# よくあるNovell IP およびIPX に関する問題の理解およびトラブルシューティング

## 目次

# 概要

このドキュメントでは、IPX プロトコルに関するさまざまな情報について説明します。 Novell について網羅的に説明することは意図せず、テーマ別によくある質問の最低限のリストを提供します。

# 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 背景説明

## IPXネットワーク番号の理解

他のネットワーク アドレスと同様に、Novell IPX ネットワーク アドレスも一意であることが必要です。 これらのアドレスは 16進フォーマットで示され、2 人の部で構成されています: ネットワーク番号およびノード番号。 IPXネットワーク番号はネットワーク管理者によって割り当てられる長く 32 ビットです。 通常システムのネットワーク インターフェース カード ( NIC ) の 1 つのためのメディア アクセス制御 ( MAC ) アドレスのノード番号は長く 48 ビットです。

- ネットワーク16 進数で表される 32 ビットの値管理者が割り当てる範囲： 0x00000001 - 0xFFFFFFFE0xFFFFFFFF はブロードキャストを表します0xFFFFFFFE がデフォルト ルートです
- ノード16 進数で表される 48 ビットの値NIC カード ( 管理目的で割り当て可能 ) の MAC アドレス

IPX ではノード番号に MAC アドレスが使用されているため、システムでは、ノードに送信することで、データ リンクで使用する MAC アドレスが予測できます。 これに対し、IP ネットワーク アドレスのホスト部分は MAC アドレスと相関関係がないので、IP ノードは Address-Resolution Protocol ( ARP; アドレス解決プロトコル ) を使用して宛先の MAC アドレスを判別する必要があります。

このアドレッシング方式では、もともと、アドレスの 1 つとして 0xFFFFFFFE を使用することが許可されていました。 NLSP が導入されてからは、デフォルト ルートを表すのに「ネットワーク - 2」が使用されます。 Cisco ルータは 0xFFFFFFFE をデフォルト ルートとして扱いますが、これは変更できます。

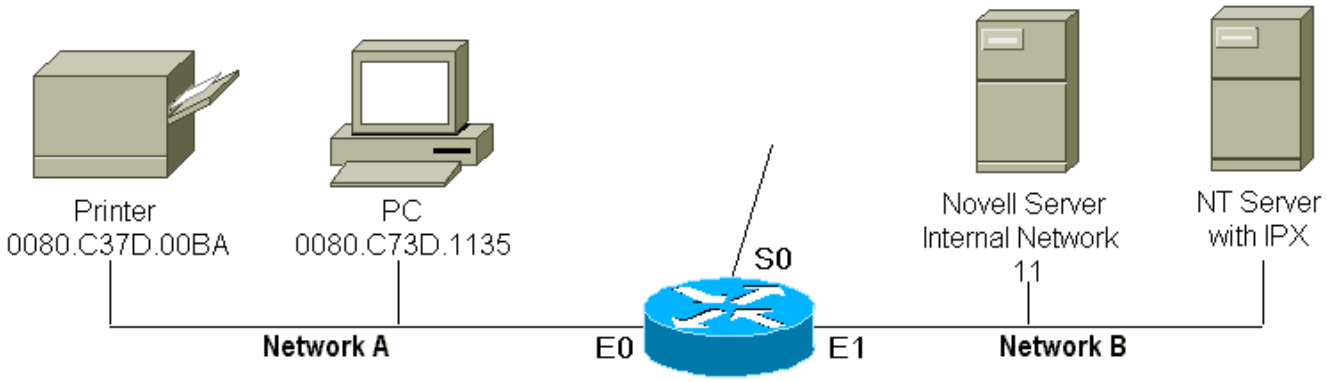
### ネットワーク.ノード アドレスの例

C15C0.0000.0000.0001

BAD.0000.123d.3423

## Novellサーバの内部および外部ネットワーク番号の理解

NetWare 3.x の導入以降、サーバ アーキテクチャはモジュール方式で構成されるようになり、各プロセス ( ゲートウェイ、ルーティング、ファイル、印刷 ) はマルチタスクのコア OS エンジンと通信します。 コアOS エンジン内部ネットワーク番号として知られている IPX ネットワークアドレスは割り当てられそのノード ID は 0000.0000.0001 常にです。 従って、各 Novell 3.x/4.x サーバにネットワークアダプタに結合 される 外部 ネットワーク 番号が付いている内部ネットワーク番号があります。 ネットワーク アダプタは、それぞれが固有のフレーム タイプを使用する複数のネットワーク アドレスにバインドできます。 さらに、Novell サーバは、複数のネットワーク アダプタを装備でき、異なるネットワーク セグメント間のルーティングが可能です。 IPX を実行する Microsoft NT Server は、0000.0000.0001 というノード ID では表示されず、内部および外部のネットワーク アドレスという概念はデフォルトでは使用されません。




```
IPX Routing  0000.0C34.E923

interface ethernet 0
   ipx network A

interface ethernet 1
   ipx network B
```

| Device | Network | Node |
|---|---|---|
| Printer | A | 0080.C73D.00BA |
| PC | A | 0080.C73D.1135 |
| RTR-E0 | A | 0000.0C34.C923 |
| RTR-E1 | B | 0000.0C29.DCFA |
| Novell Server (Int) | 11 | 0000.0000.0001 |
| Novell Server (Ext) | B | 0000.1B3D.5678 |

## Novellカプセル化

Novell のカプセル化には多くの種類があります。 イーサネットだけでも、4 つの種類があります。 同じメディア上にあるデバイス同士でも、使用するカプセル化方式が異なると通信できないので、カプセル化タイプは非常に重要です。 通常、Novell クライアントはリンクで使用できるカプセル化に適応できますが、IPX サーバでは整合性のあるカプセル化タイプがハードコードされている必要があります。

カプセル化の名前は、Novell と Cisco で異なります。 異なる種類のメディアで使用できる IPX カプセル化の概要を次の表に示します。

## IPXカプセル化の命名規則

| | Cisco IOS の命名規則 | Cisco Catalyst スイッチの命名規則 * | Novell ソフトウェアの命名規則 | LSAP | 説明 |
|---|---|---|---|---|---|
| **イーサネット** | Novell-Ether | 8023RAW | Ethernet_802.3 (raw) | FFFF | LLC または SNAP のないイーサネット |
| | ARPA | Ethernet II ( EII ) | Ethernet_II | 8137 | Ethernet II s/ タイプ 8137 |
| | SAP | 8023 | Ethernet_802.2 | E0E0 | 802.2 エンベロープを使用するイーサネット |
| | SNA | SNAP | Ethernet_S | A | Ethernet s/ 802.2 |

| | | | | | |
|---|---|---|---|---|---|
| | P | | NAP | AAA | エンベロープ + SNAP |
| **FDDI** | SNAP | SNAP | FDDI_SNAP | AAAA | 802.2 + SNAP を使用する FDDI |
| | SAP | SAP | FDDI_802.2 | E0E0 | 802.2 エンベロープを使用する FDDI |
| **トークンリング** | SAP | 該当なし | トークン リング | E0E0 | トークン リングおよび 802.2 |
| | SNAP | 該当なし | Token Ring_SNAP | AAAA | トークン リングおよび 802.2 + SNAP |

- フレーム タイプ ETHERNET_802.3 は、Novell 固有のカプセル化です。 SPX/IPX パケットを 802.3 フレーム内に直接格納し、802.2 LLC または SNAP は使用しません。 Cisco の用語では、これを Novell カプセル化 NOVELL-ETHER と呼びます。
- フレーム タイプ ETHERNET_II は、「標準」のイーサネット II フレーミングです。 SPX/IPX パケットは型コード 8137 を使用して Ethernet II 帯に、詰め込まれます。 これらの帯は 2オクテット タイプ コード/フレーム長 フィールドのだけ Novellフレームと異なります; さもなければ、それらは同一です。 Cisco の用語では、これを Novell カプセル化 ARPA と呼びます。
- フレームタイプ ETHERNET_802.2 は Netware 3.12 のための Novell の好まれたカプセル化、Netware 4.X サーバです: それは 802.2 エンベロープのイーサネットです。 Cisco の用語では、これを Novell カプセル化 SAP for 9.21 と呼びます。
- フレーム タイプ ETHERNET_SNAP は、802.2 エンベロープ + SNAP を使用するイーサネットです。 通常、これは使用されません。 Cisco の用語では、これを Novell カプセル化 SNAP と呼びます。

*** Catalyst シリーズ スイッチでの IPX の設定は、イーサネットと FDDI のブリッジ設定に対してのみ適用されます。**

## IPX ルーティングプロトコル

以下のプロトコルを使用すると、IPX ルータが認識するルートとサービスを、動的に定義して管理できます。

- SAP（Service Advertisement Protocol）： サーバやルータなどのネットワーク リソースをネットワーク クライアントが認識できるようにする IPX プロトコルです。 SAP は、個別のネットワーク サービスが存在するインターネットワーク上の場所を特定するために必要です。
- RIP（Routing Information Protocol）： ルーティング メトリックとしてホップ カウントとティックを使用する Interior Gateway Protocol（IGP）です。 ホップ カウントは、送信元と宛先の間の距離を表します。 送信元と宛先の間の往復応答時間は、ティックつまり 1/18 秒単位で表されます。 RIP は、ルーティング テーブルを学習、選択、および管理します。 RIP

は、独立したシステム内でルーティング情報を交換するために使用される距離ベクトル型プロトコルです。RIP と SAP は連携して機能し、クライアント、サーバ、およびルータがネットワーク サービスを検索して、各サービスにルーティングするのを助けます。 また、クライアントとサーバの間の通信およびルータ間の通信にも使用されます。

- IPX EIGRP： IGRP は、TCP/IP および OSI インターネットで使用される Cisco の Interior Gateway Routing Protocol です。 IGRP は、各ルータがネットワーク全体のすべてのルータ/リンク関係を知る必要がないように、距離ベクトル型のルーティング テクノロジーを使用します。 各ルータは、宛先とそれに対応する距離をアドバタイズします。 その情報を受信した各ルータは、距離を調整して、その情報を隣接ルータに伝搬します。IGRP における距離は、使用可能な帯域幅、遅延、負荷率、およびリンク信頼性の総合情報として表されます。 これにより、リンク特性を微調整して最適なパスを実現できます。EIGRP は IGRP の拡張版です。 EIGRP では IGRP と同じディスタンス ベクトル テクノロジーが使用され、基盤となる距離情報も変更されていません。 このプロトコルはコンバージェンス特性と運用効率が大幅に向上しています。 そのため、IGRP への既存の投資を保護しながら、アーキテクチャを改善することができます。 EIGRP の詳細については、次のドキュメントを参照してください。 EIGRP 概要プロトコル依存モジュールは、ネットワーク層でプロトコル固有の要件を実行します。 たとえば、IPX-EIGRP モジュールは、IPX でカプセル化された EIGRP パケットを送受信します。 IPX-EIGRP は、EIGRP パケットの解析、および受信した新しい情報の Diffusing Update Algorithm（DUAL）への通知を担当します。 IPX-EIGRP はルーティングの決定を DUAL に依頼し、その結果は IPX ルーティング テーブルに格納されます。 IPX-EIGRP には次の機能があります。自動再配布：ユーザがコマンドを入力しなくても、IPX RIP のルートは EIGRP に自動的に再配布され、IPX-EIGRP のルートは RIP に自動的に再配布されます。 no redistribute protocol ルータ サブコマンドを使用すると、再配布をオフにできます。 ルータでは、IPX-RIP と IPX-EIGRP の両方を完全に無効にすることができます。ネットワーク幅の拡大： IPX RIP では、ネットワークで可能な最大の幅は 15 ホップです。 IPX-EIGRP を有効にすると、可能な最大幅は 224 ホップになります。 EIGRP メトリックは数千というホップをサポートするのに十分な大きさであるため、ネットワークの拡張の障害となるのはトランスポート層のホップ カウンタだけです。 この問題へのシスコの対応は、IPX パケットが 15 台のルータを通過し、宛先へのネクストホップが EIGRP を介して学習された場合にトランスポート制御フィールドを増加させることだけです。 RIP 経路が宛先へのネクストホップとして使用されている場合、トランスポート制御フィールドは通常どおりに増加します。差分 SAP 更新 - 完全な SAP 更新は、EIGRP 隣接ルータが検出されるまで定期的に送信され、その後は SAP テーブルに変更があった場合にだけ送信されます。 これは EIGRP の高信頼性転送メカニズムを利用して機能するため、差分 SAP が送信されるには、IPX-EIGRP ピアが存在する必要があります。 特定のインターフェイスにピアが存在しない場合、ピアが検出されるまで、そのインターフェイスで定期的な SAP が送信されます。 この機能は、シリアル インターフェイスには自動的に設定され、LAN メディアには必要に応じて設定できます。
- **NLSP（NetWare Link Services Protocol）：** このルーティング プロトコルは、SAP および RIP と組み合わせて、またはこれらの代わりに使用できます。 大規模で複雑なインターネットワークに実装した場合の RIP および SAP に対する制限に対処します。 一般に、RIP および SAP と比較して、NLSP は、使用する帯域幅が少なく、ルーティング テーブルの更新が速く、大規模なインターネットワークへの拡張性に優れています。 NLSP は、使用される機会の少ない IPX ルーティング プロトコルです。

## Novell IPX ネットワーク ケーススタディ

## 事例 1： WAN インターフェイス上の3Comと Ciscoのインターオペラビリティ

デフォルトでは、Cisco ルータはすべてのインターフェイスで 60 秒ごとに行われる定期的 SAP アップデート用に設定されます。 ところが、Enterprise 3Com ルータでは、WAN インターフェイスはデフォルトで非定期的 SAP アップデート用に設定されています。 非定期的アップデートは、定期的にではなく、リンクが確立されたとき、リンクが管理目的で切断されたとき、またはサービス情報が変化したときにのみ実行される SAP アップデートです。 このパラメータは、SAP アップデートについてのみサポートされています。 Cisco ルータを、デフォルトの IPX 設定を使用して WAN インターフェイスで IPX を実行する 3Com ルータと接続すると、3Com ルータはデフォルトで非定期的 SAP アップデート用に設定されているので、Cisco ルータ内の IPX サーバ エントリは、リンクが確立してから、またはトポロジが変化してから 240 秒間しか存在しません。 この問題を修正するには、Cisco ルータまたは 3Com ルータで設定を変更する必要があります。

WAN インターフェイスで定期的 SAP アップデートを行うように 3Com ルータを変更するには、次の手順を実行します。

1. 次のコマンドを実行して、3Com ルータの WAN インターフェイスでの IPX 設定を確認します。 **示して下さい[! <port]|!! *] - sap 制御**例： **SH -SAP CONT**
2. 3Com ルータで WAN インターフェイスが「非定期的」に設定されている場合は、次のコマンドを使用して設定を「定期的」に変更する必要があります。 **setdefault! <port> -control=periodic sap**Cisco ルータをインターフェイスで非定期的 IPX SAP アップデートを行うように変更するには、次のインターフェイス コマンドを実行します。ipx update interval sap changes-only

## 事例 2： フレーム・リレー・ネットワークを越えたフレーム・リレー・ブロードキャスト・キューおよびIPX接続不良

IPX 用に設定され、フレームリレー クラウドのハブとして配置されている Cisco ルータでは、フレームリレー ブロードキャスト キューに関連する設定の変更が必要な場合があります。 これは、フレームリレー ブロードキャスト キューはデフォルトで単一インターフェイスのみのサイズに設定されますが、実際には、インターフェイスは複数のサイトに対応する場合があるためです。 フレームリレー ブロードキャストのデフォルトのキュー サイズは 64 であり、これをサブインターフェイスの数の 64 倍に設定する必要があります。 キュー サイズの設定が小さすぎると、WAN 経由での IPX RIP/SAP アップデートが失われる可能性があります。 IPX RIP/SAP アップデートが失われると、ハブとリモート サイトの間の接続が失われます。

**例**： 設定が小さすぎるフレームリレー ブロードキャスト キュー：

```
lt-3810b#show int s0 Serial0 is up, line protocol is up ... Encapsulation FRAME-RELAY, crc 16,
loopback not set .. Broadcast queue 61/64, broadcasts sent/dropped 17423/14021,
interfacebroadcasts 42032 Last input 3d19h, output 3d19h, output hang never Last clearing of
"show interface" counters 00:00:07 Input queue: 74/75/0 (size/max/drops); Total output drops:
14453 Queueing strategy: weighted fair Output queue: 25/1000/64/1578 (size/max
total/threshold/drops)
```

### フレームリレー ブロードキャスト キューの設定のガイドライン

フレーム リレー ブロードキャスト キュー

- 複数の Data-Link Connection Identifier（DLCI; データリンク接続識別子）上の伝送に対して複製されたブロードキャスト トラフィックを保持するために、指定したインターフェイスに

対する特殊なキューを作成するには、次のフレームリレー ブロードキャスト キュー インターフェイス設定コマンドを使用します。

- **frame-relay broadcast-queue size byte-rate packet-rate**

構文の説明

- size：ブロードキャスト キューで保持するパケットの数。 IPX RIP/SAP ネットワークに対する推奨値は、リモート サイトの数に 64 パケットを掛けた値です。 たとえば、リモート サイトの数が 7 の場合は、キューの深さを 448 に設定します。
- byte-rate： 1 秒間に送信する最大バイト数。 推奨値は、デフォルト設定の 1 秒当たり 256000 バイトです。
- packet-rate： 1 秒間に送信する最大パケット数。 推奨値は、デフォルト設定の 1 秒当たり 36 パケットです。

## 事例 3： IPX EIGRP をIPX ルーティング・プロトコルとして使用する場合のIPX SAP 不一致

特定の Novell サーバまたは IPX サービスに対する接続が、突然失われる場合があります。 Novell サーバまたは IPX サービスが、IPX SAP テーブルからランダムに消失することがあります。 また、このために、ネットワーク上の SAP ごとに SAP テーブルのサイズが異なることもあります。

これらの問題に直面する場合、これらのソフトウェアバグを表示し、これらの問題に直面しないソフトウェア バージョンにアップグレードして下さい。

これらのリリース ノートを検討して下さい:

CSCdp13795 - IPX SAP Inconsistency with IPX EIGRP

IPX Enhanced Interior Gateway Routing Protocol（EIGRP）を使用している場合、シリアル インターフェイスが短時間ダウンした後で再びアップすると、リモート サーバで Service Advertising Protocol（SAP）アップデートの不整合が発生する可能性があります。 この問題を検証するには、clear ip eigrp neighbors EXEC コマンドを入力するか、またはシリアル インターフェイスに対して no ipx linkup-request sap コマンドを入力して問題が再発しないことを確認します。

CSCdk13645 - IPX SAP Table May Become Inconsistent After Multiple Servers are Removed from the Table

IPX EIGRP 差分 SAP アップデート（RSUP）を使用していると、2 つ以上の EIGRP ネイバーの間でサーバ テーブルが整合しなくなる場合があります。 特に、複数の EIGRP ネイバーまたは 1 つのネイバーに対する複数のパスが存在する場合に、少なくとも 36 個のサーバが同時に削除され、これらのサービスに対するルートがルーティング テーブルに残っていると、この問題が発生する可能性があります。 最近ダウンした一部のサーバに対するダウン フラッシュ アップデートが送信されないインターフェイスがあるため、サーバが削除されるデバイスと削除されないデバイスが発生します。 この問題を回避するには、サーバがテーブルに残っているユニットで、IPX EIGRP ネイバーをクリアします。

フラッシュ アップデートは、ネットワーク内で発生した変更、および新しいサービスの出現または既存のサービスの消失に関する、即時アナウンスメントです。 次のラボ デバッグ出力のサンプルで示されているように、IPX が稼働しているすべてのインターフェイスにフラッシュ アップデートが送信されます。

```
5d10h: IPXSAP: positing update to 1.ffff.ffff.ffff via Serial1 (
broadcast) (flash)
5d10h: IPXSAP: positing update to 2.ffff.ffff.ffff via Serial0 (
broadcast) (flash)
5d10h: IPXSAP: positing update to 100.ffff.ffff.ffff via Etherne
t0 (broadcast) (flash)
```

### CSCdm23488 - Missing SAPs After Linkup/down

IPX EIGRP Sap-incremental で設定されるローカルルータおよびリモートルータを相互接続する IPXインターフェイスのネットワークコンフィギュレーションでは IPX EIGRP が使用されるとき（LAN 以外のデフォルトモードはインターフェイスします）、リモートルータは IPX サービスがから聞かれるが、リモートルータに接続されないローカルルータのインターフェイス（インターフェイス）が速い down/up 遷移を経る場合いくつかの SAP を失う場合があります。 回避するはリモートルータで **clear ipx eigrp neighbors** コマンドの発行によって IPX-EIGRP 隣接関係を再確立することです。

CSCdm23488 の根本原因は、リンク ダウンとリンク アップのシーケンスの後で IPX によって呼び出されるソフトウェア プロセスでのタイミングの問題です。 多数の IPX サービスが含まれると、ポイズン SAP が送信されている間にインターフェイスが稼働状態になります。 その結果、ポイズン SAP が新しいアドバタイズを上書きし、一部のサービスがアドバタイズを受け取れなくなります。

### CSCdx73624 - Missing IPX SAPs

ハブとスポークから成るフレームリレー トポロジでは、WAN クラウドで IPX RIP と IPX EIGRP の両方が稼働していると、2 つのスポークが相互の SAP を受信できません。 結果として、SAP テーブルの整合性が失われます。 回避策は、IPX RIP を無効にすることです。

## トラブルシューティングの手順

SAP が失われる問題が発生する場合は、次のトラブルシューティング手順を使用します。

- 別のフレームリレー スポークを介して SAP が学習される場合、ハブ ルータでも SAP が不明ですか、それともローカル スポーク ルータだけですか。
- 差分 SAP アップデートと定期的 SAP アップデートのどちらを使用していますか。
- 定期的アップデートを有効にしている場合は、更新された SAP アップデートをルータが受信しているかどうかを調べます。 show ipx traffic コマンドを発行して SAP カウンタを表示します。

```
System Traffic for 0.0000.0000.0001 System-Name: SAMPLE
 Time since last clear: 00:01:47
 Rcvd: 733 total, 0 format errors, 0 checksum errors, 0 bad hop count,
 4 packets pitched, 733 local destination, 0 multicast
 Bcast: 732 received, 507 sent
 Sent: 529 generated, 456 forwarded
 0 encapsulation failed, 0 no route
 SAP: 0 Total SAP requests, 0 Total SAP replies, 0 servers
```

- 特定のサーバからのすべての SAP が失われていますか。
- リンク障害と不明の SAP の間に関係がありますか。 リンクを変更した後で SAP が失われる場合は、次の手順を使用します。logging buffered コマンドを発行して、コンソール ロギングを無効にし、バッファ ロギングを有効にします。**debug ipx eigrg events** および **debug ipx eigrp neighbor {neighbor ID} コマンドを**発行して下さい。インターフェイスのリンク状態を変更します。SAP の欠落を検出した場合は、少なくとも 5 分間待って、SAP がほんとうに欠

落していることを確認します。 ハブ ルータとスポーク ルータの両方で、show ipx server コマンドと show ipx route コマンドの出力を取得します。スポーク側で、clear ipx route コマンドを発行します。show ipx server コマンドおよび show ipx route コマンドを発行して、すべての SAP が学習されているかどうかを確認します。

以上の手順で問題を解決できない場合は、debug ipx sap activity コマンドを発行することが必要な可能性があります。 デバッグ メッセージの例を次に示します。

```
3d21h: IPXSAP pv03 from net C4545 rejected, route C0324002 not in table

Oct 19 18:21:05 CDT: IPXEIGRP: SAP from FF16 rejected, route 2200 in table via different
interface
```

**注:** この debug コマンドを有効にする前に、その影響を理解しておいてください。このコマンドでは、大量の出力が生成される場合があります。 ルータに対するデバッグの影響を最小限にするため、コンソール ロギングを無効にし、十分なバッファ サイズでバッファ ロギングを有効にすることをお勧めします。

## 事例 4： コマンドshow ipx trafficがおびただしい数のフォーマットエラーを指摘する場合

例： コマンドを lt-4500-3a#show ipx traffic のように設定します。 出力結果は、次のようになります。

```
System Traffic for 0.0000.0000.0001 System-Name: dc_gw
Rcvd: 49847808 total, 1974563 format errors, 0 checksum errors,150 bad hop count,
310999 packets pitched, 1067549 local destination, 0 multicast
Bcast: 1072701 received, 1005206 sent
Sent: 2209133 generated, 48465603 forwarded
0 encapsulation failed, 3240 no route
SAP: 2174 SAP requests, 8 SAP replies, 1330 servers
899357 SAP advertisements received, 990129 sent
0 SAP flash updates sent, 535 SAP format errors, last seen from 0.0000.0000.0000
RIP: 91556 RIP requests, 22723 RIP replies, 152 routes
73769 RIP advertisements received, 20433 sent
1475 RIP flash updates sent, 0 RIP format errors
Echo: Rcvd 0 requests, 0 replies
Sent 0 requests, 0 replies
76 unknown: 76 no socket, 0 filtered, 0 no helper
0 SAPs throttled, freed NDB len 0
Watchdog:
0 packets received, 0 replies spoofed
Queue lengths:
IPX input: 0, SAP 0, RIP 0, GNS 0
SAP throttling length: 0/(no limit), 0 nets pending lost route reply
Delayed process creation: 0
EIGRP: Total received 0, sent 0
Updates received 0, sent 0
Queries received 0, sent 0
Replies received 0, sent 0
SAPs received 0, sent 0
Trace: Rcvd 0 requests, 0 replies
Sent 0 requests, 0 replies
```

show ipx traffic コマンドでのフォーマット エラーは、破棄された不正パケット（たとえば、ヘッダーが破損しているパケット）の数の部分です。 このカウンタには、ルータが設定されていないカプセル化に対して受信した IPX パケットが含まれます。

ネットワーク上のほとんどの PC は、可能な 4 つのフレーム タイプすべての GNS 要求を送信す

ることで、トークン リング ネットワークまたはイーサネット ネットワーク上の IPX のフレーム タイプを自動的に検出します。 ルータのインターフェイスは、特定のフレーム タイプにハードコードされています。 ルータのインターフェイスが、設定されているものとは異なるフレーム タイプの IPX パケットを受信すると、パケットは廃棄され、「フォーマット フィールド」の値が増分されます。 したがって、デフォルトのフレーム タイプに設定されている PC に対しては、起動時に、隣接する Cisco ルータで常に少なくとも 3 つの形式エラーが記録されます。

**show ipx traffic コマンド**に関する詳細については Novell IPX コマンドを参照して下さい。

## 事例 5： IPX SAPはWANクラウドを通過してIPXサーバテーブルに現われない場合

WAN クラウド内の Cisco ルータでは、すべての IPX ルートが IPX ルーティング テーブルに表示されます。 ただし、IPX サーバ テーブルには IPX SAP は表示されません。 AMI 回線符号化方式は、高いゼロ密度のパケットをサポートしません。 回線符号化方式は B8ZS 符号化方式にする必要があります。この方式は、高いゼロ密度を検出すると、データ ストリームを反転させてゼロを分割します。 IPX SAP パケットは、11 個の連続するゼロのデータ パターンを含むことがあります。 たとえば、タイプ 4 ファイル サーバの IPX アドレスは ABCDEF.0000.0000.0001 で、WAN クラウドで高いゼロ密度がサポートされていない場合、このアドレスは壊れます。 壊れた状態でリモート ルータに到着したパケットは廃棄されます。 その結果、IPX RIP アップデートがリモート ルータに到達しても、IPX SAP パケットは高いゼロ密度のために到達しません。

この問題を解決するには、WAN サービス プロバイダーに依頼して、WAN の回線符号化方式を B8zs に正しく設定します。

設定を検証するには、WAN クラウドに対し、500、1000、および 1500 の各バイト数で、すべてゼロのパターンの IP ping を実行します。 この高密度ゼロ パターンの IP ping が成功する場合は、回線の符号化方式に問題はありません。

```
Router#ping Protocol [ip]: Target IP address: 10.10.10.1 Repeat count [5]: Datagram size [100]:
500 Timeout in seconds [2]: Extended commands [n]: y Source address or interface: Type of
service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:
0x0000 Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape
sequence to abort. Sending 5, 500-byte ICMP Echoes to 10.10.10.1, timeout is 2 seconds: Packet
has data pattern 0x0000 !!!!! Success rate is 100 percent (5/5) Router#
```

## 事例 6： ワークステーションがネットワークコンピュータ経由でサーバの1 つに接続できない場合

ワークステーションが、すべての Novell サーバを「マイ ネットワーク」で見ることができても、「マイ ネットワーク」を通してどのサーバにも接続できない場合があります。 VLAN または複数のネットワークを通して「マイ ネットワーク」のサーバに接続するには、クライアント ワークステーションに Novell Client 32 がインストールされているか、または対応するルータで enable IPX type-20-propogation が設定されている必要があります。 さらに、キャンパス内の各ネットワーク番号が、ネットワーク全体で一意であることが必要です。 WAN での接続性を検証するには、Novell サーバの IPX PING ツールおよび Cisco ルータの PING IPX ツールを使用します。

## 事例 7： Ciscoルータを経由するIPX を使用してCitrix Winframeリソースにアクセスできない場合

show ipx servers のコマンド出力で、同じホップ/ティック カウントの距離に複数の Winframe サーバが存在することが示される場合、デフォルトでは、最初のエントリの SAP のみがクライアントに送信されます。

このことは、Novell サーバにとって問題ではありません。クライアントは最初の SAP を受け入れ、最初のサーバに到達した後、優先されるサーバがある場合は、クライアントが選択するサーバにリダイレクトされます。 Winframe にはこのような機能はありません。 クライアントが「x」という名前のサーバに対して設定されている場合、SAP テーブルで最初に「y」という名前のサーバがあるために「y」の SAP を受け取ると、クライアントは接続できません。

この問題を解決するには、同じ距離で複数の Winframe SAP があるルータに、グローバル コマンドとして ipx gns-round-robin コマンドを追加します。 ルータは SAP 応答を順次チェックし、クライアントは、ルータの SAP テーブルで最初の SAP ではない場合でも、正しいサーバの SAP を受け取ります。

## 事例 8： Novell IPX のログインが遅い

Novell のログインが遅い場合の最も一般的な原因は、ツリー ウォーキングと呼ばれる問題です。クライアントのエージェントが NDS に要求を送信する場合、要求を満たすのに適したネーム サーバが要求を常に受信するとは限りません。 要求を受信したネーム サーバは、要求を満たすことのできるネーム サーバを探す必要があります。 適切なサーバが見つかるまでに、複数のネーム サーバへのアクセスが必要になる場合があります。 情報を発見するため、ネーム サーバは、目的の情報を含むレプリカが見つかるまで、検索を実行します。 このプロセスはツリー ウォーキングと呼ばれます。 レプリカ情報にすばやくアクセスできる限り、ツリー ウォーキングは問題になりません。 しかし、WAN リンクのような低速のリンクを通してしかレプリカ情報を使用できない場合は、遅延が発生する可能性があります。 NDS を使用するすべてのアプリケーションによってツリー ウォーキングが発生する可能性がありますが、NDS ツリーを適切に設計することで、ツリー ウォーキングを最小限にできます。

ログインが遅くなる一般的な問題と Novell Web サイトごとの解決：

```
TID 10051665    Troubleshooting Slow Novell Login Problems

TID 10014302    NW5 client slow logging into IPX server

TID 2950722     Slow NT Login in Pure IP Environment

TID 10020376    The clients are getting a Slow Network Login

TID 10024740    Troubleshooting IP Login Issues

TID 10016768    Login is very slow from specific machines

TID 10021852    Slow login over a WAN link due to Contextless Login
```

**一般的なトラブルシューティング**

ログインが遅い問題の原因を識別するには、ワークステーションとの間で送受信されたすべてのパケットをキャプチャして、問題が発生している際のパケット トレースを取得します。 2 つのパケットトレースは問題を丁度判別して必要です: サーバポートの 1 つのパケットトレースおよびワークステーションの別のパケットトレース。 2 つのパケット トレースを取得することで、問題がネットワークでのパケット廃棄に関係するものかどうかを非常に簡単に判別できます。

## 事例 9： 破損したIPX SAP テーブルエントリのトラブルシューティング

IPX SAP のエントリで、無効な文字、ファントム ネットワーク、またはビットシフト/ビットスワップのある文字が表示される場合、最も多い原因は SAP エントリの破損です。 サンプル無効の文字列は含んでいます ( @! ~^ ) )。 IPX SAP フレームにはレイヤ 3 ( L3 ) のチェックサムがないので、IPX SAP のアップデートでデータの破損が発生する可能性があります。 この破損の原

因はレイヤ 2（L2）の破損ではありません。その場合は、L2 フレームでの CRC が無効になり、ルータがフレームを廃棄します。 IPX SAP の破損は常に、ハードウェアの障害によるものです。IPX 破損したSAP の出典を見つけることは IPX RIP 排他的を使用するときかなり単純です; 出典を見つけるのにホップ カウントを単に使用して下さい。 一方、IPX EIGRP を使用している場合は、トラブルシューティングが困難になります。

IPX EIGRP を使用する冗長パスおよびループ トポロジがあると、破損した SAP エントリが永続的に存在し、元のデバイスをオフにしてもタイムアウトしない場合があります。 EIGRP と RIP の混合環境から SAP が消えないのは、ネットワークに並行パスがあると、RIP と EIGRP が SAP エントリを相互に受け渡すためです。 この動作により、SAP はタイムアウトしなくなります。EIGRPは、SAP アップデートから複数の異なるルータからのアップデートを受信すると、RIP エントリが消失した場合、EIGRP から RIP にアップデートを戻します。 また、EIGRP は RIP ホップ カウントを保持しているため、原因の特定がいっそう困難になります。

前記のループ状態は、ルートではなく SAP のみに影響があります。 これは、SAP では常に最短のルートが示され、ルーティングのループは通知されないためです。 SAP はルーティング プロトコルではありません。 パス全体から EIGRP を削除すると、破損した SAP がエージング アウトできるようになります。

IPX EIGRP の動作と、破損した IPX SAP テーブル エントリのトラブルシューティングのため、IPX EIGRP:を使用するときは、次のトラブルシューティング手順を使用して IPX の破損した SAP を切り分けます。

1. ネットワークが停止している時間帯に、IPX EIGRP を無効にし、RIP を使用して破損した SAP エントリの原因を正確に特定します。 RIP はネットワーク パスのホップ カウントを使用するので、原因または発生元の特定は非常に簡単です。 この方法でのトラブルシューティングでは、停止時間中に破損フレームが生成される必要があります。 IPX SAP の破損はハードウェアによるものなので、問題は頻繁に発生せず、ランダムにしか出現しない可能性があります。 ちょうどそのときに破損した SAP がネットワークで生成されないと、原因を特定する手段はありません。 EIGRP を削除すると、EIGRP テーブル内の破損した SAP スタックはすべて消滅します。
2. 破損した SAP の共通の原因または発生源を調べます。 SAP に共通の発生源がある場合は、問題を簡単に切り分けられ、手順 1 のような面倒なトラブルシューティングを行う必要がない可能性があります。SAP の破損はすべて、ネットワーク内のどこかにあるハードウェアの障害によるものです。 これには、すべてのルータ、L3 スイッチ、IPX が稼働するサーバ（Novell サーバだけでなく）、および IPX が稼働するワークステーションが含まれます。Cisco で把握している限りでは、これまでに、IOS ソフトウェアの問題が原因で IPX SAP の破損が発生したことはありません。
3. ネットワーク接続に影響を与える IPX SAP の破損を回避するには、GNS フィルタ、GGS フィルタ、および SAP フィルタを含む IPX フィルタを設定し、ネットワーク内の有効なサーバのみに渡すようにします。 また、ipx sap follow-route-path コマンドを追加すると、破損した SAP の数を最低限にできます。 これは、ipx sap follow-route-path コマンドを使用すると、SAP アップデート内の個別のサービス（SAP）がルータでスクリーニングされるためです。 各 SAP エントリの宛先ネットワーク番号のルータ外観。 受信インターフェイスが SAP の宛先ネットワークにアクセスする最もよいインターフェイスの 1 つである場合その SAP エントリは受け入れられます。 そうではない場合は、SAP エントリは廃棄されます。ルータが破損した SAP を受信する場合は、ルートも破損している可能性があります。

## 事例 10： show ipx servers unsorted コマンド出力は故障中のサーバを表示している場合がある

特定の場合、IPX GNS ラウンド ロビンが設定されていると、テーブル内で低メトリック サービスがサービスの最低限のメトリック グループを超えて移動される問題がルータで発生することがあります。 その結果、SAP テーブルの順序が正しくなくなります。 これは既知の動作であり、GNS 出力フィルタを使用して特定のサーバだけが GNS に応答できるようにすることで、この動作による影響を解決できます。

このような問題が発生する場合は、次のソフトウェアの不具合を確認し、これらの問題が発生しないバージョンのソフトウェアにアップグレードします。

**CSCds54733 - show ipx servers unsorted Ouput Is Not In Order**

show ipx server unsorted コマンドの出力で、順序の正しくない SAP テーブルが表示されます。テーブルがこのような状態の場合、GNS SAP の応答で最も近いサービスが提供されない可能性があります。 順序が正しくないテーブルは、GNS ラウンド ロビンを有効にすると発生します。 **この問題を回避するには、no ipx gns-round-robin コマンドを発行して GNS ラウンド ロビンを無効にします。**

# Novell 5.X IP ケーススタディ

## 事例 1： クライアントがネットワーク境界を越えてNovell IPネットワークにログインするために必要な基本的なCiscoルータの設定

デフォルトでは、Novell IP クライアントはマルチキャストを使用して IP サービスを検出します。 他の方法が設定されていない場合、IP クライアントは、IGMP ( マルチキャスト ) を使用する Service Location Protocol ( SLP ) によってサーバの検出を試みます。 デフォルトでは、IOS ルータはマルチキャスト パケットを転送しません。

この問題をルータで解決する基本的な方法は、ip multicast-routing コマンドをグローバルに有効にし、各 VLAN または物理インターフェイスで ip pim dense-mode コマンドを有効にすることです。

設定例：

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot system bootflash:c6msfc-js-mz.120-7.XE1.bin
boot bootldr bootflash:c6msfc-boot-mz.120-7.XE1
!
ip subnet-zero
no ip domain-lookup
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
cns event-service server
!
!
!
```

```
interface Vlan1
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
interface Vlan11
ip address 10.1.2.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
interface Vlan12
ip address 10.1.3.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
ip classless
no ip http server
!
!
!
line con 0
transport input none
line vty 0 4
login
transport input lat pad mop telnet rlogin udptn nasi
!
end
Router#
```

マルチキャスト ルーティングを有効にすることなく、クライアント ワークステーションがネットワーク境界を越えて Novell 5.0 リソースにアクセスできるようにする方法が、他に 2 つあります。

Novellコンフィギュレーション #1（Novell Documenet: 2944038）

ワークステーションの NWHost ファイルに、サーバ名と IP アドレスのエントリを追加します。 NWHOST ファイルは、Win95 および Win98 ワークステーションの Novell\Client32 ディレクトリにあります。 簡単に利用できるサンプルが用意されています。

NT ワークステーションでは、NWHost の代わりに、クライアントは標準の MicroSoft TCP/IP ホスト ファイルを使用します。 ホスト ファイルを編集して、サーバ名とアドレスを追加します。 このファイルは Winnt/System32/Drivers/Etc/Hosts にあります。

Novell 設定 2（Novell ドキュメント 2944038 より）

NetWare 5 サーバに SLPDA.NLM をロードします。 これにより、サーバはディレクトリ エージェントとして定義されます。 SLPDA.NLM を実行するサーバの IP アドレスを、クライアントのプロパティの Service Location タブの Directory Agent リストに追加します。 Directory Agent ボックスの隣にある「Static」というラベルのボックスをクリックします。 静的なディレクトリ エージェントを定義すると、クライアントは、ディレクトリ エージェントに対してマルチキャストを行わず、指定されているディレクトリ エージェントにユニキャストを送信します。

SLP（Service Location Protocol）の概要およびディレクトリ エージェントの詳細については、support.novell.com の TID 2943614 を参照してください。

## 事例 2： 実稼働ネットワーク内のIP Multicast をイネーブルにすることは既存のIPXネットワークをダウンさせます

ネットワークで、クライアント PC に対する IPX 接続が突然完全に失われる場合があります。

これは、デフォルトでは、Novell Netware Client Software 3.x でネットワーク層プロトコルとして IPX より IP が優先されるためです。 したがって、ネットワーク内の Novell Netware ログインと IP マルチキャストに関して正しく設定されていない Novell 5.X の IP のみのサーバが有効になっていると、すべてのクライアント マシンでは Novell 5.X サーバへの接続が優先されます。 この Novell 5.X サーバで既存のネットワーク リソースが正しく認識されていない場合、クライアントは既存のリソースにアクセスできません。

この問題を解決するには、SLP を除外するように IP マルチキャスト ルーティングを設定するか、または Novell Netware 5.X サーバを正しく設定します。

### 事例 3： Novell IP はなぜNAT を実行するCiscoルータを通って動作しないのですか

NAT が実装されていると、パケット ヘッダー内の IP アドレスが変換され、特殊な状況では、パケットのデータ部分が検索されて、埋め込まれている IP アドレス参照が変換されます。 ただし、現在の Cisco NAT ソフトウェアでは、IP パケットのデータ部分に埋め込まれている NDS や SLP に対する Novell IP の参照は変換されません。 そのため、パブリック ネットワーク内のデバイスは、変換されていないプライベート アドレスを使用してリソースへの接続を試みます。 パブリック ネットワークはプライベート ネットワークとしては使用できないので、接続は失敗します。 NAT を通して Novell IP 接続を作成する代替解決策は、VPN ソリューションを使用することです。

詳細については、support.novell.com の TID 2948010 を参照してください。

### 事例 4： 遅いNovell IP ログイン

Novell IP のログインが遅い場合のトラブルシューティングは、IPX のログインが遅い場合と同じです。 Novell IPX の事例の「事例 8」を参照してください。

## よくあるコンフィギュレーションに関する質問

### なぜルータで200 以上のIPXネットワークを設定でできないのでしょうか

たとえば、Cisco ルータはルーティング テーブルでは 200 より多くの IPX ネットワークを処理できますが、ipx network コマンドを使用してルータに 200 より多くの IPX インターフェイスを設定することはできません。 この制限に達したのは最近のことで、現在では、この数のインターフェイスを提供できるレイヤ 3 スイッチがあります。 この数は IOS にハードコードされており、変更される予定はありません。 レイヤ 3 スイッチは、200 より多くのインターフェイスを実装できます。これは、ほとんどのスイッチング機能が専用の ASIC によって処理され、IP トラフィックに関する限り、この ASIC によりメイン プロセッサの負荷が軽減されているためです。 IPX インターフェイスは RIP/SAP プロセスの処理ではさらに多くの CPU パワーを必要とし、現在の制限に近付くだけでも重大な問題となる可能性があります。

### なぜルータからNovell ホストをping できないのでしょうか

Cisco ルータには 2 種類の IPX ping が実装されています。

- Cisco IPX ping： IPX アドレスに ping を試みるときにルータが使用する、デフォルトの Cisco 固有のプロトコルです。

- Novell IPX ping： Novell サーバが実行できる唯一の ping であり、Cisco の実装とは互換性がありません。

IPX 用に設定されている Cisco デバイス間の接続をテストするには、Cisco IPX ping を使用できます。 Novell サーバに ping を行う場合は、グローバル設定コマンドの ipx ping-default novell を使用して、Novell IPX ping を送信するようにルータを設定する必要があります。

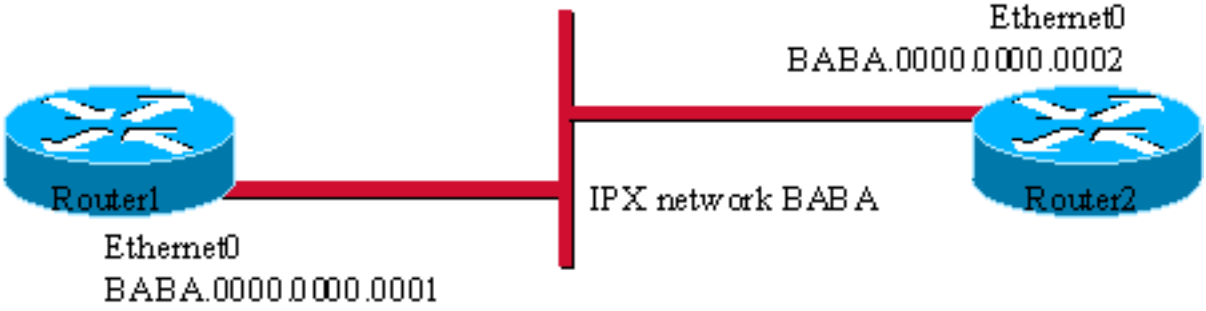
また、extended ipx ping コマンドを実行して、Novell Standard Echo オプションを選択することもできます。

Novell エコー（ping）に応答するために、Novell サーバにレスポンダをロードしておく必要があります。 Novell サーバから ping を行うには、サーバに IPXPING.NLM をロードすることも必要です。 簡単なテストで次のことが確認されています。

- Netware 3.x サーバ、Netware 4.0x サーバ、NETX クライアント、VLM クライアント（v.1.20a）、および MS Client for Netware は、Novell ping に応答しません。
- Netware 4.10 サーバ、Netware MPR v3.x、Client 32、および MS Client DOS/Win95 は、Novell ping に応答します。

当然のことですが、ping が失敗する理由には、ping プロトコル タイプの不一致以外のものもあります。 ping の成功は、IPX ルーティング テーブル（宛先アドレスへのルートが必要）、リンクの完全性（パケットの喪失）、フィルタリングなどにも依存します。 ping を使用するときは、次のガイドラインに留意してください。

- サーバへの ping を行う可能性がある場合は、IPX 接続のすべての問題が対処されていることを確認します。
- ping が失敗する場合は、可能性のあるすべての接続問題（複雑な IPX ルーティングの問題からリンク機能の問題まで）の中でも特に、サーバに IPX ping 機能が実装されていないという単純な問題である可能性があることに注意してください。 つまり、サーバへの IPX ping が失敗する場合は、意外にも、これが原因であることがよくあります。




この例では、IPX ネットワーク BABA のイーサネット インターフェイス経由で 2 つのルータが直接接続されています。 Router1 から Router2 のインターフェイスに ping を行うと、ルータは最初にデフォルトで Cisco 固有のプロトコルを使用します。

```
router1#ping ipx baba.0.0.2 Type escape sequence to abort. Sending 5, 100-byte IPX cisco Echoes
to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 4/6/8 ms
```

extended ping コマンドを使用することで、強制的に Novell ping を実行できます。

```
router1#ping ipx Target IPX address: baba.0.0.2 Repeat count [5]: Datagram size [100]: Timeout
in seconds [2]: Verbose [n]: Novell Standard Echo [n]: y Type escape sequence to abort. Sending
5, 100-byte IPX Novell Echoes to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate
```

```
is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

もう 1 つの方法として、デフォルトの ping プロトコルを Novell ping に設定できます。

```
router1#conf t Enter configuration commands, one per line. End with CNTL/Z. router1(config)#ipx
ping-default novell router1(config)#^Z 2w1d: %SYS-5-CONFIG_I: Configured from console by console
router1#ping ipx baba.0.0.2 Type escape sequence to abort. Sending 5, 100-byte IPX Novell Echoes
to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 4/6/12 ms router1#
```

ping のタイプを Novell に変更することは、Novell プロトコルを実行するホストに ping を試みる場合にのみ重要です。 Novell ホストへの ping が失敗しても、必ずしもそのホストへの接続が断たれていることを意味するとは限りません（すべての Novell ホストが Novell ping に応答するわけではありません）。 ルータへの ping は、ルータへの IPX 接続をテストするのによい方法です。

## なぜIPX ルーティングを設定できないのでしょうか

IPX ルーティングを設定するには、適切な IOS ソフトウェアが必要です。

ルータのフラッシュでデフォルトのソフトウェアが提供されていて、このデフォルト ソフトウェアで IPX がサポートされていない（IPX サポートのライセンスを購入していたとしても）ことがよくあります。 その場合は、ライセンスを供与されているソフトウェアにルータをアップグレードする必要があります。 一般に、IPX のサポートはデスクトップ機能セットの一部であり、通常はイメージ名内の「d」で識別されます。

```
c6sup-ds-mz.121-1.E2.bin
```

このデスクトップ機能セットは、IPX のサポートを含む最低限の機能セットです。 「エンタープライズ」機能セット（前記の「d」の代わりに「j」で識別される）にはデスクトップ機能セットが含まれるので、当然 IPX もサポートされます。 使用している IOS で使用可能な機能の正確な情報については、IOS のリリース ノートを確認してください。

## ipx pad-process-switched-packets コマンドとは何か

このコマンドは、奇数長のパケットをパディングし、インターフェイスでは偶数長のパケットとして送信するかどうかを制御するために使用します。 ipx pad-process-switched-packets コマンドはプロセススイッチングされるパケットに対してのみ有効なので、ipx pad-process-switched-packets コマンドを使用する前に、ファスト スイッチングを無効にする必要があります。 このコマンドが必要になったのは、一部の IPX ホストではパディングされていないイーサネット パケットが拒否されたためです。 ある種のトポロジでは、そのようなパケットはリモート イーサネット ネットワークに転送される場合があります。 特定の状況下では、中継メディアでのパディングを使用して、この問題を一時的に回避できます。

このコマンドはデフォルトで有効になっています。 ただし、Novell のイーサネット ドライバの仕様では、IPX パケットの「偶数化」は送信デバイスで行うように規定されています。 これは、従来のデバイスでは奇数長パケットが問題であったものが、現在では問題ではなくなっていますが、要件のみが残っているためです。

従来の Novell の要件に従っていないデバイスでは、奇数長のパケットが生成される場合があります。 また、ある IPX カプセル化から別の IPX カプセル化にルーティングするときも、奇数長パケットが発生する可能性があります。 カプセル化の中には長さが異なるものがあり、カプセル化が変更されると奇数長のパケットが生成される可能性があります。

## Ciscoルータは、より大きいRIP/SAP アップデートパケットの送信によってネット

### ワーク輻輳を回避するIPX パケット拡張機能をサポートしていますか

この機能はサポートされています。 デフォルトでは、IPX RIP パケットには 25 個のルートが含まれ、IPX SAP パケットには 7 個の SAP が含まれます。 RIP パケットと SAP パケットごとのルートと SAP の数は、それぞれのアップデート パケット サイズを変更することで変更できます。 詳細については、IOS コマンド リファレンスの ipx sap-max-packetsize および ipx rip-max-packetsize に関するドキュメントを参照してください。

### IP だけのためのすべての Novellサーバおよびルータの設定にもかかわらず、まだスニファートレースの IPX 帯を参照しています。 なぜなのでしょうか？

Novell Client Software 3.x は、デフォルトで、ネットワークの設定に関係なく、起動時に IP および IPX のフレームを送信して、Novell ネットワークへのログインを試みます。 この問題を解決するには、クライアント PC ですべての IPX プロトコルを手動で無効にしてください。

### VLANインターフェイス上でIPX EIGRP を有効にすると個々のインターフェイスの IPX MLS が無効になる理由

RIP ドメインと EIGRP ドメインの間で転送を行うには、ルート パケットのデータ部分の特定のフィールド（伝送制御）を変換する必要があるため、EIGRP IPX では MLS IPX が無効になります。 RIP/NLSP のために有効に されたとき IPX ルータ インターフェイスに、16 の最大ホップ数があります。 ルータが NLSP/RIP および EIGRP ルーティング ドメインの境界にあるとき、インターフェイスは EIGRP および NLSP/RIP 両方で設定されます。 この場合、パケットがルーティング ドメイン間を移動するとき、伝送制御（TC）の値は、1 ずつ増分される代わりに変換されるので、最大ホップが 16 以下に設定されている場合は、そのインターフェイスに対する MLS のサポートを削除する必要があります。 MLS-SE には使用されているルーティング プロトコルに関する情報がなく、MLS ハードウェアは伝送制御（TC）フィールドを正しく書き換えることができません。

「IPX EIGRP が設定される場合 IPX 最大ホップが 16 に設定 されるときだけ **IPX MLS eigrp 使用方法に」はよる VLAN <vlan_id> で**メッセージ現われます**ディセーブルにされます**。 他のすべての値（17 〜 254）に対しては、このような警告メッセージは表示されません。 警告は表示されますが、IPX MLS はホップの値が 16 でも正しく動作します。

16 の上の Transmit Control （TC）値を増加するコマンドは **IPX 最大ホップ <max_hops value>** です

ホップ カウントを増やしても、特に利点や欠点はありません。

## よくあるコネクティビティの問題

### IPX クライアントログインプロセスの理解

#### クライアントはどのような方法で Novell ネットワークに接続するのですか

クライアントは、特定の Nearest Directory Server（NDS）ツリーでサーバを探す必要がある場合は、サービス タイプ 0278 Get Nearest Directory Service（GNDS）要求に対する SAP タイプ 3 をブロードキャストします。 クライアントと同じルーティング セグメント上にある NDS サーバ（GNS および GNDS 要求に応答するように設定されているもの）は、属している NDS ツリーの

名前と内部 IPX 番号を示して応答します。 クライアントは、応答に含まれるツリー名と、必要なツリー名（クライアントで優先ツリーとして設定されているもの）を比較して検査します。 ツリーが正しい場合、クライアントは応答で提供されている内部 IPX 番号へのルートに対する RIP 要求をブロードキャストします。 サーバは、その内部 IPX 番号へのルートであることを伝えて応答します。 クライアントは、要求をユニキャストしてそのサーバへの接続を確立し、認証プロセスを開始します。 ローカルセグメントのサーバがサービス タイプ 0004 を提供ただできるので最初の GNDS 要求に応答しない NDS サーバでなければない 0278。 NDS レプリカを保持しないどの NDS サーバでも要求に応答しません。 どの応答にも正しい NDS ツリー名が含まれていない場合、クライアントはサービス タイプ 0278（GGDS）要求に対する SAP タイプ 1 を発行します。 同じルーティング セグメント上にあるすべての NDS サーバが、REPLY TO GET NEAREST SERVER の設定に関係なく、サービスのリストを示して応答します。 クライアントでは、GGDS に対するすべての応答を読んで、正しい NDS ツリー名を探します。 正しいツリーのエントリが見つかると、クライアントはそのサーバへの接続の確立を試みます。 これは最近サービス クエリではなく一般サービス クエリなので、クライアントは、最も近いエントリではなく、正しいツリー名を含む最初のエントリへの接続を確立しようとします。 クライアントが製本所サーバを（要求すればまたはクライアントは彼のクライアントコンフィギュレーションで設定 される 優先サーバだけ）同じプロセス起こりますもらいます、要求のサービス タイプだけが 0278 の代りに 0004 です。 サーバが OFF に設定 される GET NEREST SERVER への応答をそしてサーバ GNS （ サービス タイプ 0004 ）かに GNDS （ 0278 ） サービス タイプ 要求応答しないことをもらう場合、さらに

[Novell クライアント ログインのフローチャート]

NDS（Novell 4.11）

1. 起動時に、クライアントは GNDS 要求を送信します。 クライアントがフレーム タイプを自動検出するように設定されている場合は、フレーム タイプごとに 1 つずつ、4 つの GNDS が送信されます。
2. すべての口ーカル サーバ（または、サーバが存在しないセグメントの場合は Cisco ルータ）が、GNDS 応答を送信します。複数のサーバやルータが GNDS 要求に応答した場合、クライアントは最初の GNDS 応答を使用します。 GNDS 応答には、対応するサーバの内部ネットワーク番号とツリー名が含まれています。
3. GNDS 応答に含まれるツリーが正しい場合、クライアントは GNDS 応答で提供された内部 IPX 番号に対する RIP 要求を発行します。

[Cisco ルータはどのような方法で GetNearestServer（GNS）応答に含めるサーバを選択するのですか]

[show ipx server unsorted コマンドでは、最初の部分に、次の GNS 要求への応答で使用されるサーバの名前が表示されます。 ソフトウェア リリース 9.21 以降では、ipx gns-round-robin コマンドを使用して、メトリックが等しいサービスの間で GNS 要求に対する応答をロード バランシングさせることができます。] サーバが指示される方法は次に挙げるドキュメントに説明があります:
[サーバはどのように分類されるか]

[優先サーバがある場合とない場合では、クライアントの接続シーケンスはどのようになりますか]

優先サーバがない場合の接続シーケンスは、次の手順で実行されます。

1. サービスを見つけて下さい（GNS クエリ及び応答）
2. 保守するとルートが見つけて下さい（RIP クエリ及び応答）

3. 最も近いサーバに接続します。
4. ファイル サーバの情報を取得します。
5. バッファのサイズをネゴシエイトします。
6. 前の接続をクリアします。
7. ファイル サーバの日時を取得します。

優先サーバがある場合の接続シーケンスは、次の手順で実行されます。

1. サービスを見つけて下さい（GNS クエリ及び応答）
2. 保守するとルートが見つけて下さい（RIP クエリ及び応答）
3. 最も近いサーバに接続します。
4. ファイル サーバの情報を取得します。
5. バッファのサイズをネゴシエイトします。
6. 最も近いサーバに格納されている「優先サーバ」のプロパティ値を読み取ります。
7. 優先サーバへのルートを検索します。
8. 優先サーバに接続します。
9. 優先サーバのファイル サーバ情報を取得します。
10. バッファのサイズをネゴシエイトします。
11. 最も近いサーバとのサービス接続をクリアします。
12. 優先サーバとの前の接続をクリアします。
13. ファイル サーバの日時を取得します。

この場合も最も近いサーバとの GNS クエリ/応答が必要ですが、最も近いサーバとの接続シーケンスは完了しません。 最も近いサーバを使用して、優先サーバへの到達方法を学習します。 優先サーバへのルートを学習したなら、最も近いサーバとの接続を破棄し、優先サーバと接続シーケンスを繰り返します。

### GNS または GGS 要求に対する応答はどのようにしてフィルタリングされますか

ルータがクライアントの GNS 要求への応答に使用するメカニズムを制御すると便利です。 クライアントに応答するため、IOS はルータが認識するサーバの 1 つを選択します。 次の IOS コマンドを使用すると、このリストに含まれる特定のサーバが使用されないように設定できます。

IPX output-gns-filter {access-list-number|名前}

このコマンドをインターフェイスに適用すると、ルータは、指定されたアクセスリストに一致する最も近いサーバのみをクライアントに提供します。

## ネットワークへのクライアントの接続

### スイッチに直接接続するとクライアントをネットワークに接続できないのはなぜですか

この構成によって発生する可能性のある問題の詳細については、『PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復』を参照してください。

基本的に、PC を Catalyst スイッチのポートに直接接続する場合は、PortFast 機能を必ず有効にしてください。 CatOS でこの機能を設定するには、次のコマンドを使用します。

```
set spantree portfast enable <module/port>
```

また、トランキングおよびチャネリングの機能を備えたモジュール（たとえば、Catalyst 5000 上

の WS-X5225R およびすべての Catalyst 6000 モジュールは、トランキング/チャネリングに対応しています ) の場合は、次のコマンドを使用して、これらの機能を手動でオフにする必要があります。

**set trunk <module/port> off set port channel <module/port-range> off**

Catalyst 4000/5000 ファミリのソフトウェア 5.2 以降、および Catalyst 6000 ファミリの 5.4 以降では、これら 3 つのコマンドを 1 つのマクロ コマンドにバンドルできます。

**set port host <module/port>**

## 接続に影響するようなライセンスまたはサーバの問題がありますか

接続する Novell クライアントが最初に行うことは、GNS ( Get Nearest Server ) 要求の送信です。 この要求は、サーバまたはルータによって応答されます。 その後、クライアントは応答で指定されているサーバを使用して接続を試みます。 接続が失敗する可能性のある一般的な問題が 2 つあります。

- 接続されるサーバは GNS に応答しません。 最も近いサーバの内部ネットワーク番号が 0000.0000.0001 ではない場合、おそらく GNS を無視する NTサーバです。
- 接続したサーバでライセンスが不足している。 限られた数のクライアントだけが接続でき、それ以上接続を試みても失敗します。

**いずれの場合も、Cisco ルータが含まれる場合は、show ipx server unsort コマンドを使用して、クライアントに提供されているサーバを確認します。 その後、ipx output-gns-filter コマンドを使用して、応答として提供してはならないサーバをフィルタリングします。**

## 重複する IPX または MAC アドレスにより発生する接続の問題はありますか

通常、MAC アドレスがその一部になっているので、ネットワーク内のすべての IPX アドレスは異なる必要があります。 ところが、さまざまな状況において、ユーザは MAC アドレスをハードコードできます。その場合は、このアドレスが一意になるように十分注意する必要があります。また、たとえば、あるルータから設定をコピーして別のルータに貼り付ける場合も、IPX アドレスが重複しないようによく注意する必要があります。 ipx routing コマンドで定義される MAC アドレスを使用する WAN インターフェイスの場合は、このことが特に重要です。 次の例では、Router A と Router B の設定が重複しています。 ネットワーク管理者はすべてのインターフェイスで IPX ネットワークを変更しましたが、ipx routing 行のアップデートを忘れたため、両方の設定で同じになっています。


シリアル インターフェイスには独自の MAC アドレスがありません。 ルータは、ipx routing コマンドで指定されている MAC アドレスを使用して、シリアル インターフェイスの IPX アドレスを作成します。 この例の場合、Router A と Router B の IPX アドレスはまったく同じ AAA.0000.0C14.11E1 です。 当然のことながら、アドレスが重複する問題は、他にもさまざまな状況で発生します。 重複したアドレスによる接続の問題は TAC にはよく報告されるものなので

、IPX ネットワーク アドレスまたは MAC アドレスを割り当てるときは、十分に注意してください。

どのリンクでも、次の点に注意してください。

- すべてのサーバおよびルータには、特定のカプセル化について、一意の IPX ネットワーク番号を設定する必要があります。
- すべての MAC アドレスは一意である必要があります。

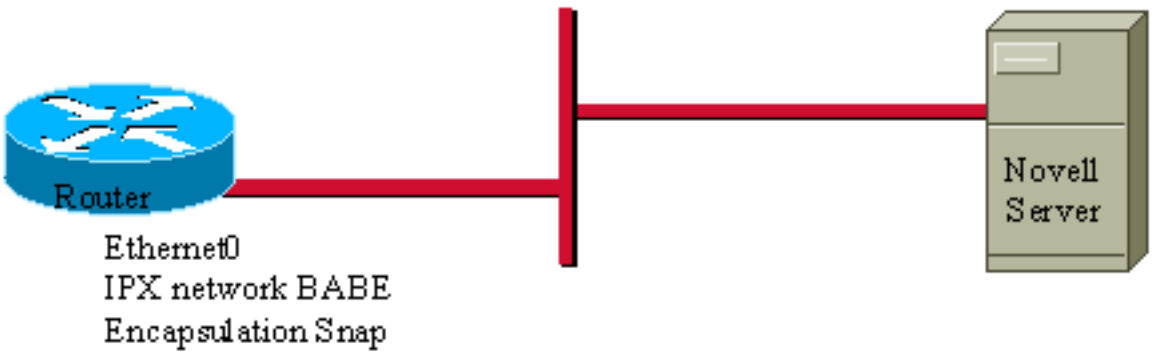
## サーバおよびサービスの表示

### 特定のサーバ/サービスにアクセスできないのはなぜですか

**クライアントが Cisco ルータを通してサーバにアクセスを試みている場合は、ルータで show ipx server コマンドを使用します。**

show ipx server コマンドを発行すると表示されるリストに探しているサーバ/サービスが含まれ、接続を遮断するアクセスリストが設定にない場合、おそらくルータは問題の原因ではありません。 ルータでサービスが表示されない場合は、サーバの IPX ネットワークがルーティング テーブルに表示されることを確認します。 **IPX ルーティング テーブルを表示するには、show ipx route コマンドを発行します。** 対応するネットワークへのルートがルータにない場合、サービスはアドバタイズされません。

サーバがルータに直接接続されていて、それでも show ipx server を発行したときに表示されない場合は、サーバとルータの両方で same IPX network に同じ IPX encapsulation を設定してあることを確認します。




この例では、Novell サーバは SNAP カプセル化に設定されていて、IPX アドレスは BABE であることに注意してください。 カプセル化が正しくない場合、サーバが送信したパケットはルータによって破棄されます。 IPX ネットワークが一致しない場合は、その不一致を指摘するエラー メッセージがサーバで表示されます。

**ルータでは、show ipx traffic コマンドを使用すると役に立つ情報が得られますが、残念ながら、特定のインターフェイスについてではなく、デバイス全体に対するものです。** format error」フィールドに注意してください。 このフィールドは、正しくないカプセル化のパケットがルータで受信されるたびに増分されます。 このカウンタが上昇している場合は、カプセル化の不一致が発生している非常に高い可能性があります。

コマンド show ipx interface [<interface>]特定のインターフェイスのための IPX 関連詳細を説明します。 インターフェイスに設定されているカプセル化タイプ、IPX アドレス、およびアクセスリ

ストが要約されています。 サーバ/サービスの可視性をトラブルシューティングするときは、特定のインターフェイスがネイバーから RIP および SAP のアップデートを受信していることを確認すると役に立ちます。 このコマンドを使用すると、これが確認できます。

## RConsole を通して IPX サーバにアクセスできないのはなぜですか

RIP と EIGRP がネットワークの情報を伝えるのに対し、SAP はサービスの情報を伝えます。 Cisco ルータが生成する各 IPX SAP パケットは、メディアのカプセル化オーバーヘッドに加えて、最大で 7 つの 64 バイト SAP エントリと、32 バイトの IPX オーバーヘッド（合計で 480 バイト）を搬送できます。 これが EIGRP パケットの内部で搬送される場合、IPX SAP パケットは、Opcode 値が 6 の標準 EIGRP ヘッダーと、それに続く、元の IPX ヘッダーを含まない標準 IPX SAP パケットの標準ペイロードで構成されます。

標準的な SAP パケットの交換では、Netware クライアントは SAP クエリをブロードキャストし、SAP サーバ タイプ フィールドで指定されているディレクトリ サーバを探します（『Novell SAP のサービスのリスト』を参照）。 SAP 応答パケットには、ディレクトリ サービスを提供するサーバの内部 IPX アドレスが格納されています。 次に、クライアントは RIP ブロードキャストを送信して、サーバの内部 IPX アドレスへのパスを探します。

次の手順により、RCONSOLE 接続が確立されます。

1. RConsole クライアントは、SAP 要求をブロードキャストしてサーバを探します。 具体的には、RConsole は、タイプが 0x107 のサーバに対する一般サービス クエリを送信します。 RConsole が PC 上で動作するためには、Cisco ルータがタイプ 0x107 のサーバへの通知を許可されている必要があります。 クライアントは、現在サーバにログインしている場合であっても、サーバ ルックアップ SAP 要求を送信します。セグメント上にサーバが存在する場合は、そのサーバがクライアントに応答します。IPX クライアントが属するセグメントにサーバが存在していない場合、ルータは、ソートされていないリストから最初の SAP エントリを選択して、IPX クライアントからの GNS 要求に応答します。 ルータの最初の SAP エントリが正しくないサーバである場合もあります。 このことは、show ipx server unsorted コマンドを発行することで確認できます。 回避策としては、正しくないサーバを遮断する SAP アクセス リストを作成し、それを GNS フィルタとして適用します。
2. クライアントは、応答した最初のサーバの内部 IPX アドレスに RIP 要求を送信します。
3. クライアントは、サーバに到達する最も速い方法を学習すると、SPX 接続要求パケットをサーバに送信します。

特定の Netware サーバに対して RConsole 接続を確立できない場合は、次の手順を使用して、原因がネットワークの問題か、またはサーバの問題かを判別します。

- すべてのサーバを認識できますか。 一部のサーバですか。 ローカルのサーバですか。 WAN 経由でのサーバですか。
- 他の IPX トラフィックに影響がありますか。
- 最も近いルータの IPX サーバ テーブルはどのようになっていますか。
- ルータの IPX ルーティング テーブルに含まれるサーバの内部ネットワーク ID はわかりますか。
- 接続元の IPX ネットワークと RConsole でアクセスしようとしているサーバを表示します。 **show versionshow runshow ipx servershow ipx route**
- Netware 4.11 または Netware 5 を使用していますか。 Novell IP ですか。 Netware 5 サーバに対して ping を実行できますか。 つまり、IP と名前で接続を試みます。 その場合、DNS は解決されません。

サーバ上の破損したデータベースが SPX 接続の問題の原因になっている場合があります。特に、破損したデータベースが他のサーバに転送されているような場合です。 通常、この問題は、DS 修復ユーティリティを実行することで解決できます。 ただし、DS を修復してもデータベースを復元できない場合は、サーバのリブートが必要になる可能性があります。 内部ネットワーク番号を使用して RConsole を接続できない場合は、Netware サーバに問題があります。

Novell の知識ベースでも、技術的なヒントがオンラインで公開されています。 IPX サーバの観点から RConsole の問題をトラブルシューティングする場合は、次のヒントが役に立ちます。 次のヒントが、Cisco ユーザ向けのリソースとして提供されています。

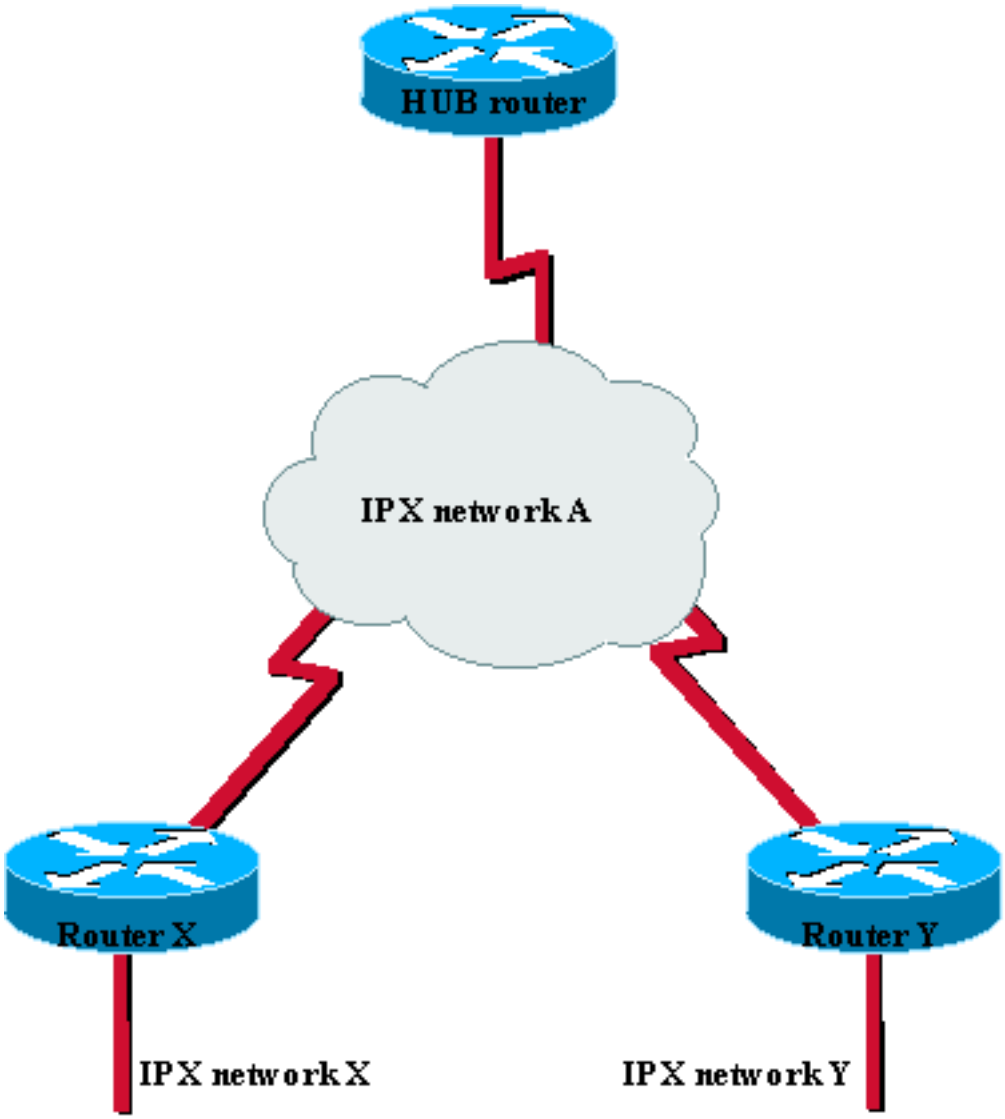
「RCONSOLE -4.10-112 SPX Establish Connection failed to establish a connection to the desired server.」

1. REMOTE.NLM はサーバにロードされていますか。 RSPX.NLM はロードされていますか。
2. DS を調査し、正常な状態ですべてが同期していることを確認しましたか。
3. RConsole SAP をフィルタで排除しているルータが工ラーの現になっている可能性があります。 SAP タイプ 0107 が RConsole SAP であり、RConsole が正常に動作するためには、この SAP がフィルタリングされないようにする必要があります。
4. NIC カードの問題により、クライアントが SPX 接続を確立できない可能性があります。
5. すべての IPX ネットワーク番号が一意であることを確認します。 これは、RConsole が接続できない第一の原因ですが、トラブルシューティングには最も困難である場合があります。
6. フレーム タイプを自動検出するのではなく、クライアントでフレーム タイプを強制的に設定します。

**回避策**

RConsole 画面で、INS を押し、ターゲット サーバの IPX 内部ネットワーク番号を入力します。 サーバの IPX 内部ネットワーク番号は、サーバ コンソールで CONFIG と入力して確認できます。 IPX 内部ネットワーク番号を手動で入力すると RConsole が動作する場合は、サーバの IPX ソケット テーブルが超過していることを意味します。 最大 IPX ソケット テーブル サイズを増加して下さい: **INETCFG - > プロトコル- > IPX - >IPX/SPX パラメータ- >Maximum IPX ソケット テーブル サイズ**。 デフォルト値は 1200 です。 2400 にこの値を最初に増加して下さい。 このテーブル サイズをリセットするには、サーバをリブートする必要があります。

## ハブおよびスポーク トポロジ内のすべてのサーバを認識できないのはなぜですか




上の図で、ハブ ルータはポイントツーマルチポイントのインターフェイスを通して他の複数のルータに接続されています。 これは、典型的なフレームリレーのハブとスポークのネットワークです。 すべてのルータはハブに同じ IPXネットワーク A.スポークルータでアドバタイズしますローカルネットワーク X および Y を接続されますが、ルータ X ルーティング テーブルのネットワーク Y を見ません ( および同様にルータ Y 表の X を見ません )。 この問題は、スプリット ホライズンに直接関係するものです。 RIP は、ルートを学習したインターフェイス上のルートをアドバタイズすることはありません。 基本的に、ハブ ルータはネットワーク X のことを WAN インターフェイス serial0 で学習し、ネットワーク A に接続して、X のことを serial0 にはアドバタイズしません。 Router Y は、やはり serial0 を介してハブ ルータに接続しますが、ネットワーク X に関して受信することはありません。

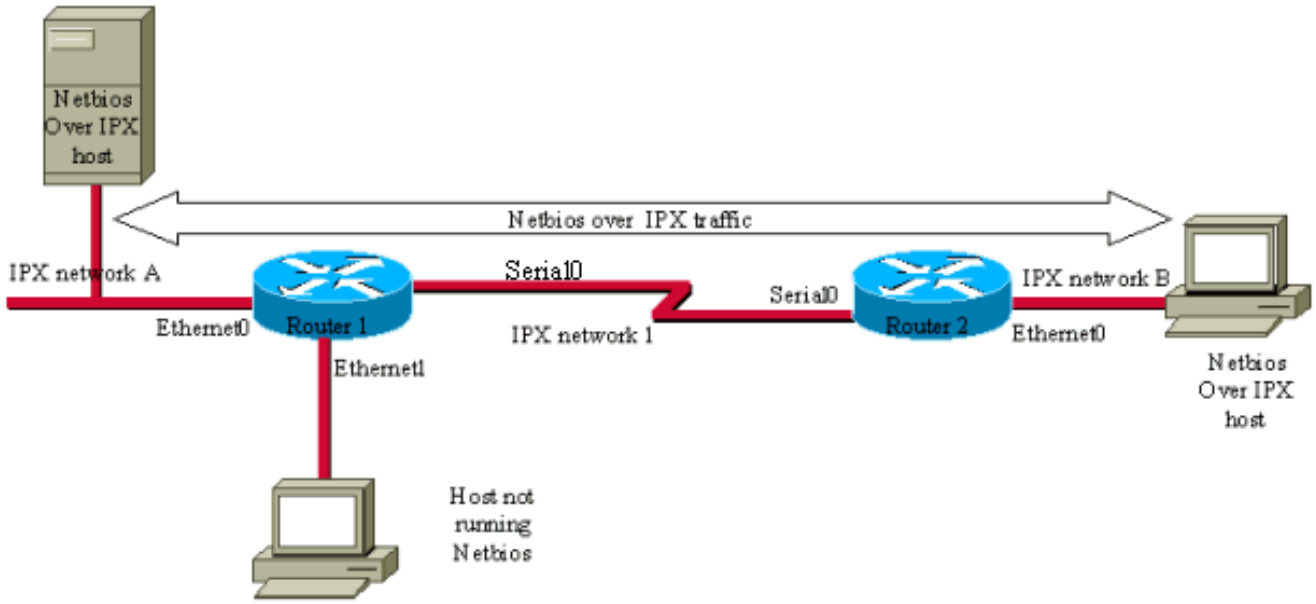
Novell の仕様では、RIP に対してスプリット ホライズンを無効にすることは許可していないので、Cisco ルータで 2 つの主要な回避策を使用できます。

- ポイントツーマルチポイントのインターフェイスを、複数のポイントツーポイント インターフェイスに置き換えます。 そのためには、ハブ ルータの serial0 に複数のサブインターフェイスを作成します。 この方法の問題は、作成するポイントツーポイント リンクごとに異なるネットワーク番号を割り当てる必要があることで、これはアドレス指定方式の変更およびルーティング テーブル サイズの増加を意味します。
- RIP を IPX EIGRP に置き換えます。 IPX EIGRP ルーティング プロトコルを使用すると、スプリット ホライズンを除去でき ( no ipx split-horizon eigrp コマンドを使用 )、低速の WAN リンクでのパフォーマンスが向上します ( 差分アップデートなど )。 唯一の欠点は、WAN

上のすべてのルータが Cisco 製品である必要があることです。

## NetBios Over IPX がルータを通過しないのはなぜですか

この問題は、NetBios over IPX がブロードキャスト タイプ 20 の IPX パケットに依存し、このパケットはルータで転送されないために発生します。 **この特定のパケットがルータで転送されるようにするには、NetBios トラフィックを伝搬するすべてのインターフェイスで、ipx type-20-propagation コマンドを設定します。**




| ルータ 1 の設定 | ルータ 2 の設定 |
|---|---|
| ipx routing 0000.0000.0001<br>!<br>interface Ethernet0<br>ipx network A<br>ipx type-20-propagation<br>!<br>interface Ethernet1<br>ipx network C<br>!<br>interface Serial0<br>ipx network 1<br>ipx type-20-propagation | ipx routing<br>0000.0000.0002<br>!<br>interface Ethernet0<br>ipx network B<br>ipx type-20-propagation<br>!<br>interface Serial0<br>ipx network 1<br>ipx type-20-propagation |

この設定には、関連する IPX 部分のみが含まれます。 この例では、ホスト A とホスト B で

NetBios over IPX が稼働しています。 Router 1 と Router 2 の IPX 設定は、きわめて基本的なものです。 ipx type-20-propagation コマンドが、NetBios over IPX トラフィックをリレーするためにサポートされるすべての単一インターフェイスに追加されています。 この場合、イーサネットセグメントには Netbios ホストがないので、Router 1 からのインターフェイス Ethernet 1 にはコマンドを追加する必要はありません。

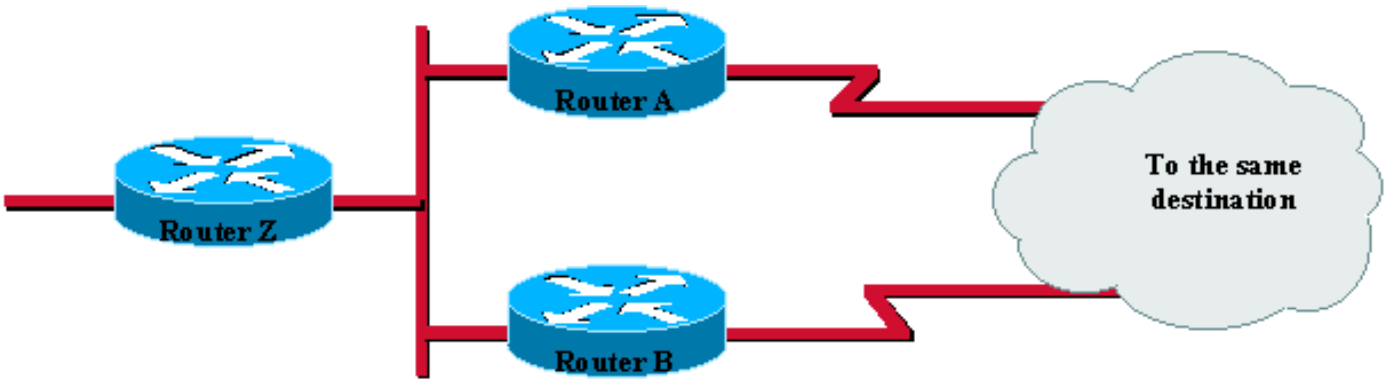
type-20-propagation コマンドは必須ですが、ネットワークのパフォーマンスに影響があることに注意してください。

# パフォーマンスの問題

## RIP ルートおよびSAP のためのメモリ使用量

| IOS | 10.0、10.2 | 10.3 以上 |
|---|---|---|
| ルート | 各ルートのための 180 バイトは、各々の追加パスのための 50 バイトを最大パスなら > 1 追加します | 各ルートのための 160 バイトは、各付加のための 70 バイトを最大パスなら > 1 追加します |
| SAP | SAP ごとに 200 バイト、SAP タイプごとに 4030 バイト追加 | SAP ごとに 200 バイト、SAP タイプごとに 4030 バイト追加、パスが 1 つ増えるごとに 50 バイト追加 |

## CiscoルータのIPX ロードバランシング



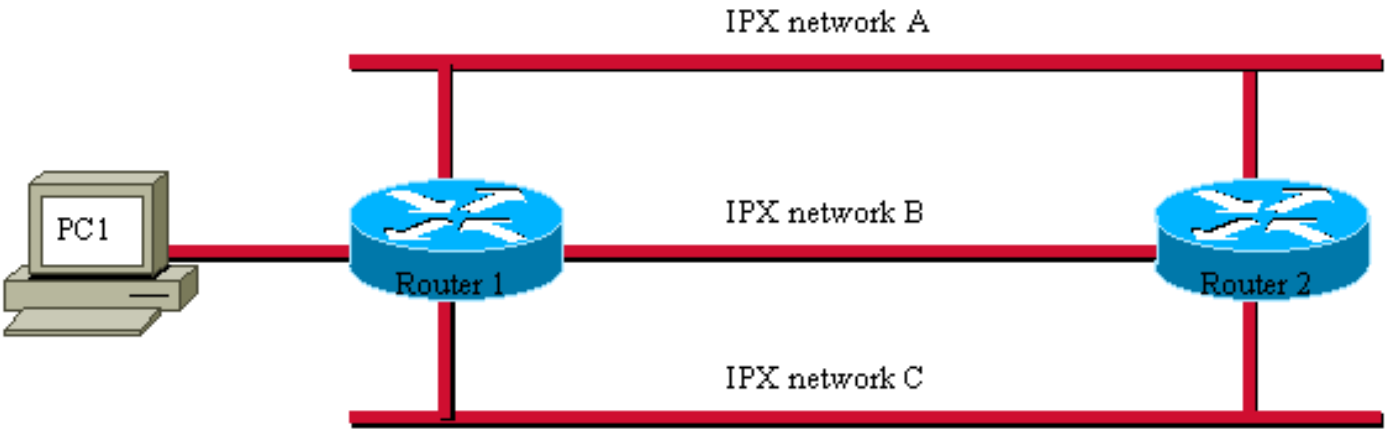

Router Z に ipx maximum-paths 2 コマンドが設定されていて、Router A および B が同じ宛先ネットワークに同じホップ数で到達する場合、Router Z は、スロー スイッチングとファスト スイッチングの両方で、ラウンドロビン方式により、Router A および B に対する宛先に各パケットを送信します。

このような場合、帯域幅が等しくない複数のパスにロード バランシングし、pburst を有効にすると、パケットの順序が正しくなくなる可能性があることに注意してください。 新しいバージョンの Netware は古いバージョンより適切にこの状況を処理しますが、このような設定におけるパフォーマンスの問題をトラブルシューティングする場合は、ロード バランシングまたは pburst を使用しないようにすることも推奨します。 IOS 11.1 以降では、ipx per-host-load-share コマンドを使用して、ホストごとにロード シェアリングを有効にすることもできます。 ホストごとのロード シェアリングは、コストが等しい複数のパスでトラフィックを送信しながら、特定のエンド ホ

ストに対するパケットは常に同じパスを使用することを保証します。

## type-20-propagation が有効になっている場合の貧弱なパフォーマンス

ルータにおける IP ヘルパーの使用はネットワークでは推奨されませんが、トラフィックの負荷に関する限り、ipx type-20-propagation コマンドの使用も推奨されません。 IP helper コマンドを使用すると、ルータはブロードキャスト パケットを取得し、次のセグメントに転送するためにユニキャスト パケット（またはダイレクト ブロードキャスト）に変換します。 ipx type-20-propagation コマンドを使用すると、ルータはブロードキャストを取得し、それをブロードキャストとして転送します。 タイプ 20 のパケットにはすでに通過したすべてのネットワークのリストが含まれ、ルータは、このリストに出現するネットワークにはパケットを転送しません。




すべてのインターフェイスで ipx type-20-propagation コマンドが有効にされていて、Router 1 と 2（たとえば、20 VLAN のトランクによって相互に接続された Catalyst 5000 および RSM の共通構成）の間には 3 つのセグメントがあるものとします。

1. PC1 がタイプ 20 のブロードキャストを発行します。
2. Router 1 は、それを取得し、そのコピーをセグメント A、B、C のそれぞれに転送します（セグメント リスト D）。
3. Router 2 は、3 つのコピーを取得し、それぞれを（1 番目のコピーのセグメント リストは DA、2 番目は DB、3 番目は DC）他の 2 つのセグメントに転送するので、パケットのコピーがさらに 6 つ作成されます（DA は B と C に、DB は A と C に、DC は A と B に送信されます）。
4. Router 1 はこれら 6 つのコピー（DAB、DAC、DBA、DBC、DCA、DCB）を取得し、すべてのパケットをそれぞれのセグメント リストに含まれない最後のセグメントに転送します。
5. Router 1 は、6 つのパケット（DABC、DACB、DBAC、DBCA、DCAB、DCBA）を取得し、いずれもすべてのセグメントを通過しているので、すべてのパケットを廃棄します。

この例では、ブロードキャストごとに 2 つのルータの間でさらに 15 個のパケットが生成されることがわかります。 2 つのルータの間に 4 つのリンク（VLAN）があると、64 パケットになります。 2 つのルータの間に 5 つのリンクがあると、325 パケットになります。以下同様です。 したがって、このコマンドを使用すると、パケットの数が増加し、ネットワークが遅くなったり停止したりする可能性があります。

このような状況を改善するには、次のコマンドを使用します。

- ipx type-20-input-checks Do additional input checks on type 20 propagation packets ipx type-20-output-checks Do additional output checks on type 20 propagation packets

これらのコマンドを設定すると、タイプ 20 のパケットを送信元に対するプライマリ ルートであるインターフェイスで受信したかどうかが確認されます。 そうでない場合、そのパケットは廃棄されます。 パケットを送信するときは、送信するネットワーク/インターフェイスがそのタイプ 20 パケットの送信元に戻るルートでないかどうかを確認し、そうである場合はパケットが廃棄されます。 これは、IPX ルータの仕様でタイプ 20 について実施するように求められている、ループに対する 8 ホップの検査に加えて行われます。

# アクセスリスト設定

## IPXネットワークの範囲のフィルタリング

IPX 拡張アクセス リストを使用すると、ネットワークの範囲をフィルタリングできます。 たとえば、大規模な IPX ネットワークがあるものとします。 すべての IPX ネットワークは、A43XXXXX および CBDXXXXX で始まります。 ネットワーク A43XXXXXX はルータに接続する必要がないので、次のコマンドを使用して各ネットワークをフィルタリングします。

```
interface Serial0

     ipx output-network-filter 805

     !

     access-list 805 deny  A43C0100

     access-list 805 deny  A43C0101

     access-list 805 deny  A43C0102

     .
     .
     .
```

このアクセス リストは、120 行まで続きます。 どうすれば、A43 で始まる IPX ネットワークをフィルタリングできるでしょうか。

そのためには、次のコマンドを使用します。

```
access-list 905 deny any A4300000.0000.0000.0000 FFFFF.FFFF.FFFF.FFFF
```

必要なルートを許可する行があることを確認します。 any キーワードは「すべてのプロトコル」を表し、必須の引数です。 このマスクは、IP のワイルドカード マスクと同じように機能します。 ホスト ビットを指定する必要があります。指定しないと、マスク オプションがなくなります。 IPX 拡張アクセス リストは、標準のリストとまったく同じ方法で使用できます。 NetWare Link Services Protocol ( NLSP ) をルーティング プロトコルとして使用している場合は、領域の

境界のルートをフィルタリングできるように、複数の領域を使用する必要があります。

# デバッグ

## デバッグ IPX パケットの出力を表示すると一部のパケットに「Bad Pkt」と なぜこれらのパケットはBad Pktと表示されるか

### 例：

```
IPX: unable to forward, no helper A0000001.0000.0000.0001(455)to B0000001.ffff.ffff.ffff(455)
typ 4IPX: Fa0/0:A000000.0000.0000.0001->B00000001.ffff.ffff.ffff ln=173 tc=01, bad pkt
```

この現象は、ソケット 455 が NetBIOS ソケット番号で、パケットの MAC 層宛先アドレスがブロードキャストであるために発生する可能性があります。 ipx type-20-propogation または ipx helper-address が設定されていない場合、ルータはこのパケットをデフォルトで廃棄します。 このような NetBIOS over IPX ダイレクト ブロードキャストの転送の詳細については、type-20-propogation の有効化に関するドキュメントを参照してください。

# 関連情報

- デスクトップ プロトコル
- テクニカルサポートとドキュメント - Cisco Systems