



T コマンド

ここでは、[T] から始まる Cisco NX-OS ユニキャスト ルーティング コマンドについて説明します。

template (BGP)

ピア テンプレートを作成し、ピア テンプレート コンフィギュレーションモードを開始するには、**template** コマンドを使用します。ピア テンプレートを削除するには、このコマンドの **no** 形式を使用します。

```
template {peer name | peer-policy name | peer-session name}
```

```
no template {peer name | peer-policy name | peer-session name}
```

シンタックスの説明

peer name	ネイバー テンプレート名を指定します。
peer-policy name	ピアポリシー テンプレート名を指定します。
peer-session name	ピアセッション テンプレート名を指定します。

コマンドのデフォルト設定

このコマンドにはデフォルト設定がありません。

コマンド モード

ネイバー アドレスファミリ コンフィギュレーション
ルータ BGP コンフィギュレーション

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

template コマンドを使用すると、ネイバーが継承する一連の定義済みアトリビュートをイネーブルにできます。



(注)

Boarder Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) ネイバーを、ピア グループとピア テンプレートの両方と連動するように設定することはできません。BGP ネイバーは、ピア グループに属するか、ポリシーをピア テンプレートから継承するようには設定できません。

ピア テンプレートでは、基本ポリシー コマンドのみサポートされます。特定のアドレス ファミリまたは NLRI コンフィギュレーション モードに限定して設定される BGP ポリシー コンフィギュレーション コマンドを、ピア テンプレートを使用して設定します。

ピア テンプレート

ピア テンプレートでは、ピアセッション テンプレートとピアポリシー テンプレートを組み合わせてネイバーの基本的な定義を行います。ネイバー テンプレートを使用するのは必須ではありませんが、使用すれば BGP の設定が簡略化できます。

ピアポリシー テンプレート

ピアポリシー テンプレートは、複数のコマンド設定をグループ化し、それを特定のアドレスファミリ内および NLRI コンフィギュレーションモード内で適用するために使用します。ピアポリシー テンプレートの作成および設定は、ピア ポリシー コンフィギュレーションモードで行います。特定のアドレス ファミリまたは NLRI コンフィギュレーション モードに対して設定する BGP ポリシー コマンドは、ピア テンプレートに設定します。ピアポリシー テンプレート コンフィギュレーションモードを開始すると、次のコマンドが使用できます。

- **suppress-inactive** — アクティブ ルートをピアのみにアドバタイズします。詳しくは **suppress-inactive** コマンドを参照してください。
- **exit** — 現在のコンフィギュレーションモードを終了します。
- **filter-list name {in | out}** — 着信および発信 BGP ルートに関する AS-PATH フィルタリストを作成します。エントリを削除するには、このコマンドの **no** 形式を使用します。
 - **in** — アクセス リストを着信ルートに適用します。
 - **out** — アクセス リストを発信ルートに適用します。
- **inherit peer-policy policy-name seq-num** — 別のピアポリシー テンプレートの設定を継承するように、ピアポリシー テンプレートを設定します。ピアポリシー テンプレートから、継承文を削除するには、このコマンドの **no** 形式を使用します。範囲：1 ~ 65535。デフォルト：継承文は設定されていません。

ピアポリシー テンプレートを評価する順序は、シーケンス番号で決まります。ルートマップのシーケンス番号と同じように、最も低いシーケンス番号が最初に評価されます。ピアポリシー テンプレートでは継承がサポートされており、ピアはピアポリシー テンプレートを7つまで直接または間接的に継承できます。ルート マップと同じように、継承されたピアポリシー テンプレートにはシーケンス番号が設定されます。ルート マップと同じように、継承したピアポリシー テンプレートは最も低いシーケンス番号を持つ継承文が最初に評価されます。ただし、ピアポリシー テンプレートが抜けることはありません。すべてのシーケンスが評価されます。BGP ポリシー コマンドが異なる値で再び適用された場合は、より低いシーケンス番号による以前の値が上書きされます。



(注)

BGP ルーティング プロセスをピア グループのメンバーにすると同時に、ピア テンプレートをグループ設定に使用するように設定することはできません。どちらか一方の設定を使用する必要があります。パフォーマンスとスケーラビリティが向上するため、ピア テンプレートを推奨します。

- **maximum-prefix max** — このネイバーからの最大プレフィクス数を指定します。範囲：1 ~ 300000。デフォルト：デフォルトでは、このコマンドはディセーブルです。最大プレフィクス数を超えると、ピアリングセッションはディセーブルになります。詳しくは **maximum-prefix** コマンドを参照してください。
- **next-hop-self** — ルータを BGP ネイバーまたはピア グループのネクストホップとして設定します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。デフォルト：ディセーブル
- **next-hop-third-party** — 可能であればサードパーティ ネクストホップを計算します。
- **no** — コマンドを無効にするか、またはデフォルト設定にします。
- **prefix-list name {in | out}** — プレフィクス リストを適用するルート タイプを指定します。エントリを削除するには、このコマンドの **no** 形式を使用します。
 - **in** — プレフィクス リストを着信ルートに適用します。
 - **out** — プレフィクス リストを発信ルートに適用します。
- **route-map name {in | out}** — ネイバーに適用するルート タイプを適用するルート マップ名を指定します。
 - **in** — ルート マップを着信ルートに適用します。
 - **out** — ルート マップを発信ルートに適用します。
- **route-reflector-client** — ルータを BGP ルート リフレクタとして設定し、指定のネイバーをそのクライアントとして設定します。ネイバーがクライアントでないことを示すには、このコマンドの **no** 形式を使用します。デフォルト：Autonomous System (AS; 自律システム) にルート リフレクタは存在しません。

デフォルトでは、AS 内のすべての **internal BGP (iBGP)** スピーカーを完全なメッシュ型にする必要があります。またネイバーは **iBGP** で学習したルートを再度ネイバーにアドバタイズすることはしません。これにより、ルーティング情報のループを防いでいます。すべてのクライアントがディセーブルになると、ローカル ルータはルート リフレクタでなくなります。

ルート リフレクタを使用する場合は、すべての **iBGP** スピーカーを完全なメッシュ型にする必要はありません。ルート リフレクタ モデルでは、1 つの **iBGP** ピアをルート リフレクタに設定します。このルート リフレクタは **iBGP** で学習したルートを **iBGP** ネイバーに渡す役割があります。この方式を使用することで、各ルータが他のすべてのルータと通信する必要がなくなります。

このコマンドで設定されたネイバーはすべてがクライアント グループのメンバーになり、残りの **iBGP** ピアはローカルルート リフレクタの非クライアント グループのメンバーになります。

- **send-community** — コミュニティ アトリビュートを BGP ネイバーに送信するように指定します。エントリを削除するには、このコマンドの **no** 形式を使用します。
- **soft-reconfiguration** — アップデートの格納を開始するように Cisco NX-OS ソフトウェアを設定します。受信したアップデートを格納しないようにするには、このコマンドの **no** 形式を使用します。デフォルト：ディセーブル。このコマンドを入力すると、アップデートの格納が開始されます。これは着信ソフト再設定を行うために必要です。BGP 発信ソフト再設定では、着信ソフト再設定をイネーブルにする必要はありません。

事前設定をすることなくソフト再設定 (ソフト リセット) を使用するには、両方の BGP ピアがソフト ルート リフレッシュ機能をサポートしている必要があります。この機能は、ピアが TCP セッションを確立する際に送信する **OPEN** メッセージに格納されてアドバタイズされます。**soft-reconfiguration** コマンドを使用して BGP セッションをクリアするとネットワークの動作に悪影響があるため、最後の手段として使用してください。

BGP ルータがこの機能をサポートしているかどうかを確認するには、**show ip bgp neighbors** コマンドを使用します。ルータがルート リフレッシュ機能をサポートしている場合は、次のメッセージが表示されます。

```
Received route refresh capability from peer.
```

peer-group-name 引数を使用して BGP ピア グループを指定すると、ピア グループのすべてのメンバーが、このコマンドで設定される特性を継承します。

ピアセッション テンプレートと同じように、ピアポリシー テンプレートを一度設定してから、ピアポリシー テンプレートを直接適用する方法か、ピアポリシー テンプレートから継承する方法で多くのネイバーに適用します。ピアポリシー テンプレートを設定すると、AS 内のすべてのネイバーに適用する BGP ポリシー コマンドの設定を簡略化できます。

ピアポリシー テンプレートでは、8 つまでのピアポリシー テンプレートからの直接および間接的な継承がサポートされます。継承されたピアポリシー テンプレートには、ルート マップと同じようにシーケンス番号が設定されます。ルート マップと同じように、継承したピアポリシー テンプレートは最も低いシーケンス番号を持つ継承文が最初に評価され、最も高いシーケンス番号の継承文が最後に評価されます。ただし、ピアポリシー テンプレートが抜けることのない点がルート マップと異なります。すべてのシーケンスが評価され、BGP ポリシー コマンドが異なる値で再び適用された場合は、より低いシーケンス番号による以前の値が上書きされます。

ピアポリシー テンプレートでは、基本ポリシー コマンドのみサポートされます。特定のアドレスファミリまたは NLRI コンフィギュレーション モードに限定して設定される BGP ポリシー コンフィギュレーション コマンドを、ピアポリシー テンプレートを使用して設定します。



(注)

BGP ネイバーを、ピア グループとピア テンプレートの両方と連動するように設定することはできません。BGP ネイバーは、ピア グループに属するか、ピア テンプレートからポリシーを継承するようにしか設定できません。

ピアセッション テンプレート

ピアセッション テンプレートは、複数の基本セッション コマンドの設定をグループ化し、それを同じセッション設定要素を持つネイバー グループに適用するために使用します。異なるアドレスファミリ内に設定されているネイバーに共通する基本セッション コマンドは、同じピアセッション テンプレート内に設定できます。ピアセッション テンプレートの作成および設定は、ピアセッション コンフィギュレーションモードで行います。ピアセッション テンプレートには、基本セッション コマンドのみ設定できます。

ピアセッション テンプレート コンフィギュレーションモードを開始すると、次のコマンドが使用できます。

- **description** *description* — ローカルまたはピア ルータに表示される説明を設定します。スペースを含めて 80 文字まで入力できます。
- **disable-connected-check** — eBGP ピアにループバック インターフェイスが設定されているときは、1 ホップだけ離れた eBGP ピアの接続検証をディセーブルにします。
- **ebgp-multihop** — 直接接続されていないネットワーク上に存在する外部ピアとの BGP による接続を受け入れたり、接続を試行します。



(注)

このコマンドを使用する場合は、必ずシスコのテクニカルサポート担当者の指示に従ってください。

- **exit** — 現在のコンフィギュレーションモードを終了します。
- **inherit peer-session** *session-name* — 別のピアセッション テンプレートの設定を継承するようにピアセッション テンプレートを設定するには、**peer-session** キーワードを使用します。ピアセッション テンプレートから継承文を削除するには、このコマンドの **no** 形式を使用します。
- **local-as** — eBGP ピア グループの AS 番号のカスタマイズを可能にします。

- **neighbor inherit peer-session** — ネイバーで設定を継承できるように、ルータがピアセッション テンプレートを送信するように設定します。
- **neighbor translate-update** — マルチプロトコル BGP をサポートできるように、NLRI 形式で BGP を稼働するルータをアップグレードします。
- **password** — 2 つの BGP ピア間の TCP 接続において MD5 認証をイネーブルにします。次の設定ツールを使用できます。
 - **0 password** — 非暗号化ネイバー パスワードを指定します。
 - **3 password** — 3DES 暗号化ネイバー パスワードを指定します。
 - **password** — 非暗号化しない (クリアテキスト) ネイバー パスワードを指定します。
- **remote-private-as** — プライベート AS 番号を発信アップデートから削除します。
- **show ip bgp template peer-policy** — ローカルで設定されているピアポリシー テンプレートを表示します。
- **show ip bgp template peer-session** — ローカルで設定されているピアセッションテンプレートを表示します。
- **shutdown** — ネイバーまたはピアグループをディセーブルにします。
- **timers keepalive-time** — キープアライブ タイマーおよびホールド タイマーの値を秒数で設定します。範囲: 0 ~ 3600。デフォルト: 60
- **update-source {ethernet mod/port | loopback virtual-interface | port-channel number[.sub-interface]}** — BGP セッションおよびアップデートの発信元を指定します。範囲: *virtual-interface* は 0 ~ 1023、*number* は 0 ~ 4096、(任意) *.sub-interface* は 1 ~ 4093 です。

基本セッション コマンドをピアセッション テンプレートに一度設定してから、ピアセッション テンプレートを直接適用する方法か、ピアセッション テンプレートから間接的に継承する方法で多くのネイバーに適用できます。ピアセッション テンプレートを設定すると、AS 内のすべてのネイバーに通常適用される基本セッション コマンドの設定を簡略化できます。

ピアセッション テンプレートでは、直接および間接的な継承がサポートされます。ピアを設定する場合は、1 回に 1 つのピアセッション テンプレートしか使用できません。また、そのピアセッション テンプレートは、間接的に継承されたピアセッション テンプレートを 1 つしか含むことができます。ただし、継承された各セッション テンプレートも、間接的に継承されたピアセッション テンプレートを 1 つ含むことができます。したがって、直接適用されるピアセッション テンプレートが 1 つだけと、そのほかに間接的に継承されるピアセッション テンプレートが 7 つまで適用できるので、直接継承されるピアセッション テンプレートからの設定と、7 つまでの間接的に継承されるピアセッション テンプレートからの設定を加えて、最大 8 つのピアセッション 設定を 1 つのネイバーに適用できます。継承されたピアセッション テンプレートが最初に評価され、直接適用されるテンプレートは最後に評価され、適用されます。したがって、基本セッション コマンドが異なる値で再び適用される場合は、あとの値が優先され、間接的に継承されたテンプレートに設定されていた前の値は上書きされます。

ピアセッション テンプレートでは、基本セッション コマンドのみサポートされます。特定のアドレス ファミリーまたは NLRI コンフィギュレーション モードに限定して設定される BGP ポリシー コンフィギュレーション コマンドを、ピアポリシー テンプレートを使用して設定します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、CORE1 という名前のピアセッション テンプレートを作成する例を示します。この例では、INTERNAL-BGP という名前のピアセッション テンプレートの設定が継承されます。

```
switch(config-router)# template peer-session CORE1
switch(config-router-stmp)#
```

次に、CUSTOMER-A という名前のピアポリシー テンプレートの作成と設定を行う例を示します。

```
switch(config-router)# template peer-policy CUSTOMER-A
switch(config-router-ptmp)# exit
switch(config-router)# route-map SET-COMMUNITY in
switch(config-router)# filter-list 20 in
switch(config-router)# inherit peer-policy PRIMARY-IN 20
switch(config-router)# inherit peer-policy GLOBAL 10
switch(config-router)# exit-peer-policy
switch(config-router)#
```

次に、ネイバー 192.168.1.1 から受け入れる最大プレフィクス数を 1000 に設定する例を示します。

```
switch(config)# router bgp 40000
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 1000
```

次に、ネイバー 192.168.2.2 から受け入れる最大プレフィクス数を 5000 に設定する例を示します。さらに、このルータを、最大プレフィクス制限の 50% (プレフィクス数 2500) に達すると警告メッセージを表示するように設定します。

```
switch(config)# router bgp 40000
switch(config-router) network 192.168.0.0
switch(config-router)# maximum-prefix 5000 50
```

次に、ネイバー 192.168.3.3 から受け入れる最大プレフィクス数を 2000 に設定する例を示します。さらに、このルータを、ディセーブルにしたピアリング セッションを 30 分後に再確立するようにも設定します。

```
switch(config)# router bgp 40000
switch(config-router) network 192.168.0.0
switch(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

次に、ネイバー 192.168.4.4 の最大プレフィクス制限 (500) を超過した場合に、警告メッセージを表示するように設定する例を示します。

```
switch(config)# router bgp 40000
switch(config-router)# network 192.168.0.0
switch(config-router)# maximum-prefix 500 warning-only
```

次に、10.108.1.1 向けのすべてのアップデートに対し、このルータをネクストホップとしてアドバタイズするように設定する例を示します。

```
switch(config)# router bgp 40000
switch(config-router)# next-hop-self
```

次に示すルータ コンフィギュレーションモードの例では、ルータが AS 109 に属しており、IP アドレス 172.16.70.23 のネイバーにコミュニティ アトリビュートを送信するように設定します。

```
switch(config)# router bgp 40000
switch(config-router)# send-community
```

次に示すアドレス ファミリ コンフィギュレーションモードの例では、ルータが AS 109 に属しており、IP アドレス 172.16.70.23 のネイバーにコミュニティ アトリビュートを送信するように設定します。

```
switch(config)# router bgp 400
switch(config-router)# address-family ipv4 multicast
switch(config-router-af)# send-community
```

次に、ネイバー 10.108.1.1 の着信ソフト再設定をイネーブルにする例を示します。このネイバーから受信されるすべてのアップデートは、着信ポリシーを無視してそのまま格納されます。あとになって着信ソフト再設定が行われるときは、格納されている情報を使用して新しい着信アップデートのセットが生成されます。

```
switch(config)# router bgp 100  
switch(config-router)# soft-reconfiguration inbound
```

関連コマンド

コマンド	説明
router bgp	ルータに割り当てる AS 番号を入力し、ルータ BGP コンフィギュレーションモードを開始します。
address-family	BGP のアドレス ファミリ モードを開始します。

test forwarding distribution perf

Forwarding Information Base (FIB; 転送情報ベース) 転送分散のパフォーマンスをテストするには、**test forwarding distribution perf** コマンドを使用します。

test forwarding distribution perf

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード すべて

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、転送分散のパフォーマンスをテストする例を示します。

```
switch# test forwarding distribution perf
```

関連コマンド	コマンド	説明
	show forwarding distribution	FIB に関する情報を表示します。

test forwarding inconsistency

Forwarding Information Base (FIB) のレイヤ 3 整合性チェッカーをトリガーするには、**test forwarding inconsistency** コマンドを使用します。

```
test forwarding inconsistency [ip | ipv4] [unicast] [vrf vrf-name] [module {slot| all}] [stop]
```

シンタックスの説明	
<i>ip</i>	(任意) IP ルートの整合性チェックを指定します。
<i>ipv4</i>	(任意) IPv4 ルートの整合性チェックを指定します。
<i>unicast</i>	(任意) ユニキャスト ルートの整合性チェックを指定します。
<i>module</i>	(任意) 1 つまたは複数のモジュールの整合性チェックを指定します。
<i>slot</i>	モジュール番号。範囲はプラットフォームに依存します。
all	(任意) すべてのモジュールの整合性チェックを指定します。
stop	(任意) 整合性チェックを停止します。

デフォルト なし

コマンドモード すべて

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、すべてのモジュールのレイヤ 3 整合性チェッカーをトリガーする例を示します。

```
switch# test forwarding inconsistency module all
```

次に、すべてのモジュールのレイヤ 3 整合性チェッカーを停止する例を示します。

```
switch# test forwarding inconsistency module all stop
```

関連コマンド	コマンド	説明
	show forwarding distribution	FIB に関する情報を表示します。

timers (GLBP)

Gateway Load Balancing Protocol (GLBP) ゲートウェイにより送信される hello パケットの間隔、および仮想ゲートウェイと仮想フォワーダ情報が有効とみなされる時間を設定するには、**timers** コマンドを使用します。各タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
timers [msec] hellotime [msec] holdtime
```

```
no timers
```

シンタックスの説明	
<i>msec</i>	(任意) 下記の (<i>hellotime</i> または <i>holdtime</i>) 引数値をミリ秒で表すことを指定します。
<i>hellotime</i>	hello 間隔。有効範囲は 1 ~ 60 秒です。デフォルトは 3 秒 (3000 ミリ秒) です。
<i>holdtime</i>	hello パケットに含まれる仮想ゲートウェイおよび仮想フォワーダの情報が無効とみなされるまでの時間。有効範囲は 2 ~ 180 秒です。デフォルトは 10 秒 (10,000 ミリ秒) です。

デフォルト

```
hellotime : 3 秒
holdtime  : 10 秒
```

コマンドモード

GLBP コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

タイマーをゲートウェイに設定しなかった場合、ゲートウェイはタイマー値を Active Virtual Gateway (AVG; アクティブバーチャルゲートウェイ) から学習します。AVG 上に設定されているタイマーは、他のすべてのタイマー設定を常に上書します。GLBP グループ内のすべてのゲートウェイが同じタイマー値を使用するようにしてください。GLBP ゲートウェイが hello メッセージを送信した場合、その情報は 1 ホールドタイムの間有効とみなされます。通常、ホールドタイムは hello タイムの値の 3 倍より大きくします ($holdtime > 3 \times hellotime$)。ホールドタイムの値範囲は、ホールドタイムを強制的に hello タイムより大きくします。

このコマンドにはライセンスは必要ありません。

例

次に、イーサネット インターフェイス 1/1 上で GLBP グループ 10 のタイマーを設定する例を示します。

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers 5 18
```

関連コマンド

コマンド	説明
glbp	GLBP コンフィギュレーションモードを開始し、GLBP グループを作成します。
timers redirect	GLBP グループのリダイレクト値およびタイムアウト値を設定します。

timers active-time

アクティブ状態に対する Enhanced Interior Gateway Routing Protocol (EIGRP) 制限時間を調整するには、**timers active-time** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
timers active-time [time-limit | disabled]
```

```
no timers active-time
```

シンタックスの説明	
<i>time-limit</i>	(任意) アクティブ制限時間 (分)。範囲は 1 ~ 65535 分です。デフォルトは 3 です。
<i>disabled</i>	(任意) タイマーをディセーブルにし、ルーティング待機時間を無制限にアクティブのままにします。

デフォルト ディセーブル

コマンド モード アドレスファミリー コンフィギュレーション
ルータ コンフィギュレーション
ルータ VRF コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン ルートが Stack in Active (SIA) 状態であると宣言するまでに、ルータが (クエリー送信後の応答を) 待機する時間を制御するには、**timers active-time** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、指定した EIGRP ルートに無制限のルーティング待機時間を設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers active-time disabled
```

timers basic

Routing Information Protocol (RIP) のネットワーク タイマーを調整するには、ルータ アドレスファミリー コンフィギュレーションモードで **timers basic** コマンドを使用します。デフォルト タイマーに戻すには、このコマンドの **no** 形式を使用します。

```
timers basic update invalid holddown flush
```

```
no timers basic
```

シンタックスの説明

<i>update</i>	アップデートが送信されるレート (秒)。デフォルトは 30 秒です。
<i>invalid</i>	ルートが無効として宣言されるまでの時間 (秒)。 <i>update</i> 引数の値の少なくとも 3 倍に設定します。アップデートでルートがリフレッシュされないと、ルートは無効になります。そのあとルートはホールドダウン (<i>holddown</i>) 状態に入り、アクセス不能としてマーク付けされ到達不能としてアドバタイズされます。ただし、このルートはパケットの転送には引き続いて使用されます。デフォルトは 180 秒です。
<i>holddown</i>	より適切なパスに関するルーティング情報が抑制される時間 (秒)。 <i>update</i> 引数の値の少なくとも 3 倍にします。ルートが到達不能であることを示すアップデート パケットを受信すると、そのルートはホールドダウン (<i>holddown</i>) 状態に入ります。ルートはアクセス不能としてマーク付けされ、到達不能としてアドバタイズされます。ただし、このルートはパケットの転送には引き続いて使用されます。ホールドダウンの期限が切れると、他の発信元によりアドバタイズされるルートが受け入れられ、ルートはアクセス不能でなくなります。デフォルトは 180 秒です。
<i>flush</i>	この時間 (秒) が経過すると、ルートはルーティング テーブルから削除されます。指定する時間は、 <i>invalid</i> 引数と <i>holddown</i> 引数を加えた合計値より大きな値にします。値が合計値より少ないと <i>holddown</i> の時間が正しく経過できないため、 <i>holddown</i> の期限が切れる前に新しいルートが受け入れられる結果になります。デフォルトは 240 秒です。

デフォルト

```
update : 30 秒
invalid : 180 秒
holddown : 180 秒
flush : 240 秒
```

コマンドモード

ルータ アドレスファミリー コンフィギュレーション

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

RIP の基本タイミング パラメータは変更できます。これらのタイマーは、ネットワーク内のすべてのルータおよびサーバで同じ値にする必要があります。



(注)

show ip protocols コマンドを使用すると、現在およびデフォルトのタイマー値を表示できます。

このコマンドにはライセンスは必要ありません。

例 次に、アップデートを 5 秒ごとにブロードキャストするように設定する例を示します。Cisco NX-OS は、15 秒（無効時間）経過してもルータから何も受信しない場合、そのルートを使用不能として宣言します。Cisco NX-OS はさらに 15 秒間（ホールドダウン時間）情報を抑制します。抑制時間が終了すると、Cisco NX-OS はルーティングテーブルからルートを削除します。

```
switch(config)# router rip Enterprise  
switch(config-router)# address-family ipv4 unicast  
switch(config-router-af)# timers basic 5 15 15 30
```

関連コマンド

コマンド	説明
<i>address-family</i>	アドレスファミリー コンフィギュレーションモードを開始します。

timers lsa-arrival (OSPF)

ソフトウェアが Open Shortest Path First (OSPF) ネイバーから同一の Link-State Advertisement (LSA; リンクステートアドバタイズメント) を受け入れる最小間隔を設定するには、**timers lsa-arrival** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timers lsa-arrival *milliseconds*

no timers lsa-arrival

シンタックスの説明	<i>milliseconds</i> ネイバーから到着する同一の LSA を受け入れる間に、経過する必要がある最小遅延時間(ミリ秒)。範囲は 10 ~ 600,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
------------------	---

デフォルト	1000 ミリ秒
--------------	----------

コマンドモード	ルータ コンフィギュレーション VRF コンフィギュレーション
----------------	------------------------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンド履歴	リリース 変更内容
	4.0(1) このコマンドが導入されました。

使用上のガイドライン	同一の LSA を受け入れる最小間隔を設定するには、 timers lsa arrival コマンドを使用します。同一の LSA とは、同一の LSA ID 番号、LSA タイプ、およびアドバタイジング ルータ ID を含んでいる LSA インスタンスのことです。設定した間隔よりも早く同一の LSA インスタンスが到着した場合、ソフトウェアはその LSA をドロップします。
-------------------	---

timers lsa-arrival コマンドの *milliseconds* 値は、ネイバーの **timers throttle lsa** コマンドの *hold-interval* 値以下にすることを推奨します。

このコマンドには、Enterprise Services ライセンスが必要です。

例	次に、同一の LSA を受け入れる最小間隔を 2000 ミリ秒に設定する例を示します。
----------	---

```
switch(config)# router ospf 1
switch(config-router)# timers lsa-arrival 2000
```

関連コマンド	コマンド	説明
	show ip ospf timers rate-limit	レート制限キュー内のすべての LSA を表示します。
	timers throttle lsa	生成されている LSA のレート制限値を設定します。

timers lsa-arrival (OSPFv3)

ソフトウェアが Open Shortest Path First version 3 (OSPFv3) ネイバーから同一の Link-State Advertisement (LSA; リンクステート アドバタイズメント) を受け入れる最小間隔を設定するには、**timers lsa-arrival** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timers lsa-arrival *milliseconds*

no timers lsa-arrival

シンタックスの説明

milliseconds ネイバーから到着する同一の LSA を受け入れる間に、経過する必要がある最小遅延時間(ミリ秒)。範囲は 10 ~ 600,000 ミリ秒です。デフォルトは 1000 ミリ秒です。

デフォルト

1000 ミリ秒

コマンドモード

ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

同一の LSA を受け入れる最小間隔を設定するには、**timers lsa arrival** コマンドを使用します。同一の LSA とは、同一の LSA ID 番号、LSA タイプ、およびアドバタイジング ルータ ID を含んでいる LSA インスタンスのことです。設定した間隔よりも早く同一の LSA インスタンスが到着した場合、ソフトウェアはその LSA をドロップします。

timers lsa-arrival コマンドの *milliseconds* 値は、ネイバーの **timers throttle lsa** コマンドの *hold-interval* 値以下にすることを推奨します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、同一の LSA を受け入れる最小間隔を 2000 ミリ秒に設定する例を示します。

```
switch(config)# router ospfv3 1
switch(config-router)# timers lsa-arrival 2000
```

関連コマンド

コマンド	説明
show ospfv3 timers rate-limit	レート制限キュー内のすべての LSA を表示します。
timers throttle lsa	生成されている LSA のレート制限値を設定します。

timers lsa-group-pacing (OSPF)

Open Shortest Path First (OSPF) Link-State Advertisement (LSA; リンクステート アドバタイズメント) を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更するには、**timers lsa-group-pacing** コマンドを実行します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timers lsa-group-pacing seconds

no timers lsa-group-pacing

シンタックスの説明	<i>seconds</i> LSA のグループ化、リフレッシュ、チェックサム、またはエージングを行う間隔 (秒)。有効範囲は 1 ~ 1800 秒です。デフォルト値は 240 秒です。				
デフォルト	このコマンドのデフォルト間隔は 240 秒です。OSPF の LSA グループ ペーシングはデフォルトでイネーブルです。				
コマンド モード	ルータ コンフィギュレーション VRF コンフィギュレーション				
サポートされるユーザロール	ネットワーク管理者 VDC 管理者				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	4.0(1)	このコマンドが導入されました。
リリース	変更内容				
4.0(1)	このコマンドが導入されました。				

使用上のガイドライン LSA アップデートの発生レートを制御し、大量の LSA でエリアがフラッディングされた時に発生する可能性のある高い CPU 利用率またはバッファ利用率を低減するには、**timers lsa-group-pacing** コマンドを使用します。OSPF の通常の導入の場合は、OSPF パケット ペーシング タイマーのデフォルト設定で十分です。OSPF パケット フラッディングの要件を満たす他のすべてのオプションを試みたあとでなければ、このパケット ペーシング タイマーを変更しないでください。集約、スタブエリアの使用、キューの調整、およびバッファの調整を試したあとで、デフォルトのフラッディング タイマーを変更するようにしてください。タイマー値を変更する際のガイドラインはありません。OSPF の導入に同じものはなく、状況ごとに検討する必要があります。

Cisco NX-OS は LSA の定期リフレッシュをグループ化して、大規模トポロジにおけるリフレッシュの LSA パッキング密度を向上させています。グループ タイマーは LSA をグループ リフレッシュする間隔を制御しますが、このタイマーでは個々の LSA をリフレッシュする頻度 (デフォルトのリフレッシュ レートは 30 分) は変わりません。

LSA グループ ペーシングの時間は、ルータが処理する LSA 数に反比例します。たとえば、約 10,000 個の LSA が存在する場合は、ペーシング間隔を減らすようにしてください。データベースが非常に小さい (40 ~ 100 個の LSA) 場合は、ペーシング間隔を 10 ~ 20 分に増やすようにしてください。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、OSPF ルーティング プロセス 1 で、LSA グループ間の OSPF グループ パケットペーシング アップデートを 60 秒間隔で行うように設定する例を示します。

```
switch(config)# router ospf 1
switch(config-router)# timers lsa-group-pacing 60
```

関連コマンド

コマンド	説明
show ip ospf	OSPF ルーティング プロセスに関する一般的な情報を表示します。

timers lsa-group-pacing (OSPFv3)

Open Shortest Path First version 3 (OSPFv3) Link-State Advertisement (LSA; リンクステートアドバタイズメント) を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更するには、**timers lsa-group-pacing** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timers lsa-group-pacing seconds

no timers lsa-group-pacing

シンタックスの説明

seconds LSA のグループ化、リフレッシュ、チェックサム、またはエージングを行う間隔 (秒)。有効範囲は 1 ~ 1800 秒です。デフォルト値は 240 秒です。

デフォルト

このコマンドのデフォルト間隔は 240 秒です。OSPFv3 の LSA グループ ペーシングはデフォルトでイネーブルです。

コマンド モード

ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

LSA アップデートの発生レートを制御し、大量の LSA でエリアがフラッディングされた時に発生する可能性のある高い CPU 利用率またはバッファ利用率を低減するには、**timers lsa-group-pacing** コマンドを使用します。OSPFv3 の通常の導入の場合は、OSPFv3 パケット ペーシング タイマーのデフォルト設定で十分です。OSPFv3 パケット フラッディングの要件を満たす他のすべてのオプションを試みたあとでなければ、このパケット ペーシング タイマーを変更しないでください。集約、スタブエリアの使用、キューの調整、およびバッファの調整を試したあとで、デフォルトのフラッディング タイマーを変更するようにしてください。タイマー値を変更する際のガイドラインはありません。OSPFv3 の導入に同じものではなく、状況ごとに検討する必要があります。

Cisco NX-OS は LSA の定期リフレッシュをグループ化して、大規模トポロジにおけるリフレッシュの LSA パッキング密度を向上させています。グループ タイマーは LSA をグループ リフレッシュする間隔を制御しますが、このタイマーでは個々の LSA をリフレッシュする頻度 (デフォルトのリフレッシュ レートは 30 分) は変わりません。

LSA グループ ペーシングの時間は、ルータが処理する LSA 数に反比例します。たとえば、約 10,000 個の LSA が存在する場合は、ペーシング間隔を減らすようにしてください。データベースが非常に小さい (40 ~ 100 個の LSA) 場合は、ペーシング間隔を 10 ~ 20 分に増やすようにしてください。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、OSPFv3 ルーティングプロセス 1 で、LSA グループ間の OSPFv3 グループ パケットペーシング アップデートを 60 秒間隔で行うように設定する例を示します。

```
switch(config)# router ospfv3 1
switch(config-router)# timers lsa-group-pacing 60
```

関連コマンド

コマンド	説明
show ospfv3	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。

timers nsf converge

Enhanced Interior Gateway Routing Protocol (EIGRP) の Nonstop Forwarding (NSF) コンバージェンスの制限時間を調整するには、**timers nsf converge** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

timers nsf converge seconds

no timers nsf converge

シンタックスの説明	<i>seconds</i>	NSF スイッチオーバー後のコンバージェンスの制限時間 (秒)。有効範囲は 60 ~ 180 秒です。デフォルトは 120 です。
------------------	----------------	---

デフォルト	120 秒
--------------	-------

コマンド モード	アドレスファミリー コンフィギュレーション ルータ コンフィギュレーション ルータ VRF コンフィギュレーション
-----------------	---

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン	スイッチオーバー後のコンバージェンスをルータが待機する時間を制御するには、 timers nsf converge コマンドを使用します。
-------------------	--

このコマンドには、Enterprise Services ライセンスが必要です。

例	次に、EIGRP の NSF コンバージェンス時間を設定する例を示します。
----------	---------------------------------------

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf converge 100
```

timers nsf route-hold

NSF 認識 Enhanced Interior Gateway Routing Protocol (EIGRP) ルータが非アクティブ ピアのルート
を保持する時間を決定しているタイマーを設定するには、**timers nsf route-hold** コマンドを使用しま
す。このルート ホールドタイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用しま
す。

timers nsf route-hold *seconds*

no timers nsf route-hold

シンタックスの説明

seconds EIGRP が非アクティブ ピアのルート
を保持する時間 (秒)。有効範囲は 20 ~ 300
秒です。デフォルトは 240 です。

デフォルト

EIGRP NSF 認識はイネーブルです。

seconds : 240

コマンドモード

アドレスファミリ コンフィギュレーション
ルータ コンフィギュレーション
ルータ VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

スイッチオーバーの動作時または well-known 障害状態時に NSF 認識ルータが NSF 対応ネイバーの
既知のルート
を保持する最大時間を設定するには、**timers nsf route-hold** コマンドを使用します。
ルート
ホールドタイマーは設定可能なため、ネットワーク パフォーマンスの調整をし、スイッチ
オーバー動作に時間がかかりすぎた場合に「ブラック ホール」ルート (無効ルートのアドバタイ
ズ) などの望ましくない影響を避けることができます。このタイマーの期限が切れると、NSF 認識
ルータはトポロジ テーブルをスキャンし無効なルートを破棄します。これにより EIGRP ピアは、
スイッチオーバー動作中に長い時間待機せずに代替ルートを探すことができます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、NSF 認識ルータのルート ホールドタイマー値を 2 分 (120 秒) に設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf route-hold 120
```

timers nsf signal

Nonstop Forwarding (NSF) 再起動の信号を Enhanced Interior Gateway Routing Protocol (EIGRP) に通知する制限時間を設定するには、**timers nsf signal** コマンドを使用します。このルート ホールド タイマーをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

timers nsf signal seconds

no timers nsf signal

シンタックスの説明	<i>seconds</i>	EIGRP がピアからの NSF 再起動の信号を待機する時間 (秒)。有効範囲は 10 ~ 30 秒です。デフォルトは 20 です。
------------------	----------------	--

デフォルト	EIGRP NSF 認識はイネーブルです。 <i>seconds</i> : 20
--------------	--

コマンドモード	アドレスファミリー コンフィギュレーション ルータ コンフィギュレーション ルータ VRF コンフィギュレーション
----------------	---

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンド履歴	リリース 変更内容
	4.0(1) このコマンドが導入されました。

使用上のガイドライン	NSF 認識ルータが NSF 対応ネイバーからの再起動の信号を待機する最大時間を設定するには、 timers nsf signal コマンドを使用します。
-------------------	--

このコマンドには、Enterprise Services ライセンスが必要です。

例	次に、NSF 認識ルータの信号タイマーを最大値 (30 秒) に設定する例を示します。
----------	---

```
switch(config)# router eigrp 1
switch(config-router) address-family ipv4 unicast
switch(config-router-af)# timers nsf signal 30
```

timers redirect

Gateway Load Balancing Protocol (GLBP) グループの Active Virtual Gateway (AVG; アクティブ バーチャル ゲートウェイ) が継続してクライアントをセカンダリ Active Virtual Forwarder (AVF; アクティブ バーチャル フォワーダ) にリダイレクトする時間を設定するには、**timers redirect** コマンドを使用します。リダイレクト タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers redirect *redirect timeout*

no timers redirect *redirect timeout*

シンタックスの説明

<i>redirect</i>	リダイレクト タイマー時間 (秒)。有効範囲は 0 ~ 3600 秒です。デフォルトは 300 秒 (5 分) です。
<i>timeout</i>	セカンダリ バーチャル フォワーダが使用できなくなるまでの時間 (秒)。有効範囲は 610 ~ 64800 秒です。デフォルトは 14,400 秒 (4 時間) です。

デフォルト

redirect : 300 秒
timeout : 14,400 秒

コマンドモード

GLBP コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

AVG によって仮想 MAC アドレスが割り当てられたバーチャル フォワーダのことを、プライマリ バーチャル フォワーダと呼びます。また、**hello** メッセージから仮想 MAC アドレスを学習したバーチャル フォワーダのことを、セカンダリ バーチャル フォワーダと呼びます。

リダイレクト (**redirect**) タイマーには、ネットワーク上のフォワーダに障害が発生し AVG によりそのフォワーダが復旧しないとみなされた時点に開始される遅延時間を設定できます。遅延時間を設定した場合、フォワーダが応答する仮想 MAC アドレスは Address Resolution Protocol (ARP; アドレス解決プロトコル) 応答の中にまだ存在していますが、実際のフォワーディング タスクは GLBP グループ内の別のグループにより処理されます。

タイムアウト (**timeout**) 時間は、ネットワーク上のフォワーダに障害が発生し、フォワーダが扱っていた MAC アドレスが GLBP グループ内のすべてのルータで非アクティブになった時点に開始される遅延時間です。タイムアウト時間が経過すると、この仮想 MAC アドレスに送信されるパケットは廃棄されます。タイムアウト時間には、仮想 MAC アドレスを含んだ ARP キャッシュ エントリをすべてのホストがリフレッシュできるだけの十分長い時間を設定する必要があります。

このコマンドにはライセンスは必要ありません。

例 次に、イーサネット インターフェイス 1/1 上で GLBP グループ 1 のリダイレクトおよびタイムアウト値を設定する例を示します。

```
switch(config)# interface ethernet 1/1  
switch(config-if)# glbp 10  
switch(config-glbp)# timers redirect 600 7200  
switch(config-glbp)# ip
```

関連コマンド

コマンド	説明
glbp	GLBP コンフィギュレーションモードを開始し、GLBP グループを作成します。
timers	GLBP の hello タイマーおよびホールド タイマーを設定します。

timers redirect

Gateway Load Balancing Protocol (GLBP) グループの Active Virtual Gateway (AVG; アクティブ バーチャル ゲートウェイ) が継続してクライアントをセカンダリ Active Virtual Forwarder (AVF; アクティブ バーチャル フォワーダ) にリダイレクトする時間を設定するには、**timers redirect** コマンドを使用します。リダイレクト タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers redirect *redirect timeout*

no timers redirect *redirect timeout*

シンタックスの説明	
<i>redirect</i>	リダイレクト タイマー時間 (秒)。有効範囲は 0 ~ 3600 秒です。デフォルトは 300 秒 (5 分) です。
<i>timeout</i>	セカンダリ バーチャル フォワーダが使用できなくなるまでの時間 (秒)。有効範囲は 610 ~ 64800 秒です。デフォルトは 14,400 秒 (4 時間) です。

デフォルト
redirect : 300 秒
timeout : 14,400 秒

コマンドモード GLBP コンフィギュレーション

サポートされるユーザロール スーパーユーザ
 VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン AVG によって仮想 MAC アドレスが割り当てられたバーチャル フォワーダのことを、プライマリ バーチャル フォワーダと呼びます。また、hello メッセージから仮想 MAC アドレスを学習したバーチャル フォワーダのことを、セカンダリ バーチャル フォワーダと呼びます。

リダイレクト (**redirect**) タイマーには、ネットワーク上のフォワーダに障害が発生し AVG によりそのフォワーダが復旧しないとみなされた時点に開始される遅延時間を設定できます。遅延時間を設定した場合、フォワーダが応答する仮想 MAC アドレスは Address Resolution Protocol (ARP; アドレス解決プロトコル) 応答の中にまだ存在していますが、実際のフォワーディング タスクは GLBP グループ内の別のグループにより処理されます。

タイムアウト (**timeout**) 時間は、ネットワーク上のフォワーダに障害が発生し、フォワーダが扱っていた MAC アドレスが GLBP グループ内のすべてのルータで非アクティブになった時点に開始される遅延時間です。タイムアウト時間が経過すると、この仮想 MAC アドレスに送信されるパケットは廃棄されます。タイムアウト時間には、仮想 MAC アドレスを含んだ ARP キャッシュ エントリをすべてのホストがリフレッシュできるだけの十分長い時間を設定する必要があります。

このコマンドにはライセンスは必要ありません。

例 次に、イーサネットインターフェイス 1/1 上で GLBP グループ 1 のリダイレクトおよびタイムアウト値を設定する例を示します。

```
switch(config)# interface ethernet 1/1
switch(config-if)# glbp 10
switch(config-glbp)# timers redirect 600 7200
switch(config-glbp)# ip
```

関連コマンド

コマンド	説明
glbp	GLBP コンフィギュレーションモードを開始し、GLBP グループを作成します。
timers	GLBP の hello タイマーおよびホールド タイマーを設定します。

timers throttle lsa (OSPF)

Open Shorterst Path First (OSPF) の Link-State Advertisement (LSA; リンクステートアドバタイズメント) 生成に対するレート制限値を設定するには、**timers throttle lsa** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
timers throttle lsa {network | router} hold-interval
```

```
no timers throttle lsa {network | router}
```

シンタックスの説明

network	ネットワーク LSA のレート制限を指定します。
router	ルータ LSA のレート制限を指定します。
hold-interval	LSA の生成に適用される後続のレート制限の時間計算に使用される増分値 (ミリ秒)。範囲は 1 ~ 600,000 ミリ秒です。デフォルトは 5000 ミリ秒です。

デフォルト

hold-interval : 5000 ミリ秒

コマンドモード

ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

LSA の生成にレート制限を適用するには、**timers throttle lsa** コマンドを使用します。このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、OSPF ネットワーク LSA スロットリングをカスタマイズする例を示します。

```
switch(config)# router ospf 1
switch(config-router)# timers throttle lsa network 10000
```

関連コマンド

コマンド	説明
show ip ospf	OSPF ルーティングプロセスに関する情報を表示します。
timers lsa arrival	ソフトウェアが OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。

timers throttle lsa (OSPFv3)

Open Shortest Path First version 3 (OSPFv3) の Link-State Advertisement (LSA; リンクステートアドバタイズメント) 生成に対するレート制限値を設定するには、**timers throttle lsa** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
timers throttle lsa {intra-area-prefix | link | network | router} hold-interval
```

```
no timers throttle lsa {network | router}
```

シンタックスの説明

intra-area-prefix	エリア内プレフィクス LSA のレート制限を指定します。
link	リンク LSA のレート制限を指定します。
network	ネットワーク LSA のレート制限を指定します。
router	ルータ LSA のレート制限を指定します。
hold-interval	LSA の生成に適用される後続のレート制限の時間計算に使用される増分値 (ミリ秒)。範囲は 1 ~ 600,000 ミリ秒です。デフォルトは 5000 ミリ秒です。

デフォルト

hold-interval : 5000 ミリ秒

コマンドモード

ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

LSA の生成にレート制限を適用するには、**timers throttle lsa** コマンドを使用します。このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、OSPFv3 ネットワーク LSA スロットリングをカスタマイズする例を示します。

```
switch(config)# router ospfv3 1
switch(config-router)# timers throttle lsa network 10000
```

関連コマンド

コマンド	説明
show ospfv3	OSPFv3 ルーティング プロセスに関する情報を表示します。
timers lsa arrival	ソフトウェアが OSPFv3 ネイバーから同一の LSA を受け入れる最小間隔を設定します。

timers throttle spf (OSPF)

Shortest-path First (SPF) 最適パスの最初のスケジュール遅延時間および OSPF の SPF 最適パス計算間の最小ホールド時間を設定するには、**timers throttle spf** コマンドを使用します。SPF スロットリングをオフにするには、このコマンドの **no** 形式を使用します。

```
timers throttle spf spf-start spf-hold spf-max-wait
```

```
no timers throttle spf spf-start spf-hold spf-max-wait
```

シンタックスの説明	
<i>spf-start</i>	初回 SPF スケジュール遅延 (ミリ秒)。範囲は 1 ~ 600000 ミリ秒です。
<i>spf-hold</i>	実行される後続の 2 つの SPF 計算間の最小ホールド時間。範囲は 1 ~ 600000 ミリ秒です。
<i>spf-max-wait</i>	実行される後続の 2 つの SPF 計算間の最大待機時間。範囲は 1 ~ 600000 ミリ秒です。

デフォルト SPF スロットリングは設定されていません。

コマンドモード ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン SPF タイマーを設定するには、**timers throttle spf** コマンドを使用します。

SPF 計算間の初回待機時間は、*spf-start* 引数で指定される時間 (ミリ秒) です。続いて適用される各待機時間は、待機時間が *spf-maximum* 引数で指定される最大時間 (ミリ秒) に達するまで、現在のホールド時間 (ミリ秒) を 2 倍した値になります。それ以降の待機時間は、値がリセットされるか SPF 計算間に LSA を受信するまで最大値のままです。

例 次に、ルータで、**timers throttle spf** コマンドの初回時間、ホールド時間、および最大時間の値をそれぞれ 5、1,000、および 90,000 ミリ秒に設定する例を示します。

```
switch(config)# router ospf 1
switch(config-router)# timers throttle spf 5 1000 90000
```

timers throttle spf (OSPFv3)

Shortest-path First (SPF) 最適パスの最初のスケジュール遅延時間および Open Shortest Path First version 3 (OSPFv3) の SPF 最適パス計算間の最小ホールド時間を設定するには、**timers throttle spf** コマンドを使用します。SPF スロットリングをオフにするには、このコマンドの **no** 形式を使用します。

```
timers throttle spf spf-start spf-hold spf-max-wait
```

```
no timers throttle spf spf-start spf-hold spf-max-wait
```

シンタックスの説明	
<i>spf-start</i>	初回 SPF スケジュール遅延 (ミリ秒)。範囲は 1 ~ 600000 ミリ秒です。
<i>spf-hold</i>	実行される後続の 2 つの SPF 計算間の最小ホールド時間。範囲は 1 ~ 600000 ミリ秒です。
<i>spf-max-wait</i>	実行される後続の 2 つの SPF 計算間の最大待機時間。範囲は 1 ~ 600000 ミリ秒です。

デフォルト SPF スロットリングは設定されていません。

コマンドモード アドレスファミリ コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン SPF タイマーを設定するには、**timers throttle spf** コマンドを使用します。

SPF 計算間の初回待機時間は、*spf-start* 引数で指定される時間 (ミリ秒) です。続いて適用される各待機時間は、待機時間が *spf-maximum* 引数で指定される最大時間 (ミリ秒) に達するまで、現在のホールド時間 (ミリ秒) を 2 倍した値になります。それ以降の待機時間は、値がリセットされるか SPF 計算間に LSA を受信するまで最大値のままです。

例 次に、ルータで、**timers throttle spf** コマンドの初期時間、ホールド時間、および最大時間の値をそれぞれ 5、1,000、および 90,000 ミリ秒に設定する例を示します。

```
switch(config)# router ospfv3 1
switch(config-router)# address-family ipv6 unicast
switch(config-router-af)# timers throttle spf 5 1000 90000
```

track (VRRP)

IPv4 を使用する仮想ルータのためにプライオリティをトラッキングするには、**track** コマンドを使用します。仮想ルータのためのプライオリティ トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
track interface {ethernet interface-num | vlan vlan-num | port-channel channel-group-num} priority value
```

```
no track interface
```

シンタックスの説明

ethernet <i>interface-num</i>	プライオリティ トラッキング対象の仮想ルータ インターフェイス。範囲は 1 ~ 255 です。
vlan <i>vlan-num</i>	プライオリティ トラッキング対象の VLAN
port-channel <i>channel-group-num</i>	プライオリティ トラッキング対象のポートチャネル グループ
priority <i>value</i>	仮想ルータのインターフェイス プライオリティ。値の範囲は 1 ~ 255 です。このルータが IP アドレスのオーナーである場合には、値は自動的に 255 に設定されます。

デフォルト

ディセーブル

コマンド モード

VRRP コンフィギュレーションモード

サポートされるユーザ ロール

スーパーユーザ
VDC 管理者

コマンド履歴

リリース	変更
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

仮想ルータのプライオリティをスイッチ内の別のインターフェイスの状態に基づいて変更するには、**track** コマンドを使用します。トラッキング対象インターフェイスがダウンすると、プライオリティは仮想ルータのプライオリティ値に戻ります。トラッキング対象インターフェイスがアップになると、仮想ルータのプライオリティはインターフェイスの状態をトラッキングする値に戻ります。

このコマンドにはライセンスは必要ありません。



(注)

インターフェイス上でプリエンプトをイネーブルにしないと、インターフェイスの状態をトラッキングすることはできません。

■ track (VRRP)

次に、仮想ルータのためにインターフェイスの状態をトラッキングする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# track interface ethernet 2/2 priority 2
```

関連コマンド

コマンド	説明
feature vrrp	VRRP をイネーブルにします。
show vrrp	VRRP 設定情報を表示します。
clear vrrp	指定の仮想ルータの全ソフトウェア カウンタをクリアします。

track interface

インターフェイス上にオブジェクト トラッキングを設定するには、**track interface** コマンドを使用します。このインターフェイスに対するオブジェクト トラッキングを削除するには、このコマンドの **no** 形式を使用します。

```
track object-id interface interface-type number {ip routing | line-protocol}
no track object-id [force]
```

シンタックスの説明	
<i>object-id</i>	トラッキング ID。範囲は 1 ~ 500 です。
interface <i>interface-type number</i>	トラッキング対象のインターフェイスを指定します。使用可能なインターフェイス タイプの一覧を表示するには、オンライン ? ヘルプを使用します。
ip routing	インターフェイスの IP ルーティングの状態をトラッキングします。
line-protocol	インターフェイスのラインプロトコルの状態をトラッキングします。
force	(任意) オブジェクト トラッキング インスタンスを完全に削除します。

コマンドのデフォルト設定 なし

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン インターフェイスの状態をトラッキングするには、**track interface** コマンドを使用します。このコマンドを使用すると、オブジェクト トラッキング コマンド モードが開始されます。非デフォルト VRF 内のオブジェクトをトラッキングするには、オブジェクト トラッキング コンフィギュレーションモードで **vrf member** コマンドを使用します。

このコマンドにはライセンスは必要ありません。

例 次に、イーサネット インターフェイス 1/2 上の IP ルーティングの状態をトラッキングする例を示します。

```
switch(config)# track 1 interface ethernet 1/2 ip routing
switch(config-track)#
```

関連コマンド	コマンド	説明
	show track	オブジェクト トラッキングに関する情報を表示します。
	track ip route	IP ルートの状態をトラッキングします。
	vrf member	非デフォルト VRF 内のオブジェクトをトラッキングします。

track ip route

IP ルート上にオブジェクト トラッキングを設定するには、**track ip route** コマンドを使用します。このルートのオブジェクト トラッキングを削除するには、このコマンドの **no** 形式を使用します。

```
track object-id ip route ip-prefix/length reachability
```

```
no track object-id [force]
```

シンタックスの説明	
<i>object-id</i>	トラッキング ID。範囲は 1 ~ 500 です。
<i>ip-prefix/length</i>	トラッキング対象のルートのプレフィクス。IP プレフィクスはドット付き 10 進表記 (X.X.X.X) です。長さは 1 ~ 32 です。
reachability	IP ルートの到達可能性をトラッキングします。
force	(任意) オブジェクト トラッキング インスタンスを完全に削除します。

コマンドのデフォルト設定 なし

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン IP ルートの状態をトラッキングするには、**track ip route** コマンドを使用します。このコマンドを使用すると、オブジェクト トラッキング コマンド モードが開始されます。非デフォルト VRF 内のオブジェクトをトラッキングするには、オブジェクト トラッキング コンフィギュレーションモードで **vrf member** コマンドを使用します。

このコマンドにはライセンスは必要ありません。

例 次に、IP ルートをトラッキングする例を示します。

```
switch(config)# track 1 ip route 10.10.10.0/8 reachability
switch(config-track)#
```

関連コマンド	コマンド	説明
	show track	オブジェクト トラッキングに関する情報を表示します。
	track ip route	インターフェイスをトラッキングします。
	vrf member	非デフォルト VRF 内のオブジェクトをトラッキングします。

transmit-delay (OSPF virtual link)

リンクステート アップデート パケットの終了に必要な予想時間をインターフェイスに設定するには、**transmit-delay** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

transmit-delay *seconds*

no transmit-delay

シンタックスの説明	<i>seconds</i>	リンクステート アップデートの送信に必要な時間 (秒)。範囲は 1 ~ 65535 秒です。デフォルトは 1 秒です。
------------------	----------------	---

デフォルト	1 秒
--------------	-----

コマンド モード	仮想インターフェイス コンフィギュレーション
-----------------	------------------------

サポートされるユーザ ロール	ネットワーク管理者 VDC 管理者
-----------------------	----------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン	仮想リンクの送信および伝搬遅延を設定するには、仮想リンク コンフィギュレーションで transmit-delay コマンドを使用します。
-------------------	---

このコマンドには、Enterprise Services ライセンスが必要です。

例	次に、再送信遅延値を 3 秒に設定する例を示します。
----------	----------------------------

```
switch(config)# router ospf 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```

transmit-delay (OSPFv3 virtual link)

リンクステート アップデート パケットの終了に必要な予想時間をインターフェイスに設定するには、**transmit-delay** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

transmit-delay *seconds*

no transmit-delay

シンタックスの説明	<i>seconds</i>	リンクステート アップデートの送信に必要な時間 (秒)。範囲は 1 ~ 65535 秒です。デフォルトは 1 秒です。
------------------	----------------	---

デフォルト	1 秒
--------------	-----

コマンド モード	仮想インターフェイス コンフィギュレーション
-----------------	------------------------

サポートされるユーザ ロール	ネットワーク管理者 VDC 管理者
-----------------------	----------------------

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン	仮想リンクの送信および伝搬遅延を設定するには、仮想リンク コンフィギュレーションで transmit-delay コマンドを使用します。
-------------------	---

このコマンドには、Enterprise Services ライセンスが必要です。

例	次に、再送信遅延値を 3 秒に設定する例を示します。
----------	----------------------------

```
switch(config)# router ospfv3 201
switch(config-router)# area 22 virtual-link 192.0.2.1
switch(config-router-vlink)# transmit-delay 3
```