802.1X 認証

改訂日:2017 年 5 月 11 日

IEEE 802.1X 認証の概要

この項では、Cisco TelePresence System で 802.1X 認証をモニタおよびトラブルシューティングする方法について説明します。802.1X は、ポートベースのネットワーク アクセス コントロールの IEEE 標準です。これにより、ユーザまたはマシンの ID に基づいて、ネットワーク接続を許可または拒否する機能、仮想 LAN(VLAN)アクセスを制御する機能、およびトラフィック ポリシーを適用する機能が提供されます。

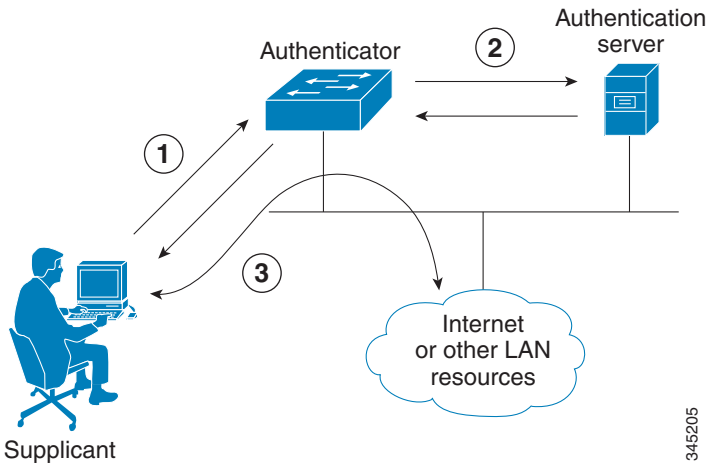
802.1X は、認証を使用してネットワークへのデバイス アクセスを許可または拒否します。イーサネット スイッチ ポートは、接続するデバイスの ID に基づいて動的にイネーブルにできます。認証されていないデバイスは、ネットワークにアクセスできません。

802.1X 認証コンポーネント

802.1X 認証には次の 3 つのネットワーク デバイスが必要です。

- **サプリカント**:LAN/ワイヤレス LAN(WLAN)へのアクセスを試行するクライアント デバイス(ラップトップやエンドポイントなど)、またはこのデバイスで動作しオーセンティケータにクレデンシャルを提供するソフトウェア。
- **オーセンティケータ**:保護されたネットワークへのアクセス ポイントとして機能するネットワーク デバイス(イーサネット スイッチやワイヤレス アクセス ポイントなど)。802.1X 認証の場合、サプリカントは、ユーザ名、パスワード、デジタル セキュリティ証明書、またはこれらの組み合わせなどのネットワーク クレデンシャルをオーセンティケータに提供します。オーセンティケータはその後、クレデンシャルを認証サーバに転送して検証します。
- **認証サーバ**:保護されたネットワークを保護するサーバ(Cisco Secure Access Control Server など)。802.1X 認証の場合、認証サーバはオーセンティケータからサプリカントのネットワーク クレデンシャルを受信し、サプリカントの ID を検証します。その後、サプリカントはネットワーク上のリソースにアクセスできるようになります。

図 8-1　802.1X 認証プロセスの図



IX システムの認証

Cisco TelePresence IX システムは、802.1X 対応サプリカントとして動作するように装備されています。802.1X 認証はデフォルトでイネーブルになっています。

(注)　スイッチ ポート（またはオーセンティケータ）はマルチドメイン モードで設定することを推奨します。

IX 802.1X 認証ステータスの確認

Cisco TelePresence System で 802.1X 認証ステータスを調べるには、次のオプションのいずれかを使用します。

- システム起動時に IX メイン ディスプレイ画面を表示します（メイン ディスプレイ画面での 802.1X 認証ステータスの確認（8-2 ページ）を参照）
- CLI コマンド、**show dot1x status** を入力します（CLI コマンドによる 802.1X 認証ステータスの確認（8-4 ページ）を参照）。

メイン ディスプレイ画面での 802.1X 認証ステータスの確認

Cisco TelePresence IX システムのメイン ディスプレイ画面で 802.1X 認証ステータスを調べるには、次の手順を実行します。

手順 1　Cisco TelePresence IX システムの電源をオフにします。

手順 2　Cisco TelePresence IX システムの電源をオンにします。

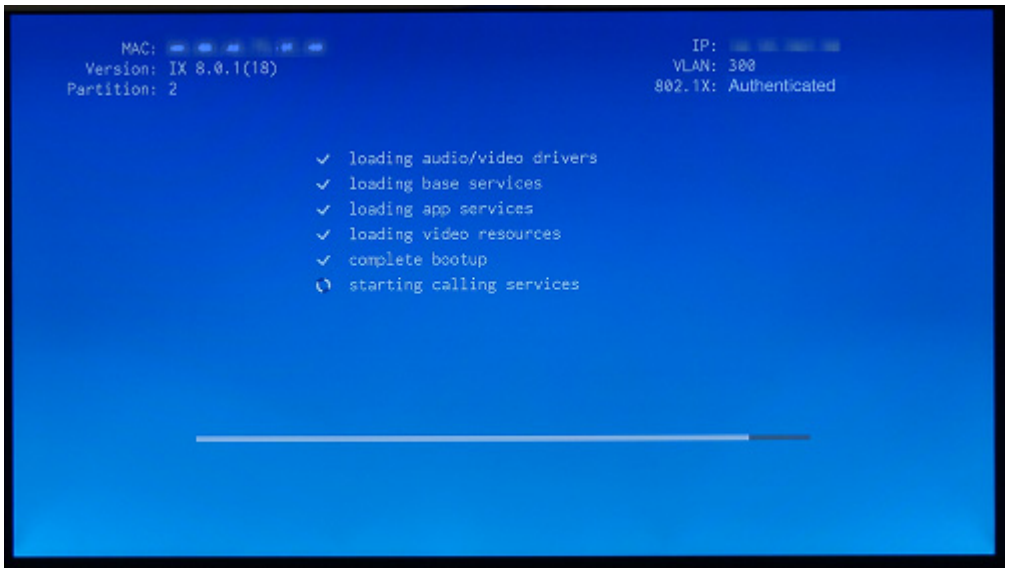
手順 3　メイン ディスプレイ画面の右下を確認します。3 画面システムでは、中央の画面の右下を確認します。802.1X がシステムで認証されているか、認証されていないか、または必要ないことを示すテキストが表示されます。

例：

```
802.1X: Connecting...
802.1X: Not Authenticated
```

Cisco TelePresence System のメイン ディスプレイ画面に表示されるこのテキストは、そのシステムでの 802.1X 認証の成功または失敗を示します。ステータス行が「不要（Not Required）」となっている場合は、802.1X 認証はそのシステムに必要ありません。

図 8-2　Cisco TelePresence System のブートアップ画面のスクリーンショット



有効なネットワークと無効なネットワークの 802.1X 認証ステータス表示の概要については、表 8-1 を参照してください。

表 8-1　802.1X 認証ステータス表示の概要

ステータス	802.1X 対応ネットワーク	802.1X 非対応ネットワーク
進行中（In Progress）	接続中/認証中（Connecting / Authenticating）	接続中（Connecting）
Success	認証	不要
失敗 (Failure)	認証されていません（Not Authenticated）	不要

（注）　802.1X 認証ステータスは、Cisco TelePresence System のプライマリ画面でのみ表示でき、セカンダリ画面（たとえば、プレゼンテーション画面や、3 画面システムの場合の左右いずれかの画面など）では表示できません。802.1X 認証ステータスがプライマリ画面に表示されない場合は、「CLI コマンドによる 802.1X 認証ステータスの確認」セクション（8-4 ページ）に示す手順に従ってください。

CLI コマンドによる 802.1X 認証ステータスの確認

CLI コマンドを使用して 802.1X 認証ステータスを確認するには、次の手順を実行します。

手順 1　CLI にログインします。

手順 2　次のコマンドを入力します。**show dot1x status**

手順 3　表示されるテキストを確認します。802.1X がシステムで認証されているか、認証されていないか、または必要ないことを示すテキストが表示されます。

例:

```
admin:show dot1x status
Authenticated
```

802.1X 認証問題のトラブルシューティング

802.1X が適切に認証しない場合は、次の項を確認してください。

- 802.1X 認証の問題のトラブルシューティング
- セキュリティ証明書の表示

802.1X 認証の問題のトラブルシューティング

表 8-2 に、802.1X 認証中に起こる可能性のある問題と考えられる解決策を要約します。

表 8-2　802.1X 認証の問題のトラブルシューティング

症状	考えられる根本的な原因	解像度
Cisco Secure ACS 認証サーバが、Cisco TelePresence System のサプリカントからのセキュリティ証明書を拒否する。	セキュリティ証明書が無効、期限切れ、または CAPF から発行されていません。	CAPF を使用して、有効で期限が切れていないセキュリティ証明書をインストールします。「セキュリティ証明書の表示」を参照してください。
Cisco TelePresence System が 802.1X 認証を失敗する。	システムの最新のログ ファイルにエラーが含まれている可能性があります。	CLI でコマンド **file list log dot1x** を使用して、ログにエラーや障害メッセージがないかを確認します。

表 8-2　802.1X 認証の問題のトラブルシューティング（続き）

症状	考えられる根本的な原因	解像度
Cisco TelePresence System のブートアップ画面に「802.1X: 不要（802.1X: Not Required）」と表示される。	イーサネット スイッチが 802.1X をサポートするように設定されていません。	イーサネット スイッチにログインし、CLI コマンド **show authentication sessions interface {FastEthernet | GigabitEthernet}** {*Interface Number*} を使用して、802.1X 認証ステータスを確認します。イーサネット スイッチが 802.1X に対応していない場合は、それを有効にします。手順については、『*Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide*』を参照してください
Cisco Secure ACS 認証サーバが、Cisco TelePresence System のサプリカントからのセキュリティ証明書を拒否する。	Cisco Secure ACS が 802.1X をサポートするように設定されていません。	802.1X をサポートするように Cisco Secure ACS（およびすべてのバックエンド ネットワーク設定）を設定します。手順については、『*Identity-Based Networking Services: IP Telephony in IEEE 802.1X-Enabled Networks Deployment and Configuration Guide*』を参照してください
Cisco TelePresence System が LSC の代わりに MIC を使用して認証を試行している。	LSC が CAPF からエクスポートされておらず、Cisco Secure ACS にインポートされていません。	LSC が CAPF からエクスポートされ、Cisco Secure ACS にインポートされていることを確認します。「LSC のインストール」を参照してください。
別の CAPF および Unified CM に移動した後、Cisco TelePresence System が 802.1X 認証を失敗する。	LSC は前の CAPF および Unified CM からインストールされたため、802.1X 認証をサポートしていません。Cisco TelePresence System を別の CAPF および Unified CM に移動するには、LSC を再インストールし、システムをアップグレードする必要があります。	Cisco Unified CM から LSC を再インストールして、Cisco TelePresence System をアップグレードします。「LSC のインストール」を参照してください。

セキュリティ証明書の表示

証明書が有効で期限切れでなく CAPF によって発行されていることを確認するために、セキュリティ証明書（MIC または LSC）を調べることができます。セキュリティ証明書の詳細については、IX システムのセキュリティ証明書の検証（5-6 ページ）を参照してください。

CLI またはサードパーティ製ツールを使用して、MIC または LSC を確認できます。

CLI からセキュリティ証明書を確認する

CLI から MIC または LSC を表示するには、次の手順を実行します。

手順 1　CLI にログインします。

手順 2　次のコマンドを入力します。**show cert {mic | lsc}**。**mic** または **lsc** のどちらか（両方ではなく）を入力してください。

手順 3　CLI 内に表示される証明書を確認します。証明書が有効で期限切れでなく CAPF によって発行されていることを確認します。

例：

```
> admin:show cert lsc
> Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5 (0x5)
Signature Algorithm( sha1WithRSAEncryption
Issuer: C=US, O=organization, OU=department, CN=CAPF-1a234bcd, ST=CA, L=CH
Validity
Not Before: Mar 23 16:10:31 2012 GMT
Not After: Mar 22 16:10:30 2017 GMT
Subject: C=US, O=organization, OU=department, CN=SEPXXXXXXXXXXXX
```

LSC がインストールされていないシステムで **show cert lsc** を入力すると、コマンド ラインは次のようになります。

```
show cert lsc
There is no certificate to display
```

セキュリティ証明書の期限が切れている、無効である、または別の送信元から発行されている場合は、CAPF を使用して新しい証明書をインストールします。

サードパーティ製ツールからのセキュリティ証明書の確認

サードパーティ製のツールを使用して MIC または LSC を確認することもできます。手順については、ツールに付属しているマニュアルを参照してください。