CHAPTER 1

製品概要

この章で説明する内容は、次のとおりです。

サポート対象ハードウェアおよびソフトウェア

Cisco 7600 シリーズ ルータによってサポートされるシャーシ、モジュール、ソフトウェア機能の詳細については、『*Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*』を参照してください。

このリリースで使用できる Cisco IOS ソフトウェア イメージの詳細については、付録 C「Cisco IOS Release 15.S ソフトウェア イメージ」を参照してください。

（注） Cisco IOS Release 12.2SR 以降のリリースの場合、Supervisor Engine 2、Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）、FlexWAN モジュールは、Cisco 7600 シリーズ ルータでサポートされません。

ユーザ インターフェイス

Release 12.2SR では、次のインターフェイスを使用する設定がサポートされます。

- CLI：次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』の「Using the Command-Line Interface」を参照してください。

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- SNMP：次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』および『*Cisco IOS Command Reference*』を参照してください。

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- Cisco IOS Web ブラウザ インターフェイス：次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using the Cisco Web Browser」を参照してください。

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

- 組み込み CiscoView：「組み込み CiscoView サポートの設定」（P.1-2）を参照してください。

組み込み CiscoView サポートの設定

ここでは、組み込み CiscoView サポートの設定について説明します。

組み込み CiscoView の概要

組み込み CiscoView ネットワーク管理システムは、Web ベースのインターフェイスです。HTTP および SNMP を使用してルータをグラフィック表示し、GUI ベースの管理および設定インターフェイスを提供します。組み込み CiscoView の Java Archive（JAR）ファイルは、次の URL からダウンロードできます。

http://www.cisco.com/cisco/software/navigator.html

組み込み CiscoView のインストールおよび設定

組み込み CiscoView のインストールおよび設定を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# dir device_name`	デバイスの内容を表示します。 組み込み CiscoView を初めてインストールする場合、または CiscoView ディレクトリが空の場合には、ステップ 4 に進んでください。
ステップ 2	`Router# delete device_name:cv/*`	CiscoView ディレクトリから既存のファイルを削除します。
ステップ 3	`Router# squeeze device_name:`	ファイル システムのスペースを回復します。
ステップ 4	`Router# archive tar /xtract tftp://ip_address_of_tftp_server/ciscoview.tar device_name:cv`	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上の tar ファイルから CiscoView ディレクトリに、CiscoView ファイルを抽出します。
ステップ 5	`Router# dir device_name:`	デバイスの内容を表示します。 冗長構成の場合は、冗長スーパーバイザ エンジンのファイル システムについてステップ 1 ～ステップ 5 を繰り返します。
ステップ 6	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	`Router(config)# ip http server`	HTTP Web サーバをイネーブルにします。

	コマンド	目的
ステップ 8	`Router(config)# snmp-server community string ro`	読み取り専用動作の SNMP パスワードを設定します。
ステップ 9	`Router(config)# snmp-server community string rw`	読み取り / 書き込み用動作の SNMP パスワードを設定します。

（注）　ルータ Web ページにアクセスするためのデフォルトのパスワードは、ルータのイネーブルレベル パスワードです。

ルータへの Web アクセスの詳細については、次の URL にある『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using the Cisco Web Browser」を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/ffcprt1/fcf005.htm

組み込み CiscoView 情報の表示

組み込み CiscoView 情報を表示するには、次の EXEC コマンドを入力します。

コマンド	目的
`Router# show ciscoview package`	組み込み CiscoView ファイルに関する情報を表示します。
`Router# show ciscoview version`	組み込み CiscoView のバージョンを表示します。

PFC および DFC がハードウェアでサポートするソフトウェア機能

ここでは、Policy Feature Card 3（PFC3; ポリシー フィーチャ カード 3）、Distributed Forwarding Card 3（DFC3; 分散型フォワーディング カード 3）、および Distributed Forwarding Card（DFC; 分散型フォワーディング カード）が提供するハードウェア サポートについて説明します。

- 「PFC3、DFC3、および DFC がハードウェアでサポートするソフトウェア機能」（P.1-3）
- 「PFC3 および DFC3 がハードウェアでサポートするソフトウェア機能」（P.1-4）

PFC3、DFC3、および DFC がハードウェアでサポートするソフトウェア機能

PFC3、DFC3、および DFC では、次に示す Cisco IOS ソフトウェア機能がハードウェアでサポートされます。

- レイヤ 3 ポートおよび VLAN インターフェイスのアクセス コントロール リスト（ACL）
  - 入 / 出力標準 ACL および拡張 ACL の許可アクションおよび拒否アクション

    （注）　ACL ロギングが必要なフローは、MSFC 上のソフトウェアで処理されます。

  - MPLS インターフェイスを除き、セッション内の最初のパケットが MSFC 上のソフトウェアで処理されたあとの再帰 ACL フロー
  - ダイナミック ACL フロー

（注）　MSFC 上のソフトウェアで処理されるアイドル タイムアウト

ACL の PFC および DFC サポートの詳細については、第 36 章「Cisco IOS ACL サポートの概要」を参照してください。ACL の設定の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*, Release 12.2』の「Traffic Filtering and Firewalls」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

- VLAN ACL（VACL）：VACL を設定するには、第 37 章「VACL の設定」を参照してください。
- **match ip address**、**set ip next-hop**、および **ip default next-hop** Policy-Base Routing（PBR; ポリシー ベース ルーティング）キーワードを使用するルートマップ シーケンスの PBR

  PBR の設定については、次の URL にある『*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2』の「Classification」および「Configuring Policy-Based Routing」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html

（注）　MSFC3 アドレスまたは MSFC4 アドレスが PBR ACL の範囲内にある場合、MSFC にアドレス指定されたトラフィックは MSFC に転送されないで、ハードウェアでポリシー ルーティングされます。MSFC3 または MSFC4 にアドレス指定されたトラフィックのポリシー ルーティングを禁止するには、その MSFC にアドレス指定されたトラフィックを拒否するように PBR ACL を設定します。

- MPLS インターフェイスを除く TCP インターセプト：TCP インターセプトを設定するには、「TCP インターセプトの設定」（P.35-2）を参照してください。
- ハードウェアが処理する NetFlow 集約：次の URL を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nde.html

PFC3 および DFC3 がハードウェアでサポートするソフトウェア機能

PFC3 および DFC3 では、次に示す Cisco IOS ソフトウェア機能がハードウェアでサポートされます。

- ポイントツーポイント Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル上の IPv4 マルチキャスト：次の URL のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

- ハードウェアの双方向 Protocol Independent Multicast（PIM）：「IPv4 双方向 PIM の機能概要」（P.31-7）を参照してください。
- 複数パスによるユニキャスト Reverse Path Forwarding（RPF; リバース パス転送）チェック：ユニキャスト RPF チェックを設定するには、「ユニキャスト RPF チェックの設定」（P.35-2）を参照してください。
- MPLS インターフェイスを除く、IPv4 ユニキャストおよびマルチキャスト トラフィックのネットワーク アドレス変換（NAT）

  ハードウェアが処理する NAT については、次の点に注意してください。

  - UDP トラフィックの NAT は、PFC3A モードではサポートされません。
  - PFC3 はマルチキャスト トラフィックの NAT をサポートしません。

  - PFC3 は、長さを指定するルートマップが設定された NAT をサポートしません。
  - インターフェイスで NAT および NDE が設定されている場合、PFC3 はすべてのトラフィックを分割パケットに格納して MSFC3 または MSFC4 に送信し、そこでソフトウェア処理します（CSCdz51590）。

  NAT を設定するには、次の URL にある『*Cisco IOS IP Configuration Guide*, Release 12.2』の「IP Addressing and Services」、「Configuring IP Addressing」、および「Configuring Network Address Translation」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html

  DoS 攻撃や設定ミスが原因で大量の NAT トラフィックが MSFC3 に送信されることがないようにするには、**mls rate-limit unicast acl {ingress | egress}** コマンドを入力します（次の URL を参照）。

  http://www.cisco.com/en/US/products/hw/switches/ps700/prod_command_reference_list.html

- PFC3 および DFC3 では、ポイントツーポイント GRE トンネル上の IPv4 マルチキャストがハードウェアでサポートされます。
- GRE トンネリングおよび IP-in-IP トンネリング：PFC3 および DFC3 は次の **tunnel** コマンドをサポートします。
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  MSFC3 および MSFC4 では、その他の **tunnel** コマンドで設定したトンネリングがサポートされます。

  tunnel ttl コマンド（デフォルトは 255）は、カプセル化パケットの TTL を設定します。

  tunnel tos コマンドでは、パケットがカプセル化される際にパケットの ToS バイトを設定します。**tunnel tos** コマンドが存在せず、QoS がイネーブルでない場合、パケットがカプセル化される際にパケットの ToS バイトには、元のパケットの ToS バイトが設定されます。**tunnel tos** コマンドが存在せず、QoS がイネーブルである場合、パケットがカプセル化される際にパケットの ToS バイトには、PFC QoS によって変更されたパケットの ToS バイトが設定されます。

  GRE トンネリングおよび IP-in-IP トンネリングを設定するには、次の資料を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

  http://www.cisco.com/en/US/docs/ios/12_2/interface/command/reference/irfshoip.html

  tunnel tos コマンドおよび **tunnel ttl** コマンドを設定するには、次の資料を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

  トンネルについては、次の点に注意してください。

  - ハードウェアが処理する各トンネルには固有の送信元が必要です。ハードウェアが処理するトンネルは宛先が異なる場合でも送信元を共有できません。ループバック インターフェイス上のセカンダリ アドレスを使用するか、複数のループバック インターフェイスを作成します 固有の送信元アドレスを使用できないと、ソフトウェア パスの輻輳中にコントロール プレーンに失敗する場合があります。
  - 各トンネル インターフェイスは、内部 VLAN を 1 つ使用します。

- 各トンネル インターフェイスは、ルータ MAC アドレスごとに追加ルータ MAC アドレス エントリを 1 つ使用します。
- PFC3A はトンネル インターフェイスの PFC QoS 機能をサポートしません。その他の PFC はすべてサポートします。
- MSFC3 および MSFC4 は、トンネル インターフェイスに出力機能が設定されたトンネルをサポートします。出力機能の例は、出力 Cisco IOS ACL、NAT（内部から外部への変換の場合）、TCP インターセプト、CBAC、暗号化などです。