# コンテント サービス スイッチに関する FAQ

## 目次



## 概要

このドキュメントでは、Cisco コンテンツ サービス スイッチ（CSS）に関するよくある質問（FAQ）について説明します。

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

## Q. どこで CSS のための MIB を見つけることができますか。

A. MIB は CSS に既にあっています。 CSS を簡易ネットワーク管理プロトコル（SNMP）ネットワーク体系のエージェントと考慮できます。 する必要があるのは CSS の SNMP パラメータを設定することだけです。 詳細については簡易ネットワーク管理プロトコル（SNMP）を設定する資料を参照して下さい。

## Q. CSS がサポートするスクリプト キープアライブの最大数とは何か。

A. CSS がサポートするスクリプト キープアライブの最大数は 255 です。 Content Services Switch に関するリリース ノートの*ソフトウェア バージョン 5.00* セクション*の新しい 機能を* Cisco 11000 シリーズ参照して下さい。

## Q. コア ファイルのクリアまたは削除の方法は。

A. **clear core コマンドを**発行して下さい。 コマンドはデバッグ モードの CSSソフトウェア バージョン 5.00 および それ 以降で利用できます。 構文は次のとおりです。

```
css150(debug)#clear core filename CR
```

## Q. ログ メッセージの注釈はどこにありますか。

A. ログメッセージの解釈に関しては、資料 ログメッセージを参照して下さい。

## Q. ピア間でお互いにロード リポートを送信する頻度を制御するコマンドはありますか。

A. dns-peer interval コマンドを使用します。 またローカル ロードのより速いメジャーを実現させるためにローカルで設定できる追加コマンドがあります:

- **エージング アウトタイマー**—古い ロード情報の ageout の時を（秒で）設定 します。
- **ティアダウン タイマ**—取り外しレポートを送信するためにシステムが待っている最大時間を設定 します（秒で）。

## Q. コードのバージョンによってライセンス キーが変わりますか。

A. いいえ、ライセンス キーはコードのバージョンによって変わりません。

## Q. ライセンス キーをなくしました。 どうすればよいのですか。

A. licensing@cisco.com に CSS のシリアル番号が付いている電子メールを送信 して下さい。 version コマンドは、フィーチャ パックを表示しますが、ライセンス キーは表示されません。

## Q. スティッキー テーブルのエントリの保持のための既定の時刻とは何時か。

A. コマンド **sticky-inact-timeout を**使用しなければ、既定の時刻がありません。 スティッキー テーブルは FIFO 基礎 ( 利用可能 な デバイスの種類およびメモリに従う 32,000 か 128,000 のエントリ、 ) で、または CSS の再度ブートするまで保存されます。

## Q. America Online （ AOL ) のようなメガ プロキシからの要求をカバーするためにスティッキー マスクを設定する方法

A. アプリケーションはユーザがセッションの全体のライフの間スタックしているように要求する場合レイヤ3 をスティッキと考慮して下さい。 スティッキ レイヤ3 はユーザ IP アドレスに基づいてサーバにユーザをスタックします。 CSS に 32,000 のスティッキー テーブルがあります、つまり 32,000 人の同時ユーザがサイトにあるときことを、表ラップする意味し、最初のユーザは「思うようにいかなく」なります。 ただし、サイトの音量は 32,000 人以上のユーザが一度にあることそのような物である場合もあります。 または顧客の大部分はメガ プロキシによってあなたに来ることができます。 このような場合、別のスティッキー 方式の使用 ( クッキー、cookieurl、または URL のような ) またはスティッキー マスクの増加を考慮して下さい。 デフォルトのスティッキ マスクは 255.255.255.255 で、これは、スティッキ テーブルの各エントリが、独立した IP アドレスであることを意味しています。 1 セッションのライフにわたるユーザがアドレス範囲で複数の異なる IP アドレスを使用するどれいくつかのメガ プロキシに状況がであります。 この状況によりいくつかの TCP 接続は 1 サーバにスタックしている得ます他の接続を同じトランザクションのための異なるサーバーにスタックしている得るために引き起こす場合があります。 結果はグローサリー カートからのいくつかの項目の損失である場合もあります。 スタックの高度メソッドの 1 つを使用できない場合クライアント ベースがこれらのメガ プロキシの 1 によって来るとき 255.255.240.0 のスティッキー マスクを使用して下さい。

## Q. アドバンストバランスセキュアソケット層 ( SSL ) を使用するときスティッキのためのオプションない理由

A. アドバンス バランス SSL は、スティッキ SSL と同じです。

## Q. どのような暗号化を Content and Application Peering Protocol （ CAPP ) か Application Peering Protocol （ APP ) は使用しますか。

A. デフォルトで、CAPP は no encryption を使用します。 APP セッションを MD5 （ MD5 ) を使用するために設定できます。 APP セッションが成立するには、ピアの両側で暗号タイプが同じであることが必要です。

## Q. 「gratuitous arp」メッセージの意味は何ですか。

A. バックアップスイッチが 3 秒以内にマスタスイッチからのハートビートを検出するとき、バックアップスイッチはマスターになるために移行し、" gratuitous arp " メッセージを送信 します。 メッセージは新しいマスタスイッチからのアドレス解決プロトコル （ ARP ) 伝達を示します。 メッセージは現在のマスタスイッチの MAC アドレスが含まれています。 無償ARP はグローバル コンフィギュレーション モードで **IP 無償ARP** によって命じます有効に なります。 それは単一のインターフェイスで有効に なり、他のインターフェイスでそれをブロックできません。

## Q. フェールオーバー モードで CSS をまたがる設定の同期化の方法は何ですか。

A. ソフトウェア バージョン 4.0 のコンフィギュレーションを同期するために、**commit config sync コマンドを**使用して下さい。 ソフトウェア バージョン 3.10 コードのコンフィギュレーションを同期するために、1 スイッチから別のものに設定を移動するために FTP を使用して下さい。

ソフトウェア バージョン 6.x および 7.x のコンフィギュレーションを同期するためにアクティブ/スタンバイかボックス間の冗長性のためにコマンド commit_redundancy をコードして下さい、使用して下さい。 または Virtual IP （ VIP ）/interface 冗長性のためにコマンド commit_vip_redundancy を使用できます。 示しますスクリプトのヘッダで commit_redundancy スクリプトのための利用可能 な コマンドラインオプションを表示するためにスクリプト commit_redundancy をコマンドを使用できます。 同じは commit_vip_redundancy コマンドに適用します。

## Q. ターミナル プログラムでは、どの設定を使用するべきですか。

A. これらの設定を使用して下さい:

- 9600 ボー
- 8 ビット
- パリティなし
- 1 ストップ ビット
- フロー制御なし

## Q. 方法が CSS の MAC アドレスをプログラムし直すありますか。

A. はい、方法があります。

**注:** 装置の裏側に、MAC アドレスとシリアル番号があります。

シリアル番号および MAC アドレスをプログラムし直すためにこれらのステップを完了して下さい。 この例では、MAC アドレスは CS800 シャーシのものです。

1. Offline Diagnostic Monitor （ ODM ）を開いて下さい。
2. ODM メインメニューでは、Technician メニューに達するためにシフトT を押して下さい。
3. 『1』 を選択 して下さい（ 設定 ）。
4. 『5』 を選択 して下さい（ 設定 された製造情報 ）。
5. 『2』 を選択 して下さい（ 設定 された バックプレーン製造情報 ）。
6. 対応するプロンプトに従い、シリアル番号および MAC アドレスのようなデータを入力して下さい。 CS800 シャーシの上のこのデータを見つけることができます。
7. ボックスをリブートします。

## Q. CSS で常置敏速な変更を行なう方法

A. ユーザとしてフレッド CSS ボックスへのログインは、ログオン資格情報を使用し。 常置敏速な変更を行なうために、このコマンドを発行して下さい:

```
Css100#prompt Redsox
<cr>
Redsox#
```

変更を保存するためにこのコマンドを発行して下さい:

```
Redsox#save_profile
```

このコマンドはユーザがログオンするたびに、CSS が同じプロンプトを使用するようにユーザ プロファイルを保存します。 類似したの使用するこの操作か。か。 UNIX のリソース ファイルは、各ユーザ向けのユニークなプロファイルを作成します。

admin として CSS およびログインに戻るとき、プロンプトはこれらの変更を示しません。 変更はユーザ別です、従ってプロンプトを新しい変更を示してもらいたいと思う各ユーザ向けの**敏速な、save_profile** コマンドを発行する必要があります。

## Q. 作動可能 および ロックされた フラッシュ間の違いとは何か。

A. この例は **show version コマンドが**下記のものを表示するフラッシュするの各種タイプを示したものです:

```
CSS150-2#show version
Version:               ap0401049s (4.01 Build 49)
Flash (Locked):        3.10 Build 33
!--- This image is the original image that was installed on the CSS. !--- The image serves as a
backup in the event that the CSS is not able !--- to boot from the operational Flash because of
an image corruption. Flash (Operational):   5.00 Build 10-
!--- This is the image that currently runs on the CSS. Type: PRIMARY Licensed Cmd Set(s):
Standard Feature Set Enhanced Feature Set SSH Server
```

## Q. フラッシュするの異なるバージョンがある理由

A. ロックされたフラッシュはその CSS で最初にインストールされたソフトウェアのバージョンを示します。 バージョンは変わり、バックアップとしてだけ動作します。 動作中のFLASH のバージョンはその CSS で現在動作するバージョンです。

## Q. リモートポートから CSS のマネージメントポートにアクセスできない理由

A. Cisco WebNS のすべてのバージョンでは 5.03 より早い、マネージメントポートはルート可能なインターフェイスではないです。 バージョン 5.03 では、マネージメントポートにポートにルート可能なインターフェイスをするためにデフォルト ゲートウェイを追加できます。

## Q. テクニカル サポートは顧客が書くカスタムスクリプト キープアライブをサポートしますか。

A. いいえ、テクニカル サポート 顧客が書くキープアライブ スクリプトをサポートしません。

## Q. CSS ディスクからコア ファイルを取除く方法

A. **show core コマンドを**発行した後、コア ファイルのリストを見つける場合、2 つの方法の 1 つのファイルを取除くことができます:

**注:** コードのバージョンによって決まる使用する方式。

- CSS50-1(config)#**llama**
  *!--- This command places the CSS in debug mode.* CSS50-1(debug)#**clear core** *corefilename*

または

- CSS50-1(config)#**llama**
  *!--- This command places the CSS in debug mode.* CSS50-1(debug)#**dir c:/Core/?**
  *!--- This command lists the names of all the core !--- files in the c:/Core directory.*
  CSS50-1(debug)#**ap_file delete c:/Core/** *corefilename*
  *!--- This command deletes the specified core file.*

## Q. CSS の RADIUSサーバに認証するとき、"RADIUS-4 を得ます: RADIUS認証は

## 理由コード 2" エラーメッセージと失敗しました。 このメッセージはどういう意味ですか。

A. このエラーメッセージは応答が CSS に達し、問題があることを示します。 RADIUSサーバの管理上に型属性を設定 する失敗は問題の原因である場合もあります。 RADIUSサーバをチェックし、型属性を確認して下さい。

## Q. スティッキー テーブルはどのように大きく、何エントリの削除を引き起こしますか。

A. （ 利用可能 な モデルタイプおよびメモリによって決まる ） CSS に**スティッキー ソース IP** およびスティッキ Secure Socket Layer （ SSL ）のためのエントリが含まれている 32,000 か 128,000 スティッキー テーブルがあります。 スティッキー テーブルは CSS のスティッキー クッキーを維持しません。 CSS のスティッキー テーブルのエントリの削除はこの場合見られます:

- デフォルトで、FIFO 方式と。 エントリは 32,000 か 128,000 バッファまでの表にです完全残ります。 現時点で、どの New エントリにより CSS は FIFO に基づいてエントリを削除します。
- **sticky-inact-timeout** 分。 コンテンツルールでは、この例が示すので、CSS がスティッキー エントリを削除するイナクティビティタイムアウトを規定できます:`CSS50-1(config)#llama`
  `!--- This command places the CSS in debug mode.` `CSS50-1(debug)#dir c:/Core/?`
  `!--- This command lists the names of all the core !--- files in the c:/Core directory.`
  `CSS50-1(debug)#ap_file delete c:/Core/ corefilename`
  `!--- This command deletes the specified core file.` **注:** CSS はこれらの項目がすべて本当のときケースの次のスティッキー 要求を拒否します:**sticky-inact-timeout** パラメータは使用されます。CSS は 32,000 か 128,000 バッファが充満しました。No エントリはタイムアウトに約あります。
- コンテンツルール。 コンテンツルールの中断およびアクティブ化によって、そのルールに適用するスティッキーな テーブル エントリの削除は見られます。

詳細については、コンテンツルールのためのスティッキー パラメータを設定する資料を参照して下さい。

## Q. どのようにローテーションからサービスを奪取できますか。

A. コンテンツルールの設定を使って ( レイヤ3 は、レイヤ4、または、CSS 動作が異なりますサービスの手動中断によって、5 ) 基盤として層にして下さいサーバ Out Of Service を奪取 します。 何回も、Web 開発者は一時的にサービスを中断し、Webページへの管理変更を行なう必要があります。 これらの Web 変更が本番時間の間に発生する場合があるので手動サービス中断が発生するときサービスにある接続を止めたいと思いません。 手動サービス中断の間にサービスに更新を行って下さい。

この例はサンプル レイヤ5、レイヤ4 およびレイヤ3 コンテンツルールを示したものです:

```
CSS50-1(config)#llama
!--- This command places the CSS in debug mode. CSS50-1(debug)#dir c:/Core/?
!--- This command lists the names of all the core !--- files in the c:/Core directory. CSS50-
1(debug)#ap_file delete c:/Core/ corefilename
!--- This command deletes the specified core file.
```

CSS はコンテンツルールがレイヤ3 またはレイヤ4 であるとある接続を転換します。 レイヤ3 またはレイヤ4 コンテンツルールの下のサービスの中断が発生する場合、CSS は接続をその存在転換し、アクティブなサービスにそのそれぞれコンテンツルールの下ですべてのそれに続く TCP 要

求を転送します。

レイヤ5 コンテンツルールの下に常駐するサービスの手動中断によって、CSS はそのサービスによって関連付ける一部またはすべての接続をリセットします。

## Q. ネットワーク近接部品は機能拡張セットですか。

A. ネットワーク近接 機能は機能拡張セットの一部でし、追加ライセンスを必要とします。 適切なライセンスなしで CSS の**近さ**コマンドを発行することを試みる場合このエラーメッセージを受け取ります:

```
CSS50-1(config)#proximity db 0 tier1
                               ^
%% Invalid License to execute command.
This command belongs to the Proximity Database.  Refer
to the user manual or contact Cisco Systems, Inc for
further information concerning license keys.
```

ライセンスを購入するために、地元のCisco 再販売業者を参照して下さい。 ライセンスを購入し、置換を必要とする場合、licensing@cisco.com に電子メールを送信 して下さい。

## Q. show dos コマンドはどんな詳細を提供しますか。

A. Cisco CSS は下記のものを含めて最新攻撃 イベントについての詳細を表示することができます:

- 発信元および宛先 IP アドレス
- イベントタイプ
- 総発生

多重なら場合不正侵入は同じサービス拒否 （ DoS ）型および送信元 および 宛先アドレスと発生します、1 つのイベントとしてそれらをマージする試みがあります。 このマージはイベントのディスプレイを減らします。

下記のものを表示するために **show dos コマンドを**発行して下さい:

- 不正侵入の総数ので CSS のブート
- これらの不正侵入および最大数の種類は毎秒を攻撃します
- 攻撃の最初および最後の発生

この例は **show dos コマンド**からの出力を示したものです:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                        0 Maximum per second:                0
LAND Attacks:                       0 Maximum per second:                0
Zero Port Attacks:                  0 Maximum per second:                0
Illegal Src Attacks:                0 Maximum per second:                0
Illegal Dst Attacks:                0 Maximum per second:                0
Smurf Attacks:                      0 Maximum per second:                0


No attacks detected
```

このリストはコマンドが下記のものを表示したものですフィールドのそれぞれの簡潔な説明を提供します:

- —のでボックスのブート 検出する DoS攻撃の総数。 発生の数と共にリストに、下記に現われる不正侵入の種類の説明を見つけることができます。
- SYN—その TCP 接続は出典始まりますが、三方 TCP ハンドシェイクを完了するためにそれは確認応答 フレームと続かれません。
- —同一の送信元 および 宛先アドレスがあるパケット。 CSS は内部 IP アドレスがフローの送信元アドレスではないようにしません。 また、CSS は帯の送信元 および 宛先アドレスが等しくないようにしません。
- —出典か宛先TCP またはゼロと等しい User Datagram Protocol （UDP; ユーザ データグラム プロトコル）ポートが含まれている帯。**注:** SmartBits より古いソフトウェアはゼロと等しい送信元ポートまたは宛先ポートが含まれている帯を送信できます。 CSS は DoS攻撃としてそれらを記録 し、これらの帯を廃棄します。
- —不正 な 送信元アドレス。
- Dst —不正 な 宛先アドレス。
- —ブロードキャスト 宛先アドレスとの Ping。 CSS は誘導ブロードキャストをデフォルトで許可しません。 ブロードキャスト アドレスにインターネット制御メッセージ プロトコル（ICMP）エコーを使用します。 CSS はアクセス コントロール リスト（ACL）によってUDPエコーポートにアクセスをブロックできます。
- イベント 毎秒の最大数。 簡易 ネットワーク 管理 プロトコル （SNMP）トラップ 閾値を設定 するのに最大イベント毎第 2 情報を使用して下さい。**注:** イベント 毎秒の最大数はプラグイン可能 な小さい形式要素ごとの最大です（SFP）。 4 SFP まである場合がある CSS 11800 の場合、たとえば、最大レート 毎秒はディスプレイに現われる 4 倍の高い場合もあります数。**注:** 別の FAQ は CSS の DoS 保護をディセーブルにすることができるかどうか尋ねます。 返事はいいえあります DoS 保護はフロー 許可 プロセスの一部です。 DoS 保護の意図は CSS のリソース、また CSS の後ろのサーバを保護することです。 DoS は設定可能な項目ではないです。 意図は透過的である DoS のためプロトコルが正しくはたらくときです。 フロー セットアッププロセスは深く DoS 機能を含みます。 機能 ヘルプは CSS 高速経路リソースを節約し、CSS が到達するデバイスを保護します。 機能はソフトウェア バージョン 3.0 および それ以降に常にあります。

また可能性のある DoS攻撃の検出のためのある特定の SNMPトラップのセットアップを考慮して下さい。 利用可能 なトラップは次のとおりです:

- **snmp trap-type enterprise** — SNMP エンタープライズ トラップをイネーブルに設定し、トラップタイプを設定するために、**snmp trap-type enterprise コマンドを**発行して下さい。 すべてのトラップをディセーブルにするために **no snmp trap-type enterprise コマンドを**発行して下さい。 エンタープライズ トラップ オプションを設定する前にエンタープライズ トラップをイネーブルに設定して下さい。 DoS攻撃 イベントが発生するとき、ログオン失敗します、または CSS サービス遷移状態エンタープライズ トラップを生成することを CSS が可能にすることができます。
- ***dos_attack_type*** — DoS攻撃 イベントが発生するとき SNMP エンタープライズ トラップを生成します。 1 つのトラップ 生成は毎秒それの間の不正侵入の数が第 2 DoS 攻撃 の タイプ 設定のためのしきい値を超過する発生します。 次のオプションがあります。**dos 不正攻撃**—不正なアドレスのためのトラップを、出典か宛先生成します。 不正なアドレスは次のとおりです:ループバック 送信元アドレスブロードキャスト 送信元アドレスループバック 宛先アドレスマルチキャストソースアドレスその送信元アドレス所有します攻撃のこの型のためのデフォルト トラップしきい値は 1 毎秒です。**dos 土地攻撃**—同一の送信元 および 宛先アドレスがあるパケットのためのトラップを生成します。 攻撃のこの型のためのデフォルト トラップしきい値は 1 毎秒です。**dos PING 攻撃**— ping の数が閾値を超過するときトラップを生成します。 攻撃のこの型のためのデフォルト トラップしきい値は 30 毎秒です。**注:** このオプシ

ョンはピングオブデス DoS攻撃をトラッキングしません。**dos smurf 攻撃**—ブロードキャスト 宛先アドレスとの ping の数が閾値を超過するときトラップを生成します。 攻撃のこの型のためのデフォルト トラップしきい値は 1 毎秒です。**dos 同期信号攻撃**—出典は始まるが、それ超過する閾値を続かれないこと三方 TCP ハンドシェイクを完了するために TCP 接続の数が確認応答 フレームとときトラップを生成します。 攻撃のこの型のためのデフォルト トラップしきい値は 10 毎秒です。

### Q. スイッチの CSS 行のサービス拒否（DoS）記憶保護機構をオフにすることができますか。

A. CSS（Cisco WebNS）のためのソフトウェアの現在行では、DoS 記憶保護機構をディセーブルにするオプションがありません。

### Q. サービス拒否（DoS）保護カウンターを消すことができますか。

A. DoS/SYN 不正侵入を記録 するカウンターをディセーブルにするオプションがありません。

**注:** DoS および SYN不正侵入に関する詳細については、提供しなさいかどんな詳細が show dos コマンドをするか FAQ ことをへの応答参照して下さいか。

### Q. アクセス リストでポート範囲を使用する方法

A. Access Control List（ACL）のポート範囲の使用は簡素化するを設定するいくつかの TCP User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポートのためのユーザアクセスをブロックしたいと思う状況がある ACL の数助けます。 たとえばネットワークの外からのボックスに入って来るすべてのユーザ向けのポート 20 ー 23 をブロックしたいと思うことを、仮定して下さい。 最初に CSS の外部ネットワークか公衆側が VLAN 2 にあると、仮定して下さい。 またネットワークの内部かサーバ側が VLAN 1.にあると仮定して下さい。 ACL構成は次のとおりです:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                        0 Maximum per second:                  0
LAND Attacks:                       0 Maximum per second:                  0
Zero Port Attacks:                  0 Maximum per second:                  0
Illegal Src Attacks:                0 Maximum per second:                  0
Illegal Dst Attacks:                0 Maximum per second:                  0
Smurf Attacks:                      0 Maximum per second:                  0


No attacks detected
```

## 関連情報

- Cisco CSS 11000 シリーズ用の販売発表の終わり
- Cisco CSS 11000 シリーズ コンテンツ サービス スイッチ 速報
- CSS 11000 シリーズ コンテンツ サービス スイッチ テクニカル サポート
- Software Center（ダウンロード）-コンテンツネットワーキング（登録ユーザのみ）
- テクニカルサポートとドキュメント - Cisco Systems