システムの運用と設定

シスコ VPC-SI には、モバイル パケット コア ネットワーク用のサブスクライバ管理サービスが備わっています。

StarOS コマンド ライン インターフェイス（CLI）に接続して設定プロセスを開始する前に、StarOS がこれらのサービスをどのようにサポートするかを理解しておくと便利です。この章では、StarOS を設定する前に考慮すべき用語と背景情報について説明します。

- 用語 （1 ページ）
- システムがコンテキストを選択する方法 （5 ページ）
- 構成ファイルの概要 （8 ページ）
- IP アドレスの表記法 （9 ページ）
- 英数字の文字列 （11 ページ）

用語

この項では、このガイド全体で使用されている重要な用語を定義します。

コンテキスト

コンテキストは、さまざまな物理ポート、論理 IP インターフェイス、およびサービスに関連する設定パラメータの論理的なグループ化またはマッピングです。コンテキストは、バーチャル プライベート ネットワーク（VPN）と考えることができます。

システムには複数コンテキストを設定することができます。各コンテキストは、他のコンテキストとは独立して設定され、動作します。コンテキストが作成されると、管理ユーザーはそのコンテキストのサービス、論理 IP インターフェイス、およびサブスクライバを設定した後、論理インターフェイスを物理ポートにバインドできます。

また、コンテキストにドメインエイリアスを割り当てることもできます。サブスクライバのドメイン名が、コンテキストに設定されているエイリアス名のいずれかと一致する場合は、そのコンテキストが使用されます。

論理インターフェイス

ポートがユーザーデータのフローを許可できるようにするには、論理インターフェイスと呼ばれるStarOSの仮想回路またはトンネルにポートを関連付ける必要があります。StarOS内では、論理インターフェイスはレイヤ3IPアドレッシングなどの上位層のプロトコル転送を行う仮想ルータインターフェイスに関連付けられた名前付きのインターフェイスです。インターフェイスは、VPN コンテキストの一部として設定され、仮想インターフェイスをネットワークにブリッジするために使用される物理ポートから独立しています。

論理インターフェイスは、イーサネット + ppp + トンネルアドレスに関連付けられており、設定プロセス時に特定のポートにバインドされます。論理インターフェイスは、バインディングによりサービスに関連付けられます。サービスは、特定の論理インターフェイスに対して設定されている IP アドレスにバインドされます。関連付けられている場合、インターフェイスはサービスによって有効化された機能の特性を引き継ぎます。

簡易 IP データアプリケーションとモバイル IP データアプリケーションをサポートするように設定するための論理インターフェイスにはいくつかのタイプがあります。次に、これらの簡単な定義を示します。

管理インターフェイス

このインターフェイスは、管理ネットワークへの接続ポイントを提供します。このインターフェイスは、StarOS のコマンド ライン インターフェイス（CLI）へのリモートアクセスをサポートしています。また、Simple Network Management Protocol（SNMP）を介したイベント通知にも対応しています。

バインディング

バインドは、システム内の要素間の関連付けです。バインドには、動的と静的という2つのタイプがあります。

静的バインドは、システム設定によって実現されます。静的バインドは、次のように関連付けを行います。

- 物理ポートに対して（特定のコンテキスト内で設定された）特定の論理インターフェイス。インターフェイスがバインドされると、トラフィックは物理的に定義された回路であるかのように、コンテキストを経由することができます。静的バインドは、任意のインターフェイスおよびポートタイプでのカプセル化方式をサポートします。
- 同じコンテキスト内の論理インターフェイスに割り当てられたIPアドレスへのサービス。これにより、インターフェイスは、サービスに必要な特性（つまり、プロトコルをサポートする）を引き継ぐことができます。

動的バインドは、プロファイルまたはシステムパラメータの設定に基づいて、サブスクライバを特定の出力コンテキストに関連付けます。これにより、ワイヤレスキャリアが複数のサービスをサポートし、複数のネットワークへのシームレスな接続を容易にすることができるため、導入の柔軟性が高まります。

管理ポートは、ローカルコンテキストでのみバインドできます。トラフィックポートまたはサブスクライバポートは、非ローカルのコンテキストでのみバインドできます。

サービス

特定の機能を有効にするには、コンテキスト内でサービスを設定します。次に、システムで設定できるサービスの例を示します。これは、ライセンスの可用性とプラットフォームのタイプによって異なります。

- ゲートウェイ GPRS サポートノード（GGSN）サービス
- サービング GPRS サポートノード（SGSN）サービス
- パケット データ サービング ノード（PDSN）サービス
- ホームエージェント（HA）サービス
- レイヤ 2 トンネリング プロトコル アクセス コンセントレータ（LAC）サービス
- ダイナミックホスト制御プロトコル（DHCP）サービス
- モビリティ マネージメント エンティティ（MME）サービス
- PDN ゲートウェイ（P-GW）サービス
- サービングゲートウェイ（S-GW）サービス
- インテリジェントポリシー制御機能（IPCF）サービス（PCC-Service、PCC-Policy、PCC-AF）

AAA サーバー

認証、許可、およびアカウンティング（AAA）サーバーは、プロファイルを保存し、認証を実行し、各モバイル データ サブスクライバのアカウンティングレコードを維持します。AAA サーバーは、AAA インターフェイスを介してシステムと通信します。システムでは、AAA サーバーへの最大 128 のインターフェイス設定がサポートされています。

モバイル IP の場合は、外部 AAA（FAAA）サーバーとホーム AAA（HAAA）サーバーが存在する可能性があることに注意することが重要です。通常、FAAA サーバーはキャリアのネットワークに存在します。HAAA サーバーは、キャリアかホームネットワークのいずれかによって所有および制御されていることがあります。HAAA サーバーがホームネットワークによって所有および制御されている場合、アカウンティングデータは AAA プロキシサーバー経由でキャリアに転送されます。

重要 モバイル IP のサポートは、ホームエージェント（HA）を含むライセンスバンドルの可用性と購入によって異なります。

サブスクライバ

サブスクライバは、サービスのエンドユーザーです。システムを介してインターネット、ホームネットワーク、またはパブリックネットワークへのアクセスを取得します。

サブスクライバには、主に次の 3 つのタイプがあります。

- **RADIUS ベースのサブスクライバ**：最も一般的なタイプのサブスクライバであるこれらのユーザーは、International Mobile Subscriber Identity（IMSI）番号、電子シリアル番号（ESN）、またはドメイン名やユーザー名によって識別されます。これらは、RADIUS AAA サーバーで設定され、認証されます。

  認証が成功すると、サブスクライバプロファイルに含まれているさまざまな属性が返されます。属性は、セッションパラメータの設定（たとえば、プロトコル設定と IP アドレスの割り当て方法）、およびサブスクライバが持っている権限などを決定します。

重要 RADIUS AAA サーバーからシステムが受信した属性設定は、システムに設定されているローカルサブスクライバの属性とパラメータよりも優先されます。

- **ローカルサブスクライバ**： これらは、主にテスト目的で使用されるサブスクライバであり、特定のコンテキスト内で設定および認証されます。RADIUS ベースのサブスクライバとは異なり、ローカルサブスクライバのユーザープロファイル（RADIUS ベースのサブスクライバによって使用される属性を含む）は、それらが作成されたコンテキスト内で設定されます。

  ローカルサブスクライバのプロファイルが最初に作成されると、そのサブスクライバの属性はシステムのデフォルトに設定されます。すべてのサブスクライバのプロファイルに同じデフォルト設定が適用されます。これには、各システムコンテキストのシステムによって自動的に作成される *default* という名前のサブスクライバが含まれます。ローカルプロファイルの属性を設定すると、サブスクライバごとに変更が行われます。

重要 ローカルサブスクライバ用に設定された属性は、コンテキストレベルのパラメータよりも優先されます。ただし、RADIUS AAA サーバーから返された属性によって、これらの属性が上書きされる可能性があります。

- **管理サブスクライバ**：管理ユーザーは、CLI を通じてシステムをモニター、制御、および設定できる権限を持つユーザーです。管理は、システムコンソールポートを介してローカルで実行されるか、Telnet またはセキュアシェル（SSH）プロトコルを使用してリモートで実行されます。管理ユーザーは通常、ローカルコンテキスト内でローカルサブスクライバとして設定されます。これは、システム管理と管理専用で使用されます。ローカルサブスクライバと同様に、管理者サブスクライバのユーザープロファイルは、サブスクライバが作成されたコンテキスト内（この場合はローカルコンテキスト内）で設定されます。た

だし、ローカルコンテキスト内または TACACS+ 内に AAA 設定が存在する場合、管理サブスクライバは RADIUS を介してリモートで認証されることもあります。

システムがコンテキストを選択する方法

この項では、コンテキストレベルの管理ユーザーまたはサブスクライバのセッションに使用するコンテキストを決定するプロセスについて説明します。このプロセスを理解することで、設定が必要なコンテキストとインターフェイスの数の設定をより適切に計画できるようになります。

コンテキストレベルの管理ユーザーセッションのコンテキスト選択

システムは、管理目的で具体的に使用する *local* という名前のコンテキストで設定されます。コンテキストレベルの管理ユーザー（コンテキスト内で設定されている）のコンテキスト選択プロセスは、MIO の管理ポートがローカルコンテキストだけに関連付けられているため、簡素化されています。したがって、システム全体の管理を担当するコンテキストレベルの管理ユーザーの送信元と接続先のコンテキストは、常にローカルコンテキストである必要があります。

コンテキストレベルの管理ユーザーは、非ローカルのコンテキストで作成できます。これらの管理アカウントには、作成されたコンテキストでのみ権限が付与されます。このタイプの管理アカウントは、そのコンテキストでローカル接続が有効になっている場合（SSHD など）、属しているコンテキストのポートに直接接続できます。

すべての FTP 接続または SFTP 接続については、MIO 管理インターフェイスを介して接続する必要があります。非ローカルのコンテキストアカウントとして SFTP または FTP を利用する場合は、*username@contextname* のユーザー名のシンタックスを使用する必要があります。

重要 FTP はサポートされていません。

ローカル認証を提供するようにシステムを設定している場合、またはコンテキストレベルの管理ユーザーを認証するために AAA サーバーと連携する場合に、コンテキスト選択プロセスはより複雑になります。

システムは、コンテキストレベルの管理ユーザーをローカルに設定する（つまり、プロファイルが設定され、独自のメモリに保存される）、またはリモートで AAA サーバー上に設定するといった柔軟性を提供します。ローカルに設定されたユーザーがシステムにログオンしようとすると、システムは認証を実行します。AAA サーバーでユーザープロファイルを設定している場合、システムは AAA サーバーに接続して認証を実行する方法を決定する必要があります。これは、セッションの AAA コンテキストを決定することによって行われます。

次の表とフローチャートは、コンテキストレベルの管理ユーザーに対して AAA コンテキストを選択するためにシステムが使用するプロセスを示しています。表の項目は、フローチャート内の丸で囲まれた番号に対応しています。

図 *1:* コンテキストレベルの管理ユーザーの ***AAA*** コンテキスト

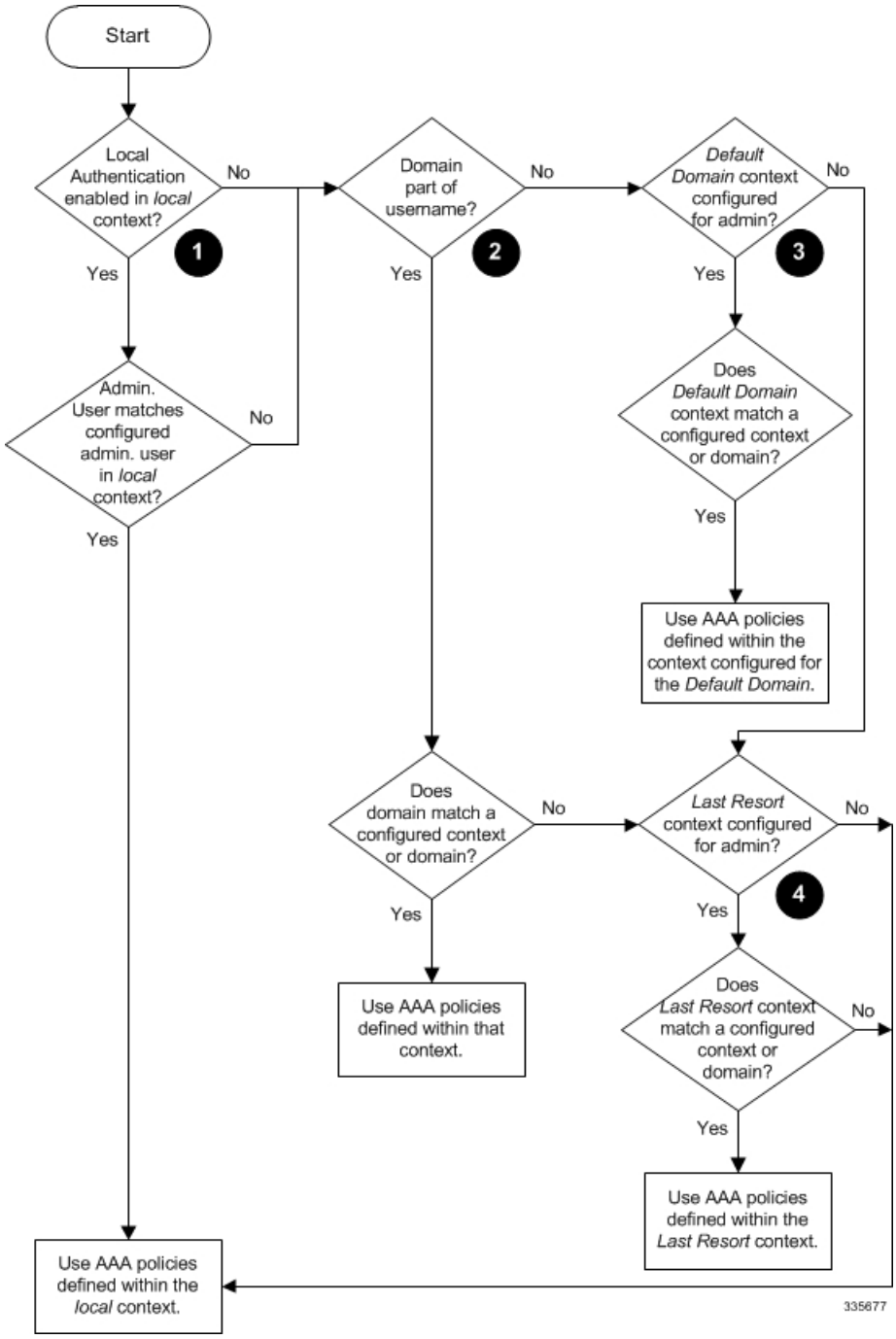

表 *1*: コンテキストレベルの管理ユーザーの *AAA* コンテキストにおける選択

項目	説明
1	認証時に、ローカルコンテキストでローカル認証が有効になっているかどうかがシステムによって判別されます。 有効になっている場合、システムはローカルコンテキストで管理ユーザーの認証を試行します。有効になっていない場合、この表の項目 2 に進みます。 管理ユーザーのユーザー名が設定されている場合、ローカルコンテキスト内の AAA 設定を使用して認証が実行されます。設定されていない場合、この表の項目 2 に進みます。
2	システムでローカル認証が無効になっている場合、または管理ユーザーのユーザー名がローカルコンテキストで設定されていない場合、システムはユーザー名の一部としてドメインが受信されたかどうかを判断します。 ドメインが存在し、設定されているコンテキストまたはドメインの名前に一致する場合、システムはそのコンテキスト内で AAA 設定を使用します。 ドメインが存在し、設定されているコンテキストまたはドメインの名前と一致しない場合、この表の項目 4 に進みます。 ユーザー名の一部としてドメインが存在しない場合、この表の項目 3 に進みます。
3	ユーザー名にドメインが指定されていない場合、またはドメインが認識されていない場合、システムは *AAA* 管理者のデフォルトドメインが設定されているかどうかを判別します。 デフォルトドメインが設定されており、設定済みコンテキストと一致する場合は、*AAA* 管理者のデフォルトドメインにおけるコンテキスト内の AAA 設定が使用されます。 デフォルトドメインが設定されていないか、設定済みコンテキストまたはドメインと一致しない場合は、次の項目 4 に進みます。
4	ドメインがユーザー名の一部として指定されていても、設定済みコンテキストと一致しなかった場合、またはドメインがユーザー名の一部として指定されていない場合、システムは *AAA* 管理者のラスト リゾート コンテキスト パラメータが設定されているかどうかを判断します。 ラストリゾートコンテキストが設定されており、設定済みコンテキストと一致する場合、そのコンテキスト内の AAA 設定が使用されます。 ラストリゾートコンテキストが設定されていない場合、または設定されたコンテキストやドメインと一致しない場合、ローカルコンテキスト内の AAA 設定が使用されます。

リリース 21.4 以降（信頼できるビルドのみ）：

- ユーザーは、それぞれのコンテキストインターフェイスを使用してのみシステムにアクセスできます。
- ユーザーが別のコンテキストインターフェイスを使用してそれぞれのコンテキストにログインしようとすると、そのユーザーは拒否されます。

- ユーザーが「authorized-keys」または「allowusers」のいずれかのコンテキストに設定されているかどうかに関係なく、この機能では、独自のコンテキストインターフェイス以外のコンテキストインターフェイスを介してログインを試行すると、これらのユーザーは拒否されます。
- ローカル以外のコンテキストに設定されているユーザーは、ログインを試行するコンテキストを指定する必要があります。例：

  ssh username@ctx_name@ctx_ip_addrs

サブスクライバセッションのコンテキスト選択

管理ユーザーの場合よりも、サブスクライバセッションのコンテキスト選択プロセスとの関係があります。特定製品のサブスクライバ セッション コンテキストの選択情報は、個々の製品の「*Administration Guide*」に記載されています。

構成ファイルの概要

システムでは、設定可能なパラメータを変更するためのファイルまたはスクリプトの使用がサポートされています。ファイルをオフラインのシステム設定に使用すると、複数のシステムでパラメータを設定するのにかかる時間が短縮されます。

システム構成ファイルは、コマンドと設定パラメータを含むASCIIテキストファイルです。構成ファイルを適用すると、システムはファイルを行単位で解析し、シンタックスをテストしてコマンドを実行します。シンタックスが正しくない場合は、CLIにメッセージが表示され、システムは次のコマンドに進みます。# で始まる行は注釈と見なされ、無視されます。

重要 **grep** キーワードおよび **more** キーワードとともに使用されるパイプ（|）は、構成ファイルの処理においてエラーを引き起こす可能性があります。したがって、システムは処理中にパイプのあるキーワードを自動的に無視します。

重要 構成ファイルは常にUNIX形式で保存してください。そうしないと、構成ファイルの処理を妨げるエラーが発生する可能性があります。

ファイル内のコマンドと設定データは、CLIプロンプトで入力した場合と同様に整理され、フォーマットされます。たとえば、CLIで *source* というコンテキストを作成する場合は、それぞれのプロンプトで次のコマンドを入力します。

```
[local]host_name# config
[local]host_name(config)# context source
[source]host_name(config-ctx)# end
```

構成ファイルを使用して *source* というコンテキストを作成するには、テキストエディタを使用して、次のもので構成される新しいファイルを作成します。

```
config
      context source
      end
```

構成ファイルを使用する際に考慮すべき重要な点がいくつかあります。

- システムは、起動プロセスの最後に構成ファイルを自動的に適用します。システムを初めて起動した後、作成した構成ファイルと、ネットワークのニーズに合わせて調整した構成ファイルを適用できます。システムが構成ファイルを使用するようにするには、『*Software Management Operations*』に記載されている手順に従ってシステムの起動パラメータを変更します。
- 起動プロセス中に適用されるだけでなく、CLI プロンプトで適切なコマンドを実行することで、いつでも構成ファイルを手動で適用できます。『*Software Management Operations*』の手順を参照してください。

重要 起動プロセス後に構成ファイルを適用しても、ブートプロセスの一部としてロードされた構成は削除されません。重複しているコマンドだけが上書きされます。

- 構成ファイルは、次の場所のいずれかに保存することができます。
  - **USB メモリスティック**：アクティブな MIO（/usb1）上の USB ポートを介してサポートされる。
  - **ネットワークサーバー**：システムがセキュアファイル転送プロトコル（SFTP）を使用してアクセスできるネットワーク上のワークステーションまたはサーバー。これは、複数のシステムが同じ設定を必要とする大規模なネットワークの展開に推奨される。
  - **/flash**：ストレージが制限されているソリッドステートデバイス。
  - **raid**：内部 RAID ストレージ。
- CLI セッション中に行った設定変更を保存するたびに、構成ファイルとして使用可能なファイルにそれらの設定を保存できます。

IP アドレスの表記法

CLI を介してポートインターフェイスを設定する場合は、IP アドレスを入力する必要があります。CLI は常に IPv4 アドレスを受け入れ、場合によっては IPv6 アドレスを代替として受け入れます。

一部の設定コマンドでは、CLI は CIDR 表記も受け入れます。受け入れ可能な IP アドレスの表記法の形式を確認するには、常に CLI コマンドのオンラインヘルプを参照してください。

IPv4 ドット付き 10 進表記

インターネット プロトコル バージョン 4（IPv4）アドレスは、4 つのオクテットに分割された 32 ビットで構成されます。これらの 4 つのオクテットは、0 ～ 255 の範囲の 10 進数の番号で記述され、各番号の間に終止符のデリミタ（ドット）を含む文字列として連結されます。

たとえば、通常はホスト名 localhost が割り当てられているループバック インターフェイスのアドレスは 127.0.0.1 です。これは、4 つのバイナリオクテット 01111111、00000000、00000000、および 00000001 で構成され、完全な 32 ビットアドレスを形成します。

IPv4 では、インターネット プロトコル アドレスに 32 ビットを使用できるため、2^{32}（4,294,967,296）アドレスがサポートされます。

IPv6 コロン区切り 16 進表記

インターネット プロトコル バージョン 6（IPv6） アドレスには、64ビットのネットワークおよび 64ビットのホストアドレスといった 2 つの論理的な部分があります。IPv6 アドレスは、16 ビット 16 進数の値のコロン（:）で区切られたの 8 つのグループで表されます

完全な IPv6 アドレスの一般的な例は、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。

16 進数は大文字と小文字が区別されません。

128 ビットの IPv6 アドレスは、次のルールを使用して省略できます。

- 16ビット値の先頭のゼロは省略できます。たとえば、アドレス fe80:0000:0000:0000:0202:b3ff:fe1e:8329 は、fe80:0:0:0:202:b3ff:fe1e:8329 として記述されます。
- アドレス内の連続したゼロの 1 つのグループは、二重コロンで置き換えることができます。たとえば、fe80:0:0:0:202:b3ff:fe1e:8329 は、fe80::202:b3ff:fe1e:8329 になります。

IPv6 では、インターネット プロトコル アドレスに 128 ビットを使用でき、2^{128} ビット（340,282,366,920,938,000,000,000,000,000,000,000,000）のインターネットアドレスをサポートできます。

CIDR 表記

Classless Inter-Domain Routing（CIDR） の表記法は、インターネット プロトコル アドレス とそれに関連付けられているルーティング プレフィクスの コンパクトな仕様です。これは、ネットワークアーキテクチャで IPv4 と IPv6 の両方のアドレッシングに使用されます。

CIDR は、IP アドレスの解釈のためのビット単位のプレフィックスベースの標準規格です。アドレスのブロックを単一のルーティングテーブルエントリにグループ化することにより、ルーティングを容易にします。これらのグループ（CIDR ブロック）は、IP アドレスのバイナリ表記で最初のビットシーケンスを共有します。

CIDR 表記は、IP アドレスとプレフィックスのサイズから構築され、後者はルーティングプレフィックスの先頭の 1 ビットの数になります。IP アドレスは、IPv4 または IPv6 の標準規格に

従って表されます。これには、区切り文字、スラッシュ（/）文字、および 10 進数で表されるプレフィックスサイズが続きます。

アドレスは、単一、個別、インターフェイスアドレス、またはネットワーク全体の開始アドレスを表すことができます。後者の場合、CIDR 表記は、ネットワークのアドレスブロック割り当てを指定します。ネットワークの最大サイズは、プレフィックス以下の残りの最下位ビットによって有効になるアドレスの数で表されます。これは、ホスト識別子と呼ばれることがよくあります。

次に例を示します。

- アドレス指定 209.165.200.224/27 は、特定の IPv4 アドレスとそれに関連付けられたルーティングプレフィックス 209.165.200.0、または同等のサブネットマスク 255.255.255.224 を表します。
- IPv4 ブロック 192.168.0.0/22 は、192.168.0.0 から192.168.3.255 までの 1024 IPv4 アドレスを表します。
- IPv6 ブロック 2001:DB8::/48 は、2001:DB8:0:0:0:0:0:0 から 2001:DB8:0:FFFF:FFFF:FFFF:FFFF:FFFF までの IPv6 アドレスを表します。
- ::1/128 は IPv6 ループバックアドレスを表します。プレフィックスサイズは 128 です。これはアドレス自体のサイズであり、このファシリティが 1 つのアドレスだけで構成されていることを示しています。

マスクまたはプレフィックスによって定義されたサブネットのアドレスの数は、$2^{\text{address size - mask}}$ として計算することができます。この場合、IPv4 のアドレスサイズは 32、IPv6 のアドレスサイズは 128 です。たとえば、IPv4 では、/29 のマスクは $2^{32 - 29} = 2^3 = 8$ addresses を与えます。

英数字の文字列

一部の CLI コマンドでは、値を定義するために英数字文字列を入力する必要があります。この文字列は、定義された最小長および最大長（文字数）を持つ連続した英数字のコレクションです。

文字セット

英数字セットは、アルファベット（ラテン文字）や数字（アラビア数字）の組み合わせです。このセットは、0 ～ 9 の数字、A ～ Z（大文字）、a ～ z（小文字）で構成されます。アンダースコア文字（_）とダッシュ/ハイフン（-）は、英数字の文字セットの一部と見なされます。

空白文字（空白文字またはスペース文字）は、通常、時間や日付スタンプなどの特定のルール定義形式を除き、英数字文字列では回避する必要があります。

以下に示す通り、英数字文字列には次の「特殊」文字を使用しないでください。

- **&**（アンパサンド）
- **’**（アポストロフィ）

- **< >**（矢印ブラケット）[以下の例外を参照してください]
- *****（アスタリスク）[以下のワイルドカードの例外を参照してください]
- **{ }**（波カッコ）
- **[ ]**（角カッコ）
- **$**（ドル記号）[以下のワイルドカード例外を参照してください]
- **!**（感嘆符）[以下の例外を参照してください]
- **( )** [丸カッコ]
- **%**（パーセント）[以下の例外を参照してください]
- **#**（ポンド記号）[以下の例外を参照してください]
- **?**（疑問符）
- **'**（引用符：シングル）
- **"**（引用符：ダブル）
- **;**（セミコロン）
- ****（バックスラッシュ）[以下の例外を参照してください]
- **/**（普通のスラッシュ）[以下の例外を参照してください]
- **～**（チルダ）
- **|**（縦棒）[以下の例外を参照してください]

ruledef、APN、ライセンスキー、およびその他の設定/表示パラメータで入力された文字列には、次の文字が表示される場合があります。

- **< >**（矢印ブラケット）[より小さい or より大きい]
- *****（アスタリスク）[ワイルドカード]
- **:**（コロン）
- **$**（ドル記号）[ワイルドカード]
- 。（ドット）
- **=**（等号）
- **!**（感嘆符）
- **%**（パーセント）
- **/**（普通のスラッシュ）
- **|**（縦棒）

次の文字を使用して、グローバル AAA 機能のユーザー名からドメインを区切ることができます。

- **@**（アットマーク）
- （ダッシュまたはハイフン）
- **#**（ハッシュまたはポンド記号）
- **%** [パーセント]
- \（バックスラッシュ）[二重スラッシュ「\\」として入力する必要があります]
- **/**（普通のスラッシュ）

引用符付き文字列

説明文で単語の間にスペースを使用する必要がある場合は、二重引用符（""）内に文字列を入力する必要があります。例：

```
interface "Rack 3 Chassis 1 port 5/2"
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。