Configuración de los Mecanismos de Manejo de Fallas y de Servidor Inalcanzable para la Resolución de Fallas de OCS en el ASR5K

Contenido

Introducción

Este documento describe cómo configurar los mecanismos de gestión de fallos (FH) y de servidor inalcanzable (SU) en la interfaz Gy para resolver los problemas que se encuentran en el sistema de carga en línea (OCS) o en lo que respecta a la conectividad entre la función de aplicación de políticas y cargas (PCEF) y OCS. La información que se describe en este documento se aplica a las funciones Home Agent (HA), Gateway General Packet Radio Service (GPRS) Support Node (GGSN) y Packet Data Network Gateway (PGW) que se ejecutan en el router de servicios agregados (ASR5K) de Cisco serie 5000.

Prerequisites

Requirements

Cisco recomienda que su sistema cumpla estos requisitos para utilizar los mecanismos FH y SU:

- El servicio de cobro mejorado (ECS) está disponible
- El PCEF existe dentro de HA, GGSN o PGW
- Hay conectividad de diámetro adecuada a través de la base de datos
- La aplicación de control de crédito de diámetro (DCCA) está disponible

Componentes Utilizados

La información en este documento se basa en todas las versiones del ASR5K.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El PCEF se conecta al OCS a través de la interfaz Gy, que utiliza Diámetro como protocolo base y DCCA. Este es el flujo de mensajes entre el PCEF y el OCS:

- **Solicitud de control de crédito (CCR)** âÂ Â Este mensaje se envía desde el PCEF al OCS. Hay tres tipos de mensajes CCR: Inicial, Actualizar y Terminar.
- **Respuesta de control de crédito (CCA)** âÂ Â Este mensaje se envía desde el OCS al PCEF en respuesta al CCR. También hay tres tipos de mensajes CCA: Inicial, Actualizar y Terminar.
- **Solicitud de reautorización (RAR)** âÂ Â Este mensaje se envía desde el OCS al PCEF cuando se requiere una nueva autorización de sesión.
- **Respuesta de reautorización (RAA)** âÂ Â Esta es la respuesta al RAR desde el PCEF al OCS.

La conectividad de diámetro se establece entre el PCEF y el OCS para habilitar el flujo de mensajes. Existe la posibilidad de que el OCS envíe mensajes negativos, la conexión de transporte podría fallar entre el PCEF y el OCS, o el mensaje podría agotarse el tiempo de espera, lo que podría causar una falla en el establecimiento de la sesión del suscriptor. Esto puede impedir que el suscriptor utilice los servicios.

Estos dos mecanismos se pueden utilizar para resolver este problema:

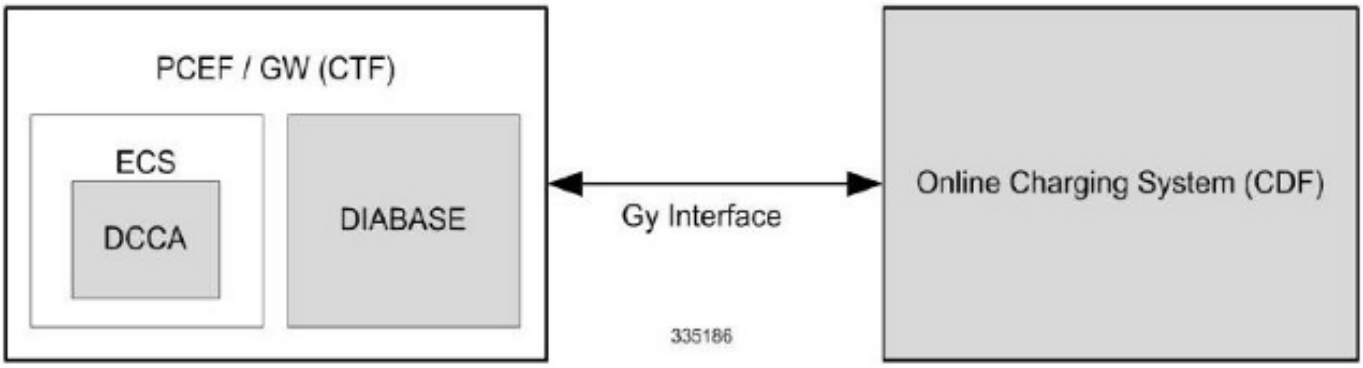
- El mecanismo FH
- El mecanismo SU

Configurar

Esta sección describe las configuraciones necesarias para soportar los mecanismos FH y SU.

Diagrama de la red

La información en este documento utiliza esta topología:



Tx-Expiry

Este es un temporizador de nivel de aplicación para la DCCA que se puede configurar en la configuración *de control de crédito de diámetro*. El valor puede oscilar entre 1 y 300 segundos.

Aquí tiene un ejemplo:

```
[local]host_name(config-dcca)# diameter pending-timeout
```

Tiempo de espera de respuesta

Se trata de un tiempo de espera de la base de datos y se puede configurar en la configuración del *punto final de diámetro*. El valor puede oscilar entre 1 y 300 segundos.

> **Nota:** El valor configurado para este temporizador debe ser mayor que el utilizado para el temporizador Tx-Expiry.

Aquí tiene un ejemplo:

```
[context_name]host_name(config-ctx-diameter)# response-timeout
```

Conmutación por fallo de sesión de diámetro

Esta función se utiliza para habilitar o inhabilitar el failover de la sesión de control de crédito del diámetro, que permite al sistema utilizar un servidor secundario cuando el servidor primario se vuelve inalcanzable. Esto se puede configurar en la configuración *de control de crédito del diámetro*.

Aquí tiene un ejemplo:

```
local]host_name(config-dcca)# diameter session failover
```

Mecanismo FH

El mecanismo FH sólo funciona si existe una conmutación por fallas de sesión de diámetro. La FH permite al sistema elegir si continuar la sesión y convertirse a desconectado, o si terminar la sesión cuando se produce un error de nivel de conexión o de mensaje.

> **Nota:** El FH está habilitado y configurado de forma predeterminada.

Configuración del Mecanismo FH

El mecanismo FH se puede configurar en la configuración *de control de crédito de diámetro*. Esta es la sintaxis que se utiliza en la configuración de FH:

```
failure-handling { initial-request | terminate-request | update-request } { continue
[ go-offline-after-tx-expiry | retry-after-tx-expiry ] | retry-and-terminate,
[ retry-after-tx-expiry ] | terminate }
```

La primera sección especifica el *tipo de solicitud*: Inicial (CCR-I), Actualizar (CCR-U) y Terminar (CCR-T).

La segunda sección especifica la *acción* que debe realizarse cuando se activa el mecanismo FH. Estas tres acciones son posibles con el mecanismo FH:

- **Continue** âÂ Â Esto permite que la sesión continúe y la convierte en desconectada. Esta función utiliza dos opciones relacionadas con la caducidad de Tx:

  Go-offline-after-tx-âÂ Â Esto comienza a cargarse fuera de línea después de que se produce el vencimiento del Tx.

  Retry-after-tx-caducidad âÂ Â Esto reintenta el servidor secundario después de que se produce el vencimiento Tx.

- **Retry-and-end** âÂ Â Esto finaliza la sesión después de que el sistema reintente el servidor secundario, si el servidor secundario tampoco está disponible. Esto también utiliza la opción **Retry-after-tx-caducidad**, que reintenta el servidor secundario después de que se produce el

vencimiento Tx.

- **Terminate** âÂ Â Esto finaliza la sesión sin ningún intento de contactar con el servidor secundario.

Comportamiento predeterminado del mecanismo FH

Esta sección describe el comportamiento predeterminado de FH cuando no hay ninguna configuración presente. De forma predeterminada, el mecanismo FH se activa durante un tiempo de espera de respuesta (RT), excepto cuando se configura la acción *Terminar*.

Si se recibe del servidor *un* par de valores de atributos (AVP) de *control de crédito-fallo-manejo*, se aplican los parámetros recibidos.

A continuación, se incluyen algunos ejemplos:

- **Petición inicial > Finalizar**
- **Update-Request > Retry-and-Terminate**
- **Terminate-Request > Retry-and-Terminate**

Flujo de llamadas detallado del mecanismo FH

Esta sección describe el flujo de llamadas detallado del mecanismo FH con todas las opciones posibles.

Solicitud inicial

Configuración de CCFH	Comando CLI	Comportamiento en Tx	Comportamiento en RT	El secundario está activo	El secundario está
Continúe	petición inicial continúe	N/A	Continúe	Secundario se hace cargo después de RT	Fuera de línea des RT. No se realizan má cuota para cualquier gru clasificación dentr después de la falla (incluso si se restaura la con DCCA)
	petición inicial continue go-offline-after vencimiento de TX	Fuera de línea	N/A	Sin conexión en Tx	Sin conexión en T
	petición inicial continue retry-after vencimiento de TX	Continúe	N/A	Secundario se hace cargo después de Tr	Sin conexión desp
Reintentar y finalizar	petición inicial retry-and-end	N/A	Reintentar	Secundario se hace cargo	Terminar después

	petición inicial retry-and-end retry-after-tx-term	Reintentar	N/A	después de RT Secundario se hace cargo después de Tr	Terminar después
Terminar	petición inicial finalizar	Terminar	N/A	Terminar después de Tx	Terminar después

Solicitud de actualización

Configuración de CCFH	Comando CLI	Comportamiento en Tx	Comportamiento en RT	El secundario está activo	El secundario está inactivo
Continúe	update-request continúe	N/A	Continúe	Secundario se hace cargo después de RT	Fuera de línea después de ot RT
	update-request continue go-offline-after vencimiento de TX	Fuera de línea	N/A	Sin conexión en Tx	Sin conexión en Tx
	update-request continue retry-after vencimiento de TX	Continúe	N/A	Secundario se hace cargo después de Tr	Sin conexión después de otro
Reintentar y finalizar	update-request retry-and-end	N/A	Reintentar	Secundario se hace cargo después de RT	Envía CCR-T después de otro
	update-request retry-and-end retry-after-tx-term	Reintentar	N/A	Secundario se hace cargo después de Tr	Envía CCR-T después de otro
Terminar	update-request finalizar	Terminar	N/A	Envía CCR-T después de Tx	Envía CCR-T después de Tx

Terminate-Request (Pedido de finalización)

Configuración de CCFH	Comando CLI	Comportamiento en Tx	Comportamiento en RT	El secundario está activo	El secundario está inactivo
Continúe	terminate-request (pedido de finalización) continúe	N/A	Reintentar	CCR-T se envía a secundario después de RT	Terminar después de otra RT
	terminate-request (pedido de finalización) continue go-offline-	Reintentar	N/A	CCR-T se envía a secundario después de	Terminar después de otro Tx

	after vencimiento de TX terminate-request (pedido de finalización) continue retry-after vencimiento de TX	Reintentar	N/A	Tx CCR-T se envía a secundario después de Tx	Terminar después de otro Tx
Reintentar y finalizar	terminate-request (pedido de finalización) retry-and-end	N/A	Reintentar	CCR-T se envía a secundario después de RT	Terminar después de otra RT
	terminate-request (pedido de finalización) retry-and-end retry-after-tx-term	Reintentar	N/A	CCR-T se envía a secundario después de Tx	Terminar después de otro Tx
Terminar	terminate-request (pedido de finalización) finalizar	Terminar	N/A	Terminar después Tr	Terminar después de Tx

Mecanismo SU

El mecanismo SU es similar al mecanismo FH, pero proporciona un control más granular sobre los procedimientos de falla. Además de la continuación de la sesión después de las fallas del nivel de mensaje y de conexión (transporte), este mecanismo se puede utilizar cuando las respuestas son lentas con respecto al OCS. También proporciona las opciones para continuar la sesión durante algún tiempo/agotamiento de la cuota antes de la finalización, o para utilizar la cuota provisional configurable (volumen y tiempo) y los reintentos de servidor configurables antes de convertir una sesión en desconectada o terminada.

Configuración del mecanismo SU

El mecanismo SU se puede configurar en la configuración *de control de crédito del diámetro*. La sintaxis que se utiliza en la configuración de la SU varía según la versión utilizada.

Para las versiones 12.1 y anteriores, esta es la sintaxis que se utiliza para la configuración del mecanismo SU:

```
servers-unreachable { initial-request { continue | terminate [ after-timer-expiry
<timeout_period> ] } | update-request { continue | terminate [ after-quota-expiry
| aftertimer-expiry <timeout_period> ] } }
```

Para las versiones 12.2 y posteriores, ésta es la sintaxis que se utiliza para la configuración del mecanismo SU:

```
servers-unreachable { behavior-triggers { initial-request | update-request }
result-code { any-error | <result-code> [ to <end-result-code> ] }
| transport-failure [ response-timeout | tx-expiry ] | initial-request
```

```
{ continue [ { [ after-interim-time <timeout_period> ] [ after-interim-volume
<quota_value> ] } server-retries <retry_count> ] | terminate [ {
[ after-interim-time <timeout_period> ] [ after-interim-volume <quota_value> ]
} server-retries <retry_count> | after-timer-expiry <timeout_period> ] }
| update-request { continue [ { [ after-interim-time <timeout_period> ]
[ after-interim-volume <quota_value> ] } server-retries <retry_count> ]
| terminate [ { [ after-interim-time <timeout_period> ] [ after-interim-volume
<quota_value> ] } server-retries <retry_count> ] | after-quota-expiry |
after-timer-expiry <timeout_period> ] } }
```

> **Nota:** En las versiones anteriores a la versión 12.2, había flexibilidad para configurar los mecanismos FH y SU de forma independiente; sin embargo, en las versiones 12.2 y posteriores, el mecanismo SU tiene precedencia sobre el mecanismo FH cuando se configura.

Si el servidor devuelve el AVP CC-FH y el mecanismo SU se configura para un conjunto de desencadenadores de comportamiento, se aplica la configuración SU; de lo contrario, se aplica el valor AVP CC-FH. De forma predeterminada, los códigos de resultado como 3002, 3004 y 3005 caen bajo *fallo de entrega* y se tratan como RT.

Estas acciones son posibles con el mecanismo SU:

- **Behavior-Trigger** âÂ Â Especifica el tipo de mensajes que pueden ser Peticiones iniciales (CCR-I) o Solicitudes de actualización (CCR-U). Hay tres opciones disponibles para estos desencadenadores:

  Result-Code âÂ Â Esto permite la configuración de códigos de resultado específicos, rango de códigos de resultado (3000-5999), o cualquier error junto con el tipo de mensaje.

  Transport-Failure âÂ Â Esta especificación activa el comportamiento en caso de falla de transporte, que es compatible con la versión 12.0 hacia atrás. Hay dos opciones disponibles para esta configuración:

  Response-Timeout âÂ Â Esta opción activa el comportamiento en RT y siempre se debe utilizar con fallas de transporte.

  Tx-Expiry âÂ Â Esta opción activa el comportamiento al vencimiento de Tx y siempre se debe utilizar con falla de transporte.

  Acciones âÂ Â Esto especifica la acción que se realiza cuando se produce un disparador SU para CCR-I o CCR-U. Esta acción varía según el tipo de mensaje y la versión de software.

- **Continue** â Â Esto permite convertir la sesión a offline y continuar. No hay otras opciones disponibles para el uso de esta acción en las versiones anteriores a la versión 12.2. En las versiones 12.2 y posteriores, las opciones de cuota provisional, reintentos de servidor y vencimiento posterior al temporizador están disponibles para la configuración con esta acción.

- **Terminate** âÂ Â Esto da como resultado la finalización de la sesión cuando el servidor se vuelve inalcanzable. Esta acción permite las opciones de cuota provisional, reintentos de servidor y vencimiento posterior al temporizador.

Estas opciones se pueden utilizar con la acción *Continuar* o *Terminar*:

- **After-interina-time** âÂ Â Esta opción permite la continuidad o terminación de la llamada después del período de tiempo de espera intermedio. Esto es similar a una cuota de tiempo antes de que se realice la acción. El valor tiene formato en segundos y puede oscilar entre 1 y 4.294.967.295.

- **After-interina-Volume** âÂ Â Esta opción asigna la cuota provisional y permite la continuidad o terminación de la sesión antes del agotamiento del volumen configurado. El valor tiene formato en bytes y puede oscilar entre 1 y 4.294.967.295.

- **Server-retries** âÂ Â Esta opción permite al PCEF reintentar el OCS antes de la continuación o finalización de la sesión. Se puede configurar el recuento de reintentos y el valor oscila entre 0 y 65.535. Si el valor es cero, el reintento no se produce y la acción se aplica inmediatamente.

Nota: Las opciones *after-interina* y *after-interina-Volume* siempre se utilizan con la opción *server-retries*, o bien las tres se pueden utilizar simultáneamente y se pueden aplicar tanto a las acciones de continuar como de finalizar. Las opciones *post-interina* y *después de volumen provisional* también asignan tiempo y cuota de volumen, y la cuota que se agota primero desencadena el reintento del servidor.

- **After-timer-Expiration** âÂ Â Esta opción especifica la duración (en segundos) de las sesiones que permanecen en estado fuera de línea antes de que se produzca la terminación. Los valores pueden oscilar entre 1 y 4.294.967.295. Esta opción sólo se aplica a las acciones de finalización.

- **After-Cuota-Expiración** âÂ Â Esta opción finaliza la sesión al agotar la cuota ya asignada.

A continuación se ofrece información importante que debe recordar:

- Las opciones *after-interina*, *after-interina-Volume* y *server-retries* se pueden utilizar de forma individual o combinada, y son aplicables tanto a las acciones de continuación como de finalización.

- La opción *after-quota-caducidad* sólo se aplica al disparador de comportamiento Update-Requests.

- La opción *after-timer-Expiration* sólo se aplica para la acción de finalización.

- Las opciones *after-interina*, *after-interina-Volume* y *server-retries* sólo se aplican a las versiones 12.2 y posteriores.

- Si se admite la conmutación por fallo de sesión de diámetro (y se configura), siempre se contacta con el servidor secundario antes de que se active el mecanismo SU.

- El servidor al que se contactó por última vez antes de que se active el mecanismo SU siempre se contacta cuando se agota el tiempo intermedio o el volumen provisional y la opción *server retries* se configura con un valor mayor que cero. Por ejemplo, si se prueba primero OCS1 y se prueba OCS2 después de un error en OCS1, la comunicación con OCS2

activa el mecanismo SU. Durante el intento de reintento del servidor, primero se contacta con OCS2 y luego con OCS1 si se recibe una respuesta negativa de OCS2.

Flujos de llamadas del mecanismo SU

El mecanismo SU se puede activar por una falla del CCR-I o del CCR-U, y la causa puede ser un código de error, falla de transporte, vencimiento Tx o RT. La acción puede ser una asignación de cuota provisional (tiempo y/o volumen), recuento de reintentos del servidor, valor del temporizador (hace que la sesión se desconecte durante un tiempo especificado y sólo para la terminación) o vencimiento de cuota (sólo para el CCR-U y la terminación) antes de que la sesión se desconecte o termine.

La cuota provisional se proporciona por sesión, no por grupo de calificación (RG) en escenarios de Control de crédito de servicios múltiples (MSCC).

Existe la posibilidad de que el servidor primario active la falla de transporte y el servidor secundario active el vencimiento Tx o el tiempo de espera de respuesta. En este escenario, el último error se considera el disparador de la falla.

Si el mecanismo SU no está configurado para cualquier disparador de falla, se activa el mecanismo FH.

> **Nota:** Las secciones siguientes proporcionan algunos ejemplos de flujo de llamadas relacionados con el mecanismo SU. Estos flujos de llamada se proporcionan bajo la suposición de que se soporta el failover de sesión de diámetro y el servidor secundario se configura con un valor de vencimiento Tx menor que el valor RT. Además, se asume que el mecanismo SU está configurado para transport-failure, Tx-vencimiento y RT.

Solicitud inicial sin desconexión de sesión

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-I al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión.

5. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-I se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, el CCR-I se envía a otro servidor.

6. Si se detecta nuevamente la falla de transporte o el tiempo de espera Tx, se repiten los pasos 2 a 5 hasta que se agote el valor *server retries* o no se produzca una respuesta satisfactoria del OCS.

7. Si el problema persiste, la sesión continúa (convertida a desconectada) o termina según la configuración.

   Nota: La cuota provisional que se consume mientras la sesión entra en modo SU debido a CCR-I no se informa en el próximo CCR-I. Toda la cuota interina utilizada se informa en el CCR-U, que sigue al CCA-I exitoso.

Solicitud inicial con desconexión de sesión

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-I al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión.

5. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-I se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, el CCR-I se envía a otro servidor.

6. Si se detecta nuevamente la falla de transporte o el tiempo de espera Tx, se repiten los pasos 2 a 5 hasta que se agote el valor *server retries* o no se produzca una respuesta satisfactoria del OCS. En este momento, el período de sesiones se desconecta sin consumir toda la cuota provisional.

7. Después de la terminación de la sesión, el PCEF envía nuevamente el CCR-I para comenzar una nueva sesión. Si esto es exitoso, entonces el PCEF envía el CCR-T, que informa de toda la cuota temporal que se utilizó.

Solicitud de actualización sin desconexión de sesión

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-U al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión.

5. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-U se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, se envía un CCR-U a otro servidor que contiene toda la cuota consumida sin informar.

6. Si se detecta nuevamente la falla de transporte o el tiempo de espera Tx, se repiten los pasos 2 a 5 hasta que se agote el valor *server retries* o no se produzca una respuesta satisfactoria del OCS.

7. La cuota consumida completa se informa al OCS con el CCR-U exitoso.

8. Si el problema persiste, la sesión continúa (convertida a desconectada) o termina según la configuración después del agotamiento del valor máximo de reintento.

Solicitud de actualización con desconexión de sesión

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-U al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión.

5. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-U se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, se envía un CCR-U a otro servidor que contiene toda la cuota consumida sin informar.

6. Si se detecta nuevamente la falla de transporte o el tiempo de espera Tx, se repiten los pasos 2 a 5 hasta que se agote el valor *server retries* o no se produzca una respuesta satisfactoria del OCS. En este momento, la sesión se desconecta antes de que consuma toda la cuota temporal.

7. El PCEF envía un CCR-T al OCS para informar de la cuota consumida completa.

8. Si el OCS responde con un código de resultados *2002*, no se necesitan los informes adicionales.

Solicitud de actualización con sesión desconocida

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-U al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión.

5. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-U se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, se envía un CCR-U a otro servidor que contiene toda la cuota consumida sin informar.

6. El OCS responde con un código de resultado *5002* (ID de sesión desconocida) para el CCR-U, lo que es posible en el escenario en el que el OCS reinició y perdió la información de ID de sesión.

7. El PCEF inicia una nueva sesión con el CCR-I y recibe el CCA-I.

8. El PCEF informa de toda la cuota provisional consumida a través de CCR-U en mensajes posteriores.

Solicitud de actualización con varios RG (situación de MSCC)

Este es el flujo de mensajes para este escenario:

1. El PCEF envía el CCR-U para RG1 al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, se activa el mecanismo SU. Esto ocurre inmediatamente para fallas de transporte, o después de la expiración del Tx para un tiempo de espera.

4. Si se configura el volumen y/o la hora provisionales, la cuota provisional se asigna a la sesión

5. En este punto, RG2 también agota toda la cuota asignada pero no inicia el CCR-U porque la sesión ya está en modo SU y comienza a consumir la cuota provisional.

6. Después del agotamiento de la cuota provisional (tiempo o volumen) y si el valor *del servidor reintenta* es mayor que cero, entonces el CCR-U se envía de nuevo al servidor que activó el mecanismo SU. Si hay otra falla, se envía un CCR-U a otro servidor que contiene toda la cuota consumida sin informar para ambos RG.

7. Si se detecta nuevamente la falla de transporte o el tiempo de espera Tx, se repiten los pasos 2 a 6 hasta que se agote el valor *server retries* o no se produzca una respuesta satisfactoria del OCS.

8. La cuota consumida completa se informa al OCS con el CCR-U exitoso.

9. Si el problema persiste, la sesión continúa (convertida a desconectada) o termina según la configuración después del agotamiento del valor máximo de reintento.

Terminate-Request (Pedido de finalización)

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR-T al OCS.

2. Se detecta un tiempo de espera o una falla de transporte. Si se detecta una falla de transporte, el PCEF inmediatamente se reintenta con el servidor secundario; de lo contrario, se activa la caducidad Tx.

3. Si el servidor secundario también tiene una falla de transporte o un tiempo de espera, la sesión se quita.

Gestión de códigos de error de CCR

Este es el flujo de mensajes para este escenario:

1. El PCEF envía un CCR al OCS y el OCS responde con un código de error.

2. El código de error se configura estáticamente en el mecanismo SU.

3. El PCEF proporciona la cuota provisional sin un reintento al servidor secundario.

Configuraciones de ejemplo de FH y SU

Esta sección proporciona un ejemplo de configuración para los mecanismos FH y SU. Cuando se configuran los mecanismos FH y SU, la SU tiene prioridad sobre la FH para el mismo disparador de comportamiento.

Aquí tiene un ejemplo:

```
credit-control group test

diameter origin endpoint test

diameter peer-select peer test

quota volume-threshold percent 10

diameter pending-timeout 80 deciseconds msg-type any

diameter session failover

trigger type rat lac

apn-name-to-be-included virtual

quota request-trigger exclude-packet-causing-trigger

failure-handling initial-request continue retry-after-tx-expiry

servers-unreachable initial-request terminate after-interim-volume 200
after-interim-time 3600 server-retries 0

servers-unreachable behavior-triggers initial-request transport-failure
tx-expiry

servers-unreachable update-request continue after-interim-volume 200
after-interim-time 3600 server-retries 50

servers-unreachable behavior-triggers update-request transport-failure
tx-expiry
```

Verificación

Para verificar que su configuración funciona correctamente, ingrese el comando **show active-load service <service name>**:

```
# show active-charging service name test


Service name: test


TCP Flow Idle Timeout : 300 (secs)

UDP Flow Idle Timeout : 300 (secs)

ICMP Flow Idle Timeout : 300 (secs)

ICMP Flow Idle Timeout : 300 (secs)

ALG Media Idle Timeout : 120 (secs)


TCP Flow-Mapping Idle Timeout : 300 (secs)
```

UDP Flow-Mapping Idle Timeout : Not Configured

Deep Packet Inspection: Enabled

Passive Mode : Disabled

CDR Flow Control : Enabled

CDR Flow Control Unsent Queue Size: 75

Unsent Queue high watermark: 56

Unsent Queue low watermark: 18

Content Filtering: Disabled

Dynamic Content Filtering: Disabled

URL-Blacklisting: Disabled

URL-Blacklisting Match-method: Exact

Content Filtering Match-method: Generic

Interpretation of Charging-rule-base-name: active-charging-group-of-ruledefs

Selection of Charging-rule-base AVP : Last

Credit Control:

Group : test

Mode : diameter

APN-name-to-be-included: gn

Trigger-Type : N/A

Failure-Handling:

```
Initial-Request : continue retry-after-tx-expiry

Update-Request : retry-and-terminate

Terminate-Request: retry-and-terminate


Server Unreachable Failure-Handling:

Initial-Request : terminate

Update-Request : continue
```

Troubleshoot

Ingrese el comando **show active-load credit-control statistics** para ver las estadísticas relacionadas con los mecanismos SU y FH. Éste es un ejemplo de salida:

```
#show active-charging credit-control statistics
...

OCS Unreachable Stats:

Tx-Expiry: 2291985 Response-TimeOut: 615

Connection-Failure: 2 Action-Continue: 0

Action-Terminated: 0 Server Retries: 2023700


Assumed-Positive Sessions:

Current: 2 Cumulative: 2196851
```

A continuación se muestran algunas notas importantes sobre este ejemplo de resultado:

- **Tx-Expiry** âÂ Â Esto indica una condición SU debido a una caducidad de Tx.
- **Response-Timeout** âÂ Â Esto indica una condición SU debido a un RT.
- **Connection-Failure** âÂ Â Esto indica una condición SU debido a una falla de transporte.
- **Action-Continue** âÂ Â Este campo indica el número de sesiones que se desconectaron.
- **Action-Terminate** âÂ Â Este campo indica el número de sesiones que se terminaron.
- **Server Retries** âÂ Â Este campo indica el número de veces que se reintentó el OCS.
- **Sesiones Supuestas-Positivas**:

  Current âÂ Â Este campo indica el número de sesiones que se encuentran actualmente en la condición SU.

Acumulative âÂ Â Este campo indica el número total de sesiones que se han movido al estado SU.

Ingrese el comando **show active-load sessions full all** para ver la información relacionada con el estado SU de la sesión. Éste es un ejemplo de salida:

```
#show active-charging sessions full all
..
..

Current Server Unreachable State: CCR-I

Interim Volume in Bytes (used / allotted): 84/ 200

Interim Time in Seconds (used / allotted): 80/ 3600

Server Retries (attempted / configured): 1/ 50
```

A continuación se muestran algunas notas importantes sobre este ejemplo de resultado:

- **Current Server Unreachable State** âÂ Â Especifica si el estado de SU actual se debe a CCR-I o CCR-U.
- **Volumen interino en Bytes (utilizado/asignado)** âÂ Â Esto muestra el volumen intermedio en bytes utilizados frente a los bytes asignados.
- **Tiempo intermedio en segundos (utilizado/asignado)** âÂ Â Muestra el volumen provisional en segundos utilizado frente a los segundos asignados.
- **Server Retries (intento/configurado)** âÂ Â Este es el número de reintentos de servidor comparado con el configurado.

Información Relacionada

- Referencia de la Interfaz de Línea de Comandos, StarOS Release 16
- Soporte técnico y documentaciónâÂÂ Cisco Systems