Content Services Switch FAQ

Contenido

Introducción
¿Dónde puedo encontrar el MIB para el CSS?
¿Cuál es el número máximo de keepalives en secuencia de comandos que el CSS soporte?
¿Cómo limpio o elimino archivos core?
¿Dónde puedo encontrar interpretaciones de los mensajes del registro?
¿Existe un comando que controle la frecuencia de envíos de informes de carga entre pares?
¿Las claves de licencia cambian con las versiones de código?
Perdí mi llave de la licencia. ¿Qué hago?
¿Cuál es el tiempo predeterminado para la retención de una entrada en una tabla fija?
¿Cómo configuro a la máscara fija para cubrir las peticiones de un proxy mega como America Online (AOL)?
¿Por qué hay ninguna opción para Sticky cuando utilizo la Secure Socket Layer de equilibrio avanzado (SSL)?
¿Qué tipo de cifrado el Content and Application Peering Protocol (CAPP) o el protocolo application peering (APP) utiliza?
¿Qué significa el mensaje "arp gratuito"?
¿Cómo sincronizo las configuraciones de CSS en el modo de fallo?
¿Qué configuración debo utilizar en un programa para terminal?
¿Hay una manera de reprogramar la dirección MAC en un CSS?
¿Cómo realizo un cambio pronto permanente en el CSS?
¿Cuál es la diferencia entre el Flash operativa y bloqueada?
¿Por qué hay diversas versiones del Flash?
¿Por qué no puedo acceder el puerto de administración del CSS de un puerto remoto?
¿El Soporte técnico de Cisco soporta el Keepalives de la secuencia de comandos personalizada que el cliente escribe?
¿Cómo quito los archivos núcleo del disco CSS?
Cuando autentico a un servidor de RADIUS con mi CSS, consigo el "RADIUS-4: Autenticación de RADIUS fallada con el mensaje de error del código de motivo el 2". ¿Qué significa el mensaje?
¿Cómo grande es la tabla fija, y qué causa la eliminación de entradas?
¿Cómo puedo sacar un servicio de la rotación?
¿Es la parte de la proximidad de la red el conjunto de características mejoradas?
¿Qué detalles el comando show dos proporciona?
¿Puedo apagar la función de telefonía de la negación de servicio (DOS) en la línea CSS de Switches?
¿Puedo apagar los contadores de la protección de la negación de servicio (DOS)?
¿Cómo utilizo los rangos de puertos en las Listas de acceso?
Información Relacionada

Introducción

Este documento aborda las preguntas más frecuentemente (FAQ) sobre Cisco Content Services Switch (CSS).

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Q. ¿Dónde puedo encontrar el MIB para el CSS?

A. El MIB está ya en el CSS. Usted puede considerar el CSS un agente en el esquema de la red del Simple Network Management Protocol (SNMP). Todo lo que usted necesita hacer es configurar los parámetros SNMP en el CSS. Refiera al documento que configura el Simple Network Management Protocol (SNMP) para más información.

Q. ¿Cuál es el número máximo de keepalives en secuencia de comandos que el CSS soporte?

A. El número máximo de keepalives en secuencia de comandos que el CSS soporte es 255. Refiera a las *nuevas funciones en la* sección de la *versión de software 5.00 del* Release Note para el Content Services Switch de las Cisco 11000 Series.

Q. ¿Cómo limpio o elimino archivos core?

A. Publique el **comando clear core**. El comando está disponible en la versión 5.00 y posterior del software CSS, en el modo del debug. La sintaxis es la siguiente:

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

Q. ¿Dónde puedo encontrar interpretaciones de los mensajes del registro?

A. Para las interpretaciones de los mensajes del registro, refiera a los mensajes del registro del documento.

Q. ¿Existe un comando que controle la frecuencia de envíos de informes de carga entre pares?

A. Puede utilizar el comando dns-peer interval. Hay también los comandos adicionales que usted puede configurar localmente para alcanzar una medida más rápida de la carga local:

- **ageout-temporizador** — Fija la época (en los segundos) del ageout de la información de la carga vieja.
- **desmontaje-temporizador** — Fija el período de tiempo máximo (en los segundos) que el sistema espera para enviar un informe de desconexión.

Q. ¿Las claves de licencia cambian con las versiones de código?

A. ¿Las claves de licencia no cambian con las versiones de código?

Q. Perdí mi llave de la licencia. ¿Qué hago?

A. Envíe un correo electrónico con el número de serie de su CSS a licensing@cisco.com. **El comando version** visualiza el paquete de características, pero no la llave de la licencia.

Q. ¿Cuál es el tiempo predeterminado para la retención de una entrada en una tabla fija?

A. A menos que usted utilice el comando sticky-inact-timeout, no hay tiempo predeterminado. La tabla fija se guarda en un basado en FIFO (32,000 o 128,000 entradas, según el tipo de dispositivo y la memoria disponibles), o hasta la reinicialización del CSS.

Q. ¿Cómo configuro a la máscara fija para cubrir las peticiones de un proxy mega como America Online (AOL)?

A. Si una aplicación requiere a un usuario ser pegada para la vida entera de la sesión, considere una capa 3 Sticky. Una capa 3 Sticky pega a un usuario a un servidor en base de la dirección IP del usuario. El CSS tiene una tabla fija de 32,000, así que significa que cuando 32,000 usuarios simultáneos están en el sitio, los abrigos de la tabla y los primeros usuarios hacen “despegados”. Sin embargo, el volumen de su sitio puede ser tal que usted tiene más de 32,000 en un momento de los usuarios. O un gran porcentaje de sus clientes puede venir a usted con un proxy mega. En estos casos, considere el uso de un diverso método simple (tal como el Cookie, el cookieurl, o el URL) o un aumento de su máscara fija. La máscara persistente predeterminada es 255.255.255.255, lo que significa que cada entrada en la tabla persistente es una dirección de IP individual. Algunas de las mega proxies tienen una situación en cuál el usuario durante la vida de una sesión utiliza varios diversos IP Addresses en un rango de direcciones. Esta situación hace algunas de las conexiones TCP conseguir pegadas a un servidor, y puede hacer otras conexiones conseguir pegadas a un diverso servidor para la misma transacción. Un resultado puede ser la pérdida de algunos elementos del carro de compras. Si usted no puede utilizar uno de los métodos más avanzados de pegarse, utilice a la máscara fija de 255.255.240.0 cuando su base del cliente viene con una de estas mega proxies.

Q. ¿Por qué hay ninguna opción para Sticky cuando utilizo la Secure Socket Layer de equilibrio avanzado (SSL)?

A. El Advanced balance SSL es lo mismo que el SSL Sticky.

Q. ¿Qué tipo de cifrado el Content and Application Peering Protocol (CAPP) o el protocolo application peering (APP) utiliza?

A. Por abandono, CAPP utiliza el no encryption. Usted puede configurar a la sesión de APP para utilizar la publicación de mensaje 5 (MD5). El tipo de encripción debe ser lo mismo en ambos pares para que la sesión de APP suba.

Q. ¿Qué significa el mensaje "arp gratuito"?

A. Cuando el switch de backup no detecta un latido del corazón del switch maestro en el plazo de 3 segundos, las transiciones del switch de backup para sentir bien al master y envían un mensaje “arp gratuito”. El mensaje indica una transmisión del Address Resolution Protocol (ARP) del nuevo

switch maestro. El mensaje contiene la dirección MAC del switch maestro actual. El arp gratuito es habilitado por el **IP gratuito-ARP** ordena en el modo de configuración global. No puede ser habilitado en una sola interfaz y bloquearla en otras interfaces.

Q. ¿Cómo sincronizo las configuraciones de CSS en el modo de fallo?

A. Para sincronizar las configuraciones en la versión de software 4.0, utilice el **comando commit config sync**. Para sincronizar las configuraciones en el código de la versión de software 3.10, usted debe utilizar el FTP para mover la configuración a partir de un Switch a otro. Para sincronizar las configuraciones en las versiones de software 6.x y 7.x cifre, utilice el comando commit_redundancy para el active/el recurso seguro o la Redundancia de casilla a casilla. O usted puede utilizar el comando commit_vip_redundancy para IP virtual (VIP) la Redundancia /interface. Usted puede utilizar el comando show script commit_redundancy para ver en la encabezado del script las opciones de la línea de comandos disponibles para el script del **commit_redundancy**. Lo mismo se aplica al **comando commit_vip_redundancy**.

Q. ¿Qué configuración debo utilizar en un programa para terminal?

A. Utilice estas configuraciones:

- 9600 baudios
- 8 bits
- Sin paridad
- 1 bit de parada
- Sin control de flujo

Q. ¿Hay una manera de reprogramar la dirección MAC en un CSS?

A. Sí, hay una manera.

Nota: Puede encontrar la dirección MAC y el número de serie en la parte posterior de la unidad.

Complete estos pasos para reprogramar el número de serie y la dirección MAC. Este ejemplo es para una dirección MAC en el chasis CS800:

1. Abra el **Offline Diagnostic Monitor (ODM)**.
2. En el menú principal ODM, presione la **rotación-T** para alcanzar el menú del técnico.
3. Elija **1** (configuración).
4. Elija **5** (fije la información de la fabricación).
5. Elija **2** (fije la información de la fabricación del backplane).
6. Siga el prompt y ingrese los datos que corresponden, por ejemplo el número de serie y el MAC address. Usted puede encontrar estos datos sobre el top del chasis CS800.
7. Reiniciar el equipo

Q. ¿Cómo realizo un cambio pronto permanente en el CSS?

A. Inicie sesión al cuadro CSS como usuario fred, y utilice sus credenciales del login. Para realizar un cambio pronto permanente, publique este comando:

```
Css100#prompt Redsox
```

```
<cr>
Redsox#
```

Publique este comando de salvar el cambio:

```
Redsox#save_profile
```

Este comando guarda el perfil del usuario de modo que cada vez que el usuario abre una sesión, el CSS utilice el mismo prompt. ¿Esta acción, similar utilizar del**?.?** los archivos de recurso en UNIX, crean un perfil único para cada usuario.

Cuando usted vuelve al CSS y inicia sesión como admin, el prompt no refleja estos cambios. Los cambios son específicos del usuario, así que usted necesita publicar los **comandos prompt y save_profile** para cada usuario que quiera hacer que el prompt refleje el nuevo cambio.

Q. ¿Cuál es la diferencia entre el Flash operativa y bloqueada?

A. Este ejemplo muestra los diversos tipos de Flash que el **comando show version** visualiza:

```
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. ¿Por qué hay diversas versiones del Flash?

A. El Flash bloqueada muestra la versión de software que fue instalada originalmente en ese CSS. La versión sigue siendo lo mismo y sirve solamente como respaldo. La versión en el Flash operacional es la versión que se ejecuta actualmente en ese CSS.

Q. ¿Por qué no puedo acceder el puerto de administración del CSS de un puerto remoto?

A. En todas las versiones de Cisco WebNS que sean anteriores de 5.03, el puerto de administración no es una interfaz enrutable. En la versión 5.03, usted puede agregar un default gateway al puerto de administración para hacer el puerto una interfaz enrutable.

Q. ¿El Soporte técnico de Cisco soporta el Keepalives de la secuencia de comandos personalizada que el cliente escribe?

A. No, Soporte técnico de Cisco no soporta los scripts del keepalive que un cliente escribe.

Q. ¿Cómo quito los archivos núcleo del disco CSS?

A. Si, después de que usted publique el **comando show core**, usted encuentra una lista de archivos núcleo, usted puede quitar los archivos en una de dos maneras:

Nota: El método que usted utiliza depende de la versión del código.

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

o

- ```
  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. Cuando autentico a un servidor de RADIUS con mi CSS, consigo el "RADIUS-4: Autenticación de RADIUS fallada con el mensaje de error del código de motivo el 2". ¿Qué significa el mensaje?

A. Este mensaje de error indica que la contestación ha alcanzado el CSS y hay un problema. Un error fijar el atributo de tipo de servicio a administrativo en el servidor de RADIUS puede ser la causa del problema. Marque al servidor de RADIUS y verifique los atributos de tipo de servicio.

Q. ¿Cómo grande es la tabla fija, y qué causa la eliminación de entradas?

A. El CSS tiene (que depende del tipo de modelo y de la memoria disponibles) una tabla fija 32,000 o 128,000 que contenga las entradas para el fuente-**IP Sticky** y el Secure Socket Layer (SSL) Sticky. La tabla fija no mantiene las cookies fijas en el CSS. La eliminación de entradas en la tabla fija en el CSS ocurre en estas situaciones:

- Por abandono, con un Método FIFO. Sigue habiendo las entradas en la tabla hasta los 32,000 o los 128,000 que el buffer es lleno. Ahora, cualquier nueva entrada hace el CSS quitar una entrada en base del (Primero en Entrar, Primero en Salir FIFO).
- minutos del **Sticky-inact-timeout**. En una regla de contenido, usted puede especificar el tiempo de espera de inactividad por el cual el CSS quita una entrada fija, pues este ejemplo muestra:
  ```
  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.
  ```
  Nota: El CSS rechaza la petición fija siguiente en un caso cuando todos estos elementos son verdades:Se utiliza el parámetro del **Sticky-inact-timeout**.El CSS ha llenado el buffer 32,000 o 128,000.No hay entradas alrededor al descanso.
- Regla de contenido. Con la suspensión y la reactivación de una regla de contenido, el retiro de las entradas de tabla fija que se aplican a esa regla ocurre.

Para más información, refiera al documento que configura los parámetros fijos para las reglas de contenido.

Q. ¿Cómo puedo sacar un servicio de la rotación?

A. Con la configuración de la regla de contenido (la capa 3, la capa 4, o acode 5) como base, el CSS se comporta diferentemente con la suspensión manual de un servicio, que toma un Out Of Service del servidor. Muchas veces, los desarrolladores Web necesitan suspender un servicio y realizar temporalmente los cambios de la administración a las páginas web. Porque estos cambios de la red pueden ocurrir durante las horas de producción, usted no quiere matar a las conexiones que existen al servicio o a los servicios cuando ocurre la suspensión de servicio manual. Realice las actualizaciones a un servicio durante la suspensión de servicio manual.
  ```

Este ejemplo muestra la capa 5 de la muestra, la capa 4, y acoda 3 reglas de contenido:

```
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.
```

El CSS desvía las conexiones que existen cuando las reglas de contenido son la capa 3 o la capa 4. Si ocurre la suspensión de un servicio bajo regla de contenido de la capa 3 o de la capa 4, el CSS desvía cualquier conexión que exista y adelante todo el TCP subsiguiente pide al servicio activo bajo esa regla de contenido respectiva.

Con la suspensión manual de un servicio que resida bajo regla de contenido de la capa 5, el CSS reajusta cualquiera o todas las conexiones que se asocien a ese servicio.

Q. ¿Es la parte de la proximidad de la red el conjunto de características mejoradas?

A. Las características de la proximidad de la red no son parte del conjunto de características mejoradas y requieren una licencia adicional. Si usted intenta publicar los **comandos proximity** en el CSS sin la licencia apropiada, usted recibe este mensaje de error:

```
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.
```

Para comprar una licencia, vea a su revendedor del Cisco local. Si usted compró una licencia y necesita un reemplazo, envíe un correo electrónico a licensing@cisco.com.

Q. ¿Qué detalles el comando show dos proporciona?

A. El Cisco CSS puede visualizar los detalles sobre la mayoría de los eventos de ataque reciente, que incluyen:

- Direcciones IP de origen y de destino
- El tipo de evento
- Acontecimientos totales

Si es múltiple los ataques ocurren con el mismo tipo y direcciones de origen y de destino de la negación de servicio (DOS), hay una tentativa de combinarlas como un evento. Esta fusión reduce la visualización de los eventos.

Publique el **comando show dos** para visualizar:

- El número total de ataques puesto que el inicio del CSS
- Los tipos de ataques y el número máximo de estos ataques por segundo
- El primer y la última aparición de un ataque

Este ejemplo muestra la salida del **comando show dos**:

```
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
```

Esta lista proporciona una Breve descripción de cada uno de los campos que el comando visualiza:

- `Ataques totales` — El número total de ataques DOS que fueron detectados puesto que el inicio del cuadro. Usted puede encontrar una descripción del tipo de ataques que aparezcan en la lista, junto con el número de acontecimientos, abajo.
- `Ataques SYN` — No se siguen las conexiones TCP que una fuente inicia pero que con una trama del acuse de recibo para completar la aceptación decontacto con TCP de tres vías.
- `Ataques de la PISTA` — Cualquier paquetes que tengan las direcciones de origen y de destino idénticas. El CSS no permite que los IP Address internos sean la dirección de origen de un flujo. También, el CSS no permite que las direcciones de origen y de destino de los bastidores sean iguales.
- `Ataques cero del puerto` — Capítulos que contienen la fuente o el TCP de destino o los puertos del User Datagram Protocol (UDP) que son iguales a cero.**Nota:** Un más viejo software del SmartBits puede enviar las tramas que contienen los puertos de origen o de destino iguales a cero. El CSS los registra como ataques DOS y cae estas tramas.
- `Ataques ilegales del src` — Direcciones de origen ilegales.
- `Ataques ilegales del dst` — Direcciones destino ilegales.
- `Ataques smurf` — Ping con una dirección destino del broadcast. El CSS no permite los broadcastes dirigidos por abandono. `Un ataque smurf` utiliza una generación de eco del Internet Control Message Protocol (ICMP) a una dirección de broadcast. El CSS puede bloquear el acceso a los puertos de eco de UDP vía el Listas de control de acceso (ACL).
- `Máximo por segundo` — El número máximo de eventos por segundo. Utilice la máximo-evento-por-segunda información para fijar los valores de umbral del Trap del Simple Network Management Protocol (SNMP).**Nota:** El número máximo de eventos por segundo es el máximo por el (SFP) enchufable del pequeño factor de forma. Para un CSS11800, por ejemplo, que puede tener hasta cuatro SFP, la velocidad máxima por segundo puede ser tan alta como cuatro veces el número que aparece en la visualización.**Nota:** Otro FAQ pregunta si usted puede inhabilitar el protección DoS en el CSS. La respuesta es no. El protección DoS es parte del proceso de la admisión del flujo. El intención de protección DoS es proteger los recursos en el CSS así como los servidores detrás del CSS. El DOS no es un elemento configurable. La intención está para que el DOS sea transparente cuando los protocolos trabajan correctamente. El proceso de configuración del flujo implica profundamente las características DOS. La ayuda de las características el CSS conserva los recursos del trayecto rápido y protege los dispositivos que el CSS alcanza. Las características están siempre presentes en el 3.0 de la versión de software y posterior.

También considere la configuración de cierto SNMP traps para la detección de ataques posibles DOS. Los desvíos disponibles son:

- **empresa del tipo de trampa SNMP** — Para habilitar las trampas Enterprise SNMP y configurar los tipos de trampa, publique el **comando snmp trap-type enterprise**. Publique el **comando no snmp trap-type enterprise** para inhabilitar todos los desvíos. Usted debe habilitar

las trampas Enterprise antes de que usted configure una opción de la trampa Enterprise. Usted puede permitir al CSS para generar las trampas Enterprise cuando ocurren los evento de ataque DoS, un login falla, o un estado de transiciones del servicio CSS.
- *dos_attack_type* — Genera las trampas Enterprise SNMP cuando ocurre un evento de ataque DoS. Una generación de trampa ocurre cada segundo en que el número de ataques durante eso excede en segundo lugar el umbral para la configuración del ataque-tipo DOS. Las opciones son:**DOS-ilegal-ataque** — Genera los desvíos para las extensiones ilegales, fuente o destino. Las extensiones ilegales son:Direcciones de origen del loopbackDirecciones de origen del broadcastDirecciones destino del loopbackDirecciones de origen multicastLas direcciones de origen esas usted poseeEl umbral de trampa predeterminado para este tipo de ataque es uno por segundo.**DOS-pista-ataque** — Genera trampas para paquetes que tienen las direcciones de origen y de destino idénticas. El umbral de trampa predeterminado para este tipo de ataque es uno por segundo.**DOS-ping-ataque** — Genera los desvíos cuando el número de ping excede el valor de umbral. El umbral de trampa predeterminado para este tipo de ataque es 30 por segundo.**Nota:** Esta opción no sigue los ataques DOS de los ping de la muerte.**DOS-smurf-ataque** — Genera los desvíos cuando el número de ping con una dirección destino del broadcast excede el valor de umbral. El umbral de trampa predeterminado para este tipo de ataque es uno por segundo.**DOS-SYN-ataque** — Genera los desvíos cuando el número de conexiones TCP que una fuente inicie pero que no se sigue con una trama del acuse de recibo para completar la aceptación decontacto con TCP de tres vías excede el valor de umbral. El umbral de trampa predeterminado para este tipo de ataque es 10 por segundo.

Q. ¿Puedo apagar la función de telefonía de la negación de servicio (DOS) en la línea CSS de Switches?

A. En la línea actual de software para el CSS (Cisco WebNS), no hay opción para inhabilitar la característica de protección DoS.

Q. ¿Puedo apagar los contadores de la protección de la negación de servicio (DOS)?

A. No hay opción para inhabilitar los contadores que registran los ataques DoS/SYN.

Nota: Para más información sobre el DOS y los Ataques SYN, vea que la respuesta al FAQ qué detalles hacen el comando show dos proporcione?.

Q. ¿Cómo utilizo los rangos de puertos en las Listas de acceso?

A. El uso de los rangos de puertos en una lista de control de acceso (ACL) ayuda a simplificar el número de ACL que hacia el lado de babor usted configuración, dada una situación en la cual usted quiera bloquear acceso del usuario para el User Datagram Protocol (UDP) algún TCP/vire. Por ejemplo, suponga que usted quiere bloquear los puertos 20 a 23 para todos los usuarios que entren en el cuadro fuera de su red. Primero, asuma que la red externa o el lado público del CSS está en el VLAN2. También asuma que el interno o el lado del servidor de la red está en el VLAN1. La configuración ACL es:

```
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
```

Información Relacionada

- Final del aviso de la venta para el Cisco CSS 11000 Series
- Boletines del Switches de servicios de contenido Cisco CSS de la serie 11000
- Soporte técnico de los CSS 11000 Series Content Services Switch
- Centro de software (descargas) - Redes de contenido (clientes registrados solamente)
- Soporte Técnico y Documentación - Cisco Systems