



Cisco Unified SIP Proxy SIP コマンド

- 「sip network」
 - 「allow-connections」
 - 「header-hide」
 - 「udp max-datagram-size」
 - 「non-invite-provisional」
 - 「retransmit count (SIP ネットワーク)」
 - 「retransmit-timer (SIP ネットワーク)」
- 「sip listen」
- 「sip record-route」
- 「sip max-forwards」
- 「sip header-compaction」
- 「sip overload redirect」
- 「sip overload reject」
- 「sip tcp connection-timeout」
- 「sip tcp max-connections」
- 「sip queue」
 - 「drop-policy」
 - 「low-threshold」
 - 「size」
 - 「thread-count」
- 「sip dns-srv」
 - 「enable (SIP DNS サーバ)」
 - 「use-naptr」
- 「sip alias」
- 「sip logging」
- 「sip peg-counting」
- 「sip privacy trusted-destination」
- 「sip privacy trusted-source」

- 「sip privacy service」
- 「sip tls」
- 「sip tls trusted-peer」
- 「route recursion」

sip network

論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip network** コマンドを使用します。このコマンドの **no** 形式はありません。

sip network network [icmp | nat | noicmp | standard]

構文の説明

| | |
|-----------------|--|
| network | SIP ネットワーク インターフェイスの名前を指定します。 |
| standard | (オプション) 標準 SIP を使用するには、ネットワーク インターフェイスを設定します。ネットワークは UDP に完全に対応しています。ネットワーク インターフェイスは、ICMP、および各エンドポイントで使用できるさまざまなソケットに対応しています。これはデフォルトの設定です。 |
| nat | (オプション) Network Address Translation (NAT) を使用するためのネットワーク インターフェイスを設定します。 |
| icmp | (オプション) インターネット制御メッセージプロトコル (ICMP) を使用するためのネットワーク インターフェイスを設定します。 |
| noicmp | (オプション) 各エンドポイントで別のソケットを使用しないようにネットワーク インターフェイスを指定します。この設定によって、ICMP 以外のエラーがサポートされます。 |

コマンド デフォルト

Standard

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

ネットワーク インターフェイスで使用されるソケットのタイプにはさまざまな特性があります。

- Standard
 - ネットワーク インターフェイスは UDP に完全に対応しています。
 - ネットワーク インターフェイスは ICMP に対応しています。
 - 各エンドポイントでさまざまなソケットを使用できます。
- ICMP
 - ネットワーク インターフェイスは ICMP に対応しています。
- No ICMP
 - ICMP エラーはサポートされません。
 - ネットワークでは各エンドポイントで別のソケットを使用しません。

- NAT
 - ネットワーク インターフェイスは NAT に対応しています。

**注意**

SIP ネットワークの作成後は、SIP ネットワークを削除することはできません。

例

次の例では、標準ネットワークを設定し、SIP ネットワーク コンフィギュレーション モードを開始する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network internal
se-10-0-0-0(cusp-config-network)>
```

次の例では、ICMP に対応するように SIP ネットワークを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external icmp
```

次の例では、ICMP エラーがサポートされないように、SIP ネットワーク インターフェイスを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external noicmp
```

関連コマンド

| コマンド | 説明 |
|--|--|
| allow-connections | TCP/TLS クライアント接続を許可するように、SIP ネットワークを設定します。 |
| header-hide | ヘッダーをマスクするように SIP ネットワークを設定します。 |
| non-invite-provisional | INVITE 以外の要求に対して 100 応答を送信できるようにします。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| show configuration active sip network | 設定された SIP ネットワークを表示します。 |

allow-connections

TCP/TLS クライアント接続を許可するように SIP ネットワークを設定するには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **allow-connections** コマンドを使用します。SIP ネットワークで TCP/TLS 接続を許可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。

allow-connections

no allow-connections

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SIP ネットワークでの TCP/TLS クライアント接続はデフォルトで有効になります。

コマンド モード

Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| バージョン | 変更内容 |
|-------|-----------------|
| 1.0 | このコマンドが追加されました。 |

例

次の例では、「internal」という名前の標準 SIP ネットワークで TCP/TLS 接続を許可する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network internal standard
se-10-0-0-0(cusp-config-network)> allow-connections
```

次の例では、「internal」という名前の標準 SIP ネットワークで TCP/TLS 接続を無効にする方法を示します。

```
se-10-0-0-0(cusp-config)> sip network internal standard
se-10-0-0-0(cusp-config-network)> no allow-connections
```

関連コマンド

| コマンド | 説明 |
|-------------------------------|---|
| header-hide | ヘッダーをマスクするように SIP ネットワークを設定します。 |
| non-invite-provisional | INVITE 以外の要求に対して 100 応答を送信できるようにします。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

header-hide

ヘッダー値をマスクするように SIP ネットワークを設定するには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **header-hide** コマンドを使用します。ヘッダー値をマスクしないように SIP ネットワークを設定するには、このコマンドの **no** 形式を使用します。

header-hide *header-name*

no header-hide *header-name*

構文の説明

header-name ネットワークに対してマスクされるヘッダー名を指定します。

コマンドモード

Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

コマンドデフォルト

ヘッダー値はマスクされません。

使用上のガイドライン

Cisco Unified SIP Proxy バージョン 1.0 の有効なヘッダー名は **via** だけです。

例

次の例では、Via ヘッダーをマスクするように SIP ネットワークを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> header-hide via
```

次の例では、Via ヘッダーをマスクしないように SIP ネットワークを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no header-hide via
```

関連コマンド

| コマンド | 説明 |
|-------------------------------|---|
| non-invite-provisional | INVITE 以外の要求に対して 100 応答を送信できるようにします。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

udp max-datagram-size

このネットワークの UDP データグラムの最大サイズを設定するには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **udp max-datagram-size** コマンドを使用します。UDP 最大データグラム サイズのデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

udp max-datagram-size *size*

no udp max-datagram-size

構文の説明

size ネットワークの UDP データグラムの最大サイズ (バイト単位) を指定します。

コマンド モード

Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.1.4 このコマンドが追加されました。

コマンド デフォルト

udp max-datagram-size : 1500

使用上のガイドライン

ネットワーク上のパケットがこの指定されたサイズよりも大きいとき、ネットワークに対して設定された TCP リスニング ポイントが存在する場合、メッセージは TCP にアップグレードされます。

例

次の例では、このネットワークの UDP データグラムの最大サイズを 2000 バイトに設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> udp max-datagram-size 2000
```

関連コマンド

| コマンド | 説明 |
|-------------------------------|---|
| non-invite-provisional | INVITE 以外の要求に対して 100 応答を送信できるようにします。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

non-invite-provisional

INVITE 以外の要求に対して 100 応答を送信できるようにするには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **non-invite-provisional** コマンドを使用します。INVITE 以外の要求に対して 100 応答を送信でき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。

non-invite-provisional {*TU3-timer-value*}

no non-invite-provisional

構文の説明

TU3-timer-value 使用する TU3 タイマーを指定します。

コマンド デフォルト

INVITE 以外の要求に対して 100 応答は送信できません。

コマンド モード

Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

TU3 送信タイプだけを使用して SIP ネットワークを設定するには、このコマンドを使用します。INVITE 以外の要求に対して 100 応答を送信できないようにする場合、TU3 タイマーを指定する必要があります。

例

次の例では、INVITE 以外の要求に対して 100 応答を送信できるようにし、TU3 タイマー値を 200 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> non-invite-provisional 200
```

次の例では、INVITE 以外の要求に対して 100 応答を送信できないようにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no non-invite-provisional
```

関連コマンド

| コマンド | 説明 |
|--------------------------|---|
| allow-connections | TCP/TLS クライアント接続を許可するように、SIP ネットワークを設定します。 |
| header-hide | ヘッダーをマスクするように SIP ネットワークを設定します。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

retransmit count (SIP ネットワーク)

SIP ネットワークの再送信回数を設定するには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **retransmit-count** コマンドを使用します。再送信回数の値をデフォルトに戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

```
retransmit-count {invite-client-transaction | invite-server-transaction |
non-invite-client-transaction} count_value
```

```
no retransmit-count {invite-client-transaction | invite-server-transaction |
non-invite-client-transaction}
```

```
default retransmit-count {invite-client-transaction | invite-server-transaction |
non-invite-client-transaction}
```

構文の説明

| | |
|--------------------------------------|---|
| invite-client-transaction | INVITE 要求の再送信回数を指定します。デフォルトは 5 です。 |
| invite-server-transaction | INVITE 要求の最終応答の再送信回数を指定します。デフォルトは 9 です。 |
| non-invite-client-transaction | INVITE 以外の要求の再送信回数を指定します。デフォルトは 9 です。 |
| <i>count_value</i> | 再送信回数を指定します。有効な範囲は 0 ~ 127 です。デフォルトは、選択された再送信回数によって異なります。 |

コマンド デフォルト

それぞれの再送信回数タイプのデフォルト値は次のとおりです。

- **invite-client-transaction** : 3
- **invite-server-transaction** : 3
- **non-invite-client-transaction** : 3

コマンド モード

Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

再送信回数の値は、許可される SIP 再送信の最大数を指定します。ネットワークの再送信遅延特性が異なる場合、特定の回数の値を、ネットワークごとに別々に設定できます。SIP による再送信回数の詳細については、RFC 3261 を参照してください。

例

次の例では、INVITE クライアントの再送信回数を 5 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> retransmit-count invite-client-transaction 5
```

■ retransmit count (SIP ネットワーク)

次の例では、クライアントの再送信回数を 18 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> retransmit-count non-invite-client-transaction 18
```

次の例では、INVITE クライアントの回数をデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no retransmit-count invite-client-transaction
```

関連コマンド

| コマンド | 説明 |
|-------------------------------|---|
| allow-connections | TCP/TLS クライアント接続を許可するように、SIP ネットワークを設定します。 |
| header-hide | ヘッダーをマスクするように SIP ネットワークを設定します。 |
| non-invite-provisional | INVITE 以外の要求に対する 100 応答を送信できるようにします。 |
| retransmit-timer | SIP ネットワークの再送信タイマー値を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

retransmit-timer (SIP ネットワーク)

SIP ネットワークの SIP 再送信タイマーの値を設定するには、Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション モードで **retransmit-timer** コマンドを使用します。再送信タイマー値をデフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

```
retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 } timer_value
```

```
no retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 }
```

```
default retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 }
```

構文の説明

| | |
|--------------------|---|
| T1 | 最初の要求の再送信間隔を設定します。デフォルトは 500 ミリ秒です。 |
| T2 | 要求の再送信の最大値を設定します。デフォルトは 4,000 ミリ秒です。 |
| T4 | 要求または応答の再送信を処理するために、完了後に NONINVITE クライアント トランザクションまたは INVITE サーバ トランザクションがアクティブのままになる時間を設定します。デフォルトは 5,000 ミリ秒です。 |
| serverTn | サーバ トランザクションの最大有効期間を設定します。デフォルトは 64,000 ミリ秒です。 |
| clientTn | クライアント トランザクションの最大有効期間を設定します。デフォルトは 64,000 ミリ秒です。 |
| TU1 | 応答の再送信を処理するために、2xx 応答の完了後に INVITE トランザクションがアクティブのままになる時間を設定します。デフォルトは 5,000 ミリ秒です。 |
| TU2 | トランザクションがタイムアウトしたと見なされてから、サーバが INVITE クライアント トランザクションまたは NONINVITE サーバ トランザクションの暫定応答または最終応答を待機する時間を設定します。デフォルトは 32,000 ミリ秒です。 |
| timer_value | 再送信タイマー値を指定します。デフォルト値は、選択された再送信タイマーによって異なります。 |

コマンドデフォルト

それぞれの再送信タイマーのデフォルト値は次のとおりです。

- **T1** : 500 ミリ秒
- **T2** : 4,000 ミリ秒
- **T4** : 5,000 ミリ秒
- **serverTn** : 64,000 ミリ秒
- **clientTn** : 64,000 ミリ秒
- **TU1** : 5,000 ミリ秒
- **TU2** : 32,000 ミリ秒

■ retransmit-timer (SIP ネットワーク)

コマンドモード Cisco Unified SIP Proxy SIP ネットワーク コンフィギュレーション (cusp-config-network)

コマンド履歴 Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン 再送信タイマー値は、SIP 再送信の期間を定義します。ネットワークの再送信遅延特性が異なる場合、特定のタイマーの値を、ネットワークごとに別々に設定できます。SIP による再送信タイマーの詳細については、RFC 3261 を参照してください。

例 次の例では、T1 再送信タイマーを 1,000 ミリ秒に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> retransmit-timer T1 1000
```

次の例では、TU1 再送信タイマーをデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip network external standard
se-10-0-0-0(cusp-config-network)> no retransmit-timer TU1
```

関連コマンド

| コマンド | 説明 |
|-------------------------------|---|
| allow-connections | TCP/TLS クライアント接続を許可するように、SIP ネットワークを設定します。 |
| header-hide | ヘッダーをマスクするように SIP ネットワークを設定します。 |
| non-invite-provisional | INVITE 以外の要求に対して 100 応答を送信できるようにします。 |
| retransmit-count | SIP ネットワークの再送信回数を設定します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip listen

特定の SIP ネットワーク、ホスト、およびポート上の SIP トラフィックをリッスンするリスナーを作成するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip listen** コマンドを使用します。SIP ネットワークからリスナーを削除するには、このコマンドの **no** 形式を使用します。

```
sip listen network_name {tcp | tls | udp} ip_address port
```

```
no sip listen network_name {tcp | tls | udp} ip_address port
```

構文の説明

| | |
|---------------------|---|
| <i>network_name</i> | SIP ネットワーク名を指定します。 |
| tcp | リスナーの転送プロトコルとして TCP が使用されるように指定します。 |
| tls | リスナーの転送プロトコルとして TLS が使用されるように指定します。 |
| udp | リスナーの転送プロトコルとして UDP が使用されるように指定します。これはデフォルトです。 |
| <i>ip_address</i> | 着信要求を受け入れるインターフェイス IP アドレスです。 |
| <i>port</i> | サーバが着信メッセージをリッスンするポートです。有効な範囲は 1024 ~ 65535 です。デフォルト値は 5060 です。 |

コマンド デフォルト

SIP ネットワーク上のリスナーはイネーブルになっていません。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

リスナーは、サーバが着信パケットをリッスンする、インターフェイス、ポート、および転送タプルです。1 台のサーバに複数のリスナーを構成できますが、サーバで SIP トラフィックを受け入れるように少なくとも 1 つのリスナーを構成する**必要があります**。ネットワークには複数のリスナーを構成できません。ネットワークの設定の変更を行う場合に、ネットワーク上のリスナーをディセーブルにする必要はありません。



注意

TCP リスナーおよび TLS リスナーを同じポート上で実行することはできません。



注意

他のすべての設定タスクを完了するまで、**sip listen** コマンドをイネーブルにしないでください。このコマンドをイネーブルにすると、システムでは、指定された SIP ネットワークから着信要求を受信し始めます。

例

次の例では、TCP を使用する「external」という SIP ネットワーク上のリスナーを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip listen external tcp 10.2.3.4 5060
```

次の例では、UDP を使用する「internal」という SIP ネットワーク上のリスナーを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip listen internal udp 192.168.1.3 5061
```

次の例では、SIP ネットワーク上のリスナーをディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip listen external tcp 10.2.3.4 5060
```

関連コマンド

| コマンド | 説明 |
|--------------------|---|
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip record-route

SIP ネットワークのレコードルーティングをイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip record-route** コマンドを使用します。SIP ネットワークのレコードルーティ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。

```
sip record-route network_name {tcp | tls | udp} ip_address [port]
```

```
no sip record-route network_name
```

構文の説明

| | |
|---------------------|--|
| <i>network_name</i> | レコードルート コンフィギュレーションに論理的に関連付けられる、SIP ネットワーク名を (sip network コマンドを使用して設定したように) 指定します。 |
| tcp | TCP により Record-Route ヘッダー フィールドにデータが入力されるように指定します。 |
| tls | TLS により Record-Route ヘッダー フィールドにデータが入力されるように指定します。 |
| udp | UDP により Record-Route ヘッダー フィールドにデータが入力されるように指定します。これはデフォルトです。 |
| <i>ip_address</i> | Record-Route ヘッダー フィールドに入力する、インターフェイス ホスト名または IP アドレスを指定します。 |
| <i>port</i> | (オプション) Record-Route ヘッダー フィールドに入力するポートを指定します。このオプションを指定しない場合、5060 が入力されます。有効な範囲は 1024 ~ 65535 です。 |

コマンド デフォルト

なし

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

レコードルーティングにより、ダイアログ内のすべての SIP メッセージが同じルートを経由することができます。SIP Record-Route ヘッダー フィールドには、メッセージが強制的に目的の SIP エンティティを経由するようにする、コンフィギュレーション インターフェイス、ポート、および転送値が含まれます。レコードルート機能は、サーバグループの SIP トラフィックを管理するロード バランサに、メッセージを送るようにするために重要です。

例

次の例では、「internal」という SIP ネットワークのレコードルーティングをイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip record-route internal udp cuspl.example.com
```

■ sip record-route

次の例では、「external」という SIP ネットワークのレコードルーティングをイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip record-route external tcp 192.168.1.3 5061
```

次の例では、「external」という SIP ネットワークのレコードルーティングをディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip record-route external
```

関連コマンド

| コマンド | 説明 |
|---|--------------------------------|
| show configuration active sip record-route | SIP レコードルート コンフィギュレーションを表示します。 |

sip max-forwards

SIP Max-Forwards ヘッダー フィールドの値を設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip max-forwards** コマンドを使用します。SIP Max-Forwards ヘッダー フィールドから値を削除し、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。

sip max-forwards *max_forward_value*

no sip max-forwards *max_forward_value*

構文の説明

max_forward_value Max-Forwards ヘッダー フィールドの値を指定します。指定できる値は 0 ~ 255 です。デフォルト値は 70 です。

コマンド デフォルト

70

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

SIP 要求の Max-Forwards ヘッダー フィールドは、要求を別のサーバに転送できる最大回数を指定します。要求がサーバによって受信されるたびに、この値が 1 減ります（要求に Max-Forwards ヘッダーがない場合は、値に 1 追加されます）。値が 0 になると、サーバは 483 (Too Many Hops) 応答で応答し、トランザクションを終了します。

Max-Forwards ヘッダー フィールドを使用して、ネットワーク内の転送ループを検出できます。



(注)

このコマンドの値は 10 以上 100 以下に設定することを推奨します。

例

次の例では、SIP Max-Forwards ヘッダー フィールドの値を 100 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip max-forwards 100
```

関連コマンド

| コマンド | 説明 |
|--------------------|---|
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip header-compaction

SIP ヘッダー圧縮をイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip header-compaction** コマンドを使用します。SIP ヘッダー圧縮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。

sip header-compaction

no sip header-compaction

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SIP ヘッダー圧縮はディセーブルです。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

| Cisco Unified SIP Proxy バージョン | 変更内容 |
|-------------------------------|-----------------|
| 1.0 | このコマンドが追加されました。 |

使用上のガイドライン

イネーブルの場合、次の SIP ヘッダーに対して圧縮ヘッダー形式が使用されます。

- Call-ID
- Contact
- Content-Encoding
- Content-Length
- Content-Type
- From
- Subject
- To
- Via

ヘッダー圧縮がディセーブルの場合、ヘッダー形式にかかわらず、すべての発信メッセージで SIP ヘッダー全体が使用されます。

例

次の例では、SIP ヘッダー圧縮をイネーブルにする方法を示します。

```
se-10-0-0-0 (cusp-config) > sip header-compaction
```

次の例では、SIP ヘッダー圧縮をディセーブルにする方法を示します。

```
se-10-0-0-0 (cusp-config) > no sip header-compaction
```

関連コマンド

| コマンド | 説明 |
|--------------------------|---|
| <code>sip network</code> | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip overload redirect

サーバが過負荷状態になったときに 300 (Redirect) 応答を送信するようにサーバを設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip overload redirect** コマンドを使用します。サーバが過負荷状態になったときにリダイレクト応答を送信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。

```
sip overload redirect redirect_ip [port redirect_port] [transport {tcp | tls | udp}]
```

```
no sip overload redirect redirect_ip [port redirect_port] [transport {tcp | tls | udp}]
```

構文の説明

| | |
|----------------------------------|--|
| <i>redirect_ip</i> | SIP Contact ヘッダー フィールドで送信されるリダイレクト インターフェイス ホスト名または IP アドレスです。以降の要求はこのアドレスでサーバにリダイレクトされます。 |
| port <i>redirect_port</i> | (オプション) リダイレクト ホストのポート。有効な範囲は 1024 ~ 65535 です。デフォルトは 5060 です。 |
| transport | (オプション) リダイレクト ホストにより使用される転送プロトコルです。 |
| tcp | TCP を転送プロトコルとして使用します。 |
| tls | TLS を転送プロトコルとして使用します。 |
| udp | UDP を転送プロトコルとして使用します。UDP は、転送プロトコルが選択されていない場合のデフォルト値です。 |

コマンド デフォルト

デフォルト ポートは 5060 で、デフォルトの転送プロトコルは UDP です。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

このコマンドは、サーバが過負荷状態になった場合のサーバの動作を設定します。拒否とリダイレクトという 2 つの動作モードがあります。リダイレクト モードを設定するには、**sip overload redirect** コマンドを使用し、拒否モードを設定するには **sip overload reject** コマンドを使用します。一度に設定できるのは 1 つのモードだけです。

拒否モードが設定されている場合、プロキシはメッセージを拒否し、過負荷状態になった場合には 503 (Server Unavailable) 応答で応答します。

リダイレクト モードが設定されている場合、プロキシはメッセージをリダイレクトし、過負荷状態になった場合には 300 (Redirect) 応答で応答します。

例

次の例では、サーバが過負荷状態になった場合に 300 (Redirect) 応答で応答するようにサーバを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip overload redirect 192.168.20.5 transport udp
```

次の例では、サーバが過負荷状態になった場合の 300 (Redirect) 応答での応答をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip overload redirect 192.168.20.5
```

関連コマンド

| コマンド | 説明 |
|----------------------------|--|
| sip overload reject | サーバが過負荷状態になったときに 503 (Server Unavailable) 応答を送信するようにサーバを設定します。 |

sip overload reject

サーバが過負荷状態になったときに 503 (Server Unavailable) 応答を送信するようにサーバを設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip overload reject** コマンドを使用します。サーバが過負荷状態になったときに拒否応答を送信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。

sip overload reject [retry-after *retry_after_time*]

no sip overload reject [retry-after *retry_after_time*]

構文の説明

retry-after *retry_after_time*

(オプション) 送信者がトランザクションを再度試行できる場合に指定する、503 (Server Unavailable) 応答の SIP Retry-After ヘッダー フィールドの送信秒数。このオプションを指定しない場合、503 (Server Unavailable) 応答に Retry-After ヘッダー フィールドが含まれません。指定できる最小値は 0 です。デフォルト値は 0 です。

コマンド デフォルト

デフォルト値は 0 です。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

このコマンドは、サーバが過負荷状態になった場合のサーバの動作を設定します。拒否とリダイレクトという 2 つの動作モードがあります。リダイレクト モードを設定するには、**sip overload redirect** コマンドを使用し、拒否モードを設定するには **sip overload reject** コマンドを使用します。一度に設定できるのは 1 つのモードだけです。

拒否モードが設定されている場合、プロキシはメッセージを拒否し、過負荷状態になった場合には 503 (Server Unavailable) 応答で応答します。

リダイレクト モードが設定されている場合、プロキシはメッセージをリダイレクトし、過負荷状態になった場合には 300 (Redirect) 応答で応答します。

例

次の例では、サーバが過負荷状態になった場合に 503 (Server Unavailable) 応答を送信するようにサーバを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip overload-reject
```

次の例では、サーバが過負荷状態になった場合に 503 (Server Unavailable) 応答を送信するようにサーバを設定し、**retry-after-time** を 60 秒に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip overload-reject 60
```

次の例では、サーバが過負荷状態になった場合の 503 (Server Unavailable) 応答の送信をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip overload-reject
```

関連コマンド

| コマンド | 説明 |
|------------------------------|--|
| sip overload redirect | サーバが過負荷状態になったときに 300 (Redirect) 応答を送信するようにサーバを設定します。 |

sip tcp connection-timeout

サーバが SIP TCP 接続を開いたままにする時間（分）を設定するには、Cisco Unified SIP Proxy コンフィギュレーションモードで **sip tcp connection-timeout** コマンドを使用します。SIP TCP 接続タイムアウト値をそのデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

sip tcp connection-timeout *timeout_value*

no sip tcp connection-timeout

構文の説明

| | |
|----------------------|---|
| <i>timeout_value</i> | アイドル TCP/TLS 接続が正常に閉じられるまでの時間（分）を指定します。受け入れられる値は 0 以上の値です。デフォルト値は 30 分です。 |
|----------------------|---|

コマンド デフォルト

30 分

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

| Cisco Unified SIP Proxy バージョン | 変更内容 |
|-------------------------------|-----------------|
| 1.0 | このコマンドが追加されました。 |

例

次の例では、SIP TCP 接続タイムアウト値を 120 分に設定する方法を示します。

```
se-10-0-0-0 (cusp-config) > sip tcp connection-timeout 120
```

関連コマンド

| コマンド | 説明 |
|--------------------------------|-----------------------|
| sip tcp max-connections | TCP/TLS 接続の最大数を設定します。 |

sip tcp max-connections

TCP/TLS 接続の最大数を設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip tcp max-connections** コマンドを使用します。システムをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

sip tcp max-connections value

no sip tcp max-connections value

構文の説明

value 許可される TCP/TLS 接続の最大数。デフォルトは 256 で、最小値は 1 です。

コマンド デフォルト

許可される TCP/TLS 接続の最大数は 256 です。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

TCP/TLS 接続が最大数に達した場合、パッシブ（着信）接続は受け入れられず、追加のアクティブ（発信）接続は行うことができます。

例

次の例では、TCP/TLS 接続の最大数を 512 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip tcp max-connections 512
```

関連コマンド

| コマンド | 説明 |
|-----------------------------------|--------------------------------------|
| sip tcp connection-timeout | サーバで SIP TCP 接続を開いたままにする時間（分）を設定します。 |

sip queue

SIP キューのプロパティを設定し、SIP キュー コンフィギュレーション モードを開始するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip queue** コマンドを使用します。SIP キュー コンフィギュレーション サブモードのすべてのプロパティをデフォルトの設定に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

sip queue {message | request | st-callback | ct-callbackresponse | timer | xcl | radius}

no sip queue {message | request | st-callback | ct-callbackresponse | timer | xcl | radius}

default sip queue {message | request | st-callback | ct-callbackresponse | timer | xcl | radius}

構文の説明

| | |
|----------------------------|--|
| message | SIP キュー コンフィギュレーション モードを開始して、メッセージキューのプロパティを設定します。メッセージキューは、トランスポート レイヤから受信される着信 SIP メッセージを管理します。 |
| request | SIP キュー コンフィギュレーション モードを開始して、要求キューのプロパティを設定します。要求キューは、サーバでただちに処理できない着信 SIP 要求を管理します。 |
| st-callback | SIP キュー コンフィギュレーション モードを開始して、st-callback キューのプロパティを設定します。st-callback キューは、サーバトランザクションへの ACK および CANCEL コールバックを管理します。 |
| ct-callbackresponse | SIP キュー コンフィギュレーション モードを開始して、ct-callback キューのプロパティを設定します。ct-callbackresponse キューは、クライアント送信に対するコールバックを管理します。 |
| timer | SIP キュー コンフィギュレーション モードを開始して、タイマー キューのプロパティを設定します。タイマー キューは SIP タイマー イベントを管理します。 |
| xcl | SIP キュー コンフィギュレーション モードを開始して、XCL キューのプロパティを設定します。xcl キューは XCL 要求を管理します。 |
| radius | SIP キュー コンフィギュレーション モードを開始して、RADIUS キューのプロパティを設定します。RADIUS キューは、RADIUS アカウンティング要求を管理します。 |

コマンド デフォルト なし

コマンド モード Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴 Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

ランタイム中に SIP キューがプロキシにより作成されました。キューは、サービスがアクティブになると、デフォルト値を使用してプロキシにより作成されます。キューがまだ存在していない場合、コマンドは失敗します。作成された SIP キューを確認するには、**show status queue** コマンドを使用します。

例

次の例では、SIP キュー コンフィギュレーション モードを開始してタイマー キューを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue timer
se-10-0-0-0(cusp-config-queue)>
```

次の例では、SIP キュー コンフィギュレーション モードを開始して st-callback キューを設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue st-callback
se-10-0-0-0(cusp-config-queue)>
```

次の例では、すべての SIP RADIUS キュー パラメータの設定をそれぞれのデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> no sip queue radius
```

関連コマンド

| コマンド | 説明 |
|--------------------------|---------------------------------|
| drop-policy | SIP キューのドロップ ポリシーを設定します。 |
| low-threshold | SIP キューの low-water-mark を設定します。 |
| show status queue | アクティブな SIP キューの統計情報を表示します。 |
| size | 特定のキューで保持できるメッセージの最大数を設定します。 |
| thread-count | 特定の SIP キューのスレッド数を設定します。 |

drop-policy

SIP キューのドロップ ポリシーを設定するには、Cisco Unified SIP Proxy SIP キュー コンフィギュレーション モードで **drop-policy** コマンドを使用します。設定されたドロップ ポリシーを削除し、デフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

drop-policy {head | tail | none}

no drop-policy {head | tail | none}

default drop-policy {head | tail | none}

構文の説明

| | |
|-------------|---|
| head | 最大キュー サイズに達したら、トランスポート レイヤで最も古いイベントをキューの先頭からドロップするように指示します。これはデフォルト値です。 |
| tail | 最大キュー サイズに達したら、トランスポート レイヤで最も新しいイベントをキューの末尾からドロップするように指示します。 |
| none | トランスポート レイヤで最大キュー サイズの制限を無視し、すべてのイベントを格納するように指示します。 |

コマンド デフォルト

先頭ドロップ ポリシーが使用されます。

コマンド モード

Cisco Unified SIP Proxy SIP キュー コンフィギュレーション (cusp-config-queue)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

例

次の例では、SIP メッセージ キューのドロップ ポリシーを head 設定に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> drop-policy head
```

次の例では、SIP st-callback キューのドロップ ポリシーを tail 設定に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue st-callback
se-10-0-0-0(cusp-config-queue)> drop-policy tail
```

次の例では、RADIUS キューのドロップ ポリシーをバインド解除設定に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> drop-policy none
```

次の例では、RADIUS キューのドロップ ポリシーをデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> no drop-policy
```

関連コマンド

| コマンド | 説明 |
|----------------------|--|
| low-threshold | SIP キューの low-water-mark を設定します。 |
| sip queue | SIP キューを作成し、SIP キュー コンフィギュレーション モードを開始します。 |
| size | 特定のキューで保持できるメッセージの最大数を設定します。 |
| thread-count | 特定の SIP キューのスレッド数を設定します。 |

low-threshold

SIP キューの `low-water-mark` を設定するには、Cisco Unified SIP Proxy SIP キュー コンフィギュレーション モードで **low-threshold** コマンドを使用します。SIP キューから `low-water-mark` の値を削除し、デフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

low-threshold *low-water-mark*

no low-threshold

default low-threshold

構文の説明

low-water-mark 最大キュー サイズの割合を指定します。有効な範囲は 1 ~ 100 です。デフォルトは 80 % です。

コマンド デフォルト

80 %

コマンド モード

Cisco Unified SIP Proxy SIP キュー コンフィギュレーション (cusp-config-queue)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

`low-water-mark` 値は、サーバが過負荷状態であると見なされなくなり、新しいイベントを受け入れ始める容量を指定します。

例

次の例では、SIP メッセージ キューの `low-water-mark` を 100 % に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> low-threshold 100
```

次の例では、RADIUS キューの `low-water-mark` を 50 % に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> low-threshold 50
```

次の例では、`ct-callback` キューの `low-water-mark` をデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue ct-callback
se-10-0-0-0(cusp-config-queue)> no low-threshold
```

関連コマンド

| コマンド | 説明 |
|--------------------|--|
| drop-policy | SIP キューのドロップ ポリシーを設定します。 |
| sip queue | SIP キューを作成し、SIP キュー コンフィギュレーション モードを開始します。 |

| コマンド | 説明 |
|---------------------|------------------------------|
| size | 特定のキューで保持できるメッセージの最大数を設定します。 |
| thread-count | 特定の SIP キューのスレッド数を設定します。 |

size

特定のキューで保持できるメッセージの最大数を設定するには、Cisco Unified SIP Proxy SIP キュー コンフィギュレーション モードで **size** コマンドを使用します。設定された SIP キュー サイズを削除し、デフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

size *queue-size*

no size *queue-size*

default size *queue-size*

構文の説明

| | |
|-------------------|--|
| <i>queue-size</i> | 特定のキューで保持できるメッセージの最大数。有効な範囲は 10 ~ 50,000 です。デフォルトは 2,000 です。 |
|-------------------|--|

コマンド デフォルト

2,000

コマンド モード

Cisco Unified SIP Proxy SIP キュー コンフィギュレーション (cusp-config-queue)

コマンド履歴

| Cisco Unified SIP Proxy バージョン | 変更内容 |
|-------------------------------|-----------------|
| 1.0 | このコマンドが追加されました。 |

使用上のガイドライン



このパラメータをより大きな値に設定する場合、メモリ消費がこのキュー サイズに正比例するため、慎重に判断する必要があります。

例

次の例では、メッセージ キュー サイズを 10,000 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> size 10000
```

次の例では、RADIUS キュー サイズを 5,000 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> size 5000
```

次の例では、RADIUS キュー サイズをデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue radius
se-10-0-0-0(cusp-config-queue)> no size 5000
```

関連コマンド

| コマンド | 説明 |
|----------------------|--|
| drop-policy | SIP キューのドロップ ポリシーを設定します。 |
| low-threshold | SIP キューの low-water-mark を設定します。 |
| sip queue | SIP キューを作成し、SIP キュー コンフィギュレーション モードを開始します。 |
| thread-count | 特定の SIP キューのスレッド数を設定します。 |

thread-count

特定の SIP キューに割り当てられるスレッドの最大数を設定するには、Cisco Unified SIP Proxy SIP キュー コンフィギュレーション モードで **thread-count** コマンドを使用します。SIP キューからスレッド数の値を削除し、デフォルト値に戻すには、このコマンドの **no** 形式または **default** 形式を使用します。

thread-count *thread_count*

no thread-count *thread_count*

default thread-count *thread_count*

構文の説明

| | |
|---------------------|---|
| <i>thread_count</i> | 指定されたキューに割り当てられるスレッドの最大数。指定できる最小値は 1 です。デフォルトは 20 です。 |
|---------------------|---|

コマンド デフォルト

20 個のスレッドが SIP キューに割り当てられます。

コマンド モード

Cisco Unified SIP Proxy SIP キュー コンフィギュレーション (cusp-config-queue)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

例

次の例では、SIP メッセージ キューのスレッド数を 40 に設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> thread-count 40
```

次の例では、メッセージ キュー スレッド数をデフォルト値に戻す方法を示します。

```
se-10-0-0-0(cusp-config)> sip queue message
se-10-0-0-0(cusp-config-queue)> no thread-count 40
```

関連コマンド

| コマンド | 説明 |
|----------------------|--|
| drop-policy | SIP キューのドロップ ポリシーを設定します。 |
| low-threshold | SIP キューの low-water-mark を設定します。 |
| sip queue | SIP キューを作成し、SIP キュー コンフィギュレーション モードを開始します。 |

sip dns-srv

SIP DNS SRV 検索コマンドを設定し、SIP DNS SRV コンフィギュレーション モードを開始するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip dns-srv** コマンドを使用します。すべての DNS SRV コンフィギュレーション サブモード パラメータ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。

sip dns-srv

no sip dns-srv

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

なし

コマンドモード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

特定のホスト名のサーバグループが設定されていない場合、最初に、/etc/hosts を使用した DSN 解決が試行されます。この処理に失敗した場合、DNS lookup が使用されます。SIP DNS SRV コンフィギュレーション サブモードでのコマンドは、DNS NAPTR/SRV lookup 関連情報を設定します。

例

次の例では、SIP DNS SRV コンフィギュレーション モードを開始する方法を示します。

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)>
```

関連コマンド

| コマンド | 説明 |
|-----------------------------|---|
| enable (SIP DNS サーバ) | ドメイン名/IP アドレス マッピングの、DNS サーバ NAPTR または SRV クエリー レコードをイネーブルにします。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |
| use-naptr | ドメイン名/IP アドレス マッピングの、DNS NAPTR の使用をイネーブルにします。 |

enable (SIP DNS サーバ)

ドメイン名/IP アドレス マッピングの、DNS サーバ NAPTR または SRV クエリーの使用をイネーブルにするには、SIP DNS サーバ コンフィギュレーション モードで **enable** コマンドを使用します。DNS サーバ NAPTR または SRV クエリー レコード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。

enable

no enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

DNS サーバ SRV クエリー レコードの使用はディセーブルです。

コマンド モード

SIP DNS サーバ コンフィギュレーション (cusp-config-dns)

コマンド履歴

| Cisco Unified SIP Proxy バージョン | 変更内容 |
|-------------------------------|-----------------|
| 1.0 | このコマンドが追加されました。 |

使用上のガイドライン

このコマンドがディセーブルになっている場合、DNS サーバ NAPTR/SRV レコードの使用はディセーブルになり、オペレーティング システムの DNS コンフィギュレーションを使用して簡易な名前解決だけが実行されます。Cisco Unified SIP Proxy ロード バランシングには DNS SRV (RFC 3263) が使用されます。

例

次の例では、DNS サーバ SRV クエリー レコードの使用をイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> enable
```

次の例では、DNS サーバ SRV クエリー レコードの使用をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> no enable
```

関連コマンド

| コマンド | 説明 |
|--------------------|---|
| sip dns-srv | SIP DNS SRV コンフィギュレーション モードを開始します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |
| use-naptr | ドメイン名/IP アドレス マッピングの、DNS NAPTR の使用をイネーブルにします。 |

use-naptr

ホスト名/IP アドレス マッピングの DNS NAPTR の使用をイネーブルにするには、SIP DNS サーバ コンフィギュレーション モードで **use-naptr** コマンドを使用します。ドメイン名/IP アドレス マッピングの DNS NAPTR の使用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。

use-naptr

no use-naptr

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

ドメイン名/IP アドレス マッピングの、DNS NAPTR の使用はディセーブルです。

コマンドモード

SIP DNS サーバ コンフィギュレーション モード (cusp-config-dns)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

例

次の例では、ホスト名/IP アドレス マッピングの DNS NAPTR の使用をイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> use-naptr
```

次の例では、ホスト名/IP アドレス マッピングの DNS NAPTR の使用をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip dns-srv
se-10-0-0-0(cusp-config-dns)> no use-naptr
```

関連コマンド

| コマンド | 説明 |
|-----------------------------|---|
| enable (SIP DNS サーバ) | ドメイン名/IP アドレス マッピングの、DNS サーバ NAPTR または SRV クエリー レコードをイネーブルにします。 |
| sip dns-srv | SIP DNS SRV コンフィギュレーション モードを開始します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip alias

このインスタンスのホスト名を設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip alias** コマンドを使用します。DNS サーバリストからホスト名を削除するには、このコマンドの **no** 形式を使用します。

sip alias {hostname}

no sip alias {hostname}

構文の説明

hostname グローバルに到達可能なシステムのホスト名を指定し、それをサーバのホスト名リストに追加します。

コマンド デフォルト

なし

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

例

次の例では、cusp.example.com をホスト名リストに追加する方法を示します。

```
se-10-0-0-0(cusp-config)> sip alias cusp.example.com
```

次の例では、cusp.example.com をサーバのホスト名リストから削除する方法を示します。

```
se-10-0-0-0(cusp-config)> no sip alias cusp.example.com
```

関連コマンド

| コマンド | 説明 |
|--------------------|---|
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |

sip logging

すべての着信および発信 SIP メッセージのロギングをイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip logging** コマンドを使用します。着信および発信 SIP メッセージのロギ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。

sip logging

no sip logging

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

SIP ロギングはディセーブルです。

コマンドモード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

SIP ロギングをオンにすると、Cisco Unified SIP Proxy のパフォーマンスに大きな影響を与えます。

例

次の例では、すべての着信および発信 SIP メッセージのロギングをイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip logging
```

次の例では、すべての着信および発信 SIP メッセージのロギングをディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip logging
```

関連コマンド

| コマンド | 説明 |
|--------------------|---|
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |
| sip queue | SIP キューを作成し、SIP キュー コンフィギュレーション モードを開始します。 |

sip privacy trusted-destination

要求されたプライバシー サービスが提供されるかどうかを判断する、プライバシーをアサートする場所を設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip privacy trusted-destination** コマンドを使用します。アサート プライバシー コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

sip privacy trusted-destination sequence *sequence_number* [condition *condition*]

no sip privacy trusted-destination sequence *sequence_number* [condition *condition*]

構文の説明

| | |
|--|---|
| sequence <i>sequence_number</i> | 確認する条件の順番を記述する、シーケンス番号を指定します。 |
| condition <i>condition</i> | (オプション) プライバシー アサーション サポートを適用する、トリガー条件名 (trigger condition コマンドを使用して設定されます) を指定します。 condition キーワードが指定されていない場合、プライバシー アサーションは無条件になります。 |

コマンド デフォルト

すべてのピアは信頼できないピアです。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

このコマンドを使用して「id」プライバシー サービスの信頼できるピアの条件を設定します。Cisco Unified SIP Proxy では、要求が信頼できないピアからのものである場合、要求から P-Asserted-Identity ヘッダーを削除し、信頼できないピアに送信される要求である場合、要求から P-Asserted-Identity を削除します。プライバシー サービスは、draft-levi-sip-diversion-08.txt の後の Diversion ヘッダーに対しても提供されます。

例

次の例では、in-network 条件が満たされる場合に宛先を信頼できるピアとして設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip privacy trusted-destination sequence 1 condition in-network
```

次の例では、すべての宛先を無条件に信頼できないものとして設定する方法を示します。

```
se-10-0-0-0(cusp-config)> no sip privacy trusted-destination sequence 1
```

関連コマンド

| コマンド | 説明 |
|-----------------------------------|--|
| sip privacy trusted-source | 要求されたプライバシー サービスが提供されるかどうかを判断する、プライバシーをアサートする場所を設定します。 |

sip privacy trusted-source

要求されたプライバシー サービスが提供されるかどうかを判断する、プライバシーをアサートする場所を設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip privacy trusted-source** コマンドを使用します。アサート プライバシー コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

no sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

構文の説明

| | |
|--|---|
| sequence <i>sequence_number</i> | 確認する条件の順番を記述する、シーケンス番号を指定します。 |
| condition <i>condition</i> | (オプション) プライバシー アサーション サポートを適用する、トリガー条件名 (trigger condition コマンドを使用して設定されます) を指定します。 condition キーワードが指定されていない場合、プライバシー アサーションは無条件になります。 |

コマンド デフォルト

すべてのピアは信頼できないピアです。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

このコマンドを使用して「id」プライバシー サービスの信頼できるピアの条件を設定します。CUSP では、要求が信頼できないピアからのものである場合、要求から P-Asserted-Identity ヘッダーを削除し、信頼できないピアに送信される要求である場合、要求から P-Asserted-Identity を削除します。プライバシー サービスは、draft-levi-sip-diversion-08.txt の後の Diversion ヘッダーに対しても提供されます。

例

次の例では、すべての発信元を無条件に信頼できるものとして設定し、値を **sequence 1** に割り当てる方法を示します。

```
se-10-0-0-0(cusp-config)> sip privacy trusted-source sequence 1
```

次の例では、すべての発信元を無条件に信頼できないものとして設定する方法を示します。

```
se-10-0-0-0(cusp-config)> no sip privacy trusted-source sequence 1
```

関連コマンド

| コマンド | 説明 |
|--|--|
| sip privacy trusted-destination | 要求されたプライバシー サービスが提供されるかどうかを判断する、プライバシーをアサートする場所を設定します。 |
| trigger condition | トリガー条件を作成し、Cisco Unified SIP Proxy トリガー コンフィギュレーション モードを開始します。 |

sip privacy service

SIP プライバシー サービスをイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip privacy service** コマンドを使用します。SIP プライバシー サービス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。

sip privacy service

no sip privacy service

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SIP プライバシー サービスはイネーブルです。

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

Cisco Unified SIP Proxy は「id」プライバシー (RFC 3325) だけを実装するため、プライバシー値に「session」、「user」、または「header」のいずれかに加え「critical」が含まれているときに、SIP プライバシー サービスがイネーブルになっている場合、Cisco Unified SIP Proxy は RFC 3323 の後に 500 件の応答を返します。

例

次の例では、SIP プライバシー サービスをイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip privacy service
```

sip tls

インターネット経由のセキュアな通信を提供する、他の SIP エンティティによる SIP トランスポート層セキュリティ (TLS) 接続をイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーションモードで **sip tls** コマンドを使用します。SIP TLS 転送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。

sip tls

no sip tls

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

SIP TLS はイネーブルではありません。

コマンドモード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| バージョン | 変更内容 |
|-------|-----------------|
| 1.0 | このコマンドが追加されました。 |

使用上のガイドライン

TLS 転送を使用する SIP リスナーを設定する前に、このコマンドを使用します。

ネットワーク経由のセキュアな通信を提供する、他の SIP エンティティによる SIP TLS 接続の使用をイネーブルにするには、このコマンドを使用します。デフォルトでは、Cisco Unified SIP Proxy に **trusted certificate** があるすべての要求中のクライアントからの TLS 接続が許可されます。このコマンドは、データ暗号化が必要で、信頼関係は必要ない場合にだけ便利です。

TLS 暗号化には、キーストアおよび対応する信頼証明書を指定するために、2 つの参加グループが必要です。TLS がイネーブルである場合、キーストア ファイルが読み取られます。結果として、**sip tls** コマンドをイネーブルにする前に、**cypto key generate** コマンドを使用してキーストアを最初に作成する必要があります。

Cisco Unified SIP Proxy は、一方向および双方向 TLS の両方をサポートします。



(注)

TLS 転送がイネーブルになっているアクティブな SIP リスナーがある場合、このコマンドはディセーブルにできません。

例

次の例では、SIP TLS 接続の使用をイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> sip tls
```

次の例では、SIP TLS 接続の使用をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no sip tls
```

関連コマンド

| コマンド | 説明 |
|-----------------------------|---|
| crypto key generate | 証明書と秘密キーのペアを生成します。 |
| sip network | 論理 SIP ネットワークを作成し、SIP ネットワーク コンフィギュレーション モードを開始します。 |
| sip tls trusted-peer | 信頼できる SIP TLS ピアを設定します。 |

sip tls trusted-peer

信頼できる SIP TLS ピアを設定するには、Cisco Unified SIP Proxy コンフィギュレーション モードで **sip tls trusted-peer** コマンドを使用します。信頼できる SIP TLS ピアを削除するには、このコマンドの **no** 形式を使用します。

```
sip tls trusted-peer {peer's-hostname}
```

```
no sip tls trusted-peer {peer's-hostname}
```

構文の説明

peer's-hostname ピアのホスト名を指定します。

コマンド デフォルト

なし

コマンド モード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

1.0 このコマンドが追加されました。

使用上のガイドライン

リモート側の ID と、信頼できる設定済みのピアの ID が一致しない限り、TLS 接続の確立は失敗します。信頼できるピアが設定されていない場合、TLS ハンドシェイクが成功すれば、接続は受け入れられます。

例

次の例では、example.com を信頼できる TLS ピアとして設定する方法を示します。

```
se-10-0-0-0(cusp-config)> sip tls trusted-peer example.com
```

次の例では、TLS 信頼済みピアとして設定された example.com を削除する方法を示します。

```
se-10-0-0-0(cusp-config)> no sip tls trusted-peer example.com
```

関連コマンド

| コマンド | 説明 |
|---------|---|
| sip-tls | 他の SIP エンティティを使用して SIP トランスポート層セキュリティ (TLS) 接続をイネーブルにします。 |

route recursion

Cisco Unified SIP Proxy の SIP ルート再帰をシステム全体でイネーブルにするには、Cisco Unified SIP Proxy コンフィギュレーション モードで **route recursion** コマンドを使用します。SIP ルート再帰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。

route recursion

no route recursion

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

ルート再帰はデフォルトでイネーブルです。

コマンドモード

Cisco Unified SIP Proxy コンフィギュレーション (cusp-config)

コマンド履歴

Cisco Unified SIP Proxy バージョン 変更内容

| | |
|-----|-----------------|
| 1.0 | このコマンドが追加されました。 |
|-----|-----------------|

使用上のガイドライン

Cisco Unified SIP Proxy は、リダイレクト応答（つまり、3xx 応答）を受信する場合、受信した Contact でルーティング ロジックが再帰的に実行されるように設定できます。受信した Contact が事前正規化された着信要求の要求 URI に配置され、サーバのルーティングおよび正規化後ロジックは新しい宛先に基づいて実行されます。複数の Contact を受信した場合、設定された q-value に基づいて順番に処理されます。複数の Contact に同じ q-value がある場合、それらは出現順に処理されます。

例

次の例では、Cisco Unified SIP Proxy でルート再帰をイネーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> route recursion
```

次の例では、Cisco Unified SIP Proxy でルート再帰をディセーブルにする方法を示します。

```
se-10-0-0-0(cusp-config)> no route recursion
```

関連コマンド

| コマンド | 説明 |
|--------------------|--|
| route group | ルート グループを作成し、ルート グループ コンフィギュレーション モードを開始します。 |
| route table | ルート テーブルを作成し、ルート テーブル コンフィギュレーション モードを開始します。 |

