# Qué hacer con mallocfail y la alta utilización de la CPU que surgen del gusano “Código rojo”

## Contenido



## Introducción

Este documento describe el gusano "Código rojo" y los problemas que puede causar en un entorno de ruteo de Cisco. Este documento también describe las técnicas para prevenir la infestación del gusano y proporciona los links a las asesorías relacionadas que describen las

soluciones para los problemas gusano-relacionados.

El gusano del “Código rojo” explota una vulnerabilidad en el servicio del índice de la versión 5.0 de Microsoft Internet Information Server (IIS). Cuando el gusano del “Código rojo” infecta un host, hace al host sondar e infectar las series aleatorias de IP Addresses, que causa un incremento repentino en el tráfico de la red. Esto es especialmente problemático si hay links redundantes en la red y/o el Cisco Express Forwarding (CEF) no se utiliza para conmutar los paquetes.

# prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

# Cómo el gusano del “Código rojo” infecta otros sistemas

El gusano "código rojo" intenta conectarse a direcciones de IP generadas aleatoriamente. Cada servidor IIS infectado puede intentar infectar el mismo conjunto de dispositivos. Usted puede localizar la dirección IP de origen y el puerto TCP del gusano porque no es spoofed. El Unicast Reverse Path Forwarding (uRPF) no puede suprimir un ataque del gusano porque la dirección de origen es legal.

# Asesores que analizan el gusano "Código Rojo"

Estas recomendaciones describen el gusano del “Código rojo”, y explican cómo parchear el software afectado por el gusano:

- Asesoría en seguridad de Cisco: Gusano del “Código rojo” - Impacto para el cliente
- Desbordamiento de memoria intermedia de la extensión ISAPI del servidor de índice ISS remoto
- .ida gusano "código rojo
- ¿CERT? Gusano consultivo del “Código rojo” CA-2001-19 que explota el desbordamiento de búfer en el servicio de indexación DLL IIS

# Síntomas

Aquí están algunos síntomas que indican que el gusano del “Código rojo” afecta a un router Cisco:

- Número grande de flujos en el NAT o tablas PAT (si usted utiliza el NAT o la PALMADITA).
- Número grande de pedidos ARP o de tormentas ARP en la red (causada por la exploración de la dirección IP).
- Uso de memoria excesiva por la entrada IP, la entrada de información ARP, el Ager de memoria caché IP y los procesos CEF.
- CPU elevada utilización en la entrada ARP, IP, el CEF y IPC.
- CPU elevada utilización en el nivel de interrupción a las tarifas con poco tráfico, o CPU elevada utilización en el nivel de proceso en la entrada IP, si usted utiliza el NAT.

Una condición de memoria baja o CPU elevada una utilización continua (el 100 por ciento) en el nivel de interrupción puede hacer a un router del ® del Cisco IOS recargar. La recarga es causada por un proceso que se comporte mal debido a las condiciones de la tensión.

Si usted no sospecha que los dispositivos en su sitio están infectados por o son la blanco del gusano del “Código rojo”, vea la sección de información relacionada para los URL adicionales en cómo resolver problemas cualquier problema que usted encuentre.

# Identifique el dispositivo infectado

Utilice el Flow Switching para identificar la dirección IP de origen del dispositivo afectado. Configure el flujo del route-cache del IP en todas las interfaces para registrar todos los flujos conmutados por el router.

Después de algunos minutos, publique el comando show ip cache flow de ver las entradas registradas. Durante la fase inicial de la infección del gusano del “Código rojo”, el gusano intenta replicarse. La replicación ocurre cuando el gusano envía las peticiones HT a los IP Addresses al azar. Por lo tanto, usted debe buscar flujo de caché las entradas con el puerto destino 80 (HT., 0050 en el maleficio).

**El IP de la demostración flujo de caché | incluya 0050 que el** comando visualiza todas las entradas del caché con un puerto TCP 80 (0050 en el maleficio):

```
Router#show ip cache flow | include 0050 ... scram scrappers dative DstIPaddress Pr SrcP DstP
Pkts Vl1 193.23.45.35 Vl3 2.34.56.12 06 0F9F 0050 2 Vl1 211.101.189.208 Null 158.36.179.59 06
0457 0050 1 Vl1 193.23.45.35 Vl3 34.56.233.233 06 3000 0050 1 Vl1 61.146.138.212 Null
158.36.175.45 06 B301 0050 1 Vl1 193.23.45.35 Vl3 98.64.167.174 06 0EED 0050 1 Vl1
202.96.242.110 Null 158.36.171.82 06 0E71 0050 1 Vl1 193.23.45.35 Vl3 123.231.23.45 06 121F 0050
1 Vl1 193.23.45.35 Vl3 9.54.33.121 06 1000 0050 1 Vl1 193.23.45.35 Vl3 78.124.65.32 06 09B6 0050
1 Vl1 24.180.26.253 Null 158.36.179.166 06 1132 0050 1
```

Si usted encuentra anormalmente un número alto de entradas con la misma dirección IP de origen, el address1 del IP de destino aleatorio, DstP = 0050 (HTTP), y las RRPP = 06 (TCP), usted ha localizado probablemente un dispositivo infectado. En este ejemplo de resultado, la dirección IP de origen es 193.23.45.35 y viene del VLAN1.

la versión 1Another del gusano del “Código rojo”, llamada el “código rojo II”, no elige totalmente una dirección IP del destino aleatorio. En lugar, el “código rojo II” guarda la porción de la red de la dirección IP, y elige una porción al azar del host de la dirección IP para propagar. Esto permite

que el gusano se separe más rápidamente dentro de la misma red.

El “código rojo II” utiliza estas redes y máscaras:

```
Mask Probability of Infection 0.0.0.0 12.5% (random) 255.0.0.0 50.0% (same class A) 255.255.0.0
37.5% (same class B)
```

Los IP Address de destino se excluyen que son 127.X.X.X y 224.X.X.X, y ningún octeto se permiten ser 0 o 255. Además, el host no intenta re-infectarse.

Para más información, refiera al código rojo (ii) .

A veces, usted no puede ejecutar el Netflow para detectar una tentativa de la infestación del “Código rojo”. Esto puede ser porque usted funciona con una versión del código que no soporte el Netflow, o porque el router tiene escaso o memoria excesivamente hecha fragmentos para habilitar el Netflow. Cisco recomienda que usted no habilita el Netflow cuando hay interfaces de ingreso múltiples y solamente una interfaz de egreso en el router, porque la Contabilización de Netflow se realiza en el trayecto de ingreso. En este caso, es mejor habilitar las estadísticas IP en la interfaz de egreso solitaria.

**Nota:** El comando ip accounting inhabilita el DCEF. No habilite las estadísticas IP en ninguna plataforma donde usted quiere utilizar el DCEF Switching.

```
Router(config)#interface vlan 1000 Router(config-if)#ip accounting Router#show ip accounting
Source Destination Packets Bytes 20.1.145.49 75.246.253.88 2 96 20.1.145.43 17.152.178.57 1 48
20.1.145.49 20.1.49.132 1 48 20.1.104.194 169.187.190.170 2 96 20.1.196.207 20.1.1.11 3 213
20.1.145.43 43.129.220.118 1 48 20.1.25.73 43.209.226.231 1 48 20.1.104.194 169.45.103.230 2 96
20.1.25.73 223.179.8.154 2 96 20.1.104.194 169.85.92.164 2 96 20.1.81.88 20.1.1.11 3 204
20.1.104.194 169.252.106.60 2 96 20.1.145.43 126.60.86.19 2 96 20.1.145.49 43.134.116.199 2 96
20.1.104.194 169.234.36.102 2 96 20.1.145.49 15.159.146.29 2 96
```

En la salida del comando show ip accounting, busque a las direcciones de origen que intentan enviar los paquetes a las direcciones de destino múltiple. Si el host infectado es en la fase de la exploración, intenta establecer las conexiones HTTP al otro Routers. Usted verá tan las tentativas de alcanzar los IP Addresses múltiples. La mayor parte de fall de estos intentos de conexión normalmente. Por lo tanto, usted ve solamente una pequeña cantidad de paquetes transferidos, cada uno con una pequeña cuenta de bytes. En este ejemplo, es probable que 20.1.145.49 y 20.1.104.194 estén infectados.

Cuando usted ejecuta el Multi-Layer Switching (MLS) en las Catalyst 5000 Series y las Catalyst 6000 Series, usted debe tomar diversas medidas para habilitar la Contabilización de Netflow y para rastrear la infestación. En un Switch del Cat6000 equipado de la Multilayer Switch Feature Card del Supervisor 1 (MSFC1) o del SUP I/MSFC2, el MLS Netflow-basado se habilita por abandono, pero el flujo-MODE es destino solamente. Por lo tanto, la dirección IP de origen no se oculta. Usted puede permitir al modo “a todo régimen” para rastrear los host infectados con la ayuda del comando set mls flow full en el supervisor.

Para el modo híbrido, utilice el **comando set mls flow full**:

```
6500-sup(enable)set mls flow full Configured IP flowmask is set to full flow. Warning:
Configuring more specific flow mask may dramatically increase the number of MLS entries.
```

Para el modo de IOS nativo, utilice el comando mls flow ip full:

```
Router(config)#mls flow ip full
```

Cuando usted habilita el modo “a todo régimen”, se visualiza una advertencia de indicar un aumento evidente en las entradas de MLS. El impacto de las entradas de MLS crecientes es

justificable por una duración breve si su red se infesta ya con el gusano del “Código rojo”. El gusano hace sus entradas de MLS ser excesivas y en la subida.

Para ver la información recopilada, utilice estos comandos:

Para el modo híbrido, utilice el **comando set mls flow full**:

```
6500-sup(enable)set mls flow full Configured IP flowmask is set to full flow. Warning:
Configuring more specific flow mask may dramatically increase the number of MLS entries.
```

Para el modo de IOS nativo, utilice el **comando mls flow ip full**:

```
Router(config)#mls flow ip full
```

Cuando usted habilita el modo “a todo régimen”, se visualiza una advertencia de indicar un aumento evidente en las entradas de MLS. El impacto de las entradas de MLS crecientes es justificable por una duración breve si su red se infesta ya con el gusano del “Código rojo”. El gusano hace sus entradas de MLS ser excesivas y en la subida.

Para ver la información recopilada, utilice estos comandos:

Para el modo híbrido, utilice el comando show mls ent:

```
6500-sup(enable)show mls ent Destination-IP Source-IP Prot DstPrt SrcPrt Destination-Mac Vlan
EDst ESrc DPort SPort Stat-Pkts Stat-Bytes Uptime Age --------------- --------------- ----- -----
- ------ ----------------- ---- ---- ---- --------- --------- ---------- ----------- -------- --
------
```

**Nota:** Se completan todos estos campos cuando están en el modo “a todo régimen”.

Para el modo de IOS nativo, utilice el **comando show mls ip**:

```
Router#show mls ip DstIP SrcIP Prot:SrcPort:DstPort Dst i/f:DstMAC ----------------------------
------------------------------------ Pkts Bytes SrcDstPorts SrcDstEncap Age LastSeen --------
-------------------------------------------------------------
```

Cuando usted determina la dirección IP de origen y el puerto destino implicados en el ataque, usted puede fijar el MLS de nuevo al modo “destino solamente”.

Para el modo híbrido utilice el comando set mls flow destination:

```
6500-sup(enable) set mls flow destination Usage: set mls flow <destination|destination-
source|full>
```

Para el modo de IOS nativo, utilice el comando mls flow ip destination:

```
Router(config)#mls flow ip destination
```

La combinación del supervisor (SUP) II/MSFC2 se protege contra el ataque porque el CEF Switching se realiza en el hardware, y se mantienen las estadísticas de Netflow. Así pues, incluso durante un ataque del “Código rojo”, si usted habilita al modo flujo completo, no hunden al router, debido al mecanismo de Switching más rápido. Los comandos de habilitar al modo flujo completo y de visualizar las estadísticas son lo mismo en el SUP I/MFSC1 y el SUP II/MSFC2.

## Técnicas de prevención

Utilice las técnicas enumeradas en esta sección para minimizar el impacto del gusano del “Código rojo” en el router.

## Bloquee el tráfico al puerto 80

Si es posible en su red, la manera más fácil de prevenir el ataque del “Código rojo” es bloquear todo el tráfico al puerto 80, que es el puerto conocido para el WWW. Construya una lista de acceso para negar los paquetes del IP destinados al puerto 80 y para aplicarlos entrantes en la interfaz que hace frente a la fuente de infección.

## Reduzca el USO de memoria de entrada de información ARP

La entrada de información ARP utiliza encima de las grandes cantidades de memoria cuando una Static ruta señala a una interfaz de broadcast, como esto:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Cada paquete para la ruta predeterminado se envía al VLAN3. Sin embargo, no hay IP Address de Next Hop especificado, y por eso, el router envía un pedido ARP para el IP Address de destino. El Next Hop Router para ese destino contesta con su propia dirección MAC, a menos que se inhabilite el proxy ARP. La contestación del router crea una entrada adicional en la tabla ARP donde el IP Address de destino del paquete se asocia a la dirección MAC del Next-Hop. El gusano del “Código rojo” envía los paquetes a los IP Addresses al azar, que agrega una nueva entrada ARP para cada direccionamiento de destino aleatorio. Cada nueva entrada ARP consume cada vez más la memoria bajo proceso de entrada de información ARP.

No cree una Static Default ruta a una interfaz, especialmente si se transmite la interfaz (los Ethernetes/Ethernet/GE/SMDS rápido) o de múltiples puntos (Frame Relay/ATM). Cualquier Static Default ruta debe señalar a la dirección IP del Next Hop Router. Después de que usted cambie la ruta predeterminado para señalar al IP Address de Next Hop, utilice el **comando clear arp-cache** de borrar todas las entradas ARP. Este comando repara el problema de la utilización de la memoria.

## Utilice conmutar del Cisco Express Forwarding (CEF)

Para bajar la utilización de la CPU en un router IOS, cambie del Fast/Optimum/Netflow Switching al CEF Switching. Hay algunas advertencias para habilitar el CEF. La siguiente sección discute la diferencia entre el CEF y la transferencia rápida, y explica las implicaciones cuando usted habilita el CEF.

# Cisco Express Forwarding vs. Fast Switching

Permita al CEF para paliar la mayor carga de tráfico causada por el gusano del “Código rojo”. CC de las versiones de software 11.1 de Cisco IOS® (), 12.0, y posterior soporte CEF en las Plataformas de Cisco 7200/7500/GSR. El soporte para el CEF en otras Plataformas está disponible en el Cisco IOS Software Release 12.0 o Posterior. Usted puede investigar más lejos con la herramienta Software Advisor.

A veces, usted no puede habilitar el CEF en todo el Routers debido a una de estas razones:

- Memoria insuficiente
- Arquitecturas de plataforma no compatible
- Encapsulaciones de interfaz no admitidas

## Comportamiento y consecuencias de el fast switching

Aquí están las implicaciones cuando usted utiliza la transferencia rápida:

- Caché conducido tráfico — El caché está vacío hasta los paquetes de los switches del router y puebla el caché.
- El primer paquete es proceso conmutado — El primer paquete es process-switched, porque el caché está inicialmente vacío.
- Caché granular — El caché se construye en un granularity de la parte de más específica de la entrada del Routing Information Base (RIB) una red principal. Si el RIB tiene /24s para la red principal 131.108.0.0, el caché se construye con /24s para esta red principal.
- se utiliza el caché de /32 — el caché de /32 se utiliza para equilibrar la carga para cada destino. Cuando el caché equilibra la carga, el caché se construye con /32s para esa red principal.**Nota:** Estos dos últimos problemas pueden causar una gran caché que consumiría toda la memoria.
- Almacenamiento en memoria inmediata en los límites de red principal — Con la ruta predeterminado, el almacenamiento en memoria inmediata se realiza en los límites de red principal.
- Memoria caché AGER — Memoria caché AGER funciona con cada minuto y marca el 1/20o (el 5 por ciento) del caché para las entradas sin utilizar bajo condiciones de memoria normales, y 1/4 (el 25 por ciento) del caché en una condición de memoria baja (200k).

Para cambiar los valores antedichos, utilice el **comando ip cache-ager-interval X Y Z**, donde:

- X es número <0-2147483> de segundos entre los funcionamientos del ager. Valor por defecto = 60 segundos.
- Y es <2-50> 1/(Y+1) del caché a envejecer por el funcionamiento (memoria baja). Valor por defecto = 4.
- Z es <3-100> 1/(Z+1) del caché a envejecer por el funcionamiento (normal). Valor por defecto = 20.

Aquí está una configuración de muestra que utiliza el **ip cache-ager 60 5 25**.

```
Router#show ip cache IP routing cache 2 entries, 332 bytes 27 adds, 25 invalidates, 0 refcounts
Cache aged by 1/25 every 60 seconds (1/5 when memory is low). Minimum invalidation interval 2
seconds, maximum interval 5 seconds, quiet interval 3 seconds, threshold 0 requests Invalidation
rate 0 in last second, 0 in last 3 seconds Last full cache invalidation occurred 03:55:12 ago
Prefix/Length Age Interface Next Hop 4.4.4.1/32 03:44:53 Serial1 4.4.4.1 192.168.9.0/24 00:03:15
Ethernet1 20.4.4.1 Router#show ip cache verbose IP routing cache 2 entries, 332 bytes 27 adds,
25 invalidates, 0 refcounts Cache aged by 1/25 every 60 seconds (1/5 when memory is low).
Minimum invalidation interval 2 seconds, maximum interval 5 seconds, quiet interval 3 seconds,
threshold 0 requests Invalidation rate 0 in last second, 0 in last 3 seconds Last full cache
invalidation occurred 03:57:31 ago Prefix/Length Age Interface Next Hop 4.4.4.1/32-24 03:47:13
Serial1 4.4.4.1 4 0F000800 192.168.9.0/24-0 00:05:35 Ethernet1 20.4.4.1 14
00000C34A7FC00000C13DBA90800
```

De acuerdo con la configuración de su memoria caché AGER, un cierto porcentaje de su edad de entradas del caché fuera de su tabla del caché rápido. Cuando la edad de entradas rápidamente, un porcentaje más grande de la tabla del caché rápido envejece, y la tabla de caché llega a ser más pequeña. Como consecuencia, la consumición de la memoria en el router reduce. Una desventaja es que el tráfico continúa fluyendo para las entradas que eran tabla de caché envejecida de los. Los paquetes iniciales son process-switched, que causa un punto corto en el consumo de la CPU en el **IP entrado** hasta que una nueva entrada de caché se construya para el flujo.

De los Cisco IOS Software Release 10.3(8), 11.0(3) y posterior, el ager de memoria caché IP se dirige diferentemente, según lo explicado aquí:

- **Los comandos ip cache-ager-interval y ip cache-invalidate-delay** están disponibles solamente si definen al **comando service internal** en la configuración.
- Si el período entre los funcionamientos de la anulación del ager se fija a 0, el proceso ager se inhabilita totalmente.
- El tiempo se expresa en segundos.

**Nota:** Cuando usted ejecuta estos comandos, la utilización de la CPU del router aumenta. Utilice estos comandos solamente cuando absolutamente es necesario.

```
Router#clear ip cache ? A.B.C.D Address prefix <CR>--> will clear the entire cache and free the
memory used by it! Router#debug ip cache IP cache debugging is on
```

## Ventajas del CEF

- La tabla de la Base de información de reenvío (FIB) se construye sobre la base de la tabla de ruteo. Por lo tanto la información de reenvío existe antes de que se remita el primer paquete. FIB también incluye entradas /32 para hosts LAN conectados de manera directa.
- La tabla de la adyacencia (ADJ) contiene la información de reescritura de la capa 2 para los saltos siguientes y los host conectados directamente (una entrada ARP crea una adyacencia CEF).
- No hay un concepto de memoria caché ager con CEF para aumentar el rendimiento de la CPU. Se borra una entrada de la BOLA si se borra una entrada de la tabla de ruteo.

**Precaución:** Una vez más una ruta predeterminado que señala a un broadcast o a una interfaz multipunto significa que el router envía los pedidos ARP para cada nuevo destino. Los pedidos ARP del router potencialmente crean una tabla de adyacencia enorme hasta el router se ejecutan de la memoria. Si el CEF no puede afectar un aparato la memoria CEF/DCEF se inhabilita. Usted necesitará habilitar manualmente el CEF/DCEF otra vez.

## Ejemplo de resultado CEF

Aquí está una cierta salida de muestra del comando show ip cef summary, ese uso de la memoria de las demostraciones. Esta salida es una foto de un Route Server del Cisco 7200 con el Cisco IOS Software Release 12.0.

```
Router>show ip cef summary IP CEF with switching (Table Version 2620746) 109212 routes, 0
reresolve, 0 unresolved (0 old, 0 new), peak 84625 109212 leaves, 8000 nodes, 22299136 bytes,
2620745 inserts, 2511533 invalidations 17 load sharing elements, 5712 bytes, 109202 references
universal per-destination load sharing algorithm, id 6886D006 1 CEF resets, 1 revisions of
existing leaves 1 in-place/0 aborted modifications Resolution Timer: Exponential (currently 1s,
peak 16s) refcounts: 2258679 leaf, 2048256 node Adjacency Table has 16 adjacencies Router>show
processes memory | include CEF PID TTY Allocated Freed Holding Getbufs Retbufs Process 73 0
147300 1700 146708 0 0 CEF process 84 0 608 0 7404 0 0 CEF Scanner Router>show processes memory
| include BGP 2 0 6891444 6891444 6864 0 0 BGP Open 80 0 3444 2296 8028 0 0 BGP Open 86 0 477568
476420 7944 0 0 BGP Open 87 0 2969013892 102734200 338145696 0 0 BGP Router 88 0 56693560
2517286276 7440 131160 4954624 BGP I/O 89 0 69280 68633812 75308 0 0 BGP Scanner 91 0 6564264
6564264 6876 0 0 BGP Open 101 0 7635944 7633052 6796 780 0 BGP Open 104 0 7591724 7591724 6796 0
0 BGP Open 105 0 7269732 7266840 6796 780 0 BGP Open 109 0 7600908 7600908 6796 0 0 BGP Open 110
0 7268584 7265692 6796 780 0 BGP Open Router>show memory summary | include FIB Alloc PC Size
Blocks Bytes What 0x60B8821C 448 7 3136 FIB: FIBIDB 0x60B88610 12000 1 12000 FIB: HWIDB MAP
TABLE 0x60B88780 472 6 2832 FIB: FIBHWIDB 0x60B88780 508 1 508 FIB: FIBHWIDB 0x60B8CF9C 1904 1
1904 FIB 1 path chunk pool 0x60B8CF9C 65540 1 65540 FIB 1 path chunk pool 0x60BAC004 1904 252
479808 FIB 1 path chun 0x60BAC004 65540 252 16516080 FIB 1 path chun Router>show memory summary
| include CEF 0x60B8CD84 4884 1 4884 CEF traffic info 0x60B8CF7C 44 1 44 CEF process 0x60B9D12C
```

```
14084 1 14084 CEF arp throttle chunk 0x60B9D158 828 1 828 CEF loadinfo chunk 0x60B9D158 65540 1
65540 CEF loadinfo chunk 0x60B9D180 128 1 128 CEF walker chunk 0x60B9D180 368 1 368 CEF walker
chunk 0x60BA139C 24 5 120 CEF process 0x60BA139C 40 1 40 CEF process 0x60BA13A8 24 4 96 CEF
process 0x60BA13A8 40 1 40 CEF process 0x60BA13A8 72 1 72 CEF process 0x60BA245C 80 1 80 CEF
process 0x60BA2468 60 1 60 CEF process 0x60BA65A8 65488 1 65488 CEF up event chunk Router>show
memory summary | include adj 0x60B9F6C0 280 1 280 NULL adjacency 0x60B9F734 280 1 280 PUNT
adjacency 0x60B9F7A4 280 1 280 DROP adjacency 0x60B9F814 280 1 280 Glean adjacency 0x60B9F884
280 1 280 Discard adjacency 0x60B9F9F8 65488 1 65488 Protocol adjacency chunk
```

### Puntos a considerar

Cuando el número de flujos es grande, el CEF consume típicamente menos memoria que rápidamente conmutando. Si la memoria es consumida ya por un Switching Cache rápido, usted debe borrar memoria caché ARP (a través del **comando clear ip arp**) antes de que usted habilite el CEF.

**Nota:** Cuando usted borra el caché, un punto se causa en la utilización de la CPU del router.

## Preguntas frecuentes del “Código rojo” y sus respuestas

### Q. Utilizo el NAT, y experimento 100 por ciento de uso de la CPU en la entrada IP. Cuando ejecuto la CPU del proc de la demostración, mi utilización de la CPU es alta en el nivel de interrupción - 100/99 o 99/98. ¿Se puede esto relacionar con el “Código rojo”?

**R.** Allí recientemente se repara un bug Cisco NAT (CSCdu63623 (clientes registrados solamente)) que implica el scalability. Cuando hay decenas de miles de flujos NAT (basados en el tipo de plataforma), el bug causa 100 por ciento de uso de la CPU en el proceso o el nivel de interrupción.

Para determinar si este bug es la razón, publique el **comando show align**, y verifiquelo si el router hace frente a los errores de alineación. Si usted ve los errores de alineación o los accesos de memoria espurios, publique el **comando show align** un par de veces y vea si los errores están en la subida. Si el número de errores está en la subida, los errores de alineación pueden ser la causa CPU elevada de la utilización en el nivel de interrupción, y no CSCdu63623 del bug Cisco (clientes registrados solamente). Para más información, refiera a los accesos espúreos y a los errores de alineación del troubleshooting.

**El comando show ip nat translation** visualiza el número de traducciones activas. La punta de la fusión para un procesador de la clase del NPE-300 es cerca de 20,000 a 40,000 traducciones. Este número varía basado en la plataforma.

Este problema de fusión fue observado previamente por un par de clientes, pero después del “Código rojo”, más clientes han experimentado este problema. La única solución alternativa es ejecutar el NAT (en vez de la PALMADITA), de modo que haya menos traducciones activas. Si usted tiene 7200, utilice un NSE-1, y baje los valores de agotamiento del tiempo NAT.

### Q. Ejecuto el IRB, y encuentro CPU elevada la utilización en el proceso de entrada de Hybridge. ¿Por qué ocurre esto? ¿Está relacionado con el “Código rojo”?

**R.** El proceso de entrada de Hybridge maneja cualquier paquete que no pueda ser Fast-Switched por el proceso IRB. La incapacidad del proceso IRB al ayune switch un paquete puede ser

porque:

- El paquete es un paquete de broadcast.
- El paquete es un paquete de multidifusión.
- El destino es desconocido, y el ARP necesita ser accionado.
- Están atravesando - el árbol BPDU.

La entrada de Hybridge encuentra los problemas si hay millares de interfaces Point-to-Point en el mismo Grupo de Bridge. La entrada de Hybridge también encuentra los problemas (pero en un grado inferior) si hay millares de VSs en la misma interfaz multipunto.

¿Cuáles son las posibles razones para los problemas con IRB? Asuma que un dispositivo infectado con el “Código rojo” analiza los IP Addresses.

- El router necesita enviar un pedido ARP para cada IP Address de destino. Una inundación de los pedidos ARP resulta en cada VC en el Grupo de Bridge para cada direccionamiento se analice que. El proceso ARP normal no causa un problema de la CPU. Sin embargo, si hay una entrada ARP sin una entrada del Bridge, el router inunda los paquetes destinados para los direccionamientos para los cuales las entradas ARP existen ya. Puede causar utilización intensa de la CPU ya que el tráfico está conmutado por proceso. Para evitar el problema, aumentar la época del Bridge-envejecimiento (valor por defecto 300 segundos o 5 minutos) de hacer juego o de exceder el tiempo de espera de ARP (valor por defecto 4 horas) para sincronizar los dos temporizadores.
- El direccionamiento que el host extremo intenta infectar es una dirección de broadcast. El router realiza el equivalente a una transmisión de subred que necesita ser reiterada por el proceso de entrada Hybridge. Esto no sucede si configuran al **comando no ip directed-broadcast**. Del Cisco IOS Software Release 12.0, inhabilitan al **comando ip directed-broadcast** por abandono, que hace todos los broadcastes dirigidos por IP ser caído.
- Aquí está un nota al margen, sin relación al “Código rojo”, y relacionado a las arquitecturas de IRB:Acode el Multicast 2 y los paquetes de broadcast necesitan ser replicados. Por lo tanto, un problema con los servidores IPX que se ejecutan en un segmento de broadcast puede derribar el link. Usted puede utilizar las políticas de suscriptor para evitar el problema. Para más información, refiera al x Digital Subscriber Line (xDSL) Bridge Support. Usted debe también considerar las listas de acceso del Bridge, que limitan el tipo de tráfico permitido pasar a través del router.
- Para paliar este problema IRB, usted puede utilizar a los grupos de Bridge múltiples, y se asegura de que hay un mapeo uno a uno para los BVI, los subinterfaces y VCs.
- RBE es superior que IRB dado que evita que los puentes se apilen todos juntos. Usted puede emigrar al RBE del IRB. Estos bug de Cisco inspiran tal migración:CSCdr11146 (clientes registrados solamente)CSCdp18572 (clientes registrados solamente)CSCds40806 (clientes registrados solamente)

## La utilización de la CPU Q.My es alta en el nivel de interrupción, y recibo los rubores si intento un registro de la demostración. El ritmo de tráfico además es un poco más alto de lo normal. ¿Cuál es la razón de esto?

**R.** Aquí está un ejemplo del **comando show logging** hecho salir:

```
Router#show logging Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) ^ this
value is non-zero Console logging: level debugging, 9 messages logged
```

Marque si usted registra a la consola. Si es así marque si hay pedidos de HTTP del tráfico. Después, el control si hay algunas listas de acceso con las palabras claves o los debugs del registro que miran el IP determinado fluye. Si los rubores están en la subida, puede ser porque la consola, generalmente 9600 dispositivo de baudio, no puede manejar la cantidad de información recibida. En este escenario, las interrupciones de las neutralizaciones del router y hacen los mensajes de la consola nada pero del proceso. La solución es inhabilitar el registro de la consola o quitar cualquier tipo de registrarle realice.

### Q. Puedo ver las tentativas numerosas de la conexión HTTP en mi router IOS que funcione con un HTTP-servidor del IP. ¿Es por la búsqueda del gusano “Código rojo”?

El “Código rojo” **A.** puede ser la razón aquí. Cisco recomienda que usted inhabilita el **comando ip http server** en el router IOS de modo que no necesite ocuparse de los intentos de conexión numerosos de los host infectados.

## Soluciones alternativas

Hay las diversas soluciones alternativas que se discuten en las recomendaciones que discuten la sección del gusano del “Código rojo”. Refiera a las recomendaciones para las soluciones alternativas.

Otro método para bloquear el gusano del “Código rojo” en el Uses Network-Based Application Recognition de los puntos de ingreso a la red (NBAR) y el Listas de control de acceso (ACL) dentro del software IOS en los routeres Cisco. Utilice este método conjuntamente con las parches recomendado para los servidores IIS de Microsoft. Para más información sobre este método, refiérase con el NBAR y los ACL para bloquear el gusano del “Código rojo” en los puntos de ingreso a la red.

## Información Relacionada

- Resolución de problemas de la memoria
- Resolución de problemas de fuga de memoria intermedia
- Resolución de problemas por uso excesivo de las CPU de los routers de Cisco
- Resolución de problemas por averías del router
- Notas técnicas de Troubleshooting - Routers
- Resolución de problemas del router
- Soporte Técnico y Documentación - Cisco Systems