ネットワーク ポリシー

- ネットワーク制御ポリシー，1 ページ
- イーサネット アダプタ ポリシー，3 ページ
- ダイナミック vNIC 接続ポリシー，5 ページ
- usNIC 接続ポリシーの作成または編集，6 ページ
- LAN および SAN 接続ポリシーについて，7 ページ
- 単一方向リンク検出（UDLD），11 ページ
- フロー制御ポリシー，14 ページ
- ネットワーク制御ポリシー，16 ページ
- Quality Of Service ポリシー，17 ページ
- ID 範囲アクセス コントロール ポリシー，18 ページ
- VMQ 接続ポリシー，19 ページ

ネットワーク制御ポリシー

このポリシーは Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、リモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Central が実行するアクション
- ファブリック インターコネクトへのパケット送信時に複数の異なる MAC アドレスをサーバが使用できるかどうか

- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

[アップリンクのアクションに失敗しました] プロパティ

デフォルトでは、ネットワーク制御ポリシー内の [アップリンクのアクションに失敗しました] プロパティは、リンクダウンの値を使用して設定されます。Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対して vEthernet または vFibre チャネル インターフェイスをダウンさせるように指示します。Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの、イーサネットと FCoE トラフィックの両方をサポートする VM-FEX 非対応の統合型ネットワーク アダプタを使用する Cisco UCS システムの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対してリモート イーサネット インターフェイスをダウンさせるように指示します。このシナリオでは、リモートイーサネットインターフェイスにバインドされている vFibre チャネル インターフェイスもダウンします。

（注） このセクションに記載されている VM-FEX 非対応の統合型ネットワーク アダプタのタイプが実装に含まれ、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、警告の値を使用して [アップリンクのアクションに失敗しました] プロパティを設定することをお勧めします。ただし、この設定にすると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる場合があります。

MAC 登録モード

MAC アドレスは、ネイティブ VLAN でのみデフォルトでインストールされます。これにより、ほとんどの実装で VLAN ポート数が最大になります。

（注） トランキング ドライバがホスト上で実行され、インターフェイスが無差別モードになっている場合、MAC 登録モードをすべての VLAN に設定することをお勧めします。

ネットワーク制御ポリシーの作成

Emulex 統合型ネットワークアダプタ（N20-AE0102）用の MAC アドレスベースのポート セキュリティはサポートされません。MAC アドレスベースのポート セキュリティがイネーブルになっている場合、ファブリック インターコネクトにより、最初にそれが学習した MAC アドレスが含まれるパケットにトラフィックが制限されます。これは、FCoE Initialization Protocol パケットで使用される送信元 MAC アドレスか、イーサネット パケットの MAC アドレスのうち、アダプタに

よって最初に送信されたほうになります。この設定により、FCoE パケットと Ethernet パケットのいずれかがドロップされることがあります。

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Create Memory Qualification] を右クリックし、[Create Network Control Policy] を選択します。

ステップ 4 [Create Network Control Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [CDP]、[MAC Register Mode]、[Action on Uplink Fail] を選択します。

ステップ 6 [MAC Security] 領域で、偽装 MAC アドレスの許可または拒否を選択します。

ステップ 7 [OK] をクリックします。

ネットワーク制御ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Network Control Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

イーサネット アダプタ ポリシー

イーサネットアダプタポリシーは、アダプタのトラフィック処理方法など、アダプタのホスト側の動作を制御します。たとえば、このようなポリシーを使用して、次のデフォルト設定を変更できます。

- キュー
- 割り込み処理
- パフォーマンス拡張

- RSS ハッシュ
- 2 つのファブリック インターコネクトによるクラスタ構成におけるフェールオーバー

オペレーティング システム固有のアダプタ ポリシー

Cisco UCS には、デフォルトで、イーサネット アダプタ ポリシーのセットが用意されています。これらのポリシーには、サポートされている各サーバオペレーティングシステムにおける推奨設定が含まれています。オペレーティング システムはこれらのポリシーに影響されます。通常、ストレージ ベンダーはデフォルト以外のアダプタ設定を要求します。ベンダーが提供しているサポート リストで必須設定の詳細を確認できます。

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

デフォルトの Windows アダプタ ポリシーを使用するのではなく、Windows オペレーティング システム用のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算する必要があります。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 のべき乗の最小値

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9

割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

イーサネット アダプタ ポリシーの作成と編集

ステップ 1 タスク バーで、「Create Ethernet Adapter Policy」と入力して、Enter キーを押します。
これにより、[Create Ethernet Adapter Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] ドロップダウン リストから、イーサネット アダプタ ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。

ステップ 4 [Resources] で、次の手順を実行します。

a) [Transmit Queues] で、割り当てる送信キュー リソースの数を入力します。
b) [Transmit Queue Ring Size] に、送信キュー内の記述子の数を入力します。
c) [Receive Queues] に、割り当てる受信キュー リソースの数を入力します。
d) [Receive Queues Ring Size] で、受信キュー内の記述子の数を入力します。

e) [Completion Queues] で、割り当てる完了キュー リソースの数を入力します。一般的に、割り当てる完了キュー リソースの数は、送信キュー リソースの数と受信キュー リソースの数の合計と一致する必要があります。

f) [Interrupts] に、割り当てる割り込みリソースの数を入力します。通常、この値は、完了キュー リソースの数と同じにします。

ステップ 5 [Settings] で、次の手順を実行します。

a) [Transmit Checksum Offloading]、[Receive Checksum Offloading]、[TCP Segmentation Offloading]、[Large TCP Receive Offloading]、[Receive Side Scaling]、[Virtual Extensible LAN (VXLAN)]、[RDMA over Converged Ethernet (RoCE)]、[Accelerated Receive Flow Steering (ARF)]、および [NVGRE] を有効にするかどうかを選択します。

b) [Interrupt Mode] を選択します。

c) [Interrupt Timer] 値をマイクロ秒単位で入力します。

d) [Interrupt Coalescing Type] を選択します。

e) [Failback Timeout] を秒単位で入力します。

ステップ 6 [Create] をクリックします。

ダイナミック vNIC 接続ポリシー

ダイナミック vNIC 接続ポリシーは、VM とダイナミック vNIC の間の接続を設定する方式を決定します。VM がインストール済みでダイナミック vNIC が設定された VIC アダプタを使用しているサーバを含んだ Cisco UCS ドメインには、このポリシーが必要です。

イーサネット アダプタ ポリシー

各ダイナミック vNIC 接続ポリシーには、イーサネット アダプタ ポリシーが含まれており、ポリシーを含むサービス プロファイルに関連付けられた任意のサーバに対して設定できる vNIC の数を指定します。

サーバの移行

（注） ダイナミック vNIC が設定されているサーバを、またはその他の移行ツールを使用して移行すると、vNIC が使用するダイナミック インターフェイスで障害が発生し、Cisco UCS Central によってその障害が通知されます。

サーバが復旧すると、Cisco UCS Central はサーバに新しいダイナミック vNIC を割り当てます。ダイナミック vNIC 上のトラフィックを監視している場合、監視元を再設定する必要があります。

ダイナミック vNIC 接続ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connection Policies] を右クリックし、[Create Dynamic vNIC Connection Policy] を選択します。

ステップ 4 [Create Dynamic vNIC Connection Policy] ダイアログボックスで、[Name]、説明（任意）、[Naming Prefix]、および [Number of Dynamic vNICs] を入力します。

ステップ 5 ドロップダウン リストから [Adapter Policy] を選択し、[Protection] レベルを設定します。

ステップ 6 [OK] をクリックします。

ダイナミック vNIC 接続ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connections Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

usNIC 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create usNIC Connection Policy」と入力して、Enter キーを押します。
これにより、[Create usNIC Connection Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 作成する usNIC の数を [Number of usNICs] に入力します。

ステップ 5 usNIC に指定するアダプタ ポリシーを [Adapter Policy] で選択します。

ステップ 6 [Create] をクリックします。

LAN および SAN 接続ポリシーについて

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 間の接続およびネットワーク通信リソースを決定します。これらのポリシーは、プールを使用してサーバにMACアドレス、WWN、および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- [admin]：LAN および SAN 接続ポリシーを作成できます
- [ls-server]：LAN および SAN 接続ポリシーを作成できます
- [ls-network]：LAN 接続ポリシーを作成できます
- [ls-storage]：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

LAN 接続ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を右クリックし、[Create LAN Connectivity Policy] を選択します。

ステップ 4 [Create LAN Connectivity Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 vNIC を LAN 接続ポリシーに追加するには、[vNICS] 領域の [Create vNIC] をクリックします。
作成した vNIC が [vNIC] テーブルに追加されます。

ステップ 6 iSCSI vNIC を LAN 接続ポリシーに追加するには、[iSCSI vNICS] 領域の [Create iSCSI vNIC] をクリックします。
作成した iSCSI vNIC が [iSCSI vNIC] テーブルに追加されます。

ステップ 7 [OK] をクリックします。

LAN 接続ポリシー用の vNIC の作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を作成する LAN 接続ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [vNICs] 領域で [Create vNIC] をクリックします。

ステップ 7 既存の vNIC テンプレートを使用するには、[Create vNIC] ダイアログボックスで名前を入力し、[MAC Address Assignment] を選択して [Use vNIC Template] チェックボックスをオンにします。
この領域では MAC プールを作成することもできます。

ステップ 8 [Details] 領域で、[Fabric ID] を選択し、使用する VLAN を選択し、[MTU] を入力します。

ステップ 9 [Pin Group] 領域で、[Pin Group Name] を選択します。

ステップ 10 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
この領域ではしきい値ポリシーを作成することもできます。

ステップ 11 [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
この領域では、イーサネット アダプタ ポリシー、QoS ポリシー、ネットワーク制御ポリシーを作成することもできます。

ステップ 12 [OK] をクリックします。

LAN 接続ポリシー用の iSCSI vNIC の作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 iSCSI vNIC を作成する LAN 接続ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [iSCSI vNICs] 領域で [Create iSCSI vNIC] をクリックします。

ステップ 7 [Create iSCSI vNIC] ダイアログボックスで、名前を入力し、[Overlay vNIC] 、[iSCSI Adapter Policy] 、および [VLAN] をドロップダウン リストから選択し、[MAC Address Assignment] を選択します。
このダイアログボックスでは、iSCSI アダプタ ポリシーと MAC プールを作成することもできます。

ステップ 8 [OK] をクリックします。

LAN 接続ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。

サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

LAN 接続ポリシーからの vNIC の削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [vNICs] テーブルで、削除する vNIC をクリックします。

ステップ 7 [vNICs] テーブル アイコン バーで [Delete] をクリックします。

ステップ 8 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

LAN 接続ポリシーからの iSCSI vNIC の削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 iSCSI vNIC を削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [iSCSI vNICs] テーブルで、削除する vNIC をクリックします。

ステップ 7 [iSCSI vNICs] テーブル アイコン バーで [Delete] をクリックします。

ステップ 8 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

単一方向リンク検出（UDLD）

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は、単一方向リンクを検出するとそのリンクを単方向としてマークします。単一方向リンクは、スパニングツリートポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 メカニズムと連動してリンクの物理ステータスを判断します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続されたインターフェイスのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるインターフェイスの誤接続に起因する単一方向リンクを検出します。アグレッシブ モードの UDLD は、光ファイバ リンクやツイストペア リンク上の片方向トラフィックに起因する単一方向リンク、および光ファイバ リンク上のインターフェイスの誤接続に起因する単一方向リンクも検出できます。

通常モードの UDLD は、光ファイバインターフェイスの光ファイバが誤接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤接続を検出しません。インターフェイスが正しく接続されていてもトラフィックが片方向である場合は、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。その場合、論理リンクは不明となり、UDLD はインターフェイスをディセーブルにしません。UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムはリンクの物理的な問題を検出しないため、

リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブモードは、そのモードをサポートするネットワークデバイス間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブ モードが有効になっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD パケットを受信しなくなると、UDLD はネイバーとの接続の再確立を試み、影響を受けたポートを管理シャットダウンします。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバまたはツイストペア リンクのインターフェイスの片方で、トラフィックの送受信ができない場合。
- 光ファイバまたはツイストペア リンクのインターフェイスの片方がダウン状態で、もう片方がアップ状態の場合。
- ケーブルのうち 1 本の光ファイバが切断されている。

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

  UDLD は、すべてのアクティブ インターフェイスで Hello パケット（別名アドバタイズメントまたはプローブ）を定期的に送信して、他のUDLD対応ネイバーについて学習し、各デバイスがネイバーに関しての最新情報を維持できるようにします。スイッチが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

  インターフェイスがディセーブルになり UDLD が実行中の場合、インターフェイスでUDLDがディセーブルになった場合、またはスイッチがリセットされた場合、UDLD は、設定変更によって影響を受けるインターフェイスの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

- イベントドリブン検出およびエコー

  UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLDデバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべてのUDLDネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ

モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、UDLD はポートをシャットダウンします。

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

- UDLD 対応インターフェイスを別のスイッチの UDLD 非対応ポートに接続すると、その UDLD 対応インターフェイスも単方向リンクを検出できなくなります。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。
- UDLD は、UDLD 対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされます。
  - イーサネット アップリンク
  - FCoE アップリンク
  - イーサネット アップリンク ポート チャネル メンバ
  - FCoE アップリンク ポート チャネル メンバ

UDLD リンク ポリシーの作成または編集

ステップ 1 タスク バーで、「Create UDLD Link Policy」と入力して、Enter キーを押します。
これにより、[Create UDLD Link Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Admin State] を有効にするかどうかを選択します。

ステップ 5 [Mode] を選択します。次のいずれかになります。

- [Normal]：UDLDは、光ファイバ接続におけるインターフェイスの誤接続に起因する単一方向リンクを検出できます。
- [Aggressive]：UDLD は、光ファイバ リンクとツイストペア リンク上の片方向トラフィックに起因する単一方向リンク、および光ファイバ リンク上のインターフェイスの誤接続に起因する単一方向リンクを検出できます。

ステップ 6 [Create] をクリックします。

リンク プロファイルの作成または編集

ステップ 1 タスク バーで、「Create Link Profile」と入力して、Enter キーを押します。
これにより、[Create Link Profile] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、リンク プロファイルを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [UDLD Link] で、リンク プロファイルに関連付ける UDLD リンク ポリシーを選択します。

ステップ 5 [Save（保存）] をクリックします。

フロー制御ポリシー

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、Cisco UCS ドメインのアップリンク イーサネット ポートが IEEE 802.3x ポーズ フレームを送信および受信するかどうかを決定します。これらのポーズ フレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。

LAN ポートとアップリンク イーサネット ポートの間でフロー制御が行われるようにするには、両方のポートで、対応する受信および送信フロー制御パラメータをイネーブルにする必要があります。Cisco UCS では、これらのパラメータはフロー制御ポリシーにより設定されます。

送信機能をイネーブルにした場合、受信パケット レートが高くなりすぎたときに、アップリンク イーサネットポートはネットワーク ポートにポーズ要求を送信します。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。受信機能をイネーブルにした場合、アップリンク イーサネットポートは、ネットワーク ポートからのポーズ要求すべてに従います。ネットワーク ポートがポーズ要求をキャンセルするまで、すべてのトラフィックはこのアップリンク ポートで停止します。

ポートにフロー制御ポリシーを割り当てているため、このポリシーを変更すると同時に、ポーズフレームやいっぱいになっている受信バッファに対するポートの反応も変わります。

フロー制御ポリシーの作成または編集

（注） Cisco UCS Manager の [Policy Resolution Control] でグローバル ポート設定を選択している場合は、すべてのローカル フロー制御ポリシーが削除され、Cisco UCS Central の同じドメイン グループに属しているグローバル フロー制御ポリシーが Cisco UCS Manager に作成されます。

ステップ 1 タスク バーで、「Create Flow Control Policy」と入力して、Enter キーを押します。
これにより、[Create Flow Control Policy] ダイアログボックスが開きます。

ステップ 2 [Domain Group Location] をクリックして、ポリシーを作成するドメイン グループを選択します。

ステップ 3 [Name] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Priority] を選択します。次のいずれかになります。

- [On]：このファブリック インターコネクト上で PPP を有効にします。
- [Auto]：このファブリック インターコネクト上で PPP を使用するかどうかを決めるために Cisco UCS とネットワークがネゴシエーションします。

ステップ 5 [Receive] を有効と無効のどちらにするかを選択します。次のいずれかになります。

- [Enabled]：ポーズ要求に従い、そのアップリンク ポート上のすべてのトラフィックは、ネットワークでポーズ要求が取り消されるまで停止されます。
- [Disabled]：ネットワークからのポーズ要求は無視され、トラフィック フローは通常どおり継続します。

ステップ 6 [Send] を有効と無効のどちらにするかを選択します。次のいずれかになります。

- [Enabled]：着信パケット レートが高くなり過ぎると、 Cisco UCS からポーズ要求がネットワークに送信されます。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。
- [Disabled]：パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。

ステップ 7 [Save（保存）] をクリックします。

ネットワーク制御ポリシー

このポリシーは Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、リモートイーサネットインターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Central が実行するアクション
- ファブリック インターコネクトへのパケット送信時に複数の異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

[アップリンクのアクションに失敗しました] プロパティ

デフォルトでは、ネットワーク制御ポリシー内の [アップリンクのアクションに失敗しました] プロパティは、リンクダウンの値を使用して設定されます。Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対して vEthernet または vFibre チャネル インターフェイスをダウンさせるように指示します。Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの、イーサネットと FCoE トラフィックの両方をサポートする VM-FEX 非対応の統合型ネットワーク アダプタを使用する Cisco UCS システムの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対してリモート イーサネット インターフェイスをダウンさせるように指示します。このシナリオでは、リモートイーサネットインターフェイスにバインドされている vFibre チャネル インターフェイスもダウンします。

（注） このセクションに記載されている VM-FEX 非対応の統合型ネットワーク アダプタのタイプが実装に含まれ、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、警告の値を使用して [アップリンクのアクションに失敗しました] プロパティを設定することをお勧めします。ただし、この設定にすると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる場合があります。

MAC 登録モード

MAC アドレスは、ネイティブ VLAN でのみデフォルトでインストールされます。これにより、ほとんどの実装で VLAN ポート数が最大になります。

（注） トランキング ドライバがホスト上で実行され、インターフェイスがプロミスキャス モードになっている場合、Mac 登録モードをすべての VLAN に設定することをお勧めします。

ネットワーク制御ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Network Control Policy」と入力して、Enter キーを押します。
これにより、[Create Network Control Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Cisco Discovery Protocol (CDP)] を有効にするかどうかを選択します。

ステップ 5 [Action on Uplink Failure] 、[MAC Address Registration] 、および [MAC Address Forging] の値を選択します。

ステップ 6 [Link Layer Discovery Protocol (LLDP) Transmit] および [Link Layer Discovery Protocol (LLDP) Receive] を有効にするかどうかを選択します。

ステップ 7 [Create] をクリックします。

Quality Of Service ポリシー

Quality Of Service（QoS）ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステム クラスを割り当てます。このシステム クラスにより、このトラフィックに対する Quality Of Service が決定されます。一部のアダプタでは、発信トラフィックでバーストやレートなど追加の制御を指定することもできます。

vNIC ポリシー、または vHBA ポリシーに QoS ポリシーをインクルードし、その後、このポリシーをサービス プロファイルにインクルードして、vNIC または vHBA を設定する必要があります。

QoS ポリシーの作成

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [QoS Policies] を右クリックして [Create QoS Policy] を選択します。

ステップ 4 [Create QoS Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Egress] 領域で [Priority] を選択し、[Burst(Bytes)] と [Rate(Kbps)] を入力し、[Host Control] を選択します。

ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーは、vNIC または vHBA テンプレートにインクルードします。

QoS ポリシーの削除

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはポリシーにアクセスする場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [QoS Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ID 範囲アクセス コントロール ポリシー

ID 範囲アクセス コントロール ポリシーを使用して、特定のドメイン グループで利用できるプールを制限します。アクセス コントロール ポリシーをプールに適用すると、選択したドメイン グループだけがそれらのプールにアクセスできます。

ID 範囲アクセス コントロール ポリシーの作成または編集

ステップ 1 タスク バーで「Create ID Range Access Control Policy」と入力して、Enter を押します。
これにより、[Create ID Range Access Control Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Domain Groups] で [Add] をクリックして、このポリシーと関連付けられている [Permitted Domain Groups] を選択します。

ステップ 5 [Create] をクリックします。

VMQ 接続ポリシー

VMQにより、管理オペレーティングシステム全体のネットワークパフォーマンスが向上します。Cisco UCS Central から、サービス プロファイルに vNIC に対する VMQ 接続ポリシーを作成できます。サーバのサービス プロファイルで VMQ vNIC を設定するには、サーバ内の少なくとも 1 つのアダプタが VMQ をサポートしている必要があります。以下のアダプタのうち少なくとも 1 つがサーバにインストールされていることを確認してください。

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

VMQ を使用するには、次のいずれかのオペレーティング システムが必要です。

- Windows 2012
- Windows 2012 R2

サービス プロファイルの vNIC 接続ポリシーを選択するときには、vNIC に対して 3 つのオプション（ダイナミック、usNIC、VMQ 接続ポリシー）のいずれか 1 つを選択してください。サービス プロファイルで 1 度に適用できる vNIC 接続ポリシーは 1 つだけです。

サービス プロファイルの vNIC に対して VMQ ポリシーを選択した場合は、サービス プロファイルで次の設定も行う必要があります。

- BIOS ポリシーで [SRIOV] を選択する。
- アダプタ ポリシーで [Windows] を選択する。

VMQ vNIC 接続ポリシーを設定するには、次の作業を実行します。

- VMQ 接続ポリシーの作成
- サービス プロファイルでのスタティック vNIC の作成
- vNIC への VMQ 接続ポリシーの適用

VMQ 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create VMQ Connection Policy」と入力して、Enter キーを押します。
これにより、[Create VMQ Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Number of VMQs] フィールドに、1 ～ 128 の数字を入力します。

ステップ 5 [Number of Interrupts] フィールドに、1 ～ 128 の数字を入力します。

ステップ 6 [Create] をクリックします。

次の作業

vNIC、vNIC テンプレート、または LAN 接続ポリシーに VMQ 接続ポリシーを関連付けます。