Cisco 7304 トラブルシューティング コンフィギュレーション ノート

目的

Cisco 7304 ルータのトラブルシューティングに関する情報は、主に Troubleshooting Assistant の対話形式のオンライン モジュールから入手できます。Troubleshooting Assistant モジュールは、シスコのソリューションに関するさまざまな資料を提供します。

このマニュアルは、Troubleshooting Assistant モジュールで提供されるシスコの資料の 1 つです。この資料は単独でもご使用いただけますが、本来の目的はオンラインの Troubleshooting Assistant モジュールで特定された問題の解決方法を提供することです。

マニュアルの内容

Cisco Systems

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

OL-1270-02-J

FastEthernet の制限

Cisco 7304 の FastEthernet ポートは管理専用です。管理以外の用途に FastEthernet ポートを使うことはできません。

Network Services Engine 100 のハードウェア リビジョンと IOS の互換性に関する注意事項

ハードウェア リビジョン 5.0 以上の Network Services Engine 100（NSE-100）をご使用の場合は、ルータを動作させるために Cisco IOS Release 12.1(12c)EX1 が必要です。

ハードウェア リビジョン番号を調べるには、**show diag** *slot-number* コマンドを入力し（*slot-number* は NSE-100 が搭載されているスロット）、出力されたハードウェア リビジョンを確認します。ハードウェア リビジョン番号が 5.0 以上で、Cisco IOS Release 12.1(12c)EX1 以上が稼働していない場合は、ご使用の IOS をサポート対象のリリースにアップグレードしてください。

ハードウェア リビジョン番号は、次の例のように出力されます。リビジョン番号が表示されたら、NSE のハードウェア リビジョンであることを確認してください。ほかのコンポーネントのリビジョン番号と間違えないようにしてください。

```
Router(boot)# show diag 0
Slot 0/1:
        NSE Card state:Primary
        Insertion time:00:00:28 ago
C7300 NSE Mainboard EEPROM:
        Hardware Revision        :5.0
        PCB Serial Number        :CAB0529JQGB
        Part Number              :73-5198-02

...
```

PXF 機能

以下の表は、Cisco 7304 ルータで使用できる Parallel eXpress Forwarding（PXF）機能とその機能を最初にサポートした IOS リリースをまとめたものです。このリストには、特別な IOS リリース トレインに導入された機能が最初に組み込まれたメジャー IOS リリースも記載してあります。

（注） Cisco IOS Release 12.1 EX、12.2 YZ、および 12.2 SZ に導入された PXF 機能はすべて Cisco IOS Release 12.2(18)S で使用可能になっています。12.2(18)S は、Cisco 7304 ルータをサポートした最初の 12.2 S リリースです。ただし例外が 1 つあり、MPLS VPN にマップされた GRE トンネルは、Cisco IOS Release 12.2(18)S の PXF 処理パスでは VRF を認識できません。

PXF 機能	PXF サブ機能	説明	最初にサポートされた Cisco IOS リリース
ACL	Turbo ACL（入力または出力）	送信元 IP アドレスとマスクのマッチング	Release 12.1(9)EX Release 12.2(18)S
		宛先 IP アドレスとマスクのマッチング	Release 12.1(9)EX Release 12.2(18)S
		IP プロトコルのマッチング	Release 12.1(9)EX Release 12.2(18)S
		IP TOS バイト（precedence または DSCP）のマッチング	Release 12.1(9)EX Release 12.2(18)S
		IP L4 送信元ポートのマッチング	Release 12.1(9)EX Release 12.2(18)S
		IP L4 宛先ポートのマッチング	Release 12.1(9)EX Release 12.2(18)S
		ACL 課金[1]（ACE によるマッチング統計）	Release 12.1(10)EX Release 12.2(18)S
Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）		GRE サポート	Release 12.1(13)EX Release 12.2(18)S
		GRE トンネル IP 送信元および宛先 VRF メンバーシップ	Release 12.2(20)S
		GRE トンネル インターフェイス上での QoS 事前分類	Release 12.1(13)EX Release 12.2(18)S
		GRE トンネル インターフェイス上での NAT	Release 12.1(13)EX Release 12.2(18)S
ICMP		echo reply メッセージ	Release 12.1(10)EX Release 12.2(18)S
		host unreachable メッセージ	Release 12.1(10)EX Release 12.2(18)S
		fragmentation required but DF set メッセージ	Release 12.1(10)EX Release 12.2(18)S
		ACL deny メッセージ	Release 12.1(10)EX Release 12.2(18)S
		time exceeded メッセージ	Release 12.1(10)EX Release 12.2(18)S

PXF 機能	PXF サブ機能	説明	最初にサポートされた Cisco IOS リリース
Multiprotocol Label Switching（MPLS）		MPLS 基本サポート	Release 12.1(12c)EX Release 12.2(18)S
		MPLS VPN サポート[2]	Release 12.1(12c)EX Release 12.2(18)S
		MPLS AToM — Ethernet over MPLS	Release 12.2(14)SZ Release 12.2(18)S
		MPLS VPN — 送信元 IP アドレスに基づく VRF 選択	Release 12.2(14)SZ Release 12.2(18)S
		MPLS トラフィック処理 — 基本的な PXF スイッチングおよび課金	Release 12.2(14)SZ3 Release 12.2(18)S
		MPLS トラフィック処理 — 負荷分散	Release 12.2(14)SZ3 Release 12.2(18)S
		MPLS トラフィック処理 — 帯域幅自動調整	Release 12.2(14)SZ3 Release 12.2(18)S
		MPLS トラフィック処理 — 1 ホップトンネルのサポート	Release 12.2(14)SZ3 Release 12.2(18)S
		MPLS トラフィック処理 — フレームリレー、802.1q、および ATM のサブインターフェイス上での MPLS トラフィック処理のサポート	Release 12.2(14)SZ3 Release 12.2(18)S
Netflow	課金およびエクスポート、v8	Autonomous System（AS; 自律システム）集計	Release 12.1(9)EX Release 12.2(18)S
		宛先プレフィクス集計	Release 12.1(9)EX Release 12.2(18)S
		プロトコルおよびポート集計	Release 12.1(9)EX Release 12.2(18)S
		送信元プレフィクス集計	Release 12.1(9)EX Release 12.2(18)S
	課金およびエクスポート、v5		Release 12.1(13)EX Release 12.2(18)S
	課金およびエクスポート、v9	BGP ネクストホップのサポート	Release 12.2(20)S
		メイン フロー キャッシュ フォーマットのエクスポート	Release 12.2(20)S
		AS 集計キャッシュのエクスポート	Release 12.2(20)S
		プロトコル ポート集計キャッシュのエクスポート	Release 12.2(20)S
		送信元プレフィクス集計キャッシュのエクスポート	Release 12.2(20)S
		宛先プレフィクス集計キャッシュのエクスポート	Release 12.2(20)S

PXF 機能	PXF サブ機能	説明	最初にサポートされた Cisco IOS リリース
Network Address Translation（NAT; ネットワーク アドレス変換）	スタティック NAT、ダイナミック NAT、およびオーバーロード設定の NAT	NAT のサポート	Release 12.1(12c)EX Release 12.2(18)S
Quality of Service（QoS; サービス品質）	モジュラ QoS コマンドライン インターフェイス機能	Class-Based Weighted Fair Queuing（CBWFQ; クラス ベース均等化キューイング）（**bandwidth** コマンド）	Release 12.2(11)YZ Release 12.2(18)S
		ACL のマッチング（アクセス グループ）	Release 12.1(9)EX2 Release 12.2(18)S
		IP DSCP のマッチング	Release 12.2(11)YZ Release 12.2(18)S
		IP precedence のマッチング	Release 12.2(11)YZ Release 12.2(18)S
		IP RTP のマッチング	Release 12.2(11)YZ Release 12.2(18)S
		MPLS EXP ビットのマッチング	Release 12.1(12c)EX Release 12.2(20)S
		QoS グループのマッチング	Release 12.2(20)S
		ATM CLP ビットのマーキング（**police** コマンドの **set atm-clp** および **set-atm-clp** *action*）	Release 12.2(11)YZ Release 12.2(18)S
		フレーム リレー廃棄適性ビットのマーキング（**police** コマンドの **set fr-de** および **set-frde-transmit** *action*）	Release 12.2(20)S
		IP precedence のマーキング	Release 12.1(9)EX2 Release 12.2(18)S
		IP DSCP のマーキング	Release 12.1(9)EX2 Release 12.2(18)S
		MPLS EXP ビットのマーキング（**police** コマンドの **set mpls experimental** および **set-mpls-exp-transmit** *action*）	Release 12.1(12c)EX 1 Release 12.2(18)S
		QoS グループのマーキング	Release 12.2(20)S
		ネスト化クラス マップ	Release 12.1(9)EX2 Release 12.2(18)S
		サブインターフェイス トラフィックのポートレベル キューイングおよび QoS	Release 12.2(20)S
		プライオリティ キューイングおよび標準キューイング	Release 12.1(9)EX2 Release 12.2(18)S
		キュー制限の設定（**queue-limit** コマンド）	Release 12.2(11)YZ Release 12.2(18)S
		モジュラ QoS CLI クラス別のトラフィック ポリシング	Release 12.1(10)EX1 Release 12.2(18)S

PXF 機能	PXF サブ機能	説明	最初にサポートされた Cisco IOS リリース
		フレーム リレーおよび802.1qサブインターフェイスにおけるネスト化トラフィック ポリシーの子ポリシーによるトラフィック ポリシング	Release 12.2(11)YZ Release 12.2(18)S
		トラフィック ポリシング（階層型入力ポリシング）	Release 12.2(20)S
		トラフィック シェーピング（**shape average** コマンドのみ）	Release 12.2(11)YZ Release 12.2(18)S
		ネスト化ポリシー マップを使用した VLAN（仮想 LAN）別またはフレーム リレー VC のトラフィック シェーピング	Release 12.2(11)YZ Release 12.2(18)S
		Weighted Random Early Detection（WRED; 重み付きランダム早期検出）— IP DSCP ベース	Release 12.2(11)YZ Release 12.2(18)S
		WRED — IP precedence ベース	Release 12.1(10)EX2 Release 12.2(18)S
	QoS MIB	モジュラ QoS CLI 機能のクラスベース QoS MIB サポート	Release 12.2(11)YZ Release 12.2(18)S
スイッチング	CEF（IPv4）	宛先単位の負荷分散	Release 12.1(9)EX Release 12.2(18)S
		Reverse Path Forwarding（RPF）	Release 12.1(10)EX1 Release 12.2(18)S
レイヤ2カプセル化	ARPA	イーサネット タイプのインターフェイスのカプセル化	Release 12.1(9)EX Release 12.2(18)S
	802.1Q	イーサネット タイプのインターフェイスまたはサブインターフェイスのカプセル化	Release 12.1(10)EX1 Release 12.2(18)S
	SNAP	イーサネット タイプのインターフェイスの入力側	Release 12.1(9)EX Release 12.2(18)S
	PPP	POS および DS3 インターフェイスのカプセル化	Release 12.1(9)EX Release 12.2(18)S
	HDLC	POS および DS3 インターフェイスのカプセル化	Release 12.1(9)EX Release 12.2(18)S
	フレーム リレー	フレーム リレーのカプセル化	Release 12.1(10)EX2 Release 12.2(18)S
	AAL5 SNAP	ATM インターフェイス/VC のカプセル化	Release 12.1(10)EX1 Release 12.2(18)S
	AAL5 MUX	ATM インターフェイス/VC のカプセル化	Release 12.1(10)EX1 Release 12.2(18)S
	AAL5 NLPID	ATM インターフェイス/VC のカプセル化	Release 12.1(10)EX1 Release 12.2(18)S

1. Cisco IOS Release 12.1(10)EX より前のリリースでは、Cisco 7304 ルータ上で ACL 課金を利用できるのは、Route Processor（RP; ルート プロセッサ）が処理したパケットに限られていました。
2. Cisco IOS Release 12.2(18)S を使用している場合、MPLS VPN にマップされた GRE トンネルでは VRF を認識できません。

PXF 機能の制限

現在のところ、PXF 機能のサポートには次の制限があります。

- ACL ログ機能はサポートされていません。

PXF でのフレーム リレーに関する制限

- PXF ではフレーム リレーのトラフィック シェーピングはサポートされていません。
- **show frame-relay pvc** コマンドの出力に含まれるのは、入力パケット数、出力パケット数、入力バイト数、出力バイト数、廃棄パケットのみです。
- フレーム リレー スイッチングおよびフレーム リレー パケットのその他の非 IP フォワーディングは、PXF プロセッサではサポートされません。これらのパケットは Route Processor（RP; ルート プロセッサ）でサポートされます。
- 現在のところ、Cisco 7304 ルータでは、フレーム リレーでの PPP（ポイントツーポイント プロトコル）はサポートされていません。
- フレーム リレーの標準 IP 機能はサブインターフェイス単位で設定できます。
- フレーム リレーのフラグメンテーションおよびフレーム リレーのヘッダー圧縮は、PXF ではサポートされていません。
- フレーム リレー Virtual Circuit（VC; 仮想回線）上のクラス キューでの WRED は、Cisco IOS Release 12.2(11)YZ からサポートされています。このリリースより前の Cisco IOS では、フレーム リレー VC での WRED はサポートされていませんでした。

GRE の制限

- GRE では、PXF アクセラレーションはユニキャスト IPv4 ペイロードに制限されます。PXF で処理されていない GRE トラフィックは RP スイッチング パスで処理されます。
- トンネルに次のいずれかの要素が設定されている場合、GRE PXF アクセラレーションは発生しません。
  - トンネル チェックサム
  - キー
  - path-mtu-discovery
  - シーケンス
  - udlr
- PXF では、再組み立てが必要な分割 GRE パケットは終端できません。再組み立てが必要な分割 GRE パケットは RP で処理されます。
- PXF は、GRE パケットを終端する前に、そのパケットを終端できる適切なトンネルを探します。適切なトンネルが見つからないと、パケットは RP で処理されます。
- トンネルを通じてルータに入り、同じトンネルまたは別のトンネルを通じてルータから出るパケットは、RP で処理されます。つまり、連続したデカプセル化とカプセル化を必要とする GRE パケットは PXF 処理パスでは処理されません。
- PXF は、MPLS over GRE 機能をサポートしていません。GRE トンネルで受信された MPLS パケットは PXF プロセッサで処理されます。

ICMP の制限

- 宛先到達不能メッセージ（host unreachable、fragmentation required but DF set、ACL deny）はインターフェイス単位でレートが制限されます。レート制限の間隔は 0.5 秒です。
- **debug ip icmp** コマンドを使用すると、ICMP デバッグ情報がイネーブルになっていても、ICMP 処理が RP で実行されます。

MPLS の制限

MPLS VPN に入る IP パケットに対しては負荷分散はアクティブになりません。

MPLS トラフィック処理の制限

次の MPLS-TE 機能はサポートされていません。

- Diff-Serv 認識 TE
- MPLS-TE インターエリア
- MPLS-TE MIB
- MPLS-TE FRR
- MPL-TE FRR MIB

NAT の制限

- **ip nat outside** インターフェイスに入るか、または **ip nat inside** インターフェイスから **ip nat outside** インターフェイスに進むすべての ICMP ECHO（ping）パケットおよび IP 分割パケットは、RP で処理されます。したがって、Cisco 7304 ルータ上で、PXF の NAT の ping テストを実行する場合は、すべての ping パケットが自動的に RP で処理されます。
- NAT でマッピング可能なトラフィック フロー（つまり、ダイナミック NAT またはスタティック NAT のエントリで使用されている ACL のどれかと一致するフロー）の最初のパケットは、その NAT エントリが PXF で見つからないと、RP で処理されます。最初のパケットが RP で処理されると、PXF に NAT エントリが作成され、そのトラフィック フロー ペアのその後のパケットは PXF プロセッサで処理されます。
- Cisco 7304 ルータがサポートしている PXF の NAT エントリ数は 32,000 です。この限界を超えるトラフィックは、RP で処理されます。
- NAT でマッピング可能な非 TCP/UDP IP トラフィックは、常に RP で処理されます。
- RP 内の 1 つの NAT ハーフ エントリ（ポート情報を含まないエントリ）によって、PXF に複数の NAT エントリを作成することも可能です。
- **show c7300 pxf interface** コマンドまたは **show pxf interface** コマンドの出力では、**ip nat outside** インターフェイス上に入力と出力両方の NAT フラグがあります（Cisco IOS Release 12.2(14)SZ では、**show c7300 pxf interface** コマンドが **show pxf interface** コマンドになります。以下の出力には **show pxf interface** が使用されていますが、場合によっては **show c7300 pxf interface** を使用する必要があります）。**ip nat inside** インターフェイス上には、入力機能フラグを含む NAT 機能のフラグはありません。

これを表す出力例を示します。インターフェイス POS 5/2 が **ip nat outside** インターフェイスであり、このインターフェイス上に入力と出力の NAT フラグがあります。

```
Router# show running-config

interface POS5/1
ip address 192.168.0.10 255.255.255.0
ip nat inside
!
interface POS5/2
ip address 171.200.1.32 255.255.0.0
ip nat outside
!
...

Router# show pxf interface all

...

PXF-If:Y 00017  PO5/1      (Down, Processing Input)
Features:in=CEF  [0x201],  out=None [0x0]  qstatus=XON

No NAT feature flags

Ingress Packets:             0   Input Drop Packets :             0
Egress Packets :             0   Output Drop Packets:             0

PXF-If:Y 00018  PO5/2      (Up, Processing Input)
Features:in=CEF NAT  [0x300],  out=NAT  [0x2]  qstatus=XON

Ingress Packets:           147   Input Drop Packets :             0
Egress Packets :           147   Output Drop Packets:             0
```

- ペイロードで IP アドレスまたはポート情報を伝送するプロトコルのパケットは、Cisco 7304 ルータでは、PXF を使用する NAT 変換はできません。これらのパケットは、代わりに RP を使用して NAT 変換されます。

  次のリストは、ペイロードで IP アドレスまたはポート情報を伝送するために、Cisco 7304 上の PXF で NAT を通じて処理できないプロトコルの例（一部）です。

  - シスコ IP Phone から CallManager へ
  - CUSeeMe
  - DNS の A および PTR のレコード
  - FTP
  - NetMeeting V2.x の H.323v1
  - H.323v2 Call Signalling（FastConnect）
  - NetMeeting V3.x の H.323v2
  - ICMP
  - IPv6 プロトコル変換 — フラグメンテーション
  - IPv6 プロトコル変換 — FTP
  - IPv6 プロトコル変換 — PAT
  - IP マルチキャスト、送信元変換
  - NetBIOS over TCP/IP
  - NetMeeting ILS ディレクトリ
  - NFS
  - PPTP
  - r コマンド（rsh、rlogin、rexec）
  - RealAudio
  - Remote Procedure Call（RPC）

- SQLNet
- StreamWorks
- TFTP
- VDOLive
- VXtreme
- Windows Media Technology（NetShow）

QoS の制限

- Cisco IOS Release 12.1(12c)EX1 では、PXF の各ポリシー マップに割り当てられるトラフィック クラスのキュー数が 4 つから 8 つに増えました。これらの 8 つのトラフィック クラス キューのうち、1 つのトラフィック クラス キューがデフォルトのトラフィック クラスに割り当てられ、もう 1 つのキューがプライオリティ キューイングに割り当てられます。Cisco IOS Release 12.2(11)YZ から、プライオリティ トラフィック用の予約キューはなくなりました。プライオリティ クラスの設定に基づいて、1 つのキューがプライオリティ トラフィック用に指定されます。ただし、デフォルト クラス トラフィック用に 1 つと、重要なローカル送信元トラフィック（キープアライブやルーティング プロトコルの hello など）用に 1 つのキューが予約されています。したがって、ユーザが設定できるのは残りの 6 つのキューです（プライオリティ用のキューを 1 つ含む）。
- Release 12.2(11)YZ 以上のイメージでは、PXF の各ポリシー マップに 8 つのトラフィック キューと 8 つのトラフィック クラスを設定できます。これらの 8 つのトラフィック クラスのうち、1 つのトラフィック クラスがデフォルトのトラフィック クラス用に予約され、もう 1 つがプライオリティ トラフィック用に予約されています。したがって、ユーザの設定には、6 つの独立したクラスがあります。
  キューとクラスの区別は重要です。キューは、クラスにキューイング コマンド（**bandwidth** または **priority**）がある場合に割り当てられます。一方、クラスには何らかの QoS アクションを含めることができます。
  Release 12.2(20)S では、使用できるトラフィック キューは 8 つのままですが、23 のトラフィック クラスを使用できるようになりました。つまり、設定可能な最大クラス数は 23 ですが、キューイング コマンドを含めることができるのは、デフォルト トラフィック クラス以外の 6 つクラスだけです。

- **match** コマンドを使用すると ACL のマッチングを実行できます。PXF トラフィックを分類するには、**match access-group** コマンドを使用して、ACL をトラフィック クラスと照合します。Cisco 7304 ルータの PXF がサポートしているのは Turbo ACL だけです。したがって、次の分類基準はサポートされていません。
  - 送信元または宛先の MAC アドレス
  - IP 固有の値（12.1EX ベースのリリースのみ。Cisco IOS Release 12.2(11)YZ からは、**match ip precedence**、**match ip dscp**、および **match ip rtp** が使用可能になりました。）
  - QoS グループ（QoS グループのマッチングは、Cisco IOS Release 12.2(20)S で導入されています。）
- 12.2(20)S より前の IOS リリースでは、1 つのサービス ポリシーに利用できるクラスは 8 つだけです。1 つのサービス ポリシーに 9 つ以上のトラフィック クラスを設定しても、エラー メッセージは表示されません。ただし、サービス ポリシーによって認識されるのは、最初の 8 つのトラフィック クラスだけです。Release 12.2(20)S では、利用可能なトラフィック キューはやはり 8 つですが、利用可能なトラフィック クラスは 23 個あります。つまり、23 のクラスを設定可能ですが、キュー コマンドを含めることができるのは、デフォルト トラフィック クラス以外の 6 つのクラスです。
- Release 12.2(20)S より前のリリースでは、各クラス マップ内の match ステートメントの最大数は 15 でしたが、Release 12.2(20)S からは、各クラス マップ内の match ステートメントの最大数が 31 になりました。
  この制限を超えても、トラフィックは指定どおり処理されますが、**show policy-map** コマンドおよびクラスベース QoS MIB の match ステートメントによる課金は発生しません。

- 個々の match ステートメントのカウンタは、親クラスのポリシー マップではサポートされません。
- 階層型ポリシー マップのポリシー マップ レベルの最大数は 2 です。
- CLI で低遅延キューイング（**priority** コマンド）を指定すると、kbps 値を入力するように要求されます。ただし、入力した kbps 値は使用されません。**priority** コマンドは、そのトラフィック クラスに属するトラフィックの送信先をプライオリティ キューに指定するための重要なコマンドです。kpbs 値自体は使用されませんが、入力する必要があります。Cisco IOS Release 12.2(11)YZ から、**priority** コマンドに *kbps* 値が必要となりました。この値は、*mir*（最大情報レート）として利用され、プライオリティ キューはこのレートにシェーピングされます。

  ただし、Cisco IOS Release 12.2(14)SZ からは、NSE-100 で **priority** コマンドの *kpbs* 値を設定できなくなりました。**priority** コマンドを含むポリシー マップをレートを指定せずに設定した場合、プライオリティ キューのポリシー マップがすべての *cir*（すべてのリンク帯域幅）を取得し、プライオリティ クラスは不適合トラフィックをすべて廃棄しなければなりません。したがって、他のトラフィック クラスの帯域幅は保証されません。プライオリティ キューには、**police** コマンドを設定できます。police に指定したレートは、プライオリティ キューの帯域幅として使用されるので、**bandwidth** コマンドを使用することによって、余った帯域幅を他のクラスに割り当てることができます。
- **rsvp** オプションは、**random-detect dscp** コマンドのオプションとして使用することはできません。
- **match atm-clp** コマンドを使用してトラフィック クラスのパケットを照合する機能は、現在のところ PXF では利用できません。ATM CLIP ビットと一緒に IP precedence/DSCP または MPLS Exp のビットをマーキングする出力サービス ポリシーでは、**set atm-clp** コマンドをその他のすべての set オプションと同時に使用できます。ただし、ポリシングでは **set-clp-transmit** コマンドを他の **set** コマンドと組み合わせて使用することはできません。ATM 対 ATM のトラフィックの場合は、出力サービス ポリシーで **set atm-clp** コマンドまたは **set-clp-transmit** コマンドを使用して明示的に変更しない限り、出力側でも入力 CLIP ビットが維持されるので注意してください。
- 階層型サービス ポリシーの親ポリシー マップでは、**set** コマンドを使用することはできません。
- 802.1Q サブインターフェイスまたはフレーム リレー VC で、ネスト化ポリシー マップの子ポリシーに使用できるのは、**bandwidth** と **priority** だけです。サブインターフェイスまたは VC および子ポリシーに MIR を指定する場合、親ポリシーに設定するクラスは、**shape** コマンドを含むデフォルト クラス 1 つだけにしなければなりません。
- トラフィックのシェーピングが可能なのは、**shape average** を適用しているインターフェイスだけです。**shape peak** などのその他のトラフィック シェーピング オプションは、現在、PXF には実装されていません。
- **queue-limit** コマンドを使用できるのは、**priority** コマンドも **random-detect** コマンドも設定されていないクラスだけです。**random-detect** が設定されているクラスでは、WRED 方式でクラスのキュー サイズを計算するために *max-threshold* 値が使用されます。**queue-limit** コマンドまたは random-detect の最大スレッシュホールドによるクラス キュー サイズの設定が可能なのは、Cisco IOS Release 12.2(11)YZ 以上の IOS リリースだけです。
- Release 12.2(20)S では、サポートする階層型ポリシー マップの設定タイプが増え、この新しい設定機能によって、新たに次の制限が生じました。
  - 階層型サービス ポリシーを作成するためにクラス マップ内に **service-policy** コマンドを入力する場合、階層型サービス ポリシー内のクラス数は、ポリシー マップ当たり最大 23 個です。この制限値は、階層型サービス ポリシー単位ではなく、ポリシー マップ単位で適用される点に注意してください。1 つのポリシー マップに複数の階層型サービス ポリシーを指定することが可能ですが、これらの階層型サービス ポリシー全体のクラス数の合計が 23 を超えないようにする必要があります。子ポリシーのデフォルト トラフィック クラスは、これらの 23 クラスの 1 つとしてカウントされます。
  - 子ポリシー マップに **bandwidth** コマンドおよび **priority** コマンドを設定できるのは、親クラス マップに **shape** コマンドが設定されている場合だけです。親クラスはデフォルト クラスでなければなりません。また、親ポリシー マップに別のクラスを追加することができません。

- Release 12.2(20)S では、サブインターフェイス トラフィックに対してポートレベルのキューイングと QoS を利用できます。サブインターフェイス トラフィックに対するポートレベルのキューイングと QoS の機能を使用すると、802.1q サブインターフェイスと DLCI に、ポートレベルの QoS の設定を適用できます。802.1q サブインターフェイスと DLCI に個別に QoS 機能を適用することも可能です。802.1q サブインターフェイスまたは DLCI の設定がポートレベルの QoS 設定と矛盾する場合は、常に 802.1q サブインターフェイスと DLCI 上の QoS 設定がポートレベルの QoS 設定よりも優先されます。

  フレーム リレーとイーサネットのポートを特定の DLCI または 802.1q サブインターフェイスと照合することはできませんが、DLCI および 802.1q サブインターフェイス上のトラフィックはその他の一致基準によって照合可能です。
- あるクラスのトラフィックを照合する場合、ACL の一致や MPLS EXP 値の一致よりも qos-group の一致が優先されます。
- 階層型入力ポリシングの目的は、まずデフォルト トラフィックの合計をポリシングしてから、ネストされた各トラフィック クラスに属すトラフィックのポリシング（マーキングによって）または廃棄を実行することです。

  階層型入力ポリシングの設定では、子ポリシー マップに最大 23 個のユーザ定義クラスを含めることができます。ただし、子ポリシーを含むサービス ポリシーは、必ずデフォルト トラフィック クラスに設定する必要があります。さらに、このデフォルト トラフィック クラスは、親ポリシー マップ上の唯一のクラスでなければなりません。

Reverse Path Forwarding（RPF）の制限

セカンダリ アドレスを持つインターフェイス上に RPF が設定されている場合、そのインターフェイス上で受信されたパケットはすべて RP で処理されます。

PXF 処理の概要

PXF でサポートされていない入力機能をインターフェイスに設定した場合、そのインターフェイスに着信するデータ パケットはどれも PXF プロセッサでは処理されず、RP で処理されます。同様に、PXF でサポートされていない出力機能をインターフェイスに設定した場合、そのインターフェイスから発信されるデータ パケットの出力機能は PXF プロセッサでは処理されず、RP で処理されます。

したがって、PXF でまだサポートされていない機能がインターフェイスに設定されていると、PXF でサポートされている機能のパフォーマンスも予想を下回る可能性があります。

必要な機能がサポートされていない場合

サポートされていない PXF 機能がサポートされる時期については、購入された代理店にお問い合わせください。Cisco TAC は、サポート時期に関する情報を保持していないので、これに関する質問には対応できません。

課金情報

7304 ルータでは、他のルータよりも、**show** コマンドで取得される課金情報が少なくなっています。これは、オーバーヘッドを回避するために、現在、PXF プロセッサから取得可能な課金情報が最低限に抑えられているからです。

PXF プロセッサ内にこのような情報を保持し、RP から取り出して、**show** コマンドや MIB 変数に取り込む処理では、かなりのオーバーヘッドが発生することがあります。したがって、PXF プロセッサ内では不可欠な課金情報のみが処理されます。

ACL 課金

ACL 課金機能を使用すると、ユーザは **show** コマンドによって、ACL エントリに一致するパケット数を追跡できます。アクセス リストに関する情報を表示する **show** コマンドは、**show ip access-lists** など、たくさんあります。このような **show** コマンドの多くは、各 ACL エントリに一致する PXF 交換パケットと RP 交換パケットの数が両方出力されるように、機能が拡張されています。以前は、このような **show** コマンドの出力では、各 ACL エントリに一致する RP 交換パケットの数だけが表示されていました。

PXF 用 ACL 課金機能は、Cisco IOS Release 12.1(10)EX で導入されています。

PXF コンフィギュレーションの例

ACL のコンフィギュレーション例

単純な ACL（0 ～ 99）

送信元 IP アドレスとマスクのマッチング

```
access-list access-list-number {deny | permit} source [source-wildcard]
access-list access-list-number {permit} source [source-wildcard]
```

拡張 ACL（100 ～ 199）

送信元および宛先 IP アドレスとマスクのマッチング

```
access-list access-list-number {deny | permit} IP source source-wildcard
destination destination-wildcard
```

IP プロトコルのマッチング

```
access-list access-list-number {deny | permit} protocol source source-wildcard
destination destination-wildcard
```

IP TOS バイトのマッチング

```
access-list access-list-number {deny | permit} protocol source source-wildcard
destination destination-wildcard [tos tos]
```

IP precedence 値のマッチング

```
access-list access-list-number {deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence]
```

IP DSCP 値のマッチング

```
access-list access-list-number {deny | permit} protocol source source-wildcard
destination destination-wildcard [DSCP dscp]
```

IP L4 送信元ポートまたは宛先ポートのマッチング

```
access-list access-list-number {deny | permit} {tcp | udp} source source-wildcard
[operator [source-port]] destination destination-wildcard [operator
[destination-port]]
```

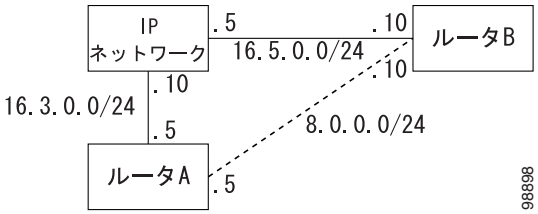
ACL 課金

次のコマンド出力では、各 ACL にパケットが一致した回数が表示されています。この出力が Cisco IOS Release 12.1(9)EX を稼働している Cisco 7304 ルータのものである場合、各 Access Control Entry（ACE; アクセス制御エントリ）の一致数は、その ACE に一致した RP 交換パケットの数を示します。この出力が Cisco IOS Release 12.1(10)EX 以降を稼働している Cisco 7304 ルータのものである場合、各 ACE の一致数は、その ACE に一致した RP 交換パケットと PXF 交換パケットの合計数を示します。

```
Router# show ip access-lists source_only
Extended IP access list source_only (Compiled)
    permit udp host 1.1.1.3 eq snmp host 2.1.1.3 (994598 matches)
    permit udp host 1.1.1.3 eq snmptrap host 2.1.1.3 (994598 matches)
    deny udp host 1.1.1.3 eq xdmcp host 2.1.1.3 (994596 matches)
    deny udp host 1.1.1.3 eq ntp host 2.1.1.3 (994595 matches)
```

GRE コンフィギュレーションの例

基本的な GRE コンフィギュレーション



次の例では、IP ネットワークを通じてルータ A とルータ B を接続するために、単純な GRE トンネルが設定されています。このコンフィギュレーションでは、次の点に留意してください。

- トンネルの送信元は、ルータ上に存在するいずれかの物理 IP アドレス、またはループバックアドレスです。
- トンネルの送信元は、IP アドレスまたはインターフェイス名で指定できます。
- up/up 状態のトンネルでは、トンネルの宛先へのルートが存在していなければなりません。次の例では、これらのルートを指定するためにスタティック ルートが使用されています。

ルータ A

```
interface tunnel 0
ip address 8.0.0.5
tunnel source 16.3.0.5
tunnel destination 16.5.0.0

ip route 16.5.0.0 255.255.255.0 16.3.0.10
```

ルータ B

```
interface tunnel 0
ip address 8.0.0.10
tunnel source 16.5.0.0
tunnel destination 16.3.0.5


ip route 16.3.0.5 255.255.255.0 16.5.0.10
```

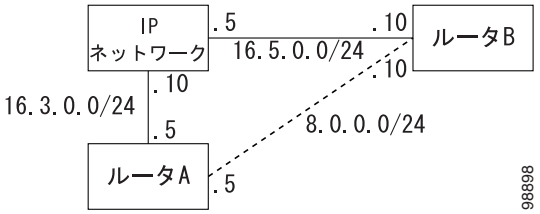
QoS の事前分類例

パケットがトンネルでカプセル化され、物理インターフェイスを通じて送出される場合、そのインターフェイスに設定されている QoS 機能はいずれも、トンネル（外側）のヘッダーのみを認識します。同じトンネルを通過する異なるパケットはすべてトンネル ヘッダーが同じになります。したがって、たとえ物理インターフェイスが輻輳状態であっても、QoS はこれらのパケットを同じように処理します。

このような設定が望ましい場合はほとんどなく、QoS は元の（内側の）パケット ヘッダーに基づいて適用される必要があります。そのためには、カプセル化される前にパケットを分類し、QoS 適用時に、分類情報を利用できるようにしなければなりません。

インターフェイス レベルの **qos pre-classify** コマンドを使用すると、トンネルでカプセル化される前に強制的にパケットを分類することができます。

下記の図は、次の例のような QoS 事前分類が適用される場合の設定を表しています。



ルータ A の QoS 事前分類例

```
class-map match-all source_address
 match access-group 5


policy-map set_ip
 class source_address
  set ip precedence 2


interface Loopback0
 ip address 25.0.0.5 255.255.255.0
!
```

（QoS 事前分類は、このトンネル インターフェイスには設定されません。）

interface Tunnel0

ip address 8.0.0.5 255.255.255.0

tunnel source Loopback0

tunnel destination 5.0.0.5

.

（QoS 事前分類は、出力インターフェイスに適用されます。）

interface POS2/1

ip address 16.3.0.5 255.255.255.0

service-policy output set_ip

no keepalive

clock source internal

end

!

ip route 0.0.0.0 0.0.0.0 tunnel0

ip route 5.0.0.5 255.255.255.255 16.3.0.10

access-list 5 permit 16.21.0.0 0.0.0.255

たとえ上記のアクセス リストと送信元アドレスが一致するパケットが入ってきても、トンネルを通過するパケットには QoS は適用されません。この場合、**show policy-map interface pos2/1** コマンドの出力は次のようになります。

```
Router# show policy-map interface pos2/1
 POS2/1

  Service-policy output:set_ip

    Class-map:set_ip (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 5
      QoS Set
        ip precedence 3
          Packets marked 0

    Class-map:class-default (match-any)
      87532 packets, 7355760 bytes
      5 minute offered rate 68000 bps, drop rate 0 bps
      Match:any
```

これは、パケットがカプセル化され、アクセス リストと一致している元の（内側の）ヘッダーが認識できないためです。カプセル化後もヘッダーが認識できるようにするには、トンネルに **qos pre-classify** コマンドを設定する必要があります。

interface t0

ip address 8.0.0.5

tunnel source 16.3.0.5

tunnel destination 16.5.0.5

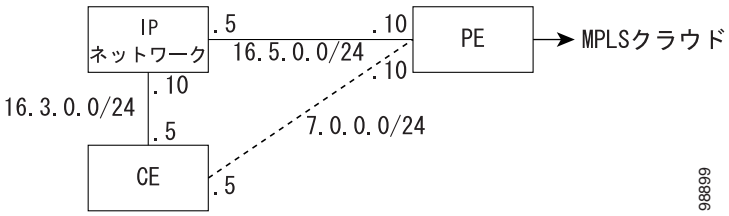
qos pre-classify

このようにすると、**show policy-map interface pos2/1** に、クラス マップと一致するトンネル パケットとそのトンネル パケットに適用された QoS が表示されます。

```
Router# show policy-map interface pos2/1
 POS2/1

  Service-policy output:set_ip

    Class-map:set_ip (match-all)
      3328 packets, 279552 bytes
      5 minute offered rate 15000 bps, drop rate 0 bps
      Match:access-group 5
      QoS Set
        ip precedence 2
          Packets marked 3328

    Class-map:class-default (match-any)
      2 packets, 370 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

GRE トンネルと MPLS VPN のマッピング

この例では、GRE トンネルは、Customer Edge（CE; カスタマー エッジ）と Provider Edge（PE; プロバイダー エッジ）の間で機能しています。MPLS クラウドに送出する場合、PE はまずトンネルを終了してからラベルを付けます。CE に送出する場合、PE は着信ラベルを廃棄してからパケットをカプセル化します。この例を図示すると、次のようになります。



CE

interface Loopback0

ip address 25.0.0.5 255.255.255.0

!

interface Tunnel0

ip address 7.0.0.5 255.255.255.0

（トンネルの送信元としてループバック アドレスが使用されます。）

tunnel source Loopback0

tunnel destination 5.0.0.5

.

.

.

（次のコマンドによって、トンネルへのデフォルト ルートが設定されます。）

ip route 0.0.0.0 0.0.0.0 Tunnel0

（次のコマンドによって、トンネルの宛先へのルートが指定されます。）

ip route 5.0.0.5 255.255.255.255 16.3.0.10

PE

interface Loopback0

ip address 5.0.0.5 255.255.255.255

!

interface Tunnel1

ip address 7.0.0.10 255.255.255.0

tunnel source Loopback0

tunnel destination 25.0.0.5

!

（次のコマンドによって、トンネルの宛先へのルートが指定されます。）

ip route 25.0.0.5 255.255.255.255 16.5.0.5

基本的な VRF 認識 GRE トンネルの設定

```
interface tunnel0
 ip vrf forwarding green
 ip address 10.3.3.3 255.255.255.0
 tunnel source loop 0
 tunnel destination 10.5.5.5
 tunnel vrf blue
```

マルチプロトコル ラベル スイッチングの例

基本的な MPLS コンフィギュレーション

ip cef

mpls ip

mpls label range *minumum maximum*

mpls label protocol {**ldp** | **tdp**}

interface *interface-name number*

mpls ip

mpls label protocol {**ldp** | **tdp**}

値の入力例

```
interface gigabitethernet0/1
 ip address 74.0.0.1 255.0.0.0
 no keepalive
 negotiation auto
mpls label protocol ldp
tag-switching ip
```

MPLS VPN の定義

これは、CE ルータに接続されている PE の設定例です。このコンフィギュレーションを正しく機能させるためには、基本的な MPLS も設定する必要があります。

ip vrf *vrf-name*

rd *vpn-route-distinguisher*

route-target [**import** | **export** | **both**] *route-target-vpn-ext-community*

interface *interface-name number*

ip vrf forwarding *vrf-name*

値の入力例

```
ip vrf v11
 rd 11:11
 route-target export 11:11
 route-target import 11:11

interface gigabitethernet0/0
 ip vrf forwarding v11
ip address 80.0.0.1 255.0.0.0
no keepalive
negotiation auto
```

MPLS VPN 操作の確認

show ip vrf

show ip vrf [**brief** | **detail** | **interfaces**} *vrf-name*

show ip route vrf *vrf-name*

show ip protocols vrf *vrf-name*

show ip cef vrf *vrf-name*

show ip interface *interface-number*

show ip bgp vpnv4 all [**tags**]

show tag-switching forwarding vrf *vrf-name* [**prefix mask/length**] [**detail**]

show mpls interface [**interfaces** | **detail** | **all**]

show mpls forwarding-table [**prefix** | **detail** | **interface** | **label** | **vrf** | **lsp tunnel**]

PE から PE の BGP ルーティング セッションの設定

router bgp *autonomous-system*

neighbor [*ip-address* | *peer-group-name*] **remote-as** *number*

neighbor *ip-address* **update-source loopback0**

neighbor *ip-address* **activate**

値の入力例

```
router bgp 1
no synchronization
no bgp default ipv4-unicast
bgp log-neighbor-changes
redistribute connected
neighbor 71.71.71.71 remote-as 1
neighbor 71.71.71.71 update-source loopback0
neighbor 71.71.71.71 activate
no auto-summary
```

PE から CE の BGP ルーティング セッションの設定

router bgp *autonomous-system*

neighbor [*ip-address* | *peer-group-name*] **remote-as** *number*

neighbor *ip-address* **activate**

値の入力例

```
router bgp 1
address-family ipv4 vrf v12
neighbor 42.0.0.1 remote-as 65001
neighbor 42.0.0.1 activate
no auto-summary
no synchronization
exit-address-family
```

PE から CE の RIP ルーティング セッションの設定

router rip

version 2

address-family ipv4 [**unicast**] **vrf** *vrf-name*

version 2

network *prefix*

network *prefix*

address-family ipv4 [**unicast**] **vrf** *vrf-name*

redistribute rip

値の入力例

```
router rip
version 2

address-family ipv4 vrf v11
version 2
network 11.0.0.0
network 30.0.0.0

address-family ipv4 vrf v11
redistribute rip
```

PE または CE へのスタティック ルートのルーティング セッションの設定

ip route vrf *vrf-name address mask address*

値の入力例

ip route vrf v11 11.11.11.11 255.255.255.255 40.0.0.3

PE と CE の間の OSPF セッションの設定

router ospf *process-id* **vrf** *vpn-name*

network *ip-address subnet-mask* **area** *area-id*

network *ip-address subnet-mask* **area** *area-id*

address-family ipv4 vrf *vrf-name*

redistribute ospf *process-id* **match internal** *route-type-number* **external** *route-type-number*

値の入力例

```
router ospf 200 vrf v11
 network 40.0.0.0 0.255.255.255 area 5
 network 54.54.54.54 0.0.0.0 area 5
address-family ipv4 vrf v11
 redistribute ospf 200 match internal external 1 external 2
```

基本的な VRF 認識 GRE トンネルの設定

```
interface tunnel0
 ip vrf forwarding green
 ip address 10.3.3.3 255.255.255.0
 tunnel source loop 0
 tunnel destination 10.5.5.5
 tunnel vrf blue
```

MPLS トラフィック処理

MPLS トラフィック処理の設定については、上記の例のほかに、次のマニュアルも参考になります。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/traffeng.htm

以下に示すのは、トラフィック処理を含む MPLS コンフィギュレーションの例です。MPLS トラフィック処理の例すべてに **tunnel mpls traffic-eng** コマンド オプションが使用されています。

```
Router# show running-config
Building configuration...

Current configuration :3785 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname l7300
!
boot bootldr bootdisk:c7300-boot-mz
logging snmp-authfail
logging queue-limit 100
mpls label protocol tdp
mpls ldp logging neighbor-changes
tag-switching tdp router-id Loopback0

interface Loopback0
 ip address 5.0.0.5 255.255.255.255

interface Tunnel1
 ip unnumbered Loopback0
 load-interval 30
 tunnel destination 20.0.0.5
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng auto-bw
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth  10
 tunnel mpls traffic-eng path-option 1 explicit name path

interface POS2/1
 ip address 16.11.0.5 255.255.255.0
 no ip mroute-cache
 load-interval 30
 no keepalive
 mpls traffic-eng tunnels
 clock source internal
 ip rsvp bandwidth 133000 133000
```

```
!
interface POS2/2
 ip address 16.7.0.5 255.255.255.0
 no ip mroute-cache
 load-interval 30
 no keepalive
 mpls traffic-eng tunnels
 clock source internal
 ip rsvp bandwidth 133000 133000

router ospf 1
 log-adjacency-changes
 network 5.0.0.0 0.0.0.255 area 0
 network 8.0.0.0 0.0.0.255 area 0
 network 16.7.0.0 0.0.0.255 area 0
 network 16.11.0.0 0.0.0.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

ip explicit-path name path enable
 next-address 16.7.0.10
 next-address 16.17.0.10
!
ip explicit-path name PATH enable
 next-address 16.11.0.10
 next-address 16.17.0.10
```

AAL5NLPID の設定

interface atm3/0.1 point-to-point

pvc 5/50

encapsulation aal5nlpid

Ethernet over MPLS

Ethernet over MPLS の例については、『*MPLS AToM—Ethernet over MPLS*』の「Configuration Examples」を参照してください。

送信元 IP アドレスに基づく VRF 選択

送信元 IP アドレスに基づく VRF 選択の例は、『*MPLS VPN—VRF Selction Based on Source IP Address*』の「Configuration Examples」を参照してください。

MPLS EXP ビットのマッチングおよびマーキング

このマニュアルの「QoS の例」（p.30）を参照してください。

その他の MPLS 関連コマンド

mpls ip propagate ttl

mpls ip default-route

mpls ldp explicit null

interface *interface-name number*

mpls mtu *bytes*

Netflow のコンフィギュレーション例

AS

このコンフィギュレーションを正しく機能させるためには、BGP をイネーブルにする必要があります。

```
ip flow-export version 5 [origin-as | peer-as]
!
interface POS4/0
 ip address 172.16.1.1 255.255.255.0
 ip route-cache flow
 ...
!
ip flow-aggregation cache as
 cache entries 1024
 cache timeout inactive 10
 cache timeout active 1
 export destination 172.16.2.10 9995
enabled
```

BGP ネクストホップ

```
ip flow-export version 9 [origin-as | peer-as] bgp-nexthop
```

値の入力例

```
ip flow-export version 9 peer-as bgp-nexthop
ip flow-aggregation cache as
 cache timeout active 1
 export version 9
 export destination 16.16.16.10 7777
 enabled
```

プロトコル ポート

```
interface POS4/0
 ip address 172.16.1.1 255.255.255.0
 ip route-cache flow
...
!
ip flow-aggregation cache protocol-port
 cache entries 1024
 cache timeout inactive 10
 cache timeout active 1
 export destination 172.16.2.10 9995
enabled
```

送信元プレフィクス

```
interface POS4/0
 ip address 172.16.1.1 255.255.255.0
 ip route-cache flow
...
!
ip flow-aggregation cache source-prefix
 cache entries 1024
 cache timeout inactive 10
 cache timeout active 1
 export destination 172.16.2.10 9995
enabled
```

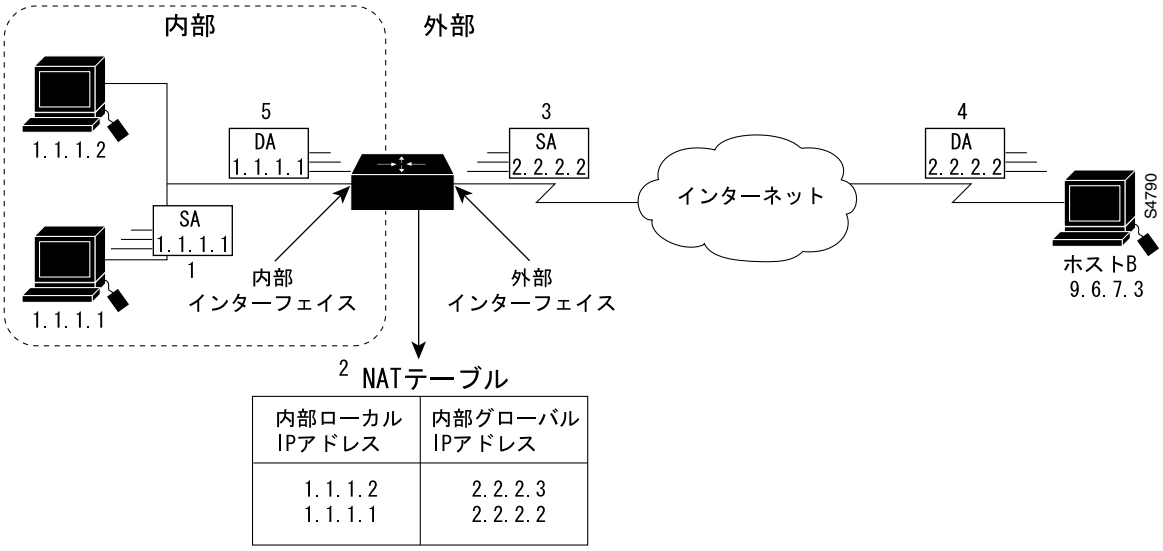
宛先プレフィクス

```
interface POS4/0
 ip address 172.16.1.1 255.255.255.0
 ip route-cache flow
...
!
ip flow-aggregation cache destination-prefix
 cache entries 1024
 cache timeout inactive 10
 cache timeout active 1
 export destination 172.16.2.10 9995
 enabled
```

NAT の例

内部から外部へのスタティックな変換

次の例は、内部の未登録スタブ ネットワーク ホストのアドレスを、スタティックな 1 対 1 方式で、外部の登録済み IP アドレスにマップする方法を示しています。この例では、内部スタブ ネットワークから出るパケットに関して、内部のローカル IP アドレス 1.1.1.2 と 1.1.1.1 が、アドレス 2.2.2.3 と 2.2.2.2 にスタティックにマップされています。




```
interface Ethernet2/1
     ip address 1.0.0.3 255.0.0.0
     ip nat inside
!
ip nat inside source static 1.1.1.2 2.2.2.3
ip nat inside source static 1.1.1.1 2.2.2.2
```

内部から外部へのダイナミックな変換

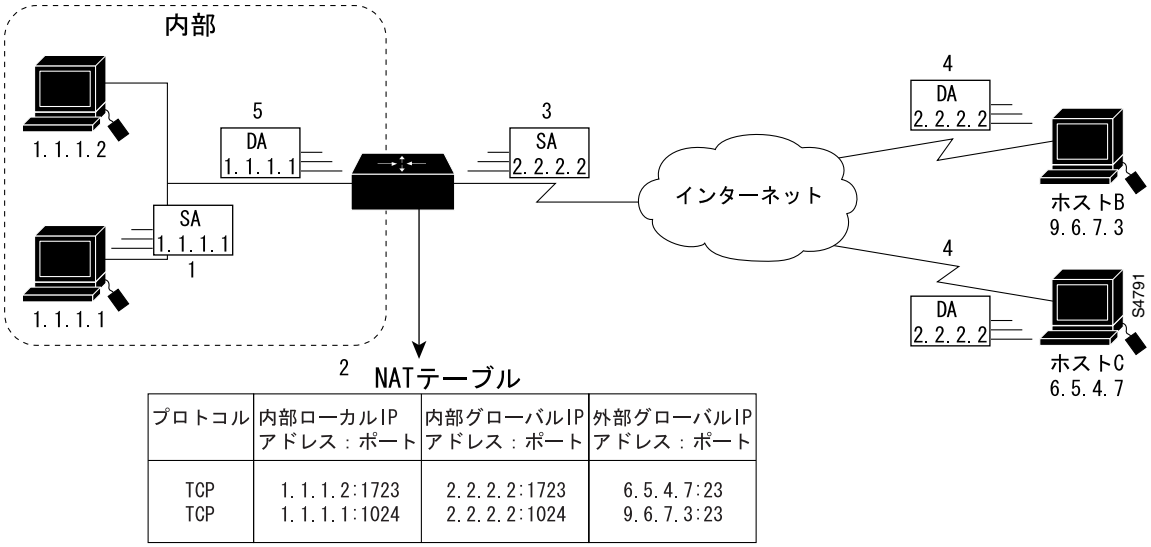
次の例では、3 つの異なる内部スタブ ネットワークのアドレスが、異なる外部アドレス プールを使用して変換されています。アクセス リスト 1、2、3 は、それぞれプール 1、プール 3、プール 5 に対応しています。

```
interface FastEthernet1/0
     ip address 10.0.0.1 255.0.0.0
     ip nat inside
!
interface FastEthernet3/0
     ip address 30.0.0.1 255.0.0.0
     ip nat inside
!
interface FastEthernet5/0
     ip address 50.0.0.1 255.0.0.0
     ip nat inside
!
ip nat pool pool1 20.1.0.1 20.1.255.254 netmask 255.0.0.0
ip nat pool pool2 40.1.0.1 40.1.255.254 netmask 255.0.0.0
ip nat pool pool3 60.1.0.1 60.1.255.254 netmask 255.0.0.0
ip nat inside source list 1 pool pool1
ip nat inside source list 2 pool pool2
ip nat inside source list 3 pool pool3
!
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 permit 30.0.0.0 0.255.255.255
access-list 3 permit 50.0.0.0 0.255.255.255
```

内部グローバル アドレスのオーバーロード（Port Address Translation［PAT; ポート アドレス変換］）

内部グローバル アドレスのオーバーロードを利用すると、ルータは多くのローカル アドレスに 1 つのグローバル アドレスを使用できるようになり、内部グローバル アドレスを保護することができます。オーバーロードが設定されている場合、グローバル アドレスは、UDP/TCP ポートなどの情報を使用して、元どおりの正しいローカル アドレスに変換されます。

次の例では、net-208 というアドレス プールが作成されています。このプールには、171.69.233.208 ～ 171.69.233.233 のアドレスが含まれています。アクセス リスト 1 は、192.168.1.0 ～ 192.168.1.255 の送信元アドレスを持つパケットを許可します。変換が存在していない場合、アクセス リスト 1 に一致するパケットはこのプールのアドレスに変換されます。このルータは、複数のローカル アドレス（192.168.1.0 ～ 192.168.1.255）に同じグローバル アドレスを使うことを許可します。また、このルータは接続を区別するためにポート番号を保持しています。



プロトコル	内部ローカルIP アドレス：ポート	内部グローバルIP アドレス：ポート	外部グローバルIP アドレス：ポート
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask 255.255.255.240
ip nat inside source list 1 pool net-208 overload
!
interface serial0
     ip address 171.69.232.182 255.255.255.240
     ip nat outside
!
interface ethernet0
     ip address 192.168.1.94 255.255.255.0
     ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

外部アドレスから内部アドレスへの変換

外部から内部へのスタティックな変換

ip nat outside source static *global-ip local-ip*

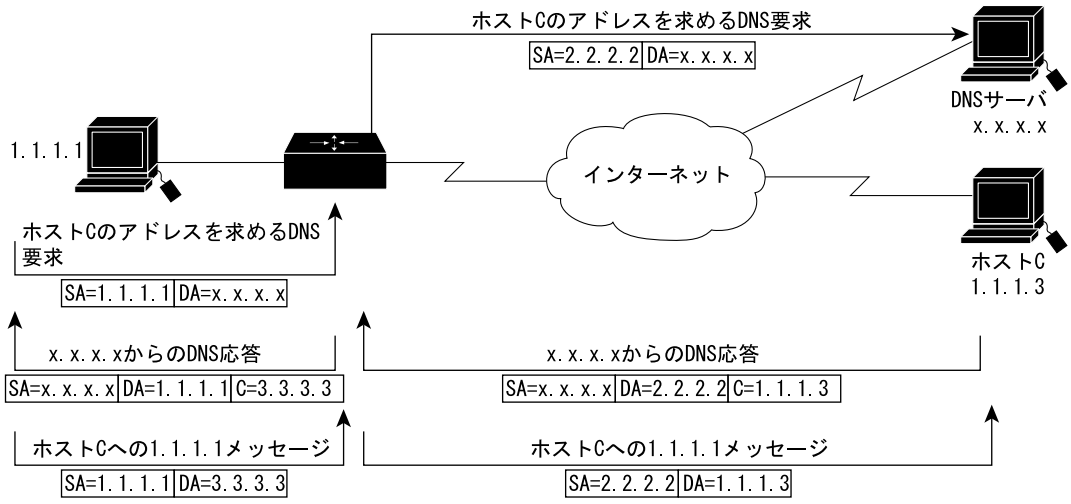
外部から内部へのダイナミックな変換

ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}

access-list *access-list-number* **permit** *source* [*source-wildcard*]

ip nat outside source list *access-list-number* **pool** *name*

次の例では、インターネット上の誰かがローカル ネットワーク内のアドレスを合法的に使用しようとしています。この外部ネットワークにアクセスするには、特別な変換が必要です。プール net-10 は、外部ローカル IP アドレスのプールです。ステートメント `ip nat outside source list 1 pool net-10` によって、外部オーバーラッピング ネットワーク内のホストのアドレスはこのプールのアドレスに変換されます。



NATテーブル

内部ローカル IPアドレス	内部グローバル IPアドレス	外部グローバル IPアドレス	外部ローカル IPアドレス
1.1.1.1	2.2.2.2	1.1.1.3	3.3.3.3

S4792

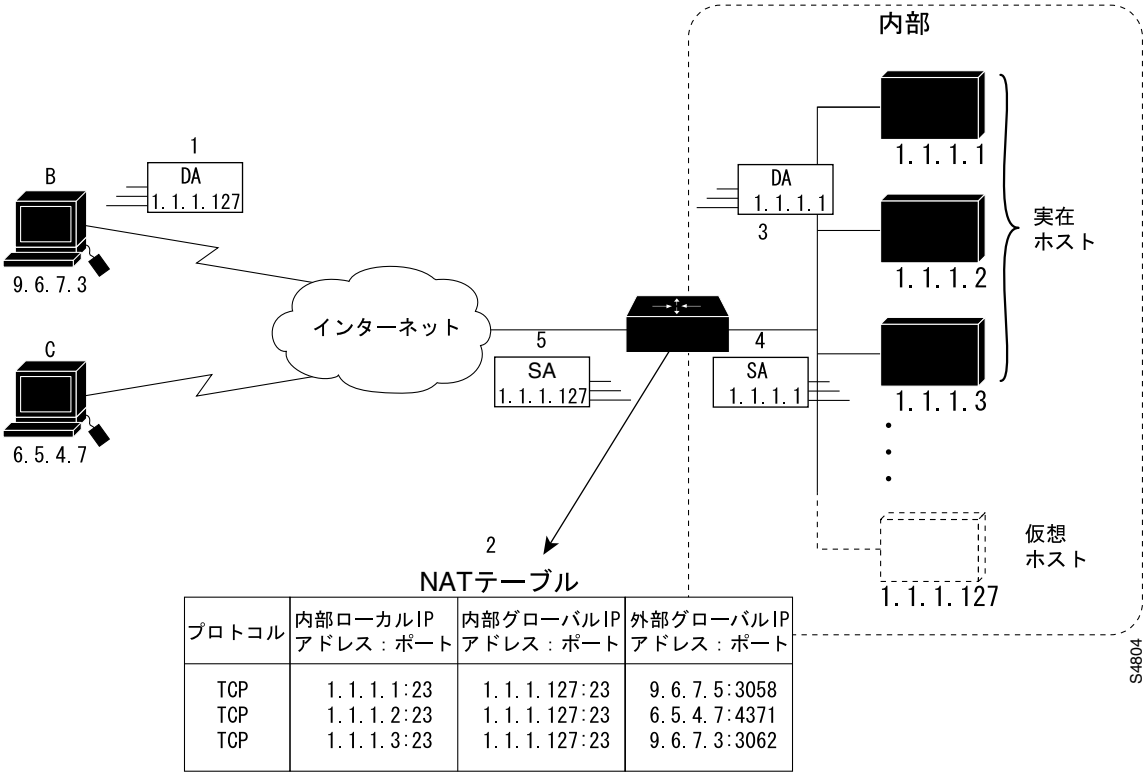
```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface serial 0
     ip address 171.69.232.192 255.255.255.240
     ip nat outside
!
interface ethernet0
     ip address 192.168.1.94 255.255.255.0
     ip nat inside
access-list 1 permit 192.168.1.0 0.0.0.255
```

また、ACL ごとに異なる内部アドレス プールが選択されるようにすることも可能です。これは、異なる内部アドレス用の複数のプールから外部アドレスに変換する例（前述）と同じです。

```
interface FastEthernet2/0
     ip address 20.0.0.1 255.0.0.0
     ip nat outside
!
interface FastEthernet4/0
     ip address 40.0.0.1 255.0.0.0
     ip nat outside
!
interface FastEthernet6/0
     ip address 60.0.0.1 255.0.0.0
     ip nat outside
!
ip nat pool pool1inside 10.1.0.1 10.255.255.254 netmask 255.0.0.0
ip nat pool pool2inside 30.1.0.1 30.255.255.254 netmask 255.0.0.0
ip nat pool pool3inside 50.1.0.1 50.255.255.254 netmask 255.0.0.0
ip nat outside source list 4 pool pool1inside
ip nat outside source list 5 pool pool2inside
ip nat outside source list 6 pool pool3inside
```

TCP の負荷分散

次の例は、仮想アドレスを定義し、その仮想アドレスへの接続を複数の実在ホストの間に分散することを目的としています。プールによって実在ホストのアドレスが定義され、アクセス リストによって仮想アドレスが定義されます。変換がまだ存在していなければ、シリアル 0（外部インターフェイス）からの TCP パケットのうち、宛先がアクセス リストに一致するパケットはプール内のアドレスに変換されます。



プロトコル	内部ローカルIP アドレス：ポート	内部グローバルIP アドレス：ポート	外部グローバルIP アドレス：ポート
TCP	1.1.1.1:23	1.1.1.127:23	9.6.7.5:3058
TCP	1.1.1.2:23	1.1.1.127:23	6.5.4.7:4371
TCP	1.1.1.3:23	1.1.1.127:23	9.6.7.3:3062

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
     ip address 192.168.15.129 255.255.255.240
     ip nat outside
!
interface ethernet 0
     ip address 192.168.15.17 255.255.255.240
     ip nat inside
!
access-list 2 permit 192.168.15.1
```

外部から内部ポートへのスタティックな変換の設定

アドレスをインターフェイス アドレスに変換する場合、内部ネットワーク上のサービスに対して外部から開始された接続（電子メールなど）が正しい内部ホストに到達できるようにするには、コンフィギュレーションを追加する必要があります。次のコマンドを使用することによって、特定のサービスを特定の内部ホストに対応付けることができます。

ip nat inside source static { **tcp** | **udp** } *localaddr localport globaladdr globalport*

この例では、SMTP ポート（25）に外部から接続が開始された場合、内部ホスト 192.168.10.1 に接続されます。

```
ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25
```

NAT の確認

show c7300 nat pxf statistics

show ip nat translations

show ip nat statistics

QoS の例

CBWFQ

```
policy-map child-policy-map-name
 class class-map-name
 bandwidth [kbps | percent percentage]
 bandwidth remaining percent percentage
```

ネスト化ポリシー マップの例

次に示すのは、ネスト化ポリシー マップの設定例です。ネスト化ポリシー マップを使用すると、フレーム リレーVC や VLAN などのサブインターフェイスに QoS 機能を提供できます（Cisco 7304 の PXF の場合、他の QoS 機能もサポートされていますが、この QoS 機能はトラフィック シェーピングです）。

```
policy-map child-policy-map-name
 class class-map-name
 priority [kpbs | percent percentage]
 class class-map-name
 bandwidth [kbps | percent percentage]

policy-map parent-policy-map-name
 class class-default
 shape average cir
 service-policy child-policy-map-name

interface interface-type interface-number
 service-policy parent-policy-name
```

ACL のマッチング

```
class-map [match-all | match-any] class-map-name
 match access-group [access-list-number | name named-access-list]
```

FTP パケットをトラフィック クラスと照合するための ACL マッチング

```
class-map match-all ftp-class
 match access-group 109

access-list 109 permit tcp any any eq ftp
```

IP DSCP のマッチング

```
class-map [match-all | match-any] class-map-name
 match ip dscp ip-dscp-value ip-dscp values ...（最大 8 つの ip-dscp 値）
```

IP precedence のマッチング

```
class-map [match-all | match-any] class-map-name
 match ip precedence ip-prec-value ip-prec-value...（最大 8 つの ip-prec 値）
```

IP RTP のマッチング

```
class-map [match-all | match-any] class-map-name
 match ip rtp ip-rtp-value ip-rtp-value...（最大 8 つの ip-rtp 値）
```

MPLS EXP ビットのマッチング

```
class-map match-all mpls
 match mpls experimental 7
```

QoS グループのマッチング

```
class mpls
 match qos-group 6
```

ATM CLP のマーキング

```
policy-map policy-map-name
 class class-map-name
 set atm-clp atm-clp-value
```

フレーム リレー DE ビットのマーキング

次の例では、**set** コマンドおよび **police** コマンドを使用してフレーム リレー DE ビットがマーキングされています。

```
policy-map mpls
 class mpls
 set fr-de

policy-map mpls
 class mpls
 police 200000 300000 200000 conform-action set-frde-transmit 7 exceed-action
set-frde-transmit 3 violate-action set-frde-transmit 4
```

IP precedence のマーキング

```
policy-map policy-map-name
 class class-map-name
 set ip precedence precedence-value
```

IP DSCP のマーキング

```
policy-map policy-map-name
 class class-map-name
 set ip dscp dscp-value
```

MPLS EXP ビットのマーキング

```
policy-map policy-map-name
 class class-map-name
 set mpls experimental mpls-exp-value

police 200000 300000 200000 conform-action set-mpls-exp-transmit 1exceed-action
set-mpls-exp-transmit 2 violate-action set-mpls-exp-transmit 3
```

QoS グループのマーキング

次の例では、**set** コマンドおよび **police** コマンドを使用して、QoS グループがマーキングされています。

```
policy-map mpls
 class mpls
 set qos-group 7

policy-map mpls
 class mpls
 police 200000 300000 200000 conform-action set-qos-transmit 7 exceed-action
set-qos-transmit 3 violate-action set-qos-transmit 4
```

低遅延キューイング（プライオリティ キューイング）

Cisco IOS Release 12.2(14)SZ より前の低遅延キューイング — プライオリティ キューがすべての帯域幅を取得し、他のキューは残った帯域幅を取得

```
policy-map policy-map-name
 class class-map-name
 priority kpbs
```

Cisco IOS Release 12.2(14)SZ 以上の低遅延キューイング — プライオリティ キューがすべての帯域幅を取得し、他のキューは残った帯域幅を取得

```
policy-map policy-map-name
 class class-map-name
 priority
```

Cisco IOS Release 12.2(14)SZ 以上の低遅延キューイング — プライオリティ キューは police のレートに設定され、他のキューは残りの帯域幅を取得

```
policy-map policy-map-name
 class class-map-name
 priority
 police bps burst-normal burst-max conform-action action exceed-action action
[violate-action action]
```

サブインターフェイス トラフィックのポートレベル キューイングおよび QoS

Cisco IOS Release 12.2(20)S では、ポートレベルのキューイング機能が導入され、フレーム リレー DLCI および 802.1q サブインターフェイスにもポートレベルの QoS ポリシーを適用できるようになりました。フレーム リレー DLCI または 802.1q サブインターフェイスに直接 QoS ポリシーを適用する場合、フレーム リレー DLCI または 802.1q サブインターフェイスに直接適用される QoS ポリ

シーのコンフィギュレーションが使用されます。Release 12.2(20)S より前では、フレーム リレー DLCI と 802.1q サブインターフェイスの QoS ポリシーは、DLCI またはサブインターフェイスに直接設定しなければなりませんでした。

Virtual Private Network（VPN; 仮想私設網）の QoS

```
interface interface-name
 qos pre-classify
```

キュー制限の設定

```
policy-map policy-map-name
 class class-map-name
 queue-limit number-of-packet
```

トラフィック ポリシング

```
policy-map policy-map-name
 class class-map-name
 police bps burst-normal burst-max conform-action action exceed-action action
[violate-action action]
```

トラフィック ポリシング（階層型入力ポリシング）

```
class c1
 police x1 y1 conform action1 exceed action2
class c2
 police x2 y2 conform action3 exceed action4

policy-map parent
 class class-default
 police x3 y3 conform action5 exceed action6
 service-policy child
```

トラフィック シェーピング

```
policy-map policy-map-name
 class class-map-name
 shape average cir
```

WRED — IP precedence の例

```
policy-map wred
 class class-default
 random-detect exponential-weight-constant weight
 random-detect precedence [IP-precedence minimum-threshold maximum-threshold
max-probability-denominator]
 bandwidth [kbps | percent percentage]
```

WRED — IP DSCP の例

```
policy-map wred
 class class-default
 random-detect dscp-based
 random-detect dscp dscp-codepoint-value
```

モジュラ QoS コマンドライン インターフェイスの例

次の例では、インターフェイス POS4/0 から送出されるすべての FTP トラフィックは、IP precedence ビットが 1 にマークされて転送されます。一方、すべての WWW トラフィックは、IP precedence ビットが 2 にマークされて転送されます。この例では、FTP トラフィックと、IP precedence ビットが 5 にマークされているトラフィックはプライオリティ キューを使用して転送されますが、HTTP トラフィックはデフォルト キューを使用して転送されます。

IP precedence ビットが 5 にマークされているトラフィックは、アクセス リストを使用して分類されます。

```
access-list 109 permit tcp any any eq ftp
access-list 110 permit tcp any any eq www
access-list 111 permit ip any any eq precedence 5

class-map match-all ftp-class
 match access-group 109

class-map match-all www-class
 match access-group 110

class-map match-all prec5-class
 match access-group 111

policy-map intpos40
 class ftp-class
 set ip precedence 1
 class www-class
 set ip precedence 2
 class prec5-class
 priority 1

interface pos4/0
 service-policy output intpos40
```

フレーム リレーのモジュラ QoS CLI の例

フレーム リレー VC の QoS コンフィギュレーションについては、「ネスト化ポリシー マップの例」（p.30）を参照してください。

次の例では、サブインターフェイス POS4/0.1 から送出される FTP トラフィックはすべて、IP precedence ビットが 7 にマークされて転送されます。

```
access-list 109 permit tcp any any eq ftp

class-map match-all ftp-class
 match access-group 109

policy-map ftp-low-priority
 class ftp-class
 set ip precedence 7

interface pos4/0.1 point-to-point
 ip address 10.1.1.1 255.0.0.0
 frame-relay interface-dlci 100
 service-policy output ftp-low-priority
```

RPF

パケットの受信インターフェイスを通じて、またはデフォルト ルートから、送信元 IP に到達可能なパケットを受け入れ、その他は廃棄します。

```
ip verify unicast reverse-path
または
ip verify unicast source reachable-via rx allow-default
```

ACL を使用し、着信したインターフェイスを通じて送信元 IP に到達可能なパケットをフィルタリングします。

```
ip verify unicast reverse-path 109
または
ip verify unicast source reachable-via rx 109
```

Forwarding Information Base（FIB; 転送情報ベース）に送信元 IP アドレスがあるパケットを受け入れ、その他は廃棄します。

```
ip verify unicast source reachable-via any
```

ACL を使用して、FIB に送信元 IP アドレスがないパケットをフィルタリングします。

```
ip verify unicast source reachable-via any 109
```

インターフェイスのプライマリまたはセカンダリのアドレスの 1 つと送信元および宛先の IP が一致するパケットを受け入れます。これは、self-ping 機能が要求される場合に必要となります。allow-self-ping が設定されていないと、self-ping パケットは廃棄されます。

```
ip verify unicast reverse-path allow-self-ping 109
または
ip verify unicast source reachable-via rx allow-self-ping 109
または
ip verify unicast source reachable-via any allow-self-ping 109
```

パスワードの回復

パスワードを忘れた場合は、次の手順に従って新しいパスワードを定義してください。

ステップ 1 端末、または端末エミュレーション機能を備えた PC をルータのコンソール ポートに接続します。次の端末設定を使用します。

9600 ボーレート
パリティなし
8 データ ビット
2 ストップ ビット
フロー制御なし

コンソール ケーブルの仕様については、『*Console and Auxiliary Port Signals and Pinouts*』を参照してください。

ステップ 2 ルータの EXEC プロンプトを表示できる場合は、**show version** を入力して、コンフィギュレーション レジスタの設定を記録してください。通常、この設定値は 0x2102 または 0x102 です。

ステップ 3 （ログインまたは TACACS パスワードをなくしたために）ルータの EXEC プロンプトが表示されない場合は、コンフィギュレーション レジスタが 0x2102 に設定されているとみなすことができます。

ステップ 4 電源スイッチを使用して、ルータの電源をオフにし、再びオンにします。

ステップ 5 電源投入から 60 秒以内に **Break** キーを押して、ルータを ROMmon 状態にします。ブレーク シーケンスが動作しない場合は、『*Standard Break Key Sequence Combinations During Password Recovery*』を参照して、その他のキーの組み合わせを試してください。

ステップ 6 rommon 1> プロンプトに **confreg** を入力します。これで、コンフィギュレーションをロードせずに disk0: から起動するように、ソフトウェア コンフィギュレーション レジスタが変更されます。コンフィギュレーションを変更するかどうかの確認を求められたら、**y** を入力して、ダイアログに応答します（次の出力例を参照）。

```
rommon 1> confreg

    Configuration Summary
enabled are:
load rom after netboot fails
console baud:9600
boot:image specified by the boot system commands
      or default to:cisco2-c7300

do you wish to change the configuration? y/n  [n]: y
enable  "diagnostic mode"? y/n  [n]:
enable  "use net in IP bcast address"? y/n  [n]:
disable "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]: y
change console baud rate? y/n  [n]:
change the boot characteristics? y/n  [n]:


    Configuration Summary
enabled are:
load rom after netboot fails
ignore system config info
console baud:9600
boot:image specified by the boot system commands
      or default to:cisco2-c7300

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
>
```

ステップ 7 rommon 2> プロンプトに **reset** を入力します。ルータが再起動しますが、保存されているコンフィギュレーションは無視されます。

ステップ 8 初期コンフィギュレーション ダイアログを開始するかどうかの確認を求められたら、**no** を入力します。または、**Ctrl-C** を押して、初期セットアップ手順を省略します。

ステップ 9 Router> プロンプトに、**enable** を入力します。イネーブル モードに入り、Router# プロンプトが表示されます。

ステップ 10 **config mem** または **copy start running** を入力して、Nonvolatile Random-Access Memory（NVRAM; 不揮発性 RAM）に保存されているスタートアップ コンフィギュレーションをメモリにコピーします。

ステップ 11 **wr term** または **show running** を入力します。

show running および **wr term** コマンドを入力すると、ルータのコンフィギュレーションが表示されます。このコンフィギュレーションの場合は、すべてのインターフェイスの下に **shutdown** コマンドが表示されます。これは、すべてのインターフェイスが現在シャットダウン中であることを意味します。また、パスワードを暗号化フォーマット、または暗号化されていないフォーマットで表示することもできます。

ステップ 12 **config term** を入力して、変更します。プロンプトは hostname(config)# になります。

ステップ 13 **enable secret** <*password*> を入力します。

ステップ 14 使用するインターフェイスごとに、**no shutdown** コマンドを入力します。**show ip interface brief** コマンドを入力した場合、使用する各インターフェイスの Status および Protocol は up と表示されなければなりません。

ステップ 15 **config-register 0x2102**、またはステップ 2 で記録した値を入力します。

ステップ 16 **End** または **Ctrl-Z** を入力して、コンフィギュレーション　モードを終了します。プロンプトは hostname# になります。

ステップ 17 **reload** を入力してルータを再起動し、新しいパスワード作成前のステートに戻します。

ステップ 18 **write mem** または **copy running startup** を入力して、変更を行います。

ステップ 19 新しいパスワードを使用して、ルータにログインします。

パスワード回復手順の例

新しいパスワードを定義して、Cisco 2600 ルータのパスワードを回復する例を示します。この例は、Cisco 7304 ルータでの回復手順とほとんど同じです。

```
Router> enable
Password:
Password:
Password:
% Bad secrets

Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 3 minutes
System returned to ROM by abort at PC 0x802D0B60
System image file is "flash:c2600-is-mz.120-7.T"

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor board ID JAB031202NK (3878188963)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
--More-- 8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)

Configuration register is 0x2102
```

```
Router>
!--- The router was just power cycled and during bootup a
!--- break sequence was sent to the router.
!

*** System received an abort due to Break Key ***

signal= 0x3, code= 0x500, context= 0x813ac158
PC = 0x802d0b60, Vector = 0x500, SP = 0x80006030
rommon 1> confreg

    Configuration Summary
enabled are:
load rom after netboot fails
console baud:9600
boot:image specified by the boot system commands
      or default to:cisco2-C2600

do you wish to change the configuration? y/n  [n]: y
enable  "diagnostic mode"? y/n  [n]:
enable  "use net in IP bcast address"? y/n  [n]:
disable "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]: y
change console baud rate? y/n  [n]:
change the boot characteristics? y/n  [n]:


    Configuration Summary
enabled are:
load rom after netboot fails
ignore system config info
console baud:9600
boot:image specified by the boot system commands
      or default to:cisco2-C2600

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
rommon 2 > reset


System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 32768 Kbytes of main memory


program load complete, entry point: 0x80008000, size: 0x6fdb4c

Self decompressing the image : ################################
################################################################
################################################################
################################################################
################################ [OK]


 Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
 cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor board ID JAB031202NK (3878188963)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)


 --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

00:00:19: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up
00:00:19: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:00:19: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
00:00:19: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down
00:00:19: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0, changed state to
down
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state
to up
Router>
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state
  to up
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
  to down
00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state
  to down
00:00:50: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
00:00:50: %LINK-5-CHANGED: Interface BRI0/0, changed state to administratively down
00:00:52: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively
  down
00:00:52: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively
  down
00:00:52: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively
  down
00:00:52: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down
00:00:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state
  to down
00:00:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state
  to down
Router>
Router> enable
Router# copy start run
Destination filename [running-config]?
1324 bytes copied in 2.35 secs (662 bytes/sec)
Router#
```

```
00:01:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
  down
00:01:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:2, changed state to
  down
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# enable secret cisco
Router(config)# ^z
00:01:54: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip interface brief

Interface      IP-Address        OK?     Method     Status                    Protocol
Ethernet0/0    10.200.40.37      YES     TFTP       administratively down     down
Serial0/0      unassigned        YES     TFTP       administratively down     down
BRI0/0         193.251.121.157   YES     unset      administratively down     down
BRI0/0:1       unassigned        YES     unset      administratively down     down
BRI0/0:2       unassigned        YES     unset      administratively down     down
Ethernet0/1    unassigned        YES     TFTP       administratively down     down
Serial0/1      unassigned        YES     TFTP       administratively down     down
Loopback0      193.251.121.157   YES     TFTP       up                        up
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# int Ethernet0/0
Router(config-if)# no shut
Router(config-if)#
00:02:14: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:02:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state
  to up
Router(config-if)# int BRI0/0
Router(config-if)# no shut
Router(config-if)#
00:02:26: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to down
00:02:26: %LINK-3-UPDOWN: Interface BRI0/0:2, changed state to down
00:02:26: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up
00:02:115964116991: %ISDN-6-LAYER2UP: Layer 2 for Interface BR0/0, TEI 68 changed
  to up
Router(config-if)# ^z
Router#
00:02:35: %SYS-5-CONFIG_I: Configured from console by console
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 3 minutes
System returned to ROM by abort at PC 0x802D0B60
System image file is "flash:c2600-is-mz.120-7.T"

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor board ID JAB031202NK (3878188963)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
--More-- 8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)
```

```
Configuration register is 0x2142

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-reg 0x2102
Router(config)#^z
00:03:20: %SYS-5-CONFIG_I: Configured from console by console

Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

Router uptime is 3 minutes
System returned to ROM by abort at PC 0x802D0B60
System image file is "flash:c2600-is-mz.120-7.T"

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
Processor board ID JAB031202NK (3878188963)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
--More-- 8192K bytes of processor board System flash partition 1 (Read/Write)
8192K bytes of processor board System flash partition 2 (Read/Write)

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#
```

TFTP または RCP サーバ アプリケーションによるソフトウェア イメージのインストール

ここでは、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバまたは Remote Copy Protocol（RCP）サーバ アプリケーションを使用して、「RAM から起動する」シスコのルータに Cisco IOS ソフトウェアをインストールする方法について説明します。

最初に実行可能コードを RAM 内で圧縮解除し、コードを実行して、IOS ソフトウェア イメージを実行するルータは、「RAM から起動する」ルータといいます。Cisco 7304 ルータなどが該当します。

（注） このマニュアルに記載されたトラブルシューティング　ツールを使用するには、登録ユーザとしてログインする必要があります。

手順の概要

（注） この手順で参照している資料のなかには、Cisco 7304 ルータ固有のコマンドおよび出力が記載されていないものもあります。slot0: または bootflash: という記述がある場合は、それぞれ Cisco 7304 ルータの disk0: および bootdisk: に置き換えてください。

- TFTP サーバをインストールします。

  TCP/IP 対応ワークステーションまたは PC に、TFTP サーバまたは RCP サーバ アプリケーションをインストールする必要があります。これらのアプリケーションをインストールしたあとで、最小限の設定を行う必要があります。

  - TFTP アプリケーションは、TFTP *クライアント*でなく TFTP *サーバ*として動作するように設定する必要があります。
  - 発信ファイル　ディレクトリを指定する必要があります。発信ファイル　ディレクトリは、Cisco IOS ソフトウェア イメージが格納されるディレクトリです。ほとんどの TFTP アプリケーションには、これらの設定作業を支援するセットアップ ルーチンが組み込まれています。

（注） ソフトウェア フィーチャ パック CD-ROM に収録されている TFTP サーバは、Windows 95 が稼働する PC 上で使用できます。その他のオペレーティング システムについては、多数の TFTP または RCP アプリケーションが独立ソフトウェア ベンダーから提供されています。また、WWW のパブリック ソースからシェアウェアとして入手することもできます。ソフトウェア フィーチャ パック CD に収録されている TFTP サーバ アプリケーションは、Cisco.com から入手することもできます。

  - Windows 95/98/NT 用の TFTP サーバをダウンロードします。

- Cisco IOS ソフトウェア イメージを、ご使用のワークステーションまたは PC にダウンロードします。

  ご使用のルータに対して有効な Cisco IOS ソフトウェア イメージをロードする必要もあります。ご使用のハードウェアおよびソフトウェア機能がイメージでサポートされていること、およびルータにイメージを実行するためのメモリが十分にあることを確認してください。Cisco IOS ソフトウェア イメージをまだロードしていない場合、またはロードしたイメージが要件をすべて満たしているかどうか不明である場合は『*How to Choose a Cisco IOS Software Release*』を参照してください。

ソフトウェアのインストールおよびアップグレード手順

TFTP サーバまたは RCP サーバ アプリケーションを使用して、Cisco IOS ソフトウェアをインストールする手順は、次のとおりです。

（注） RCP アプリケーションの場合は、TFTP という記述をすべて RCP に置き換えてください。たとえば、**copy tftp disk0:** コマンドではなく、**copy rcp disk0:** コマンドを使用します。また、RCP アプリケーションでは、TFTP よりも設定作業が多くなります。

ステップ 1 ルータにコンソール セッションを確立します。

ルータにコンソール セッションを確立するには、コンソールへの直接接続、または仮想 Telnet 接続を行います。ただし、Telnet 接続はソフトウェア インストレーションの再起動フェーズ中に終了するため、Telnet 接続よりもコンソールへの直接接続を推奨します。コンソール接続の場合は、ロール状ケーブル（通常は黒いフラット ケーブル）を使用して、ルータのコンソール ポートと PC の COM ポートを接続します。PC 上で Hyperterminal アクセサリ アプリケーションを起動して、次のように設定します。

9600 ビット / 秒の速度
8 データ ビット
0 パリティ ビット
2 ストップ ビット
フロー制御なし

ステップ 2 TFTP サーバにルータとの IP 接続機能があることを確認します。

TFTP サーバにルータとの IP 接続機能があるかどうかを調べるには、ルータの IP アドレスおよび（必要に応じて）デフォルト ゲートウェイが設定されているかどうかを確認します。ルータに ping を送信して、ルータと TFTP サーバがネットワークで接続されていることを確認します。IP アドレスの詳細については、「TFTP または RCP サーバを使用してイメージをインストールする場合の一般的な問題」（p.47）を参照してください。

ステップ 3 TFTP サーバからルータに新しいソフトウェア イメージをコピーします。

```
Router> enable
Password: password
Router#
Router# copy tftp disk0:
```

コンソール ポートを介してルータに接続したあとに、> または rommon> プロンプトが表示された場合、ルータは ROM モニタ（ROMmon）モードになっています。ROMmon の回復手順については、「ROMmon prompt: rommon#>」を参照してください。

必要に応じて、装置間でイメージをコピーできます。

（注） ルータ ソフトウェアをアップグレードする前に、ルータ コンフィギュレーションのコピーを保存してください。アップグレードしても、NVRAM に格納されたコンフィギュレーションには影響がありません。

ステップ 4 TFTP サーバの IP アドレスを指定します。

```
Address or name of remote host [255.255.255.255]? 172.17.247.195
```

ステップ 5 インストールする Cisco IOS ソフトウェア イメージのファイル名を指定します。TFTP サーバのイメージのファイル名によって、インストールされるイメージ名が異なります。

```
Source file name? c7300-js-mz.121-9.EX
```

ステップ 6 宛先ファイル名を指定します。ルータにロードされた新しいソフトウェア イメージには、このファイル名が付けられます。イメージには任意の名前を付けることができますが、通常は UNIX イメージのファイル名を付けます。

```
Destination file name? c7300-js-mz.121-9.EX
```

コピー処理には数分間かかります。所要時間はネットワークによって異なります。コピー処理中に、アクセスされたファイルを示すメッセージが表示されます。

感嘆符（!）は、コピー処理が実行中であることを示します。それぞれの感嘆符は、10 個のパケットが正常に転送されたことを示します。イメージのチェックサム検証は、イメージが disk0: に書き込まれたあとに実行されます。

ソフトウェアの転送問題のトラブルシューティングについては、「TFTP または RCP サーバを使用してイメージをインストールする場合の一般的な問題」（p.47）を参照してください。

ステップ 7 リロードする前に、インストレーションおよびコマンドが正しいことを確認してください。

イメージが適切にインストールされていること、および **boot system** コマンドに指定されたロード対象ファイルが適切であることを確認します。イメージおよび boot コマンドの確認方法については、「TFTP または RCP サーバを使用してイメージをインストールする場合の一般的な問題」（p.47）を参照してください。

```
Router# reload
*Mar 1 00:30:49.972: %SYS-5-CONFIG_I: Configured from console by console
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm] yes
```

ステップ 8 ルータが適切なイメージを使用して動作していることを確認します。リロードの完了後は、ルータ上で目的の Cisco IOS ソフトウェア イメージが稼働していなければなりません。**show version** コマンドを使用して確認できます。

イメージの検証に関する問題については、「TFTP または RCP サーバを使用してイメージをインストールする場合の一般的な問題」（p.47）を参照してください。

Cisco 7304 ルータの出力例

```
Router# dir disk0:

Directory of disk0:/

1  -rw-     4970544   Jul 02 2001 08:25:54 c7300-js-mz.121-9.EX
16273408 bytes total (13488128 bytes free)

Router# copy tftp disk0:
Address or name of remote host []? 172.17.247.195
Source filename []?c7300-js-mz.121-9.EX
Destination filename [c7300-js-mz.121-9.EX]?
Accessing tftp://172.17.247.195/ c7300-js-mz.121-9.EX...
Loading c7300-js-mz.121-9.EX from 172.17.247.195 (via Ethernet0/0):
!!!!!!!!!!!!!!!!!!!!!!
(...)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying checksum...  OK (0x6BA0)
4970544 bytes copied in 125.731 secs (67263 bytes/sec)

Router# reload
Proceed with reload? [confirm]
6d23h: %SYS-5-RELOAD: Reload requested
...
```

TFTPまたはRCPサーバを使用してイメージをインストールする場合の一般的な問題

（注） この手順で参照している資料のなかには、Cisco 7304 ルータ固有のコマンドおよび出力が記載されていないものもあります。slot0: または bootflash: という記述がある場合は、それぞれ Cisco 7304 ルータの disk0: および bootdisk: に置き換えてください。

（注） RCP アプリケーションの場合は、TFTP という記述をすべて RCP に置き換えてください。たとえば、**copy tftp disk0:** コマンドではなく、**copy rcp disk0:** コマンドを使用します。

ブート モード中の保存

保存コマンド（**write mem** または **copy running-config startup-config**）は使用しないでください。現在のコンフィギュレーションの保存を求めるプロンプトが表示されたら、**no** と応答します。ブートモード中に保存すると、コンフィギュレーションの一部または全体が消去されることがあります。

```
router(boot)# reload
*Mar  1 00:30:49.972: %SYS-5-CONFIG_I: Configured from console by console

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

*Mar  1 00:30:58.932: %SYS-5-RELOAD: Reload requested
```

デフォルト ゲートウェイ

デフォルト ゲートウェイは、次の条件が両方満たされる場合だけ設定できます。

- ルータ上で、ルーティングをサポートしていないブート イメージが稼働している。
- IP ルーティングがディセーブルである。

コンフィギュレーションへのデフォルト ゲートウェイの追加

デフォルト ゲートウェイの IP アドレスを判別したのち、コンフィギュレーション モードで、次のコマンドを入力します。

ip default-gateway *ip address*

TFTP サーバおよびルータが同じネットワーク内にあることの確認

TFTP サーバとルータのイーサネット インターフェイスについて、IP アドレスおよびマスクを比較する必要があります（次の 2 つの例を参照）。

- TFTP サーバの IP アドレスは 172.17.247.195 で、マスクは 255.255.0.0 です。ルータのインターフェイス イーサネット 0 の IP アドレスは 172.17.3.192 で、マスクは 255.255.0.0 です。この例では、TFTP サーバとルータのイーサネット インターフェイスは同じネットワーク内にあるため、デフォルト ゲートウェイは不要です。

- TFTP サーバの IP アドレスは 172.17.247.195 で、マスクは 255.255.0.0 です。ルータのインターフェイス イーサネット 0 の IP アドレスは 172.10.3.192 で、マスクは 255.255.0.0 です。この例では、TFTP サーバとルータのイーサネット インターフェイスは異なる IP ネットワーク上にあるため、ルータにデフォルト ゲートウェイを設定する必要があります。

デフォルト ゲートウェイが設定されているかどうかの判別

デフォルト ゲートウェイは常にネクストホップになります。すべてのパケットは、TFTP サーバまたは Telnet セッション送信元のいずれか、または両方が組み込まれているワークステーションに到達するために、このホップを通過しなければなりません。ルータにデフォルト ゲートウェイが設定されている場合、**show running-config | include default-gateway** コマンドを実行すると、デフォルト ゲートウェイの IP アドレスが表示されます。

```
Router# show running-config | include default-gateway
ip default gateway 172.19.251.37
```

IP アドレス

ルータの IP アドレスおよびマスクの判別

使用するコンフィギュレーション ファイル内で、インターフェイス イーサネット ステートメントの下にある **IP address** コマンドを調べます（次の例を参照）。

```
Router> en
Password:
Router# show run
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime

.....................

interface fastEthernet 0/0
  ip address 172.17.3.192 255.255.0.0
```

Windows 95 の TFTP サーバの IP アドレスの判別

ツールバーで、**Start** を選択し、**Run** を選択します。**winipcfg** を入力して、**OK** をクリックすると、IP コンフィギュレーション ダイアログ ボックスが表示されます。

UNIX ワークステーションの TFTP サーバの IP アドレスの判別

netstat -in コマンドを入力します。ワークステーションのインターフェイスの IP アドレスが表示されます。ルータ ネットワークに接続されているインターフェイスを選択します。

ソフトウェア転送中のエラーのトラブルシューティング

コピー処理中の［Text checksum verification failure］

コピー処理中に感嘆符（!）の代わりに多数のピリオド（.）が表示される場合は、次の例のようなメッセージが表示されることがあります。

```
COPY: Text checksum verification failure
TFTP from 172.17.247.195 failed/aborted
Verifying checksum... invalid (expected 0x62B7,
computed 0x60B9)
```

dir disk0: コマンドを入力すると、次の例のようなメッセージが表示されることがあります。

```
router# dir disk0:
Directory of disk0:/
1 -rw- 3437967 c7300-js-mz.121-9.EX
2 -rw- 3489036 c7300-js-mz.121-9.EX
3 -rw- 290304 c7300-js-mz.121-9.EX [invalid checksum]
```

どちらの場合も、ファイルがメモリに適切にコピーされていないため、チェックサムに失敗しています。再コピーする必要があります。最初に、TFTP サーバにコピーしたファイルと元のファイルのサイズが同じであることを確認します（ルータ内のファイル サイズはバイト単位で表示されますが、TFTP サーバのファイル サイズはキロバイト単位で表示されることがあります）。ネットワークが非常にビジーである場合は、このような動作が生じる場合もあります。ネットワークの負荷が低下してから再度コピーを行うか、TFTP サーバとルータをイーサネットで直接接続して、ファイルをダウンロードしてください。

［Error opening tftp］

［Error opening tftp］エラーの例を示します。

```
router# copy tftp disk0:
Address or name of remote host [172.17.0.5]?
Source filename [c7300-js-mz.121-9.EX]?
Destination filename [c7300-js-mz.121-9.EX]?
Accessing tftp://172.17.0.5/c7300-js-mz.121-9.EX...
%Error opening tftp://172.17.0.5/c7300-js-mz.121-9.EX (No such file or directory)
```

ファイルが TFTP サーバのルート ディレクトリ内にあることを確認し、入力したファイル名が正しいかどうかをチェックします。間違いやすい文字には、I（大文字の i）、l（小文字の L）、および 1（数字の 1）などがあります。

タイムアウト エラー メッセージ

TFTP サーバが PC 上で起動していることを確認します。また、ファイルがルート ディレクトリ内にあることを確認します（TFTP アプリケーション ソフトウェア メニューバーで、**View — >Options** を選択します）。

［Can't open file］

TFTP サーバが PC 上で動作していることを確認します。コピーしたファイル名が正しいことを確認します。間違いやすい文字には、I（大文字の i）、l（小文字の L）、および 1（数字の 1）などがあります。

装置間でソフトウェア イメージをコピーする場合の装置の指定

次の表に、**copy tftp**、**copy rcp**、**dir** などの特定のコマンド内で装置を指定する場合に使用するコマンド オプションのリストを示します。コマンド オプションは、プラットフォームごとに異なります。アスタリスク（*****）が付いているオプションは、Cisco 7304 ルータでは無効です。

コマンド オプション	オプションの説明
bootdisk:	bootdisk: ファイル システムにコピーします。
disk0:	disk0: ファイル システムにコピーします。
flash:*	flash: ファイル システムにコピーします。
ftp:	ftp: ファイル システムにコピーします。
lex:	lex: ファイル システムにコピーします。
null:	null: ファイル システムにコピーします。
nvram:	nvram: ファイル システムにコピーします。
rcp:	rcp: ファイル システムにコピーします。
running-config	現在のシステム コンフィギュレーションを更新（結合）します。
slot0:*	slot0: ファイル システムにコピーします。
slot1:*	slot1: ファイル システムにコピーします。
startup-config	スタートアップ コンフィギュレーションにコピーします。
system:	system: ファイル システムにコピーします。
tftp:	tftp: ファイル システムにコピーします。

***** Cisco 7304 ルータで無効な **copy tftp** または **copy rcp** コマンド オプションです。

コマンド オプションの例を次に示します。

```
Router# copy tftp disk0:
Address or name of remote host [255.255.255.255]? 172.17.247.195
Source file name? c7300-js-mz.121-9.EX
Destination file name? c7300-js-mz.121-9.EX
. . . .

Router# dir disk0:
Directory of disk0:/

    1  -rw-     2351828   Jul 02 2001 08:25:54 c7300-js-mz.121-9.EX

16273408 bytes total (13488128 bytes free)
```

新しいソフトウェア イメージをリロードするための準備

- 新しいソフトウェア イメージが適切に保存されていることを確認します。

  dir disk0: コマンドを使用してファイルが保存済みであること、ファイル サイズが正しいこと、およびチェックサムが無効であることを示すメッセージが表示されていないことを確認します。ファイルが表示されない場合、ファイル名の後ろに［invalid checksum］が表示される場合、またはファイル サイズが TFTP サーバ上のファイル サイズと一致しない場合は、インストレーションを再度行う必要があります（ルータ内のファイル サイズはバイト単位で表示されますが、TFTP サーバのファイル サイズはキロバイト単位で表示されることがあります）。

- BOOT 環境変数が正しいソフトウェア イメージを示していることを確認します。

  BOOT 環境変数の内容、CONFIG_FILE 環境変数で指定されるコンフィギュレーション ファイルの名前、BOOTLDR 環境変数の内容、およびコンフィギュレーション レジスタ設定を表示するには、**show bootvar** コマンドを使用します。

BOOT 環境変数は、さまざまな装置で起動可能なイメージのリストを指定します。CONFIG_FILE 環境変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。BOOTLDR 環境変数は、起動のために ROM で使用されるブート イメージが格納された装置およびファイル名を指定します。これらの環境変数は、**boot system**、**boot config**、および **boot bootldr** コマンドを使用して、それぞれ設定します。

```
Router> en
Password:
Router# show bootvar
BOOT variable = disk0:c7300-p-mz.121-99.WS_DAILY_BUILD_20010706,12
CONFIG_FILE variable does not exist
BOOTLDR variable =
Configuration register is 0x2102
```

- ブート システム コマンドが、コンフィギュレーション ファイル内で正しい順番に並んでいることを確認します。

  ルータは、コンフィギュレーション ファイルに入力された順番で、ブート システム コマンドを格納および実行します。リスト内のブート システム コマンド エントリで指定された装置またはファイル名が無効な場合、そのエントリは省略されます。

```
router> en
Password:
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#boot system flash disk0:c7300-js-mz.121-9.EX
Router(config)#boot system flash disk0:
```

ソフトウェア イメージの検証に関するトラブルシューティング

不正なバージョン

show version コマンドの出力に表示されたバージョンが、ロードされたファイルと異なる場合は、「新しいソフトウェア イメージをリロードするための準備」（p.50）に記載された手順に従ってください。

表示解除されないブート プロンプト

リロード後も、ブート プロンプトが表示されている場合は、「新しいソフトウェア イメージをリロードするための準備」（p.50）に記載された手順に従ってください。

コンフィギュレーション レジスタ値が正しいことを確認します。最後の桁は 2 でなければなりません。**show version** コマンドを使用すればこの確認ができます。値が正しくない場合は、有効な値を復元して、ルータをリロードする必要があります。

PPP ネゴシエーションのデバッグ

ここでは、PPP が正しく動作している場合に表示されるメッセージや、PPP ネゴシエーション中に問題が発生した場合に表示されるメッセージを含めて、**debug ppp negotiation** がイネーブルの場合の出力例を示します。

PPP ネゴシエーションに成功した場合

PPP ネゴシエーションに成功すると、ライン プロトコルはアップになり、Link Control Protocol（LCP; リンク制御プロトコル）ステートはオープンになります。

```
Router#
*Mar 16 15:14:41.757:Se0/1 LCP:O CONFREQ [Listen] id 91 len 10
*Mar 16 15:14:41.757:Se0/1 LCP:   MagicNumber 0x521AE3AB (0x0506521AE3AB)
*Mar 16 15:14:41.757:Se0/1 LCP:I CONFREQ [Listen] id 1 len 10
*Mar 16 15:14:41.757:Se0/1 LCP:   MagicNumber 0x51C7619B (0x050651C7619B)
*Mar 16 15:14:41.761:Se0/1 LCP:O CONFACK [Listen] id 1 len 10
*Mar 16 15:14:41.761:Se0/1 LCP:   MagicNumber 0x51C7619B (0x050651C7619B)
*Mar 16 15:14:41.761:Se0/1 LCP:I CONFACK [ACKsent] id 91 len 10
*Mar 16 15:14:41.761:Se0/1 LCP:   MagicNumber 0x521AE3AB (0x0506521AE3AB)
*Mar 16 15:14:41.761:Se0/1 LCP:State is Open
*Mar 16 15:14:41.765:Se0/1 PPP:Phase is UP
```

この例における次の部分は、交換処理を示します。

O CONFREQ

Outgoing Configuration Request パケットがリモート ルータに送信されます。

I CONFREQ

Incoming Configuration Request パケットがリモート ルータから送信されます。

O CONFACK

Outgoing Configuration Acknowledgement がリモート ルータに送信されます。これによって、リモート ルータから送信された CONFREQ が ACK（確認）されます。このパケットの MagicNumber は、CONFREQ パケットの送信内容と一致する必要があります。

I CONFACK

Incoming Configuration Acknowledgement がリモート ルータから送信されます。これによって、ローカル ルータから送信された CONFREQ が ACK（確認）されます。このパケットの MagicNumber は、CONFREQ パケットの送信内容と一致する必要があります。

次の例では、**show interface** コマンドを使用して、PPP カプセル化を使用するインターフェイスの情報を表示します。

```
Router# sh int s0/1
Serial0/1 is up, line protocol is up
  Hardware is PQUICC with Fractional T1 CSU/DSU
  Internet address is 172.16.1.2/24
  MTU 1500 bytes, BW 384 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open:IPCP, CDPCP
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:09:13
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/128 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     31 packets input, 1034 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     123 packets output, 3196 bytes, 0 underruns
     0 output errors, 0 collisions, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

ローカル ルータがリモート ピアからパケットを受信していない場合

次の例では、リモート ピア ルータが返信を送信しないために、ローカル ルータが LCP CONFREQ の送信中にタイムアウトします。この問題が発生した場合は、次の点をチェックしてください。

- リモート ピアが PPP カプセル化用に設定されていること
- リモート ピアで **debug ppp neg** がイネーブルに設定されていて、CONFREQ パケットを受信中であること

```
Router#
*Mar 16 15:07:28.811:Se0/1 LCP:O CONFREQ [REQsent] id 5 len 10
*Mar 16 15:07:28.811:Se0/1 LCP:   MagicNumber 0x52142927 (0x050652142927)
*Mar 16 15:07:30.814:Se0/1 LCP:TIMEout:State REQsent
*Mar 16 15:07:30.814:Se0/1 LCP:O CONFREQ [REQsent] id 6 len 10
*Mar 16 15:07:30.814:Se0/1 LCP:   MagicNumber 0x52142927 (0x050652142927)
*Mar 16 15:07:32.814:Se0/1 LCP:TIMEout:State REQsent
*Mar 16 15:07:32.814:Se0/1 LCP:O CONFREQ [REQsent] id 7 len 10
*Mar 16 15:07:32.814:Se0/1 LCP:   MagicNumber 0x52142927 (0x050652142927)
*Mar 16 15:07:34.817:Se0/1 LCP:TIMEout:State REQsent
*Mar 16 15:07:34.817:Se0/1 LCP:O CONFREQ [REQsent] id 8 len 10
*Mar 16 15:07:34.817:Se0/1 LCP:   MagicNumber 0x52142927 (0x050652142927)
```

```
Router# sh int s0/1
Serial0/1 is up, line protocol is down
  Hardware is PQUICC with Fractional T1 CSU/DSU
  Internet address is 172.16.1.2/24
  MTU 1500 bytes, BW 384 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Listen
  Closed:IPCP, CDPCP
  Last input 2w1d, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:00:21
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/128 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     9 packets output, 126 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

リモート ピアがローカル ルータからパケットを受信していない場合

次の例では、ローカル ルータは CONFREQ の送信、CONFREQ の受信、およびリモート ピアへの CONFACK の送信を行っています。ただし、リモート ピアは CONFREQ パケットを受信していないため、CONFACK を返信していない可能性があります。このような場合は、ローカル ルータに問題がある可能性があります。次の点をチェックしてください。

- ローカル ルータの設定
- リモート ピアのデバッグ出力（チェックするには、リモート ピアで **debug ppp negotiation** をイネーブルにします。）

```
Router#
*Mar 16 15:14:41.757:Se0/1 LCP:O CONFREQ [Listen] id 91 len 10
*Mar 16 15:14:41.757:Se0/1 LCP:   MagicNumber 0x521AE3AB (0x0506521AE3AB)
*Mar 16 15:14:41.757:Se0/1 LCP:I CONFREQ [Listen] id 1 len 10
*Mar 16 15:14:41.757:Se0/1 LCP:   MagicNumber 0x51C7619B (0x050651C7619B)
*Mar 16 15:14:41.761:Se0/1 LCP:O CONFACK [Listen] id 1 len 10
*Mar 16 15:14:41.761:Se0/1 LCP:   MagicNumber 0x51C7619B (0x050651C7619B)
*Mar 16 15:14:43.761:Se0/1 LCP:TIMEout:State ACKsent
*Mar 16 15:14:43.761:Se0/1 LCP:O CONFREQ [ACKsent] id 92 len 10
*Mar 16 15:14:41.761:Se0/1 LCP:   MagicNumber 0x521AE3AB (0x0506521AE3AB)
*Mar 16 15:14:45.761:Se0/1 LCP:TIMEout:State ACKsent
*Mar 16 15:14:45.761:Se0/1 LCP:O CONFREQ [ACKsent] id 93 len 10
*Mar 16 15:14:41.761:Se0/1 LCP:   MagicNumber 0x521AE3AB (0x0506521AE3AB)
```

```
Router# sh int s0/1
Serial0/1 is up, line protocol is down
  Hardware is PQUICC with Fractional T1 CSU/DSU
  Internet address is 172.16.1.2/24
  MTU 1500 bytes, BW 384 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP ACKSENT
  Open:IPCP, CDPCP
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:09:13
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/128 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     31 packets input, 1034 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     123 packets output, 3196 bytes, 0 underruns
     0 output errors, 0 collisions, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

ネットワーク内のループ

ローカル ルータから送信されたパケットと同じパケットをこのローカル ルータが受信する場合は、ネットワークにループがあります。ローカル ルータとリモート ピア ルータを結ぶラインがループしています。

debug ppp negotiation の出力に、ラインがループしている可能性があることを示すメッセージが含まれています。この場合、ネットワークにはループがあります。サービス プロバイダーにこの問題を報告してください。

```
Router# sh int s0/0:0
Serial0/0:0 is up, line protocol is down (looped)
  Hardware is PQUICC Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, crc 16, loopback not set
  Keepalive set (10 sec)
   LCP Listen
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:29
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:weighted fair
  Output queue:0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     20 packets input, 280 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     20 packets output, 280 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions

Router#debug ppp neg
PPP protocol negotiation debugging is on
2d23h:Se0/0:0 LCP:TIMEout:State REQsent
2d23h:Se0/0:0 LCP:O CONFREQ [REQsent] id 13 len 10
2d23h:Se0/0:0 LCP:   MagicNumber 0x117C9F70 (0x0506117C9F70)
2d23h:Se0/0:0 LCP:I CONFREQ [REQsent] id 13 len 10
2d23h:Se0/0:0 LCP:   MagicNumber 0x117C9F70 (0x0506117C9F70)
2d23h:Se0/0:0 LCP:O CONFNAK [REQsent] id 13 len 10
2d23h:Se0/0:0 LCP:   MagicNumber 0x117CA73C (0x0506117CA73C)
2d23h:Se0/0:0 LCP:I CONFNAK [REQsent] id 13 len 10
2d23h:Se0/0:0 LCP:   MagicNumber 0x117CA73C (0x0506117CA73C)
2d23h:Se0/0:0 PPP:Line appears to be looped back
```

この例では、O CONFREQ の MagicNumber は I CONFREQ と同じです。この場合は、ルータは送信したパケットとまったく同じパケットを受信したと考えられます（PPP デバッグ メッセージを参照）。

マニュアルの入手方法

シスコの製品マニュアル、テクニカル サポート、およびその他のリソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

WWW 上の次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Cisco Documentation CD-ROM パッケージでご利用いただけます。Documentation CD-ROM は毎月更新されるので、印刷資料よりも新しい情報が得られます。この CD-ROM パッケージは、単独または年間契約で入手することができます。

Cisco.com 登録ユーザの場合、Subscription Store からオンラインで Documentation CD-ROM（Customer Order Number DOC-CONDOCCD=）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace

マニュアルの発注方法

マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Networking Products MarketPlace からシスコ製品のマニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com 登録ユーザの場合、Subscription Store からオンラインで Documentation CD-ROM（Customer Order Number DOC-CONDOCCD=）を発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

テクニカル サポート

シスコシステムズでは、技術上のあらゆる問題の支援窓口として、TAC Web サイトを含む Cisco.com を運営しています。お客様およびパートナーは TAC Web サイトからマニュアル、トラブルシューティングに関するヒント、およびコンフィギュレーション例を入手できます。Cisco.com にご登録済みのお客様は、TAC ツール、ユーティリティなど、TAC Web サイトで提供するすべてのテクニカル サポート リソースをご利用いただけます。Cisco.com へのご登録については、製品を購入された代理店へお問い合わせください。

Cisco.com

Cisco.com は、いつでもどこからでも、シスコシステムズの情報、ネットワーキング ソリューション、サービス、プログラム、およびリソースにアクセスできる対話形式のネットワーク サービスです。

Cisco.com は、広範囲の機能やサービスを通してお客様に次のような利点を提供します。

- 業務の円滑化と生産性の向上
- オンライン サポートによる技術上の問題の解決
- ソフトウェア パッケージのダウンロードおよびテスト
- シスコのトレーニング資料および製品の発注
- スキル査定、トレーニング、認定プログラムへのオンライン登録

また、Cisco.com に登録することにより、各ユーザに合った情報やサービスをご利用いただくことができます。Cisco.com には、次の URL からアクセスしてください。

http://www.cisco.com
http://www.cisco.com/jp

TAC

シスコの製品、テクノロジー、またはソリューションについて技術的な支援が必要な場合には、TAC をご利用いただくことができます。TAC では、2 種類のサポートを提供しています。TAC Web サイトと TAC Escalation Center です。どのタイプのサポートをご利用になるかは、問題の緊急性とサービス契約（該当する場合）に記載された条件によって決まります。

TAC への問い合わせは、問題の緊急性に応じて分類されます。

- プライオリティ レベル 4（P4）— シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要な場合。
- プライオリティ レベル 3（P3）— ネットワークのパフォーマンスが低下している。ネットワークが十分に機能していないが、ほとんどの業務運用を継続できる場合。
- プライオリティ レベル 2（P2）— ネットワークのパフォーマンスが著しく低下したため業務に重大な影響があるにもかかわらず、対応策が見つからない場合。
- プライオリティ レベル 1（P1）— ネットワークがダウンし、すぐにサービスを回復しなければ業務に致命的な損害が発生するにもかかわらず、対応策が見つからない場合。

TAC Web サイト

P3 および P4 レベルの問題については、TAC Web サイトを利用して、お客様ご自身で問題を解決し、コストと時間を節約することができます。このサイトでは各種のオンライン ツール、ナレッジ ベース、およびソフトウェアを、いつでも必要なときに利用できます。TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/tac

シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラーは、TAC Web サイトのすべてのテクニカル サポート リソースをご利用いただけます。Cisco TAC Web サイトの一部のサービスには、Cisco.com のログイン ID とパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

Cisco.com の登録ユーザは、TAC Web サイトで技術上の問題を解決できなかった場合、次の URL から TAC Case Open ツールのオンライン サービスを利用することができます。

http://www.cisco.com/en/US/support/index.html

インターネットを利用する場合、P3 および P4 の問題については、お客様ご自身の言葉で状況を説明し、必要なファイルを添付できるよう、TAC Web サイトで Case Open ツールを利用することをお勧めします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

TAC Escalation Center

TAC Escalation Center では、P1 および P2 レベルの問題に対応しています。このレベルに分類されるのは、ネットワークの機能が著しく低下し、業務の運用に重大な影響がある場合です。TAC Escalation Center にお問い合わせいただいた P1 または P2 の問題には、TAC エンジニアが対応します。

TAC フリーダイヤルの国別電話番号は、次の URL を参照してください。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

ご連絡に先立って、お客様が契約しているシスコ サポート サービスがどのレベルの契約となっているか（たとえば、SMARTnet、SMARTnet Onsite、または Network Supported Accounts［NSA; ネットワーク サポート アカウント］など）、お客様のネットワーク管理部門にご確認ください。また、お客様のサービス契約番号およびご使用の製品のシリアル番号をお手元にご用意ください。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press では、ネットワーク関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。『*Internetworking Terms and Acronyms Dictionary*』、『*Internetworking Technology Handbook*』、『*Internetworking Troubleshooting Guide*』、『*Internetworking Design Guide*』などです。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』は、シスコシステムズが発行する月刊誌で、業界の専門家向けにネットワーク分野の最新情報を提供します。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- 『*iQ Magazine*』は、シスコシステムズが発行する月刊誌で、ビジネス リーダーや経営幹部向けにネットワーク業界の最新情報を提供します。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- トレーニング ― シスコシステムズはネットワーク関連のトレーニングを世界各地で実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/le31/learning_learning_resources_home.html

お問い合わせは、購入された各代理店へご連絡ください。

CISCO SYSTEMS

シスコシステムズ株式会社
URL:http://www.cisco.com/jp/
問合せ URL:http://www.cisco.com/jp/service/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL.03-5549-6500　FAX.03-5549-6501

OL-1270-02-J