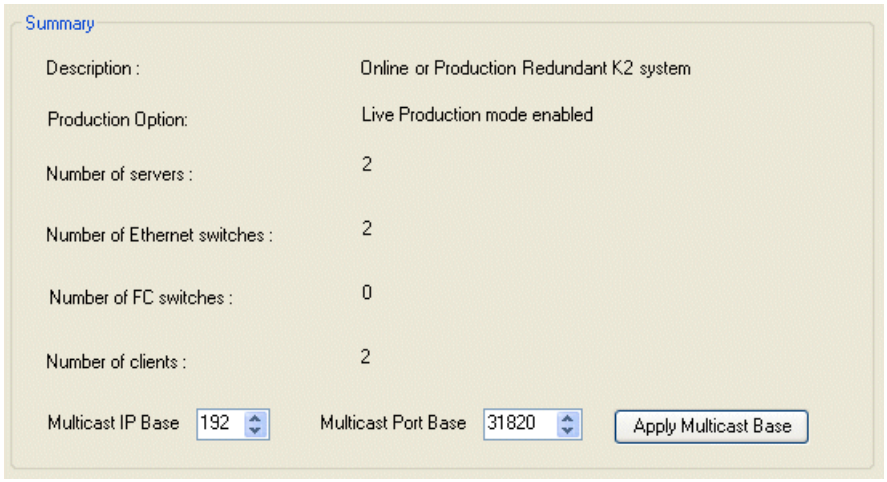


2. Log in to the K2Config application with the administrator account.

   The K2Config application opens.

3. In the K2Config application tree view, select each K2 Summit system attached to the K2 SAN and verify that the **Write Filter Enabled** setting shows that the write filter is not enabled on the K2 Summit system.
4. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.

   The SAN summary information is displayed.



5. Select the multicast IP base.

   The K2 Summit system applies channel-specific IP addresses from this base.

   Your choices are constrained to those specified by IANA for multicast.

6. Select the multicast port base.

   This is the first UDP port address for elementary streams.

7. Click **Apply Multicast Base** to apply the settings.
8. When prompted, confirm your change and the restart of the K2 Summit systems.

The multicast settings are applied to all K2 Summit system attached to the K2 SAN.

Using Storage Utility

When doing configuration or service work on the media file system, the media database, or the RAID storage devices of an existing K2 SAN, the primary tool is the Storage Utility.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 SAN inoperable or result in the loss of all your media.***

Use K2 SAN installation instructions to using Storage Utility as you initially set up and configure a K2 SAN. You should refer to those instructions for information that is specific to your K2 SAN.

Accessing Storage Utility

Prerequisites are as follows:

- You must open Storage Utility from within the K2Config application. Access permissions are passed from the K2Config application to the Storage Utility as it opens, so make sure that you are logged in with sufficient permissions.

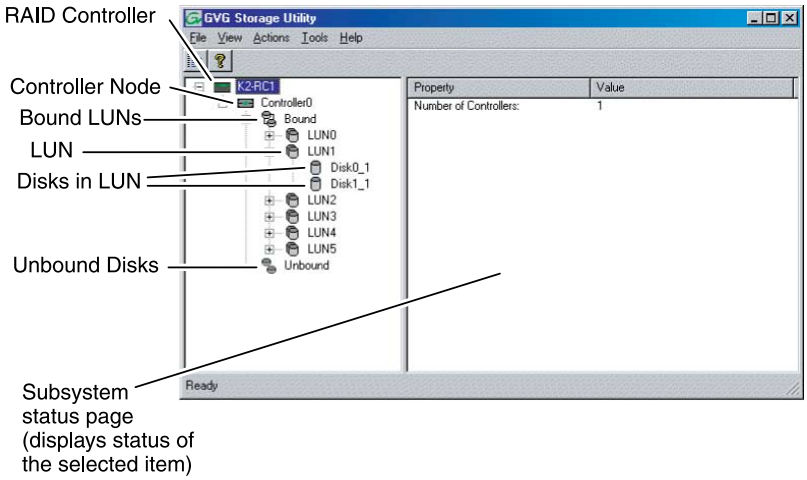
  You can open Storage Utility in the following ways:

  - In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree. Then click the **Storage Utility** button. Storage Utility opens. In this case the connection to the RAID storage devices is via the K2 Media Server first configured, depending on the level of the SAN.
  - In the K2Config application tree view, open the node for a K2 Media Server and select the **File System Server** node to open its property page. On the property page click **Launch Storage Utility**. Storage Utility opens. In this case the connection to the RAID storage devices is via the selected K2 Media Server. Use this method for nearline SANs.

NOTE: Do not run Storage Utility on a shared storage K2 client.

NOTE: Do not run Storage Utility as a stand-alone application, separate from the K2Config application. To maintain a valid K2 SAN all storage configuration must be controlled and tracked through the K2Config application.

Overview of Storage Utility



The Storage Utility user interface includes a tree view in the left-hand pane, and a status information area displayed in the right-hand pane. The tree view displays the hardware that make up the RAID storage system. The context menus in the tree view are used to configure storage. The right-hand status pane displays information about the item selected in the tree view. The tree view hierarchy is as follows:

- Controllers in device - Provides a logical grouping of the RAID Controllers in a primary RAID chassis.
- Controller - Represents the RAID Controllers found. These are numbered in the order discovered. The controller icon represents both RAID Controller A and, if installed, RAID Controller B. To determine if an optional RAID Controller B is installed, select the Controller icon in the tree view, then examine the status pane for peer status.
- Bound Disks - Expanding the Bound node displays all bound disks.
- RANK - Represents a bound RANK. Expanding the RANK node displays the disk modules that make up the RANK.
- UnBound disks - Expanding the UnBound node, displays all unbound disk modules.
- Disks - Represents the disk modules. The Storage Utility detects disks available and lists them on the opening screen.

Use Storage Utility for working on the media file system and database.

Related Topics

About RANKs and LUNs in Storage Utility on page 269

Working on the media file system and database

Use the procedures in this section when doing configuration or service work on the media file system or the media database of an existing K2 SAN.

Checking the media file system

Prerequisites are as follows:

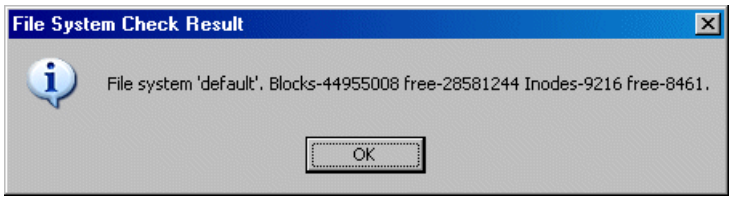
- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be offline.
- K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but offline.

This procedure checks the media file system but retains current media files.

NOTE: This procedure can take 20 hours or more on a large SAN. Do not start this process unless you have adequate time set aside.

1. In Storage Utility, click **Tools | Check File System**.
2. A message box appears "Checking media file system. Please wait". Observe progress.

   If problems are discovered they are reported. If the check process passes, when the process is complete a message appears to confirm success.



3. Click **OK** to dismiss the results.
4. Messages appear "…online mode now?" and "…continue?". Do one of the following:

   - Click **Yes** to put the system in online mode. This is the recommended option in most cases. For example, even if you plan to next clean unreferenced files and/or movies, that operation requires that the system be online, so you should put it online now. When you click Yes, AppCenter channels go online.
   - Click **No** to keep the system in offline mode. This is not recommended for most cases. Only do this when you are sure that subsequent operations require the system to be offlline.

Your file system has been checked.

Cleaning unreferenced files and movies

Prerequisites are as follows:

- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be online.
- All iSCSI clients and K2 clients in the K2 SAN must be online.

- K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but online.

These procedures allow you to keep the media database and the media files in sync. You can check the movies (clips) in the media database for the references to media files that should be currently stored on the media disks. Likewise, you can check for media files that are not referenced by a movie in the media database. If you find any unreferenced files or movies, you can delete them.

Clean unreferenced files

1. In Storage Utility, click **Tools | Clean Unreferenced Files**.
2. A message box appears "…searching …Please wait". Observe progress.
3. A message box reports results. Respond as follows:
   - If no unreferenced files are found, click **OK** to dismiss the results.
   - If unreferenced files are discovered, you are prompted to delete them. Click **Yes** to delete the files or **No** to leave the files intact.

The process writes a log file to `C:\profile\logFS.txt`, which you can check for more information.

Clean unreferenced movies

1. In Storage Utility, click **Tools | Clean Unreferenced Movies**.
2. A message box appears "…searching …Please wait". Observe progress.
3. A message box reports results. Respond as follows:
   - If no unreferenced movies are found, click **OK** to dismiss the results.
   - If unreferenced movies are discovered, you are prompted to delete them. Click **Yes** to delete the movies or **No** to leave the movies intact.

The process writes log files to `C:\profile\cleanupDB.txt` and `C:\profile\MediaDB.txt`, which you can check for more information.

Making a new media file system

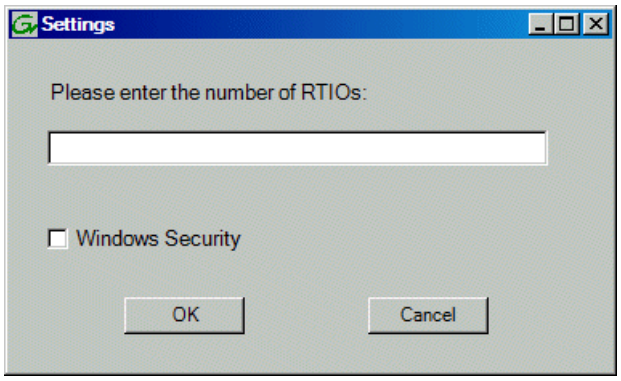
The requirements for this procedure are as follows:

- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

If your SNFS file system name is currently "default", when you make a new file system the name changes to "gvfs_hostname", where hostname is the name of the primary FSM.

NOTE: You lose all media with this procedure.

1. In Storage Utility, click **Tools | Make New File System**.
   The Settings dialog box opens.



2. For Real Time Input Output (RTIOs), enter the number specified for the design of your K2 SAN. Contact your Grass Valley representative if you do not know this number.
3. For Windows Security, configure as follows:
   - If a K2 SAN with only K2 clients, leave this setting unchecked.
   - If a K2 SAN with Aurora Edits, refer to the *Aurora Edit Installation and Configuration Guide*.
4. Click **OK**.
   The Configuration File dialog box opens.
5. On the Configuration File dialog box, you can view media file system settings, but do not attempt to change them. Click **Accept**.
   A "Making new file system. Please wait" message box displays progress.
6. When a message "Succeeded to make the new file system…" appears, click **OK**.
7. Restart the K2 Media Server.
8. You now have a blank (empty) file system. Proceed as follows:
   - On a 7.x SAN, you also have a blank database. Do not perform additional operations on the database. Skip to the next step in this procedure.
   - On a 3.x SAN, the media database still contains references to media files which are no longer present in the file system. To clear the media database do the following:

   a) In the K2Config application tree view, open the node for the K2 Media Server and select the **Database Server** node to open its property page.
   b) On the Database Server property page click **Erase media database**.
      A message box displays progress.
   c) Wait until a message confirms that the process is complete. This can take several minutes.
   d) If you have redundant K2 Media Servers, repeat these steps to clear the media database on the other (redundant) server.
9. Close Storage Utility.

10. If you have Macintosh systems accessing the K2 SAN, you should check that the SNFS file system volume is configured correctly on the Macintosh systems.
11. Place the K2 SAN back online.

Expanding the media file system by capacity

Prerequisites are as follows:

- The system must have one LUN per RANK. Expansion by capacity is not supported on systems with multiple LUNs per RANK.
- The expansion chassis that you add to your K2 SAN must have unbound, unlabeled disks.

NOTE: This procedure should only be attempted under the supervision of qualified Grass Valley support personnel. Contact your Grass Valley representative for assistance.

If you need to increase the storage capacity of your K2 SAN, you can do so by adding one or more Expansion Chassis, up to the maximum number of chassis allowed for your level of storage.

1. Rack the Expansion Chassis.
2. If a redundant K2 SAN, do the following:
   a) Verify that MPIO is updated to the latest version on all shared storage K2 clients.
   b) Put the system into an "original primary" state. This means that for all redundant devices (switches, servers, RAID controllers, etc.) the current device acting as primary is the one that was initially configured as primary when the system was originally installed.
3. On the K2 Media Server with the role of primary media file system/metadata server, save a copy of the following files to a different location:

   `D:\snfs\config\default.cfg` (on some systems this file is named `gvfs_hostname.cfg`, where hostname is the name of the SNFS file system server.)

   `D:\snfs\config\cvlabels`
4. Power down the K2 SAN, including RAID storage devices.
5. Power up the RAID storage devices. Verify that they stabilize in an operational state with no errors indicated.
6. Power down RAID storage devices.
7. Cable and configure the Expansion Chassis.
8. Power up the RAID storage devices. Verify that they stabilize in an operational state with no errors indicated.
9. Start up the K2 SAN.
10. Bind the RANKs in the Expansions Chassis using Background Bind.
11. When binding is complete, put the K2 SAN in an offline state as follows:
    a) You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
    b) When you access Storage Utility, the K2 SAN must be offline.
    c) All iSCSI clients and K2 clients in the K2 SAN must be shut down.
12. Restart all K2 Media Servers. Do not use the standard startup processes here. Just start up the server(s) and wait until the Windows desktop appears. Especially do not use Server Control Panel or start Failover Monitor.

13. In Storage Utility, select **Tools | Expand File System By Capacity**.

    The first of a series of informational screens opens.

14. Work through the informational screens to verify information. When the option to retry becomes available, if the new disks are not labeled correctly, retry to start the process. If you are not sure, you can retry to be sure. Doing so does not cause problems.
15. A message box reports progress. When a message reports success, the process is complete.
16. Restart the K2 SAN.
17. If a redundant K2 SAN, test failover capabilities.

Expanding the media file system by bandwidth

If you want to retain your media file system and yet expand the bandwidth of your K2 SAN, you must use the following procedures for dynamic bandwidth expansion. This process allows you to add RANKs to the stripe group, thereby expanding its width, without reinitializing the file system. This keeps the existing media intact. The additional RANKs can be made up of new disks in existing RAID chassis, disks in new Expansion Chassis, or disks in new primary RAID chassis.

After the file system is expanded, existing media is still striped across the original narrower stripe group, so it can not take advantage of the increased bandwidth. Also, if there is a significant portion of the storage pool occupied by this existing media, its presence reduces the extent to which new media can use the increased bandwidth. For this reason the dynamic bandwidth expansion process provides the Restripe Utility, which restripes the existing media across the new wider stripe group. This enables both the existing media and new media to get full benefit of the increased bandwidth.

If the media on your file system has a high turnover rate and you know existing media is to be deleted soon, you have the option of disabling the Restripe Utility. This saves the system resources and time required to restripe media.

The expansion chassis that you add to your K2 SAN must have unbound, unlabeled disks. If it currently has disks bound or labeled, connecting it to your system can cause errors.

Dynamic bandwidth expansion is supported only with K2 system software version 3.2 and higher.

Dynamic bandwidth expansion is supported on systems with one LUN per RANK and on systems with multiple LUNs per RANK.

NOTE: Adding RAID storage devices changes your system design and must be specified for your K2 SAN by Grass Valley. Do not attempt to add RAID storage devices without support from Grass Valley.

Procedures for expanding the media file system by bandwidth

Grass Valley personnel who have received K2 SAN training can use the following procedures.

Prepare system for bandwidth expansion

1. If a redundant K2 Storage System, do the following:
   a) Verify that MPIO is updated to the latest version on all shared storage K2 clients.
   b) Put the system into an "original primary" state.

      This means that for all redundant devices (switches, servers, RAID controllers, etc.) the current device acting as primary is the one that was initially configured as primary when the system was originally installed.
2. Back up configuration files from the primary K2 Media Server. To do this, save a copy of the following files to a different location:

   `D:\snfs\config\cvlabels`

   `D:\snfs\config\default.cfg`

   On some systems this file is named `gvfs_hostname.cfg`, where hostname is the name of the SNFS file system server.

   If there is a problem with the expansion process, contact Grass Valley Support for instructions on using these files to recover.
3. If K2 storage contains Aurora media, do additional steps.
4. Verify recovery disk images. Update if necessary

Related Topics

Identifying current primary/backup K2 Media Servers on page 281

Expanding bandwidth for Aurora products on page 318

Set up and configure RAID for bandwidth expansion

1. Rack any new RAID equipment
2. Stop all media access and power down K2 clients and other clients.
3. Clean unreferenced files and movies.

   K2 Media Servers with role of file system/metadata server, both primary and redundant, must be powered up but offline.
4. Power down the remaining devices of the K2 SAN.
5. Add disks or RAID equipment to support the additional RANKs

   As applicable, remember to set Fibre Channel addresses on RAID controllers and chassis addresses on Expansion Adapters.
6. Start up the RAID equipment.
7. Start up the primary K2 Media Server.

   If there are multiple K2 Media Servers, this is the server that takes the role of media file system server. On a redundant K2 SAN, this is the server functioning as primary when the system was last powered down.

8. From the control point PC, open the K2Config application and launch Storage Utility.

   Make sure that versions are correct and consistent on both new and existing RAID storage devices.

9. Verify versions of controller microcode and disk firmware. Update if necessary.

   Make sure that versions are compatible on both new and existing disks and RAID storage devices.

10. Bind RANKs using the new disks.

    Wait for the binding process to complete.

    Do not unbind or bind existing RANKs. Doing so destroys all data. If in doubt, flash drive lights to identify disks.

11. Close Storage Utility.
12. Restart the primary K2 Media Server.

    Do not use the standard startup processes here. Just start up the server and wait until the Windows desktop appears. On a redundant K2 SAN, do not use Server Control Panel or manually start.

13. Check the Windows Device Manager to verify that the server "sees" both the old RANKs and the new RANKs.
14. Start up the remaining K2 Media Servers that are connected to the K2 SAN.

    Do not use the standard startup processes here. Just start up the server(s) and wait until the Windows desktop appears. On a redundant K2 SAN, do not use Server Control Panel or manually start.

Related Topics

Cleaning unreferenced files and movies on page 310
Accessing Storage Utility on page 308
Checking controller microcode on page 321
About full/background bind on page 325

Configure the media file system for bandwidth expansion

1. If Aurora media is present, modify `VolumeConfig.xml`.
2. Stop services (if running) on K2 Media Servers. .

   On a redundant K2 SAN stop the Server Monitor Service. On a non-redundant K2 SAN stop the MetaData service.

3. From the control point PC, open the K2Config application and launch Storage Utility.
4. In Storage Utility make sure both old RANKs and new RANKs are displayed.
5. In Storage Utility, select **Tools | Expand File System By Bandwidth** and answer **Yes** to confirm.

6. A dialog box opens asking if you want to restripe existing media after bandwidth expansion. Proceed as follows:

   - Click **Yes** in most cases. This is the typical response. In any case this does no harm.
   - Click **No** only if you are sure you do not need to restripe existing media, such as in the following cases:

     - You have very little existing media so the fact that it cannot use the new stripe group does not impact future media operations or capacity.
     - Your existing media is to be deleted soon so you don't care if it uses the new stripe group.

   The first of a series of informational screens opens.

7. Work through the informational screens.

   When prompted to retry, if you are not sure if the process started, you can retry to be sure. Doing so does not cause problems.

   The expansion process runs. A dialog box displays progress

8. Wait for the process to complete. On a large system this can take over 30 minutes.
9. A "…succeeded…" message is displayed when done. Click **OK** and Storage Utility closes.
10. The K2Config application displays a message informing you to restart servers. Click **OK**.
11. Make sure Storage Utility is closed before proceeding.
12. If directed, modify RTIOS.

    Depending on your use of the expanded file system, you might need to change the RTIOS value. This value can be calculated only by Grass Valley Support. Do this step only under the direction of Grass Valley Support.

    As directed, use a text editor to modify the SNFS configuration file on K2 Media Servers (both primary and backup) with the role of media file system/database server.

    NOTE: Don't use the SNFS configuration tool to modify the system configuration. Doing so causes unexpected changes in the configuration file, resulting in a failure of the expansion process.

13. Restart all K2 Media Servers.

    Make sure to first start servers with the role of media file system/metadata server.

    When the server that takes the role of FTP server starts, one of the following happens:

    - If you answered "Yes" to restripe existing media in the step above, the Restripe Utility automatically launches and begins restriping media.
    - If you answered "No" to restripe existing media in the step above, the Restripe Utility does not launch.

14. In the K2Config application, do the following for each K2 Media Server with role of iSCSI bridge to verify that you see the correct number of drives:
    a) On the **iSCSI Bridge Server Configuration** page, click **View Target Drives** and proceed as follows:
    - If you see all drives, both old and new, no further sub-steps are necessary. Skip to the next step in this procedure.
    - If some drives are listed as unexposed, continue with the remaining sub-steps in this step.

    b) Click **Check**.
    c) Restart the K2 Media Server.
    d) Repeat this step to make sure you now see the correct number of drives.
15. Monitor the Restripe Utility.

    On a file system with a large amount of existing media, this can take days.

    NOTE: Do not stop the FTP server once the restripe process begins.

    a) Record system information

    Make sure you keep diagrams and other on-site documentation up to date.

Related Topics

Expanding bandwidth for Aurora products on page 318
Accessing Storage Utility on page 308
Managing the Restripe Utility on page 319

Expanding bandwidth for Aurora products

The "Expansion by bandwidth" feature is supported on K2 Storage Systems that store media from both K2 products and Aurora products. If the storage system contains media from Aurora products and you want to retain that media, additional steps are required, as follows:

1. Before starting the file system expansion, using Notepad or another text editor, open the following file:

   `V:\VolumeConfig.xml`
2. To the existing XML content, add lines with XML tags `<MainFolder>` and `<AtticFolder>` to specify the main folder and attic folder for your Aurora media. For example, if the main folder is "VibrintAVFiles" and the attic folder is "VibrintAttic", the resulting XML content is as follows:

```
<VolumeConfig>
   <Type>K2 Storage</Type>
   <Model>Grass Valley PFR700</Model>
   <StripeSize>512</StripeSize>
   <Security>Not Supported</Security>
   <MainFolder>V:\VibrintAVFiles</MainFolder>
   <AtticFolder>V:\VibrintAttic</AtticFolder>
</VolumeConfig>
```

3. Save and close the `VolumeConfig.xml` file.
4. Proceed with bandwidth expansion process.

Managing the Restripe Utility

If you answer "Yes" to the dialog box that asks about restriping existing media, after the bandwidth expansion process completes, Storage Utility exits with a special code. On receiving the special exit code, the K2 System Configuration application sets the current date in the registry of the K2 Media Server that takes the role of FTP server.

When the FTP server restarts, the Restripe Utility automatically opens. The Restripe Utility reads the date set in the registry, finds clips and files created before that date, and restripes the clips and files, one at a time.

1. You can monitor the Restripe Utility in the following ways:
   - While the Restripe Utility is running, it is represented by an icon in the system tray. You can right-click this icon and open the Restripe Utility window.
   - IMAGE HERE
   - The Restripe Utility window reports first on the progress of K2 clips being restriped, then on the progress of files being restriped.
   - Click the Report button for a list of clips and files that failed to be restriped, if any.
   - When the Restripe Utility completes its processes, it reports its results to *C:\profile\RestripeResult.txt*. Open this file in Notepad to verify successful results.
2. You can start and stop the Restripe Utility manually as follows:
   - At any time while the Restripe Utility is in the process of restriping clips, you can right-click the icon in the system tray, and select **Abort**. This stops the restripe process and closes the Restripe Utility.

     NOTE: Stopping the Restripe Utility before it completes its processes leaves some of your existing media still striped across the original narrower stripe group. Once the Restripe Utility is stopped, you cannot restripe that existing media.

Recovering the media database

Use the topics in this section to understand and implement recovery strategies for your K2 storage media database.

About the automatic database backup process

Every 15 minutes the K2 system checks to see if any media operations have changed the media database. If a change has occurred, the K2 system creates a backup file of the media database. The backup file is saved in the same directory as the media database using a rotating set of three file names. These files are named `media.db_bakX` where `X` is the number in the rotation. Each time a backup occurs, the oldest backup file is overwritten. If some condition renders one of the backup files un-writable, the backup file following that in the rotation is subsequently used for every backup until the condition is resolved.

Identifying a corrupt media database

1. Check the following symptoms, as they could indicate a corrupt media database:
   - On startup, the Grass Valley MetaDataService is unable to start. This is indicated in the Services control panel if the Grass Valley MetaDataService does not display as Started.
   - The K2 log displays a "…file is encrypted or is not a database…" error.
2. As soon as you suspect a corrupt media database, stop all media access and take the K2 system offline.

Restoring the media database

1. Stop all media access and take the K2 system offline.

   If a K2 SAN, follow procedures to take connected K2 client systems and K2 Media Servers offline. Shutdown connected K2 client systems. Refer to the *K2 SAN Installation and Service Manual*.
2. Navigate to the V:\media directory.

   If a K2 SAN, access this directory from a K2 Media Server with role of media file system server.
3. Make a copy of the media.db and media.db_bak* files and store them in a secure location.
4. Stop the Grass Valley MetaDataService as follows:
   - If a stand-alone K2 system, use the Services control panel to stop the service.
   - If a K2 SAN, use Server Control Panel to stop the service on primary, and if present, backup K2 Media Server with role of file system server.
5. Determine which backup file is the most recent good file by examining the file modification date on each backup file.
6. Rename the current *media.db* file (which is assumed to be corrupt) to another name, and rename the most recent good *media.db_bakX* file to *media.db*.
7. Restart the K2 system following normal procedures.
8. Confirm that the systems come up correctly with the restored database now in place.
9. Use Storage Utility **Clean Unreferenced Files** and **Clean Unreferenced Movies** to repair any inconsistencies between the contents of the database and the file system.

Working with RAID storage

This section refers to K2 10G RAID storage devices.

K2 Level 2, 3, 10, 20, 30, and 35 RAID storage devices were released with previous versions of K2 SANs. Refer to previous versions of this manual for information about those levels.

Use the procedures in this section when doing configuration or service work on the RAID storage devices of an existing K2 SAN.

Checking RAID storage subsystem status

Some limited status information for storage subsystems is displayed in the Storage Utility. This can be helpful when configuring storage. You can view status information by selecting items in the tree view.

Item in tree view	Status information displayed
Controllers in Device	Number of Controllers
Controller	Peer Status
	Primary IP
	Serial Number
	Slot
	Peer Slot
	Microcode Version
Bound	Number of RANKS or LUNs
RANK	Binding Type, such as RAID 1
	State (online or offline)
	Number of Logical Units
Disk	Firmware
	Vendor
	State
	Product ID
	Capacity
Unbound	Number of disks

Checking controller microcode

As explained in the previous section, to check controller microcode, in Storage Utility select the controller in the tree view and the microcode version is displayed.

Identifying disks

When you do maintenance or service work on your RAID storage, it is important for many tasks that you positively identify the disk or disks on which you are working. Your primary indicators for this are the numbering of the disks in Storage Utility and the ability to flash the disk LED on a physical disk or a group of disks.

DP0 disk numbering

In Storage Utility, RAID disks are numbered with a hexadecimal convention. Disk modules are identified based on the chassis address and physical location. When Expansion chassis are all connected to DP0, disks are numbered as follows:

Chassis...	Connects to...	With disk numbering as follows:			
Primary	DP0 (internal connection)	00	01	02	03
		04	05	06	07
		08	09	0A	0B
Expansion 1	DP0	10	11	12	13
		14	15	16	17
		18	19	1A	1B
Expansion 2	DP0	20	21	22	23
		24	25	26	27
		28	29	2A	2B
Expansion 3	DP0	30	31	32	33
		34	35	36	37
		38	39	3A	3B
Expansion 4	DP0	40	41	42	43
		44	45	46	47
		48	49	4A	4B
Expansion 5	DP0	50	51	52	53
		54	55	56	57
		58	59	5A	5B
Expansion 6	DP0	60	61	62	63
		64	65	66	67
		68	69	6A	6B
Expansion 7	DP0	70	71	72	73
		74	75	76	77
		78	79	7A	7B

DP0/DP1 disk numbering

When Expansion chassis are connected to DP0 and DP1 in an alternating pattern, the disk numbering is as follows. With this pattern, the first Expansion chassis connected to DP1 always has a chassis address of 8, regardless of how many Expansion chassis are connected to DP0:

Chassis...	Connects to...	With disk numbering as follows:			
Primary	DP0 (internal connection)	00	01	02	03
		04	05	06	07
		08	09	0A	0B
Expansion 2	DP0	10	11	12	13
		14	15	16	17
		18	19	1A	1B
Expansion 4	DP0	20	21	22	23
		24	25	26	27
		28	29	2A	2B
Expansion 6	DP0	30	31	32	33
		34	35	36	37
		38	39	3A	3B
Expansion 8	DP0	40	41	42	43
		44	45	46	47
		48	49	4A	4B
Expansion 10	DP0	50	51	52	53
		54	55	56	57
		58	59	5A	5B

Chassis...	Connects to...	With disk numbering as follows:			
—	—	—			
Expansion 1	DP1	80	81	82	83
		84	85	86	87
		88	89	8A	8B
Expansion 3	DP1	90	91	92	93
		94	95	96	97
		98	99	9A	9B
Expansion 5	DP1	A0	A1	A2	A3
		A4	A5	A6	A7
		A8	A9	AA	AB
Expansion 7	DP1	B0	B1	B2	B3
		B4	B5	B6	B7
		B8	B9	BA	BB
Expansion 9	DP1	C0	C1	C2	C3
		C4	C5	C6	C7
		C8	C9	CA	CB

Flashing disk LEDs

Storage Utility's Identify feature allows you to flash the disk LEDs so that you can physically locate a specific disk module or group of disk modules that make up a RANK. Always use the disk identify feature before removing and replacing a failed disk module. Accidentally removing the wrong disk module can destroy data.

1. Open Storage Utility and in the tree view expand all nodes so that all disks are displayed.
2. Open the bezel on the RAID storage chassis or otherwise make sure you can see disk LEDs.
3. Identify the disks in a RANK or identify a single disk, as follows:
   a) In the Storage Utility tree view, right-click a RANK or right-click a single disk, then select **Identify RANK** or **Identify Disk** in the context menu. A message box opens with a message that informs you that a disk or disks are blinking.
   b) The LEDs for the disk or disks display a flashing pattern. Verify the location of the disk or disks.

Get controller logs

1. In the Storage Utility tree view, select the controller.
2. Click **Actions | Get Controller Logs**.
3. A message informs you of the location of the logs.
4. Find the log files on the K2 Media Sever at *C:\logs*.

Unbind RANK

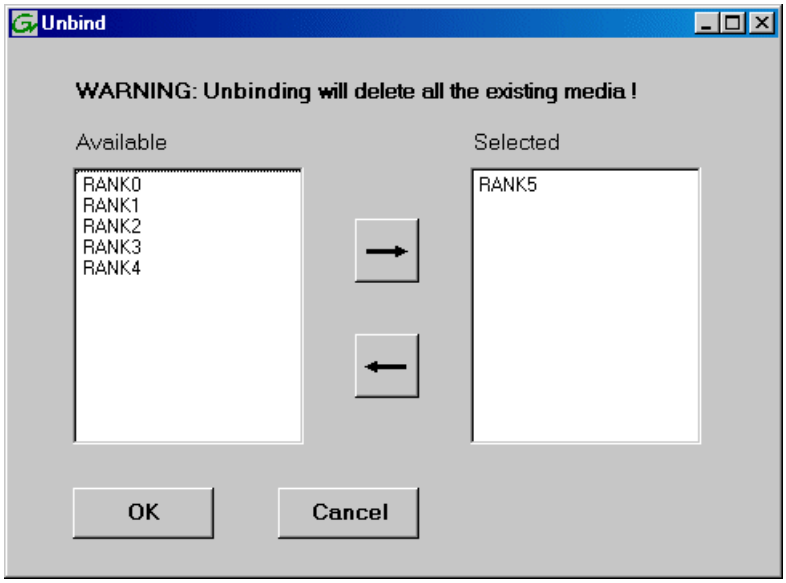
Prerequisites are as follows:

- You must access Storage Utility (via the K2Config application login) with permissions equivalent to K2 administrator or higher.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

Unbinding reverses the bind process. Unbinding might be needed when reconfiguring a SAN.

⚠ ***CAUTION: Unbinding destroys all data stored on disk modules***

1. In the tree view, right-click the RANK and select **Unbind**.
2. When warning messages appear "…destroy all existing media…" and "Are you sure?", click **OK** to continue. The Unbind dialog box opens.



3. Verify that the RANK or RANKs you intend to unbind is in the Selected box. If not, select RANKs and click the arrow buttons until the RANKs you intend to bind are in the Selected box and the RANKs you do not intend to unbind are in the Available box.

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click **OK** to close the Unbind dialog box and begin the unbinding process. The Progress Report dialog box opens, showing the status of the unbinding process.
5. When progress reports 100% complete, the RANK is unbound.
6. Restart the K2 Media Server.

Related Topics

About RANKs and LUNs in Storage Utility on page 269

About full/background bind

When binding RAID disks, you can choose to do either a full bind or a background bind. Background bind is recommended. These binding processes are described as follows:

- Full bind — During this process, the K2 SAN must be in the offline mode. While the full bind process is underway, disks are not available for data access of any kind. On a large SAN, the full bind process can take many hours, so you should plan ahead for this process. For example, binding 750 Gig SATA drives can take up to 3 days.
- Background bind — During this process, the K2 SAN can be in a restricted online mode. Disks are available for data access, but the overall performance of the RAID storage is significantly reduced. While the background bind process is underway, you can initiate media access on your SAN for limited testing of operations, such as record, play, and transfer, but do not run media access at full bandwidth. The background bind process is useful when doing initial system installation and configuration, as it does not require the long wait time required for full bind. You can have RAID disks binding while you move on to other tasks that require RAID media access.

With either type of binding process, you should bind multiple RANKs simultaneously, to reduce the overall time required to bind disks.

Bind RANK

Prerequisites are as follows:

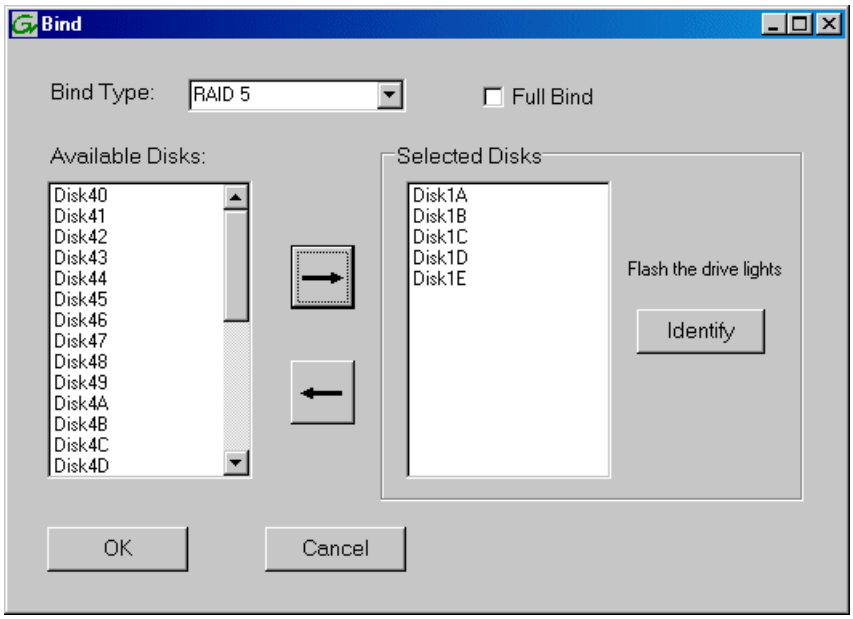
- You must access Storage Utility (via the K2 System Configuration application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

Binding disk modules formats them into a logical units called RANKs. The disks that make up a RANK are accessed as a contiguous disk space. Disk modules must be bound before they can be part of the video storage file system.

For simplicity, the Storage Utility only allows binding the first available (at the top of the Available Disks list) contiguous disk modules into RANKs. After binding, disk modules become slot specific and cannot be moved to other disk module slots.

1. In the tree view, right-click the **Unbound** node and select **Bind**. (Peer controllers that share the same set of disks are automatically selected as a pair.)

   The Bind dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



2. Leave **Full Bind** unchecked. Refer to the previous section “About full/background bind”.
3. In the **Bind TYPE** drop down box, select the RAID type. Refer to the installation chapter earlier in this document for your level of SAN for specific instructions.
4. In the Available Disks box, select contiguous disks at the top of the list as appropriate for the RAID type. (TIP: Use ‘shift-click’ or ‘control-click’ to select disks.)
5. Click the add (arrow) button to add disks to the Selected Disks list.

   NOTE: As an aid in identifying a disk module’s physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

6. Click **OK** to close the Bind dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
7. Close the Progress Report and repeat these steps for other unbound disks.
8. Upon 100% completion, click **Close** in Progress Report window.
9. Restart the K2 Media Server.

Related Topics

Identifying disks on page 321
About full/background bind on page 325
Binding Hot Spare drives on page 327
About RANKs and LUNs in Storage Utility on page 269

Binding Hot Spare drives

Prerequisites are as follows:

- You must access Storage Utility (via the K2 System Configuration application login) with permissions equivalent to K2 administrator or higher.
- When you access Storage Utility, the K2 SAN must be offline.
- All iSCSI clients and K2 clients in the K2 SAN must be shut down.

You can bind disks as hot spare drives. Hot spare drives are on standby and are used in the event of a drive failure in a RANK. If a drive fails, the RAID Controller automatically selects a hot spare drive to use in place of the failed drive. This prevents the system from operating in a degraded state.

If the drives you want to designate as hot spares are bound as part of a RANK, you must unbind the drives first, then bind them as hot spares. To function as a Hot Spare, the drive must be at least as fast and have at least as much capacity as the failed drive it replaces.

1. In Storage Utility, right-click the **Unbound** node for a controller, then select **Bind** in the context menu. (Peer controllers that share the same set of disks are automatically selected as a pair.)

   The Binding dialog box opens showing all unbound disks for the controller listed in the Available Disk list.

2. Select **Hot Spare** using the BIND TYPE drop-down box.
3. In the Available Disks box, select the disk(s) to be used as hot spares, then click the add (arrow) button to add them to the Selected Disks list.

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click **OK** to close the Binding… dialog box and begin the binding process. The Progress Report dialog box opens, showing the status of the binding process.
5. Upon 100% completion, click **Close** in Progress Report window.
6. Restart the K2 Media Server.

Loading RAID controller and expansion chassis microcode

You might be instructed in K2 Release Notes to upgrade the RAID Controller microcode and/or expansion chassis on the RAID chassis. This allows you to take advantage of the RAID enhancements and benefit from improved reliability.

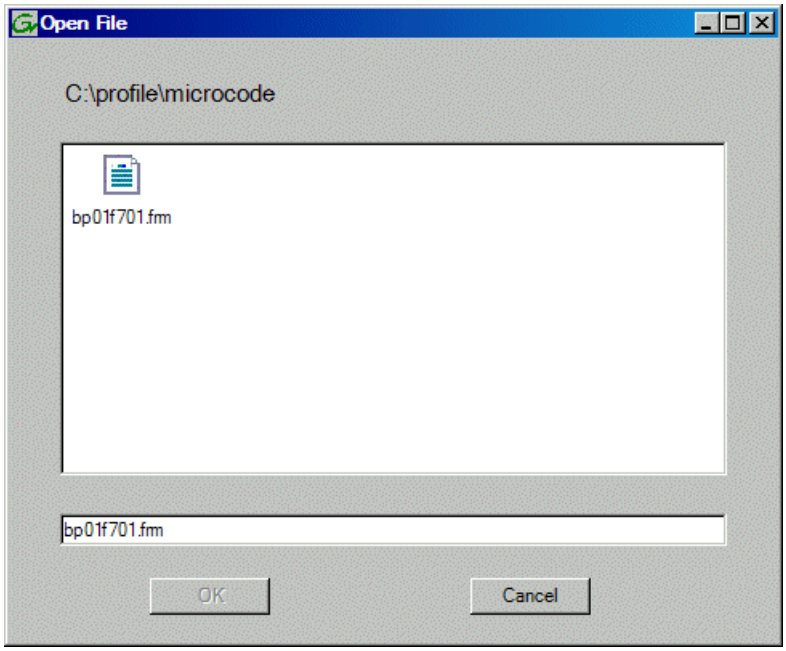
1. If upgrading expansion chassis microcode, take the RAID system offline.

2. In Storage Utility, right-click a controller in the tree view, then do one of the following:

   - To load controller microcode select **Advanced | Load Controller Microcode**
   - To load expansion chassis microcode select **Advanced | Load Disk Enclosure Microcode**

   Redundant controllers that share the same set of disks are automatically selected and upgraded as a pair.

   The Open File dialog box appears.



3. In the Open File dialog box, browse to the latest controller microcode file, select the file, and click **OK**.
4. The Progress Report window appears showing the microcode upgrade task and the percentage completion.
5. On 100% completion, proceed as follows:

   - If the RAID controller chassis has redundant controllers, power cycle the RAID controller chassis, then restart the K2 Media Server.
   - If the RAID controller chassis does not have redundant controllers, no power cycle is required. The firmware download is complete.

Downloading disk drive firmware

Prerequisites are as follows:

- All K2 clients and other clients must be powered down, or in some other way disconnected from the K2 SAN.
- The K2 Media Server through which Storage Utility is connected to the RAID Storage must be powered up.

- All other K2 Media Servers must be powered down.

You might be instructed in K2 Release Notes to upgrade disk drive firmware. This allows you to take advantage of the disk drive enhancements and benefit from improved performance and reliability.

To determine your disk drive type and current firmware version, select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane. Use the following procedure if you need to download disk drive firmware.

NOTE: The disk drives on each controller are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.

1. Refer to *K2 Release Notes* to determine firmware types, versions, files, and any other special instructions regarding the particular disk drive firmware you are downloading.
2. In the Storage Utility, right-click a controller in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.

   The Open File dialog box opens.

   ⚠ ***CAUTION: Do not attempt to download firmware to a single disk, unless directed to do so by Grass Valley. Downloading to a single disk can trigger a disk rebuild, with potential loss of data.***

3. In the Open File dialog box, browse to the desired firmware file for your disks, select the file, and click **OK**.

   As instructed by a message that appears, watch the lights on the drives. For each drive, one at a time, the lights flash as firmware loads. Wait until the lights on all the drives on which you are downloading firmware have completed their flashing pattern. This can take several minutes.

   The Progress Report window appears showing the disk firmware download task and the percentage complete.

4. When finished, restart the K2 Media Server.

Replacing a disk module

In the event of a disk drive failure, you'll repair the system by replacing the disk module as soon as possible. Refer to the Instruction Manual for your RAID storage chassis for information on removing and replacing disk modules.

NOTE: Always use Storage Utility to physically identify the failed disk module. Accidently removing the wrong disk module can destroy all media on the disk drives.

When the RAID controller detects that the disk module has failed, it automatically disables the disk module. This is reported in Storage Utility, and you should verify that the disk module is disabled before removing it.

In some cases you might suspect that the disk module is going bad, but the controller has not yet detected a failure and has therefore not yet disabled the drive. In this case you should manually disable the disk module before you remove it. This avoids momentary interruptions in signal output that can occur. The disabled state is persistent and the disk remains disabled even if the RAID chassis is restarted. After replacing the disabled disk module, the disk rebuild process starts automatically, which also enables the disk module.

1. Open Storage Utility.

2. Expand the tree view to display bound disks.

   NOTE: Disks modules may not be visible in the tree view if they are part of a newly bound RANK. You must restart your RAID chassis and the K2 Media Server to allow the drive modules to be seen in Storage Utility.

3. Identify the disk in question.
4. Select the disk module icon and check its status, then proceed as follows:

   - If the disk module reports as disabled, proceed to the next step in this procedure.
   - If the disk module reports as online, right-click the disk module and select **Advanced | Disable Drive**, then click **OK** to continue. A message "…operation succeeded…" appears. The disk is disabled, as reported by the disk fault LED.

   NOTE: If you accidentally disable the wrong disk module, you can enable it again by removing it and then replacing it in the chassis.

5. Remove and replace the disk module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.

   On inserting the replacement disk module, the RAID controller automatically starts rebuilding the drive. You can verify rebuild status by looking at the disk access LED on the front of the disk module, or by checking disk status in Storage Utility.

6. Wait approximately 1 minute for the disk to initialize.

   The disk ready LED is flashing.

7. To check rebuild status, do the following:

   a) Select the replacement disk icon in Storage Utility, then view the disk status in the right-hand pane. You may need to refresh the Storage Utility display. On completion, the drive status changes from Rebuilding to Online.

Related Topics

Identifying disks on page 321

Replacing a controller

If the RAID chassis has a single controller (non-redundant), you must take the K2 SAN offline before replacing a failed controller. Refer to procedures in the Instruction Manual for your RAID storage chassis. The remainder of this procedure does not apply to non-redundant systems.

If the RAID chassis has redundant controllers and is properly cabled and configured for a redundant K2 SAN, you can replace a failed controller while media access is underway, as described in this procedure. When a controller detects a fault on its redundant partner controller, the good controller disables the faulty controller automatically. In most cases an error message informs you of the fault and when you check the controller's status in Storage Utility it reports as disabled.

However, you can also manually disable a controller. In the event that one of the RAID controllers appears operational, but also reports faults through various log files and status indicators, you can choose to disable the controller and replace it. Disabling the controller and removing it in this way avoids interruptions in signal output that can occur if the module fails or if it is simply hot swapped while it is the active controller. When the replacement RAID controller module is installed, it is automatically enabled and becomes the backup controller.

On a RAID chassis with two controllers, if the replacement controller's firmware is not the same as the firmware on the redundant (currently installed) controller, the firmware on the replacement controller is automatically upgraded or downgraded to match the current system level firmware.

NOTE: Refer to the Instruction Manual for your RAID storage chassis for procedures on removing and replacing the RAID controller module.

1. Open the Storage Utility.
2. Expand the tree view to display the controllers.
3. Select the controller and check its status, then proceed as follows:
   - If the faulty controller reports as disabled, proceed to the next step in this procedure.
   - If the faulty controller reports as online, right-click the controller icon in the tree view, and select **Advanced | Disable Controller 0** or **Disable Controller 1**, then click **OK** to continue.

   The RAID controller is disabled. You can check controller status in the Storage Utility. You may need to refresh the display.

   NOTE: If you accidentally disable the wrong controller, you can enable it again by removing it and then replacing it in the chassis.
4. Remove and replace the disabled RAID controller module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.
5. On inserting the replacement RAID controller, it initializes and is automatically enabled to become the "backup" RAID controller.

Configuring RAID chassis network and SNMP settings

Through Storage Utility you can configure the following settings on a RAID chassis:

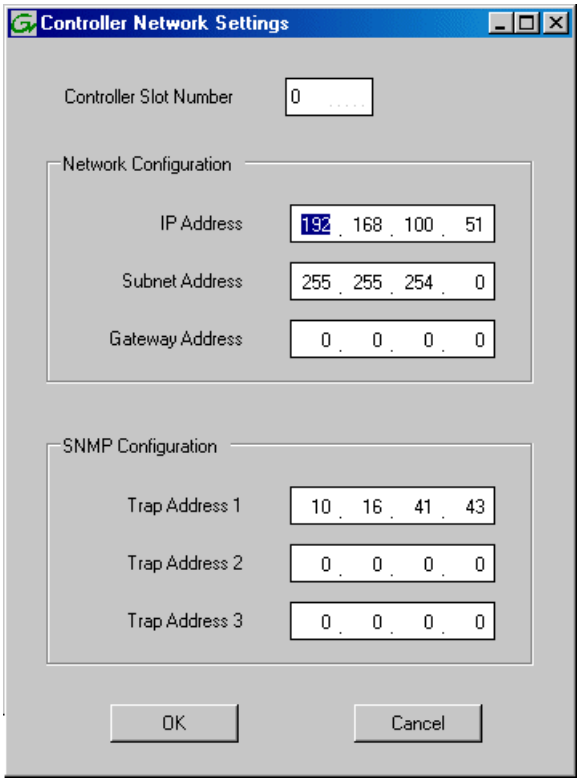
- IP address
- Subnet mask
- Gateway Address
- SNMP trap destinations

Whenever you modify control network settings or FTP/streaming network settings on any device, you must then redeploy the hosts file if that is your name resolution mechanism.

For the 10G RAID chassis, network and SNMP settings are set and stored on the RAID controller. Therefore, if the RAID chassis has two controllers, each controller must be configured separately, as in the following procedure.

1. In the K2Config application tree view, open the node for a K2 Media Server and select the **File System Server** node to open its property page. On the property page click **Launch Storage Utility**. Storage Utility opens. You can now configure the network settings on the controller connected to the selected K2 Media Server.

2. In the Storage Utility, right-click the icon for a RAID controller and select **Configuration | Network Properties**. The Network Settings dialog box opens.



3. In the Controller Slot Number field enter **0** and then press **Enter**. The settings from controller 0 are loaded into the Controller Network Settings dialog box and are available for you to modify.
4. Enter the control network IP address and other network settings.
5. You want SNMP trap messages go to the NetCentral server PC, so for SNMP Configuration enter the IP address of the NetCentral server PC. You can also enter IP addresses for other SNMP managers to which you want to send SNMP trap messages.
6. If the RAID chassis has two controllers, in the Controller Slot Number field enter **1** and then press **Enter**. The settings from controller 1 are loaded into the Controller Network Settings dialog box and are available for you to modify. Repeat the previous steps to configure controller 1.
7. Click **OK** to save settings and close.
8. Restart the RAID chassis to put SNMP configuration changes into effect.

Replacing a controller

If the RAID chassis has a single controller (non-redundant), you must take the K2 SAN offline before replacing a failed controller. Refer to procedures in the Instruction Manual for your RAID storage chassis. The remainder of this procedure does not apply to non-redundant systems.

If the RAID chassis has redundant controllers and is properly cabled and configured for a redundant K2 SAN, you can replace a failed controller while media access is underway, as described in this procedure. When a controller detects a fault on its redundant partner controller, the good controller

disables the faulty controller automatically. In most cases an error message informs you of the fault and when you check the controller's status in Storage Utility it reports as disabled.

However, you can also manually disable a controller. In the event that one of the RAID controllers appears operational, but also reports faults through various log files and status indicators, you can choose to disable the controller and replace it. Disabling the controller and removing it in this way avoids interruptions in signal output that can occur if the module fails or if it is simply hot swapped while it is the active controller. When the replacement RAID controller module is installed, it is automatically enabled and becomes the backup controller.

On a RAID chassis with two controllers, if the replacement controller's firmware is not the same as the firmware on the redundant (currently installed) controller, the firmware on the replacement controller is automatically upgraded or downgraded to match the current system level firmware.

NOTE: Refer to the Instruction Manual for your RAID storage chassis for procedures on removing and replacing the RAID controller module.

1. Open the Storage Utility.
2. Expand the tree view to display the controllers.
3. Select the controller and check its status, then proceed as follows:
   - If the faulty controller reports as disabled, proceed to the next step in this procedure.
   - If the faulty controller reports as online, right-click the controller icon in the tree view, and select **Advanced | Disable Controller 0** or **Disable Controller 1**, then click **OK** to continue.

   The RAID controller is disabled. You can check controller status in the Storage Utility. You may need to refresh the display.

   NOTE: If you accidentally disable the wrong controller, you can enable it again by removing it and then replacing it in the chassis.
4. Remove and replace the disabled RAID controller module.

   Refer to procedures in the Instruction Manual for your RAID storage chassis.
5. On inserting the replacement RAID controller, it initializes and is automatically enabled to become the "backup" RAID controller.

Working with Ethernet switches

Use the following sections when designing, configuring, or servicing a Gigabit Ethernet switch that is part of an existing K2 SAN.

Design considerations for Ethernet switches

The following information was qualified using the HP ProCurve switch. You must use the HP ProCurve switch for iSCSI traffic. However, for control and FTP/streaming traffic, it is allowed to use a different brand of switch, such as a Cisco Catalyst switch, if required by your site. If you are using a non-HP switch, apply the information accordingly. Refer to the documentation you received with the switch as necessary.

The primary factors that influence the number and configuration of switches on a K2 SAN are as follows:

- Redundancy — Non-redundant K2 SANs have only one media (iSCSI) network and can operate with a single switch. Redundant K2 SANs have an "A" media network and a "B" media network and require at least two switches, so that the A network and the B network never share the same switch. Media traffic does not cross between an "A" switch and a "B" switch, so if there are Inter-Switch Links (ISLs) between redundant switches, media traffic does not use these ISLs.
- Separation of iSCSI traffic — Media (iSCSI) traffic must be kept separate from control traffic, FTP/streaming traffic, and any other type of traffic. The recommended way to provide this separation is to configure each switch to have two VLANs, with half the switch's ports on each VLAN. The media (iSCSI) traffic uses one VLAN and all other traffic uses the other VLAN. This "other" traffic can include both FTP and control traffic, as it is allowed that they be on the same VLAN. On very large multiple switch systems, designers with sufficient knowledge can use other options for providing the separation of iSCSI traffic, such as using one switch or fabric exclusively for media traffic and another switch or fabric exclusively for non-media traffic.
- FTP bandwidth — This is a consideration if using multiple switches that share the FTP traffic. In this case you must use sufficient ISLs to provide the bandwidth needed to support your FTP traffic load between switches. Only control traffic and FTP traffic use ISLs, but since FTP traffic is more variable and has potentially higher bandwidth needs, it is the primary consideration when designing ISLs. You do not need to consider iSCSI bandwidth on ISLs.

Using three 1 Gig ISLs to connect switches is the default configuration for all K2 SANs. This provides sufficient bandwidth for most FTP traffic loads. The10 Gig ports on the switch connect to the K2 Media Server and are available for connection to the optional NH server. Other ISL configurations are also available, as explained below.

Connect and configure ISLs only as specified in the following table, taking your FTP bandwidth into consideration:

Maximum FTP bandwidth	Trunk/ISLs required
Less than 100 MB/sec	A trunk with three 1 Gb/s ISLs
100 - 300 MB/sec	A trunk with five 1 Gb/s ISLs
More than 300 MB/sec	A trunk with two 10 Gb/s ISLs

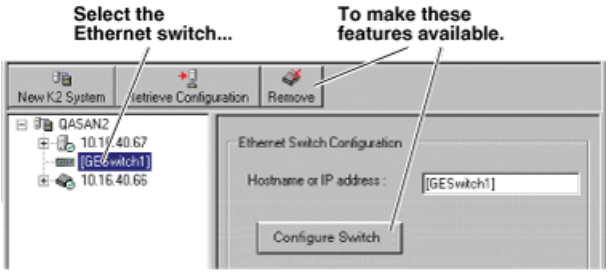
NOTE: One Gig ISLs must be an odd number (3 or 5).

- Port count — The number of client connections, FTP/streaming connections, and other connections determine how many ports are required. As the port count increases, you must use switches with more ports and/or multiple switches. When multiple switches are used, the port count assigned to each VLAN and the ports used for ISLs must be considered.

Based on these factors, determine the number of switches, the number of ports on each switch, and the ISLs required for your system needs. You can find procedures for configuring the HP ProCurve switch in the chapters elsewhere in this manual for installing each level. Adapt the procedures according to your switch design as you configure your switches.

Configuring a switch through the K2Config application

In the K2 System Configuration (K2Config) application , features for working on a Ethernet switch are as follows:



From the K2Config application, you can click the **Configure Switch** button to open the switch's web configuration application. Refer to the installation procedures elsewhere in this document for switch configuration information.

Verifying spanning tree settings

Use the following procedures to check and (if necessary) set your HP ProCurve Ethernet switches to have the proper spanning tree settings. These procedures apply to the 2900 series switches. Refer to installation chapters earlier in this manual for the complete switch configuration procedures.

Check the switch firmware version

Do not do this task if:

- Your HP ProCurve 29xx series switch already has the current required firmware version.

Do this task if:

- Your HP ProCurve 29xx series switch does not have the current required firmware version.

Refer to compatibility information earlier in these release notes for firmware version requirements.

You must have the proper version of firmware on the switch to be able to check and make the settings.

1. Telnet to the switch and login with the administrator username and password.
2. At the switch console command (CLI) prompt, type the following, then press **Enter**:

   `menu`

   If prompted to save the current configuration, answer no (press the n key) to proceed.

   The main menu opens.
3. From the main menu, tab to **Command Line (CLI)** and press **Enter**. The command prompt appears.

4. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

   ```
   show flash
   ```

   Information is displayed similar to the following example:

   ```
   HP_iSCSI_switch1# show flash
   Image           Size(Bytes)   Date    Version
   -----           ----------  --------  -------
   Primary Image   : 6737518   07/25/08  T.13.23
   Secondary Image : 5886358   10/26/06  T.11.12
   Boot Rom Version: K.12.12
   Current Boot    : Primary
   ```

5. Check the Primary Image Version and refer to related topics in "K2 Release Notes" for information about currently supported versions. If instructed to change the firmware on the switch, do so before continuing.
6. Check the Primary Image Version and refer to compatibility information earlier in these release notes. If instructed to change the firmware on the switch, do so before continuing.

Related Topics

Upgrading firmware on HP switch on page 75

Check spanning tree settings

1. If you have not already done so, telnet to the switch and login with the administrator username and password.
2. At the switch console command (CLI) prompt, type the following and press **Enter**:

   ```
   show spanning-tree
   ```

   Spanning tree information is displayed.

3. Check the spanning tree information and make sure that settings are correct, as follows:

   ```
   STP Enabled: Yes
   Force Version: RSTP-operation
   ```

4. If settings are correct, no further configuration is required.
5. If settings are not correct, you have the following options:

   - If you have one switch only and the switch is not connected to any other switches, these spanning tree settings are recommended, but not required. You should make the correct settings at your next opportunity when it is convenient.
   - If your switch is connected to another switch, either because you have a multi-switch K2 SAN or for any other reason, these spanning tree settings are required. You must correct your spanning tree settings as soon as possible.

Changing spanning tree settings requires a restart of the switch, so you must make the settings while the K2 SAN is offline. When you can take your system offline, configure RSTP (spanning tree).

Configure RSTP

The following procedure is for the HP ProCurve switch 29xx series. Do not use this procedure on other switch models.

1. Stop all media access on the K2 SAN.

2. If you have not already done so, telnet to the switch and login with the administrator username and password.
3. At the switch console command (CLI) prompt, type the following and then press **Enter**:

   `configure`

   You are now in configuration mode.
4. Set spanning tree to RSTP. To do this, type the following, then press **Enter**:

   `spanning-tree force-version rstp-operation`

   This configures spanning tree, but it does not turn spanning tree on. You must turn spanning tree on using the switch's Web interface.
5. Type the following, then press **Enter**:

   `menu`

   When prompted, save the configuration by pressing the y key.

   The main menu opens.
6. Proceed as follows, depending on the STP Enabled setting that you discovered when you checked spanning tree settings:

   - If STP Enabled is already set to Yes, no further configuration is required. Restart the switch to put changes into effect.
   - If STP Enabled is set to No, you must enable spanning tree using the switch's Web interface.

Enable spanning tree

The following procedure is for the HP ProCurve switch 29xx series. Do not use this procedure on other switch models.

1. From the control point PC or another PC, make sure that you have a direct Ethernet cable connection to the switch, with no switches, routers, proxies, or other networking devices in between.
2. On the PC, open Internet Explorer and type the switch's IP address in the Address field, as in the following example.

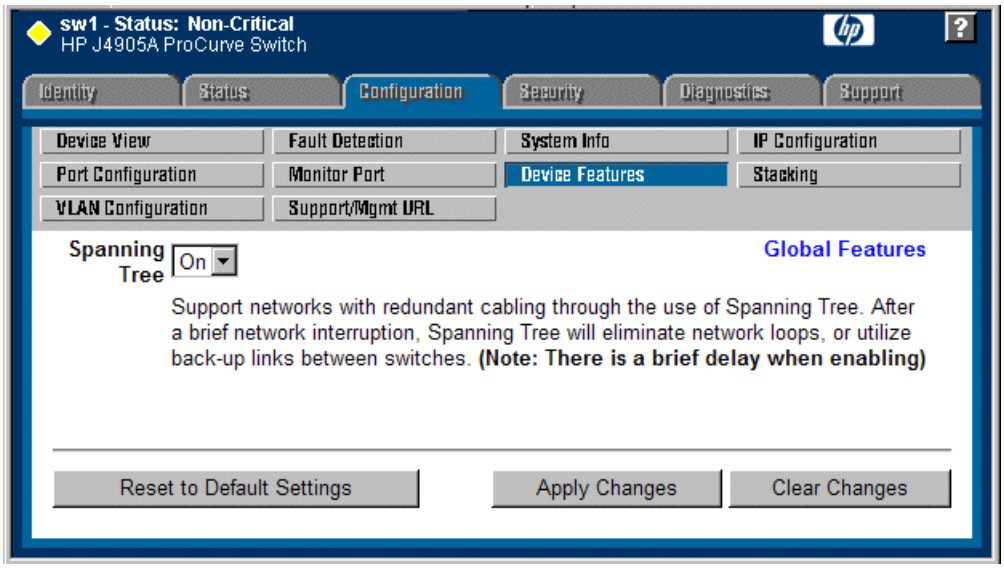
   `http://192.168.100.61`

   This should be the name or IP address as currently configured on the switch.
3. Press **Enter** to open the switch's configuration application.

   NOTE: The configuration application for the HP ProCurve switch requires Java.

   You can also access the switch's configuration application from the K2Config application.

4. In the switch's configuration application, choose **Configuration**, then **Device Features**.



5. Set Spanning Tree to **On** and click **Apply Changes**.

   If prompted, log in with the switch's administrator username and password.

6. Close the switch configuration application.
7. Restart the switch to put changes into effect.

Upgrading firmware on HP switch

1. If you have not already done so, install a TFTP Server.

   For example, to install *tftpd32.exe*, go to *http://tftpd32.jounin.net/*.

2. Open the TFTP Server.
3. Make sure your current working directory includes the **.swi* file that you are using for the upgrade.
4. Execute the copy command with the following syntax:

   ```
   copy tftp flash <ip-address> <remote-os-file> [ < primary | secondary > ]
   ```

   Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

   For example, to download a software file named T_13_23.swi from a TFTP server with the IP address of 10.16.34.3 1, use the following:

   ```
   ProCurve # copy tftp flash 10.16.34.3 T_13_23.swi
   ```

5. When prompted `The primary OS image will be deleted. continue [y/n]?`, press **Y**.

   When the switch finishes downloading the software file from the server, it displays the progress message `Validating and Writing System Software to FLASH...`

6. Wait until the CLI prompt re-appears, then continue with the next step in this procedure.
7. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

   `show flash`

   Information is displayed similar to the following example:

```
HP_iSCSI_switch1# show flash
Image           Size(Bytes)   Date    Version
-----           ----------  --------  -------
Primary Image   : 6737518   07/25/08  T.13.23
Secondary Image : 5886358   10/26/06  T.11.12
Boot Rom Version: K.12.12
Current Boot    : Primary
```

8. Verify that the new software version is in the expected flash area (primary or secondary).
9. Restart the switch from the flash area that holds the new software (primary or secondary).

Appendix **A**

Custom K2 SAN systems

This section contains the following topics:

- *About custom K2 SAN systems*
- *About custom K2 SAN information*
- *System diagrams*
- *Explanations and procedures*

About custom K2 SAN systems

Custom systems extend the infrastructure of standard K2 SAN product bundles. For example, a custom K2 SAN has multiple primary RAID chassis connecting to K2 Media Servers via a Fibre Channel fabric consisting of one or more Fibre Channel switches. This is an extension of the Fibre Channel infrastructure of a standard K2 SAN, which has a single primary RAID chassis connecting to one or more K2 Media Servers via direct Fibre Channel connection. Only qualified Grass Valley personnel that have received K2 SAN technical training should attempt to design, install, and configure custom K2 SAN systems. Refer to related topics in this document for more information on custom K2 SAN systems.

About custom K2 SAN information

The information in this section applies to custom-designed K2 SAN systems, built with recently released Grass Valley hardware and software products. Custom systems of this type are also called Level 40 systems.

This information assumes that the reader understands and has access to the baseline information about standard, pre-defined K2 SAN systems as presented in customer documentation. The customer documents that relate to the K2 SAN system are as follows:

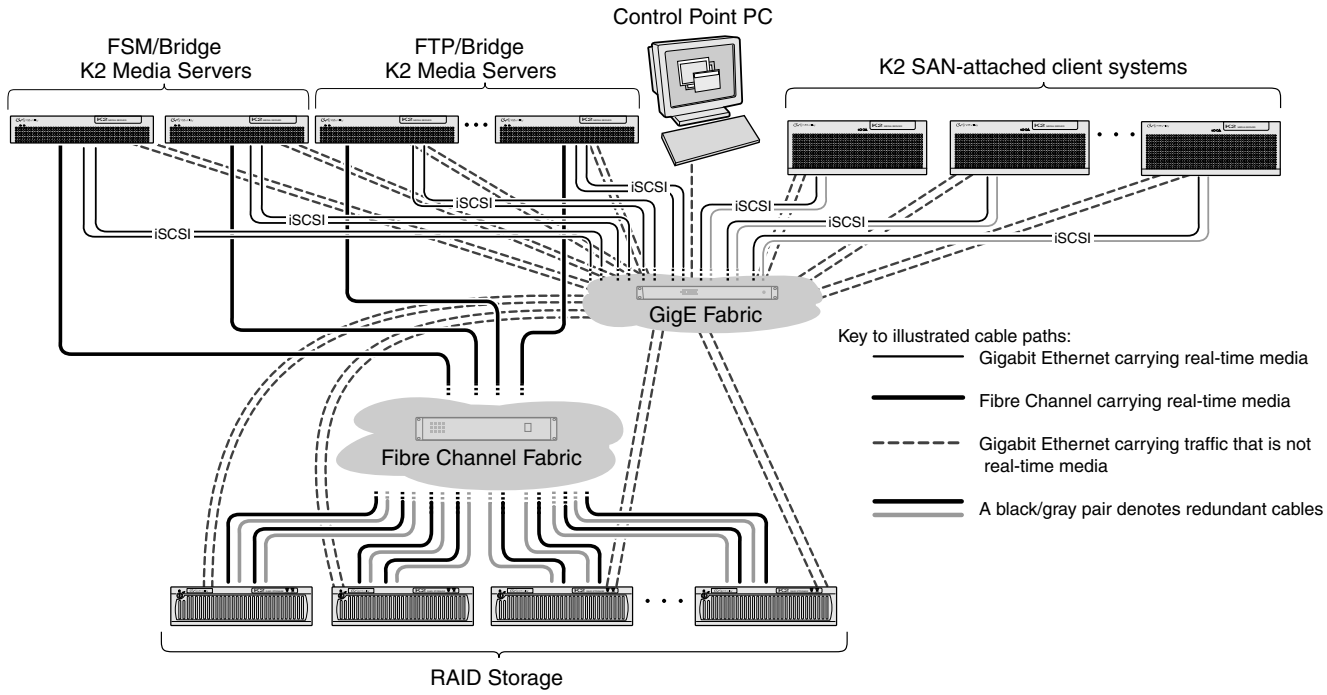
- K2 SAN Installation and Service Manual
- K2 System Guide
- K2 RAID Instruction Manual
- K2 Release Notes

These documents are intended for customers with standard systems. While much of the information in these customer documents also applies to custom systems, in most cases you must interpret and extend the information in order to apply the procedures to a custom system.

System diagrams

The following sections provide high-level diagrams of example systems with guidelines for commissioning and operating.

iSCSI extended (redundant FSMs)



This system differs from the Level 3R system as follows:

- A Fibre Channel switch fabric, comprised of one or more Fibre Channel switches, is interposed between K2 Media Servers and the RAID Storage devices. This allows more RAID Storage devices to be connected, which provides higher bandwidth and more storage space.
- Additional FTP/Bridge K2 Media Servers are added, providing additional iSCSI bridges to support more clients and higher bandwidth clients.

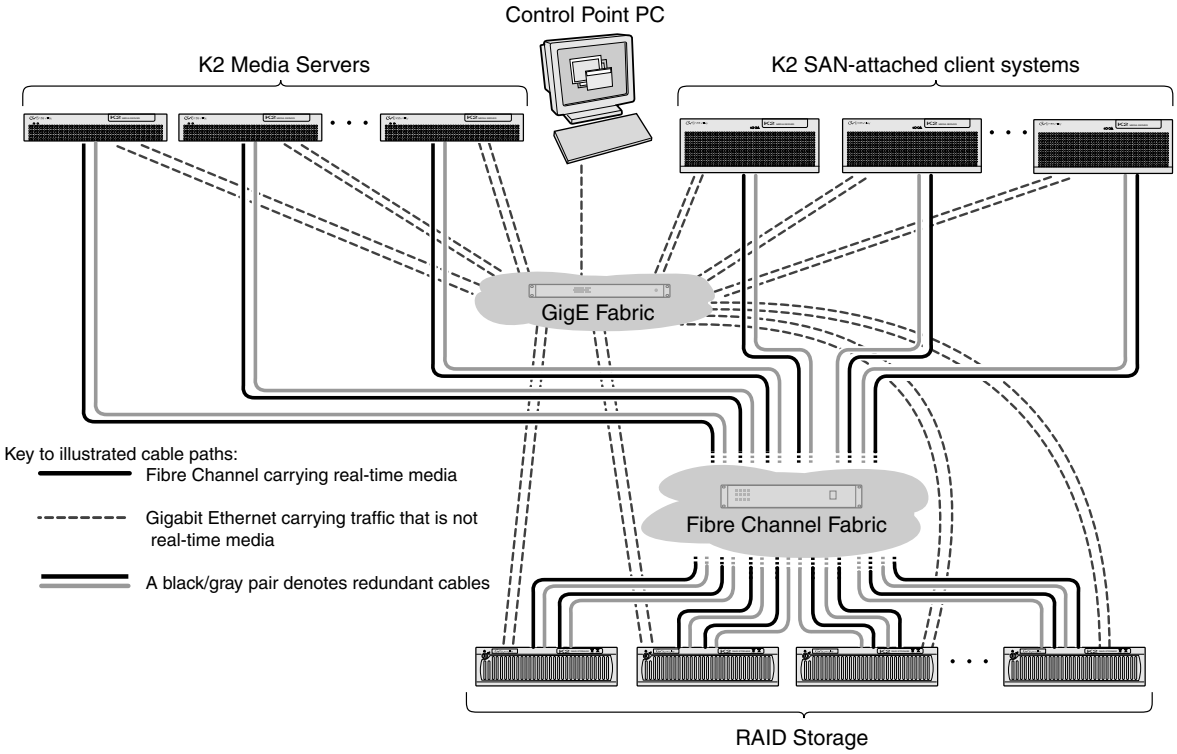
Guidelines for this system are as follows:

- The Fibre Channel switch fabric must be zoned.

Related Topics

Fibre Channel switch zoning on page 347

Fibre Channel connected clients (redundant FSMs)



This system differs from the iSCSI extended system as follows:

- K2 SAN-attached client systems have a Fibre Channel card installed and are connected directly to the Fibre Channel Fabric. This replaces the iSCSI layer.
- Because there is no iSCSI, there is no need for multiple K2 Media Servers to act as iSCSI bridges, reducing the total number of K2 Media Servers required.
- There is a RAID chassis dedicated for file system metadata.
- The FSM K2 Media Servers read/write data over Fibre Channel only to the metadata RAID chassis.
- The FSM K2 Media Servers must "see" (be on the same Fibre Channel fabric with) the media RAID, even though they do not read/write data to the media RAID.

Guidelines for this system are as follows:

- When adding a K2 SAN-attached client system in K2Config, set the Storage access option to **Fibre Channel**.
- When configuring the system in K2Config, select the **Server redundancy** option.

Explanations and procedures

The following information might or might not apply to your particular custom system. Make sure you understand the application of the information to your own custom system.

General guidelines

The following guidelines apply to all systems:

- Update to version 3.0.1.21 or higher before attempting to configure a custom system.
- For redundant systems, if there is only one RAID storage device, you can mix RAID 1 (for file system metadata) and RAID 5 or RAID 6 (for media storage) in the same chassis. However, if there are two or more RAID storage devices, you must reserve one chassis for RAID 1, with the remaining chassis used for RAID 5 or RAID 6.
- When you change the RTIOS, you must reboot the system for it to take effect.
- For a Fibre Channel SAN, the 8 Gig controller must be set to Fabric.
- When connecting iNavi make sure the browser has scripting turned on.

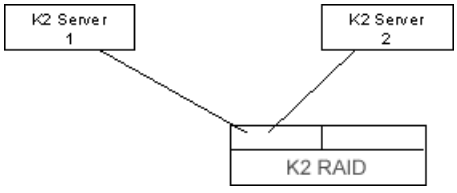
K2 RAID Fibre Channel port redundant configuration

In addition to the Level 3 non-redundant and Level 3 redundant configurations, you can also cable and use K2 RAID Fibre Channel ports for Fibre Channel port redundancy, as explained in this section.

For clarity, Level 3 non-redundant and Level 3 redundant configurations are included in the following illustrations:

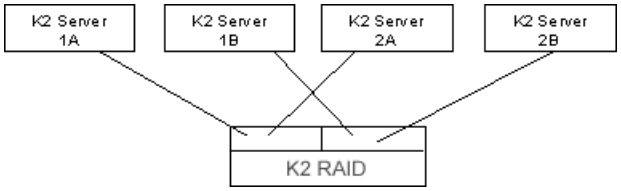
L3 non-redundant

Two K2 Servers connect to one RAID controller.



L3 redundant

Four K2 Servers connect to two RAID controllers. Servers 1A and 1B are redundant. Servers 2A and 2B are redundant.

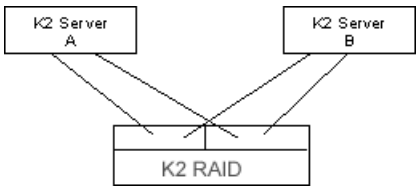


In the above examples, one K2 Server connects to one RAID controller only. This means there is no redundancy (failover) at the Fibre Channel port level. Redundancy in a system that uses this configuration must therefore be at the K2 Client/K2 Server level. For example, in a L3 redundant system, K2 clients can connect to either of a redundant K2 Server pair. This means that if K2 Server 1A goes down, K2 Clients connect to K2 Server 1B.

FC port redundant

NOTE: Do not use the FC port redundant configuration without first consulting with Grass Valley Server Engineering.

Two K2 Servers each connect to two RAID controllers. Servers A and B are redundant.



With this configuration the redundancy is at the Fibre Channel port level. If one of the FC ports, cables, or RAID controllers fails, the redundant connection takes over.

The following rules and policies apply to the FC port redundant configuration:

- Only use this configuration on systems that do not have a conflicting failover policy. For example, if a system is assembled with an iSCSI failover mechanism AND a Fibre Channel port failover mechanism, the policies of these two failover mechanisms can conflict during a failover event and result in scrambled data pathways. Examples of systems without conflicting failover policies are as follows:
  - A system with iSCSI clients that are non-redundant. This means the clients have just one connection to the iSCSI VLAN (media ports on GigE switch). Since there is no iSCSI failover in this type of system, there is no conflict with the Fibre Channel failover policy.
  - A system with Fibre Channel connected clients. Fibre Channel clients can be non-redundant (one FC cable connected to the FC switch) or redundant (two FC cables connected to the FC switch). The Fibre Channel failover policy is cohesive between FC client connections and FC RAID connections, so there is no conflict.
- Do not use this configuration on a system with redundant iSCSI clients, as this introduces a conflicting failover policy. If iSCSI clients are redundant and K2 Server FC ports are redundant, failover conflicts occur that render the system inoperable.

Installing SANsurfer Switch Manager software

Use the SANsurfer Switch Manager application to configure the QLogic Fibre Channel Switch. Install the software on the Control Point PC.

1. Close all programs currently running and insert the SANsurfer Switch Manager Installation Disk into CD-ROM drive.
2. Open the CD with Windows Explorer. Locate and run the following installation program file:

   `Windows_5.00.xx.xx.exe`
3. Follow on-screen instructions to install the software. Click Next to accept defaults.

Uninstalling SANsurfer Switch Manager software

When uninstalling the software, use the QLogic uninstall program in Program Files.

NOTE: Do not attempt to use Windows Control Panel Add/Remove Programs to uninstall SANsurfer Switch Manager.

The `UninstallerData` folder in the Install directory contains the uninstall program. Also, a shortcut/link to the uninstall program was installed in the installation directory during the SANsurfer Switch Manager installation process. The default installation directory is:

`C:\Program Files\QLogic_Corporation\SANsurfer`

1. Browse for the uninstall program file or the shortcut/link that points to the uninstall program file.

   The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANsurfer Switch Manager application.
2. Double-click the uninstall program file or shortcut/link, and follow the instructions to uninstall the SANsurfer Switch Manager application.

Fibre Channel switch domains

If a system has more than one SCSI Fibre Channel switch, such as in a redundant system, it is required that each switch have a unique domain number. This is a requirement for switches with ISLs AND for switches without ISLs. The Fibre Channel switch zoning procedure provides instructions for assigning domain numbers.

Fibre Channel switch zoning

The following procedure applies to a fabric with two QLogic SANbox 5600 Fibre Channel switches. On each switch there are two hard zones. All four zones are discrete—there are no ISLs connecting switches.

With this procedure you do the following on each switch:

- Assign a domain number to the switch
- Create a zone set
- Create two zones in the zone set
- Change the zone types from soft to hard (ACL)

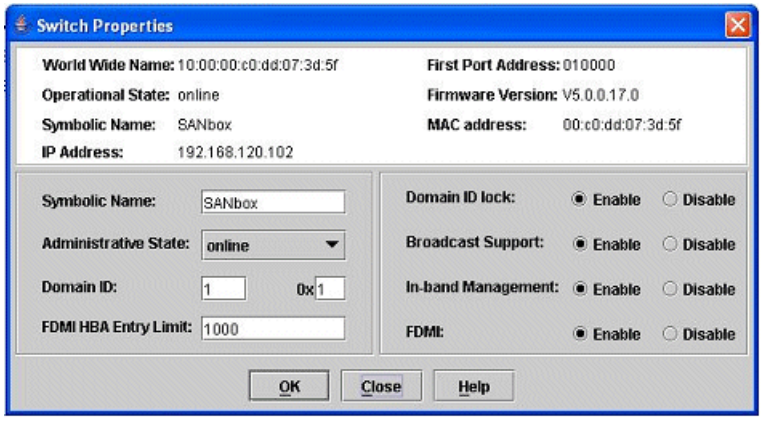
- Assign ports to zones

1. In SANsurfer Switch Manager, expand the tree view and select a Fibre Channel switch. For the purposes of this procedure, this switch is designated as switch A.

   The Faceplate display opens.

2. Open the **Switch** menu and select **Switch Properties**.

   The Switch Properties dialog box opens.



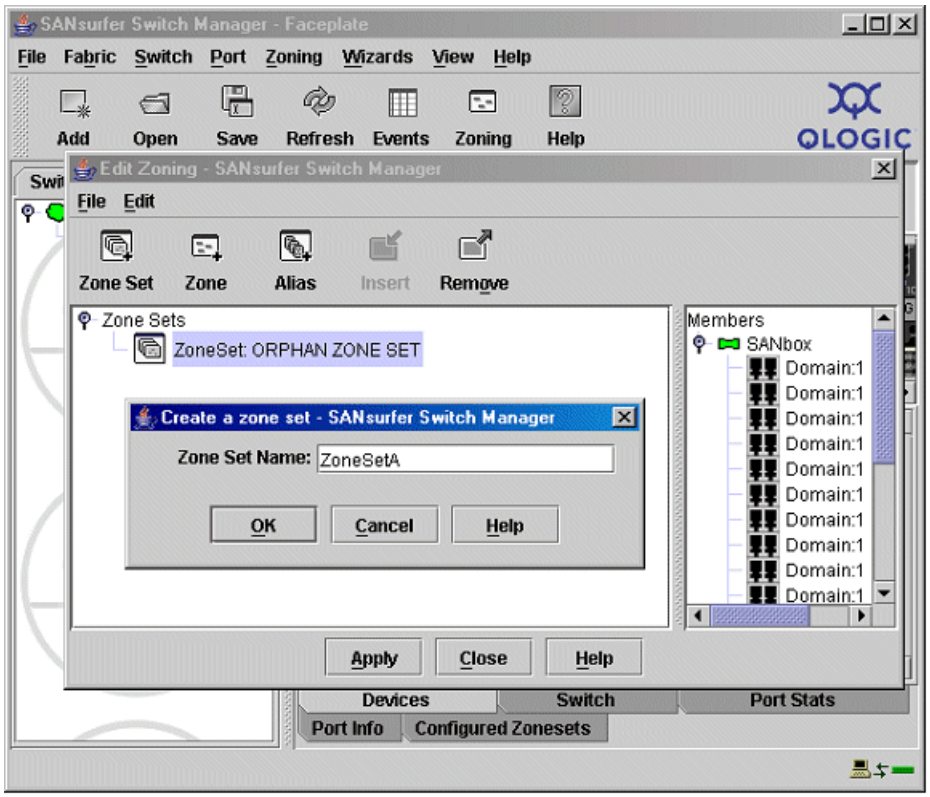
3. Set **Domain ID** to **1**.
4. Set **Domain ID lock** to **Enable**.
5. Click **OK**.

   SANsurfer Switch Manager updates the switch. When a message box reports status complete, click **OK**.

   The Switch Properties dialog box closes.

6. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.

7. Open the Edit menu, and select **Create Zone Set** to open the Create A Zone Set dialog.



8. Enter `ZoneSetA` as the name for the zone set, and click the **OK** button.

   The new zone set name is displayed in the Zone Sets tree. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, -, ^, and $.

9. Right-click **ZoneSetA** and select **Create A Zone** from the popup menu.

10. In the Create a Zone dialog, enter `Zone1` as the name for the new zone and click the **OK** button.

    The new zone name is displayed in the Zone Sets tree.

    NOTE: If you enter the name of a zone that already exists in the database, the SANsurfer Switch Manager application will ask if you would like to add that zone and its membership to the zone set.

11. Right-click **ZoneSetA** and select **Create A Zone** from the popup menu.

12. In the Create a Zone dialog, enter `Zone2` as the name for the new zone, and click the **OK** button.

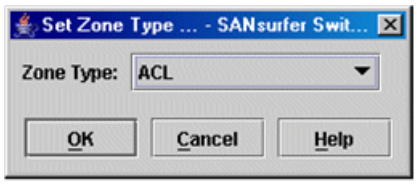
    The new zone name is displayed in the Zone Sets tree.

13. Click the **Apply** button. In the Save Zoning & Error Check dialog, click **Save Zoning**, then **Yes**, **OK**, and **Close** on subsequent message boxes.

    You can ignore a "Error activating zone set" message.

14. When a zone is created, its zone type is soft. For Zone1 and Zone2, change the zone type to a hard zone as follows:

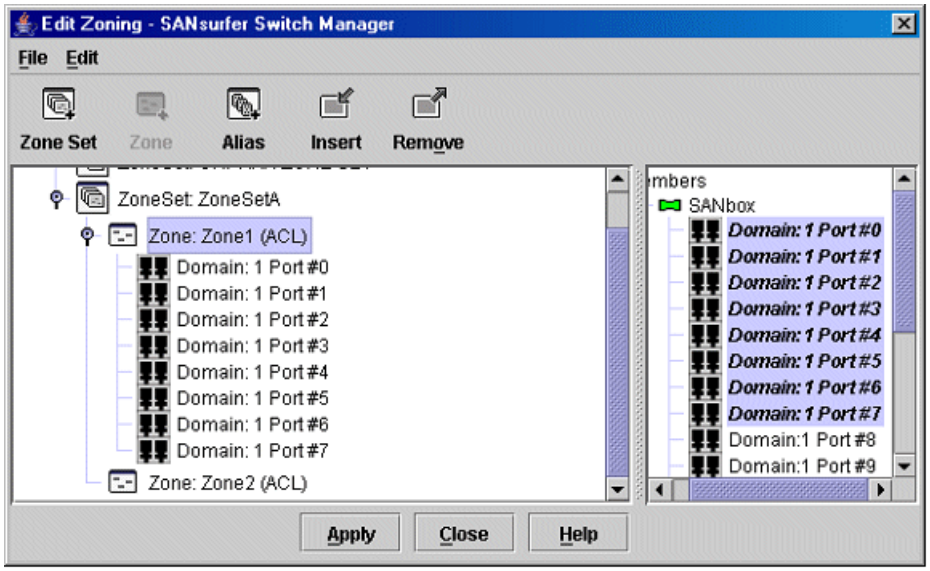
    a) In the Zone Sets tree, right-click the zone and select **Set Zone Type** from the popup menu.



    b) In the Set Zone Type dialog, open the Zone Type pull-down menu and select **ACL**, then click the **OK** button.

    c) Repeat steps for the other zone.

15. In the Port/Device tree on the right of the Edit Zoning dialog box, select ports **0 - 7** (Shift + Click) and drag them into the **Zone1**.



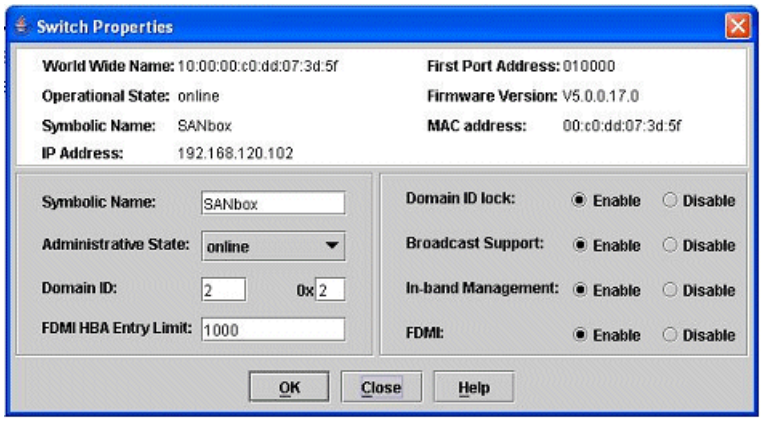
16. Click the **Apply** button. In the Save Zoning & Error Check dialog, click **Save Zoning**, then **Yes**, **OK**, and **Close** to save changes to the zoning database.

17. In the Port/Device tree on the right of the Edit Zoning dialog box, select ports **8 - 15** (Shift + Click) and drag them into the **Zone2**.

18. Click the **Apply** button. In the Save Zoning & Error Check dialog, click **Save Zoning**, then **Yes**, **OK**, and **Close** on to save changes to the zoning database.
19. Close the Edit Zoning dialog box.
20. Connect to the other switch as necessary to configure. In SANsurfer Switch Manager, expand the tree view and select the other Fibre Channel switch. For the purposes of this procedure, this switch is designated as switch B.

    The Faceplate display opens.
21. Open the **Switch** menu and select **Switch Properties**.

    The Switch Properties dialog box opens.



22. Set **Domain ID** to **2**.
23. Set **Domain ID lock** to **Enable**.
24. Click **OK**.

    SANsurfer Switch Manager updates the switch. When a message box reports status complete, click **OK**.

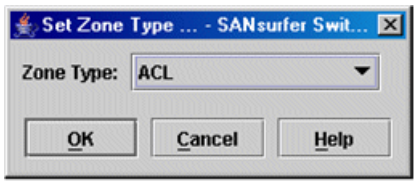
    The Switch Properties dialog box closes.
25. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
26. Open the Edit menu, and select **Create Zone Set** to open the Create A Zone Set dialog.
27. Enter `ZoneSetB` as the name for the zone set and click the **OK** button.

    The new zone set name is displayed in the Zone Sets tree.
28. Right-click **ZoneSetB** and select **Create A Zone** from the popup menu.
29. In the Create a Zone dialog, enter `Zone3` as the name for the new zone and click the **OK** button.

    The new zone name is displayed in the Zone Sets tree.
30. Right-click **ZoneSetB** and select **Create A Zone** from the popup menu.
31. In the Create a Zone dialog, enter `Zone4` as the name for the new zone and click the **OK** button.

    The new zone name is displayed in the Zone Sets tree.
32. Click the **Apply** button to save changes to the zoning database.

33. When a zone is created, its zone type is soft. For Zone3 and Zone4, change the zone type to a hard zone as follows:
    a) In the Zone Sets tree, right-click the zone and select **Set Zone Type** from the popup menu.



    b) In the Set Zone Type dialog, open the Zone Type pull-down menu and select **ACL**, then click the **OK** button.
    c) Repeat steps for the other zone.
34. In the Port/Device tree on the right of the Edit Zoning dialog box, select ports **0 - 7** (Shift + Click) and drag them into the **Zone3**.
35. Click the **Apply** button. In the Save Zoning & Error Check dialog, click **Save Zoning**, then **Yes**, **OK**, and **Close** to save changes to the zoning database.
36. In the Port/Device tree on the right of the Edit Zoning dialog box, select ports **8 - 15** (Shift + Click) and drag them into the **Zone4**.
37. Click the **Apply** button. In the Save Zoning & Error Check dialog, click **Save Zoning**, then **Yes**, **OK**, and **Close** to save changes to the zoning database.
38. Close the Edit Zoning dialog box.

The Fibre Channel switch zoning procedure is complete.

Fibre Channel fabric cabling

Make your cable connections symmetrical when cabling a multiple switch fabric. For example, for a K2 SAN-attached client system (or Server) that has redundant connections that each go to a different switch, if you make one connection to port 1 on switch A, make the other connection to port 1 on switch B. This is especially important on switches that are not interconnected by ISLs, as the Fibre Channel failover path can get confused if redundant cable connections are not in the same order on both switches.

The preceding procedure, "Fibre Channel switch zoning", applies to a system with four K2 Media Servers, two 16 port Fibre Channel switches, and four K2 RAID storage chassis with redundant controllers. To cable the Fibre Channel fabric for such a system, do the following:

- Each K2 Media Server is connected to a different zone. For example, connect as follows:
  - Connect K2 Media Server 1 to switch A port 0 (Zone 1)
  - Connect K2 Media Server 2 to switch A port 8 (Zone 2)
  - Connect K2 Media Server 3 to switch B port 0 (Zone 3)
  - Connect K2 Media Server 4 to switch B port 8 (Zone 4)

  There is only one Fibre Channel connection at each K2 Media Server. The second Fibre Channel port on each K2 Media Server not used.

- Each K2 RAID storage chassis is connected to all four zones. For example, connect RAID chassis 1 as follows:
  - Connect controller 0 port HP0 to switch A port 1 (Zone 1)
  - Connect controller 0 port HP1 to switch A port 9 (Zone 2)
  - Connect controller 1 port HP0 to switch B port 1 (Zone 3)
  - Connect controller 1 port HP1 to switch B port 9 (Zone 4)

  Connect RAID chassis 2, 3, and 4 similarly.

Appendix **B**

Trademarks and Agreements

This section contains the following topics:

- *Trademarks*
- *JPEG acknowledgment*

Trademarks

Grass Valley, STRATUS, K2, Aurora, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP, NetCentral, NewsBrowse, NewsEdit, NewsQ, NewsShare, NewsQ Pro, and Media Manager are either registered trademarks or trademarks of Grass Valley USA, LLC. in the United States and/or other countries. Grass Valley USA, LLC. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Grass Valley USA, LLC. trademarks and other proprietary rights may be found at www.grassvalley.com. Other trademarks and logos used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom.

JPEG acknowledgment

This software is based in part on the work of the Independent JPEG Group.

Index

A

Acronis, See recovery
adapters
    identifying 289
    naming 290
    reordering 291
administrative share on SiteConfig control point PC 77
Aurora
    expanding media file system by bandwidth 318

B

backup, See recovery
bandwidth
    about iSCSI 230
    determining K2 client iSCSI 230
basic nearline K2 SANs
    configuring 187, 190, 208
    configuring file system servers 196, 203, 214, 221
    configuring FTP servers 204
    configuring networks 149, 184, 195, 213, 225
    configuring server roles 193, 211, 223
    configuring servers 192, 203
    configuring software 194
    defining 129, 153, 188, 206
    prerequisites 187
basic online and production K2 SANs
    configuring 127, 130
    configuring database servers 145
    configuring file system clients NH servers 150, 185
    configuring file system servers 136, 142
    configuring FTP servers 146
    configuring iSCSI bridges 144
    configuring networks 135
    configuring NH FTP servers 151
    configuring NH server roles 147, 182
    configuring NH servers 147, 181
    configuring NH servers networks 149, 184, 195, 213, 225
    configuring NH servers software 148, 183
    configuring server roles 133
    configuring servers 132, 142
    configuring software 134
basic online and production K2 SANs *(continued)*
    defining 129, 153, 188, 206
    prerequisites 127
battery
    recovering from failure on K2 Media Server 296
bind/unbind
    basic nearline 198, 216
    basic online and production 138
    full/background 325
    hot spares 327
    RANK 324
    redundant nearline 198, 216
    redundant online and production 162
bridges, See iSCSI

C

cable
    HP switch basic nearline 54
    HP switch basic online or production 52
    HP switch redundant nearline 54
    HP switch redundant online or production 53
    K2 Media Server basic online or production 55
    K2 Media Server redundant online or production 55
    K2 RAID 57
    K2 RAID basic nearline 59
    K2 RAID basic online or production 58
    K2 RAID redundant nearline 60
    K2 RAID redundant online or production 59
    K2 Summit basic 51
    K2 Summit redundant 51
    length 52
    serial K2 Media server pinout 56
    server NH10GE basic nearline 57
    server NH10GE online or production 56
    server NH10GE redundant nearline 57
checklists
    infrastructures 40
    installations 40
    networks 40
    pre-installations 40
    SAN configurations 42
    software 41

clients 241, 276
  assigning FTP servers 241
  powering off 242
  taking offline 242
connect kit
  SiteConfig 78
control network
  SiteConfig 83
control networks
  descriptions 42
control point PCs
  accessing K2 SANs from multiple PCs 278
  description 258
  installing SiteConfig 77
  powering on 250
  screen resolution 77
  setting up 76
  system requirements 77
controllers
  replacing 330, 332
custom K2 SANs 342

D

database servers
  configuring basic online and production 145
  configuring redundant online and production 172
  configuring redundant online and production server B 179
databases
  configuring K2 clients on SANs 237
  recovering 319
definitions
  K2 storage terms 32
Dell 610 NH10GE
  cable redundant nearline 57
  cable basic nearline 57
  cable online or production 56
Dell R610 K2 Media Server
  cable basic online or production 55
  cable redundant online or production 55
deploying
  K2 software 114
deployment groups
  configuring 114
descriptions
  basic nearline K2 SANs 35
  basic online or production K2 SANs 33
  control networks 42
descriptions *(continued)*
  K2 SAN systems 32
  media (iSCSI) networks 44
  redundant nearline K2 SANs 36
  redundant online or production K2 SANs 34
  streaming/FTP networks 43
devices
  adding generic client to K2 SANs 241, 276
  adding to K2 SANs 276
Discovery Agent
  installing on K2 Media Server 122
DiscoveryAgentServiceSetup.msi 78
disk image, See recovery
disks
  binding basic nearline 198, 216
  binding basic online and production 138
  binding redundant nearline 198, 216
  binding redundant online and production 162
  flashing LEDs 323
  identifying 321
  loading firmware 328
  replacing module 329
domain
  configuring K2 Media Server 288
DP0/DP1 disk numbering 322

E

Ethernet
  adding switches to K2 SANs 277
  checking firmware versions 335
  configuring switches 335
  configuring switches via serial connection 64
  configuring switches via web connection 67
  design considerations for switches 333
  flow control on switches 74
  powering on switches 250
  QOS on switches 73
  RSTP settings on switches 336
  setting up switches 64
  spanning tree settings on switches 335, 336
  switch descriptions 259
  switch specifications 259
  upgrading firmware versions 75, 338
Ethernet switches
  upgrading firmware 75, 338
EULA 115
expanding media file system
  by bandwidth 314

expanding media file system *(continued)*
by bandwidth for Aurora products 318
by capacity 313

F

failover
recovering 284
triggering 283
failover behaviors 250
control team 251, 253
K2 Media Server 254
K2 Media Server with control team 255
media (iSCSI) 251, 253
pre-failover 251
features
K2 SANs 30
new 31
Fibre Channel
address ID 57
SiteConfig 103
fabric cabling 352
installing driver 296
K2 client connections 344
port redundant configuration 345
switch manager software 347
switch zones 347
file system clients
configuring K2 clients on SANs 238
file system servers
configuring basic nearline K2 SANs 196, 203, 214, 221
configuring basic online and production K2 SANs 136, 142
configuring redundant nearline K2 SANs 196, 203, 214, 221
configuring redundant nearline server B 226
configuring redundant online and production K2 SANs 159, 169
configuring redundant online and production server B 177
file systems
creating new basic nearline 201, 219
creating new basic online and production 140
creating new redundant nearline 201, 219
creating new redundant online and production 166
firmware
checking versions on switches 335
loading on RAID controller 327
firmware *(continued)*
loading on RAID disk 328
upgrading on Ethernet switches 75, 338
upgrading versions on switches 75, 338
flow control
Ethernet switches 74
FTP
assigning clients to servers 241
FTP/streaming network descriptions 43
FTP servers
configuring basic nearline 204
configuring basic online and production 146
configuring basic online and production NH servers 151
configuring redundant nearline 222
configuring redundant online and production 173
configuring redundant online and production NH servers 186
configuring server B redundant nearline 180, 227
configuring server B redundant online and production 180, 227
FTP/streaming network
SiteConfig 85

G

generic clients
configuring on SANs 241, 276

H

heartbeat cable pinout 56
host tables, See hosts files
hosts files 45
writing to devices 110
tips 45
hot spares
binding 327
HP switch
cable basic nearline 54
cable basic online or production 52
cable redundant nearline 54
cable redundant online or production 53
rack 52

I

image, See recovery

infrastructures
checklists 40
installations
checklists 40
installing
SiteConfig system requirements 77
iSCSI
about bandwidth 230
configuring basic online and production bridges 144
configuring initiator for K2 clients on SANs 239
configuring redundant online and production bridges 171
configuring redundant online and production server B bridges 178
determining K2 client bandwidth 230
media (iSCSI) network descriptions 44
replacing interface adapter 295
viewing assignments 280
iSCSI network
SiteConfig 87

J

java 77
jpeg
acknowledgment 356

K

K2 client
SiteConfig support 96
K2 clients
accessing features 301
adding to K2 SANs 302
configuring databases on SANs 237
configuring file system client on SANs 238
configuring iSCSI initiator client on SANs 239
configuring networks on SANs 236
configuring on SAN 233
configuring software on SANs 235
determining iSCSI bandwidth 230
identifying software versions 303
modifying control network settings 304
modifying media network settings 304
placing online 302
preparing 231
prerequisites 230
removing from K2 SANs 303
shutting down or restarting 302
K2 clients *(continued)*
taking offline 302
K2 Media Server
network SiteConfig 93, 103
SiteConfig support 96
adding to K2 SANs 277
K2 Media Servers
cable basic online or production 55
cable redundant online or production 55
accessing features 285
configuring IP 293
descriptions 260
identifying primary/backup from local server 282
identifying primary/backup from NetCentral 281
identifying primary/backup from the application 281
identifying software versions 287
licenses 231
licensing 299
modifying network settings 287
on domain 288
placing in service 287
powering off 244
recovering from failed system battery 296
removing from K2 SANs 293
replacing on K2 SANs 293
services 297
shutting down or restarting 287
specifications 260
taking out of service 285
K2 RAID
See also RAID basic nearline
cable 57
cable basic nearline 59
cable basic online or production 58
cable redundant nearline 60
cable redundant online or production 59
See also RAID basic nearline
K2 SANs
accessing features 274
configuring K2 clients 233
powering off 244
powering off devices 245
powering on basic online and production 246
powering on devices 245
powering on nearline 249
powering on redundant online and production 247
removing 278
renaming 276
system diagram basic nearline 50

K2 SANs *(continued)*
system diagram basic online or production 48
system diagram redundant nearline 50
system diagram redundant online or production 49
K2 Summit
network SiteConfig 91, 98
cable basic 51
cable redundant 51
configure write filter with K2Config 305
K2 System Configuration, See K2Config
K2Config
about 265
and SiteConfig settings 274
opening 266

L

LEDs
flashing RAID 323
legal
jpeg acknowledgment 356
trademarks 356
Level 40 342
licenses
verify on servers 231
licensing
adding 300
archiving 301
deleting 301
difficulties 300
K2 SANs 126
requesting 299
live streaming
configure multicast 306
login
SiteConfig 273
logs
RAID controller 323
LUNs
in Storage Utility 269

M

mapped network drive on SiteConfig control point PC 77
media file system
checking 310
expanding by bandwidth 314
expanding by capacity 313
media file system *(continued)*
making new 311
media network
SiteConfig 87
media networks
descriptions 44
metadata, See database
microcode
checking RAID controller microcode 321
loading on RAID controller 327
loading on RAID disk 328
Microsoft Windows
system requirement 77
MPIO
installing 232
multicast
configure for live streaming 306
MXF
about reference files 280

N

NetCentral
about 269
identifying primary/backup K2 Media Servers 281
screen resolution 77
networks
requirements for SiteConfig installation 77
checklists 40
configuring basic nearline K2 SANs 149, 184, 195, 213, 225
configuring basic online and production file system clients NH servers 150, 185
configuring basic online and production K2 SANs 135
configuring basic online and production NH servers 149, 184, 195, 213, 225
configuring K2 clients on SANs 236
configuring RAID basic nearline 136, 196
configuring RAID basic online and production 136, 196
configuring RAID redundant nearline 160, 214
configuring RAID redundant online and production 160, 214
configuring RAID settings 330, 332
configuring redundant nearline K2 SANs 149, 184, 195, 213, 225
configuring redundant nearline server B 149, 184, 195, 213, 225

networks *(continued)*
configuring redundant online and production file system clients NH servers 150, 185
configuring redundant online and production K2 SANs 159, 176
configuring redundant online and production NH servers 149, 184, 195, 213, 225
configuring redundant online and production server B 159, 176
configuring Server 2008 for domain 288
configuring Server 2008 IP 293
considerations and constraints 44
control network descriptions 42
hosts files 45
media (iSCSI) network descriptions 44
modifying control network settings on K2 client 304
modifying K2 Media Server control network settings 287
modifying K2 Media Server FTP network settings 288
modifying K2 Media Server media network settings 288
modifying media network settings on K2 client 304
restoring configuration on K2 Media Server 289
streaming/FTP network descriptions 43
tips 44
NH K2 Media Servers
descriptions 261
specifications 261
NH servers
configuring redundant online and production 147, 181
NH10GE servers
cable redundant nearline 57
cable basic nearline 57
cable online or production 56
non-redundant, See basic

O

offline
K2 clients 302
K2 Media Servers 285
K2 SANs 279
online
K2 clients 302
K2 Media Servers 287
K2 SANs 279
overviews
K2 SANs 30

P

passwords 272
pinouts
K2 Media heartbeat serial cable 56
power management settings 292
powering off
SAN clients 242
K2 client 302
K2 Media Servers 244
K2 SANs 244
RAID 245
SAN devices 245
powering on
basic online and production K2 SANs 246
control point PCs 250
Ethernet switches 250
K2 Media Servers 287
K2 SANs 245
nearline K2 SANs 249
redundant online and production K2 SANs 247
pre-installations
checklists 40
prerequisite files, SiteConfig 80
prerequisites
adding K2 clients 230
basic nearline K2 SANs 187
basic online and production K2 SANs 127
redundant nearline K2 SANs 205
redundant online and production K2 SANs 151
primary/backup K2 Media Servers
identifying 281

Q

QOS
Ethernet switches 73
K2 SANs 126
QuickTime
about reference files 280

R

rack
switch 52
RAID

RAID *(continued)*
See also K2 RAID
bind RANK 325
binding disks basic nearline 198, 216
binding disks basic online and production 138
binding disks redundant nearline 198, 216
binding disks redundant online and production 162
binding hot spares 327
checking controller microcode 321
checking subsystem status 321
configuring basic nearline 136, 160, 196, 214
configuring basic online and production 136, 160, 196, 214
configuring network and SNMP settings 330, 332
configuring networks and SNMP basic nearline 136, 196
configuring networks and SNMP basic online and production 136, 196
configuring networks and SNMP redundant nearline 160, 214
configuring networks and SNMP redundant online and production 160, 214
configuring redundant nearline 136, 160, 196, 214
configuring redundant online and production 136, 160, 196, 214
controller logs 323
descriptions 261
identifying disks 321
loading controller microcode 327
loading disk firmware 328
powering off 245
replacing controller 330, 332
replacing disk module 329
unbind RANK 324
See also K2 RAID
RANKs
in Storage Utility 269
recovery
about disk image process 116
activating Windows 123
creating image for E 118
media database 319
recommended process 117
restoring from generic image 120
restoring from system-specific image 119
strategies 116
redundancy
managing on K2 SANs 281
redundant nearline K2 SANs
check V:drives 204, 227
configuring 190, 205, 208
configuring file system server B 226
configuring file system servers 196, 203, 214, 221
configuring FTP server B 180, 227
configuring FTP servers 222
configuring networks 149, 184, 195, 213, 225
configuring networks server B 149, 184, 195, 213, 225
configuring server B roles 193, 211, 223
configuring server roles 193, 211, 223
configuring servers 210, 221
configuring software 212, 224
configuring software server B 212, 224
defining 129, 153, 188, 206
prerequisites 205
redundant online and production K2 SANs
check V:drives 186
configuring 151, 154
configuring database server B 179
configuring database servers 172
configuring file system clients NH servers 150, 185
configuring file system server B 177
configuring file system servers 159, 169
configuring FTP server B 180, 227
configuring FTP servers 173
configuring iSCSI bridges 171
configuring networks 159, 176
configuring networks server B 159, 176
configuring NH FTP servers 186
configuring NH server roles 147, 182
configuring NH servers 147, 181
configuring NH servers networks 149, 184, 195, 213, 225
configuring NH servers software 148, 183
configuring server B iSCSI bridges 178
configuring server B roles 157, 174
configuring server roles 157, 174
configuring servers 156, 169
configuring software 158, 175
configuring software server B 158, 175
defining 129, 153, 188, 206
prerequisites 151
reference files
about MXF 280
about QuickTime 280
configuring type 280

Remote Desktop
about 270
accessing 270
renaming
K2 SANs 276
restarting
K2 client 302
K2 Media Servers 287
Restripe Utility 319
roles
configuring basic nearline K2 SANs 193, 211, 223
configuring basic online and production K2 SANs 133
configuring basic online and production NH servers 147, 182
configuring redundant nearline K2 SANs 193, 211, 223
configuring redundant nearline server B 193, 211, 223
configuring redundant online and production K2 SANs 157, 174
configuring redundant online and production NH servers 147, 182
configuring redundant online and production server B 157, 174
routers
and SiteConfig 77
RSTP
settings on switches 336

S

sales tool 82
SAN configurations
checklists 42
security
applications 272
on K2 systems 272
serial cable pinout 56
Server 2008
configuring for domain 288
DHCP 293
Server Control Panel
about 267
using the stop button 286
services
K2 Media Servers 297
shutdown, See powering off
SiteConfig
support on K2 devices 96
about 264
and K2Config settings 274
credentials 273
Discovery Agent 78
discovery Server 2008 DHCP 293
importing system descriptions 127
installing 77
installing, about 77
main window 264
Network Configuration Connect Kit 78
opening 264
prerequisite files 80
upgrading 78
SiteConfig Discovery Agent
installing on K2 Media Server 122
SNMP
configuring RAID basic nearline 136, 196
configuring RAID basic online and production 136, 196
configuring RAID redundant nearline 160, 214
configuring RAID redundant online and production 160, 214
configuring RAID settings 330, 332
software
SiteConfig on K2 SAN 116
checking on devices 115
checklists 41
configuring basic nearline K2 SANs 194
configuring basic online and production K2 SANs 134
configuring basic online and production NH servers 148, 183
configuring deployment groups 114
configuring K2 clients on SANs 235
configuring redundant nearline K2 SANs 212, 224
configuring redundant nearline server B 212, 224
configuring redundant online and production K2 SANs 158, 175
configuring redundant online and production NH servers 148, 183
configuring redundant online and production server B 158, 175
deploying K2 software 114
identifying K2 client versions 303
identifying K2 Media Server versions 287
MPIO installing 232

spanning tree
    check settings on switches 336
    enable on switches 337
    settings on switches 335
Storage Utility
    about 268
    accessing 308
    overview 309
    RANKs and LUNs 269
streaming network
    SiteConfig 85
streaming/FTP networks
    descriptions 43
Summit, See K2 Summit
switch
    See also Ethernet
    rack 52
        See also Ethernet
switch HP
    cable basic nearline 54
    cable basic online or production 52
    cable redundant nearline 54
    cable redundant online or production 53
switches
    Ethernet and SiteConfig 77
system concepts 42
system descriptions
    K2 SAN 82
    importing into SiteConfig 127
system diagram
    K2 SAN basic nearline 50
    K2 SAN basic online or production 48
    K2 SAN redundant nearline 50
    K2 SAN redundant online or production 49

T

telnet
    Ethernet switches 64
terms
    devices 258
    K2 storage 32
trademarks 356

U

unreferenced files and movies
    cleaning 310
upgrade software
    SiteConfig on K2 SAN 116
upgrading
    firmware on Ethernet switches 75, 338

V

V:drives
    checking 180
    checking V:drive redundant nearline K2 SANs 204, 227
    checking V:drive redundant online and production K2 SANs 186

W

Windows
    activating 123
    setup 123
Windows Remote Desktop, See Remote Desktop
write filter
    configure with K2Config 305

X

XML
    system requirement 77