



DMVPN の Per-Tunnel QoS

DMVPN の Per-Tunnel QoS 機能は、DMVPN のトンネルごとの QoS サポートを提供し、IPSec トンネル インターフェイスのトンネルごとの QoS パフォーマンスを向上させます。



(注)

セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『[Next Generation Encryption](#)』（NGE）ホワイト ペーパーを参照してください。

- [機能情報の確認, 1 ページ](#)
- [DMVPN の Per-Tunnel QoS の前提条件, 2 ページ](#)
- [DMVPN の Per-Tunnel QoS の制約事項, 2 ページ](#)
- [DMVPN の Per-Tunnel QoS について, 4 ページ](#)
- [DMVPN の Per-Tunnel QoS の設定方法, 6 ページ](#)
- [DMVPN の Per-Tunnel QoS の設定例, 12 ページ](#)
- [DMVPN の Per-Tunnel QoS の参考資料, 18 ページ](#)
- [DMVPN の Per-Tunnel QoS の機能情報, 19 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、[Bug Search Tool](#) およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

DMVPN の Per-Tunnel QoS の前提条件

- DMVPN の Per-Tunnel QoS 機能を設定する前に、シスコ エクスプレス フォワーディング スイッチングを設定する必要があります。
- スポークで Next Hop Resolution Protocol (NHRP) グループを設定し、ハブの QoS ポリシーに NHRP グループをマッピングするには、トンネルごとの QoS を使用しない DMVPN 用にスポークおよびハブを設定しておく必要があります。

DMVPN の Per-Tunnel QoS の制約事項

- DMVPN の Per-Tunnel QoS 機能では、次のカプセル化およびトランスポート プロトコルの組み合わせのみがサポートされます。
 - DMVPN 経由の IPv4 の Per-Tunnel QoS と IPv4 トランスポート (Cisco IOS XE Release 3.6S 以降で有効)。
 - DMVPN 経由の IPv6 の Per-Tunnel QoS と IPv4 トランスポート (Cisco IOS XE Release 3.8S 以降で有効)。
 - DMVPN 経由の IPv4 の Per-Tunnel QoS と IPv6 トランスポート (Cisco IOS XE Release 3.11S 以降で有効)。
 - DMVPN 経由の IPv6 の Per-Tunnel QoS と IPv6 トランスポート (Cisco IOS XE Release 3.11S 以降で有効)。
 - DMVPN 経由の MPLS VPN の Per-Tunnel QoS と IPv4 トランスポート (2547oDMVPN) (Cisco IOS XE Release 3.15S 以降で有効)。
 - DMVPN 経由の MPLS VPN の Per-Tunnel QoS と IPv6 トランスポート (2547oDMVPN) (Cisco IOS XE Release 3.15S 以降で有効)。
- ある特定の DMVPN トンネルインターフェイスの場合、1つのトランスポートプロトコルとして、IPv4 または IPv6 のみを使用できます。ただし、同じデバイスでも別の DMVPN トンネルインターフェイスでは IPv4 または IPv6 トランスポートプロトコルを同時に使用できます。Per-Tunnel QoS を IPv4 および IPv6 DMVPN パッセンジャのトラフィック パケット用に設定して、アウトバウンド物理インターフェイス (IPv4 か IPv6、またはその両方) に関連付けることができます。独自の制限付き QoS ポリシーが設定されたアウトバウンド物理インターフェイスでは、この DMVPN トンネルトラフィックで DMVPN 以外の IPv4 または IPv6 トラフィック、もしくは両方を混在させることができます。
- DMVPN の Per-Tunnel QoS 機能は、次をサポートしません。
 - DMVPN 経由の IPv4、IPv6、または MPLS (マルチプロトコル ラベル スイッチング) VPN の Per-Tunnel QoS と レイヤ 2 トンネルプロトコル (L2TP) トランスポート。

◦ ポートチャネル インターフェイスまたは集約ポートチャネル インターフェイスでの DMVPN 経由の IPv4、IPv6、または MPLS VPN の Per-Tunnel QoS。

- Per-Tunnel QoS サービス ポリシーは出力方向でのみサポートされます。
- この機能では、クリプトエンジンの前にユーザがキューイングおよびスケジューリングを設定できる機能の追加はサポートされません。
- IP アドレスが変わらない外部ヘッダーが個々のフローキューの選択に使用されるため、均等化キューイングは DMVPN の Per-Tunnel QoS ポリシー マップでは使用しないでください。均等化キューイングを使用すると、そのクラスを通過するすべてのトラフィックに対して同じキューが選択されることになります。
- QoS サービス ポリシーは、DMVPN トンネル インターフェイスで Per-Tunnel QoS サービス ポリシーとともにトンネルが発信される、メインインターフェイスまたはサブインターフェイスでサポートされます。ただし、メインまたはサブインターフェイスのサービス ポリシーについては、次のような一定の制限があります。
 - サービス ポリシーは、Per-Tunnel QoS サービス ポリシーとともにメイン インターフェイスまたはサブインターフェイスのいずれかでサポートされますが、両方ではサポートされません。
 - メイン インターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、クラスデフォルトのシェーパのみに制限されます（含めることができるのは **class** **class-default** コマンドと **shape** コマンドのみです）。2 つの異なる QoS サービス ポリシーがメインインターフェイスまたはサブインターフェイスとトンネル インターフェイスに同時に適用されている場合、QoS 設定をメインインターフェイスまたはサブインターフェイスに追加できません。
 - メイン インターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、トンネル インターフェイスのサービス ポリシーより先に適用する必要があります。
 - メインインターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、QoS サービス ポリシーをトンネル インターフェイスに適用したときにのみ有効性が確認されます。メインインターフェイスまたはサブインターフェイスのサービス ポリシーは、トンネルの移動または変更時にはチェックされません。
 - メイン インターフェイスまたはサブインターフェイスのポリシー マップに新しいクラスまたは機能を追加する操作はサポートされていません。新しいクラスまたは機能が CLI でブロックされることはありませんが、予期しない動作を引き起こす可能性があります。
 - メイン インターフェイスまたはサブインターフェイスのサービス ポリシーに対する **policy-map** カウンタ（**show policy-map interface** コマンドで出力される）では、すべてのパケットが計上されない場合があるため、使用または参照しないでください。ただし、これによって QoS 機能が影響を受けることはありません。この場合も、メインインターフェイスまたはサブインターフェイス上のトラフィック（そのインターフェイス上のすべての DMVPN トンネルトラフィックを含む）は、シェーパによって制限されます。

DMVPN の Per-Tunnel QoS について

DMVPN の Per-Tunnel QoS の概要

Dynamic Multipoint VPN (DMVPN) の Per-Tunnel QoS 機能を使用すると、トンネル別インスタンス（スポーク別ベース）で DMVPN ハブからスポークへのトンネルの出力方向で、DMVPN ハブに Quality of Service (QoS) ポリシーを適用できます。トンネル別インスタンスの DMVPN ハブに対する QoS ポリシーにより、各スポークにトンネルトラフィックをシェーピングし（親ポリシー）、ポリシングのためにトンネルを通る個別のデータフローを区別（子ポリシー）できます。特定のスポークにハブが使用する QoS ポリシーは、そのスポークが設定されている特定の NHRP (Next Hop Resolution Protocol) グループに基づいて選択されます。同じ NHRP グループに複数のスポークを設定できますが、各スポークのトンネルトラフィックは個別に測定されてシェーピングおよびポリシングされます。

この機能は、インターネットプロトコルセキュリティ (IPSec) を使用するかどうかにかかわらず、DMVPN で使用できます。

DMVPN の Per-Tunnel QoS 機能をイネーブルにすると、総称ルーティングカプセル化 (GRE) /IPsec トンネルパケットのアウトバウンド物理インターフェイスでキューイングとシェーピングが実行されます。DMVPN の Per-Tunnel QoS 機能を使用すると、QoS でのパケットのシェーピングと帯域幅キューイングに関するパケットサイズの計算に GRE ヘッダー、IPsec ヘッダー、レイヤ2（物理インターフェイス用）ヘッダーが含まれるようになります。

DMVPN の Per-Tunnel QoS の利点

DMVPN の Per-Tunnel QoS 機能を導入する前に、すべてのスポークの集約された発信トラフィックまたはスポーク別（手動による各種の設定が必要）の発信トラフィックのいずれかのみを測定するように、Dynamic Multipoint VPN (DMVPN) ハブの Quality of Service (QoS) を設定することができます。

DMVPN の Per-Tunnel QoS 機能には次の利点があります。

- QoS ポリシーが DMVPN ハブにアタッチされ、トンネルトラフィックをマッチングする基準が各スポークレジスタとして自動的にハブで設定される（手動による各種の設定が不要）。
- ハブからスポークへのトラフィックをスポーク別に制限できる。
- ハブは過剰なトラフィックを小さなスポークに送信（およびオーバーラン）できない。
- 「使用量の多い」スポークが使うアウトバウンドハブ帯域幅の量を制限できるため、トラフィックによってハブのリソースが独占されて他のスポークがリソースを使えなくなる事態を回避できる。

DMVPN の NHRP QoS プロビジョニング

Next Hop Resolution Protocol (NHRP) は、NHRP グループを使用して DMVPN の Per-Tunnel QoS 機能をプロビジョニングします。

NHRP グループはこの機能で導入された新機能で、Dynamic Multipoint VPN (DMVPN) ノード（スポーク）によって DMVPN ハブに伝送されるグループ ID 情報です。ハブはこの情報を使って、ローカルで定義されている、リモート ノードの Quality of Service (QoS) ポリシー インスタンスを選択します。

DMVPN 総称ルーティングカプセル化 (GRE) トンネルインターフェイス上のスポーク ルータで NHRP グループを設定できます。NHRP グループ名は、スポークからハブに定期的に送信される NHRP 登録要求ごとにハブに送信されます。

NHRP グループと QoS ポリシーのマッピングは、ハブ DMVPN GRE トンネルインターフェイスで設定されます。スポークから受信された NHRP グループストリングは、ハブツースポーク トンネルに出力方向で適用される QoS ポリシーにマッピングされます。

スポークに NHRP グループを設定しても、ハブにはすぐに送信されません。次の定期登録要求時に送信されます。スポークは、GRE トンネルインターフェイスごとに 1 つの NHRP グループのみに属することができます。スポークを複数の DMVPN ネットワーク（複数の GRE トンネルインターフェイス）の一部として設定する場合は、GRE トンネルインターフェイスごとに異なる NHRP グループ名をスポークに設定できます。

スポークから NHRP グループが受信されない場合は QoS ポリシーが適用されず、そのスポークにすでに適用されている QoS ポリシーはすべて削除されます。前の NHRP 登録で NHRP グループが受信されていない場合にスポークから NHRP グループが受信されると、対応する QoS ポリシーが適用されます。以前の NHRP 登録要求と同じ NHRP グループをスポークから受信した場合、そのスポークにはすでに QoS ポリシーが適用されていることになるため、何も実行されません。前の NHRP 登録要求時とは異なった NHRP グループをスポークから受信すると、適用されている QoS ポリシーはすべて削除され、新しい NHRP グループに対応した QoS ポリシーが適用されます。

スポーク間接続のトンネルごとの QoS

QoS : DMVPN のスポーク間 Per-Tunnel QoS 機能により、DMVPN クライアントは Next Hop Resolution Protocol (NHRP) を使用してスポークツースポーク接続を構築し、トンネル別 QoS ポリシーを使用している別の DMVPN クライアントとのダイレクトクリプト トンネルを確立できます。

この機能によって適応型 QoS over DMVPN 機能が拡張され、使用可能な帯域幅に基づく動的シェーパを使って効率的に帯域幅を管理できるようになります。

スポークツースポーク接続は、**nhrp attribute group** コマンドを使用してスポークで設定されたグループ ID 情報が、NHRP ベンダー プライベート拡張 (VPE) によってスポーク間で交換されるときに確立されます。NHRP ベンダー プライベート拡張は、NHRP 制御パケット (NHRP 解決要求および応答のパケット) にカプセル化されています。

ネットワークの 2 つのスポーク（スポーク A とスポーク B）がハブに接続されているとします。スポーク A に **nhrp attribute group** コマンドが設定され、スポーク A とスポーク B の間にトラ

フィックが存在する場合、スポーク A からの解決要求にベンダー プライベート拡張 (VPE) の一部としてグループ ID 情報が含まれます。スポーク B は解決要求を受信すると、VPE ヘッダーを抽出し、解決要求パケットの一部として受信した拡張タイプを確認します。VPE 拡張にグループタイプが含まれている場合、NHRP VPE パーサーでグループ情報が抽出され、一致するマップが存在するかどうかを確認されます。一致するマップが見つかったら、QoS は対象のインターフェイスでポリシーを適用します。

DMVPN の Per-Tunnel QoS の設定方法

DMVPN の Per-Tunnel QoS 機能を設定するには、スポークに Next Hop Resolution Protocol (NHRP) グループを定義し、その NHRP グループをハブの Quality of Service (QoS) ポリシーにマッピングします。

スポークでの NHRP グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel number**
4. 次のいずれか 1 つを入力します。
 - **ip nhrp group group-name**
 - **nhrp group group-name**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# 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。

	コマンドまたはアクション	目的
ステップ 3	interfacetunnelnumber 例 : Device(config)# interface tunnel 1	トンネルインターフェイスを設定し、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ます。
ステップ 4	次のいずれか 1 つを入力します。 • ipnhrpgroupgroup-name • nhrpgroupgroup-name 例 : Device(config-if)# ip nhrp group spoke_group1 例 : Device(config-if)# nhrp group spoke_group1	スポークに Next Hop Resolution Protocol (NHRP) グループを設定します。
ステップ 5	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

スポークでの NHRP グループ属性の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interfacetunnelnumber**
4. **nhrpgroupgroup-name**
5. **nhrpattributegroupgroup-name**
6. **nhrpmapgroupgroup-nameservice-policyoutputqos-policy-map-name**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# 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 3	interfacetunnelnumber 例 : Device(config)# interface tunnel 1	トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	nhrpgroupgroup-name 例 : Device(config-if)# nhrp group spoke_group1	スポークに Next Hop Resolution Protocol (NHRP) グループを設定します。
ステップ 5	nhrpattributegroupgroup-name 例 : Device(config-if)# nhrp group attribute spokel	スポークに QoS グループ ID 情報を設定します。
ステップ 6	nhrpmapgroupgroup-nameservice-policyoutputqos-policy-map-name 例 : Device(config-if)# nhrp map group spoke_group1 service-policy output group1_parent	Quality of Service (QoS) ポリシーマッピングに Next Hop Resolution Protocol (NHRP) グループを追加します。
ステップ 7	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ハブの QoS ポリシーへの NHRP グループのマッピング

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel number**
4. 次のいずれかを実行します。
 - **ip nhrp map group group-name service-policy output qos-policy-map-name**
 - **nhrp map group group-name service-policy output qos-policy-map-name**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# 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 3	interface tunnel number 例 : Device(config)# interface tunnel 1	トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかを実行します。 • ip nhrp map group group-name service-policy output qos-policy-map-name • nhrp map group group-name service-policy output qos-policy-map-name 例 : Device(config-if)# ip nhrp map group spoke_group1 service-policy output group1_parent	ハブの Quality of Service (QoS) ポリシー マッピングに Next Hop Resolution Protocol (NHRP) グループを追加します。

	コマンドまたはアクション	目的
	例 : <pre>Device(config-if)# nhrp map group spoke_group1 service-policy output group1_parent</pre>	
ステップ 5	end 例 : <pre>Device(config-if)# end</pre>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN の Per-Tunnel QoS の確認

手順の概要

1. **enable**
2. **showdmvpndetail**
3. **show ip nhrp**
4. **showipnhrpgroup** *[group-name]*
5. 次のいずれかを実行します。
 - **showipnhrpgroup-map** *[group-name]*
 - **shownhrpgroup-map** *[group-name]*
6. **showpolicy-mapmultipoint** *[tunnel tunnel-interface-number]*
7. **showtunnelendpoints**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : <pre>Device> enable</pre>	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	showdmvpndetail 例 : <pre>Device# show dmvpn detail</pre>	各セッションの Dynamic Multipoint VPN (DMVPN) 詳細情報（ネクストホップサーバ (NHS) および NHS のステータス、暗号セッション情報、ソケットの詳細など）を表示します。

	コマンドまたはアクション	目的
		出力には、スポークから受信した Next Hop Resolution Protocol (NHRP) グループ、およびスポーク トンネルに適用されている Quality of Service (QoS) ポリシーが含まれます。
ステップ 3	show ip nhrp 例 : Device# show ip nhrp	NHRP キャッシュと、スポークから受信した NHRP グループを表示します。
ステップ 4	show ip nhrp group [group-name] 例 : Device# show ip nhrp group	NHRP グループ マッピングを表示します。 出力には、関連付けられた QoS ポリシーの名前とその QoS ポリシーを使用しているトンネル エンドポイントのリストが含まれます。
ステップ 5	次のいずれかを実行します。 show ip nhrp group-map [group-name] show nhrp group-map [group-name] 例 : Device# show ip nhrp group-map group1-parent 例 : Device# show nhrp group-map group1-parent	ハブで設定されているグループとポリシーのマップ、および QoS ポリシーが適用されているトンネルを表示します。
ステップ 6	show policy-map multipoint [tunnel tunnel-interface-number] 例 : Device# show policy-map multipoint tunnel 1	マルチポイント トンネルに適用されている QoS ポリシーの詳細を表示します。
ステップ 7	show tunnel endpoints 例 : Device# show tunnel endpoints	マルチポイント トンネルの送信元および宛先エンドポイントに関する情報、およびスポーク トンネルで適用されている QoS ポリシーを表示します。

DMVPN の Per-Tunnel QoS の設定例

例：スポークでの NHRP グループの設定

次の例では、3 つのスポークに 2 つの Next Hop Resolution Protocol (NHRP) グループを設定する方法を示します。

1 番目のスポークの設定

```
interface tunnel 1
ip address 209.165.200.225 255.255.255.224
no ip redirects
ip mtu 1400
ip nhrp authentication testing
ip nhrp group spoke_group1
ip nhrp map 209.165.200.226 203.0.113.1
ip nhrp map multicast 203.0.113.1
ip nhrp network-id 172176366
ip nhrp holdtime 300
ip tcp adjust-mss 1360
ip nhrp nhs 209.165.200.226
tunnel source fastethernet 2/1/1
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
ip address 203.0.113.2 255.255.255.0
```

2 番目のスポークの設定

```
interface tunnel 1
ip address 209.165.200.227 255.255.255.224
no ip redirects
ip mtu 1400
ip nhrp authentication testing
ip nhrp group spoke_group1
ip nhrp map 209.165.200.226 203.0.113.1
ip nhrp map multicast 203.0.113.1
ip nhrp network-id 172176366
ip nhrp holdtime 300
ip tcp adjust-mss 1360
ip nhrp nhs 209.165.200.226
tunnel source fastethernet 2/1/1
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
ip address 203.0.113.3 255.255.255.0
```

3 番目のスポークの設定

```
interface tunnel 1
ip address 209.165.200.228 255.255.255.224
no ip redirects
ip mtu 1400
ip nhrp authentication testing
ip nhrp group spoke_group2
ip nhrp map 209.165.200.226 203.0.113.1
ip nhrp map multicast 203.0.113.1
ip nhrp network-id 172176366
ip nhrp holdtime 300
```

```
ip tcp adjust-mss 1360
ip nhrp nhs 209.165.200.226
tunnel source fastethernet 2/1/1
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
ip address 203.0.113.4 255.255.255.0
```

例：スポークでの NHRP グループ属性の設定

次の例では、2つのスポークに2つの Next Hop Resolution Protocol (NHRP) グループ属性を設定する方法を示します。

1 番目のスポークの設定

```
class-map match-any class2
match ip precedence 5
end
!
policy-map p2
class class2
priority percent 60
end
!
interface Tunnel0
ip address 10.0.0.2 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication hlthere
ip nhrp attribute group1
ip nhrp map group group1 service-policy output p2
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 253
ip nhrp nhs 10.0.0.1
ip nhrp registration timeout 600
ip nhrp cache non-authoritative
no ip mroute-cache
tunnel source 172.17.0.2
tunnel mode gre multipoint
tunnel key 253
tunnel protection ipsec profile dmvpn-profile
end
```

2 番目のスポークの設定

```
class-map match-any class1
match ip precedence 5

policy-map policy p1
class class1
priority 70

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication hlthere
ip nhrp attribute group1
ip nhrp map group group1 service-policy output p1
ip nhrp map multicast 172.17.0.2
ip nhrp map 10.0.0.2 172.17.0.2
ip nhrp network-id 253
ip nhrp nhs 10.0.0.2
ip nhrp registration timeout 600
ip nhrp cache non-authoritative
no ip mroute-cache
```

```

tunnel source 172.17.0.1
tunnel mode gre multipoint
tunnel key 253
tunnel protection ipsec profile dmvpn-profile
end

```

例：ハブの QoS ポリシーへの NHRP グループのマッピング

次の例では、ハブの Quality of Service (QoS) ポリシーに Next Hop Resolution Protocol (NHRP) グループをマッピングする方法を示します。この例に示す階層型 QoS ポリシー（親：group1_parent/group2_parent、子：group1/group2）は、Dynamic Multipoint VPN (DMVPN) の Per-Tunnel QoS 機能の設定に使用されます。またこの例では、ハブで、NHRP グループ spoke_group1 を QoS ポリシー group1_parent に、NHRP グループ spoke_group2 を QoS ポリシー group2_parent にそれぞれマップする方法も示しています。

```

class-map match-all group1_Routing
match ip precedence 6
class-map match-all group2_Routing
match ip precedence 6
class-map match-all group2_voice
match access-group 100
class-map match-all group1_voice
match access-group 100
policy-map group1
class group1_voice
priority 1000
class group1_Routing
bandwidth percent 20
policy-map group1_parent
class class-default
shape average 3000000
service-policy group1
policy-map group2
class group2_voice
priority percent 20
class group2_Routing
bandwidth percent 10
policy-map group2_parent
class class-default
shape average 2000000
service-policy group2
interface tunnel 1
ip address 209.165.200.225 255.255.255.224
no ip redirects
ip mtu 1400
ip nhrp authentication testing
ip nhrp map multicast dynamic
ip nhrp map group spoke_group1 service-policy output group1_parent
ip nhrp map group spoke_group2 service-policy output group2_parent
ip nhrp network-id 172176366
ip nhrp holdtime 300
ip nhrp registration unique
tunnel source fastethernet 2/1/1
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
ip address 209.165.200.226 255.255.255.224

```

例 : DMVPN の Per-Tunnel QoS の確認

次の例では、スポークから受信された Next Hop Resolution Protocol (NHRP) グループに関する情報と、各スポークトンネルに適用されている Quality of Service (QoS) ポリシーを表示する方法を示します。このコマンドはハブで実行できます。

```
Device# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
=====
Interface Tunnel1 is up/up, Addr. is 209.165.200.225, VRF ""
  Tunnel Src./Dest. addr: 209.165.200.226/MGRE, Tunnel VRF ""
  Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
Type:Hub, Total NBMA Peers (v4/v6): 3
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb  Target Network
-----
1      209.165.200.227      192.0.2.2      UP 00:19:20      D      192.0.2.2/32
NHRP group: spoke_group1
  Output QoS service-policy applied: group1_parent
1      209.165.200.228      192.0.2.3      UP 00:19:20      D      192.0.2.3/32
NHRP group: spoke_group1
  Output QoS service-policy applied: group1_parent
1      209.165.200.229      192.0.2.4      UP 00:19:23      D      192.0.2.4/32
NHRP group: spoke_group2
  Output QoS service-policy applied: group2_parent
Crypto Session Details:
=====
Interface: tunnel1
Session: [0x04AC1D00]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.227/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1 id: 209.165.200.227
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.227
    Active SAs: 2, origin: crypto map
    Outbound SPI : 0x9B264329, transform : ah-sha-hmac
    Socket State: Open
Interface: tunnel1
Session: [0x04AC1C08]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.228/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1 id: 209.165.200.228
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.228
    Active SAs: 2, origin: crypto map
    Outbound SPI : 0x36FD56E2, transform : ah-sha-hmac
    Socket State: Open
Interface: tunnel1
Session: [0x04AC1B10]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.229/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1 id: 209.165.200.229
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.229
    Active SAs: 2, origin: crypto map
    Outbound SPI : 0xAC96818F, transform : ah-sha-hmac
    Socket State: Open
Pending DMVPN Sessions:
```

次に、スポークから受信された NHRP グループに関する情報を表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show ip nhrp

192.0.2.240/32 via 192.0.2.240
  Tunnel1 created 00:22:49, expire 00:01:40
```

```

Type: dynamic, Flags: registered
NBMA address: 209.165.200.227
  Group: spoke_group1
192.0.2.241/32 via 192.0.2.241
  Tunnel1 created 00:22:48, expire 00:01:41
Type: dynamic, Flags: registered
NBMA address: 209.165.200.228
  Group: spoke_group1
192.0.2.242/32 via 192.0.2.242
  Tunnel1 created 00:22:52, expire 00:03:27
Type: dynamic, Flags: registered
NBMA address: 209.165.200.229
  Group: spoke_group2

```

次に、ハブの NHRP グループ マッピングの詳細、およびマッピングで定義されている各 NHRP グループを使用しているトンネルのリストを表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show ip nhrp group-map
```

```

Interface: tunnel1
  NHRP group: spoke_group1
  QoS policy: group1_parent
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  198.51.100.220/203.0.113.240
  198.51.100.221/203.0.113.241
  NHRP group: spoke_group2
  QoS policy: group2_parent
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  198.51.100.222/203.0.113.242

```

次に、トンネルエンドポイントに適用されている特定の QoS ポリシーに関する統計情報を表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show policy-map multipoint
```

```

Interface tunnel1 <--> 203.0.113.252
  Service-policy output: group1_parent
  Class-map: class-default (match-any)
    29 packets, 4988 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
      queue limit 750 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 3000000, bc 12000, be 12000
      target shape rate 3000000
  Service-policy : group1
    queue stats for all priority classes:
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
  Class-map: group1_voice (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: access-group 100
    Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0
  Class-map: group1_Routing (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 6
    Queueing
      queue limit 150 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 20% (600 kbps)
  Class-map: class-default (match-any)
    29 packets, 4988 bytes

```



```

    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    queue limit 350 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
Interface tunnel1 <--> 203.0.113.253
    Service-policy output: group1_parent
Class-map: class-default (match-any)
    29 packets, 4988 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
    queue limit 750 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 3000000, bc 12000, be 12000
    target shape rate 3000000
Service-policy : group1
    queue stats for all priority classes:
        queue limit 250 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
    Class-map: group1_voice (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: access-group 100
        Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0
    Class-map: group1_Routing (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: ip precedence 6
        Queueing
        queue limit 150 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        bandwidth 20% (600 kbps)
    Class-map: class-default (match-any)
        29 packets, 4988 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any
        queue limit 350 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
Interface tunnel1 <--> 203.0.113.254
    Service-policy output: group2_parent
Class-map: class-default (match-any)
    14 packets, 2408 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any
    Queueing
    queue limit 500 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 2000000, bc 8000, be 8000
    target shape rate 2000000
Service-policy : group2
    queue stats for all priority classes:
        queue limit 100 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
    Class-map: group2_voice (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: access-group 100
        Priority: 20% (400 kbps), burst bytes 10000, b/w exceed drops: 0
    Class-map: group2_Routing (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: ip precedence 6
        Queueing
        queue limit 50 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0

```

```

bandwidth 10% (200 kbps)
Class-map: class-default (match-any)
  14 packets, 2408 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any
queue limit 350 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

```

DMVPN の Per-Tunnel QoS の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IP NHRP コマンド	『Cisco IOS IP Addressing Services Command Reference』
基本的なシスコ エクスプレス フォワーディングの設定	『IP Switching Cisco Express Forwarding Configuration Guide』
NHRP の設定	『IP Addressing: NHRP Configuration Guide』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DMVPN の Per-Tunnel QoS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1 : DMVPN の Per-Tunnel QoS の機能情報

機能名	リリース	機能情報
Per-Tunnel QoS	Cisco IOS XE Release 3.11S	DMVPN の Per-Tunnel QoS 機能は、DMVPN のトンネルごとの QoS サポートを提供し、IPSec トンネル インターフェイスのトンネルごとの QoS パフォーマンスを向上させます。 Cisco IOS XE Release 3.11S では、この機能が強化されて IPv6 アドレスがサポートされるようになりました。 次のコマンドが導入または変更されました。ip nhrp group、ip nhrp map、ip nhrp map group、nhrp group、nhrp map group、show dmvpn、show ip nhrp、show ip nhrp group-map、show nhrp group-map、show policy-map multipoint tunnel
QoS : DMVPN のスポーク間 Per-Tunnel QoS	Cisco IOS XE Release 3.15S	QoS : DMVPN のスポーク間 Per-Tunnel QoS 機能により、DMVPN クライアントは Next Hop Resolution Protocol (NHRP) を使用してスポークツースポーク接続を構築し、トンネル別 QoS ポリシーを使用している別の DMVPN クライアントとのダイレクトクリプトトンネルを確立できます。 次のコマンドが導入または変更されました。nhrp attribute group、show dmvpn、show ip nhrp、show ip nhrp group