FUJITSU

CA92344-0341-08
2016 年 04 月
富士通株式会社

PRIMERGY コンバージドファブリックスイッチブレード (10Gbps 18/8+2) コンバージドファブリックスイッチ (CFX2000R/F)

コンバージドファブリック機能説明書

FUJITSU

第1章　C-Fabric 機能

1.1 C-Fabric 機能概要

1.1.1　C-Fabric とは

C-Fabricとは、Converged Fabric（コンバージドファブリック）の略称であり、富士通独自のイーサネットファブリックを指すものです。

従来のイーサネットスイッチではSTP(Spanning Tree Protocol)を使用せずにループトポロジを形成できず、そのため複数のリンクを有効に利用できない、ネットワーク設計を綿密に実施しなければならない等の課題がありましたが、C-Fabricによりイーサネットファブリックを構築することで、それらの問題を解決することができます。
C-Fabricは以下の効果を実現しています。

- 複数のリンクを全て有効に、かつ効果的に利用することによって高スループットを実現。
- ファブリックのループトポロジを自動検知する。また自動的に再構成を実現することが可能。
- C-Fabricを構築するスイッチ群は全て仮想的に１つのスイッチとして動作。データの転送処理だけでなく管理面でも１つのスイッチとして管理することが可能になり、運用管理の効率化を実現。

C-Fabricを使用する際には必ず本ドキュメントの「第3章C-Fabricの留意事項」と別ドキュメントの「コンバージドファブリックスイッチ製品 ご使用上の留意・注意事項」を参照してください。

1.1.2　用語・略称

当機能説明書内で使用するC-Fabric機能の用語定義を以下に記述します。

- ファブリック

  １台のスイッチとして構築した複数ドメインを相互接続し、論理的に１台のスイッチとして見せる論理スイッチをファブリックと呼びます。

- ドメイン

  複数のスイッチをISL（Inter Switch Link）で接続し、全体を１つのスイッチとして見せる単位をドメインと呼びます。

- C-Fabricスイッチブレード

  PRIMERGYコンバージドファブリックスイッチブレード(10Gbps 18/8+2)を指します。

- CFX2000

  ToR(Top of Rack)スイッチであるコンバージドファブリックスイッチ[CFX2000F/CFX2000R]を指します。

- 接続インタフェース
  - CIR(Clean Interface with Redundancy)
    Core Networkと接続されるインタフェースを指します。
    Rootドメインに属するスイッチのみ定義可能です。
  - EP(End Point)
    サーバ等のエンド端末と接続されるインタフェースを指します。
    Rootドメインを含め全てのドメインで定義可能です。
  - ISL(Inter Switch Link)
    ドメイン内部の接続に使用されるインタフェースを指します。
    ISLとして使用するポートは、ユーザが定義可能です。
  - US(Upstream)
    ファブリック内部のドメイン間接続に使用されるインタフェースを指します。
    ファブリックはRootドメインをルートとするツリー構成なので、ドメイン間接続の両端ポートは、Rootドメイン側とその反対側という括りで定義可能です。USはRootドメイン側の定義となります。
    C-Fabric構築時に自動判定され、定義も自動で実施します。
  - DS(Downstream)
    US同様にドメイン間接続に使用されるインタフェースを指します。
    Rootドメインと反対側に属する定義となります。
    C-Fabric構築時に自動判定され、定義も自動で実施します。

- ファブリック代表仮想IPアドレス
  ファブリックを仮想的に１つのスイッチとして見立てた際の、その仮想スイッチに割り当てられるIPアドレスを指します。
  IPv4／IPv6どちらのアドレスも付与可能です。

- ドメイン代表仮想IPアドレス
  ファブリック内部の各ドメインを代表するIPアドレスを指します。
  IPv4／IPv6どちらのアドレスも付与可能です。
  SNMP Trap等のスイッチ側からの通知について、当IPアドレスを使用します。

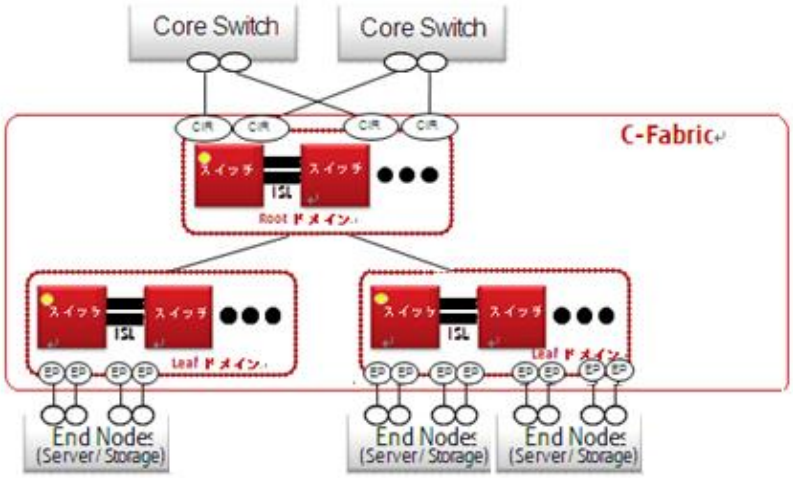
- かんたん設定
  CFX2000R/Fの工場出荷時設定です。ファームウェア版数V03.00NY0046以降でサポートします。
  以下のような設定
  40Gbps(port17,21,25,29, 49, 53, 57, 61)のポートを全てISLポートとして設定。
  Domain mode = Root
  CEE有効
  FCFライセンスキー搭載状態時にFCF A系有効(上記ISLを除くすべてのポート)
  通常出荷品を(Fabric ID, Domain ID, Switch ID)=(1, 1, 0)
  交換用部品(保守部品)を(Fabric ID, Domain ID, Switch ID)=(1, 1, 9)
  としているため、対象の40Gbpsポート同士を接続するだけで、C-Fabricの物理構築が可能です。

1.2 C-Fabric の構成

1.2.1 C-Fabric 物理構成

C-FabricはC-Fabricスイッチブレードおよび CFX2000を複数台組み合わせ、仮想的に1台のスイッチを自動で組み上げ、富士通独自のイーサネットファブリックを構築するものです。
C-Fabricは8台までの同種のスイッチをISL(Inter Switch Link)で接続し、ドメインという管理単位を作成します。そしてドメインを1単位とするツリー構成を取ることでファブリックを構築します。
（冗長化を実現するため1つのドメインに最低でも2台のスイッチを接続することを推奨します。）
ドメインによるツリーは2階層で、上位のドメインをRootドメイン、下位をLeafドメインと呼びます。
Leafドメインの下にLeafドメインを配置することはできません。また、Rootドメインはファブリック内に1つのみ構築可能です。

C-Fabricは初期構築時に各スイッチに装置を識別するためのIDおよびISLポートの定義を行い、後は機器同士を接続するだけで構築できます。それにより、システム導入にかかる時間を劇的に改善できます。
また、C-Fabricはデータ通信に対して仮想的に1台のスイッチとして動くだけでなく、管理についても仮想的に1台のスイッチとして動作します。設定は自動的に全スイッチに反映されるため、管理工数の削減にも威力を発揮します。
C-Fabricは外部との接続インタフェースとしてCIR(Clean Interface with Redundancy)およびEP(End Point)を定義します。CIRはCore Networkとの接続に、EPはサーバ等のエンド端末との接続に最適なインタフェースを提供します。C-FabricはRootドメインから外部のCore Networkと接続するように想定されており、CIRはRootドメイン以外で定義することはできません。
C-Fabric内部の接続に関してユーザはISLポート設定以外に何も定義する必要はありません。内部接続ポートはC-Fabric構築時に自動判定され、定義も自動で実施されます。



ドメイン間の接続(RootドメインとLeafドメインとの接続等)は自動的にMLAG(複数スイッチをまたいだ

LAG)が構成されます。冗長性を確保するためにドメイン間はメッシュ状になるように接続してください。

こんな事に気をつけて

・接続インタフェース（US/DS/CIR/EP）を自動判別する際、通信可能になるまで10秒～１分程度掛かる場合があります。ファームウェアV02.20 NY0042以降では即時外部ポート(CIR/EP)に設定できるコマンドが実行できるため、そのコマンドを実施してください。
(ファームウェアV02.20 NY0046以前でFCoEを使用するポートに即時外部ポート設定はできません)
・IDやISLの設定後にケーブル接続を行う場合、初めにISLポートを接続した後に、ドメイン間(Root-Leaf間)のケーブルを接続してください。ISLポートを接続する前にドメイン間のケーブルを接続すると、同じIDのドメインを複数認識することによりファブリック構築に問題があると判断され、スイッチが縮退し、そのポートがオフラインになります。
・ドメイン間のポートがダウンした場合、ドメイン間MLAGのMACアドレステーブルがクリアされるため、再度MACアドレス学習が行われるまで、unicast通信もフラッディングされます。
・ドメイン間のポートがアップする際には、ドメイン間MLAGの再構築が行われるため、パケットが数個ドロップする場合があります。
・CIR/EPを複数本外部に接続する場合、MAC learningをoffにする必要があります。一般的なスイッチはVlan ID, MACアドレスで学習しますが、本スイッチはVFAB ID, MACアドレスで学習するため、本設定が必要となります。詳細は巻末のC-Fabricの留意事項(13)を参照してください。
・スイッチダウン等の故障でスイッチ交換を実施する場合、故障していないスイッチ群の故障スイッチへの接続ポートが、ループ防止のためにoffline(fabric)の状態になっている場合があります。その場合、Root Domain Master スイッチ上のCLIで"online ether <port num>"コマンドを実行し、ポートを有効にして交換スイッチを接続してください。
・スイッチの再起動等でパスの切り替えが発生する際に通信が数パケット途切れる場合があります。
・Switch IDが0または9の時、ISLポート以外のポート状態は誤った接続を防止するためoffline(fabric)になります。

1.2.1.1 Master スイッチと Slave スイッチ

ドメイン内のスイッチ管理はドメイン内のMasterスイッチが代表して行います。Masterスイッチはドメイン内のスイッチ1台が自動的にIDの大小や起動順序により選出されます。Masterスイッチ以外は全てSlaveスイッチとなります。MasterスイッチがDomainから外れた際にはSlaveスイッチから新たにMasterスイッチが選出されます。
C-Fabricの設定はファブリック全体で１つであり、RootドメインのMasterスイッチが設定を管理します。

ドメイン内のスイッチを区別するためのIDをSwitch IDと呼び、0から9まで設定できます。実際に有効なのは1から8までで、0はファブリック接続時に空いているIDを、9は前回接続されていたIDを自動的に設定します。

こんな事に気をつけて

C-FabricスイッチブレードをBX400 S1シャーシに搭載して使用する場合、シャーシのバックプレーン内のISL専用ポート(ポート番号35)は使用することができません。BX400 S1シャーシにC-Fabricスイッチブレードを搭載する場合は必ず「PRIMERGY コンバージドファブリックスイッチブレード(10Gbps 18/8 + 2) ユーザーズガイド」を参照しポート35をオフラインに設定してください。

1.2.1.2 Root ドメインと Leaf ドメイン

C-Fabricはドメインをツリー構造に接続することで構築します。最上位のドメインをRootドメインと呼び、Rootドメイン以外のドメインをLeafドメインと呼びます。ドメインは同種のスイッチのみで構築する必要があります。

※C-Fabricスイッチブレードでドメインを構築する場合、C-Fabricスイッチブレードのみで構築する必要があります。また、CFX2000でドメインを構築する場合も、CFX2000のみで構築する必要があります。

ドメインの区別はDomain IDによって行われます。IDの範囲は1から32です。もし、IDの設定間違い等でファブリックに異常なDomain IDのスイッチが接続された場合、そのスイッチは縮退状態となり、意図的に機能が停止されます。その際にDomain IDは(設定値+32)で表示されます。
また、ドメインには他にDomain modeの設定もあります。値はLeaf, Rootの二つで、初期値はLeafになっています。(かんたん設定時にはRootに設定)

ファブリック構築時、ファブリック内の複数ドメインがRootに設定されている場合、優先度を比較して、より優先度が高いドメインをRootドメインとします。
優先度の低いドメインはCFAB縮退モード(異常ドメイン)として動作します。

優先度	状態
高	ファブリック内のドメインとして動作中
↓	スイッチがCFX2000
	ドメイン IDの小さい装置
低	MAC Addressが小さい装置

ファブリック構築時、ファブリック内に同一のドメインIDを持つドメインが複数存在する場合は、
優先度を比較します。
優先度の低いドメインはCFAB縮退モード(異常ドメイン)として動作します。

優先度	状態
高	Root ドメイン ID と ファブリックIDが同じ
↓	ファブリック内のドメインとして動作中
	Root ドメインに近いドメイン
低	MasterスイッチのMAC Addressが小さい装置

こんな事に気をつけて

CFX2000はC-Fabricスイッチブレードより下位のドメインになることはできません。つまりRootドメインをC-Fabricスイッチブレードで構成し、LeafドメインをCFX2000で構成することはできません。

1.2.1.3 C-Fabric の設定と管理

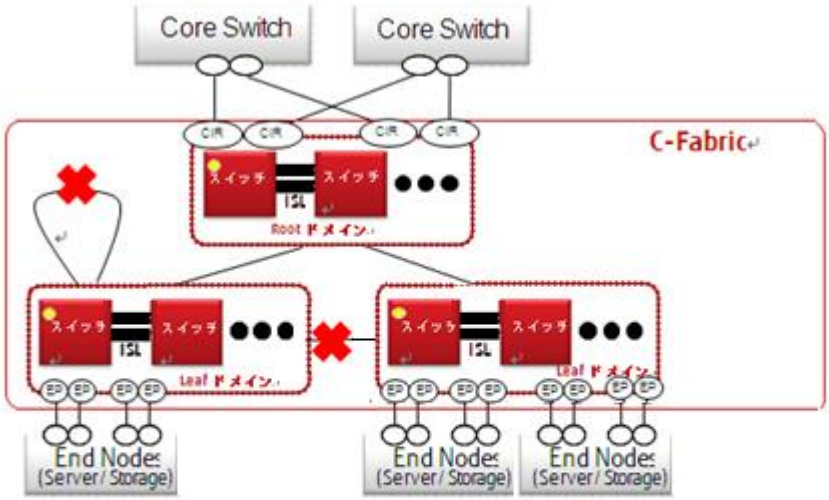
C-Fabricは、ファブリック全体で１つの仮想IPアドレス(ファブリック代表仮想IPアドレス)を設定できます。IPv4／IPv6どちらのアドレスも付与可能です。
ファブリック代表仮想IPアドレスへログインすると、RootドメインのMasterスイッチにログインすることになるので、C-Fabricの設定や情報の表示をこのIPアドレスにアクセスするだけで行うことができます。

また、C-Fabricを構成するスイッチのSNMP TRAP等の通知やMIB情報の取得についてはドメイン単位で実施します。そのため、これら情報取得を行う際は、ドメイン単位に仮想IPアドレス(ドメイン代表仮想IPアドレス)を指定する必要があります。
ドメイン代表仮想IPアドレスへのtelnet/ssh/ftp などによるログインはできません。

こんな事に気をつけて

・Rootドメインのドメイン代表仮想IPアドレスは使用できません。Rootドメインの情報を取得したい場合、ファブリック代表仮想IPアドレスを使用してください。
・スイッチ個別にマネージメントポート(oobポート)を使用することができます。
・oobポートは上記仮想IPアドレスと同じネットワークアドレスのIPを割り振ることはできません。
oobポートに接続できるようにしておけば、ファブリックから切り離されたスイッチへのアクセスも可能となり、障害発生時のアクセスが容易になります。
・仮想IPアドレスへのアクセスはdefault vfab経由でのみ可能です。また、CPU負荷を下げるため、default vfabはできる限り管理専用で使用し、ブロードキャスト、マルチキャストパケットが大量にDefault vfabに流れることが無いようにしてください。

Rootドメインは各ドメインとの接続情報を収集しファブリック全体の接続情報を構築します。また、その情報をもとに接続形態(ツリー構造)のチェックとUS, DSのポート設定を自動で行います。
ドメイン間の接続がツリー構造になっていないポートを検出した場合、該当ポートをBlockingポートに設定し通信の遮断を行います。
下図は非ツリー構造検出のイメージであり、×印に接続されているポートがBlockingポートとなります。構成によってはユーザの意図しないポートがBlockingポートに設定されツリー構造を構築する場合もあります。



1.2.1.4 CFAB 縮退モード

C-Fabric構成で異常と判断されたスイッチおよびドメインが最低限の機能を残し機能を制限している状態をCFAB縮退モードと呼びます。
CFAB縮退モードはファブリック/ドメイン内のスイッチとして見えてはいるが、通常のデータ通信が行えない状態(ISL以外の全ポートがDown状態)になります。(C-Fabricの制御通信のみ可能)
ただし、ファブリック内からのログインとManagement LANとコンソールからの操作は可能であり、下記操作が可能です。(Configモードでは一部の設定が変更可能)

- configure
- exit
- show
- reset

スイッチIDやドメインIDの重複などでCFAB縮退モードになっている場合には、異常と判断されているスイッチにファブリック内のRootドメインからログインし、定義の変更を行うことで通常スイッチおよび通常ドメインとして運用することが可能になります。
ただし、ファブリックIDの不一致などの場合には物理的に違うファブリックと判断するため、そのスイッチにファブリック内からログインすることはできません。
CFAB縮退モードのエラー内容は、show cfab statusコマンドで確認できます。

こんな事に気をつけて

異常原因を修復後にCFAB縮退モードから復旧するには、装置のリセットまたはonlineコマンドによるポートのリンクアップが必要となります。

1.2.1.5 C-Fabric 物理構成初期値とかんたん設定

C-Fabricの物理構成関連の装置初期値(初期化コマンド(reset clear)実行時の値)は以下となっています。

ISLポート設定なし
Domain mode = Leaf
(Fabric ID, Domain ID, Switch ID) = (1, 1, 0)

ボックス型スイッチのCFX2000R/Fについては、工場出荷時の値が上記とは異なり、かんたん設定になっています。かんたん設定時の値は以下となっています。

40Gbps(port17,21,25,29, 49, 53, 57, 61)のポートを全てISLポートとして設定。
Domain mode = Root
CEE有効
FCFライセンスキー搭載状態時にFCF A系有効(上記ISLを除くすべてのポート)
通常出荷品を(Fabric ID, Domain ID, Switch ID)=(1, 1, 0)
交換用部品(保守部品)を(Fabric ID, Domain ID, Switch ID)=(1, 1, 9)

また、かんたん設定時にはプロンプトに"ez"が表示されるようになっています。これにより、装置がかんたん設定で使用されているのかどうかを確認することができます。かんたん設定を解除したい場合、初期化コマンド(reset clear)を実行し、装置の初期化を行ってください。
※　かんたん設定の構成が環境に合わない場合は、最初にreset clearで初期化をする必要があります。

ez-configコマンドを実行することにより、かんたん設定にすることができます。このコマンドを実行する場合はreset clear実行し、スイッチを初期化してから実行してください。

かんたん設定のスイッチでファブリックを構築する場合は、
①スイッチの40Gbpsポート(port17,21,25,29, 49, 53, 57, 61)同士を接続する
②どれか一つのスイッチのコンソールポートからコマンドラインにログインし、ez-initを実行
で構築完了となります。
(ファブリック内の全てのスイッチがかんたん設定(Switch ID=0)だと自動割り当てされないので、どれか一つのスイッチ上でez-initコマンドを入力する必要があります。)

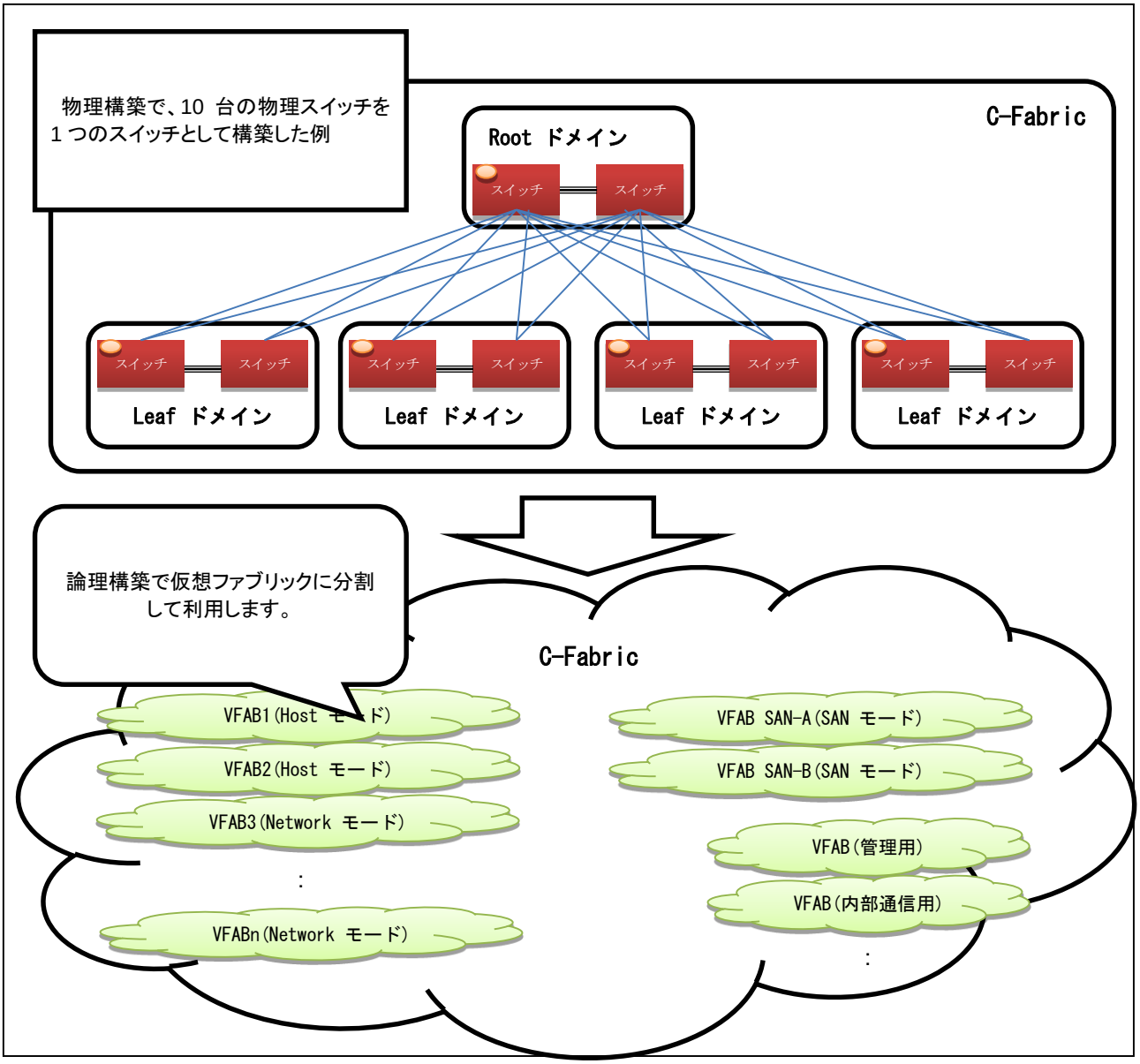
こんな事に気をつけて

かんたん設定時に40GbpsのISL設定の解除やIDの変更を行うとプロンプトに'ez'が表示されたまま、それらの設定変更がされてしまうので、IDやISLの変更を行う場合は、かんたん設定を解除したうえで、設定を行ってください。かんたん設定は初期化コマンドであるreset clearを実行すれば解除されます。

1.2.2 C-Fabric 論理構成

C-Fabricでは、構築したファブリックを論理的に分割し、仮想ファブリック(VFAB)として管理できます。

VFABをテナントに割り当てることで、マルチテナントに対応することができます。テナント向けのVFAB以外に、C-Fabric管理用のdefault VFAB、FCoEの通信を行うためのSANモードVFABを提供します。
※FCoE: Fibre Channel over Ethernet、SAN: Storage Area Network



VFABには、以下3種類のモードがあり、用途に応じて使い分けることが可能です。

• Hostモード

Hostモードは、EPからの通信をCIRへ透過します。EPに接続されるホストインターフェースとCIRポートが１対1で対応づけられ、CIRがホストインターフェースと同等に扱うことが可能となるモードです。

ネットワークの機器に依存せず、接続性を保証します。

HostモードではCIR間の通信は行われません。

VFABを定義する際にEPにのみvlanを割り当てるだけで、そのEPに対応づけられたCIR側には自動的にVLANが割り当てられます。

対応づけられたCIRがダウンした場合は、自動的にファイルオーバーが行われ、別のCIRにEPのVLANが割り当てられます。

Hostモードに組み込まれたCIRポートが新たに追加された場合、既存のCIRのVLAN割り当てはすべてクリアされ、最初からVLAN割り当てが行われます。

• Networkモード

Networkモードは、EPとCIRを通常のL2スイッチで接続するのと同等に扱うことが可能となるモードです。Hostモードとは異なりCIR同士の通信も可能であり、EPだけではなくCIRにもVLANを手動で割り当てる必要があります。

•SANモード

SANモードは、FCoE(Fibre Channel over Ethernet)をサポートするストレージ装置との接続を提供するモードです。

SANモードはA系/B系の2系統を定義することで、SANネットワークの冗長構成を可能にします。

VFABを定義する際には、VFAB ID、VFABに組み込まれるインターフェース(EPとCIR)、そして各インターフェースで使用するVLANを指定する必要があります。

C-FabricにはVLAN IDをCIRポートで変更するVLAN Translate機能があります。例えばEPでVlan ID:100を使用し、CIRから出力するフレームをVlan ID:200へ変更。またC-Fabric外部からVlan ID:200のフレームをCIRで受信し、EPへVlan ID:100でフレームを転送することができます。

こんな事に気をつけて

・以下のような場合はVFAB設定が適用されません。

・VFABで使用するインタフェースグループの設定が存在しない場合（初期設定以外）

・ホストモード動作時にVLAN自動設定CIRインタフェース設定(vfab cir-ports)がない場合

・SANモード動作時に指定したインタフェースが自装置系統(A系/Ｂ系)のSANモードと異なる場合

・使用できるVFAB/VLAN数はVLAN変換テーブルの大きさに依存します。テーブルサイズはスイッチ1台あたり8192ですが、ハッシュ値による管理の為、最大値に達する前に許容を上回る重複が発生し設定できなくなる場合があります。各ポートに適用されるVFAB/VLANの合計数が3000を超える場合、不要な

VFAB/VLANを減らす、もしくはスイッチを増やしてノードを分散させる等の対策を行ってください。

1.3 他機能との併用について

VFAB動作時の他機能との併用および注意事項について記載します。

1. リンクアグリゲーション機能

C-Fabric構成装置をまたいだLAG機能(MLAG:Multi-chassis Link Aggregation)をサポートします。MLAGはドメイン内の装置間で構成可能です。
詳細は、リンクアグリゲーション機能を参照してください。

2. CEE機能

CEE機能は、すべてのVFABに対して共通の設定が適用されます。
以下にサポートするCEE機能を記載します。詳細は、CEE機能を参照してください。

・PFC(Priority-based Flow Control)機能
ロスレスチャネルをサポートするために優先度ベースのフロー制御であるPFC機能をサポートします。

・ETS(Enhanced Transmission Selection)機能
PFCで利用する優先度をpriorityグループと見なし、各priorityグループ単位での帯域制御するETS機能をサポートします。C-Fabricを利用するVM装置は本機能で提供されたpriorityで通信が行われます。

・DCBX(Data Center Bridging Exchange)機能
PFC機能やETS機能のサポート有無等の情報を交換します。

3. AMPP連携動作

AMPP(Automatic Migration of Port-Profile)機能との連携をサポートします。
詳細は、エッジ仮想スイッチ機能を参照してください。

4. VEPA連携動作

VEPA(Virtual Ethernet Port Aggregation)機能との連携をサポートします。
詳細は、エッジ仮想スイッチ機能を参照してください。

第2章　その他機能概要

2.1 オートネゴシエーション機能

オートネゴシエーション機能とは、IEEE802.3uに規定された2装置間のプロトコルであり、優先順位に従い通信速度、通信モード（全二重／半二重）やフロー制御の設定を自動的に行う機能です。インバンド(10G/40Gのポート)に関してリンクスピードについてはオードネゴシエーションされませんが、フロー制御設定がオートネゴシエーションにより設定されます。

こんな事に気をつけて

・SFP+ポートで1000BASE-SX/1000Base-Tモジュール、または、QSFP+ポートで40GBASE-CR4ケーブルを使用している場合、オートネゴシエーションモードで動作します。上記以外のモジュールを使用している場合は、固定モードで動作します。オートネゴシエーションでリンクスピードは変更されませんが、フロー制御設定がネゴシエーションされることになります。
・SFP+ポートで1000Base-Tモジュールを使用する場合、1000Base-Tでのみ動作します。
10Base-T/100Base-TXでは動作しません。
・C-Fabric スイッチブレードでは、ポート35はオートネゴシエーションモードで動作します。
なお、バックプレーンポートの接続モード（オートネゴシエーションモード、または、固定モード）
は、サーバ側の接続モード設定に応じて決まります。

· オートネゴシエーション（Auto-Nego）同士の接続は、相互に通信できるモードの中から、決められたアルゴリズムにより通信モードが設定されます。

2.2 フロー制御機能

本装置では、IEEE802.3xに基づくPauseフレームによるフロー制御機能をサポートしています。
フロー制御の設定による各ポートの動作を以下に示します。

こんな事に気をつけて

フロー制御を適用した場合、接続相手が本装置の該当ポートにフレーム送信できなくなることがあります。
この場合、接続相手のバッファ容量によって、本装置に設定している優先機能の優先度に関係なくフレーム廃棄されることがあります。このため、音声や画像などを使用するネットワークの場合は、フロー制御を無効にしてください。
また、接続相手によっては、データフレームの転送性能が劣化することがあります。
フロー制御でPauseフレームを送信するかどうかは、入力ポートの受信バッファ残量で判断されます。ratecontrolで出力キューの長さが制限されているポートに転送されるフレームは出力キュー側で廃棄されるため、入力ポートの受信バッファには溜まりません。結果として、フレームが廃棄されるにも関わらずPauseフレームは送信されません。フロー制御を確実に行うためにはratecontrol の設定がされたポートに転送されることもないようにしてください。

<Auto-nego モードの場合>

フロー制御設定		システム動作
送信	受信	
Off 設定	Off 設定	IEEE802.3x に示されるフロー制御設定を、Pause= なし、Asymmetric Pause= なし（※ 1）としてオートネゴシエーションし、接続相手のフロー制御設定により処理を実行する（※ 2）。
On 設定	Off 設定	IEEE802.3x に示されるフロー制御設定を、Pause= なし、Asymmetric Pause= あり（※ 1）としてオートネゴシエーションし、接続相手のフロー制御設定により処理を実行する（※ 2）。
Off 設定	On 設定	IEEE802.3x に示されるフロー制御設定を、Pause= あり、 Asymmetric Pause= あり（※ 1）としてオートネゴシエーションし、接続相手のフロー制御設定により処理を実行する（※ 2）。
On 設定	On 設定	IEEE802.3x に示されるフロー制御設定を、Pause= あり、 Asymmetric Pause= あり（※ 1）としてオートネゴシエーションし、接続相手のフロー制御設定により処理を実行する（※ 2）。

※ 1）“2 してオートは、対称な Pause 送信／受信能力のあり／なしを示し、“Asymmetric Pause”は、非対称な Pause 送信／受信能力のあり／なしを示します。
対称とは、送信=off／受信=off、送信=on／受信=on のように、送信と受信の設定が対称であることを示します。
また、非対称とは、送信=on／受信=off、送信=off／受信=on のように、送信と受信の設定が非対称であることを示しています。

※ 2）Auto-nego モード時のフロー制御設定は、接続相手のフロー制御設定により、以下の表のとおりに設定されます。

自装置のフロー制御設定		接続相手のフロー制御設定		Auto-nego 結果	
送信	受信	Pause	Asymmetric Pause	Pause 送信	Pause 受信
Off 設定	Off 設定	D.C.	D.C.	N	N
On 設定	Off 設定	なし	D.C.	N	N
		あり	なし	N	N
		あり	あり	Y	N
Off 設定	On 設定	なし	なし	N	N
		なし	あり	N	Y
		あり	D.C.	N（※）	Y
On 設定	On 設定	なし	なし	N	N
		なし	あり	N	Y
		あり	D.C.	Y	Y

※）オートネゴシエーションの結果、送信Pause=Yとなるが、自設定に従って、送信Pause=Nとする。

- D.C. ：Don't Care
- Pause フレーム送信時
  - Y ：フロー制御のためにPause フレームを送出する
  - N ：Pause フレームを送出しない
- Pause フレーム受信時
  - Y ：Pause フレームを受信することがあるため、その場合は受信処理（フロー制御）を行う
  - N ：Pause フレームを受信しない（受信した場合は、Pause フレームを廃棄し、何も処理しない）

<固定モードの場合>

フロー制御設定		通信モード	システム動作	
送信	受信		送信方向	受信方向
Off 設定	Off 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を 実行しない（※ 1）
On 設定	Off 設定	全二重固定	フロー制御のため Pause フレームを送信する。	Pause フレーム受信時は、フロー制御を 実行しない（※ 1）
Off 設定	On 設定	全二重固定	Pause フレーム送出なし	Pause フレーム受信時は、フロー制御を 実行する。
On 設定	On 設定	全二重固定	フロー制御のため Pause フレームを送信する。	Pause フレーム受信時は、フロー制御を 実行する。

※ 1）Pause フレーム受信時は無視する。

2.3 フォワーディングモード変更機能

本装置では、スイッチングの方式として、カットスルーモードとストアアンドフォワードモードを選択することができます。

カットスルーモード

本装置にパケットの先頭部分が入力した後に転送先のポートからパケットを送出します。パケットの全体が入力するのを待たずに転送が行われるため、転送に伴うパケットの遅延(レイテンシ)を最小限に抑えることができます。

ストアアンドフォワードモード

本装置にパケットの全体が入力した後に転送先のポートからパケットを送出します。

こんな事に気をつけて

カットスルーモードを選択した場合には、レイテンシが短縮できる半面、エラーパケットを中継してしまいます。ストアアンドフォワードモードの場合はエラーパケットが入力されても中継しませんが、半面レイテンシはパケットデータを蓄積する分だけカットスルーモードより長くなります。

2.4 MAC アドレス学習/MAC フォワーディング機能

本装置では、MACアドレス学習機能として以下の機能をサポートしています。·

MACアドレス学習基本機能

受信パケットの送信元MACアドレスをダイナミックに学習して、FDB（Forwarding Data Base）に登録する機能です。登録したMACアドレスは、エージングアウト時間まで保持し続けます。エージングアウト時間は構成定義コマンドで変更できます（初期値は300秒）。

ポートがリンクダウンした場合は、FDB上の該当ポートから学習したエントリを削除します。

MACアドレス自動学習停止機能

構成定義によって、装置単位でダイナミックなMACアドレスの学習を停止する機能です。

FDBクリア機能

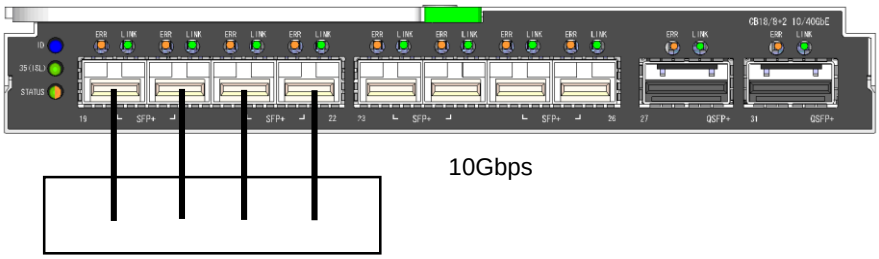
ダイナミックに学習したFDBエントリを削除する機能です。ポート単位、MACアドレス単位など条件指定することもできます。

こんな事に気をつけて

MACアドレス学習は一般的なL2スイッチのVLAN IDとMACアドレスではなく、VFAB IDとMACアドレスでの学習となります。そのため、構成によっては異なるVLAN IDで同じMACアドレスを使用する場合に通信ができなくなる可能性があります。詳細は本ドキュメントの"第3章 C-Fabricの留意事項"を参照してください。

2.5 リンクアグリゲーション機能

リンクアグリゲーション機能とは、複数のポートを多重化し、1本の高速リンク（トランク・グループ）として扱うための機能です。この機能を使用すると、リンクアグリゲーションを構成しているポート(メンバポート）の1本が故障した場合に、そのトラフィックをほかのメンバポートに分散することによって、リンクの冗長性を高めることができます。リンクアグリゲーション機能は、ポートチャネルもしくはポート・トランキングとも呼ばれます。本製品ではメンバポートを構成する場合は、グループ数1～200(ドメイン単位)、1グループ最大10ポート(装置単位)で構成することができます。同一ドメインのC-Fabric構成装置をまたいだリンクアグリゲーション機能(MLAG)もサポートします。



トランク・グループへのトラフィックは、送信パケットのMACアドレスまたは、IPアドレスで判断し、負荷分散されます。
負荷分散のアルゴリズムは以下の方式から選択して指定することができます。

- 送信先MACアドレスと送信元MACアドレスを元にした負荷分散（初期設定値）
- 送信先MACアドレスを元にした負荷分散
- 送信元MACアドレスを元にした負荷分散
- 送信先IPアドレスと送信元IPアドレスを元にした負荷分散
- 送信先IPアドレスを元にした負荷分散
- 送信元IPアドレスを元にした負荷分散

トランク・グループを通信可能とさせる最小メンバポート数を指定することができます。
その場合メンバポートが上記指定数有効となるまでトランク・グループの通信を抑止します。
(有効でないポートとは、例えばリンクダウンしたメンバポートなどは有効でないポートです。)
上記設定は冗長構成などでトランク・グループを必要な帯域が確保できるまで通信させたくない場合に使用します。

こんな事に気をつけて

- 多重化されたポートは、論理的な 1 本のポートとして扱われます。
- リンクアグリゲーションは接続インタフェースが、CIR/EP/ISL のみ使用できます。
  C-Fabric 構築時、US または DS として自動判定された場合もリンクアグリゲーションとして機能します。
- CIR または EP のポートがリンクアグリゲーションでリンクアップしている時、それ以降にリンクアップする物理ポートが同一のトランク・グループ設定である場合、ポートの自動判定は行われずにリンクアグリゲーションとして動作します。そのため、スイッチとリンクアグリゲーションのメンバポートと

を接続した場合、そのポートが自動判定されないためフレームループが発生する可能性があります。

・リンクアグリゲーションのメンバポートがダウンした場合、リンクアグリゲーションの MAC アドレステーブルがクリアされるため、再度 MAC アドレス学習が行われるまで、unicast 通信もフラッディングされます。

・ ファームウェア版数 V02.20 NY0042 以前では、CEE が有効時にポートの type を linkaggregation に変更、もしくは linkaggregation から通常ポートに変更する場合、設定の save と全スイッチの reset が必要となります。

2.5.1 LACP 機能

LACP機能とは、IEEE802.3 準拠のLACPを利用したリンクアグリゲーションです。LACPを取り付けたシステム間で実現可能な最大レベルのリンクアグリゲーションを継続的に提供します。
LACPの利用によってリンクアグリゲーションの整合性確認や、リンクの正常性確認、障害検知の確度を向上できます。

導入のメリット

· 隣接装置と整合性を確認するので、たとえばポートを差し間違えていたといったようなミスがあった場合でも、プロトコルレベルで一本一本正しいリンク先に接続されていることを確認しながら通信を開始します。そのため誤った接続先へ通信してしまうことがありません。
· 隣接装置からの LACP パケットが一定時間受信されない場合は、リンク異常と判断するので、装置ポートの異常検出範囲を超えたリンクの障害検知が可能です。
· ポートがオートネゴシエーションに設定された場合であっても、回線速度が異なるリンクをリンクアグリゲーションのトランク・グループに含めません。

こんな事に気をつけて

· LACP を利用したリンクアグリゲーションは、接続先も LACP を有効にする必要があります。リンクアグリゲーション動作モードに static を指定したなどの LACP 以外のリンクアグリゲーションとは接続できません。
· リンクアグリゲーション動作モードに passive を指定して、接続先も同様に passive とするとリンクアグリゲーションは構成されません。どちらか一方は active と指定してください。双方を active と指定してもかまいません。
· ファームウェア(V02.20 NY0042, V02.20 NY0043V02.30 NY0046)で LACP を用いた Linkaggregation を使用する場合、全メンバポートのリンクダウン時から 1 ポートだけリンクアップさせると Tag 付パケットの通信ができなくなる障害があります。LACP を用いた Linkaggregation を使用する場合、最初は必ずメンバポートが複数リンクアップするようにしてください。(複数ポートをリンクアップさせた後は、その後、リンクダウン等で 1 ポートのみのリンクアップの状態になっても問題ありません。)
・LACP を使用したリンクアグリゲーションの強制アップ設定を有効にしたポートではリンクの障害検知はできません。リンクの障害検知を行いたい場合は、LACP を使用したリンクアグリゲーションの強制アップ設定を無効にしてください。

その他の注意事項については、「2.5 リンクアグリゲーション機能」を参照してください。

2.6 LLDP 機能

LLDP（Link Layer Discovery Protocol）とは、自装置情報を広報することにより隣接装置の把握や接続状態の確認などを行う隣接探索プロトコルです。LLDP情報は、同一物理LANに接続された装置にだけ届き、ルータを超えた先には届きません。
本装置のLLDP機能はIEEE802.1ABに準拠し、以下に示す機能を提供します。

- 自装置情報をLLDPで送信
- LLDPで受信した隣接装置情報を保持
- LLDPに関する情報をMIBとして管理し、SNMP機能でMIBを取得
- 隣接情報が更新されたことをSNMPトラップで通知
- LLDP設定情報、自装置情報、隣接装置情報、統計情報を表示

本装置から送信するLLDP情報には以下に示す情報を含むことができます。またオプション情報は、送信しないように指示することができます。なお、1500バイト以上の情報は送信できないので、この場合には不要なオプション情報は送信しないようにしてください。特に、CEE機能使用時には、1500バイトを越えると、CEEの動作に必要な情報が送信されなくなるので注意してください。実際に送信される内容は、コマンドで確認できます。

- 装置識別情報（代表MACアドレス） （必須）
- 物理ポート識別情報（ifIndex MIB） （必須）
- 保持時間情報（TTL） （必須）
- 物理ポート解説情報（ifDescr MIB） （オプション）
- 装置名称情報（sysName MIB） （オプション）
- 装置解説情報（sysDescr MIB） （オプション）
- 装置主要機能情報（スイッチ／ルータ） （オプション）
- 物理ポート管理アドレス情報（MAC/IPv4/IPv6）（オプション）
- ポートVLAN ID 情報（オプション）
- プロトコルVLAN ID 情報（オプション）
- VLAN名称情報（オプション）
- プロトコルVLAN種別情報（オプション）
- 物理ポート設定情報（オプション）
- 物理ポート電源供給情報 （オプション）
- リンクアグリゲーション情報（オプション）
- 最大フレームサイズ情報（オプション）

隣接装置から受信したLLDP情報は、LLDP情報に含まれている保持時間が経過するまで保持します。保持している隣接情報は、show lldpコマンドで確認できます。詳細は「コンバージドファブリックコマンドリファレンス」を参照してください。

本装置で保持できる隣接情報の最大数を以下に示します。最大保持数を超えたために保持できなかった情報は破棄し、統計情報に破棄したことを計数します。

条件	保持数	
	C-Fabric スイッチブレード	CFX2000
装置全体での最大保持数	510	960
1ポートでの最低保障保持数	1	1
装置全体での共有保持数	476	896
1ポートでの最大保持数（※)	477	897

※） 1ポートで共用分をすべて保持した場合（ほかのポートでは1 台分しか保持できない）

こんな事に気をつけて

・ C-Fabric 構築時、CIR または EP として自動判別された接続インタフェースで本機能を使用する場合、LLDP 機能の動作設定を有効にする必要があります。

・ CIR または EP の LLDP 情報(ポート VLAN ID 情報、VLAN 名称情報)には、VFAB VLAN 情報が設定されます。

2.7 MAC フィルタ機能

MACフィルタ機能では、本装置を経由するパケットをMACアドレス、パケット形式、COS値、IPアドレス、ポート番号などの組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、ネットワークへの負荷を軽減することができます。本装置を通過したパケットがACL 内の"acl mac" 定義、"acl ip" 定義、"acl ip6" 定義、"acl tcp" 定義、"acl udp" 定義、および"acl icmp" 定義に該当した場合にMACフィルタ処理が動作します。

MACフィルタの条件

以下の条件を指定することによって、パケットデータの流れを制御できます。

- パケット入力ポート
  フィルタ処理の対象となるパケット入力ETHERポート
- 動作
  フィルタ処理の対象となるパケットが入力ETHERポートに入力された場合の動作（遮断または透過）
- ACL番号
  MACフィルタの条件となるパケットパターンを定義したACL 番号

MACフィルタ機能の適用範囲

MACフィルタ機能では、ACL で指定したパケットパターンのフィルタを以下の単位で適用指定できます。

- ETHERポート
  ether コマンドで設定します。ETHERポートに対して、指定したACL のパケットパターンに一致した入力パケットに対して、フィルタ処理を実施します。

装置に設定可能な上限

装置に設定可能な上限を以下の表に示します。

1 ～ 2 の項目毎に設定可能上限数と優先度が設けられています。

項	コマンド	優先度	設定可能上限数
1	Macfilter	高	128
2	ip6filter	高	128

2.8 QoS 機能

Qos機能とは、優先制御や優先制御の書き換えを行って、通信の品質を確保する機能です。

2.8.1 優先制御機能

優先制御機能とは、パケットをキューイングし、対応付けされたキューの優先度に従って出力する機能です。
優先制御機能は、入力パケットに対するユーザプライオリティの決定、ユーザプライオリティに対する本装置内部のキューへの対応付け、キューの優先制御の各機能から構成されています。

入力パケットに対するユーザプライオリティは、IEEE802.1pに準拠したCoS、およびタグなし受信パケットに対するデフォルトプライオリティで決定されます。

ユーザプライオリティ付けされたパケットは、そのプライオリティに対応付けられた出力ポート（自装置あてポート含む）の複数のキューにキューイングされます。キューの数は4個で、ユーザプライオリティ値と本装置内部のキューの対応付けは変更可能です。キューはそれぞれ0～3の優先度を持っており、数字が大きくなるにしたがって優先度が上がります。

キューイングされたパケットはキューの優先制御方式に従って出力されます。優先制御方式はStrict Priority Queuing（Strict）、もしくはWeighted Round Robin(WRR) または Weighted Deficit Round Robin（WDRR）から選択します。

ユーザプライオリティ値と優先度の関係

本装置の初期設定および優先制御を行う場合のユーザプライオリティ値と装置内部のキューの推奨設定を、以下に示します。

ユーザプライオリティ値 （Traffic type）	本装置内部の キューの初期設定	優先制御を行う場合のキュー設定 （推奨）
0（Best Effort）	1	1
1（Background）	0	0
2（予備）	0	0
3（Excellent　Effort）	1	1
4(Controlled Load)	2	2
5(Video)	2	2
6(Voice)	3	3
7(Network Control)	3	3

ユーザプライオリティを割り当てる設定

順位	入力パケットのプライオリティの決定方法	有効とする設定
1	CoS	VLAN Tag制御情報上位3ビット(プライオリティ)による。
1	Tagなし受信パケット	qos priority <queue_priority>

優先制御の処理方法

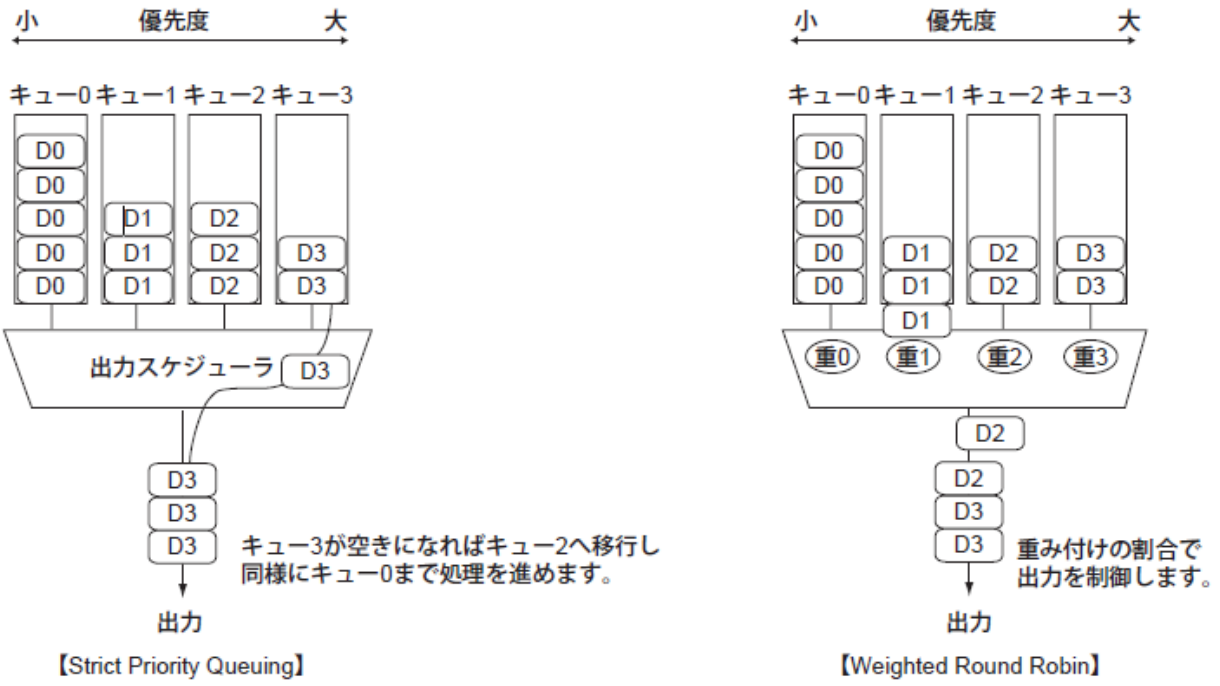
優先制御の処理には、Strict、WRR、WDRRのいずれかを設定します。

• Strict　：優先度の高いキューのフレームを最優先に処理します。

・WRR　：キューごとに一定の数値（出力比）を設定し、相対的な優先制御を行います。たとえば、キュー3 に10 を、キュー0 に1 を設定した場合、キュー3 とキュー0 は10：1 の割合で処理が行われます。

・WDRR ：キューごとに一定の数値（出力比）を設定し、相対的な優先制御を行います。WRRはパケット数を制御するのに対し、WDRRはデータ量を制御します。

以下に、Strict WRRの処理例を示します。



こんな事に気をつけて

・ 本装置で DSCP や CoS 値を書き換える(変更する)ことはできません。

2.9 ブロードキャスト／マルチキャストストーム制御機能

ブロードキャスト／マルチキャストストーム制御機能とは、障害によってブロードキャスト／マルチキャストのパケットがネットワークを大量に流れた場合、それ以外のパケットの通信を阻害しないように、パケットを制御する機能です。

本装置は、ブロードキャスト/マルチキャストパケット流量のしきい値を設定し、ポート単位で制御します。ブロードキャスト/マルチキャストパケットの流量がしきい値を超えた場合は、パケットを破棄またはポートを閉塞し、流量を制限します。

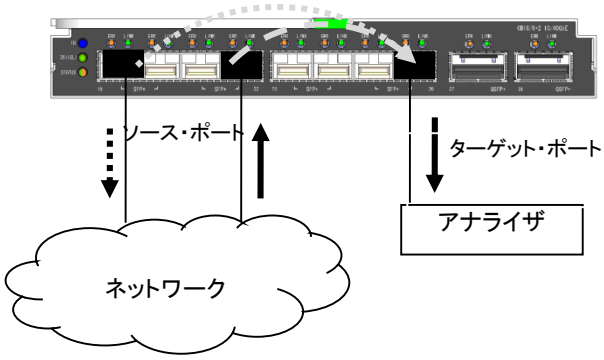
こんな事に気をつけて

ブロードキャスト/マルチキャストパケットの流量がしきい値を超えポート閉塞した場合、そのポート閉塞を解除するには、onlineコマンドによる閉塞解除の指定が必要となります。

1518byteを超えるタグなしフレーム、または 1522byteを超えるタグ付きフレームに対して、ブロードキャスト/マルチキャストストーム制御が行われません。

2.10　ポート・ミラーリング機能

ポート・ミラーリング機能とは指定したターゲットポートに、指定したソースポートの受信／送信／送受信トラフィックをコピーし転送することで、ソースポートのトラフィックを監視する機能です。
ポート・ミラーリング機能を使用する場合は、まずターゲットポートに、LANアナライザなどトラフィックの状況を監視するプローブ装置を接続し、スイッチの設定でターゲットポートと監視するソースポートを指定します。
本装置では複数のソースポートを指定することができます。ただし、複数ポートを指定する際には、対象となるソースポートのトラフィックの合計が、ターゲットポートの帯域を超えないようにしてください。
なお、ソースポートのフロー制御を有効に設定していた場合、ソースポートの通信帯域がターゲットポートの通信帯域を超えると、ソースポートのフロー制御が動作し、実通信側にも影響を及ぼしますので、注意してください。



こんな事に気をつけて

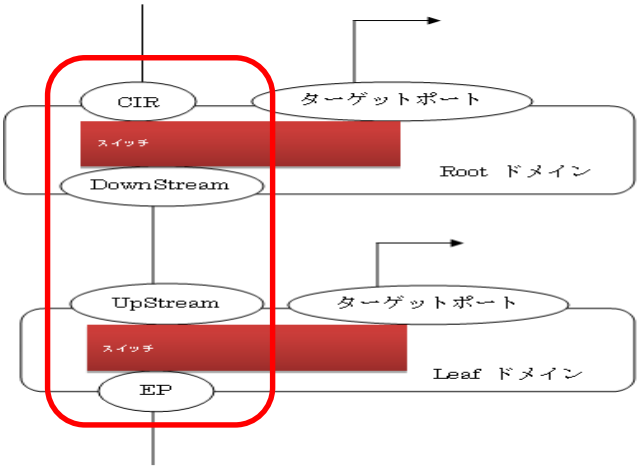
・ミラーのターゲットポートは装置で1ポートしか設定できません。
・ミラーのターゲットポートを設定した場合、そのポートはターゲット専用のポートとなります。他の用途では使用できません。
・ミラーのターゲットで指定したポートをソースとして指定することはできません。
・ミラーのソースポートとターゲットポートは同一の装置のみ指定可能です。
・ミラーのソースポートがターゲットポートに対して複数ある場合、ターゲットポートの帯域を超えた分のパケットは廃棄されます。
・他装置のポートをソースとして指定することはできません。
・ソースポートにリンクアグリゲーショングループを指定した場合は自装置に定義されたポートのみ監視対象となります。
・ターゲットポートに出力されるパケットのVLANタグの有無とその内容については、実際にソースポートで送受信されたパケットと異なる場合があります。ターゲットポートに出力されるパケットは以下のようになります。
　- 送信パケットをミラーリングする場合以下の条件により異なります。
　　➢　装置自発フレームの場合、ソースポートの VLAN 設定に基づいてタグが付けられ、ターゲット

ポートより出力されます。

- 装置自発フレーム以外の場合、必ずタグがつきます。
  タグ付き送信パケットの場合、そのパケットの VLAN タグと、VFAB VLAN ID の２つが付けられてターゲットポートより出力されます。ダブルタグの場合、そのパケットの VLAN タグ２つとも付けられてターゲットポートより出力されます。
  タグ無し送信パケットの場合、Protocol-Based VLAN, Port-Based VLAN 等により適切に VLAN タグが付けられてターゲットポートより出力されます。
- "cfab dot1ad tpid" コマンドにて、ソースポートの TPID 値を未設定時値以外に設定している場合、ターゲットポートから出力されるパケットで受信時にはなかった VLAN タグの TPID 値が出力パケットと異なり、0x8100 となります。

- 受信パケットをミラーリングする場合
  ターゲットポートに出力されるパケットのVLANタグの有無は、入力時のパケットと一致します。

・以下の図の構成で、赤線内の VFAB に対して vfab vlan cir translateコマンドで VFAB VLAN 変換設定された C-Fabric 内で CIR/EP/DS/US からの送受信をミラーリングした際、ターゲットポートから 出力されるパケットの VLAN Tag の形式と内容の差異を以下の表で示します。



CIR ポートをソースポートとしたときの送受信パケットのミラーリングの場合

ミラー動作モード / CIR入力パケット	受信
Untag	Untag
Single Tag	Single Tag (CIR入力パケットと同一の VLAN ID)
Double Tag	Double Tag (CIR入力パケットと同一の VLAN ID)

ミラー動作モード / CIR出力パケット	送信
Untag	Single Tag (VFAB VLAN ID(※1))
Single Tag	Double Tag (VFAB VLAN ID(※1) + CIR出力パケットと同一の VLAN ID)
Double Tag	Double Tag (CIR出力パケットと同一の VLAN ID)

EP(Endpoint) ポートをソースポートとしたときの送受信パケットのミラーリングの場合

ミラー動作モード / EP入力パケット	受信
untag	Untag
Single Tag	Single Tag (EP入力パケットと同一の VLAN ID)
Double Tag	Double Tag (EP入力パケットと同一のVLAN ID)

ミラー動作モード / EP出力パケット	送信
Untag	Single Tag (VFAB VLAN ID(※1))
Single Tag	Double Tag (VFAB VLAN ID(※1) + EP出力パケットと同一のVLAN ID)
Double Tag	Double Tag (EP出力パケットと同一のVLAN ID)

DS(DownStream) ポートをソースポートとしたときの送受信パケットのミラーリングの場合

ミラー動作モード / DS入力パケット(※2)	受信
Single Tag	Single Tag (VFAB VLAN ID(※1))
Double Tag	Double Tag (DS入力パケットと同一のVLAN ID)

ミラー動作モード / DS出力パケット(※2)	送信
Single Tag	Single Tag (VFAB VLAN ID(※1))
Double Tag	Double Tag (VFAB VLAN ID(※1) + CIR に入力されたパケットと同一の VLAN ID)

US(UpStream) ポートをソースポートとしたときの送受信パケットのミラーリングの場合

ミラー動作モード / US入力パケット(※2)	受信
Single Tag	Single Tag (VFAB VLAN ID(※1))
Double Tag	Double Tag (US入力パケットと同一のVLAN ID)

ミラー動作モード / US出力パケット(※2)	送信
Single Tag	Single Tag (VFAB VLAN ID(※1))
Double Tag	Double Tag (US出力パケットと同一のVLAN ID)

※1 …デフォルト VFAB の場合は 2。

FIP スヌーピング機能有効時の SAN の A 系 VFAB の場合は 8、SAN の B 系 VFAB の場合は 9。

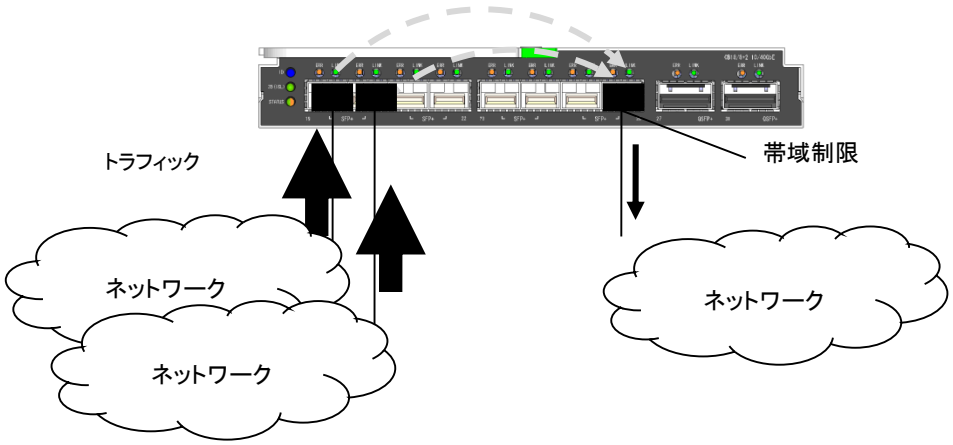
FIP スヌーピング機能無効時の SAN の A 系 VFAB の場合は 10、SAN の B 系 VFAB の場合は 11。

上記以外の VFAB では、VFAB 識別番号 + 100 の値の VLAN ID。

※2 … 対象のソースポートにて untag パケットの入出力が行われることはない。

2.11　出力レート制限機能

出力レート制御機能とは、大量のトラフィックが後続のネットワークに流れないよう、出力ポートの流量を制限する機能です。



本装置は、出力の制限値を設定し、帯域幅をポート単位で制御します。トラフィックの帯域幅がしきい値を超えた場合は、帯域幅を超えるトラフィックが破棄されます。

こんな事に気をつけて

WRR および WDRR を用いた優先制御機能と出力レート制御機能を併用することはできません。

2.12　ポート閉塞機能

ポート閉塞機能とは、物理ポートのリンクダウン状態（ポート閉塞状態）をonlineコマンド発行によるユーザ指示があるまで保持する機能です。障害要因によっては、物理ポートのリンクアップ、リンクダウンが繰り返し発生する可能性があります。そのような場合、本装置は意図的にリンクダウン状態（ポート閉塞状態）を継続させることで、冗長経路が存在する場合は、安定した通信を保つことができます。ポート閉塞状態への遷移は、以下で制御します。

・offlineコマンド発行による手動閉塞
・通信制御機能の連携動作による自動閉塞
・接続ポートのリンク状態変化による自動閉塞

こんな事に気をつけて

・offlineコマンドは、管理者クラスだけ発行可能です。
・閉塞状態となったポートは、onlineコマンドによる閉塞解除指定でポート閉塞を解除してください。
・構成定義を変更した場合、変更内容によっては閉塞が解除される場合があります。
・RootドメインMasterスイッチでofflineコマンドをポート指定なしに発行した場合、ファブリック内すべての装置のポート(CIR/EP)が閉塞されます。なお、ファブリック構成に使用しているポート(ISL/UP/DS)を閉塞する場合は、単独でポートを指定する必要があります。

offline コマンド発行による手動閉塞

Ethernetポート制御コマンドであるofflineコマンドを発行することによってポートを閉塞状態とします。

通信制御機能の連携動作による自動閉塞

ブロードキャスト／マルチキャストストーム制御機能などを使用した場合に、ポート閉塞状態への遷移指定が可能です。本装置でポート閉塞状態への遷移をサポートしている通信制御機能は以下のとおりです。

・ ブロードキャスト／マルチキャストストーム制御機能

接続ポートのリンク状態変化による自動閉塞

接続ポートのリンク状態の変化を契機にポートを閉塞状態にすることを可能にします。
本装置でポート閉塞状態への遷移が可能なリンク状態変化は以下のとおりです。

・起動時閉塞
装置起動時および動的定義反映時にポートを閉塞状態とします。
・リンクダウン回数による閉塞
構成定義で指定した回数分リンクダウンを検出した場合に、ポートを閉塞状態とします。

2.13 IP ホスト機能

IPホスト機能で使用する経路情報は、ルーティングテーブルで管理され、IP パケットの転送先の判断に使用します。
ここでは、IPホスト機能で使用する経路情報の種類、管理方法およびIP ホスト機能で使用する経路情報を制御する機能について説明します。

2.13.1 IP ホスト機能で使用する経路情報の種類

IPホスト機能で使用する経路情報は、以下に示す情報で分類されます。

•インタフェース経路（IPv4）
インタフェースに割り当てたIPv4ネットワークまたはIPv4アドレスを示します。ループバックインタフェースに割り当てたIPv4アドレスは、ホストルート（32ビットネットワークマスク）として管理されます。

•インタフェース経路（IPv6）
インタフェースに割り当てたIPv6プレフィックスを示します。構成定義としてIPv6プレフィックスを設定したときや、Router Advertisement Message でIPv6プレフィックス情報を受信したときに生成されます。ループバックインタフェースに割り当てたIPv6アドレスは、ホストルート（128ビットネットワークマスク）として管理されます。

•RA経路（IPv6）
受信したRouter Advertisement（RA）Messageの情報に基づき、生成されるデフォルトルートを示します。

•スタティック経路（IPv4/IPv6）
構成定義として設定し、装置に保持される経路情報を示します。

IP ホスト機能で使用する経路情報は、以下に示す優先度値で管理されます。

●ＩＰｖ4

ＩＰホスト機能で使用する経路情報	優先度値
インタフェース経路	0(固定)
スタティック経路	1(変更可)

●ＩＰｖ6

ＩＰホスト機能で使用する経路情報	優先度値
インタフェース経路	0(固定)
スタティック経路	1(変更可)
RA経路	12(固定)

2.14 IPv6 機能

IPv6 とは、現在、主に利用されているIPv4を置き換えるための次世代インターネットプロトコルです。
本装置では、IPv6 パケットでのホスト機能動作を行うことができます。
本装置がサポートしているIPv6 ホスト機能は、以下のとおりです。

- 静的な経路設定
- Router Advertisement Message 受信によるアドレスの自動設定
- Router Advertisement Message 受信によるデフォルト経路の自動設定
- Router Advertisement Message 受信によるND情報の自動設定
- ソースアドレスの自動選択

また本装置では、IPv4 パケットだけでなくIPv6 パケットも転送することができます。
本装置がサポートしているIPv6 ルータ機能は以下のとおりです。

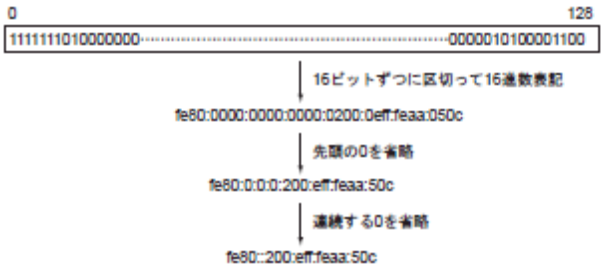
- 静的または動的な経路設定
- パケットフィルタリング

こんな事に気をつけて

- IPv6ホスト機能時は、ICMPv6リダイレクトメッセージは送信しません。
- IPv6ルーティング機能を使用する場合、プレフィックス長が65 ～ 127 の経路情報をルーティングテーブルに登録することはできません。

IPv6 アドレスの表記方法

128 ビットのIPv6 アドレスを表記する場合は、そのアドレスを「:」（コロン）で16 ビットずつに区切って、その内容を16 進数で記述します。個々の16 進数の値について先頭の0 は省略することができます。連続して0 が続く場合は、1 つのIPv6 アドレスの表記で1 回限り「::」で省略することができます。



IPv6 アドレス体系

IPv6 アドレスは、IPv4 アドレスがネットワーク部とホスト部に分離することができるように、プレフィックスとインタフェースID に分離します。一般的には、プレフィックスのビット長（プレフィックス長）は64 ビットで利用されます。プレフィックス長を含めてアドレス表記をする場合は、プレフィックス長はアドレスの後ろに「/」で区切って付与します。

IPv6 で利用することができるアドレスは、先頭のビット数によって利用方法が決められています。本装置で利用できるアドレスは以下のようなものがあります。

- Global Unicast Addresses
  通常利用するアドレスです。一般的には、契約したISP から割り当てられたアドレスや、IPv6 ルータから受信したRouter Advertisement Message 情報を元に自動生成されたアドレスとなります。
- Link-Local Unicast Addresses（fe80::/64）
  リンク内（ルータを介さないで通信できる範囲）だけで有効な特別なアドレスです。このアドレスは先頭の10ビットが1111 1110 10 で始まります。通常は11 ビット目から64 ビット目まではすべて0 となります。
- Multicast Addresses
  マルチキャストアドレスです。先頭の8 ビットが1111 1111 となります。

静的または動的な経路設定

IPv6 のネットワークとルーティングの概念は、IPv4 の場合とほぼ同じです。装置が持つ経路情報に従って転送先を決定します。この経路情報を装置に持たせる方法として、静的な経路設定（スタティックルーティング）と動的な経路設定（ダイナミックルーティング）があります。

スタティックルーティングとは、経路情報を構成定義として設定し利用します。この経路情報は構成定義を変更しない限り変更されることはありません。

ダイナミックルーティングとは、ルーティングプロトコルを利用する通信によって、ネットワーク上のほかのノードから経路情報を学習して利用します。本装置はダイナミックルーティングをサポートしません。

Router Advertisement Message 受信によるアドレスの自動設定

本装置では、Router Advertisement Messageの受信機能をサポートしています。
Router Advertisement Message には、そのネットワークで利用するプレフィックス情報が含まれています。プレフィックス情報を受信した場合、有効期限を管理するためのプレフィックスリストを生成し、インタフェース IDを付加したIPv6アドレスを自動設定します。受信したプレフィックス情報は、show ipv6 ra prefix-listコマンドで参照できます。また、自動設定したIPv6 アドレスは、show ipv6 routeまたはshow interfaceコマンドで参照できます。

こんな事に気をつけて

- 1つのインタフェースで複数のプレフィックス情報を受信する場合は、自動生成の設定を必要な数だけ追加してください。
- 有効期限が365 日を超えたプレフィックス情報（無期限は除く）を受信した場合、365 日の有効期限として動作します。
- プレフィックス情報のプレフィックス長が64以外の場合、そのプレフィックス情報は破棄されます。
- プレフィックス情報のオンリンクフラグと自動アドレス生成フラグが設定されている場合、IPv6 アドレスをインタフェースに設定します。

Router Advertisement Message 受信によるデフォルト経路の自動設定

Router Advertisement Messageを受信した場合、送信ルータのリンクローカルアドレスを中継ゲートウェイとするデフォルト経路を設定します。
複数のルータよりRouter Advertisement Messageを受信した場合、デフォルトルータとして利用できるデフォルトルータリストを生成し、この一覧の中でパケットが到達可能なルータをデフォルトルータとして設定します。
生成したデフォルトルータリストは、show ipv6 ra default-router-listコマンドで参照できます。
また、show ipv6 route コマンドで、設定されたデフォルトルータを参照できます。

こんな事に気をつけて

- 複数ルータからRouter Advertisement Messageを受信した場合、ルータプレファレンスによる優先制御は動作しません。この場合、最初に受信したルータをデフォルトルータとします。
- Router Advertisement Messageによるデフォルト経路の優先度値は12で設定します。スタティックのデフォルト経路と混在運用する場合、スタティック経路の優先度値を変更してください。

Router Advertisement Message 受信による ND 情報の自動設定

Router Advertisement Messageには、通信時に使用する隣接情報（ND情報）が含まれています。
Router Advertisement Messageを受信し、受信メッセージに含まれているND情報と本装置で保持しているND情報が異なる場合は、ND情報の更新が行われます。以下に、本装置で保持しているND情報とその初期値を示します。

- 隣接装置の到達性についての有効期間（初期値は30 秒）

- 隣接装置の到達性確認を行うNeighbor Solicitation（NS）Messageの送信間隔（初期値は1 秒）
- 最大ホップ数（初期値は64）
- 受信ネットワーク上で推奨するMTU長（初期値は1500 バイト）

ソースアドレスの自動選択

IPv6 では、インタフェースに複数のIPv6アドレスが割り当てられることが一般的です。本装置から通信を始め、アプリケーションによって明示的にソースアドレスを指定しない場合は、複数のIPv6 アドレスの中から一定のルールに基づいてアドレスの選択を行います。

本装置がサポートするソースアドレスの選択ルールは、以下のRFCおよびドラフトに準拠します。

- RFC3484：Default Address Selection for Internet Protocol version 6 （IPv6）

2.15 SNMP 機能

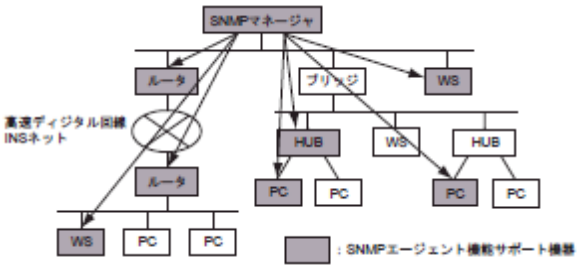
SNMP（Simple Network Management Protocol）とは、IP 層および TCP 層レベルの情報を収集、管理するための IP 管理用のプロトコルです。SNMP 機能では、管理する装置を SNMP マネージャ、管理される装置を SNMP エージェントと言います。SNMP 機能でネットワークを管理する場合、管理する側は SNMP マネージャ機能を、管理される側は SNMP エージェント機能をサポートしている必要があります。

SNMP マネージャ機能は、ネットワーク上の端末の稼動状態や障害状態を一元管理します。SNMP エージェント機能は、SNMP マネージャの要求に対して MIB（Management Information Base：管理情報ベース）という管理情報を返します。

SNMP 機能は、この 2 つの機能を使用して、SNMP マネージャと SNMP エージェントとの間で MIB に定義されたパラメタを送受信してネットワークを管理します。本装置では、SNMPv1、SNMPv2c および SNMPv3 をサポートします。また、標準 MIB および富士通拡張 MIB をサポートしています。C-Fabric 構成では、SNMP マネージャとの通信は関連するドメイン内の Master スイッチが行います。

Master スイッチは、自装置のみならず同一ドメイン内に所属するすべての Slave スイッチの MIB を SNMP マネージャからの要求に応じて取得して返します。また、同一ドメイン内に所属する Slave スイッチで発生した TRAP は、Master スイッチへ通知します。Master スイッチは、スイッチの TRAP や Slave スイッチから通知された TRAP を SNMP マネージャへ通知します。

SNMP 機能による管理



ヒント

◆ **MIBとは**

MIBには、装置のベンダに関係ない標準MIBと装置ベンダ固有の拡張MIBがあります。RFC1213などで定義される標準MIB は管理ノードのそれぞれの管理対象（オブジェクト）にアクセスするための仮想の情報領域です。RFCでは、SNMPエージェントが取り付けるべき管理情報を定義しています。管理情報には、SNMPノードとしてのシステム情報（システム名や管理者名など）やTCP/IP に関連する統計情報があります。しかし、RFCで定義されている項目では伝送路やHUBなどを十分に管理できません。そのため、各種プロトコルの情報や各社の装置ごとのベンダ固有情報に合わせてMIBを拡張します。これを拡張MIBと言います。MIBはASN.1（Abstract Syntax Notation 1）という形式で定義します。SNMPマネージャが拡張MIBを管理するためには、SNMPエージェント側でその拡張MIBを公開して、SNMPマネージャがその拡張MIBの情報を収集するように定義する必要があります。

こんな事に気をつけて

以下のような時にMIB取得が失敗することがあります。

・取得対象のMIBが動的に変わることがあるMIB値(dot1dTpFdbグループなど)の場合

・commit中やsave中の場合

※commitやsaveなどのタイミングでMIB取得を行うと、SNMPマネージャ側でタイムアウトする場合があります。その場合はSNMPマネージャ側のタイマ値を調節(3s～5s)してください。

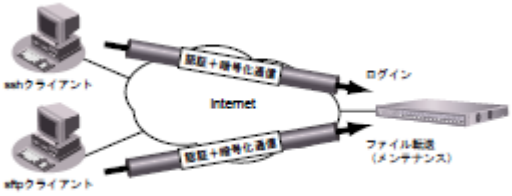
2.15.1 RMON 機能

RMON（Remote Network Monitoring）とは、ネットワーク監視のための標準規格であり、遠隔地にあるLANのトラフィックやエラーなどの通信状況を監視する機能です。
RMON機能はSNMP機能を拡張したものであり、SNMPエージェント側でLANの統計情報を蓄積しておき、SNMPマネージャ（またはRMONマネージャ）からの要求に応じて蓄積したデータをSNMPの応答として返します。
本装置では以下のRMONグループをサポートします。

- statistics グループ
  監視対象ETHERポート上のパケット数やエラー数などの基本的な統計情報を収集します。
- historyグループ
  statistics グループで収集する情報とほぼ同じ統計情報を履歴情報として保持します。履歴情報は一定期間の統計情報として装置内で保持されますので、SNMPマネージャ（またはRMONマネージャ）は一連の統計情報をまとめて取得することができます。

2.16　SSH サーバ機能

SSHサーバ機能とは、TELNETサーバ機能と同じリモートログイン機能（sshサーバ）とFTP サーバ機能と同じリモートファイル転送機能（sftpサーバ）をサポートしています。TELNET サーバ機能およびFTPサーバ機能では、平文テキストデータのまま通信するため、通信内容の傍受や、改ざんが行われる危険性があります。SSHサーバ機能では、ホスト認証および暗号化通信により、安全で信頼できるログイン機能およびファイル転送機能を利用することができます。



※一時点ではどちらか一方の接続のみ

本装置の電源投入時およびリセット時に本装置のSSHホスト認証鍵が生成されます。生成時間は、数十秒から数分です。SSHホスト認証鍵生成開始時と完了時にシスログが出力され、生成完了した時点から本装置にSSH接続することができます。
SSHクライアントソフトウェアにあらかじめ接続相手のSSHホスト認証鍵を設定しておく必要がある場合は、本装置でshow ssh server key dsa コマンドまたはshow ssh server key rsa コマンドを実行して表示されるSSHホスト認証鍵を設定します。
本装置にSSH接続した際に、本装置のSSHホスト認証鍵がSSHクライアント側に送信されて、設定または保存されている鍵と異なる場合は、SSH接続が拒否されます。したがって、装置交換などにより、SSHホスト認証鍵が変更された場合は、SSHクライアントソフトウェアに設定または保存されているSSHホスト認証鍵を再設定するか削除してからSSH接続します。
そのあと、パスワード入力プロンプトが表示されますが、SSHホスト認証などの処理により、表示されるまで多少時間がかかります。
また、serverinfo sshやserverinfo sftp コマンドをoffに設定することにより、SSHサーバ機能を完全に停止させることができます。
sshクライアントとsftpクライアントはSSHポートに接続するため、serverinfoコマンドのsshまたはsftpのどちらかがonの場合、本装置のSSHポートは接続できる状態のままであるため、offに設定した方はパスワード入力まで行われたあとに接続拒否されます。

こんな事に気をつけて

・SSHサーバ機能が完全に停止している状態で本装置を起動し、serverinfoコマンドでSSH機能のどちらかを有効にして設定を反映した場合、SSHホスト認証鍵の生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。
・本装置のSSHサーバ機能は対話ログイン機能のみのサポートとなります。リモートマシンのコマンドを実行する機能はサポートしていません。

以下に、sftp接続とftp接続の相違点を示します。

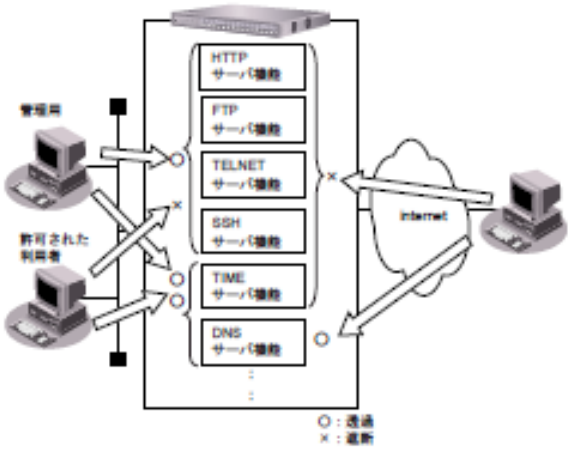
項目	sftp接続	ftp接続
ユーザID指定	接続前に指定 （一部のsftpクライアントは接続開始時に指定する）	接続後に指定 （一部のftpクライアントは接続前に指定する）
バイナリモード指定	なし	あり
パッシブモード指定	なし	あり

本装置でサポートするSSHサーバ機能

項目	サポート内容
SSHサーババージョン	OpenSSH 3.9p1
SSHプロトコルバージョン	SSHプロトコルバージョン2 だけをサポート
SSHポート番号/プロトコル	22 ／TCP
IPプロトコルバージョン	IPv4、IPv6
ホスト認証プロトコル	RSA
ホスト認証アルゴリズムの種類	ssh-rsa, ssh-dss
暗号方式の種類	aes128-cbc、3des-cbc、blowfish-cbc、cast128-cbc、arcfour、aes192-cbc、aes256- cbc、rijndael-cbc@lysator.liu.se、aes128-ctr、aes192-ctr、aes256-ctr
メッセージ認証コードの種類	hmac-md5、hmac-sha1、hmac-ripemd160、hmac-ripemd160@openssh.com、hmacsha1- 96、hmac-md5-96
同時接続数	5

2.17　アプリケーションフィルタ機能

アプリケーションフィルタ機能では、本装置で動作する各サーバ機能に対してアクセスを制限することができます。これにより、本装置のメンテナンスまたは本装置のサーバ機能を使用する端末を限定し、セキュリティを向上することができます。



2.18　ログイン機能

ログイン機能とは、コンソール接続によるログインおよびtelnet接続によるスイッチへログインする機能です。
外部ユーザ認証機能を使用してスイッチへログインする場合は、RADIUS機能、TACACS+機能、LDAP機能を参照して下さい。

C-Fabric内の各スイッチが、ログイン可能なIPアドレスは、以下の表の通りです。

接続先 IP アドレス (IP アドレス体系) / C-Fabric 内スイッチ		ファブリック代表仮想 IP (IPv6/IPv4)	Management LAN 用 IP (IPv6/IPv4)
Root ドメイン	Master	○	○
	Slave	—	○
Leaf ドメイン	Master	—	○
	Slave	—	○

○：ログイン可 —：ログイン不可

C-Fabric内においてコンソールやtelnet接続でログイン後にgoコマンドを使用してC-Fabric内の各スイッチへの移動が可能になります。
goコマンドを実行するスイッチによる移動範囲は以下の表の通りです。
また、goコマンドについては、コマンドリファレンスを参照して下さい。

項番	実行元スイッチ	go コマンド	Root ドメイン		Leaf ドメイン		CFAB 縮退モード異常スイッチ
			Master スイッチ	Slave スイッチ	Master スイッチ	Slave スイッチ	
1	Root ドメイン Master スイッチ	**go fabric**	—	—	—	—	—
2		**go domain**	—	—	○	—	—
3		**go master**	—	—	—	—	—
4		**go switch**	—	○	○	○	○
5	Root ドメイン Slave スイッチ	**go fabric**	○	—	—	—	—
6		**go domain**	—	—	—	—	—
7		**go master**	○	—	—	—	—
8		**go switch**	—	—	—	—	—
9	Leaf ドメイン Master スイッチ	**go fabric**	○	—	—	—	—
10		**go domain**	—	—	—	—	—
11		**go master**	—	—	—	—	—
12		**go switch**	—	—	—	—	—
13	Leaf ドメイン Slave スイッチ	**go fabric**	○	—	—	—	—
14		**go domain**	—	—	—	—	—
15		**go master**	—	—	○	—	—
16		**go switch**	—	—	—	—	—
17	CFAB 縮退モード異常スイッチ	**go fabric**	○	—	—	—	—
18		**go domain**	—	—	—	—	—
19		**go master**	○	—	○	—	—
20		**go switch**	—	—	—	—	—

○：ログイン可 —：ログイン不可

2.19 RADIUS 機能

RADIUS機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（RADIUSサーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、ユーザの認証情報や設定情報、ユーザごとの接続時間を集約して管理することができます。本装置では、RADIUSクライアント機能をサポートしています。RADIUSクライアント機能は、以下のRADIUSサポート機能からAAAを経由して利用されます。

以下に、それぞれの機能で利用可能なAAA情報を示します。

RADIUS サポート機能	認証方式（authentication）	ユーザ情報（authorization）	アカウンティング（accounting）
C-Fabricログイン認証	RADIUS認証	使用しません	使用しません

本装置のRADIUSクライアント機能は、複数台のRADIUSサーバを使用したバックアップ構成または負荷分散構成が可能です。

RADIUSサーバとして定義された認証サーバは、alive状態とdead状態を持ちます。
それぞれの状態の意味は以下のとおりです。

- alive状態
  サーバが使用可能である状態です。
  優先度が高い（定義上の数値が小さい）サーバから優先して使用されます。
  同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。
- dead状態
  サーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかにalive状態のサーバが存在する場合、定義した優先度の値は使用されません。
  復旧待機時間で指定した時間が経過すると、自動的にalive状態に復旧します。
  認証を行う場合、すべてのサーバがdead状態になると、ランダムに1つのサーバで試行し、応答の得られたサーバはalive状態に復旧します。

C-Fabric構成では、RADIUSサーバとの通信は関連する各ドメインのMasterスイッチが行います。各ドメインのMasterスイッチのコンソールからのログインおよび運用LAN/Management LANからのtelnet接続などによるログインを行った場合に対象となるMasterスイッチがRADIUSサーバへの認証要求を送出しMasterスイッチとRADIUSサーバ間でユーザ認証を行うことが出来ます。

こんな事に気をつけて

- RADIUSプロトコルの制約で、同時に認証が行える数は256です。同時に257 以上の認証を行った場合は、両方とも失敗します。
- RADIUSクライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAAグループにRADIUSクライアント機能（aaa radius）とユーザ情報（aaa user）の両方を定義した場合、RADIUSクライアント機能で認証が行われます。RADIUSクライアント機能で認証が成功した場合ユーザ情報は利用されませんが、認証に失敗した場合は、次にユーザ情報で認証を行います。

2.20 TACACS+機能

TACACS+機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（TACACS+サーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、認証（Authentication）、認可（Authorization）およびアカウンティング（Accounting）情報を集約して管理することができます。
本装置では、TACACS+クライアント機能のユーザ認証機能とコマンド認可機能をサポートしています。
ユーザ認証機能とは、アクセスユーザが本装置にログイン時に認証処理を行います。
コマンド認可機能とは、アクセスユーザが本装置の提供するコマンド実行時に認可処理を行います。

TACACS+クライアント機能は、複数台の TACACS+サーバを使用したバックアップ構成または負荷分散構成が可能です。

それぞれの状態の意味は以下のとおりです。

・alive 状態
　サーバが使用可能である状態です。
　優先度が高い(定義上の数値が小さい)サーバから優先して使用されます。
　同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。

・dead 状態
　サーバとの TCP 接続失敗やサーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかに alive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
　復旧待機時間で指定した時間が経過すると、自動的に alive 状態に復旧します。
　認証または認可を行う場合、すべてのサーバが dead 状態になると、ランダムに 1 つのサーバで試行し、応答の得られたサーバは alive 状態に復旧します。

C-Fabric構成では、TACACS+サーバとの通信は関連する各ドメインのMasterスイッチが行います。各ドメインのMasterスイッチのコンソールからのログインおよび運用LAN/Management LANからのtelnet接続などによるログインを行った場合に対象となるMasterスイッチがTACACS+サーバへの認証要求を送出しMasterスイッチとTACACS+サーバ間でユーザ認証を行うことが出来ます。

こんな事に気をつけて

・TACACS+クライアント機能のアカウンティング機能はサポートしていません。
・RADIUS クライアント機能との併用はできません。AAA グループに RADIUS クライアント機能(aaa radius)と TACACS+クライアント機能(aaa tacacsp)の両方を定義した場合、TACACS+クライアント機能は無効となります。AAA グループに TACACS+クライアント機能とユーザ情報(aaa user)の両方を定義した場合は、TACACS+クライアント機能で認証が行われます。TACACS+クライアント機能で認証が失敗しても、ユーザ情報での認証は行われません。
・TACACS+サーバ用共有鍵の定義を省略した場合、認証や認可データは暗号化されません。認証や認可データを暗号化する場合は、共有鍵を定義してください。

・TACACS+コマンド認可機能は、TACACS+ユーザ認証機能を使用してログインした場合のみ有効となります。
・TACACS+ユーザ認証時の権限クラスは、管理者パスワード(password admin set)設定の有無に依存します。
・TACACS+コマンド認可機能は、Web 設定およびＦＴＰ／ＳＦＴＰでは動作しません。
・TACACS+コマンド認可機能で、実際に実行するコマンドとは別のコマンドに対する認可の設定が必要なものは、以下になります。

実行するコマンド	認可設定が必要なコマンド
diff	show running-config(running-config に対して diff を実行する場合)
show tech-support	show(show コマンド全体)
save	show(show コマンド全体)
load	構成定義コマンド全体

以下に管理者パスワードの有無による認証時の権限クラスを示します。

＜管理者パスワードなしの場合＞

一般ユーザクラスでの認証のみ行います。

＜管理者パスワードありの場合＞

管理者クラスでの認証を行い、認証が失敗した場合に一般ユーザクラスでの認証を行います。

2.21 LDAP 機能

LDAP機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（LDAPサーバ）を利用して行う機能です。複数の装置で同じAAA情報が必要な場合や、大量のユーザ情報を管理する場合など、認証（Authentication）情報を集約して管理することができます。
本装置では、LDAPクライアント機能のユーザ認証機能をサポートしています。
ユーザ認証機能とは、アクセスユーザが本装置にログイン時に認証処理を行います。

LDAP クライアント機能は、複数台の LDAP サーバを使用したバックアップ構成または負荷分散構成が可能です。

それぞれの状態の意味は以下のとおりです。

・alive 状態

サーバが使用可能である状態です。
優先度が高い(定義上の数値が小さい)サーバから優先して使用されます。
同じ優先度のサーバが複数存在する場合は、ランダムにサーバが選択されます。

・dead 状態

サーバとの TCP 接続失敗やサーバあてのリクエストがタイムアウトしたことにより、そのサーバの使用を一時的に停止している状態です。ほかに alive 状態のサーバが存在する場合、定義した優先度の値は使用されません。
復旧待機時間で指定した時間が経過すると、自動的に alive 状態に復旧します。
認証を行う場合、すべてのサーバが dead 状態になると、ランダムに 1 つのサーバで試行し、応答の得られたサーバは alive 状態に復旧します。

C-Fabric構成では、LDAPサーバとの通信は関連する各ドメインのMasterスイッチが行います。各ドメインのMasterスイッチのコンソールからのログインおよび運用LAN/Management LANからのtelnet接続などによるログインを行った場合に対象となるMasterスイッチがLDAPサーバへの認証要求を送出しMasterスイッチとLDAPサーバ間でユーザ認証を行うことが出来ます。

こんな事に気をつけて

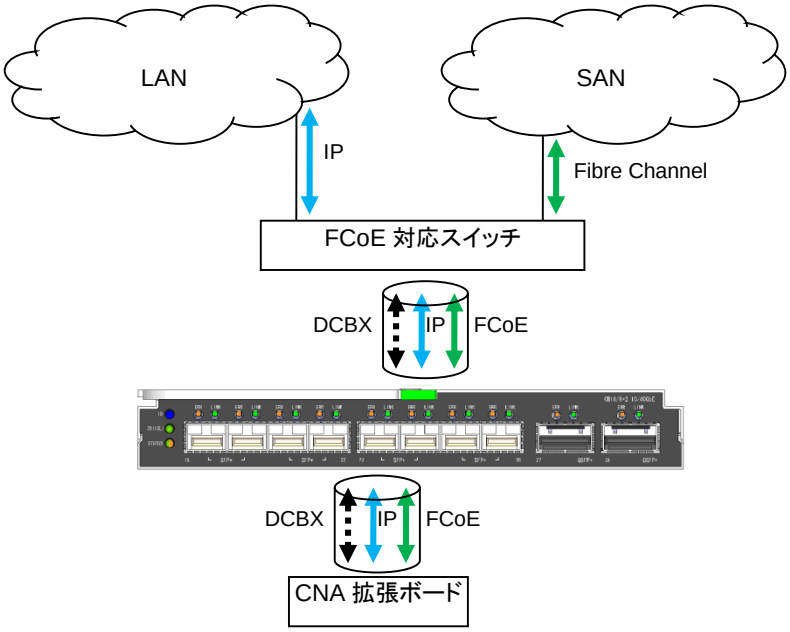
・RADIUS クライアント機能および TACACS+クライアント機能との併用はできません。AAA グループに RADIUS クライアント機能(aaa radius) または TACACS+クライアント機能(aaa tacacsp)と LDAP クライアント機能を定義した場合、LDAP クライアント機能は無効となります。AAA グループに LDAP クライアント機能とユーザ情報(aaa user)の両方を定義した場合は、LDAP クライアント機能で認証が行われます。LDAP クライアント機能で認証が失敗しても、ユーザ情報での認証は行われません。

2.22 SYSLOG 機能

SYSLOGとは、装置の動作状況や発生したイベント情報などをメッセージ(ログ)として採取する機能であり、採取されたメッセージをIPネットワーク上で他の装置へ送受信するプロトコルです。
SYSLOG機能では、ネットワークを通じメッセージを管理する装置をSYSLOGサーバと言います。

C-Fabric構成では、SYSLOGサーバとの通信は関連するRoot ドメインのMasterスイッチが行います。Root ドメインのMasterスイッチは、C-Fabric構成内に所属するすべてのスイッチのSYSLOGメッセージを収集します。それにより、Root ドメインのマスタスイッチとsyslogサーバは、すべてのスイッチのSYSLOGメッセージを管理することが出来ます。

2.23 CEE 機能



CEE (Converged Enhanced Ethernet) 機能とは、従来の LAN, IPC, SAN など、タイプの異なる通信を一つのネットワークに統合するために必要な拡張を Ethernetに追加したものです。SAN (Storage Area Network)用のプロトコルである Fibre Channelを Ethernetで送受信するための FCoE (Fibre Channel over Ethernet) 等で利用されます。本装置では、CEE 機能として以下の要素技術をサポートしています。

ETS (Enhanced Transmission Selection)
複数のトラフィッククラス (Traffic Class. または優先度 Priority) のフローをトラフィッククラスグループ (Traffic Class Group TCG. またはPriority Group PG) としてまとめ、その流量を制御することで各トラフィッククラスグループの最小帯域を確保する機能です。IEEE802.1Qaz として検討されています。各トラフィッククラスグループには、LAN, IPC, SAN など、タイプの異なる通信を割り当てることが想定されています。

DCBX (Data Center Bridging eXchange)
CEE装置のピア間で交換される情報を定義し、ETS (IEEE802.1Qaz) の一部として検討されています。各ピアのETSやPFC設定情報をお互いに通知し、可能であれば設定を整合させる処理を行います。LLDPの拡張として実現されています。

PFC (Priority-based Flow Control)
2.2 節で説明したフロー制御機能はリンクレベルの制御でしたが、これを優先度 (Priority) ごとのフロー制御ができるように拡張するもので、IEEE802.1Qbb として検討されています。たとえばFCoEのようにフレームロスに弱いプロトコル用に設定されたPriorityやPGはPFCを有効にし、ロスを許容しても高いスループットが求められるフローは PFCを無効にするような運用が想定されています。

CEEの設定は、保存後に再起動が行われて初めて適用されます。再起動はRootドメインのマスタスイッチだけではなく、全てのスイッチで再起動が必要となります。

こんな事に気をつけて

- CEE 機能が有効な場合は、ETHERポートに対するACL によるキュー指定またはキュー変更機能の設定は無効となります。
- CEE 機能が有効な場合は、WRR、WDRR を用いた優先制御機能、VLANに対するACL によるキュー指定またはキュー変更機能の設定、2.2 節で説明したリンクレベルのフロー制御機能、qos cosmap コマンドによるプライオリティ毎の格納キュー設定は無視されます。
- トラフィッククラスグループ 15を使用する場合、トラフィッククラスグループ 15は最優先で転送され、その他のトラフィッククラスグループは残りの帯域をそれぞれ指定された帯域幅の割合で分けあいながら転送されます。
- PFCはDCBXによるピア間でのネゴシエーションが完了して初めて有効になります。
- PFCが有効なトラフィッククラスグループのフレームに関しては出力キューの長さが制限されません。このため PFC が有効なトラフィッククラスグループのフレームが多数滞留する状況では他のトラフィッククラスグループまたは他ポート宛のフレームが廃棄されやすくなる可能性があります。
- CEE 機能は 2300Bytes 以下のサイズのフレームに対して有効です。それ以上のサイズのフレームについてはフロー制御が有効に機能しないことや帯域制御が期待通りにならないことがあります。
- トラフィッククラスグループの帯域は百分率で指定しますが、実際に制御可能な最小帯域と最大帯域の比には制限があります。PFC が無効なトラフィッククラスグループのみが 2 つ定義されている場合、最小帯域と最大帯域の比は最大 1:14 になります。PFC が無効なトラフィッククラスグループのみが 3 つ定義されている場合、最小帯域と最大帯域の比は最大 1:7 になります。また、PFC が有効なトラフィッククラスグループが定義されている場合、最小帯域と最大帯域の比は最大 1:4 程度になります。例えば、10Gbps のポートに対してPFCが有効なトラフィッククラスグループとPFCが無効なトラフィッククラスグループを1つずつ定義して使用する場合、帯域をそれぞれ 10 および 90 と設定しても実際には 2Gbps と 8Gbps 程度になるように制御されます。
- CEE 機能が有効な場合、PG15のフレームをCIRにフルワイヤで印加するとファブリック構成を維持出来ません。
- 新しいスイッチがC-Fabricに組み込まれた場合にもCEEを有効にするために再起動が必要となります。C-Fabricにスイッチを追加すると、Rootドメインのマスタスイッチから設定が自動的にダウンロードされるので、その後追加したスイッチの再起動をしてください。

2.24　エッジ仮想スイッチ機能

エッジ仮想スイッチ(Edge Virtual Bridging)機能とは、サーバ仮想化環境においてサーバに接続する隣接スイッチに必要な機能です。サーバ仮想化環境ではサーバ仮想化ソフト上で動作する仮想スイッチが存在し、仮想マシン間の通信をスイッチングします。このため、隣接スイッチでは仮想スイッチの形態に応じた処理が必要となります。本装置ではエッジ仮想スイッチ機能として以下の要素技術をサポートしています。

・Virtual Ethernet Port Aggregator (VEPA)

仮想スイッチの処理を外部の物理スイッチにオフロードする技術です。物理スイッチは個々の仮想マシンを MAC アドレスで識別し、同一物理サーバ上の仮想マシン宛のフレームはリフレクティブリレー(フレームの同物理ポートでの折り返し通信)により送信を行います。

・Automatic Migration of Port-Profile (AMPP)

仮想化環境においては、サーバ上の VM が、故障や負荷の分散の理由等で別のサーバ上に移動した際、該当 VM の持つプロファイル情報（VLAN や QoS、ACL 設定など）について、移動先のサーバに繋がるスイッチのポート上に定義を行う必要があります。

本 AMPP 機能にて VM の移動をスイッチ側で検知し、スイッチ側で移動元のプロファイル情報削除および移動先のプロファイル情報定義を自動で追尾して行うことを可能とします。

こんなことに気をつけて

・リンクアグリゲーションで機能を定義する場合はそのリンクアグリゲーションを構成する全てのポートで同様に定義してください。

2.25 FCoE 機能

FCoE(Fibre Channel over Ethernet)とは、SAN(Storage Area Network)とLAN(Local Area Network)をイーサネットで統合するためのプロトコルで、ANSI T11委員会においてFC-BB-5として標準化されています。

ファイバチャネルが保証するロスレスはFCoEでも必須となります。本装置では、CEE(Converged EnhancedEthernet)機能のPFC(Priority-based Flow Control)によりロスレスを実現し、ETS（Enhanced Transmission Selection）により、帯域の分離を実現します。

本装置のFCoE機能はFC-BB-5 Rev 2.00に準拠しており、コントロールプレーンとしてFIP(FCoE Initialization Protocol)、データプレーンとしFCoEプロトコルをサポートし、ファイバチャネルサービスクラス3で通信を行います。FIPは、ENode(FCoE Node)とFCF(FCoE Forwarder)の間の仮想リンクの確立と維持に使用します。FCoEプロトコルは、ファイバチャネルフレームをイーサネットフレーム内にカプセル化して伝送します。

本装置は、FCoE機能として、FCF機能、FIPスヌーピング機能をサポートします。

FCoE機能を使用する場合はVFABをSANモードで設定する必要があります。SANモードのVFABを設定しない場合FCoE関連のフレームが転送されない為、たとえ外部にFCFがある場合もC-Fabricを通してのFCoE通信を行うことはできません。

FCF 機能

FCFは、ファイバチャネルのスイッチに相当し、ENodeへのファイバチャネルサービスの提供とENode間のFCoEフレーム通信の転送を行う機能です。C-Fabric構成では、FCFはRootドメインスイッチにFCFを配置することができます。またFCoE機能を使用するためにはSANモードVFAB(A系/B系)を定義する必要があります。本装置では、FCF機能として以下の要素技術をサポートしています。

ログイン
ファイバチャネルファブリックにログインするための機能です。ENodeとFCFの間で、FIPを使用して互いの検出とパラメタ交換を行い仮想リンクを確立することで、FCoEフレームによる通信を可能にします。

FCoEフレーム転送
FCoEフレームにカプセル化されたファイバチャネルフレームの宛先ファイバチャネルIDに基づき、FCoEフレームのMACアドレスを書き換えて転送します。

ネームサーバ
ファイバチャネルのGeneric Serviceで規定されたDirectory Serviceが提供するサービスの一つです。ファイバチャネルファブリックにログインしたENodeの情報を管理し、ENodeに対して登録/検索/削除のサービスを提供します。本装置のネームサーバは、FC-GS-6 Rev 9.4に準拠しています。

ゾーニング
ファイバチャネルファブリックにログインしたENodeのアクセス範囲を限定する機能です。同じゾーンに属するメンバ同士の通信を許可し、異なるゾーンのメンバとの通信を許可しないことで不正アクセスを防止します。

NPIV(N_Port_ID Virtualization)
ENodeとFCFの間に確立した仮想リンクを多重化する技術です。

こんな事に気をつけて

・FCF機能を使用するには、C-Fabricを構成する全てのスイッチにFCFライセンスオプションを挿入する必要があります。
・FCFライセンスオプションありのC-Fabric構成に、FCFライセンスオプションが挿入されていないスイッチが接続された場合、FCFライセンスオプションが挿入されていないスイッチがCFAB縮退モードで動作します。
また、FCFライセンスオプションなしのC-Fabric構成に、FCFライセンスオプションが挿入されているスイッチが接続された場合、FCFライセンスオプションが挿入されているスイッチがFCFライセンスオプションの挿入なしとして動作します。
・複数のFCFを接続して1つのファイバチャネルファブリックを構成する機能はサポートしていません。
・ファイバチャネルファブリックを仮想化して論理的に分割する機能はサポートしていません。

FIP スヌーピング機能

FIPスヌーピングとは、FCoEにファイバチャネルと同等のロバストネスを保証する機能です。

ファイバチャネルでは、ファイバチャネルデバイスがファイバチャネルファブリックを介して通信する場合は、事前にファイバチャネルスイッチにログインする必要があります。ポイントツーポイントで接続するため、全ての通信をファイバチャネルスイッチで管理することでセキュリティを確保することができます。

しかし、FCoEでは、ENodeとFCFの間にイーサネットブリッジが介在するとポイントツーポイントが保証されなくなります。本装置では、ENodeとFCFの間のFIPフレーム通信をスヌープしてACLを動的に制御することで、不正な通信を遮断して、ファイバチャネルと同等のセキュリティを確保します。

C-Fabric構成では、FCoE機能を有効に設定することでCIRとEPに自動でFIPスヌーピングが設定されます。

2.26　ループ検出機能

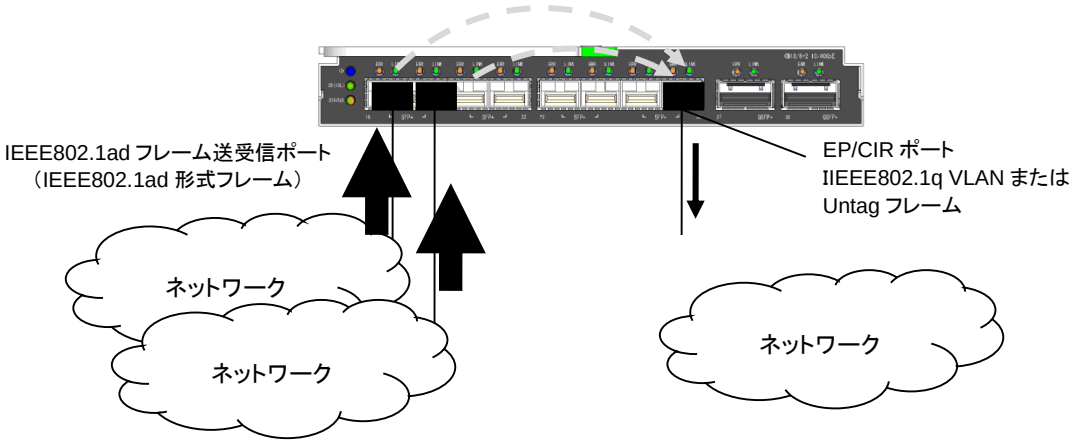
本装置では、ネットワーク上でのパケットのループを防止するためにループ検出およびループしているポートを閉鎖または論理的に遮断することができます。Fabric内のCIRおよびEPの各ポートから送信するループ監視フレームによって、自Fabricが送信したパケットを受信することでパケットのループを検出し、該当するポートを閉鎖または論理的に遮断してループを防止します。

こんな事に気をつけて

・トラフィックが高負荷状態になった場合、ループを検出することはできません。ブロードキャスト／マルチキャストストーム制御機能を併用してください。
・ループ検出時にポートを閉塞する指定を行っていた場合、閉塞されたポートは自動では復旧しません。online コマンドで復旧してください。
・ループ時、異なる VFAB に同一の Tag 付き VLAN ID を設定した場合は、ループを検出します。

2.27　IEEE802.1ad フレーム送受信機能

IEEE802.1adフレーム送受信機能は、C-Fabric外部ポートで受信したIEEE802.1ad形式のフレームをC-Fabric内部に透過的に転送することができます。また他C-Fabric外部ポートで受信したフレームをIEEE802.1ad形式のフレームとして転送することができます。



こんな事に気をつけて

・IEEE802.1ad フレーム送受信機能を使用する物理ポートまたはリンクアグリゲーションポートでは通常 VFAB での Single Tag フレームまたは Untag フレームの送受信は行えません。
　また使用する S-Tag の VLAN ID は以下のようになっています。

VFAB 識別番号	S-Tag VLAN ID
1～3000	VFAB 識別番号+100
default	2

・IEEE802.1ad フレーム送受信機能を使用する物理ポートまたはリンクアグリゲーションポートではその VFAB が使用する全ての VFAB VLAN 情報が同報される場合があります。
・IEEE802.1ad フレーム送受信機能を使用する物理ポートまたはリンクアグリゲーションポートが C-Fabric 内部ポート(US/DS/ISL ポート)として使用された場合は IEEE802.1ad フレーム送受信機能の設定は無効扱いとなり無視されます。
・IEEE802.1ad フレーム送受信機能が有効なポートでは、AMPP 機能はサポートしていません。
・IEEE802.1ad フレーム送受信機能が有効なポートでは、FIP フレームの転送を行いません。
・IEEE802.1ad フレーム送受信機能が有効なポートでは、LLDP 機能をサポートしています。
・IEEE802.1ad フレーム送受信機能が有効なポートでは、ループ検出機能はサポートしていません。

2.28 VLAN スルーモード

VLANスルーモードは対象のvfabで全てのuntag/tag vlanを転送させる設定です。全てのvlanを転送してもよいポートに本設定を行うと、設定の手間が省け、またVLAN用テーブルのエントリ節約にもなります。

VLANスルーモードはポートに対してmodeのon/offを設定し(interface configモードで設定)、vfabと対象のインターフェースグループを設定(global configで設定)します。

具体的にコマンドラインを記述すると、

```
(config-if)#vfab through mode <mode>
(config)#vfab <vfab_id> through ifgroup <interface_group_id_list>
```

で設定することができ、また、untagのvlan idを設定するために

```
(config)#vfab <vfab_id> through untag <vid> ifgroup <interface_group_id_list>
```

を実行することができます。
設定は以下コマンドで確認することができます。

```
(config)# show vfab through
[Machine status:root/master     Switch:1/1]
VFAB ID mode       Untag interface
------- ------- ----- -----------
(1)        (2)        (3)     (4)
default network            1/1/0/24
1          network   11       1/1/0/25
                     11       1/1/0/26
                     11       1/1/0/27
```

VLANスルーモードに設定したポートは他VFABの設定はできません。

第3章　C-Fabric の留意事項

C-Fabric機能を使用するうえで、この章で述べる留意事項があります。
※C-Fabricを使用する際には「コンバージドファブリックスイッチ製品 ご使用上の留意・注意事項」も合わせて参照してください。

1) 装置の保守交換時の対応について

スイッチが故障し、保守用部品との交換が必要となった場合、設定を復元するために、以下のデータを復元する必要があります。修理依頼の際は、保守作業員に情報を提供してください。

交換対象スイッチの

・Fabric ID
・Domain ID
・Domain mode
・Switch ID
・ISLポート番号
・ISLポートの種類(ノーマルまたはLink Aggregation)
・マネジメントポート(oob)の設定値
・C-Fabricのユーザ名、パスワード
・装置名(sysname)[CFX2000のみ]
・CEE設定の設定情報

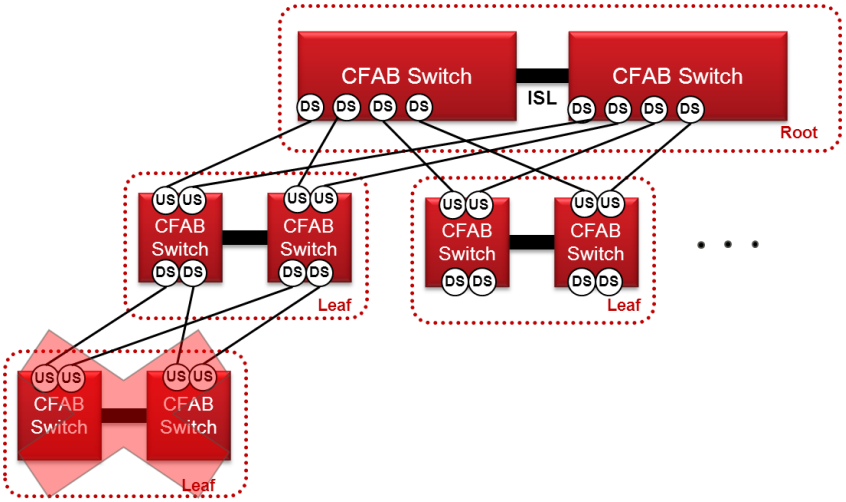
1台のスイッチ構成(RootドメインをRoot Masterスイッチのみで運用する場合)の交換の場合は追加で

・退避させた設定ファイル

V02.30 NY0046以前のファームウェアを使用する場合

チーミング/ボンディングがAuto Failback有効の場合、保守交換時に通信できなくなる場合があるので、その場合はサーバもしくはOS側で保守交換対象品に接続されたポートをofflineにしてください。

2) 下図のようにLeafドメインの下にLeafドメインを接続するような3層のファブリックは使用できません。

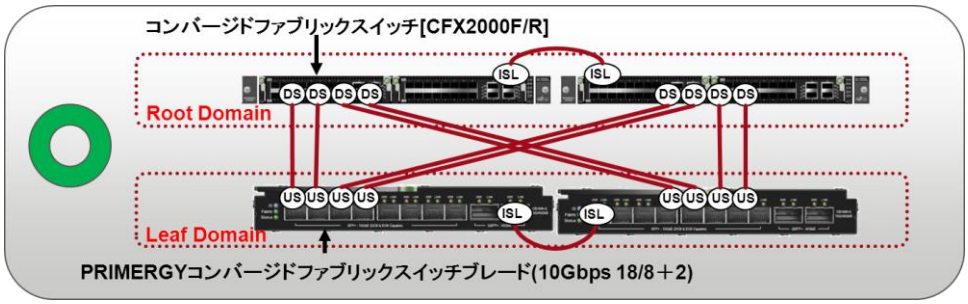


3) EP/CIRポートに対しては、"cfab port-mode external"コマンドを実施し、リンクアップ即通信ができるように設定してください。(本コマンドはV02.20 NY0042以降サポート, LAGに関しては"linkaggregation x x cfab port-mode external"コマンドで設定)
V02.11 NY0033以前を使用している場合、もしくは上記コマンドを設定していない場合、ファブリックの認識を行うためポートがリンクアップしてからパケット転送できるようになるまで10秒～1分ほどかかる場合があります。その為、サーバのNICチーミング機能を使用する場合、Failback機能は無効にする必要があります。Failbackを有効にした場合、障害から復帰したポートのリンクアップにより、LAN通信の切り戻しが発生した後、1分ほど通信できなくなってしまいます。

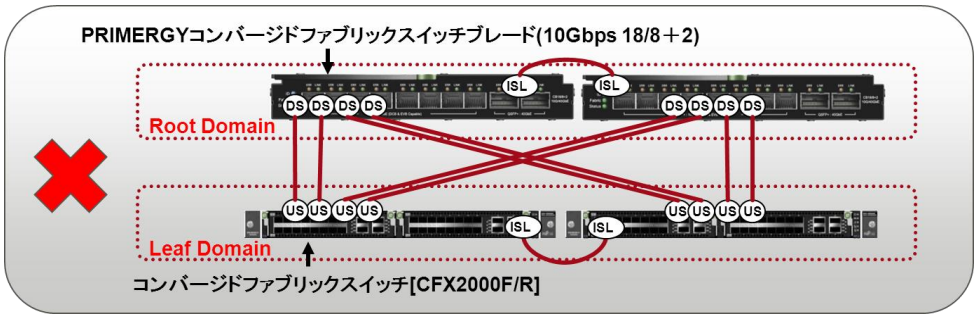
4) VFAB VLAN設定数について
VFAB VLAN設定はC-Fabric全体として33000個まで設定可能です。ただし、VFAB VLAN登録はポートまたはLAG単位での装置内部のエントリを消費し、さらにVFAB VLAN変換設定が有効な場合は、その接続ドメイン数分のエントリを消費します。また装置内部エントリ数は1台につき最大8192エントリです。しかし、実際にはVFAB VLAN登録はハッシュ値を使用して管理しているため、最大数を使い切る前に許容を上回る重複が発生し、VFAB VLAN登録不可能となります。各ポートに適用されるVFAB/VLANの合計数が3000を超える場合、不要なVFAB/VLANを減らす、もしくはスイッチを増やしてノードを分散させる等の対策を行ってください。

5) ファブリックを構築する際にCFX2000をPRIMERGYコンバージドファブリックスイッチブレード(10Gbps 18/8＋2)のドメインツリー配下にすることはできません。例えばRootドメインをPRIMERGYコンバージドファブリックスイッチブレード(10Gbps 18/8＋2)で構成し、Leafドメインを本製品で構成することはできません。

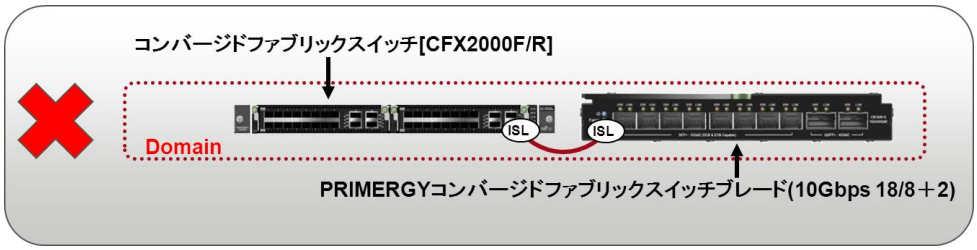
下図はサポート構成。RootドメインがCFX2000で、LeafドメインがC-Fabricスイッチブレード



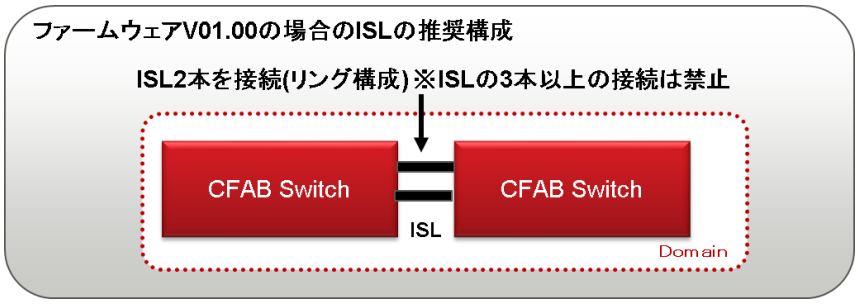
下図は非サポート構成。RootドメインがC-Fabricスイッチブレードで、LeafドメインがCFX2000

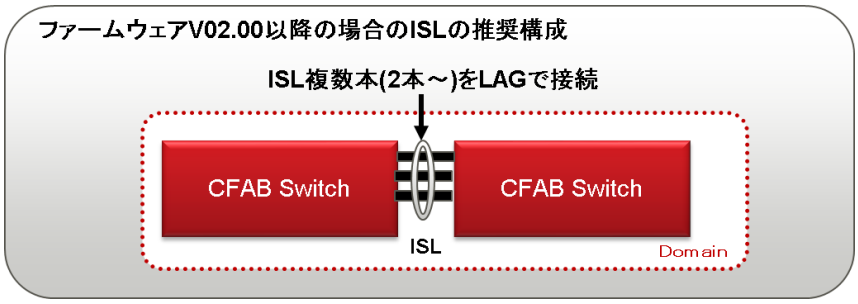


6) ドメインは全て同じ種類のスイッチで構築する必要があります。下図のような構成はできません。



7) ドメインを構築する際、ISLポート接続は冗長化のために複数接続することを推奨します。ISLポートを1本にした場合、何らかの原因でISLポートがダウンしてしまうと、ファブリック上のトラフィック全体に影響が出る可能性があります。
ファームウェア版数V01.00を使用している場合、ISLは3本以上接続することができません。ISLは最大2本の接続(リング状の接続)となります。
ファームウェア版数V02.00以降を使用する場合、ISLは3本以上接続することができます。またISLのLink Aggregation(LAG)を組むことが可能です。ファームウェア版数V02.00以降を使用する場合、ISLは2本以上を使用したLAG接続を推奨します。
(ISLのLAGはV02.00からサポート)



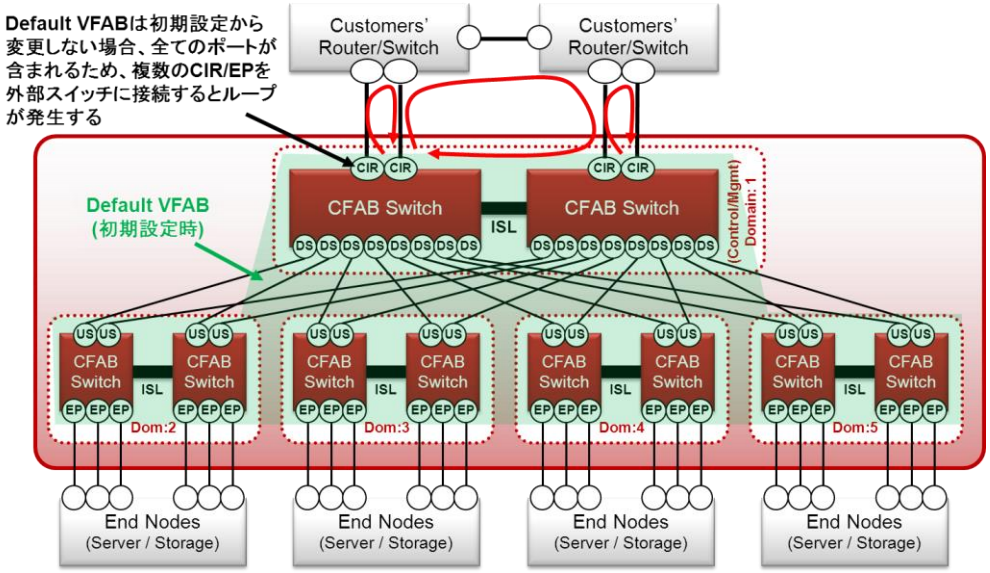


8) Untag/Tag VLAN設定について
同一インターフェースには、untag vlan定義を持つVFABは1つのみ設定可能です。
(例. port1にvfab1 untag 10を設定したらport1にvfab2のuntagは設定できない)
V02.11 NY0033以前を使用している場合、VLAN設定について以下制限があります。
VFAB内で単一VLAN IDをtagとuntag両方で設定することはできません。(V02.20 NY0042で制限解除)
(例. vfab 1でtag vlan 10とuntag vlan 10を使用することはできない)
同一VFAB内で複数VLAN IDのuntag VLANを設定することはできません。V02.20 NY0042で制限解除)
(例. vfab1でuntag vlan 10とuntag vlan 20を使用することはできない)

9) ホストモードを使用する際のVLAN定義削除時のリンクダウンについて
ホストモードでVLAN定義を削除した場合、削除したVLANがわりあてられていたCIRポートが一瞬リンクダウンします。

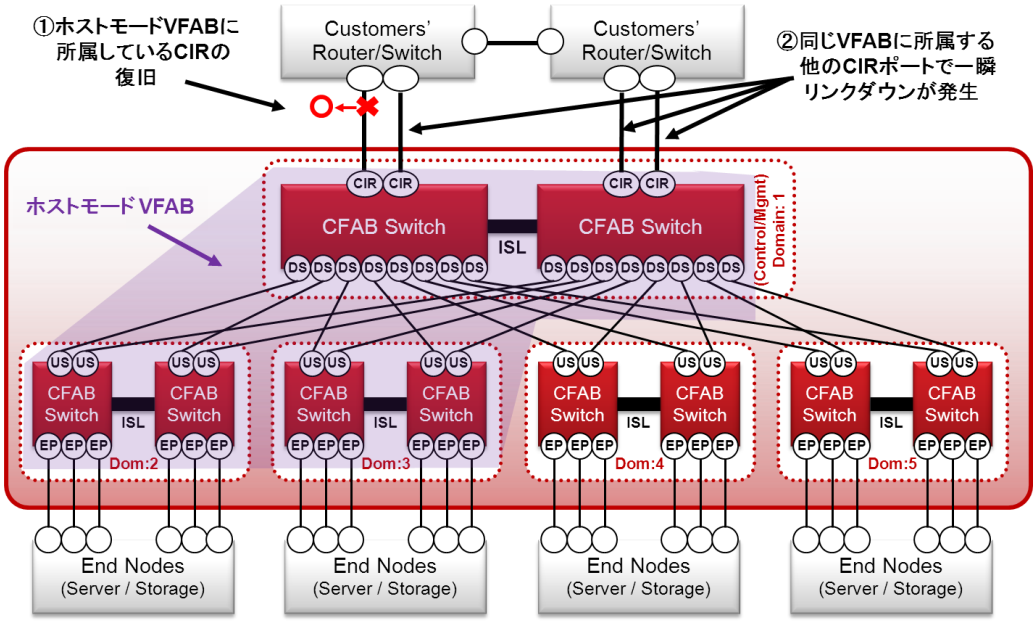
10) ホストモードを使用する際のCIRの接続先ポート設定について
ホストモードで使用するCIRの接続先ポートのSTPはdisableになるように設定してください。

11) Default VFABは初期設定のまま運用せずに、ホストモードへの変更や、ポートへの割り当て設定などを行ってください。Default VFABは初期設定ではネットワークモードで動作し、また全てのポートに割り当てられます。その為、複数の外部接続ポート(EndpointまたはCIRポート)と外部スイッチが接続されている場合、初期設定のまま使用するとループが発生してしまいます。
特にホストモードのVFABを使用する場合、複数のポートを外部スイッチに接続する構成をとりやすいのでお気を付けください。
また、Default VFABの設定は変更を加えると、全ポートへの割り当ては自動的に解除されるので、ポートへの割り当てを必ず行ってください。

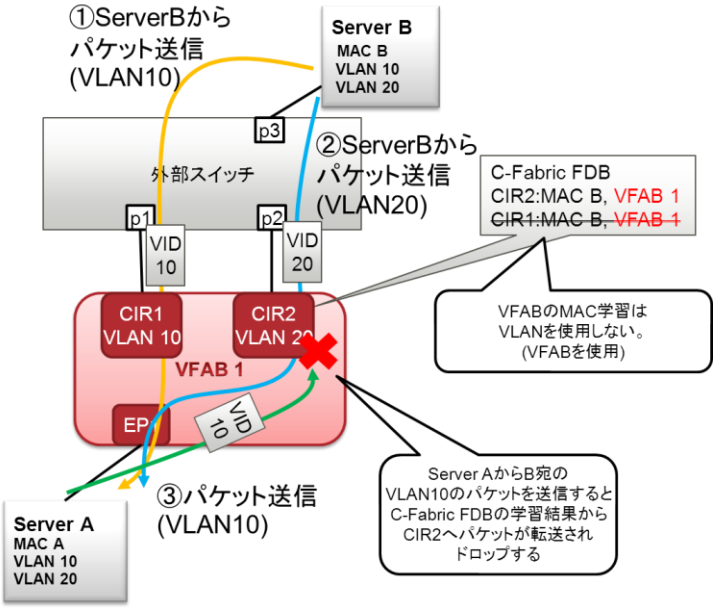


Default VFABは管理用のVFABです。CPU負荷を下げるため、できる限り管理専用のネットワークとして使用し、ブロードキャストやマルチキャストが大量に流れないようにすることを推奨します。

12) 外部スイッチ接続時の通信疎通障害を防止するため、ファームウェアV02.00以降では、ホストモードのVFABに所属するCIRポートのリンク復帰時に、そのVFABに所属する他のCIRポートを一瞬リンクダウンさせ、外部スイッチのMACアドレステーブルを更新するようになっています。

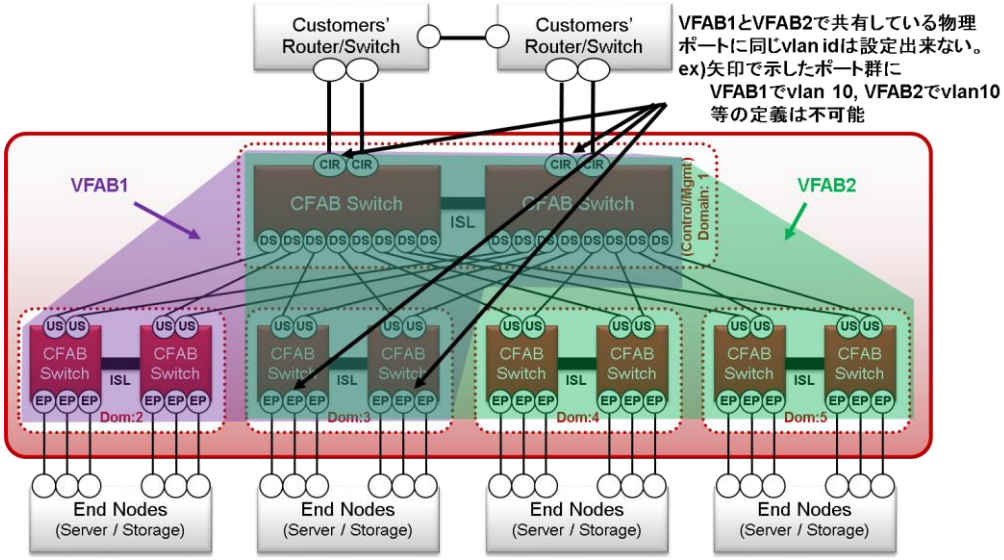


13) LAGを使用せずに複数のポートが外部スイッチに接続されている場合、同一MACアドレスで異なるVLAN IDをもつフレームを受信した際に通信ができない場合があります。
上記問題を回避するために、外部スイッチ複数ポートが接続される場合、それらのポート全てのMACアドレス学習をoffに設定してください。MACアドレス学習無効はC-Fabricのコマンドライン上で、対象ポートのインターフェースコンフィグ上で”mac learning off”コマンドを実行することで無効にできます。学習を無効にした際はknown unicastで外部ポートへ送信されるべきパケットが、unknown unicastとして、スイッチの他のポートへフラッディングされることになります。

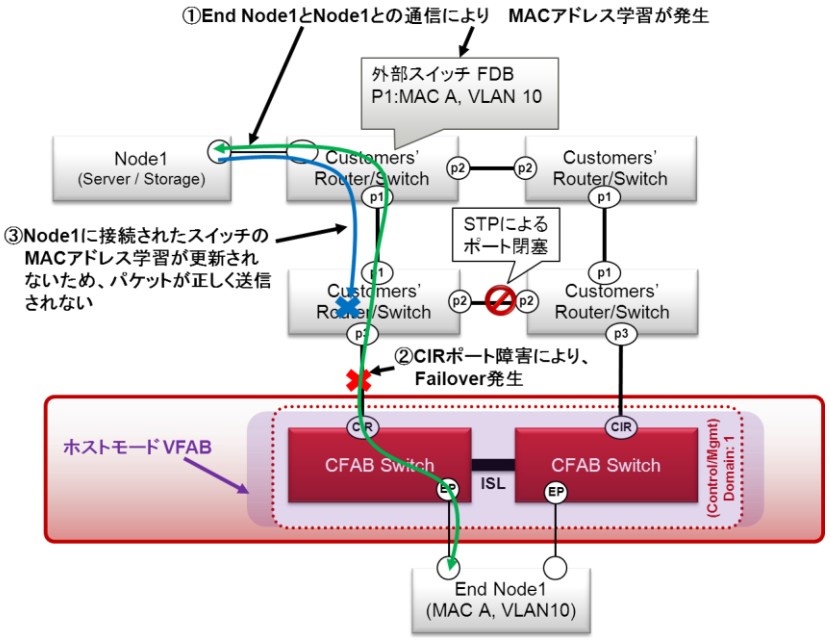


14) CEEの設定をした場合、スイッチのリブートが必要となります。その際は設定を行うRootドメインのMasterスイッチだけではなく、全てのスイッチの再起動が必要となりますので、スイッチの追加等を行う場合は、ファームウェア更新が発生しない場合でもC-Fabricに接続後、再起動を行うようにしてください。

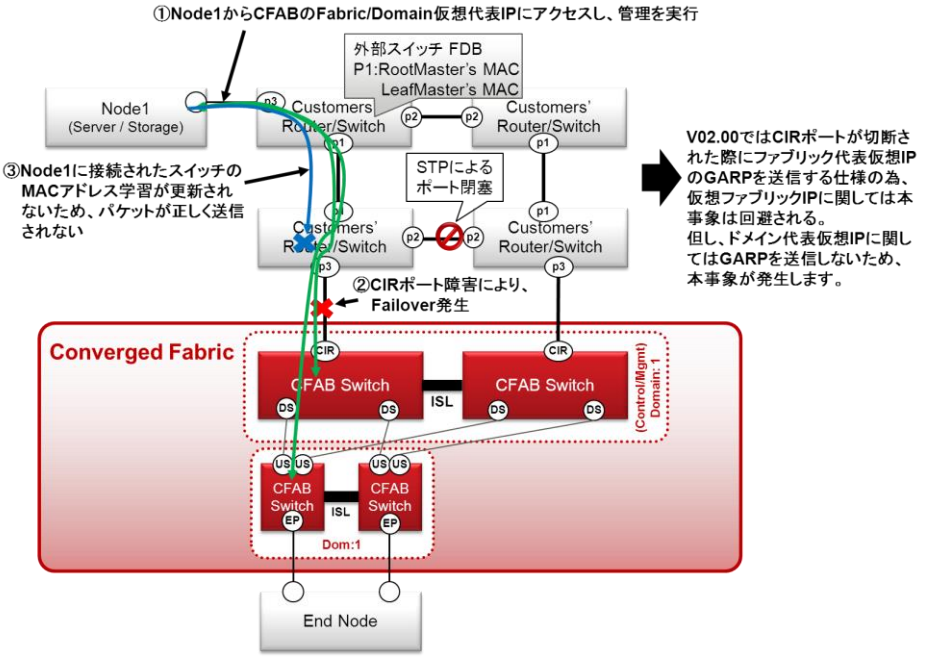
15) 同じ物理ポートにはVFABが異なっていても同じVLANを設定することはできません。例えば、同じ物理ポートにVFAB1のvlan 10とVFAB2のvlan 10を設定することはできません。



16) 下図のように、ホストモードで、複数のCIRポートを外部スイッチに接続し、外部スイッチの先にさらにスイッチがあり、STPを使用している場合、CIRポートに障害が発生した際に、MACアドレス学習に問題が発生し、通信ができなくなってしまう場合があります。



17) 下図のように、ホストモードで複数の CIR ポートを外部スイッチに接続し、外部スイッチの先にさらにスイッチがあり、STP を使用している場合、CIR ポートに障害が発生した際に、MAC アドレス学習に問題が発生するため、ノードから C-Fabric の管理用 IP にアクセスすることができなくなる可能性があります。ファームウェア版数 V02.00 以降ではファブリック代表仮想 IP に関しては CIR ポートの障害時に GARP を出す仕様のため問題ありませんが、ドメイン代表仮想 IP に関しては GARP を出さない為、問題が発生します。



18) ファブリックを構築した際、各種IDやISL関連を除くローカルに設定した値は、Rootマスタで設定されたものが優先されます。ポートのuse offなどの設定も上書きされてしまうため、ファブリック構築前にローカルで設定したものをそのまま維持したい場合は、ファブリック構築後、Rootマスタ上から再度同じ設定を行う必要があります。特にPRIMERGYコンバージドファブリックスイッチブレード(10Gbps 18/8＋2)を使用する場合、初期設定でポート35がuse offになっているので、ファブリック構築後にRootマスタの設定を適用するとuse off設定が消えてしまうので気を付ける必要があります。

19) 以下条件時にshowコマンドを実行した場合、RootドメインのMasterスイッチ以外の情報を取得できない場合があります。取得できなかった場合は再度showコマンドを実行してください。
・ファームウェアアップデート中
・commitコマンド、saveコマンド実行直後
・他セッションでコマンド実行中

20) FCoE機能を使用する場合は、サーバに接続されたポートのFIP-Snooping機能を無効にしてください。FIP-Snoopingの機能の無効はInterface Configモードで"fip-snooping disable"コマンドを実行することにより設定できます。

21) hostモードを使用する場合、CIRポートの切り替え時に数秒通信ができなくなる場合があります。ハートビートのタイムアウト値が数秒程度の場合、hostモードのCIRを経由しないようにするか、networkモードを使用した設計をしてください。

22) FCoEを使用する場合、typeコマンドによるEndpoint/CIRの定義は必須となります。