

SIEMENS

SIMATIC NET

SCALANCE 工業用イーサネットスイッチ SCALANCE X-400

設定マニュアル

はじめに	1
SCALANCE X-400 による工業用 ネットワークのネットワーク管理	2
IP アドレスの割り当て	3
ウェブ型管理ツールおよびコマンド ラインインタフェースを用いた設定 手順	4
SNMP を用いた設定と診断	5
PROFINET IO の機能	6
C プラグ	7
ファームウェアアップデート	8
付録	A

安全指針

本書は、身体の安全を守り、器物の損傷を防止するために順守していただくべき注意事項を記載しています。身体の安全に関わる注意事項には要注意マークを付け、器物の損傷に関わる注意事項には要注意マークを付けていません。注意事項は危険度の高い順に次のように表示しています。



危険

適切な対策を取らなければ死亡や重傷事故を招きます。



警告

適切な対策を取らなければ死亡や重傷事故を招くおそれがあります。



注意（要注意マークあり）

適切な対策を取らなければ怪我を負うおそれがあります。

注意（要注意マークなし）

適切な対策を取らなければ器物の損傷を招くおそれがあります。

注

記載事項を考慮しなければ、意図しない結果もしくは状況に至るおそれがあります。

複数の危険度にまたがる場合は、危険度の最も高いものが表示されます。身体の安全に関わる注意事項（要注意マークあり）には、器物の損傷に関わる注意事項を含む場合があります。

有資格者

装置やシステムの設定および操作は、必ず本書の内容に従って実施してください。装置の設定や操作は有資格者しか行うことができません。本書の安全事項という有資格者とは、所定の安全規範および安全基準に従って装置、システム、回路の調整、接地、およびラベル付けの作業を行うことを許可された者をいいます。

想定使用範囲

下記の点に注意してください。



警告

本装置は、カタログまたは技術資料に記載の用途に対して、ならびにシーメンスが承認もしくは推奨する他社製の装置または部品とともにのみご使用いただけます。本製品が正しくかつ期待どおりに機能するためには、これを正しく輸送、保管、設置、組立し、慎重に操作・保守することが必要です。

商標

®の付いた名称はすべて Siemens AG の登録商標です。本書で使用するその他の名称は商標である可能性があり、第三者がそれを自己の目的のために使用すると権利者の権利侵害となる場合があります。

免責事項

本書の内容がハードウェアおよびソフトウェアの実情と一致するよう、弊社では万全の注意を払っておりますが、それが完璧である保証はありません。ただし本書の内容は定期的にチェックしており、必要な修正があれば改訂時に盛り込みます。

目次

1	はじめに	1-1
1.1	SCALANCE X-400 に関する文書	1-1
1.2	設定マニュアルの内容	1-2
2	SCALANCE X-400 による工業用ネットワークのネットワーク管理	2-1
2.1	SCALANCE X-400 における設定オプション	2-1
2.2	SCALANCE X-400 の機能と特徴	2-2
3	IP アドレスの割り当て	3-1
3.1	IP アドレスの構成	3-1
3.2	IP アドレスの初期割り当て	3-2
3.3	シリアルインタフェースを用いた IP アドレスの割り当て	3-3
3.4	BOOTP クライアントによる SCALANCE X-400 の IP アドレス割り当て	3-4
3.5	DHCP クライアントによる SCALANCE X-400 の IP アドレス割り当て	3-5
3.6	プライマリセットアップツールによる IP アドレスの割り当て	3-6
4	ウェブ型管理ツールおよびコマンドラインインタフェースを用いた設定手順	4-1
4.1	ウェブ型管理ツールおよびコマンドラインインタフェースに関する基本事項	4-2
4.1.1	はじめに	4-2
4.1.2	ウェブ型管理ツール (WBM) の疑似ランブ	4-5
4.1.3	ウェブ型管理ツールの基本操作	4-6
4.1.4	コマンドラインインタフェース (CLI)	4-7
4.2	システムメニュー	4-9
4.2.1	System Configuration メニュー	4-9
4.2.2	System Restart and Defaults メニュー	4-10
4.2.3	System Save & Load メニュー	4-13
4.2.4	System Event Log Table メニュー	4-15
4.2.5	System Version Numbers メニュー	4-17
4.2.6	C-PLUG Information メニュー	4-18
4.3	X-400 メニュー	4-20
4.3.1	X-400 Status メニュー	4-20
4.3.2	X-400 Ring Configuration メニュー (SCALANCE X408-2)	4-23
4.3.3	X-400 Fault Mask メニュー	4-25
4.3.4	X-400 Standby Mask メニュー	4-27
4.3.5	X-400 Counters メニュー	4-29
4.4	エージェントメニュー	4-31
4.4.1	Agent Configuration メニュー	4-31
4.4.2	Agent SNMP Configuration メニュー	4-37

4.4.3	SNMPv1 Trap Configuration メニュー	4-39
4.4.4	SNMPv3 Groups メニュー	4-41
4.4.5	SNMPv3 Users メニュー	4-44
4.4.6	Agent Event Configuration メニュー	4-47
4.4.7	Agent Digital Input Configuration メニュー (SCALANCE X414-3E)	4-49
4.4.8	Agent E-Mail Configuration メニュー	4-51
4.4.9	Agent DHCP Configuration メニュー (SCALANCE X408-2)	4-53
4.4.10	Agent Time Configuration メニュー	4-54
4.4.11	Agent PNIO Configuration メニュー (SCALANCE X408-2)	4-56
4.5	スイッチメニュー	4-57
4.5.1	Switch Configuration メニュー	4-58
4.5.2	Current Unicast Filter メニュー	4-61
4.5.3	Current Multicast Group メニュー	4-65
4.5.4	GMRP Configuration メニュー	4-70
4.5.5	IGMP Snooping Configuration メニュー	4-70
4.5.6	Broadcast Blocking Mask メニュー	4-71
4.5.7	Load Limits Configuration メニュー (SCALANCE X414-3E)	4-72
4.5.8	Load Limits Rates メニュー (SCALANCE X408-2)	4-75
4.5.9	Current VLAN Configuration メニュー	4-77
4.5.10	VLAN Port Parameters メニュー	4-82
4.5.11	GVRP Configuration メニュー	4-84
4.5.12	Spanning Tree Configuration メニュー	4-85
4.5.13	Spanning Tree Ports Parameters メニュー	4-88
4.6	ルータメニュー (SCALANCE X414-3E)	4-92
4.6.1	Router Configuration メニュー	4-92
4.6.2	Subnets メニュー	4-93
4.6.3	Current Routes メニュー	4-96
4.6.4	RIPv2 Configuration メニュー	4-99
4.6.5	RIPv2 Interfaces メニュー	4-100
4.6.6	OSPFv2 Configuration メニュー	4-105
4.6.7	OSPFv2 Areas メニュー	4-107
4.6.8	OSPFv2 Area Ranges メニュー	4-110
4.6.9	OSPFv2 Interfaces メニュー	4-111
4.6.10	OSPFv2 Virtual Links メニュー	4-116
4.6.11	OSPFv2 Neighbors メニュー	4-119
4.6.12	OSPFv2 Link State Database メニュー	4-121
4.7	Port Status メニュー	4-122
4.8	統計メニュー	4-127
4.8.1	Packet Size Statistic メニュー	4-127
4.8.2	Packet Type Statistic メニュー	4-129
4.8.3	Error Statistic メニュー	4-131
5	SNMP を用いた設定と診断	5-1
6	PROFINET IO の機能	6-1
6.1	PROFINET IO の使用	6-1
6.2	HW Config での設定	6-8
6.3	PROFINET IO のアクセスオプション	6-12

7	C プラグ	7-1
8	ファームウェアアップデート	8-1
8.1	機能的ファームウェアによるファームウェアアップデート	8-1
8.1.1	TFTP を用いたファームウェアアップデート	8-1
8.1.2	FTP を用いたファームウェアアップデート	8-1
8.2	ブートソフトを用いたファームウェアアップデート	8-2
8.2.1	シリアルポートを介したファームウェアアップデート	8-2
8.2.2	イーサネットポートと FTP を使ったファームウェアアップデート	8-5
A	付録	A-1
A.1	付録 A : PC と SCALANCE X-400 のシリアルポートの接続	A-1
A.2	付録 B : SCALANCE X-400 の MIB オブジェクト	A-3
A.3	付録 C : フレームのタギング	A-8
	用語の説明	Glossary-1
	索引	Index-1

表目次

表 4-1	コマンドラインインタフェース : CLI¥ ... >	4-8
表 4-2	System Configuration : CLI¥SYSTEM>	4-10
表 4-3	System Configuration : CLI¥SERVICE>	4-10
表 4-4	System Restart & Defaults : CLI>	4-12
表 4-5	System Restart & Defaults : CLI¥SYSTEM>	4-12
表 4-6	System Save & Load : CLI¥SYSTEM>	4-14
表 4-7	System Save & Load : CLI¥SYSTEM¥SAVELOAD>	4-15
表 4-8	System Event Log Table : CLI¥SYSTEM>	4-16
表 4-9	System Version Numbers : CLI>	4-17
表 4-10	System Version Numbers : CLI¥SYSTEM>	4-18
表 4-11	C-PLUG Information : CLI¥SYSTEM¥C-PLUG>	4-20
表 4-12	X-400 Status : CLI¥X-400>	4-23
表 4-13	X-400 Ring Configuration : CLI¥X-400¥RING>	4-24
表 4-14	SCALANCE X-400 Fault Mask : CLI¥X-400>	4-26
表 4-15	X-400 Standby Mask : CLI¥X-400>	4-28
表 4-16	X-400 Standby Mask : CLI¥X-400¥STANDBY>	4-28
表 4-17	X-400 Counters : CLI¥X-400>	4-31
表 4-18	Agent Configuration : CLI¥AGENT>	4-34
表 4-19	Agent Configuration : CLI¥AGENT>	4-36
表 4-20	Agent SNMP Configuration : CLI¥AGENT¥SNMP	4-39
表 4-21	SNMPv1 Trap Configuration : CLI¥AGENT¥SNMP>	4-40

表 4-22	SNMPv3 Groups : CLI¥AGENT¥SNMP¥GROUP>	4-43
表 4-23	SNMPv3 Users : CLI¥AGENT¥SNMP¥USER>	4-47
表 4-24	Agent Event Configuration : CLI¥AGENT¥EVENT>	4-49
表 4-25	Agent Digital Input Configuration : CLI¥AGENT¥DIGIN>	4-51
表 4-26	Agent E-Mail Configuration : CLI¥AGENT¥EMAIL>	4-52
表 4-27	Agent DHCP Configuration : CLI¥AGENT¥DHCPCONF>	4-54
表 4-28	Agent Time Configuration : CLI¥AGENT¥TIME>	4-56
表 4-29	Agent PROFINET IO Configuration : CLI¥AGENT¥PNIOCONF>	4-57
表 4-30	Switch Configuration : CLI¥SWITCH>	4-61
表 4-31	Current Unicast Filter : CLI¥SWITCH¥UCAST>	4-65
表 4-32	Current Multicast Groups : CLI¥SWITCH¥MCAST>	4-69
表 4-33	GMRP Configuration : CLI¥SWITCH¥MCAST>	4-70
表 4-34	IGMP Configuration : CLI¥SWITCH¥MCAST>	4-71
表 4-35	IGMP Configuration : CLI¥SWITCH¥MCAST¥IGMP>	4-71
表 4-36	Broadcast Blocking Mask : CLI¥SWITCH¥>	4-72
表 4-37	Load Limits Configuration : CLI¥SWITCH>	4-74
表 4-38	Load Limits Configuration : CLI¥SWITCH¥LIMITS>	4-77
表 4-39	Current VLAN Configuration : CLI¥SWITCH¥VLAN>	4-81
表 4-40	VLAN Port Parameters : CLI¥SWITCH¥VLAN>	4-84
表 4-41	GVRP Configuration : CLI¥SWITCH¥VLAN>	4-85
表 4-42	Spanning Tree Configuration : CLI¥SWITCH¥STP>	4-87
表 4-43	Spanning Tree Ports Parameters : CLI¥SWITCH¥STP>	4-91
表 4-44	Router Configuration : CLI¥ROUTER>	4-93
表 4-45	Subnets : CLI¥ROUTER¥SUBNETS>	4-95
表 4-46	Current Routes : CLI¥ROUTER¥ROUTES>	4-98
表 4-47	RIPv2 Configuration : CLI¥ROUTER¥RIP>	4-100
表 4-48	RIPv2 Interfaces : CLI¥ROUTER¥RIP¥RIP¥IFACE>	4-104
表 4-49	OSPFv2 Configuration : CLI¥ROUTER¥OSPF>	4-106
表 4-50	OSPFv2 Areas : CLI¥ROUTER¥OSPF¥AREAS>	4-109
表 4-51	OSPFv2 Area Ranges : CLI¥ROUTER¥OSPF¥AREAS¥RANGES>	4-111
表 4-52	OSPFv2 Interfaces : CLI¥ROUTER¥OSPF¥AREAS¥IFACE>	4-115
表 4-53	OSPFv2 Virtual Links : CLI¥ROUTER¥OSPF¥AREAS¥VLINKS>	4-118
表 4-54	OSPFv2 Neighbors : CLI¥ROUTER¥OSPF>	4-120
表 4-55	OSPFv2 Link State Database : CLI¥ROUTER¥OSPF>	4-122
表 4-56	Port Status : CLI¥PORT>	4-126
表 4-57	Statistics : CLI¥PORT>	4-127

はじめに

本書の目的

この設定マニュアルには、モジュール式工業用イーサネットスイッチ SCALANCE X-400 の設定に役立つ情報を記載しています。SCALANCE X-400 によって実現される各種技術の概要を示すとともに、ウェブ型管理ツールおよびコマンドラインインターフェースでの設定方法を説明します。

本書の対象製品

この設定マニュアルは以下のソフトウェアバージョンについて有効です。

- SCALANCE X-400 のファームウェア：バージョン 1.2
- プライマリセットアップツール：バージョン 3.0
- SNMP/OPC サーバ：バージョン 6.2.1

1.1 SCALANCE X-400 に関する文書

設定マニュアルの内容

本書はモジュール式工業用イーサネットスイッチ SCALANCE X-400 の設定について記載しています。

SNMP、RST（高速スパニングツリー）、VLAN、ルーティング（SCALANCE X414-3E）、電子メールなどの機能を使用するには、SCALANCE X-400 スイッチの設定作業が必要です。本書はファームウェアアップデートや C プラグについても取り上げています。

設定を行う前に装置の実装と接続が必要です。この作業については操作説明書に記載されています。

操作説明書の内容

『工業用イーサネットスイッチ SCALANCE X-400 操作説明書』には、スイッチに関する基本情報のほかに SCALANCE X-400 製品（スイッチ、メディアモジュール、エクステンダモジュール）に関する説明が記載されています。また SCALANCE X-400 の稼働準備（実装、配線、モジュールの使用など）についても書かれています。

1.2 設定マニュアルの内容

章立て

各章の概要を以下にまとめます。

テーマ	章
SCALANCE X-400 文書の概要	1 章
SCALANCE X-400 で使用できる機能および設定	2 章
IP アドレスの構造と SCALANCE X-400 に IP アドレスを割り当てる方法	3 章
SCALANCE X-400 の設定方法、ならびに対応する CLI コマンドの使い方、またはウェブ型管理ツールの編集ページ	4 章
SNMP を用いた SCALANCE X-400 の管理	5 章
接続した SCALANCE X-400 スイッチに対して使用できる PROFINET IO オプション	6 章
C プラグ（コンフィギュレーションプラグ）に関して使用できるオプション	7 章
ファームウェアのアップデート	8 章

SCALANCE X-400 による工業用ネットワークの ネットワーク管理

2.1 SCALANCE X-400 における設定オプション

RS-232 インタフェース

SCALANCE X-400 スイッチは RS-232 ポートを備えています。ヌルモデムケーブル（クロスケーブル）とターミナルプログラム（Windows の HyperTerminal など。付録 A も参照）を使えば、PC または PG をこのポートに接続することができます。アウトバンドポート（SCALANCE X414-3E のみ）およびインバンドポートに対する IP アドレスの手動割り当てにはこのポートが使用されます（3.3「シリアルインタフェースを用いた IP アドレスの割り当て」を参照）。CLI コマンドもすべて使用できます。

SCALANCE X414-3E のみ：CPU モジュールのイーサネットポート（アウトバンドポート）

SCALANCE X414-3E の CPU モジュールはファストイーサネットポートを備えています。このポートは管理機能専用です。このアウトバンドポートの IP アドレスは RS-232 ポートを使って割り当てられます（3.3「シリアルインタフェースを用いた IP アドレスの割り当て」を参照）。アウトバンドポートでは次に示すプロトコルまたはサービスを使用できます。

- ウェブ型管理ツール（HTTP ベース）
- Telnet
- SNMP
- トラップ
- FTP
- TFTP
- 電子メール

付記

CPU モジュールのシリアルポートまたはイーサネットポートを使った SCALANCE X-400 管理部へのアクセスは、ネットワーク障害時にも可能です（アウトオブバンド・マネジメント）。

スイッチポート経由の管理を行うためのイーサネットポート（インバンドポート）

IP アドレスをインバンドポートに割り当てるには以下の方法があります。

- RS-232 ポート（3.3「シリアルインタフェースを用いた IP アドレスの割り当て」を参照）
- プライマリセットアップツール（バージョン 3.0 以上）
- BOOTP（3.4「BOOTP クライアントによる SCALANCE X-400 の IP アドレス割り当て」を参照）
- DHCP（3.5「DHCP クライアントによる SCALANCE X-400 の IP アドレス割り当て」を参照）

インバンドポートでは次の示すプロトコルまたはサービスを使用できます。

- ウェブ型管理ツール（HTTP ベース）
- Telnet
- SNMP
- トラップ
- FTP
- TFTP
- 電子メール

ルーティング機能を使えば SCALANCE X-400（X414-3E）は複数のインバンドアドレスをもつことができます。ただしプライマリセットアップツール（PST）使用時には 1 つのインバンドアドレス（エージェントの IP アドレス）しか割り当てできません。それ以外のアドレスは WBM、CLI、SNMP を使って割り当てることが必要です。

付記

ルーティング機能は SCALANCE X414-3E でのみ使用できます。

付記

ルーティング機能を有効にすると、DHCP/BOOTP によるアドレス設定は行えません。

2.2 SCALANCE X-400 の機能と特徴

10Mbps および 100Mbps による既存サブネットの統合

SCALANCE X-400 はツイストペアポートにおいて以下の性質を自動検出します。

- 送信ペアと受信ペア（オートクロス）
- 伝送速度（10Mbps または 100Mbps）
- モード（全二重または半二重）

この機能により、サブネットをツイストペアによって SCALANCE X-400 に容易に統合できます。

注

ストレートケーブルを使用した場合でも、2つのポートを1台の SCALANCE X-400 に接続するなどすれば、イーサネットネットワーク内にイリーガルなループが生じることがあります。そのようなループが存在すると、ネットワーク過負荷やネットワーク障害の原因になります。

付記

オートネゴシエーションモードで動作する SCALANCE X-400 のポートを、オートネゴシエーションモードでない相手装置に接続する場合には、その相手装置を固定的に半二重モードに設定する必要があります。

ギガビットイーサネットポート

SCALANCE X414-3E はギガイーサポートを2つ、SCALANCE X408-2 はギガイーサポートを4つ備えています。これらのポートはとくにスイッチ間の大容量接続に適しており、以下の性質を備えています。

- 送信ペアと受信ペアの自動検出（オートクロス）
- 伝送速度（10Mbps、100Mbps、1000Mbps）
- 全二重

付記

1Gbps の伝送を行うには、4 対（8 心）のカテゴリー5e 以上のツイストペアケーブルが必要です。2 対（4 心）では最大 100Mbps の伝送が可能です。

リング形での高速冗長化

SCALANCE X-400 がリング形トポロジーの一部を構成する場合、それは冗長化マネージャ（RM）の役割を果たすことができます。伝送リンクが正常である間、SCALANCE X-400 はバス形トポロジーの開始点または終端点のように振る舞い、フレームの循環を防ぎます。SCALANCE X-400 がリンクの障害を検出すると、最高 0.3 秒の早さでリングポート間の接続を開通させます。それによってリング上のすべての機器間の接続が復旧します。

SCALANCE X-400 の装置で構成されるリングは 1000Mbps で運用できます。SCALANCE X-200 または OSM/ESM があるリングでは、SCALANCE X-400 スイッチを冗長化マネージャとして使用することも、また 100Mbps リングにおける通常のノードとして使用することもできます。

ネットワークセグメントの冗長結合

SCALANCE X-400、X-200、または OSM/ESM で構成されるリング形もしくはバス形ネットワークは、適切な配線と設定を行うことによって冗長構成を取るよう結合できます (4.3.4「X-400 Standby Mask メニュー」参照)。

ネットワークセグメントの冗長結合の詳細については『工業用イーサネットスイッチ SCALANCE X-400 操作説明書』をご覧ください。

ストア&フォワード

SCALANCE X-400 は受信データパケットの CRC 値を計算し、有効なチェックサムをもつデータのみ転送します (ストア&フォワード方式)。誤りのあるパケットは転送されません。ストア&フォワード方式の場合、リンクごとに異なる伝送速度でネットワークを運用することができます。

仮想ネットワークのサポート (VLAN 使用)

仮想ネットワーク (VLAN) と通常の LAN に物理的な差はありません。VLAN に固有の特徴は、装置群を 1 つの装置グループとして構成できることです。複数のこのような装置グループが、物理的に一度しか存在しない 1 つのネットワークインフラを使用します。1 つの物理ネットワーク上にいくつかの「仮想ネットワーク」がつけられます。データ交換やときにブロードキャストの転送までもが 1 つの VLAN 内で行われます。

VLAN はフレームの拡張によって実現されます。発着アドレスの後ろに 4 バイトの追加情報が挿入されます。フレームのタグgingについては付録 C をご覧ください。

VLAN をサポートしない末端装置およびサブネットを仮想ネットワークに組み込めるよう、スイッチは VLAN 付加情報の追加・削除を行えます。SCALANCE X-400 は装置の接続ポートを元に VLAN の割り当てを行えます (ポート VLAN)。最大 62 のポート VLAN と 2 つの既定 VLAN の設定が可能です。VLAN は IEEE 802.1Q に規定されています。

高速スパンニングツリー

高速スパンニングツリープロトコル (RSTP) を用いると、2 端末間に複数の経路が存在するネットワークを運用できます。RSTP は 1 経路のみを許容し、それ以外のデータトラフィック用 (冗長) ポートを不使用とすることにより、ネットワーク内のループ形成を防止します。SCALANCE X-400 スイッチは RSTP とスパンニングツリー (STP) の両方をサポートします。

SCALANCE X414-3E においてスパンニングツリーまたは高速スパンニングツリーのいずれかを使用するときは、R1 および R2 の 2 つの DIL スイッチをオンに設定することが必要です。SCALANCE X408-2 については X-400 Ring Configuration メニューにおいて *Ring Redundancy* オプションをオフにする必要があります。RSTP/STP とリング形冗長構成を同時に使用することはできません。

STP は IEEE 802.1D-1998 に、また RSTP は IEEE 802.1w-2001 にそれぞれ規定されています。

C プラグ

C プラグは、SCALANCE X-400 のあらゆる設定情報を格納する脱着式メディアです。SCALANCE X-400 の交換時には前の装置に挿入していた C プラグを新しい装置にそのまま挿入するだけです。新しい SCALANCE X-400 が前の装置の設定で起動します。

アドレステーブル

SCALANCE X-400 のアドレステーブルには受信フレームの転送先ポートに関する情報が書かれています。このテーブルにはスタティックな内容（ユーザが設定）とダイナミックな内容（SCALANCE X-400 が受信したフレームに基づいて学習）の両方が存在します。

ポートのロック

ポートに対してこの機能をオンにすると、SCALANCE X-400 は送信元アドレスがアドレステーブルに存在するときのみ、そのポートで受信したフレームを転送します。

付記

リングポートはロック機能を有効（enabled）にすることができません。

ミラーリング

ミラーリングは、あるポートのデータトラフィックを別のポート（監視ポート）にコピーする機能です。運用に影響を与えることなくデータトラフィックの分析をこの監視ポートで行えます。

電子メール機能

あるイベントが発生したときに SCALANCE X-400 が電子メールを送信するように設定できます。

イベントログテーブル

イベントログテーブルは、SCALANCE X-400 の動作中に発生したイベントをロギングします。ユーザはログ採取したいイベントを指定できます。

時刻同期

SCALANCE X-400 ではシステム時刻を外部クロック送信機に同期させることができます。この機能を使用するには、SICLOCK クロック送信機や、スイッチがフレームを評価できる SNTP サーバなどが必要です。この機能により、イベントログテーブルのログデータがもつタイムスタンプがシステム全体で共通化できます。そのためシステム全体での発生時刻順にイベントがソートでき、問題原因の特定作業が効率化されます。

フロー制御

SCALANCE X-400 は、半二重と全二重でのフロー制御をサポートします。

BOOTP/DHCP

SCALANCE X-400 は、BOOTP サーバまたは DHCP サーバによる動的な IP アドレス割り当てに対応しています。

バージョン 2 のファームウェアでは、DHCP を有効にしていれば DHCP モードを選択できます。それ以前のバージョンの場合、DHCP は MAC アドレスを使って実現されます。

付記

ルーティング機能（SCALANCE X414-3E のみ）を有効にしている場合、DHCP および BOOTP は無効になります。

付記

DHCP と BOOTP が対応できるのはインバンドのエージェント IP 設定のみです。SCALANCE X414-3E におけるアウトバンドのエージェント IP 設定は手動でしか設定できません。

PROFINET IO

バージョン 2 のファームウェアでは、スイッチを PROFINET IO 機器として使用することができます。

Telnet

SCALANCE X-400 の CLI（コマンドラインインタフェース）は LAN またはインターネットから Telnet を使って制御できます。

付記

同時に 3 本までの CLI 接続（シリアルと LAN）が可能です。

SNMPv3

SCALANCE X-400 は、SNMPv1、SNMPv2、および SNMPv3 をサポートします。なかでも SNMPv3 はユーザ管理をプロトコルレベルで実行するだけでなく、セキュリティ機能（認証など）を提供します。SNMPv3 に関するユーザおよびグループの設定作業は、ウェブ型管理ツール、CLI（コマンドラインインタフェース）、または MIB オブジェクトへの直接アクセスによって行えます（MIB オブジェクトへの直接アクセスは精通者以外にはお勧めできません）。

IGMP スヌーピングと IGMP クエリ

SCALANCE X-400 は、IGMP スヌーピングだけでなく IGMP クエリ機能もサポートします。IGMP スヌーピングを有効にしていると IGMP フレームが評価され、マルチキャストフィルタテーブルがその情報を使って更新されます。IGMP クエリ機能も有効な場合、SCALANCE X-400 は IGMP クエリも送信し、IGMP に準拠するノードから応答を引き出します。

SCALANCE X414-3E のみ：レイヤ 3 機能（ルーティング）

SCALANCE X414-3E はルータとして設定することもできます。それによって多くの IP サブネットが相互接続可能となります。スタティックルーティングまたは RIP/OSPF ルータプロトコルあるいはその両方が使用できます。これらの標準化プロトコルを使用すれば、ネットワーク内に存在する他のルータと設定を同期させることが可能です。

IP アドレスの割り当て

はじめに

SCALANCE X-400 では設定と診断に関して多様な機能を使用できます。このような機能をネットワーク経由で使用する際には IP（インターネットプロトコル）が使われます。

IP プロトコルには IP アドレスを用いる独自のアドレス体系が備わっています。IP は OSI 参照モデルでいうレイヤ 3 のプロトコルであってハードウェアには依存しないため、柔軟なアドレス割り当てが可能です。その反面、レイヤ 2 通信（装置に対して MAC アドレスが固定的に付与される）とは異なり、装置に IP アドレスを明示的に割り当てる作業が必要になります。

この章では IP アドレスの構成について説明したあと、IP アドレスを SCALANCE X-400 に割り当てるいくつかの方法を示します。

SCALANCE X-400 に関する IP アドレスの種類

SCALANCE X-400 は IP アドレスを複数もつことができます。

- アウトバンド IP アドレス（SCALANCE X414-3E のみ）は管理作業に使用します。
- インバンドエージェント IP アドレスは管理作業に使用します。
- 上記以外の IP アドレス
この IP アドレスはルーティング専用のものでして設定できます（SCALANCE X414-3E のみ）。DHCP による設定はできないため、ウェブ型管理ツール、CLI、SNMP を使って割り当てる必要があります。

3.1 IP アドレスの構成

RFC 1518 と RFC 1519 のアドレスクラス

IP アドレスの範囲	最大ネットワーク数	1 ネットワーク当たりの最大ホスト数	クラス	CIDR
001.x.x.x~126.x.x.x	126	16777214	A	/8
128.0.x.x~191.255.x.x	16383	65534	B	/16
192.0.0.x~223.255.255.x	2097151	254	C	/24
マルチキャストグループ			D	
実験用			E	

IP アドレスは 4 バイトです。各バイトは 10 進数で表記され、前後をドットで区切ります。従って次のような構成になります。xxx は 0 から 255 までの数字です。

xxx.xxx.xxx.xxx

IP アドレスの割り当て

3.2 IP アドレスの初期割り当て

IP アドレスは、ネットワーク ID とホスト ID という 2 つの部分で構成されます。それによってさまざまなサブネットを生成することができます。IP アドレスのうちネットワーク ID に使用するバイト数とホスト ID に使用するバイト数によって IP アドレスのアドレスクラスが決まります。

サブネットマスク

サブネットはホスト ID のビットを使って作成できます。上位ビットがサブネットのアドレスを表し、残りのビットがそのサブネット内のホストアドレスを表します。

サブネットはサブネットマスクによって定義されます。サブネットマスクの構成は IP アドレスと同様です。サブネットマスクのあるビット位置が「1」とすると、それに対応する IP アドレスのビットはサブネットアドレスに属します。それ以外のビットはコンピュータ（ローカルホスト）のアドレスに属します。

クラス B ネットワークの例を以下に示します。

クラス B ネットワークの標準的なサブネットアドレスは「255.255.0.0」です。すなわち後ろの 2 バイトをサブネットの定義に使えます。かりに 16 個のサブネットを定義する必要がある場合、サブネットアドレスの第 3 バイトは「11110000」（2 進表記）にせねばなりません。このケースだとサブネットマスクは「255.255.240.0」になります。

2 つの IP アドレスが同じサブネットに属するかどうかは、2 つの IP アドレスとサブネットマスクについてビットごとの AND（論理積）を取ればわかります。両方の論理演算で結果が同じになれば両方の IP アドレスは同じサブネットに属します。たとえば 141.120.246.210 と 141.120.252.108 などがそうです。

LAN の外ではネットワーク ID とホスト ID の区別は意味がありません。その場合、パケットは IP アドレス全体をみて転送されます。

付記

サブネットマスクのビット表記では「1」を左詰にしてください（1 と 1 の間に 0 が入ってはなりません）。

3.2 IP アドレスの初期割り当て

設定ツール

SCALANCE X-400 に対する IP アドレスの初期割り当ては、ウェブ型管理ツールまたは Telnet による CLI（コマンドラインインタフェース）では行うことができません。これらの設定ツールを使うには IP アドレスがすでに付与されている必要があるためです。

IP アドレスが付与されていない未設定装置の IP アドレス割り当てには、以下の方法を使用できます。

- シリアルインタフェースと CLI
- DHCP
- BOOTP
- STEP 7

- NCM PC
- プライマリセットアップツール（インバンドポート経由のみ）

付記

出荷状態のモジュールまたは Restore Factory Defaults（工場設定値へのリセット）を行った場合には、デフォルトとして DHCP が設定されています。DHCP サーバが LAN 内にあり、しかもそれが SCALANCE X-400 の DHCP 要求に対して応答する場合、モジュールの最初の起動時に IP アドレス、サブネットマスク、およびゲートウェイが自動的に割り当てられます。DHCP と BOOTP が付与する IP アドレスは、固定アドレスと同様、Restore Memory Defaults では削除されません。

注

SCALANCE X414-3E では、アウトバンドポートとインバンドポートの IP アドレスを別々のサブネットにする必要があります。

例：

IP アドレス（アウトバンドポート）：140.90.45.66

IP アドレス（インバンドポート）：140.91.23.66

サブネットマスク

（アウトバンドポートとインバンドポート）：255.255.0.0

3.3 シリアルインタフェースを用いた IP アドレスの割り当て

クロスケーブルの接続とログイン

SCALANCE X-400 の IP アドレスをシリアルインタフェースを用いて指定する手順は以下のとおりです。

1. SCALANCE X-400 のシリアルポートと PC をクロスケーブルで接続します。
2. ターミナルエミュレーションソフトを起動します。Windows では HyperTerminal などを使えます（手順については付録 A をご覧ください）。
3. 接続が確立されたら「Login.」というメッセージが出力されます。*admin*（管理者用）または *user*（ユーザ用。権限が制限されている）のいずれかのアクセス権に従ってログインし、Return キーを押します。
4. 「Password.」のプロンプトが出たらパスワードを入力します。下の付記もよくお読みください。
5. 「CLI>」と出力されたらサブメニューに進むために「AGENT」と入力します。この段階で、IP アドレスを設定するコマンドを入力できます。コマンドについては次章で説明します。

IP アドレスの割り当て

3.4 BOOTP クライアントによる SCALANCE X-400 の IP アドレス割り当て

付記

新たなパスワードが設定されていない（工場設定値のままである）場合、管理者ログイン用の有効なパスワードは「admin」、パーミッションが限定されるユーザログイン用のパスワードは「user」です。

シリアルインタフェースから問題なくログインできたらコマンドを入力できます。ログオフするには「exit」コマンドを使用します。ケーブルを抜いてもセッションは終了しません。

付記

パスワードを忘れた場合には、CPU モジュール（X414-3E の場合）または電源モジュール（X408-2 の場合）の SELECT/SET ボタンを使うことによって工場設定値にリセットできます。基本状態の表示モードが A（D1 と D2 のランプがともに off）のときに SELECT/SET ボタンを 12 秒間押し続けます（12 秒経過前にボタンを離すとリセットをキャンセルできます）。それまでに行った設定がすべて工場設定値に戻るため、「admin」と「user」のパスワードが再度有効になります。

CLI のコマンド

IP アドレスを CLI（コマンドラインインタフェース）で設定する AGENT サブメニュー配下のコマンドについては、「Agent Configuration メニュー」の項に記載しています。

CLI の一般的な事項については「コマンドラインインタフェース（CLI）」をご覧ください。

3.4 BOOTP クライアントによる SCALANCE X-400 の IP アドレス割り当て

アドレス割り当て処理

BOOTP（Bootstrap Protocol）は IP アドレスを自動割り当てするプロトコルです。このタイプのアドレス割り当てを行うには、ネットワーク内に BOOTP サーバが必要です。

IP アドレスをもたないノード（BOOTP クライアント）が自身の MAC アドレスを使ってネットワーク上の全装置に BOOTP クエリを送出します（MAC のブロードキャストアドレス：FF-FF-FF-FF-FF-FF）。サーバからの応答もブロードキャストで送られ、そこには IP アドレスだけでなく、そのクライアントの MAC アドレスも入っています。これを受け取ったクライアントは、MAC アドレスをもとにそれが自分用の IP アドレスかどうかを判断します。

BOOTP は UDP プロトコルを使用し、BOOTP サーバでは UDP ポート 67 を、BOOTP クライアントではポート 68 を使用します。

SCALANCE X-400 と BOOTP

出荷時には DCP (従ってプライマリセットアップツールまたは NCM を用いたアクセス) および DHCP が有効、BOOTP が無効になっています。

3.5 DHCP クライアントによる SCALANCE X-400 の IP アドレス割り当て

DHCP の特長

DHCP (Dynamic Host Configuration Protocol) は BOOTP を拡張したものです。ただし、いくつかの重要な相違点があります。

- DHCP の使用はブート段階に限定されません。通常の動作中にも使用できます。
- 割り当てた IP アドレスはある一定の時間 (「リースタイム」といいます) 内でのみ有効です。それを過ぎると、新たな IP アドレスを要求するか、または現行の IP アドレスのリースタイムを延長することが必要です。
- 一般に固定アドレスの割り当ては行われません。すなわち、クライアントが IP アドレスを再度要求すると、通常は前とは異なるアドレスが割り当てられます。ただし、固定アドレスを割り当てるように DHCP サーバを設定することも可能です。

付記

DHCP が採用する体系では、IP アドレスは短時間 (リースタイム) の間しか割り当てられません。リースタイム終了時になっても DHCP サーバが見つからずに新規要求ができない場合、IP アドレス、サブネットマスク、およびゲートウェイは静的な値に変わります。

そのため DHCP サーバがなくても、最後に割り当てた IP アドレスを使って装置にアクセスすることが可能です。このような方式はオフィス機器では一般的ではありませんが、プラントではエラーフリー動作にとって必要な対策です。

DHCP クライアントはサーバに RELEASE を送出することもあるため、サーバはそのアドレスを別の装置に割り当てることができます。そのためネットワーク内に不一致が生じることがあります。

対処法 :

DHCP を無効に設定してから以下のいずれかを実施します。

- SCALANCE X-400 の IP アドレスを DHCP が割り当てていないアドレスに変更する
 - DHCP サーバのアドレスプールからその装置に割り当てられた IP アドレスを削除する
- 動的なアドレス割り当てと静的に割り当てるアドレスの混用はなるべく避けてください。
-

3.6 プライマリセットアップツールによる IP アドレスの割り当て

はじめに

PST（プライマリセットアップツール）は、IP アドレスをもたない未設定装置に対して IP アドレスを割り当てることができます。

前提条件

それを行うには、装置がデフォルトの MAC アドレス（イーサネットアドレス）をもち、かつネットワーク内においてオンラインでアクセスできることが必要です。

付記

詳しくはプライマリセットアップツールの設定マニュアルをご覧ください。

プライマリセットアップツールは SIEMENS - Automation and Drives - Service & Support のウェブサイト（エントリーID：19440762）でも入手できます。このエントリーID の URL は下記のとおりです。

<http://support.automation.siemens.com/ww/view/en/19440762>

ウェブ型管理ツールおよびコマンドライン インタフェースを用いた設定手順

はじめに

SCALANCE X-400 の機能や性能を最大限に活用できるよう、使用状況に合わせて装置設定を変更できます。SCALANCE X-400 を設定する方法は 2 とおりあります。

- SCALANCE X414-3E は、CPU モジュールのシリアルポートまたはイーサネットインタフェースの接続がなされていれば、コマンドラインインタフェースを用いた設定が可能です。
- SCALANCE X408-2 は、シリアルインタフェースの接続がなされていればコマンドラインインタフェースを用いた設定が可能です。
- ウェブ型管理ツール (WBM) はウェブブラウザを使って SCALANCE X-400 の設定を行います。SCALANCE X-400 とのインターネット接続が必要です。

注

SCALANCE X-400 への不正アクセス防止のため、使用する設定手段に応じて以下の対策が必要です。

- シリアルインタフェース経由の CLI
SCALANCE X-400 へのアクセスを終了するときは exit コマンドによるログオフが必要です。Windows のコンソールを閉じるだけやケーブル接続の切断だけでは十分ではありません。
 - Telnet
2 分間入力がないと Telnet 接続は自動的に切断されます。
 - ウェブ型管理ツール (WBM)
使用しているブラウザのウィンドウをすべて閉じてください。WBM を再度使用するにはパスワードが必要です。
-

付記

変更した設定内容は約 1 分後または再起動後にフラッシュメモリにおいて有効になります。そのため装置のスイッチを切る前に CLI またはウェブ型管理ツールで Restart コマンドを実行することを推奨します。それによってすべての変更内容が確実に保存されます。

付記

SNMP による管理、RMON (Remote Monitoring)、トラップを使用するにはネットワーク管理端末が必要です。これは SCALANCE X-400 製品には付属していません。

注

ウェブ型管理ツールのテキストボックスへの文字入力には a~z、A~Z、0~9 の文字のみ使用できます (特殊文字は使用できません)。

4.1 ウェブ型管理ツールおよびコマンドラインインタフェースに関する基本事項

4.1.1 はじめに

ウェブ型管理ツールの原理

SCALANCE X-400 にはウェブ型管理ツールのための HTTP サーバが組み込まれています。ウェブブラウザで SCALANCE X-400 にアクセスすると、ユーザの入力に応じた HTML ページがクライアント PC に送られてきます。

ユーザは SCALANCE X-400 から送られてくる HTML ページに設定データを入力します。SCALANCE X-400 はこの情報をチェックし、その内容に合わせて応答ページを生成します。この方法の大きな長所は、クライアント側にウェブブラウザがあればよく、特別なソフトウェアが必要ないことです。

ウェブ型管理ツールのシステム条件

- ウェブ型管理ツールを使用するには SCALANCE X-400 に IP アドレスが付与されていることが必要です。
- ウェブ型管理ツールを使用するには SCALANCE X-400 とクライアント PC の間にイーサネット接続が必要です。
- Microsoft Internet Explorer のバージョン 5.5 以上の使用を推奨します。
- ウェブ型管理ツールの全ページにおいて JavaScript が必要です。ブラウザの設定で JavaScript が有効になっていることを確認してください。

付記

ブラウザは、ページにアクセスするたびにそのページがサーバからリロードされないように設定する必要があります。ページの動的コンテンツの更新は他の方法で行われます。正しい設定を行うには、Internet Explorer の[ツール] > [インターネットオプション] > [全般]メニューにおいて[インターネット一時ファイル]の[設定]ボタンを使用します。

[保存しているページの新しいバージョンの確認]の下にある[自動的に確認する]の項目を選択します。

- ウェブ型管理ツールは HTTP プロトコルを使用するため、ファイアウォールを使用している場合はポート 80 を開けておく必要があります。

ウェブ型管理ツールのメニュー構成

ウェブ型管理ツールのメニュー構成を以下に示します。

ウェブ型管理ツールおよびコマンドラインインタフェースを用いた設定手順

4.1 ウェブ型管理ツールおよびコマンドラインインタフェースに関する基本事項

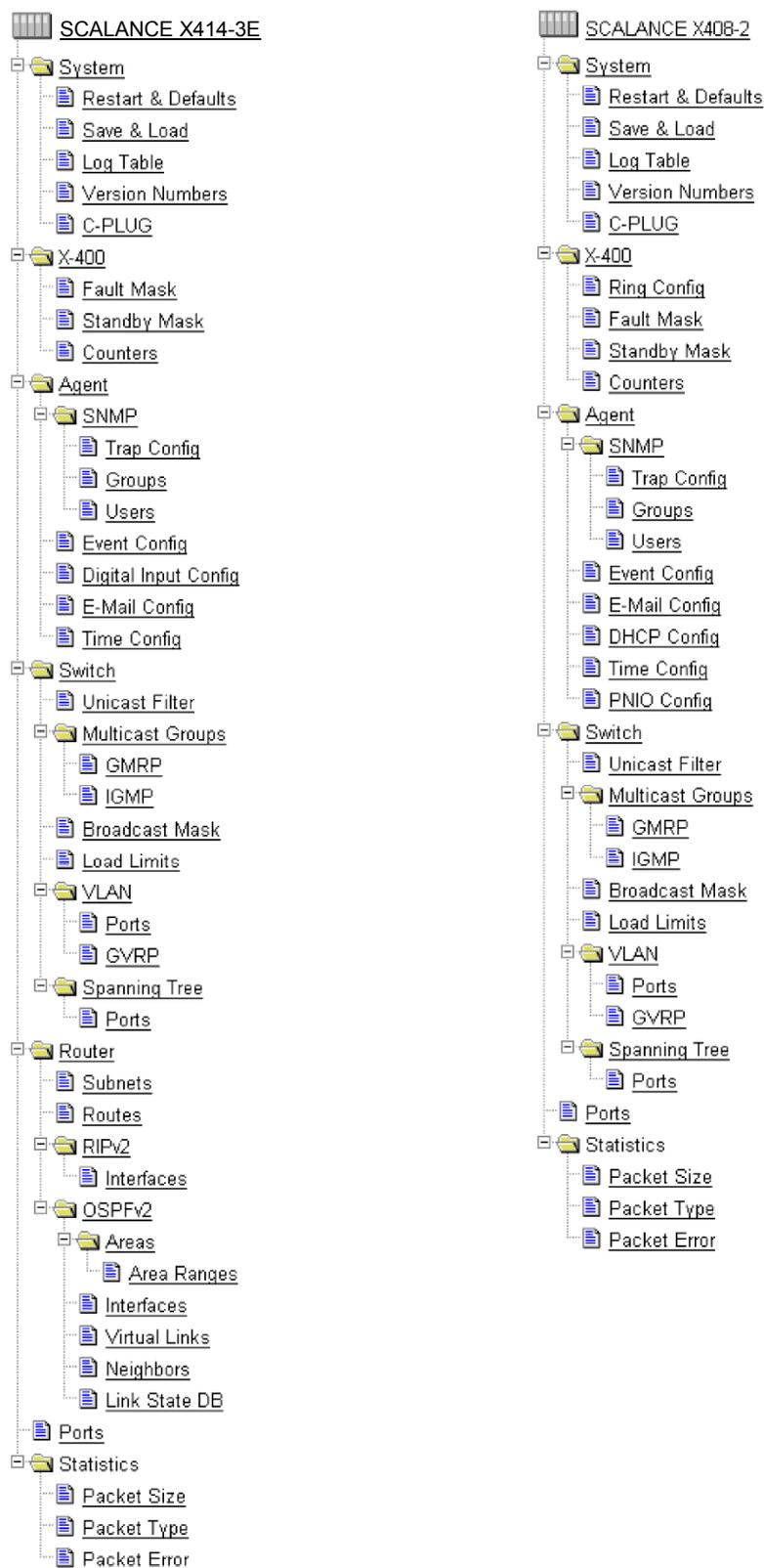


図 4-1 SCALANCE X414-3E と SCALANCE X408-2 のメニュー構成

4.1.2 ウェブ型管理ツール (WBM) の疑似ランプ

稼働状態の表示

SCALANCE X-400 の各コンポーネントには、装置の稼働状態を示すランプがいくつかあります。装置の位置によっては SCALANCE X-400 に直接アクセスできないことがあるため、ウェブ型管理ツールにはランプを疑似的に表示する機能があります。

画面の上 1/4 には SCALANCE X-400 に実装されるモジュールとランプの略図が示されます。ただし、ランプのトラフィック表示は実際と異なり点滅しません。ランプ表示の意味については『SCALANCE X-400 操作説明書』に記載されています。

図のモジュールの上にかかれた名前をクリックすると、装置のボタンと同じように疑似ランプの表示モード (DM1/DM2 または D1/D2 のランプ) を変えることができます。

付記

SCALANCE X414-3E のメディアモジュール用エクステンダが疑似表示されるには、少なくとも 1 枚のモジュールが実装されている必要があります。

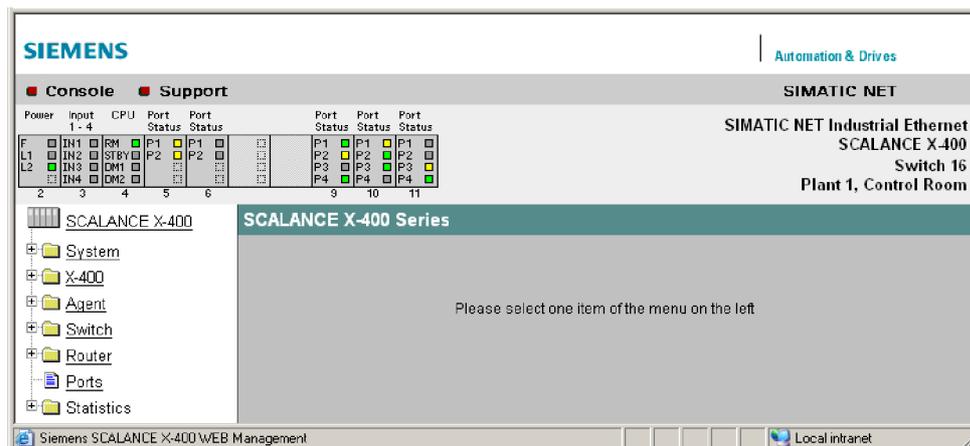


図 4-2 SCALANCE X414-3E の疑似ランプ

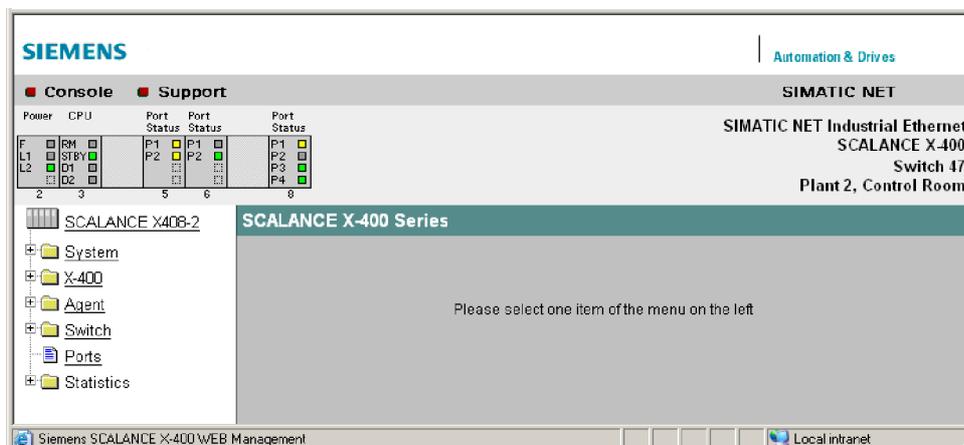


図 4-3 SCALANCE X408-2 の疑似ランブ

4.1.3 ウェブ型管理ツールの基本操作

ナビゲーションバー

WBM の上部メニューバーには次のリンクがあります。

- Console
コンソールウィンドウが開きます。このウィンドウでは CLI コマンドを使用できます。スイッチとは Telnet 接続によって接続されます。
- Support
このリンクをクリックするとシーメンス社のサポートページが開きます。ただし、サポートページにアクセスするにはインターネットに接続できる環境が必要です。

Refresh による表示の更新

設定データを表示するページの最下部には[Refresh]ボタンがあります。このボタンをクリックすると SCALANCE X-400 の最新データが要求され、最新ページが表示されます。

Set Values による設定の保存

設定変更が可能なページの最下部には[Set Values]ボタンがあります。このボタンをクリックすると、入力した設定データが SCALANCE X-400 に保存されます。

付記

設定データの変更は管理者ログイン時のみ行えます。

4.1.4 コマンドラインインタフェース (CLI)

CLI を Windows コンソールから起動する

CLI を Windows コンソールから起動するには以下の手順に従います。

1. Windows コンソールを開き、telnet コマンドに続いて SCALANCE X-400 の IP アドレスを入力します。C:¥>telnet <IP アドレス>
2. ログイン名とパスワードを入力します。

CLI をウェブ型管理ツールで起動する

ウェブ型管理ツールの上部メニューバーにおいて[Console]をクリックします。開いたコンソールには CLI コマンドを直接入力できます。IP アドレスはウェブ型管理ツールがもっており、ログインデータは WBM の起動時に入力しているの必要ありません。

コマンドのショートカット

CLI コマンドをフル入力する代わりに最初の 1 文字または数文字を入力して Tab キーを押すという方法があります。その場合、入力した文字で始まるコマンドのひとつが表示されます。所望のコマンドと異なる場合は、Tab キーをもう 1 度押して次のコマンドを表示させます。

ディレクトリ構成

CLI でコマンドを入力するにはまずメニューかサブメニューを開く必要があります。この章では各メニューに用意されているコマンドを表形式で示します。表にはコマンドそのもののみを記載しています。

ポートの指定体系

ポートの指定には下記に示す体系が用いられます。

- 最初の数字はスロット番号を表します。基本装置にはスロット 5 から 11 まであります。ツイストペア用エクステンダはスロット 12 と 13、メディアモジュール用エクステンダはスロット 12 から 15 までです。
- 2 番目の数字はピリオドで区切られ、ポート番号を表します。

たとえば「6.2」はスロット 6 のポート 2 です。

CLI コマンドを表す記号

CLI コマンドは一般にパラメータ (引数) が 1 つ以上あります。シンタックス表記では次のように書かれます。

- 必須パラメータは山カッコに入れて表します。
例: <IP アドレス>

イタリックで書かれた部分に実際の値を入力します。たとえば上記のパラメータでは以下のような実際の IP アドレスを入力します。

141.120.246.210

必須パラメータを省略すると、たいていのコマンドは現在値を表示します。

- いずれかの入力値を入れる場合には各入力値をパイプ文字 (|) で区切ります。その場合、示された値の1つをパラメータとして指定します。

例 : <E|D>

「E」か「D」のいずれかを入力します。

- 必須パラメータとして数値が必要な場合には値の範囲を指定することもできます。

例 : <0...255>

0 から 255 までの値を入力します。

メニューに依存しないコマンド

以下のコマンドはどのメニューまたはサブメニューにおいても使用できます。

表 4-1 コマンドラインインタフェース : CLI¥ ... >

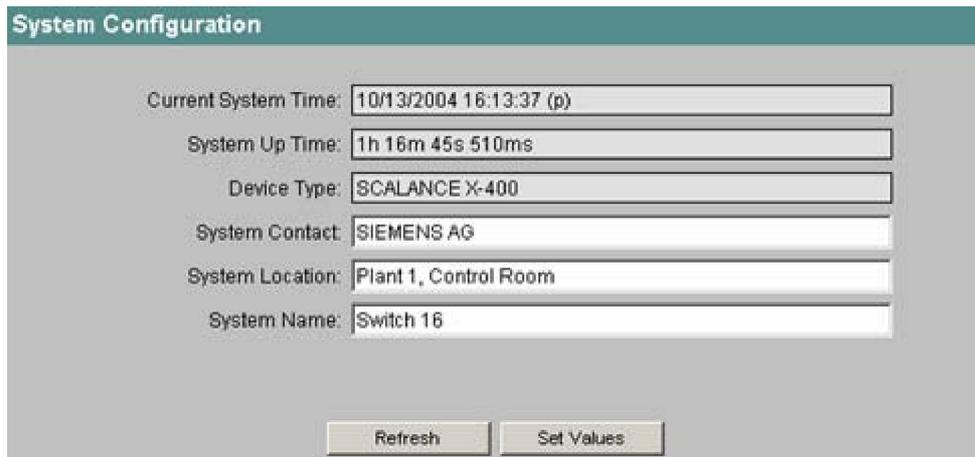
コマンド	説明	備考
/	1つ上位のメニューに移動します。	
?	そのメニューで使用できるコマンドを表示します。	
exit	CLI/Telnet のセッションを終了します。	
restart	SCALANCE X-400 を再起動します。	
About	現在のメニューに関する情報を表示します。	

4.2 システムメニュー

4.2.1 System Configuration メニュー

装置の基本情報

[System]フォルダのアイコンをクリックするとこの画面が表示されます。



The screenshot shows a web interface titled "System Configuration". It contains several input fields with the following values: "Current System Time: 10/13/2004 16:13:37 (p)", "System Up Time: 1h 16m 45s 510ms", "Device Type: SCALANCE X-400", "System Contact: SIEMENS AG", "System Location: Plant 1, Control Room", and "System Name: Switch 16". At the bottom, there are two buttons: "Refresh" and "Set Values".

図 4-4 System Configuration の画面

Current System Time (読み出し専用)

システム時間はユーザによって設定されるか、または time-of-day フレーム (SINEC H1 時間フレームまたは SNTP) によって同期されます。設定したときの方法もわかります。

- (m) 手動で設定されました。
- (t) SIMATIC の time-of-day フレームによって設定されましたが、クロック送信機による同期は行われていません。
- (s) SIMATIC の time-of-day フレームによって設定され、クロック送信機による同期が行われています。
- (p) SNTP プロトコルによって設定されました。

System Up Time (読み出し専用)

最後に再起動してからの経過時間です。

Device Type (読み出し専用)

機種名です。

System Contact

装置の管理責任者の名前を入力します。

System Location

装置の設置場所（部屋番号など）を入力します。

System Name

装置の簡単な説明を入力します。

CLI のシンタックス

表 4-2 System Configuration : CLI¥SYSTEM>

コマンド	説明	備考
setsysc <Name>	sysContact の MIB オブジェクトを設定します。	管理者のみ。
setsysl <location>	sysName の MIB オブジェクトを設定します。	管理者のみ。
setsysn <device name>	sysLocation の MIB オブジェクトを設定します。	管理者のみ。

表 4-3 System Configuration : CLI¥SERVICE>

コマンド	説明	備考
passwd <admin user> <password>	admin または user に対して新しいパスワードを設定します。	管理者のみ。

4.2.2 System Restart and Defaults メニュー

デフォルトへのリセット

この画面には装置を再起動するボタンのほか、装置をデフォルト値にリセットするオプションがあります。

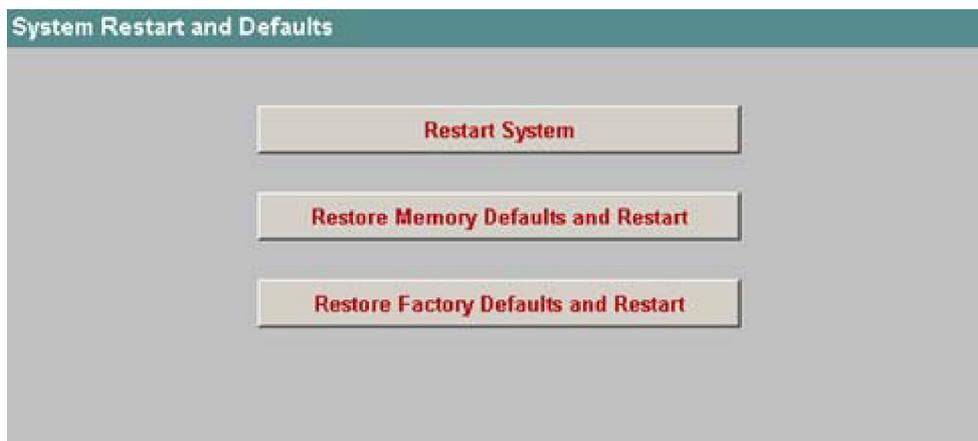


図 4-5 System Restart and Defaults の画面

付記

SCALANCE X-400 の再起動に関しては以下の点に注意してください。

- SCALANCE X-400 の再起動を行うには管理者権限が必要です。
 - SCALANCE X-400 の再起動を行う場合は、必ずこのメニューのボタンまたは対応する CLI コマンドを用いてください。装置の電源再投入は行わないでください。
 - 変更内容は WBM の各ページの[Set Values]ボタンをクリックした段階で保存されます。再起動の前に設定データを保存する必要はありませんし、またそのような操作は行えません。
-

Restart System ボタン

SCALANCE X-400 を再起動します。ダイアログボックスにおいて再起動の実行を確定することが必要です。再起動すると SCALANCE X-400 は初期化され、内部ファームウェアがリロードされて自己診断が行われます。学習によって得たアドレステーブルのエントリは消去されます。SCALANCE X-400 の再起動中もブラウザウィンドウは開いたままにしておかれません。

Restore Memory Defaults and Restart ボタン（ファームウェア 1.2 版以前）

下記のパラメータを除いて工場設定値にリセットします。

- IP アドレス（インバンドとアウトバンド）
- サブネットマスク（インバンドとアウトバンド）
- デフォルトゲートウェイの IP アドレス
- DHCP/BOOTP フラグ
- システム名
- システム収容位置
- システム連絡先

Restore Memory Defaults and Restart ボタン（ファームウェア 2.0 版）

下記のパラメータを除いて工場設定値にリセットします。

- IP アドレス（インバンドとアウトバンド）
- サブネットマスク（インバンドとアウトバンド）
- デフォルトゲートウェイの IP アドレス
- DHCP/BOOTP フラグ
- システム名
- システム収容位置
- システム連絡先

- リング形冗長機能
- スタンバイ機能
- STP/RSTP
- PNIO 装置名（端末の名前）

自動的に再起動が行われます。ユーザモードではこのボタンは表示されません。

Restore Factory Defaults and Restart ボタン

設定を工場設定値にリセットします。保護されたデフォルト値もリセットされます。ユーザモードではこのボタンは表示されません。

付記

すべての値が工場設定値にリセットされるため、IP アドレスも失われます。そのため SCALANCE X-400 にはプライマリセットアップツールかシリアルインタフェースでしかアクセスできなくなります。

CLI のシンタックス

表 4-4 System Restart & Defaults : CLI>

コマンド	説明	備考
restart	SCALANCE X-400 の再起動。	管理者のみ。 このコマンドはすべてのメニューから実行できます

表 4-5 System Restart & Defaults : CLI¥SYSTEM>

コマンド	説明	備考
defaults	工場設定値にリセットします。保護された設定もリセットされます。装置は再起動されます。	管理者のみ。 このコマンドの作用は、WBM で [Restore Factory Defaults and Restart] ボタンをクリックしたときと同じです。
memreset	工場設定値にリセットします。保護された設定は保持されます。装置は自動的に再起動されます。	管理者のみ。 このコマンドの作用は、WBM で [Restore Memory Defaults and Restart] ボタンをクリックしたときと同じです。

4.2.3 System Save & Load メニュー

TFTP サーバを用いたデータ交換

WBM では、設定情報を外部ファイルに保存したり、逆に外部ファイルから SCALANCE X-400 にロードすることができます。またログ情報をファイルに保存したり、ファイルから新しいファームウェアをロードすることもできます。System Save & Load メニューではこの作業に必要なエントリを作成できます。

System Save & Load

TFTP Server IP Address: 192.168.200.1

TFTP Server IP Port: 69

Configuration File: cfg20000915.bt Save

Load and Restart

Log Table File: log20000915.bt Save

Firmware File: cv122005.lad Load

Refresh Set Values

図 4-6 System Save & Load の画面

TFTP Server IP Address

データ交換を行いたい TFTP サーバの IP アドレス。

TFTP Server IP Port

データ交換が処理される TFTP サーバのポート。必要であればデフォルト値の 69 を必要な値に変えることができます。

Configuration File

SCALANCE X-400 にロードしたい設定ファイルまたは現在の設定情報を保存したい保存先の名前（32 文字以内／ときにフォルダパス付き）。

Log Table File

ログテーブルの内容を保存したいファイルの名前（32 文字以内／必要ならフォルダパス付き）。

Firmware File

新しいファームウェアをロードしたいロード元ファイルの名前（32 文字以内／ときにフォルダパス付き）。

TFTP を使ったデータのロードもしくは保存の手順

1. [TFTP Server IP Address]欄に TFTP サーバの IP アドレスを入力します。
2. データの保存先ファイルまたはデータのロード元ファイルの名前（32 文字以内）を当該欄に入力します。
3. 次のエントリーについてデータの保存またはロードを行う前に[Set Values]ボタンをクリックします。
4. [Save]ボタンのクリックによって保存処理を開始します。ファイルからデータをロードするときは [Load]ボタンを、また設定ファイルをロードしたいときは[Load and Restart]ボタンをクリックします。装置は新しい設定で再起動します。

設定データの再利用

設定データを保存して読み出すことで、複数台の SCALANCE X-400 が同じ構成をもつ場合や IP アドレスを DHCP 経由で割り当てるときに作業量を減らすことができます。

SCALANCE X-400 の設定が終わったら設定データを TFTP サーバに保存します。

このファイルを、設定したい他のすべての SCALANCE X-400 にダウンロードします。

各装置に個別の設定が必要なときはオンラインで行うことが必要です。

設定データは保存時にエンコードされるため、ファイルをテキストエディタで編集することはできません。

CLI のシンタックス（ファームウェア 1.2 版以前）

表 4-6 System Save & Load : CLI¥SYSTEM>

コマンド	説明	備考
server <IP アドレス> [:ポート]	データ交換を行う TFTP サーバの IP アドレスを指定します。ポート指定はオプションです。	管理者のみ。 デフォルト値 : 0.0.0.0
cfgname <ファイル名>	設定データをロードする元のファイルまたは設定データを保存する先のファイルの名前（32 文字以内）を指定します。	管理者のみ。
cfgsave	設定データを TFTP サーバ上のファイルに保存します。	管理者のみ。
cfgload	TFTP サーバ上のファイルから設定データをロードします。	管理者のみ。
logname <ファイル名>	ログテーブルを保存する先のファイルの名前（32 文字以内）を指定します。	管理者のみ。
logsave	ログテーブルを TFTP サーバ上のファイルに保存します。	管理者のみ。
fwname <ファイル名>	ファームウェアをロードする元のファイルの名前（32 文字以内）を指定します。	管理者のみ。 デフォルト値 : 未定義
fwload	ファイルからファームウェアをロードします。	管理者のみ。

CLI のシンタックス (ファームウェア 2.0 版)

表 4-7 System Save & Load : CLI¥SYSTEM¥SAVELOAD>

コマンド	説明	備考
server <IP アドレス> [:ポート]	データ交換を行う TFTP サーバの IP アドレスを指定します。ポート指定はオプションです。	管理者のみ。 デフォルト値 : 0.0.0.0
cfgname <ファイル名>	設定データをロードする元のファイルまたは設定データを保存する先のファイルの名前 (32 文字以内) を指定します。	管理者のみ。
cfgsave	設定データを TFTP サーバ上のファイルに保存します。	管理者のみ。
cfgload	TFTP サーバ上のファイルから設定データをロードします。	管理者のみ。
logname <ファイル名>	ログテーブルを保存する先のファイルの名前 (32 文字以内) を指定します。	管理者のみ。
logsave	ログテーブルを TFTP サーバ上のファイルに保存します。	管理者のみ。
fwname <ファイル名>	ファームウェアをロードする元のファイルの名前 (32 文字以内) を指定します。	管理者のみ。 デフォルト値 : 未定義
fwload	ファイルからファームウェアをロードします。	管理者のみ。

4.2.4 System Event Log Table メニュー

イベントのログ採取

SCALANCE X-400 スイッチではイベントのログ採取および *Log Table* メニューでのログ表示を行えます。たとえば SNMP の認証失敗やポートの接続状態の変化などが記録できます。ログ採取を行うイベントの種類は [Agent] > [Event Config] のメニューで指定できます。ログテーブルの内容は SCALANCE X-400 の電源を切っても保持されます。

Restart	Sys. Up Time	Event
469	00:35:13	10/13/2004 15:31:31 (p) Link down on port 9.4.
469	00:34:16	10/13/2004 15:30:32 (p) Link up on port 9.4.
469	00:34:14	10/13/2004 15:30:30 (p) Link down on port 9.1.
469	00:32:45	10/13/2004 15:29:00 (p) (R)STP: topology change detected.
469	00:32:15	10/13/2004 15:28:30 (p) (R)STP protocol enabled, details: Running in RSTP (802.1w) mode.
469	00:32:15	10/13/2004 15:28:30 (p) (R)STP protocol disabled.
469	00:26:31	10/13/2004 15:22:41 (p) (R)STP: topology change detected.
469	00:26:14	10/13/2004 15:22:24 (p) Link up on port 9.1.
469	00:26:10	10/13/2004 15:22:21 (p) Link up on port 10.1.

図 4-7 System Event Log Table の画面

Restart 欄は対応するイベントが発生する前の装置の再起動を示します。

Sys. Up Time 欄は SCALANCE X-400 が再起動してからの経過時間を HH:MM:SS のフォーマットで示します。

Refresh ボタン

表示を最新のものに更新します。

Clear Log ボタン

ログテーブルの内容を消去します。

CLI のシンタックス

表 4-8 System Event Log Table : CLI¥SYSTEM>

コマンド	説明	備考
events <show clear>	ログテーブルの内容を表示または消去します。	ログテーブルの消去は管理者のみが行えます。ログテーブルの内容は SCALANCE X-400 の電源を切っても保持されます。
addlog <テキスト>	ログテーブルに文章を挿入します。文中の空白はそのまま空白として処理されます。	

4.2.5 System Version Numbers メニュー

ハードウェアとソフトウェアの版数

SCALANCE X-400 の現在のハードウェアとソフトウェアの版数を表示します。

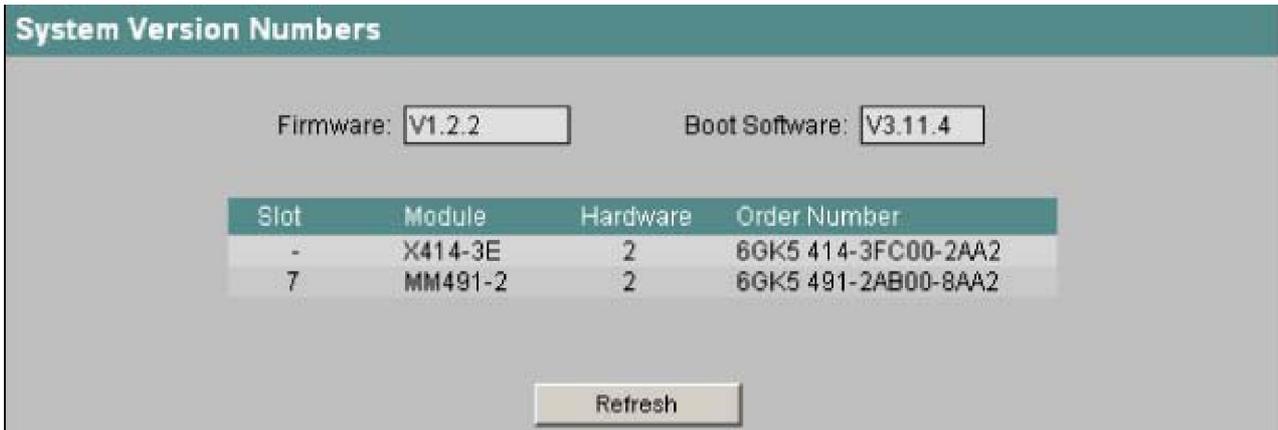


図 4-8 System Version Numbers の画面

Boot Software

ブートソフトウェアの版数が表示されます。ブートソフトウェアはスイッチに恒久的に格納され、新しいファームウェアのロードに使用されます。

Firmware

SCALANCE X-400 で動いているファームウェアの版数です。

基本装置とモジュールのデータを示す表

表の 1 行目には SCALANCE X-400 の基本装置の版数が表示されます。Slot は基本装置のスロット番号です。基本装置そのもののデータについては（モジュールは存在しない／しえないため）この欄は「-」になります。Hardware はモジュールまたは基本装置の版数、Order Number は注文番号です。

CLI のシンタックス

表 4-9 System Version Numbers : CLI>

コマンド	説明	備考
info	SCALANCE X-400 の現在のソフトウェア版数などの情報を表示します。	

表 4-10 System Version Numbers : CLI¥SYSTEM>

コマンド	説明	備考
version	SCALANCE X-400 の現在のハードウェア版数を表示します。	

4.2.6 C-PLUG Information メニュー

C プラグの内容

このメニューでは C プラグに関する詳細が表示されます。C プラグのフォーマットや新しい内容の書き込みも行えます。

The screenshot shows the 'C-PLUG Information' menu with the following fields and values:

- C-PLUG State: NOT ACCEPTED
- C-PLUG Device Group: SCALANCE X-400
- C-PLUG Device Type: SCALANCE X414-3E
- Configuration Revision: 1
- File System: SIMATIC NET FS
- File System Size: 3145728 Byte
- File System Usage: 1048576 Byte
- C-PLUG Info String: 6GK5 414-3FC00-2AA2
SCALANCE X414-3E
HW: V1
SW: V3.1
- Modify C-PLUG: Load default Configuration to C-PLUG and Restart (dropdown menu)
- Buttons: Modify, Refresh

図 4-9 C-PLUG Information の画面

このメニューのテキストボックスはすべて読み出し専用です。

C-PLUG State

C プラグの状態が表示されます。以下の状態があります。

- ACCEPTED
有効かつ一致する内容をもつ C プラグが装置に挿入されています。
- NOT ACCEPTED
C プラグが挿入されていないか、または挿入されていても内容が無効もしくは不適合です。装置の稼働中に C プラグがフォーマットされた場合にもこの状態が表示されます。
- NOT ACCEPTED, HEADER CRC ERROR
内容に誤りのある C プラグが挿入されています。
- NOT PRESENT
装置には C プラグが挿入されていません。

C-PLUG Device Group

その C プラグを以前に使用した SIMATIC NET 製品シリーズを示します。

C-PLUG Device Type

その C プラグを以前に使用した上記製品シリーズの機種を示します。

Configuration Revision

設定構造のバージョンを示します。この情報はその装置がサポートする設定オプションに関連するものであり、実際のハードウェア構成には関係しません。したがってモジュールやエクステンダを追加・削減してもこの情報は変わりません。ただしファームウェア更新を行うと変わることがあります。

File System

C プラグ上のファイルシステムの種類を示します。

File System Size

C プラグ上のファイルシステムの最大記憶容量を示します。

File System Usage

C プラグにおけるファイルシステムの占有量を示します。

C-PLUG Info String

その C プラグを以前に使用した装置に関する追加情報（注文番号、機種名、ハードウェアとソフトウェアの版数など）をすべて示します。

Modify C-PLUG リストボックスと Modify ボタン

管理者でログインしている場合にのみ使用できます。C プラグの内容の変更方法を指定します。以下の選択肢があります。

- **Copy internal Configuration to C-PLUG and Restart**
スイッチの内蔵フラッシュメモリに格納された設定情報が C プラグにコピーされ、そのあと再起動されます。
この機能は次に示す重要な場面で必要になります。
C プラグを挿入した状態で装置を起動したが、C プラグに書かれている設定情報にエラーが含まれているか、またはその装置のものとは異なっている場合。装置の起動後に設定を変えていなければ、この機能を用いて C プラグの内容を最初の装置設定に上書きすることができます。
- **Copy default Configuration to C-PLUG and Restart**
設定をすべて工場設定値にして C プラグに格納します。続いて再起動が行われ、SCALANCE X-400 が工場設定値を使って立ち上がります。
- **Clean C-PLUG (Low Level Format, Configuration lost)**
C プラグの全データを消去し、低レベルフォーマットを開始します。自動再起動は行われず、装置にはエラーが表示されます。このエラーは再起動または C プラグの取り外しによって解消されます。

選択して[Modify]ボタンをクリックすると、その機能が実行されます。

CLI のシンタックス

表 4-11 C-PLUG Information : CLI¥SYSTEM¥C-PLUG>

コマンド	説明	備考
info	C プラグの現在の状態を表示します。	WBM の <i>C-PLUG Information</i> と同じ内容を表示します。
copyint	C プラグをメインメモリの内容で上書きします。	管理者のみ。 WBM の <i>Copy internal Configuration to C-PLUG and Restart</i> コマンドと同じ機能です。
copydef	C プラグをデフォルトパラメータで初期設定します。	管理者のみ。 WBM の <i>Copy default Configuration to C-PLUG and Restart</i> コマンドと同じ機能です。
clean	C プラグのデータをすべて消去し、低レベルフォーマットを実行します。	管理者のみ。 WBM の <i>Clean C-PLUG</i> コマンドと同じ機能です。

4.3 X-400 メニュー

4.3.1 X-400 Status メニュー

運転状態に関するデータ

[X-400]フォルダのアイコンをクリックするとこの画面が表示されます。

この画面では、スイッチが冗長化マネージャで運転されているかどうかや、その場合にリングが開いているか閉じているかが表示されます。スタンバイ機能に関する装置状態も示されます。このほか電源や障害状態についても示されます。この画面のテキストボックスは読み出し専用です。

X-400 Status

Standby Function:

Standby Status:

RM Function:

RM Status:

Ring Ports:

Power Line 1:

Power Line 2:

Fault Status:

図 4-10 X-400 Status の画面

Standby Function

- Master :
装置は相手側装置と接続され、かつマスタとして動作しています。通常運転時、この装置のスタンバイポートはアクティブです。
- Slave :
装置は相手側装置と接続され、かつスレーブとして動作しています。通常運転時、この装置のスタンバイポートは非アクティブです。
- Disabled :
スタンバイリンクは無効化されています。装置はマスタとスレーブのいずれでもありません。スタンバイポートはスタンバイ機能のない通常ポートとして動作しています。
- Waiting for Connection... :
相手側装置との接続がまだ確立されていません。スタンバイポートは非アクティブです。この状態が示される場合、相手側装置の設定がこちら側の装置と一致しない（接続名が正しくない、スタンバイリンクが無効など）か、または物理的な障害（装置障害やリンク断など）が存在します。
- Connection Lost :
相手側装置との接続が失われています。この状態が示される場合、物理的な障害（装置障害やリンク断など）が存在するか、または相手側装置の設定が変更されています（接続名が正しくない、スタンバイリンクが無効など）。

スタンバイリンクの設定および有効化・無効化については、4.3.4「X-400 Standby Mask メニュー」のセクションをご覧ください。ここでは状態情報についてのみ説明します。

Standby Status

- active :
スタンバイポートはアクティブです。
- passive :
スタンバイポートは非アクティブです。

RM Function

- disabled :
スイッチは冗長化マネージャとして動作していません。
- enabled :
スイッチは冗長化マネージャとして動作しています。
SCALANCE X414-3E の DIL スイッチは「RM on」の位置にあります。SCALANCE X408-2 では RM 機能は CLI または WBM を使って有効化されます。

RM Status

- passive :
スイッチは冗長化マネージャとして動作し、かつリングが開かれています。すなわちスイッチ類とリングポートの間の回線は問題なく機能しています。スイッチが冗長化マネージャとして動作していない（RM Function が disabled）場合にも passive と表示されます。
- active :
スイッチは冗長化マネージャとして動作し、かつリングが閉じています。すなわちスイッチ類とリングポートの間の回線が断線しています（問題があります）。冗長化マネージャは 2 つのリングポートを開通し、断線したバス形トポロジを復旧させます。

Ring Ports

リングポートとして機能するポートの位置を示します。SCALANCE X414-3E については以下の場合があります（設定は装置の DIL スイッチで行います）。

- 2 つのギガビットポートがリングポートである (5.1/5.2)
- 1 枚目のファストイーサネット用メディアモジュールにある 2 つのポートがリングポートである (6.1/6.2)
- 1 枚目のファストイーサネット用メディアモジュールにある第 1 のポートと、2 枚目のファストイーサネット用メディアモジュールにある第 1 のポートがリングポートである (6.1/7.1)

SCALANCE X408-2 におけるリング形冗長機能とリングポートの設定は、CLI または WBM を用いて行います。

付記

リング形冗長機能が完全に無効化されている場合にはリングポートは表示されず、代わりに「Ring Redundancy disabled」と表示されます。

Power Line 1

- up :
電源 1 (ライン 1) は給電されています。
- down :
電源 1 (ライン 1) に給電がないか、または許容電圧を下回っています。

Power Line 2

- up :
電源 2 (ライン 2) は給電されています。
- down :
電源 2 (ライン 2) に給電がないか、または許容電圧を下回っています。

Fault Status

SCALANCE X-400 の障害状態を表示します。表示される可能性のあるエラーメッセージを下の表にまとめます。複数の問題が同時に発生した場合には該当するものが上下に併記されます。

以下のエラーメッセージがあります。

エラーメッセージ	意味
Redundant power line down	二重化電源の障害です。
Link down on monitored port	監視対象ポートに対するリンクが切断されています。
More than one RM in ring	冗長化マネージャとして動作する装置がリング内に複数台存在します。
Valid only for SCALANCE X414-3E: RM DIL switch changed. Please restart!	RM の DIL スイッチの設定が変更されたため、スイッチの設定が装置の設定データと合わなくなりました。装置の設定変更を適用するには再起動が必要です。
Non-recoverable ring error	復旧できないリング障害が発生しました。
Factory Defaults, please restart	工場設定値にリセットされたため、現在の動作状態が装置の設定データと合わなくなりました。装置の設定変更を適用するには再起動が必要です。
No Fault	障害は検出されていません（信号用接点に変化がなく、障害ランプも点いていません）。

CLI のシンタックス

表 4-12 X-400 Status : CLI#X-400>

コマンド	説明	備考
info	SCALANCE X-400 の状態を表示します。	

4.3.2 X-400 Ring Configuration メニュー (SCALANCE X408-2)

SCALANCE X-400 のリング構成

付記

SCALANCE X414-3E のリング設定は DIL スイッチを用いて行います。

付記

Ring Configuration メニューは SCALANCE X408-2 で使用できます（ファームウェア 2.0 版）。

Ring Redundancy enabled チェックボックス

これをチェックするとリング形冗長機能がオンになります。この画面で設定したリングポートが使用されます。

Redundancy Manager (RM) enabled チェックボックス

これをチェックするとスイッチは冗長化マネージャとして機能します。

付記

スイッチが冗長化マネージャとして機能するには、リング形冗長機能がオンになっていることが必要です。

Ring Ports リストボックス

リング形冗長構成でリングポートとして使用するポートを指定します。

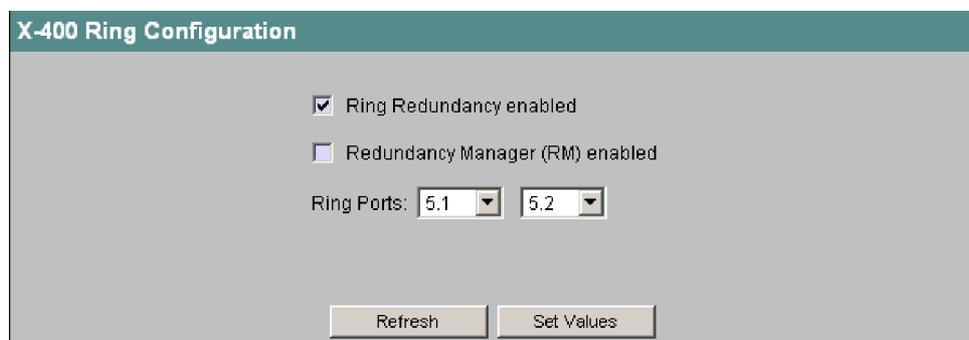


図 4-11 X-400 Ring Configuration の画面

注

工場設置値にリセットすると、リング形冗長機能はオン、冗長化マネージャはオフ、リングポートはポート 5.1 と 5.2 に設定されます。接続構成によってはリセット前に正しい設定だった SCALANCE X-400 においてフレームのループが発生し、データトラフィックが廃棄される原因になります。

CLI のシンタックス

表 4-13 X-400 Ring Configuration : CLI#X-400#RING>

コマンド	説明	備考
info	SCALANCE X-400 の現在のリング構成を表示します。	

コマンド	説明	備考
red [E D]	リング形冗長構成のオン・オフを行います。	管理者のみ。
rm [E D]	冗長化マネージャのオン・オフを行います。	管理者のみ。
ports [<ポート 1> <ポート 2>]	リングポートを指定します。両方のポートを指定する必要があります。	管理者のみ。

4.3.3 X-400 Fault Mask メニュー

障害マスクの機能

障害マスクは、SCALANCE X-400 で監視したときに信号用接点を作動させる障害状態を規定します。障害状態の例には、給電の有無、供給電圧の過小、相手先装置とのリンク断などがあります。信号用接点が発動すると装置の障害ランプが点灯するほか、イベントテーブルの設定に応じてトラップ送信、電子メール送信、ログテーブルへの記録を行うことができます。

ポートの装置関連リンク監視

SCALANCE X-400 は装置関連リンクの監視を行います。SCALANCE X-400 のリンク監視を有効にしている場合には、リンクの復旧または障害によってもメッセージシステムに影響を与えます。

装置上での障害マスク設定

障害マスクは SCALANCE X-400 前面にある SELECT/SET ボタンを使っても設定できます。詳しくは『工業用イーサネットスイッチ SCALANCE X-400 操作説明書』をご覧ください。

WBM を使った設定

WBM では電源の監視と装置関連リンクの監視について設定できます。

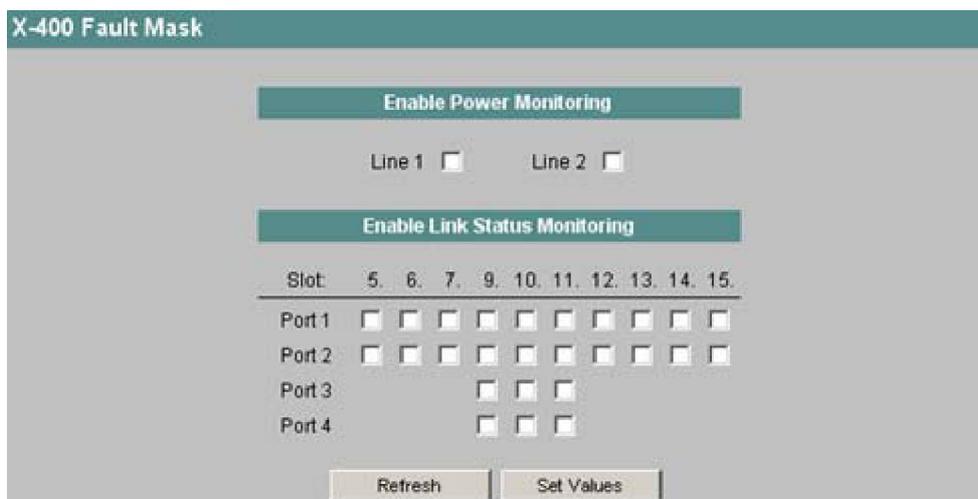


図 4-12 SCALANCE X414-3E の障害マスクの例

Enable Power Monitoring チェックボックス

2本ある電源供給線 1 と 2 について監視するものを指定します。監視しているラインのいずれか (line 1 または line 2) に給電がないか、または電圧が低すぎる (14 V 未満) 場合には、メッセージシステムによって障害が示されます。

Enable Link Status Monitoring チェックボックス

接続状態を監視したいスロット/ポートのチェックボックスを選択します。リンク監視を有効にしている場合に、ケーブルの未接続や接続先装置の電源オフなどによって有効なリンクがそのポートに確立されていないと、エラーが通知されます。

エラー通知の手段は、SCALANCE X-400 の設定に応じて以下のものが可能です。
信号用接点、障害ランプ、SNMP トラップ、電子メール、ログテーブルへの記録

CLI のシンタックス

表 4-14 SCALANCE X-400 Fault Mask : CLI¥X-400>

コマンド	説明	備考
link <E D> [ポート]	選択したポートのポート監視 (リンク監視) を有効または無効にします。ポートの指定がないときはすべてのポートが有効化・無効化されます。	管理者のみ。 パラメータに複数のポートを指定する場合は各ポートを空白で区切る必要があります。
power <E D> <1 2 1, 2>	電源コネクタ L1 と L2 の監視を有効または無効にします。	管理者のみ。

4.3.4 X-400 Standby Mask メニュー

リングの冗長結合

リング形冗長構成とは別に、SCALANCE X-400 はファームウェア 1.2 版現在、リングの冗長結合をサポートします（断線→バス形トポロジーを含みます）。冗長結合では 2 つのリングが 2 本のイーサネット接続によって結合されます。これを実施するには、一方のリングにマスタとスレーブの装置ペアを構成し、リングポートを使って互いを監視します。障害発生時には一方のイーサネット接続（マスタ）から他方のイーサネット接続（スレーブ）にデータトラフィックの流れを切り替えます。

イーサネット配線およびマスタとスレーブのトポロジー的な位置については、『工業用イーサネットスイッチ SCALANCE X-400 操作説明書』をご覧ください。

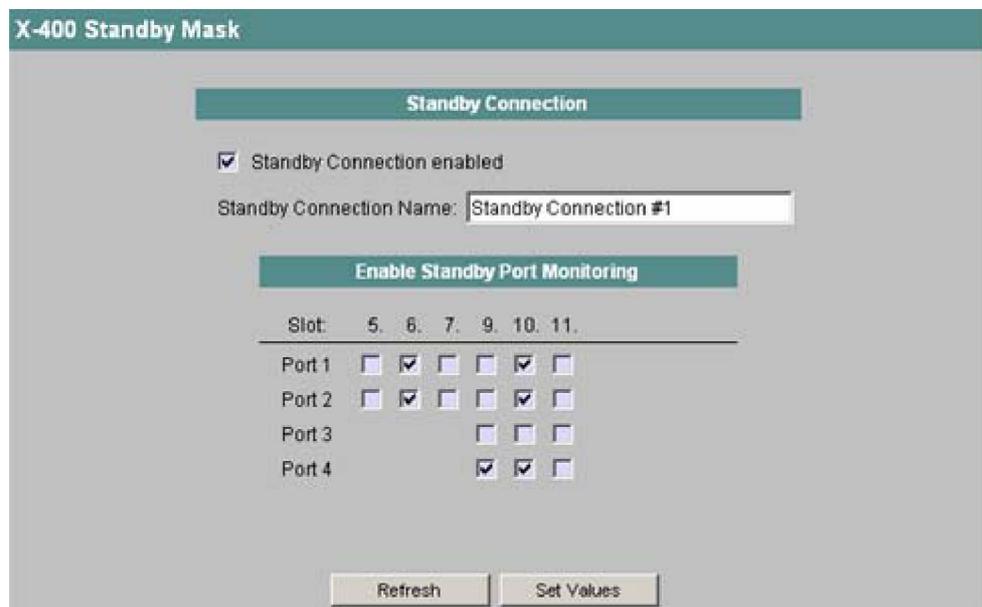


図 4-13 SCALANCE X414-3E のスタンバイマスクの例

Standby Connection enabled チェックボックス

スタンバイ機能のオン・オフを指定します。

Standby Connection Name

スタンバイ接続の名前を入力します。マスタ - スレーブの装置ペアはスタンバイ接続名によって定義します（両装置とも同じリングに属することが必要です）。これを行うにはリング内の 2 台の装置に対して同じ名前を入力します。目的に合わせて任意の名前が付けられますが、1 つの名前はネットワーク全体で 1 つの装置ペアにしか使用できません。

Enable Standby Port Monitoring チェックボックス

スタンバイポート（データトラフィックの切り替えに関わるもの）にするポートを指定します。問題がない状態ではマスタのスタンバイポートのみが動作し、それがデータトラフィックを処理します。マスタまたはマスタのスタンバイポートのいずれかのリンクに障害が発生すると、マスタのすべてのスタンバイポートは機能を停止し、スレーブのスタンバイポートが動作します。それによってリンクが復旧します。

注

いくつかのリングに対してリンクが存在する（Standby Port Monitoring で複数のポートがチェックされている）場合、スタンバイマスタとスタンバイスレーブは各リングに対して 1 本のイーサネット接続しかもつことができません。そうしないとフレームのループが発生し、データトラフィックが廃棄される原因になります。

CLI のシンタックス（ファームウェア 1.2 版以前）

表 4-15 X-400 Standby Mask : CLI¥X-400>

コマンド	説明	備考
info	SCALANCE X-400 の状態を表示します。	
standby <E D>	スタンバイ機能を有効化・無効化します。	管理者のみ。
stbports <E D> [ポート]	スタンバイポート監視を有効化・無効化します。	管理者のみ。
conname [接続名]	スタンバイ接続名を表示・指定します。	管理者のみ。

CLI のシンタックス（ファームウェア 2.0 版）

表 4-16 X-400 Standby Mask : CLI¥X-400¥STANDBY>

コマンド	説明	備考
info	スタンバイ構成の情報を表示します。	
standby <E D>	スタンバイ機能を有効化・無効化します。	管理者のみ。
stbports <E D> [ポート]	スタンバイポート監視を有効化・無効化します。	管理者のみ。
conname [接続名]	スタンバイ接続名を表示・指定します。	管理者のみ。

リング間をつなぐ冗長リンクの設定

リング間をつなぐ冗長リンクの設定手順は下記のとおりです。

1. リング内でマスタおよびスレーブとする装置、ならびにマスタおよびスレーブにおいて他のリングとのイーサネット接続に用いるポートを決定します。MAC アドレスの大きいほうがマスタになります。

付記

二重化されるイーサネットケーブルは設定が完了するまで接続しないでください。完了前に接続するとフレームのループが発生し、データトラフィックが廃棄される原因になります。冗長リンクを無効にする場合も同様です。

2. スタンバイ接続名を決め、これをマスタとスレーブの両装置について入力します。

付記

1 つのスタンバイ接続名（装置のペアに対して付与される）はネットワーク内で 1 つしか使用できません。

2. スタンバイ接続名を決め、これをマスタとスレーブの両装置について入力します。
3. [Enable Standby Port Monitoring]チェックボックスをチェックし、マスタとスレーブにおけるスタンバイポートを指定します。
4. [Standby Connection enabled]のオプションをチェックします。
5. [Set Values]ボタンをクリックして設定を確定します。
6. この段階ではじめて二重化イーサネットケーブルを接続します。

付記

二重化のイーサネットケーブルは必ず正しいポート、すなわち設定したスタンバイポートに接続してください。異なるポートに接続するとフレームのループが発生し、データトラフィックが廃棄される原因になります。

4.3.5 X-400 Counters メニュー

信号用接点の作動と二重化回路

運用中の問題発生の有無および頻度（信号用接点の作動頻度など）はカウンタを使って監視します。

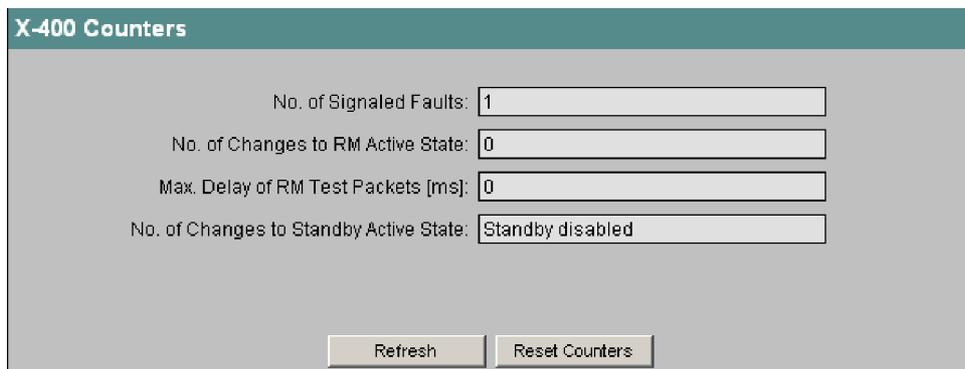


図 4-14 X-400 Counters の画面

No. of Signaled Faults

そのスイッチの信号用接点が作動した回数を示します。

No. of Changes to RM Active State

ここに値が表示されるのは、SCALANCE X-400 が冗長化マネージャとして動作する場合のみです（「X-400 Ring Configuration メニュー」の項を参照）。

SCALANCE X-400 がアクティブ状態に移行した回数を表します。冗長化マネージャがリングポートにつながるラインの断線を検出したときにこの状態になります。

Max. Delay of RM Test Packets[ms]

この値も SCALANCE X-400 が冗長化マネージャとして動作するとき（[Redundancy Manager enabled] のチェックボックスをチェック）にのみ表示されます。

SCALANCE X-400 が冗長化マネージャモードにある場合、スイッチとの接続ラインに対してリングポートから試験フレームを送出し、その伝播時間を測定します。その試験フレームについて発生する最大遅延時間を表示します。

No. of Changes to Standby Active State

この値は SCALANCE X-400 が冗長化マネージャとして動作する場合にのみ表示されます（「X-400 Ring Configuration メニュー」の項を参照）。

この値は SCALANCE X-400 のスタンバイ状態がパッシブからアクティブに変わった回数を示します。スタンバイマスタ側のリンクが障害になった場合にカウントされます。

Reset Counters ボタン

SCALANCE X-400 のカウンタをリセットします。SCALANCE X-400 への給電遮断などによって再起動が実施されると、カウンタがリセットされます。

CLI のシンタックス

表 4-17 X-400 Counters : CLI#X-400>

コマンド	説明	備考
counters	以下のカウンタ値を表示します。 <ul style="list-style-type: none"> Changes to RM active state 冗長化マネージャとして機能する SCALANCE X-400 がリングを閉じた回数 Max. delay of RM Test Telegrams 冗長化マネージャが送出した試験フレームの最大遅延時間 	
resetc	SCALANCE X-400 のカウンタをリセットします	管理者のみ。

4.4 エージェントメニュー

4.4.1 Agent Configuration メニュー

はじめに

[Agent]フォルダのアイコンをクリックすると Agent Configuration 画面が現れます。この画面では IP アドレスに関する設定を行えます。SCALANCE X-400 の IP アドレスを動的に割り当てるか固定アドレスを割り当てるかを指定できます。装置アクセスに関して Telnet や RMON などのオプションを有効化することもできます。

SCALANCE X414-3E の IP 設定

SCALANCE X414-3E に関する IP 設定を行います。スイッチングポート (In-Band 側) と CPU モジュールのイーサネットポート (Out-Band 側) が区別されています。

付記

CPU の IP アドレスとスイッチングポートの IP アドレスは異なるサブネットに属することが必要です。

IP Address

SCALANCE X414-3E または CPU モジュールの IP アドレスです。WBM とスイッチの接続に用いている IP アドレスを変更すると接続が切れます。接続しなおすにはウェブブラウザに新しいアドレスを入力します。

Subnet Mask

SCALANCE X414-3E または CPU モジュールのサブネットマスクを入力します。

The screenshot shows the 'Agent Configuration' interface. It has a title bar 'Agent Configuration' in a dark green header. Below it, there are two sections: 'Agent Enabled Features' and 'Agent IP Configuration'. The 'Agent Enabled Features' section contains a grid of checkboxes: E-Mail (checked), FTP (checked), TELNET (checked), RMON (unchecked), BOOTP (unchecked), DHCP (unchecked), DCP (checked), and SNTP (checked). The 'Agent IP Configuration' section has two columns: 'In-Band' and 'Out-Band'. Each column has input fields for IP Address, Subnet Mask, and Default Gateway. The In-Band IP Address is 192.168.202.70, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.202.202. The Out-Band IP Address is 192.168.200.70, Subnet Mask is 255.255.255.0, and there is no Default Gateway field. Below these are fields for Agent VLAN ID (1) and MAC Address (08-00-06-96-D1-7C for In-Band, 08-00-06-96-D1-7B for Out-Band). At the bottom, there are 'Refresh' and 'Set Values' buttons.

図 4-15 SCALANCE X414-3E の Agent Configuration 画面

SCALANCE X408-2 の IP 設定

SCALANCE X408-2 に関する IP 設定を行います。

付記

SCALANCE X408-2 では CPU モジュールにあるイーサネットポートは変更できません。変更できるのはスイッチングポートのみです。

SCALANCE X408-2 では DCP による IP アドレス割り当てはつねに有効になっており、無効にできません。

Subnet Mask

SCALANCE X408-2 のサブネットマスクを入力します。

The screenshot shows the 'Agent Configuration' interface. It has a title bar 'Agent Configuration' in a dark green header. Below it, there are two main sections, each with a green header bar. The first section is 'Agent Enabled Features' and contains seven checkboxes: E-Mail (checked), FTP (checked), TELNET (checked), RMON (unchecked), BOOTP (unchecked), DHCP (checked), and SNTP (checked). The second section is 'Agent IP Configuration' and contains five input fields: IP Address (192.168.200.71), Subnet Mask (255.255.255.0), Default Gateway (192.168.200.200), Agent VLAN ID (1), and MAC Address (08-00-06-AB-59-01). At the bottom of the form, there are two buttons: 'Refresh' and 'Set Values'.

図 4-16 SCALANCE X408-2 の Agent Configuration 画面

SCALANCE X-400 に関する設定

E-Mail チェックボックス

SCALANCE X-400 の E-Mail 機能を有効または無効に設定します。この機能については「Agent E-Mail Configuration メニュー」の項をご覧ください。

FTP チェックボックス

FTP サーバによるファームウェアのダウンロードを有効または無効に設定します。この件については 8 章「ファームウェアアップデート」をご覧ください。

TELNET チェックボックス

Telnet 経由による SCALANCE X-400 のアクセスを有効または無効に設定します。

RMON チェックボックス

SCALANCE X-400 は RMON (Remote Monitoring) 機能をサポートします。リモートモニタリング機能を使えば、RMON をサポートするネットワーク管理端末が SNMP を使って装置の診断データを収集、作成、読み出しすることができます。このような診断データ (ポートの負荷トレンドなど) を利用することによってネットワーク内の問題を早期に発見し、解決することが可能になります。RMON の設定は統計機能に影響を与えません (「Statistics メニュー」の項を参照)。

BOOTP チェックボックス

これをチェックすると SCALANCE X-400 はネットワーク内の BOOTP サーバを探し、そのサーバから供給されるデータに基づいて IP パラメータを設定します。この機能については、3.4 「BOOTP クライアントによる SCALANCE X-400 の IP アドレス割り当て」をご覧ください。

DHCP チェックボックス

これをチェックすると SCALANCE X-400 はネットワーク内の DHCP サーバを探し、そのサーバから供給されるデータに基づいて IP パラメータを設定します。この機能については、3.5 「DHCP クライアントによる SCALANCE X-400 の IP アドレス割り当て」をご覧ください。

SNTP チェックボックス

SCALANCE X-400 のシステム時計をネットワーク内の SNTP サーバによって同期させる機能を有効または無効に設定します。

Default Gateway

SCALANCE X-400 が別のサブネットにある装置（診断装置や電子メールサーバなど）と通信する必要があるときは、デフォルトゲートウェイの IP アドレスをここに入力する必要があります。

Agent VLAN ID

インバンド管理の VLAN ID をここに入力します。

MAC Address

SCALANCE X-400 または CPU モジュールの MAC アドレスです。

CLI のシンタックス（ファームウェア 1.2 版以前）

表 4-18 Agent Configuration : CLI#AGENT>

コマンド	説明	備考
ip <IP アドレス>	SCALANCE X-400 のインバンドポートに対する IP アドレスを設定します。ドットで区切った 4 つの十進数を指定してください。 パラメータを省略すると、現在設定されているインバンド IP アドレスが表示されます。	管理者のみ。 ウェブブラウザ、Telnet、SNMP を使って SCALANCE X-400 にアクセスするには IP アドレスを入力する必要があります。IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
subnet <サブネットマスク>	SCALANCE X-400 のインバンドポートに対するサブネットマスクを設定します。ドットで区切った 4 つの十進数を指定してください。	管理者のみ。 ウェブブラウザ、Telnet、SNMP を使って SCALANCE X-400 にアクセスするにはサブネットマスクを入力する必要があります。IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
oip <IP アドレス>	SCALANCE X414-3E のアウトバンドポートに対する IP アドレスを設定します。形式はこの表の上記コマンドと同じです。	管理者のみ。
osubnet <サブネットマスク>	SCALANCE X414-3E のアウトバンドポートに対するサブネットマスクを設定します。形式はこの表の上記コマンドと同じです。	管理者のみ。

コマンド	説明	備考
gateway <IP アドレス>	デフォルト IP ゲートウェイの IP アドレスを設定します。ドットで区切った 4 つの十進数を指定してください。	管理者のみ。 ルータ経由で SCALANCE X-400 にアクセスし、かつ通信相手が SCALANCE X-400 とは異なるサブネット内にある場合には、IP アドレスの入力が必要です。ゲートウェイはインバンド IP アドレスまたはアウトバンド IP アドレスのサブネット内に置かれていることが必要です。 IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
bootp <E D>	BOOTP を有効・無効にします。	管理者のみ。 デフォルト値：無効
dhcp <E D>	DHCP を有効・無効にします。	管理者のみ。 デフォルト値：有効
dcp <E D>	DCP を有効・無効にします。DCP プロトコルは、プライマリセットアップツールによって使用されます。	管理者のみ。 デフォルト値：有効
mail <E D>	電子メール機能を有効・無効にします。	管理者のみ。
ftp <E D>	FTP を有効・無効にします。	管理者のみ。
telnet <E D>	Telnet を有効・無効にします。	管理者のみ。 デフォルト値：有効
rmon <E D>	リモートモニタリングを有効・無効にします。	管理者のみ。 デフォルト値：無効
ping [-c 回数] [-s データ長] <IP アドレス>	いくつかのパケットを指定 IP アドレスに送出します。回数とデータ長のパラメータを省略すると 128 バイトのパケットを 10 回送出します。 例： ping -c 5 -s 256 192.168.1.1 データ長 256 バイトのパケット 5 個を 192.168.1.1 の IP アドレスに送出します。	

CLI のシンタックス (ファームウェア 2.0 版)

表 4-19 Agent Configuration : CLI¥AGENT>

コマンド	説明	備考
ip <IP アドレス>	SCALANCE X-400 のインバンドポートに対する IP アドレスを設定します。ドットで区切った 4 つの十進数を指定してください。 パラメータを省略すると、現在設定されているインバンド IP アドレスが表示されます。	管理者のみ。 ウェブブラウザ、Telnet、SNMP を使って SCALANCE X-400 にアクセスするには IP アドレスを入力する必要があります。IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
subnet <サブネットマスク>	SCALANCE X-400 のインバンドポートに対するサブネットマスクを設定します。ドットで区切った 4 つの十進数を指定してください。	管理者のみ。 ウェブブラウザ、Telnet、SNMP を使って SCALANCE X-400 にアクセスするにはサブネットマスクを入力する必要があります。IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
oip <IP アドレス>	SCALANCE X414-3E のアウトバンドポートに対する IP アドレスを設定します。形式はこの表の上記コマンドと同じです。	管理者のみ。
osubnet <サブネットマスク>	SCALANCE X414-3E のアウトバンドポートに対するサブネットマスクを設定します。形式はこの表の上記コマンドと同じです。	管理者のみ。
gateway <IP アドレス>	デフォルト IP ゲートウェイの IP アドレスを設定します。ドットで区切った 4 つの十進数を指定してください。	管理者のみ。 ルータ経由で SCALANCE X-400 にアクセスし、かつ通信相手は SCALANCE X-400 とは異なるサブネット内にある場合には、IP アドレスの入力が必要です。ゲートウェイはインバンド IP アドレスまたはアウトバンド IP アドレスのサブネット内に置かれていることが必要です。 IP アドレスは BOOTP/DHCP サーバによって自動的に割り当てられることも可能です。
bootp <E D>	BOOTP を有効・無効にします。	管理者のみ。 デフォルト値：無効
dhcp <E D>	DHCP を有効・無効にします。	管理者のみ。 デフォルト値：有効
dcp <E D>	DCP を有効・無効にします。DCP プロトコルは、プライマリセットアップツールによって使用されます。	管理者のみ。 デフォルト値：有効
mail <E D>	電子メール機能を有効・無効にします。	管理者のみ。
ftp <E D>	FTP を有効・無効にします。	管理者のみ。
telnet <E D>	Telnet を有効・無効にします。	管理者のみ。 デフォルト値：有効

コマンド	説明	備考
rmon <EID>	リモートモニタリングを有効・無効にします。	管理者のみ。 デフォルト値：無効
ping [-c 回数] [-s データ長] <IP アドレス>	いくつかのパケットを指定 IP アドレスに送出します。回数とデータ長のパラメータを省略すると 128 バイトのパケットを 10 回送出します。 例： ping -c 5 -s 256 192.168.1.1 データ長 256 バイトのパケット 5 個を 192.168.1.1 の IP アドレスに送出します。	

4.4.2 Agent SNMP Configuration メニュー

SNMP の動作

ネットワーク管理端末は SNMP (Simple Network Management Protocol) を用いることによって SCALANCE X-400 のような SNMP 対応ノードの設定と監視を行えます。これを行うには、データ交換を行う SCALANCE X-400 に SNMP エージェントをインストールする必要があります。フレームには以下の 3 種類があります。

- Read (管理端末が SCALANCE X-400 から値を取り出す)
- Write (管理端末が SCALANCE X-400 に値を書き込む)
- 登録されたノードにイベント (トラップ) を送出する。エージェントは登録された管理端末にメッセージを送出する。

SNMPv1 と比較した SNMPv3 (および SNMPv2) の改善点

SNMPv3 (および SNMPv2) は初期の SNMPv1 に比べて以下の点が改善されています。

- 管理端末が互いに通信しあえる
- 多段階セキュリティ方式 (データの暗号化、ユーザの認証)
- ユーザ定義ができるセキュリティ設定

SNMP に関するアクセス権限

SNMP プロトコルを使用するときにはコミュニティ文字列によってアクセス権限を指定します。コミュニティ文字列ではユーザ名やパスワードに関する情報が 1 つの文字列に含まれています。読み出し権限と書き込み権限に対しては異なるコミュニティ文字列を定義します。SNMPv2 の一部と SNMPv3 では、より複雑でより安全な認証が可能です。

付記

セキュリティ確保のため、デフォルト値を public または private として使用しないでください。

SCALANCE X-400 に関する SNMP の設定

[SNMP]フォルダのアイコンをクリックすると Agent SNMP Configuration の画面が現れます。

Agent SNMP Configuration の画面では SNMP に関する基本的な設定を行います。使用したい SNMP 機能に従ってチェックボックスをチェックします。詳細設定（トラップ、グループ、ユーザ）については個別のメニューが WBM に用意されています。SNMPv3 enabled のオプションを選んでいなくても画面での設定作業は可能ですが、内容は反映されません。

図 4-17 Agent SNMP Configuration の画面

SNMPv1/v2/v3 チェックボックス

SCALANCE X-400 に対して SNMPv1・SNMPv2・SNMPv3 の有効・無効を設定できます。

SNMPv3 only チェックボックス

これをチェックすると SNMPv3 のみが有効になります。SNMPv1 と SNMPv2 の機能は使用できません。

Read Only チェックボックス

これをチェックすると、SNMPv1/v2c に関する SNMP 変数が読み出しのみ行えます。

Read Community String

SNMP プロトコルに対する読み出し用コミュニティ文字列（最大 63 文字）を入力します。

Write Community String

SNMP プロトコルに対する書き込み用コミュニティ文字列（最大 63 文字）を入力します。

Traps チェックボックス

SNMPv1/v2c トラップの送出を有効または無効にします。

CLI のシンタックス

表 4-20 Agent SNMP Configuration : CLI¥AGENT¥SNMP

コマンド	説明	備考
snmp <D 3 E>	SNMP の有効・無効を設定します。パラメータの意味は次のとおりです。 D : SNMP を無効にします 3 : SNMPv3 のみを有効にします E : SNMPv1・SNMPv2・SNMPv3 を有効にします	管理者のみ。 デフォルト値 : SNMPv1/v2/v3 が有効
getcomm <文字列>	読み出し用コミュニティ文字列 (最大 32 文字) を設定します。デフォルトは <i>public</i> です。	管理者のみ。
setcomm <文字列>	書き込み用コミュニティ文字列 (最大 32 文字) を設定します。デフォルトは <i>private</i> です。	管理者のみ。
traps <E D>	SNMPv1 トラップの有効・無効を設定します。	管理者のみ。

4.4.3 SNMPv1 Trap Configuration メニュー

アラームイベントに対する SNMP トラップ

アラームイベントが発生すると、SCALANCE X-400 は同時に 10 台の (ネットワーク管理) 端末に対してトラップ (アラームフレーム) を送出することができます。トラップが送出されるのは Agent Event Configuration メニューで指定したイベントが発生した場合のみです (「Agent Event Configuration メニュー」の項を参照)。

付記

トラップを送出するには、SNMP Configuration メニューで Traps のオプションを有効にすることが必要です。

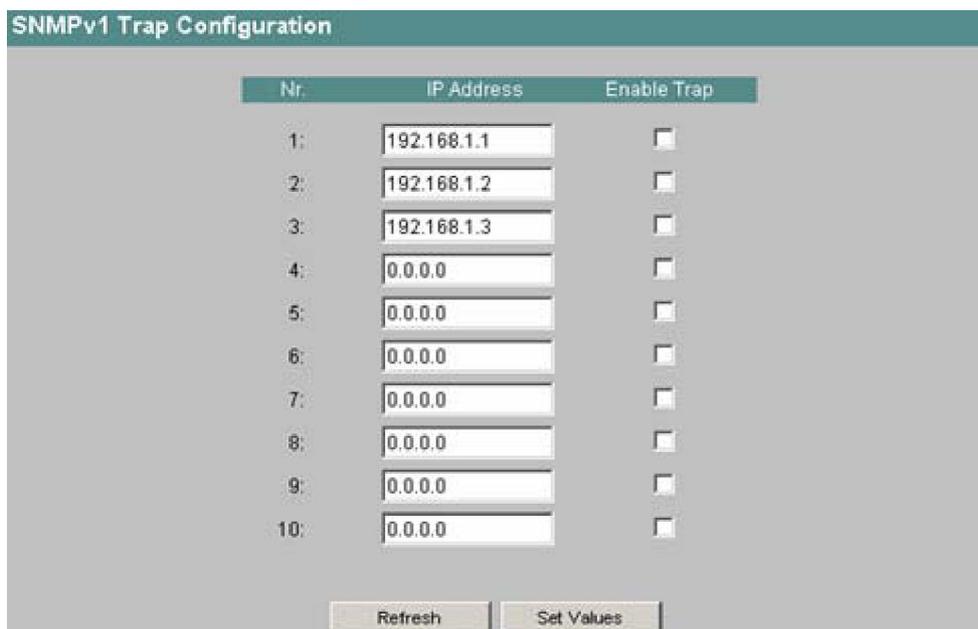


図 4-18 SNMPv1 Trap Configuration の画面

IP Address

SCALANCE X-400 がトラップを送出する先の端末の IP アドレスを入力します。

Enable Trap チェックボックス

指定の端末にトラップを送るには IP アドレスの隣にあるチェックボックスをチェックします。

CLI のシンタックス

表 4-21 SNMPv1 Trap Configuration : CLI#AGENT#SNMP>

コマンド	説明	備考
settrap <項番> <IP アドレス> <E D>	トラップ受信端末の番号（1～10 の番号）に対応する IP アドレスを指定し、その IP アドレスをもつ端末へのトラップ送信を有効または無効にします。	管理者のみ。 デフォルト値：0.0.0.0
showtrap	現在のトラップ設定を表示します。	

4.4.4 SNMPv3 Groups メニュー

セキュリティの設定とパーミッションの付与

SNMPバージョン3では認証と暗号化の有無をプロトコルレベルで設定できます。このセキュリティレベルと読み書きパーミッションの割り当てはグループ単位で行います。設定内容は自動的にグループの全メンバーに適用されます。



Group Name	Auth	Priv	Read	Write
Private	x	x	x	x
Protected	x	-	x	x
Public	-	-	x	-

図 4-19 SNMPv3 Groups の画面

Group Name 欄

定義済みのグループ名がすべてここに表示されます。グループ名をクリックするとウインドウが開き、グループのパラメータ設定を変更できます。

Auth 欄

×印が付いているグループは認証が有効になっています。

Priv 欄

×印が付いているグループは暗号化が有効になっています。

Read 欄

×印が付いているグループは読み出しアクセスが有効になっています。

Write 欄

×印が付いているグループは書き込みアクセスが有効になっています。

New Entry ボタン

新規グループを作成するにはこのボタンをクリックします。

SNMPv3 グループの設定

グループ名をクリックするとグループの属性を変更するウインドウが開きます。

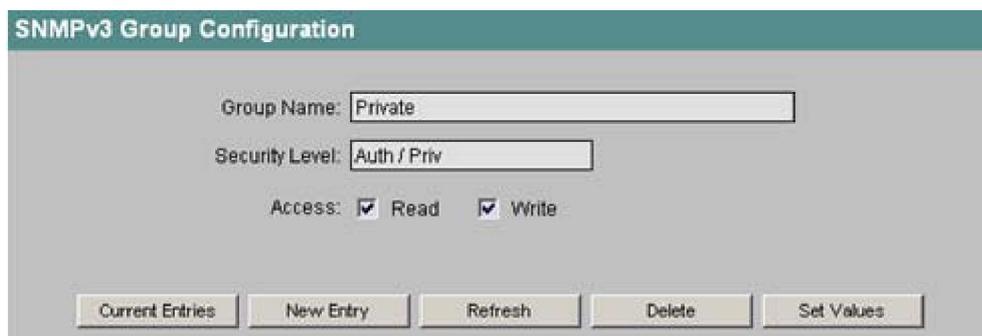


図 4-20 SNMPv3 Group Configuration の画面

Group Name

グループ名がここに表示されます。このデータは読み出し専用です。グループ名が付与できるのはグループ作成時のみであり、あとから変更することはできません。

Security Level

認証と暗号化の有無を示します。セキュリティレベルには以下の3種類があります。

セキュリティレベル	機能	備考
no Auth / no Priv	認証なし、暗号化なし	
Auth	MD5 または SHA のアルゴリズムを用いた認証／暗号化なし	
Auth / Priv	MD5 または SHA のアルゴリズムを用いた認証と DES3 アルゴリズムを用いた暗号化	

Read と Write のチェックボックス

読み出しアクセス、書き込みアクセス、通知の有効・無効を設定します。

Current Entries ボタン

クリックすると SNMPv3 グループのリストに戻ります。

New Entry ボタン

新規グループの作成ウィンドウが開きます。

Delete ボタン

グループの削除を行います。そのグループにメンバーが登録されている場合は、そのグループの削除およびそのグループのセキュリティレベルの変更は行えません。

新規グループの作成

SNMPv3 Group Configuration 画面で[New Entry]ボタンをクリックすると、新規グループの作成ウィンドウが開きます。



図 4-21 SNMPv3 Group Configuration II の画面

Group Name

グループ名をここに入力します。グループ名は 2 文字以上、32 文字以下としてください。

Security Level

そのグループのセキュリティレベルを選択します。

Read と Write のチェックボックス

グループメンバに対して読み出しアクセスおよび書き込みアクセスの許可・不許可を設定します。

CLI のシンタックス

表 4-22 SNMPv3 Groups : CLI%AGENT%SNMP%GROUP>

コマンド	説明	備考
info	すべての SNMPv3 グループを表示します。	
add <グループ名> [NOAUTH AUTH PRIV] [- RO RW]	新しい SNMPv3 グループを追加します。セキュリティレベルは以下のパラメータによって指定します。 NOAUTH : 認証なし、暗号化なし。 AUTH : MD5 または SHA のアルゴリズムを用いた認証。暗号化はなし。 PRIV : MD5 または SHA のアルゴリズムを用いた認証と DES3 アルゴリズムを用いた暗号化。 読み書きアクセスは以下のパラメータによって指定します。 -: 読み出しアクセスも書き込みアクセスも許容しない。 RO : 読み出しアクセスを許容 (読み出しのみ)。 RW : 書き込みアクセスを許容 (読み書き可能)。	管理者のみ。
edit <グループ名> [- RO RW]	アクセス権限を設定します。 読み書きアクセスの指定には以下のパラメータを使用できます。 -: 読み出しアクセスも書き込みアクセスも許容しない。 RO : 読み出しアクセスのみを許容。 RW : 読み出しアクセスと書き込みアクセスをともに許容。	管理者のみ。

コマンド	説明	備考
delete <グループ名>	指定の名前をもつ SNMPv3 グループを削除します。	管理者のみ。
clearall	すべての SNMPv3 グループをリストから削除します。	管理者のみ。

4.4.5 SNMPv3 Users メニュー

ユーザごとのセキュリティ設定

ユーザ単位のセキュリティモデルはユーザ名をもとに機能します。すなわち各フレームにユーザ ID が埋め込まれます。このユーザ名と該当するセキュリティ設定は、送信側と受信側の双方によってチェックされます。ユーザは以下の属性によって規定されます。

- ユーザ名 :
自由に設定できる名前です。
- セキュリティ名 :
認証プロトコルに対応した名前です。
- 認証プロトコル :
認証プロトコルの種類です。
- 認証鍵
認証プロトコルの秘密鍵です。
- 秘匿プロトコル
暗号化処理の種類です。
- 秘密鍵
暗号化における秘密パスワードです。

この画面には、SNMPv3 ユーザが表示されます。ユーザ名が User Name 欄に、ユーザが属するグループ名が Group 欄に表示されます。

User Name	Group	Auth	Priv
PrivateMD5	Private	MD5	DES
PrivateSHA	Private	SHA	DES
ProtectedMD5	Protected	MD5	none
ProtectedSHA	Protected	SHA	none
Public	Public	none	none

図 4-22 SNMPv3 Users の画面

User Name 欄

定義済みのユーザ名がすべてここに表示されます。ユーザ名をクリックすると新しいウィンドウが開き、ユーザのパスワードを変更できます。

Group 欄

ユーザが属するグループを示します。

Auth 欄

そのユーザに対して使用される認証アルゴリズムを示します。

Priv 欄

そのユーザに対して使用される暗号化方法を示します。

New Entry ボタン

新規ユーザを作成するにはこのボタンをクリックします。

SNMPv3 ユーザの設定

ユーザ名をクリックするとユーザの属性を変更するウィンドウが開きます。

The image shows a configuration window titled "SNMPv3 Users Configuration". It contains several input fields: "User Name" with the value "PrivateMD5", "Group Name" with "Private", "Security Level" with "Auth / Priv", "Authentication Algorithm" with a dropdown menu showing "MD5", "Authentication Password", "Authentication Password Confirmation", "Privacy Password", and "Privacy Password Confirmation". At the bottom, there are five buttons: "Current Entries", "New Entry", "Refresh", "Delete", and "Set Values".

図 4-23 SNMPv3 Users Configuration の画面

User Name

ユーザ名がここに表示されます。このデータは読み出し専用です。ユーザの作成後にユーザ名を変更することはできません。

Group Name

ユーザ名が属するグループを表示します。

そのグループに対して認証が必要なときは認証アルゴリズムを選択し、認証パスワードを入力します。またそのグループに対して暗号化を有効にしているときは暗号化のパスワードを入力します。

Security Level

そのグループに適用されるセキュリティレベル（認証と暗号化）を示します。セキュリティレベルの種類については 4-42 ページをご覧ください。

Authentication Algorithm リストボックス

MD5 または SHA のアルゴリズムを選択できます。

Authentication Password / Authentication Password Confirmation

認証パスワードを入力します。パスワードは 32 文字以内としてください。

Privacy Password / Privacy Password Confirmation

暗号化パスワードを入力します。パスワードは 32 文字以内としてください。

Current Entries ボタン

クリックすると SNMPv3 ユーザのリストに戻ります。

New Entry ボタン

新規ユーザの作成およびそのユーザが属するグループ名とグループの設定を行えます。

Delete ボタン

ユーザの削除を行います。

新規ユーザの作成

SNMPv3 Users Configuration 画面で[New Entry]ボタンをクリックすると、新規ユーザの作成ウィンドウが開きます。



図 4-24 SNMPv3 Users Configuration II の画面

User Name

新しいユーザ名をここに入力します。

Group Name

新しいユーザが属するグループを選択します。

CLI のシンタックス

表 4-23 SNMPv3 Users : CLI¥AGENT¥SNMP¥USER>

コマンド	説明	備考
info	SNMPv3 ユーザをすべて示すリストを表示します。	
add <ユーザ名> <グループ名> [NONE MD5 SHA] [認証パスワード] [暗号化パスワード]	新しい SNMPv3 ユーザをグループに追加します。 そのグループに対して認証が必要なときはパラメータにアルゴリズムを指定します (MD5 または SHA)。 そのグループに対して認証または暗号化が必要なときは必要なパスワードを指定します (それぞれ 32 文字以下とします)。	管理者のみ。
edit <ユーザ名> [NONE MD5 SHA] [認証パスワード] [暗号化パスワード]	SNMPv3 ユーザの属性を変更します。 そのグループに対して認証が必要なときはパラメータにアルゴリズムを指定します (MD5 または SHA)。 そのグループに対して認証または暗号化が必要なときは必要なパスワードを指定します (それぞれ 32 文字以下とします)。	管理者のみ。
delete <ユーザ名>	指定の名前をもつ SNMPv3 ユーザを削除します。	管理者のみ。
clearall	すべての SNMPv3 ユーザをリストから削除します。	管理者のみ。

4.4.6 Agent Event Configuration メニュー

SCALANCE X-400 のシステムイベント

この画面では、システムイベントに対する SCALANCE X-400 の対応方法を指定します。各イベントに対する SCALANCE X-400 の対応方法を有効にするには、該当するチェックボックスをチェックします。以下の対応方法があります。

- SCALANCE X-400 が電子メールを送信する
- SCALANCE X-400 が SNMP トラップを送信する
- SCALANCE X-400 がログファイルに記録する

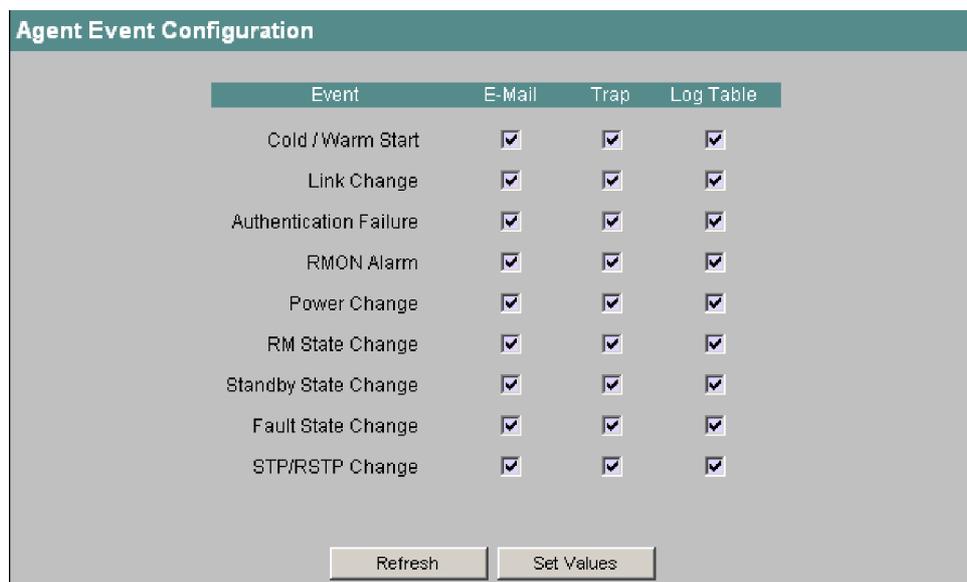


図 4-25 Agent Event Configuration の画面

以下のイベントについて SCALANCE X-400 の対応方法を指定できます。

Cold/Warm Start

SCALANCE X-400 がユーザによって電源投入または再起動されました。

Link Change

ポートで障害が発生したか、または以前に障害が発生したポートでデータトラフィックが再び処理されています。

Authentication Failure

誤ったパスワードまたは不適切なアクセス権を用いた SNMP アクセスがありました。

RMON Alarm

リモートモニタリングに関するアラームまたはイベントが発生しました。

Power Change

このイベントが発生するのは電源ライン 1 と 2 が監視されるときだけです。ライン 1 または 2 に変化があったことを示します。

RM State Change

冗長化マネージャがリングの断線または再確立を検出し、ラインの切り替えまたは切り戻しを行いました。SCALANCE X-400 が冗長化マネージャとして動作するには、それに合った装置設定を行うことが必要です（「X-400 Ring Configuration メニュー」の項を参照）。

Standby State Change

スタンバイ接続が確立された装置（マスタまたはスレーブ）が他のリングにつながるリンク（スタンバイポート）をアクティブまたは非アクティブにしました。データトラフィックは一方のイーサネット接続（マスタ）から他方のイーサネット接続（スレーブ）に切り替えられました（4.3.4 「X-400 Standby Mask メニュー」を参照）。

Fault State Change

障害状態が変化しました。障害状態はポート監視、信号用接点の作動、または電源監視と関係している場合があります。

STP/RSTP Change

STP または RSTP のトポロジーが変化しました。

CLI のシンタックス

表 4-24 Agent Event Configuration : CLI¥AGENT¥EVENT>

コマンド	説明	備考
info	現在のイベント設定を表示します。	
setec [CW LC AF RA PC RC SC RS FC] <E D> <E D> <E D>	システムイベントに対する SCALANCE X-400 の対応方法を指定します。イベントの指定には以下の記号を使用します。 CW : Cold/Warm Start LC : Link Change AF : Authentication Failure RA : RMON Alarm PC : Power Change RC : RM State Change SC : Standby State Change FC : Fault State Change RS : STP/RSTP Change イベントを指定すると、設定される対応方法が各イベントに対して形成されます。 後続の 3 つのパラメータは<E>または<D>で指定され、次の順序で SCALANCE X-400 の対応方法に対応します。 • 電子メール • トラップ • ログテーブルへの記録 例： Link Change の発生時に電子メールを送出したい場合、以下のようなコマンドを入力します。 setec LC E D D	管理者のみ。

4.4.7 Agent Digital Input Configuration メニュー (SCALANCE X414-3E)

付記

デジタル入力とその関連機能が使用できるのは SCALANCE X414-3E だけです。

デジタル入力の使用例

SCALANCE X414-3E にはデジタル入力が 8 つ備わっており、さまざまな用途に使用できます。

- 例 1 : I/O を使わずプロセス制御で OLM を監視**
 中央管理用 I/O モジュールのない状態で S7-400 コントローラを使用し、I/O は PROFIBUS OLM で光接続されているものと仮定します。OLM の信号用接点を SCALANCE X-400 のデジタル入力に使用し、診断に利用することができます。既存 OLM の信号用接点を SCALANCE X-400 のデジタル入力に対して使用すると、コンポーネントを追加しなくても OLM の監視が可能です。
- 例 2 : ドア接点**
 キャビネットのドア接点を SCALANCE X-400 のデジタル入力につなげます。イベントを適切に設定すればキャビネット内の不審な動きが監視できます。

変化およびデジタル入力に関するイベント

入力の状態変化（立ち上がりと立ち下がり）があった場合に通知するイベントをデジタル入力ごとに指定できます。以下の通知方法があります。

- SCALANCE X-400 が電子メールを送信する
- SCALANCE X-400 が SNMP トラップを送信する
- SCALANCE X-400 がログファイルに記録する

Input	E-Mail	Trap	Log Table	Name
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #1
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #2
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #3
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #4
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #5
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #6
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #7
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Digital Input #8

図 4-26 Agent Digital Input Configuration の画面

Name

各デジタル入力に対してわかりやすい名前を付けることができます。

CLI のシンタックス

表 4-25 Agent Digital Input Configuration : CLI#AGENT#DIGIN>

コマンド	説明	備考
info	SCALANCE X414-3E のデジタル入力の状態を表示します。	
showdic	SCALANCE X414-3E のデジタル入力の設定を表示します。	
setdic [入力番号] <E D> <E D> <E D>	デジタル入力に対するイベント設定を電子メール、トラップ、ログテーブル記録の順に指定します。入力番号を省略すると、指定の設定が全入力に適用されます。 例： setdic 5 E D E 入力 5 に信号が通知されると、スイッチは電子メールを送信するとともにログテーブルへの記録を行います。トラップは送出されません。	管理者のみ。
name <1 ... 8> <名前>	デジタル入力にわかりやすい名前を付けます。名前は 64 文字以下とします。	管理者のみ。

4.4.8 Agent E-Mail Configuration メニュー

電子メールによるネットワーク監視

SCALANCE X-400 には、アラームイベント発生時に（ネットワーク管理者などに）電子メールを自動送信するオプションがあります。電子メールには送信元装置の識別情報、アラーム原因に関する簡単な説明、およびタイムスタンプが記載されます。これによってノード数の少ないネットワークにおいて電子メールによる中央型ネットワーク監視が実現します。電子メールによるイベントメッセージを受信したらブラウザから WBM を立ち上げ、送信者の識別情報をもとに詳しい診断情報を読み出せます。

電子メールを送信できるのは以下の場合のみです。

- SCALANCE X-400 において電子メール機能が有効化され、受信側の電子メールアドレスが設定されている。
- 当該イベントに対して電子メール機能が有効化されている（「Agent Event Configuration メニュー」の項を参照）。
- SCALANCE X-400 が到達できる SMTP サーバがユーザのネットワーク内に存在する。
- SMTP サーバの IP アドレスが SCALANCE X-400 に設定されている。

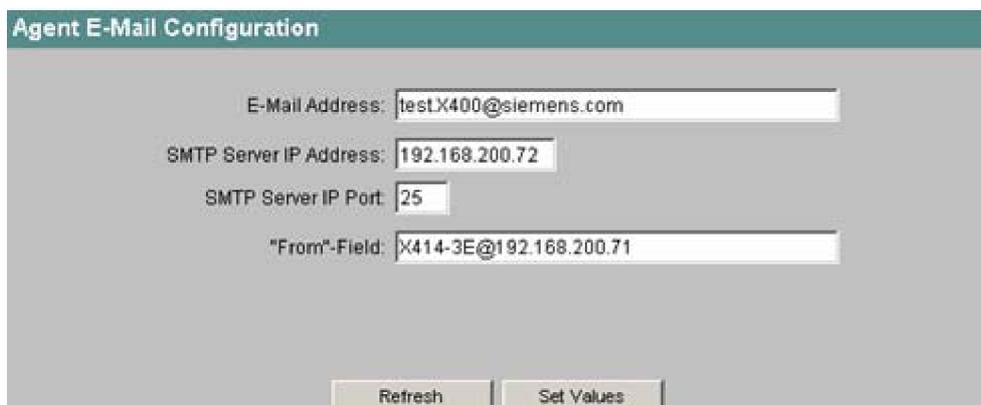


図 4-27 Agent E-Mail Configuration の画面

E-Mail Address

障害発生時に SCALANCE X-400 が送出する電子メールの宛先メールアドレスを入力します。

SMTP Server IP Address

電子メール送信に用いる SMTP サーバの IP アドレスを入力します。

SMTP Server IP Port

電子メール送信に使用する IP ポートです。必要であればデフォルト値の 25 と異なる値に変更することもできます。

"From" Field

電子メールの送信元アドレスです。

付記

SMTP サーバの属性および設定によっては電子メールについて「From」のテキストボックスに入力することが必要です。SMTP サーバの管理者に確認してください。「From」のテキストボックスは WBM、CLI、または SNMP への直接アクセスによって行えます。

CLI のシンタックス

表 4-26 Agent E-Mail Configuration : CLI¥AGENT¥EMAIL>

コマンド	説明	備考
server <IP アドレス> [:ポート番号]	SMTP の IP アドレスとポート番号を指定します。	管理者のみ。 デフォルト値 : 0.0.0.0:25
email <電子メールアドレス>	SCALANCE X-400 が送出する電子メールの宛先アドレスを指定します。このアドレスは 50 文字以下とします。	管理者のみ。 デフォルト値 : 無効 デフォルトアドレス : user@host.domain

コマンド	説明	備考
from [送信者を示す文言]	SCALANCE X-400 が送出する電子メールの送信元を指定します。このアドレスは 50 文字以下とします。	管理者のみ。

4.4.9 Agent DHCP Configuration メニュー (SCALANCE X408-2)

DHCP モードの設定

付記

DHCP の設定はファームウェア 2.0 版から対応しています。

DHCP サーバの設定において装置を識別する方法はいくつかあります。

- MAC アドレス
- 自由に定義できるクライアント ID
- システム名
- PROFINET IO の装置名

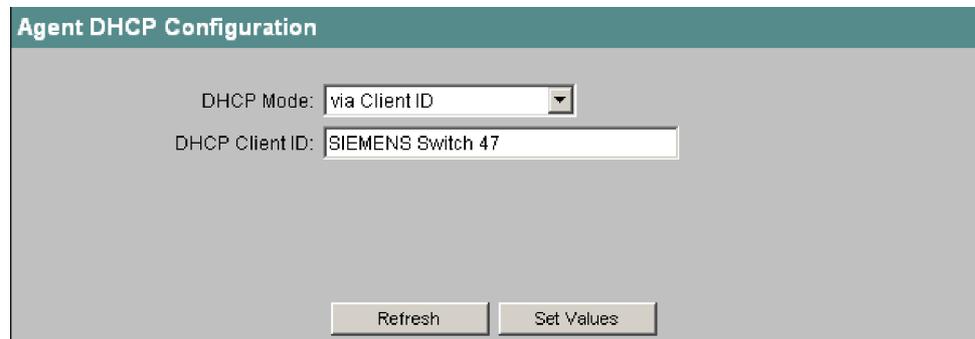


図 4-28 Agent DHCP Configuration の画面

DHCP Mode リストボックス

DHCP モードを設定します。

付記

Agent Configuration メニューで DHCP を有効にしていない場合にはモード選択は行えず、「disabled」と表示されます。

DHCP Client ID

DHCP モードが「via Client ID」の場合、DHCP サーバによって評価される文字列をここに指定し、装置に付与することができます。

CLI のシンタックス

表 4-27 Agent DHCP Configuration : CLI¥AGENT¥DHPCONF>

コマンド	説明	備考
info	現在の DHCP 設定を表示します。	
dhcpcmode [モード]	DHCP モードを設定します。使用できるモードは次のとおりです。 <ul style="list-style-type: none"> • MAC (MAC アドレス) • CLID (クライアント ID) • SYSN (装置名) • DEVN (PNIO の装置名) 	管理者のみ。
clidid [ClientID]	DHCP のクライアント ID を設定します。この値は「DHCP via Client ID」が設定されたときに使用されます。クライアント ID は自由に定義できます。	管理者のみ。

4.4.10 Agent Time Configuration メニュー

ネットワーク内の時刻同期

ネットワーク内の時刻同期には SNTP (Simple Network Time Protocol) が使用されます。しかるべきフレームがネットワーク内の SNTP サーバによって送出されます。SCALANCE X-400 は時刻フレームを受信するクライアントとしてこのサーバにログオンします。

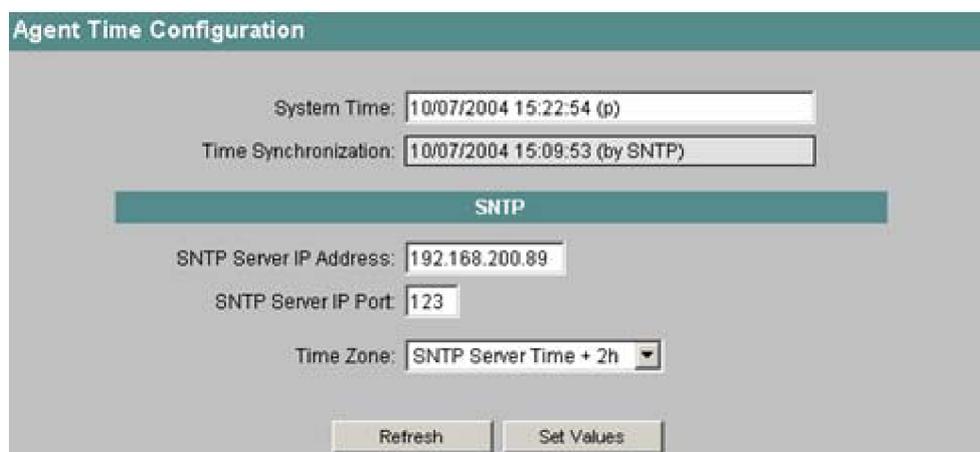


図 4-29 Agent Time Configuration の画面

System Time

現在のシステム時間を表示します。時刻同期ができなかった場合には「Date/time not set」と表示されます。

日時は手動で設定することもできます。入力形式は *MM/DD/YYYY HH:MM:SS* です。その場合、このテキストボックスに表示される日時の最後には「(m)」と表記されます。またシステム時間がサーバ同期によって設定されている場合には日時の最後には「(p)」と表記されます。

Time Synchronization

この値は読み出し専用です。最後に時刻同期が行われた時間を示します。

SNTP Server IP Address

SCALANCE X-400 が時刻同期に使うフレームを送る SNTP サーバの IP アドレスを入力します。

SNTP Server IP Port

SNTP サーバが使用できるポートを入力します。

Time Zone リストボックス

SNTP サーバはつねに UTC（世界標準時）を送出するため、SCALANCE X-400 の位置に対応する時間帯を選択します。時間帯に合わせて時刻を再計算し、現地時間に表示します。なお SCALANCE X-400 には夏時間と冬時間の切り替え機能はありません。

SICLOCK

SCALANCE X-400 のシステム時間は SICLOCK クロック送信機によって同期することもできます。その場合の同期には、「09-00-06-01-FF-EF」というアドレスに送出されるマルチキャストフレームが使用されます。SCALANCE X-400 は SNTP サーバへのログオン時にも SICLOCK フレームの評価を行います。

付記

時間の飛びを防止するため、ネットワークには SICLOCK クロック送信機と SNTP サーバのいずれか一方のみが存在するように留意してください。

CLI のシンタックス

表 4-28 Agent Time Configuration : CLI¥AGENT¥TIME>

コマンド	説明	備考
time [日付] [時間]	SCALANCE X-400 上の時刻を表示または設定します。 日時が表示されるときには、時刻の設定時間および設定方法も表示されます。 (m) : 手動によって設定されました。 (t) : 時刻は SIMATIC 時刻フレームによって設定されましたが、クロック送信機とは同期されていません。 (s) : 時刻は SIMATIC 時刻フレームによって設定され、クロック送信機と同期されています。 (p) : 時刻は SNTP プロトコルによって設定されました。	管理者のみ。 入力形式 : MM/DD/YYYY HH:MM:SS
server <IP アドレス> [:ポート番号]	SNTP サーバの IP アドレスを設定します。 ポートの設定はオプションです。	管理者のみ。
timezone [-12 ... 13]	SNTP サーバとシステム時間の時差を設定します。	管理者のみ。

4.4.11 Agent PNIO Configuration メニュー (SCALANCE X408-2)

PROFINET IO の設定

付記

PROFINET IO の機能は SCALANCE X408-2 のファームウェア 2.0 版で使用できます。

ここでは、NCM を使った PROFINET IO のハードウェア設定で付与したのと同じ PROFINET IO 装置名を設定します。

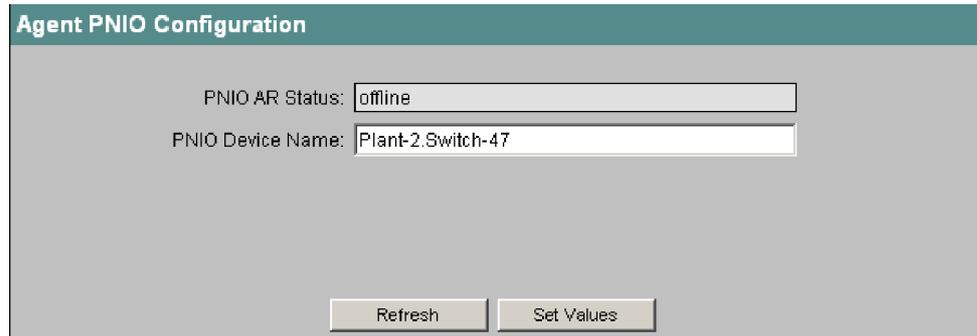


図 4-30 Agent PNIO Configuration の画面

PNIO AR Status

PROFINET IO の Application Relation 状態（コントローラとデバイスの関係）を示します。すなわち、PROFINET コントローラに対してオンラインかオフラインかを示します。

ここでいう「オンライン」とは、PROFINET IO コントローラとの接続が確立し、コントローラがその設定データをデバイスに送り込んでおり、デバイスが状態データを PROFINET IO コントローラに送信可能である状態をいいます。この状態を「データ交換中」といい、この間は PROFINET IO コントローラについて設定したパラメータをデバイス上で変更することはできません。

PNIO Device Name

HW Config の設定に従って PROFINET IO 装置名（端末の名前）を入力します。

CLI のシンタックス

表 4-29 Agent PROFINET IO Configuration : CLI¥AGENT¥PNIOCONF>

コマンド	説明	備考
info	現在の PNIO 設定を表示します。	
devname [装置名]	PNIO 装置名を設定します。	管理者のみ。

4.5 スイッチメニュー

はじめに

このメニューでは SCALANCE X-400 のスイッチ機能（レイヤ 2 相当）を設定します。以下の機能があります。

- 基本的なスイッチ設定：ミラーリング、エージング、フロー制御など
- ユニキャスト、マルチキャスト、ブロードキャストの各フレームに適用するフィルタテーブル
- IGMP/GRMP によるマルチキャストグループ管理

- スパニングツリープロトコルの使用
- VLAN の設定および GVRP フレームによる動的な設定

4.5.1 Switch Configuration メニュー

プロトコル設定とスイッチ機能

[Switch]フォルダのアイコンをクリックすると Switch Configuration 画面が開きます。この画面では SCALANCE X-400 で有効にする機能、およびデータトラフィックの管理に使用するプロトコルを指定します。

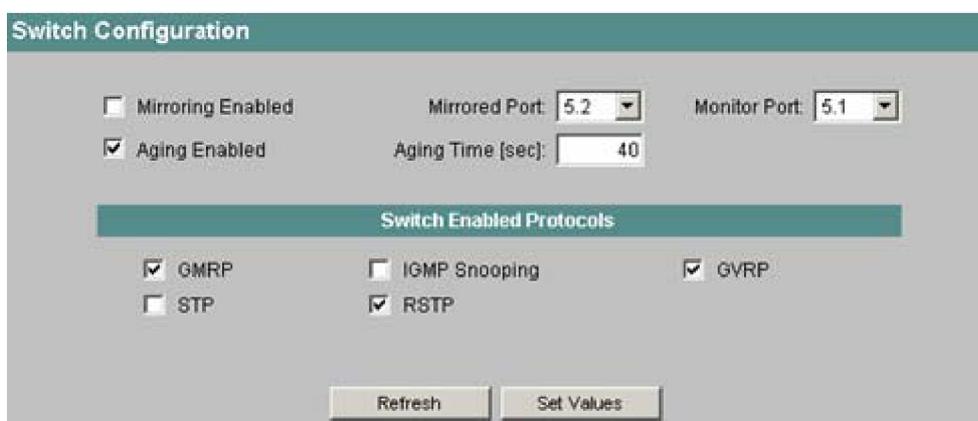


図 4-31 Switch Configuration の画面

ミラーリングとエージング

画面の上半分では以下の設定を行えます。

Mirroring Enabled チェックボックス

ミラーリングとは、スイッチが備えるあるポート(ミラー対象ポート)のデータトラフィックを別のポート(監視ポート)にコピーすることをいいます。

監視ポートにプロトコルアナライザを接続すれば、監視ポートでの接続を遮断することなくミラー対象ポートのデータトラフィックを記録できます。ただしこれを行うには監視ポートとして使用できる空きポートがスイッチにある必要があります。

付記

SCALANCE X-400 のポートはすべてミラー対象ポートとして監視することが可能ですが、リングポートを監視ポートにすることはできません。

ミラー対象ポートの最大データレートが監視ポートの最大データレートよりも大きい場合、データ紛失によって正しい監視ができないことがあります。

監視ポートに通常の末端端末を接続する場合にはミラーリング機能を無効にする必要があります。

Mirrored Port / Monitor Port リストボックス

ミラーリングにおけるコピー元とコピー先のポートを選択します。

Aging Enabled チェックボックス

SCALANCE X-400 は接続しているノードの送信元アドレスを自動的に学習します。スイッチはこの情報を用いて特定の関連ノードにデータフレームを転送します。それによって他のノードに関連するネットワーク負荷が軽減されます。

その送信元アドレスが学習したアドレスと一致するフレームを SCALANCE X-400 がある一定時間内に受信しないと、学習したそのアドレスは削除されます。この仕組みをエージングといいます。エージングは、ある末端装置（プログラミングデバイスなど）が別のスイッチポートに接続されるなどの場合に誤配を防止します。

このチェックボックスをチェックしない場合、学習したアドレスの自動削除は行われません。

Aging Time [sec]

その送信元アドレスが学習したアドレスと一致するフレームを SCALANCE X-400 が受信しなかった場合にそのアドレスが削除される経過時間を入力します。

SCALANCE X408-2 におけるエージングタイムのデフォルト値は 30 秒です。この値は 15 秒から 3825 秒の範囲で 15 秒刻みで設定できます。SCALANCE X414-3E におけるデフォルト値は 40 秒です。この値は 10 秒から 1000000 秒の範囲で自由に設定できます。

データトラフィックの管理プロトコル

画面の下半分では、以下に示す SCALANCE X-400 のグローバル機能の有効・無効が設定できます。

GMRP チェックボックス

GMRP は GARP Multicast Registration Protocol の略語です。また GARP は Generic Attribute Registration Protocol の略語です。これはマルチキャストフレームを効率的に転送するための仕組みです。

ノードは GID (GARP 情報宣言) を用いることによって SCALANCE X-400 をマルチキャストアドレスの受信者として登録することができます。SCALANCE X-400 はこの登録情報を GIP (GARP 情報伝播) フレームの形で自機のポートに送ります。その結果、そのアドレスは他のスイッチにも知れ渡ることとなり、それらのスイッチはそのアドレスに宛てたマルチキャストフレームをそのアドレスの登録情報を受信したポートにのみ送ります。このような方法により、マルチキャストフレームによって生じる負荷がネットワーク全体で軽減されます。またマルチキャストに登録されていないノードに対してマルチキャストフレームが送信されることもなくなります。

このチェックボックスをチェックすると、全ポートを対象にしたマルチキャストフィルタテーブルに GMRP の登録情報が追加され、自動的に生成されます。

チェックしないと下記ようになります。

- SCALANCE X-400 は受信した GMRP フレームの評価を行いません。
- SCALANCE X-400 は自機の GMRP フレームを送りません。

IGMP Configuration チェックボックス

IGMP は Internet Group Management Protocol の略語です。これは IP プロトコルを発展させたものであり、マルチキャストグループに対して IP アドレスの割り当てを可能にします。

SCALANCE X-400 はマルチキャスト受信装置から送られてくる IGMP フレームをチェックし、得られた情報を自機のマルチキャストフィルタテーブルに格納します。フィルタテーブルでは IGMP Configuration によるフィルタデータはそれとわかるように表示されます。

このチェックボックスをチェックすると IGMP のデータがフィルタテーブルに書き込まれ、IGMP フレームはそれに従って転送されます。

付記

GMRP と IGMP を同時に使用することはできません。

GVRP チェックボックス

GVRP は GARP VLAN Registration Protocol の略語です。このチェックボックスをチェックすると GVRP が許容されます。その場合、ポートに対応する VLAN の設定が GVRP を用いて動的に行えます。

STP (スパンニングツリー) チェックボックス

スパンニングツリーは、冗長ネットワーク構成においてループを防止する方法です。チェックボックスの設定によってこのスパンニングツリー機能を有効または無効にできます。スパンニングツリーにおける一般的な再構成時間は 20~30 秒です。

RSTP (高速スパンニングツリー) チェックボックス

RSTP (高速スパンニングツリー) はスパンニングツリーを改良したものです。RSTP の目的は再構成時間を数秒に短縮することです。

チェックボックスをチェックすると RSTP が有効になります。これはリング形冗長構成を使用していないときのみ可能です。あるポートにおいてスパンニングツリーフレームが検出されると、そのポートは RSTP から STP (スパンニングツリー) に戻ります。

付記

RSTP を使用すると、フレームの重複や追い越しをもたらすループが一時的に形成されることがあります。お使いの用途でこのような現象が許容されない場合には、リング形冗長構成 HSR や低速のスパンニングツリーといった代替方法を使用してください。

付記

STP/RSTP による冗長化アルゴリズムとリング形冗長機能は併用できません。SCALANCE X-400 は同時に複数の方法を使用することができません。リング形冗長機能をオンにしているときに STP/RSTP を有効にしようとすると、その旨のメッセージが出力されます。

STP/RSTP を無効にすると、SCALANCE X-400 は STP/RSTP のリスニングモードで動作します。その場合、STP/RSTP が無効であってもスイッチは STP/RSTP の設定フレームをトランスペアレントに転送します。トポロジー変更フレームであることをスイッチが認識すれば、ノードリストが通常より早く更新されるように一時的にエイジングタイムを短くします。その時間が経過すればエイジングタイムは元の値に戻されます。

CLI のシンタックス

表 4-30 Switch Configuration : CLI#SWITCH>

コマンド	説明	備考
info	スイッチメニューの現在の設定を表示します。	
mirror <E D>	ミラーリングを有効・無効にします。	管理者のみ。
m_ports <ミラー対象ポート> <監視ポート>	ミラーリングを行うポートを指定します。第 1 パラメータはデータトラフィックを記録するポート、第 2 パラメータはプロトコルモニタを行うポートです。	管理者のみ。
aging <E D>	エージング機能を有効・無効にします。	管理者のみ。 デフォルト値：有効
agetime <秒数>	エージングタイムを指定します。デフォルト値は SCALANCE X408-2 が 30 秒、SCALANCE X414-3E が 40 秒です。	管理者のみ。
gmrp <E D>	SCALANCE X-400 の全ポートに対して GMRP 機能を有効・無効にします。	管理者のみ。
igmp <E D>	SCALANCE X-400 の全ポートに対して IGMP 機能を有効・無効にします。	管理者のみ。
gvrp <E D>	SCALANCE X-400 の全ポートに対して GVRP 機能を有効・無効にします。	管理者のみ。
stp <E D>	SCALANCE X-400 の全ポートに対してスパンニングツリー機能を有効・無効にします。	管理者のみ。
rstp <D S R>	SCALANCE X-400 の全ポートに対して高速スパンニングツリー機能を有効・無効にします。パラメータの意味は次のとおりです。 D：STP/RSTP を無効にします。 S：スパンニングツリーを有効にします。 R：高速スパンニングツリーを有効にします。	管理者のみ。

4.5.2 Current Unicast Filter メニュー

アドレスのフィルタリング

この画面にはフィルタテーブルの現在の内容が表示されます。このテーブルにはユニキャストアドレスフレームの送信元アドレスが並んでいます。テーブルの内容はノードがポートにフレームを送出するときに動的に作成できるほか、ユーザのパラメータ設定によって静的に作成することもできます。

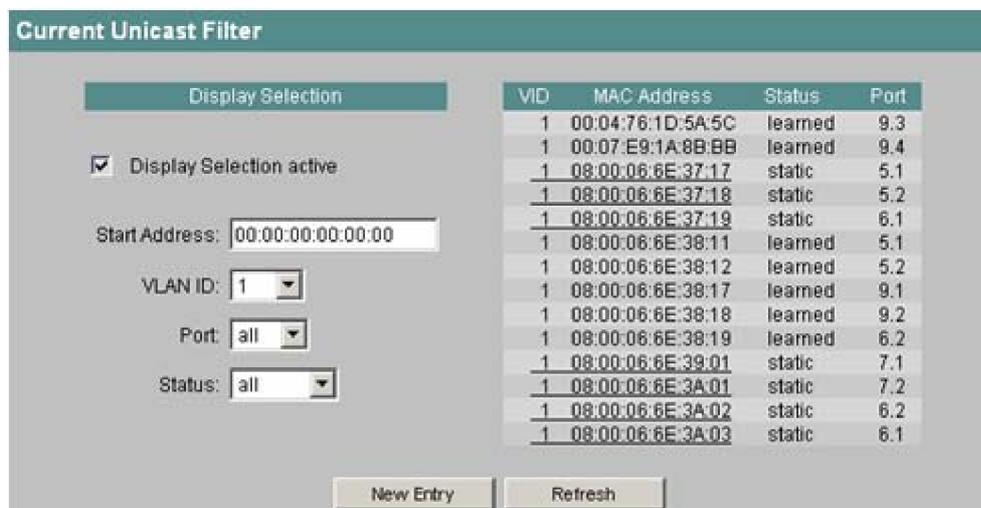


図 4-32 Current Unicast Filter の画面

表示アドレスの選択

Display Selection Active チェックボックス

これをチェックすると選択した要素しか表示されません。チェックしなければすべてのアドレスが表示されます。

Start Address

フィルタテーブルに保存される MAC アドレスのうち、ここに指定したアドレス以降のものが表示されます。何も入力しなければ、保存される最小アドレスのものから表示されます。

VLAN ID リストボックス

何らかの値を入力すると、対応する VLAN ID をもつアドレスのみが表示されます。VLAN ID として有効な値は 1 から 4096 です。VLAN ID を選択したくないときは「all」を選択します。

Port リストボックス

この設定を利用すると、ある特定のポートに対応するノードのアドレスのみ表示させることができます。「all」を選択すると全ポートに対応するアドレスが表示されます。

Status リストボックス

この設定を利用すると、特定の状態のアドレスのみを表示させることができます。選択可能な状態は次のとおりです。

- learned (学習したアドレス)
- static (ユーザが設定したアドレス)
- all (学習したアドレスとユーザが設定したアドレス)

フィルタテーブルに表示される情報

フィルタテーブルの4つの欄には以下の情報が示されます。

- VID**
 そのMACアドレスに割り当てられたVLAN IDです。MACアドレスにVLAN IDが割り当てられていないときは「1」が表示されます。
- MAC Address**
 ノードのMACアドレス（SCALANCE X-400が学習したもの、またはユーザが設定したもの）。
- Status**
 各アドレスの状態を示します。状態が「learned」の場合、そのノードからフレームを受信することによって当該アドレスを学習したことを表します。また「static」はそのアドレスがユーザによって固定的に設定されたことを表します。スタティックアドレスは恒久的に保存されます。すなわちエージングタイムが経過しても、あるいはスイッチを再起動しても削除されません。「invalid」は、その値がSCALANCE X408によって評価されていないことを表します。そのような値はウェブ型管理ツールからポート番号なしで入力されました。
- Port**
 当該アドレスのノードにつながるスロットとポートを示します。宛先アドレスがこのアドレスに一致するフレームをSCALANCE X-400が受信すると、フレームはこのポートに転送されます。

フィルタの設定

static 状態のMACアドレスをクリックするとフィルタ設定画面が開きます。

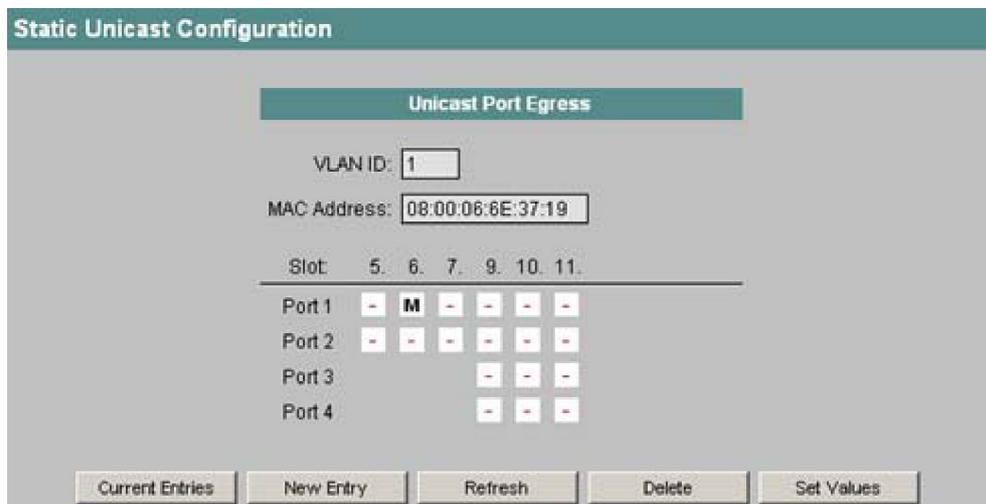


図 4-33 Static Unicast Configuration の画面

Slot / Port リストボックス

入力した宛先アドレスをもつフレームが転送される先のスロットとポートを選択します。該当するボックスをクリックすると状態が表示されます。記号の意味は以下のとおりです。

- M**
 (Member) ユニキャストフレームはこのポートから送出されます。
- このポートからはユニキャストフレームは送出されません。

- #
このポートは無効です。
- ?
VLAN の設定がユニキャストの設定と相反します。そうした事態が発生するのは、ユニキャスト設定において VLAN に属さない宛先ポートを選択した場合です。

新規項目の作成

アドレステーブルに新規項目を追加するには[New Entry]ボタンをクリックします。Static Unicast Configuration 画面が開き、必要な項目を作成できます。

図 4-34 Static Unicast Configuration II の画面

VLAN ID

MAC アドレスが属する VLAN の ID を入力します。何も設定しないと、基本設定として VLAN ID=1 (デフォルト VLAN) が設定されます。

MAC Address

アドレステーブルに追加したい MAC アドレスを入力します。このアドレスが受信フレームの宛先アドレスと照合されます。

Slot / Port リストボックス

設定した宛先アドレスをもつフレームが転送される先のスロットとポートを選択します。該当するボックスをクリックすると「M」と表示されます。

無効なポートには「#」の印が付きます。「?」の場合は VLAN の設定とユニキャストの設定の間に不一致があります。

付記

ユニキャストアドレスに対して指定できるポートは 1 つだけです。

Current Entries ボタン

クリックすると、MAC アドレスの一覧に戻ります。

New Entry ボタン

クリックすると、フィルタテーブルに新規項目を作成できます。

Delete ボタン

クリックすると、表示されている項目がフィルタテーブルから削除されます。

CLI のシンタックス

表 4-31 Current Unicast Filter : CLI¥SWITCH¥UCAST>

コマンド	説明	備考
info	SCALANCE X-400 のアドレステーブルの内容を表示します。	
find <MAC アドレス> [VLAN ID] [ポート番号] [S L]	SCALANCE X-400 のアドレステーブルから MAC アドレスを探します。その宛先アドレスをもつ受信フレームが送られる先のポート番号も表示します。 VLAN ID を指定しない場合は、すべての VLAN について指定 MAC アドレスを探します。 オプションとしてポート番号を指定することもできます。その場合は指定のポートのみを探します。 もう 1 つのオプションとして、固定アドレスと学習アドレスを分けて指定することもできます。 S : 固定アドレス L : 学習アドレス	
add <MAC アドレス> <ポート番号> <VLAN ID>	アドレステーブルに静的なユニキャストアドレス項目を 1 つ以上追加します。空白で区切った複数のポートを入力することもできます。	管理者のみ。
edit <MAC アドレス> <ポート番号> <VLAN ID>	アドレステーブルの項目の内容を変更します。	管理者のみ。
delete <MAC アドレス> <VLAN ID>	アドレステーブルの固定アドレスの項目を削除します。	管理者のみ。

4.5.3 Current Multicast Group メニュー

マルチキャストのアプリケーション

多くの場合、フレームにはユニキャストアドレスが設定され、ある 1 つの受信者に宛てて送信されます。あるアプリケーションが同じデータを複数の相手に送信する場合、1 つのマルチキャストアドレスを使ってデータを送信すると、全体のデータ量を削減することができます。一部のアプリケーションでは固定的なマルチキャストアドレスが用意されています (NTP、IETF1 Audio、IETF1 Video など)。

ネットワーク負荷の軽減

ユニキャストフレームの場合に比べ、マルチキャストフレームはスイッチに対する負荷が高くなります。マルチキャストフレームは一般にスイッチの全ポートに送られます。マルチキャストフレームによる負荷を軽減する方法には以下の3つがあります。

- マルチキャストのフィルタテーブルにアドレスを固定的に登録しておく
- IGMP パラメータ付与フレームを受信することによってアドレスを動的に登録する (IGMP Configuration)
- GMRP フレームによって能動的かつ動的にアドレスに登録する

このような方法を取れば、マルチキャストフレームは当該アドレスに登録されたポートにしか送信されなくなります。

Current Multicast Group の画面には、フィルタテーブルに現在登録されているマルチキャストフレームならびにその宛先ポートが表示されます。内容には動的なもの (SCALANCE X-400 によって学習されたもの) と静的・固定的なもの (ユーザが設定したもの) とがあります。

付記

SCALANCE X414-3E のフィルタテーブルに学習アドレスが 500 個を超えて登録されている場合、冗長化ネットワークの再構成時間は 300 ミリ秒を超える可能性があります。

VID	MAC Address	Status	Port Member List												
			5	6	7	9	10	11	12	13	14	15	16		
1	09:00:06:AA:01:02	static	MM	FF	MM	MMMM	----	----	----	----	----	----	----	----	----
1	09:01:02:03:04:05	static	MM	--	--	MMMM	MMMM	MMMM	----	----	----	----	----	----	----

図 4-35 Current Multicast Group の画面

フィルタテーブルに表示される情報

フィルタテーブルの4つの欄には以下の情報が示されます。

VID

その MAC アドレスに割り当てられた VLAN ID です。

MAC Address

ノードの MAC アドレス (SCALANCE X-400 が学習したもの、またはユーザが設定したもの)。

Status

各アドレスの状態を示します。以下の状態があります。

- **static**
そのアドレスはユーザによって固定的に設定されました。スタティックアドレスは恒久的に保存さ

れます。すなわちエイジングタイムが経過しても、あるいはスイッチを再起動してもアドレスは削除されません。

- **IGMP**
そのアドレスに対応する宛先ポートは IGMP Configuration によって得られました。
- **GMRP**
そのアドレスに対応する宛先ポートは受信した GMRP フレームによって登録されました。

Port List

各スロットに対応する欄があります。そこにはそのポートが属する先のマルチキャストグループが示されます。記号の意味は以下のとおりです。

- **M**
(Member) マルチキャストフレームはこのポートから送出されます。
- **R**
(Registered) マルチキャストグループのメンバーです。登録は GMRP フレームによって行われました。
- **I**
(IGMP) マルチキャストグループのメンバーです。登録は IGMP フレームによって行われました。
- **-**
マルチキャストグループのメンバーではありません。このポートからはマルチキャストフレームは送出されません。
- **F**
(Forbidden) マルチキャストグループのメンバーではありません。さらにこのアドレスは GMRP による動的学習を行ってはありません。

新規項目の作成

アドレステーブルに新規項目を追加するには[New Entry]ボタンをクリックします。Static Multicast Configuration 画面が開き、必要な項目を作成できます。

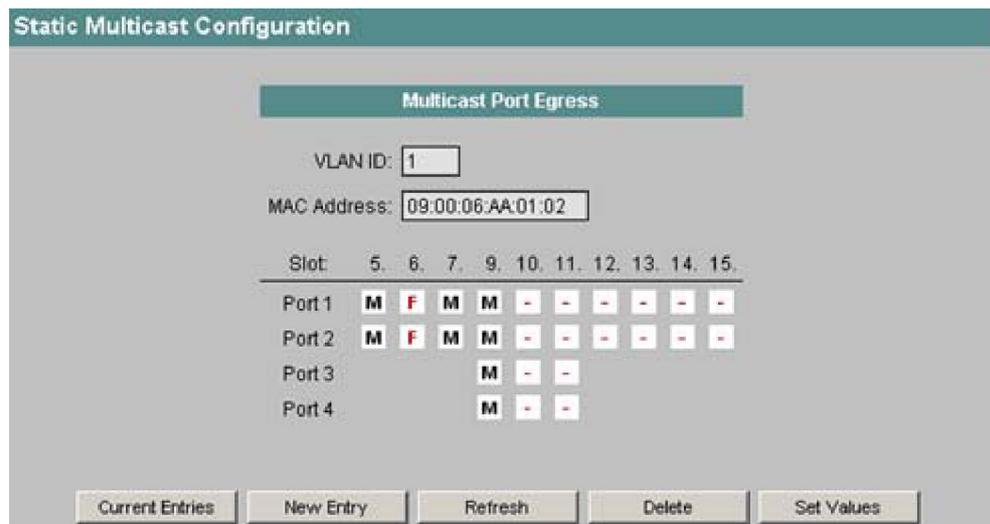


図 4-36 Static Multicast Configuration の画面

VLAN ID

MAC アドレスが属する VLAN の ID を入力します。何も設定しないと、基本設定として VLAN ID=1 (デフォルト VLAN) が設定されます。

MAC Address

アドレステーブルに追加したい MAC アドレスを入力します。

Slot / Port リストボックス

マルチキャストフレームに対するポートの対応を選択します。

- **M**
(Member) マルチキャストフレームはこのポートから送出されます。
- **-**
マルチキャストグループのメンバーではありません。このポートからはマルチキャストフレームは送出されません。
- **F**
(Forbidden) マルチキャストグループのメンバーではありません。さらにこのアドレスは GMRP による動的学習を行ってはなりません。
- **#**
そのポートは無効です。
- **?**
そのポートは指定の VLAN のメンバーではありません。

付記

マルチキャストアドレスには複数のポート (宛先ノード) が指定できます。

Current Entries ボタン

クリックすると、MAC アドレスの一覧に戻ります。

New Entry ボタン

クリックすると、フィルタテーブルに新規項目を作成できます。

Delete ボタン

クリックすると、表示されている項目がフィルタテーブルから削除されます。

アドレス項目の変更

static 状態の MAC アドレス (アドレスリストで下線を引いたもの) をクリックすると、そのアドレスに対する *Static Multicast Configuration* の画面が開きます。必要な設定を行ったあとで [Set Values] ボタンをクリックし、内容を確定します。

CLI のシンタックス

表 4-32 Current Multicast Groups : CLI¥SWITCH¥MCAST>

コマンド	説明	備考
info	SCALANCE X-400 のアドレステーブルの内容を表示します。	
add <VLAN ID> <MAC アドレス> [- [ポート番号,] [m [ポート番号,] [f [ポート番号,]	<p>静的なマルチキャストアドレス項目をアドレステーブルに追加します。記号の意味は以下のとおりです。</p> <ul style="list-style-type: none"> - マルチキャストグループのメンバーではありません。このポートからはマルチキャストフレームは送出されません。 m マルチキャストフレームはこのポートから送出されます。 f マルチキャストグループのメンバーではありません。さらにこのアドレスは GMRP による動的学習を行ってはいけません。 <p>例： add 2 01:02:03:04:05:06 m 5.1-5.2 f 9.2-9.4 MAC アドレスを VLAN ID=2 に割り当てます。ポート 5.1 と 5.2 はメンバーで、9.2 から 9.4 は禁止です。 add 3 01:02:03:04:05:06 m VLAN ID=3 に対してアドレス項目を追加します。すべての既存ポートがメンバーです。</p>	管理者のみ。
find <MAC アドレス> [VLAN ID]	SCALANCE X-400 のアドレステーブルから MAC アドレスを探します。その宛先アドレスをもつ受信フレームが送られる先のポート番号も表示します。 VLAN ID を指定しない場合は、すべての VLAN について指定 MAC アドレスを探します。	
edit <VLAN ID> <MAC アドレス> [- [ポート番号,] [m [ポート番号,] [f [ポート番号,]	アドレステーブルの項目の内容を変更します。記号 (-、m、f) の意味は add コマンドと同じです。	管理者のみ。
delete <MAC アドレス> <VLAN ID>	アドレステーブルの固定アドレスの項目を削除します。	管理者のみ。

4.5.4 GMRP Configuration メニュー

GMRP の有効化

各ポートにおける GMRP の有効・無効をチェックボックスを用いて指定します。ポートに対して GMRP を無効にするとそのポートには何も登録されず、GMRP フレームを送ることはできません。

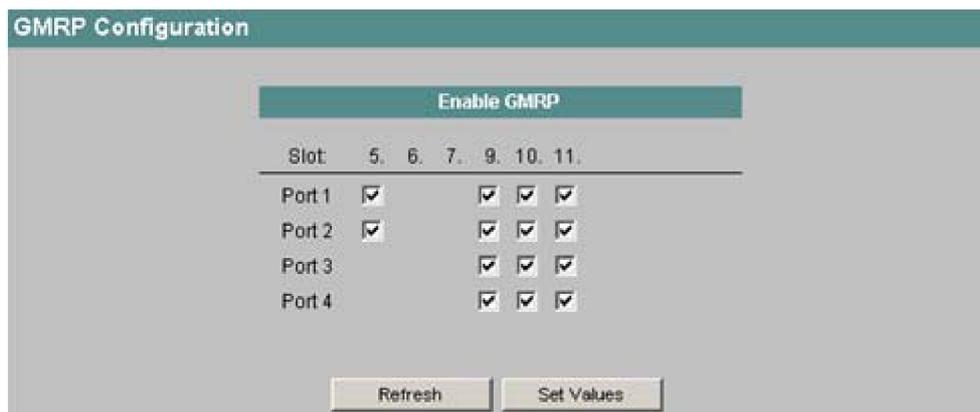


図 4-37 GMRP Configuration の画面

CLI のシンタックス

表 4-33 GMRP Configuration : CLI≠SWITCH≠MCAST>

コマンド	説明	備考
grmpport <E D> [ポート番号]	当該ポートに対する GMRP 機能を有効または無効にします。どのポートも指定しない場合は全ポートについて有効または無効になります。	管理者のみ。

4.5.5 IGMP Snooping Configuration メニュー

エージングタイムの指定

このメニューでは IGMP 設定に対するエージングタイムが設定できます。IGMP によって作成された項目は、新しい IGMP フレームによってアップデートされないかぎり、指定時間が経過するとアドレステーブルから削除されます。この処理は全ポートに対して実施されます。ポートごとに指定することはできません。

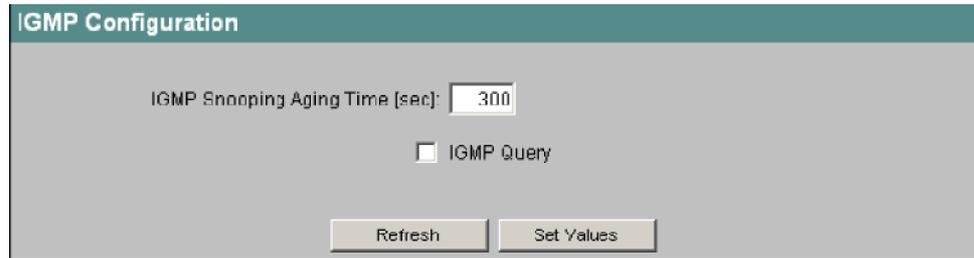


図 4-38 IGMP Configuration の画面

IGMP Snooping Aging Time [sec]

エージングタイムを秒数で指定します。

IGMP Query チェックボックス

SCALANCE X-400 が IGMP クエリの送出行うときはこのボックスをチェックします。

CLI のシンタックス (ファームウェア 1.2 版以前)

表 4-34 IGMP Configuration : CLI¥SWITCH¥MCAST>

コマンド	説明	備考
igmptime [時間]	IGMP のエージングタイムを指定します。パラメータを省略すると、IGMP の現在のエージングタイムを表示します。	管理者のみ。
igmpqry <E D>	IGMP クエリを有効または無効にします。	管理者のみ。

CLI のシンタックス (ファームウェア 2.0 版)

表 4-35 IGMP Configuration : CLI¥SWITCH¥MCAST¥IGMP>

コマンド	説明	備考
igmptime [時間]	IGMP のエージングタイムを指定します。パラメータを省略すると、IGMP の現在のエージングタイムを表示します。	管理者のみ。
igmpqry <E D>	IGMP クエリを有効または無効にします。	管理者のみ。

4.5.6 Broadcast Blocking Mask メニュー

ブロードキャストフレームの転送遮断

このメニューではブロードキャストフレームの転送を個々のポートについてブロックすることができます。

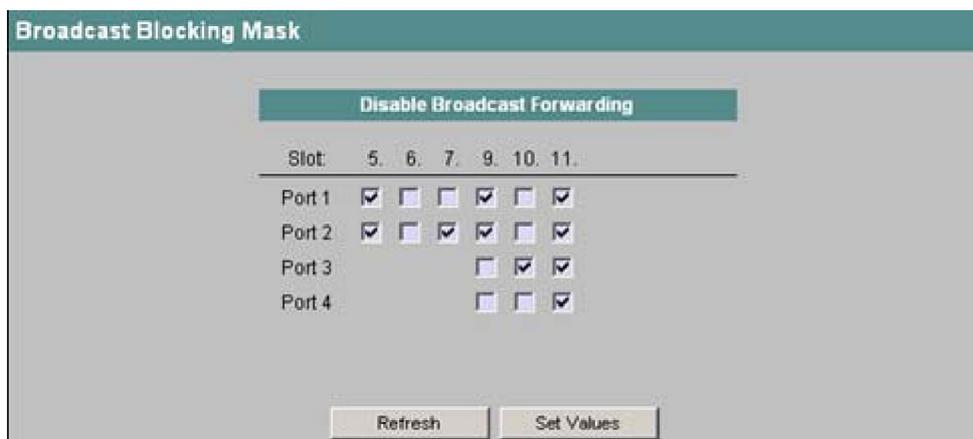


図 4-39 Broadcast Blocking Mask の画面

Disable Broadcast Forwarding チェックボックス

ブロードキャストフレームの転送を遮断したいポートを指定します。

付記

通信プロトコルによってはブロードキャストを用いないと動作しないものがあります。その場合にブロックを設定するとデータ通信ができないおそれがあります。この画面の設定を行うときは、ブロードキャストが不要であり、それを明確に止めたいことを確認してください。

CLI のシンタックス

表 4-36 Broadcast Blocking Mask : CLI¥SWITCH¥

コマンド	説明	備考
blkcast <E D> [ポート番号] (blkcast=ブロードキャストの遮断)	指定ポートにおけるブロードキャスト転送を有効または無効にします。	管理者のみ。

4.5.7 Load Limits Configuration メニュー (SCALANCE X414-3E)

受信フレーム数の制限

このメニューではあるポートから 1 秒間に受信する最大パケット数を指定できます。ハードウェアの観点から複数のポートが 1 つのポートブロックにまとめられます。しかし設定値 (packets [s]) は 1 ポート当たりの値です。入力した制限値を適用するフレームのカテゴリを指定できます。

- Unicast (宛先ルックアップ NG)
- Multicast

- Broadcast

	Port Block	Unicast (DLF)	Multicast	Broadcast	Packets [s]
1	Port 5.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	262143
2	Port 5.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	262143
3	Slots 6, 7, 11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	262143
4	Slots 9, 10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	262143
5	Slots 12, 13, 14, 15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	262143

Refresh Set Values

図 4-40 Load Limits Configuration の画面

Port Block

ポートは以下のポートブロックに分類されます。設定値はそのポートブロックに属する全ポートに適用されます。

ポートブロック 1
スロット 5 のポート 1

ポートブロック 2
スロット 5 のポート 2

ポートブロック 3
スロット 6、7、11 のポート

ポートブロック 4
スロット 9 と 10 のポート

ポートブロック 5
実装されるエクステンダのポート。すなわちツイストペア用エクステンダではスロット 12 と 13 のポート、メディアモジュール用エクステンダではスロット 12 から 15 のポートです。

この欄には実際に使用されるスロットのみ表示されます。たとえばエクステンダが未実装のときはブロック 5 のポートは表示されません。テキストボックスは読み出し専用です。

Unicast (DLF)、Multicast、Broadcast のチェックボックス

1 秒間の最大パケット数はここでチェックを付けたパケットタイプに適用されます。

Packets [s]

そのポートブロックが受信するフレームの最大数です。この値を超えるパケットは廃棄されます。

付記

リングポートは回線障害検出のために定期的にマルチキャストフレームを送出しています。そのためポートブロックにリングポートが含まれるときは、冗長化マネージャが正しく機能するようマルチキャストフレームの受信制限は使用しないでください。

CLI のシンタックス

表 4-37 Load Limits Configuration : CLI¥SWITCH>

コマンド	説明	備考
limits [ブロック番号] [<E D> <E D> <E D>] [パケット数/秒]	スイッチが各ポートブロックに対して処理する受信パケットの最大数を指定します。ポートブロックの定義は下記のとおりです。 <ul style="list-style-type: none"> • スロット 5 のポート 1 • スロット 5 のポート 2 • スロット 6、7、11 のポート • スロット 9 と 10 のポート • 実装されるエクステンダのポート。すなわちツイストペア用エクステンダではスロット 12 と 13 のポート、メディアモジュール用エクステンダではスロット 12 から 15 のポートです。 E または D は (下記の順で) 3 つの指定をオプションで行えます。 <ul style="list-style-type: none"> • Unicast (DLF) • Multicast • Broadcast 入力パケットの最大数をオプションで指定できます。 例 : <ul style="list-style-type: none"> • limits 1 E D E 1000 ポートブロック 1 に対してユニキャストとブロードキャストを有効に、またマルチキャストを無効にし、1 秒間に最大受信パケット数を 1000 に設定します。 • limits 1 D E D 1000 ポートブロック 1 に対してユニキャストとブロードキャストを無効に、またマルチキャストを有効にし、パケットレートはそのままとします。 • limits 2 2000 パケットタイプの設定はそのまま、ポートブロック 2 に対するパケットレートを変更します。 	最大パケット数を指定できるのは管理者のみです。パラメータとしてポートブロックのみを指定した場合には現在値が表示されます。この形式のコマンドは全ユーザが使用できます。

4.5.8 Load Limits Rates メニュー (SCALANCE X408-2)

送受信データの転送速度制限

このメニューでは設定されている負荷上限値（1 秒間の最大フレーム数）が表示されます。設定値（packets [s]）は 1 ポート当たりの値です。入力した上限値を適用するフレームのカテゴリーを指定することができます。対応する項目をクリックすると設定画面が開きます。

Load Limits Rates				
Port	Ingress Limiting Mode	Ingress Limiting Rate	Egress Limiting Rate	
5.1	All Frames	not limited	not limited	
5.2	All Frames	not limited	not limited	
6.1	Broadcast, Multicast, DLF	128 Mbps	256 Mbps	
6.2	Broadcast, Multicast	32 Mbps	64 Mbps	
8.1	All Frames	not limited	not limited	
8.2	All Frames	not limited	not limited	
8.3	Broadcast	128 Kbps	256 Kbps	
8.4	All Frames	not limited	not limited	

Refresh

図 4-41 Load Limits Rates の画面

Port

表示内容に対応するスロット番号とポート番号を示します。[Port]欄の項目をクリックすると、そのポートの設定画面が開きます。

Ingress Limiting Mode

受信データの上限値の適用対象となるフレームタイプが表示されます。

Ingress Limiting Rate

受信データに対して設定されている転送速度の上限値です。

Egress Limiting Rate

送信データに対して設定されている転送速度の上限値です。

付記

送信データに対する上限値はつねにすべてのパケットに対して適用されます。

上限値の設定

[Port]欄の項目をクリックすると「Load Limits Rates Configuration」画面が開きます。

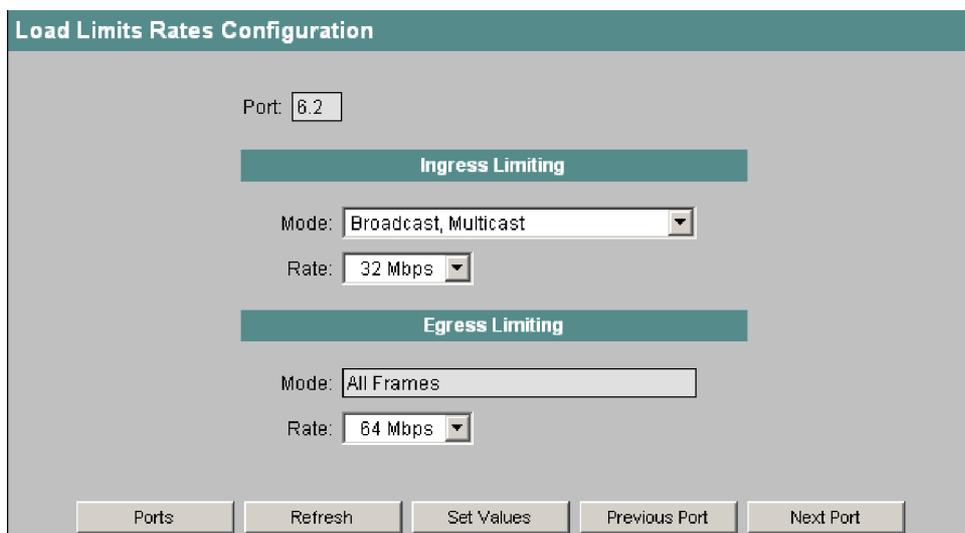


図 4-42 Load Limits Rates Configuration の画面

Port

表示内容に対応するスロット番号とポート番号を示します。このフィールドは変更できません。

Mode リストボックス (Ingress Limiting 側)

受信データについて選択した上限値の適用対象となるフレームタイプを以下のものから選択できます。

- Unicast (宛先ルックアップ NG)
- Multicast
- Broadcast

Rate リストボックス (Ingress Limiting 側)

受信データの最大転送速度を候補値から選択できます。「not limited」を選択すると「Ingress Limiting Mode」は意味をもたなくなります。

Mode (Egress Limiting 側)

送信データの転送速度は全フレームに適用されることが示されます。このフィールドは変更できません。

Rate リストボックス (Egress Limiting 側)

送信データの最大転送速度が候補値から選択できます。

付記

リングポートは回線障害検出のために定期的にマルチキャストフレームを送出しています。そのためリングポートについては、冗長化マネージャが正しく機能するようマルチキャストフレームの受信制限は使用しないでください。

CLI のシンタックス

表 4-38 Load Limits Configuration : CLI¥SWITCH¥LIMITS>

コマンド	説明	備考
info [ポート番号]	パケット制限に関する現在の設定値を表示します。設定値はポートに従って表示されます。	パラメータ（ポート番号）を指定すると対象値のみが表示されます。
inmode <モード> [ポート番号]	ポートにおける受信制限モードを指定します。 <モード>のパラメータには以下の値を設定できます。 B=ブロードキャスト BM=ブロードキャスト、マルチキャスト BMU=ブロードキャスト、マルチキャスト、ユニキャスト (DLF) ALL=全フレーム 例： inmode B 5.1 ポート 5.1 の受信制限モードをブロードキャストに設定します。	ポート番号を省略すると、設定内容が全ポートについて変更されます。
ingress <速度> [ポート番号]	ポートにおける受信制限速度を指定します。 <速度>のパラメータには以下の値を設定できます。 128K、256K、512K、1M、2M、4M、8M、16M、32M、64M、128M、256M 上記の「K」は Kbps を、「M」は Mbps を表します。 例： ingress 256K 5.1, 6.2 ポート 5.1 と 6.2 の受信制限速度を 256 Kbps に設定します。	ポート番号を省略すると、設定内容が全ポートについて変更されます。
egress <速度> [ポート番号]	ポートにおける送信制限速度を指定します。 <速度>のパラメータには以下の値を設定できます。 128K、256K、512K、1M、2M、4M、8M、16M、32M、64M、128M、256M 上記の「K」は Kbps を、「M」は Mbps を表します。 例： egress 2M 5.1, 8.1-8.4 ポート 5.2 と 8.1~8.4 の送信制限速度を 2Mbps に設定します。	ポート番号を省略すると、設定内容が全ポートについて変更されます。

4.5.9 Current VLAN Configuration メニュー

ノードの物理位置によらないネットワーク定義

VLAN (Virtual LAN、仮想 LAN) はノードの物理位置に関係なく構成できるネットワークです。マルチキャストおよびブロードキャストのフレームは論理的なネットワーク構成で決まる範囲内ではしか使用できないため、それらのフレームを仮想ネットワークに送ることはできません。そのため VLAN はブロードキャストドメインとも呼ばれます。VLAN のメリットは、他の VLAN のノードやネットワークセグメントにおいてネットワーク負荷を低減できることです。

VLAN の種類

VLAN にはいくつかの種類があります。

- ポート VLAN (レイヤ 2)
- MAC アドレス型 VLAN (レイヤ 2)
- IP アドレス型 VLAN (レイヤ 3)

SCALANCE X-400 はポート VLAN をサポートしています。これにより、SCALANCE X-400 のパラメータ設定や GVRP フレームを使った設定が可能になります。

ポート VLAN の設定手順

設定にはポート VLAN に対応したプログラムを使用できます。VLAN の設定は下記の手順で行います。

1. 1 つ以上の VLAN 構築について基準を作成します。
2. 各 VLAN に割り当てるノードを指定します。
3. 設定リストを作成します。各ノードに VLAN ID を割り当て、接続を行う装置および接続の確立に用いるポートを指定します。
4. スイッチに対して以下の設定を行います。
 - その装置で使用するすべての VLAN の定義
 - どのポートがどの VLAN を扱うかに関する指定
 - ポートを出入りするフレームの処理方法 (送受信フィルタ) の指定
 - 各ポートから送出されるフレームにおけるタグgingの有無
 - スイッチの設定を静的に行うか GVRP を用いて動的に行うかの決定

VLAN に関する重要なルール

VLAN の設定・運用を行う際には以下のルールに従ってください。

- VLAN またはマルチキャストグループ利用時にリングの切り替え時間を 300ms にするには、すべての VLAN ならびにすべてのマルチキャストグループにおいてすべてのリングポートを静的な方法でメンバー登録することが必要です。
- VLAN ID が「0」のフレーム (VLAN タグに優先度しか設定されていないフレームなど) は、タグのないフレームとして処理されます。
- デフォルトではスイッチ上の全ポートが VLAN タグのないフレームを送出し、末端ノードがそうしたフレームを受信できるようにします。すべてのノードがタグ付きフレームを解釈できるとは限らないため、そのような基本設定が必要になります。
- VLAN をサポートするスイッチは、デフォルトにおいてすべてのポートが VLAN ID 「1」 (デフォルト VLAN) を与えられます。

付記

VLAN ID 「500」は将来用に確保されており、すでに設定がなされています。

ポートに末端ノードが接続されている場合、送出フレームはタグなしで送出します（静的アクセスポート）。一方、そのポートにさらにスイッチがつながっている場合、フレームにはタグを付加します（トランクポート）。

VLAN と SCALANCE X-400

Current VLAN Configuration の画面には、VLAN に関する現在の割り当て状況が表示されます。

VID	Name	Status	Port Member List												
			5	6	7	9	10	11	12	13	14	15			
1	Default VLAN 1	static	UU	UU	UU	UUUU	UUUU	UUUU	UU	UU	UU	UU	UU		
5	MyVlan	static	--	--	--	----	MMMM	MMFF	--	--	--	--			

図 4-43 Current VLAN Configuration の画面

テーブルの 4 つの欄にはそれぞれ以下の情報が示されます。

VID

VLAN ID。1 から 4094 までの数字です。

Name

VLAN の定義時に与える名前。あくまで表示上のものであり、設定内容には影響しません。

Status が「static」のものは VID または Name の欄をクリックすると、Static VLAN Configuration の画面が開きます。そこでは各ポートが属する VLAN の設定を行えます。ただし VLAN ID とその名前は新規追加のときにしか指定できず、あとから変更することはできません。それらを変更したい場合にはいったんそれを削除し、必要な変更を盛り込んだ状態で改めて作成しなおすことが必要です。

Status

ポートフィルタテーブルの項目のタイプを示します。「static」は、アドレスがユーザによってスタティックアドレスとして登録されたことを示します。「gvrp」は、設定が GVRP フレームによって登録されたことを示します。ただしこれが可能なのは、SCALANCE X-400 において GVRP が使用可能にされている場合に限りです。

Port Member List

各スロットまたはポートに対する VID を示します。記号の意味は次のとおりです。

- 「-」
ポートはその VLAN のメンバーではありません。
- M
(Member) ポートはその VLAN のメンバーです。送出されるフレームには VLAN タグが付加され、そこには左端に示す VID が入っています。
- R
(Registered) ポートはその VLAN のメンバーです。登録は GVRP フレームによって行われました。

- U
(Untagged)ポートはその VLAN のメンバーです。送出されるフレームに VLAN タグはありません。
- F
(Forbidden)ポートはその VLAN のメンバーではなく、また GVRP によってその VLAN をそのポートに登録することはできません。

新たに作成したときには全ポートが「-」になります。

VLAN の設定

[New Entry]ボタンをクリックすると、VLAN 使用時における各ポートのフレーム送出方法を指定できます。Static VLAN Configuration の画面が開き、必要な入力を行えます。

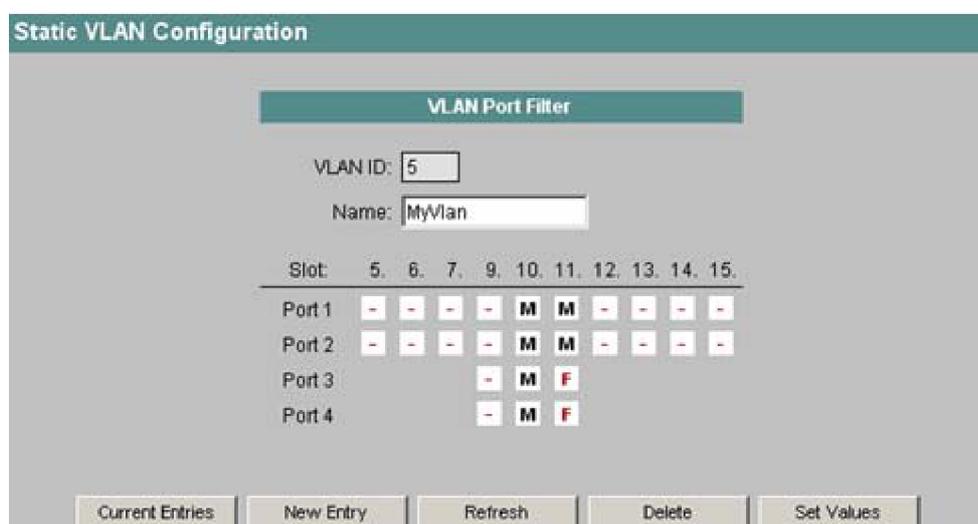


図 4-44 Static VLAN Configuration の画面

VLAN ID

VLAN の ID を入力します。VLAN ID は 1 から 4094 までの数字です。

Name

VLAN の名前を入力します。名前は設定にはまったく影響しません。

Slot と Port のリストボックス

その VLAN に関して各ポートがフレームを送出するときの動作を指定できます。デフォルトでは「-」が設定されています。ボックスをクリックするごとに内容が次に移ります。記号の意味は次のとおりです。

- 「-」
ポートはその VLAN のメンバーではありません。
- M
(Member)ポートはその VLAN のメンバーです。送出されるフレームには VLAN タグが付加され、そこには 1 行目に示す VLAN ID が入っています。
- R
(Registered)ポートはその VLAN のメンバーです。登録は GVRP フレームによって行われました。

- **U**
(Untagged)ポートはその VLAN のメンバーです。送出されるフレームに VLAN タグはありません。VLAN タグをサポートしない末端装置にこのポートから送るときは U を指定します。
- **F**
(Forbidden)ポートはその VLAN のメンバーではなく、また GVRP によってその VLAN をそのポートに登録することはできません。

Current Entries ボタン

クリックすると VLAN の一覧に戻ります。

New Entry ボタン

クリックすると新規 VLAN の設定を行えます。

Set Values ボタン

クリックすると設定内容が SCALANCE X-400 に保存されます。

Delete ボタン

クリックすると表示の設定が削除されます。

CLI のシンタックス

表 4-39 Current VLAN Configuration : CLI¥SWITCH¥VLAN>

コマンド	説明	備考
info	現在設定されている VLAN の内容およびポートとの関係を示します。	
add <VLAN ID> [名前] [- [ポート番号],] [m [ポート番号],] [u [ポート番号],] [f [ポート番号]]	<p>新しい VLAN を作成します。</p> <ul style="list-style-type: none"> • ポート番号 その VLAN に対して設定するポートを指定します。 • 「-」 ポートはその VLAN のメンバーではありません。 • m ポートはその VLAN のメンバーです。フレームは VLAN タグを付加して送出されます。 • u ポートはその VLAN のメンバーです。フレームは VLAN タグなしで送出されます。 • f ポートはその VLAN のメンバーではなく、また GVRP によってその VLAN に動的に割り付けることはできません。 <p>例： add 2 VLAN ID 「2」 およびデフォルト名が「Vlan 2」の新規 VLAN を生成します。</p> <p>add 4 MyName m, f 5.2 VLAN ID 「4」 および名前が「MyName」の新規 VLAN を生成します。ポート 5.2 を除くすべてのポートがメンバーであり、そのポートのみが禁止です。</p>	管理者のみ。

コマンド	説明	備考
edit <VLAN ID> [名前] [- [ポート番号],] [m [ポート番号],] [u [ポート番号],] [f [ポート番号]]	<p>ポートが属する VLAN を変更します。オプションとして名前も変更できます。パラメータの意味は add コマンドと同じです。</p> <p>例： edit 2 OtherName VLAN ID が 2 の VLAN の名前を「OtherName」に変更します。</p> <p>edit 3 OtherName - 10.1 VLAN ID が 3 の VLAN の名前を「OtherName」に変更し、この VLAN からポート 10.1 を外します。</p>	管理者のみ。
delete <VLAN ID>	SCALANCE X-400 の設定から指定 ID の VLAN を削除します。	管理者のみ。

4.5.10 VLAN Port Parameters メニュー

受信フレームの処理

この画面では SCALANCE X-400 が受信フレームを処理する基準を示します。

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
5.1	0	1	all	enabled
5.2	0	1	all	enabled
9.1	0	1	all	enabled
9.2	0	1	all	enabled
9.3	0	1	all	enabled
9.4	0	1	all	enabled
10.1	0	1	all	enabled
10.2	0	1	all	enabled
10.3	0	1	all	enabled
10.4	0	1	all	enabled
11.1	0	1	all	enabled
11.2	0	1	all	enabled
11.3	0	1	all	enabled
11.4	0	1	all	enabled

Refresh

図 4-45 VLAN Port Parameters の画面

テーブルの 5 つの欄にはそれぞれ以下の情報が示されます。

Port

このスロットとポートに関する情報が右に表示されます。

Priority

VLAN タグに示される CoS (サービスクラス) の優先度。タグのないフレームを受信した場合にはポートごとに優先度を与えることができます。この優先度は、他のフレームに対する処理方針を規定します。

優先度は 0 から 7 までの 8 段階があり、7 が最優先です (IEEE 802.1p ポートの優先度)。フレームのタグングについては付録 C をご覧ください。

Port VID

受信フレームに VLAN タグが付加されていない場合は、ここで指定する VLAN ID を入れたタグが付加され、そのポートのスイッチングルールに従って送出されます。

Acceptable Frames

VLAN タグをもたないフレームの処理方法を指定します。以下の値を使用できます。

- tagged only
SCALANCE X-400 はタグのないフレームをすべて廃棄します。
- all
SCALANCE X-400 はすべてのフレームを転送します。

Ingress Filtering

受信フレームの VID が評価される (enabled) かされない (disabled) かが示されます。

VLAN ポートの設定

Ports 欄の値をクリックすると、受信フレームに関するポート属性を変更する画面が開きます。

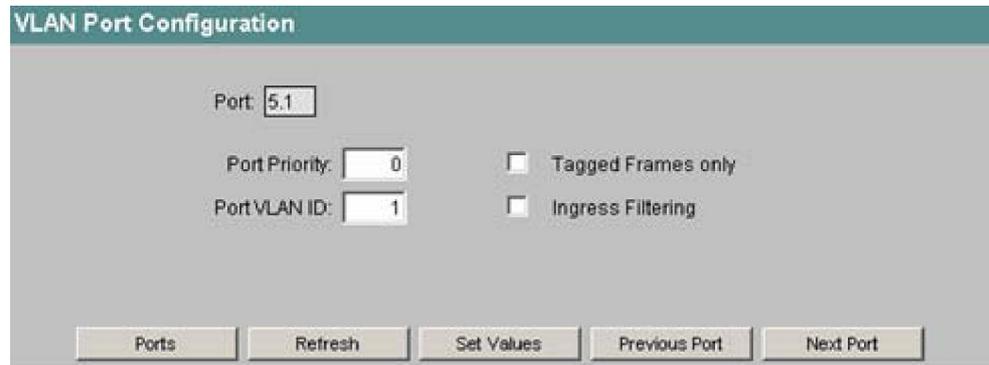


図 4-46 VLAN Port Configuration の画面

Port

このボックスは、ここに表示されるスロットとポートに関するものです。変更はできません。

Port Priority

タグなしフレームに与えられる優先度です。

Port VLAN ID

タグなしフレームに与えられる VLAN ID です。

Tagged Frames only チェックボックス

このボックスをチェックするとタグなしフレームが廃棄されます。チェックしない場合は設定内容に従って以下の規則が適用されます。

Ingress Filtering チェックボックス

このボックスをチェックすると、受信フレームの VLAN ID によって転送処理が決まります。受信フレームの VLAN ID を使用するには SCALANCE X-400 において VLAN を構築し、当該ポートをその VLAN のメンバーとすることが必要です。

設定した VLAN ID をもつ受信フレームは転送され、異なる VLAN ID をもつ受信フレームは廃棄されます。VLAN ID をもたないフレームを受信したときは設定した VLAN ID に向けて転送されます。

CLI のシンタックス

表 4-40 VLAN Port Parameters : CLI#SWITCH#VLAN>

コマンド	説明	備考
portvid <VLAN ID> [ポート番号]	指定ポートで受信した VLAN タグのないフレームに対して<VLAN ID>が入った VLAN タグを付加します。	管理者のみ。
accept <tag all> [ポート番号]	VLAN タグのないフレームの処理方法を指定します。 <ul style="list-style-type: none"> tag SCALANCE X-400 はタグのないフレームをすべて廃棄します。 all SCALANCE X-400 はすべてのフレームを転送します。 	管理者のみ。
ingress <E D> [ポート番号]	受信フレームに対する VID 評価の実施・不実施を指定します。	管理者のみ。
ports	ポートと対応する VLAN 設定の概要を表示します。	

4.5.11 GVRP Configuration メニュー

GVRP 機能の有効化

GVRP フレームを使うと、末端ノードまたはスイッチは SCALANCE X-400 のポートに VID を登録することができます。各ポートに対する GVRP 機能の有効化は GVRP Configuration メニューで行えます。

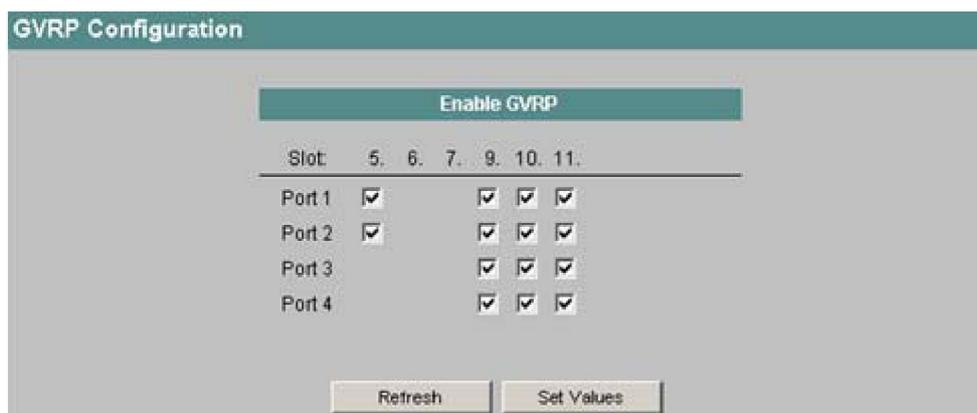


図 4-47 GVRP Configuration 画面

Enable GVRP のチェックボックス

ボックスをチェックすると、GVRP フレームによる VLAN 登録が対応ポートにおいて可能になります。SCALANCE X-400 はそのポートから GVRP フレームを送出することもできます。

CLI のシンタックス

表 4-41 GVRP Configuration : CLI#SWITCH#VLAN>

コマンド	説明	備考
gvrpport <E D> [port1, port2, ...]	GVRP による VLAN の動的な登録を指定ポートに対して可能または不可能にします。	管理者のみ。

4.5.12 Spanning Tree Configuration メニュー

冗長接続におけるループ防止

スパニングツリープロトコル (STP) を用いると、2 端末間に複数本の接続があるネット構成を実現できます。データトラフィックに対して 1 本のパスのみを許容し、それ以外の (冗長用) ポートを不使用とすることにより、ネットワーク内のループ発生を防止します。通信障害が発生すればデータは代替パスを使って転送されます。スパニングツリーの機能は、コンフィグレーションフレームとトポロジー変化通知フレームの交換を通して実現されます。

コンフィグレーションフレームを使ったネットワークトポロジーの定義

スイッチどうしは BPDU (Bridge Protocol Data Unit) というコンフィグレーションフレームをやりとりしてトポロジーを計算します。ルートブリッジの選択とネットワークトポロジーの生成はこのフレームを使って行われます。ルートブリッジとは、関連するすべての機器を対象にスパニングツリーをコントロールするブリッジです。BPDU はブリッジポートの状態変化についても通知します。

高速スパニングツリー

高速スパニングツリープロトコル (RSTP) はスパニングツリープロトコルを発展させたものであり、再構成時間が改善されました。スパニングツリーの標準的な再構成時間が 20~30 秒であるのに対し、高速スパニングツリーでは 1 秒程度です。これは以下のような対策によって実現されました。

- エッジポート
Hello タイム (2 つのコンフィグレーションフレームの間隔) が経過すると、エッジポートに指定されたポートが作動します。Hello タイムが経過すると、スイッチはコンフィグレーションフレームがもう来ないと判断したうえ、そのポートがエッジポートであることを認識します。ユーザが Hello タイムを使いたくない場合は、そのポートにおいてスパニングツリーを止めることができます。
- ポイントツーポイント (隣接する 2 スイッチによる直接的な通信)
スイッチを直接つなぐことによって状態変更 (ポートの再構成) を遅延なく行えます。
- 代替ポート (ルートポートの代役)
ルートポートの代わりとなるポートが設定されます。ルートブリッジとの接続が失われた場合には、再構成によって代替ポートとの接続をただちに確立することができます。
- フィルタテーブル
高速スパニングツリーでは再構成の影響を受けるポートがフィルタテーブルからただちに削除されます。一方、スパニングツリーの場合、ポートの削除ポイントはそのポートがフィルタテーブルに登録された時間によって決まります。

- イベントに対する反応
高速スパニングツリーは接続の異常終了といったイベントにただちに反応します。スパニングツリーのようにタイムアウトを待つことはありません。

以上のように、高速スパニングツリーでは基本的に多くのパラメータについて代替方法があらかじめ設定されており、ネットワーク構成に関する属性をある程度考慮することによって再構成時間を短縮しています。

スパニングツリーの設定と SCALANCE X-400

STP のパラメータは *Spanning Tree Configuration* メニューで表示・設定することができます。

Spanning Tree Configuration			
Bridge Priority:	32768	Root Priority:	28672
Bridge Address:	08:00:06:AA:62:12	Root Address:	08:00:06:AA:08:02
Root Port:	10.1	Root Cost:	19
Topology Changes:	1	Last Topology Change:	9m
Bridge Hello Time [s]:	2	Root Hello Time [s]:	2
Bridge Forward Delay [s]:	15	Root Forward Delay [s]:	15
Bridge Max Age [s]:	20	Root Max Age [s]:	20
<input type="button" value="Refresh"/> <input type="button" value="Set Values"/>			

図 4-48 Spanning Tree Configuration の画面

画面左側には SCALANCE X-400 の設定が、また右側にはルートブリッジの設定が表示されます。ルートブリッジの設定は SCALANCE X-400 が受信するスパニングツリーフレームから取得できます。そのためこのデータは読み出し専用です。SCALANCE X-400 がルートブリッジの場合には左右のデータが同じになります。各パラメータの意味は次のとおりです。

Bridge Priority / Root Priority

ルートブリッジになるスイッチは bridge priority によって決まります。優先度が最も高いブリッジ（すなわちこの値が最も低いもの）がルートブリッジになります。同じ優先度のスイッチがネットワーク内に複数台ある場合は、MAC アドレスの数値が最も低いスイッチがルートブリッジになります。bridge priority と MAC アドレスを合わせたものがブリッジ識別子 (bridge identifier) です。ルートブリッジはすべての経路変更を管理するため、フレーム遅延が少なくなるようになるべく中心的な位置に設置します。bridge priority の値は 4096 の倍数で、0 から 65,535 の間です。

Bridge Address / Root Address

SCALANCE X-400 とルートブリッジの MAC アドレスです。

Root Port

装置がルートブリッジとの通信に使用するポートです。

Topology Changes / Last Topology Change

SCALANCE X-400 側の値は、最後の再起動以降にスパニングツリーによって再構成が行われた回数を示します。ルートブリッジ側では、最後に再構成が行われてからの経過時間が分で示されます（値の最後に m が付きます）。

Bridge Hello Time / Root Hello Time

各ブリッジはコンフィグレーションフレーム (BPDU) を定期的に送出します。この2つのフレームの送出間隔を Hello タイムといいます。

Bridge Forward Delay / Root Forward Delay

新しい構成データはブリッジによって即座に使用されるのではなく、Forward Delay で指定される時間の経過後に有効になります。この方式により、すべてのブリッジが必要な情報を得てから新トポロジーでの運用を開始できるようになります。デフォルト値は 15 秒です。

Bridge Max Age / Root Max Age

Max Age は、ブリッジがコンフィグレーションフレーム (BPDU) を待つ上限時間です。この時間が経過するとブリッジはネットワークの再構成を試みます。デフォルト値は 20 秒です。

CLI のシンタックス

表 4-42 Spanning Tree Configuration : CLI \neq SWITCH \neq STP>

コマンド	説明	備考
info	スパニングツリーに関する現在の設定を表示します。	
bprio <0...61440>	SCALANCE X-400 のブリッジ優先度を指定します。	管理者のみ。
hellotm <1 ... 10>	2つのBPDUの送出間隔を秒数で指定します。	管理者のみ。
fwddelay <4 ... 30>	ネットワーク構成情報が有効になるまでの遅延時間を秒数で指定します。	管理者のみ。 デフォルト値 : 15 秒
maxage <6 ... 40>	ネットワーク構成情報の最長待ち時間を指定します。	管理者のみ。 デフォルト値 : 20 秒

4.5.13 Spanning Tree Ports Parameters メニュー

ポート別パラメータ

この画面では、ユーザまたは SCALANCE X-400 の自動機能によって設定された現在のポートパラメータを表示します。

Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. t. P.
5.1	enabled	128	20000	disabled	1	yes	no
5.2	enabled	128	20000	disabled	1	yes	no
7.1	enabled	128	200000	disabled	1	yes	no
7.2	enabled	128	200000	disabled	1	yes	no
9.1	enabled	128	200000	disabled	4	yes	no
9.2	enabled	128	200000	disabled	2	yes	no
9.3	enabled	128	200000	forwarding	6	yes	no
9.4	enabled	128	200000	forwarding	4	yes	no
10.1	enabled	128	200000	disabled	3	yes	no
10.2	enabled	128	200000	disabled	4	yes	no
10.3	enabled	128	200000	disabled	2	yes	no
10.4	enabled	128	200000	disabled	1	yes	no
11.1	enabled	128	200000	disabled	4	yes	no
11.2	enabled	128	200000	disabled	3	yes	no
11.3	enabled	128	200000	disabled	1	yes	no
11.4	enabled	128	200000	disabled	2	yes	no

Refresh

図 4-49 (Rapid) Spanning Tree Ports Parameters の画面

ポートテーブルの 8 つの欄にはそれぞれ以下の情報が示されます。

Port

このスロットとポートに関する情報が右に表示されます。

STP Status

そのポートに対してスパニングツリーが有効 (enabled) か無効 (disabled) かを示します。

Priority

スパニングツリーによって計算したパスがスイッチの複数ポートで可能な場合、優先度が最も高い (すなわちこのパラメータ値が最小の) ポートが選択されます。優先度には 0 から 255 の値を指定できます。デフォルト値は 128。

Path Cost

このパラメータはパス選択の計算に使用されます。値が小さいほどパスの使用確率が高くなります。同じ値のポートがスイッチに複数ある場合にはポート番号が最小のものが使用されます。

パスコストの計算の大部分は伝送速度に基づきます。可能な伝送速度が大きいほど Path Cost の値は小さくします。

スパニングツリーにおける代表的な値は次のとおりです。

- 1000Mbps=4
- 100Mbps=19
- 10Mbps=100

高速スパニングツリーにおける代表的な値は次のとおりです。

- 1000Mbps=20,000
- 100Mbps=200,000
- 10Mbps=2,000,000

値は個別に設定することもできます。

State

ポートの現在の状態を示します。以下の状態があります。

- disabled
ポートは受信のみを行い、STP のコンフィグレーションには関与しません。
- blocking
閉塞モードでは BPDU の受信は行われず。
- listening
この状態では BPDU の受信と送信が行われます。ポートは STP に関与します。
- learning
転送状態の前の段階です。ポートはトポロジー（すなわちノードアドレス）を積極的に学習しているところです。
- forwarding
再構成時間の後にネットワーク内で再び動作状態になり、データフレームの送受信を行います。

Fwd Transitions

listening 状態から forwarding 状態に遷移する回数を示します。

Edge

以下の値があります。

- yes
このポートにはエッジポートがつながっています。
- no
このポートには STP または RSTP の装置があります。

エッジポートが接続されている場合、SCALANCE X-400 はスパニングツリーフレームを考慮することなく、ポート切り替えをより短時間で行えます。この設定にもかかわらずスパニングツリーフレームを受信した場合、ポートはスイッチに対して自動的に「no」の設定に切り替わります。

P.t.P.

RSTP に準拠した 2 台のネットワーク機器がこのポートを介して互いに接続されている場合には、ポイントツーポイントのリンクが存在します。これには以下の 4 つの状態があります。

- ForceTrue
半二重接続であっても直接のリンクがあるとみなされます。
- ForceFalse
全二重接続であっても直接のリンクはないとみなされます。
- Auto
ポイントツーポイントは自動的に検出されます。ポートが半二重（Shared Media Connection）に設定されている場合、直接のリンクはないとみなされます。

- No
ポイントツーポイントのリンクは存在しません。

STP/RSTP に関するポートの設定

左端のポート名をクリックすると、*Spanning Tree Port Configuration* 画面が開きます。

図 4-50 (Rapid) Spanning Tree Port Configuration の画面

STP enabled チェックボックス

そのポートで STP/RSTP を使用したい場合にはこのボックスをチェックします。

Admin Edge Port チェックボックス

そのポートに末端装置が接続されている場合にはこのボックスをチェックします。チェックしない場合、リンクが変化するとネットワークの再構成が行われます。

Priority

ポートの優先度を 0 から 255 の数値で指定します。

Admin Path Cost

Path Cost のパラメータ値を入力できます。ゼロを入力すると Path Cost の値は計算によって決まります。

Path Cost

Admin Path Cost でゼロを入力した場合には Path Cost の計算値がここに表示されます。Admin Path Cost にゼロ以外の値を入力した場合にはここにその値が表示されます。

Admin Point to Point Status チェックボックス

3 種類の設定が可能です。

- Point to Point Connection をチェック
ポートテーブルの ForceTrue に対応します。
- Shared Media Connection をチェック
ポートテーブルの ForceFalse に対応します。
- Point to Point Connection と Shared Media Connection をチェック
ポートテーブルの Auto に対応します。

付記

ポイントツーポイントとは、2 台のスイッチを直接接続することを意味します。また Shared Media Connection には、たとえばハブとの接続があります。

CLI のシンタックス

表 4-43 Spanning Tree Ports Parameters : CLI¥SWITCH¥STP>

コマンド	説明	備考
portstp <E D> [ポート番号]	指定ポートに対して STP を有効または無効にします。	管理者のみ。 パラメータとして複数ポートを指定したいときは、ポート番号を空白またはハイフンで区切ることができます。
portprio <ポート番号> <0 ... 255>	ポートの優先度を指定します。	管理者のみ。
pathcost <ポート番号> <0 ... 65535>	ポートのパスコストを指定します。	管理者のみ。
edgeport <ポート番号> <T F>	STP または RSTP をサポートするエッジポート (T) もしくはスイッチ (F) がこのポートにつながっているかどうかを指定します。STP/RSTP を受信すると、値「F」が表示されます。	
ptpport <ポート番号> <A T F>	ポイントツーポイントのリンクは 2 台のスイッチ間に直通リンクを確立します。このとき以下の選択肢があります。 <ul style="list-style-type: none"> • A ポートは全二重か半二重かによってポイントツーポイントかどうか認識します。全二重ならポイントツーポイントで、半二重ならポイントツーポイントではない (共有媒体である) とみなします。 • T そのポートが半二重であってもポイントツーポイントのリンクとみなします。 • F そのポートが全二重であっても、ポイントツーポイントのリンクはないものとみなします。 	
Ports	ポートの概要および対応する RSTP の設定を表示します。	

4.6 ルータメニュー (SCALANCE X414-3E)

付記

ルーティング機能を備えているのは SCALANCE X414-3E のみです。

はじめに

SCALANCE X414-3E をルータとして設定するには、最初に少なくとも 2 つのサブネットを構築したうえで、あらかじめ作成した VLAN にそれぞれのサブネットを割り当てる作業が必要です。この段階でスタティックルート (固定経路) の設定や、RIP や OSPF といったルータプロトコルの有効化が可能になります。

VLAN の設定については「Current VLAN Configuration メニュー」をご覧ください。

4.6.1 Router Configuration メニュー

はじめに

[Router]フォルダのアイコンをクリックすると Router Configuration 画面が現れます。この画面を使うと、SCALANCE X-400 を IPv4 ルータに設定できます。

ルーティング情報をネットワーク内に配布するにあたっては RIPv2 と OSPFv2 のプロトコルが使用できますが、ここでその選択を行えます。各プロトコルに関する詳しい設定は対応するサブメニューにあります。



図 4-51 Router Configuration の画面

SCALANCE X-400 の設定

RIP チェックボックス

RIP (Routing Information Protocol) バージョン 2 を有効にします。

付記

最低 1 つのインタフェースを RIP に設定したら、そのルータはただちに RIP プロトコルを使用します。

OSPF チェックボックス

OSPF (Open Shortest Path First) バージョン 2 を有効にします。

付記

ルータ ID がすでに与えられている場合、最低 1 つのインタフェースを OSPF に設定したら、そのルータはただちに OSPF プロトコルを使用します。

CLI のシンタックス

表 4-44 Router Configuration : CLI#ROUTER>

コマンド	説明	備考
setrip <E D>	RIP を有効または無効にします。	管理者のみ。
setospf <E D>	OSPF を有効または無効にします。	管理者のみ。

4.6.2 Subnets メニュー

サブネットの構築

SCALANCE X-400 を IPv4 ルータとして運用するには、複数の (最低 2 つの) サブネットを構築する必要があります。

1 つめのサブネットはエージェント設定に対応します (「エージェントメニュー」のセクションをご覧ください)。データの変更はそこでしか行えません。

それ以外のすべてのサブネットはここで作成できます ([New Entry] ボタンをクリックします)。1 つのサブネットは、VLAN メニューで以前に作成した 1 つの VLAN ID と必ず対応します。



図 4-52 Router Subnets の画面

VID 欄

IP サブネットの VLAN ID です。

IP Address 欄

サブネットの IP アドレスです (他との重複がないものとします)。

Subnet Mask 欄

IP サブネットのサブネットマスクです。サブネットマスクの左詰ビット表記に現れる「1」の列が、IP アドレスのネットワーク ID を表します。

Name 欄

サブネットに対して自由に付与できる名前です。1 つめのサブネットマスクの名前はエージェント設定と一致している必要があり、「Agent Configuration」と決まっています。

Status 欄

サブネットの状態です。以下の 4 つの状態があります。

- static
- invalid :
状態が「invalid」であるサブネットは設定エラーを示すため、対処が必要です。
- BOOTP :
ブートストラップ・プロトコル (IP アドレスの自動割り当てを行うプロトコル)
- DHCP :
Dynamic Host Configuration Protocol (BOOTP の改良版)

新しい IP サブネットの作成

Router Subnets 画面の[New Entry]ボタンをクリックすると新しいサブネットを作成できます。サブネットの設定は「Router Subnet Configuration」メニューで行えます。



図 4-53 Router Subnet Configuration の画面

VLAN ID

その IP サブネットのパケットが送信される VLAN の ID を入力します。ID の値の範囲は 1 から 4094 です (VLAN ID については「Current VLAN Configuration メニュー」をご覧ください)。

付記

エージェントの VLAN ID は再利用できません。それ以外のすべての VLAN ID は複数回使用できます。

IP Address

その IP サブネットの IP アドレスを入力します。IP アドレスは一回しか使用できません。

付記

「/」の記号と 1 から 30 までの数字を後ろに続ければ、サブネットも同時に定義できます。

Subnet Mask

いま作成している IP サブネットのサブネットマスクを入力します。サブネットマスクは「1」を左詰したビットフィールドで定義します。

Name

サブネットの名前を入力します (名前は機能にはまったく影響しません)。

CLI のシンタックス

表 4-45 Subnets : CLI¥ROUTER¥SUBNETS>

コマンド	説明	備考
info	現在のサブネットを表示します。	管理者のみ。
add <VID> <IP アドレス> <サブネット> [名前]	新しいサブネットを追加します。「サブネット」のパラメータはサブネットマスクを指定します。	管理者のみ。
edit <VID> <IP アドレス> [サブネット] [名前]	サブネットを変更します。「サブネット」のパラメータはサブネットマスクを指定します。	管理者のみ。
delete <VID> <IP アドレス>	サブネットを削除します。	管理者のみ。

CLI の「info」コマンドを入力するとテーブル (ウェブインタフェースのテーブルと同様のもの) が表示されます。ただし Status 欄は 2 文字 (St) で表示されます。

以下の状態があります (ウェブインタフェースも参照してください)。

- BP (BOOTP)
- DP (DHCP)
- st (static)
- ?? (invalid)

4.6.3 Current Routes メニュー

ルーティングテーブル

このメニューではルーティングテーブルを表示します。スタティックルーティングテーブルへのデータ登録もここから行えます。

ルーティングテーブルは一般に受信パケットの転送ルールを羅列したものです。パケットのルーティングを行う場合、その宛先アドレスをルーティングテーブルに登録されたアドレスと比較します。アドレス全体ならびにサブネットマスクが最もよく一致するルーティングデータ（最長プレフィックスの検索方法を使用）がそのパケットの転送方法を表します。

複数のルートを作成してスタティックルートの設定を行えば、ルーティングプロトコルを使わずに IP ルータを構築できます。

ルーティングテーブルにおいて状態が「local」になっているルーティングデータは、設定されたサブネットであることを示します。

Destination	Subnet Mask	VID	Next IP Address	Name	Metric	Status	HW
3.0.0.0	255.0.0.0	4	4.0.0.3	Dynamic	1	ospf	yes
1.0.0.0	255.0.0.0	1	1.0.0.1	Dynamic	0	local	yes
2.0.0.0	255.0.0.0	2	2.0.0.1	Dynamic	0	local	yes
4.0.0.0	255.0.0.0	4	4.0.0.1	Dynamic	0	local	yes
5.0.0.0	255.0.0.0	5	5.0.0.1	Dynamic	0	local	yes
8.0.0.0	255.0.0.0	8	8.0.0.1	Dynamic	0	local	yes

図 4-54 Current Routes の画面

Destination 欄

そのルートの宛先アドレスです。

Subnet Mask 欄

左の宛先アドレスにおける有効ビットを示します。「1」を左詰した形式になります。

VID 欄

そのルールを適用した場合にパケットが転送される IP サブネットに対応する VLAN ID を示します。

Next IP Address 欄

次にアクセスする装置の IP アドレスです。

Name 欄

名前はルーティング処理に影響を与えません。

スタティックルートには名前を与えることができます。ルートがダイナミックの場合には「Dynamic」になります。

Metric 欄

ルータと宛先の距離を示します。

Status 欄

ルートが OSPF または RIP のプロトコルによって生成されたのか、あるいはスタティックルートまたはローカルルートとして作成されたのかを示します。

スタティックルートは[New Entry]ボタンを使って手動で作成します。

ローカルルートはサブネット生成時に自動的に作成されます。

HW 欄

HW (ハードウェア) 欄は、ハードウェアへのルートの割り付けについて示します。以下の区別があります。

- yes :
ハードウェアに保存可能です。
- in use :
すでにハードウェアに保存されています。
- no :
ハードウェアに保存してはなりません。
スタティックルートの場合には「yes」か「no」を設定できます。「in use」と表示されるのは、ルートがハードウェアに保存され、しかも実際に使用されている場合に限られます。

新規スタティックルートの作成

Current Routes ダイアログの[New Entry]ボタンを使えば新しいルートを作成できます。この方法で作成されるルートはすべてスタティックになります。

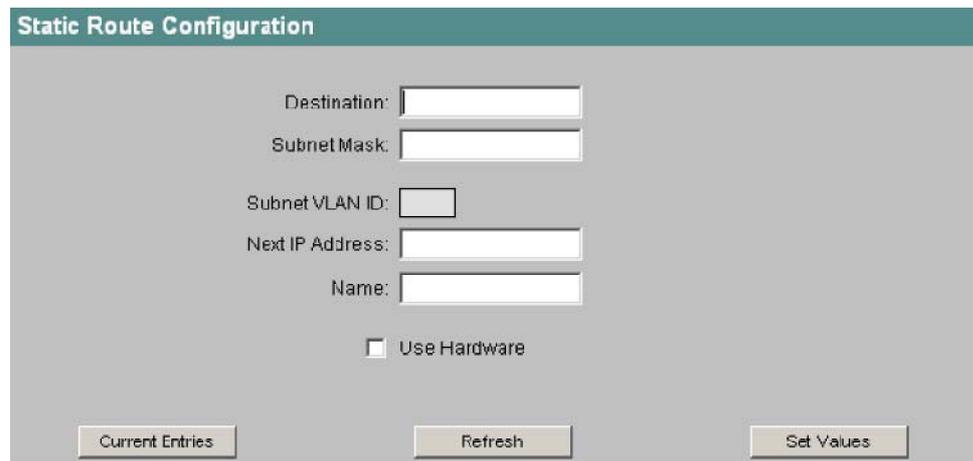


図 4-55 Static Route Configuration の画面

Destination

ルーティングテーブルの項目に対応する IP アドレスを入力します。

Subnet Mask

そのルーティング項目のサブネットマスクを入力します。これは、ルーティング比較において対象となるアドレスのビット位置を示します。

Subnet VLAN ID 表示欄

Next IP Address から自動的に計算されます。新規システムの場合は空欄です。

Next IP Address

このルートにおける次のパケット送出先ルータの IP アドレスを入力します。そのルータは接続されるサブネット内に存在する必要があります。

Name

ルートの名前を入力します (名前は機能にはまったく影響しません)。

Use Hardware チェックボックス

ルートをハードウェアに書き込みたい場合はこのボックスをチェックします。これを有効にすると、パケットが最初に正常転送されたときにこのルートがハードウェアに書き込まれます。以後は効率のよい転送処理が可能になります。

付記

ハードウェアへのルートの書き込みは、必要な記憶容量が残っている場合にのみ行われます。

CLI のシンタックス

表 4-46 Current Routes : CLI#ROUTER#ROUTES>

コマンド	説明	備考
info	現在のルート情報を表示します。	管理者のみ。
add <IP アドレス> <サブネット> <次の IP> [E D] [名前]	新しいルートを追加します。E D パラメータは「Use Hardware」のオン・オフに対応します。	管理者のみ。
edit <IP アドレス> [次の IP] [E D] [名前]	ルート情報を変更します。E D パラメータは「Use Hardware」のオン・オフに対応します。	管理者のみ。
delete <IP アドレス>	ルートを削除します。	管理者のみ。

CLI の「info」コマンドを入力するとテーブル（ウェブインタフェースのテーブルと同様のもの）が表示されます。ただし Metric 欄と Status 欄は 2 文字（Me と St）で表示されます。

以下の状態があります。

- OS (OSPF)
- RI (RIP)
- st (スタティック)
- lo (ローカル)
- ot (その他)
- ?? (無効)

ハードウェア (HW) 欄には以下の状態があります（ウェブインタフェースの説明もご覧ください）。

- 可 : X (大文字)
- 使用中 : * (アスタリスク)
- 不可 : - (マイナス記号)

4.6.4 RIPv2 Configuration メニュー

はじめに

RIPv2 Configuration 画面では RIP プロトコルに関する基本パラメータのほか、一部の基本的な統計カウンタを設定できます。

付記

このメニューで行った設定を有効にするには、Router Configuration メニューにおいて RIP を有効にすることが必要です。

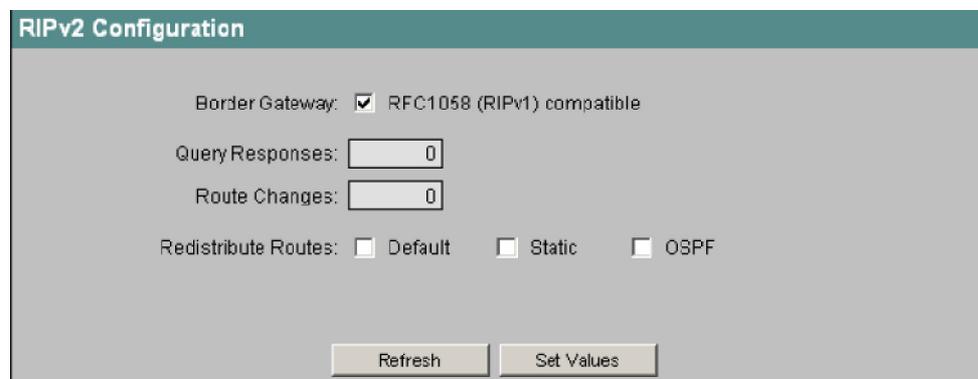


図 4-56 RIPv2 Configuration の画面

Border Gateway チェックボックス

このチェックボックスは、ルータを初期の RIPv1 ルータとともに運用する場合にのみチェックしてください。このときサブネットルートは特定のクラスにグループ分けされ、いわゆるスーパーネットは使用されません。この機能を使用すれば、RIPv1 ルータに対して最大限の親和性が得られます。

Query Responses 表示欄

応答のあった特別なルーティングクエリの数。

Route Change 表示欄

ルーティングテーブルが変更された回数。

Redistribute Routes チェックボックス (Default/Static/OSPF)

RIP で転送を行う既知ルートを指定します。Default/Static/OSPF のルートタイプに対して異なる選択を行えます。

付記

このボックスをチェックするのは、異なるネットワークをつなぐゲートウェイ（境界ゲートウェイ）の場合のみとしてください。また Default と Static をネットワーク内で多く有効にしすぎると、（たとえば転送ループによる負荷の増大などによって）問題が発生するおそれがあります。

CLI のシンタックス

表 4-47 RIPv2 Configuration : CLI#ROUTER#RIP>

コマンド	説明	備考
info	現在の RIP 設定を表示します。	
rfc1058 <E D>	RFC1058 (RIPv1) との併用を可能にします。	管理者のみ。
redistr <E D> <E D> <E D>	「再送信ルート」を有効または無効にします。 第 1 パラメータ : デフォルトルート 第 2 パラメータ : スタティックルート 第 3 パラメータ : OSPF ルート	管理者のみ。

4.6.5 RIPv2 Interfaces メニュー

はじめに

RIPv2 Interfaces ダイアログは RIP プロトコルを使用するすべての IP サブネットの概要を示します。
[New Entry] ボタンをクリックすると、RIP に関する新しいサブネットを登録できます。

付記

RIP について新しいサブネットを登録するには、Router Subnets メニューを使ってサブネットをあらかじめ作成しておく必要があります。

IP Address	Send Updates	Receive Updates	Default Metric	Authent Type	Bad Packets	Bad Routes	Updates Sent
21.0.0.2	RIPv2	RIPv1v2	1	none	0	0	0
22.0.0.2	RIPv2	RIPv1v2	1	none	0	0	0

図 4-57 RIPv2 Interfaces の画面

IP Address 欄

RIP 対応サブネットの IP アドレス (このテーブルの唯一の識別子)。サブネットに関するその他のパラメータ (サブネットマスクなど) は Router Subnets ダイアログで見ることができます。

Send Updates 欄

最新情報 (アップデート) の送出方法を示します。以下のケースがあります。

- no send
アップデートは送出されません。
- RIPv1
RIPv1 のアップデートが RFC 1058 に従って送出されます。
- RIPv1-compatible
RIPv2 のアップデートが RFC 1058 のルールに従ってブロードキャストで送出されます。
- RIPv2
RIPv2 のアップデートがマルチキャストで送出されます。
- RIPv1 demand と RIPv2 demand
明示的なクエリに対する応答としてのみ RIP パケットが送出されます。
このオプションを使用するのは、お使いのルータが他のルータと WAN インタフェースを介して通信する場合に限られます。

Receive Updates 欄

受信 RIP パケットのうち許容されるものを示します。以下のケースがあります。

- no receive
パケットは一切許容されません。
- RIPv1
RIPv1 ルータからのパケットのみ許容されます。
- RIPv2
RIPv2 ルータからのパケットのみ受信および処理されます。
- RIPv1/v2
このインタフェースでは全種類の RIP プロトコルが許容されます。

Default Metric 欄

このインタフェースにおいてデフォルトルートに付与されているメトリック (指標値) を示します。「0」はデフォルトルートが使用されないことを示します。それ以外の場合は、1 から 15 の値が有効です。

Authent. Type 欄

認証タイプを示します。以下のケースがあります。

- 認証なし
- 単純なパスワード
- MD5 を使った認証

Bad Packets 欄

廃棄されたために無視されることとなった受信 RIP パケット数。

Bad Routes 欄

有効 RIP パケットのルートのうち考慮されなかったルートの数。

Updated Sent 欄

このインタフェースにおける「トリガ型情報送出」の回数。

新規 RIPv2 インタフェースの作成

RIPv2 Interfaces ダイアログの[New Entry]ボタンをクリックすると新規インタフェースが作成できます。以下のような画面が現れます。

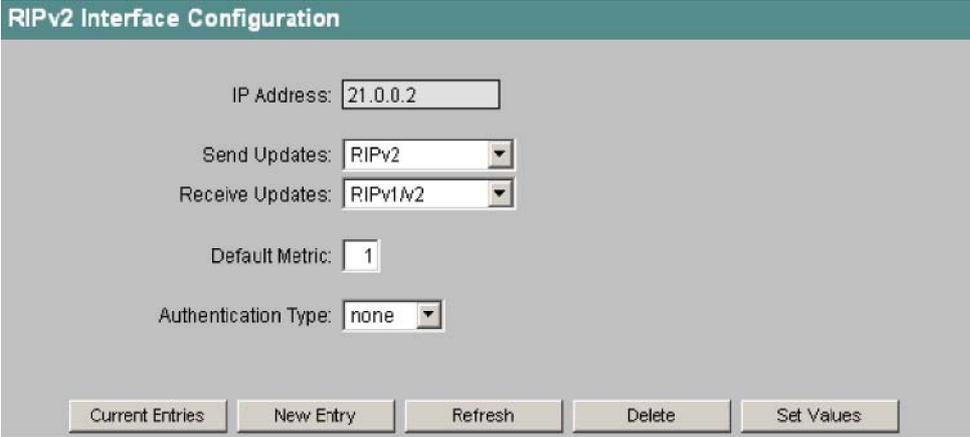


図 4-58 RIPv2 Interface Configuration の画面

IP アドレス

RIP の設定を行うインタフェースの IP アドレスを入力します。この IP アドレスはすでに IP サブネットとして設定されていることが必要です。

Send Updates ドロップダウンリスト

RIP の最新情報（アップデート）の送出方法を選択します。アップデートパケットにはローカルシステムのルーティングテーブルが入っています。以下の選択肢があります。

- no send
アップデートを送出しません。
- RIPv1
RIPv1 のアップデートを RFC 1058 に従って送出します。
- RIPv1-compatible
RIPv2 のアップデートを RFC 1058 のルールに従ってブロードキャストで送出します。
- RIPv2
RIPv2 のアップデートをマルチキャストで送出します。
- RIPv1 demand と RIPv2 demand
これが必要になるのは WAN インタフェースの場合にのみです。その場合、明示的なクエリに対する応答としてのみ RIP パケットが送出されます。

付記

自ネットワーク内に RIPv1 装置がまったくない場合には「RIPv2」に設定してください。

Receive Updates ドロップダウンリスト

受信パケット（アップデート）を許容する基準を指定します。以下の選択肢があります。

- no receive
アップデートを受容しません。
- RIPv1
RIPv1 のアップデートを受容します。
- RIPv2
RIPv2 のアップデートを受容します。
- RIPv1/v2
RIPv1 と RIPv2 のアップデートを受容します。

Default Metric

このインタフェースでデフォルトルートに付与するメトリック（指標値）を示します。RIP ではホップ数のメトリックを使用します。この方式では「使用ルータ数」によって距離を指定します。値の範囲は 1~15 です（「0」に設定するとデフォルトルートは使用されません）。

以下のルールが適用されます：値が大きいほど宛先までの距離が長くなります

Authentication Type ドロップダウンリスト

RIP パケットの認証方法を選択します。以下の選択肢があります。

- none : 認証なし（デフォルト）
- simple : パスワードと確認による認証
- MD5 : Keyed MD5 を用いた認証（パスワードと確認とキーID）

これらの方法はパケットの認証のために使用されるだけです。データの暗号化は行われません。

Key ID

付記

「Key ID」のテキストボックスは「MD5」の認証方法を指定した場合にのみ表示されます。

パスワードを鍵に使用するときの鍵 ID を入力します。鍵 ID はプロトコルによって転送されるため、すべての隣接ルータでは同じ鍵を同じ鍵 ID で保存する必要があります。

Password/Confirmation

付記

「Password/Confirmation」のテキストボックスは「MD5」または「simple」の認証方法を指定した場合にのみ表示されます。

認証にパスワードを用いる場合には MD5 において鍵が必要であり、それをここに入力します。

CLI のシンタックス

表 4-48 RIPv2 Interfaces : CLI¥ROUTER¥RIP¥RIP¥IFACE>

コマンド	説明	備考
add <IP アドレス> [送信 Upd] [受信 Upd] [メトリック]	現在のインタフェースを表示します。 新規インタフェースを追加します。 送信 Upd に指定できる値 : <ul style="list-style-type: none"> • SV1 : RIPv1 • SV1C : RIPv1 互換 • SV1D : RIPv1 要求 • SV2 : RIPv2 • SV2D : RIPv2 要求 • SNO : 送出なし 受信 Upd に指定できる値 : <ul style="list-style-type: none"> • RV1 : RIPv1 • RV2 : RIPv2 • RV1V2 : RIPv1/v2 • RNO : 受信なし 	管理者のみ。
edit <IP アドレス> [送信 Upd] [受信 Upd] [メトリック]	インタフェースを変更します。 送信 Upd に指定できる値 : <ul style="list-style-type: none"> • SV1 : RIPv1 • SV1C : RIPv1 互換 • SV1D : RIPv1 要求 • SV2 : RIPv2 • SV2D : RIPv2 要求 • SNO : 送出なし 受信 Upd に指定できる値 : <ul style="list-style-type: none"> • RV1 : RIPv1 • RV2 : RIPv2 • RV1V2 : RIPv1/v2 • RNO : 受信なし 	管理者のみ。
auth <IP アドレス> <認証タイプ> [パスワード] [鍵 ID]	インタフェースの認証タイプを変更しま す。 指定できるタイプ : <ul style="list-style-type: none"> • None • Simple • MD5 (この場合のみ「鍵 ID」が必要で す) 	管理者のみ。
delete <IP アドレス>	インタフェースを削除します。	管理者のみ。

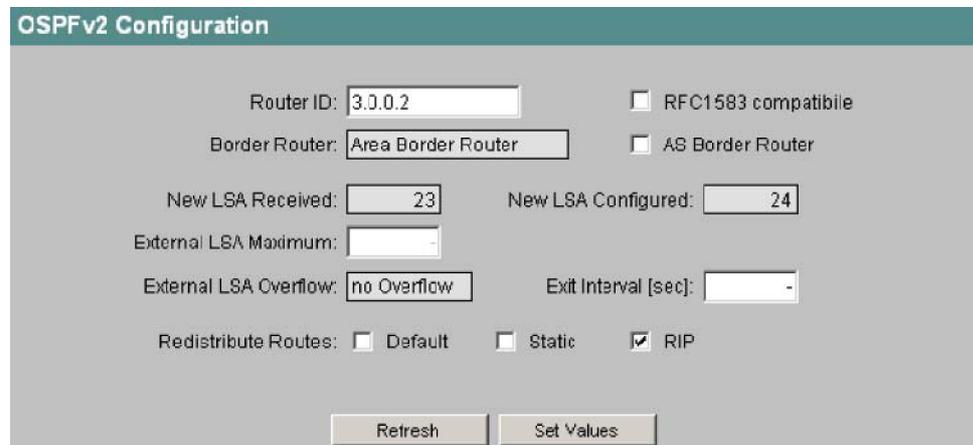
4.6.6 OSPFv2 Configuration メニュー

はじめに

OSPFv2 Configuration ダイアログとそのサブダイアログでは OSPF プロトコルのパラメータを設定できます。

OSPFv2 は管理下の IPv4 ネットワーク (自律システム、AS) をいくつかのエリアに分割します。全ルータのリンク状態をそのエリア内で交換し、各ルータがネットワークについて完全な現状データをもてるようにします。この現状データはリンク状態データベース (LSDB) において管理されます。その結果、各ルータはそのエリア内のすべてのルートを Dijkstra アルゴリズムに従って自機内で決定できます。

エリアが異なれば現状データの傾向も異なります。そのためルータの交換は、距離ベクトルアルゴリズムによって決定できる集団的なルートに限定されます。



The image shows the OSPFv2 Configuration dialog box. It has a title bar 'OSPFv2 Configuration'. The settings are as follows:

- Router ID: 3.0.0.2
- Border Router: Area Border Router
- New LSA Received: 23
- New LSA Configured: 24
- External LSA Maximum: (empty)
- External LSA Overflow: no Overflow
- Exit Interval [sec]: (empty)
- Redistribute Routes: Default, Static, RIP
- Checkboxes: RFC1583 compatible, AS Border Router
- Buttons: Refresh, Set Values

図 4-59 OSPFv2 Configuration の画面

Router ID

OSPF インタフェースの IP アドレスを入力します。このアドレスは一意であることが必要です。

RFC 1583 compatible チェックボックス

この設定が必要なのは、RFC 2328 と互換性のない古い OSPFv2 ルータをいまだに使用している場合に限られます。

Border Router 表示欄

境界ルータの状態を表示します。ローカルシステムが少なくとも 2 つのエリアにおいてアクティブメンバであれば、それは境界ルータです。

AS Border Router チェックボックス

ルータが AS 境界ルータとして動作している場合、すなわち複数のプロトコル世界を扱っている (たとえば追加的な RIP ネットワークを運用している) 場合には、これをチェックします。

New LSA Received カウンタ

LSA (リンク状態通知パケット) の受信数。アップデートと自身の LSA はカウント対象外です。

New LSA Configured カウンタ

そのローカルシステムが送出した各種 LSA の数。

External LSA Maximum

外部 LSDB に制限を課したい場合には、外部 LSA の最大数を入力します。

External LSA Overflow 表示欄

外部 LSA の最大数を超えたかどうかを示します。

Exit Interval [sec]

OSPF ルータがオーバーフロー状態から抜け出そうと試みるまでの待機時間を秒数で入力します。「0」を入力すると、OSPF ルータは再起動後にオーバーフロー状態から脱却しようとするだけです (ルータのメインメニューにおけるオン・オフを契機とします)。

Redistribute Routes チェックボックス (Default/Static/RIP)

OSPF で転送を行う既知ルートを指定します。Default/Static/RIP のルートタイプに対して異なる選択を行います。

付記

このボックスをチェックするのは、異なるネットワークをつなぐゲートウェイ (境界ゲートウェイ) の場合のみとしてください。また Default と Static をネットワーク内で多く有効にしすぎると問題 (転送ループなど) が発生するおそれがあります。

CLI のシンタックス

表 4-49 OSPFv2 Configuration : CLI#ROUTER#OSPF>

コマンド	説明	備考
info	現在の OSPF 設定を表示します。	
id <ルータ ID>	ルータ ID (IP アドレス) を設定します。	管理者のみ。
rfc1583 <E D>	RFC1583 との互換性の有無を設定します。	管理者のみ。
asbr <E D>	AS 境界ルータのオン・オフを設定します。	管理者のみ。
lsamax <最大値>	外部 LSA の最大値を設定します。	管理者のみ。
exitint <秒数>	脱却に関する待機時間を設定します。	管理者のみ。
redistr <E D> <E D> <E D>	「再送信ルート」を有効または無効にします。 <ul style="list-style-type: none"> • 第 1 パラメータ : デフォルトルート • 第 2 パラメータ : スタティックルート • 第 3 パラメータ : RIP ルート 	管理者のみ。
ospfdbg [E D] [デバッグタイプ]	OSPF のデバッグ機能を有効または無効にします。 ヘルプを表示するには「ospfdbg ?」と入力します。	管理者のみ。

4.6.7 OSPFv2 Areas メニュー

概要

自律システム (AS) はいくつかのエリアに分割することができます (「OSPFv2 Configuration メニュー」の項を参照)。

このダイアログではルータの OSPF エリアをモニタすることができます。設定パラメータのほかに統計値も表示されます。

OSPFv2 Areas							
Area ID	Area Type	Summary	Metric	Updates	LSA Cnt	Area BR	AS BR
<u>0.0.0.0</u>	Backbone			1	3	0	0
<u>0.0.0.2</u>	Normal			1	3	0	0
<u>0.0.0.3</u>	Normal			1	3	0	0
<u>0.0.0.4</u>	Normal			1	3	0	0
<u>0.0.0.5</u>	Normal			1	2	0	0
<u>0.0.0.6</u>	Normal			1	3	0	0
<u>0.0.0.7</u>	Normal			1	3	0	0
<u>0.0.0.8</u>	Normal			1	3	0	0

図 4-60 OSPFv2 Areas の画面

Area ID 欄

各エリアの番号を示します。エリア ID は 0 から 255 までの 4 つの数字からなります。これは一意であることが必要です。

「0.0.0.0」はバックボーンエリアです。

各エリアの LSDB はエリア内の全ルータに対して同期されます。

Area Type 欄

エリアのタイプを示します。以下のエリアタイプがあります。

- Normal
- Stub
- NSSA
- Backbone : ここではバックボーンエリアが強調表示されます。

Summary 欄

そのエリアに対してサマリ LSA が生成可能かどうかを示します。これが重要になるのはスタブエリアの場合だけです。以下の値があります。

- import : サマリ LSA はそのエリアに送信されます。
- disregard : サマリ LSA はそのエリアに送信されません。

Metric 欄

スタブエリアにおいて使用されるデフォルトルートのもトリックを示します。スタブエリア以外のエリアでは何も表示されません。

Updated 欄

ルーティングテーブルの計算回数。

LSA Cnt 欄

そのエリアの LSDB に記録されている LSA の数。

Area BR 欄

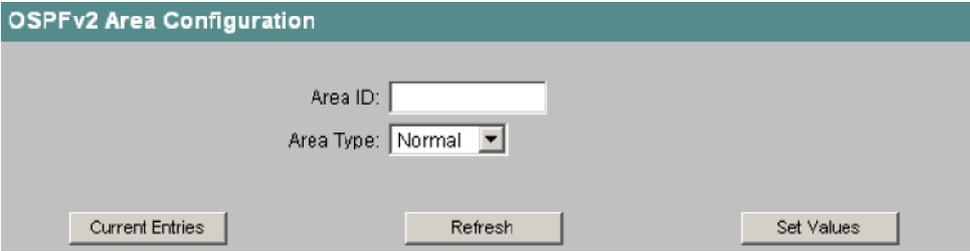
そのエリア内で到達可能なエリア境界ルータ (ABR) の数。

ASBR 欄

そのエリア内で到達可能な自律システム境界ルータ (ASBR) の数。

新しい OSPFv2 エリアの作成

OSPFv2 Areas ダイアログの[New Entry]ボタンをクリックすると新しいエリアを作成できます。



The image shows a dialog box titled "OSPFv2 Area Configuration". It contains two input fields: "Area ID:" followed by a text box, and "Area Type:" followed by a dropdown menu currently set to "Normal". At the bottom of the dialog, there are three buttons: "Current Entries", "Refresh", and "Set Values".

図 4-61 OSPFv2 Area Configuration の画面

Area ID

エリアの番号を入力します。

Area Type ドロップダウンリスト

以下のエリアタイプがあります。

- Normal
- Stub
- NSSA

付記

バックボーンエリアについては Area Type を「Normal」に、また Area ID を「0.0.0.0」にします。

Import Summary チェックボックス

付記

Import Summary のチェックボックスは、エリアタイプを「Stub」にしたときのみ表示されます。

このボックスをチェックすると、そのエリア内でサマリ LSA が生成および配信されます。その場合、ネットワーク全域内の通信にデフォルトルートは必要ありません。

付記

そのスタブエリア内に境界ルータが 1 台しかないときは、このオプションを有効にする必要はありません。

Default Metric

付記

Default Metric のテキストボックスは、エリアタイプを「Stub」にしたときのみ表示されます。

そのエリア内で使用されるデフォルトルートのメトリックを入力します。

CLI のシンタックス

表 4-50 OSPFv2 Areas : CLI¥ROUTER¥OSPF¥AREAS>

コマンド	説明	備考
info	現在のエリアについて表示します。	
add <エリア ID> <タイプ> [E D] [メトリック]	新しいエリアを追加します。 使用できるタイプ： <ul style="list-style-type: none"> Standard Stub NSSA [E D]とメトリックはスタブエリアの場合のみ指定できます。 [E D]=サマリのインポートの有効化または無効化	管理者のみ。
edit <エリア ID> [タイプ] [E D] [メトリック]	「cliRouterOspfAreasEdit」 エリアを変更します。 使用できるタイプ： <ul style="list-style-type: none"> Standard Stub NSSA [E D]とメトリックはスタブエリアの場合のみ指定できます。 [E D]=サマリのインポートの有効化または無効化	管理者のみ。
delete <エリア ID>	エリアを削除します。	管理者のみ。

4.6.8 OSPFv2 Area Ranges メニュー

概要

OSPFv2 Area Ranges ダイアログではアドレス範囲を作成できます。伝搬時にさまざまなアドレス範囲をグループ化できます。この機能によってエリア内のサマリ LSA の数を低減できます。

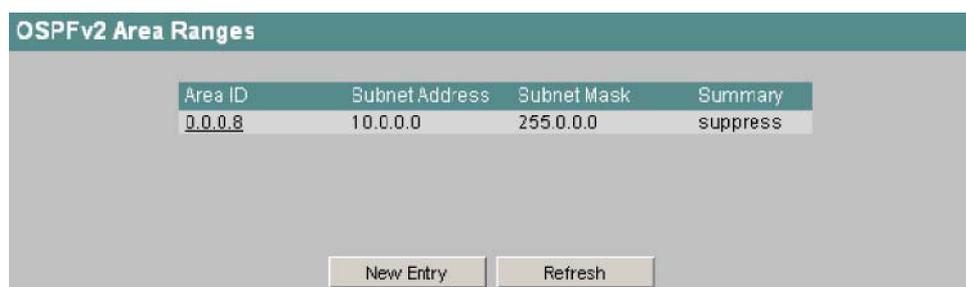


図 4-62 OSPFv2 Area Ranges の画面

Area ID 欄

アドレス範囲に対応するエリア ID です。

Subnet Address 欄

グループ化するネットワークエリアのアドレスです。

Subnet Mask 欄

グループ化するネットワークエリアのサブネットマスクです。

Summary 欄

グループアドレス範囲の通知を行うかどうかを示します。

新しい OSPFv2 エリア範囲の作成

OSPFv2 Area Ranges ダイアログの[New Entry]ボタンをクリックすると、1 エリアにつき 4 つのエリア範囲を作成できます。

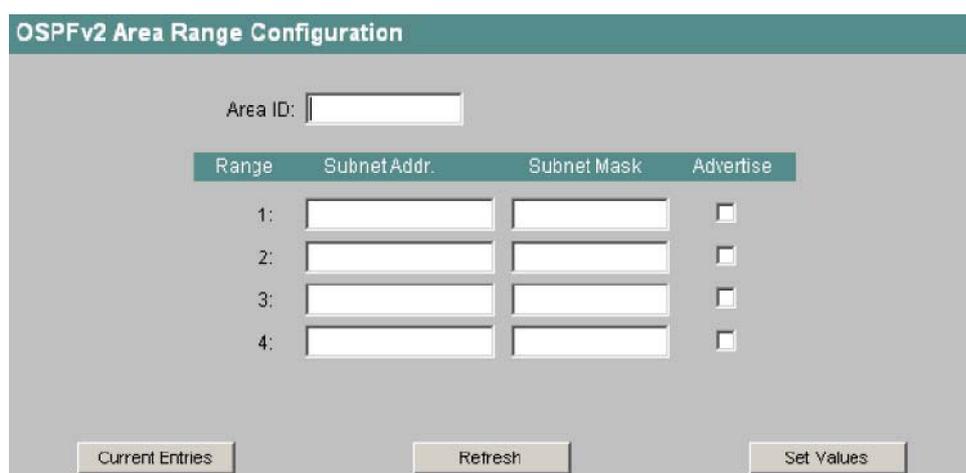


図 4-63 OSPFv2 Area Range Configuration の画面

Area ID

アドレス範囲を作成したいエリアの番号を入力します。

Subnet Addr.

グループ化するネットワークのアドレスを入力します。

Subnet Mask 欄

グループ化するネットワークのサブネットマスクを入力します。

Advertise チェックボックス

グループ化したネットワークを使用して送信するにはこのオプションをチェックします。

CLI のシンタックス

表 4-51 OSPFv2 Area Ranges : CLI¥ROUTER¥OSPF¥AREAS¥RANGES¥

コマンド	説明	備考
info	現在のエリア範囲を表示します。	
add <エリア ID> <サブネットアドレス> <サブネットマスク> [E/D]	新しいエリア範囲を追加します。 E/D=サマリ通知をオンまたはオフに設定 します。	管理者のみ。
edit <エリア ID> <サブネットアドレス> <サブネットマスク> <E/D>	エリア範囲の設定を変更します。	管理者のみ。
delete <エリア ID> <サブネットアドレス> <サブネットマスク>	エリア範囲を削除します。	管理者のみ。

4.6.9 OSPFv2 Interfaces メニュー

概要

このダイアログでは、OSPF について設定したすべての IP インタフェースをモニタできます。設定パラメータと統計値が 2 ページ構成で表示されます。

ページ間を移動するには「>>」または「<<」のボタンをクリックします。

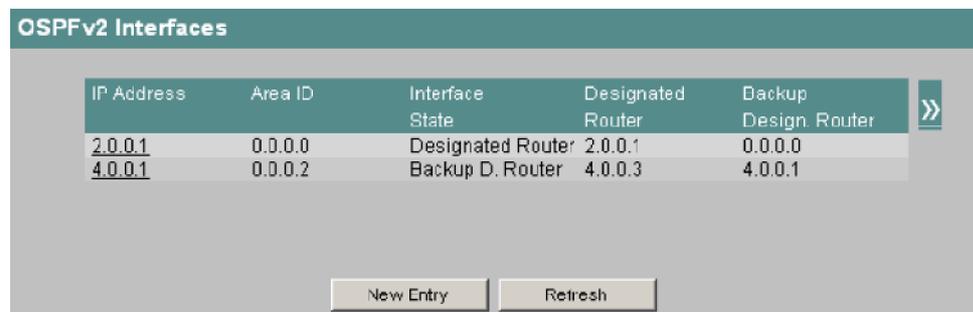


図 4-64 OSPFv2 Interfaces の画面

IP Address 欄

設定されている OSPF インタフェースの IP アドレスです。

Area ID 欄

そのインタフェースに対応するエリアを示します。

Interface State 欄

インタフェースの状態を示します。以下の状態があります。

- Down : インタフェースには何も接続されていません。
- Waiting : インタフェースの準備およびネゴシエーション中です。
- Designated Router : 当ルータがこのネットワークを主管し、ネットワーク LSA が作成されます。
- Backup D. Router : 当ルータは指定ルータの予備系です。
- Other : インタフェースは動作中であり、当ルータは指定ルータでも予備系指定ルータでもありません。

Designated Router 欄

そのインタフェースに対する指定ルータの IP アドレスです。

Backup Designated Router 欄

そのインタフェースに対する予備系指定ルータの IP アドレスです。

OSPFv2 Interfaces の 2 ページ目

IP Address	OSPF Status	Priority	Trans Delay	Retrans Interval	Hello Interval	Dead Interval	Authn. Type	Events
2.0.0.1	enabled	1	1	5	10	40	none	2
4.0.0.1	enabled	1	1	5	10	40	none	3

図 4-65 OSPFv2 Interfaces 画面の 2 ページ目

IP Address 欄

そのインタフェースの IP アドレスです。

OSPF Status 欄

そのインタフェースの OSPF ステータスです。以下の状態があります。

- enabled : そのインタフェースでは OSPF が可能です。
- disabled : そのインタフェースでは OSPF は使用できません。

Priority 欄

そのインタフェースにおける当ルータの優先度です。優先度は、ネットワークにおける指定ルータの選定において、ある一定の役割を果たします。値が大きいほど優先度は高くなります。

Trans Delay 欄

リンク状態更新パケットの転送に必要なると推定される秒数。LAN では通常「1」です。

Retrans Interval 欄

データベースの同期時に受信が確認されなかったパケットを再送するときの待機時間を示します。

Hello Interval 欄

Hello パケットの送出間隔を示します。

Dead Interval 欄

その期間中に Hello パケットを受信しなかったときに相手ルータを「存在しない」とみなす時間です。

Authent. Type 欄

そのインタフェースに対して選択されている認証方法です。以下のケースがあります。

- none : 認証なし
- simple : パスワードを用いた認証
- MD5 : Keyed MD5 を用いた認証

Events 欄

インタフェース状態が変化した回数。

新しい OSPFv2 インタフェースの作成

OSPFv2 Interfaces ダイアログの[New Entry]ボタンをクリックすると、OSPF について新しいインタフェースを設定できます。

付記

OSPF インタフェースを新たに作成するには、あらかじめそのインタフェースを IP サブネットとして作成しておく必要があります。

注

パラメータの選択には十分な注意を払ってください。正しい隣接関係を構築するには IP サブネット内の全ルータで同じパラメータを設定する必要があります。設定を誤ると、ルータが互いに見えない状態になります。

The screenshot shows a web interface titled "RIPv2 Interface Configuration". It contains several input fields and dropdown menus:

- IP Address: [text input]
- Send Updates: [RIPv1-Compat dropdown]
- Receive Updates: [RIPv1v2 dropdown]
- Default Metric: [text input]
- Authentication Type: [none dropdown]
- Key ID: [? text input]

 At the bottom of the form, there are three buttons: "Current Entries", "Refresh", and "Set Values".

図 4-66 OSPFv2 Interface Configuration の画面

IP Address

設定したいインタフェースの IP アドレスを入力します。

Area ID

そのインタフェースが属するエリアの番号を入力します。

Interface enabled チェックボックス

このインタフェースで OSPF トラフィックを扱いたい場合はこのオプションをチェックします。

Priority

ルータの優先度を入力します。この値が使われるのは指定ルータの選定時だけです。同じ IP サブネット内であってもルータごとに異なる選択を行えます。

Transit Delay

リンク状態更新パケットの送出時に見込まれる遅延を秒数で入力します。LAN では通常「1」を指定します。値の範囲は 1~3600 です。

Retransmission Interval

受領確認パケットを受信しなかったときにパケットを再送するまでの待機時間を秒数で入力します。LAN では通常「5」を指定します。

Hello Interval

Hello パケットの送出間隔を秒数で入力します。値の範囲は 1~65,535 です。

Router Dead Interval

その期間中に Hello パケットを受信しなかった場合に相手ルータを「障害」とみなす時間を秒数で入力します。

Authentication Type ドロップダウンリスト

そのインタフェースに対する認証方法を選択します。以下の選択肢があります。

- none : 認証なし
- simple : パスワードを用いた認証
- MD5 : Keyed MD5 を用いた認証

Key ID

付記

「Key ID」のテキストボックスは「MD5」の認証方法を指定した場合にのみ表示されます。その場合のみ、いくつかの鍵を使用できます。

パスワードを鍵に使用するときの鍵 ID を入力します。鍵 ID はプロトコルによって転送されるため、すべての隣接ルータにおいて同じ鍵を同じ鍵 ID で保存する必要があります。

Password/Confirmation

認証にパスワードを用いる場合には MD5 において鍵が必要であり、それをここに入力します。

CLI のシンタックス

表 4-52 OSPFv2 Interfaces : CLI¥ROUTER¥OSPF¥AREAS¥IFACE>

コマンド	説明	備考
info	現在のインタフェース設定を表示します。	
add <IP アドレス> <エリア ID> [EID] [優先度]	新しいインタフェースを追加します。 [EID]=インタフェースの有効・無効を設定します。	管理者のみ。
edit <IP アドレス> [エリア ID] [EID] [優先度]	インタフェースの設定を変更します。 [EID]=インタフェースの有効・無効を設定します。	管理者のみ。
timing <IP アドレス> [<パラメータ=値>]	インタフェースのタイマ設定を変更します。 可能な設定： • TD：転送遅延 • RI：再送タイマ • HI：Hello の間隔 • DI：障害判定タイマ	管理者のみ。
auth <IP アドレス> <認証タイプ> [パスワード]	インタフェースの認証設定を変更します。 可能なタイプ： • none • simple • MD5	管理者のみ。
delete <IP アドレス>	インタフェースを削除します。	管理者のみ。

4.6.10 OSPFv2 Virtual Links メニュー

概要

各エリア境界ルータ（複数のエリアに接続されるルータ）は、プロトコルに関係する理由によってバックボーンエリアにアクセスできることが必要です。エリア境界ルータがバックボーンエリアに直接つながっていない場合には、バックボーンエリアとの仮想リンクが生成されます。

このメニューではそうした仮想リンクのモニタを行えます。

Neighbor Router ID	Transit Area ID	Virt Link State	Trans Delay	Retrans Interval	Hello Interval	Dead Interval	Authent. Type	Events
3.0.0.2	0.0.0.2	down	1	5	10	60	none	0

図 4-67 OSPFv2 Virtual Links の画面

Neighbor Router ID 欄

設定されている隣接ルータのルータ ID。

Transit Area ID 欄

ルータが近隣ルータと仮想接続を行うエリアのエリア ID。

Virt. Link State 欄

仮想リンクの状態。以下の状態があります。

- down : 仮想リンクは使用できません。
- point-to-point : 仮想リンクは使用できます。

Trans Delay 欄

仮想リンクを使ったリンク状態更新パケットの転送に必要と推定される秒数。

Retrans Interval 欄

受信確認がなされなかったパケットを再送するときの待機時間（秒数）。

Hello Interval 欄

仮想リンクを使った Hello パケットの送出間隔（秒数）。

Dead Interval 欄

その期間中に Hello パケットを受信しなかったときに隣接ルータを「障害」とみなす時間（秒数）。

Authent. Type 欄

仮想リンクに対する認証方法です。以下のケースがあります。

- none : 認証なし
- simple : パスワードを用いた認証
- MD5 : Keyed MD5 を用いた認証

Events 欄

インタフェース状態が変化した回数。

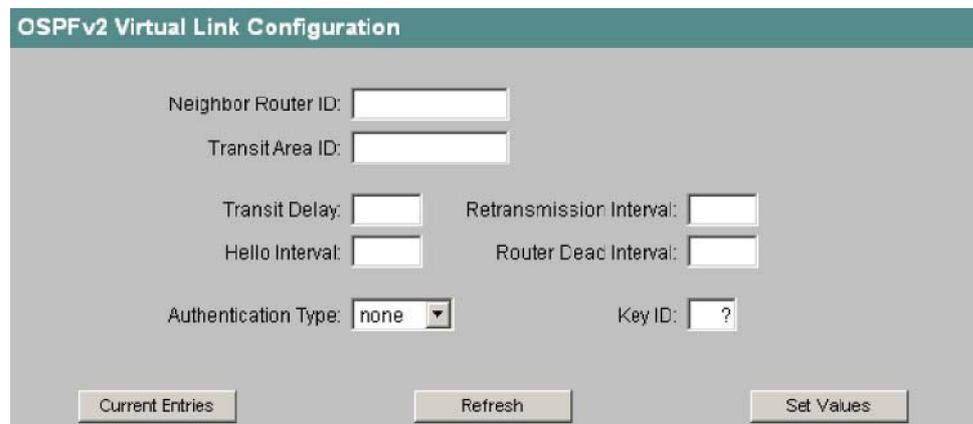
新しい仮想リンクの作成

OSPFv2 Virtual Links ダイアログの[New Entry]ボタンをクリックすると、新しい仮想リンクを作成できます。

付記

仮想リンクを作成するときには、通過エリアとバックボーンエリアの両方について設定されていることが必要です。

仮想リンクは両端で同じ設定にしてください。



The image shows a configuration window titled "OSPFv2 Virtual Link Configuration". It contains several input fields and buttons. The fields are: "Neighbor Router ID:" with a text box; "Transit Area ID:" with a text box; "Transit Delay:" with a text box; "Retransmission Interval:" with a text box; "Hello Interval:" with a text box; "Router Dead Interval:" with a text box; "Authentication Type:" with a dropdown menu showing "none"; and "Key ID:" with a text box containing a question mark. At the bottom, there are three buttons: "Current Entries", "Refresh", and "Set Values".

図 4-68 OSPFv2 Virtual Link Configuration の画面

Neighbor Router ID

仮想リンクの他端における相手装置のルータ ID を入力します。

Transit Area ID

対向する 2 台の装置の間に介在するエリアのエリア ID を入力します。

Transit Delay

リンク状態更新パケットの送出時に見込まれる遅延を秒数で入力します。値の範囲は 1~3600 です。

Retransmission Interval

受領確認パケットを受信しなかったときにパケットを再送するまでの待機時間を秒数で入力します。値の範囲は 1~3,600 です。

Hello Interval

Hello パケットの送出間隔を秒数で入力します。値の範囲は 1~65,535 です。

Router Dead Interval

その期間中に Hello パケットを受信しなかった場合に相手ルータを「障害」とみなす時間を秒数で入力します。

Authentication Type ドロップダウンリスト

そのインタフェースに対する認証方法を選択します。以下の選択肢があります。

- none : 認証なし
- simple : パスワードを用いた認証
- MD5 : Keyed MD5 を用いた認証

Key ID

付記

「Key ID」のテキストボックスは「MD5」の認証方法を指定した場合にのみ表示されます。その場合のみ、いくつかの鍵を使用できます。

パスワードを鍵に使用するときの鍵 ID を入力します。鍵 ID はプロトコルによって転送されるため、すべての隣接ルータにおいて同じ鍵を同じ鍵 ID で保存する必要があります。

Password/Confirmation

認証にパスワードを用いる場合には MD5 において鍵が必要であり、それをここに入力します。

CLI のシンタックス

表 4-53 OSPFv2 Virtual Links : CLI%ROUTER%OSPF%AREAS%VLINKS>

コマンド	説明	備考
info	仮想リンクの現在の設定を表示します。	
add <ルータ ID> <エリア ID> [<パラメータ=値>]	新しい仮想リンクを追加します。 可能な設定 : • TD : 転送遅延 • RI : 再送タイマ • HI : Hello の間隔 • DI : 障害判定タイマ	管理者のみ。
edit <ルータ ID> <エリア ID> [<パラメータ=値>]	仮想リンクの設定を変更します。 可能な設定 : • TD : 転送遅延 • RI : 再送タイマ • HI : Hello の間隔 • DI : 障害判定タイマ	管理者のみ。
auth <ルータ ID> <エリア ID> <認証タイプ> [パスワード]	仮想リンクの認証設定を変更します。 可能なタイプ : • none • simple • MD5	管理者のみ。
delete <ルータ ID> <エリア ID>	仮想リンクを削除します。	管理者のみ。

4.6.11 OSPFv2 Neighbors メニュー

概要

このダイアログでは OSPF の隣接ルータ（ネイバ）をモニタできます。これには関連ネットワーク内で動的に検知されるネイバのほか、設定による仮想ネイバも含まれます。

Current OSPFv2 Neighbors								
Neighbor IP Address	Neighbor Router ID	Neighbor State	Transit Area ID	Assoc. Area Type	Priority	Hello Suppr.	Retrans Queue	Events
4.0.0.3	3.0.0.3	full	-	Normal	1	no	0	6
3.0.0.2	3.0.0.2	down	0.0.0.2	-	-	no	0	0

Refresh

図 4-69 OSPFv2 Neighbors の画面

Neighbor IP Address 欄

そのネットワーク内にある隣接ルータ（ネイバ）の IP アドレス。

Neighbor Router ID 欄

ネイバのルータ ID。両アドレスが同じでもかまいません。

Neighbor State 欄

ネイバの状態です。以下の状態があります。

- down : ネイバに到達できません。
- attempt and init : 初期化中の一時的状態。
- two-way : Hello パケットの双方向受信。
- exchange start, exchange and loading : リンク状態データベースの情報交換中。
- full : データベースが同期化されている状態。

付記

2 台の対向装置の片方が指定ルータまたは待機系指定ルータの場合には、「full」の状態が安定ネイバとしての正常状態です。それ以外では「two-way」の状態が正常な安定状態です。

Transit Area ID 欄

ネイバの通過エリア ID（ネイバが仮想である場合）。

Assoc. Area Type 欄

ネイバ間の関係が維持される土台となるエリアタイプ。以下のエリアタイプがあります。

- Standard
- Stub
- NSSA

Priority 欄

ネイバのルータ優先度。これが重要になるのはネットワークの指定ルータを選定する場合だけです。仮想ネイバの場合、この情報は意味がありません。

Hello Suppr.欄

ネイバに対して Hello パケットが抑止されているかどうかを示します。通常は「no」です。

Retrans Queue 欄

未送パケットに関するキューの長さ。

Events 欄

状態変化の回数。

付記

2 台の対向装置の片方が指定ルータまたは待機系指定ルータの場合には、「full」の状態が安定ネイバとしての正常状態です。それ以外では「two-way」の状態が正常な安定状態です。

Transit Area ID 欄

ネイバの通過エリア ID (ネイバが仮想である場合)。

Assoc. Area Type 欄

ネイバ間の関係が維持される土台となるエリアタイプ。以下のエリアタイプがあります。

- Normal
- Stub
- NSSA

Priority 欄

ネイバのルータ優先度。これが重要になるのはネットワークの指定ルータを選定する場合だけです。仮想ネイバの場合、この情報は意味がありません。

Hello Suppr.欄

ネイバに対して Hello パケットが抑止されているかどうかを示します。通常は「no」です。

Retrans Queue 欄

未送パケットに関するキューの長さ。

Events 欄

状態変化の回数。

CLI のシンタックス

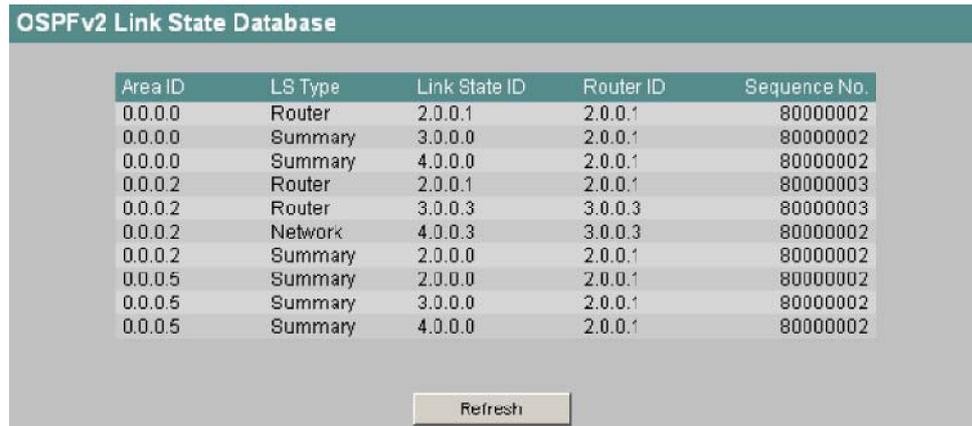
表 4-54 OSPFv2 Neighbors : CLI¥ROUTER¥OSPF>

コマンド	説明	備考
info	隣接ルータ (ネイバ) の現在の状態を表示します。	

4.6.12 OSPFv2 Link State Database メニュー

概要

リンク状態データベース (LSDB) は、エリア内の全リンクを管理するための一括データベースです。その内容は LSA (リンク状態通知情報) です。LSA のなかでとくに重要なデータがこのダイアログに表示されます。



Area ID	LS Type	Link State ID	Router ID	Sequence No.
0.0.0.0	Router	2.0.0.1	2.0.0.1	80000002
0.0.0.0	Summary	3.0.0.0	2.0.0.1	80000002
0.0.0.0	Summary	4.0.0.0	2.0.0.1	80000002
0.0.0.2	Router	2.0.0.1	2.0.0.1	80000003
0.0.0.2	Router	3.0.0.3	3.0.0.3	80000003
0.0.0.2	Network	4.0.0.3	3.0.0.3	80000002
0.0.0.2	Summary	2.0.0.0	2.0.0.1	80000002
0.0.0.5	Summary	2.0.0.0	2.0.0.1	80000002
0.0.0.5	Summary	3.0.0.0	2.0.0.1	80000002
0.0.0.5	Summary	4.0.0.0	2.0.0.1	80000002

Refresh

図 4-70 OSPFv2 Link State Database の画面

Area ID 欄

その LSA (リンク状態通知情報) が属するエリアの ID。

LS Type 欄

LSA の種類です。以下のものがあります。

- Router
- Network
- Summary
- ASBR (自律システム境界ルータ)

Link State ID 欄

その LSA を表す一意の ID。

Router ID 欄

その LSA を生成したルータの ID。

Sequence No. 欄

LSA のシーケンス番号です。LSA が更新されるたびにシーケンス番号は 1 ずつ増えます。

CLI のシンタックス

表 4-55 OSPFv2 Link State Database : CLI#ROUTER#OSPF>

コマンド	説明	備考
Inkstate	リンク状態データベースの現在の内容を表示します。	

4.7 Port Status メニュー

ポート設定の表示

[Ports]フォルダのアイコンをクリックすると Port Status 画面が開きます。

この画面では、データ転送に関する設定が SCALANCE X-400 の全ポート（エクステンダ実装時はそのポートも含まれます）について表示されます。

Port	Type	Mode	Negotiation	Flow Ctrl.	Status	Link	Lock
5.1	TP 1000 T	10M HD	enabled	disabled	enabled	down	disabled
5.2	TP 1000 T	10M HD	enabled	disabled	enabled	down	disabled
9.1	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
9.2	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
9.3	TP 100 TX	100M HD	enabled	disabled	enabled	up	disabled
9.4	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
10.1	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
10.2	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
10.3	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
10.4	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
11.1	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
11.2	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
11.3	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled
11.4	TP 100 TX	10M HD	enabled	disabled	enabled	down	disabled

Refresh

図 4-71 Port Status の画面

テーブルには 8 つの欄があり、それぞれに以下の情報が示されます。

Port

表示内容に対応するスロット番号とポート番号を示します。

Type

ポート種別を示します。スロットによっては複数種類のモジュールやポートを使用できるため、この情報は重要です。以下のポート種別があります。

- TP 1000 TX
- TP 100 TX
- FO 1000 SX
- FO 1000 LX
- FO 100 FX
- FO 100 FX LD

Mode

伝送速度（10/100/1000Mbps）と伝送モード（全二重/FD または半二重/HD）。

Negotiation

オートネゴシエーション機能のオン・オフを示します。

Flow Ctrl.

フロー制御の有無を示します。

Status

ポートが使用可能状態かどうかを示します。データトラフィックが流れるのは使用可能（enabled）のポートのみです。

Link

ネットワークとのリンクの状態を示します。以下の場合があります。

- up
そのポートではネットワークとのリンクが確立し、リンクインテグリティ（リンク正常性）信号を受信しています。
- down
リンクが落ちています。原因には、たとえば接続先装置の電源オフなどがあります。

Lock

ポートロックの有無を示します。以下の状態があります。

- enabled
送信元アドレスが SCALANCE X-400 のアドレステーブルに存在しないフレームは廃棄されます。SCALANCE X-400 は対応するノードの送信元アドレスをアドレステーブルに書き込むことはしません。
- disabled（デフォルト）
送信元アドレスが SCALANCE X-400 のアドレステーブルに存在しないフレームでも転送されます。また、SCALANCE X-400 は対応するノードの送信元アドレスをアドレステーブルに書き込みます。

ポート設定の変更

Port 欄のポート名をクリックすると Port Configuration ページが開きます。そのポートにおけるデータ転送の処理方法を指定できます。

付記

光ポートは全二重モードかつ最大伝送速度でのみ動作します。そのため光ポートでは以下の設定は行えません。

- オートネゴシエーション
- 伝送速度
- 伝送モード

図 4-72 Port Configuration の画面

Port

設定を表示したいスロット番号とポート番号を指定します。

Port enabled チェックボックス

このポートでデータトラフィックを扱うにはこのボックスをチェックします。

Lock enabled チェックボックス

このボックスをチェックすると、SCALANCE X-400 はこのポートにおいてユニキャストアドレスの学習を行いません。

FD Flow Control enabled チェックボックス

全二重モードに関するフロー制御を有効または無効にします。ただしフロー制御が機能するのは、ポートが全二重モードで動作するときに限られます。フロー制御を有効にしたのに機能しない場合は、画面を再表示 (Refresh) したときにチェックマークが消えます。フロー制御が機能できる環境になる場合、再設定の必要はありません。

HD Flow Control enabled チェックボックス

半二重モードに関するフロー制御を有効または無効にします。ただしフロー制御が機能するのは、ポートが半二重モードで動作するときに限られます。

付記

SCALANCE X-400 では、ポートが過負荷になった場合に、いくつかの自動機能によって他のポートや高優先クラス (QoS) への影響を軽減もしくは回避します。言い換えると、たとえフロー制御をオンにしてもフレームが廃棄されるケースがあります。

スイッチが送信可能なフレーム数よりも多くのフレームを受信すると、ポートの過負荷が発生します。このような現象は、たとえば伝送速度の違いなどによって起こります。

Auto Negotiation enabled チェックボックス

ポートのオートネゴシエーションをオンまたはオフにします。これをチェックしない (オートネゴシエーションをオフにする) 場合、Mode のリストボックスにおいてポートの伝送速度と全二重・半二重の設定を行えます。これをチェックすると、それらのパラメータは末端ノードを接続した SCALANCE X-400 によって自動的にネゴシエート (調整) されます。

付記

対向ポートにオートクロス機能を使用したい場合はオートネゴシエーションをオフにしないでください。

Port Name

ここにポートの名前を入力できます。

Port Type

ポート種別がここに表示されます。値はハードウェアによって決まっているため変更できません。

Ports ボタン

全ポートのテーブルに戻ります。

CLI のシンタックス

表 4-56 Port Status : CLI#PORT>

コマンド	説明	備考
info [ポート番号]	データトラフィックに関する現在のポート設定（実際の状態）を表示します。	
cfg [ポート番号]	データトラフィックについて設定されているポート設定（望ましい状態）を表示します。	
status <E D> [ポート番号]	指定ポートにおけるデータトラフィックの処理を可能または不可にします。	管理者のみ。
fd_flow <E D> [ポート番号]	全二重モードでのフロー制御をオンまたはオフにします。	管理者のみ。
hd_flow <E D> [ポート番号]	半二重モードでのフロー制御をオンまたはオフにします。	管理者のみ。
autoneg <E D> [ポート番号]	オートネゴシエーションをオンまたはオフにします。	管理者のみ。
name <ポート番号> <名前>	指定のポートに名前（64 文字以内）を付与します。	管理者のみ。
speed <10H 10F 100H 100F 1000F ?> [ポート番号]	ポートに伝送速度を割り当てます。 10H : 10Mbps・半二重 10F : 10Mbps・全二重 100H : 100Mbps・半二重 100F : 100Mbps・全二重 1000F : 1000Mbps・全二重 パラメータに疑問符を入力すると設定値が表示されます。	管理者のみ。

4.8 統計メニュー

受信フレームの計数と評価

SCALANCE X-400 は内部統計カウンタ（RMON: Remote Monitoring カウンタ）を備えており、各ポートの受信フレーム数を以下の基準でカウントしています。

- フレーム長
- フレーム種別
- 不良フレーム

この情報を見れば、データトラフィックの概要とネットワーク上の問題について知ることができます。

CLI のシンタックス

表 4-57 Statistics : CLI#PORT>

コマンド	説明	備考
stat <S T E clear> [ポート番号]	受信フレーム数を以下の基準でソートして表示します。 S : フレーム長 T : フレーム種別 E : 不良フレーム clear を指定するとカウンタがリセットされます。	複数ポートの指定が可能です。 例： stat S 5.1 6.1-7.2 というコマンドを入力すると、ポート 5.1 および 6.1~7.2 で受信したフレームの長さを表示します。

4.8.1 Packet Size Statistic メニュー

パケット長ごとの受信フレーム数

Packet Size Statistic ページには各ポートで受信されたパケット数がサイズ別に示されます。

[Reset Counters] ボタンをクリックすると全ポートのカウンタがリセットされます。

Packet Size Statistic						
Port	64	65-127	128-255	256-511	512-1023	1024-1518
5.1	0	0	0	0	0	0
5.2	0	0	0	0	0	0
6.1	0	0	0	0	0	0
6.2	0	0	0	0	0	0
7.1	0	0	0	0	0	0
7.2	0	0	0	0	0	0
9.1	1547	586	8	6009	3036	135
9.2	1114	403	4	5	0	0
9.3	25	45	0	24	12	0
9.4	85	66	0	104	53	21
10.1	11	43	0	0	0	0
10.2	115	84	0	55	39	39
10.3	8	24	0	0	0	0
10.4	152	81	1	39	29	40
11.1	37	71	0	1	0	0
11.2	309	185	0	199	115	72
11.3	357	143	0	133	93	86
11.4	2454	717	23	3548	1857	449
12.1	0	0	0	0	0	0
12.2	0	0	0	0	0	0
13.1	0	0	0	0	0	0
13.2	0	0	0	0	0	0
14.1	0	0	0	0	0	0
14.2	0	0	0	0	0	0
15.1	0	0	0	0	0	0
15.2	0	0	0	0	0	0

Refresh Reset Counters

図 4-73 Packet Size Statistic の画面

Port 欄の数字をクリックすると、そのポートに対するパケットサイズ統計量のグラフ (Packet Size Statistics Graphic) が表示されます。調整可能なグラフを使ってカウント値が表示されます。

統計量のグラフ表示

このページでは各ポートの受信フレーム数がグラフ形式で表示されます。表示はフレーム長に基づき、以下の範囲ごとに棒グラフで示されます。

- 64 バイト
- 65~127 バイト
- 128~255 バイト
- 256~511 バイト
- 512~1023 バイト
- 1024~1518 バイト

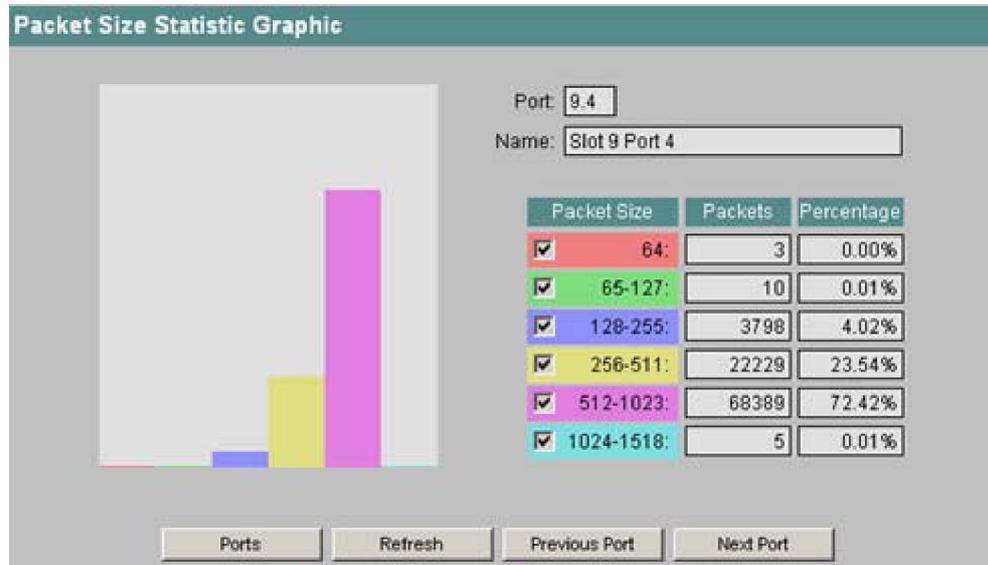


図 4-74 Packet Size Statistic Graphic の画面

Packet Size 欄のチェックボックスを使えばグラフの表示内容を指定できます。範囲のチェックボックスを選択すると、その範囲に対応する Packets 欄の値だけがグラフに表示されます。Percentage 欄には、対応する長さの packets がそのポートの全 packets 数において占めるパーセンテージが示されます。パーセンテージの計算においてはチェックした長さのみが考慮されます。

[Previous Port] ボタンと [Next Port] ボタンを使えば前後のポートに移動できます。

4.8.2 Packet Type Statistic メニュー

パケットタイプごとの受信フレーム数

Packet Type Statistic ページには各ポートで受信されたユニキャスト、マルチキャスト、ブロードキャストの packets 数が示されます。

[Reset Counters] ボタンをクリックすると全ポートのカウンタがリセットされます。

Port	Unicast	Multicast	Broadcast
5.1	0	0	0
5.2	0	0	0
6.1	0	0	0
6.2	0	0	0
7.1	0	0	0
7.2	0	0	0
9.1	10261	1148	94
9.2	328	1126	92
9.3	81	24	1
9.4	306	22	1
10.1	43	10	1
10.2	323	8	1
10.3	24	8	0
10.4	333	8	1
11.1	69	34	6
11.2	835	38	7
11.3	788	23	1
11.4	8372	608	68
12.1	0	0	0
12.2	0	0	0
13.1	0	0	0
13.2	0	0	0
14.1	0	0	0
14.2	0	0	0
15.1	0	0	0
15.2	0	0	0

Refresh Reset Counters

図 4-75 Packet Type Statistic の画面

Port 欄の数字をクリックすると、そのポートに対するパケットタイプ統計量のグラフ (Packet Type Statistic Graphic) が表示されます。調整可能なグラフを使ってカウント値が表示されます。

統計量のグラフ表示

このページでは各ポートの受信フレーム数がグラフ形式で表示されます。表示はフレームタイプに基づき、以下の範囲ごとに棒グラフで示されます。

- Unicast
- Multicast
- Broadcast

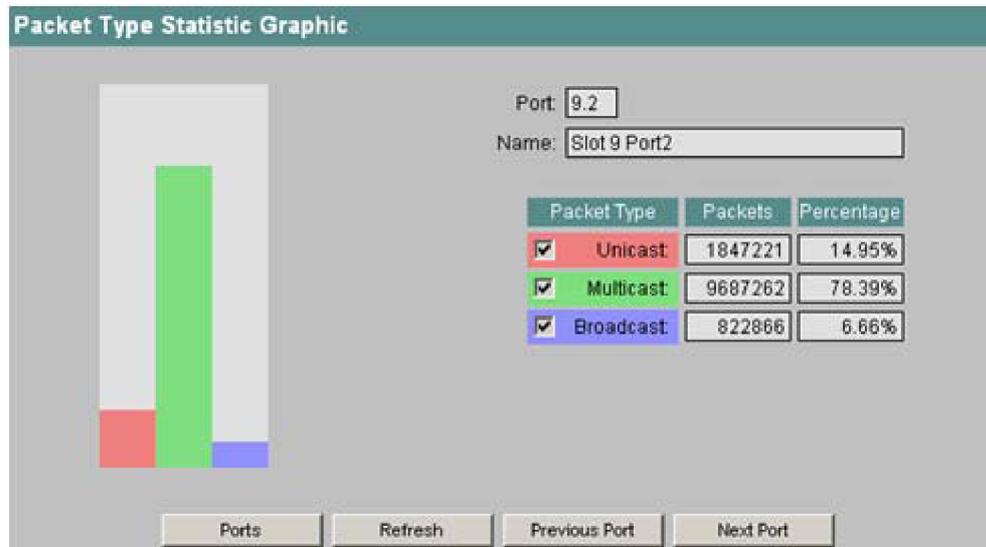


図 4-76 Packet Type Statistic Graphic の画面

Packet Type 欄のチェックボックスを使えばグラフの表示内容を指定できます。パケットタイプのチェックボックスを選択すると、それに対応する *Packets* 欄の値だけがグラフに表示されます。*Percentage* 欄には、対応するパケットタイプのパケットがそのポートの全パケット数において占めるパーセンテージが示されます。パーセンテージの計算においてはチェックしたパケットタイプのみが考慮されます。

[Previous Port]ボタンと[Next Port]ボタンを使えば前後のポートに移動できます。

4.8.3 Error Statistic メニュー

受信パケットにおけるエラー数

Packet Error Statistic ページには各ポートで受信した不良フレーム数が表示されます。以下のエラータイプが区別されます。

- CRC
CRC のチェックサムが不一致のパケット
- Undersize
長さが 64 バイト未満のパケット
- Oversize
長さが 1518 バイト (VLAN タグ付きフレームの場合は 1522 バイト) を超えるパケット
- Fragments
長さが 64 バイト未満かつ CRC のチェックサムが不一致のパケット
- Jabbers
長さが 1518 バイト (VLAN タグ付きフレームの場合は 1522 バイト) を超え、かつ CRC のチェックサムが不一致のパケット
- Collisions
衝突の検出

[Reset Counters]ボタンをクリックすると全ポートのカウンタがリセットされます。

Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
5.1	0	0	0	0	0	0
5.2	0	0	0	0	0	0
6.1	0	0	0	0	0	0
6.2	0	0	0	0	0	0
7.1	0	0	0	0	0	0
7.2	0	0	0	0	0	0
9.1	0	0	0	0	0	0
9.2	0	0	0	0	0	0
9.3	0	0	0	0	0	0
9.4	0	0	0	0	0	0
10.1	0	0	0	0	0	0
10.2	1	0	0	0	0	0
10.3	0	0	0	0	0	0
10.4	0	0	0	0	0	0
11.1	0	0	0	0	0	0
11.2	0	0	0	0	0	0
11.3	0	0	0	0	0	0
11.4	0	0	0	0	0	0
12.1	0	0	0	0	0	0
12.2	0	0	0	0	0	0
13.1	0	0	0	0	0	0
13.2	0	0	0	0	0	0
14.1	0	0	0	0	0	0
14.2	0	0	0	0	0	0
15.1	0	0	0	0	0	0
15.2	0	0	0	0	0	0

Refresh Reset Counters

図 4-77 Packet Error Statistic の画面

Port 欄の数字をクリックすると、そのポートに対するパケットエラー統計量のグラフ (Packet Error Statistic Graphic) が表示されます。調整可能なグラフを使ってカウント値が表示されます。

統計量のグラフ表示

このページでは不良フレーム数がグラフ形式で表示されます。表示はエラー要因に基づき、以下のエラー要因ごとに棒グラフで示されます。

- CRC
- Undersize
- Oversize
- Jabbers
- Collisions

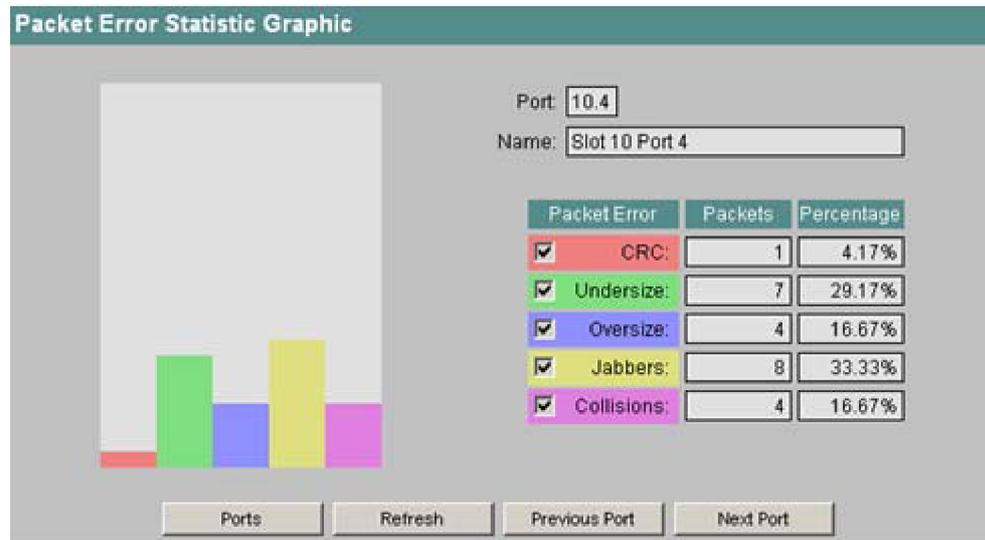


図 4-78 Packet Error Statistic Graphic の画面

Packet Error 欄のチェックボックスを使えばグラフの表示内容を指定できます。エラータイプのチェックボックスを選択すると、それに対応する *Packets* 欄の値だけがグラフに表示されます。*Percentage* 欄には、対応するエラータイプのパケットがそのポートの全パケット数において占めるパーセンテージが示されます。パーセンテージの計算においてはチェックしたエラータイプのみが考慮されます。

[Previous Port]ボタンと[Next Port]ボタンを使えば前後のポートに移動できます。

SNMP を用いた設定と診断

SNMP を用いた SCALANCE X-400 の設定

ネットワーク管理端末は、SCALANCE X-400 のような SNMP 対応ノードの設定および監視を SNMP (Simple Network Management Protocol) によって行うことができます。これを実行するためにノードには SNMP エージェントが実装されており、これによってノードは管理端末との間で GET/SET リクエストを使ったデータ交換を行います。SCALANCE X-400 は SNMPv1、SNMPv2、SNMPv3 をサポートします。

設定データは SCALANCE X-400 のなかの MIB (Management Information Base) と呼ばれるデータベースに格納されており、管理端末やウェブ型管理ツールを使ってアクセスします。

SIMATIC NET の SNMP OPC サーバ

SNMP OPC サーバは、SNMP のデータを IOPC インタフェースにおいて TCP/IP ネットワークから SNMP を用いて入手することを可能にします。SNMP OPC サーバを用いれば、SNMP 対応機器の診断・設定データが OPC クライアントシステム (WinCC など) からアクセスできます。

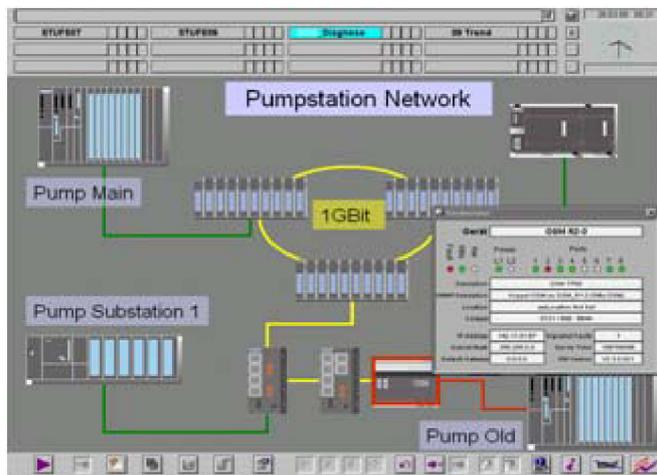


図 5-1 SIMATIC NET の SNMP OPC サーバを用いて実現される WinCC のネットワーク診断の例

SNMP に非対応の機器も、IP アドレスを使用することによってプラント見取図に表示させることができます。それによって、たとえば単純な装置診断を行えるだけでなく、TCP/IP ネットワーク全体の冗長ネットワーク構成やネットワーク負荷分散などの詳しい情報を表示できます。さらにこのデータをモニタすれば装置障害が早期に検出・局所化できます。このように運転の安全性やプラントの稼働率が向上します。監視対象装置の設定は STEP 7 (NCM PC も使用可能) を使って SNMP OPC サーバで行います。

SIMATIC NET の SNMP OPC サーバについては下記のページに詳しい記述があります。

<http://www.siemens.com/snmp-opc-server>

SNMP OPC の MIB コンパイラとプロファイル

SNMP OPC サーバを使って装置から監視できる情報は装置プロファイルによって決まります。付属の MIB コンパイラを使えば既存のプロファイルを修正できるほか、SNMP 対応装置について新しい装置プロファイルを作成できます。

SNMP OPC サーバの MIB コンパイラを使うには SMiv1 標準に準拠した MIB ファイルが必要です。そのため SCALANCE X-400 については修正版の SMiv2 プライベート MIB ファイルが必要になります。SCALANCE X-400 の SMiv1 MIB ファイルと既製の装置プロファイルは用意されており、以下の場所からダウンロードできます。

<http://support.automation.siemens.com/WWW/view/en/22015045>

標準 MIB

MIB は、RFC に規定される標準的な MIB とプライベート MIB とに分かれます。プライベート MIB には標準 MIB がない製品独自の拡張定義が含まれます。

SCALANCE X-400 は以下の MIB をサポートします。

- RFC 1213 : MIB II (egp と transmission を除くすべてのグループ)
- RFC 2233 : Interface MIB (グループ 4、5、6、7、10、11、13)
- RFC 1286、RFC 1493 : Bridge MIB (dot1dBase と dot1dStp)
- RFC 1724 : RIP Version 2 MIB Extension (SCALANCE X414-3E)
- RFC 1757 : RMON MIB (statistics、history、alarm、event)
- RFC 1850 : OSPF Version 2 Management Information Base (SCALANCE X414-3E)
- RFC 2665 : Ethernet-Like MIB (dot3StatsTable : SMiv2 向け)
- RFC 2674p : P BRIDGE MIB (グループ 1、2、3、4、6、8、9)
- RFC 2674q : Q BRIDGE MIB (グループ 1、3、4、6、7、8、5 の一部)
- RFC 1907 : SNMPv2 MIB (グループ 5、6、7、8、9)
- RFC 2571 : SNMP FRAMEWORK MIB (SNMPv3 MIB : グループ 1)
- RFC 2572 : SNMP MPD MIB (SNMPv3 MIB : グループ 1)
- RFC 2573 : SNMP NOTIFICATION MIB
(SNMPv3 MIB : グループ 1、2)
- RFC 2573 : SNMP PROXY MIB
- RFC 2573 : SNMP TARGET MIB (SNMPv3 MIB : グループ 1、2、3)
- RFC 2574 : SNMP USER-BASED SM MIB
(SNMPv3 MIB : グループ 1)
- RFC 2575 : SNMP VIEW-BASED ACM MIB
(SNMPv3 MIB : グループ 1)

プライベート MIB

SCALANCE X-400 のプライベート MIB については本書の付録 B をご覧ください。

SCALANCE X-400 のプライベート MIB ファイルへのアクセス

SCALANCE X-400 のプライベート MIB ファイルは下記の手順で表示できます。

1. ウェブブラウザ (Internet Explorer など) を立ち上げて下記の URL を入力します。入力時には大文字と小文字の違いに注意してください。
`http://<SCALANCE X-400 の IP アドレス>/snScalanceX400.mib`
2. ログインが済んでいない場合にはログインウィンドウが開きます。ログインすると装置のプライベート MIB ファイルにアクセスできます。
3. Internet Explorer の場合、メニューで[表示] > [ソース]を選択します。それ以外のブラウザではそれに対応するメニューを選択してソースコードを開きます。Internet Explorer をデフォルト設定のまま使用している場合、プライベート MIB ファイルは Notepad で開かれ、テキストファイルとして保存できます。プライベート MIB ファイルには各オブジェクトの説明も入っています。

PROFINET IO の機能

6.1 PROFINET IO の使用

PROFINET IO の使用

接続した SCALANCE X-400 の診断、パラメータ割り当て、アラームメッセージ生成は、PROFINET IO を用いて行うこともできます。

この章では、接続した SCALANCE X-400 スイッチに対して PROFINET IO オプションを使用する方法について説明します。

以下の例では、PNIO コントローラ V2 が PROFINET IO チェーンによって設定済みであることを前提にしています (PROFINET IO システムマニュアルもご覧ください)。

付記

STEP 7 (V5.4 SP1) が必要です。

PROFINET IO チェーンを用いたハードウェア設定の例を図 6-1 に示します。

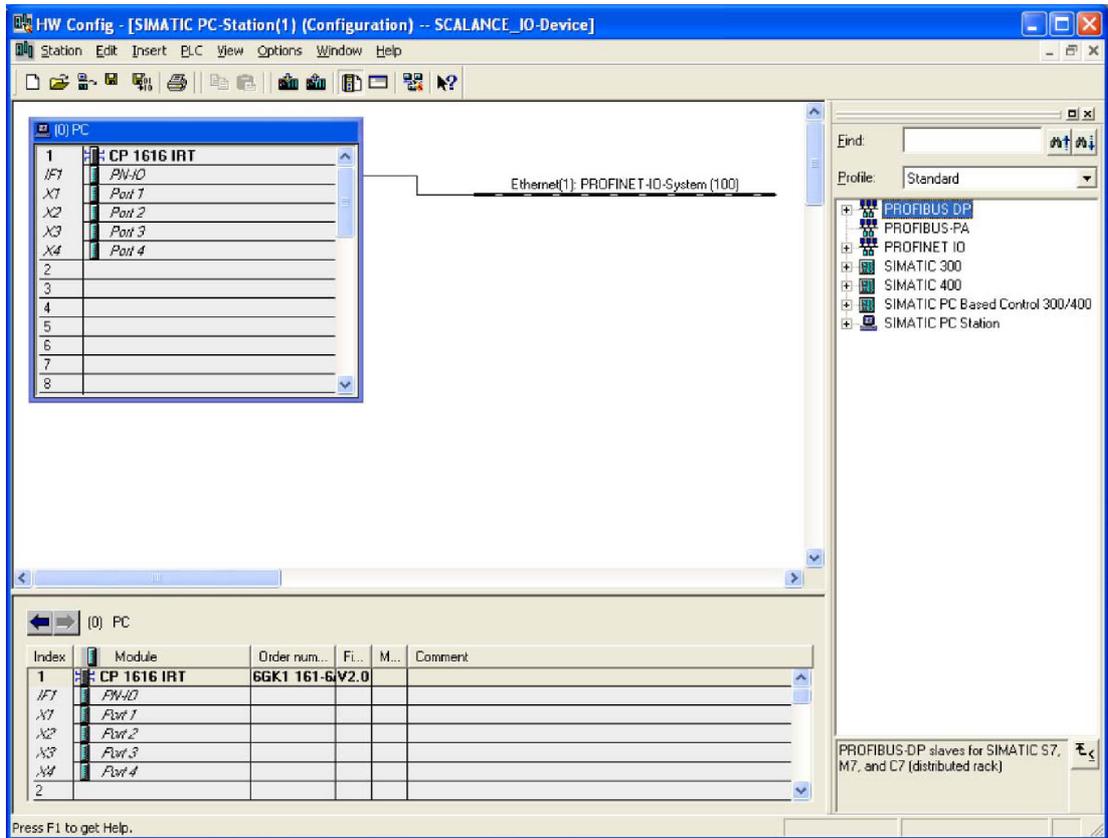


図 6-1 PROFINET IO による端末のハードウェア設定

SCALANCE X-400 の追加

個々のスイッチを PROFINET IO 機器とするには、PROFINET IO 配下のモジュールリストに SCALANCE X-400 シリーズの装置が入っていることが必要です。

SCALANCE X-400 シリーズの装置をモジュールリストに初めて追加するには、下記の手順に従ってください。

手順

1. ダイアログで[HW Config]を選択し、Options の[Install GSD files]を選ぶと、次のような画面が開きます。

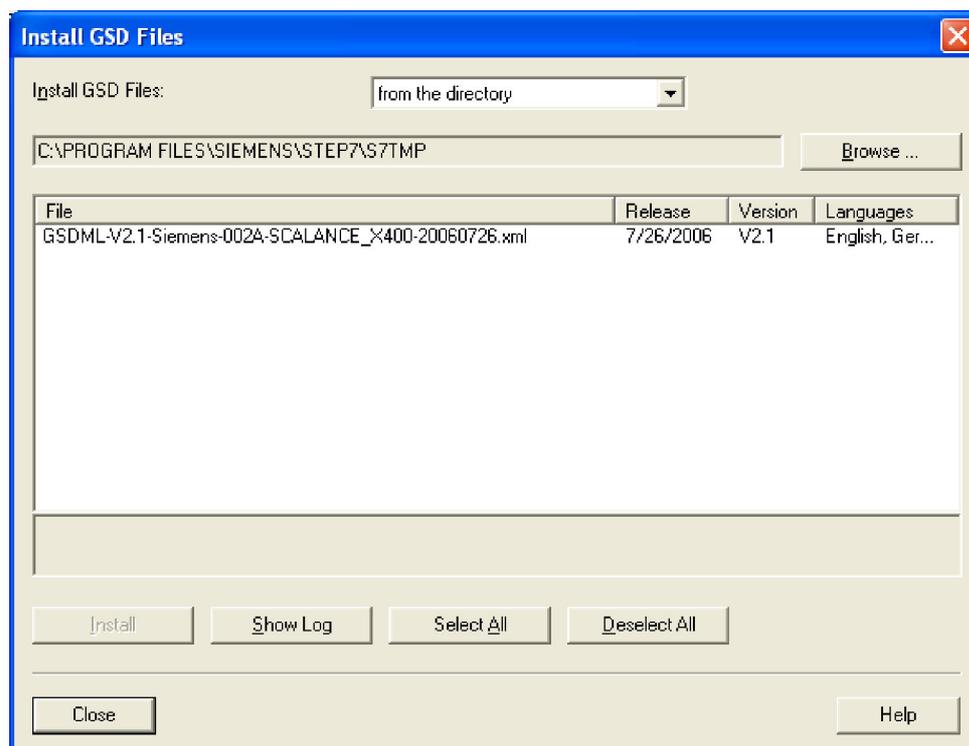


図 6-2 Install GSD Files の画面

2. Browse 機能を使って使用する xml ファイルの場所を探します
(たとえば GSDML-V2.1-Siemens-002A-SCALANCE_X400-YYYYMMDD.xml。左記の Y、M、D は
ファイル発行日です)。
3. [Install] ボタンを使ってそれを確定します。
SCALANCE X-400 シリーズの装置がモジュールリストに入ります(次図のモジュールリスト参照)。
4. 必要な SCALANCE X-400 をハードウェアリストから選択します。たとえば SCALANCE X408-2 で
あれば、[PROFINET IO] > [Network Components] > [SCALANCE X-400 Switches] > [SCALANCE
X408-2]となります。それを PROFINET IO システムにドラッグします。

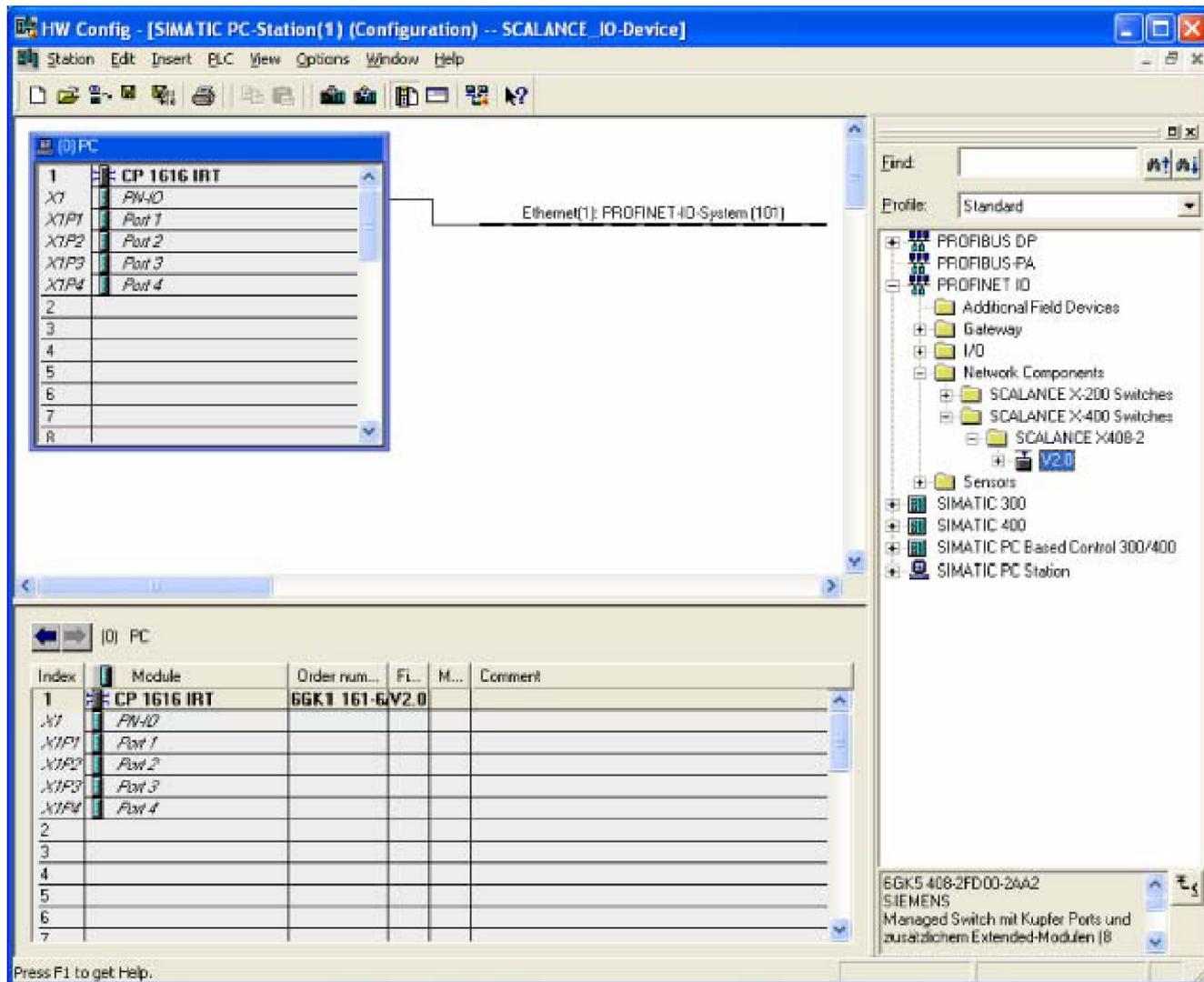


図 6-3 HW Config 2 : PROFINET IO SCALANCE スイッチの追加

5. [(1) SCALANCE]アイコンをクリックすると画面下部に SCALANCE のスロットが表示されます。Slot=0 をダブルクリックすると、次図に示すように SCALANCE (置換モジュール) のグローバルパラメータを設定できます。
6. スロット 2 と 3 のモジュールに対応するパラメータを設定できます。
7. ポートのスロットをクリックしてパラメータを設定します。

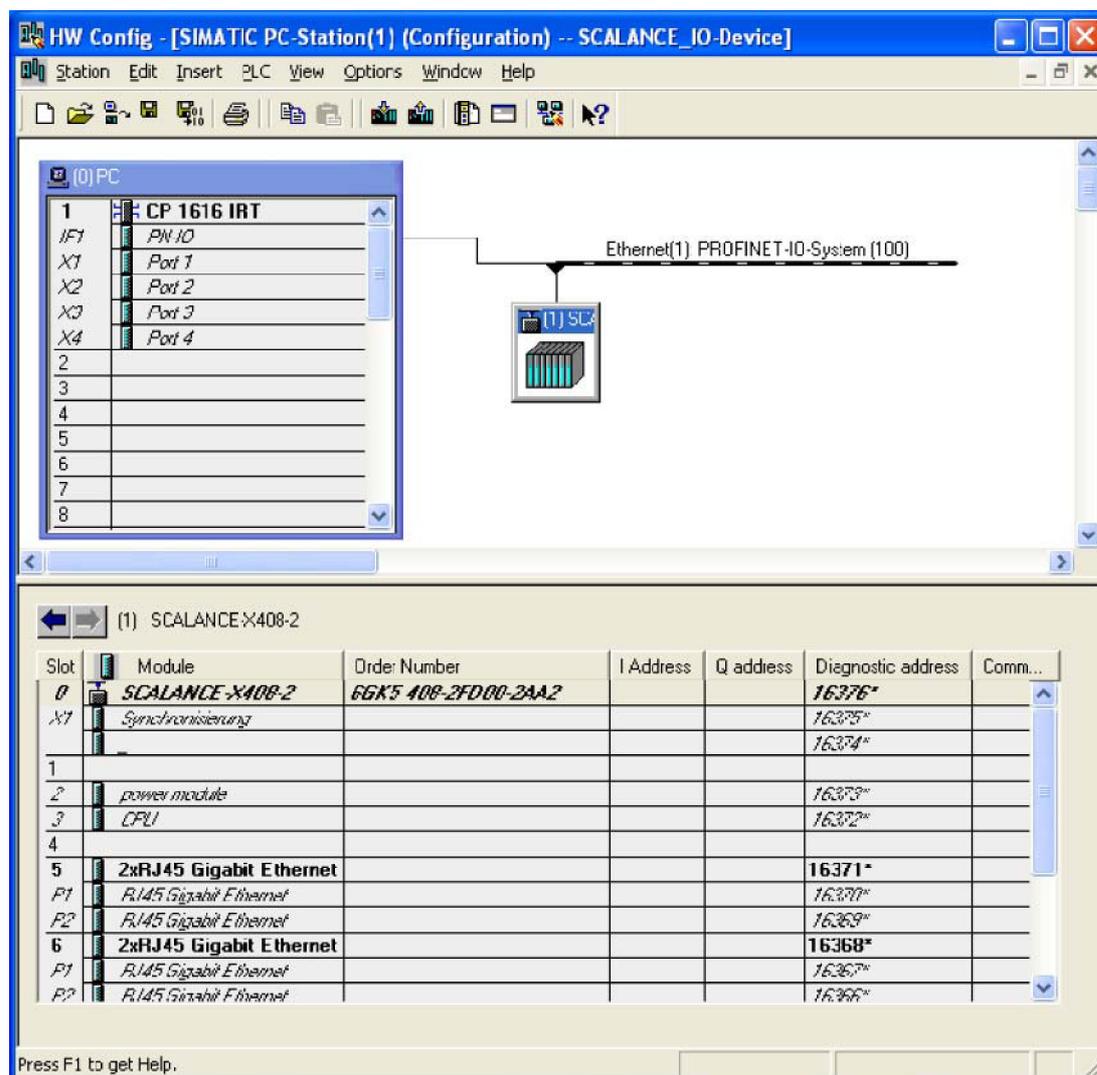


図 6-4 HW Config : PROFINET IO に関するグローバルパラメータの設定

- HW Config において SCALANCE X408-2 の Object Properties ダイアログを開きます（アイコンを右クリックして[Object Properties]を選択します）。PROFINET IO 装置の名前を入力し、[OK]をクリックすると、ダイアログが閉じます。

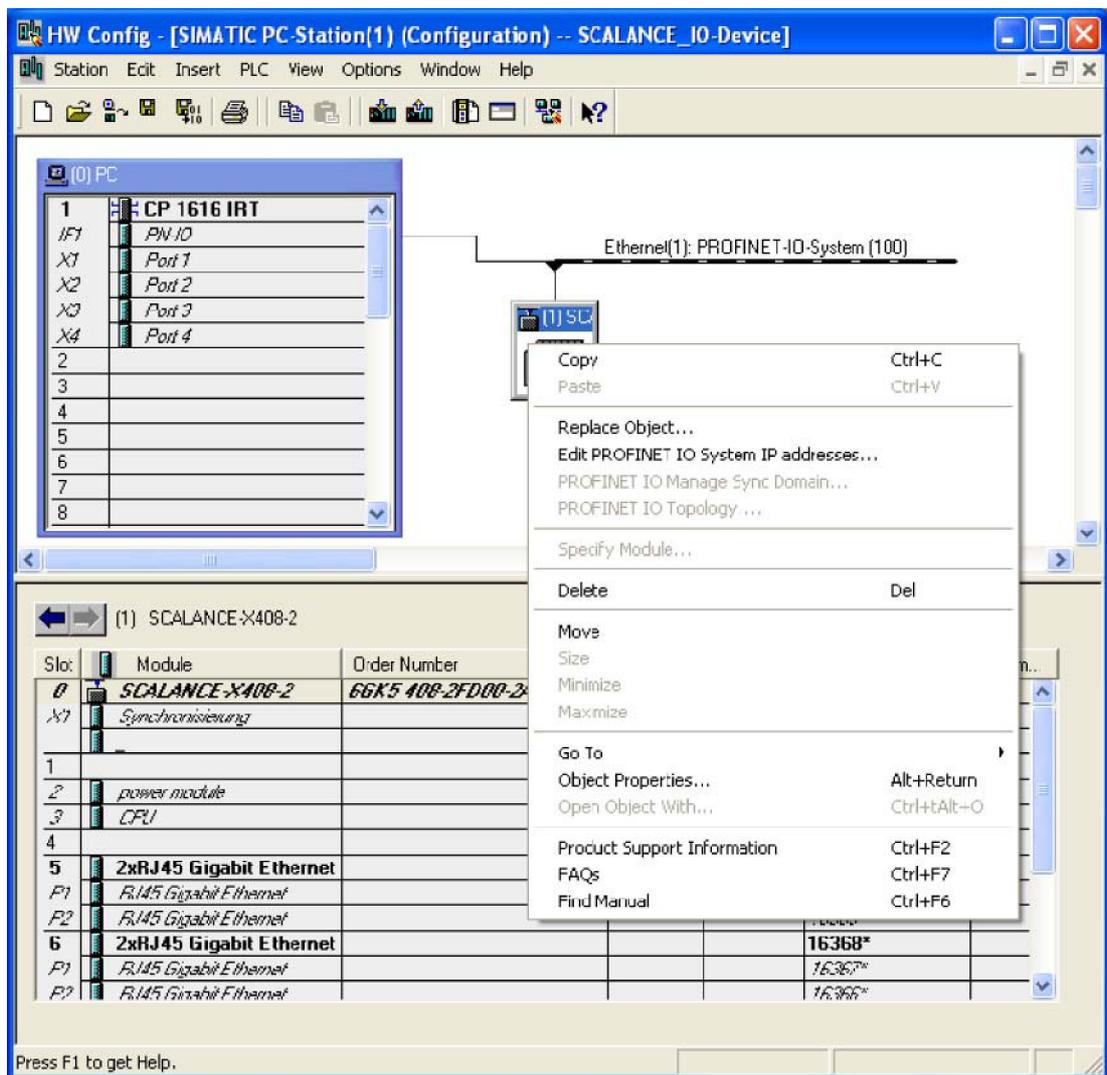


図 6-5 ハードウェア設定

9. ハードウェア設定を保存してコンパイルします。
10. [Station]メニューで[Save and Compile]を選択します。
11. 装置をネットワークに接続して電源を入れます。

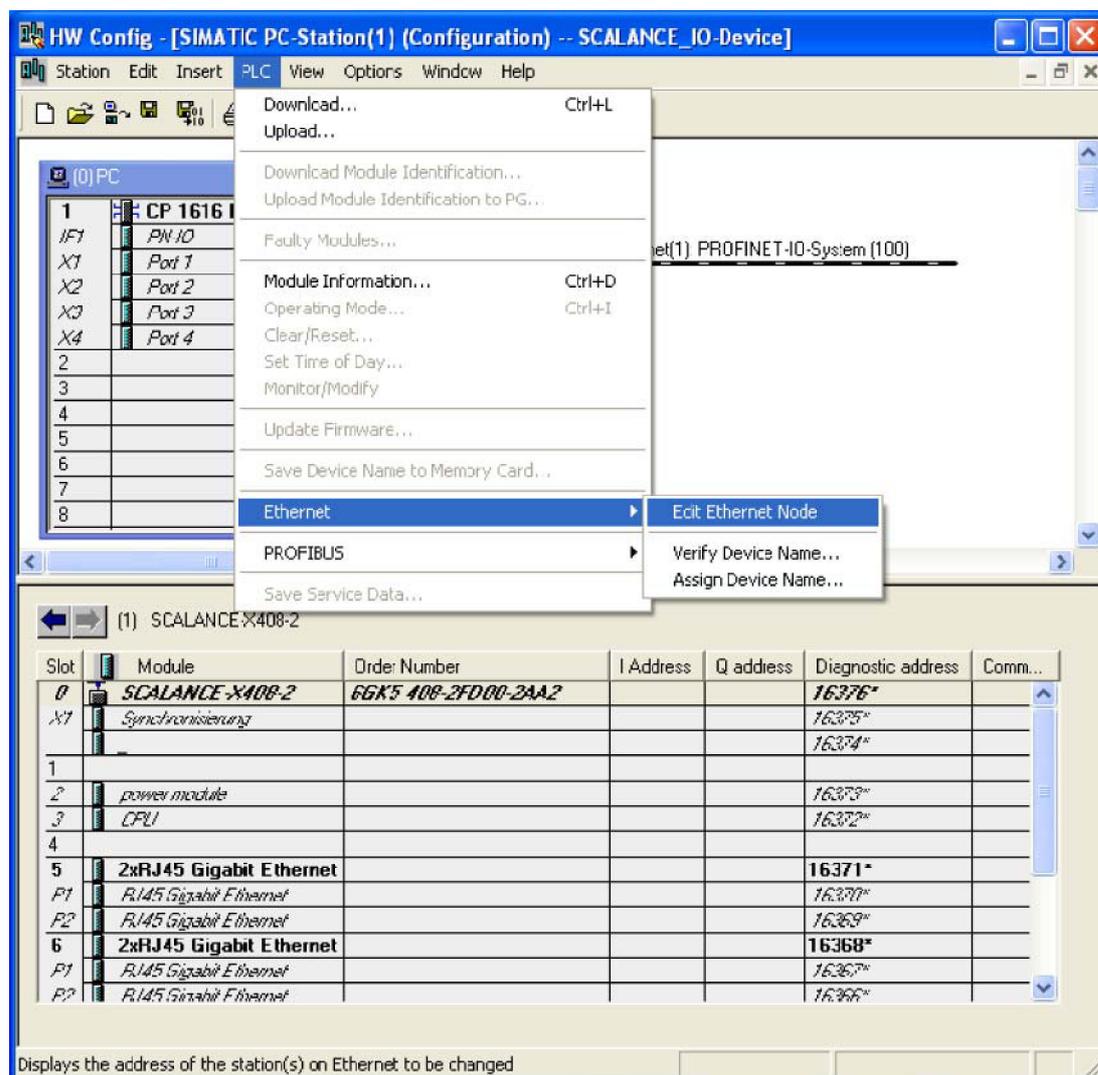


図 6-6 PROFINET IO の装置名の付与

装置名を SCALANCE X408-2 に転送するには、PG と PROFINET IO 装置がオンラインで接続されている必要があります。

1. 装置名を SCALANCE X408-2 に転送するには[PLC]メニューにおいて[Ethernet] > [Assign Device Name]を選択します。

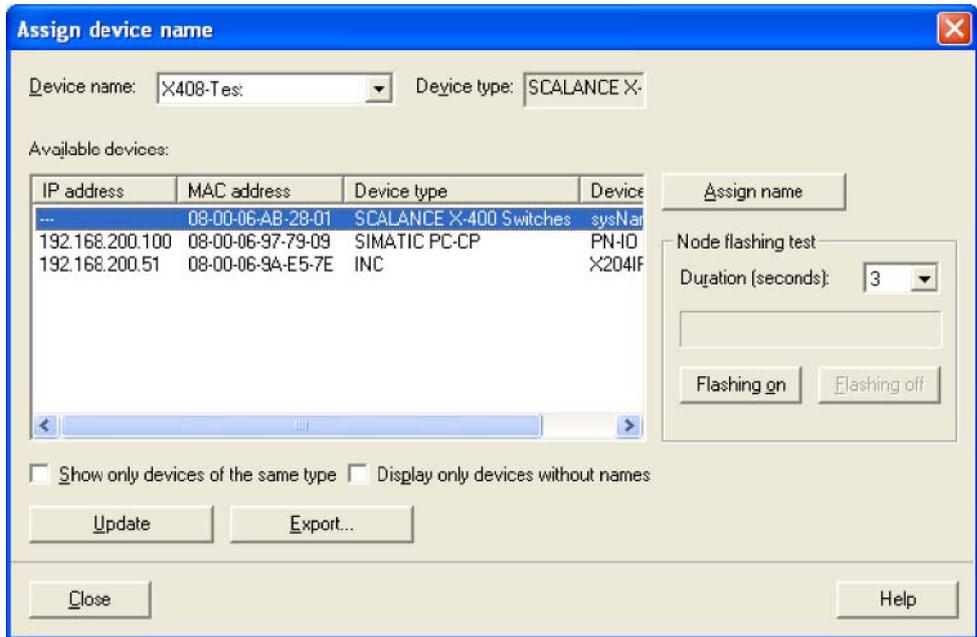


図 6-7 装置名の付与

PROFINET IO 装置を複数台使用している場合には、Assign device name ダイアログにすべて表示されます。その場合、装置の MAC アドレスを表示される MAC アドレスと比較し、該当する IO 装置を選択します。[Flashing On]や[Flashing Off]のボタンを使用すると、割り付け結果を目で確認することもできます（選択した SCALANCE のランプがすべて点滅します）。

1. Assign device name ダイアログの[Assign name]ボタンをクリックします。これで装置名が SCALANCE に恒久的に保存されます。名前割り付けが完了したらその名前がダイアログ中に表示されます。
2. ハードウェア設定をコントローラ（この例では CP 1616）にダウンロードします。これを行うには [PLC]メニューにおいて[Download to Module]を選択します。

6.2 HW Config での設定

電源モジュールの設定

電源に関するスイッチパラメータを設定できます。

Redundant power supply

- Not monitored
2 台ある電源の片方に障害が発生してもアラームは通知されません。
- Monitored
2 台ある電源の片方に障害が発生するとアラームが通知されます。

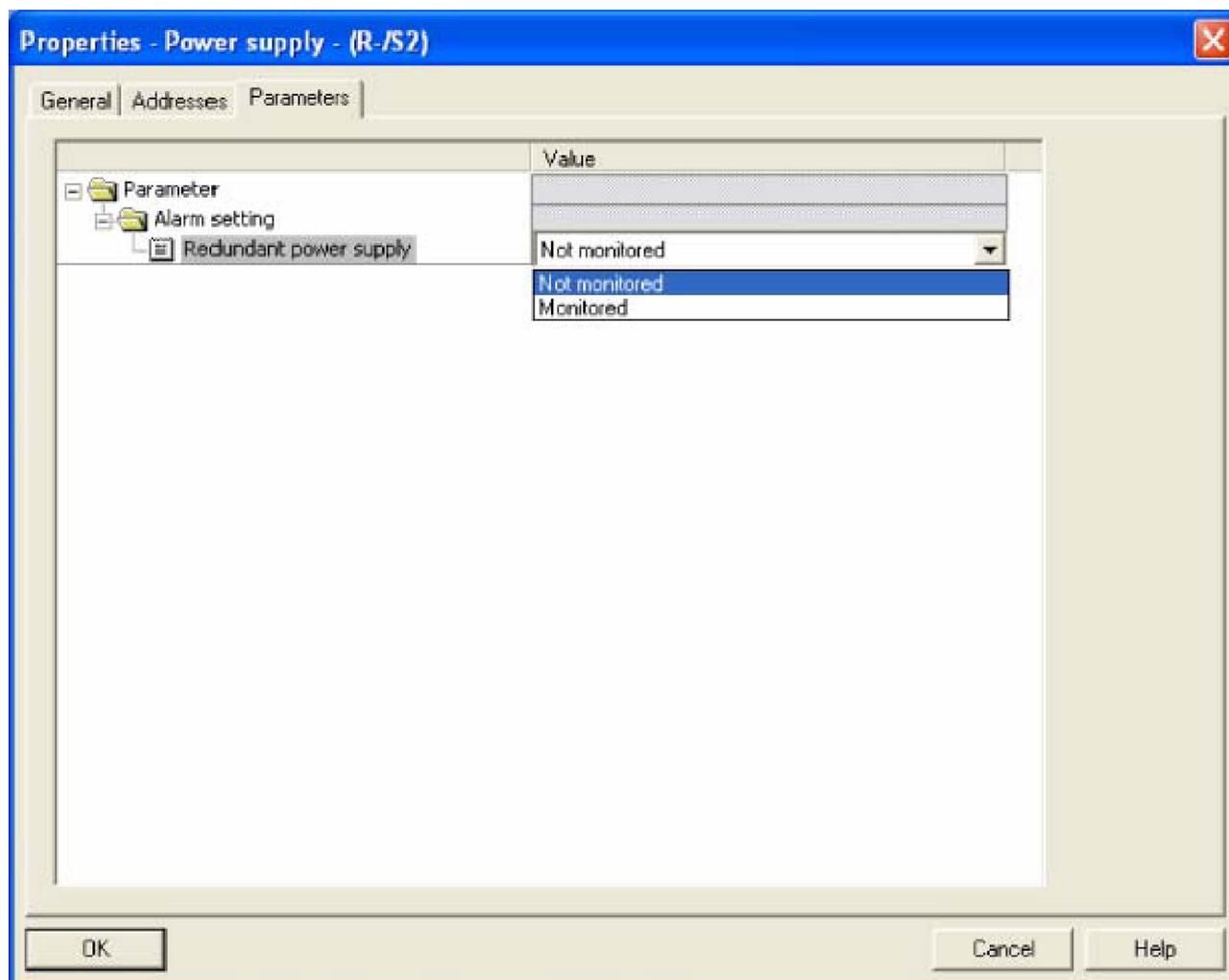


図 6-8 Properties - power module の画面

CPU の設定

CPU モジュールに関するスイッチパラメータを設定できます。

C-PLUG

- Not monitored
C プラグの監視は行われません。
- Monitored
C プラグが障害になるとアラームが発生します。

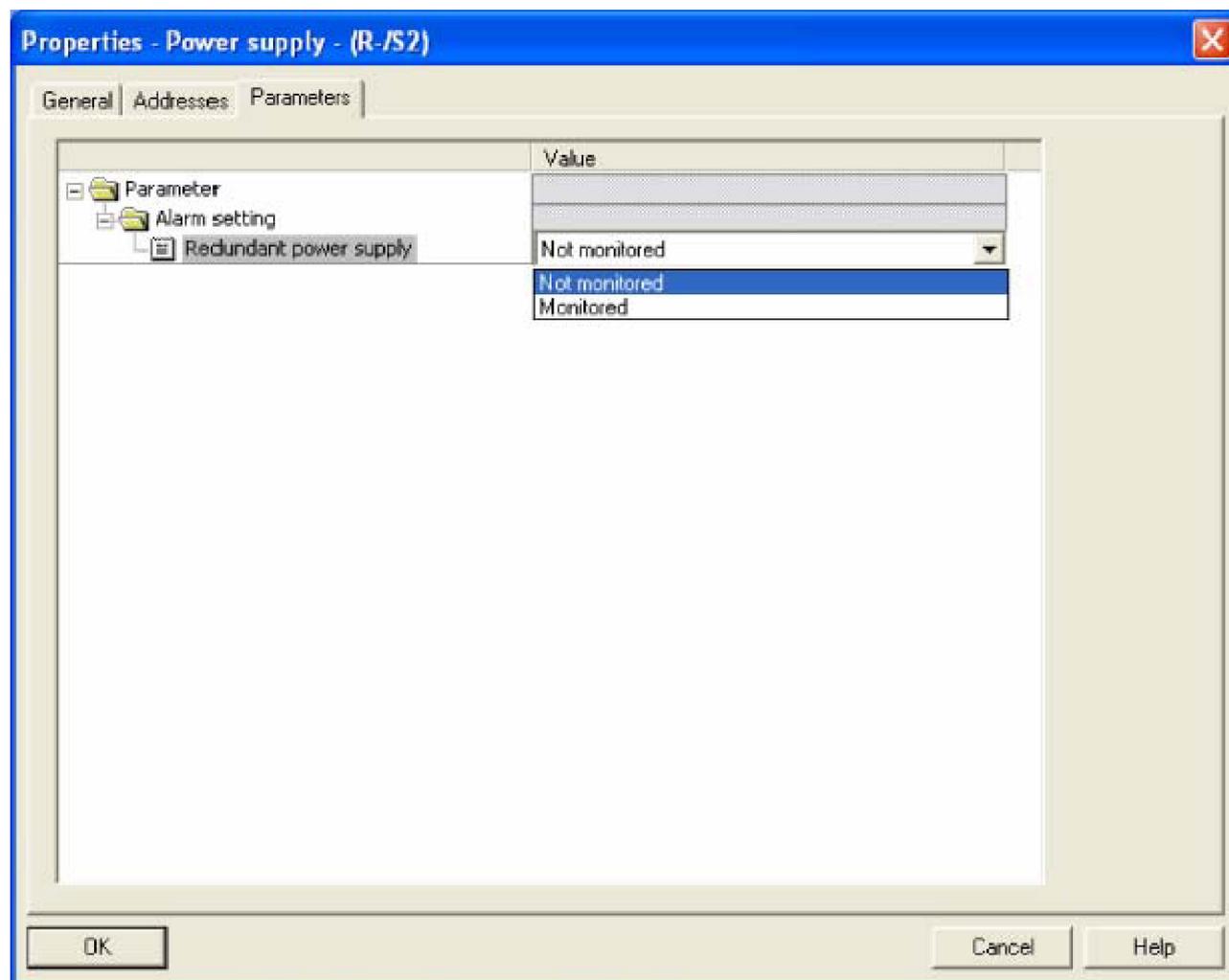


図 6-9 Properties - CPU の画面

ポートごとの設定

各ポートに関する設定を行えます。

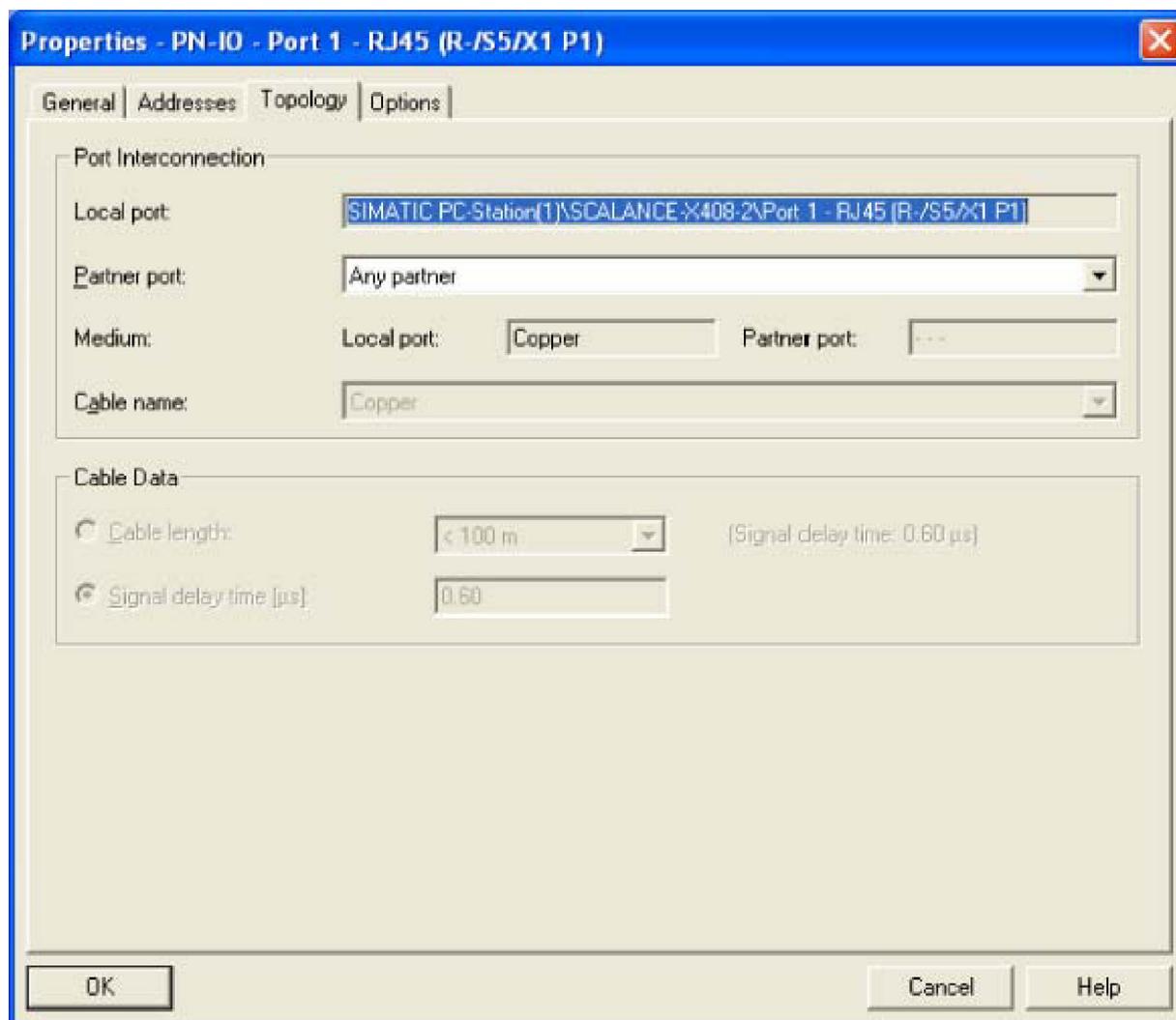


図 6-10 Properties - RJ-45 Gigabit Ethernet

次版の GSD ではトポロジーの設定が可能になります。

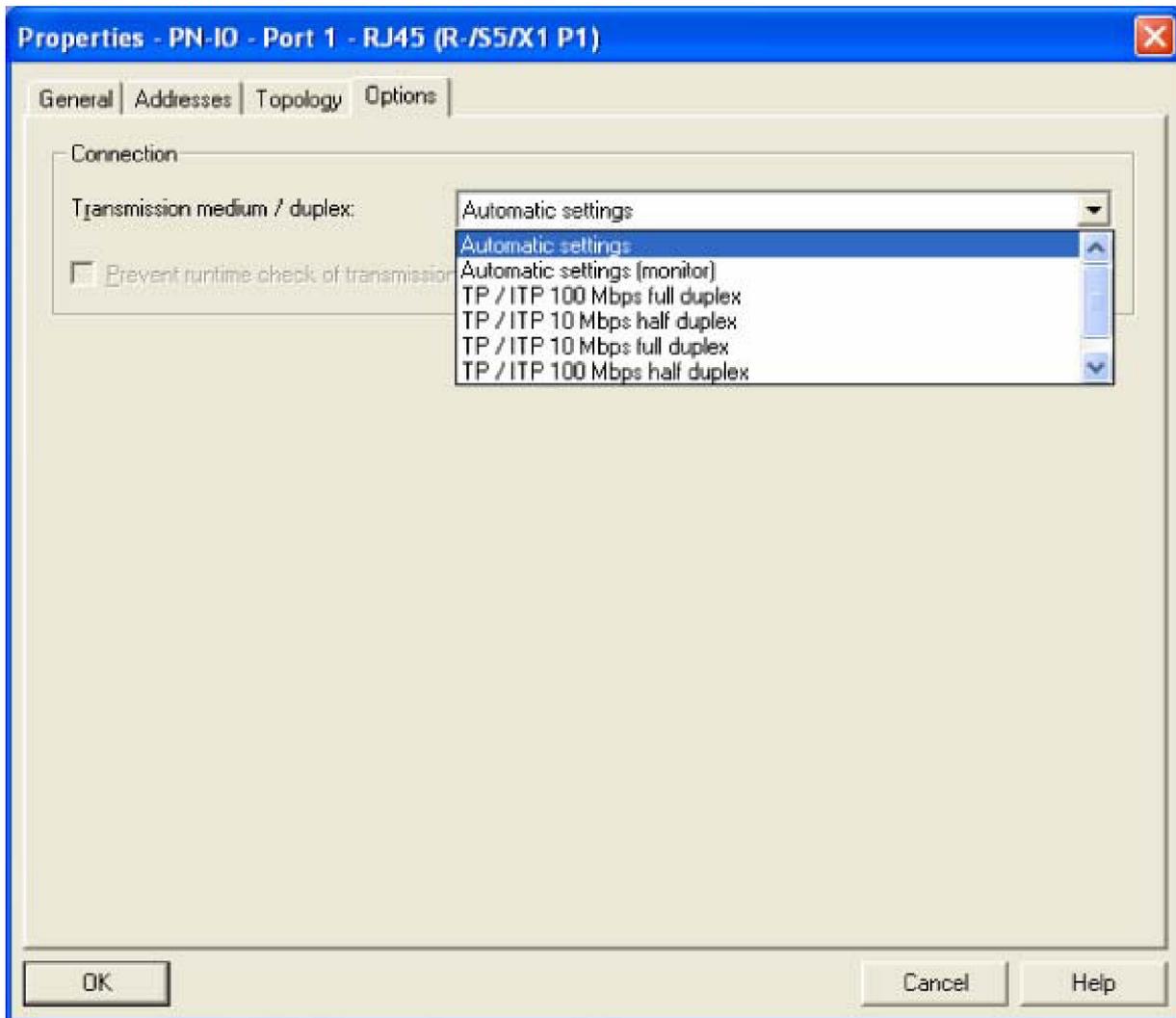


図 6-11 Properties - RJ-45 Gigabit Ethernet のポート設定

変更できる設定

ポートの伝送速度は Autonegotiation または 100Mbps full duplex などの固定値に設定できます。

6.3 PROFINET IO のアクセスオプション

スロットの機能

SCALANCE X-400 シリーズの装置は、最大 4 つのポートをもつスロットをいくつか備えています。1 つのポートに個別に付与することができない機能は、デバイスアクセスポイント（スロット 0）または別の上位モジュール（CPU モジュールと電源モジュール）に対して割り当てます。

スロット 0	<ul style="list-style-type: none"> アラーム (IEC) データレコード (IEC) 	デバイスアクセスポイント (DAP) <ul style="list-style-type: none"> インタフェース接続
スロット 2	<ul style="list-style-type: none"> アラーム 0x200 データレコード 10、12 	電源モジュール <ul style="list-style-type: none"> 二重化電源
スロット 3	<ul style="list-style-type: none"> アラーム 0x201、0x202、0x204 データレコード 11、13 	CPU モジュール <ul style="list-style-type: none"> C プラグ
スロット 5、6、8	<ul style="list-style-type: none"> アラーム (IEC) データレコード (IEC) 	スイッチポート 5.1~8.4 <ul style="list-style-type: none"> アラーム応答 ポート状態

アラームの生成

ユーザはポートの割り当てと必要な特性を正確に設定します。そのためには設定内容と実装状態が一致しなければなりません。もしも STEP7 においてポート 3 が未接続の設定になっていれば、実際の実装もそれに合わせる必要があります。STEP7 によって設定した電源の障害マスクは恒久的に保存されませんが、ポートの障害マスクはリセットされます。DataEX を終了すると STEP7 で行った障害マスクの設定は保持され、PROFINET が動作しなくてもその後もそのまま適用されます。

- Effect of the button during DataEX
ボタンを操作しても何も起こりません。ランプの点滅は障害マスクに変更がないことを表します。
- Effect of other signaling mechanisms during DataEX
ウェブインタフェースと CLI の両方において障害マスクは STEP7 の設定どおりに表示されます。変更はできません。「Setting not possible because of PNIO」というメッセージが表示されます。

データレコードの構造

データレコード 10 (電源、パラメータ設定)

アクセス権限：読み書き可

構造：

```
typedef struct {
  Word BlockType;
  Word BlockLength;
  Byte BlockVersionHigh;
  Byte BlockVersionLow;
  DWord Alarm_enable; };
```

BlockType

1：固定

BlockLength

6 : 装置データでは固定。Type と Length を除いたデータ長を示します。

BlockVersionHigh

1 : 装置データでは固定。上位の版数を示します。

BlockVersionLow

1 : 装置データでは固定。下位の版数を示します。

Enable_alarms

このビット列は監視対象を指定します。ビットが立っていればそのアラーム源は有効です。

未使用 ビット 1~31	Red_power ビット 0
0	0 : 二重化電源の監視なし
	1 : 二重化電源の監視あり

付記

このデータレコードは装置がデータ転送モードにないときにも読み出せます (PG アクセス)。そのスロットに対する現在のアラーム設定がわかります。すなわち、診断のために現在の状態を再度読み出すことができます。

データレコード 12 (電源、モジュール状態)

そのポートに対する現在のアラーム設定を与えます。

アクセス権限 : 読み出しのみ

```
typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
DWord status; };
```

BlockType

1 : 固定

BlockLength

6 : 装置データでは固定。Type と Length を除いたデータ長を示します。

BlockVersionHigh

1 : 装置データでは固定。上位の版数を示します。

BlockVersionLow

1 : 装置データでは固定。下位の版数を示します。

Status :

未使用 ビット 2~31	Fault_line_status ビット 1	Power line redundancy ビット 0
0	信号用接点の現在状態に関する情報 0 : 回線障害、受動的 1 : 回線障害、能動的	二重化電源に関する情報 0 : 二重化なし 1 : 二重化あり

付記

このデータレコードは装置がデータ転送モードにないときにも読み出せます (PG アクセス)。すなわち、診断のために現在の状態を再度読み出すことができます。

データレコード 11 (CPU、パラメータ設定)**構造**

```
typedef struct {
    Word BlockType;
    Word BlockLength;
    Byte BlockVersionHigh;
    Byte BlockVersionLow;
    Word Alarm_Mode;
    DWord Alarm_Parameter; };
```

BlockType

1 : 固定

BlockLength

6 : 装置データでは固定。Type と Length を除いたデータ長を示します。

BlockVersionHigh

1 : 装置データでは固定。上位の版数を示します。

BlockVersionLow

1 : 装置データでは固定。下位の版数を示します。

Alarm_Mode

未使用 ビット 2~31	enhanced_Alarm_Mode ビット 1	Red_power ビット 0
0	機能なし	0 : 二重化電源の監視なし
		1 : 二重化電源の監視あり

付記

このデータレコードは装置がデータ転送モードにないときにも読み出せます (PG アクセス)。そのスロットに対する現在のアラーム設定がわかります。すなわち、診断のために現在の状態を再度読み出すことができます。

データレコード 13 (CPU、モジュール状態)

構造

```
typedef struct {
    Word BlockType;
    Word BlockLength;
    Byte BlockVersionHigh;
    Byte BlockVersionLow;
    DWord PortState;
    byte PortType;
    byte reserved; };
```

BlockType

1 : 固定

BlockLength

6 : 装置データでは固定。Type と Length を除いたデータ長を示します。

BlockVersionHigh

1 : 装置データでは固定。上位の版数を示します。

BlockVersionLow

1 : 装置データでは固定。下位の版数を示します。

Status

未使用 ビット 2~31	C-PLUG_status ビット 0~1
0	ネットワーク機器の C プラグに関する情報 0 : C プラグが挿入されており、問題なし 1 : C プラグの挿入なし 2 : C プラグは挿入されているが問題あり (タイプ不適合) 3 : C プラグは挿入されているが問題あり (チェックサムエラー)

付記

このデータレコードは装置がデータ転送モードにないときにも読み出せます (PG アクセス)。すなわち、診断のために現在の状態を再度読み出すことができます。

C プラグ

用途

C プラグは、モジュール式スイッチの設定データを保存するための脱着式メディアであり、製品に挿入して使います。基本装置の交換時に C プラグを差し替えるだけで、以前の設定データをそのまま利用できます。

注

C プラグの脱着は必ず装置の電源のスイッチを切ってから行ってください。

動作概要

電力は末端機器から供給されます。電源を切っても C プラグのデータはすべて保存されます。

空の C プラグ（工場設定または Clean 機能による消去済みのもの）を挿入して機器を起動すると、SCALANCE X-400 の全設定データがこの中に自動的に保存されます。状態が「Accepted」の場合には、稼働中に行った設定変更がオペレータの操作なしに C プラグに保存されます。

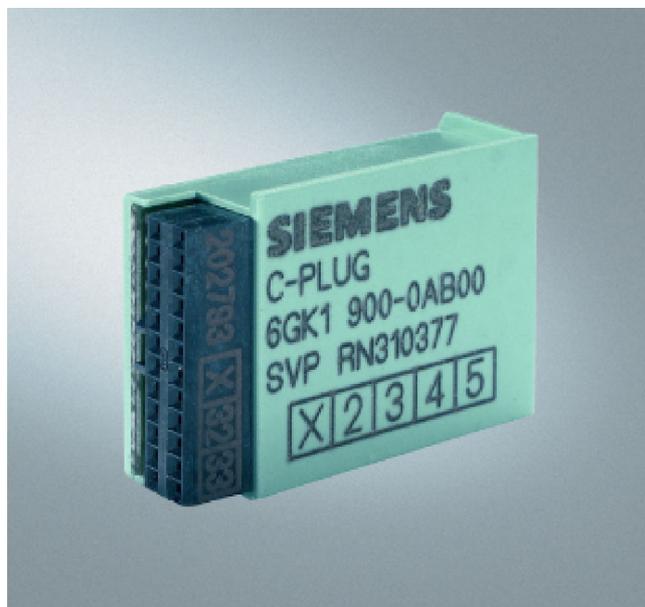


図 7-1 C プラグ

Accepted の C プラグを挿入した状態で装置を起動すると、装置は C プラグの設定データを自動的に使用します。ただしこれが行われるのは、データが適合機種によって書き込まれた場合にかぎります。

C プラグを使用すれば基本装置の交換を簡単かつ短時間に行えます。装置を交換するときは、C プラグを前の装置から外して新しい装置に挿入します。新しい装置を最初に起動すると、以前の装置と同じ設定で立ち上がります。ただし、ベンダによって設定される MAC アドレスを除きます。

注

SCALANCE X-400 を交換する場合、メディアモジュールに関する設定、ならびに SCALANCE X414-3E を使用する場合は DIL スイッチの設定とエクステンダのオプション設定についても採用することが必要です。

診断

適合機種の設定データがない C プラグを挿入した場合、C プラグを不注意で取り出した場合、あるいは C プラグが正しく動作しなかった場合は、装置の診断機能（ランプ、ウェブ型管理ツール、SNMP、CLI）によって異常が示されます。

起動時の動作

	C プラグ	SCALANCE X-400 の起動パターン
1	未実装	内部設定データ（内部設定データが存在する場合）または工場設定値で立ち上がる
2	データなし	内部設定データで立ち上がり、それがただちに C プラグに自動的にコピーされる
3	自装置の設定データあり	C プラグの設定データで立ち上がる
4	他装置の設定データあり	他装置の C プラグの設定データで立ち上がる
5	他機種の設定データあり	内部設定データで立ち上がり、電源モジュールに赤ランプが点灯するほか、ログに記録される
6	欠陥あり	内部設定データで立ち上がり、電源モジュールに赤ランプが点灯するほか、ログに記録される

ケース 1 および 2 の場合、スイッチの CPU モジュールと C プラグの設定データは同じです。ケース 3 と 5 の場合、設定データは異なりますが、手動で一致させることができます。ケース 6 では Clean 機能を使って C プラグの再フォーマットをするという方法があります。それでも問題が解消しない場合は C プラグを交換します。

注

SCALANCE X414-3E でケース 4（スイッチの交換）が発生した場合、物理的なスイッチの設定ではなく、C プラグの DIL スイッチの設定が使用されます。相違があることは診断オプションによって通知されます。

ファームウェアアップデート

8.1 機能的ファームウェアによるファームウェアアップデート

8.1.1 TFTP を用いたファームウェアアップデート

ウェブ型管理ツールまたはコマンドラインインタフェース

TFTP を用いたファームウェアアップデートについては「System Save & Load メニュー」の項をご覧ください。

8.1.2 FTP を用いたファームウェアアップデート

コンソールからのアクセス

SCALANCE X-400 が IP アドレスをもち、PC または PG との間にイーサネット接続が確立されている場合は、以下の手順でファームウェアをアップデートします。

1. コンソールウィンドウを開き、ftp コマンドに続けて SCALANCE X-400 の IP アドレスを入力します。
例 : ftp 192.168.20.54
2. ログイン名とパスワードは WBM や CLI と同じものを入力します。
3. put コマンドに続けてファームウェアファイルの名前を入力します。
例 : put v100031.lad
4. アップロードが完了すると ftp 接続が閉じ、再起動が行われます。

8.2 ブートソフトを用いたファームウェアアップデート

ブートソフトを用いたアップデートの必要性

ファームウェアによるアップデートが実施できない場合には、ブートソフトを用いたファームウェアアップデートが必要になります。そのようなケースとしては、ファームウェアの不良や点滅動作中の電源断などがあります。

ブートローダモードの開始手順

PC または PG を SCALANCE X-400 のシリアルポートに接続していることが必要です。以下の手順でブートローダモードに変更します。

1. SCALANCE X-400 のスイッチ操作によって表示のモードを A または D にします。SELECT/SET ボタンを押さない状態が 1 分以上続くと、自動的に表示モード A に切り替わります。
2. ボタンを 12 秒以上押し続けると、装置が再起動します。
3. 再起動している間に PC または PG のキーボードでいずれかのキーを押します。

SCALANCE X-400 が機能的ファームウェアを備えている場合、接続される ftp サーバと通信できるモードにおいて SCALANCE X-400 が自動的に処理を開始します。ただし SCALANCE X-400 に IP アドレスが付与されていることが必要です。

8.2.1 シリアルポートを介したファームウェアアップデート

手順

SCALANCE X-400 のシリアルポートを使ってファームウェアをダウンロードする手順は以下のとおりです。

1. ターミナルプログラム (HyperTerminal など) を使って PC を SCALANCE X-400 のシリアルポートに接続します。詳細は付録 A に記載しています。
2. SCALANCE X-400 をリセットします。表示モードを A または D に切り替えます (SELECT/SET ボタンを押さない状態が 1 分以上続くと、自動的に表示モード A に切り替わります)。SELECT/SET ボタンを 12 秒以上押し続けます。ブートローダを停止するには、起動処理中にいずれかのキーを押します。HyperTerminal の場合は以下のメッセージが表示されます。

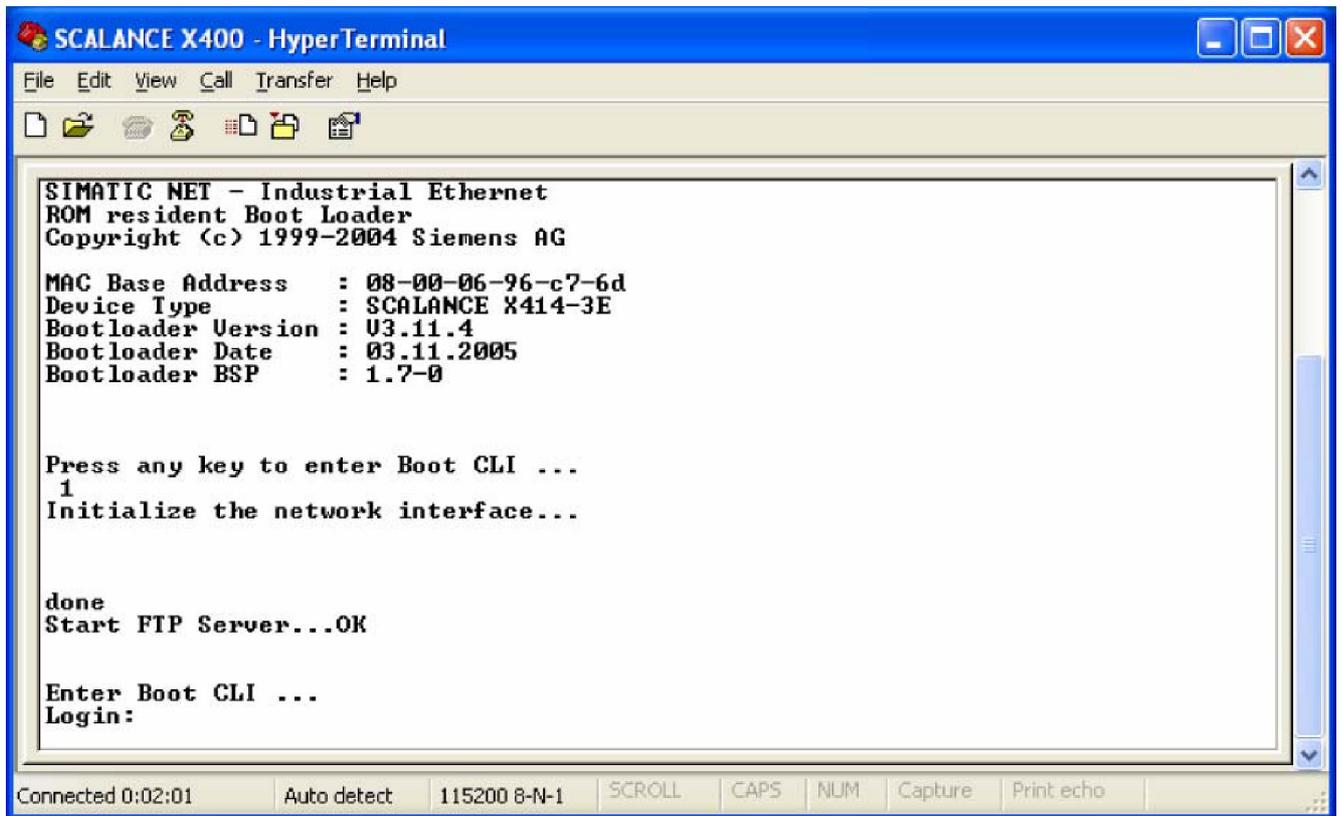


図 8-1 HyperTerminal

- ブートローダのコマンドラインインタフェースに下記のデータでログインします。
Login: siemens
Password: siemens
- ldimage コマンドを入力すると以下のメッセージが表示されます。
XMODEM waiting for file
ATTENTION: do not switch off till the COMPLETED or FAILED message appears... CCCCCC
- メニューから Transfer > Send File を選択します。HyperTerminal において以下のダイアログが開きます。

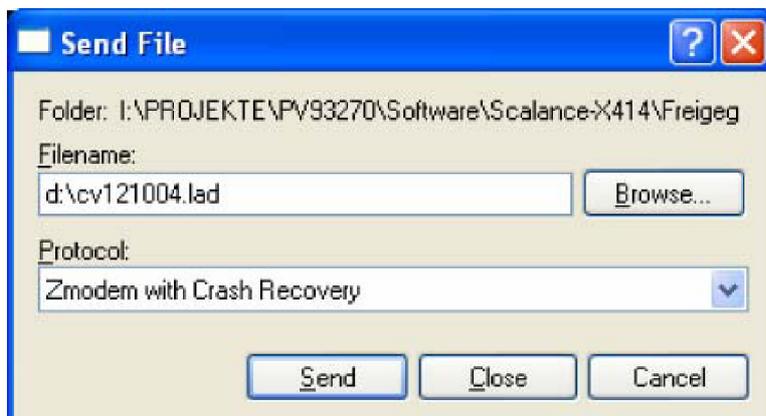


図 8-2 Send File ダイアログ

- ロードするファイル名を入力し、プロトコルには Xmodem を選択します。[Send]ボタンをクリックするとアップロードが開始されます。新たなダイアログが開いてアップロードの進行状況が表示されます。

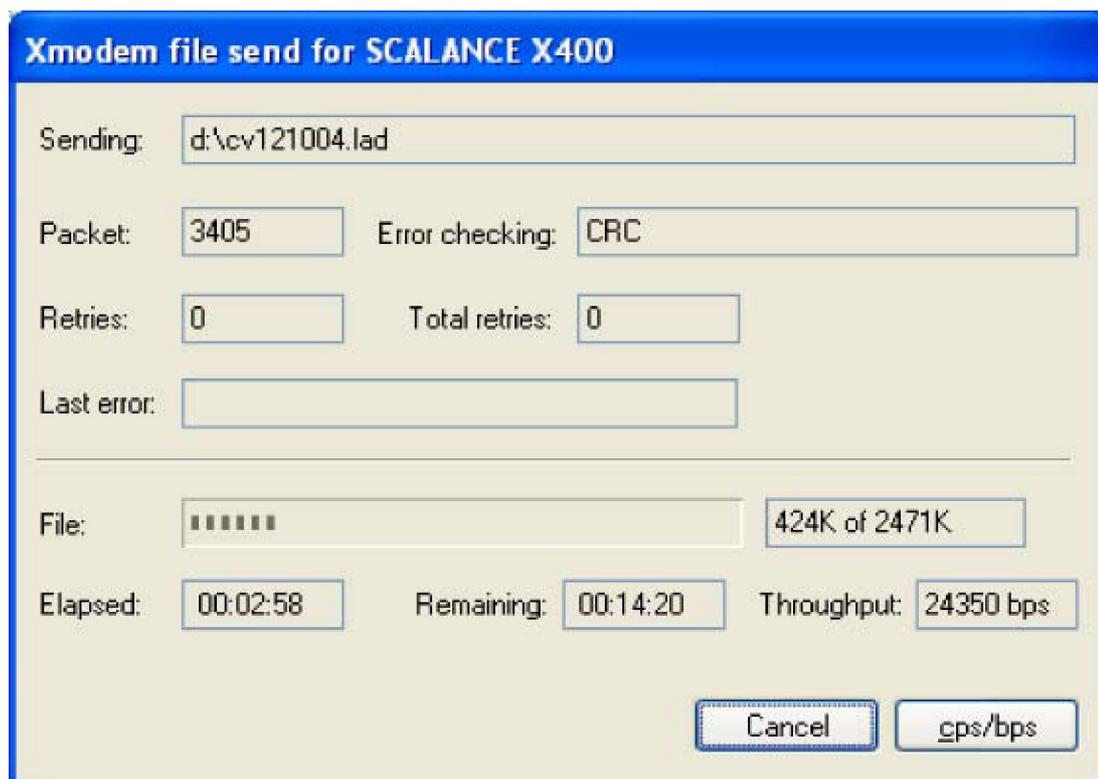


図 8-3 Xmodem によるファイル送信

- アップロードが完了したら以下のメッセージが表示されます。

FlashWriteCOMPLETED

装置を再起動します。

付記

アップロード中は PC と SCALANCE X-400 の接続を切ったり、SCALANCE X-400 に給電する電源装置のスイッチを切ったりしないでください。

信号線の問題によってアップロードが中断された場合、装置は次回の起動時に旧版のファームウェアで立ち上がります。その段階で改めてファームウェアのアップロードを行ってください。

給電の停止によって SCALANCE X-400 へのファームウェアの格納が不完全だった場合には、ブート終了後に「Can't load image from flash -> wrong crc」というメッセージが表示されます。この場合もファームウェアのアップロードをやりなおしてください。

8.2.2 イーサネットポートと FTP を使ったファームウェアアップデート

手順

SCALANCE X-400 のブート機能が IP アドレスをもち、PC または PG との間にイーサネット接続が確立している場合、ファームウェアのダウンロード手順は以下ようになります。

1. コンソールウィンドウを開き、ftp コマンドに続けて SCALANCE X-400 の IP アドレスを入力します。
例 : ftp 192.168.20.54
2. ログイン名とパスワードにはいずれも「siemens」と入力します。
3. put コマンドに続けてファームウェアファイルの名前を入力します。
例 : put v100031.lad
4. アップロードが完了すると ftp 接続が閉じ、再起動が行われます。自動による再起動が完了するまでそのまま待機します。

付録

A

A.1 付録 A : PC と SCALANCE X-400 のシリアルポートの接続

HyperTerminal

HyperTerminal のプログラムは Windows 95/98/NT/2000/XP の OS で使用でき、[スタート]メニューの [プログラム] > [アクセサリ] にあります。このプログラムを使えば以下の作業を行えます。

- SCALANCE X-400 のシリアルポートを用いたファームウェアのアップロード
- コマンドラインインタフェースからのコマンド入力

手順

PC と SCALANCE X-400 のシリアルポートとを接続する手順は下記のとおりです。

1. PC と SCALANCE X-400 のシリアルポートを市販のクロスケーブルで接続します。
2. HyperTerminal のプログラムにおいて [ファイル] メニューの [新しい接続] を選択します。新しい接続に対応するプロパティウインドウが開きます。
3. 接続パラメータは以下の値とします。
ビット/秒 : 115200
データビット : 8
パリティ : なし
ストップビット : 1
プロトコル : なし

ピン配置

PC に接続するため、クロスケーブルの一端には 9 ピンまたは 24 ピンの D-sub メスコネクタが、また他端には 9 ピンの D-sub メスコネクタが備わっています。各ケーブルのピン配置を以下にまとめます。

付録

A.1 付録A : PC と SCALANCE X-400 のシリアルポートの接続

信号名	PC のコネクタ		接続先	SCALANCE X-400 のコネクタ
	25 ピンのジャック ピン	9 ピンのジャック ピン		9 ピンのジャック ピン
TD (Transmit Data)	2	3		3
RD (Receive Data)	3	2		2
RTS (Request to Send)	4	7		7
CTS (Clear to Send)	5	8		8
SG (Signal Ground)	7	5		5
DTR (Data Set Ready)	6	6		6
DTR (Data Terminal Ready)	20	4		4

図 A-1 ピン配置

付記

SIMATIC プログラミングデバイスでは、シリアルポートが 25 ピンのメスコネクタの場合があります。その場合には市販されているオスメス変換アダプタ (25 ピンオス~25 ピンオス) を使用してください。

A.2 付録 B : SCALANCE X-400 の MIB オブジェクト

MIB II 規格の重要なオブジェクト

装置状態監視に用いられる MIB II の SNMP 変数の一部を以下に示します。MIB II には SNMP 準拠のすべての装置によって通常サポートされる SNMP 変数がすべて記述されています。

System グループの MIB オブジェクト

オブジェクト	アクセス権	説明
sysDescr	読み出しのみ	最大 255 文字の文字列です。 値にはメーカーごとに決まる装置 ID が含まれます。
sysObjectID	読み出しのみ	装置独自の SNMP 変数にアクセスする際に使用されるアドレス (オブジェクト ID) がここに出力されます : 1.3.6.1.4.1.4196.1.1.5.4 プライベートオブジェクト ID が宣言されていない場合、オブジェクト ID は[0,0]です。デフォルトでは値「0」が設定されます。
sysUpTime	読み出しのみ	最後にリセット (電源投入など) されてからの経過時間。100 分の 1 秒単位で示されます。
sysContact	読み書き可	担当者の情報をここに入力できます (デフォルト : 空の文字列)。 可能な値 : 最大 255 文字の文字列。
sysName	読み書き可	装置の名前をここに入力できます (デフォルト : 空の文字列)。 可能な値 : 最大 255 文字の文字列。
sysLocation	読み書き可	装置の位置をここに入力できます (デフォルト : 空の文字列)。 可能な値 : 最大 255 文字の文字列。
sysServices	読み出しのみ	ISO/OSI モデルに規定されるコンポーネントの機能 (サービス) を示します。 各層の機能 : <ul style="list-style-type: none"> • 物理層 (リピータなど) • データリンク、サブネット (ブリッジ、イーサネットスイッチなど) • インターネット (IP ゲートウェイ、ルータなど) • エンドツーエンド (IP ホストなど) • アプリケーション (メールサーバなど) データ型 : 32 ビットの整数

Interface グループの MIB オブジェクト

オブジェクト	アクセス権	説明
ifNumber	読み出しのみ	そのコンポーネントで使用できるインタフェースの数。 SCALANCE X414-3E の場合、このオブジェクトには「69」の値が出力されます（物理ポート 26 基、内部（仮想）ポート 42 基、CPU モジュールのアウトバンドポート 1 基）。 SCALANCE X408-2 の場合、このオブジェクトには「18」の値が出力されます（物理ポート 8 基、内部（仮想）ポート 9 基、接続のないアウトバンドポート 1 基）。 データ型：32 ビットの整数
ifDescr	読み出しのみ	ポートの説明です。他のポート情報が付随することもあります。 可能な値：最大 255 文字の文字列。
ifType	読み出しのみ	SCALANCE X-400 については「ethernet-csmacd(6)」または「gigabitEthernet(117)」の値が入力されます。 データ型：整数
ifSpeed	読み出しのみ	イーサネットポートのデータ転送速度を bps 値で表します。 SCALANCE X-400 の場合は 10Mbps、100Mbps、1000Mbps のいずれかです。 データ型：Gauge
ifOperStatus	読み出しのみ	イーサネットポートの現在の動作状態を示します。以下の値が可能です。 <ul style="list-style-type: none"> • 確立中(1) • ダウン(2) • 試験中(3) • 不明(4) • スリープ(5)（外部アクション待ち） • 存在しない(6) • 下位レイヤのダウン(7) 試験中(3)の状態は、ユーザデータ転送が行われていないことを示します。 データ型：整数
ifLastChange	読み出しのみ	当該ポートが現在の状態で動作している時間の長さ。値は 100 分の 1 秒単位で示されます。 データ型：TimeTicks
ifInErrors	読み出しのみ	エラーによって上位層プロトコルに渡されなかった受信パケット数。 データ型：Counter
ifOutErrors	読み出しのみ	エラーによって送出されなかったパケット数。 データ型：Counter

ポート番号

SNMP では「m.n」(m : スロット番号、n : ポート番号) という形式でポートを指定することができません。SNMP ではポートの指定にインタフェース番号を使用します。インタフェース番号とポートの対応を以下に示します。

SCALANCE X414-3E のポート対応表

インタフェース番号	ポート	エクステンダがない ときのポート名	メタル用エクステンダ があるとき	光用エクステンダが あるとき
51380225	ポート 1	5.1	5.1	5.1
51380226	ポート 2	5.2	5.2	5.2
51380227	ポート 3	6.1	6.1	6.1
51380228	ポート 4	6.2	6.2	6.2
51380229	ポート 5	7.1	7.1	7.1
51380230	ポート 6	7.2	7.2	7.2
51380231	ポート 7	9.1	9.1	9.1
51380232	ポート 8	9.2	9.2	9.2
51380233	ポート 9	9.3	9.3	9.3
51380234	ポート 10	9.4	9.4	9.4
51380235	ポート 11	10.1	10.1	10.1
51380236	ポート 12	10.2	10.2	10.2
51380237	ポート 13	10.3	10.3	10.3
51380238	ポート 14	10.4	10.4	10.4
51380239	ポート 15	11.1	11.1	11.1
51380240	ポート 16	11.2	11.2	11.2
51380241	ポート 17	11.3	11.3	11.3
51380242	ポート 18	11.4	11.4	11.4
51380243	ポート 19	-	12.1	12.1
51380244	ポート 20	-	12.2	12.2
51380245	ポート 21	-	12.3	13.1
51380246	ポート 22	-	12.4	13.2
51380247	ポート 23	-	13.1	14.1
51380248	ポート 24	-	13.2	14.2
51380249	ポート 25	-	13.3	15.1
51380250	ポート 26	-	13.4	15.2

SCALANCE X408-2 のポート対応表

インタフェース番号	ポート	ポート名
51380225	ポート 1	5.1
51380226	ポート 2	5.2
51380227	ポート 3	6.1
51380228	ポート 4	6.2
51380229	ポート 5	8.1
51380230	ポート 6	8.2
51380231	ポート 7	8.3
51380232	ポート 8	8.4

例 :

IfOperStatus.51380225 というオブジェクトは、SCALANCE X-400 のポート 1 の動作状態（確立中やダウンなど）を決定します。

SCALANCE X-400 の重要なプライベート MIB オブジェクト

OID

SCALANCE X-400 におけるプライベート MIB オブジェクトのオブジェクト ID は下記のとおりです。

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).iScalanceX(5).iScalanceX400(4)

オブジェクト	アクセス権	説明
snX400FaultState	読み出しのみ	信号用接点の状態を示します。 可能な値 : • 1 : エラーなし • 2 : エラーあり データ型 : 整数
snX400ReportFaultIndex	読み出しのみ	エラーには発生順に追い番が与えられます。この 4 バイト変数はその番号を表します。
snX400ReportFaultState	読み出しのみ	ある番号に対応するエラーメッセージを格納します。
snX400RmMode	読み出しのみ	冗長化マネージャのモードです。 • SCALANCE X-400 は冗長化マネージャです。 • SCALANCE X-400 は冗長化マネージャではありません。

オブジェクト	アクセス権	説明
snX400RmState	読み出しのみ	冗長化マネージャがアクティブかパッシブかを示します。 可能な値 : <ul style="list-style-type: none"> 1 : 冗長化マネージャはパッシブです。SCALANCE X-400 は冗長化マネージャとして動作し、リングは開いています。すなわち、その装置に接続される SCALANCE X-400 のラインは正常に動作しています。冗長化マネージャモードがオフのときにも「パッシブ状態」として表示されます。 2 : 冗長化マネージャはアクティブです。SCALANCE X-400 は冗長化マネージャとして動作し、リングは閉じています。すなわち、その装置に接続される SCALANCE X-400 のラインに障害（問題）があります。冗長化マネージャはリングポート間の接続を開通し、バス構成を復旧させます。 データ型 : 整数
snX400RmStateChanges	読み出しのみ	冗長化マネージャが「アクティブ状態」に切り替わった度数を示します。 データ型 : Counter
snX400StandbyMode	読み出しのみ	スタンバイ機能のモードです。 <ul style="list-style-type: none"> スタンバイ機能はオン スタンバイ機能はオフ
snX400StandbyState	読み出しのみ	スタンバイ状態を示します。 <ul style="list-style-type: none"> 1 装置はマスタかつパッシブです。 3 装置はスレーブかつパッシブです。 5 装置はマスタかつアクティブです。 7 装置はスレーブかつアクティブです。 257 装置はスタンバイ接続のために相手先装置を探しています。 300 スタンバイ機能はオフ状態です。 データ型 : 整数
snX400StandbyStateChanges	読み出しのみ	スタンバイ状態が「アクティブ」に切り替わった度数を示します。 データ型 : Counter
snBootStrapVersion	読み出しのみ	ブートローダのファームウェア版数。「major.minor」の形で表されます。
snHwVersion	読み出しのみ	システムのハードウェア版数。「major.minor」の形で表されます。
snSwVersion	読み出しのみ	システムのソフトウェア版数です。
snInfoSerialNr	読み出しのみ	装置のシリアル番号です。
snMacAddressBase	読み出しのみ	SCALANCE X-400 の MAC アドレスです。

オブジェクト	アクセス権	説明
snX400ModuleIdentMLFB	読み出しのみ	モジュールの MLFB 番号です。
snoX400PwerSupply1State	読み出しのみ	電源入力 1 の状態です。
snX400PowerSupply2State	読み出しのみ	電源入力 2 の状態です。
snX400ReportDigitalInState	読み出しのみ	デジタル入力の状態です (SCALANCE X414-3E)。

A.3 付録 C : フレームのタギング

イーサネットフレームを 4 バイト拡張する

CoS (Class of Service : フレーム優先処理) とポート VLAN (仮想 LAN) の機能を実現するため、IEEE 802.1 Q にはイーサネットフレームに VLAN タグを付加する拡張方式が規定されています。

付記

VLAN タグを付加すると、イーサネットフレームの最大許容長が 1518 バイトから 1522 バイトに増えます。ネットワーク上の末端ノードがこの長さおよびフレームタイプを処理できるかどうかを確認する必要があります。対応していない場合、そのノードには標準長のフレームしか送ることができません。

追加の 4 バイトは、データフレームのヘッダにおいて送信元アドレスとイーサネットのタイプ・長さフィールドの間に挿入されます。

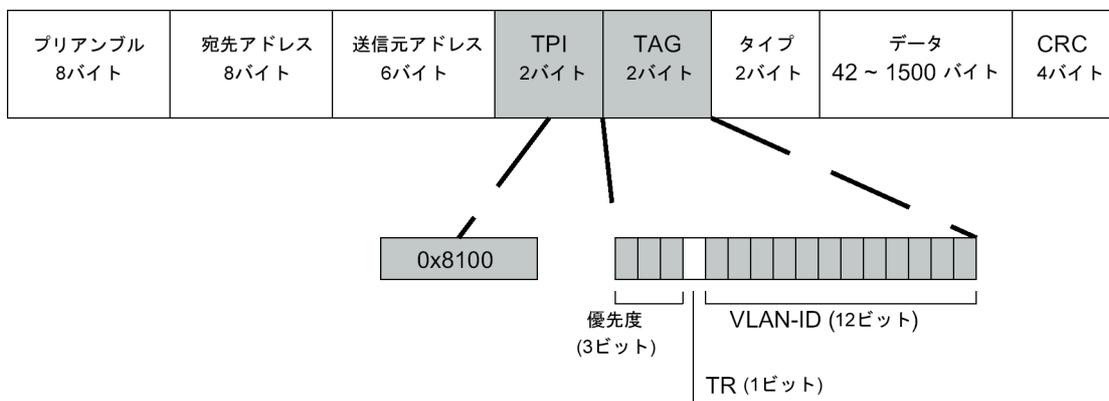


図 A-2 タグ付きフレームの構成

VLAN タグには、タグプロトコル識別子 (TPI) フィールドとタグ制御情報フィールドが含まれます。

タグプロトコル識別子フィールド

前の 2 バイトはタグプロトコル識別子 (TPI) フィールドで、値はつねに 0x8100 です。この値は、そのデータフレームに VLAN 情報または優先度情報が含まれていることを示します。

タグ制御情報フィールド

後半の 2 バイトはタグ制御情報 (TCI) フィールドで、以下の情報を含みます。

CoS

タグ付きフレームには CoS (Class of Service) と呼ばれる 3 ビットの優先度フィールドがあります。これは IEEE 802.1p に基づく優先度で、その内容は以下のとおりです。

CoS ビット	データの種類
000	実時性が要求されないデータトラフィック (ベストエフォート未満 [基本設定])
001	通常のデータトラフィック (ベストエフォート [バックグラウンド])
010	未使用 (標準)
011	未使用 (最上エフォート)
100	遅延 100ms 以下のデータ転送
101	保証型サービス、インタラクティブなマルチメディア
110	保証型サービス、インタラクティブな音声伝送
111	未使用

データフレームの優先処理を行うには、優先度の低いデータフレームをバッファリングできるキューがコンポーネント内に存在することが必要です。

SCALANCE X-400 には並列キューが 4 つあり、それを使って優先度の異なるフレームを処理できます。優先度が最も高いフレームが最初に処理されます (Strict Priority 法)。この方法により、たとえデータトラフィックが高負荷の場合であっても最高優先フレームが転送できます。

CFI

TR ビットは、トークンリングのカプセル化処理の識別子として使用されます。

VLAN ID

残り 12 ビットでは最大 4096 の VLAN ID を指定できます。以下のルールがあります。

VLAN-ID	説明
0	フレームには優先度情報しかなく (優先度タグ付きフレーム)、有効な VLAN ID がありません。
1~4096	有効な VLAN ID です。フレームに対して 1 つの VLAN が対応します。優先度情報をもたせることもできます。

用語の説明

BOOTP

IP アドレスを自動的に割り当てるためのプロトコル。BOOTP サーバによって IP アドレスが与えられる。

BPDU (Bridge Protocol Data Unit)

スパニングツリープロトコルで使用される経路情報フレーム。BPDU には 2 種類がある。コンフィギュレーション BPDU は経路決定に必要な情報をすべて含む。これに対し、トポロジー変化通知 BPDU にはプロトコル ID、プロトコル版数、および BDU タイプのみが含まれる。これはトポロジーの変化を通知する。

CIDR (Classless Inter-Domain Routing)

現行の 32 ビットの IP アドレス空間を有効活用する手法を規定する。ルーティングテーブルの情報量低減とアドレス範囲の有効利用を目的に 1993 年に導入された。CIDR を使えば、従来のネットワーククラスによらないルーティングが可能になる。

CLI

コマンドラインインタフェース。ターミナルを用いる SCALANCE X-400 の設定方法。CLI はシリアルインタフェースでも、あるいは CPU のファストイーサネットインタフェースを使った Telnet でも使用できる。

CoS (Class of Service)

VLAN フレームを処理する際の優先度。IEEE 802.1p には 8 段階の優先度が規定される。

CRC (Cyclic Redundancy Check)

フレームの誤りを検出するために伝送プロトコルで使用されるチェックサム。

C プラグ (configuration plug)

設定データやプロジェクトエンジニアリングデータを格納するための脱着式メディア。装置交換時に C プラグを差し替えることで以前の設定がそのまま利用できる。

DES3 (Data Encryption Standard 3)

対称的な暗号化スキーム。すなわちデータの暗号化と復号化に同じ鍵が使用される。DES3 [3DES と書かれる] は、セキュリティ強化のためにアルゴリズムを 3 回実施することを意味する。

DHCP (Dynamic Host Configuration Protocol)

BOOTP と同じく IP アドレスを自動的に割り当てるためのプロトコル。ただし、DHCP の場合は装置の稼働中にアドレスを割り当てることができる。

DLF (Destination Lookup Failure)

設定されている宛先アドレスがまだ学習されていないフレームをスイッチが処理するときにこれが発生する。そのようなフレームは通常、全ポートに転送される。

GARP (Generic Attribute Registration Protocol)

VLAN とマルチキャストグループを定義できる登録プロトコル。これには以下の 2 種類がある。

GMRP : マルチキャストグループをセットアップする

GVRP : VLAN を登録する

GMRP (GARP Multicast Registration Protocol)

GMRP フレームを使用することで、ノードは自分がマルチキャストアドレスの受信者であることをスイッチに登録できる。スイッチはこの登録フレームを専用フレームで各ポートに送信する。これによって他のスイッチがそのアドレスを知るところとなり、そのアドレスの登録フレームを受信したポートにのみ、そのアドレスのマルチキャストフレームが送信される。

GVRP (GARP VLAN Registration Protocol)

VLAN の情報をスイッチ間で交換するためのプロトコル。GVRP フレームを使えば、ポートに対してノードがある特定の VLAN ID を登録することができる。

IETF (Internet Engineering Task Force)

インタフェースに関するあらゆる側面を扱う委員会。標準化に関する提案を行う。

IGMP (Internet Group Management Protocol)

IP プロトコルの拡張であり、マルチキャストグループへの IP アドレスの登録などを行える。

IPv4

インターネットプロトコルのバージョン 4 は 1981 年の RFC 791 において規定された。IPv4 は 32 ビットアドレスを使用するため、最大で 4,294,967,296 個の一意のアドレスが使用できる。IPv4 アドレスは通常、4 つに区切られた十進数で表記される。それぞれ 8 ビットであるため各ブロックは 0 から 255 までの値が可能である。

MD5 (Message Digest 5)

デジタル署名を生成する方法の 1 つ。指定のデータに対して再現可能な一意の値を計算する。

MIB (Managed Information Base)

SNMP によるネットワーク管理において必要となるすべてのデータを網羅したツリー構造。

NTP (Network Time Protocol)

インターネット上でクロック送信機を使用可能にする TCP/IP ベースのプロトコル。NTP を簡素化した SNTP (Simple Network Time Protocol) は計算が簡略化されている分、精度が落ちる。

OSPFv2 (Open Shortest Path First バージョン 2)

RFC 1247 に規定されるリンク状態ルーティングプロトコル。各ルータはネットワークの現状データをもっており、それがリンク状態データベース (OSPF LSDB) に入っている。ルータはこのデータベースをもとに最短パス優先アルゴリズム (SPF) によって経路を計算する。RIP と違って OSPF では階層的なルーティングが可能であり、ネットワークは独立した複数のエリアに分割される。ルータは RIP のようなルーティングテーブルの交換を行わず、リンク状態の更新を行う。

RFC (Request For Comments)

インターネットに関する仕様、提案、構想、およびガイドラインは RFC の形で発表される。1989 年以降、RFC のフォーマットは RFC 1111 によって規定されている。

各 RFC には具体的なステータスがあり、それによって種類が特定される。プロトコルを提出してチェックを受けている段階は「Initial (初期)」段階である。そのプログラムをスタンダードとして提案すると「Proposed Standard (スタンダード素案)」となる。少なくとも 2 つの独立した実施対象において試行されると「Draft Standard (ドラフトスタンダード)」になる。さらにチェックを受け、有効なスタンダードとして認められるとようやく「Standard (スタンダード、規格)」となる。RFC のなかには新しいプロトコルによって差し替えられるものがあるため、そのような古いプロトコルは「Historic (旧版)」として保管される。実験段階のプロトコルは「Experimental (実験用)」という言葉が付く。

いったん公開された RFC は修正も改版もされない。必要な場合は必ず新しい RFC と差し替えられる。新しい RFC は「Obsolete xxx」の識別子によって、また古い RFC は「Obsoleted By xxx」の識別子によって識別される。「Updates xxx」の識別子を使えば新しい RFC を修正または拡張することができる。RFC 文書は南カリフォルニア大学情報科学研究所 (USC-ISI) が管理している。

RIPv2 (Routing Information Protocol バージョン 2)

RFC 1723 に規定される。RIPv1 の改良版である。バージョン 1 と比較した場合、RIPv2 でも VLSM (可変長サブネットマスク) をサポートするが、ブロードキャストではなくマルチキャストを使用する。また認証も行う。RIPv2 は階層のないネットワークしか認識できないため、ネットワークを分割することはできない。

RMON (Remote Monitoring)

リモートモニタリング。RMON に準拠した装置を使えば診断データがその装置上に収集され、ネットワーク管理端末を使って読み出すことができる。すなわちネットワーク問題が早期に発見され、解決できる。

RMON のメリットは場所に依存しないことである。適切なレポート用ソフトウェアを使えば、ネットワーク内のどの場所からでも収集データが分析できる。

SHA (Secure Hash Algorithm)

この方法は、指定のデータに対して 160 ビット長の再現可能な一意の値を計算する。

SNMP (Simple Network Management Protocol)

ネットワーク管理情報を転送するための標準プロトコルの 1 つ。

Telnet

このプロトコルを使用することで、LAN またはインターネット上の他装置との間にインタラクティブな接続を確立できる。その装置に直接つながっているかのようにユーザはターミナルと同じオプションを使用できる。

TFTP (Trivial File Transfer Protocol)

データ転送を行うための UDP を使った簡易なプロトコル。サイズ制限があるため、わずかなメモリしかもたないネットワークノードでも使用することができる。

UTC (Universal Time Coordinated)

国際原子時をもとにした全世界で有効な基準時。

WBM

ウェブ型管理ツール。WBM を使えば設定および診断をウェブブラウザで実行できる。ユーザによる入力は HTTP プロトコルを使って装置に送信され、装置は HTTP を使ってユーザに返信を返す。

アウトバンド IP アドレス

スイッチはアウトバンド IP アドレスを用いることによって外部的に（ルーティング型ないし交換型ネットワークを経由せずに）特定できる。SCALANCE X414-3E ではスロット 4 に収容される CPU モジュールのイーサネットインタフェースがこれに関与する。

インバンド IP アドレス

スイッチはインバンド IP アドレスを用いることでルーティング型ないし交換型ネットワークにおいて特定可能となる。SCALANCE X-400 ではスロット 5 から 11 のポートがこれに関与する。

冗長化マネージャ (RM)

リング形トポロジーに使用されるネットワークノードで、他スイッチとの接続が正常である場合にはリングポート間のフレーム転送を行わない。2 スイッチ間の接続が途切れるとリングポート間でフレーム転送を行い、全スイッチ間の接続を再確立する。

スパニングツリー

このプロトコルは、複数の冗長ネットワーク接続においてループの発生を防止する。接続上に通信障害が発生すると、全ノード間に必ず 1 つの接続のみが存在するようにネットワークを自動再構成する。

デフォルトゲートウェイ

送信先アドレスの端末が同じ LAN 内にない場合、フレームはすべてこのネットワークノードに転送される。

マルチキャスト

マルチキャストアドレスをもつフレームは、そのアドレスを受信する用意ができていないすべてのノードによって受信される。

索引

B

BOOTP, 2-6, 3-2, 3-4, 4-33
BPDU (Bridge Protocol Data Unit) , 4-85

C

CLI コマンド, 4-6
 コマンドのショートカット, 4-7
 コマンドを表す記号, 4-7
CoS (Class of Service) , A-9
CRC, 4-131
C プラグ, 2-4

D

DHCP, 2-6, 3-2, 3-5, 4-33
DLF (Destination Lookup Failure) , 4-72

F

Forward Delay, 4-87
Fragments, 4-131

G

GMRP, 4-57, 4-70
GSD file, 6-2
GVRP, 4-60, 4-84

H

Hello タイム, 4-85
HW Config, 6-2
HyperTerminal, 3-3, A-1

I

IGMP Configuration, 2-6, 4-59
IGMP クエリ, 2-6
IP アドレス, 3-1, 3-2, 4-31
 設定ツール, 3-2

J

Jabbers, 4-131

M

Max Age, 4-87
MD5, 4-103
MIB, 5-1
 MIB オブジェクト, 3, 6
 標準 MIB, 5-2
 プライベート MIB, 5-3

N

NCM PC, 3-3
NTP, 4-65

O

Oversize, 4-131

P

Path Cost, 4-90
Priority, 4-88
PROFINET IO, 6-1
 PROFINET IO 装置, 6-2

- R**
- Rapid Spanning Tree, 4-60
- Refresh, 4-6
- RFC
 - RFC 1213, 5-2
 - RFC 1286, 5-2
 - RFC 1518, 3-1
 - RFC 1519, 3-1
 - RFC 1724, 5-2
 - RFC 1757, 5-2
 - RFC 1850, 5-2
 - RFC 1907, 5-2
 - RFC 2233, 5-2
 - RFC 2571, 5-2
 - RFC 2572, 5-2
 - RFC 2573, 5-2
 - RFC 2574, 5-2
 - RFC 2575, 5-2
 - RFC 2665, 5-2
 - RFC 2674p, 5-2
 - RFC 2674q, 5-2
- RMON, 4-33
- S**
- Set Values, 4-6
- SHA のアルゴリズム, 4-42
- SICLOCK, 4-55
- SICLOCK クロック送信機, 2-5
- SMTP サーバ, 4-51
- SNMP, 4-37, 5-1
 - SNMPv1, 5-1
 - SNMPv2, 5-1
 - SNMPv3, 2-6, 5-1
 - SNMPv3 ユーザ, 4-44
 - SNMP トラップ, 4-39
- STEP 7, 3-2
- T**
- Telnet, 4-33
- TFTP サーバ, 4-13
- U**
- Undersize, 4-131
- Unicast Filter, 4-61
- V**
- VLAN, 2-4, 4-77
 - VLAN ID, 9
 - VLAN タグ, 8
- あ**
- アウトバンドポート, 2-1, 3-3
- アドレスのテーブル, 2-5
- アドレスのフィルタリング, 4-61
- アラームイベント, 4-51
- い**
- イーサネットポート, 2-1
- イベントログテーブル, 2-5
- インタフェース
 - RS-232 インタフェース, 2-1
 - アウトバンドポート, 2-1
 - イーサネットポート, 2-1
 - インバンドポート, 2-2
 - ギガビットイーサネットポート, 2-3
 - シリアルポート, 2-1, 1
 - ファストイーサネットポート, 2-1
- インバンドポート, 2-2, 3-3

う

ウェブ型管理ツール, 4-2, 8-1

え

エージングタイム, 4-59, 4-70

お

オートクロス, 2-2, 2-3

オートネゴシエーション, 4-124, 6-12

き

ギガビットイーサネットポート, 2-3

疑似ランプ, 4-5

さ

再起動, 4-11

サブネットマスク, 3-2, 4-32

し

時間帯, 4-55

時刻

SICLOCK, 2-5, 4-55

SNTP (Simple Network Time Protocol) , 4-54

時間帯, 4-55

時刻同期, 2-5

世界標準時, 4-55

同期, 4-54

時刻同期, 2-5

障害マスク, 4-25

冗長化

高速冗長化, 2-3

冗長化マネージャ, 2-3

冗長結合, 2-4

衝突, 4-131

す

ストア&フォワード, 2-4

スパニングツリー, 2-4, 4-60

高速スパニングツリー, 2-4, 4-85

スロットの機能, 6-12

せ

世界標準時, 4-55

そ

装置名, 6-7

て

データレート, 2-3

デジタル入力, 4-50

デフォルトゲートウェイ, 4-11, 4-34

電源モジュールの設定, 6-8

電子メール機能, 2-5, 4-33, 4-51

アラームイベント, 4-51

ラインの監視, 4-51

と

統計量, 4-128

動作モード

全二重, 2-2, 2-5

半二重, 2-2, 2-5

ぬ

ヌルモデムケーブル, 2-1, 3-3

ピン配置, A-1

は

ハードウェア構成, 6-6

ひ

ピン配置

ヌルモデムケーブル, A-1

ふ

ファームウェアアップデート, 8-1

フィルタ

アドレスのフィルタリング, 4-61

フィルタテーブル, 4-63

フィルタの設定, 4-63

フロー制御, 2-5

ほ

ポイントツーポイント, 4-85

ポート

アウトバンドポート, 3-3

インバンドポート, 2-2, 3-3

ポート設定, 4-124

ポート設定, 4-124

ポートのロック, 2-5

ま

マルチキャスト, 4-65

み

ミラーリング, 2-5, 4-58

め

メニュー構成, 4-3

ら

ラインの監視, 4-51

り

リングポート, 4-22

る

ルーティング

ルーティング機能, 2-2

レイヤ 3 機能, 2-7

れ

レイヤ 3 機能

ルーティング, 2-7

ルーティング機能, 2-2

ろ

ログイン, 3-3