



ポートユニキャストおよびマルチキャストフラッディングブロック

この章では、Catalyst 4500 シリーズ スイッチ上でマルチキャストおよびユニキャスト フラッディング ブロックを設定する方法について説明します。この章の内容は、次のとおりです。

- 「フラッディング ブロックの概要」 (P.48-1)
- 「ポート ブロックの設定」 (P.48-1)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

フラッディング ブロックの概要

Media Access Control (MAC; メディア アクセス制御) アドレスが期限切れになるか、スイッチによって学習されなかったために、不明のユニキャストまたはマルチキャスト トラフィックがスイッチ ポートにフラッディングすることがあります (この状態は、特に Private VLAN (PVLAN) 独立ポートでは望ましくありません)。ポートにユニキャストおよびマルチキャスト トラフィックがフラッディングしないようにするには、**switchport block unicast** および **switchport block multicast** コマンドを使用して、スイッチでのフラッディング ブロックをイネーブルにします。



(注)

フラッディング ブロック機能は、すべてのスイッチド ポート (PVLAN ポートを含む) でサポートされ、ポートが転送するすべての Virtual LAN (VLAN; 仮想 LAN) に適用されます。

ポート ブロックの設定

デフォルトでは、スイッチは不明の宛先 MAC アドレスを持つパケットをすべてのポートにフラッディングします。不明のユニキャストおよびマルチキャスト トラフィックがスイッチ ポートに転送される場合、セキュリティ問題が生じる可能性があります。このようなトラフィックの転送を防ぐために、不明のユニキャストまたはマルチキャスト パケットをブロックするようにポートを設定できます。



(注)

ユニキャストまたはマルチキャストトラフィックのブロックは、スイッチポート上で自動的にはいネーブルになりません。明示的に設定する必要があります。

インターフェイス上でのフラディングするトラフィックのブロック



(注)

有効なインターフェイスは、物理インターフェイス（たとえば、GigabitEthernet 1/1）または EtherChannel グループ（port-channel 5 など）です。ポートチャネルのマルチキャストまたはユニキャストトラフィックをブロックする場合、ポートチャネルグループのすべてのポートでブロックされます。



(注)

Cisco IOS Release 12.2(52)SG から、IPv4 および IPv6 の不明なマルチキャストトラフィックフラディングだけがブロックされます。レイヤ 2 の不明なマルチキャストフラディングはブロックされません。この動作は、ポート上の不明なマルチキャストフラディングのブロックを設定すると、ポートへのブロードキャストトラフィックもブロックされるという問題の解決によるものです。

インターフェイスへのマルチキャストおよびユニキャストパケットのフラディングをディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# 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 2	Switch(config)# interface interface-id	インターフェイス コンフィギュレーション モードを開始し、スイッチポート インターフェイスのタイプおよび番号を入力します（たとえば、 GigabitEthernet 1/1 ）。
ステップ 3	Switch(config-if)# switchport block multicast	ポートへの不明マルチキャストの転送をブロックします。
ステップ 4	Switch(config-if)# switchport block unicast	ポートへの不明ユニキャストの転送をブロックします。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show interface interface-id switchport	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、ギガビットイーサネットインターフェイス 1/1 上でユニキャストおよびマルチキャストフラディングをブロックし、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
Switch# show interface gigabitethernet1/1 switchport
Name: Gi1/3
Switchport: Enabled

<output truncated>

Port Protected: On
```

```

Unknown Unicast Traffic: Not Allowed
Unknown Multicast Traffic: Not Allowed

Broadcast Suppression Level: 100
Multicast Suppression Level: 100
Unicast Suppression Level: 100

```

ポート上での通常の転送の再開

ポート上で通常の転送を再開するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# 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 2	Switch(config)# interface <i>interface-id</i>	インターフェイス コンフィギュレーション モードを開始し、スイッチポート インターフェイスのタイプおよび番号を入力します (たとえば、GigabitEthernet 1/1)。
ステップ 3	Switch(config-if)# no switchport block multicast	ポートへの不明マルチキャストのフラディングをイネーブルにします。
ステップ 4	Switch(config-if)# no switchport block unicast	ポートへの不明ユニキャストのフラディングをイネーブルにします。
ステップ 5	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show interface <i>interface-id</i> switchport	入力を確認します。
ステップ 7	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

