管理プレーン保護の実装

管理プレーン保護（MPP）機能では、ネットワーク管理パケットのデバイスへの着信を許可するインターフェイスを制限できます。ネットワーク オペレータは MPP 機能を使用して、1 つ以上のルータ インターフェイスを管理インターフェイスとして指定できます。

MPP 保護機能は、MPP 配下のすべての管理プロトコルと同様、デフォルトではディセーブルになっています。インターフェイスをアウトオブバンドまたはインバンドとして設定すると、MPP が自動的に有効になります。これにより、MPP 配下のすべてのプロトコルもイネーブルになります。MPP がディセーブルでプロトコルがアクティブな場合、トラフィックはすべてのインターフェイスを通過できます。

アクティブなプロトコルが存在する状態で MPP がイネーブルになると、管理トラフィックを許可するデフォルトの管理インターフェイスはルートプロセッサ（RP）およびスタンバイ ルート プロセッサ（SRP）のイーサネット インターフェイスのみになります。MPP をイネーブルにする他のすべてのインターフェイスについては、手動で管理インターフェイスとして設定する必要があります。

以後は、デフォルト管理インターフェイスと事前に MPP インターフェイスとして設定したインターフェイスのみがデバイス宛のネットワーク管理パケットを受け付けます。他のすべてのインターフェイスは、デバイス宛のネットワーク管理パケットをドロップします。論理インターフェイス（またはデータ プレーンに存在しない他のすべてのインターフェイス）は、入力物理インターフェイスに基づいてパケットをフィルタリングします。

管理プレーン保護の利点

MPP 機能を設定すると、次の利点があります。

- すべてのインターフェイスで管理プロトコルを許可することを超える、デバイスの管理目的でのアクセス制御。

- 非管理インターフェイスでのデータ パケットのパフォーマンス向上。
- ネットワークの拡張性のサポート。
- インターフェイス単位のアクセス コントロール リスト（ACL）を使用することによる、デバイスへの管理アクセス制限の作業の簡易化。
- デバイスへのアクセスを制限するために必要な ACL 数の削減。
- スイッチングインターフェイスおよびルーティングインターフェイス上でパケットフラッディングの CPU への到達を防止。

管理プレーン保護の実装に関する制約事項

管理プレーン保護（MPP）の実装には次の制約事項があります。

- 現在、MPP は拒否またはドロップされたプロトコル要求を追跡していません。
- MPP 設定では、プロトコル サービスをイネーブルにはできません。MPP はさまざまなインターフェイスでサービスを利用可能にする役割のみを果たします。プロトコルは明示的にイネーブル化されます。
- インバンドインターフェイスで受信する管理要求は、その場で必ずしも認知されるわけではありません。
- MPP設定に加えた変更は、その変更よりも前に確立されているアクティブなセッションには影響を与えません。
- 現在、MPP は、TFTP、Telnet、簡易ネットワーク管理プロトコル（SNMP）、セキュアシェル（SSH）、XML、Netconf などのプロトコルに対して着信する管理要求のみを制御します。
- MPP は MIB をサポートしていません。

インバンドインターフェイスの管理プレーン保護のデバイスの設定

インバンド管理インターフェイスは、データ転送パケットだけでなく管理パケットも処理する、物理インターフェイスまたは論理インターフェイスです。インバンド管理インターフェイスは、共有管理インターフェイスとも呼ばれています。ネットワークに追加した直後のデバイスや、ネットワークですでに動作しているデバイスを設定するには、この作業を実行します。この作業では、特定のインターフェイスを通じてのみTelnetのルータへのアクセスが許可されるインバンドインターフェイスとして、MPP を設定する方法について説明します。

デフォルトでないVRFでインバンドMPPインターフェイスを設定するには、次の作業を追加で実行します。

- デフォルトでないインバンド VRF のインターフェイスを設定します。
- グローバル インバンド VRF を設定します。
- Telnet の場合は、インバンド VRF に対して Telnet VRF サーバを設定します。

手順

ステップ 1 **configure**

ステップ 2 control-plane

例：

```
RP/0/RP0/cpu 0: router(config)# control-plane
RP/0/RP0/cpu 0: router(config-ctrl)#
```

コントロール プレーン コンフィギュレーション モードを開始します。

ステップ 3 management-plane

例：

```
RP/0/RP0/cpu 0: router(config-ctrl)# management-plane
RP/0/RP0/cpu 0: router(config-mpp)#
```

管理プレーン保護を設定してプロトコルを許可および拒否し、管理プレーン保護コンフィギュレーション モードを開始します。

ステップ 4 inband

例：

```
RP/0/RP0/cpu 0: router(config-mpp)# inband
RP/0/RP0/cpu 0: router(config-mpp-inband)#
```

インバンド インターフェイスを設定し、管理プレーン保護インバンド コンフィギュレーション モードを開始します。

ステップ 5 **interface** {*type instance* | **all**}

例：

```
RP/0/RP0/cpu 0: router(config-mpp-inband)# interface HundredGigE 0/9/0/0
RP/0/RP0/cpu 0: router(config-mpp-inband-Gi0_0_1_0)#
```

特定のインバンド インターフェイスを設定するか、すべてのインバンド インターフェイスを設定します。管理プレーン保護インバンド インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを使用します。

- **all** キーワードを使用して、すべてのインターフェイスを設定します。

ステップ 6 **allow** {*protocol* | **all**} [**peer**]

例：

```
RP/0/RP0/cpu 0: router(config-mpp-inband-Gi0_0_1_0)# allow Telnet peer
RP/0/RP0/cpu 0: router(config-telnet-peer)#
```

指定されたプロトコルまたはすべてのプロトコルに対するインバンド インターフェイスとして、インターフェイスを設定します。

- *protocol* 引数を使用して、指定管理インターフェイスで管理プロトコルを許可します。
  - SNMP（バージョンも）
  - セキュア シェル（v1 および v2）
  - TFTP
  - Telnet
  - Netconf
  - XML
- **all** キーワードを使用して、プロトコルのリストで指定されるすべての管理トラフィックを許可するようにインターフェイスを設定します。
- （任意）**peer** キーワードを使用して、インターフェイスでピア アドレスを設定します。

ステップ 7 **address ipv4** {*peer-ip-address* | *peer ip-address/length*}

例：

```
RP/0/RP0/cpu 0: router(config-telnet-peer)# address ipv4 10.1.0.0/16
```

このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレスを設定します。

- *peer-ip-address* 引数を使用して、このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレスを設定します。
- *peer ip-address/length* 引数を使用して、ピア IPv4 アドレスのプレフィックスを設定します。

ステップ 8 **commit**

ステップ 9 **show mgmt-plane** [**inband** |] [**interface** {*type instance*}]

例：

```
RP/0/RP0/cpu 0: router# show mgmt-plane inband interface HundredGigE 0/9/0/0
```

インターフェイスのタイプやインターフェイスでイネーブルにされるプロトコルなど、管理プレーンに関する情報を表示します。

- （任意）**inband** キーワードを使用して、管理パケットおよびデータ転送パケットを処理するインターフェイスであるインバンド管理インターフェイスの設定を表示します。
- （任意）**interface** キーワードを使用して、特定のインターフェイスの詳細を表示します。

アウトオブバンドインターフェイスの管理プレーン保護のデバイスの設定

アウトオブバンドは、管理プロトコルトラフィックの転送または処理だけを許可するインターフェイスを意味します。アウトオブバンド管理インターフェイスは、ネットワーク管理トラフィックだけを受信するようネットワーク オペレータによって定義されます。転送（またはカスタマー）トラフィックの利点は、ルータの管理が妨害されないことであり、これにより、サービス拒否攻撃の可能性が大幅に低減します。

アウトオブバンド インターフェイスは、アウトオブバンド インターフェイス間のトラフィックのみを転送するか、ルータ宛の管理パケットを終端します。また、アウトオブバンド インターフェイスをダイナミック ルーティング プロトコルに加えることができます。サービス プロバイダーはルータのアウトオブバンドインターフェイスに接続し、ルータが提供可能なすべてのルーティング ツールおよびポリシー ツールを使用して、独立したオーバーレイ管理ネットワークを構築します。

アウトオブバンド MPP インターフェイスを設定するには、次の作業を実行します。

- アウトオブバンド VRF のインターフェイスを設定します。
- グローバル アウトオブバンド VRF を設定します。
- Telnet の場合は、アウトオブバンド VRF に対して Telnet VRF サーバを設定します。

手順

ステップ 1 **configure**

ステップ 2 control-plane

例：

```
RP/0/RP0/cpu 0: router(config)# control-plane
```

```
RP/0/RP0/cpu 0: router(config-ctrl)#
```

コントロール プレーン コンフィギュレーション モードを開始します。

ステップ 3 management-plane

例：

```
RP/0/RP0/cpu 0: router(config-ctrl)# management-plane
RP/0/RP0/cpu 0: router(config-mpp)#
```

管理プレーン保護を設定してプロトコルを許可および拒否し、管理プレーン保護コンフィギュレーション モードを開始します。

ステップ 4 out-of-band

例：

```
RP/0/RP0/cpu 0: router(config-mpp)# out-of-band
RP/0/RP0/cpu 0: router(config-mpp-outband)#
```

帯域外インターフェイスまたはプロトコルを設定し、管理プレーン保護帯域外コンフィギュレーション モードを開始します。

ステップ 5 **vrf** *vrf-name*

例：

```
RP/0/RP0/cpu 0: router(config-mpp-outband)# vrf target
```

帯域外インターフェイスのバーチャルプライベートネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）リファレンスを設定します。

- *vrf-name* 引数を使用して、VRF に名前を割り当てます。

ステップ 6 **interface** {*type instance* | **all**}

例：

```
RP/0/RP0/cpu 0: router(config-mpp-outband)# interface HundredGigE 0/9/0/0
RP/0/RP0/cpu 0: router(config-mpp-outband-if)#
```

特定のアウトオブバンド インターフェイス、またはすべてのアウトオブバンド インターフェイスをアウトオブバンドインターフェイスとして設定します。管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始するには、**interface** コマンドを使用します。

- **all** キーワードを使用して、すべてのインターフェイスを設定します。

ステップ 7 **allow** {*protocol* | **all**} [**peer**]

例：

```
RP/0/RP0/cpu 0: router(config-mpp-outband-if)# allow TFTP peer
RP/0/RP0/cpu 0: router(config-tftp-peer)#
```

指定されたプロトコルまたはすべてのプロトコルに対するアウトオブバンドインターフェイスとして、インターフェイスを設定します。

- *protocol* 引数を使用して、指定管理インターフェイスで管理プロトコルを許可します。
  - HTTP または HTTPS
  - SNMP（バージョンも）
  - セキュア シェル（v1 および v2）
  - TFTP
  - Telnet
  - Netconf
- **all** キーワードを使用して、プロトコルのリストで指定されるすべての管理トラフィックを許可するようにインターフェイスを設定します。
- （任意）**peer** キーワードを使用して、インターフェイスでピア アドレスを設定します。

ステップ 8 **address ipv6** {*peer-ip-address* | *peer ip-address/length*}

例：

```
RP/0/RP0/cpu 0: router(config-tftp-peer)# address ipv6 33::33
```

このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレスを設定します。

- *peer-ip-address* 引数を使用して、このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレスを設定します。
- *peer ip-address/length* 引数を使用して、ピア IPv6 アドレスのプレフィックスを設定します。

ステップ 9 **commit**

ステップ 10 **show mgmt-plane** [**inband** | **out-of-band**] [**interface** {*type instance*} | **vrf**]

例：

```
RP/0/RP0/cpu 0: router# show mgmt-plane out-of-band interface HundredGigE 0/9/0/0
```

インターフェイスのタイプやインターフェイスでイネーブルにされるプロトコルなど、管理プレーンに関する情報を表示します。

- （任意）**inband** キーワードを使用して、管理パケットおよびデータ転送パケットを処理するインターフェイスであるインバンド管理インターフェイスの設定を表示します。
- （任意）**out-of-band** キーワードを使用して、アウトオブバンド インターフェイス設定を表示します。
- （任意）**interface** キーワードを使用して、特定のインターフェイスの詳細を表示します。
- （任意）**vrf** キーワードを使用して、アウトオブバンドインターフェイスのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送リファレンスを表示します。

例

次に、MMP 下での特定の IP アドレスに対するインバンドおよびアウトオブバンド インターフェイスを設定する例を示します。

```
configure
 control-plane
  management-plane
   inband
    interface all
     allow SSH
     !
    interface HundredGigE 0/9/0/0
     allow all
     allow SSH
     allow Telnet peer
      address ipv4 10.1.0.0/16
    !
   !
    interface HundredGigE 0/9/0/0
     allow Telnet peer
      address ipv4 10.1.0.0/16
     !
    !
   !
   out-of-band
    vrf my_out_of_band
    interface HundredGigE 0/9/0/0
     allow TFTP peer
      address ipv6 33::33
     !
    !
   !
  !
 !

show mgmt-plane

Management Plane Protection

inband interfaces
```

```
----------------------

interface - HundredGigE0_9_0_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - HundredGigE0_9_0_0
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - HundredGigE0_9_0_0
        tftp configured -
                peer v6 allowed - 33::33

show mgmt-plane out-of-band vrf

Management Plane Protection -
        out-of-band VRF - my_out_of_band
```

管理プレーン保護の実装について

管理プレーン保護機能をイネーブルにする前に、次の概念について理解しておく必要があります。

インターフェイス上のピア フィルタリング

ピア フィルタリング オプションでは、特定のピアまたはピア範囲からの管理トラフィックの設定を許可します。

コントロール プレーン保護

コントロール プレーンは、ルート プロセッサ上のプロセス レベルで稼働するプロセスの集合であり、ほとんどの Cisco ソフトウェアの機能に高レベルの制御を提供します。直接的または間接的にルータを宛先とするすべてのトラフィックは、コントロールプレーンによって処理されます。管理プレーン保護はコントロール プレーン インフラストラクチャ内で動作します。

管理プレーン

管理プレーンは、ルーティングプラットフォームの管理に関連するすべてのトラフィックの論理的なパスです。層およびプレーンで構成される通信アーキテクチャの 3 つのプレーンの 1 つである管理プレーンは、ネットワークの管理機能を実行し、すべてのプレーン（管理、制御、

およびデータ）間で機能を調整します。また、管理プレーンはネットワークとの接続を通じてデバイスの管理に使用されます。

管理プレーンで処理されるプロトコルの例は、簡易ネットワーク管理プロトコル（SNMP）、Telnet、SSH、XML および Netconf です。これらの管理プロトコルは、モニタリングやコマンドライン インターフェイス（CLI）のアクセスに使用されます。デバイスに対し、内部送信元（信頼ネットワーク）へのアクセスを制限することが重要です。