APPENDIX B

# ネットワークと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークに Cisco IronPort アプライアンスを接続するための戦略の一部を示します。

この付録では、次の内容について説明します。



## イーサネット インターフェイス

Cisco IronPort X1050、C650、および C350 アプライアンスには、構成（オプションの光ネットワーク インターフェイスがあるかどうか）に応じて最大 4 個のイーサネット インターフェイスがシステムの背面パネルにあります。次のラベルが付いています。

- Management
- Data1
- Data2
- Data3
- Data4

# IP アドレスとネットマスクの選択

ネットワークを設定するときは、発信パケットを送信するインターフェイスを、Cisco IronPort アプライアンスが一意に選択できるようにする必要があります。この要件によって、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは 1 つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとして任意の IP アドレスを 1 つ使用して、インターフェイスからパケットを送信できます。このプロパティは、Virtual Gateway テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは、IP アドレスの残りのビットです。有効な 4 オクテット アドレスのビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。この形式では、スラッシュの後ろにビット数（1 ～ 32）が続きます。

ネットマスクは、単純にバイナリの 1 を数える方法で表現できます。`255.255.255.0` は「`/24`」になり、`255.255.240.0` は「`/20`」になります。

## インターフェイスの設定例

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。Cisco IronPort アプライアンスの場合は、これらのインターフェイス名を、3 つの Cisco IronPort インターフェイス（Management、Data1、Data2）の中の 2 つのインターフェイスで表現できます。

**ネットワーク 1：**

各インターフェイスが、別のネットワークになっている必要があります。

| インターフェイス | IP アドレス | ネットマスク | ネット アドレス |
|---|---|---|---|
| Int1 | 192.168.1.10 | 255.255.255.0 | 192.168.1.0/24 |
| Int2 | 192.168.0.10 | 255.255.255.0 | 192.168.0.0/24 |

192.168.1.X にアドレス指定されたデータ（ここで X は自身のアドレスを除く 1 ～ 255 のいずれか。この場合は 10）は、Int1 から送出されます。192.168.0.X にアドレス指定されたデータは、Int2 から送出されます。これらの形式でないその他のアドレス（一般的には、外部の WAN またはインターネット）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイは、これらのネットワークのいずれかに存在する必要があります。そして、デフォルト ゲートウェイがパケットを転送します。

**ネットワーク 2：**

2 つの異なるインターフェイスのネットワーク アドレス（IP アドレスのネットワーク部分）は同じにすることができません。

| イーサネット インターフェイス | IP アドレス | ネットマスク | ネット アドレス |
|---|---|---|---|
| Int1 | 192.168.1.10 | 255.255.0.0 | 192.168.0.0/16 |
| Int2 | 192.168.0.10 | 255.255.0.0 | 192.168.0.0/16 |

これは、2 つのイーサネット インターフェイスが同じネットワーク アドレスを持つという、競合した状態を表しています。Cisco IronPort アプライアンスからのパケットが 192.168.1.11 に送信された場合、パケットの配信に使用するイーサネット インターフェイスを決定することができません。2 つのイーサネット インターフェイスが 2 つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。Cisco IronPort アプライアンスでは、競合するネットワークを設定できません。

2 つのイーサネット インターフェイスを同じ物理ネットワークに接続することはできますが、Cisco IronPort アプライアンスが一意の配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

# IP アドレス、インターフェイス、およびルーティング

グラフィカル ユーザ インターフェイスまたは CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、3 つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定された次のような Cisco IronPort アプライアンスがあるとします（すべて /24 と仮定）。

| イーサネット | IP |
|---|---|
| **Management** | 192.19.0.100 |
| **Data1** | 192.19.1.100 |
| **Data2** | 192.19.2.100 |

デフォルト ゲートウェイは 192.19.0.1 です。

AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、Data1（192.19.1.100）の IP を選択した場合、すべての TCP トラフィックが Data1 イーサネット インターフェイスから発生することが予想されます。しかし、トラフィックは、デフォルト ゲートウェイとして設定したインターフェイス（ここでは Management）から送出されますが、送信元アドレスは Data1 の IP になります。

# 要約

Cisco IronPort アプライアンスは、パケットを配信できる一意のインターフェイスを常に識別できなければなりません。この決定を行うために、Cisco IronPort アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせて使用します。次の表に、ここまで説明してきた例をまとめます。

| | 同じネットワーク | 異なるネットワーク |
|---|---|---|
| **同じ物理インターフェイス** | 許可 | 許可 |
| **異なる物理インターフェイス** | 不許可 | 許可 |

# Cisco IronPort アプライアンスの接続時の戦略

Cisco IronPort アプライアンスを接続する際には、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メール トラフィックよりもはるかに少量です。
- 2 つのイーサネット インターフェイスが、同じネットワーク スイッチに接続されているが別のホスト ダウンストリーム上の単一のインターフェイスとのトークで終了する場合、またはすべてのデータがすべてのポートにエコーされるネットワーク ハブに接続されている場合、2 つのインターフェイスを使用しても得られる利点はありません。
- 1000Base-T で動作しているインターフェイスでの SMTP カンバセーションは、100Base-T で動作している同じインターフェイスでのカンバセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークの別の箇所にボトルネックがある場合、ネットワークへの接続を最適化しても意味はありません。ボトルネックが最も頻繁に発生するのは、インターネットへの接続、および接続プロバイダーが存在するアップストリームです。

接続に使用する Cisco IronPort アプライアンスのインターフェイス数と、インターフェイスのアドレスを指定する方法は、基になるネットワークの複雑さによって左右されます。ネットワーク トポロジまたはデータ量から必要になる場合を除いて、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。