



APPENDIX **B**

ネットワーク アドレスと 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 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。

この付録の主なトピックは次のとおりです。

- 「イーサネット インターフェイス」(P.B-585)
- 「IP アドレスとネットマスクの選択」(P.B-586)
- 「IronPort アプライアンスの接続時の戦略」(P.B-589)

イーサネット インターフェイス

IronPort X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンスには、システムの背面パネルに構成に応じて 4 つものイーサネット インターフェイスが搭載されています (オプションの光ネットワーク インターフェイスの有無を問いません)。これらには次のようなラベルが付けられています。

- Management
- Data1
- Data2
- Data3
- Data4

IronPort C60 および C30 アプライアンスには、システムの背面パネルにイーサネット インターフェイスが 3 つ搭載されています。これらには次のようなラベルが付けられています。

- Management
- Data1
- Data2

IronPort C150/160 アプライアンスには、システムの背面パネルにイーサネット インターフェイスが 2 つ搭載されています。これらには次のようなラベルが付けられています。

- Data1
- Data2

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場合、IronPort アプライアンスが発信パケットを送信するインターフェイスを一意に選択できる必要があります。この要件により、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する一部の内容が決定されます。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、特定のネットワーク上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。4 オクテットアドレスの有効ビット数は、**Classless Inter-Domain Routing (CIDR; クラスレス ドメイン間ルーティング)** スタイルで表現されることがあります。すなわち、ビット数（1 ~ 32）の先頭にスラッシュが付きます。

ネットマスクはこうした表現を、単純にバイナリ表記で 1 を数える形で行うことができます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20」となります。

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。IronPort アプライアンスの場合、これらのインターフェイス名は、3 つの IronPort インターフェイス (Management、Data1、Data2) のうちのいずれか 2 つを表します。

ネットワーク 1:

インターフェイスはそれぞれ、別々のネットワークに配置する必要があります。

| 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 に進みます。192.168.0.x にアドレス指定されたデータはすべて、Int2 に進みます。このような形式に該当しないその他のアドレス (WAN やインターネット上のアドレスである可能性が高い) が指定されているパケットはデフォルトのゲートウェイに送信されます。このゲートウェイは、これらのネットワークのいずれかに存在している必要があります。次に、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 |

この場合、2つの異なる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矛盾した状態になっています。IronPort アプライアンスからのパケットを 192.168.1.11 に送信する場合に、どのイーサネット インターフェイスを使用してパケットを送信すべきかを決定する方法がありません。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。IronPort アプライアンスを使用すると、矛盾を含むネットワークを設定できなくなります。

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、IronPort アプライアンスが一意的な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

GUI 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（デフォルトのゲートウェイ）が選択した内容より優先されます。

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 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 |

デフォルトのゲートウェイは 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、ユーザはすべての TCP トラフィックが data1 イーサネット インターフェイスを介して発生すると想定します。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されているインターフェイス（この場合は Management）から発生し、data1 の IP の送信元アドレスのスタンプが付されます。

まとめ

IronPort アプライアンスは、配信するパケットが経由す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、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で使用します。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 | 可 | 可 |
| 異なる物理インターフェイス | 不可 | 可 |

IronPort アプライアンスの接続時の戦略

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。

- 管理トラフィック（CLI、Web インターフェイス、ログ配信）は通常、電子メールのトラフィックに比べて小さいサイズになります。
- 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。
- 1000 Base-T で動作するインターフェイスを介した SMTP キャンパセーションは、100 Base-T で動作する同じインターフェイスを介した場合より若干速くなりますが、これは理想的な条件下でのみです。
- 配信ネットワークのその他の部分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がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続する IronPort アプライアンス インターフェイスの数や、それらのアドレスを指定する方法は、基幹ネットワークの複雑さを考慮した上で決定する必要があります。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、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。

