Future X Communications

FXC9324XG Management Guide

基本設定

2014 年 2 月 Ver.1.0

FXC株式会社

本マニュアルについて

■ 本マニュアルでは、FXC9324XG の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI （コマンドラインインタフェース）または Web ブラウザで行います。

製品取り扱い時のご注意

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

- 煙が出たら
- 異常な音、においがしたら
- 内部に水・異物が入ったら
- 製品を高所から落としたり、破損したとき

①電源を切る（電源コードを抜く）
②接続ケーブルを抜く
③販売店に修理を依頼する

・下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。

● 電源ケーブルや接続ケーブルを傷つけない

・電源ケーブルを傷つけると火災や感電の原因となります。
・重いものをのせたり、引っ張ったりしない。
・加工したり、傷つけたりしない。
・熱器具の近くに配線したり、加熱したりしない。
・電源ケーブルを抜くときは、必ずプラグを持って抜く。

● 内部に水や異物を入れない

・火災や感電の原因となります。
・万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。

● 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。

● 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。

- 下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。

● 指定の電圧で使う

マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

- 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
- 毛足の長いジュウタンなどの上に直接設置しない。
- 布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

1. イントロダクション

1.1 主な機能

本機はレイヤ 2 スイッチングおよびレイヤ 3 ルーティングの、豊富な機能を提供します。

本機は管理エージェントを搭載し、各種設定を行うことができます。
ネットワーク環境に応じた適切な設定を行うことや、各種機能を有効に設定することで、機能を最大限に活用できます。

機能	解説
Configuration Backup and Restore	管理ステーション、または FTP/TFTP サーバを使用
Authentication	Console, Telnet, web ーユーザ名 / パスワード , RADIUS,TACACS+ Web ー HTTPS Telnet ー SSH SNMPv1/2c ーコミュニティ名 SNMPv3 ー MD5 、SHA パスワード Port ー IEEE802.1x 認証、MAC アドレスフィルタリング
General Security Measures	AAA ARP inspection DHCP Snooping (Option 82 リレー情報を含む) IP Source Guard Port Authentication – IEEE 802.1X Port Security – MAC address filtering
Access Control Lists	最大 256 の IP ACLs、96 の MAC/IP および IPv6 ルールをサポート
DHCP	クライアント、リレー、サーバー
DNS	クライアントおよびプロキシサービス
Port Configuration	スピード、通信方式、フローコントロール
Rate Limiting	ポートごとの入力・出力帯域制御
Port Mirroring	26 セッション、1 つの分析ポートに対する 1 つまたは複数ポートのミラーリング
Congestion Control	レート制限、ブロードキャストストーム用のスロットリング
Port Trunking	スイッチ単位最大 25 個までのトランクをサポート (スタック単位 :32) – スタティックまたはダイナミックトランキング (LACP)
Broadcast Storm Control	サポート
Address Table	最大登録可能 MAC アドレス数 16k、スタティック MAC アドレス 1024 ・ホストテーブルのエントリ数：IPv4- 最大 8K, IPv6- 最大 4K : ・ARP キャッシュ : 8K ・スタティック ARP: 256 ・IP ルーティングテーブル : IPv4(8K), IPv6(4K) ・スタティック IP ルート：512 ・IP インタフェース : 512 ・L2 マルチキャストグループ : 1024
IP Version 4 and 6	IPv4 および IPv6 アドレッシング、マネージメント、
IEEE802.1D Bridge	動的スイッチング及び MAC アドレス学習

Store-and-Forward Switching	ワイヤスピードスイッチングをサポートし、不良フレームを軽減
Virtual LANs	IEEE802.1Q タグ付 VLAN/ ポートベース VLAN/ プロトコルベース VLAN/ プライベート VLAN（最大 256 グループ）
Traffic Prioritization	ポートプライオリティ、トラフィッククラスマッピング、キュースケジューリング、DSCP、TCP/UDP ポート
Quality of Service	DiffServ サポート
Link Layer Discovery Protocol	ネイバー製品についての基本情報の検出に使用
Router Redundancy	VRRP(Virtual Router Redundancy Protocol) によるルータのバックアップ
IP ルーティング	Routing Information Protocol (RIP), Open Shortest Path First (OSPFv2/v3), スタティックルート、Equal-Cost Multipath Routing (ECMP)
ARP	静的、動的アドレス設定、プロキシ ARP サポート
Multicast Filtering	Layer 2 の IGMP スヌーピングおよびクエリ、Layer 3 の MLD スヌーピング、クエリおよび IGMP、マルチキャスト VLAN 登録
Multicast Routing	IPv4 用の PIM-DM および PIM-SM のサポート、IPv6 用 PIM-DM のサポート

1.2 ソフトウェア機能

本機は多くの機能を有し、それにより、効果的なネットワークの運用を実現します。
ここでは、本機の主要機能を紹介します。

設定のバックアップ及び復元

TFTP サーバを利用して現在の設定情報を保存することができます。
また、保存した設定情報を本機に復元することも可能です。

認証 /Authentication

本機はコンソール、Telnet、Web ブラウザ経由の管理アクセスに対する本機内又はリモート認証サーバ (RADIUS/TACACS+) によるユーザ名とパスワードベースでの認証を行います。また、Web ブラウザ経由では HTTPS を、Telnet 経由では SSH を利用した認証オプションも提供しています。

SNMP、Telnet、Web ブラウザでの管理アクセスに対しては IP アドレスフィルタリング機能も有しています。

各ポートに対しては IEEE802.1x 準拠のポートベース認証をサポートしています。本機能では、EAPOL(Extensible Authentication Protocol over LANs) を利用し、IEEE802.1x クライアントに対してユーザ名とパスワードを要求します。その後、認証サーバにおいてクライアントのネットワークへのアクセス権を確認します。

その他に、HTTPS によるセキュアなマネージメントアクセスや、Telnet アクセスを安全に行う SSH もサポートしています。また、各ポートへのアクセスには MAC アドレスフィルタリング機能も搭載しています。

ACL/Access Control Lists

ACL では IP アドレス、プロトコル、TCP/UDP ポート番号による IP フレームのフィルタリングもしくは、MAC アドレス、イーサネットタイプによるフレームのフィルタリングを提供します。ACL を使用することで、不要なネットワークトラフィックを抑制し、パフォーマンスを向上させることができます。

また、ネットワークリソースやプロトコルによるアクセスの制限を行うことでセキュリティのコントロールが行えます。

DHCP

DHCP サーバを使ってホストデバイスへの IP アドレスの割り当てを行います。DHCP はブロードキャスト方式を用いているため、DHCP サーバとそのクライアントは物理的に同じサブネット上でなければなりません。実際にはどのサブネット上にも DHCP サーバがないため、DHCP リレーをサポートしており異なるネットワークの DHCP サーバからローカルクライアントを動的に設定することも可能です。

ポート設定 /Port Configuration

本機ではオートネゴシエーション機能により対向機器に応じて各ポートの設定を自動的に行える他、手動で各ポートの通信速度、通信方式及びフローコントロールの設定を行うことができます。

通信方式を Full-Duplex にすることによりスイッチ間の通信速度を 2 倍にすることができます。IEEE802.3x に準拠したフローコントロール機能では通信のコントロールを行い、パケットバッファを越えるパケットの損失を防ぎます。

帯域制御 /Rate Limiting

各インタフェースにおいて送信及び受信の最大帯域の設定を行うことができます。設定範囲内のパケットは転送されますが、設定した値を超えたパケットは転送されずにパケットが落とされます。

ポートミラーリング /Port Mirroring

本機は任意のポートからモニターポートに対して通信のミラーリングを行うことができます。ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、トラフィックを解析することができます。

ポートトランク /Port Trunking

複数のポートをバンド幅の拡大によるボトルネックの解消や、障害時の冗長化を行うことができます。本機で手動及び IEEE802.3ad 準拠の LACP を使用した動的設定で行うことができます。

本機では最大 32 グループのトランクをサポートしています。

ブロードキャストストームコントロール /Broadcast Storm Control

ブロードキャストストームコントロール機能は、ブロードキャスト通信によりネットワークの帯域が占有されることを防ぎます。ポート上で本機能を有効にした場合、ポートを通過するブロードキャストパケットを制限することができます。ブロードキャストパケットが設定しているしきい値を超えた場合、しきい値以下となるよう制限を行います。

静的アドレス /Static Addresses

特定のポートに対して静的な MAC アドレスの設定を行うことができます。設定された MAC アドレスはポートに対して固定され、他のポートに移動することはできません。設定された MAC アドレスの機器が他のポートに接続された場合、MAC アドレスは無視され、アドレステーブル上に学習されません。

静的 MAC アドレスの設定を行うことにより、指定のポートに接続される機器を制限し、ネットワークのセキュリティを提供します。

IP アドレスのフィルタリング /IP ADDRESS FILTERING

スタティックアドレスは、本機の特定のインタフェースへの割り当てが可能です。指定のインタフェースにスタティックアドレスを割り当てると変更することはできません。スタティックアドレスを他のインタフェースに割り当てると、そのアドレスは無視され、アドレステーブルへの書き込みも行われません。スタティックアドレスを用いて、特定ポートへの認識されたホストのアクセスを規制することによりネットワークのセキュリティを行います。

IEEE802.1D ブリッジ /IEEE 802.1D Bridge

本機では IEEE802.1D ブリッジ機能をサポートします。

MAC アドレステーブル上で MAC アドレスの学習を行い、その情報に基づきパケットの転送を行います。本機では最大 8K 個の MAC アドレスの登録を行うことが可能です。

ストア & フォワード スイッチング /Store-and Forward Switching

本機ではスイッチング方式としてストア＆フォワードをサポートします。

本機では 2Mbit のバッファを有し、フレームをバッファにコピーをした後、他のポートに対して転送します。これによりフレームがイーサネット規格に準拠しているかを確認し、規格外のフレームによる帯域の占有を回避します。また、バッファにより通信が集中した場合のパケットのキューイングも行います。

スパニングツリーアリゴリズム /

STP では、分散アルゴリズムを使用して、スパニングツリーネットワークのルートとして機能するブリッジングデバイス（STP 対応のスイッチ、ブリッジ、またはルータ）を選択します。それぞれのブリッジングデバイス（ルートデバイス以外）からルートデバイスにパケットを転送する際にそのデバイスで最小パスコストを実現するルートポートが選択されます。それから、それぞれの LAN からルートデバイスにパケットを転送する際にその LAN で最小パスコストを実現する代表ブリッジングデバイスが選択されます。代表ブリッジングデバイスに接続されているすべてのポートが代表ポートとして割り当てられます。最小コストのスパニングツリーが判別されると、すべてのルートポートと代表ポートが有効になり、その他のすべてのポートが無効になります。そのため、ネットワークパケットがルートポートと代表ポートの間でのみ転送されるようになり、想定されるあらゆるネットワークループが回避されます。

- Spanning Tree Protocol (STP, IEEE 802.1D) – このプロトコルは、ループ検知を行います。セグメント間に物理パスが複数ある場合は、このプロトコルはパスを 1 つ選択し、それ以外のパスは無効にして、ネットワーク上の 2 つのステーション間に存在するルートは 1 つのみです。これにより、ネットワークのループを回避されます。選択したパスが何らかの理由で失敗した場合は、代替パスが有効と有効となり接続は継続されます。

- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – STP よりも極めて速やかに再設定を実現します（STP が 30 秒以上であるのに対し、RSTP は 1 ～ 3 秒）。

- 802.1D STP 規格。これは STP の代替機能を目的としています。STP プロトコルメッセージを接続先のデバイスから検出すると、ポートを自動的に STP 対応モードに再設定することにより、古い規格で動作しているスイッチとの相互接続を行うことが可能です。

- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – VLAN グループに基づく独立したスパニングツリーをサポートすることを目的としています。複数のスパニングツリーを使用することで、複数の転送パスを提供し、負荷分散を実現できるようになります。1 つまたは複数の VLAN をグループ化してマルチプルスパニングツリーインスタンス（MSTI: Multiple Spanning Tree Instance）も設定することも可能です。MSTP では、インスタンスごとに別々のマルチプルスパニングツリー（MST: Multiple Spanning Tree）を構築して、割り当てられている各 VLAN グループ間の接続性を維持します。さらに、MSTP では、通常設定されているすべての MSTP を含む領域の内部スパニングツリー（IST: Internal Spanning Tree）が構築されます。

VLAN/Virtual LANs

本機は最大 4,093 グループの VLAN をサポートしています。VLAN は物理的な接続に関わらず同一のコリジョンドメインを共有するネットワークノードとなります。

本機では IEEE802.1Q 準拠のタグ付 VLAN をサポートしています。VLAN グループメンバーは GVRP を利用した動的な設定及び手動での VLAN 設定を行うことができます。VLAN の設定を行うことにより指定した通信の制限を行うことができます。

VLAN によりセグメントを分ける事で以下のようなメリットがあります。

- 細かいネットワークセグメントにすることによりブロードキャストストームによるパフォーマンスの悪化を回避します。
- 物理的なネットワーク構成に関わりなく、VLAN の設定を変更することでネットワークの構成を簡単に変更することが可能です。
- 通信を VLAN 内に制限することでセキュリティが向上します。
- プライベート VLAN を利用することにより設定可能な VLAN 数に制限がある中で、同一 VLAN 内の各ポート間の通信を制限し、アップリンクポートとの通信のみを行うことが可能となります。
- プロトコルベース VLAN により、プロトコルタイプに基づいたトラフィックの制限を行うことが可能です。

IEEE 802.1Q トンネリング (QINQ)

自社のネットワークで複数の顧客のトラフィックを伝播するサービスプロバイダを対象としています。QinQ トンネリングを使用して、異なる顧客が同じ内部 VLAN ID を使用する場合でも顧客固有の VLAN およびレイヤ 2 プロトコルの設定が保持されるようにします。そのようなことを実現するため、顧客のフレームがサービスプロバイダのネットワークに入るときに SPVLAN（Service Provider VLAN）タグを挿入し、フレームがネットワークを出るときに SPVLAN タグを取り除きます。

プライオリティ /Traffic Prioritization

本機では 4 段階のキューと Strict 又は WRR キューイング機能によりサービスレベルに応じた各パケットに優先順位を設定することができます。これらは、入力されるデータの IEEE802.1p 及び 802.1Q タグにより優先順位付けが行われます。

本機能により、アプリケーション毎に要求される優先度を個別に設定することができます。

また、本機では IP フレーム上の ToS オクテット内のプライオリティビットを利用した優先順位の設定など、いくつかの方法により L3/L4 レベルでの優先順位の設定も行うことができます。

QoS(QUALITY OFSERVICE)

DiffServ（Differentiated Services）は、ホップ単位で個々のトラフィックタイプの要件を満たすことができるようにネットワークリソースの優先度を設定するためのポリシーベースの管理方式を提供します。それぞれのパケットは、ネットワークに入るときに、アクセスリスト、IP 優先順位、DSCP 値、または VLAN リストに基づいて分類されます。アクセスリストを使用すると、各パケットに含まれているレイヤ 2、レイヤ 3、またはレイヤ 4 情報に基づいてトラフィックを選択できるようになります。設定されているネットワークポリシーに基づき、各種のトラフィックを転送方法別にマーキングすることができます。

IP ルーティング /IP ROUTING

レイヤ 3 の IP ルーティングを行います。高速のスループットを確保するために、同一のセグメント上のトラフィックをすべて転送し、異なるサブネット間のトラフィックのみルーティングを行います。ワイヤースピードのルーティングにより、ボトルネックの問題や従来のルータに関連のある設定上の問題もなく、ネットワークセグメントを簡単にリンクしたり、VLAN を設定することが可能です。スタティックルーティングでサポートされているユニキャストトラフィックのルーティングは、RIP(Routing Information Protocol) および OSPF(Open Shortest Path First) です。

- Static Routing – トラフィックは、本機で設定されている IP インタフェース間で自動的にルーティングを行います。静的に設定されているホスト、またはサブネットアドレスは、スタティックルーティングテーブルで指定されている next-hop エントリに応じてルーティングされます。

- RIP – このプロトコルは、距離ベクトル方式を用いてルーティングを行います。ルーティングは、距離ベクトル、ホップ数を最小化して決定され、通信コストを大まかに見積もる役割を行います。

- OSPF – この方式は、リンクステートルーティングプロトコルを用いて最短パスツリーを生成し、このツリーに応じてルーティングテーブルを構築します。この方式では、リンクステートルーティングプロトコルを使用して、ショートパスを設定して、ツリーに応じてルーティングテーブルを構築します。ルータが増えると、ネットワークの変更に瞬時に対応するため、RIP よりもより早く最適なルーティングを設定します。OSPFv2 は IPv4 用のトラフィック、OSPFv3 は IPv6 用のトラフィックのルーティングを行います。

イコールコストマルチパスロードバランス /EQUAL-COST MULTIPATH LOAD BALANCING

同じ宛先に対するパスコストが等価である複数のパスがルーティングテーブルで検出されると、ECMP によりまずコストがルーティングテーブル内のエントリ内で一番低いかどうかチェックされます。コストがテーブル内のエントリで一番低い場合は、スイッチはコストが同じ最大 8 つまでのパスを使用して、宛先に転送されるトラフィックの負荷を分散させます。ECMP では、スタティックルーティングテーブルで手動で設定されるイコールコストマルチパスと OSPF（Open Shortest Path First）アルゴリズムによって動的に生成されるイコールマルチパスのいずれかが使用されます。つまり、スタティックエントリと OSPF エントリのいずれかが使用され、両方が使用されることはありません。

ルータ冗長 /ROUTER REDUNDANCY

ルータ冗長プロトコル (VRRP) は、仮想 IP アドレスを使用して、1 つのプライマリルータと複数のバックボーンルータをサポートします。バックアップルータは、マスタルータで障害が発生した場合にワークロードを引き継ぐように設定したり、トラフィックの負荷を共有するように設定したりすることができます。ルータ冗長化の主要な目的は、固定ゲートウェイを指定して設定されたホストデバイスが、プライマリゲートウェイがダウンした場合にネットワークの接続性を保持できるようにすることです。

アドレス解決プロトコル / ADDRESS RESOLUTION PROTOCOL

本機では、ARP および Proxy ARP を用いて IP アドレスと MAC(ハードウェア）アドレス間の変換を行います。IP ルーティングが有効になっている場合、ルータは、自らのルーティングテーブルを使用してルートを決定し、アドレス解決プロトコル（ARP: Address Resolution Protocol）を使用してワンホップ手前のルータからのトラフィックを次のルータに転送します。ARP は、IP アドレスを物理レイヤ（つまり、MAC）アドレスにマップするために使用されます。ルータ（または、何らかの標準ベースのルータ）は、IP フレームを受信すると、最初に、宛先アドレスに対応する MAC アドレスを ARP キャッシュで検索します。MAC アドレスが見つかると、ルータは、その MAC アドレスをフレームヘッダ内の該当のフィールドに書き込み、そのフレームをネクストホップに転送します。パケットが最終的な宛先に配信されるまで、それぞれのルーティングデバイスが宛先 IP アドレスを受信先方向のネクストホップの MAC アドレスにマップするという方法で、IP トラフィックが最終的な宛先へのパスに沿って渡されます。

マルチキャストフィルタリング /Multicast Filtering

正常なネットワークの通信に影響させず、リアルタイムでの通信を確保するために、VLAN のプライオリティレベルを設定し、マルチキャスト通信を特定し各 VLAN に対して割り当てることができます。

本機では IGMP Snooping 及び Query を利用し、マルチキャストグループの登録を管理します。

マルチキャストルーティング /MULTICAST ROUTING

本製品は、IPv4 PIM-DM または PIM-SM（Protocol-Independent Multicasting - Dense Mode または Sparse Mode）だけでなく、IPv6 PIM-DM を使用して、マルチキャストトラフィックを別々のサブネットワークにルーティングすることができます。IPv4 PIM（本書では PIMv4 とも記述）では、IGMP 対応レイヤ 2 スイッチおよびホストから送信されるメッセージに依存して、ホストがマルチキャストグループに対する加入または脱退を希望しているかどうかが判別されます。IPv6 PIM（本書では PIMv6 とも記述）では、IPv6 と同等の IGMPv2 である MLDv1（Multicast Listener Discovery）を使用します。PIM-DM は、ローカルネットワークなどのように、マルチキャストグループメンバーを使用する可能性が高いネットワークを対象としています。PIM-DM は、インターネットなどのように、マルチキャストグループメンバーを使用する可能性が低いネットワークを対象としています。

また、本製品で PIM が有効になっていない場合や、ネットワークで他のマルチキャストルーティングプロトコルが使用されている場合は、マルチキャストルータに接続されているスイッチポートを、マルチキャストトラフィックを転送するように設定することができます（「マルチキャストルータのスタティックインターフェースの指定」を参照）。

1.3 初期設定

本機の初期設定は設定ファイル "Factory_Default_Config.cfg" に保存されています。
本機を初期設定にリセットするためには、"Factory_Default_Config.cfg" を起動設定ファイルとします。

基本的な設定項目の初期設定は以下の表の通りです。

機能	パラメータ	初期設定
Console Port Connection	Baund Rate	115200bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0(disabled)
Authentication and Security Measures	Privileged Exec Level	Username”admin” Password”admin”
	Normal Exec Level	Username”guest” Password”guest”
	Enable Privileged Exec from Normal Exec Level	Password”super”
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Redirect	Disabled
SNMP	SNMP Agent	Enabled
	Community Strings	“public“(read only) “private“(read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View:default view Group:public(read only) private(read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP(all ports)	Disabled

Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (500 packets/sec)
Address Table	Aging Time	300seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode(Egress mode)	Hybrid:tagged/untagged frames
	GVRP(global)	Disabled
	GVRP(port interface)	Disabled
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Weighted Round Robin	Queue:0 1 2 3 4 5 6 7 Weight:1 2 4 6 8 10 12 14
	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	DHCP assigned
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled Relay:Disabled Server:Disabled
	DNS	Client/Proxy:Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout:20 minutes Proxy:Disabled
Unicast Routing	RIP	Disabled
	OSPFv2	Disabled
	OSPFv3	Disabled
Router Redundancy	VRRP	Disabled

Multicast Filtering	IGMP Snooping (Layer 2)	Snooping:Enabled Querier:Disabled
	MLD Snooping (Layer 2 IPv6)	Snooping: Enabled Querier: Disabled
	Multicast VLAN Registration	Disabled
	IGMP (Layer 3) IGMP Proxy (Layer 3	Disabled Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled(but no server defined)
SNTP	Clock Synchronization	Disabled

2. 本機の管理

2.1 本機への接続

2.1.1 設定方法

本機は、ネットワーク管理エージェントを搭載し SNMP、RMON よるネットワーク経由での管理を行うことができます。また、PC から本機に直接接続しコマンドラインインタフェース (Command Line Interface/CLI) を利用した設定及び監視を行うことも可能です。

[注意] 初期設定状態では、DHCP サーバーよる IP アドレスの取得を行うよう設定されています。この設定の変更を行う場合は 2.3.3 項「IP アドレスの設定」を参照して下さい。

設定オプション

本機の CLI へは本体のコンソールポートへの接続及びネットワーク経由での Telnet による接続によりアクセスすることができます。

対応の WEB ブラウザは Internet Explorer 5.x 以上または Netscape Navigator 6.2 以上または Mozilla Firefox 2.0.0.0 以上です。

本機には SNMP (Simple Network Management Protocol) に対応した管理エージェントが搭載されています。ネットワークに接続されたシステムで動作する、SNMP に対応した管理ソフトから、本機の SNMP エージェントにアクセスし設定などを行うことが可能です。

本機の CLI、WEB インタフェース及び SNMP エージェントからは以下の設定を行うことが可能です。

- ユーザ名、パスワードの設定
- 管理 VLAN の IP インタフェースの設定
- SNMP パラメータの設定
- 各ポートの有効 / 無効
- 各ポートの通信速度及び Full/Half Duplex の設定
- 帯域制御による各ポートの入力及び出力帯域の設定
- IEEE 802.1X セキュリティ、あるいはスタティックアドレスフィルタリングを介したポートアクセスの制御
- ACLs(Access Control Lists) を介したパケットのフィルタリング
- IEEE802.1Q 準拠のタグ付 VLAN (最大 4093 グループ) の設定
- GVRP 自動 VLAN 登録の有効化
- IGMP マルチキャストフィルタリング設定
- HTTP(WEB インタフェース使用)、FTP/TFTP(コマンドライン、または WEB インタフェース）経由のファームウェアのアップロード及びダウンロード

- スパニングツリーの設定
- Class of Service (CoS) プライオリティキューの設定
- 静的トランク及び LACP 設定
- ポートミラーリングの有効化
- 過剰なブロードキャストトラフィックのポートのストームコントロールの設定
- システム情報及び統計情報の表示
- 同じ IP アドレスによるスタックユニットの設定

2.1.2 接続手順

本機のシリアルポートと PC を RS-232C ケーブルを用いて接続し、本機の設定及び監視を行うことができます。

PC 側では VT100 準拠のターミナルソフトウェアを利用して下さい。PC を接続するための RS-232C ケーブルは、本機に同梱されているケーブルを使用して下さい。

[注意] スタックを設定している場合には、マスターユニットのコンソールポートへ接続をしてください。

手順 :

（1）RS-232C ケーブルの一方を PC のシリアルポートに接続し、コネクタ部分のねじを外れないように止めます。

（2）RS-232C ケーブルのもう一方を本機のコンソールポートに接続します。

（3）パソコンのターミナルソフトウェアの設定を以下の通り行ってください。

通信ポート ---------- RS-232C ケーブルが接続されているポート
(COM ポートは PC に依存します。)
通信速度 ---------- 9600 ～ 115200 ボー (baud)
データビット -------- 8bit
ストップビット ----- 1bit
パリティ ---------- なし
フロー制御 ---------- なし
エミュレーション -- VT100

[注意] HyperTerminal をご使用になる場合は、Windows キーではなくて、Terminal キーを選択してください。

（4）上記の手順が正しく完了すると、コンソールログイン画面が表示されます。

[注意] コンソール接続に関する設定、および CLI による設定方法の詳細については、別紙の『CLI 設定』マニュアルを参照して下さい。

2.1.3 リモート接続

ネットワークを経由して本機にアクセスする場合は、事前にコンソール接続又は DHCP、BOOTP により本機の IP アドレス、サブネットマスク、デフォルトゲートウェイを設定する必要があります。

本機の IPv4 アドレスは、デフォルト設定では DHCP を介して取得します。手動で IP アドレスの設定を行う場合の設定方法は P20 「IP アドレスの設定」を参照して下さい。

[注意] 本機は同時に最大 8 セッションまでの Telnet 接続が行えます。IP アドレスの設定が完了すると、ネットワーク上のどの PC からも本機にアクセスすることができます。PC 上からは Telnet、WEB ブラウザ、ネットワーク管理ソフトを使うことにより本機にアクセスすることができます。

[注意] VLAN グループには本機の管理用に IP インタフェースのアドレスの設定が可能です。マスターユニットには管理アクセス用の VLAN インタフェースのポートメンバは含まれません。

本機の IP パラメータを設定すると、接続先のネットワークからプログラムにアクセスすることが可能です。ネットワークに接続されているパソコンから Telnet を使ってアクセス可能です。本機は、WEB ブラウザ（**WEB ブラウザは Internet Explorer 5.x 以上または Netscape Navigator 6.2 以上または Mozilla Firefox 2.0.0.0 以上**）、SNMP ネットワーク管理ソフトウェアを使ってパソコンより管理することも可能です。

搭載されているプログラムは基本設定機能への アクセスのみ可能です。すべての SNMP 管理機能にアクセスするには、SNMP 対応ネットワーク管理ソフトウェアを使用する必要があります。

2.2 スタック設定

インストレーションガイドに記載のとおり、本機でスタック可能な台数は 8 台までです。スタック内の 1 台が設定用タスクおよびファームウェアのアップデートを行うマスターとして機能します。その他のユニットについてはすべてスレーブモードとして機能し、マスターが失敗した場合にその管理機能を自動的に引き継ぎます。

スタック内のユニットを設定するには、本機の前面にあるユニット番号を確認して、WEB またはコンソール管理用インタフェースから適切なユニット番号を選択してください。

2.2.1 スタックマスタの選択

[注意] ユニットのナンバリングを行う場合には、以下の点に注意してください。

- マスターユニットはスタックの電源を最初に投入する際、以下のルールに応じてマスターユニットを選択します。
  - スタック内のユニットの 1 つの「 Master Select 」ボタンを押す場合は、ユニットはスタックマスターとして機能します。
  - 複数のユニットの「Master Select」ボタンを押す場合は、スタックマスターのボタンを押されたユニット中から、システムは最下位の MAC アドレスをもつユニットをスタックマスターとして選択されます。
  - いずれかのユニットの「Master Select」ボタンを押す場合は、システムは最下位の MAC アドレスをもつユニットをスタックマスターとして選択されます。
- スタックの電源を最初に投入する際、マスターユニットは、リングトポロジの場合は ”unit 1” として設定され、ライントポロジの場合は単純に上から順番にナンバリングされ、最初のユニットが ”unit 1” となります。このユニットの識別番号は、本機の前面にある Stack Unit ID LED で表示されます。WEB インタフェースでは画面上から、CLI でもそれぞれ選択することが可能です。
- マスターユニットに障害が生じて、他のユニットによりスタックの機能が引き継がれる場合、ユニット番号はそのまま変更されません。
- スタック内のユニットに障害が生じたり、スタックからユニットを取り外す場合は、ユニット番号はそのまま変更しません。スタック内のユニットを取り換えても、障害のあるユニットの元の設定値は新たに交換後のユニットに復元されます。
- ユニットを一旦取り外した後にスタックに再度取り付けた場合、スタックした際に設定されたユニット番号のまま変更されません。
- スタックからユニットを取り外して、スタンドアロンユニットとして電源を「On」にすると、スタックした際に設定されたユニット番号のまま変更されません。

2.2.2 バックアップユニットの選択

マスターユニットを起動すると、スタック内のスレーブユニットすべての設定情報の同期化を継続します。マスターユニットに障害が起きたり、電源が落ちると、新しいマスターユニットが先述した選択ルールに応じて選択されます。選択されたバックアップユニットは新しいスタックマスターとして設定情報をすべて引き継ぎます。スタック内の論理上ダウンしたユニットかどうかを確認するには、スタック内のマスターユニットの次に最下位の MAC アドレスをスレーブユニットに設定します。

2.2.3 スタック障害、あるいはトポロジーの変更のリカバリ

スタック内のリンクまたはユニットに障害が生じた場合、trap メッセージが送信され、障害のあるイベントは記録されます。スタックはシステム障害、またはトポロジーの変更が生じるとリブートします。マスターユニットに障害が生じた場合は、バックアップユニットが新規マスターユニットとして全てのオペレーションを継承し、スタックのリブートが終わると、別のバックアップユニットが選ばれます。電源の問題によりユニットをスタックから取り外したり、新しいユニットをスタックに追加する場合は、当初のユニット ID はリブート後もそのままで、新しいユニットには最下位のユニット ID が割り当てられます。

回線および WRAP-AROUND トポロジのリンクが切れた場合

スタック内のユニットはすべてスタックケーブルを介して接続してください。単に上から順番にカースケード接続を行ってもユニットの接続は可能です。スタック内のリンクまたはユニットに障害が生じた場合は、このライントポロジを使って、スタックを 2 分割します。スタック内で障害の起こる可能性のあるユニットからのトラフィックを受信しなくなると、そのユニットの Stack Link LED がフラッシュを開始してスタックリンクが切れたことを知らせます。

スタックに失敗すると、どのユニットの Master ボタンを押さない場合は、Master ボタンをもつユニットか、最下位の MAC アドレスをもつユニットマスターユニットが 2 つのスタックセグメントから選択されます。スタックはリブートし、オペレーションを再開しますが、新規のスタックセグメントの両方に表示される共有の VLAN の IP アドレスが同じであることを確認してください。IP アドレスの競合の問題を回避するには、失敗したリンクまたはユニットを手動で設定し直す必要があります。

wrap-around スタックトポロジーを使用する場合は、SPOF（単一障害）により、スタック全体に障害が生じることはありません。

[注意] スタックが無効の場合は、両方のスタックセグメントの共有の VLAN（有効なポート接続をもつ）に対して同じ IP アドレスを設定してください。

管理アクセスの IP インタフェースの復活

スタック機能は管理および設定用の自律システムの 1 つです。スタックに設定された IP インタフェースを介してスタックを管理することが可能です。マスターには管理用アクセスに使用する VLAN インタフェースの有効なポートメンバを含まれません。ただし、管理用アクセスに接続するユニットに障害が生じたり、VLAN インタフェース内のその他のユニット上に有効なポートメンバーがない場合は、IP アドレスは使用できません。管理用アクセスの IP アドレスをそのままご使用になりたい場合は、スタック管理用のプライマリ VLAN のユニットにポートメンバーを設定する必要があります。

設定の回復

スタック内のユニットに障害が生じた場合、ユニット番号はそのまま使用されます。スタック内のユニットを交換した場合は、ユニットの設定は新しく交換されたユニットにリストアされます。これはマスターユニットにもスレーブユニットにも適用されます。

2.2.4 スタックの番号の変更

起動用の設定ファイルは、ユニット識別番号に応じてスタック内の各ユニットに設定値をマッピングします。トポロジーの変更や失敗が生じた後にナンバリングを行わない場合は、WEB インタフェース、または CLI の “Renumbering” コマンドを使用してユニット番号をリセットすることができます。その場合は、スタックマスターの電源を落とす前に、新しい設定値を起動用設定ファイルに保存してください。

2.2.5 スタックで使用するコードの確認

Consistent Runtime Code in Each Switch – スタック内のそれぞれのユニットのメインボードで動作しているファームウェアのバージョンをマスターユニットと同じバージョンにしてください。Auto-ID の割り当てが完了した後、マスターユニットはファームウェアのバージョンが同じかどうかを確認します。スレーブユニットの起動用に設定されているファームウェアのバージョン (runtime code など）がマスターユニットと異なる場合は、スタックは特殊なスタックモードとなり、バックアップユニットは以下の場合に無効になります。

- マスターユニットは、スタンドアロンで通常動作を開始します。
- マスターユニットは、スタック内のユニットをすべて確認し、スタックトポロジーを継続します。
- それ以外のユニットはすべて機能不可となります（すべてのポートは無効です)。
- 無効なユニットを設定するための user-initiated コマンドはすべて破棄されますが、マスターユニットは無効なユニットに対して以下の情報を通信することが可能です。
    - イメージのダウンロード
    - スタックトポロジー情報
    - システム設定情報がマスタにすでにストアされている場合

Special Stacking モードでは、CLI を介してシステムにログインすると警告メッセージが表示され、ファームウェアのダウンロードが必要である旨通知されます。CLI、WEB, あるいは SNMP を使用して、TFTP サーバからマスターユニットにランタイムファームウェアをダウンロードすることが可能です。マスターユニットは、“Next boot image” としてファームウェアをストアし、異なるファームウェアのバージョンが動作するバックアップユニットにそのファームウェアをダウンロードします。ファームウェアのダウンロード方法の詳細については、P30 「システムファイルの管理」を参照してください。

2.3 基本設定

2.3.1 コンソール接続

CLI ではゲストモード (normal access level/Normal Exec) と管理者モード (privileged access level/Privileged Exec) の 2 つの異なるコマンドレベルがあります。ゲストモード (Normal Exec) を利用した場合、利用できる機能は本機の設定情報などの表示と一部の設定のみに制限されます。本機のすべての設定を行うためには管理者モード (Privileged Exec) を利用し CLI にアクセスする必要があります。

2 つの異なるコマンドレベルは、ユーザ名とパスワードによって区別されています。初期設定ではそれぞれに異なるユーザ名とパスワードが設定されています。

管理者モード (Privileged Exec) の初期設定のユーザ名とパスワードを利用した接続方法は以下の通りです。

（1）コンソール接続を初期化し、<Enter> キーを押します。ユーザ認証が開始されます。

（2）ユーザ名入力画面で "admin" と入力します。

（3）パスワード入力画面で "admin" と入力します。
(入力したパスワードは画面に表示されません)

（4）管理者モード (Privileged Exec) でのアクセスが許可され、画面上に "Console#" と表示が行われます。

2.3.2 パスワードの設定

[注意] 安全のため、最初に CLI にログインした際に "username" コマンドを用いて両方のアクセスレベルのパスワードを変更するようにしてください。

パスワードは最大 8 文字の英数字です。大文字と小文字は区別されます。

パスワードの設定方法は以下の通りです。

（1）コンソールにアクセスし、初期設定のユーザ名とパスワード "admin" を入力して管理者モード (Privileged Exec) でログインします。

（2）"configure" と入力し <Enter> キーを押します。

（3）"username guest password 0 password" と入力し、<Enter> キーを押します。
”Password” 部分には新しいパスワードを入力します。

（4）"username admin password 0 password" と入力し、<Enter> キーを押します。
”Password” 部分には新しいパスワードを入力します。

[注意] "0" は平文パスワード、"7" は暗号化されたパスワードを入力します。

```
Username: admin
Password:

      CLI session with the FXC 10/100/1000 is opened.
      To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

2.3.3 IP アドレスの設定

本機の管理機能にネットワーク経由でアクセスするためには、IP アドレスを設定する必要があります。

IP アドレスの設定は下記のどちらかの方法で行うことができます。

手動による設定

- IP アドレスとサブネットマスクを手動で入力し、設定を行います。本機に接続する PC が同じサブネット上にない場合には、デフォルトゲートウェイの設定も行う必要があります。

動的設定

- ネットワーク上のBOOTP又はDHCPアドレスアロケーションサーバにIPv4設定リクエストを送信します。複数のサブネットを含むローカルネットワークで使用する IPv6 グローバルユニキャストアドレスには手動でのみ設定可能です。詳細については、

- ネットワーク上の BOOTP 又は DHCP サーバに対し､IP アドレスのリクエストを行い自動的に IP アドレスを取得します。有効な IPv4 アドレスは、0 ～ 255 までの 4 桁の 10 進数で、ピリオドを使用して区切られた表記です。このフォーマット以外については、CLI プログラムでは対応不可です。

手動による設定

IP アドレスを手動で設定します。セグメントの異なる PC から本機にアクセスするためにはデフォルトゲートウェイの設定も必要となります。

[注意] IPv4 アドレスは、デフォルト設定では DHCP により入手します。

IPv4 アドレスの割り当て

IPv4 アドレスの設定を行う前に、必要な下記の情報をネットワーク管理者から取得して下さい。

- （本機に設定する）IP アドレス
- デフォルトゲートウェイ
- サブネットマスク

IPv4 アドレスを設定するための手順は以下の通りです。

（1）interface モードにアクセスするために、管理者モード (Privileged Exec) で "interface vlan 1" と入力し、<Enter> キーを押します。

（2）"ip address *ip-address netmask*" と入力し、<Enter> キーを押します。
"*ip-address*" には本機の IP アドレスを、"*netmask*" にはネットワークのサブネットマスクを入力し、<Enter> キーを押します。

（3）Global Configuration モードに戻るために、"exit" と入力し、<Enter> キーを押します。

（4）本機の所属するネットワークのデフォルトゲートウェイの IP アドレスを設定するために、"ip default-gateway *gateway*" と入力し、<Enter> キーを押します。
"*gateway*" にはデフォルトゲートウェイの IP アドレスを入力します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

IPv6 アドレスの設定

ここでは、マルチセグメントネットワーク上で使用するネットワークプレフィックスおよびアドレスのホスト部分など、ローカルサブネット内の接続用の “link local” の設定方法、“global unicast” アドレスの設定方法について説明します。

IPv6 プレフィックス、あるいはアドレスは 8 桁の 16 bits の 16 進数値を使用して、RFC 2373 の ”IPv6 Addressing Architecture” に応じてフォーマット化する必要があります。アドレスでダブルコロンを 1 つ使用して、未定義フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。そ

Link Local Address — リンクローカルアドレスはすべて FE80~FEBF のプレフィックスで設定してください。このアドレスタイプにより、同一のローカルサブネットの接続先のデバイスに対して IPv6 を介してアクセス可能です。

また、ユーザにより設定したアドレスがサブネット上の別のデバイスで使用中のアドレスとの競合を検出した場合は、該当のアドレスの使用は中断され、ローカルサブネット上の他のデバイスとの競合のないリンクローカルアドレスが自動的に設定されます。その他の IPv6 アドレスの設定方法の詳細については、別紙の『WEB 設定』マニュアルに記載されている「1.14.2 スイッチの IP アドレスの設定（IPv6）」を参照して下さい。

IPv6 アドレスを設定するための手順は以下の通りです。

（1）Global Configuration モードから、“interface vlan 1” と入力して、インタフェース設定モードにアクセスし、<Enter> キーを押します。

（2）以下の画面のように、“ipv6 address” の後に続けて、ipv6 アドレスの 8 桁の 16 ビットの 16 進数値を入力し、その後に ” link-local” コマンドのパラメータを入力し、<Enter> キーを押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF11:6700/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

動的設定

IPv4 アドレスの入手方法

“bootp”、または “dhcp” オプションを使用すると システムはサービスリクエストのブロードキャストを直ちに開始します。IP は有効になりますが、BOOTP または DHCP による応答を受信するまで無効の状態となります。BOOTP または DHCP サーバから IP 設定情報を入手するまで再送 時間算出法を介して数分ごとにリクエストをブロードキャストします。BOOTP および DHCP の値には、IP アドレス、サブネットマスク、デフォルトゲートウェイが含まれます。

DHCP/BOOT サーバの応答が遅い場合、“ip dhcp restart client” コマンドを使用してサービスリクエストのブロードキャストを再開しなければならない場合があります。

[注意]　“ip dhcp restart client” コマンドを使用して、設定されているすべての VLAN のサービスリクエストのブロードキャストを開始して、BOOTP または DHCP を介してアドレスの設定を行うことも可能です。DHCP が VLAN 上に設定されている場合は、このコマンドを使用する必要がある場合があるため、すでにシャットダウンされているメンバーポートは有効になります。

“bootp” 、または “dhcp” オプションを startup-config ファイルに保存する場合 (手順 6)、本機は電源を「ON」にすると同時にサービスリクエストのブロードキャストを開始します。

ネットワーク上の BOOTP、または DHCP アドレス割り当てサーバとの通信により本機を自動的に設定するには、以下の手順に従ってください。

（1）インタフェース設定モードにアクセスするために、Global Configuration モードで “interface vlan 1” と入力して、<Enter> キーを押します。

（2）インタフェース設定モードでは、以下のコマンドのいずれかを使用してください。

- DHCP を介して IP 設定を行うには、“ip address dhcp” と入力し、<Enter> キーを押します。
- BOOTP を介して IP 設定を行うには、“ip address bootp” と入力して <Enter> キーを押します。

（3）“end” と入力して、Privileged Exec モードに戻り、<Enter> キーを押します。

（4）数分後、“show ip interface” コマンドを入力して IP 設定が完了していることを確認し、<Enter> キーを押します。

（5）“copy running-config” を入力して、設定の変更を保存します。起動用ファイル名を入力して、<Enter> キーを押します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
Address is 00-00-E8-93-82-A0
Index: 1002, MTU: 1500
Address Mode is DHCP
IP Address: 192.168.0.2 Mask: 255.255.255.0
Proxy ARP is disabled
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.
\Write to FLASH finish.
Success.
```

IPv6 アドレスの入手方法

Link Local Address - IPv6 アドレスの設定にはいくつかの方法があります。最も簡単な方法は、“link local” アドレス (FE80 のプレフィックスにより識別) を自動的に設定する方法です。このアドレスタイプにより、本機は同一のローカルサブネットの接続先のデバイスに IPv6 アドレスを介してアクセス可能となります。

本機の IPv6 リンクローカルアドレスを設定するには、次の手順に従ってください。

（1）interface configuration モードにアクセスするために、global configuration モードで "interface vlan 1" と入力し <Enter> キーを押します。

（2）“ipv6 enable” と入力後、<Enter> キーを押します。

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND retransmit interval is 1000 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

Address for Multi-segment Network — 複数のサブネットを含むネットワークでは、IPv6 は手動で設定しなければなりません。詳細については、「 IPv6 アドレスの設定方法」を参照してください。現行のソフトウェアでは、IPv6 の DHCP をサポートしておりません。

2.3.4 DHCP サーバにより参照されている設定ファイルのダウンロード方法

DHCP サーバから本機に伝達される情報には、ダウンロード用の設定ファイル、ファイルにアクセス可能な TFTP サーバが含まれる場合があります。DHCP サーバからの IP 設定リクエスト以外に、初期設定時の設定ファイルを使用すると、bootup 設定ファイル名およびファイルの保存先の TFTP サーバ名を要求してきます。リモート bootup file ファイルのダウンロードが可能な情報を受信した場合は、ファイルをローカルバッファに保存してから、処理を再開してください。

以下の DHC クライアントの動作に注意してください。

- TFTP サーバから受信した bootup 用設定ファイルは、元のファイル名でストアされます。このファイル名が本機にすでにある場合は新しいファイルに上書きされます。
- bootup 用設定ファイル名が初期設定時の設定ファイルと同じ場合はダウンロード手順は終了し、以降の DHCP クライアント要求を送信することはありません。
- 本機が DHCP サーバにより受信した情報に応じて bootup 用設定ファイルのダウンロードに失敗した場合は、以降の DHCP クライアント要求を送信することはありません。
- 本機が bootup 処理を完了する前に DHCP による応答を受信しなかった場合は、分単位で DHCP クライアント要求の送信を続けます。これらの要求は、本機のアドレスを手動で設定した場合のみ終了しますが、アドレスモードの設定を「DHCP」に戻すと再開します。
- bootup 用設定ファイルを本機の DHCP デーモン（ここでは、Linux 対応のシステム）に正常に送信するには、以下の情報で設定する必要があります。
- オプション 60, 66, 67 のステートメントがデーモンの設定ファイルに追加可能

オプション	キーワード	パラメータ
60	vendor-class-identifier	ベンダークラスの識別子を指す文字列
66	tftp-server-name	tftp サーバ名を指す文字列
67	bootfile-name	bootfile 名を指す文字列

- デフォルト設定では、DHCP オプション 66/67 パラメータは、DHCP サーバ応答に伝播されません。オプション 66/67 情報で DHCP による応答を求めるには、本機により送信された DHCP クライアント要求には、この情報を求める ”parameter request list” が含まれます。
- それ以外に、クライアント要求には、DHCP サーバがデバイスを識別することが可能な “vendor class identifier” が含まれ、ダウンロード用の適切な設定ファイルを選択します。
- この情報は、オプション 55 および 124 に含まれます。

オプション	キーワード	パラメータ
55	dhcp-parameter-request-list	',' で区切られたパラメータのリスト
124	vendor-class-identifier	ベンダークラス識別子を指す文字列

以下の例では、Linux 対応 DHCP デーモン (dhcpd.conf ファイル）の設定例を挙げています。サーバはオプション 43 にカプセル化された ”option 66/67” で応答します。“Vendor class one” のセクションでは、DHCP リクエストパケットのベンダークラスの識別子がこのファイルで指定した識別子と一致すると、サーバは、DHCP 応答パケットの ”option 66/67” にカプセル化された ”option 43” を送信します。“Vendor class two” セクションでは、サーバは常に ”option 66/67” を送信して、サーバ (92.168.255.101) から “test2” の設定ファイルをダウンロードするように本機に通知します。

```
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
server-name "Server1";
Server-identifier 192.168.255.250;
#option 43 with encapsulated option 66, 67
Table 3: Options 60, 66 and 67 Statements
Option
Statement
Keyword Parameter
60 vendor-class-identifier a string indicating the vendor class
identifier
66 tftp-server-name a string indicating the tftp server name
67 bootfile-name a string indicating the bootfile name
Table 4: Options 55 and 124 Statements
Option
Statement
Keyword Parameter
55 dhcp-parameter-request-list a list of parameters, separated by ','
124 vendor-class-identifier a string indicating the vendor class
identifier
option space dynamicProvision code width 1 length 1 hash size 2;
option dynamicProvision.tftp-server-name code 66 = text;
option dynamicProvision.bootfile-name code 67 = text;
subnet 192.168.255.0 netmask 255.255.255.0 {
range 192.168.255.160 192.168.255.200;
option routers 192.168.255.101;
option tftp-server-name "192.168.255.100";#Default Option 66
option bootfile-name "bootfile"; #Default Option 67
}
class "Option66,67_1" { #DHCP Option 60 Vendor class
one
match if option vendor-class-identifier = "FXC9324XG.cfg";
#option 43
option vendor-class-information code 43 = encapsulate
dynamicProvision;
#option 66 encapsulated in option 43
option vendor-class-information.tftp-server-name "192.168.255.100";
#option 67 encapsulated in option 43
option vendor-class-information.bootfile-name "test1"
}
class "Option66,67_2" { #DHCP Option 60 Vendor class
two
match if option vendor-class-identifier = "FXC9324XG.cfg";
option tftp-server-name "192.168.255.101";
option bootfile-name "test2";
}
```

[注意] dhcpd.conf ファイルの **vendor-class-identifier の “FXC9324XG.cfg” を使用してください。**

2.3.5 SNMP 管理アクセスを有効にする

本機には、SNMP バージョン 1, 2c, 3 クライアントをサポートしている SNMP(Simple Network Management Protocol) エージェントが含まれます。バージョン 1, 2c クライアントの管理用アクセスを提供するには、コミュニティストリングを指定する必要があります。本機は、SNMP 管理ステーション側が本機にリクエストを送信する際 (情報を戻したり、パラメータの設定を行う)、本機は要求したデータを提供したり、指定したパラメータの設定を行います。本機は、トラップメッセージ（イベントが発生したことをマネージャに通知する）を介して情報をマネージャによりリクエストがなくても SNMP マネージャに送信するように設定することが可能です。

本機は、MIB ツリー全体への読取りアクセス用の “public” コミュニティストリング、読取り / 書込みアクセス用の “private” についてのデフォルトの MIB View(例えば、SNMPv3 対応）を提供します。ただし、お使いのセキュリティ要件に合致したバージョン 1 または 2c コミュニティストリングに新規 views を割り当てることが可能です（詳細については、別紙の『WEB 設定』マニュアルの「SNMPv3 ビューの設定」の項を参照してください。

コミュニティ名（SNMP バージョン 1 および 2C クライアント）

コミュニティ名 (Community Strings) は、本機からトラップ情報を受け取る SNMP ソフトウェアの認証と、SNMP ソフトウェアからのアクセスをコントロールするために使用されます。指定されたユーザもしくはユーザグループにコミュニティ名を設定し、アクセスレベルを決定することができます。

初期設定でのコミュニティ名は以下のとおりです。

- public — 読み取り専用のアクセスが可能です。public に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧のみが行えます。
- private — 読み書き可能なアクセスができます。private に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧及び変更をすることが可能です。

[注意] SNMP を利用しない場合には、初期設定のコミュニティ名を削除して下さい。コミュニティ名が設定されていない場合には、SNMP 管理アクセス機能は無効となります。

SNMP バージョン 1, 2c クライアントから SNMP 経由での不正なアクセスを防ぐため、コミュニティ名は初期設定から変更して下さい。コミュニティ名の変更は以下の手順で行います。

（1）管理者モード (Privileged Exec) の global configuration モードから "snmp-server community string mode" と入力し <Enter> キーを押します。
"string" にはコミュニティ名、"mode" には rw（read/wirte、読み書き可能）、ro（read only、読み取り専用）のいずれかを入力します（初期設定では ”read only” となります)。

（2）（初期設定などの）登録済みのコミュニティ名を削除するために、"no snmp-server community string" と入力し <Enter> キーを押します。
"string" には削除するコミュニティ名を入力します。

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

[注意]　SNMP バージョン 1, 2c クライアントへのアクセスのサポートが必要ない場合は、デフォルトのコミュニティストリングを削除して、SNMP バージョン 1, 2c クライアントからの SNMP 管理用アクセスを無効してください。

トラップ・レシーバ（Trap Receivers）

本機からのトラップを受ける SNMP ステーション（トラップ・レシーバ）を設定することができます。Trap レシーバを設定するには、“snmp-server host” コマンドを使用します。

Privileged Exec の global 設定モードは、以下のとおり入力してください。

“snmp-server host host-address community-string [version {1 | 2c | 3 {auth | noauth | priv}}]”

ここで、“host-address” は trap レシーバの IP アドレスであり、“communitystring” はバージョン 1/2c ホストのアクセス権、またはバージョン 3 のホストのユーザ名を指します。“version” は、SNMP クライアントのバージョン、“auth | noauth | priv” はそれぞれ ″ 認証あり ″、″ 認証なし ″、″SNMPv3 クライアントに対しての認証 ″ を意味します。

これらのパラメータの詳細については、別紙の『CLI 設定』に記載されている "snmp-server host" を参照してください。以下の例では、SNMP クライアントのタイプごとに trap ホストを設定します。

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

SNMP バージョン 3 クライアントへのアクセスの設定

SNMPv3 クライアントの管理用アクセスを設定するには、view を設定して、クライアントが読み書き可能な MIB を作成し、view をグループに設定した後、ユーザをグループに設定します。以下の例では、MIB-2 ツリーブランチ全体を含む “mib-2” の view を 1 つ設定し、IEEE 802.1d bridge MIB を含むもう一つの view を設定します。

それぞれの読み取り、読み取り / 書取り view を “r&d” というグループに設定して、MD5 or SHA を介してグループ認証を指定します。次の手順では、v3 ユーザをグループに割り当て、MD5 は認証用であることを表し、認証用のパスワードには “greenpeace”、暗号化用のパスワードには “einstien” を使用します。

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace
priv
des56 einstien
Console(config)#
```

SNMP v3 クライアントからのアクセスするための設定方法については、別紙の『CLI 設定』マニュアルおよび『WEB 設定』マニュアルの中の「SNMP の設定」の項を参照してください。

2.4 システムファイルの管理

本機のフラッシュメモリ上に CLI、WEB インタフェース、SNMP から管理可能な 3 種類のシステムファイルがあります。これらのファイルはファイルのアップロード、ダウンロード、コピー、削除、及び起動ファイルへの設定を行うことができます。

3 種類のファイルは以下の通りです。

- **Configuration(設定ファイル)** — このファイルはシステムの設定情報が保存されており、設定情報を保存した際に生成されます。保存されたシステム起動ファイルに設定することができる他、サーバに TFTP 経由でアップロードしバックアップを取ることができます。
  "Factory_Default_Config.cfg" というファイルはシステムの初期設定が含まれており、削除することはできません。システムが初期設定値で boot すると、マスターユニットは各ユニットの識別子、MAC アドレスの情報などを含め、スタックの初期化用のシステム設定を含む “startup1.cfg” という名前のファイルを同様に設定します。初期設定用のファイルからの設定値はこのファイルにコピーされ、本機の boot 用に使用されます。詳細については、P31 「設定ファイルの保存および復元」を参照してください。

- **Operation Code(オペレーションコード)** — 起動後に実行されるシステムソフトウェアでランタイムコードとも呼ばれます。オペレーションコードは本機のオペレーションを行なう他、CLI または WEB インタフェースを提供します。

- **Diagnostic Code(診断コード)** — POST(パワー・オン・セルフテスト) として知られているソフトウェア (システム・ブートアップ時の実行プログラム)。

本機はフラッシュメモリのサイズに制限があるため、オペレーションコードを 2 つまで保存することができます。診断コードと設定ファイルに関しては、フラッシュメモリの容量の範囲内で無制限に保存することができます。

フラッシュメモリでは、各種類のそれぞれ 1 つのファイルが起動ファイルとなります。

システム起動時には診断コードファイルとオペレーションコードファイルが実行されます。その後設定ファイルがロードされます。設定ファイルは、ファイル名を指定してダウンロードされます。

実行中の設定ファイルをダウンロードした場合、本機は再起動されます。実行中の設定ファイルを保存用ファイルに保存しておく必要があります。起動中の設定をダウンロードする場合は、システムは起動し、設定値は起動設定ファイルから保存ファイルにコピーする必要があります。

2.4.1 設定ファイルの保存および復元

Configuration コマンドでは、起動中の設定ファイルの修正のみ可能ですが、本機の reboot 時には保存されません。不揮発性記憶域に現在の設定の変更を保存するには、“copy” コマンドを使って起動中の設定ファイルをコピーする必要があります。

新しい起動用設定ファイル名を予め指定しておく必要があります。本機のファイル名は、大文字小文字を区別した 1 ～ 31 文字で、スラッシュ (“\ “ または、“/”) を含めてはなりません。またファイル名の最初の文字にピリオド (”.”) を使用してはなりません（使用可能な文字 :A-Z, a-z, 0-9, “.”, “-”, “_”)。

フラッシュメモリには複数のユーザにより作成された設定ファイルを複数保存することが可能ですが、本機の boot 時にロードされる “startup” ファイルに設定できるファイルは 1 つのみです。copy running-config startupconfig コマンドは、通常新規ファイルを起動用ファイルとして設定します。予め保存されている設定ファイルを選択するには、boot system config:<filename> コマンドを使用してください。

保存されている設定ファイルの上限は、使用可能なフラッシュメモリに応じて異なります。使用可能なフラッシュメモリのサイズは、dir コマンドを使用してチェックすることが可能です。

現行の設定を保存するには、以下のコマンドを入力してください。

（1）Privileged Exec モードで、“copy running-config startup-config” と入力して、<Enter> キーを押します。

（2）start-up ファイル名を入力して、<Enter> キーをクリックします。

```
Console#copy running-config startup-config
Startup configuration file name []: startup

\Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

バックアップサーバから設定をリストアするには、次のコマンドを入力してください。

（1）Privileged Exec モードで “copy tftp startup-config” と入力して、<Enter> キーをクリックします。

（2）TFTP サーバのアドレスを入力して、<Enter> キーをクリックします。

（3）サーバにストアされている起動用のファイル名を入力して、<Enter> キーをクリックします。

（4）本機の起動用のファイル名を入力して、<Enter> キーをクリックします。

```
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

付録 A. トラブルシューティング

Telnet 又は Web ブラウザ、SNMP ソフトウェアから接続できない。

- スイッチに電源が投入されていることを確認して下さい。
- 管理端末とスイッチを接続するネットワークケーブルが、正しく接続されていることを確認して下さい。
- スイッチとの接続と接続先のポートが、無効になっていないか確認して下さい。
- 有効な IP アドレス、サブネットマスク、及びデフォルトゲートウェイが設定されたエージェントであることを確認して下さい。
- 管理端末が管理 VLAN（初期設定では VLAN 1）に接続していることを確認して下さい。
- 管理端末の IP アドレスが、スイッチが接続している IP インタフェースと同じサブネットの IP アドレスであることを確認して下さい。
- タグ付VLANグループに所属するIPアドレスを使用してスイッチへの接続を行おうとしている場合は、管理端末、及びネットワークへの接続を中継するスイッチに接続しているポートの設定が正しいタグになっていることを確認して下さい。
- Telnet で接続できない場合は、同時に接続できる Telnet セッション数の最大値を超過している可能性があります。時間を置いて再度接続してみて下さい。

セキュアシェルを使用した接続ができない。

- SSH での接続ができない場合は、同時に接続できる Telnet/SSH セッション数の最大値を超過している可能性があります。時間を置いて再度接続してみて下さい。
- SSH サーバの制御パラメータがスイッチに対して正しく設定されており、SSH クライアントソフトウェアが管理端末に対して正しく設定されていることを確認して下さい。
- スイッチの公開キーを生成し、このキーを SSH クライアントに提供していることを確認して下さい。
- 各 SSH ユーザアカウント（ユーザ名、認証レベル、パスワードを含む）を設定していることを確認して下さい。
- （公開キーによる認証機能を使用している場合）クライアントの公開キーをスイッチに取り込んでいることを確認して下さい。

シリアルポート接続から内蔵の設定プログラムに接続できない。

- ターミナルエミュレーションプログラムが、以下の通り設定されていることを確認して下さい。

  ターミナル　　：VT100 互換
  データビット　：8 ビット
  ストップビット：1 ビット
  パリティ　　：なし
  通信速度　　：115200 bps(デフォルト値)

- 同梱のシリアルケーブルを使用していることを確認して下さい。

パスワードを無くしてしまった、又は忘れてしまった。

- お買い上げの販売店または、当社指定のサービス窓口にご連絡下さい。

FXC9324XG Management Guide (FXC14-DC-200003-R1.0)

初版　　2014 年 2 月

Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide
FXC9324XG
Management Guide

FXC株式会社