

**Hitachi NAS Platform, powered by  
BlueArc®**

**Network Administration Guide**

## 対象製品

Hitachi NAS Platform 10.2

## 輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

なお、ご不明な場合は、弊社担当営業にお問い合わせください。

## 商標類

Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

## 発行

2013 年 8 月（第 1 版）K6603829

## 著作権

All Rights Reserved. Copyright (C) 2013, Hitachi, Ltd.

# 目次

はじめに.....	5
表記.....	6
関連資料.....	6
<b>1. ネットワークインターフェース.....</b>	<b>7</b>
1.1 概要.....	8
1.2 ネットワークインターフェース.....	8
1.3 IP アドレッシング.....	9
1.3.1 VLAN サポート.....	9
1.3.2 ジャンボフレームサポート.....	10
1.4 Gigabit Ethernet データインターフェースを構成する.....	10
1.4.1 リンク集約.....	11
(1) リンク集約ステータスを表示する.....	11
(2) 集約の構成を表示または変更する.....	11
(3) 集約を追加する.....	13
(4) 集約を削除する.....	15
1.4.2 IP アドレッシング.....	16
(1) 既存の IP アドレスを表示する.....	16
(2) IP アドレスを追加する.....	17
(3) IP アドレスを削除する.....	17
(4) IP ネットワークの拡張設定を変更する.....	19
<b>2. IP ルーティング.....</b>	<b>23</b>
2.1 IP ルーティング.....	24
2.1.1 デフォルトゲートウェイ.....	24
2.1.2 静的ルート.....	24
2.1.3 動的ルート.....	25
2.1.4 HNAS のルーティングテーブルを管理する.....	25
<b>3. ネームサービス.....</b>	<b>29</b>
3.1 ネームサービスの概要.....	30
3.1.1 DNS 及び DDNS.....	30
(1) CIFS 名を登録する.....	30
(2) セキュアな DDNS 更新.....	30
3.1.2 WINS.....	30
3.2 ネームサービスを構成する.....	31
3.2.1 ネームサービスの指定と優先順位付け.....	31

4. ディレクトリサービス.....	35
4.1 ディレクトリサービスの概要.....	36
4.1.1 NIS (NFS 用) .....	36
4.1.2 LDAP.....	36
4.2 ディレクトリサービスを構成する.....	37
4.2.1 NIS 及び LDAP サービスの有効化と構成.....	37
4.2.2 NIS を有効/無効にする.....	37
4.2.3 NIS 構成を表示する.....	38
4.2.4 NIS サーバを追加する.....	40
4.2.5 NIS 構成を変更する.....	40
4.2.6 構成済み NIS サーバの優先順位を変更する.....	41
4.2.7 NIS サービスを提供するように LDAP を構成する.....	42
4.2.8 LDAP サーバを追加する.....	43
4.2.9 LDAP 構成を変更する.....	44
4.2.10 LDAP サーバを変更する.....	45
4.2.11 ネームサービスの順序を変更する.....	45
5. 内部 LAN.....	47
5.1 内部 LAN の構成.....	48
5.1.1 System Monitor 上のデバイスを構成する.....	49



# はじめに




- 表記
- 関連資料

# 表記

このマニュアルでは下記の表記を使用しています。

用語	意味
LITERAL	コマンド、ファイル、ルーチン、パス名、シグナル、メッセージ、及びプログラム言語構成などの文字情報を固定スペースフォントで表します。
<i>Replaceable</i>	変数や定義など可変値をイタリック文字で表します。またマニュアル名もイタリック文字で表します。
[と]	コマンドや指示文の任意入力値を括弧内に示します。
...	前述の要素が繰り返し可能なことを表します。
GUI 要素	ウィンドウ、スクリーン、ダイアログボックス、メニュー、ツールバー、アイコン、ボタン、ボックス、フィールド、及びリストなど GUI 要素名を示します。

このマニュアルでは下記の表記を使用しています。このマニュアルを読み進む前に、下記のアイコンとそれらの意味を確認してください。

アイコン	意味	説明
	参考(tip)	タスクを完了するのに役立つ補足情報を示します。
	重要(note)	システムのインストールや運用を効率よく行う上で有用な情報を示します。
	注意(Caution)	データや機器に破損の恐れがある場合に注意を促します。要求条件を理解するまで決して次のステップへ進まないでください。

## 関連資料

- *System Access Guide*  
システム管理者が Web Manager (GUI) や Command Line Interface (CLI) でシステムにアクセスする手順と、システム管理者向けの参考資料などを提供します。(PDF)
- *G2 Hardware Reference*  
Hitachi NAS Platform<sup>TM</sup>, powered by BlueArc<sup>®</sup> ハードウェアの概要と、問題の解決方法、障害コンポーネントの交換方法について説明します。(PDF)
- *CLI Reference*  
コマンドをコマンドプロンプトで入力してシステムを管理する方法について説明します。(HTML)
- *Release Notes*  
システムソフトウェアの最新情報と、製品添付情報への訂正及び追加情報を提供します。

# ネットワークインターフェース

- 1.1 概要
- 1.2 ネットワークインターフェース
- 1.3 IP アドレッシング
- 1.4 Gigabit Ethernet データインターフェースを構成する

# 1.1 概要

HNAS システムのネットワーキングの概念と手順を以下のセクションで説明します。

- IP ルーティング  
静的ルート、デフォルトゲートウェイ、動的ルートの他、ルーティングの優先順序についても簡単に説明します。
- ネットワークインターフェースの概要  
ジャンボフレームの使用方法、データ LAN および管理 LAN の IP アドレス設定、クラスタリング、VLAN サポート。
- ネームサービス  
DNS, NIS, WINS, LDAP など。

# 1.2 ネットワークインターフェース

各ノードは、Gigabit Ethernet (GbE) ポートと 10 Gbps Ethernet (10 GbE) ポートのいずれかと、10/100 Ethernet ポートを備えています。

- 最大六つの GbE ポート  
銅ケーブルと RJ45 コネクタをサポートします。  
これらのポートはジャンボフレームをサポートし、個別に構成するか、IEEE 802.3ad リンク集約を使用してトランキング構成でき、データ LAN への高性能なアクセスを提供します。
- 二つの 10GbE ポート  
ファイバーケーブル用の XFP (10 Gigabit Small Form-factor Pluggable) をサポートします。  
これらのポートはジャンボフレームをサポートし、個別に構成するか、IEEE 802.3ad リンク集約を使用してトランキング構成でき、データ LAN への非常に高性能なアクセスを提供します。
- 10/100Ethernet ポート  
標準の RJ-45 コネクタを使用し、HNAS の内部 LAN に接続するために使用されます。

ネットワーククライアントは、逆ルーティングまたはリンク集約として構成された Gigabit Ethernet (GbE) データインターフェースまたは 10 Gbps Ethernet (10GbE) インターフェースを使用して、HNAS にアクセスします。

- 逆ルーティングでは、管理者は各ポートを、IP サブネットをサポートするように構成して、最大六つの個別の IP サブネットへの HNAS の物理的な接続をサポートします。
- リンク集約 (またはトランキング) では、管理者は複数の GbE ポートまたは 10GbE ポートを一つの集約に構成し、それが一つの EVS または複数の EVS に割り当てられます。



**重要** 集約内の全てのポートが同じタイプ/速度でなければなりません (全て GbE ポートまたは全て 10GbE ポート)。

集約は一つの MAC アドレスと、少なくとも一つの IP アドレスを持ちます。集約は、その集約を使用する各 EVS の IP アドレスを必要とします。すなわち、集約が複数の EVS に割り当てられる場合には、集約は複数の IP アドレスを持ちます。一つの集約内の全てのポートが同じタイプ/速度である限り、物理ポートを任意の組み合わせで集約できます。HNAS は、初期には、GbE ポート 1 を含む一つのポート集約で構成されています。

リンク集約は、接続ごとのネットワークインターフェース帯域幅を増加させます。また、リンク集約は、ネットワークインフラストラクチャーの障害から HNAS を保護します。例えば、集約内のいくつかのリンクに障害が発生しても、集約内の他のリンクがトラフィックを引き継ぎます。



HNAS は Link Aggregation Control Protocol (LACP) をサポートします。これは、LACP をサポートするスイッチに HNAS が接続されたときに、リンク集約設定を自動的に構成します。

システムは、同じ HNAS に逆ルーティングとリンク集約が同時に存在する混在環境をサポートします。

## 1.3 IP アドレッシング

HNAS は、データ LAN、内部 LAN、及びクラスタリングの IP アドレス要件を区別します。

- ファイルサービス (データ LAN)  
ネットワーククライアントは、HNAS のファイルサービスにサービス IP アドレス経由でアクセスします。これは、HNAS の GbE ポート経由でのみアクセスできます。複数の IP アドレスをファイルサービスに割り当てることができます (これらの IP アドレスは同じネットワークにあって、別のネットワークにあってはかまいませんが、一意であることが必要です)。
- 管理サービス (内部 LAN)  
これらの IP アドレスは、Web Manager によって、または HNAS の組み込み管理インターフェースを使用して HNAS を管理するときに使用されます。HNAS は、10/100Ethernet ポートに割り当てられる、少なくとも一つの IP アドレスを必要とします。追加の管理 IP アドレスを GbE ポートに割り当てて、SSC を使用して、ネットワークポート経由で管理機能を直接実行できます。



**重要** 内部 LAN の管理サービス IP アドレスを構成するときには、IP アドレスのサブネットマスクが SMU の内部 LAN (*eth1* ポート) のサブネットマスクと一致することを確認してください (255.255.255.0 など)。また、内部 LAN の範囲内の IP アドレスを選んでください (192.0.2.2~254 など)。これは、HNAS を SMU 上の Managed Server として構成するとき使用される管理サービス IP アドレスになります。

- クラスタリング  
クラスタとして構成するときには、各ノードに、内部 LAN に接続する 10/100 管理ポートの一意な IP アドレスが必要です。これらの一意なアドレスによって、クラスタノードは相互に通信できる他、Quorum Device (QD) とも通信できます。

### 1.3.1 VLAN サポート

VLAN (仮想 LAN) は、デバイスの物理的位置や物理的に接続されているネットワークに関係なく、一連のデバイスを一つの専用ネットワーク上で動作しているように見せます。これらのデバイスは、物理的接続に関係なく、個別の論理ネットワーク (物理ネットワーク内の論理ネットワーク) を形成し、その VLAN のノード宛てでない全てのトラフィックを無視します。

VLAN をサポートするには、VLAN ネットワークに参加するデバイスをリンクする各スイッチを、VLAN トラフィックを正しくサポートするように構成し、VLAN トラフィックをネットワーク上の他のトラフィックから切り離す (切り離しておく) ように構成する必要があります。非常に複雑な構成にすることができ、例えば、専用の物理サブネットを VLAN の一部にしたり、そのサブネットを処理するスイッチに受信トラフィックの VLAN タグを削除させ、送信トラフィックに VLAN タグを追加させたりすることができます。

VLAN 構成は複雑になりがちなので、このセクションでは、HNAS による VLAN タギングのサポートについてのみ説明します。

HNAS は、データ LAN インターフェース (GbE 及び 10GbE ポート) の VLAN タギングをサポートします。HNAS の VLAN サポートは、802.1Q 標準と互換性がありますが、次のような例外があります。

- 優先順位をマークするために 802.1Q を使用します。
- トークンリングを設定します (受信時には無視され、送信時にはクリアされます)。

- HNAS はスタック VLAN (連続する VLAN タグ) をサポートしません。

HNAS の VLAN 実装では、VLAN が一つの仮想ネットワークに対応することを前提としています。結果として、各 IP サブネットは一つの VLAN 内にのみ属することができます。ただし、一つの VLAN 内に複数の IP サブネットを構成することができます。VLAN はオプションであり、VLAN タグはデフォルトでは追加されません。

VLAN を構成するには、各ソースサブネットの VLAN 識別子 (ID) を追加し、ノード上で `vlan` コマンドを使用して、特定のサブネットに VLAN タグを関連付けます。現在の VLAN 設定を表示するためにも、同じコマンドが使用されます。

HNAS が VLAN タグを使用するように構成されている場合、

- VLAN 内のサブネットに属するポートから送信されるトラフィックにタグが付けられます。すなわち、VLAN タグ (サブネット ID) が送信データフレームのヘッダーに追加されます。全ての送信パケットに、ソースデバイスが属するサブネットの VLAN タグ (ID) が付けられます。
- HNAS が受信する全てのトラフィックが評価されます。VLAN タグを含まない場合、または VLAN タグが HNAS に関連付けられているサブネット ID の一つと一致しなかった場合、パケット (データフレーム) は無視されます。

### 1.3.2 ジャンボフレームサポート

HNAS の全ての GbE インターフェースは、イーサネット標準の 1,518 バイトより大きなイーサネットフレームを送信できるジャンボフレームをサポートします。大量転送に必要なフレーム数を減らすことにより、ジャンボフレームは転送速度を高めまます。ジャンボフレームは、イーサネットネットワーク上で標準フレームと共存します。

全ての GbE インターフェースは、無条件でジャンボフレームを受信し、構成の変更は不要です。GbE インターフェースは、1,519~9,000 バイトの MTU サイズを指定することによって、ジャンボフレームを送信するように構成できます。ジャンボフレーム送信を構成するには、「[1.4.2 \(4\) IP ネットワークの拡張設定を変更する](#)」を参照して、次の設定を構成します。

- IP MTU for Off-Subnet Transmits (bytes)
- TCP MTU
- Other Protocol MTU



**注意** ジャンボフレーム拡張のないネットワーク機器は、ジャンボフレームを破棄して、オーバーサイズパケットエラーを記録することがあります。ジャンボフレーム送信を構成する前に、ルート上 (と各終端) の全てのネットワーク機器がジャンボフレームをサポートすることを確認してください。ジャンボフレームを有効にし、サブネット上のネットワーク機器またはクライアントがジャンボフレームをサポートしない場合、HNAS との通信が失われることがあります。

ジャンボフレームを使用した IP データ送信の成功は、宛先 IP アドレスまたはサブネットワークに依存します。宛先 IP アドレスまたはサブネットワークの最大 MTU サイズは、IP ルーティングテーブルの属性として構成されます。

## 1.4 Gigabit Ethernet データインターフェースを構成する

GbE (Gigabit Ethernet) と 10GbE (10 Gigabit Ethernet) ポート構成には、次のコンポーネントのセットアップが必要です。

1. リンク集約
2. IP アドレッシング

HNAS によって提供されるファイル及びブロックサービスのための IP 拡張設定とルーティングテーブル設定。

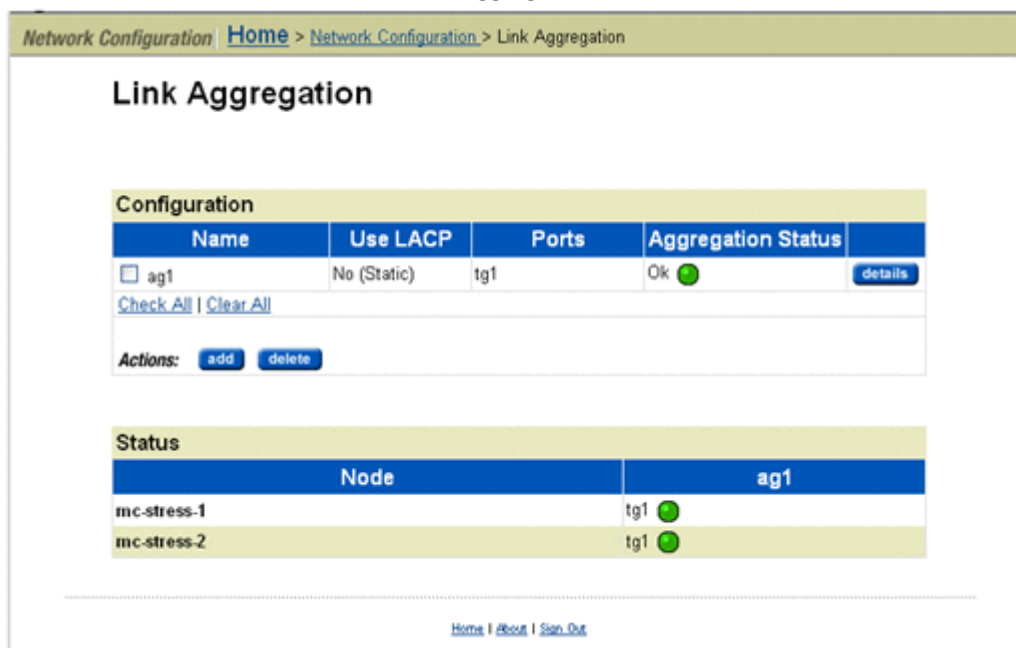
## 1.4.1 リンク集約

### (1) リンク集約ステータスを表示する

リンク集約は、複数の GbE または 10GbE ポートを一つの論理リンクにして、帯域幅を増加させます。集約によって、GbE または 10GbE ポートを使用したノードとリモートデバイス間の通信チャンネルの容量と可用性を高めることができます。

集約では、二つ以上のリンク（GbE または 10GbE）ポートがグループ化されて一つの論理ユニットを形成し、対応帯域幅を増やし、耐障害性のある冗長リンクを作成します。集約はロードバランシングも提供し、処理及び通信アクティビティがトランク内の複数のリンクに分散されるため、一つのリンクに負荷が集中することがありません。集約は、リンクの可用性を高め、リンク容量を増加させます。

集約のステータスを表示するには、[Link Aggregation] 画面に移動します。



下の表では、この画面のフィールドについて説明します。

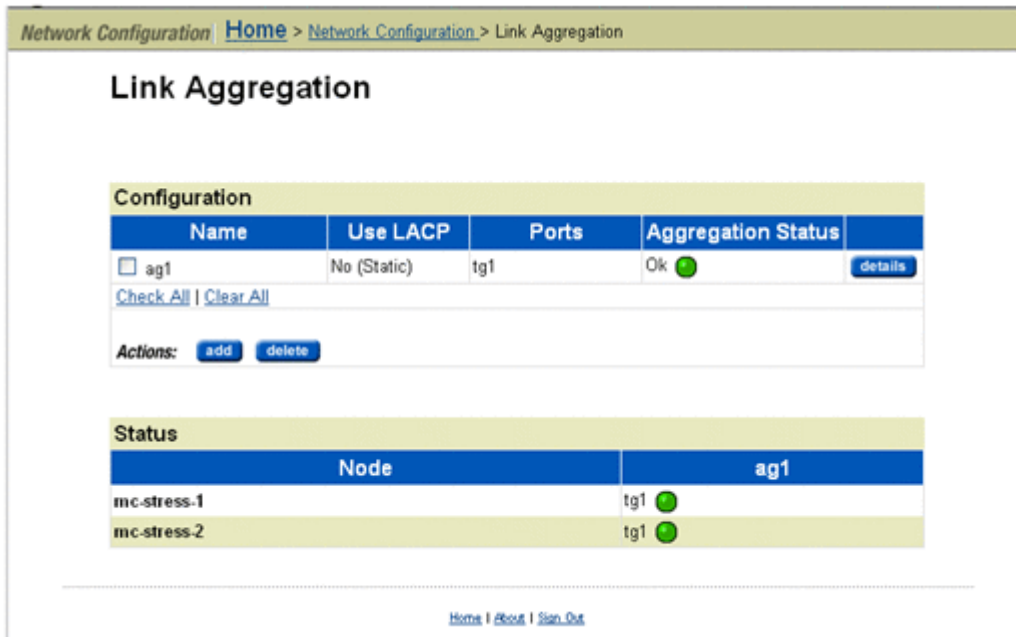
項目/フィールド	説明
Name	集約の名前（ag1, ag2, ag3, ag4, ag5, ag6）です。
Use LACP	集約が LACP を使用するかどうかを示します。集約が LACP を使用しない場合、集約は静的です。集約が LACP を使用する場合、集約は動的です。
Ports	集約で使用されるポートのリスト。「gex」という名前のポートは Gigabit Ethernet ポートであり、「tgx」という名前のポートは 10GbE（10 Gigabit Ethernet）ポートです。
Status	集約のステータスです。
Node	各ノードについて、構成された各集約の現在のステータスが表示されます。

### (2) 集約の構成を表示または変更する

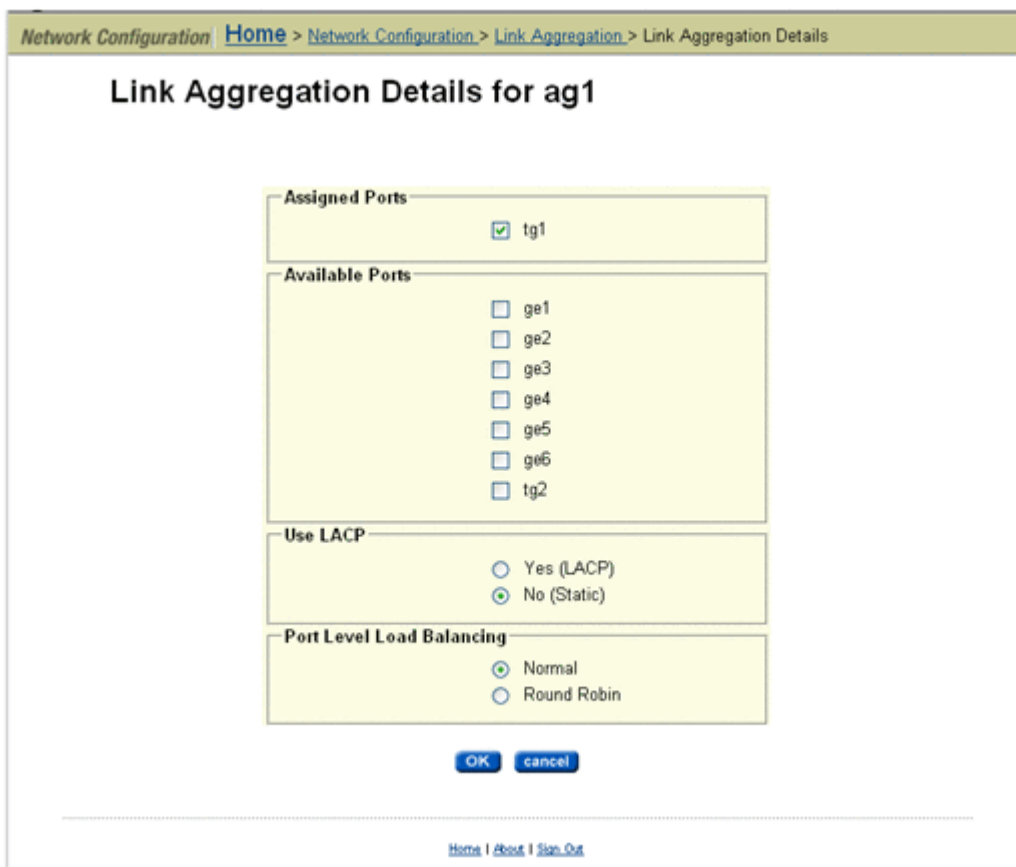
集約の構成を表示または変更するには

1. [Link Aggregation] 画面に移動します。

[Network Configuration] 画面で [Link Aggregation] を選択して、[Link Aggregation] 画面を表示します。現在構成済みの全ての集約が一覧表示されます。



2. 構成を表示または変更する集約を選択します。  
 集約の構成を表示または変更するには、[details] をクリックして、集約の [Link Aggregation Details] 画面を表示します。



次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
Assigned Ports	この集約に現在割り当てられているポートを一覧表示します。「gex」という名前のポートは Gigabit Ethernet ポートであり、「tgx」という名前のポートは 10GbE (10

項目／フィールド	説明
	Gigabit Ethernet) ポートです。集約からポートを削除するには、削除するポート名の横にあるチェックボックスをオフにします。
Available Ports	集約に追加できる GbE (Gigabit Ethernet) 及び tg (10GbE) ポート。「gex」という名前のポートは Gigabit Ethernet ポートであり、「tgx」という名前のポートは 10GbE (10 Gigabit Ethernet) ポートです。集約にポートを追加するには、追加するポート名の横にあるチェックボックスをオンにします。
Use LACP	この集約が LACP を使用するかどうかを指定します。LACP を使用しない集約は静的集約と呼ばれ、LACP を使用する集約は動的集約と呼ばれます。
Port level Load Balancing	<p>集約内の全てのポートで使用されるポートのロードバランシング方式を表示します。</p> <ul style="list-style-type: none"> <li>• [Normal] は、HNAS が、一つの「会話」のための全てのトラフィックを適切な集約内の物理ポートの一つを経由してルーティングすることを意味します。HNAS のハッシュ関数とルーティング関数によって、どのパケットが集約のどの物理ポートを使用するかが決まります。例えば、特定の TCP 接続の全てのトラフィックは常に同じ物理ポートを経由してルーティングされます (リンクがドロップしない限り)。</li> <li>• [Round Robin] は、トラフィックを形成するパケットが各ポートを順に使用してルーティングされることを意味します。例えば、最初のパケットは最初のポートに送られ、2 番目のパケットは次のポートに送られるというようにして、全てのポートが使用されます。その後、トラフィックは再び最初のポートに送られます。このルーティング方式では、全てのポートがほぼ等しく使用されるので、リンクのスループットが最大化されます。ラウンドロビンの欠点は、クライアントが順序のバラバラな TCP トラフィックに、高速で対応できる必要があることです。LACP 仕様 (802.3ad) は、実装は適切なルールに従って、順序がバラバラなトラフィックと重複パケットを最小化することを要求しています。ラウンドロビンによるロードバランシングは、この要件をまったく無視しています。ただし、HNAS のハッシュ関数では複数の物理ポートに会話をうまく分散できない場合があります。リンクの利用率が下がり、スループットが低下することがあります。このような場合、ラウンドロビンによるロードバランシングは、リンクの利用率を高め、スループットを高めることができます。集約で使用するポートローディング方式の横にあるラジオボタンを選択します。</li> </ul>

### 3. 必要な変更を加えます。

集約の構成を変更する場合、[Link Aggregation Details] 画面を使用して、次のことができます。

- 集約からポートを削除する。
- 集約で使用するロードバランシングのタイプを変更する。
- 集約にポートを追加する。

### 4. 変更を保存します。

[OK] をクリックして変更を保存するか、[cancel] をクリックして、[Link Aggregation] 画面に戻ります。

## (3) 集約を追加する

集約を追加するには

### 1. [Add Link Aggregation] 画面に移動します。

[Network Configuration] 画面で [Link Aggregation] を選択し、[add] をクリックして、[Add Link Aggregation] 画面を表示します。

Network Configuration [Home](#) > Network Configuration > Link Aggregation > Add Link Aggregation

## Add Link Aggregation

**Name**

ag3  
 ag4  
 ag5  
 ag6  
 ag7  
 ag8

**Available Ports**

ge1  
 ge2  
 ge3  
 ge4  
 ge5  
 ge6  
 tg2

**Use LACP**

Yes (LACP)  
 No (Static)

**Port Level Load Balancing**

Normal  
 Round Robin

[Home](#) | [About](#) | [Sign Out](#)

2. 集約の構成を設定します。

[Add Link Aggregation] 画面のチェックボックスとラジオボタンを使用して、集約の構成を設定します。

項目/フィールド	説明
Name	使用可能な集約名（現在使用されていない集約名）を一覧表示します。この集約の名前を選択するには、集約で使用する名前横にあるラジオボタンをオンにします。
Available Ports	集約に追加できる GbE (Gigabit Ethernet) 及び tg (10GbE) ポート。「gex」という名前のポートは Gigabit Ethernet ポートであり、「tgx」という名前のポートは 10GbE (10 Gigabit Ethernet) ポートです。集約にポートを追加するには、追加するポート名横にあるチェックボックスをオンにします。
Use LACP	この集約が LACP を使用するかどうかを指定します。LACP を使用しない集約は静的集約と呼ばれ、LACP を使用する集約は動的集約と呼ばれます。
Port level Load Balancing	集約内の全てのポートで使用されるポートのロードバランシング方式を表示します。 <ul style="list-style-type: none"> <li>• [Normal] は、HNAS が、一つの「会話」のための全てのトラフィックを適切な集約内の物理ポートの一つを経由してルーティングすることを意味します。HNAS のハッシュ関数とルーティング関数によって、どのパケットが集約のどの物理ポートを使用するかが決まります。例えば、特定の TCP 接続の全てのトラフィックは常に同じ物理ポートを経由してルーティングされます（リンクがドロップしない限り）。</li> <li>• [Round Robin] は、トラフィックを形成するパケットが各ポートを順に使用してルーティングされることを意味します。例えば、最初のパケットは最初のポートに送られ、2 番目のパケットは次のポートに送られるというようにして、全てのポートが使用されます。その後、トラフィックは再び最初のポートに送</li> </ul>

項目/フィールド	説明
	<p>られます。このルーティング方式では、全てのポートがほぼ等しく使用されるので、リンクのスループットが最大化されます。</p> <p>ラウンドロビンの欠点は、クライアントが順序のバラバラな TCP トラフィックに、高速で対応できる必要があることです。</p> <p>LACP 仕様 (802.3ad) は、実装は適切なルールに従って、順序がバラバラなトラフィックと重複パケットを最小化することを要求しています。ラウンドロビンによるロードバランシングは、この要件をまったく無視しています。ただし、HNAS のハッシュ関数では複数の物理ポートに会話をうまく分散できない場合があり、リンクの利用率が下がり、スループットが低下することがあります。</p> <p>このような場合、ラウンドロビンによるロードバランシングは、リンクの利用率を高め、スループットを高めることができます。</p> <p>集約で使用するポートローディング方式の横にあるラジオボタンを選択します。</p>

3. 設定を適用します。

設定を確認します。設定を適用するには [OK] をクリックします。キャンセルするには、[Cancel] をクリックします。

#### (4) 集約を削除する

集約を削除するには

1. [Link Aggregation] 画面に移動します。



**注意** 集約を削除するときは注意してください！

集約を削除する前に、集約に関連付けられている全ての IP アドレス、GbE、及び 10GbE ポートを削除する必要があります。

[Network Configuration] 画面で [Link Aggregation] をクリックして、[Link Aggregation] 画面を表示します。

Network Configuration | Home > Network Configuration > Link Aggregation

### Link Aggregation

**Configuration**

Name	Use LACP	Ports	Aggregation Status	
<input type="checkbox"/> ag1	No (Static)	tg1	Ok <span style="color: green;">●</span>	<a href="#">details</a>

[Check All](#) | [Clear All](#)

**Actions:** [add](#) [delete](#)

**Status**

Node	ag1
mc-stress-1	tg1 <span style="color: green;">●</span>
mc-stress-2	tg1 <span style="color: green;">●</span>

[Home](#) | [About](#) | [Sign Out](#)

2. 削除する集約を選択します。

削除する集約の名前の横にあるチェックボックスをオンにします。

3. 集約を削除します。

[Actions] セクションの [delete] をクリックします。次に、確認ダイアログの [OK] をクリックします。

## 1.4.2 IP アドレッシング

データ LAN 経由でアクセスできるように HNAS を構成するには、少なくとも二つの IP アドレスが必要です。これらの IP アドレスは、次のとおりです。

- HNAS 管理のための System Management Unit (SMU) 上のパブリック IP アドレス (データ LAN 上の IP アドレス)
- ファイルサービスに使用する、少なくとも一つの集約グループ上のパブリック IP アドレス  
全ての GbE ポートがリンク集約を使用する場合、一つの IP アドレスが集約グループ内の全てのポートをサポートします。



**重要** 逆ルーティング用に構成された場合 (GbE ポートごとの個別構成にした場合)、各ポートは独自の IP アドレスを持つ必要があります。

### (1) 既存の IP アドレスを表示する

既存の IP アドレスを表示するには、[Network Configuration] 画面から [IP Addresses] 画面に移動します。

IP Address	Subnet Mask	EVS	Port	Type	Cluster Node	
<input type="checkbox"/> 192.0.2.20	255.255.255.0		eth1	Cluster Node	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.0.2.21	255.255.255.0		eth1	Cluster Node	mc-stress-2	<a href="#">details</a>
<input type="checkbox"/> 192.0.2.22	255.255.255.0	mc	eth1	Admin Services	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.0.2.23	255.255.255.0	mc	eth1	Admin Services	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.168.40.100	255.255.240.0	evs04	ag1	File Services	mc-stress-2	<a href="#">details</a>
<input type="checkbox"/> 192.168.40.95	255.255.240.0	mc	ag1	Admin Services	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.168.40.97	255.255.240.0	evs01	ag1	File Services	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.168.40.98	255.255.240.0	evs02	ag1	File Services	mc-stress-1	<a href="#">details</a>
<input type="checkbox"/> 192.168.40.99	255.255.240.0	evs03	ag1	File Services	mc-stress-2	<a href="#">details</a>

Check All | Clear All

Actions: [add](#) [delete](#)

Shortcuts: [EVS Management](#)

Home | About | Sign Out

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
IP Address	HNAS 管理またはファイルサービスのために使用される IP アドレス。
Subnet Mask	サービスまたはクラスタノードのサブネットマスク。
EVS	次のいずれか。 <ul style="list-style-type: none"><li>• クラスタ構成では、管理サービス EVS のための IP アドレス</li><li>• ファイルサービス IP がバインドされている EVS (Virtual Server) のラベル</li><li>• ラベルが表示されない場合、IP アドレスはノード管理用 IP</li></ul>
Port	IP アドレスによって使用される次のインターフェース。 <ul style="list-style-type: none"><li>• [agX] は、GbE 集約の一つを示します。</li><li>• [eth0] または [eth1] は、Hitachi NAS Platform の 10/100 ポートです。</li></ul>
Type	ノードのサービスまたは構成のタイプ： <ul style="list-style-type: none"><li>• Admin Services : クラスタの管理サービスに関連付けられている IP アドレス 管理サービス IP アドレスは、データ LAN または内部 LAN 上のいずれかです。</li><li>• File Services : クラスタのファイルサービスに関連付けられている IP アドレス ファイルサービスの IP アドレスは、データ LAN 上であることが必要です。</li><li>• Cluster node : 物理クラスタノードに関連付けられている IP アドレス</li></ul>



項目/フィールド	説明
	ファイル及び管理サービスはノード間で移行できるので、クラスタノード IP アドレスはサービスではなくノードとの通信に使用されます。
Cluster Node	クラスタとして構成された場合、IP アドレスが現在割り当てられているクラスタノードの名前。

## (2) IP アドレスを追加する

ポートまたは集約に IP アドレスを追加するには

1. [Add IP Address] 画面に移動します。

[Home] 画面で [Network Configuration] を選択し、[IP Addresses] をクリックして、[IP Addresses] 画面を表示し、最後に [add] をクリックして、[Add IP Address] 画面を表示します。

2. IP アドレスを割り当てる Virtual Server (EVS) を選択します。  
ドロップダウンリストから、IP アドレスを割り当てる EVS を選択します。または、IP アドレスを管理サービスに使用するように指定します。
3. ポートを選択します。  
集約または管理ポートを選択します。  
ドロップダウンリストから、集約（「agX」）または管理ポート（「eth0」または「eth1」）を選択します。



**重要** EVS に IP アドレスを割り当てるときには、「agX」ポートを指定する必要があります。

4. IP アドレッシングを定義します。  
選択したポートの IP アドレスとサブネットマスクを入力します。
5. 設定を適用します。  
設定を確認します。設定を適用するには [OK] をクリックします。キャンセルするには、[Cancel] をクリックします。

## (3) IP アドレスを削除する



**注意** IP アドレスを削除するときは注意してください！  
このステップの説明に従って IP アドレスを削除する前に、IP アドレスを割り当てる EVS を無効にしてください。IP アドレスが削除されたら、EVS を再び有効にします。これにより、削除されるときに IP アドレスが使用中ということがなくなります。



注意 内部 LAN (eth1) の IP アドレスは変更しないでください。変更が必要な場合は、お問い合わせください。

IP アドレスを削除するには

1. EVS を無効にします。
  - a. [Server Settings] 画面で [EVS Management] をクリックして、[EVS Management] 画面を表示します。

The screenshot shows the 'EVS Management' page. At the top, there is a breadcrumb trail: 'Server Settings > Home > Server Settings > EVS Management'. Below this is a 'Filter' section with the text 'No Filtering Applied' and a 'filter' button. The main content is a table with the following columns: Label, Type, Cluster Node, Status, First IP Address, and First Port. There are three rows of data, each with a checkbox on the left and a 'details' button on the right. Below the table are 'Actions' (enable, disable, add) and 'Shortcuts' (IP Addresses, EVS Migration). At the bottom, there are links for 'Home', 'About', and 'Sign Out'.

Label	Type	Cluster Node	Status	First IP Address	First Port
<input type="checkbox"/> AdminEVS	Admin Services	hnasj1-1	Online	192.0.2.10 ...	eth1 ...
<input type="checkbox"/> EVS-CNS	File Services	hnasj1-1	Online	192.168.5.31	ag1
<input type="checkbox"/> EVS01	File Services	hnasj1-1	Online	192.168.5.30	ag1

- b. IP アドレスを割り当てる EVS の名前の横にあるチェックボックスをオンにして、[disable] をクリックします。
2. IP アドレスを削除します。
    - a. [Network Configuration] 画面で [IP Addresses] をクリックして、[IP Addresses] 画面を表示します。

The screenshot shows the 'IP Addresses' page. At the top, there is a breadcrumb trail: 'Network Configuration > Home > Network Configuration > IP Addresses'. Below this is a table with the following columns: IP Address, Subnet Mask, EVS, Port, Type, and Cluster Node. There are nine rows of data, each with a checkbox on the left and a 'details' button on the right. Below the table are 'Actions' (add, delete) and 'Shortcuts' (EVS Management). At the bottom, there are links for 'Home', 'About', and 'Sign Out'.

IP Address	Subnet Mask	EVS	Port	Type	Cluster Node
<input type="checkbox"/> 192.0.2.20	255.255.255.0		eth1	Cluster Node	mc-stress-1
<input type="checkbox"/> 192.0.2.21	255.255.255.0		eth1	Cluster Node	mc-stress-2
<input type="checkbox"/> 192.0.2.22	255.255.255.0	mc	eth1	Admin Services	mc-stress-1
<input type="checkbox"/> 192.0.2.23	255.255.255.0	mc	eth1	Admin Services	mc-stress-1
<input type="checkbox"/> 192.168.40.100	255.255.240.0	evs04	ag1	File Services	mc-stress-2
<input type="checkbox"/> 192.168.40.95	255.255.240.0	mc	ag1	Admin Services	mc-stress-1
<input type="checkbox"/> 192.168.40.97	255.255.240.0	evs01	ag1	File Services	mc-stress-1
<input type="checkbox"/> 192.168.40.98	255.255.240.0	evs02	ag1	File Services	mc-stress-1
<input type="checkbox"/> 192.168.40.99	255.255.240.0	evs03	ag1	File Services	mc-stress-2

- b. 削除する IP アドレスを選択して、[delete] をクリックします。
3. EVS を再び有効にします。

- a. [Server Settings] 画面で [EVS Management] をクリックして、[EVS Management] 画面を表示します。

Server Settings | Home > Server Settings > EVS Management

### EVS Management

Filter  
No Filtering Applied  
filter

Label	Type	Cluster Node	Status	First IP Address	First Port	
<input type="checkbox"/> AdminEVS	Admin Services	hmasj1-1	Online	192.0.2.10 ...	eth1 ...	details
<input type="checkbox"/> EVS-CNS	File Services	hmasj1-1	Online	192.168.5.31	ag1	details
<input type="checkbox"/> EVSD1	File Services	hmasj1-1	Online	192.168.5.30	ag1	details

Check All | Clear All

Actions: enable | disable | add

Shortcuts: IP Addresses | EVS Migration

Home | About | Sign Out

- b. 再び有効にする EVS を選択して、[enable] をクリックし、EVS を再び有効にします。

#### (4) IP ネットワークの拡張設定を変更する

追加の構成にアクセスするには、Advanced Mode が有効でなければなりません (Advanced Mode については、『*User Administration Guide*』を参照してください)。

1. [Advanced IP Configuration] 画面に移動します。  
[Network Configuration] 画面で [Advanced IP Configuration] をクリックして、画面を表示します。

## Advanced IP Configuration

**Global Settings**

IP Reassembly Timer:  seconds

Ignore ICMP Echo Requests:

IP MTU for Off-Subnet Transmits:  bytes

TCP Keep Alive:

TCP Keep Alive Timeout:  seconds

TCP MTU:  bytes

Other Protocol MTU:  bytes

ARP Cache Timeout:  seconds

Ignore ICMP Redirect:

[apply](#) [reset](#)

Ports	Port	Current Settings
<input type="checkbox"/>	ag1	Using Global Settings <a href="#">details</a>
<input type="checkbox"/>	eth1	Using Global Settings <a href="#">details</a>
<input type="checkbox"/>	eth0	Using Global Settings <a href="#">details</a>

Actions: [customize](#) [restore](#)

[Home](#) | [About](#) | [Sign Out](#)



**重要** クラスタ構成では、[Advanced IP Configuration] 画面の IP アドレス設定は、クラスタ内の全てのノードに適用されます。ノードを個別に構成することはできません。

[Global Settings] 領域にはグローバル構成を設定するフィールドとエントリがあり、これが全ての集約とポートのデフォルト設定になります。

Global Settings	デフォルト
IP Reassembly Timer (seconds)	15
Ignore ICMP Echo Requests	オフ
IP MTU for Off-Subnet Transmits (bytes)	1,500
TCP Keep Alive	オン
TCP Keep Alive Timeout (seconds)	7,200
TCP MTU (bytes)	1,500
Other Protocol MTU (bytes)	1,500
ARP Cache Timeout (seconds)	60
Ignore ICMP Redirect	オフ



**重要** [Global Settings] は HNAS に適用されます。すなわち、グローバル設定として指定された値は、全ての集約（及び集約を構成する GbE ポート）で最初に使用されます。後で、HNAS 上の定義済み集約（ポート）ごとに、個々の構成設定を定義できます。

[Ports] には、構成済みの全ての集約とポートが一覧表示され、集約／ポートがグローバル構成を使用しているか、それともカスタマイズされた構成を使用しているかが示されます。

Ports	説明とデフォルト値
Port	HNAS 内の現在構成済みの集約またはポートの名前を一覧表示します。 デフォルト : ag1~agx, eth0, eth1
Current Settings	集約またはポートがデフォルト（グローバル）設定を使用しているか、カスタマイズされた設定を使用しているかを示します。

Ports	説明とデフォルト値
	集約/ポートがカスタマイズされた設定を使用している場合は、[details] ボタンも表示されます。[details] をクリックすると、カスタマイズされた構成を既に使用している集約の構成を編集できます。

2. グローバル設定を変更します。

[Actions] では、グローバル設定について次のアクションが使用できます。

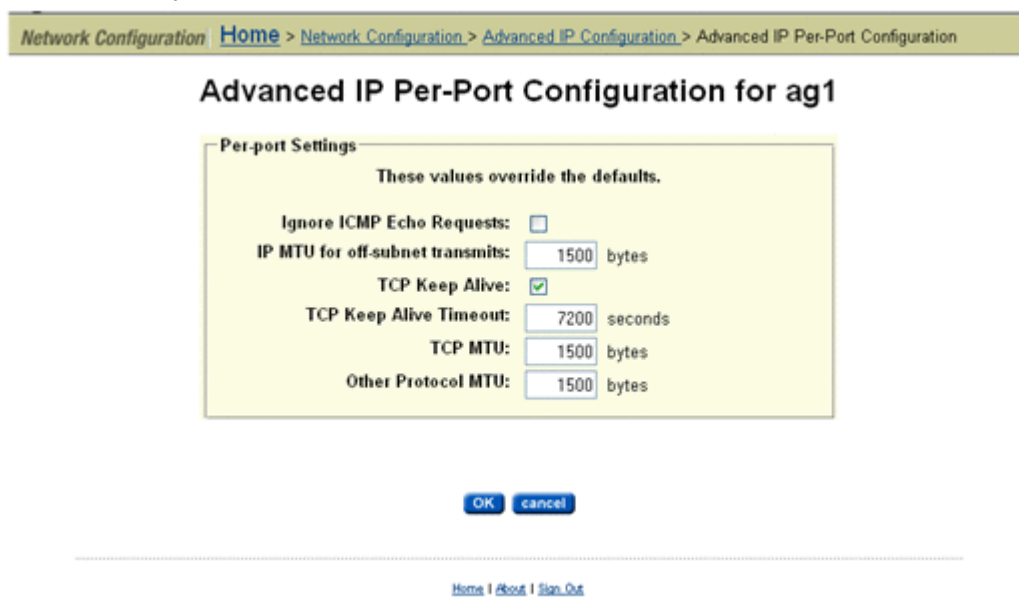
- グローバル設定をカスタマイズするには、[Global Settings] 領域のフィールドの値を変更することによって、グローバル構成設定として使用する値を指定します。デフォルトでは、全ての集約（ポート）がグローバル設定を使用します。グローバル設定の値に必要な変更を加えたら、[apply] をクリックして変更を保存します。
- グローバル設定を工場出荷時のデフォルト値に戻すには、[reset] をクリックします。

IP アドレス構成の完了後、HNAS を再起動しなければならない場合があります。そのようなメッセージが表示された場合は、指示に従って HNAS を再起動してください。

3. ポートごとの設定をカスタマイズまたは元に戻します。

[Actions] では、特定の集約について次のアクションが使用できます。

- 現在選択されている集約（[Ports] フィールドで選択されている集約）の設定をカスタマイズするには、[customize] をクリックして、[Advanced IP Per-Port Configuration] 画面を表示します。



この画面のデフォルトの IP 構成設定を以下に示します。

Per-port Settings	デフォルト設定
Ports, a list of available Ethernet or aggregation ports	リストの最初のポート
Ignore ICMP Echo Requests	オフ
IP MTU for Off-Subnet Transmits (bytes)	1500
TCP Keep Alive	オン
TCP Keep Alive Timeout (seconds)	7200
TCP MTU	1500
Other Protocol MTU	1500

フィールドに新しい値を入力して、[OK] をクリックします。新しい設定は、グローバル設定に優先します。

- 集約（ポート）の設定をグローバル構成に戻すには、[Ports] フィールドの集約を選択して、[restore] をクリックします。[Ports] フィールドで選択した集約とその GbE インターフェースの全ての設定が消去されて、デフォルト（グローバル設定）に戻されます。
- カスタマイズされた構成を使用している集約の設定を変更するには、[details] をクリックして、[Advanced IP Per-Port Configuration] 画面を表示します（上記参照）。フィールドに新しい値を入力して、[OK] をクリックします。新しい設定は、グローバル設定に優先します。

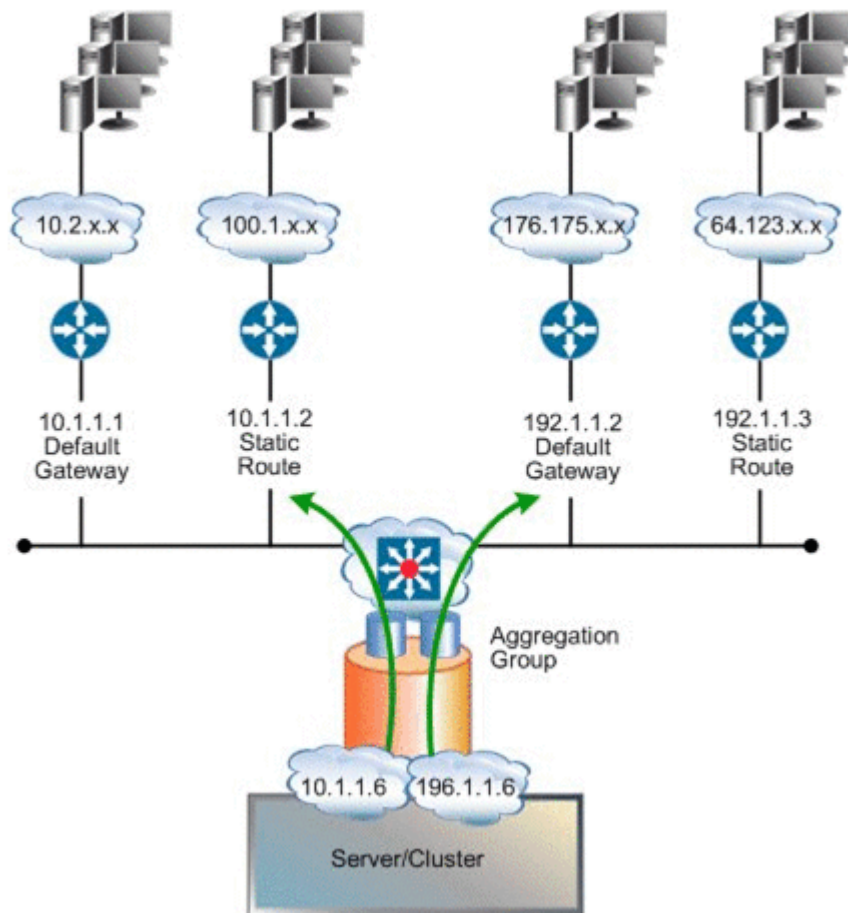
IP 構成の完了後、HNAS を再起動しなければならない場合があります。そのようなメッセージが表示された場合は、指示に従って HNAS を再起動してください。

# IP ルーティング

## □ 2.1 IP ルーティング

## 2.1 IP ルーティング

構成に応じて、HNAS は、デフォルトゲートウェイ、静的ルート、及び動的ルートの三つの方法で IP トラフィックをルーティングできます。次の図は、ルート経由でさまざまな IP ネットワークと通信するための HNAS の構成例を示しています。



### 2.1.1 デフォルトゲートウェイ

HNAS は、IP トラフィックをルーティングするための複数のデフォルトゲートウェイをサポートします。複数の IP ネットワークに接続される際には、HNAS が接続するネットワークごとにデフォルトゲートウェイを追加します。この構成では、HNAS は、送信パケットで指定された送信元 IP アドレスと同じサブネット上のゲートウェイとを照合することによって、適切なデフォルトゲートウェイによりトラフィックをルーティングできます。

複数のデフォルトゲートウェイがある場合、HNAS は IP トラフィックを論理的にルーティングするので、特定の HNAS に接続している全てのネットワークの静的ルートを指定する必要はありません。

### 2.1.2 静的ルート

静的ルーティングは、ネットワーク内のデータの固定されたパスとなります。ネットワーク上の HNAS がルーター経由で追加のネットワークに接続される場合、各ネットワークへの静的ルートを指定することによって、その HNAS とリモートネットワーク間の通信を有効にできます。

静的ルートは、ルーティングテーブルでセットアップされます。テーブル内の各エントリは、宛先 ID、ゲートウェイアドレス、及び（ときには）サブネットマスクから成ります。HNAS のルーティ



ングテーブル内の静的ルートのエントリーは持続的です。すなわち、HNAS が再起動しても、ルーティングテーブルの静的ルーティングエントリーは変化しません。

HNAS は、ネットワークベースとホストベースの両方の静的ルートをサポートします。特定のネットワーク上の全てのコンピューターへのルートをセットアップするには、[Network] オプションを選択します。通常のルーターアドレス以外のネットワーク上の特定のコンピューターへのルートをセットアップするには、[Host] オプションを選択します。静的ルートの最大数は、127 です（デフォルトゲートウェイも含めて）。

### 2.1.3 動的ルート

ルートをルーティングテーブルに動的に追加できる ICMP リダイレクトと RIP バージョン 2 (RIPv2) をサポートします。

- ICMP リダイレクトは、ルーターがルーティング情報を HNAS に送り返すための業界標準です。あるルーターが、送信先へのより良いルートを提供する別のルーターを検出したときには、HNAS に ICMP リダイレクトを送信し、HNAS のルーティングテーブルに検出したルート情報を一時的に上書きします。ルーターが自動的にルート情報を設定するため、管理者が手動でルーティングテーブルを設定する必要はありません。

HNAS は、ルーターのアドレスを発見できる ICMP ルーターディスカバリーもサポートします。ICMP ルーターは、アドレスを定期的にマルチキャストします。HNAS がこれらのマルチキャストを受信すると、そのルーターをルーティングテーブルに組み込みます。HNAS のルーティングテーブルに表示されたルーターは、ゲートウェイとして使用できます。

ICMP ルーターディスカバリーは、CLI コマンド `irdp` を使用して制御されます。詳細については、『*CLI Reference*』を参照してください。

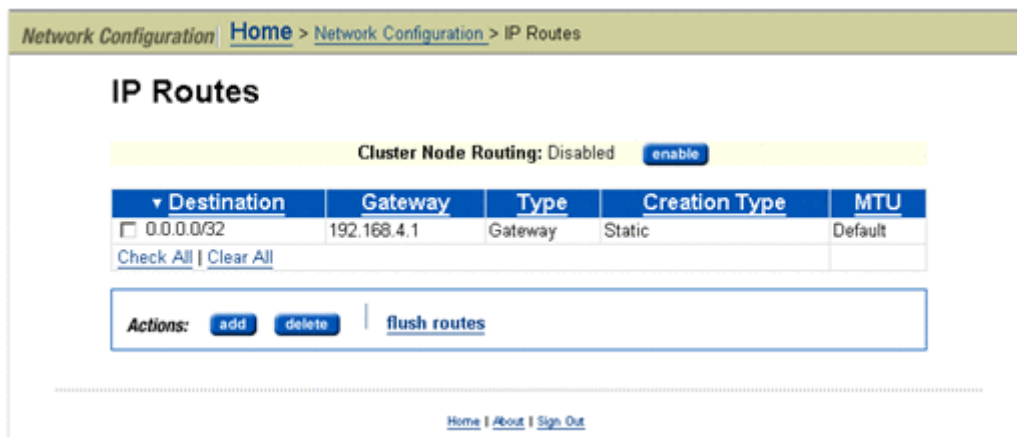
- RIPv2 も業界標準であり、HNAS は他のネットワークデバイスによって提供された更新に基づいて、ルートを自動的に発見して、ルーティングテーブル内のルートを更新できます。RIPv2 は、CLI コマンド `rip` を使用して制御されます。詳細については、『*CLI Reference*』を参照してください。

HNAS は動的ホストルートを 10 分間、ルーティングキャッシュに保存します。この時間が経過すると、HNAS が別の ICMP リダイレクトを受信するまで、選択された送信先へのパケットは、ルーティングテーブルで指定されたルートを使用します。

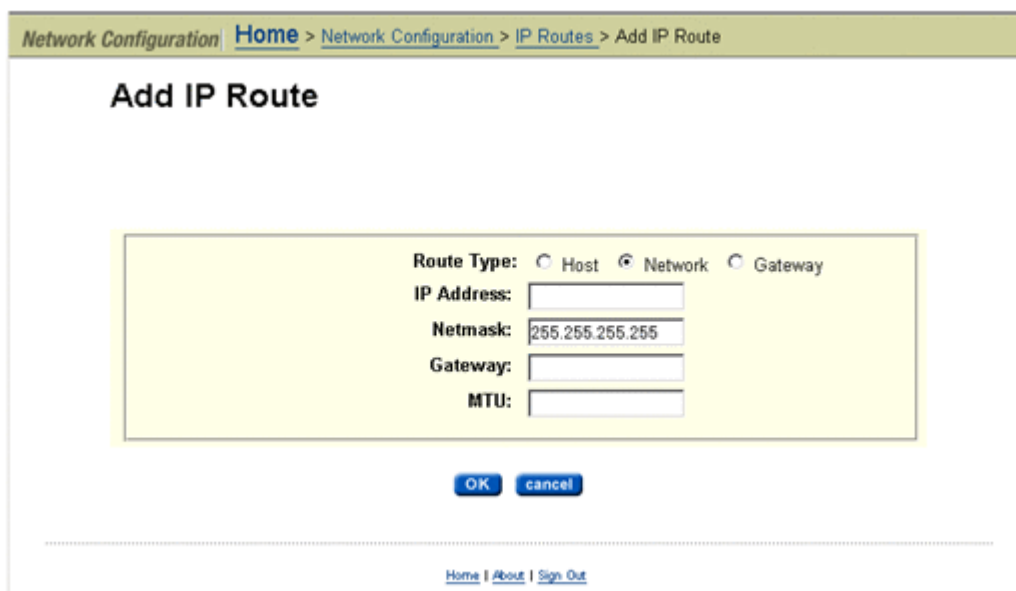
### 2.1.4 HNAS のルーティングテーブルを管理する

HNAS は、パケットを送信するときに最も具体的なルートを選びます。ホストルートは、ネットワーク上の特定のコンピューターを指すので、最も具体的です。ネットワークルートは、特定のネットワークを指すので、次に具体的です。ゲートウェイは最も具体的でないルートなので、HNAS にとっては 3 番目のルーティングオプションです。したがって、HNAS がパケットを送信するときにホストルートを見つけた場合は、ネットワークルートやゲートウェイではなく、そのルートを選びます。同様に、ホストルートが使用できないときには、HNAS は該当するネットワークルートを選び、ホストルートもネットワークルートもないときには、HNAS はパケットをデフォルトゲートウェイに送信します。

HNAS のルーティングテーブルを管理するには、[Network Configuration] 画面で [IP Routes] をクリックして、[IP Routes] 画面を表示します。



- ルートを削除するには：  
削除するルートの横にあるチェックボックスをオンにして，[delete] をクリックします。  
動的ルートを個別に削除することはできません。全ての動的ルートを削除するには，[flush routes] をクリックして，キャッシュをフラッシュします。
- ルートを追加するには：  
[add] をクリックして，[Add IP Route] 画面を表示します。



- ホストベースで静的ルーティングを設定するには，[Host] ラジオボタンを選択して，送信先ホストの IP アドレスと，ホストにアクセスするゲートウェイを指定します。ホストベースのルートの場合，ネットマスクは常に 255.255.255.255 です。[Host] ルートタイプを選択すると，このネットマスクが自動入力されます。
- ネットワークベースで静的ルーティングを設定するには，[Network] ラジオボタンを選択して，IP アドレスとネットマスクに基づいて送信先ネットワークを指定します。また，送信先ネットワークにアクセスするゲートウェイを指定します。
- デフォルトゲートウェイを設定するには，[Gateway] ラジオボタンを選択して，ルートタイプを選択した後，[Gateway] フィールドにデフォルトゲートウェイの IP アドレスを入力します。[IP Address] 及び [Netmask] フィールドは自動入力されます。
- 最大転送単位を入力する場合は，[MTU] フィールドに入力します。入力がない場合は，[Global Settings] で設定している値となります。
- ルーティングキャッシュをフラッシュするには：

[flush routes] をクリックします。



# ネームサービス

- 3.1 ネームサービスの概要
- 3.2 ネームサービスを構成する

## 3.1 ネームサービスの概要

管理者は、HNAS がローカルネームサーバと連携して、次の名前解決法をサポートするように構成できます。

- Domain Name System (DNS)
- Dynamic Domain Name System (DDNS)
- Windows Internet Naming Service (WINS)

これらの方法は、コンピューター識別子 (IP アドレスなど) をコンピューターの名前に関連付けます。これにより、ダイアログボックスで、IP アドレスではなくコンピューター名を指定できます。

### 3.1.1 DNS 及び DDNS

TCP/IP ネットワークでは、ホスト名から IP アドレスへの解決のために、Domain Name System (DNS) が使用されます。

DNS では、全てのホスト名と IP アドレスのレコードを手動で作成する必要があります。Microsoft は、Windows2000 から Dynamic DNS をサポートしました。これは、認証されたホストをホスト名と IP アドレスのレコードに自動的に追加できる DNS データベースであり、これによってレコードを手動で作成する必要がなくなりました。

#### (1) CIFS 名を登録する

EVS がオンラインになると、HNAS は、EVS に関連付けられた構成済みの ADS CIFS 名と IP アドレスのそれぞれについて、構成済みの DNS サーバにエントリを登録します (正引き及び逆引きゾーンの両方に)。このように、EVS は、構成された IP アドレスごとに一つのエントリを DDNS に記録します。HNAS に複数の ADS CIFS 名が構成されていた場合、構成された各 CIFS 名のそれぞれの IP アドレスのエントリが登録されます。

DNS サーバに登録されるホスト名はそれぞれ、20 分間の Time To Live (TTL) プロパティを持ちます。これは、DNS サーバとアプリケーションがそのホスト名をキャッシュできる時間の長さです。レコードの TTL は時間の経過と共に短くなり、TTL がゼロに達すると、レコードはキャッシュから削除されます。TTL の有効期限が切れた場合は、クライアントは最新名検索を実行して、詳細を入手する必要があります。

DNS サーバは、24 時間ごとにホスト名をリフレッシュします。このリフレッシュは、最初の登録が完了してから開始されます。例えば、HNAS が起動時に名前を登録した場合、起動後 24 時間ごとに DNS エントリをリフレッシュします。HNAS が名前を登録またはリフレッシュできなかった場合は、リカバリーモードになり、5 分ごとに登録を再試行します。登録が成功すると、再び、24 時間ごとのリフレッシュサイクルが開始されます。

#### (2) セキュアな DDNS 更新

HNAS は、セキュアな DDNS 更新とセキュアでない DDNS 更新の両方をサポートします。デフォルトでは、Microsoft Windows 2000, 2003, 及び 2008 の DDNS サーバは、「セキュア」な、Kerberos 認証された登録のみを受け入れます。Microsoft と Microsoft 以外の両方の DDNS サーバをサポートするために、HNAS は、まず、セキュアでない DDNS への登録を試みます。セキュアでない登録が失敗した場合、HNAS はセキュアな登録を試みます。

### 3.1.2 WINS

WINS は、NetBIOS 名から IP アドレスへの解決を行い、HNAS がネットワーク上の CIFS クライアントと通信するために使用されます。



重要 WINS は、Windows 2008 では推奨されません。

## 3.2 ネームサービスを構成する

ネームサービス構成では、ネームサービスとその優先順位を指定する必要があります。次のセクションでは、これらのタスクを完了する方法を説明します。

### 3.2.1 ネームサービスの指定と優先順位付け

ネームサービスを指定し、優先順位を付けるには

1. [Name Services] 画面に移動します。

[Network Configuration] 画面で [Name Services] をクリックして、[Name Services] 画面を表示します。

2. 要求された情報を入力します。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS Security Context	現在選択されている EVS セキュリティコンテキストを表示します。この画面で行ったネームサービスの変更は、現在選択されている EVS セキュリティコンテキストにのみ適用されます。 <ul style="list-style-type: none"> <li>• EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。</li> <li>• EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のネームサービス設定を変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。</li> </ul> [change] をクリックして、別の EVS セキュリティコンテキストを選択するか、グローバル構成を選択します。
DNS Servers	最大三つの DNS サーバの IP アドレス。複数の DNS サーバを入力した場合、検索は、一覧表示された順序で DNS サーバを使用して行われます。

項目/フィールド	説明
Domain Search Order	<p>検索キーワードとして使用するドメインサフィックス（「ourcompany.com」など）を入力します。</p> <p>コンピューター名を検索するとき、DNS サーバはサフィックス順に検索します。例えば、HNAS が「uk.ourcompany.com」と「us.ourcompany.com」というエントリを含む場合、「author」という名前のホストの IP アドレスが要求された場合、「author.uk.ourcompany.com」に対するクエリーが生成され、次に「author.us.ourcompany.com」に対するクエリーが生成されます。ただし、システムは親ドメインである「ourcompany.com」は検索しません。</p> <p>注：</p> <p>サフィックスとコンピューターのホスト名の組み合わせで、完全修飾ドメイン名を形成します。</p> <p>表示されたリストにサフィックスを付加するには、[Add] をクリックします。サフィックスを削除するには、表示されたリストからサフィックスを選択して、[X] をクリックします。</p> <p>複数のドメインサフィックスを使用するときには、上矢印と下矢印を使用してリストボックス内の順序を変えることで、サフィックスの検索順序を選択します。</p>
WINS Servers	<p>プライマリ WINS サーバをセットアップするには、[Primary] WINS サーバフィールドに IP アドレスを入力します。</p> <p>セカンダリ WINS サーバがある場合は、[Secondary] WINS サーバフィールドに IP アドレスを入力します。</p>

3. 変更を保存します。  
[apply] をクリックして保存します。
4. ネームサービスが一つだけの場合も、そのネームサービスが [Name Services Order] 画面に表示されていることを確認します。
  - a. [Name Services Order] 画面に移動します。  
[Network Configuration] 画面で [Name Services Order] をクリックして、[Name Services Order] 画面を表示します。[Available Name Services] と [Selected Name Services] が個別のセクションに一覧表示されます。



- b. ネームサービスを選択及び選択解除して、[Selected Name Services] リストを作成します。  
[Available Name Services] ボックスからネームサービスを選択して [Selected Name Services] ボックスに移動するには、右矢印ボタンを使用します。逆に、ネームサービスを削除するには、左矢印ボタンを使用します。
  - c. 選択したネームサービスの使用順序を変更します。  
上/下矢印ボタンを使用して、[Selected Name Services] ボックス内の選択したネームサービスの使用順序を変更します。
  - d. 設定を適用します。



設定を確認します。設定を適用するには [apply] をクリックします。



# ディレクトリサービス

- 4.1 ディレクトリサービスの概要
- 4.2 ディレクトリサービスを構成する

## 4.1 ディレクトリサービスの概要

管理者は、HNAS がローカルディレクトリサーバと連携して、ネットワークリソースの場所や管理をサポートするように構成できます。次のディレクトリサービスを使用できます。

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

これらのサービスは、識別子をユーザー、グループ、デバイス、ボリューム、フォルダ、及びその他のネットワークリソースに関連付けます。これらのサービスは、何らかの種類の識別子をリソースに関連付けて、リソース単位ではなく、幅広いアクセスポリシーを指定できるようにし、この情報をネットワーク全体からアクセスできるようにします。

### 4.1.1 NIS (NFS 用)

NIS データベースは、Unix ベースのネットワークの簡単な管理を提供します。このデータベースは、ユーザーとグループに関する詳細や、個々のクライアントマシンに関する詳細（ネットワーク上のクライアントにログインするユーザーの認証を容易するための、IP アドレスとホスト名など）を提供します。

HNAS は NIS をサポートし、NIS を使用するように構成されているときには、次のものを提供できます。

- NFS ユーザー及びグループアカウント情報の取得
- ホスト名から IP アドレスへの解決を行うネームサービス
- FTP ユーザー認証

### 4.1.2 LDAP

多くの組織は、既存の NIS インフラストラクチャーを、より信頼性と拡張性があり、よりセキュアな LDAP システムに置き換えつつあります。NIS と同じサービス（ユーザー及びグループ情報の取得、名前解決サービス、及び FTP ユーザー認証）の提供に加えて、LDAP は次のような利点も備えています。

- LDAP は現在のデータとレプリケーションデータのデータ同期をより頻繁に行うので、正確さが増します。
- Secure Sockets Layer (SSL) と Transport Layer Security (TLS) を使用して通信を暗号化します。
- NIS データベースへの匿名アクセスの代わりに、LDAP データベースへの接続を認証します。

HNAS は、最も一般的な次の二つの LDAP サービス実装を含めて、LDAP バージョン 2 をサポートします。

- Sun Directory Server
- OpenLDAP



**重要** LDAP を使用して NIS Netgroup の解決はできません。Netgroup が必要な場合は、ローカル Netgroup を使用する必要があります。

---

## 4.2 ディレクトリサービスを構成する

ディレクトリサービスの構成には、サービスの有効化、ディレクトリサーバの指定、ディレクトリサーバの構成または優先順位付けが必要です。以下のセクションでは、これらのタスクを完了する方法を説明します。

### 4.2.1 NIS 及び LDAP サービスの有効化と構成

このセクションでは、Web Manager を使用して NIS 及び LDAP サービスを有効にし、構成する方法を説明します。

NIS サービスの構成には、以下のタスクが含まれます。

- NIS の有効化と無効化
- NIS 構成の表示
- NIS サーバの追加
- NIS 構成の変更
- 構成済み NIS サーバの優先順位の変更
- NIS サービスを提供するように LDAP を構成

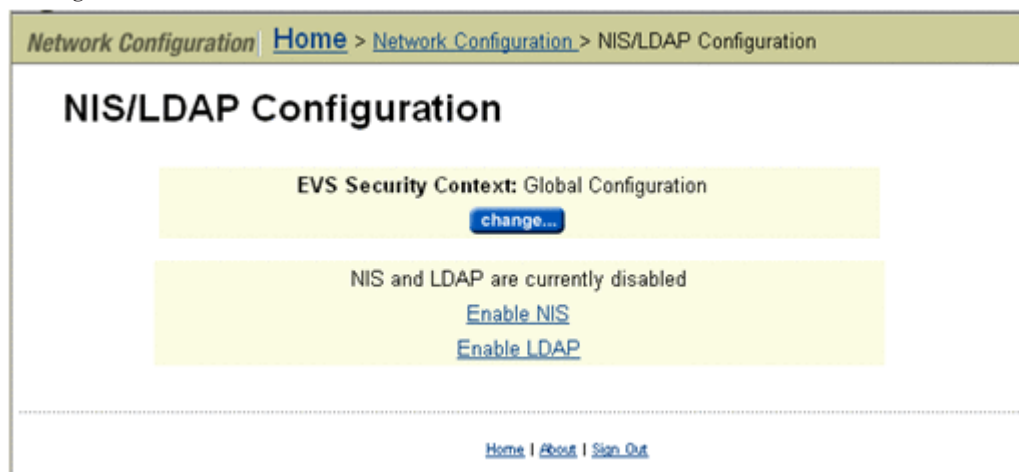


重要 HNAS は LDAP バージョン 2 をサポートします。

### 4.2.2 NIS を有効／無効にする

使用するネットワーク情報サービスを決めた後（「3.1 ネームサービスの概要」を参照）、以下の説明に従って、NIS または LDAP を有効にします。

1. [NIS/LDAP Configuration] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックして、[NIS/LDAP Configuration] 画面を表示します。



2. NIS または LDAP を有効にします。  
[Enable NIS] または [Enable LDAP] をクリックします。
3. [Name Services Order] 画面に移動します。  
[Network Configuration] 画面で [Name Services Order] をクリックして、[Name Services Order] 画面を表示します。

## Name Services Order

- NIS/LDAP を使用するネームサービスとして追加します。  
[Available Name Services] リストから、NIS/LDAP を選択し、右向き矢印をクリックします。
- 設定を適用します。  
設定を確認します。適用するには [apply] をクリックします。

### 4.2.3 NIS 構成を表示する

現在のドメインの NIS 構成を表示するには、次のようにします。

- [NIS/LDAP Configuration] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックして、[NIS/LDAP Configuration] 画面を表示します。

## NIS/LDAP Configuration

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS Security Context	現在選択されている EVS セキュリティコンテキスト、つまり、個別セキュリティコンテキストまたはグローバルセキュリティコンテキストを表示します。[change] をクリックして、別の EVS セキュリティコンテキストを選択するか、グローバル構成を選択します。別の EVS セキュリティコンテキストを選択すると、NIS/LDAP 構成設定が適用されるコンテキストが変更されます。
Domain	システムがクライアントである NIS ドメインの名前。
Rebind	HNAS が構成済み NIS サーバへの接続を試みる頻度。1~15 分の値を入力します。

項目/フィールド	説明
Timeout	HNAS がドメインをチェックするときに、NIS サーバからの応答を待つ時間（ミリ秒）。100～10,000 ミリ秒の値を入力します。デフォルト値は 300 ミリ秒です。
Broadcast For Servers	HNAS がネットワーク上の使用可能な NIS サーバを発見できるようにします。HNAS は同じ NIS ドメインにあることが必要で、HNAS のネットワーク上にあることが必要です。
IP Address	現在構成されている NIS サーバの IP アドレスを表示します。
Priority	<p>選択された NIS サーバの優先度（値が小さいほど、優先順位が高ブロードキャストによって発見された NIS サーバは優先順位を持ちません。[details] ボタンをクリックして優先順位を割り当てた場合、NIS サーバタイプは「User Defined」になり、「User Defined」の NIS サーバは、ブロードキャストによって発見された NIS サーバより優先されます。い）。NIS ドメインに複数の NIS サーバが含まれる場合、システムは再バインドチェックのときに、最も優先度の高い NIS サーバへのバインドを試みます。</p> <p>注：</p> <p>ブロードキャストによって発見された NIS サーバは優先順位を持ちません。[details] ボタンをクリックして優先順位を割り当てた場合、NIS サーバタイプは「User Defined」になり、「User Defined」の NIS サーバは、ブロードキャストによって発見された NIS サーバより優先されます。</p>
Type	<p>NIS サーバのタイプ。</p> <p>注：</p> <p>[Broadcast for Servers] オプションによって、NIS サーバを自動的に発見できるようにユーザーが定義できます。ユーザーによって定義された NIS サーバは、優先順位に関係なく、ブロードキャストによって発見された NIS サーバに優先して試行されます。</p>

2. NIS サーバを追加及び削除し、NIS サーバの詳細を表示し、NIS サーバの優先順位を変更し、または NIS 構成を変更します。
  - NIS サーバを追加するには：

[add] をクリックします。「[4.2.4 NIS サーバを追加する](#)」の説明を参照してください。
  - NIS サーバを削除するには：

NIS サーバを選択して、[delete] をクリックします。
  - 構成を変更するには：

[modify] をクリックします。「[4.2.5 NIS 構成を変更する](#)」の説明を参照してください。
  - 詳細なプロパティを表示する、または、NIS サーバの優先順位を変更するには：

NIS サーバを選択し、[details] をクリックします。「[4.2.6 構成済み NIS サーバの優先順位を変更する](#)」の説明を参照してください。
  - LDAP に切り替えるには：

[Switch to using LDAP] をクリックします。変更は全ての登録されたサーバに適用されません。
  - NIS を無効にするには：

[Disable NIS and LDAP] をクリックします。変更は全ての登録されたサーバに適用されません。
  - ネームサービスの順序を変更するには：

[Name Services Order] をクリックして、[Name Services Order] 画面に移動し、ネームサービスの順序を指定します。詳細については、「[4.2.11 ネームサービスの順序を変更する](#)」を参照してください。

## 4.2.4 NIS サーバを追加する

NIS サーバを追加するには

1. [Add NIS Server] 画面に移動します。  
[Home] 画面で [Network Configuration] を選択してから [NIS Configuration] を選択し、[add] をクリックして、[Add NIS Server] 画面を表示します。



2. 要求された情報を入力します。  
[Server IP Address] フィールドに、追加する NIS サーバの IP アドレスを入力します。  
[Priority] フィールドで、この NIS サーバの優先度をドロップダウンリストから選択します (最も低い番号が最も高い優先順位です)。



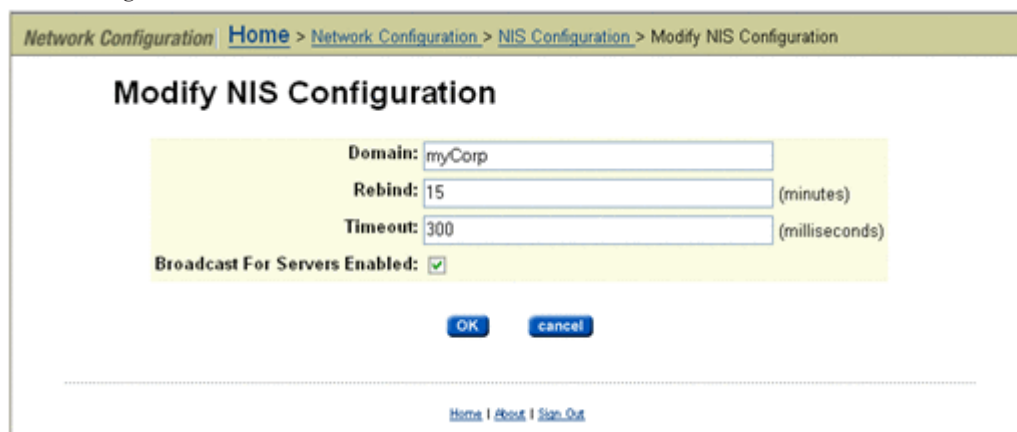
**重要** NIS ドメインに複数の NIS サーバが含まれる場合、システムは再バインドチェックのときに、最も優先度の高い NIS サーバへのバインドを試みます。

3. 新しい NIS サーバの追加を反映します。  
[OK] をクリックします。

## 4.2.5 NIS 構成を変更する

NIS 構成を変更するには

1. [Modify NIS Configuration] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックし、[NIS/LDAP Configuration] 画面を表示します。画面が表示されたら、[modify] をクリックして、[Modify NIS Configuration] 画面を表示します。



2. 要求された情報を入力します。
  - a. [Domain], [Rebind], 及び [Timeout] フィールドの値を編集します。
  - b. [Broadcast for Servers] を有効または無効にします。  
[Broadcast for Servers Enabled] チェックボックスをオンにすると、HNAS はドメイン内の NIS サーバを発見して、自動的にバインドできるようになります。有効にすると、HNAS



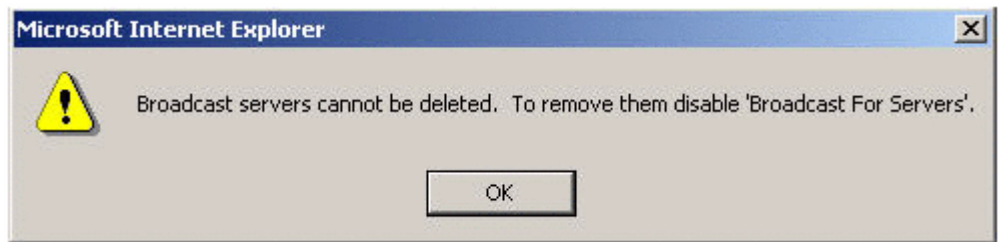
は構成済みの NIS ドメイン内の NIS サーバを検索します。これらの NIS サーバはブロードキャストによって発見されるので、HNAS と同じ論理ネットワーク上にあることが必要です。



**重要** NIS サーバがブロードキャストによって発見されたら、[details] をクリックしてその NIS サーバを構成します。後で [Broadcast for Servers] チェックボックスをオフにしても、NIS サーバ構成は削除されません。その後も使用できます。

ブロードキャストによって発見された NIS サーバは、定期的にポーリングされて、応答性が確認され、NIS 検索要求が行われたときには、最も応答性の高い NIS サーバが選択されます。

ブロードキャストによって発見された NIS サーバを削除するには、[Broadcast for Servers] を無効にします ([Broadcast for Servers] チェックボックスをオフにします)。[Broadcast for Servers] が有効な場合、ブロードキャストによって発見された NIS サーバを削除しようとすると、次のようなエラーメッセージが表示されます。



3. 構成を適用します。

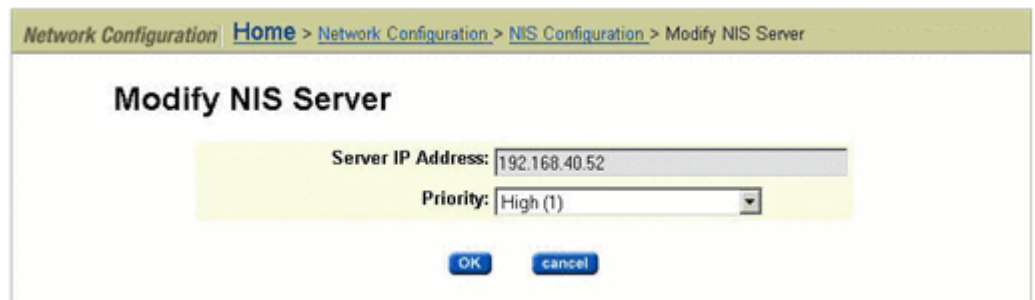
構成が正しいことを確認します。設定を適用するには [OK] をクリックします。キャンセルするには、[cancel] をクリックします。

## 4.2.6 構成済み NIS サーバの優先順位を変更する

構成済み NIS サーバの優先順位を変更するには

1. [Modify NIS Server] 画面に移動します。

[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックして、[NIS/LDAP Configuration] 画面を表示します。画面が表示されたら、[details] をクリックして、[Modify NIS Server] 画面を表示します。



2. 要求された情報を入力します。

[Priority] フィールドで、この NIS サーバの優先度をドロップダウンリストから選択します (最も低い番号が最も高い優先順位です)。



**重要** NIS ドメインに複数の NIS サーバが含まれる場合、システムは再バインドチェックのときに、最も優先度の高い NIS サーバへのバインドを試みます。

3. 設定を適用します。

設定を確認します。適用するには [OK] をクリックします。キャンセルするには、[cancel] をクリックします。

## 4.2.7 NIS サービスを提供するように LDAP を構成する

NIS サービスを提供するように LDAP を構成するには

1. [NIS/LDAP Configuration] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックして、[NIS/LDAP Configuration] 画面を表示します。

Network Configuration | [Home](#) > Network Configuration > NIS/LDAP Configuration

### NIS/LDAP Configuration

EVS Security Context: Global Configuration  
[change...](#)

**LDAP**

Domain:  
User Name:  
TLS: Disabled  
Schema: RFC-2307  
[modify](#)

IP Address	Port	TLS Port	DNS Name	Status	
<input type="checkbox"/> 192.168.2.80	389 [Default]	636 [Default]		<span style="color: green;">●</span> Ok	<a href="#">details</a>

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#) [Switch to using NIS](#) | [Disable NIS and LDAP](#)

Shortcuts: [Name Services Order](#)

[Home](#) | [About](#) | [Sign Out](#)

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS Security Context	現在選択されている EVS セキュリティコンテキスト、つまり、個別セキュリティコンテキストまたはグローバルセキュリティコンテキストを表示します。[change] をクリックして、別の EVS セキュリティコンテキストを選択するか、グローバル構成を選択します。別の EVS セキュリティコンテキストを選択すると、NIS/LDAP 構成設定が適用されるコンテキストが変更されます。
Domain	システムがクライアントである LDAP ドメインの名前。 例：Hitachi Data Systems.com
User Name	この LDAP サーバについて権利と権限を持つ管理者のユーザー名。256 文字までの名前を指定できます。ただし、スペースを含む場合は、名前を二重引用符で囲む必要があります。 例：cn="Directory Manager",dc=server1,dc=com
TLS	TLS 及び SSL 接続を有効または無効にします。
Schema	LDAP サーバで使うスキーマの規格。
IP Address	現在バインドされている NIS サーバの IP アドレス。
Port	管理者が構成できる標準ポート。デフォルトのポートは 389 です。
TLS Port	管理者が構成できるセキュアポート。デフォルトのポートは 636 です。
DNS Name	LDAP サーバの完全修飾ホスト名です。
Status	LDAP サーバのステータスを表示します。

2. 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] 画面には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面で行った NIS/LDAP 構成の変更は、現在選択されている EVS セキュリティコンテキストにのみ適用されます。

- EVS がグローバル構成を使用している場合、NIS/LDAP 構成設定の変更は EVS に影響を与えません。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル NIS/LDAP 構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS の NIS/LDAP 構成設定を変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

[change] をクリックして、別の EVS セキュリティコンテキストを選択するか、グローバル構成を選択します。

### 3. 構成を作成/変更/削除します。

[Actions/Shortcuts] では、次のアクションやショートカットを使用できます。

- LDAP サーバを追加するには：  
[add] をクリックして、「[4.2.8 LDAP サーバを追加する](#)」の説明を参照してください。
- LDAP サーバを削除するには：  
LDAP サーバを選択して、[delete] をクリックします。
- 構成を表示または変更するには：  
[details] をクリックします。「[4.2.9 LDAP 構成を変更する](#)」の説明を参照してください。
- 詳細なプロパティを表示する、または、LDAP サーバのプロパティを変更するには：  
LDAP サーバを選択し、[details] をクリックします。「[4.2.10 LDAP サーバを変更する](#)」の説明を参照してください。
- NIS に切り替えるには：  
[Switch to using NIS] をクリックします。変更は全ての登録されたサーバに適用されます。
- NIS 及び LDAP を無効にするには：  
[Disable NIS and LDAP] をクリックします。変更は全ての登録されたサーバに適用されません。
- ネームサービスの順序を変更するには：  
[Name Services Order] をクリックして、[Name Services Order] 画面に移動し、ネームサービスの順序を指定します。

## 4.2.8 LDAP サーバを追加する

HNAS は LDAP バージョン 2 をサポートします。LDAP サーバを追加するには、次のようにします。

### 1. [Add LDAP Server] 画面に移動します。

[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックして、[NIS/LDAP Configuration] 画面を表示します。画面が表示されたら、[add] をクリックして、[Add LDAP Server] 画面を表示します。

Network Configuration [Home](#) > Network Configuration > NIS Configuration > Add LDAP Server

## Add LDAP Server

Server IP Address or Host Name:

Port:

TLS Port:

[Home](#) | [About](#) | [Sign Out](#)

- [Server IP Address or Host Name] フィールドに、LDAP サーバの IP アドレスまたはホスト名を入力します。  
LDAP サーバの IP アドレスまたは解決可能なホスト名を入力します。
- [Port] フィールドに、LDAP サーバの新しい標準ポート番号を入力します。  
これは、LDAP サーバとの通信に使用される標準ポートです。デフォルトのポートは 389 です。
- [TLS Port] フィールドに、LDAP サーバの新しいセキュアポート番号を入力します。  
これは、LDAP サーバとの通信に使用されるセキュアポートです。デフォルトのポートは 636 です。
- 新しい LDAP サーバ情報を保存します。  
[OK] をクリックします。

## 4.2.9 LDAP 構成を変更する

LDAP 構成を変更するには

- [Modify LDAP Configuration] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] をクリックし、[NIS/LDAP Configuration] 画面を表示します。画面が表示されたら、[modify] をクリックして、[Modify LDAP Configuration] 画面を表示します。

Network Configuration [Home](#) > Network Configuration > NIS/LDAP Configuration > Modify LDAP Configuration

## Modify LDAP Configuration

Domain:

User Name:

Password:

TLS Enabled:

Schema:

[Home](#) | [About](#) | [Sign Out](#)



**重要** このオプションは、登録済みユーザーと匿名ログインユーザーの両方をサポートします。

- 要求された情報を入力します。
  - [Domain], [User Name], 及び [Password] フィールドを編集します。

- TLS を有効または無効にするには、[TLS Enabled] チェックボックスをオンまたはオフにします。
  - [Schema] ドロップダウンリストを利用して、LDAP サーバで使うスキーマの規格を次のオプションから選択します。
    - RFC-2307
    - MS Services for Unix
    - MS Identity Management for Unix
3. 構成を適用します。
- 構成が正しいことを確認します。設定を適用するには [OK] をクリックします。キャンセルするには、[cancel] をクリックします。

## 4.2.10 LDAP サーバを変更する

LDAP サーバのプロパティを変更するには

1. [Modify LDAP Server] 画面に移動します。  
[Network Configuration] 画面で [NIS/LDAP Configuration] を選択し、変更する LDAP サーバ構成を選択して、[details] をクリックし、[Modify LDAP Server] 画面を表示します。

2. 現在の構成情報を変更／更新します。
  - a. [Server IP Address or Host Name] フィールドに、LDAP サーバの新しい IP アドレスまたは新しいホスト名を入力します。
  - b. [Port] フィールドに、LDAP サーバの新しい標準ポート番号を入力します。  
これは、LDAP サーバとの通信に使用される標準ポートです。デフォルトのポートは 389 です。
  - c. [TLS Port] フィールドに、LDAP サーバの新しいセキュアポート番号を入力します。  
これは、LDAP サーバとの通信に使用されるセキュアポートです。デフォルトのポートは 636 です。
3. 構成を適用します。  
構成が正しいことを確認します。設定を適用するには [OK] をクリックします。キャンセルするには、[cancel] をクリックします。

## 4.2.11 ネームサービスの順序を変更する

ネームサービスが使用される順序を変更するには

1. [Name Services Order] 画面に移動します。  
[Home] 画面で [Network Configuration] を選択し、[Name Services Order] をクリックします。

## Name Services Order



- 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面で行ったネームサービスの順序の変更は、現在選択されている EVS セキュリティコンテキストにのみ適用されます。

- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のネームサービスの順序設定を変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

[change] をクリックして、別の EVS セキュリティコンテキストを選択するか、グローバル構成を選択します。

- 使用するネームサービスを選択します。

[Available Name Services] リストから、使用するネームサービスを選択し、右向き矢印をクリックします。

- ネームサービスの順序を設定します。

[Selected Name Services] リストには、使用される順序でネームサービスが表示されます。リストの上の方にあるネームサービスは、リストの下の方にあるネームサービスより先に使用されます。

リスト内のネームサービスの位置を変更するには、ネームサービスを選択して、上矢印または下矢印を使用して、そのネームサービスが使用される順序を変更します。

- 設定を適用します。

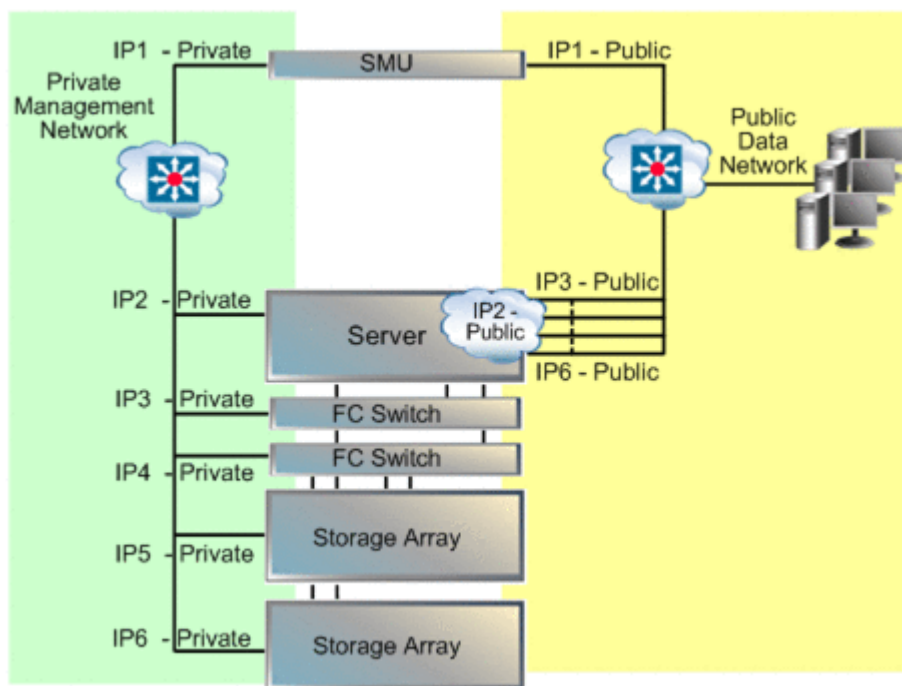
設定を確認します。適用するには [apply] をクリックします。

## 内部 LAN

- 5.1 内部 LAN の構成

## 5.1 内部 LAN の構成

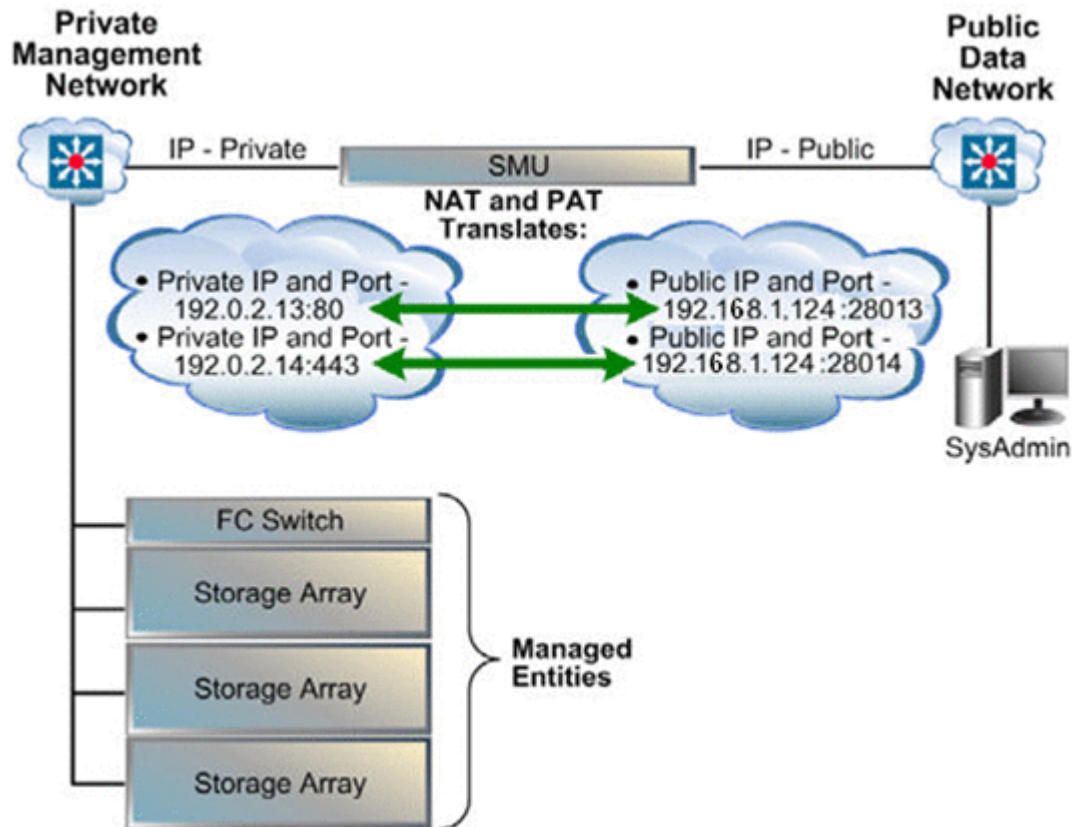
HNAS は、Fibre Channel スイッチ、ストレージシステムなど、主にイーサネットを通じて管理される多数の補助デバイスと連携して動作します。企業内 LAN への影響を最小化するために、SMU は Network Address Translation (NAT) 及び Port Address Translation (PAT) を使用して、SMU が窓口になることで、補助デバイスを企業内 LAN から切り離します。



例えば、内部 LAN 内のデバイスに対する HTTP 要求は、実際には、SMU の管理 LAN (*eth0*) IP アドレスと NAT ポート (例: 192.168.1.124:28013) に対して行われます。SMU はこの要求を、内部 LAN 上のデバイスのプライベート IP アドレスと HTTP ポート (例: 192.0.2.13:80) に変換してデバイスに送信します。

内部 LAN の IP アドレス範囲には、SMU の内部 LAN (*eth1*) IP アドレスの最初の三つのオクテットが共通する IP アドレスだけが含まれます。例えば、SMU 内部 LAN IP アドレスが「192.0.2.1」の場合、内部 LAN 上のデバイスのアドレスは、「192.0.2.2」～「192.0.2.254」の範囲内であることが必要です。





内部 LAN を独立させることにより、次のような大きな利点があります。

- SMU による HNAS と補助デバイスの通常の監視に必要なネットワークトラフィックが、企業内 LAN 上で発生しません。
- 内部 LAN 上のデバイスは、データ LAN の貴重な IP アドレスを消費しません。
- SMU は内部 LAN 上の全てのデバイスを発見できるので、セットアップが容易になります。
- 内部 LAN はデータ LAN よりセキュアです。

内部 LAN の代わりに、補助デバイスの一部または全部をデータ LAN に置くこともできます。このような構成では、一部の補助デバイスを内部 LAN に隔離したシステムと、他の補助デバイスをデータ LAN に置くシステムとを混在することができます。



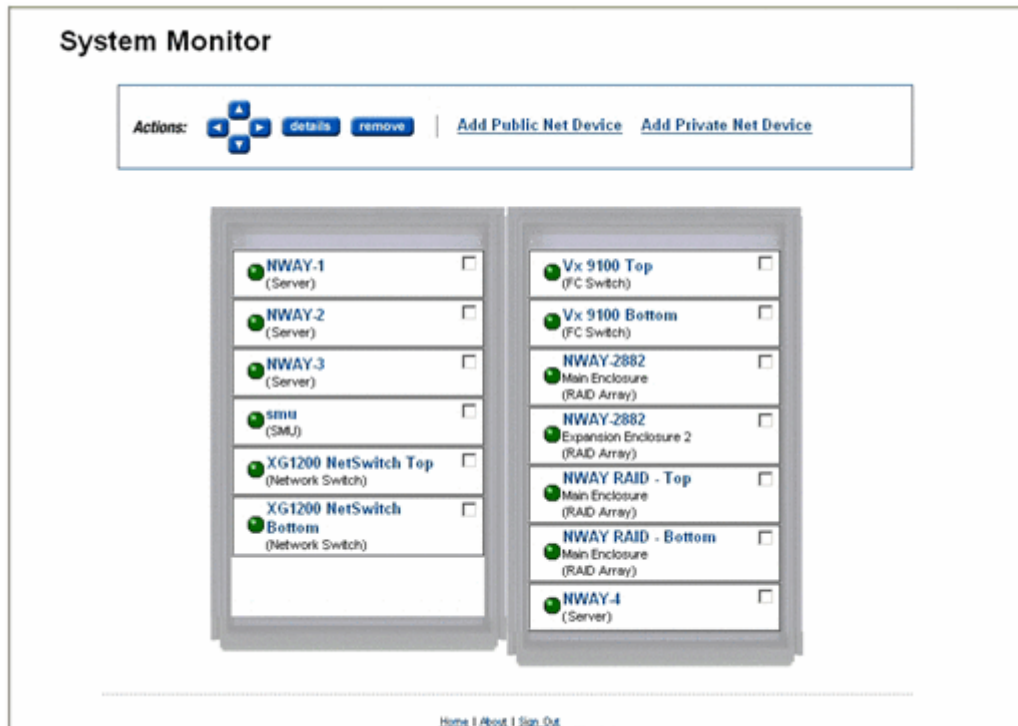
**重要** データ LAN 上のデバイスは、ネットワーク内の静的 IP アドレスを必要とします。

### 5.1.1 System Monitor 上のデバイスを構成する

[System Monitor] 画面で、HNAS を構成するデバイスを容易に表示し、監視することができます。

[System Monitor] 画面でデバイスを構成するには

1. [System Monitor] 画面に移動します。  
[Home] 画面で [System Monitor] をクリックして、[System Monitor] 画面を表示します。



- 任意に [System Monitor] 画面のデバイスを並べ替えることができます。  
デバイスの位置を変えるには、チェックボックスをオンにしてから、[Action] セクションの矢印を使用します。
- 任意に [System Monitor] 画面のデバイスのステータスまたは詳細を表示することができます。  
次の表の行には、HNAS システムを構成する基本的デバイスが一覧表示されています。この表は、デバイスリストのデバイスの名前をクリックしたときの動作を示しています。

デバイス/説明	デバイスをクリックしたとき	[details] ボタンをクリックしたとき
<b>ノード</b> このデバイスは、ネットワークへの複数の Gigabit Ethernet インターフェースと、メインエンクロージャへの複数の Fibre Channel インターフェースを備えています。クラスタ構成では、最大四つのノードを登録できます。	[Cluster Node] 画面をロードします。	
<b>SMU</b> System Management Unit	[SMU Status] 画面をロードします。	
<b>NDMP バックアップデバイス</b> HNAS はバックアップデバイスを自動的に検出して、システムモニターに追加します。HNAS は他のサーバと共有される FC ネットワークに接続されることもあるので、FC リンクで検出されたバックアップデバイスを自動的に利用しません。バックアップデバイスは、自動的に発見され、Status Monitor に追加されます。	[NDMP Devices] 画面をロードします。	デバイスと通信できる場合は、デバイスの [NDMP Details] 画面をロードします。デバイスと通信できない場合は、[NDMP Device List] 画面をロードします。
<b>FC スイッチ</b> FC スイッチ (及びケーブル) は、FC デバイス (一般にストレージアレイ) を HNAS に接続します。 注：	スイッチが追加されたときに指定されたプロトコルに応じて、スイッチの組み込み管理ユーティリティまたは	[FC Switch Details] 画面をロードします。

デバイス/説明	デバイスをクリックしたとき	[details] ボタンをクリックしたとき
[FC Switches] 画面で FC スイッチを追加すると、System Monitor に自動的に追加されます。	スイッチの [FC Switch Details] 画面をロードします。FC スイッチを追加する方法については、『 <i>Server and Cluster Administration Guide</i> 』を参照してください。	

4. 任意に、デバイスを追加、削除、または詳細を表示することができます。
- [Actions] では、選択したデバイスに対して、次のアクションを適用できます。
- デバイスを削除するには、[remove] をクリックします。
  - 特定のデバイスに関する詳細を表示するには、[details] をクリックします。
  - データ LAN に存在するデバイスを追加するには、[Add Public Net Device] をクリックします。
  - 内部 LAN に存在するデバイスを追加するには、[Add Private Net Device] をクリックします。



**重要** 内部 LAN 上のデバイスは、Network Address Translation (NAT) によってデータネットワークから隠されます。

デバイスが System Monitor に追加された後、System Monitor でデバイス名をクリックすると、次のようになります。

- HTTP, HTTPS, または Telnet を使用して、各デバイスの (内蔵の) 管理ユーティリティが Web ブラウザで開きます。
- SMU はデバイスのアクティビティと HNAS の接続を定期的にチェックします。デバイスがネットワークの ping に応答しなかった場合、System Monitor はデバイスの色を赤色に変え、SMU はアラートを発行します (SMU に SNMP トラップを送信するようにデバイスを構成することもできます)。
- SMU にデバイスの MIB がある場合、デバイスからのイベントがイベントログに追加されます。

