© 2011-2015 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://portal.hds.com.

**Notice:** Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.
Hitachi Data Systems products and services can be ordered only under the terms and conditions of Hitachi Data Systems’ applicable agreements. The use of Hitachi Data Systems products is governed by the terms of your agreements with Hitachi Data Systems.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Dynamic Provisioning, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, Domino, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, zSeries, z/VM, z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Some parts of ADC use open source code from Network Appliance, Inc. and Traakan, Inc.

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are copyright 2001-2009 Robert A. Van Engelen, Genivia Inc. All rights reserved. The software in this product was in part provided by Genivia Inc. and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

The product described in this guide may be protected by one or more U.S. patents, foreign patents, or pending applications.

**Notice of Export Controls**

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.
## Contents

**Preface** ........................................................................................................ 6  
Contacting Hitachi Data Systems.........................................................................6  
Related Documentation.........................................................................................6  

1 Configuring the SMU Network........................................................................10  
Overview of SMU Network Configuration..........................................................11  
Setting up SMU network configuration.................................................................13  
Updating the SMU network configuration settings...............................................15  

2 Networking interfaces ....................................................................................18  
Network interface details.................................................................................... 19  
VLAN support.....................................................................................................20  
  Creating VLAN interfaces..................................................................................20  
  Deleting VLAN interfaces................................................................................21  
  Converting subnet-VLANs to use VLAN interfaces...........................................22  
  Example of converting legacy VLANs into new static VLANs..........................23  
Understanding routing by EVS...........................................................................25  
Jumbo frames support.........................................................................................25  

3 Configuring the gigabit ethernet data interfaces.............................................28  
Link aggregations ...............................................................................................29  
  Displaying or changing the aggregation configuration......................................30  
  Adding aggregations.........................................................................................31  
  Deleting aggregations......................................................................................31  
IP addressing.......................................................................................................32  
  Displaying existing IP addresses......................................................................33  
  Adding an IP address.........................................................................................34  
  Removing an IP address...................................................................................34  
  Using advanced IP configuration......................................................................36
Preface

In PDF format, this guide provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.

Contacting Hitachi Data Systems

2845 Lafayette Street
Santa Clara, California 95050-2627
U.S.A.
https://portal.hds.com
North America: 1-800-446-0744

Related Documentation

**Release Notes** provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

**Administration Guides**

- **System Access Guide** (MK-92HNAS014)—In PDF format, this guide explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
- **Server and Cluster Administration Guide** (MK-92HNAS010)—In PDF format, this guide provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading firmware, monitoring servers and clusters, the backing up and restoring configurations.
- **Storage System User Administration Guide** (MK-92HNAS013)—In PDF format, this guide explains user management, including the different types of system administrator, their roles, and how to create and manage these users.
- **Network Administration Guide** (MK-92HNAS008)—In PDF format, this guide provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.
- **File Services Administration Guide** (MK-92HNAS006)—In PDF format, this guide explains about file system formats, and provides information about

---

Hitachi NAS Platform Network Administration Guide
creating and managing file systems, and enabling and configuring file services (file service protocols).

- **Data Migrator Administration Guide (MK-92HNAS005)** — In PDF format, this guide provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- **Storage Subsystem Administration Guide (MK-92HNAS012)** — In PDF format, this guide provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.
- **Snapshot Administration Guide (MK-92HNAS011)** — In PDF format, this guide provides information about configuring the server to take and manage snapshots.
- **Replication and Disaster Recovery Administration Guide (MK-92HNAS009)** — In PDF format, this guide provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.
- **Antivirus Administration Guide (MK-92HNAS004)** — In PDF format, this guide describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.
- **Backup Administration Guide (MK-92HNAS007)** — In PDF format, this guide provides information about configuring the server to work with NDMP, and making and managing NDMP backups. Also includes information about Hitachi NAS Synchronous Image Backup.
- **Command Line Reference** — Opens in a browser, and describes the commands used to administer the system.

---

**Note:** For a complete list of Hitachi NAS open source software copyrights and licenses, see the System Access Guide.

---

**Hardware References**

- **Hitachi NAS Platform 3080 and 3090 G1 Hardware Reference (MK-92HNAS016)** — Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- **Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference (MK-92HNAS017)** — Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- **Hitachi NAS Platform Series 4000 Hardware Reference (MK-92HNAS030)** (MK-92HNAS030) — Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
• Hitachi High-performance NAS Platform (MK-99BA012-13)—Provides an overview of the NAS Platform 3100/NAS Platform 3200 server hardware, and describes how to resolve any problems, and replace potentially faulty parts.

Best Practices
• Hitachi USP-V/VSP Best Practice Guide for HNAS Solutions (MK-92HNAS025)—The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
• Hitachi Unified Storage VM Best Practices Guide for HNAS Solutions (MK-92HNAS026)—The HNAS system is capable of heavily driving a storage array and disks. The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
• Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere (MK-92HNAS028)—This document covers VMware best practices specific to HDS HNAS storage.
• Hitachi NAS Platform Deduplication Best Practice (MK-92HNAS031) —This document provides best practices and guidelines for using HNAS Deduplication.
• Hitachi NAS Platform Best Practices for Tiered File Systems (MK-92HNAS038) —This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
• Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide (MK-92HNAS045)—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
• Brocade VDX 6730 Switch Configuration for use in an HNAS Cluster Configuration Guide (MK-92HNAS046)—This document describes how to configure a Brocade VDX 6730 switch for use as an ISL (inter-switch link) or an ICC (inter-cluster communication) switch.
• Best Practices for Hitachi NAS Universal Migrator (MK-92HNAS047)—The Hitachi NAS Universal Migrator (UM) feature provides customers with a convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.
• Hitachi NAS Platform Storage Pool and HDP Best Practices (MK-92HNAS048)—This document details the best practices for configuring and using HNAS storage pools, related features, and Hitachi Dynamic Provisioning (HDP).
Configuring the SMU Network

This section describes how to set up the SMU network configuration and includes:
- Details to consider before you begin the configuration.
- Adding the SMU configuration for IPv4 and IPv6.
- Modifying the SMU network configuration.

- Overview of SMU Network Configuration
- Setting up SMU network configuration
- Updating the SMU network configuration settings
Overview of SMU Network Configuration

The SMU network configuration supports both IPv4 and IPv6 addresses. You can configure the SMU network for:

- IPv4 on the private management interface eth1 and on the public management interface on eth0.
- IPv4 on eth0 and eth1 and also enable IPv6 on the public management interface (eth0) with stateless auto-configuration, or static address.

The IPv6 address configuration enables:

- Connection to the GUI in a browser using the IPv6 address, or a host name resolving to an IPv6 address.
- Connection to the SMU CLI using the IPv6 address, or a host name resolving to an IPv6 address.

The initial configuration of the SMU defaults with:

- IPv6 enabled.
- Auto-configuration of addresses enabled.
- No static IPv6 address.
- A single link-local IPv6 address.

The following graphic illustrates a SMU configured with IPv4 only:
The next graphic illustrates an SMU configured with IPv4 and IPv6:
Setting up SMU network configuration

Before configuring the SMU using the SMU setup wizard, you must first define the SMU network configuration details. After you add the configuration details in the **SMU Network Configuration** page, the system requires a reboot. For this reason, it is recommended that you determine the exact configuration details and then add the SMU network configuration before launching the SMU setup wizard. If necessary, consult your network administrator.
### Procedure

1. Navigate to **Home > SMU Administration > SMU Network Configuration** to display the **SMU Network Configuration** page.

![SMU Network Configuration](image)

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the host name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain for the SMU.</td>
</tr>
<tr>
<td><strong>IPv4 Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>eth0</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the SMU.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the netmask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the IP address of the gateway for the SMU.</td>
</tr>
<tr>
<td><strong>eth1</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The default address for the SMU's eth1 port is 192.0.2.1. The private management network address must end with .1, to simplify the management relationship of the SMU with secondary devices.</td>
</tr>
<tr>
<td>Netmask</td>
<td>This is a read-only field and defaults to 255.255.255.0.</td>
</tr>
<tr>
<td><strong>Private network device ports</strong></td>
<td>Displays a list of the devices attached to the management network, and the device details.</td>
</tr>
<tr>
<td><strong>IPv6 Configuration (eth0 only)</strong></td>
<td></td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable IPv6 Addresses</td>
<td>Enables IPv6 and to specify the IPv6 configuration. The fields in this section do not apply if the check box is not enabled.</td>
</tr>
<tr>
<td>Static IP Address (optional)</td>
<td>If appropriate, enter the static IP address in CIDR format. Contact your network administrator if you need more information.</td>
</tr>
<tr>
<td>Gateway (optional)</td>
<td>Enter the address of the gateway for the SMU. You can leave this field blank and allow the SMU to use an advertised router as a gateway. If a specific gateway is required, check the router and use its configured IPv6 address for the interface connected to the subnet on which the SMU resides.</td>
</tr>
<tr>
<td>Use stateless autoconfiguration (SLAAC)</td>
<td>Generates an address from the prefixes contained in the router advertisements.</td>
</tr>
<tr>
<td>Current Addresses</td>
<td>Displays any current static, SLAAC, and link-local addresses.</td>
</tr>
</tbody>
</table>

**Apply Network Settings**

| After Changes Are Applied      | Specify the action after changes are applied: reboot SMU or shutdown SMU.                                                                                                                                     |
| apply                          | Saves changes, which are effective as soon as they are applied. Depending on what you specified in the After changes are applied setting, the SMU will either reboot or shut down. |

2. After you enter the configuration, choose **reboot SMU** or **shutdown SMU**, and then click **apply**. The system will reboot or shutdown, depending on the selection.

**Updating the SMU network configuration settings**

Generally, after you establish the SMU network configuration, you will not need to make modifications. However, there might be a situation in which you need to make updates. For example, your organization might determine that you need to use IPv6. You can enable IPv6 here and define the appropriate IPv6 configuration details.

**Procedure**

1. Navigate to **Home > SMU Administration > SMU Network Configuration** to display the **SMU Network Configuration** page.

The following table describes the fields on this page. You can make modifications as necessary.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td></td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the host name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain for the SMU.</td>
</tr>
<tr>
<td><strong>IPv4 Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>eth0</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the SMU.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the netmask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the IP address of the gateway for the SMU.</td>
</tr>
<tr>
<td><strong>eth1</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The default address for the SMU's eth1 port is 192.0.2.1. The private management network address must end with .1, to simplify the management relationship of the SMU with secondary devices.</td>
</tr>
<tr>
<td>Netmask</td>
<td>This is a read-only field and defaults to 255.255.255.0.</td>
</tr>
<tr>
<td><strong>Private network device ports</strong></td>
<td>Displays a list of the devices attached to the management network, and the device details.</td>
</tr>
<tr>
<td><strong>IPv6 Configuration (eth0 only)</strong></td>
<td></td>
</tr>
<tr>
<td>Enable IPv6 Addresses</td>
<td>Enables IPv6 and to specify the IPv6 configuration. The fields in this section do not apply if the check box is not enabled.</td>
</tr>
<tr>
<td>Static IP Address (optional)</td>
<td>If appropriate, enter the static IP address in CIDR format. Contact your network administrator if you need more information.</td>
</tr>
<tr>
<td>Gateway (optional)</td>
<td>Enter the address of the gateway for the SMU. You can leave this field blank and allow the SMU to use an advertised router as a gateway. If a specific gateway is required, check the router and use its configured IPv6 address for the interface connected to the subnet on which the SMU resides.</td>
</tr>
<tr>
<td>Use stateless autoconfiguration (SLAAC)</td>
<td>Generates an address from the prefixes contained in the router advertisements.</td>
</tr>
<tr>
<td>Current Addresses</td>
<td>Displays any current static, SLAAC, and link-local addresses.</td>
</tr>
<tr>
<td><strong>Apply Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>After Changes Are Applied</td>
<td>Specify the action after changes are applied: <strong>reboot SMU</strong> or <strong>shut down SMU</strong>.</td>
</tr>
<tr>
<td>apply</td>
<td>Saves changes, which are effective as soon as they are applied. Depending on what you specified in the <strong>After changes are applied</strong> setting, the SMU will either reboot or shut down.</td>
</tr>
</tbody>
</table>
Networking interfaces

This section presents storage server system networking concepts and procedures for configuring the public data network and the private management network, in the following sections:

- IP routing, including static routes, default gateways, and dynamic routes, with a brief discussion of routing precedence.
- Overview of the network interfaces, including the usage of jumbo frames and IP addressing for the public data network, the private management network, clustering, and VLAN support.
- Network statistics, historical and near-real-time.

- Network interface details
- VLAN support
- Understanding routing by EVS
- Jumbo frames support
Network interface details

Each storage server is equipped with either a Gigabit Ethernet (1 GbE) port or 10 Gigabit Ethernet (10 GbE) ports and 10/100 Ethernet ports:

- Up to six GbE ports, that support copper and fiber SFPs (Small Form-factor Pluggables). These ports support jumbo frames, and may be configured either individually or trunked together using IEEE 802.3ad link aggregation to provide high-performance access to the public data network.

- Two 10 GbE ports, that support copper and fiber XFPs (10 Gigabit Small Form-factor Pluggables).

- HNAS 4060/4080/4100 systems have four 10GbE ports (SFP+ modules).

- HNAS 3000/4000 series have RJ45 GbE ports.

- 10/100/1000 Ethernet ports use standard RJ-45 connectors, and are used to connect to the storage server’s private management network.

- The physical Ethernet network interfaces allow the server to communicate with other devices on the IP networks to which the server is connected. These devices may be other nodes in the cluster, storage subsystems, the SMU, or clients. The NAS server can connect to IP networks that use IPv4 or IPv6 addressing, and some commands and Web Manager fields support CIDR addressing.

Network clients use either the Gigabit Ethernet (GbE) data interfaces or the 10 GbE Ethernet interfaces, configured for multihoming or link aggregation, to access the storage server:

- With multihoming, the administrator can configure each IP address on a different subnet.

- With link aggregation (or trunking), the administrator can configure multiple GbE ports or 10 GbE ports together into an aggregation. An IP address is assigned to both an EVS and an aggregation.

Note: All ports in an aggregation must be of the same type/speed (either all GbE ports or all 10 GbE ports).

An aggregation typically has a single MAC address, and at least one IP address; however, an aggregation can be configured with without any IP addresses, although the use of the aggregation would be limited. Physical ports can be aggregated in any combination, as long as all ports in each aggregation are of the same type/speed.

Link aggregation isolates the server from network infrastructure failure; for example, if some of the links in an aggregation fail, the other links in the aggregation share the traffic.

The server supports Link Aggregation Control Protocol (LACP). The aggregation must be statically configured. State is then synchronized.
between the switch and server, and the switch can use the state information to configure aggregations automatically (if this feature is supported).

The system supports mixed environments with simultaneous multihoming and link aggregation on the same server or cluster.

**VLAN support**

A physical network can be partitioned into multiple, isolated distinct broadcast domains called a virtual LAN or VLAN. For more background details see [https://tools.ietf.org/html/rfc3069](https://tools.ietf.org/html/rfc3069).

A VLAN interface is the way an HNAS provides access to a VLAN on a file-serving interface. You should create a VLAN interface for each tagged VLAN for each file-serving interface over which the HNAS needs to communicate. In order to create a VLAN interface, use `vlan-interface-create`. Other commands for manipulating VLAN interface commands are `vlan-interface-show` and `vlan-interface-delete`. For further details on these commands, see the CLI Reference.

Once a VLAN interface has been created, IP addresses can be added to it using the `evs` and `evsipaddr` commands in the normal way.

Once VLAN interfaces are defined, the HNAS server will expect ALL traffic on that VLAN trunk (interface) to be tagged.

---

**Note:** Do NOT create a VLAN interface for the native VLAN, as it may result in a loss of connectivity (if an address is assigned to a VLAN interface, the server will discard untagged packets for that address).

Note that VLAN interfaces are configured per aggregation: VLAN 1 on ag1 is different from VLAN 1 on ag2.

See the `ipadv` man page for more information about configuration settings for VLAN interfaces. `ipadv` configuration settings apply identically regardless of the VLAN interface creation mechanism.

---

**Note:** VLAN interfaces that have been dynamically created by the deprecated `vlan` command will only appear in the ifconfig display. For these deprecated VLAN interfaces, IP addresses are added using `evsipaddr` command specifying the aggregation interface name and not the VLAN interface name. See [Converting subnet-VLANS to use VLAN interfaces on page 22](#).

**Creating VLAN interfaces**

VLAN interfaces are explicitly created and deleted by the administrator. To create a VLAN interface, supply the base aggregation interface name and the VLAN tag. Then associate IP addresses with those VLAN interfaces using the `evs` or `evsipaddr` commands.
Procedure

1. To create a VLAN interface, use the `vlan-interface-create` command and supply the base aggregation interface name and the VLAN tag.

   $ vlan-interface-create --interface ag1 433
   Created ag1-vlan0433

   $ vlan-interface-create --interface ag1 499
   Created ag1-vlan0499

   For further details on `vlan-interface-create`, see the CLI Reference.

2. Use the `vlan-interface-show` command to show the VLAN interface names.

   $ vlan-interface-show
   ag1-vlan0433
   ag1-vlan0499

   For further details on `vlan-interface-show`, see the CLI Reference.

3. Associate IP addresses with those VLAN interfaces using the `evs create` command. Use the `evs list` command to show a list of the VLAN interfaces with IP addresses.

   $ evs create -l EVS1 -i 10.0.0.10/8 -p ag1-vlan0433
   $ evs create -l EVS2 -i 192.16.0.10/16 -p ag1-vlan0499

   $ evs list
   
   5     Service  EVS1   Yes     Online   10.0.0.10          ag1-vlan0433
   6     Service  EVS2   Yes     Online   192.16.0.10        ag1-vlan0499

   For further details on `evs create` and `evs list`, see the CLI Reference.

4. You can also use `evsipaddr` to associate IP addresses with VLAN interfaces

   $ evsipaddr -e 1 -a -i 192.168.1.1 -m 255.255.255.0 -p ag1-vlan0433

Deleting VLAN interfaces

To delete VLAN interfaces, use the `vlan-interface-delete` command and supply the base aggregation interface name and the VLAN tag.

Procedure

1. Use the `vlan-interface-delete` command and supply the base aggregation interface name and the VLAN tag.

   vlan-interface-delete -i ag1 433

   Removal of a VLAN interface is subject to the restriction that no addresses be assigned to it anywhere in the cluster. For further details on `vlan-interface-delete`, see the CLI Reference.
Converting subnet-VLANs to use VLAN interfaces

In releases prior to 12.0, VLANs were created based on a subnet mask. This topic describes how to convert such subnet-VLANs to use VLAN interfaces instead.

The subnet-VLANs are maintained by the `vlan` command, see the CLI reference for more details. From 12.0 onwards, new subnet-VLANs cannot be created but the `vlan` command allows existing subnet-VLANs to be displayed and deleted. 12.2 code has a script to convert legacy VLANs into the new-style static VLANs. Use this procedure to run the script and convert the VLANs.

**Procedure**

1. The script does not run under the HNAS CLI but is available on the HNAS platform, from HNAS Version 12.2, via the Linux console and is located at: `/opt/mercury-utils/bin/vlan-convert-config.rb`. Access the Linux console on the HNAS platform:
   - a. ssh to the SMU IP address
   - b. Enter `q` to drop to the Linux prompt of the SMU
   - c. `ssh manager@<cluster node ip>`
   - d. Enter password, the default is `nasadmin`
   - e. Enter `exit` to exit Bali
   - f. Enter `su`
   - g. Enter password, default is `nasadmin`

2. The vlan conversion script is stored on the HNAS server. To obtain the script (from an HNAS called `xyz`), enter:

   ```bash
   # scp manager@xyz:/opt/mercury-utils/bin/vlan-convert-config.rb .
   manager@xyz's password:
   vlan-convert-config.rb              00%   23KB  22.9KB/s   00:00
   #
   ```

3. Use the `vlan-convert-config.rb` script to convert subnet-VLANs to VLAN interfaces:

   ```bash
   vlan-convert-config.rb [--user <user>] [--password <password>] <hnas-server>
   ```

   Where:

   - `user <username>` username used to access the server
   - `password <password>` password used to access the server
   - `<hnas-server>` is the hostname or address of the HNAS server

   **Note:** If the user option is supplied without a corresponding password the script will prompt for the password but without displaying the entered text.
Note: When executing the script on the Linux console the name localhost can be used to identify the HNAS server. In this case it will normally not be necessary to supply the username and password.

Example:
/opt/mercury-utils/bin/vlan-convert-config.rb localhost > /tmp/vlan-conv-commands

4. The script will output the commands to be run to do the conversion. Review these changes before applying them to the system.
cat /tmp/vlan-conv-commands

5. Apply the generated commands to the HNAS:
source /tmp/vlan-conv-commands

6. Keep a copy of the script output for reference in case a downgrade to a version of firmware below 12.0 is needed, as it will be necessary to convert back.

Example of converting legacy VLANs into new static VLANs
In releases prior to 12.0, VLANs were created based on a subnet mask. This example shows how to convert such subnet-VLANs to use VLAN interfaces instead.

A sample command and the vlan-conv commands generated by the script are shown.

Procedure

1. Sample command:

```
manager@hnas (bash) :/opt/mercury-utils/bin$ ./vlan-convert-config.rb localhost > /tmp/vlan-conv-commands
```

```
#!/bin/sh
# These are the commands suggested to upgrade the VLAN configuration.
# Running this script will disrupt communications with the HNAS.
# Created for HNAS localhost at 2014-10-14T07:51:46-07:00 [Version 12.2.3750.00].

# Please review this generated script before using it.
ssc localhost <<SSC-EOS

# Disable any EVS that only contain addresses on a tagged VLAN before updating the configuration.
echo Disabling any EVS with tagged VLAN prior to re-configuration ...
evs disable -e 1 --confirm

echo Removing VLAN IP addresses from EVS prior to re-configuration ...
# Remove the address 172.31.61.61/24 on ag1 from EVS 2:evs2 Networking interfaces 23
```
evsipaddr -e 2 --remove --confirm --ip 172.31.61.61

# Remove existing (legacy) VLAN configuration.
vlan remove-all

# Create new VLAN interfaces.
# Processing address 172.31.62.62/24 for ag1-vlan0200.
vlan-interface-create --interface ag1 200
# Processing address 172.31.61.61/24 for ag1-vlan0100.
vlan-interface-create --interface ag1 100

echo Preparing to reconfigure IP addresses on VLANs ...
sleep 5

# Reconfigure IP addresses on VLANs.
# Move address to VLAN interface.
evsipaddr -e 1 --update --confirm --ip 172.31.62.62/24 --port ag1-vlan0200
# Restore previously removed address to VLAN interface.
evsipaddr -e 2 --add --ip 172.31.61.61/24 --port ag1-vlan0100

# Enable any EVS that were previously disabled.
echo Enabling the EVS that were previously disabled ... 
evs enable -e 1

2. After reviewing the vlan-conv commands, execute the generated file on the HNAS server.

```
manager@hnas(bash):/tmp$ source ./vlan-convert-commands
```

HDS NAS OS Console
MAC ID : 34-4E-9E-37-3B-F2

```
hnas:$
hnas:$ # Disable any EVS that only contain addresses on a tagged VLAN before updating the configuration.
hnas:$ echo Disabling any EVS with tagged VLAN prior to re-configuration ...
Disabling any EVS with tagged VLAN prior to re-configuration ...
hnas:$ # Disable EVS 1:HNAS-G3
hnas:$ evs disable -e 1 --confirm
hnas:$
hnas:$ # Remove all addresses in VLANs from still enabled EVS before updating the configuration.
hnas:$ # This applies to EVS with non-VLAN address assignments in order to minimise disruption to non-VLAN services.
hnas:$ echo Removing VLAN IP addresses from EVS prior to re-configuration ...
Removing VLAN IP addresses from EVS prior to re-configuration ...
hnas:$ # Remove the address 172.31.61.61/24 on ag1 from EVS 2:evs2
hnas:$ evsipaddr -e 2 --remove --confirm --ip 172.31.61.61
Warning: Removing IP address 172.31.61.61 while EVS is ONLINE
hnas:$
hnas:$ # Remove existing (legacy) VLAN configuration.
hnas:$ vlan remove-all
hnas:$
hnas:$ # Create new VLAN interfaces.
hnas:$ # Processing address 172.31.62.62/24 for ag1-vlan0200.
hnas:$ vlan-interface-create --interface ag1 200
Created ag1-vlan0200
hnas:$ # Processing address 172.31.61.61/24 for ag1-vlan0100.
hnas:$ vlan-interface-create --interface ag1 100
Created ag1-vlan0100
hnas:$ echo Preparing to reconfigure IP addresses on VLANs ...
Preparing to reconfigure IP addresses on VLANs ...
```
Understanding routing by EVS

Routing by EVS restricts the choice of source addresses available to the routing engine to those associated with the source EVS. Routing by EVS is always enabled in multi-tenancy mode. Routing by EVS can also be enabled when not in multi-tenancy mode.

Some subsystems already use the current EVS to influence routing decisions. With routing by EVS enabled, many subsystems, such as DNS, which normally would not use the EVS to influence routing decisions, now would use routing by EVS. If routing by EVS is to be enabled in non-multi-tenant mode, it is necessary to use the `routing-by-evs-enable` command. See the CLI reference for `routing-by-evs` commands:

- `routing-by-evs-enable`
- `routing-by-evs-disable`
- `routing-by-evs-show`

Jumbo frames support

All GE interfaces of a server support jumbo frames, which enable transmission of Ethernet frames larger than the Ethernet standard of 1,518 bytes. By reducing the number of frames required for large transfers, jumbo frames effectively increase transfer rate. Jumbo frames co-exist with standard frames on an Ethernet network.

All GE interfaces receive jumbo frames unconditionally, without any configuration changes. A GE interface can be configured to transmit jumbo frames by specifying an MTU size of between 1,519 and 9,600 bytes. To configure jumbo frame transmission, see Using advanced IP configuration on page 36 to configure the following settings:

- IP MTU for off-subnet transmits - bytes
- TCP MTU
- Other Protocol MTU
**Caution:** Networking equipment lacking the jumbo frames extension may drop jumbo frames and record an oversize packet error. Before configuring jumbo frame transmission, verify that all network equipment along the route (and at each end point) supports jumbo frames. If you enable jumbo frames and either network equipment or clients on the subnet do not support jumbo frames, you may experience a loss of communication with the server/cluster.

Successful IP data transmission using jumbo frames depends on the destination IP address or sub-network. The maximum MTU size for a destination IP address or sub-network is configured as an attribute in the IP routing table. The MTU value is the lowest of:

- Routes in the routing table matching the destination address that have a non-default MTU
- The global MTU setting
- The interface MTU setting
- Any MTU routes configured in the MTU table, matching the source address
Configuring the gigabit ethernet data interfaces

GE (gigabit Ethernet) and 10 GbE (10 gigabit Ethernet) port configuration requires setting up the following components:

- Link aggregations.
- IP addressing, including advanced IP settings and routing table settings, for file and block services provided by the server.

- Link aggregations
- IP addressing
Link aggregations

In a link aggregation, two or more like (GE or 10 GbE) ports are grouped, forming a single logical unit, to increase bandwidth capability and create resilient and redundant links. An aggregation also provides load balancing where the processing and communications activity is distributed across several links in a trunk so that no single link is overwhelmed. Aggregations provide higher link availability and increased link capacity.

To view the status of an aggregation, navigate to the **Link Aggregation** page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the aggregation (agX, where X is the aggregation number).</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>HNAS 3xx0 series and HNAS 4040 supports up to 8 aggregations and HNAS 4060, 4800 and 4100 series supports up to 4 aggregations.</td>
</tr>
</tbody>
</table>
| Use LACP   | Type of aggregation that is configured: Link Aggregation Configuration Protocol (LACP) or static (default). The behavior of the aggregation types vary in the following ways:  
  - Static: Configures the switch to which the aggregated links are connected to match the link aggregation settings defined on the server.  
  - LACP: Allows the LACP protocol to automatically configure the link aggregation settings on the switch. To use this setting, make sure to use a network switch that supports the LACP protocol. If the LACP timeout period is not long enough, you can adjust it using the CLI. |
| Ports      | List of ports used in the aggregation. Ports named "gex" are Gigabit Ethernet (GE) ports, and ports named "tgx" are 10 Gigabit Ethernet (10 GbE) ports. |
| details    | Displays the configuration of the selected port. You can edit the values on the page that is displayed. |
**Displaying or changing the aggregation configuration**

**Procedure**

1. Navigate to **Home > Network Configuration > Link Aggregation** to display the **Link Aggregation** page, which lists all currently configured aggregations.
2. Click **details** to display the aggregation’s **Link Aggregation Details** page.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Click add to open the <strong>Add Link Aggregation</strong> page. The add button is disabled when either all aggregate group names are used up or no more GbE ports are available to aggregate.</td>
</tr>
<tr>
<td>delete</td>
<td>Select an aggregation and click delete.</td>
</tr>
<tr>
<td>Status</td>
<td>The detailed status for each port associated with the aggregation on each server or cluster node.</td>
</tr>
<tr>
<td></td>
<td>Status LED values:</td>
</tr>
<tr>
<td></td>
<td>• Green: OK</td>
</tr>
<tr>
<td></td>
<td>• Amber: Degraded</td>
</tr>
<tr>
<td></td>
<td>• Red: Down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned Ports</td>
<td>Lists the ports currently assigned to this aggregation. Ports named &quot;gex&quot; are gigabit Ethernet ports, and ports named &quot;tgx&quot; are 10 GbE (10 gigabit Ethernet) ports. To remove a port from the aggregation, empty the check box next to the name of the port you want to remove.</td>
</tr>
<tr>
<td>Available Ports</td>
<td>The available GE (gigabit Ethernet) and tg (10 GbE) ports that can be added to the aggregation. Ports named &quot;gex&quot; are gigabit Ethernet ports, and ports named &quot;tgx&quot; are 10 GbE (10 gigabit Ethernet) ports. To add a port to the aggregation, fill the check box next to the name of the port you want to add.</td>
</tr>
<tr>
<td>Use LACP</td>
<td>Specify whether the aggregation should use LACP. An aggregation that does not use LACP is called a static aggregation, and an aggregation that does use LACP is called a dynamic aggregation.</td>
</tr>
<tr>
<td>Port level Load Balancing</td>
<td>Displays the port load balancing scheme used for all ports in the aggregation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Normal</strong> means that the server routes all traffic for a given &quot;conversation&quot; through one of the physical ports in the appropriate aggregation. The server’s hash and routing functions determine which packets use which physical ports of the aggregation. For example, all traffic for a particular TCP connection will always be routed through the same physical port (unless the link drops).</td>
</tr>
</tbody>
</table>
• **Round robin** means that the packets making up the traffic are routed through the ports in sequential order. For example, the first packet goes down the first port, the second packet goes down the next port and so on until all ports have been used. Then the traffic starts again at the first port. This routing scheme ensures that all the ports are more or less equally used, to provide maximum link throughput.

The disadvantage of round robin is that the clients must be able to cope with out of order TCP traffic at high speed.

The LACP specification (802.3ad) requires that an implementation must follow the appropriate rules to minimize out of order traffic and duplicated packets. Round robin load balancing directly contravenes this requirement. However, there are situations where the server’s hash functions cannot balance the conversations across physical ports very well, resulting in poor link utilization and reduced throughput. In these cases, round robin load balancing can improve link utilization and improve throughput.

Select the radio button next to the port loading scheme you want the aggregation to use.

<table>
<thead>
<tr>
<th>OK</th>
<th>Saves configuration changes, and closes the page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. If you want to change the aggregation’s configuration, you can use the **Edit Link Aggregation Details** page to:

- Remove ports from the aggregation.
- Change the type of load balancing used in the aggregation.
- Add ports to the aggregation.

4. Click **OK** to save the changes, or click **cancel** to return to the **Link Aggregation** page.

## Adding aggregations

**Procedure**

1. Navigate to **Home > Network Configuration > Link Aggregation**, and then click **add** to display the **Add Link Aggregation** page:

2. Using the check boxes and radio buttons on the **Add Link Aggregation** page, specify the configuration of the aggregation.

3. Verify your settings, then click **OK** to apply the settings, or **Cancel** to decline.

## Deleting aggregations

**Procedure**

1. Navigate to **Home > Network Configuration > Link Aggregation** to display the **Link Aggregation** page.
**Caution:** Aggregation deletion alert! Before deleting an aggregation, all IP addresses, GE, and 10 GbE ports associated with the aggregation must be removed.

2. Fill the check box by the name of the aggregation you want to delete.
3. Click **delete** to immediately remove the aggregation.

**Note:** When deleting an aggregation, there is no confirmation required. When you click **delete**, the aggregation will be deleted immediately.

---

**IP addressing**

The server distinguishes between IP address requirements for the public data network, the private management network, and clustering:

- **File services (public data network).** Network clients access the server’s file services through file service IP addresses, which are accessible only through the server’s GbE ports. Multiple IP addresses can be assigned for file services (these IP addresses may be on the same or different networks).

- **Administration services (private management network).** These IP addresses are used when managing a server or cluster, through the Web Administration Manager or using the server’s embedded management interfaces. On the HNAS 3000/4000 series, the server requires at least one IP address, which is assigned to the 1 GbE Ethernet port. Additional administrative IP addresses can be assigned to front-end file services ports, so that management functions may be performed directly through these network ports using SSC (*Hitachi NAS Platform*/*clusters*).

**Note:** When configuring an Administration Services IP address on the private management network, verify that the subnet mask for the IP address matches that of the SMU’s private management network (eth1 port); for example, 255.255.255.0. Also, choose an IP address that resides within the private management network’s range; for example, 192.0.2.2-254. This should be the Administrative Services IP address used when configuring a server as the managed server on the SMU.

- **Clustering.** When configured as a cluster, each node requires a unique IP address for the management port connected to the private management network. These unique addresses enable cluster node to communicate with each other and with the Quorum Device (QD).

**Note:** When using Data Migrator to Cloud, a different configuration is required. See the *Data Migrator Administration Guide* for details.
Displaying existing IP addresses

Procedure

1. Navigate to Home > Network Configuration > IP Addresses.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addresses</td>
<td>IP address used for Admin or File services or for server/cluster node management.</td>
</tr>
<tr>
<td>Label</td>
<td>The label of the EVS (virtual server) to which the file services IP is bound.</td>
</tr>
</tbody>
</table>
| Port | The interface used by the IP address:  
  - agX identifies one of the GE aggregations  
  - eth0 or eth1 identifies a 10/100/1000 port for a Hitachi NAS Platform  
  - mgmnt1 identifies the 10/100 management port for a Hitachi High-performance NAS Platform |
| Type | Type of services or configuration of the server:  
  - Admin Services: an IP address associated with the Administrative Services for the cluster. Administration Services IP address may be on the public data network or on the private management network.  
  - File services: an IP address associated with the File Services for the cluster. File Services IP addresses must be on the public data network.  
  - Cluster node: the IP address associated with the physical cluster node. Because File and Administrative services may migrate between nodes, the Cluster Node IP address is used to communicate with the node instead of a service. |
| details | Click the details button on the line for a listed IP address to view the Modify IP Address display, where you can change the port IPv4 and/or IPv6 settings. |
| add | Click the add button to add an IP address. |
| delete | Click the delete button to delete one or more selected IP addresses in the IP address list. |
Adding an IP address

Procedure

1. Navigate to **Home > Network Configuration > IP Addresses > add** to display the **Add IP Address** page.

2. Select a Virtual Server (EVS) to which to assign the IP address.

   From the list, select the EVS to which the IP will be assigned. Alternatively, specify that the IP address should be used for Admin Services.

3. Select an aggregation or management port:

   From the list, select an aggregation (agX), or a management port (mgmnt1 for a *Hitachi High-performance NAS Platform*, or eth0 or eth1 for a *Hitachi NAS Platform)*.

   **Note:** When assigning an IP address to a file-serving EVS, an ag port must be specified.

4. Enter the IP address and Subnet Mask for the selected port.

5. Verify your settings, then click **OK** to apply the settings or **cancel** to decline.

Removing an IP address

**Caution:** IP address deletion alert! Before following the instructions in this procedure, disable the EVS to which the IP address is assigned. Once the IP address has been removed, the EVS should be reenabled. This ensures that IP addresses are not in use at the time they are removed.
Procedure

1. Navigate to Home > Server Settings > EVS Management to display the EVS Management page.

2. Select the EVS to which the IP is assigned, then click disable.

3. Navigate to Home > Network Configuration > IP Addresses to display the IP Addresses page.

4. Select the IP Address to delete, then click delete.

5. Navigate to Home > Server Settings > EVS Management to display the EVS Management page.

6. Select the EVS to be reactivated and click enable to reenable the EVS.
Using advanced IP configuration

Procedure

1. Navigate to **Home > Network Configuration > Advanced IP Configuration** to display the **Advanced IP Configuration** page.

The following table describes the fields on this page:

The Global Settings area contains the fields and entries that make up the global configuration, which then become the default settings for all aggregations and ports.

<table>
<thead>
<tr>
<th>Global Settings</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Reassembly Timer (seconds)</td>
<td>15</td>
<td>Controls the time before which an incomplete IP datagram is discarded.</td>
</tr>
<tr>
<td>Ignore ICMP Echo Requests</td>
<td>No (empty)</td>
<td>When selected, instructs the system not to respond to Internet Control Message Protocol (ICMP) echo requests.</td>
</tr>
<tr>
<td>IP MTU for Off-Subnet Transmits (bytes)</td>
<td>1500</td>
<td>Specifies the maximum IP packet size used when transmitting to a different subnet.</td>
</tr>
<tr>
<td>TCP Keep Alive</td>
<td>Yes (filled)</td>
<td>When selected, instructs the system to send a keep alive packet when it has received no data or acknowledgment packets for a connection within the specified timeout period.</td>
</tr>
</tbody>
</table>
## Global Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Keep Alive timeout (seconds)</td>
<td>7200</td>
<td>Specifies the number of seconds to Keep alive a connection.</td>
</tr>
<tr>
<td>TCP MTU (bytes)</td>
<td>1500</td>
<td>Specifies the size of the maximum transmission unit (MTU) for the TCP.</td>
</tr>
<tr>
<td>Other Protocol MTU (bytes)</td>
<td>1500</td>
<td>Specifies the size of the MTU for protocols other than TCP.</td>
</tr>
<tr>
<td>ARP Cache Timeout (seconds)</td>
<td>60</td>
<td>Controls the time before which an unused ARP entry is removed from the caching table.</td>
</tr>
<tr>
<td>Ignore ICMP Redirect</td>
<td>No (empty)</td>
<td>Specifies whether to ignore ICMP redirects.</td>
</tr>
<tr>
<td>Port</td>
<td>Default: ag1 - agx, eth0, eth1, and mgmt1.</td>
<td>Lists the name of each currently configured aggregation or port in the server/cluster.</td>
</tr>
</tbody>
</table>

### Current Settings

Indicates whether the aggregation or port uses the default (global) settings, or customized settings. If the aggregation/port uses customized settings, the details button displays. Click details to edit the configuration of an aggregation that already uses a customized configuration.

### customize

Displays advanced IP per-port configuration, which provides you with a way to set configuration on a per-port basis.

**Note:** If you customize the values for a particular port, the new values override the global values for that port only.

### restore

Restores global settings to factory default values.

---

### Table 3-1 Recommended MTU settings

<table>
<thead>
<tr>
<th>Scenario</th>
<th>IP MTU for off-subnettransmits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server and clients on same IP subnetwork</td>
<td>Interface MTU used (1500 recommended)</td>
</tr>
<tr>
<td>Server and clients on different IP subnetworks but sharing the same Class A, B, or C network prefix</td>
<td>1500</td>
</tr>
<tr>
<td>Server and clients on different networks (UDP)</td>
<td>1500</td>
</tr>
</tbody>
</table>

---

2. For global settings, the following actions are available:
To customize the global settings, specify the values you want to use for the global configuration settings by changing the values of the fields in the Global Settings area. All aggregations (ports) will use the global settings by default. Once you have made the changes you want in the global settings values, click apply to save your changes.

To restore the global settings to the factory default values, click reset.

3. For specific aggregations, the following actions are available:

- To customize settings for the currently selected aggregation (the aggregation selected in the Ports field), click customize to display the Advanced IP Per-Port Configuration page.

<table>
<thead>
<tr>
<th>Per-port Settings</th>
<th>Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports, a list of available Ethernet or aggregation ports</td>
<td>First port in list</td>
</tr>
<tr>
<td>Ignore ICMP Echo Requests</td>
<td>No (empty)</td>
</tr>
<tr>
<td>IP MTU for Off-Subnet Transmits (bytes)</td>
<td>1500</td>
</tr>
<tr>
<td>TCP Keep Alive</td>
<td>Yes (filled)</td>
</tr>
<tr>
<td>TCP Keep Alive Timeout (seconds)</td>
<td>7200</td>
</tr>
<tr>
<td>TCP MTU</td>
<td>1500</td>
</tr>
<tr>
<td>Other Protocol MTU</td>
<td>1500</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

Enter the new values in the fields, and click OK. The new settings will override the global settings.

- To restore the settings of an aggregation (port) to the global configuration, select an aggregation in the Ports field, and then click restore. The settings for the aggregation selected in the Ports field, and all of its GE interfaces, will be erased, and will revert to the default (global settings).

- To change the settings of an aggregation that uses a customized configuration, click details to display the Advanced IP Per-Port Configuration page (described above). Enter the new values in the fields, and click OK.

The new settings will override the global settings.

After completing the IP configuration, you may have to reboot the server. If instructed to do so, follow the instructions to reboot the server.
This section presents storage server system networking concepts and procedures for configuring the public data network and the private management network, in the following sections:

- IP routing, including static routes, default gateways, and dynamic routes, with a brief discussion of routing precedence.
- Overview of the network interfaces, including the usage of jumbo frames and IP addressing for the public data network, the private management network, clustering, and VLAN support.
- Network statistics, historical and near-real-time.

□ IP routing details
**IP routing details**

Depending on configuration, the storage server can route IP traffic in three ways: through Default Gateways, Static Routes, and Dynamic Routes. The illustration below shows how a server may be configured to communicate with various IP networks through routes:

**Default gateways**

The server supports multiple default gateways for routing IP traffic. When connected to multiple IP networks, add a default gateway for each network to
which the server is connected. This configuration allows the server to direct traffic through the appropriate default gateway by matching source IP addresses specified in outgoing packets with the gateway on the same subnet.

With multiple default gateways, the server routes IP traffic logically, reducing the need to specify static routes for every network that connects with a particular server.

**Static routes**

Static routing provides a fixed path for data in a network. When a server on a network is connected to additional networks through a router, communication between that server and the remote networks can be enabled by specifying a static route to each network.

Static routes are set up in a routing table. Each entry in the table consists of a destination network address, a gateway address, and a subnet mask. Entries for static routes in the server’s routing table are persistent, meaning that, if a server is restarted, the route table preserves the static routing entries.

The server supports both network- and host-based static routes. Select the **Network** option to set up a route to address all of the computers on a specific network. Select the **Host** option to address a specific computer on a different network than its usual router address. The maximum possible number of static routes is 127 (default gateways also count against this total).

In most cases, for IPv6, it is not necessary to specify a gateway as it is automatically discovered through the received router advertisements.

**Dynamic routes**

The server supports **ICMP redirects** and **RIP versions 1 and 2**, which allow it to dynamically add routes to its route table:

- **ICMP redirects** is an industry standard for routers to convey routing information back to the server. When one router detects that another router offers a better route to a destination, it sends the server a redirect that temporarily overrides the server’s routing table. Being router-based, dynamic redirects do not require any configuration, but they can be viewed in the routing table.

- The server supports ICMP router discovery, which allows it to discover the addresses of routers. ICMP routers periodically multicast their addresses; when the server receives these multicasts, it incorporates the routers into its routing table. Once a router appears in the server’s routing table, it can be used as a gateway.

- **ICMP router discovery** is controlled using the CLI command `irdp`. For more information, see the **Command Line Reference**.


- **RIPv2** is also an industry standard, allowing servers to automatically discover routes and then update routes in the route table based on updates provided by other network devices. RIPv2 is controlled using the CLI command **rip**. For more information, refer to the *Command Line Reference*.

The server stores dynamic host routes in its route cache for 10 minutes. When the time has elapsed, packets to a selected destination use the route specified in the routing table until the server receives another ICMP redirect.

**Managing the server’s route table**

The server chooses the *most specific* route available for outgoing IP packets. The host route is the *most specific*, since it targets a specific computer on the network. The network route is the next most specific, since it targets a specific network. A gateway is the least specific route, hence the third routing option for the server. Therefore, if a server finds a host route for an outgoing IP packet, it will choose that route over a network route or gateway. Similarly, when a host route is not available, the server will choose a corresponding network route or, in the absence of host and network routes, the server will send the packet to a default gateway.

**Viewing IP routes**
Procedure

1. Navigate to **Home > Network Configuration > IP Routes.**

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Node Routing</td>
<td>Can be enabled or disabled for a particular IP route.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination device's IP address.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateway IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>A route can be of type Host, Network, or Gateway.</td>
</tr>
<tr>
<td>Creation Type</td>
<td>A route is either Static or Dynamic. Static indicates the route was created manually and dynamic indicates it was created by a switch.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit, the largest size Ethernet frame that can be sent.</td>
</tr>
<tr>
<td><strong>add</strong></td>
<td>Opens the <strong>Add IP Route</strong> page. When you add a new route, you also automatically flush the route table.</td>
</tr>
<tr>
<td><strong>delete</strong></td>
<td>Deletes the selected static routes and also automatically flushes the route table. Flashes the route table.</td>
</tr>
<tr>
<td><strong>flush routes</strong></td>
<td>Flushing the route table is the only way to delete dynamic routes.</td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td>Opens the <strong>IP Addresses</strong> page.</td>
</tr>
</tbody>
</table>

The server can be configured to route IP traffic through the network in three different ways:

- Static routes. These provide a means to forward data in a network through a fixed path; they are set up by specifying their details in a routing table. The maximum possible static routes is 127.
- Default gateways. These can also be used for routing IP communication. When connected to multiple IP networks, add a default gateway for each network to which the server is connected.
When configured in this way, the server will direct traffic through the appropriate default gateway by matching the source IP address specified in outgoing packets with the gateway on the same subnet.

- Dynamic host routes. The server also supports **ICMP redirects**, which provide a means for routers to convey routing information back to the system. When one router detects that another offers a better route to a destination, it sends a redirect that temporarily overrides the system's routing table. This is called a dynamic host route. The system stores these dynamic host routes in its route cache for ten minutes only. Once this time period has elapsed, packets to the selected destination use the route specified in the routing table until the system receives another ICMP redirect. The host route cache can store up to 65,000 dynamic routes at a time.

**Adding IP routes**

**Procedure**

1. Navigate to **Home > Network Configuration > IP Routes** to display the **IP Routes** page.
2. Click **add**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Route Type** | • **Host**: Addresses a specific computer that is on a different network than the router through which it would be normally addressed.  
                   • **Network**: Addresses all of the computers on a specific network.  
                   • **Gateway**: Targets a default gateway.                                                                                                                                                 |
| **IP Address** | Specifies the address of the host computer, target network, or gateway.  
                   • For host-based static routing, enter the IP address of the destination device and the gateway through which the host should be accessed. Note that the netmask will always be 255.255.255.255 for host-based routes.  
                   • For network-based static routing, specify the target network based on the IP and netmask, and the gateway through which the host should be accessed.                                                                 |
| **Netmask**   | Use for netmasks.                                                                                                                                                                                              |
| **Gateway**   | Use for gateways.                                                                                                                                                                                              |
| **MTU**       | Enter the MTU.                                                                                                                                                                                                 |
| **OK**        | Saves configuration changes and closes the page.                                                                                                                                                              |
| **cancel**    | Closes the page without saving configuration changes.                                                                                                                                                         |

**Deleting an IP route**
Procedure

1. Navigate to Home > Network Configuration > IP Routes to display the IP Routes page.
2. Fill the check box next to the route to delete and then click delete.
3. Click OK to confirm the deletion of the IP route.

⚠️ Note: Dynamic routes cannot be deleted individually. To delete all dynamic routes, flush the cache by clicking flush routes.

For non-dynamic routes, use the following CLI commands:
- `irp flush`
- `mdp-flush`
- `rip flush`

See the CLI man pages for more information.
You can configure the server to work with a local name server and to support the available name resolution methods.

Available name resolution methods:
- Domain Name System (DNS)
- Dynamic Domain Name System (DDNS)
- Windows Internet Naming Service (WINS)
- NIS and LDAP are also supported for name resolution. These are described in a subsequent chapter.

These methods associate computer identifiers (for example, IP addresses) with computer names. This allows you to specify computer names rather than IP addresses in dialog boxes.
DNS and DDNS

On TCP/IP networks, the Domain Name System (DNS) is used to resolve host names into IP addresses.

With DNS, records must be created manually for every host name and IP address. Starting with Windows 2000, Microsoft enabled support for Dynamic DNS, a DNS database which allows authenticated hosts to automatically add a record of their host name and IP address, eliminating the need for manual creation of records.

Registering a CIFS name

When an EVS goes online, the server registers one entry with the configured DNS servers (in both the forward and reverse lookup zones) for each configured ADS CIFS name and IP address associated with the EVS. Thus, the EVS records one entry in DDNS for every configured IP address. If a server has more than one configured ADS CIFS name, an entry for each IP address for each configured CIFS name is registered.

Each hostname registered with the DNS server has a Time To Live (TTL) property of 20 minutes, which is the amount of time other DNS servers and applications are allowed to cache it. The record's TTL dwindles with passing time and when the TTL finally reaches zero, the record is removed from the cache. After the 20-minute expiration point, the client must execute a fresh name lookup for more information.

The hostname is refreshed every 24 hours. This refresh commences after the first successful registration. For example, if the server registers its name at bootup, then every 24 hours after the bootup it refreshes its DNS entry. If the server cannot register or refresh its name, it goes into recovery mode with an attempt to register every 5 minutes. Once it successfully registers, it will resume the 24 hours-per-refresh cycle.

Secure DDNS updates

The storage server supports both secure and insecure DDNS updates. By default, Microsoft Windows 2000, 2003, and 2008 DDNS servers only accept “secure”, Kerberos-authenticated registrations. To support both Microsoft and non-Microsoft DDNS servers, the server will first attempt to register with DDNS insecurely. If the insecure registration fails, the server will attempt a secure registration.
WINS

WINS resolves NetBIOS names to IP addresses, and is used by the server to communicate with CIFS clients on the network. NetBIOS (and by extension, WINS) is not supported when multi-tenancy is enabled.

⚠️ **Note:** WINS is deprecated in Windows 2008.
Configuring name services

Name services configuration requires specifying and/or prioritizing name services. The following section provides information on how to complete these tasks.

- [ ] Specifying and prioritizing name services
Specifying and prioritizing name services

Procedure

1. Navigate to **Home > Network Configuration > Name Services** to display the **Name Services** page.

![Name Services page]

The following table describes the fields on this page.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context. Changes to the name services using this page apply only to the currently selected EVS security context.</td>
</tr>
<tr>
<td></td>
<td>• If an EVS uses the Global Configuration, any changes made to the global configuration settings affects the EVS.</td>
</tr>
<tr>
<td></td>
<td>• If an EVS uses an individual security context, changes made to the global configuration settings do not affect the EVS. To change the name services settings of an EVS using an individual security context, you must select the EVS' individual security context to make changes, even if those settings are the same as the settings used by the global security context. Click <strong>change</strong> to select a different EVS security context or to select the global configuration.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Specifies the IP addresses of up to three DNS servers. If more than one DNS server is entered, the search will be performed using the DNS servers in the order listed.</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Specifies the DNS domain name to use.</td>
</tr>
<tr>
<td>Domain Search Order</td>
<td>Enter a Domain suffix (for example: ourcompany.com) to use as a search keyword. When searching for a computer name, the DNS server searches using suffix order. For example, if the server contains the entries</td>
</tr>
</tbody>
</table>
### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uk.ourcompany.com and us.ourcompany.com, a request for the IP address of a host named author generates a query for author.uk.ourcompany.com and then for author.us.ourcompany.com. However, the system does not search the parent Domain ourcompany.com.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The suffix, combined with a computer’s host name, makes up a fully qualified domain name. To append a suffix to the displayed list, click Add.

To delete a suffix, select it from the displayed list, and then click X.

When using multiple domain suffixes, select the search order for the suffixes by using the up and down arrows to change their order within the list box.

<table>
<thead>
<tr>
<th>WINS Servers</th>
<th>To setup a primary WINS server, enter the IP address in the Primary WINS server field. If there is a secondary WINS server, enter the address in the Secondary WINS server field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>apply</td>
<td>Save your changes.</td>
</tr>
</tbody>
</table>

2. Enter the requested information.
3. Click **apply** to save your changes.
4. For instances of just one name service, verify that the name service appears in the **Name Services Ordering** configuration page:

   a. From the **Network Configuration** page, click **Name Services Order** to display the **Name Services Ordering** page, which lists **Available Name Services** and **Selected Name Services** in separate sections:

   ![Name Services Order page](image)

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Click <strong>change</strong> to change the EVS.</td>
</tr>
<tr>
<td>Available Name Services</td>
<td>Name services to choose from.</td>
</tr>
<tr>
<td>Selected Name Services</td>
<td>Name services that have been selected.</td>
</tr>
<tr>
<td><strong>apply</strong></td>
<td>Alters the name services ordering.</td>
</tr>
</tbody>
</table>

   b. Use the change button to change the security context, if needed.

   c. Select and deselect name services to create a list of **Selected Name Services**. Use the left/right arrow keys to select name services from the **Available Name Services** box and move them to the **Selected Name Services** box, and vice-versa to deselect name services.

   d. Adjust the order of usage for selected name services.

   Use the up/down arrow keys to change the order of usage for selected name services in the **Selected Name Services** box.

   e. Apply settings.

   Verify settings, and click **OK** to apply the settings, or **cancel** to decline.
The administrator can configure the server to work with a local directory server and to support the location, administration, and management of network resource. The following directory service methods are available:

- Network Information Service (NIS)
- Lightweight Directory Access Protocol (LDAP)

These services associate identifiers with users, groups, devices, volumes, folders, and other network resources. These services associate an identifier of some kind with a resource, allowing you to specify policies for access on a broad basis, rather than explicitly on a per-resource basis, and to have this information accessible throughout your network.

- NIS (for NFS)
- LDAP advantages
**NIS (for NFS)**

NIS databases provide simple management and administration of Unix-based networks. These databases can provide details about users and groups, also individual client machines (including IP address and host name, to facilitate authentication for users logging in to clients on the network).

The server supports NIS and, when configured to use NIS, can provide the following:

- NFS user and group account information retrieval
- Name services for resolving host names to IP addresses
- (FTP) authentication

**LDAP advantages**

Many organizations are replacing their existing NIS infrastructure with the more reliable, scalable and secure system LDAP. In addition to providing the same services as NIS (user and group information retrieval, name service resolution, and FTP user authentication), LDAP also provides the following advantages:

- Improved accuracy, due to LDAP’s more frequent data synchronization of current and replicated data.
- Communications encryption using Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
- Authentication of connections to the LDAP database, instead of anonymous access to NIS databases.

The server supports LDAP version 2 and 3 (the default is version 3), including two of the most common LDAP service implementations:

- Sun Directory Server
- OpenLDAP
Configuring directory services

Directory services configuration requires enabling services, as well as specifying directory servers, configuring, and/or prioritizing directory servers. The following sections provide information on how to complete these tasks.

- Enabling and configuring NIS and LDAP services
- Enabling and disabling NIS
- Displaying the NIS configuration
- Adding NIS servers
- Modifying the NIS configuration
- Changing the priority of a configured NIS server
- Configuring LDAP to provide NIS services
- Adding an LDAP server
- Modifying the LDAP configuration
- Modifying the LDAP server
- Changing name services order
Enabling and configuring NIS and LDAP services

This section discusses how to enable and configure NIS and LDAP services using the Web Manager.

- Enabling and Disabling NIS
- Viewing the NIS Configuration
- Modifying the NIS Configuration
- Changing the Priority of Configured NIS Servers
- Configuring LDAP to Provide NIS Services

Note: The HNAS server supports LDAP version 2 and version 3.

Enabling and disabling NIS

After deciding which network information service to use, follow these instructions to enable NIS or LDAP:

Procedure

1. Navigate to Home > Network Configuration > NIS/LDAP Configuration to display the NIS/LDAP Configuration page:

2. Click Enable NIS or Enable LDAP.
Displaying the NIS configuration

Procedure

1. Navigate to Home > Network Configuration > NIS/LDAP Configuration to display the NIS/LDAP Configuration page.

Information displayed on the NIS/LDAP Configuration page depends on whether NIS is enabled or LDAP is enabled. When NIS is enabled, the NIS/LDAP Configuration page displays the following information:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context; either an individual security context or the global security context. Click change to select a different EVS security context or to select the global configuration. Selecting a different EVS security context changes the context to which the NIS/LDAP configuration settings apply.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the NIS domain for which the system is a client.</td>
</tr>
<tr>
<td>Rebind</td>
<td>Frequency of server attempts to connect to its configured NIS servers. Enter a value from 1 to 15 minutes.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Amount of time (in milliseconds) to wait for a response from an NIS server when checking the Domain for servers. Enter a value from 100 to 10,000 milliseconds. The default value is 300 milliseconds.</td>
</tr>
<tr>
<td>Broadcast For Servers</td>
<td>Enables server to discover the available NIS servers on the network. Servers must be in the same NIS domain and present on the server’s network.</td>
</tr>
</tbody>
</table>
### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Displays the IP addresses of the NIS servers which are currently configured.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority level for the selected NIS server (lowest value is highest priority). If the NIS Domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebind check.</td>
</tr>
<tr>
<td>Note: Servers discovered by broadcast do not have a priority. If you assign a priority after clicking the details button, the NIS server type becomes “User Defined,” and “User Defined” NIS servers are prioritized before servers discovered through broadcast.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of NIS server.</td>
</tr>
<tr>
<td>Note: Servers can be automatically discovered through the Broadcast for Servers option. They may be defined by the user, and user defined servers, regardless of priority, are tried before servers found by broadcast.</td>
<td></td>
</tr>
<tr>
<td>add</td>
<td>Takes you to the page in which you can add an NIS server.</td>
</tr>
<tr>
<td>Name Services Order</td>
<td>Shortcut to the page in which you can change the order in which to apply name services.</td>
</tr>
<tr>
<td>Switch to using LDAP</td>
<td>Takes you to the equivalent page for LDAP server configuration.</td>
</tr>
<tr>
<td>Disable NIS and LDAP</td>
<td>Enables you to disable the NIS and LDAP services.</td>
</tr>
</tbody>
</table>

When LDAP is enabled, the **NIS/LDAP Configuration** page displays the following information:

### Table 8-2 LDAP enabled

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context; either an individual security context or the global security context. Click <strong>change</strong> to select a different EVS security context or to select the global configuration. Selecting a different EVS security context changes the context to which the NIS/LDAP configuration settings apply.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the LDAP Domain for which the system is a client. For example: <code>Hitachi_Data_Systems.com</code></td>
</tr>
</tbody>
</table>
2. Add and delete servers, view server details and change server priorities, or modify the NIS configuration:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To add servers:</td>
<td>Click add, then refer to the instructions in Adding NIS Servers.</td>
</tr>
<tr>
<td>To delete servers:</td>
<td>Select a server, then click delete.</td>
</tr>
<tr>
<td>To modify the configuration:</td>
<td>Click modify, then refer to the instructions in Modifying the NIS Configuration.</td>
</tr>
<tr>
<td>To view detailed properties and/or change server priority:</td>
<td>Select a server, then click details.</td>
</tr>
<tr>
<td>To switch to LDAP:</td>
<td>Click Switch to using LDAP. The change applies to all servers.</td>
</tr>
<tr>
<td>To disable NIS:</td>
<td>Click Disable NIS and LDAP. The change applies to all servers.</td>
</tr>
<tr>
<td>To modify the name services order:</td>
<td>Click Name Services Order to navigate to the Name Services Ordering page, where name service ordering is specified.</td>
</tr>
</tbody>
</table>
Adding NIS servers

Procedure

1. Navigate to **Home > Network Configuration > NIS/LDAP Configuration**, then click **add** to display the **Add NIS Server** page:
2. In the **Server IP Address** field, enter the IP address of the NIS server you want to add.
3. In the **Priority** field, select a priority level for this NIS server from the drop-down list (lowest number is highest priority).

![Note: If the NIS Domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebinding check.]

4. Click **OK** to apply the addition of the new NIS server.

Modifying the NIS configuration

Procedure

1. Navigate to **Home > Network Configuration > NIS/LDAP Configuration** to display the **NIS/LDAP Configuration** page, then click **modify** to display the **Modify NIS Configuration** page, which displays the following fields.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Name of the NIS domain for which the system is a client.</td>
</tr>
<tr>
<td>Rebind</td>
<td>Frequency of server attempts to connect to its configured NIS servers. Enter a value from 1 to 15 minutes.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Amount of time (in milliseconds) to wait for a response from an NIS server when checking the Domain for servers. Enter a value from 100 to 10,000 milliseconds. The default value is 300 milliseconds.</td>
</tr>
<tr>
<td>Broadcast for servers</td>
<td>Enables server to discover the available NIS servers on the network. Servers must be in the same NIS domain and present on the server's network.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

2. Enter the requested information.
   a. Edit the values in the **Domain**, **Rebind** and **Timeout** fields.
   b. Enable/disable **Broadcast For Servers**.
Fill the “Broadcast for Servers Enabled” checkbox to enable the server to discover and automatically bind to NIS servers in the domain. Once enabled, the server will search for NIS servers in its configured NIS domain. These servers are found by broadcast and therefore must be on the same logical network as the server.

**Note:** After a server has been found by broadcast, click details to configure that server. If you later clear the Broadcast for Servers checkbox, the server configuration is not deleted; it is retained for possible later use.

NIS servers found by broadcast are regularly polled for responsiveness and, when a request for NIS lookup is made, the most responsive server is selected.

To remove NIS servers found by broadcast, disable “Broadcast for Servers” (clear the “Broadcast for Servers” checkbox). If “Broadcast for Servers” is enabled, an attempt to remove NIS servers found by broadcast results in an error message.

3. Verify that the configuration is correct, then click **OK** to apply its settings or **cancel** to decline.

### Changing the priority of a configured NIS server

**Procedure**

1. Navigate to **Home > Network Configuration > NIS/LDAP Configuration** to display the **NIS/LDAP Configuration** page, then click **details** to display the **Modify NIS Server** page.

2. In the **Priority** field, select the priority level for this NIS server from the drop-down list (lowest number is highest priority).

**Note:** If the NIS domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebind check.

3. Verify your settings, then click **OK** to apply or **cancel** to decline.
Configuring LDAP to provide NIS services

Procedure

1. Navigate to **Home > Network Configuration > NIS/LDAP Configuration** to display the **NIS/LDAP Configuration** page. Click enable NIS.

   ![NIS/LDAP Configuration Page](image)

Information displayed on the **NIS/LDAP Configuration** page depends on whether NIS is enabled or LDAP is enabled. When NIS is enabled, the **NIS/LDAP Configuration** page displays the following information:

**Table 8-3 NIS enabled**

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context; either an individual security context or the global security context. Click <strong>change</strong> to select a different EVS security context or to select the global configuration. Selecting a different EVS security context changes the context to which the NIS/LDAP configuration settings apply.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the NIS domain for which the system is a client.</td>
</tr>
<tr>
<td>Rebind</td>
<td>Frequency of server attempts to connect to its configured NIS servers. Enter a value from 1 to 15 minutes.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Amount of time (in milliseconds) to wait for a response from an NIS server when checking the Domain for servers. Enter a value from 100 to 10,000 milliseconds. The default value is 300 milliseconds.</td>
</tr>
<tr>
<td>Broadcast For Servers</td>
<td>Enables server to discover the available NIS servers on the network. Servers must be in the same NIS domain and present on the server’s network.</td>
</tr>
</tbody>
</table>
Field/Item | Description
---|---
IP Address | Displays the IP addresses of the NIS servers which are currently configured.
Priority | Priority level for the selected NIS server (lowest value is highest priority). If the NIS Domain contains multiple servers, the system will try to bind to the server with the highest priority level whenever it performs a rebind check.

**Note:** Servers discovered by broadcast do not have a priority. If you assign a priority after clicking the details button, the NIS server type becomes “User Defined,” and “User Defined” NIS servers are prioritized before servers discovered through broadcast.

Type | Type of NIS server.

**Note:** Servers can be automatically discovered through the Broadcast for Servers option. They may be defined by the user, and user defined servers, regardless of priority, are tried before servers found by broadcast.

add | Takes you to the page in which you can add an NIS server.
Name Services Order | Shortcut to the page in which you can change the order in which to apply name services.
Switch to using LDAP | Takes you to the equivalent page for LDAP server configuration.
Disable NIS and LDAP | Enables you to disable the NIS and LDAP services.

When LDAP is enabled, the **NIS/LDAP Configuration** page displays the following information:

**Table 8-4 LDAP enabled**

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context; either an individual security context or the global security context. Click <strong>change</strong> to select a different EVS security context or to select the global configuration. Selecting a different EVS security context changes the context to which the NIS/LDAP configuration settings apply.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the LDAP Domain for which the system is a client. For example: Hitachi_Data_Systems.com</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Name</td>
<td>User name of the administrator who has rights and privileges for this LDAP server. The name can be up to 256 characters in length; however, if it includes spaces, the name must be enclosed in double quotes. For example: cn=&quot;Directory Manager&quot;,dc=server1,dc=com</td>
</tr>
<tr>
<td>Schema</td>
<td>Name of the schema that is specified.</td>
</tr>
<tr>
<td>TLS</td>
<td>Enable/disable the TLS and SSL connection.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the NIS servers to which the server is currently bound.</td>
</tr>
<tr>
<td>Port</td>
<td>Standard port that is configurable by the administrator. The default port is 389.</td>
</tr>
<tr>
<td>TLS Port</td>
<td>The secure port that is configurable by the administrator. The default port is 636.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>Fully qualified hostname of the LDAP server.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the LDAP server.</td>
</tr>
<tr>
<td>add</td>
<td>Takes you to the page in which you can add an NIS server.</td>
</tr>
<tr>
<td>delete</td>
<td>Enables you to delete an NIS server from those listed.</td>
</tr>
<tr>
<td>Switch to using LDAP</td>
<td>Takes you to the equivalent page for LDAP server configuration.</td>
</tr>
<tr>
<td>Disable NIS and LDAP</td>
<td>Enables you to disable the NIS and LDAP services.</td>
</tr>
<tr>
<td>Name Services Order</td>
<td>Shortcut to the page in which you can change the order in which to apply name services.</td>
</tr>
</tbody>
</table>

2. If necessary, change the **EVS Security Context**. The **EVS Security Context** displays the currently selected EVS security context. Changes to the NIS/LDAP configuration using this page apply only to the currently selected EVS security context.

   - If an EVS uses the Global configuration, any changes made to the NIS/LDAP configuration settings will affect the EVS.
   - If an EVS uses an Individual security context, changes made to the global NIS/LDAP configuration settings will not affect the EVS. To change the NIS/LDAP configuration settings of an EVS using an individual security context, you must select the EVS' individual security context to make changes, even if those settings are the same as the settings used by the global security context.

   Click **Change** to select a different EVS security context or to select the global configuration.

3. Add and delete servers, view server details and change server priorities, or modify the NIS configuration:
Option | Description
---|---
To add servers: | Click add, then refer to the instructions in Adding NIS Servers.
To delete servers: | Select a server, then click delete.
To modify the configuration: | Click modify, then refer to the instructions in Modifying the NIS Configuration.
To view detailed properties and/or change server priority: | Select a server, then click details.
To switch to LDAP: | Click Switch to using LDAP. The change applies to all servers.
To disable NIS: | Click Disable NIS and LDAP. The change applies to all servers.
To modify the name services order: | Click Name Services Order to navigate to the Name Services Ordering page, where name service ordering is specified.

### Adding an LDAP server
HNAS supports LDAP version 2 and version 3.

**Procedure**

1. From the Network Configuration page, click NIS/LDAP Configuration to display the NIS/LDAP Configuration page, then click add to display the Add LDAP Server page. The fields on this page are described in the table below.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Address or Host Name</td>
<td>Allows you to specify the IP address or resolvable host name for the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Allows you to specify the standard port used for communication with the LDAP server (default: 389).</td>
</tr>
<tr>
<td>TLS Port</td>
<td>Allows you to specify the secure port used for communication with the LDAP server (default: 636).</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

2. In the Server IP Address or Host Name field, enter the IP address or the host name of the LDAP server.
Enter the IP address or a resolvable host name for the LDAP server.
3. In the Port field, enter the new standard port number for the LDAP server.
The standard port used to communicate with the LDAP server. The default port is 389.

4. In the TLS Port field, enter the new secure port number for the LDAP server.

The secure port used to communicate with the LDAP server. The default port is 636.

5. Save the new LDAP server information.

Click **OK**.

---

**Note:** A system administrator can query the LDAP server for information about hosts configured into netgroups. You may discover whether a host is in a specific netgroup hierarchy or not, as well as all of the netgroups to which a host belongs. The `nis-is-host-in-netgroup` and `nis-netgroups-for-host` commands are used to check whether a host is a member of a specified netgroup, or to determine the set of netgroups to which a host belongs.

---

### Modifying the LDAP configuration

**Procedure**

1. From the **Network Configuration** page, click **NIS/LDAP Configuration** to display the **NIS/LDAP Configuration** page, then click **modify** to display the **Modify LDAP Configuration** page. The fields on this page are described below.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Name of the LDAP domain for which the system is a client.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name of the administrator who has rights and privileges for this LDAP server. The name can be up to 256 characters in length; however, if it includes spaces, the name must be enclosed in double quotes. For example: <code>cn=&quot;Directory Manager&quot;,dc=server1,dc=com</code></td>
</tr>
<tr>
<td>Password</td>
<td>Password that corresponds to the user name.</td>
</tr>
<tr>
<td>TLS Enabled</td>
<td>Enable/disable Transport Layer Security to enable secure communication with the LDAP server.</td>
</tr>
<tr>
<td>Schema</td>
<td>Enables you to specify a schema to use. Available options:</td>
</tr>
<tr>
<td></td>
<td>• RFC-2307</td>
</tr>
<tr>
<td></td>
<td>• MS Services for Unix</td>
</tr>
<tr>
<td></td>
<td>• MS Identity Management for Unix</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

**Note:** This option supports both registered and anonymous login of users.

2. Enter the requested information:
   - Enter the **Domain**, **User Name** and **Password** fields.
   - Fill or clear the **TLS Enabled** checkbox to enable/disable TLS.

3. Verify that the configuration is correct, then click **OK** to apply the settings or **cancel** to decline.

## Modifying the LDAP server

### Procedure

1. From the **Network Configuration** page, select **NIS/LDAP Configuration**, then select the LDAP server configuration you want to change, and click **details** to display the **Modify LDAP Server** page. The fields on this page are describe in the table below.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Address or Host Name</td>
<td>Shows the IP address or host name assigned to the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Allows you to specify the standard port number to use for communication with the LDAP server (default: 389).</td>
</tr>
<tr>
<td>TLS Port</td>
<td>Allows you to specify the secure port used for communication with the LDAP server (default: 636).</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

2. Change/update current configuration information.
   a. In the **Server IP Address** or **Host Name** field, enter the new IP address or the new host name of the LDAP server.
   b. In the **Port** field, enter the new standard port number for the LDAP server. The default port is 389.
   c. In the **TLS Port** field, enter the new secure port number for the LDAP server. The default port is 636.

3. Verify that the configuration is correct, then click **OK** to apply the settings or **cancel** to decline.
Changing name services order

Procedure

1. From the Home page, click Network Configuration, then click Name Services Order.

   ![Network Configuration Interface](image)

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Click <em>change</em> to change the EVS.</td>
</tr>
<tr>
<td>Available Name Services</td>
<td>Name services to choose from.</td>
</tr>
<tr>
<td>Selected Name Services</td>
<td>Name services that have been selected.</td>
</tr>
<tr>
<td><strong>apply</strong></td>
<td>Alters the name services ordering.</td>
</tr>
</tbody>
</table>

2. The EVS Security Context displays the currently selected EVS security context. Changes to the name services order using this page apply only to the currently selected EVS security context.
   - If an EVS uses the Global configuration, any changes made to the global configuration settings will affect the EVS.
   - If an EVS uses an Individual security context, changes made to the global configuration settings will not affect the EVS. To change the name services ordering settings of an EVS using an individual security context, you must select the EVS' individual security context to make changes, even if those settings are the same as the settings used by the global security context.

   Click **Change** to select a different EVS security context or to select the global configuration.

3. From the Available Name Services list, select the name services you want to use, and click the right arrow.

4. The Selected Name Services list displays the name services in the order in which they will be used. Name services higher in the list are used before services lower in the list.
5. Verify your settings, then click **OK** to apply or **cancel** to decline.
Configuring the private management network

The storage server operates in conjunction with a number of auxiliary devices, including Fibre Channel switches, RAID storage subsystems from some manufacturers, and power management units, primarily managed through Ethernet. In order to minimize the impact on an enterprise network, the SMU uses Network Address Translation (NAT) and Port Address Translation (PAT) to isolate the storage server from the main network:
For example, an HTTP request for a device in the private management network would actually be made to the public on the SMU’s eth0 interface, on a NAT-ed port (i.e., 192.168.1.124:28013). The SMU translates this request to the private IP address and actual HTTP port of the device on the private management network (i.e. 192.0.2.13:80), the NAT port.

The IP address range of the private management network includes only those IP addresses sharing the first three octets of the SMU’s private (eth1) management network IP address. For example, for an SMU private management network IP address of 192.0.2.1, devices on the private management network must have addresses in the range of 192.0.2.2 – 192.0.2.254:

Significant advantages occur with a separate private management network:
- Network traffic required for normal SMU monitoring of the server and auxiliary devices will not be on the enterprise network.
- Devices on the private management network will not take up valuable IP addresses on the public data network.
- The SMU can discover all devices on the private management network, aiding setup.
- The private management network is more secure than the public data network.
As an alternative to the private management network, some or all of the auxiliary devices can be placed on the public data network. Such a configuration allows mixed systems, with some auxiliary devices isolated on the private management network, and others on the public data network.

**Note:** Devices on the public network require static IP addresses within the network.

- [ ] Recommended management network IP address ranges
- [ ] Configuring the management network
- [ ] Configuring devices on the system monitor
Recommended management network IP address ranges

The next table lists the recommended standard management network IP address allocation for the private management network.

<table>
<thead>
<tr>
<th>Device</th>
<th># of IPs</th>
<th>Range Start</th>
<th>Range End</th>
<th>Example/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet</td>
<td></td>
<td>192.0.2.0</td>
<td>192.0.2.254</td>
<td></td>
</tr>
<tr>
<td>SMU 1</td>
<td>1</td>
<td>192.0.2.1</td>
<td>192.0.2.1</td>
<td>Primary SMU</td>
</tr>
<tr>
<td>SMU 2</td>
<td>1</td>
<td>192.0.2.253</td>
<td>192.0.2.253</td>
<td>Backup SMU (if present)</td>
</tr>
<tr>
<td>Server/Cluster administration</td>
<td>8</td>
<td>192.0.2.2</td>
<td>192.0.2.9</td>
<td>NAS storage system administrative services</td>
</tr>
<tr>
<td>Cluster nodes</td>
<td>49</td>
<td>192.0.2.200</td>
<td>192.0.2.248</td>
<td>Physical cluster node</td>
</tr>
<tr>
<td>FC switches</td>
<td>16</td>
<td>192.0.2.10</td>
<td>192.0.2.25</td>
<td>Brocade</td>
</tr>
<tr>
<td>Storage arrays</td>
<td>150</td>
<td>192.0.2.30</td>
<td>192.0.2.179</td>
<td>LSI, Xyrayex, HDS</td>
</tr>
<tr>
<td>10Gbps Ethernet switches</td>
<td>16</td>
<td>192.0.2.180</td>
<td>192.0.2.195</td>
<td>N-way cluster interconnect switches (if present)</td>
</tr>
<tr>
<td>Internal Management Network Ethernet switch</td>
<td>1</td>
<td>192.0.2.254</td>
<td>192.0.2.254</td>
<td>HP ProCurve</td>
</tr>
<tr>
<td>Third-party devices</td>
<td>4</td>
<td>192.0.2.196</td>
<td>192.0.2.199</td>
<td>APC, tape library</td>
</tr>
<tr>
<td>KVM over IP</td>
<td>1</td>
<td>192.0.2.249</td>
<td>192.0.2.249</td>
<td>LANtronix</td>
</tr>
<tr>
<td>SSE laptop</td>
<td>3</td>
<td>192.0.2.250</td>
<td>192.0.2.252</td>
<td>Reserved for Service/Support</td>
</tr>
</tbody>
</table>

Configuring the management network

Procedure

1. Navigate to Home > SMU Administration > Management Network to display the Management Network page.
2. Enter the requested information.
   The Management Network page allows you to configure the private management network address of the SMU’s eth1 interface. The default address for the SMU’s eth1 port is 192.0.2.1. Because the public network does not include this address, it falls into a distinctly different range than the SMU’s public eth0 address.
Note: The private management network address must end with .1, to simplify the management relationship of the SMU with secondary devices.

Note: The NAT Port range is provided for information only. It is rare that these values will ever need to be known.

3. Once defined, record the IP address settings separately for future reference when configuring the server's Administration Services IP address and subnet mask, and click apply.

Configuring devices on the system monitor

The system monitor allows you to easily display and monitor the devices that make up your storage system.

Procedure

1. Naviage to Home > System Monitor to display the System Monitor page.

2. Optionally, rearrange the sequence of components in the System Monitor. To change the position of any component, fill its checkbox to select, then use the arrows in the Action section.
3. Optionally, display status or details for any component in the **System Monitor**.

The rows in the following table list the basic components that make up a HNAS system. This table indicates what happens when you click on a component’s name in the component list:

<table>
<thead>
<tr>
<th>Component/Description</th>
<th>Clicking the component</th>
<th>Clicking the details button</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage Server</strong></td>
<td>Loads the <strong>Server Status</strong> page.</td>
<td></td>
</tr>
<tr>
<td>This component provides Ethernet interfaces for connecting to the Public Data Network and the Private Management Network, as well as Fibre Channel interfaces used to connect to storage subsystems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Main Enclosure</strong></td>
<td>Loads the <strong>Enclosure Status</strong> page.</td>
<td>Loads the <strong>System Drives</strong> page.</td>
</tr>
<tr>
<td>Contains dual power supplies, and dual RAID drive controllers. Depending on the model, the main enclosure may contain disk drives.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Expansion Enclosure</strong></td>
<td>Loads the <strong>Enclosure Status</strong> page.</td>
<td>Loads the <strong>System Drives</strong> page.</td>
</tr>
<tr>
<td>Expansion enclosures contain disk drives and power supplies, but do not contain any RAID controllers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SMU</strong></td>
<td>Loads the <strong>SMU System Status</strong> page.</td>
<td></td>
</tr>
<tr>
<td>The System Management Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>System Power Unit</strong></td>
<td>Loads the <strong>UPS Status</strong> page.</td>
<td>Loads the <strong>UPS Configuration</strong> page.</td>
</tr>
<tr>
<td>This component is also known as an uninterruptible power supply (UPS).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NDMP Backup Devices</strong></td>
<td>Loads the <strong>NDMP Devices</strong> page.</td>
<td>Loads the <strong>NDMP Details</strong> page for the device if the device can be contacted, or loads the <strong>NDMP Device List</strong> page if the device cannot be contacted.</td>
</tr>
<tr>
<td>The server automatically detects and adds backup devices to the system monitor. Since the storage server could be connected into a FC network shared with other servers, it does not automatically make use of backup devices found on its FC links. Backup devices are automatically discovered and added to the Status Monitor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FC Switches</strong></td>
<td>Loads either the embedded management utility for the switch, or the <strong>FC Switch Details</strong> page for the switch, depending on the protocol specified when</td>
<td>Loads the <strong>FC Switch Details</strong> page.</td>
</tr>
<tr>
<td>FC switches (and cables) connect FC devices, generally storage arrays, to the server(s).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Component/Description

<table>
<thead>
<tr>
<th>Clicking the component</th>
<th>Clicking the details button</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Note:" /> Upon adding an FC switch through the FC Switches page, it is automatically added to the System Monitor.</td>
<td></td>
</tr>
</tbody>
</table>

### Other Components

Any component can be added to the system monitor. If the device supports a web-based management interface, the management interface can be launched directly from the server management interface.

<table>
<thead>
<tr>
<th></th>
<th>Loads the embedded management utility for the device.</th>
<th>Loads either the Add Public Net Device or the Add Private Net Device page. Settings for the component can be changed from this page.</th>
</tr>
</thead>
</table>

4. Optionally, add, remove, or display details about a device. The following **Actions** are available and apply to selected components:

- Click **remove** to delete a component.
- Click **details** to display details regarding a particular component.
- Click **add Public Net Device** to add a device residing on the public (data) network.
- Click **add Private Net Device** to add a device residing on the public (data) network.

**Note:** Devices on the private management network are “hidden” from the data network through Network Address Translation (NAT).

Once a device has been added to the System Monitor, clicking its name in the System Monitor:

- Opens its embedded management utility in the Web browser, using either HTTP, HTTPS, or Telnet.
- The SMU periodically checks for device activity and connectivity with the server; if a device fails to respond to network “pings”, the System Monitor changes its color to red and the SMU issues an alert (devices can also be configured to send SNMP traps to the SMU).
- Events from the device will be added to the event log if the SMU has a MIB for the device.