



Luxul L2/L3ネットワークスイッチ 取扱説明書

対象モデル: XMS-2624P, XMS-5248P, XMS-7048P
AMS-1208P, AMS-2616P, AMS-2624P, AMS-4424P
AMS-2600

- ▶ 基本的な設置方法
- ▶ 基本的なシステム設定
- ▶ IP設定とルーティング
- ▶ PoE
- ▶ VLANs
- ▶ プライベートVLAN
- ▶ スパニングツリー

LUXUL

目次

■はじめに	1
■基本的な設置方法	2
ラックの取り付け	2
イーサネットと電源の接続	2
ネットワークケーブル接続	2
IPアドレスの設定	3
接続	3
ログイン	3
■ネットワークスイッチの基本	5
■基本的な設定方法: システム	6
System	6
Information	6
IP	7
NTP	9
Time	10
Log	12
■POEについて	14
■基本的な設定方法: POE	15
■VLANについて	17
■基本的な設定方法: VLAN	18
グローバルVLAN設定	18
ポートVLAN設定	19
VLANの許可	20
VLANの禁止事項	20
■基本的な設定方法: プライベートVLAN	21
VLANメンバーシップ	22
VLANポートの分離	23
■スパンニングツリーについて	24
■基本的な設定方法: スパンニングツリー	25
ブリッジ設定	25
MSTIマッピング	27
MSTIの優先順位	28
CISTポート	29
MSTIポート	31
変更した設定を起動時に適用するには	33

はじめに

本書は、内蔵のWebインターフェースを使用したLuxulネットワークスイッチのインストールと基本的なセットアップについて説明します。

- ▶AMS-2600
- ▶AMS-1208P,AMS-2616P,AMS-2624P,AMS-4424P
- ▶XMS-2624P,XMS-5248P,XMS-7048P

注意: このガイドでは、複数の異なるLuxul L2/L3ネットワークスイッチについて説明します。このガイドに記載されているすべての機能が、スイッチのすべてのモデルに適用されるわけではありません。モデル固有の機能については、**個々の仕様をご確認ください。**



本書は、ネットワークの基本的な概念について十分な実践的知識があり、ネットワークスイッチとその機能に精通していることを前提としています。ネットワークスイッチ、ルーティング、およびその他の高度なネットワークングの概念に精通していない場合は、Luxulネットワークスイッチを設定する前に、これらの概念を理解しておくことをお勧めします。

luxul.com/educational-webinarsにアクセスすると、基本ネットワークワーキングからリモートアクセス、VPN、ルーティング、VLANなどの比較的高度なトピックまで、有益なオンラインセミナーがあります。

■安全上のご注意

取扱説明書には、お使いになる方や他の人への危害と財産の損害を未然に防ぎ、安全に正しくお使いいただくために、重要な内容を記載しています。以下の注意事項をよくお読みの上、正しくお使いください。

注意事項は危険や損害の大きさと切迫の程度を明示するために、誤った扱いをすると生じることが想定される内容を次の定義のように「警告」「注意」の二つに区分しています。

 警告	この表示を無視して誤った取り扱いをすると、死亡または重傷を負う可能性が想定される内容です。
 注意	この表示を無視して誤った取り扱いをすると、傷害を負う可能性または物的損害が発生する可能性が想定される内容です。

警告

- 水に入れたり、ぬらしたりしないでください。火災や感電の原因になります。
- AC100V 50/60Hz の電源で使用してください。これ以外の電源では、火災や感電の原因となります。
- 必ず専用の電源コードを使用してください。これ以外のものを使用すると火災の原因となります。
- 付属の電源ケーブルを他の製品に使用しないでください。
- 電源コードの上に重い物をのせたり、熱器具に近づけたり、無理に引っ張ったりしないでください。コードが破損して火災や感電の原因になります。電源コードが傷んだら（断線や芯線の露出など）、直ちに使用を中止し販売店に交換をご依頼ください。
- 水が入った容器や金属片などを、機器の上に置かないでください。こぼれたり、中に入ったりすると、火災や感電の原因となります。
- 万一、落したり筐体を破損した場合は、直ちに使用を中止し、修理を依頼してください。そのまま使用すると、火災の原因となります。
- 雷が鳴り出したら、金属部分や電源プラグに触れないでください。感電の恐れがあります。
- 煙がでる、異臭がする、水や異物が入った、破損した等の異常がある時は、ただちに電源プラグをコンセントから抜き、修理を依頼してください。異常状態のまま使用すると、火災や感電の原因となります。
- 分解や改造は行わないでください。お客様が保守できる部品は、内部にはありません。分解や改造は保証期間内でも保証の対象外となるばかりでなく、火災や感電の原因となります。

注意

- 不安定な場所に設置しないでください。落下によるけがの原因となります。
- 以下のような場所に設置しないでください。
 - ・ 直射日光の当たる場所
 - ・ 湿気の多い場所
 - ・ 温度の特に高い場所、または低い場所
 - ・ ほこりの多い場所
 - ・ 振動の多い場所
- 機器をラックに設置する場合は、必ず専用のラックマウント金具（オプション）を使用し、重量を支えるために全てのネジをしっかりと固定してください。落下すると、けがや器物を破損する原因となります。
- 配線は、電源コードを抜いてから説明書に従って正しく行ってください。電源コードを差し込んだまま配線すると、感電する恐れがあります。また、誤配線によるショート等は火災の原因となります。
- 電源を入れる前に、音量を最小にしてください。突然大きな音が出て聴覚障害などの原因となります。
- 機器の移動は、電源プラグをコンセントから抜き、他の機器との接続を全て外してから行ってください。
- ぬれた手で電源プラグを抜き差ししないでください。感電の原因となります。
- 電源プラグを抜くときに、電源コードを引っ張らないでください。コードが傷つき火災や感電の原因となります。

■はじめに

このたびは本製品をご購入いただき、誠にありがとうございます。

まずこちらの取扱説明書をお読みいただき、性能をご理解いただいた上で用途に応じた最適な使用方法を追求してください。

保証について

- ・ 保証書は必ず「お買い上げ年月日」「お買い上げ店名 / 所在地」の記入をご確認いただき、製品とともにお受け取りください。お買い上げ日より 2 年間は保証期間です。保証書記載事項に基づき、無償修理等を保証させていただきます。修理等はお買い上げの販売店までご依頼ください。
- ・ お買い上げ時に「お買い上げ年月日」「お買い上げ店名 / 所在地」が正しく記入されていない場合は、保証書が無効になり、無償修理を受けられないことがあります。記載内容が不十分でしたら、速やかに販売店にお問い合わせください。
- ・ 改造など通常の使用範囲を超えた取扱いによる故障や、設計・製造以外の要因で起きた不都合は期間内であっても保証の対象外となります。

故障かな？と思われる症状が出たときには

こちらの取扱説明書をもう一度お読みになり、接続や操作などをご確認ください。それでも改善されないときはお買い上げの販売店までお問い合わせください。調整・修理いたします。

目次

■はじめに	1
■基本的な設置方法	2
ラックの取り付け	2
イーサネットと電源の接続	2
ネットワークケーブル接続	2
IPアドレスの設定	3
接続	3
ログイン	3
■ネットワークスイッチの基本	5
■基本的な設定方法: システム	6
System	6
Information	6
IP	7
NTP	9
Time	10
Log	12
■POEについて	14
■基本的な設定方法: POE	15
■VLANについて	17
■基本的な設定方法: VLAN	18
グローバルVLAN設定	18
ポートVLAN設定	19
VLANの許可	20
VLANの禁止事項	20
■基本的な設定方法: プライベートVLAN	21
VLANメンバーシップ	22
VLANポートの分離	23
■スパンニングツリーについて	24
■基本的な設定方法: スパンニングツリー	25
ブリッジ設定	25
MSTIマッピング	27
MSTIの優先順位	28
CISTポート	29
MSTIポート	31
変更した設定を起動時に適用するには	33

はじめに

本書は、内蔵のWebインターフェースを使用したLuxulネットワークスイッチのインストールと基本的なセットアップについて説明します。

▶AMS-2600

▶AMS-1208P,AMS-2616P,AMS-2624P,AMS-4424P

▶XMS-2624P,XMS-5248P,XMS-7048P

注意: このガイドでは、複数の異なるLuxul L2/L3ネットワークスイッチについて説明します。このガイドに記載されているすべての機能が、スイッチのすべてのモデルに適用されるわけではありません。モデル固有の機能については、個々の仕様をご確認ください。

本書は、ネットワークの基本的な概念について十分な実践的知識があり、ネットワークスイッチとその機能に精通していることを前提としています。ネットワークスイッチ、ルーティング、およびその他の高度なネットワークングの概念に精通していない場合は、Luxulネットワークスイッチを設定する前に、これらの概念を理解しておくことをお勧めします。

luxul.com/educational-webinarsにアクセスすると、基本ネットワークワーキングからリモートアクセス、VPN、ルーティング、VLANなどの比較的高度なトピックまで、有益なオンラインセミナーがあります。

基本的な設置方法

ネットワークスイッチの設定を開始する前に、安全で安定した場所に設置し、ネットワークに接続するか、ネットワークスイッチにコンピューターを接続して設定する必要があります。Luxulスイッチをすでにインストールし、ネットワークを接続して、コンピューターからアクセスできる場合は、6ページの「基本的な設定方法:システム」というタイトルの次の章に進みます。

① 機器の設置手順

Luxul AMSおよびXMSシリーズのネットワークスイッチは、ラックに取り付ける必要があります。損傷を防ぐため、安定した安全なラックに設置してください。

適切な通気と放熱のために、ネットワークスイッチの周囲に十分な空間を確保してください。直射日光の当たる場所に置かないでください。ネットワークスイッチの上に重い物を置かないでください。また、コンセントのアース接続が正しく機能していることを確認してください。

ラックの取り付け

同梱のラックマウントブラケットは、19インチサーバーラックまたはオーディオラックへの設置に最適です。付属のネジを使用して、L型ブラケットを本体の両側に取り付け、ラック内の空きスペースに水平に設置します。必要に応じてサポートアングルなどをご使用ください。

② イーサネットと電源の接続

イーサネットと電源の接続

RJ-45ケーブルを使用して、サーバー、ルーター、その他のスイッチを含むイーサネット対応デバイスにスイッチを接続します。クロスケーブルは不要です。

AMSおよびXMSシリーズスイッチは、10/100/1000Mbpsイーサネット、10/100Mbps半二重/全二重モード、および1000Mbps全二重モードをサポートしています。すべてのRJ-45ポートはAuto MDI/MDIXをサポートし、通常のポートまたはアップリンクポートとして使用できます。

背面パネルには、AC入力ソケットと電源スイッチがあります。付属の電源ケーブルを使用して、本体をサージ防護されたコンセントに接続します。

ネットワークケーブル接続

RJ-45ポートに接続するには、CAT-5、CAT-5e、またはCAT-6シールドなしツイストペアを使用できます。最高のパフォーマンスと1000Mbpsでの安定したデータ転送を保証するには、CAT-6シールド付きツイストペアを使用してください。SFPポートに接続する場合は、使用するSFP光モジュールのスペクトルに合わせて光ファイバーケーブルを選択してください。

注意: 複数のアップリンクチャンネルによってループが作成され、ネットワーク障害が発生する可能性があります。スイッチ間、またはスイッチとルーター間に1つのアップリンクチャンネルのみが存在することを確認します。

注意: 電源投入時、SFP光インターフェースに対応するポートLEDが初期化されるまでに少し時間がかかる場合があります。これは、スイッチの初期化と起動の正常な動作です。

注意: ネットワークスイッチの最適なパフォーマンスのために、PoEスイッチに接続されているすべての外部PoEデバイスの合計消費量を超えないようにしてください。(AMS-1208Pの場合は130W、AMS-2616PおよびAMS-2624Pの場合は250w、AMS-2624PおよびXMS2624Pの場合は370W、XMS-5248PおよびXMS-7048Pの場合は740W)

③アクセスの準備

IPアドレスの設定

Luxulネットワークスイッチが192.168.0.Xアドレススキームのネットワークに接続されていて、コンピューターも同じサブネット上でIPアドレスを設定している場合は、次の手順「アクセスとセットアップ」に進むことができます。

注意: ネットワーク上の別のデバイスがスイッチのデフォルトIPアドレスと同じIPアドレスを共有している場合は、スイッチの設定をする間、そのデバイスに一時的に別のアドレスを割り当てるかまたはケーブルを抜いて切断する必要があります。

もしネットワークを192.168.0.X以外のアドレススキームで使用する場合は、スイッチの設定に使用するコンピューターを一時的にスタティックIPアドレスで設定する必要があります。その場合、コンピューターのIPアドレスを192.168.0.Xの範囲のアドレスに設定します(スイッチと同じアドレスではありません)。次にゲートウェイのアドレスを、使用するスイッチのIPアドレスと同じに設定します(下の表を参照)。これで「アクセスとセットアップ」に進むことができます。

スイッチの設定が完了したら、コンピューターのIPアドレス設定を通常の「自動/DHCP取得」に戻すことができます。

注意: コンピューターのIPアドレスの変更と接続の詳細については、<http://luxul.com/ip-addressing/>にアクセスしてください。

④アクセスとセットアップ

接続

イーサネットケーブルを使用してコンピューターをスイッチに接続し、スイッチの電源を入れます。

ログイン

LuxulネットワークスイッチのWeb設定にアクセスするには、Webブラウザを開き、アドレスフィールドにデフォルトのIPアドレスを入力します(以下の表を参照)。デフォルトのユーザー名とパスワードを使用してスイッチにログインします。

デフォルトIP:(下表参照)

ユーザー名: admin

パスワード: admin

設定する機器のデフォルトIPアドレスは、次の表を参照してください。

モデル名	デフォルトのIPアドレス
AMS-2600	192.168.0.2
AMS-1208P	192.168.0.3
AMS-2616P, AMS-2624P, AMS-4424P, XMS-2624P, XMS-5248P, XMS-7048P	192.168.0.4

本機のWeb設定にログインしたら、次の章「基本的な設定方法: システム」の説明に従って設定を続行します。

⑤ハードウェア操作

AMSシリーズの前面パネルには、緑色から青色に切り替わる2色のLink/Act LEDインジケータがあります。さらに前面パネルには、1000MbpsおよびPoEモードを確認できるLEDインジケータと、システムおよび電源LEDインジケータがあります。

インジケータ	状態	説明
電源	点灯	本機の電源がオンになっています。
	消灯	電源が切れているか、AC電源に接続されていません。背面パネルの電源接続と電源スイッチを確認します。
Link/Act	点灯	ポートにデバイスが接続されています。
	点滅	ポートはデータの送受信中です。
	消灯	ポートにデバイスが接続されていません。
1000 Mbps	点灯	1000Mbps対応デバイスが接続されています。
	消灯	デバイスが接続されていないか、デバイスが1000Mbps対応ではありません。
PoE	点灯	PoE対応デバイスが接続されていて、本機がデバイスに電源を供給しています。
	消灯	PoE対応デバイスが接続されていないか、PoEがこのポートで有効になっていません。
SYSTEM	点灯	本機が起動中です。
	点滅	スイッチは正常に動作しています。
	消灯	本機が起動および初期化プロセス中であるか、オンになっていません。
起動時、ポートLEDはセルフテストのため1秒間点滅します。		

ネットワークスイッチの基本

新しく本機のセットアップを開始する前に、いくつかの高度なネットワークに関する基本的な知識があると便利です。本書では、基本的なネットワークングをすでに理解していることを前提としています。基本を理解していない場合は、luxul.com/educational-webinarsにアクセスして、IPネットワークングの基本、有線、ワイヤレスネットワークングから、リモートアクセスやゲストネットワークアクセスのためのVLANの使用などの高度なトピックまで、さまざまなテーマに関する有益なオンラインセミナーをご覧ください。

ネットワークスイッチとは？

基本的にネットワークスイッチは、コンピューターネットワーク上で複数のデバイスを接続し、あるデバイスから別のデバイスにデータを受信、処理、転送します。単純なネットワークHUBとは異なり、スイッチは、各ポートから同じデータをブロードキャスト転送するのではなく、受信する必要があるデバイスにのみデータを転送できます。

レイヤーとは？

技術的な詳細は別として、ネットワークにおける「レイヤー」は、異なるレベルの機能と操作の標準を説明しています。

- ▶レイヤー1のスイッチは、最も基本的なもので、物理層で機能し、デバイスを相互に接続します。
- ▶レイヤー2のスイッチは、データリンク層と連携し、ハードウェアを使用してマルチポートブリッジのように機能します。
- ▶レイヤー3のスイッチは、ネットワーク層で機能し、アドレス指定、ルーティング、トラフィック制御などのマルチノードネットワークを管理します。レイヤー3のスイッチは、3つのスイッチの中で最も能力が高く、ルーターに非常によく似た機能を提供しますが、より多くの物理ポートを備えています。

スイッチには、データリンク層とネットワーク層を含む1つ以上のレイヤーで動作するものがあります。複数のレイヤーで同時に動作するデバイスは、マルチレイヤースwitchと呼ばれます。本書で紹介するLuxulネットワークスイッチは、マルチレイヤースwitchです。

管理型と非管理型

ネットワークスイッチには、管理型と非管理型の2つの基本タイプがあります。非管理型スイッチには設定インターフェースやパラメーターがなく、一般的にプラグアンドプレイタイプです。ほとんどの非管理型スイッチは、設定を必要としないため、レイヤー1スイッチです。

管理型スイッチには、スパニングツリープロトコルやポートミラーリング、仮想LAN(VLAN)の作成や変更など、管理機能が含まれていルーターめ、通常はレイヤー2またはレイヤー3スイッチです。本書の対応モデルは、レイヤー3管理型スイッチです。

管理型スイッチの動作を基本的に理解してから設定を始めましょう。

基本的な設定方法:システム

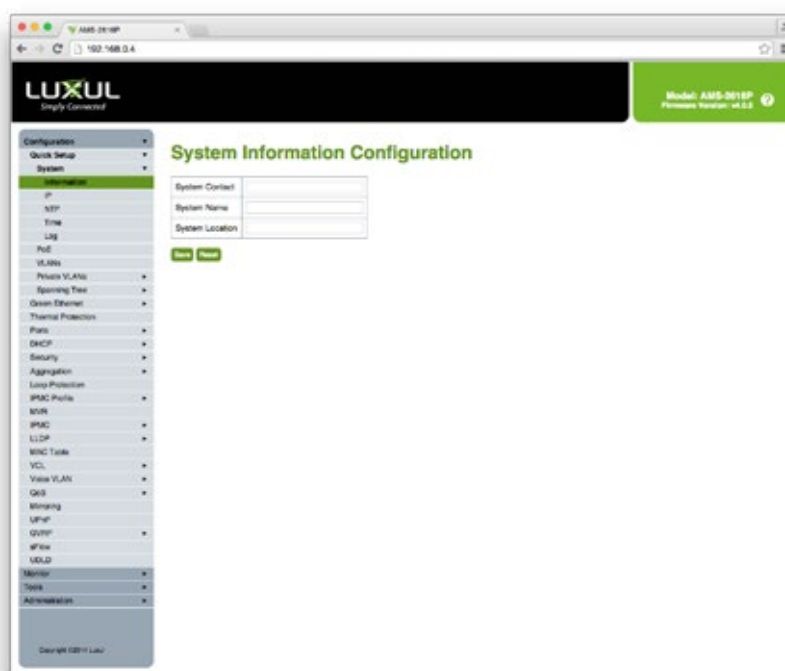
この章では、情報、IP、NTP、時刻、ログなど、設定インターフェースのSystemセクションにある機能の設定について説明します。

System

System Contact(システムの連絡先)、System Name(システム名)、System Location(システムの場所)などのシステム情報を構成することで、スイッチの場所や機能を簡単に識別できます。これは、複数の場所に複数のスイッチを設置する場合に特に役立ちます。

Information

システム情報設定にアクセスするには、下図の左側にあるナビゲーションメニューで Configuration>Quick Setup>System>Information の順にクリックします。



システム情報の設定画面

System Contact: 本機の管理者の名前や連絡先情報。0～128文字で入力できますが、スペースは使用できません。

System name: 本機の識別を容易にするために割り当てる名称です。ここで設定した名称は、ローカルネットワーク上のスイッチのホスト名としても使用されます。0～128文字で入力でき、標準のホスト名規則に従います。使用できる文字は、数字、アルファベットの大文字、小文字、ハイフンです。

スペースや特殊文字(!@#\$など)は使用できません。ホスト名の最初の文字はアルファベット文字でなければならず、最後の文字はハイフンであってはなりません。

System Location: スwitchの設置場所（例: Telephone Closet、3rd floor）。0～128文字で入力でき、スペースを含むすべての文字が入力可能です。

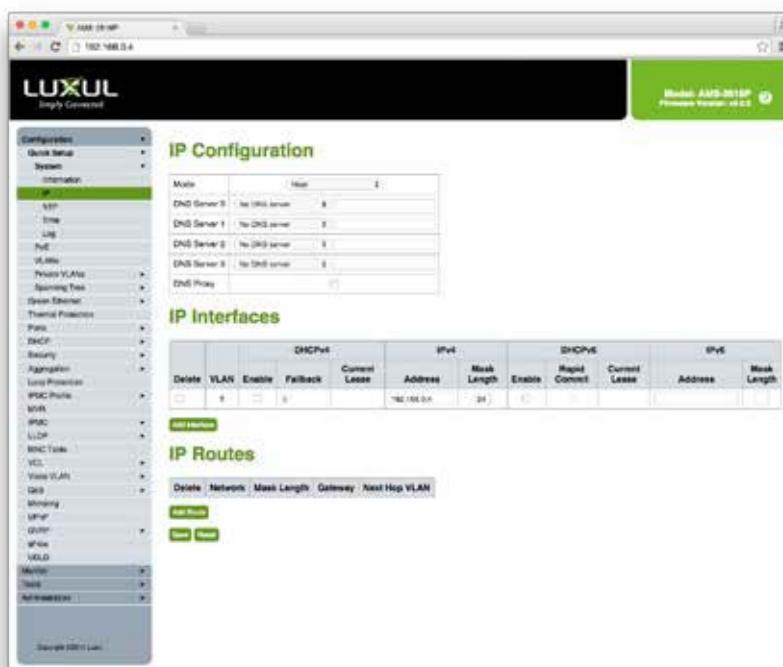
▶**Save**: 未保存の変更を保存します。

▶**Reset**: 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

IP

本機のIPアドレスは、デフォルトで192.168.0.4（またはAMS-1208Pの場合は192.168.0.3）に設定されています。IPアドレスは、VLAN1のDHCPサーバー経由でも取得できます。カスタムIPアドレスを手動で設定するには、本機のデフォルト設定をネットワークと互換性のあるアドレスに変更します。また、DNSサーバーとデフォルトゲートウェイを設定し、本機が日時情報を取得できるようにすることをお勧めします。

IP設定を構成するには、ナビゲーションメニューからConfiguration>Quick Setup>System>IPを選択します。



IP設定画面

IP設定

Mode: IPスタックをホストとして動作させるかルーターとして動作させるかを設定します。ホストモードでは、インターフェース間のIPトラフィックはルーティングされません(VLANを含みます)。ルーターモードでは、トラフィックはすべてのインターフェース(VLANを含みます)間でルーティングされます。

DNS Server: 本機のDNS(Domain Name System)機能を設定します。以下のモードがサポートされています。

- ▶**From any DHCPv4 interfaces**: DHCPリリースからDHCPv4対応インターフェースに提供された最初のDNSサーバーが使用されます。
- ▶**No DNS server**: DNSサーバーは使用しません。
- ▶**Configured IPv4**: DNSサーバーのIPアドレス(IPv4)を指定できます。
- ▶**From this DHCPv4 interface**: 提供されたDNSサーバーをどのDHCPv4対応インターフェースから構成するかを指定します。

- ▶ **From any DHCPv6 interfaces:** DHCPリースからDHCPv6対応インターフェースに提供された最初のDNSサーバーが使用されます。
- ▶ **Configured IPv6:** DNSサーバーのIPアドレス (IPv6) を指定できます。
- ▶ **From this DHCPv6 interface:** 提供されたDNSサーバーをどのDHCPv6対応インターフェースから構成するかを指定します。
- ▶ **DNS Proxy:** DNSプロキシを有効にすると、本機は設定されたDNSサーバーにDNS要求を中継し、本機を経由して接続されているクライアント機器にDNSリゾルバとして応答します。

IPインターフェース

Delete: 既存のIPインターフェースを削除します。

VLAN: このIPインターフェースに関連付けられたVLANです。このVLAN内のポートのみがこのIPインターフェースにアクセスできます。このフィールドは、新しいインターフェースを作成するときのみ入力に使用できません。

DHCPv4

- ▶ **DHCPv4 – Enable:** このチェックボックスをオンにしてDHCPクライアントを有効にします。有効にすると、本機はDHCPサーバーを使用してインターフェースのIPv4アドレスとマスクを構成します。DHCPクライアントは、ローカルDNSルックアップを提供するために、構成されたシステム名をホスト名としてアナウンスします。
- ▶ **DHCPv4 – Fallback:** 本機がDHCPリースを取得しようとする秒数です。この期間が経過すると、構成されたIPv4アドレスがIPv4インターフェースアドレスとして使用されます。ゼロの値はフォールバックメカニズムを無効にし、有効なDHCPリースが取得されるまで再試行を続けます。使用可能な範囲は0～4294967295秒です。
- ▶ **DHCPv4 – Current Lease:** アクティブなリースを持つDHCPインターフェースの場合、この列には、DHCPサーバーによって提供される現在のインターフェースアドレスが表示されます。
- ▶ **IPv4 – IPv4 Address:** インターフェースのスタティックIPv4アドレス(デフォルトで192.168.0.4に設定)です。インターフェース上でIPv4操作が不要な場合は、このフィールドを空白のままにすることができます。DHCPが有効な場合、このフィールドは使用されません。
- ▶ **IPv4 – Mask Length:** IPv4ネットワークマスクのビット数 (CIDR表記とも呼ばれます) です。有効な値は、IPv4アドレスの0～30ビットです。インターフェース上でIPv4操作が不要な場合は、このフィールドを空白のままにすることができます。DHCPが有効な場合、このフィールドは使用されません。

DHCPv6

- ▶ **DHCPv6 – Enable:** このチェックボックスをオンにしてDHCPクライアントを有効にします。有効にすると、本機はDHCPサーバーを使用してインターフェースのIPv6アドレスとマスクを構成します。DHCPクライアントは、ローカルDNSルックアップを提供するために、構成されたシステム名をホスト名としてアナウンスします。
- ▶ **DHCPv6 – Rapid Commit:** 新しいリースがインターフェースに通知されるとすぐに、本機がIPv6アドレスを変更できるようにします。
- ▶ **DHCPv6 – Current Lease:** アクティブなリースを持つDHCPインターフェースの場合、この列には、DHCPサーバーによって提供される現在のインターフェースアドレスが表示されます。

IPv6

- ▶ **IPv6 – Address:** インターフェースのスタティックIPv6 (デフォルトでは192.168.0.4が設定されています)。インターフェース上でIPv6操作が不要な場合は、このフィールドを空白のままにすることができます。
- ▶ **IPv6 – Mask Length:** IPv6ネットワークマスクのビット数 (CIDR表記とも呼ばれます) です。有効な値は、IPv6アドレスの1～128ビットです。インターフェース上でIPv6操作が不要な場合は、このフィールドを空白のままにすることができます。

IPルート

Delete: 既存のIPルートを削除します。

Network: このルートの宛先IPネットワークまたはホストアドレスです。有効な形式は、標準IPv4またはIPv6表記です。デフォルトでは、値0.0.0.0またはIPv6::表記を使用できます。

Mask Length: 宛先IPネットワークまたはホストマスクのビット数（CIDR表記とも呼ばれます）です。有効な値は、IPv4ルートの場合は0～32ビット、IPv6ルートの場合は0～128ビットです。デフォルトルートのみマスク長が0になります。

Gateway: ルートゲートウェイのIPアドレス。有効な形式は、標準IPv4またはIPv6表記です。ゲートウェイとネットワークは同じサブネット内にある必要があります。

Next Hop VLAN(IPv6のみ): ゲートウェイに関連付けられている特定のIPv6インターフェースのVLAN ID(VID)です。指定されたVIDの範囲は1～4094で、対応するIPv6インターフェースが有効な場合にのみ有効です。IPv6ゲートウェイアドレスがリンクローカルアドレスの場合、ゲートウェイのネクストホップVLANを指定する必要があります。

IPv6ゲートウェイアドレスがリンクローカルアドレスでない場合、本機はネクストホップVLANを無視します。

▶**Add Interface:** Add Interfaceをクリックして、新しいIPインターフェースを追加します。最大8つのインターフェースがサポートされます。

▶**Add Route:** Add Routeをクリックして、新しいIPルートを追加します。最大32のルートがサポートされます。

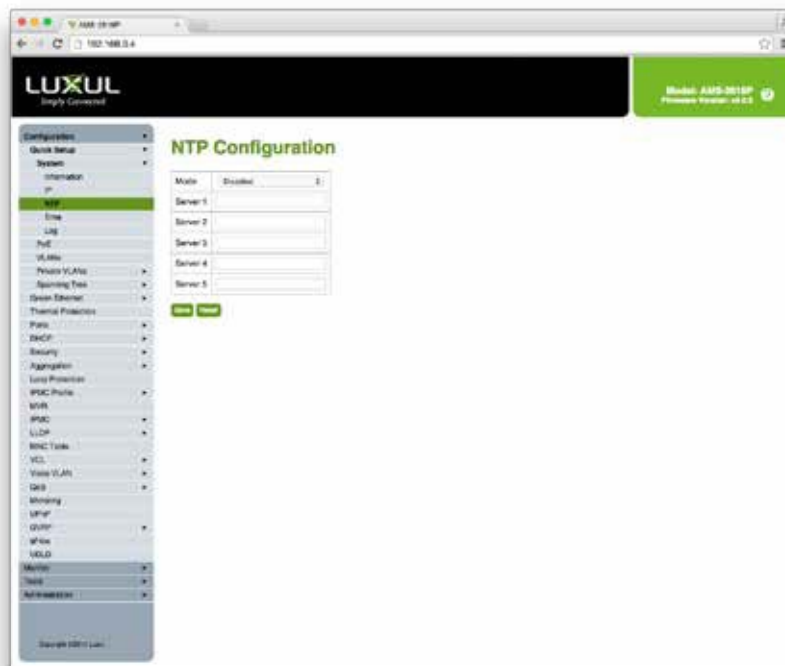
▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

NTP

NTP(Network Time Protocol)は、グリニッジ標準時(GMT)に基づいてネットワーク時間を同期します。NTPモードを使用する場合は、NTPサーバーを手動で指定する必要があります。本機で構成を保存した後、時間を同期します。

NTP設定を構成するには、ナビゲーションメニューからConfiguration>Quick Setup>System>NTPを選択します。



NTP設定画面

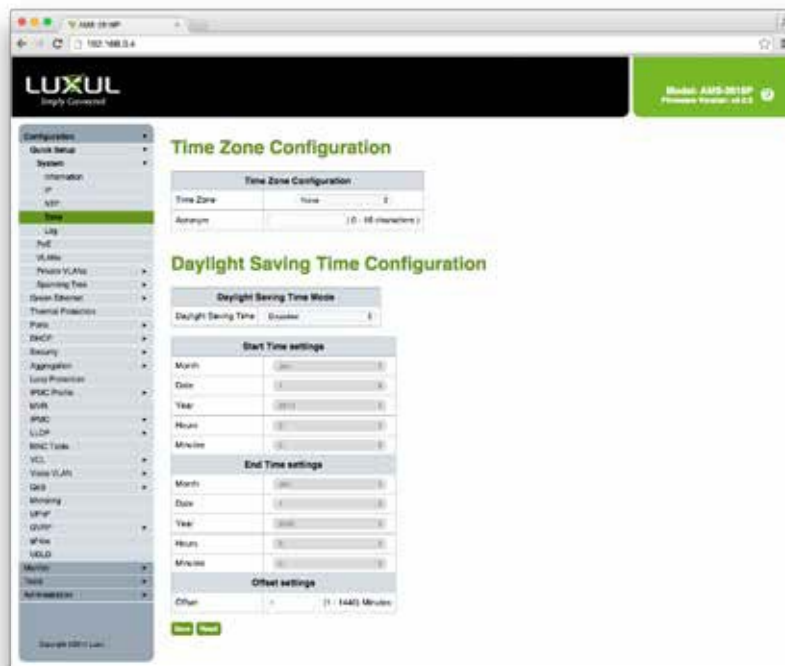
- ▶**Mode Menu:** NTPが有効か無効かを示します。
- ▶**Server1～5:** NTPサーバーのDNS、IPv4、またはIPv6アドレスを入力します。アドレスのリストは、任意のオンライン検索エンジンでNTPサーバーを検索するだけです。
- ▶**Save:** 未保存の変更を保存します。
- ▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

Time

本機はシステム時刻を設定し、サマータイムのオプションを適用する自動設定機能があります。

タイムゾーンとサマータイムを設定するには、ナビゲーションメニューから

Configuration>Quick Setup>System>Timeの順に選択します。



時刻設定画面

タイムゾーンの設定

- ▶ **Time Zone:** 世界中のさまざまなタイムゾーンを一覧表示します。ドロップダウンから適切なタイムゾーンを選択します。
- ▶ **Acronym:** タイムゾーンの頭文字を設定できます。これは、選択したタイムゾーンの識別に役立つユーザー設定可能な頭字語です。(範囲: 最大16文字、スペースなし、特殊文字なし)

サマータイムの設定

- ▶ **Daylight Saving Time Mode:** NTPサーバー設定と一緒にサマータイムを使用するには、サマータイムをRecurring(繰り返し)またはNon-Recurring(非繰り返し)に設定します。

開始時刻の設定

- ▶ **Month:** DST(サマータイム)の開始月を選択します。
- ▶ **Date:** DST(サマータイム)の開始日を選択します。
- ▶ **Year:** DST(サマータイム)の開始年を選択します。
- ▶ **Hours:** DST(サマータイム)の開始時間を選択します。
- ▶ **Minites:** DST(サマータイム)の開始分を選択します。

終了時刻の設定

- ▶ **Month:** DST(サマータイム)の終了月を選択します。
- ▶ **Date:** DST(サマータイム)の終了日を選択します。

- ▶**Year:**DST(サマータイム)の終了年を選択します。
- ▶**Hours:**DST(サマータイム)の終了時間を選択します。
- ▶**Minutes:**DST(サマータイム)の終了分を選択します。

サマータイム設定

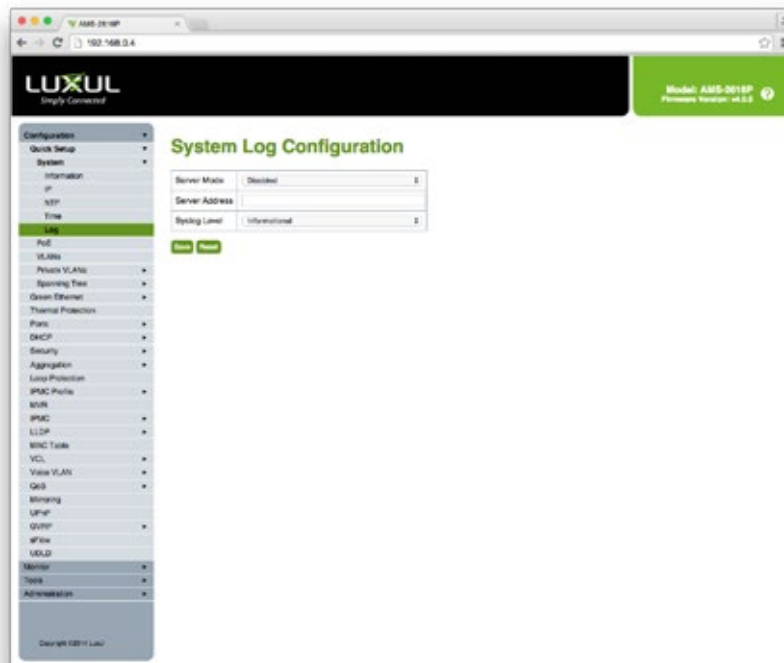
Offset: サマータイム中に追加する分数を入力します。(範囲:1~1440)

- ▶**Save:** 未保存の変更を保存します。
- ▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

Log

ログを使用すると、本機がログファイルのリモート保存と管理に使用するログサーバーを設定できます。

システムログを設定するには、ナビゲーションメニューからConfiguration>Quick Setup>System>Logを選択します。



システムログ設定画面

システムログの設定

- ▶**Server Mode:** Syslogサーバーの設定を有効または無効にします。

- ▶ **Server Address:** SyslogサーバーのIPv4アドレスを示します。本機にローカルDNSサーバーが設定されている場合、サーバードレスをホスト名にすることができます。

Syslog Level: Syslogサーバーに送信されるメッセージのレベルを示します。メッセージレベルには、情報メッセージ(重大度6以下)、通知メッセージ(重大度5以下)、警告(重大度4以下)、エラー(重大度3以下)の4つがあります。可能なモードは次のとおりです。

- ▶ **Informational:** 本機は情報メッセージ、通知メッセージ、警告、エラーを送信します。
- ▶ **Notice:** 本機は通知メッセージ、警告、エラーのみを送信します。
- ▶ **Warning:** 本機は警告とエラーのみを送信します。
- ▶ **Error:** 本機はエラーのみを送信します。

▶ **Save:** 未保存の変更を保存します。

▶ **Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

POEについて

Power over Ethernet(またはPoE)は、イーサネットケーブルを介してデータとともに電力を渡すシステムです。これにより、1本のケーブルで、ワイヤレスアクセスポイントやIPカメラなどのデバイスにデータ接続と電力の両方を提供できます。この機能は、スイッチを他のネットワークデバイスの電源装置として使用することで、ネットワークの設置とメンテナンスを簡素化できます。

イーサネットケーブルを介して電源を伝送するための一般的な技術がいくつかあり、IEEE802.3によって2つが標準化されています。電源は、イーサネットケーブルの未使用の導線上で、または各ペア線にコモンモード電圧を印加することによって伝送されます。後者は、バランス型マイクに電源を供給するファンタム電源に似ています。

IEEE PoE規格では、上記2つの電力伝送方式に関する標準化に加えて、電源供給側と受電側との間の信号伝達を提供します。この信号伝達により、電源供給側は接続されたデバイス(受電側)に必要な電力量を感知して調整できます。

電力の供給量

システム設計および設置時の課題の1つは、ネットワークスイッチの総電力供給量よりも小さくなるように、機器の総消費電力を考慮することです。本機の電源は、ポート数ではなく、合計電力供給量を決定します。

例えば、AMS-1208P AVシリーズは、最大130WのPoE電力供給が可能です。8台のカメラ監視システムを計画し、各カメラが10Wを消費する場合、合計消費電力は80Wとなり、130Wを十分に下回ります。ただし、各カメラが20W消費する場合は、合計消費電力が130Wの合計電力供給量を超えてしまいます。

接続する機器によっては、ポート数ではなく、総電力供給量の大きなスイッチが必要になる場合があります。

ケーブル長

Power over Ethernet(PoE)は、ケーブルの引き回し後に十分な電圧がある場合にのみ、接続されたデバイスに電源を供給します。PoEデバイスまでのケーブル長は最大約100mです。これを超えると電圧が低下し、不安定になります。本機から100mを超えるPoEデバイスを接続する必要がある場合は、PoEエクステンダーを使用してください。

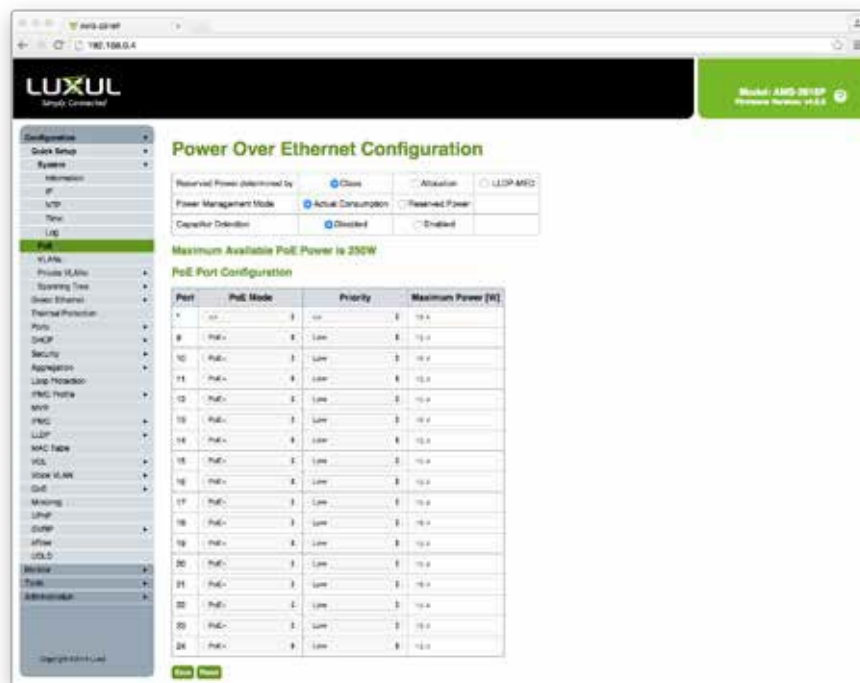
基本的な設定方法:POE

Power Over Ethernet(PoE)は、イーサネット経由でリモートデバイスに電力を送信します。例えば、IP電話、無線アクセスポイント、IPカメラ、直接ACライン電源に接続するのが難しい/高価なデバイスなどに使用します。

POEの設定

PoE Portの設定を含む本機のPoE設定を行います。

PoE設定を構成するには、ナビゲーションメニューからConfiguration>Quick Setup>PoEを選択します。



PoE設定画面

Reserved Power determined by: Ports/PDsが電源を確保する方法を3つのモードのいずれかから設定します。

- ▶ **Allocated:** 各ポートが供給する電力量を割り当てます。各Port/PDのAllocated(割当)/Reserved(予約)電力は、PoEポート設定のMaximum Power(最大電力)フィールドで指定します。
- ▶ **Class:** 各ポートは、接続されたPD(受電デバイス)のクラスに従って、どの程度の電源を供給するかを自動的に決定します。4つの異なるクラスがあり、対応するワット数はクラス1(4W)、クラス2(7W)、クラス3(15.4W)、クラス4(30W)です。このモードでは、Maximum Powerフィールドは使用しません。
- ▶ **LLDP-MED:** このモードは、各ポートがLLDPプロトコルを使用してPoE情報を交換することによって供給する電力量を決定します。クラスモードと同様に動作します。ポートにLLDP情報が提供されない場合、ポートはクラスモードを使用して電源を供給します。このモードでは、Maximum Powerフィールドは使用しません。

注意: ポートへの供給電力よりも多くの電力を使用しようとする場合、ポートのPoE給電がシャットダウンします。

Power Management Mode: ポートのPoEシャットダウン時に設定する2つのモードのいずれかを設定できます。

- ▶ **Actual Consumption:** このモードでは、すべてのポートの実際の消費電力が内蔵の電源装置が供給できる電力を超えた場合、または特定のポートの実際の消費電力がそのポートの供給電力を超えた場合、ポートのPoE給電がシャットダウンします。ポートは、POEポートの優先順位に従ってシャットダウンします。2つのポートの優先順位が同じ場合、ポート番号が大きいポートから先にシャットダウンします。
- ▶ **Reserved Power:** 合計供給電力が内蔵の電源装置が供給できる電力を超えると、ポートのPoE給電がシャットダウンします。このモードでは、PD(受電デバイス)が電源装置から使用可能な電力より多くの電力を要求した場合、POE給電はオンになりません。

Capacitor Detection: 従来のPOEデバイスで使用するCapacitor Detection(容量検出)を有効/無効にできます。

PoEポート設定

Port: PoE設定に対応するポート番号を表示します。PoEに対応していないポートは表示されません。

PoEモード: ポートのPoEモードを設定します。

- ▶ **Disabled:** このポートはPoEが無効です。
- ▶ **PoE:** 802.3af PoEを有効にします(クラス3 PDは15.4Wに制限)。
- ▶ **PoE+:** 802.3at PoE+を有効にします(クラス4 PDは30Wに制限)。

Priority: ポートの優先順位を設定します。

- ▶ **Low:** 優先順位の低いPD(受電デバイス)はLowに設定します。これはデフォルト設定です。
- ▶ **High:** 優先中位のPDは、優先順位Lowの機器よりも重要ですが、Criticalよりは優先順位が下がります。
- ▶ **Critical:** PD(受電デバイス)がローカルネットワークにとって最も重要な場合に設定します。

注意: プライオリティが最も低いLow設定のポートは、ポート番号が大きいポートからPoE給電がシャットダウンされます。

Maximum Power: Allocation Reserved Power(割当予約電力)設定と併せて使用するポートの最大電力値を指定できます。最大供給電力は30Wです。

- ▶ **Save:** クリックして変更を保存します。
- ▶ **Reset:** 変更を取り消し、以前に保存した値に戻します(Saveをクリックすると使用できなくなります)。

VLANSについて

A virtual local area network(仮想ローカルエリアネットワーク、仮想LANまたはVLAN)は、共通の要件を持つホストのグループで、物理的な場所に関係なく、同じブロードキャストドメインに接続されているかのように通信する機能です。

VLANでは単一のネットワークが分割されて、相互に分離された複数の異なるブロードキャストドメインを作成します。これにより、パケットは、1つ以上のルーターを介してのみそれらの間を通過できます。VLANは、物理ローカルエリアネットワーク(LAN)と同じ属性を持ちますが、同じ物理ネットワークスイッチ上にない場合でも、デバイスをグループ化できます。

つまり、VLANはゲートを有しているかに関わらず、デバイスとデータフローとの間に仮想フェンスを構築します。

用途

VLANは、設置場所、セキュリティ、ネットワーク管理などの問題に対処します。VLAN設定のルーターまたはスイッチは、ブロードキャストフィルタリング、セキュリティ、アドレス集約、およびトラフィックフロー管理を提供します。

VLANは、単一の物理的なインフラ上に複数のレイヤー3ネットワークを作成するのにも役立ちます。たとえば、DHCPサーバーがネットワークスイッチに接続されている場合、DHCP用に設定されているそのスイッチ上の任意のホストが機能します。VLANを使用することで、ネットワークを簡単に分割して、一部のホストがそのDHCPサーバーを使用せずにリンクローカルアドレスを取得したり、別のDHCPサーバーからアドレスを取得したりすることができます。

VLANを使用することを考慮する最も一般的な理由のいくつかを次に示します。

セキュリティの強化

VLAN上の特定のデバイスを分離すると、ネットワークとネットワーク上のデバイスのセキュリティを強化できます。

VLANの最も一般的なアプリケーションの1つはゲストネットワークです。ゲストネットワークVLANでは、クライアントはインターネットや特定のローカルデバイスにアクセスできますが、サーバーなどの他のプライベートLANデバイスにはアクセスできません。VLANベースのゲストネットワークでは、特定のアクセスポイントSSIDとそれらに接続されているクライアントは、特定のVLANに分離されます。通常、このVLANはインターネットにアクセスできますが、LAN上の他のものにはアクセスできません。

セキュリティカメラやクレジットカード処理装置は、セキュリティやPCI(Payment Card Industry)準拠のためにVLAN上で分離できる他のデバイスの例です。VLANを使用して、特定のVLANに対するネットワーク攻撃やその他の問題を封じ込めるためにも使用できます。これにより、ネットワーク全体のセキュリティが強化されます。

ネットワーク混雑の低減

また、デバイスを独自のVLAN上に分離すると、混雑が軽減され、ネットワークパフォーマンスが向上します。別のVLAN上にあるシステムやデバイスの例としては、VoIP電話システム、ストリーミングメディア、セキュリティカメラなどがあります。

特定のアプリケーション

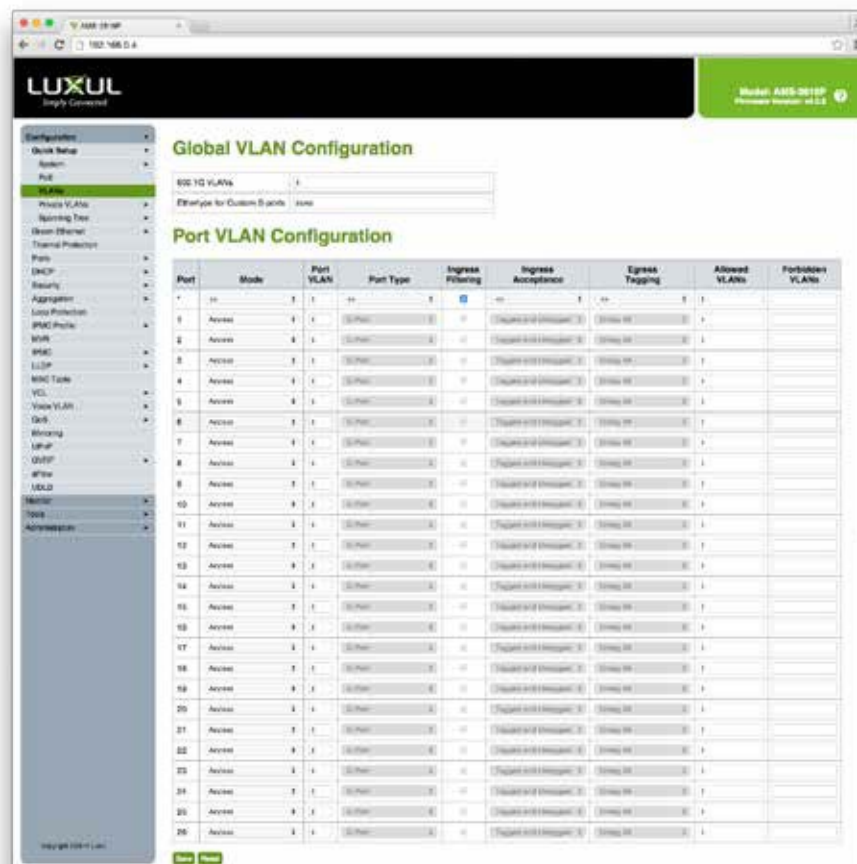
VLANを使用するもう1つの一般的なアプリケーションは、HDMI over IPソリューションです。このAV over IPシステムでは、ビデオ信号を送信機から受信機にルーティングするためにVLANが使用されます。この運用では、VLANは同時にネットワーク混雑を軽減し、同じ物理ネットワーク上で動作する制御システムの信頼性と使いやすさを向上させます。

注意: VLANの詳細と、分離された仮想ネットワークまたはゲストネットワークの作成方法については、luxul.com/educational-webinars/にアクセスし、コース5: VLANs & Guest Networksというタイトルのビデオをクリックしてください。

基本的な設定方法:VLANS

VLAN(Virtual Local Area Network)を使用すると、単一の物理スイッチを2つ以上の論理スイッチに分割できます。VLANは、ローカルネットワークのセキュリティ保護、ローカルネットワーク上の通信パケットの制御、VoIPなどの遅延の影響を受けやすいシステムのレイテンシー問題の解決に使用できます。

VLAN設定を構成するには、ナビゲーションメニューからConfiguration>Quick Setup>VLANsを選択します。



VLAN設定画面

グローバルVLAN設定

802.1Q VLAN: 802.1Q VLANを作成し、どのVLANアクセスモードポートに接続できるかを定義できます。トランクモードまたはハイブリッドポートモードでも、許可されたアクセスVLANを使用してVLANを作成する必要があります。デフォルトでは、VLAN1のみが存在します。個々のVLANがカンマで区切られている構文を使用してリストを追加することで、より多くのVLANを作成できます。範囲はハイフンで指定できます。次の例では、VLAN1、10、11、12、13、200、および300を作成します。

1,10-13,200,300

区切り文字の間にスペースは使用できません。

Ethertype for Custom S-Ports: カスタムSポートに使用するEtherType/TPIDを指定できます。この設定は、ポートタイプがS-Custom-Portに設定されているポートにのみ使用されます。イーサタイプの一覧については、<http://standards.ieee.org/develop/regauth/ethertype/eth.txt>をご覧ください。

ポートVLAN設定

Port: VLAN設定に対応するポート番号を表示します。

ポートモード

ポートの動作を決定するポートモードを設定できます。

Access: アクセスポートは通常、クライアントデバイス(ラップトップPC、IP電話など)への接続に使用します。

- ▶ 1つのVLANのメンバーにしかありません。デフォルトはVLAN1です。
- ▶ タグなしパケットとCタグ付きパケットを受け入れます。
- ▶ アクセスVLANにタグ付けされていないすべてのパケットを破棄します。
- ▶ 出力は、すべてのパケットがタグなしで送信されます。

Trunk: トランクポートは複数のVLANからのトラフィックを同時に伝送でき、通常は他のスイッチまたはVLAN対応ルーターへの接続に使用されます。

- ▶ デフォルトでは、トランクポートは既存のすべてのVLANのメンバーです。Allowed VLANs (VLAN許可)を設定して制限できます。
- ▶ デフォルトでは、ポートVLANとして分類されたパケットを除くすべてのパケットは、出力時にタグ付けされます。ポートVLANとして分類されたパケットは、出力時にタグ付けされません。
- ▶ この構成では、すべてのパケットにタグ付けするように出力タグ付けを変更できます。タグ付けされたパケットのみが入力で受け入れられます。

Hybrid: ハイブリッドポートは、多くの点でトランクポートに似ていますが、ポート設定の追加機能があります。トランクポートで説明されている特性に加えて、ハイブリッドポートは以下の追加機能をサポートします。

- ▶ VLAN Tag Unaware (VLANタグ非対応)、C-Tag Aware (Cタグ対応)、S-Tag Aware (Sタグ対応)、またはS-custom-Tag Aware (Sカスタムタグ対応)に設定可能です。
- ▶ Ingress (入力) フィルターリングを設定できます。

パケットの入力受け入れと出力タグ付けの構成は、個別に構成できます。

ポートVLAN

ポートのデフォルトVLAN ID(PVID)を設定できます。許可されるVLANの範囲は1~4095で、デフォルトはVLAN1です。ポートがVLAN Unaware (VLAN非対応)として設定され、フレームがUntagged (タグなし)、またはVLAN Awareness (VLAN対応)が有効ですが、フレームがPriority Tagged (優先タグ付き: VLAN ID=0)の場合、入力パケットはポートVLANとして分類されます。出力タグ付けがUnTag Port VLAN (タグなしポートVLAN)に設定されている場合、ポートVLANとして分類された出力パケットはタグ付けされません。ポートVLANは、アクセスモードのポートのアクセスVLANで、トランクまたはハイブリッドモードのポートのネイティブVLANです。

ポートタイプ

ハイブリッドモードのポートでは、パケットVLANタグを使用して特定のVLANへの受信時にフレームを分類するかどうかに影響するポートタイプを変更できます。出力のタグ付けが必要な場合、ポートタイプによってタグのTPIDが決まります。

- ▶ **Unaware:** 入力では、タグ付きまたはタグなしのすべてのパケットVLANがポートVLANとして設定され、タグは出力で削除されません。
- ▶ **C-Port:** TPID = 0x8100のVLANタグを持つ入力パケットは、タグに埋め込まれたVLAN IDに設定されます。フレームがUntagged(タグなし)またはPriority Tagged(優先タグ付き)の場合、フレームはポートVLANにタグ付けされます。パケットが出力でタグ付けされる場合は、Cタグでタグ付けされます。
- ▶ **S-Port:** On TPID=0x8100または0x88A8のVLANタグを持つ入力パケットは、タグに埋め込まれたVLAN IDに設定されます。フレームがUntagged(タグなし)またはPriority Tagged(優先タグ付き)の場合、フレームはポートVLANにタグ付けされます。パケットが出力でタグ付けされる場合は、Sタグでタグ付けされます。
- ▶ **S-Custom-Port:** TPID=0x8100またはCustom-S Ports用に設定されたEthertypeと等しいVLANタグを持つ入力パケットは、タグに埋め込まれたVLAN IDに設定されます。フレームがUntagged(タグなし)またはPriority Tagged(優先タグ付き)の場合、フレームはポートVLANにタグ付けされます。パケットが出力でタグ付けされる場合は、Sタグでタグ付けされます。

入力フィルーターリング

ハイブリッドポートでは、入力フィルーターリングを変更できます。アクセスポートとトランクポートでは、常に入力フィルーターリングが有効になっています。入力フィルーターリングが有効になっている場合、VLANにタグ付けされたパケットは、そのメンバーでないポートでは破棄されます。入力フィルーターリングが無効になっている場合、VLANにタグ付けされたパケットは、そのポートがメンバーになっていないことが受け入れられ、転送されます。ただし、ポートはメンバーではないVLANにタグ付けされたパケットを送信しません。

受信時の受け入れ

ハイブリッドポートを使用すると、受信時に受け入れられるパケットのタイプを変更できます。

- ▶ **Tagged and Untagged:** タグ付きパケットとタグなしパケットの両方が受け入れられます。
- ▶ **Tagged Only:** タグ付きパケットのみが受信時に受け入れられます。タグ付けされていないパケットは破棄されます。
- ▶ **Untagged Only:** タグなしパケットのみが受信時に受け入れられます。タグ付きパケットは破棄されます。

出力でタグ付け

トランクモードとハイブリッドモードのポートは、送信時のパケットのタグ付けを制御できます。

- ▶ **UnTag Port VLAN:** ポートVLAN内で分類されたパケットはタグなしで送信されます。その他のパケットは、関連するルーターと共に送信されます。
- ▶ **Tag All:** ポートVLANに分類されているかどうかにかかわらず、すべてのパケットがタグ付きで送信されます。
- ▶ **Untag All:** ポートVLANに分類されているかどうかに関係なく、すべてのパケットがタグなしで送信されます。
(このオプションは、ハイブリッドモードのポートでのみ使用できます)

VLANの許可

トランクモードとハイブリッドモードのポートでは、メンバーになることを許可するVLANを制御できます。アクセスポートは、ポートVLANの1つのVLANのメンバーにしかありません。フィールドの構文は、Allowed Access VLANsフィールドで使用される構文と同じです。デフォルトでは、ポートはすべてVLANのメンバーになることが可能であり、1~4095に設定されます。許可されたVLANは空白のままにすることができ、ポートは既存のVLANのいずれのメンバーにもなりません。ただし、VLANがトランク用に設定されている場合は、すべての不明なVLANを伝送できません。

VLANの禁止事項

ポートは、1つ以上のVLANのメンバーになることを許可されないように設定できます。これは、ダイナミックVLANプロトコルのMVRPやGVRPが意図しないVLANに動的にポートを追加しないようにする必要がある場合に便利です。構文は、Allowed Access VLANsフィールドで使用する構文と同じです。デフォルトの場合、このフィールドは空白のままで、ポートをすべての既存のVLANのメンバーにできます。

▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

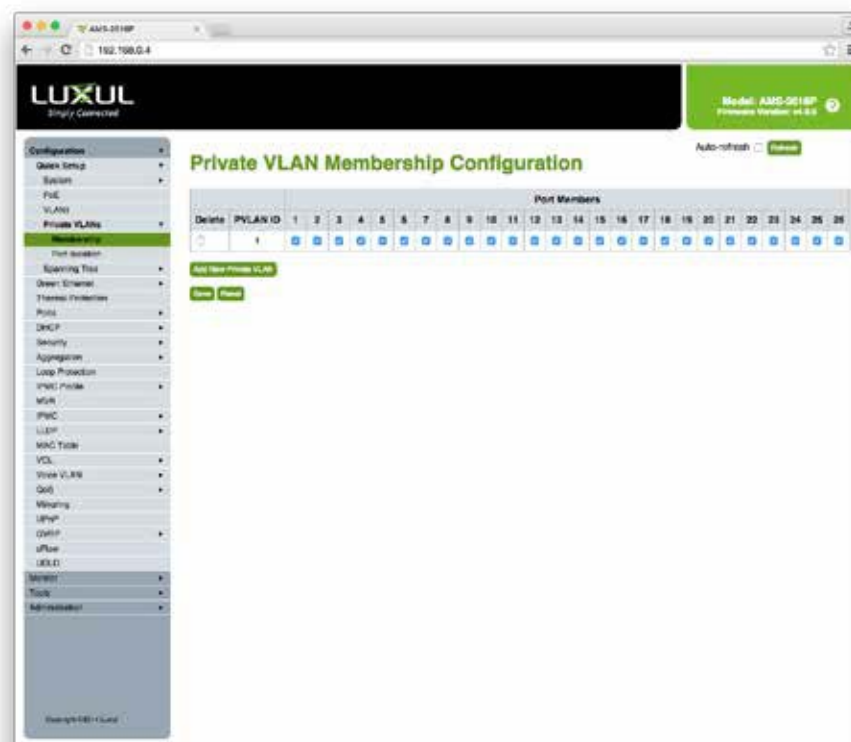
基本的な設定方法: プライベートVLAN

プライベートVLAN内のポート間の通信は許可されますが、プライベートVLANのメンバーでないポートは、そのVLAN内のデータを通すことができません。

VLANメンバーシップ

最大4095個のVLANをサポートするプライベートVLANメンバーシップ設定を定義できます。このページでは、各VLANのポートメンバーを追加および削除できます。

VLANメンバーシップ設定は、ナビゲーションメニューからConfiguration>Private VLANs>Membershipを選択します。



VLANメンバーシップ設定画面

Delete: プライベートVLANメンバーシップのエントリを削除します。Saveボタンを押して保存すると削除が実行されます。

PVLAN ID: プライベートVLANのIDを表示および設定します。このIDは、Configuration>VLANsで設定された Allowed Access VLANに対応しています。

Port Members: プライベートVLANに含めるポートを選択します。対応するボックスをオンにして、プライベートVLANにポートを追加します。ポートをVLANから削除するには、**対応する**ボックスのチェックを外します。デフォルトでは、すべてのポートがメンバーとして選択された状態でPVLAN ID1が作成されます。

▶**Refresh:** プライベートVLANメンバーシップ設定を更新します。

▶**Add New Private VLAN:** 新しいプライベートVLANエントリを追加します。

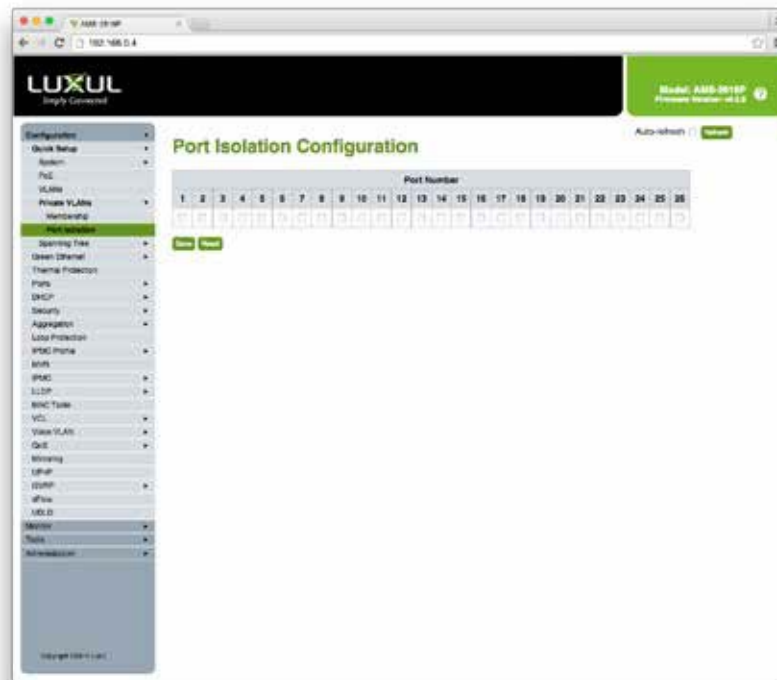
▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

VLANポートの分離

このページは、VLAN内のポートの分離を有効または無効に設定します。VLANのポートメンバーは、同じVLAN上の他の分離されたポートに分離できます。

VLANポート分離を設定するには、ナビゲーションメニューからConfiguration > Private VLANs > Port Isolationを選択します。



VLANポート分離設定画面

Port Number: 指定したポートを分離したり、分離を解除したりします。オンに設定されているポートはポート分離 (Port Isolation) が有効で、オフに設定されているポートはポート分離が無効です。デフォルトでは、ポート分離はすべてのポートで無効になっています。

- ▶ **Refresh:** クリックすると、Port Isolation設定ページが更新されます。
- ▶ **Save:** 未保存の変更を保存します。
- ▶ **Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

スパニングツリーについて

スパニングツリープロトコル(STP)は、任意のブリッジされたイーサネットローカルエリアネットワークのループフリー・トポロジを保証するネットワークプロトコルです。STPの基本的な機能は、ブリッジループおよびそれに伴うブロードキャスト放射を防ぐことです。スパニングツリーを使用すると、ネットワーク設計に予備(リダンダント)リンクを含めて、アクティブリンクに障害が発生した場合、ブリッジループの危険なしに、またはこれらのバックアップリンクを手動で有効/無効にする必要なしに、自動バックアップパスを提供することもできます。

名前が示すように、スパニングツリーは接続されたイーサネットスイッチのネットワーク内にツリーを作成し、スパニングツリーの一部ではないリンクを無効にして、任意の2つのネットワークノード間に単一のアクティブパスを残します。

ループの排除

スイッチがSTPなしのループで接続されている場合、ループを防止するものがないため、各スイッチは受信した最初のブロードキャストパケットを無限に複製します。

STPは、1つ以上のリンクをブロックすることでループを防止します。使用中のリンクの1つがダウンすると、以前にブロックされたリンクにフェイルオーバーします。スパニングツリーがどのリンクを使用するかを選択する方法は、それが見ることのできるトポロジに完全に依存します。

スパニングツリートポロジの背後にある考え方は、ブリッジがループのないトポロジのサブセット、つまりツリーを発見できるということです。またSTPはLAN全体にまたがることで、ネットワークのすべての部分に到達するのに十分な接続性があることを確認します。

スパニングツリー設定

ブリッジは、最初にネットワークに接続されたとき、またはトポロジが変更されたときに、スパニングツリーアルゴリズムを実行します。

ブリッジがConfiguration Message(設定メッセージ)を確認すると、スパニングツリーアルゴリズムを開始します。これは、すべてのデータが流れる「ルートブリッジ」の選択から始まります。

次に、各ブリッジはルートブリッジへの最短パスを決定し、「センター」への到達方法を確認します。2回目の選択は各LANで行われ、指定ブリッジ、つまりルートブリッジに最も近いブリッジが選択されます。指定ブリッジは、LANからルートブリッジに向かってパケットを転送します。

個々のブリッジの最後のステップは、ルートポートの選択です。これは単に「ルートブリッジに向けてデータを送信するために使用するポート」を意味します。

注意: ポートがignore(無視)として設定されていない限り、ブリッジ上のすべての単一ポート(エンドポイントに接続されているポートも含みます)はスパニングツリーに参加します。

新しく接続されたブリッジは、再設定メッセージを送り、他の接続されたデバイスは準拠されます。スパニングツリーの計算中は、すべてのトラフィックが30~50秒間停止します。

スパニングツリーの欠点

STPの欠点の1つは、ネットワークを介して1つのノードから別のノードへの物理的または等価コストの複数のパスが多数ある場合でも、すべてのトラフィックがスパニングツリーで定義された1つのパスに沿って流れることです。この利点は、トラフィックループが回避されることですが、トラフィックを独自のパスに制限するコストは、代替パス(場合によってはより直接的なパス)をブロックすることを意味します。つまり、潜在的なネットワーク容量を十分に実現することはできません。

基本的な設定方法:スパンニングツリー

スパンニングツリープロトコル(STP)は、ネットワークループの検出と無効化に使用されますが、ネットワークスイッチ間のバックアップリンクも提供します。これにより、ネットワークスイッチはネットワーク内の他のブリッジした機器(STP準拠のスイッチ、ブリッジまたはルーター)と対話し、ネットワーク上の任意の2つのステーション間に1つのルートのみが存在することを確認し、プライマリリンクがダウンしたときに自動的に引き継ぐバックアップリンクを提供します。

ブリッジ設定

スパンニングツリーブリッジとSTPシステム設定を行えます。

STPブリッジ設定は、ナビゲーションメニューからConfiguration>Spanning Tree>Bridge Settingsを選択します。



STPブリッジ設定画面

基本設定

Protocol Version: 本機が使用するSTP Protocolのバージョンを設定します。

- ▶ **STP:** v1スパンニングツリーを実行します。
- ▶ **RSTP:** 高速スパンニングツリーを実行します。(STP v1と下位互換性があります)
- ▶ **MSTP:** マルチプルスパンニングツリーを実行します。(STP v1およびRSTPと下位互換性があります)

Bridge Priority: ブリッジの優先度を設定します。優先度の値は降順です(つまり、100の優先度は1000よりも高くなります)。ブリッジプライオリティと、6バイトのMACアドレスと連結されたMSTIインスタンスがブリッジIDを形成します。MSTPの場合、CISTの優先順位に当たります。変更を行う場合はネットワーク管理者に問い合わせてください。

Forward Delay: ルートおよび指定ポートBPDUの送信時に使用する遅延を設定します。有効な範囲は4～30秒で、デフォルトは15秒です。変更を行う場合はネットワーク管理者に問い合わせてください。

Max Age: ルートブリッジによって送信されるBPDUの最大経過時間を設定できます。有効な範囲は6～40秒で、デフォルトは20秒です($\text{MaxAge} \leq (\text{FwdDelay} - 1) * 2$ である必要があります)。変更を行う場合はネットワーク管理者に問い合わせてください。

Maximum Hop Count: MSTPリージョンの境界で生成されるSTP BPDUの残ホップ数を設定します。有効な範囲は6～40ホップです。変更を行う場合はネットワーク管理者に問い合わせてください。

Transmit Hold Count: ブリッジポートが1秒あたりに送信できるBPDUの数を設定します。1秒あたりの制限を超えると、次のBPDUの送信が遅延されます。有効な範囲は1秒あたり1～10BPDUです。変更を行う場合はネットワーク管理者に問い合わせてください。

高度な設定

Edge Port BPDU Filtering: エッジポートとして明確に設定されたポートがBPDUを送受信するかどうかを設定できます。

Edge Port BPDU Guard: エッジポートとして明確に設定されたポートが、BPDUの受信時に自身を無効にするかどうかを設定します。有効な場合、ポートはエラー無効状態になり、アクティブなトポロジーから削除されます。

Port Error Recovery: エラー無効状態のポートが自動的に再有効化できるかどうかを設定します。リカバリが有効になっていない場合、ポートを無効にする必要があります。通常のSTP動作を再開するには、再度有効にします。この状態は、システムの再起動によってもクリアされます。

Port Error Recovery Timeout: ポートエラーから復帰する時間を設定します。有効な範囲は30～86400秒です。

▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

MSTIマッピング

本機にマルチプルスパンニングツリープロトコルを実装すると、CISTに明示的にマッピングされていないVLANからBPDUを受信すルーターめ、CISTは明示的なマッピングに使用できません。CIST内に複数のVLANが設定されている場合は、MSTIにマッピングされているVLANのリストを設定する必要があります。複数のVLANを入力する場合は、カンマまたはスペースで区切ることができます。VLANは、1つのMSTIにのみマッピングできます。未使用のMSTIは空のままにしておきます。

MSTIマッピングを設定するには、ナビゲーションメニューからConfiguration>Spanning Tree>MSTI Mappingを選択します。



MSTI設定

構成の識別

Configuration Name: VLANを識別する名前をMSTPインスタンスマッピングに設定します。MSTIリージョン内でスパンニングツリーを共有するには、ブリッジが同じ名前、リビジョン、およびVLANからMSTIへのマッピング構成を共有する必要があります。名前を設定する必要があり、最大32文字です。使用できる文字は、数字、アルファベットの大文字、小文字、ハイフンです。

Configuration Revision: 上記の名前のMSTPインスタンスのリビジョンを設定します。値は0～65535の整数である必要があります。

MSTIマッピング

MSTI: MSTI マッピング行に対応するMSTI IDを表示します。

VLANs Mapped: MSTIにマッピングされたVLANのリストを入力します。VLANは、1～4094の単一の整数、またはハイフンで区切られた範囲(20～40)として指定でき、それぞれをカンマまたはスペースで区切る必要があります。VLANは、1つのMSTIにのみマッピングできます。未使用のMSTIは空のままにしておきます。

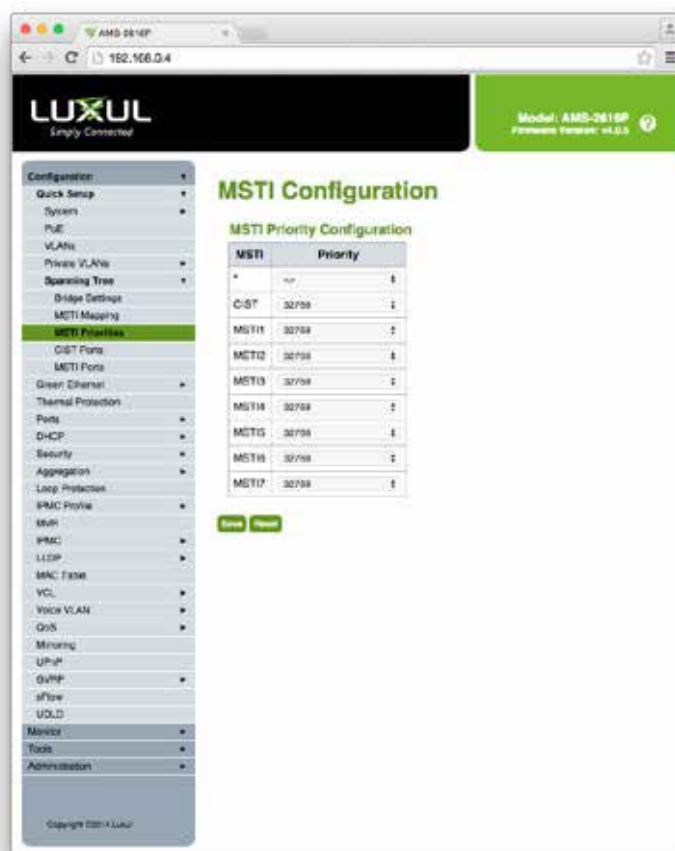
▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

MSTIの優先順位

本機にスパンニングツリーインスタンスを実装する場合、CISTはデフォルトのインスタンスであり、常にアクティブであり、ブリッジプライオリティを制御します。MSTプライオリティでは、本機のMSTIインスタンスの優先順位を設定できます。優先順位の値は降順です(つまり、100の優先順位は1000よりも高くなります)。

MSTプライオリティを設定するには、ナビゲーションメニューからConfiguration>Spanning Tree>MSTI Prioritiesを選択します。



MSTI設定画面

MSTI:ブリッジインスタンスを表示します。CISTはデフォルトインスタンスで、常にアクティブです。

Priority: インスタンスの優先度ごとにブリッジ優先順位を設定できます。値は降順です(つまり、100の優先順位が1000よりも高くなります)。通常、MSTIインスタンスの優先順位をCISTの優先順位より低く保つことをお勧めします。

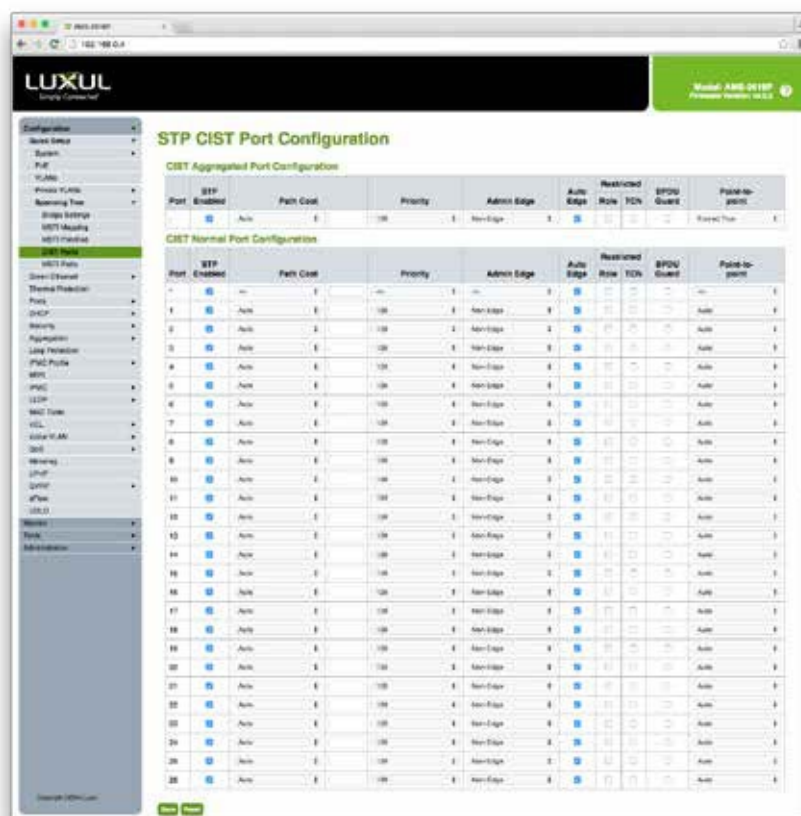
▶**Save:** 未保存の変更を保存します。

▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

CISTポート

本機にスパニングツリーインスタンスを実装する場合は、スパニングツリーをアクティブにするルーターめのCISTポートの設定が必要になります。

STP CISTポートの設定を行うには、ナビゲーションメニューからConfiguration>Spanning Tree>CIST Portsを選択します。



STP CISTポートの設定

CIST集約ポート構成およびCIST通常ポート構成

Port: CIST設定に対応するポート番号を表示します。集約ポート構成を使用する場合、設定はすべての有効なポートに適用されます。

STP Enabled: 指定したスイッチポートでSTPを有効/無効にします。

Path Cost: ポートのパスコストを設定できます。自動設定では、物理リンク速度と802.1Dの推奨値を使用してパスコストを設定します。特定の設定を使用して、値を定義できます。パスコストは、ネットワークのアクティブトポロジーを確立するときに使用されます。パスコストの低いポートはフォワーディング（転送）ポートとして選択され、パスコストの高いポートはバックアップリンクとして使用されます。有効な値の範囲は1～200000000です。

Priority: ポートの優先順位を設定します。同じポートコストを持つポートの優先順位を制御するために使用します。（パスコストを参照）。

AdminEdge: ポートがエッジデバイスに直接接続されているかどうかを設定します。これにより、エッジポートの方がエッジポート以外のポートよりも、フォワーディングステートへの移行が高速になります。このフラグの値は、AdminEdgeとAutoEdgeの設定に基づきます。Edgeに設定すると、Monitor>Spanning Tree>Port StatusでEdgeと表示されます。

- ▶ **Edge:** ポートはエッジポートとして設定されており、フォワーディングステートへの移行が高速になります。
- ▶ **Non-Edge:** ポートはエッジポートとして設定されておらず、通常の移行タイミングに従います。これはデフォルト値です。
- ▶ **AutoEdge:** スイッチがエッジポート検出を試みるかどうかを設定できます。これにより、ポートでBPDUが受信されているかどうかでAdminEdgeの状態を取得できます。

Restricted Role: 最良のスパニングツリーの優先順位が設定されている場合でも、CISTまたは任意のMSTIのルートポートとして選択されないように、ポートを制限できます。ルートポートが選択されると、ポートがバックアップとして選択されます。

制限付きロールは、ネットワークのコア領域の外部のブリッジがスパニングツリーアクティブトポロジーに影響しないように、ネットワーク管理者が設定できます。この機能はルートガードとも呼ばれます。

警告: この設定により、スパニングツリーの接続が失われる可能性があります。

Restricted TCN: 受信したトポロジー変更通知とトポロジー変更を他のポートに伝達しないように、ポートを制限できます。制限付きTCNは、ネットワークのコア領域の外部のブリッジがその領域内でアドレスフラッシュを引き起こさないように、ネットワーク管理者によって設定できます。使用例は、接続されたLANの物理リンク状態が頻繁に遷移する場合です。

注意: この設定は、学習されたステーションの位置情報が正しくないためにスパニングツリーアクティブトポロジーに変更された後、接続が一時的に失われる可能性があります。

BBPDU Guard: 有効なBPDUを受信すると、ポート自体を無効に設定できます。ポートエッジの状態は、この設定には影響しません。この設定が原因でエラーディセーブル状態になったポートも、ブリッジポートエラー回復設定の対象になります。

Point to Point: ポートが共有メディアではなくポイントツーポイントLANに接続するかどうかを設定できます。

- ▶ **Auto:** ポイントツーポイントのステータスが自動的に検出されます。これはデフォルト設定です。
- ▶ **Forced True:** 本機を強制的にポイントツーポイント設定にできます。
- ▶ **Forced False:** 強制的にポイントツーポイント設定を無効にできます。

注意: ポイントツーポイントLANは、共有メディアよりもフォワーディングステートへの移行が高速です。

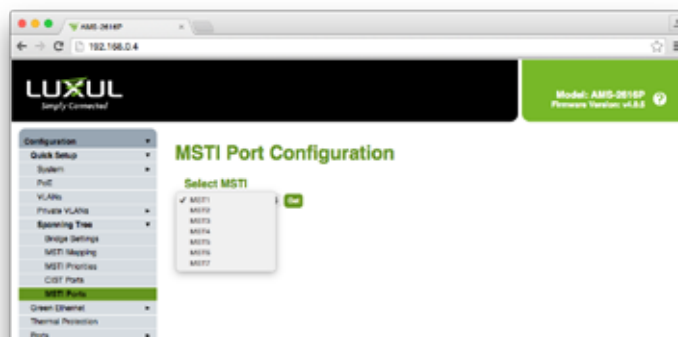
▶ **Save:** 未保存の変更を保存します。

▶ **Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

MSTIポート

本機にマルチプルスパニングツリーインスタンスを実装する場合は、スパニングツリーのMSTIポート設定を有効にする必要があります。

MSTIポートを設定するには、ナビゲーションメニューからConfiguration>Spanning Tree>MSTI Portsを選択します。

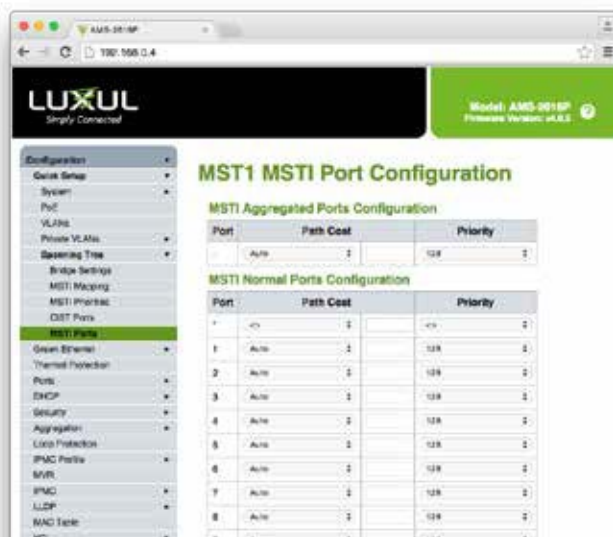


MSTIポート設定(MSTIの選択)

MST#Drop-down: 選択するMSTIをドロップダウン表示します。

MST#: 設定するMSTIを選択します。

▶**Get:** 選択したMSTIの構成用ページを開きます。



MSTIポートの設定

Port: MSTI 設定に対応するポート番号を表示します。

Path Cost: ポートのパスコストを設定できます。自動設定では、物理リンク速度と802.1Dの推奨値を使用してパスコストを設定します。特定の設定を使用して、値を定義できます。パスコストは、ネットワークのアクティブトポロジーを確立するときに使用します。低いパスコストのポートはフォワーディング(転送)ポートとして選択され、高いパスコストのポートはバックアップリンクとして使用されます。有効な値の範囲は1~200000000です。

Priority: ポートの優先順位を設定します。ポートコストが同じポートの優先順位を調整するために使用します。(パスコストを参照)。

▶**Save:** 未保存の変更を保存します。

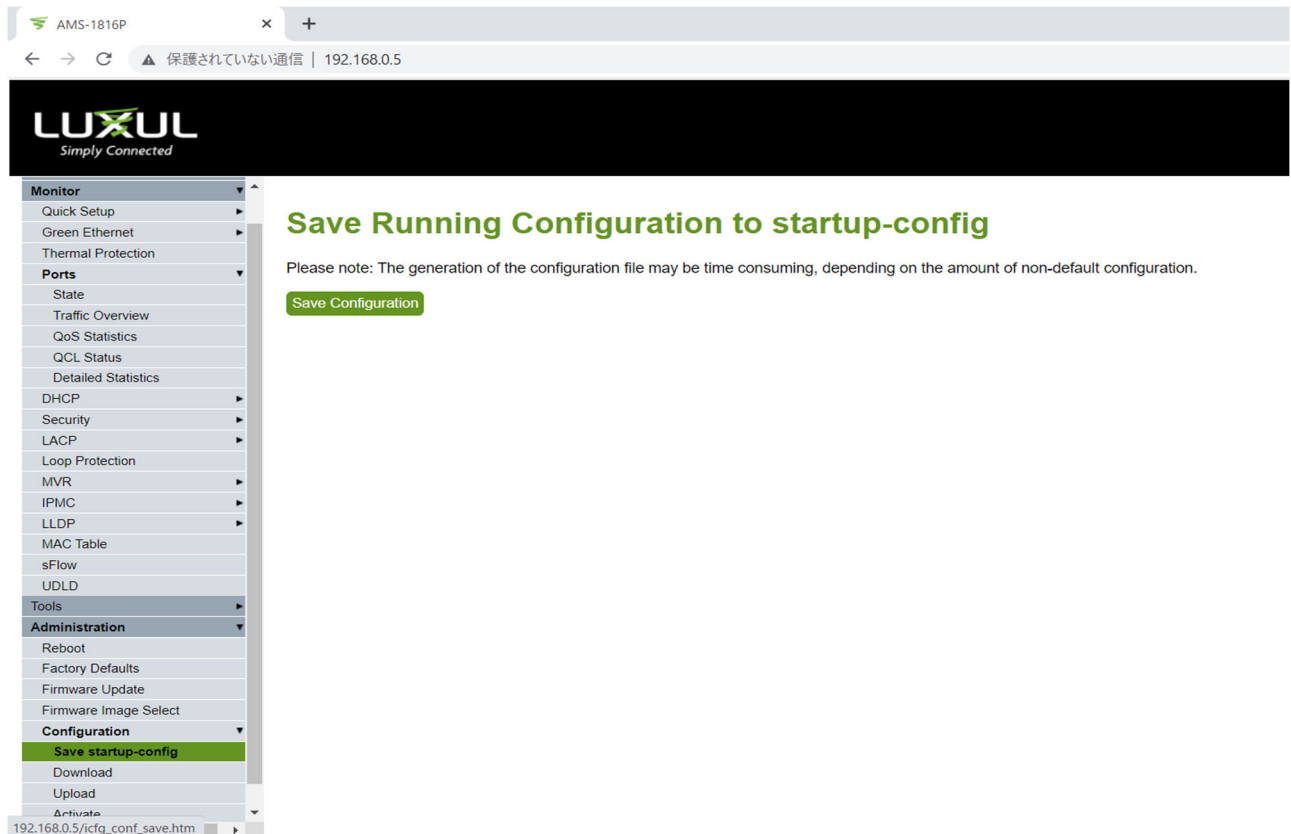
▶**Reset:** 未保存の変更をキャンセルし、以前に保存した値に戻します。変更が保存されると使用できなくなります。

変更した設定を起動時に適用するには

各項目で設定を変更し、Saveボタンを押して保存した設定は、電源が入っている間は適用されていますが、一度電源を切ると変更前の設定に戻ってしまいます。

再起動してもカスタマイズした設定を適用したままにするには、最後に「startup-config（起動時設定）」に保存する必要があります。

Administration>Configuration>Save startup-config に移動して、「Save Configuration」ボタンを押します。



LUXUL™

- この製品を安全にお使いいただくために、設置・運用には十分な安全対策を行ってください。
- 商品写真やイラストは、実際の商品と一部異なる場合があります。
- 掲載内容は発行時のもので、予告なく変更されることがあります。変更により発生したいかなる損害に対しても、弊社は責任を負いかねます。
- 記載されている商品名、会社名等は各社の登録商標、または商標です。



ヒビノインターサウンド株式会社

〒105-0022 東京都港区海岸2-7-70 TEL: 03-5419-1560 FAX: 03-5419-1563

E-mail: info@hibino-intersound.co.jp <https://www.hibino-intersound.co.jp/>