Hitachi NAS Platform

NAS File OS 15.3 or later

Network Administration Guide

MK-92HNAS008
October 2024

Contents

Preface

This guide provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services. Note that some features apply only to individual platforms and may not be applicable to your configuration.

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.

Command Line References

The Command Line Reference provides information on the commands used to manage your system, and includes relevant information on the operation of your hardware and software. Depending on the model of your server or cluster node, refer to the Command Line Reference that is appropriate for your system.

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 5200 and 5300*
- *Command Line Reference for model VSP One File 32*
- *Command Line Reference for VSP One File models 34/38*

Administration Guides

- *System Access Guide* (MK-92HNAS014)—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)—Provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading software, monitoring servers and clusters, and backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—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)—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)—Explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).
- *Data Migrator Administration Guide* (MK-92HNAS005) —Provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—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)—Provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009)—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)—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)—Provides information about configuring the server to work with NDMP, and making and managing NDMP backups.
- *Hitachi Virtual SMU Administration Guide* (MK-92HNAS074)—Provides information about how to install and configure and upgrade a virtual System Management Unit (SMU).
- *Hitachi NAS REST API Reference* (MK-92HNAS098) (MK-92HNAS100)—Documents NAS REST API to administer Hitachi storage systems using standard HTTP protocol operations.

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

Hardware References

The Hardware Reference provides detailed information about server hardware and components.

- *Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference* (MK-92HNAS030)
- *Hitachi NAS 5000 Series Hardware Reference* MK-92HNAS089
- *Hitachi Virtual Storage Platform One File 32 Hardware Reference* (MK-24VSP1F000)
- *Hitachi Virtual Storage Platform One File 34 and File 38 Hardware Reference* (MK-24VSP1F001)

Best Practices

- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers best practices specific to using VMware vSphere with the Hitachi NAS platform.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031)—This document provides best practices and guidelines for using 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.
- *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 Data Systems SU 12.x Network File System (NFS) Version 4 Feature Description* (MK-92HNAS056)—This document describes the features of Network File System (NFS) Version 4.
- *Hitachi NAS HDP Best Practices* (MK-92HNAS057)—This document lists frequently asked questions regarding the use of Hitachi Dynamic Provisioning.
- *Hitachi Multi-tenancy Implementation and Best Practice Guide* (MK-92HNAS059)—This document details the best practices for configuring and using Multi-Tenancy and related features, and EVS security.
- *Hitachi NAS Platform HDP Best Practices* (MK-92HNAS063)—This document details the best practices for configuring and using storage pools, related features, and Hitachi Dynamic Provisioning (HDP).
- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.

- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

Accessing product documentation

Product user documentation is available on: https://docs.hitachivantara.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Support Website is the destination for technical support of products and solutions sold by Hitachi. To contact technical support, log on to the Hitachi Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Community is a global online community for Hitachi customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi.

Thank you!

Chapter 1: Network interfaces

This section contains information on network interfaces, link aggregation, and jumbo frames support.

File serving interfaces

NAS servers provide the following file serving physical interfaces:

Models 5200 / 5300

- **tg1 - tg6** - 10 GbE interfaces (SFP+)

NAS module

- **tg1 - tg6** - 10 GbE interfaces (SFP+)

Models 4060 / 4080 / 4100

- **tg1 - tg4** - 10 GbE interfaces (SFP+)

File serving physical interfaces enable network clients to access an EVS on the storage server. These interfaces are commonly added together in a link aggregation to increase redundancy and throughput of data.

Link aggregation

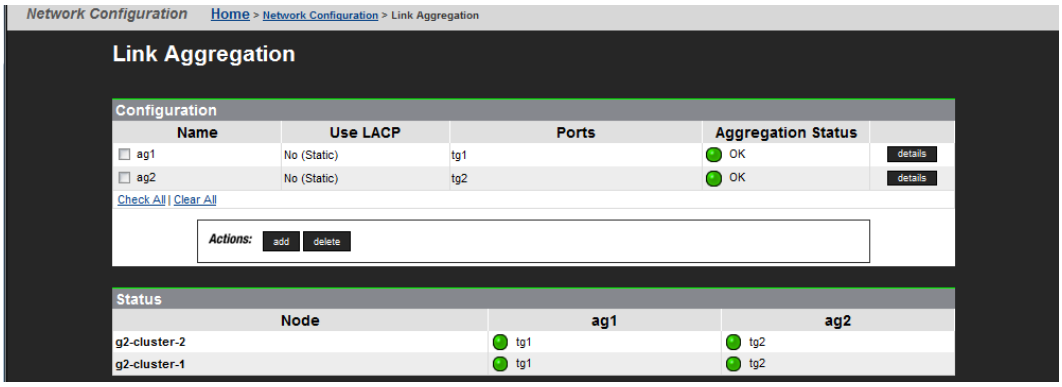
In a link aggregation, one or more file serving interfaces are grouped to form a single logical interface. This functionality can increase bandwidth capability and create resilient and redundant links. Aggregating multiple network links does not increase performance of a single client TCP connection, but it does enable more individual connections to be served faster by using more available links and by reducing contention within a link. An aggregation also provides load balancing where the processing and communications activity is distributed across several links in a trunk. Therefore, aggregations provide higher link availability and increased Link Aggregation Group (LAG) capacity.

Note: All interfaces in an aggregation must be of the same type/speed (either all 1 Gbps interfaces or all 10 Gbps interfaces).

An aggregation is assigned a unique MAC address which is different on each cluster node. Each aggregation can have multiple IP addresses. It is possible to configure an aggregation without any IP addresses, but this prevents communication through that interface. For example, in a cluster, an aggregation associated with an EVS appears on all nodes but is only active on the node that the EVS is running on because the EVS holds the IP address. If the EVS fails over onto another node, the IP address moves with the EVS, activating the aggregation on the new node.

The server supports static aggregations. It also supports the Link Aggregation Control Protocol (LACP) for dynamic aggregations.

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



Note: Models 5200/5300 and the NAS module support up to six link aggregations. Models 4060/4080/4100 support up to four aggregations.

Link Aggregation Control Protocol (LACP)

The server supports the Link Aggregation Control Protocol (LACP), which it uses to manage an individual link's transmission state (within a Link Aggregation Group). The server controls the LACP relationship between multiple switches. The server determines which network interfaces are in use and can bring up alternative network interfaces during a failure. For example, if the server does not receive any LACP messages from the primary switch (the waiting time is determined by the configured LACP timeout), the server can use the network interfaces connected to the secondary switch instead.

LACP aggregates are not automatically created or populated. The administrator must first create an aggregate interface, then enable LACP on that interface.

Note: The server always sends LACP data units set to ACTIVE. However, the switch can be in active or passive mode.

LACP timeouts

The server supports both short (one second) and long (30 second) LACP timers. A short timeout is three seconds (three x one second). A long timeout is 90s (three x 30 seconds). Therefore, the link times out after three missed messages. Long timeouts are recommended to upgrade upstream network devices without causing path failover on the server. The default NAS setting is a short timeout.

Typical LACP configurations

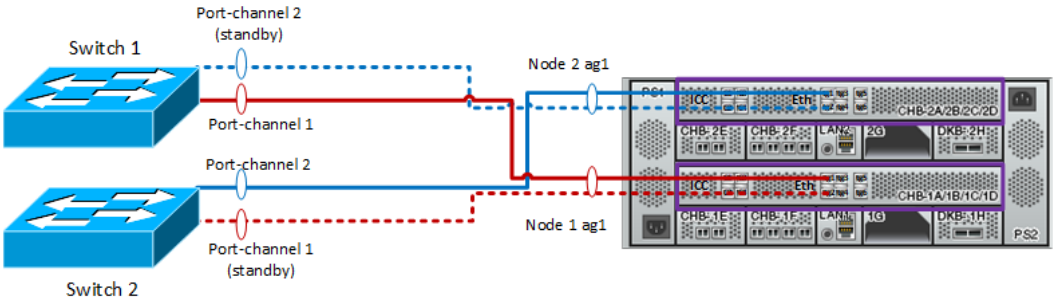
There are several typical configurations when using LACP with NAS servers and multiple switches for resiliency:

- Split-LAG with Layer-2 redundancy
- Split-LAG with Layer-2 redundancy and increased bandwidth
- Split-LAG with a single logical switch

Note: Static aggregation is not supported in a split-LAG scenario with two independent switches.

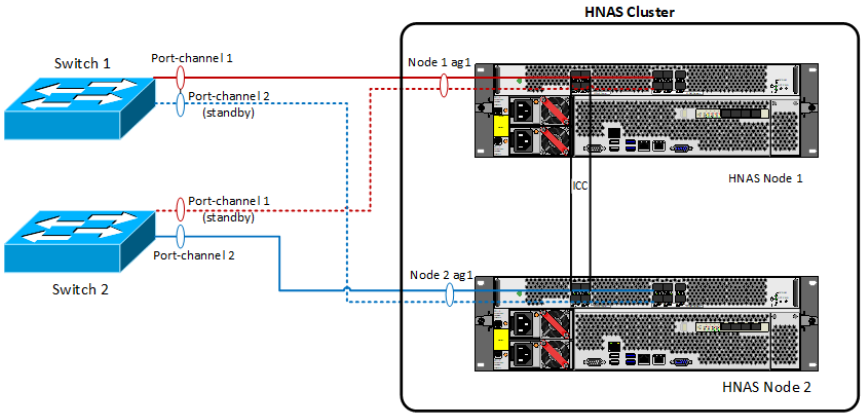
Split-LAG with Layer-2 redundancy (NAS module)

With LACP enabled, the two NAS modules in a Unified setup can be connected to a pair of independent switches configured with one link aggregation (over two file-serving interfaces), as shown in the example below. In this setup, only one of the ports in the aggregate will be active; since the switches are independent from each other LACP will disable the other interface, as illustrated by the dotted lines.



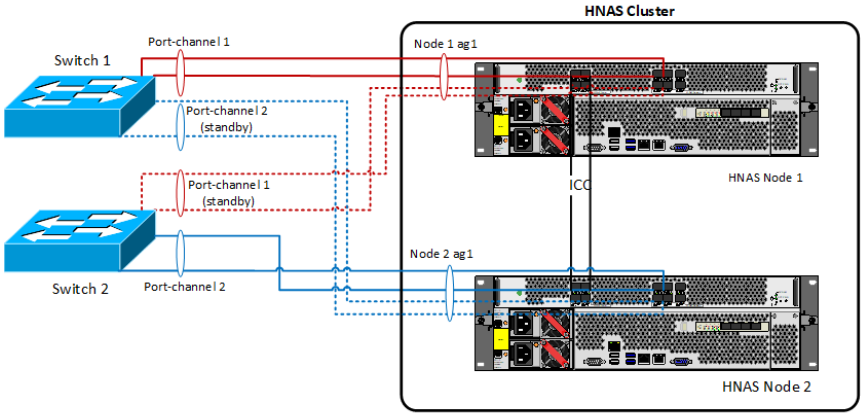
Split-LAG with Layer-2 redundancy (HNAS cluster)

With LACP enabled, a pair of clustered HNAS servers can be connected to a pair of independent switches configured with one link aggregation (over two file-serving interfaces), as shown in the example below. In this setup, only one of the ports in the aggregate will be active; since the switches are independent from each other LACP will disable the other interface, as illustrated by the dotted lines.



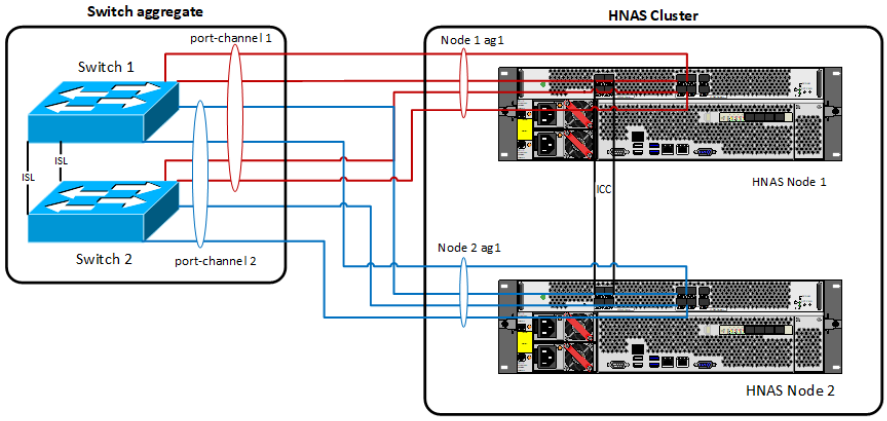
Split-LAG with Layer-2 redundancy and increased bandwidth

This configuration is a continuation of the previous example, using a link aggregation over four file-serving interfaces to two separate switches. This doubles the active and standby links, as shown in the example below:



Single logical switch with Layer-2 redundancy and increased bandwidth

This configuration includes a pair or switches connected in such a way as to appear as one logical switch. The HNAS servers are configured with a link aggregation over four file-serving interfaces, as shown in the example below. In this scenario since the switches are logically connected and no longer independent, a single port channel will extend across the switches and use all available links, and therefore all the ports will become active. This is the most optimal configuration for link aggregation across two switches.



VLAN interfaces

A physical network can be partitioned into multiple, isolated distinct broadcast domains called virtual LANs or VLANs. The NAS server supports a maximum of 256 VLANs with a range of VLAN IDs from 1 to 4094 (0 and 4095 are invalid).

A server can provide access to a VLAN using a VLAN interface on an aggregate interface. Administrators can create a VLAN interface for each tagged VLAN for each aggregate interface over which the NAS server needs to communicate. For example, VLAN 1 on ag1 is different from VLAN 1 on ag2.

Note: If an address is assigned to a VLAN interface, the server discards untagged packets for that address. Therefore, do NOT create a VLAN interface for the native or otherwise untagged VLAN, as it can result in a loss of connectivity.

Non-file serving interfaces

NAS servers provide non-file serving physical interfaces. These interfaces use standard RJ45 connectors.

The servers use auto-negotiation for speed/duplex/flow control by default. We recommend a 1Gbps speed for the switch uplink port for the non-file serving interfaces with full duplex, bi-directional flow control enabled.

A non-file serving interface must be connected to access the internal NAS Manager and to use the following features:

- V2I
- VASA Provider
- Data Migrator to Cloud (DM2C)

NAS module

These models provide a single 10/100/1000 Ethernet non-file serving interface. It is possible to connect to this interface as follows:

- SSH to either the "Unified Management IP Address" (shown in the **IP Addresses** page of the NAS Manager) or the address shown on the maintenance utility "Network Settings" page.
- SSC to either the "Unified Management IP Address" or the address shown on the maintenance utility "Network Settings" page.

Connecting to the NAS module using these IP addresses provides the user with a command line interface. See the CLI Reference manual for available commands.

To access the NAS Manager in a Web browser, use the "Unified Management IP Address" appended with the port number 20443. The browser connection must be secure (HTTPS).

HNAS server

These models provide two 10/100/1000 Ethernet non-file serving interfaces as follows:

- eth1
- eth0

eth1

This interface is mandatory and enables users to communicate with the NAS Manager, any auxiliary devices, and the non-file serving interfaces of other HNAS servers. During initial setup of the HNAS server, this interface is configured with an IP address. This interface can also be configured with a separate cluster node IP address if the server is intended to be part of a cluster.

eth0

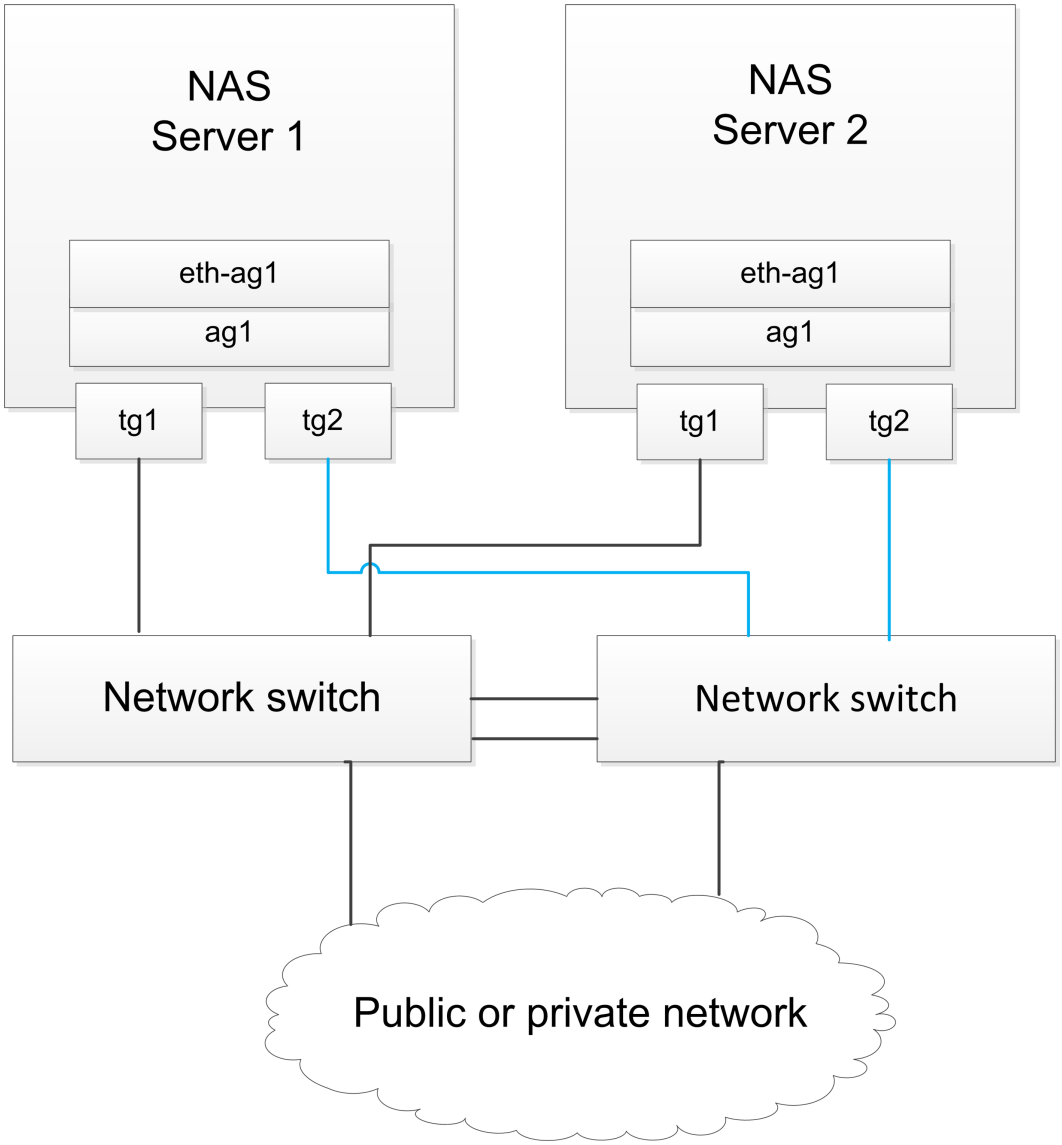
This interface is optional and enables the user to configure file services on the server as well as create and configure Enterprise Virtual Servers (EVSs).

During initial setup of the HNAS server, this interface is configured with an IP address. Connecting to the HNAS server using this IP address enables direct access to the server management interface and provides users with a command line interface. See the CLI Reference manual for available commands.

Note: Remember to secure the NAS password which is exposed when using the eth0 interface.

Aggregate Linux interfaces

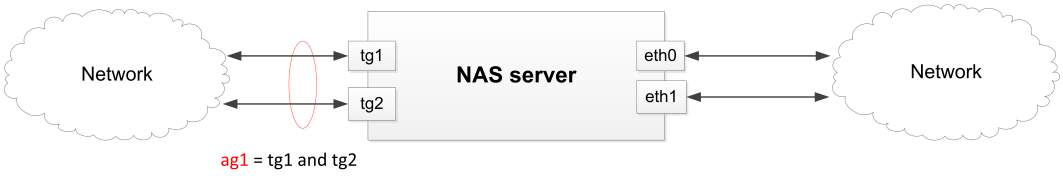
The NAS server provides the ability to access the file serving interfaces (agX) from Linux, using a virtual Linux network interface (eth-agX), which is bound to a specific agX interface as shown below:



Using an aggregate Linux interface (instead of eth0 or eth1) provides a potentially faster route for data and management traffic. It also enables the non-file serving interfaces (eth0 and eth1) and the file serving aggregations to be physically separate while providing Linux access to both sets of interfaces.

Example

For the scenario below:



The Administrator can create **eth-ag1** over **ag1** as shown below:

```
aggregate-linux-interface-create --interface ag1
```

Now, any functionality that is available on eth0 and eth1, is also available on the file serving interfaces. This can include using SSH with the Admin EVS IP address.

For information on how to manage the eth-agX interfaces, see the following CLI commands:

- **aggregate-linux-interfaces**
- **aggregate-linux-interface-show**
- **aggregate-linux-interface-create**
- **aggregate-linux-interface-delete**

Typical non-file serving interface configurations: NAS module

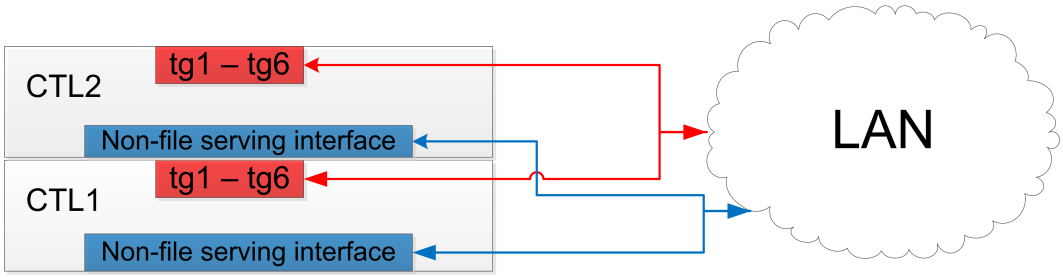
There are two typical configurations for the NAS module non-file serving interface:

- Single network for both management and file-serving functionality
- Separate networks for management and file-serving functionality

All NAS module configurations use the embedded SMU.

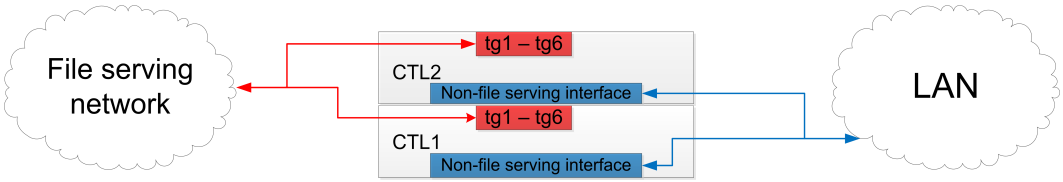
Single network for both management and file-serving functionality

In this configuration, the NAS module is connected to a single LAN and both the file-serving interfaces and the non-file serving interface connect to this network.



Separate networks for management and file-serving functionality

In this configuration, the non-file serving interface on the NAS module is connected to the management network and the file-serving interfaces are connected to a data network.



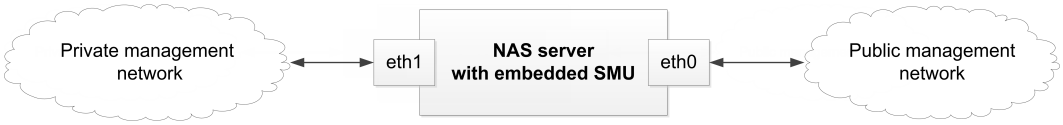
Typical non-file serving configurations: HNAS servers

There are three typical configurations for non-file serving interfaces on a NAS Platform Series 4000 and NAS Platform Series 5000 :

- Single HNAS server (embedded SMU)
- Single HNAS server (external SMU)
- Clustered HNAS servers (external SMU)

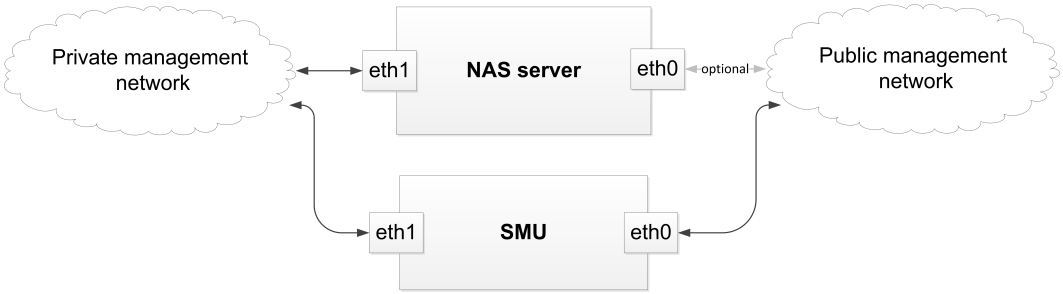
Single HNAS server (embedded SMU)

In this configuration, the HNAS server uses an embedded SMU (NAS Manager) where eth1 is connected to the private management network and eth0 is connected to the public management network.



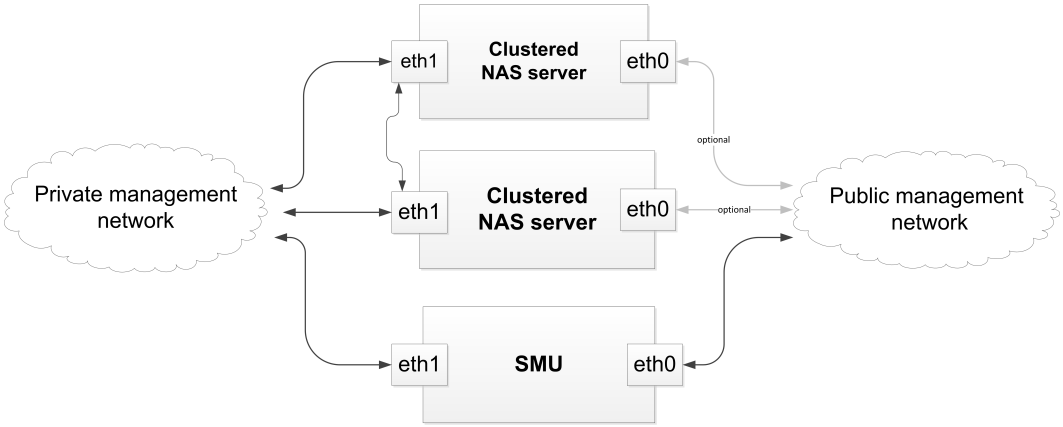
Single HNAS server (external SMU)

In this configuration, the HNAS server uses an external SMU. This is necessary when maintaining external configuration backups and also when preparing the HNAS server to join a cluster. In this case, eth1 on the HNAS server and eth1 on the SMU are connected to the same private management network, and eth0 on the HNAS server is optionally connected to the public management network.



Clustered HNAS servers (external SMU)

In this configuration, the HNAS server is part of a cluster with an external SMU. In this case, eth1 on each HNAS server and eth1 on the SMU are connected to the same private management network, and eth0 on each HNAS is optionally connected to the public management network.



Jumbo frames support

All file serving interfaces of a server support jumbo frames. Jumbo frames enable transmission of Ethernet frames with a payload larger than 1500 bytes, and these frames co-exist with standard frames on an Ethernet network.

All file serving interfaces receive jumbo frames unconditionally, without any configuration changes. It is possible to configure a file serving interface to transmit jumbo frames by specifying an MTU size of between 1,501 and 9,600 bytes.

To use jumbo frame transmission, configure the following settings:

- IP MTU for off-subnet transmits - bytes
- TCP MTU
- Other Protocol MTU

Caution: Networking equipment that lacks the jumbo frames extension can 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, it is possible to experience a loss of communication with the server or 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 IP MTU in use is the lowest of:

- The interface IP MTU setting
- Any IP MTU specified by the selected route
- Any IP MTU specified by the MTU command

The recommended MTU size is 8972 bytes (to compensate for the IP and ICMP headers).

Cluster switch configuration

When configuring switches for use with NAS server clusters, there are several guidelines to follow in order to optimize the transfer of data.

Note: The following guidelines are specific to the cluster interconnect network (the connections between the cX ports). They do not refer to the file-serving or management/maintenance networks.

Network infrastructure

Each cluster must have its own isolated/private cluster interconnect (ICC) layer-2 network as system performance depends upon the cluster interconnect network delay and bandwidth. The cluster interconnect network must be designed to limit network congestion and therefore it requires dedicated bandwidth rather than sharing bandwidth with other networks. Consider using a redundant network infrastructure for cluster interconnect.

A cluster with 2 nodes (HNAS server models) can have direct connections. Port C1 in one node must connect to port C1 in the other node, and port C2 in one node must connect to port C2 in the other node. NAS modules are inherently 2-node clusters and use their own internal connections, so no cabling or switch infrastructure is required.

A cluster of 3 nodes or more requires at least two switches for redundancy. Connections should be as follows:

- NAS Platform Series 4000 models: All C1 ports must connect to the same switch infrastructure, and all C2 ports must connect to the same switch infrastructure. The switch infrastructure for C1 and C2 can be separate and isolated from each other.

- NAS modules and NAS Platform Series 5000 models: C1 ports, and optionally C2, should connect to each other in the same switch infrastructure. C3, and optionally C4 ports, should connect to each other in the same infrastructure. Note that the use of C2 and C4 ports is optional and only necessary when additional NVRAM mirroring bandwidth is required.

Jumbo frames

Jumbo frames must be enabled. Specifically, the switch must be able to pass frames of at least 9216 bytes.

Spanning Tree

This feature must be disabled on the switch ports connected to the NAS servers, so that the ports will not attempt negotiation and therefore boot faster. This is sometimes known as portfast.

Interswitch link

Each physical connection must have a minimum of 10Gbps bandwidth, to avoid potential congestion and packet loss. Techniques to accommodate for asymmetric bandwidth (such as 10Gbps to multiple 1Gbps) might not be sufficient in this context.

For redundancy, the ISL in a cluster with more than 3 nodes needs to be an aggregation; there is also a small benefit for aggregating 3-node clusters, but it is not required. The recommended minimum number of (10 Gbps) physical links is half the number of cluster nodes, rounding down for odd-sized clusters.

You can also use ISLs for the connections between sites with cluster members on separate networks. ISLs must provide adequate bandwidth, as cluster protocol performance is not optimised in the event of packet loss.

Where more than one link's bandwidth is needed, close attention must be paid to the switches' frame distribution algorithm(s). The small number of source and destination addresses in a cluster creates a significant risk of very uneven traffic distribution within a link aggregation. Do not use non-compliant algorithms that could allow frame reordering, such as round-robin. Consider using switches with faster "uplink" ports instead.

Egress tagging must be enabled on ISL ports.

VLANs

ICC traffic must be isolated from any other traffic that may run on the switch. This is usually done by the use of VLANs.

For NAS Platform Series 4000 models, the C1 and C2 networks must be isolated from each other. Therefore, if they share the same switch infrastructure each should have its own dedicated VLAN.

For servers models with four ICCs (NAS Platform Series 5000), there is no requirement to isolate the two ICC networks (C1 or C2 and C3 or C4) from each other.

The server's cluster interface is not VLAN-aware and does not support VLAN configuration, so the switch ports must be untagged members.

Priority

The server uses 802.1Q priority tagging to manage congestion. Management traffic is carried in priority tagged frames with Priority Code Point 2; mirroring traffic is tagged with Priority Code Point 0; CNS traffic is tagged with Priority Code Point 1. Under the recommended default traffic class mappings (see IEEE 801.1G-2014, Annex I.4), the management traffic has a higher priority than the mirroring traffic and the CNS traffic has the lowest priority.

Note: Fast-path traffic must not be assigned to a higher traffic class than management traffic.

It is required that the switch must be configured to observe the 802.1Q priorities. Some switches have an optional switch to enable strict adherence to 802.1Q priorities - on those switches, enable that option. For priority information to be propagated properly, ISL ports must be tagged VLAN members (of the default VLAN where VLANs are not required for segregation).

Chapter 2: Routing overview

This section contains IP routing concepts. Depending on configuration, the server can route IP traffic in three ways: through *Default Gateways*, *Static Routes*, and *Dynamic 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 NAS server supports gateway, network and host static routes. The `Default` option sets up a gateway and does not require a destination. 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. 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 statically configure gateways as they are automatically discovered through the received router advertisements.

Dynamic routes

The NAS server supports ICMP redirects and RIP versions 1 and 2, which enable it to dynamically add routes to its route table.

ICMP redirects

This is a mechanism 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 stores dynamic host routes in its routing table for up to 10 minutes. When a dynamic host route expires, it is removed from the routing table. When subsequent packets are sent to the selected destination, the choice of gateway is determined by the remaining routes in the routing table until the server receives another ICMP redirect. The server creates a dynamic host route for each redirect received. The host route cache can store up to 65,000 dynamic routes at a time.

ICMP router discovery

The NAS server supports ICMP router discovery, which enables 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.

ICMP router discovery is controlled using the CLI command **`irdp`**. For more information, see the *Command Line Reference*. A router discovered using IRDP is propagated to the routing table as a default gateway.

The NAS server discovers IPv6 default gateways through ICMPv6 router advertisements.

RIP (v1 and v2)

RIP is an industry standard protocol that enables servers to automatically discover routes and then update routes in the route table based on updates provided by other network devices. RIP (v1 and v2) is controlled using the CLI command **`rip`**. For more information, refer to the *Command Line Reference*.

Managing routes

The server selects the most specific route available for outgoing IP packets. The *host route* is the most specific, as it targets a specific computer on the network. The *network route* is the next most specific, as it targets a specific network. A *gateway* is the least specific route. Therefore, if a server finds a host route for an outgoing IP packet, it selects that route over a network route or gateway. Similarly, when a host route is not available, the server selects a corresponding network route or, in the absence of host and network routes, the server sends the packet to a default gateway.

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 when not in multi-tenancy 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`**

Chapter 3: Name and directory services

This section contains information on the local name and directory services that the server can support. These services help the server to support the location, administration, and management of network resources.

Name services

The server supports the following name resolution methods:

- Domain Name System (DNS)
- NIS and LDAP (see Directory services)
- Windows Internet Naming Service (WINS)

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

The server supports Dynamic Domain Name System (DDNS) for updating a name server.

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.

Note: Disable DDNS if the SMB3 Continuous Availability feature is in use on the server.

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. After it successfully registers, it resumes the 24 hours-per-refresh cycle.

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.

Directory services

The server supports the following directory service methods:

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

These services associate identifiers with users, groups, devices, volumes, folders, and other network resources. This functionality enables Administrators to specify policies for access on a broad basis, rather than explicitly on a per-resource basis, and to have this information accessible throughout the network.

NIS (for NFS and FTP)

NIS databases provide simple management and administration of Unix-based networks. These databases can provide details about users and groups, and 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 integration with NIS directory services which can provide the following:

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

LDAP advantages

Many organizations are replacing their existing NIS infrastructure with the more reliable, scalable and secure LDAP system. 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:

- Oracle Directory Server
- OpenLDAP

Chapter 4: Using IPv6

This section contains an overview of IPv6 and information on using IPv6 with the NAS server.

IPv6 overview

The current Internet protocol address standard, IPv4, uses a 32-bit address and has an insufficient number of available addresses for global usage. The next generation Internet protocol address standard, IPv6, uses a 128-bit address. This provides a much larger pool of addresses. The NAS server supports both IPv4 and IPv6 at the same time (dual-stack).

Address formats

An IPv4 address consists of dotted quads, for example 127.0.0.1.

For an IPv6 address, each 16 bits of the 128 bit address is represented as a hexadecimal number separated by a colon (:) as shown below:

```
2001:db8:0:0:1:0:0:1
```

Repeated fields of zeroes can be replaced by :: as shown below:

```
2001:db8::1:0:0:1 or 2001:db8:0:0:1::1
```

There can only be one :: in the text representation of an address.

IPv6 addresses have a 64-bit netmask which consists of the 64 leftmost bits of the address which is represented in CIDR format as shown below:

```
2001:db8::/64
```

This represents an address range of 2001:db8:0:0:0:0:0:0 to 2001:db8:0:0:ffff:ffff:ffff:ffff.

Address resolution

IPv6 uses NDP (Neighbor Discovery Protocol) instead of ARP for address resolution and IRDP for router discovery.

IPv6 and the NAS server

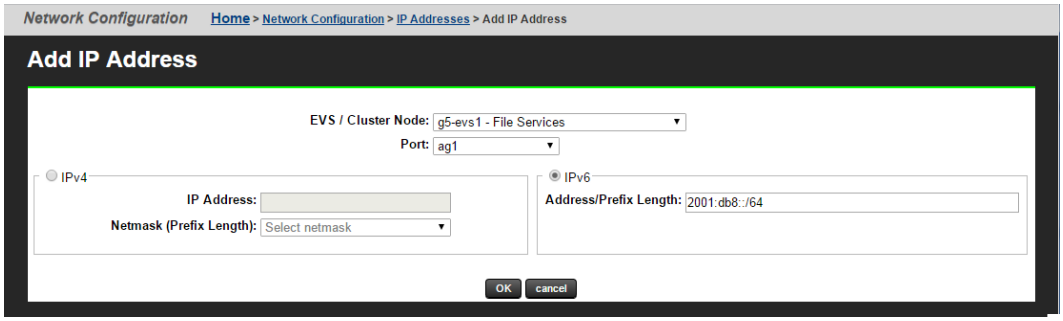
On the NAS server, wherever an IP address is specified, it is possible to add IPv4 or IPv6 addresses. If the NAS server is configured with IPv6 addresses, clients can connect to it using IPv6. However, to connect to it from both IPv4 and IPv6 clients, it is necessary to configure both IPv4 and IPv6 addresses.

Note: The NAS server does not support SLAAC on file-serving interfaces.

Using the NAS Manager with IPv6

It is possible to use the NAS Manager to configure IPv6 addresses for file-serving and non-file serving interfaces, routes and name services.

For example, the Administrator can set an IPv6 address for ag1 on the file-serving interfaces. The format is <address>/<prefix length> as shown below:



This page is also where an IPv6 address is configured for the Admin Services Node. This is necessary in order to launch the NAS Manager over IPv6. It is not possible to configure an IPv6 address on a cluster node.

Using CLI commands with IPv6

Each CLI command that accepts IPv4 addresses also accepts IPv6 addresses, for example, the **evs** command as shown below:

```
> evs create -i 2001:db8::/64 -p ag2 -n 1
```

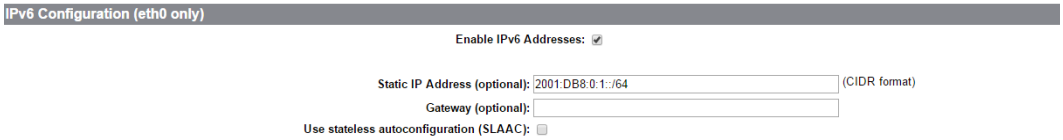
Some commands, for example **ping**, have an IPv6 variant **ping6**, as shown below:

```
> ping6 -c10  2001:db8:220a:480:baac:6fff:fe80:5962
32 bytes from 2001:db8:220a:480:baac:6fff:fe80:5962 icmp_seq=0 time=6 ms
32 bytes from 2001:db8:220a:480:baac:6fff:fe80:5962 icmp_seq=1 time <1 ms
32 bytes from 2001:db8:220a:480:baac:6fff:fe80:5962 icmp_seq=2 time <1 ms
```

IPv6 and non-file serving interfaces

On the NAS server, an IPv6 address can be configured on the Admin Services Node - eth0 or eth1. On the SMU, IPv6 addresses are configurable on both eth0 and eth1. On an external SMU, eth0 is considered to be a public interface and eth1 is considered to be a private interface that is used for internal communication. The eth0 interface must always retain an IPv4 address. The IPv6 configuration is in addition to the IPv4 configuration.

The Administrator can configure a static IPv6 IP address for an external SMU as shown in the example below or use the SLAAC option where the address is generated from router advertisements.



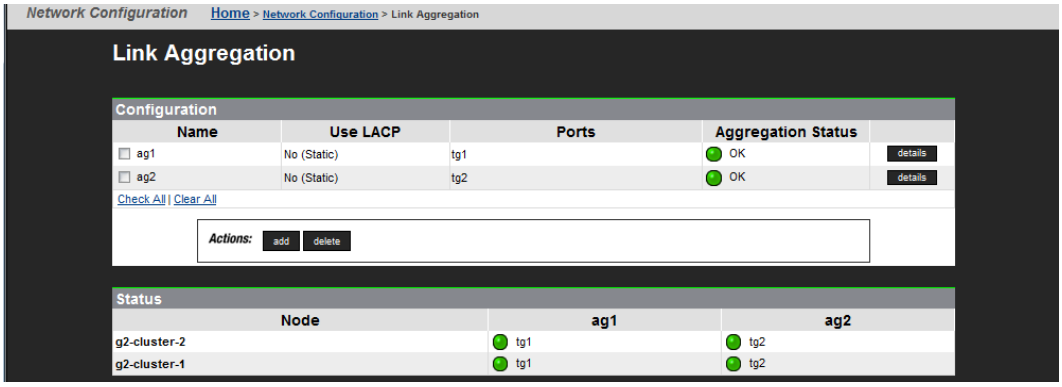
The Administrator can use this address to launch the external SMU GUI (NAS Manager) and it also enables the external SMU to manage a server with an IPv6 Admin Services Node address.

Chapter 5: Configuring link aggregation

This section contains information on viewing current link aggregation details, adding and removing link aggregations, and configuring aggregate Linux interfaces.

Viewing link aggregations

To view the status of an aggregation, navigate to the **Network Configuration -> Link Aggregation** page:



Adding link aggregations

Procedure

1. Navigate to **Network Configuration > Link Aggregation**, then click **add** to display the Add Link Aggregation page.
2. Specify the configuration of the aggregation as required.
3. Verify the settings, then click **OK** to apply the settings, or **cancel** to decline.

Field / Item	Description
Name	This field lists the available aggregation names. Select a name from the list.

Available ports	This field lists the available **ge** (gigabit Ethernet) and **tg** (10 GbE) interfaces to add to the aggregation. To add an interface to the aggregation, select the check box next to the name of the interface.
Use LACP	This field specifies whether the aggregation uses 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.
Port level load balancing	This field displays the port load balancing scheme in use for all interfaces in the aggregation. The options are: ▪ **Normal** - the server distributes all traffic for a given conversation through one of the physical interfaces in the appropriate aggregation. The server's hash and routing functions determine which packets use which physical interfaces. For example, all traffic for a particular TCP connection is always distributed through the same physical interface (unless the link drops). However, the server is not guaranteed to respond to the same client on the same interface. ▪ **Round robin** - the server selects outgoing interfaces in sequential order, on a packet-by-packet basis. This aggregation load balancing function ensures that all the interfaces are more or less equally used. 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, it can be useful when, for example, running security scan request traffic, by increasing throughput. Select the radio button next to the required load balancing scheme.

Editing link aggregations

Edit the configuration of an aggregation on the Link Aggregation Details page:

- Remove interfaces from the aggregation
- Add interfaces to the aggregation
- Select an aggregation type: static or LACP
- Change the type of load balancing in use for the aggregation

Procedure

1. Navigate to **Network Configuration > Link Aggregation** to display the Link Aggregation page, which lists all currently configured aggregations.
2. Click **details** to display an aggregation's Link Aggregation Details page.
3. The **Assigned Ports** field lists the interfaces currently assigned to this aggregation. To remove an interface from the aggregation, deselect the check box next to the name of the interface.
4. The **Available Ports** field lists the available **ge** (gigabit Ethernet) and **tg** (10 GbE) interfaces that can be added to the aggregation. To add an interface to the aggregation, select the check box next to the name of the interface.
5. The **Use LACP** field specifies whether the aggregation uses LACP. Select **Yes** to 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.
6. Select a Port load balancing scheme in the **Port level load balancing** field. The options are Normal and Round robin.
7. Click **OK** to save the changes, or click **cancel** to return to the Link Aggregation page without saving the changes.

Deleting link aggregations

Caution: Before deleting an aggregation, remove all IP addresses, **ge** and **tg** interfaces associated with the aggregation.

Procedure

1. Navigate to **Network Configuration > Link Aggregation** to display the Link Aggregation page.
2. Select the check box next to the aggregation name to delete.
3. Click **delete** to remove the aggregation. When deleting an aggregation, there is no confirmation required. The aggregation is deleted immediately.

Configuring LACP

To enable LACP for an aggregation using the CLI instead of the NAS Manager, use the **`aggedit`** command as shown in the example below:

```
aggedit lacp ag1
```

where `ag1` is the required aggregation interface.

File serving interfaces which are connected to a LACP enabled switch must be manually added to an LACP aggregation as shown in the example below:

```
aggedit add ag1 tg1,tg2
```

where ag1 is the aggregation and `tg1` and `tg2` are the file serving interfaces.

To view the status of LACP for an aggregation, use the **`lacp`** command.

Configuring LACP timeouts

To set a short LACP timeout, use the **`lacp-set-timeout-short`** command as shown in the example below:

```
lacp-set-timeout-short ag1
```

where `ag1` is the required aggregation interface.

To set a long LACP timeout, use the **`lacp-set-timeout-long`** command as shown in the example below:

```
lacp-set-timeout-long ag2
```

where `ag2` is the required aggregation interface.

Additional commands

- **`agg`** - this command lists any existing aggregations
- **`lacp-set-timeout-default`** - this command selects the default LACP timeout (short timeout)
- **`lacp-show`** - this command displays the LACP configuration

Configuring aggregate Linux interfaces

To view any existing aggregate Linux interfaces, on the command console, enter the following command:

`aggregate-linux-interface-show`

The interfaces appear as shown in the example below:

```
$ aggregate-linux-interface-show
eth-ag1
$
```

Creating a new interface

All new aggregate Linux interfaces must be associated with an existing file serving link aggregation.

To create a new interface, enter the following command:

`aggregate-linux-interface-create --interface <interface>`

For example:

```
$ aggregate-linux-interface-create --interface ag1
```

In this example, the server creates an interface named eth-ag1 which uses ag1 to send and receive management traffic.

Deleting an existing interface

To remove an existing interface, enter the following command:

`aggregate-linux-interface-delete <eth-ag-interface>`

For example:

```
$ aggregate-linux-interface-delete eth-ag1
```

In this example, the server deletes an interface named eth-ag1 but ag1 is not removed.

Chapter 6: Configuring VLAN interfaces

This section contains information on configuring, adding, and deleting VLAN interfaces.

Adding 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.

VLAN interfaces that have been dynamically created by the deprecated **vlan** command only appear in the ifconfig display. For further information on converting a dynamic VLAN interface into a static VLAN interface, see the **VLAN conversion** Appendix.

Procedure

1. To create a VLAN interface, use the **vlan-interface-create** command and supply the base aggregation interface name and the VLAN tag as shown in the examples below:

```
$ 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 display the existing 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 the 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 172.16.0.10/16 -p ag1-vlan0499


$ evs list
    5     Service  EVS1   Yes    Online   10.0.0.10        ag1-vlan0433
    6     Service  EVS2   Yes    Online   172.16.0.10      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 as follows:

```
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.

Advanced VLAN interface configuration

A global configuration setting applies to all interfaces, including VLAN interfaces, except those for which a specific configuration exists. However, settings for a parent aggregation interface do not apply to the associated VLAN interfaces; for example, a configuration for ag2 does not affect traffic over ag2-vlan0017.

To apply an MTU setting to a specific VLAN interface, it is necessary to create a specific configuration for the full interface name of the VLAN. For example, to change the MTU for VLAN 17 on ag2, create a specific configuration for ag2-vlan0017 and set the required values.

Before creating a specific VLAN interface configuration, use the **`ifconfig`** command to view all the names of all available VLAN interfaces. VLAN interfaces created using the deprecated **`VLAN`** command appear in this list as well as VLAN interfaces created using the **`VLAN-interface-create`** command.

To create a configuration for a VLAN interface

Enter the following command:

```
ipadv -x create -p <vlan interface name>
```

For example:

```
ipadv -x create -p ag12-vlan0017
```

To set the MTU size for a VLAN interface

For TCP packets:

```
ipadv --tcpmtu <tcpmtu> -p <VLAN interface name>
```

For example:

```
ipadv --tcpmtu 9000 -p ag2-vlan0017
```

Alternatively:

```
ipadv -m 9000 -p ag2-vlan0017
```

For non-TCP packets (UDP/ICMP):

```
ipadv --othermtu <othermtu> -p <VLAN interface name>
```

For example:

```
ipadv --othermtu 9000 -p ag2-vlan0017
```

Alternatively:

```
ipadv -n 9000 -p ag2-vlan0017
```

For off-subnet values:

```
ipadv --offsubnetmtu <offsubnetmtu> -p <VLAN interface name>
```

For example:

```
ipadv --offsubnetmtu 9000 -p ag2-vlan0017
```

Alternatively:

```
ipadv -o 9000 -p ag2-vlan0017
```

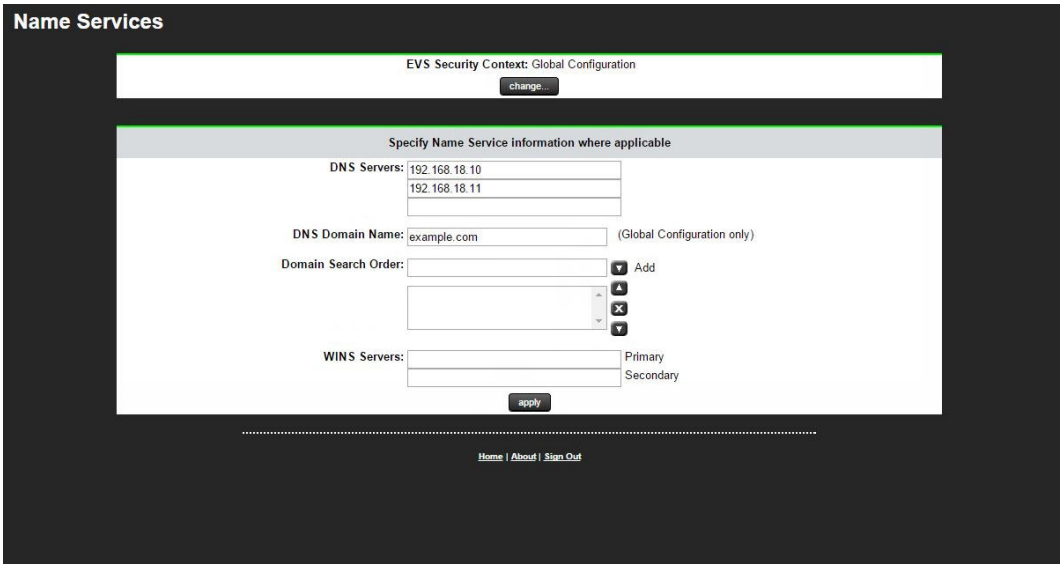
Chapter 7: Configuring name and directory services

This section contains information on specifying and prioritizing name services and configuring NIS and LDAP servers.

Specifying name services

Procedure

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



The following table describes the fields on this page:

Field/Item	Description
EVS Security Context	Displays the currently selected EVS security context. Changes to the name services using this page apply only to the currently selected EVS security context. ▪ If an EVS uses the Global Configuration, any change made to the global configuration settings affects the EVS. ▪ 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 **change** to select a different EVS security context or to select the global configuration.
DNS Servers	Specifies the IP addresses of up to three DNS servers. If more than one DNS server is entered, the search is performed using the DNS servers in the order listed.
DNS Domain Name	Specifies the DNS domain name to use.
Domain Search Order	Enter a Domain suffix (for example, `example.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 `uk.example.com` and `us.example.com`, a request for the IP address of a host named author generates a query for `author.uk.example.com` and then for `author.us.example.com`. However, the system does not search the parent Domain `example.com`. **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.
WINS Servers	To set up a primary WINS server, enter the IP address in the Primary WINS server field.

Field/Item	Description
	If there is a secondary WINS server, enter the address in the Secondary WINS server field.
apply	Save your changes.

2. Enter the requested information.
3. Click **apply** to save your changes.

Note: The new name service appears on the **Name Services Order** page.

Prioritizing name services

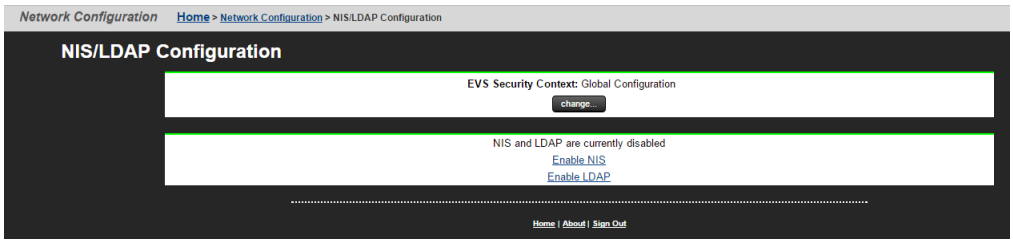
Procedure

1. Navigate to **Network Configuration > Name Services order**.
2. Use the change button to change the security context, if required. Changes to the name services on 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 affect the EVS. 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, even if those settings are the same as the settings used by the global security context.
3. Select and deselect name services to create a list of preferred name services. Use the left and right arrow keys to select name services from the Available Name Services box and move them to the Selected Name Services box. To deselect a name service, use the arrows to move the name service back into the Available Name Services box.
4. Adjust the order of usage for selected name services. Use the up and down arrow keys to change the order of usage for selected name services in the Selected Name Services box.
5. Click **apply** to save the changes.

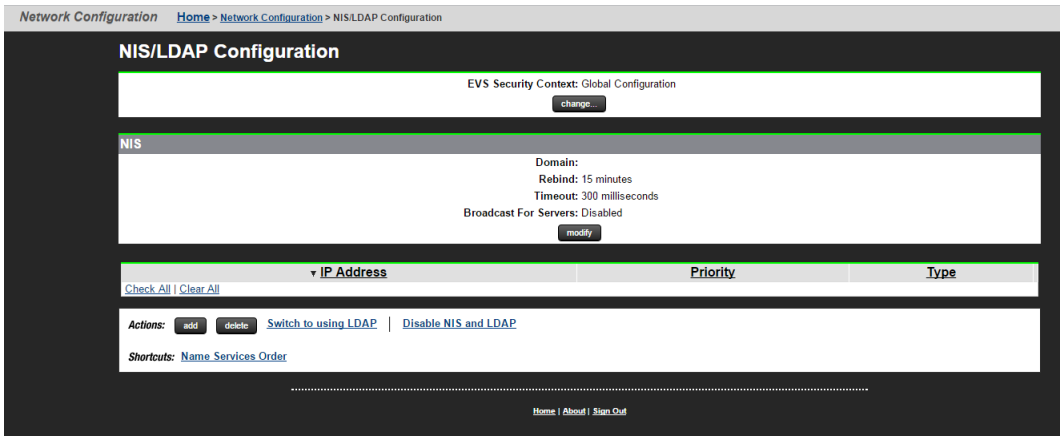
Configuring NIS servers

Before using NIS, it is necessary to enable NIS for the server.

To enable NIS, navigate to **Network Configuration > NIS/LDAP Configuration** and click **Enable NIS**.



The current NIS configuration settings appear as shown in the following example:



This page contains the following options:

- **Modify** - this option enables the Administrator to change the NIS configuration settings
- **Add** - this option enables the Administrator to add a new NIS server
- **Delete** - this option enables the Administrator to remove an existing NIS server
- **Switch to using LDAP** - this option enables LDAP mode and displays the LDAP configuration settings
- **Disable NIS and LDAP** - this option disables NIS and LDAP

CLI commands

The following commands are available:

- **`nis-ldap-mode`** - this command selects whether the server uses LDAP or NIS servers to satisfy NIS queries
- **`nis-state`** - this command enables and disables the NIS client
- **`nis-show`** - this command displays the current NIS client settings
- **`nis-set`** - this command displays and sets the NIS client parameters
- **`nis-server`** - this command displays and sets the servers which are available for the NIS client to contact

Modifying NIS servers

Procedure

1. Navigate to **Network Configuration > NIS/LDAP Configuration**.
2. Click **modify**.
3. Modify the settings as described in the table below.

Field / Item	Description
EVS Security Context	This field displays the currently selected EVS security context. Changes to the name services on this page apply only to the currently selected EVS security context. If an EVS uses the Global Configuration, any change made to the global configuration settings affects the EVS. 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, 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.
Domain	Enter the name of the NIS domain for which the system is a client.
Rebind	This field requires the frequency of the server's attempts to connect to its configured NIS servers. The default value is 15 minutes.
Timeout	This field requires the amount of time (in milliseconds) to wait for a response from an NIS server when checking the Domain for servers. The default value is 300 milliseconds.
Broadcast For Servers	If selected, this field enables the server to discover the available NIS servers on the network. The servers must be in the same NIS domain and present on the server’s network.

4. Click **apply**.

Adding NIS servers

Procedure

1. Navigate to **Network Configuration > NIS/LDAP Configuration**.
2. Click **add**.
3. Modify the settings as described in the table below.

Field / Item	Description

Server IP address	Enter the IP address of the new NIS server which can satisfy NIS queries.
Priority	Enter the priority level for the selected NIS server (lowest value is highest priority). If the NIS domain contains multiple servers, the system attempts 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 the Administrator assigns a priority after clicking the **details** button, the NIS server type becomes “User Defined”. User Defined NIS servers are prioritized before servers discovered through broadcast. The options are: ▪ low (3) ▪ medium (2) ▪ high (1)

4. Click **OK**.

Deleting NIS servers

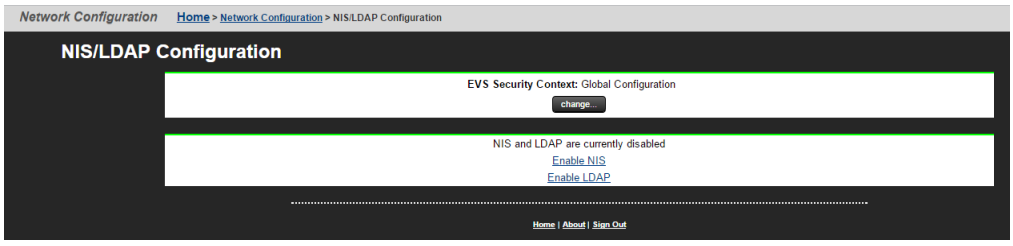
Procedure

1. Navigate to **Network Configuration > NIS/LDAP Configuration**.
2. Select a server to delete.
3. Click **delete**.

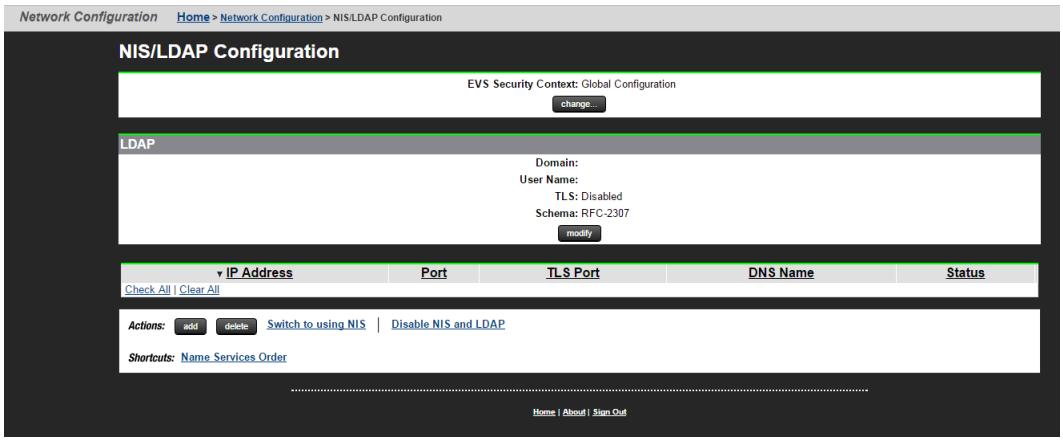
Configuring LDAP servers

Before using LDAP, it is necessary to enable LDAP for the server.

To use LDAP, navigate to **Network Configuration > NIS/LDAP Configuration** and click **Enable LDAP**.



The current LDAP configuration settings appear as shown in the following example:



This page contains the following options:

- **Modify** - this option enables the Administrator to change the LDAP configuration settings
- **Add** - this option enables the Administrator to add a new LDAP server
- **Delete** - this option enables the Administrator to remove an existing LDAP server
- **Switch to using NIS** - this option enables NIS only mode and displays the NIS configuration settings
- **Disable NIS and LDAP** - this option disables NIS and LDAP

CLI commands

The following commands are available:

- **`nis-ldap-mode`** - this command selects whether the server uses NIS servers only or LDAP in order to satisfy NIS queries
- **`nis-state`** - this command enables and disables the NIS client (the NIS client also must be enabled in order to use LDAP)
- **`ldap-server`** - this command displays and configures the servers which are available for the LDAP client to contact
- **`ldap-stats`** - this command displays statistics describing the response latency of LDAP servers for different NIS (RFC 2307) request types
- **`ldap-security`** - this command displays and sets the LDAP parameters
- **`ldap-schema`** - this command displays and sets the LDAP client settings for schema selection

Modifying LDAP configuration

Procedure

1. Navigate to **Network Configuration > NIS/LDAP Configuration**.

2. Click **modify**.
3. Modify the settings as described in the table below:

Field / Item	Description
Domain	Enter the name of the LDAP domain for which the system is a client.
Username	This field contains the username of the Administrator for the LDAP servers. 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=”Directory Manager”,dc=example,dc=com
Password	This field contains the password that corresponds to the username.
TLS Enabled	Select this option to enable Transport Layer Security which provides secure communication with the LDAP server.
Schema	This field contains the name of the schema to use. The options are: ▪ RFC-2307 ▪ MS Services for Unix ▪ MS Identity Management for Unix ▪ MS Active Directory

4. Click **apply**.

Note: This option supports both registered and anonymous user logins.

Adding LDAP servers

Procedure

1. Navigate to **Network Configuration > NIS/LDAP Configuration**.
2. Click **add**.
3. Modify the settings as described in the table below.

Field / Item	Description
Server IP address or Host name	Enter the IP address or Host name of the new LDAP server.

Port	This field specifies the standard port number to use for communication with the LDAP server. The default value is 389.
TLS Port	This field specifies the secure port to use for communication with the LDAP server. The default value is 636.

4. Click **OK**.

Note: An Administrator can query the LDAP server for information about hosts configured into netgroups using the **`nis-is-host-in-netgroup`** and **`nisnetgroups-for-host`** commands.

Deleting LDAP servers

Procedure

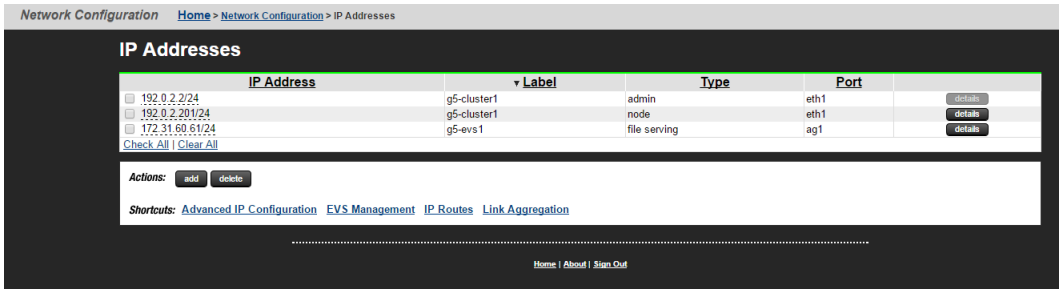
1. Navigate to **Network Configuration > NIS/LDAP Configuration**.
2. Select a server to delete.
3. Click **delete**.

Chapter 8: Configuring IP addresses

This section contains information on viewing, adding, and deleting IP addresses for the server.

Viewing IP addresses

To view the existing IP addresses, navigate to **Network Configuration > IP Addresses**.



The following table describes the fields on this page:

Field / Item	Description
Unified Management IP Addresses (NAS module only)	The IP addresses of both nodes in the NAS module. These addresses are read-only and cannot be modified in the NAS Manager. To change these addresses, use the maintenance utility.
IP Addresses	This field contains the IP address for the Admin and File services or for server/cluster node management.
Label	This field contains the name of the EVS (virtual server) that is assigned to the IP address.
Type	This field contains the type of services or configuration of the server:

	▪ **Admin** - an IP address associated with the Administrative Services for the cluster. Administration Services IP address can be on the public data network or on the private management network. ▪ **File serving** - an IP address associated with the File Services for the cluster. File Services IP addresses must be on the public data network. ▪ **Node** - the IP address associated with the physical cluster node. As File and Administrative services can migrate between nodes, the Cluster Node IP address communicates with the node instead of a service.
Port	This field contains the interface in use by the IP address: ▪ **agX** identifies one of the file serving aggregation interfaces ▪ **eth-agX** identifies one of the Aggregate Linux interfaces ▪ **agX-vlanXXXX** identifies one of the VLAN interfaces ▪ **eth0** or **eth1** identifies a 10/100/1000 interface for a Hitachi NAS Platform ▪ **mgmnt1** identifies the 10/100 management interface for a Hitachi High performance NAS Platform
Details	Click this button to view the **Modify IP Address** page. This page enables the Administrator to change the interface IPv4 and/or IPv6 settings.

Adding IP addresses

Note: It is not possible to add or modify an IP address for a NAS module. Use the maintenance utility to perform these functions.

Procedure

1. Navigate to **Home** > **Network Configuration** > **IP Addresses** > **add**. The **Add IP Address** page appears.
2. Select a Virtual Server (EVS) to assign to the IP address.
3. Select an aggregation or management interface:
   - **agX** identifies one of the file serving aggregation interfaces
   - **eth-agX** identifies one of the aggregate Linux interfaces
   - **agX-vlanXXXX** identifies one of the VLAN interfaces
   - **eth0** or **eth1** identifies a 10/100/1000 interface for an HNAS server

Note: When assigning an IP address to a file-serving EVS, the Administrator must specify a link aggregation or VLAN interface.

4. Enter the IP address and Subnet Mask for the selected interface.
5. Verify the settings, and then click **OK** to apply the settings or **cancel** to decline.

Deleting IP addresses

Caution: IP address deletion alert! Before following the instructions in this procedure, ensure that the IP address is not in use. Active connections are terminated on removal and clients can become unresponsive.

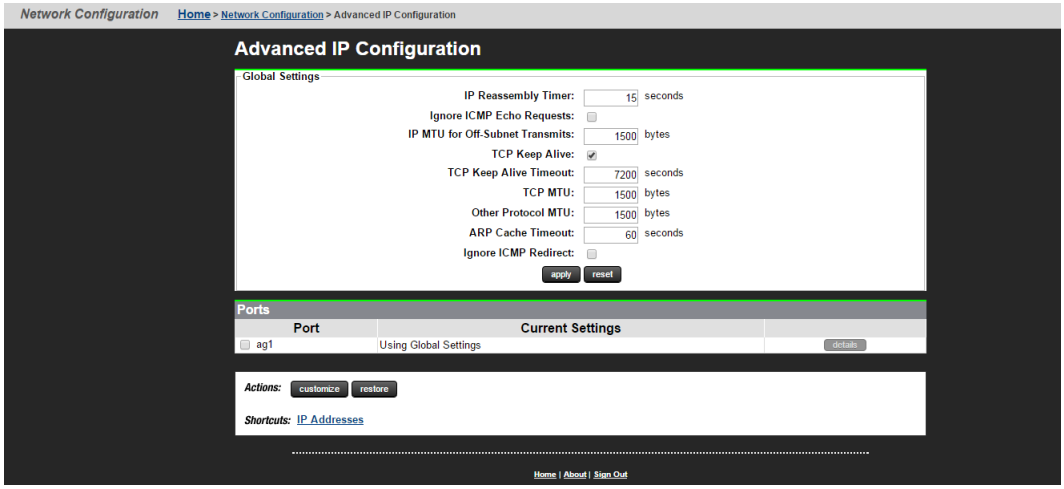
Note: It is not possible to delete an IP address for a NAS module. Use the maintenance utility to perform this function.

Procedure

1. Navigate to **Server Settings** > **EVS Management**.
2. Select the EVS to which the IP is assigned, then click **disable**.
3. Navigate to **Network Configuration** > **IP Addresses**.
4. Select the IP Address to delete, then click **delete**.
5. Navigate to **Server Settings** > **EVS Management**.
6. Select the EVS again and click **enable** to re-activate the EVS.

Advanced IP configuration

To configure additional settings for IP addresses, navigate to **Network Configuration > Advanced IP Configuration**.



Global settings

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

Note: These settings do not apply to ports eth0 or eth1.

The following table describes the fields on this page:

Global settings	Default	Description
IP Reassembly Timer (seconds)	15	This field sets the time before which the server discards an incomplete IP datagram.
Ignore ICMP Echo Requests	No (empty)	When selected, this option instructs the system not to respond to Internet Control Message Protocol (ICMP) echo requests.
IP MTU for Off- Subnet Transmits (bytes)	1500	This field specifies the maximum IP packet size in use when transmitting to a different subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, the effective MTU is 1280 bytes when this option is configured to be less than 1280.
TCP Keep Alive	Yes (filled)	When selected, this option 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.
TCP Keep Alive timeout (seconds)	7200	This field specifies the number of seconds to keep a connection alive.
TCP MTU (bytes)	1500	This field specifies the size of the maximum transmission unit (MTU) in use for TCP packets when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes. For IPv6 traffic, the effective MTU is 1280 bytes when this option is configured to be less than 1280.
Other Protocol MTU (bytes)	1500	This field specifies the size of the MTU for protocols other than TCP when transmitting to a locally configured subnet. The valid range is 68 to 9600 bytes . For IPv6 traffic, the effective MTU is 1280 bytes when this option is configured to be less than 1280.
ARP Cache Timeout (seconds)	60	This field controls the time before which the server removes an unused ARP entry from the caching table.
Ignore ICMP Redirect	No (empty)	This field specifies whether to ignore ICMP redirects.
Port	ag1 - agX	This field lists the name of each currently configured aggregation port (interface) in the server/cluster.
Current Settings		This field indicates whether the aggregation port uses the default (global) settings, or customized settings. If the aggregation port uses customized settings, the **details**

		button appears. Click on the **details** button to edit the customized configuration.

To customize the global settings, specify the values to use for the global configuration settings by changing the values of the fields in the Global Settings area. All aggregations (interfaces) use the global settings by default. Click **apply** to save the changes.

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

Interface settings

To customize settings for an individual aggregation port (interface), select it in the Ports field and click **customize**. The **Advanced IP Per-Port Configuration** page appears.

The following table describes the fields on this page:

Per-port settings	Default settings
Ignore ICMP Echo Requests	No (empty)
IP MTU for Off-Subnet Transmits (bytes)	1500
TCP MTU	1500
Other Protocol MTU	1500

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

To restore the settings of an interface to the global configuration, select an interface in the Ports field, and then click **restore**. The settings for the interface revert to the default (global settings).

CLI commands

Use the **ipadv** command to view or change these settings. It is also possible to configure an MTU value on a per-route basis using the **mtu** command.

Advanced IP configuration using the CLI

The **ipeng** command permits the manipulation of low level IP parameters. Only use this command under instruction from your support provider.

To reset all parameters to their default values, use the following command:

```
ipeng -d
```

Some of the parameters can be set on a per-interface basis, the rest are global settings.

To create a specific configuration for an interface, use the following command:

```
ipeng -x create -g <interface>
```

An interface-specific configuration must be created before specific values can be set for that interface. The interface-specific configuration can be created prior to creating the interface.

To delete an interface-specific configuration, use the following command:

```
ipeng -x delete -g <interface>
```

The **ipeng** command has the following default settings:

Parameter	Default value	Command
Def wnd (bytes)	64240	ipeng -w 64240
Delayed acks	On	ipeng -y on
Slow start ca	On	ipeng -s off
SS restart double mss	On	ipeng -r on
Nagle	Off	ipeng -n off
Silly window avoid	On	ipeng -a on
Slow start on idle	On	ipeng -i on
Fast retx fast recovery	On	ipeng -f on
Intelliseg	Off	ipeng -I on
Loose Karn enable	On	ipeng -k on
Strict TIME_WAIT enable	Off	ipeng -T on
Quick R1 teardown	Off	ipeng -q off
Minimum RTO	300	ipeng -o 300
Maximum RTO	64000	ipeng -O 64000
SACK enable	On	ipeng -S on
PAWS enable	On	ipeng -P on
TCP Window Scaling enable	On	ipeng -W on
TCP Window Scale factor	2	ipeng -F 2
TCP Window Scale size	262143	For information only
TCP Rate Control	On	ipeng -R on

The following sections provide additional information on the most important **`ipeng`** settings.

TCP throughput

TCP throughput does not depend on the transfer rate itself. It depends on the product of the transfer rate and the round-trip delay (the bandwidth delay product). Standard TCP uses a 16-bit window size, which means that it can send a maximum of 64KBytes before it requires an acknowledgement from the receiver. By using window scaling, window sizes of up to 2^{30} bytes (1 GiB) are possible.

We recommend using a default window size of 64240 bytes. To set this value, use the following command:

```
ipeng -w 64240
```

When the NAS server is receiving a stream of data packets, by sending fewer than one acknowledgment per data packet received, it can increase the efficiency of its own transmit path, of the network, and also that of the client. However, when the bandwidth delay product is large (for example, over a WAN), not delaying acknowledgements can increase write throughput.

A good practice is to enable delayed acknowledgements. Use the following command:

```
ipeng -y on
```

Window scaling

A good practice is to enable window scaling on networks where the bandwidth delay product is large. This will only affect connections if the client also supports window scaling.

To enable window scaling, use the following command:

```
ipeng -W on
```

To disable window scaling, use the following command:

```
ipeng -W off
```

This feature causes an increase in buffer usage in the server. Therefore, it has a 'factor' option which enables the user to change the scale of the window size. Each increment of the scale factor doubles the window size, so the value must be as low as possible in order to maximize performance. The window size set by the scale factor appears in the **TCP Window Scale size** parameter.

To change the scale factor, use the following command:

```
ipeng -F 2
```

TCP Rate Control

This feature aims to control the transmit rate on the NAS server to match the connected switch or clients.

To turn on TCP Rate Control, use the following command:

```
ipeng -R on
```

Consult your support provider before changing any of the TCP Rate Control parameters.

Protection against wrapped sequence numbers (PAWS)

High transfer rates can threaten TCP reliability because TCP depends on the existence of a limit on the lifetime of a packet, the maximum segment lifetime (MSL). A TCP sequence number is 32 bits wide. At a high enough transfer rate, a 32-bit sequence number can wrap within the time that a packet is delayed in a queue. Protection against wrapped sequence numbers (PAWS) uses 32-bit TCP timestamps to effectively double the width of its sequence numbers.

A good practice is to enable PAWS. Use the following command:

```
ipeng -P on
```

Avoiding packet loss

Beginning transmission into a network with unknown conditions requires TCP to slowly probe the network to determine the available capacity. This avoids congesting the network with a large burst of data. The TCP slow start algorithm performs this function at the beginning of a transfer or after repairing loss detected by the re-transmission timer.

However, in the case of packet loss, the slow start algorithm can lead to poor throughput. Therefore, a good practice is to turn off the slow start option. Use the following command:

```
ipeng -s off
```

Recovering from packet loss

The NAS server has a default minimum re-transmit time-out of 300ms. When the re-transmit timer expires, TCP doubles the value of the re-transmit time-out. We recommend enabling Karn's algorithm (which determines when to reset the re-transmit time-out value) on the NAS server. This can increase read throughput.

To enable Karn's algorithm, use the following command:

```
ipeng -k on
```

Another option, SACK (Selective ACKnowledgement), is useful when there are multiple dropped segments. Without SACK, the connection has to wait for the normal retransmit timeout to expire. SACK allows the receiver to tell the transmitter which segments are missing so the sender can re-transmit only the missing segments.

However, SACK implementation increases system load, and therefore does not work well when packet loss is high. Disable SACK under these circumstances.

To disable SACK, use the following command:

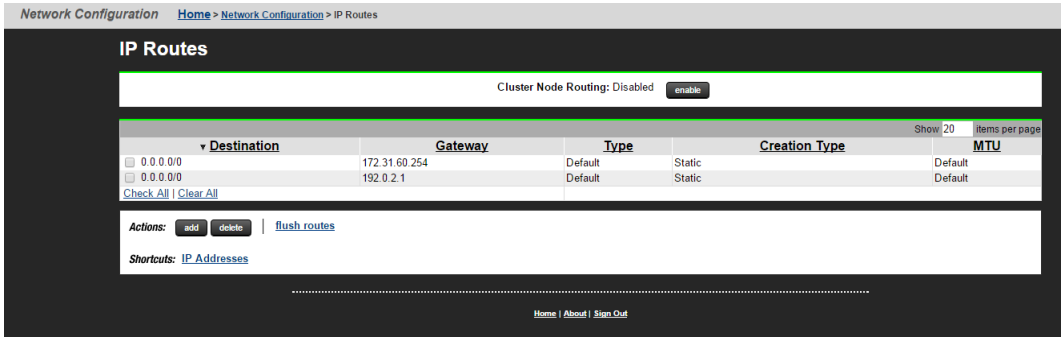
```
ipeng -S off
```

Chapter 9: Configuring routes

This section contains information on configuring default gateways, static IP routes, and dynamic IP routes.

Viewing IP routes

To view the existing IP routes, navigate to **Network Configuration > IP Routes**.



The following table describes the fields on this page:

Field / Item	Description
Cluster Node Routing	When this option is disabled (default behavior), the configured routes are propagated to all nodes in a cluster. If this option is enabled, it is possible to configure different routes for each node in a cluster. **Caution:** If an EVS fails over to a node that is missing a required route, network traffic can no longer reach the required destination. **Caution:** Clicking on the enable/disable button will result in IP routes being removed from the server. This may lead to an inability to manage the system and a loss of access to end users.
Destination	For a Network route, this field displays the IP address and Address Prefix Length of the destination. For a Host route, this field displays an IP address only.
Gateway	This field displays the gateway IP address of the route.
Type	This field displays the type of route, which can be Host, Network, or Gateway.
Creation Type	A route is either static or dynamic. Static indicates a manually created route and dynamic indicates a route created by a switch.
MTU	This is the Maximum Transmission Unit which is the largest size Ethernet frame that the server can send for the route.

Note: Fields that are not required for a route type are grayed out and cannot be configured.

Adding IP routes

To add an IP route, navigate to **Network Configuration > IP Routes** and click the **add** button.

The following table describes the fields on this page:

Field / Item	Description
Route Type	This field requires the type of route, which can be Host, Network, or Default (Gateway). Select the `Host` option to set an address for a specific computer on a different network than its usual router address. Select the `Network` option to set up a route to address all of the computers on a specific network.
Destination	For a Network route, this field requires the IP address and Address Prefix Length of the destination. For a Host route, this field requires an IP address only. Invalid addresses are: Numbers > 255, broadcast addresses, and unreachable gateways.
Gateway	This field requires the gateway IP address of the route.
MTU	This field requires the Maximum Transmission Unit which is the largest size Ethernet frame that the server can send for this route. This is an optional field. This value must lie between 68 and 9600 inclusive for IPv4 routes and between 1280 and 9600 inclusive for IPv6 routes. If the MTU is not specified, the server applies a default of 1500.

Note: Fields which are not required for a route type are grayed out and cannot be configured.

Deleting IP routes

Procedure

1. Navigate to **Network Configuration > IP Routes**.
2. Select 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**. This operation applies only to the cluster node on which the command is executed.

   To flush other dynamic routes, use the following CLI commands:

   - **`irdp flush`**
   - **`ndp-flush`**
   - **`rip flush`**

   See the CLI Reference for further information.

Chapter 10: Managing networks and devices

This section contains information on configuring non-file system interfaces and managing system devices using the NAS Manager.

Configuring non-file serving interfaces

Configure the IP address of the eth1 interface with an external NAS Manager. For NAS modules, configuration is set using the maintenance utility rather than NAS Manager.

Procedure

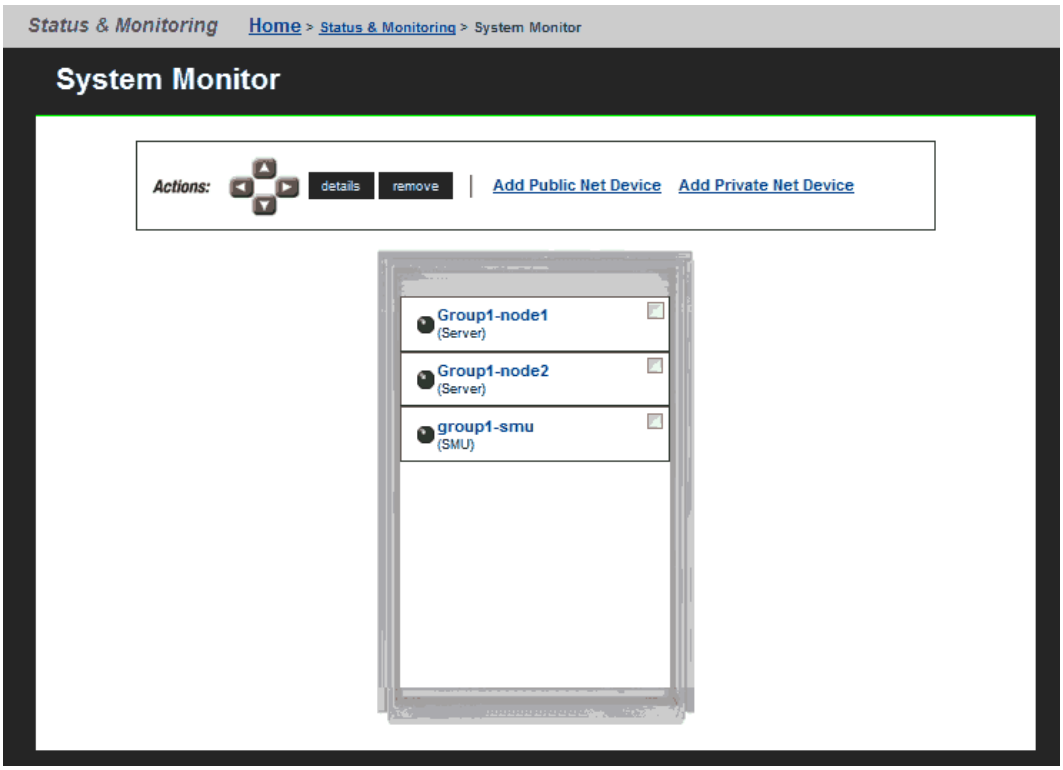
1. Navigate to **Home > SMU Administration > SMU Network Configuration** to display the SMU Network Configuration page.
2. Enter the requested information. The SMU Network Configuration page enables the Administrator to configure the IP address of the eth1 interface. The default address for the eth1 interface is 192.0.2.1. The eth1 address must end with . 1, to simplify the management relationship of the SMU with secondary devices. The mask is fixed to 255.255.255.0. For information only, click on the **Private network device ports** link to view details about the interfaces that the server uses for internal communication.
3. Record the IP address settings separately for future reference, and click apply.

Configuring devices on the system monitor

The system monitor allows you to display and monitor the devices that make up your storage system. For NAS modules, an external NAS Manager can be configured to display status of applicable devices.

Procedure

1. Navigate to **Home** > **System Monitor** to display the **System Monitor** page:



2. Optionally, change the position of any component by selecting its check box and using the arrows in the Action section.
3. Optionally, display the status or details for any component.
   The following table lists basic NAS server components and indicates what happens when you click a component name in the component list:

Component/Description	Clicking the component	Clicking the details button
Storage Server 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.	Loads the **Server Status** page.	
Main Enclosure Contains dual power supplies, and dual RAID drive controllers. Depending on the model, the main enclosure may contain disk drives.	Loads the **Enclosure Status** page.	Loads the **System Drives** page.

Component/Description	Clicking the component	Clicking the details button
Expansion Enclosure Expansion enclosures contain disk drives and power supplies, but do not contain any RAID controllers.	Loads the **Enclosure Status** page.	Loads the **System Drives** page.
NAS Manager The internal or embedded NAS Manager application.	Loads the NAS Manager page.	
System Power Unit This component is also known as an uninterruptible power supply (UPS).	Loads the **UPS Status** page.	Loads the **UPS Configuration** page.
NDMP Backup Devices 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.	Loads the **NDMP Devices** page.	Loads the **NDMP Details** page for the device if the device can be contacted, or loads the **NDMP Device List** page if the device cannot be contacted.
FC Switches (HNAS server only) FC switches (and cables) connect FC devices, generally storage arrays, to the server(s). **Note:** Upon adding an FC switch through the FC Switches page, it is automatically added to the System Monitor.	Loads either the embedded management utility for the switch, or the **FC Switch Details** page for the switch, depending on the protocol specified when the switch was added. For more information, see the *Server and Cluster Administration Guide*).	Loads the **FC Switch Details** page.

Component/Description	Clicking the component	Clicking the details button
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.	Loads the embedded management utility for the device.	Loads either the **Add Public Net Device** or the **Add Private Net Device** page. Settings for the component can be changed from this page.

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 private (management) network.

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

   After a device is added to the System Monitor:
   - Clicking its name opens its embedded management utility in the Web browser, using either HTTP, HTTPS, or Telnet.
   - The NAS Manager 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 NAS Manager issues an alert (devices can also be configured to send SNMP traps to the NAS Manager).
   - Events from the device are added to the event log if the NAS Manager has a MIB for the device.

Chapter 11: Troubleshooting

This section contains information on checking the network status of the NAS server and also how to detect any potential issues.

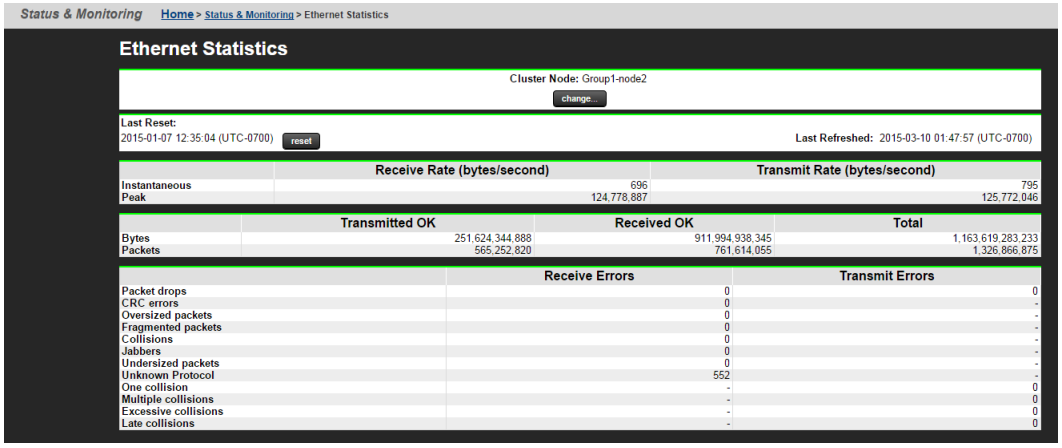
Network health information

The NAS server provides information on the current network health status through the NAS Manager.

Ethernet Statistics

To access this page, navigate to **Network Configuration > Ethernet Statistics**.

This page displays information on transmit and receive rates as well as throughput, error and collision information as shown below:



There are two additional Ethernet statistics pages:

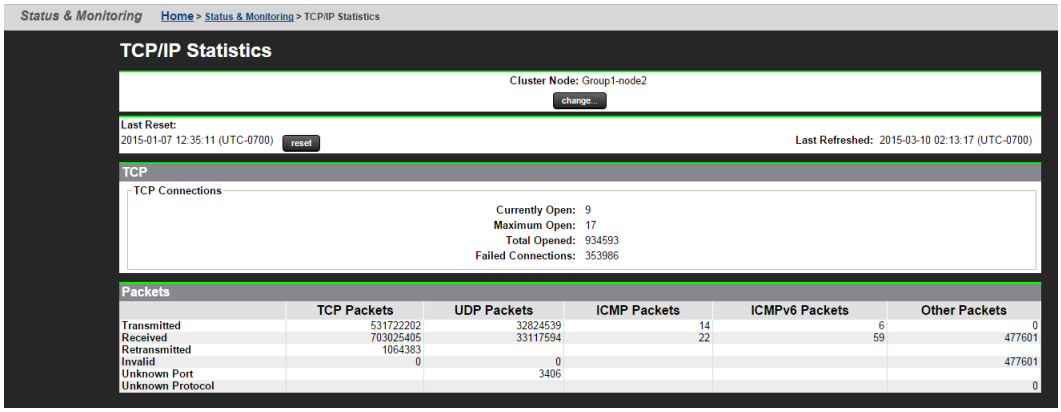
- **Ethernet Statistics (per port) - Aggregation ports -** this page contains network information on a per aggregation basis, for example, ag1, ag2...
- **Ethernet Statistics (per port) - Physical ports** - this page contains network information on a per physical port basis, for example, tg1, tg2...

Navigate to the **Network Configuration > Ethernet Statistics (per port)** page in order to view the Aggregation ports page. On this page, there is a link to the **Ethernet statistics (per port) - Physical ports** page.

TCP/IP Statistics

To access this page, navigate to **Network Configuration > TCP/IP Statistics**.

This page displays information on connections, segments, UDP, ICMP and TCP as shown below:



There are two additional TCP/IP statistics pages:

- **TCP/IP Statistics (per port) - Aggregation ports -** this page contains network information on a per aggregation basis, for example, ag1, ag2...
- **TCP/IP Statistics (per port) - Physical ports** - this page contains network information on a per physical port basis, for example, tg1, tg2...

Navigate to the **Network Configuration > TCP/IP Statistics (per port)** page to view the Aggregation ports page. On this page, there is a link to the **TCP/IP statistics (per port) - Physical ports** page.

Additional commands

The NAS server also provides the following CLI commands which display information on the current network health status:

- **`agg`** - this command lists any existing aggregations
- **`ethernetstats`** - this command displays statistics for each Ethernet interface
- **`tcpstats`** - this command displays statistics for TCP protocol packets
- **`udpstats`** - this command displays statistics for UDP protocol packets
- **`ip-stats-other`** - this command displays statistics for all other IP protocol packets
- **`icmpstats`** - this command displays statistics for ICMP protocol packets
- **`icmpv6stats`** - this command displays statistics for ICMP v6 protocol packets
- **`arp`** - this command displays the IP to MAC address mappings
- **`ndp-dump`** - this command displays the IPv6 to MAC address mappings and also displays any on-link prefixes and discovered routers

Detecting network issues

The server contains an automatic diagnosis system which identifies, categorizes, and prioritizes problems and then presents the information to the user through the console.

To activate the diagnosis system, use the **trouble** command.

This command contains 'groups' which refer to parts of the server and its storage. For example, there is a Network group and a Storage group. Trouble also contains 'reporters'. These are individual programs that investigate issues within the groups.

For example, the Network group contains the following reporters:

```
CLUSTER-2:$ trouble --list-reporters network
Group   Reporter           Pri Brd Subject of warnings
-----   --------           --- --- -------------------
network aggregation        170 MMB Aggregation status
network network-statistics 180 MMB Network interface statistics
network nim-vlsi           190 MMB NIM VLSIsettings
network network-interfaces 200 MMBNetwork interfaces link status
network remote-nfs         270 MMB RemoteNFS
network nisclient          280 MMB Nisclient status
network wins               290 MMB UnreachableWINS servers
network ip-eng-adv         300 MMB ipeng/ipadv status
network mac-cluster        340 MMB MAC_10status
network mac-network        340 MMB MAC_1status
network external-migration-protocol-errors 350 MMB External migration protocol errors
network packet-capture     380 MMB Checks that packet-capture is not running
network remote-http        400 MMB Remote HTTP
```

There are two types of reporters:

- Fault reporters - these detect issues that can cause degradation of service.
- Performance reporters - these detect performance values which are out-of-range (unexpectedly high or low).

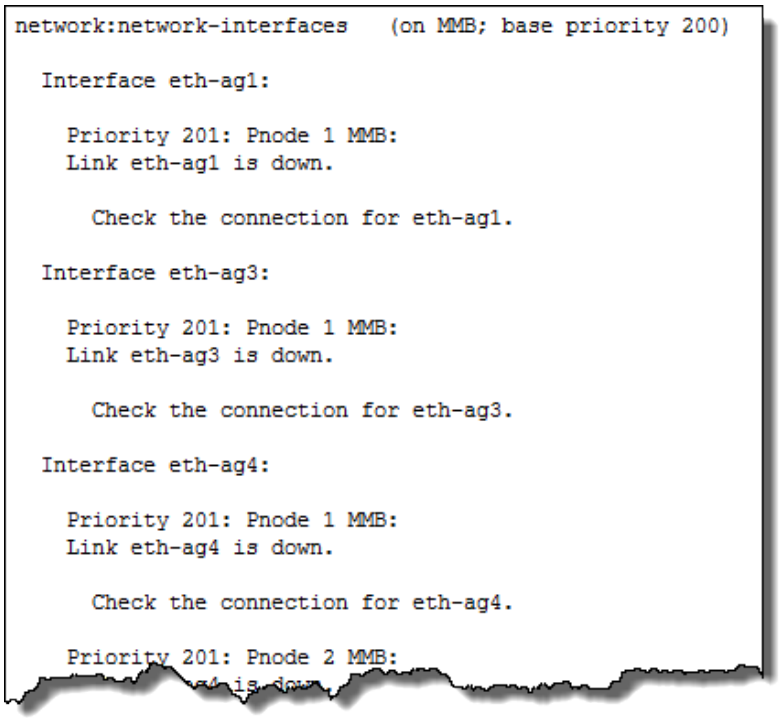
This command operates over all cluster nodes unless configured otherwise.

Example of common command usage

The following command reports all issues with the network group.

trouble network

The report appears as shown in the example below:



Collecting network packets

It is possible to perform a complete capture of network packets on a NAS server using the **`packet-capture`** command. This is useful when the server is experiencing protocol errors.

Once started, this command collects all header and content packets from the NAS server and stores them in a file in NAS memory. This file is named `tmp` and it can grow to a maximum size of 32MB or 15000 frames (whichever is reached first).

To retrieve this file, use the **`nail`** command to email it to a user. Alternatively, use the **`ssget`** command to send it to the NAS Manager for later collection. The **`ssget`** command works from an ssc connection and, therefore, is usable locally or on a server connected to an external SMU.

The file format is .pcap. To analyze the contents the following filter applications are supported:

- **`tcpdump`**
- **`tshark`**
- **`wireshark`**

The **`packet-capture`** command also supports aggregations as shown in the example below:

```
packet-capture --start ag1
```

Caution: Server performance is severely degraded during packet capture. It is recommended to use port mirroring on the upstream switch instead of using the packet capture command on the NAS server.

Appendix A: VLAN conversion

Previously, VLANs were configured by defining an association between a VLAN ID and a subnet (using a network address and a subnet mask). It is no longer possible to create subnet VLANS. This topic describes how to convert subnet-VLANs to use VLAN interfaces. Seek guidance from your support provider before attempting the conversion procedure.

The subnet VLANs are maintained by the **`vlan`** command. This command enables the NAS server to display and remove existing subnet VLANs. However, a script is also available to convert legacy subnet-based VLANs to the new static VLANs. The following procedure describes how to run the script and convert the VLANs.

The procedure has three stages:

- Accessing the NAS Linux console
- Retrieving and running the script
- Converting a subnet VLAN

Accessing the NAS Linux console

The script does not run under the NAS CLI but is available on the NAS platform (from version 12.2), through the Linux console.

To access the NAS Linux console:

1. SSH to the SMU IP address
2. Enter `q` to drop to the operating system prompt of the SMU
3. Enter `ssh manager@<cluster node ip>`
4. Enter the password.
5. Enter `exit`
6. Enter `su`
7. Enter the password.

Retrieving and running the script

On the NAS Linux console, the script is located at: `/opt/mercury-utils/bin/vlan-convert-config.rb`.

To obtain the script (from a NAS server named *xyz*) and copy it onto a local Linux client, enter the following command:

```
# 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
#
```

Either on the NAS Linux console or a local Linux client, run the script with the following parameters:

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

Where:

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

Note: If the user option is supplied without a corresponding password, the script prompts for the password without displaying the entered text.

On the NAS Linux console only

When executing the script on the NAS Linux console, the name localhost can be used to identify the NAS server. In this case it is normally not necessary to supply the username and password.

For example:

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

Converting a subnet VLAN

The script outputs the commands to run in order to perform the conversion. Review these changes before applying them to the system by running the following command:

```
cat /tmp/vlan-conv-commands
```

Apply the generated commands to the NAS by running the following command:

```
source /tmp/vlan-conv-commands
```

Keep a copy of the script output for reference in case a downgrade to a version of firmware below 12.0 is required, as this information is necessary in order to convert back.

Example VLAN conversion

This example demonstrates how to convert subnet-VLANs to use VLAN interfaces. A sample command and the **`vlan-conv`** commands generated by the script are shown below.

Enter a command as shown in the example below:

```
manager@hnas(bash):/opt/mercury-utils/bin$ ./vlan-convert-config.rb
localhost > /tmp/vlan-conv-commands
manager@hnas(bash):/opt/mercury-utils/bin$ cat /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 ...
# Disable EVS 1:HNAS-G3
evs disable -e 1 --confirm

# Remove all addresses in VLANs from still enabled EVS before updating the
configuration.
# This applies to EVS with non-VLAN address assignments in order to
minimise disruption to non-VLAN services.
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
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
```

```
SSC-EOS
```

After reviewing the **vlan-conv** commands, execute the generated file on the NAS server.

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

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 ...
hnas:$ sleep 5
hnas:$
hnas:$ # Reconfigure IP addresses on VLANs.
hnas:$ # Move address to VLAN interface.
hnas:$ evsipaddr -e 1 --update --confirm --ip 172.31.62.62/24 --
port ag1-vlan0200
hnas:$ # Restore previously removed address to VLAN interface.
hnas:$ evsipaddr -e 2 --add --ip 172.31.61.61/24 --port ag1-vlan0100
hnas:$
hnas:$ # Enable any EVS that were previously disabled.
hnas:$ echo Enabling the EVS that were previously disabled ...
Enabling the EVS that were previously disabled ...
```

```
hnas:$ evs enable -e 1
hnas:$ manager@hnas(bash):/tmp$
```

Appendix B: Network ports

This section contains information about the default ports in use for services on a NAS server and on an external SMU.

NAS (listening ports)

Port	Protocol		IP address type
21	FTP	TCP	EVS
22	SSH	TCP	Management *
25	SMTP relay (HNAS server only)	TCP	Management *
80	HTTP (NAS Manager on HNAS server, maintenance utility on NAS module)	TCP	Management *
111	Port mapper	TCP/UDP	EVS
135	DCERPC endpoint info	TCP	EVS
137	NetBIOS name lookup service, including WINS	UDP	EVS
138	SMB (CIFS) over NetBIOS	UDP	EVS
139	SMB (CIFS) over NetBIOS	TCP	EVS
161	SNMP agent	UDP	Management *
202	VSS	TCP	Management * (EVS only on NAS module)
206	SSC	TCP	Management *
443	HTTPS (NAS Manager on HNAS server, maintenance utility on NAS module)	TCP	Management *
445	SMB over TCP	TCP	EVS
762	rquota	TCP/UDP	EVS
800	RPC	TCP/UDP	EVS
2049	NFS	TCP/UDP	EVS
3205	iSNS	TCP	EVS
3260	iSCSI	TCP	EVS
4045	lockd	TCP/UDP	EVS
4048	mountd	TCP/UDP	EVS
4050	statd	TCP/UDP	EVS
8080	SOAP API (HTTP)	TCP	Management *
8443	SOAP API (HTTPS)	TCP	Management *

8444	REST API (HTTPS)	TCP	Management *
10000	NDMP control	TCP	EVS
10001, or configurable range	NDMP data port	TCP	EVS
11106	Statistics server	TCP	Management *
20080	HTTP (NAS Manager on NAS module only)	TCP	Management *
20443	HTTPS (NAS Manager on NAS module only)	TCP	Management *
34741	VAAI	TCP/UDP	EVS
59516	Quorum device communication (HNAS server only)	UDP	Cluster node
59535-59536	Cluster communication	UDP	Cluster node
59550	Object replication	TCP	EVS

Note: The NFS v2/v3 protocol family supports dynamic ports via the portmap protocol. Our implementation of it uses static ports, configurable with `rpcport` , defaulting to the numbers below for lockd, mountd, NFS, rquota and statd.

***** On an HNAS server, the **management IP address** refers to the admin service node and cluster node IP addresses. On a NAS module, it refers to the NAS module management IP address.

NAS as a client

The NAS server uses these destination ports on a peer server.

Port	Protocol	
25	SMTP	TCP
53	DNS	TCP/UDP
80,443	Data Migrator to Cloud	TCP
88	Kerberos	TCP/UDP
123	NTP	UDP
139	SMB (CIFS) over NetBIOS	TCP
162	SNMP traps	UDP
389	LDAP	TCP/UDP
445	SMB over TCP	TCP
464	Kerberos Password Change (kpasswd)	TCP/UDP
636	LDAP over TLS	TCP/UDP
1344	ICAP AV	TCP
2049	NFS	TCP/UDP
4048	mountd	TCP/UDP
59550	Object replication	TCP
Set by the peer server	NDMP data port	TCP

External SMU (listening ports)

Port	Protocol		IP address type
22	SSH	TCP	Management *
25	SMTP relay (Only in SMU gateway mode)	TCP	Management *
80	HTTP GUI	TCP	Management *
123	NTP	UDP	Management *
162	SNMP trap receiver	UDP	Management *
443	HTTPS GUI	TCP	Management *
59515-59536	Quorum device (HNAS server only)	UDP	Cluster node

***** On an HNAS server, the **management IP address** refers to the admin service node and cluster node IP addresses. On a NAS module, it refers to the NAS module management IP address.

External SMU as a client

The external SMU uses these destination ports on a peer server.

Port	Protocol	
25	SMTP relay	TCP
123	NTP	UDP
443	HTTPS Standby SMU Backups	TCP
8443	SOAP requests to NAS	TCP
11106	Statistics server	TCP
2001	HCS device manager updates	TCP

Hitachi

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact