# Lidando com mallocfail e utilização elevada de CPU, resultante do worm "código vermelho”

## Índice



## Introdução

Este documento descreve o worm “Code Red” e os problemas que ele pode causar em um ambiente de roteamento Cisco. Este documento igualmente descreve técnicas para impedir a infestação do worm e fornece os links aos consultivos relacionados que descrevem soluções para

problemas worm-relacionados.

O worm do “código vermelho” explora uma vulnerabilidade no serviço do deslocamento predeterminado da versão 5.0 de Microsoft Internet Information Server (IIS). Quando o worm do “código vermelho” contamina um host, faz com que o host sonde e contamine uma série aleatória de endereços IP de Um ou Mais Servidores Cisco ICM NT, que causa um aumento agudo no tráfego de rede. Isto é especialmente problemático se há uns enlaces redundantes na rede e/ou o Cisco Express Forwarding (CEF) não está usado para comutar pacotes.

# Pré-requisitos

## Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

# Como o worm do “código vermelho” contamina outros sistemas

O worm "Código Vermelho" tenta se conectar a endereços IP gerados aleatoriamente. Cada servidor IIS contaminado pode tentar contaminar o mesmo conjunto de dispositivo. Você pode seguir o endereço IP de origem e a porta TCP do worm porque não é falsificado. O Unicast Reverse Path Forwarding (uRPF) não pode suprimir um ataque do worm porque o endereço de origem é legal.

# Consultivos que discutem o worm "Código Vermelho"

Estes relatórios formais descrevem o worm do “código vermelho”, e explicam como remendar o software afetado pelo worm:

- Consultivo de segurança Cisco: Worm "código vermelho" - impacto para o cliente
- Excesso de buffer do Index Server ISAPI Extension de IIS remoto
- Worm .ida "código vermelho"
- CERT? Worm consultivo do “código vermelho CA-2001-19” que explora o excesso de buffer no serviço de indexação DLL IIS

# Sintomas

Estão aqui alguns sintomas que indicam que um roteador Cisco está afetado pelo worm do “código vermelho”:

- Número grande de fluxos no NAT ou tabelas PAT (se você usa o NAT ou a PANCADINHA).
- Número grande de requisições ARP ou de tempestades ARP na rede (causada pela varredura do endereço IP de Um ou Mais Servidores Cisco ICM NT).
- Uso da memória excessiva pela entrada IP, pela entrada ARP, pelo Ager do cache IP e pelos processos CEF.
- Utilização elevada da CPU na entrada ARP, IP, no CEF e no IPC.
- Utilização elevada da CPU a nível de interrupção em taxas do tráfego baixo, ou utilização elevada da CPU a nível de processo na entrada IP, se você usa o NAT.

Uma condição de memória baixa ou uma utilização elevada da CPU sustentada (100 por cento) a nível de interrupção podem fazer com que um roteador do ® do Cisco IOS recarregue. O reload é causado por um processo que se porte mal devido às condições do esforço.

Se você não suspeita que os dispositivos em seu local estão contaminados por ou são o alvo do worm do “código vermelho”, veja a seção Informação Relacionada para URL adicionais em como pesquisar defeitos todas as edições que você encontrar.

# Identifique o dispositivo infectado

Use o switching de fluxo para identificar o endereço IP de origem do dispositivo afetado. Configurar o fluxo do cache de rota IP em todas as relações para gravar todos os fluxos comutados pelo roteador.

Após alguns minutos, emita o comando show ip cache flow ver as entradas gravadas. Durante a fase inicial da infecção do worm do “código vermelho”, o worm tenta replicate. A replicação ocorre quando o worm envia pedidos HT aos endereços IP de Um ou Mais Servidores Cisco ICM NT aleatórios. Consequentemente, você deve procurar entradas do fluxo de cache com porta do destino 80 (o HT., 0050 encanta dentro).

O fluxo de cache da mostra IP | inclua 0050 que o comando indica todas as entradas de cache com uma porta TCP 80 (0050 encantam dentro):

```
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
```

Se você encontra anormalmente um alto número de entradas com o mesmos endereço IP de origem, endereço IP de Um ou Mais Servidores Cisco ICM NT[1] do destino aleatório, DstP = 0050 (HTTP), e PR = 06 (TCP), você encontrou provavelmente um dispositivo infectado. Neste exemplo de emissor, o endereço IP de origem é 193.23.45.35 e vem do VLAN1.

a versão [1]Another do worm do “código vermelho”, chamada o “código vermelho II”, não escolhe totalmente um endereço IP de Um ou Mais Servidores Cisco ICM NT do destino aleatório. Em lugar de, o “código vermelho II” mantém a porção de rede do endereço IP de Um ou Mais

Servidores Cisco ICM NT, e escolhe uma parcela aleatória do host do endereço IP de Um ou Mais Servidores Cisco ICM NT a fim propagar. Isto permite que o worm espalhe-se mais rapidamente dentro da mesma rede.

O “código vermelho II” usa estas redes e 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)
```

Os endereços IP de destino que são excluídos são 127.X.X.X e 224.X.X.X, e nenhum octeto são reservados ser 0 ou 255. Além, o host não tenta re-contaminar-se.

Para mais informação, refira o código vermelho (ii) .

Às vezes, você não pode executar o Netflow para detectar uma tentativa da infestação do “código vermelho”. Isto pode ser porque você executa uma versão de código que não apoie o Netflow, ou porque o roteador tem insuficiente ou memória excessivamente fragmentada para permitir o Netflow. Cisco recomenda que você não permite o Netflow quando há umas interfaces de ingresso múltiplas e uma somente uma interface de saída no roteador, porque o Netflow Accounting está executado no caminho de ingresso. Neste caso, é melhor permitir a contabilidade IP na interface de saída solitária.

**Nota:** O comando ip accounting desabilita o DCEF. Não permita a contabilidade IP em nenhuma plataforma onde você quer usar o switching dCEF.

```
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
```

Na saída do comando show ip accounting, procure os endereços de origem que tentam enviar pacotes aos endereços de destino múltiplo. Se o host infectado se realiza na fase da varredura, tenta estabelecer conexões de HTTP ao outro Roteadores. Assim você verá tentativas de alcançar endereços IP de Um ou Mais Servidores Cisco ICM NT múltiplos. A maioria da falha destas tentativas de conexão normalmente. Consequentemente, você vê somente um pequeno número de pacotes transferidos, cada um com um contagem de byte pequeno. Neste exemplo, é provável que 20.1.145.49 e 20.1.104.194 estão contaminados.

Quando você executa o Multi-Layer Switching (MLS) no Catalyst 5000 Series e no Catalyst 6000 Series, você deve tomar etapas diferentes para permitir o Netflow Accounting e seguir para baixo a infestação. Em Cat6000 comute equipado com o Multilayer Switch Feature Card do Supervisor 1 (MSFC1) ou o SUP I/MSFC2, MLS Netflow-baseado é permitido à revelia, mas o fluxo-MODE é somente destino. Consequentemente, o endereço IP de origem não é posto em esconderijo. Você pode permitir o modo do “FULL-fluxo” de seguir para baixo host infectados com a ajuda do comando set mls flow full no supervisor.

Para o modo híbrido, use o **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 o modo de IOS nativo, use o comando mls flow ip full:

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

Quando você permite o modo do “FULL-fluxo”, um aviso está indicado para indicar um aumento dramático nas entradas de MLS. O impacto das entradas de MLS aumentadas é justificável por uma curta duração se sua rede é infestada já com o worm do “código vermelho”. O worm faz com que suas entradas de MLS sejam excessivas e na elevação.

Para ver a informações recolhidas, use estes comandos:

Para o modo híbrido, use o **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 o modo de IOS nativo, use o **comando mls flow ip full**:

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

Quando você permite o modo do “FULL-fluxo”, um aviso está indicado para indicar um aumento dramático nas entradas de MLS. O impacto das entradas de MLS aumentadas é justificável por uma curta duração se sua rede é infestada já com o worm do “código vermelho”. O worm faz com que suas entradas de MLS sejam excessivas e na elevação.

Para ver a informações recolhidas, use estes comandos:

Para o modo híbrido, use o 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:** Todos estes campos estão preenchidos quando reagem do modo do “FULL-fluxo”.

Para o modo de IOS nativo, use o **comando show mls ip**:

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

Quando você determina o endereço IP de origem e a porta do destino envolvidos no ataque, você pode ajustar o MLS de volta ao modo “somente destino”.

Para o modo híbrido use o comando set mls flow destination:

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

Para o modo de IOS nativo, use o comando mls flow ip destination:

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

A combinação II/MSFC2 do supervisor (SUP) é protegida do ataque porque o CEF switching é executado no hardware, e as estatísticas de Netflow são mantidas. Assim, mesmo durante um ataque do “código vermelho”, se você permite o modo fluxo completo, o roteador não é inundado, devido ao mecanismo de switching mais rápido. Os comandos permitir o modo fluxo completo e indicar as estatísticas são os mesmos no SUP I/MFSC1 e no SUP II/MSFC2.

## Técnicas de prevenção

Use as técnicas alistadas nesta seção para minimizar o impacto do worm do “código vermelho” no

roteador.

## Obstrua o tráfego à porta 80

Se é praticável em sua rede, a maneira a mais fácil de impedir o ataque do “código vermelho” é obstruir todo o tráfego à porta 80, que é a porta bem conhecida para o WWW. Construa uma lista de acesso para negar os pacotes IP destinados à porta 80 e para aplicá-los de entrada na relação que enfrenta o origem da infecção.

## Reduza o USO de memória da entrada ARP

A entrada ARP usa-se acima das quantias enormes da memória quando uma rota estática aponta a uma interface de transmissão, como esta:

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

Cada pacote para a rota padrão é enviado ao VLAN3. Contudo, não há nenhum endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte especificado, e assim, o roteador envia uma requisição ARP para o endereço IP de destino. O roteador de próximo salto para esse destino responde com seu próprio MAC address, a menos que o proxy ARP for desabilitado. A resposta do roteador cria uma entrada adicional na tabela ARP onde o endereço IP de destino do pacote é traçado ao MAC address do salto seguinte. O worm do “código vermelho” envia pacotes aos endereços IP de Um ou Mais Servidores Cisco ICM NT aleatórios, que adiciona uma entrada de ARP nova para cada endereço de destino aleatório. Cada entrada de ARP nova consome cada vez mais a memória sob o processo de entrada ARP.

Não crie uma rota padrão estática a uma relação, especialmente se a relação é a transmissão (Ethernet/Ethernet/GE/SMDS rápido) ou a multiponto (Frame Relay/ATM). Toda a rota padrão estática deve apontar ao endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador de próximo salto. Depois que você muda a rota padrão para apontar ao endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte, use o **comando clear arp-cache** cancelar todas as entradas de ARP. Este comando fixa o problema da utilização de memória.

## Use o switching do Cisco Express Forwarding (CEF)

A fim abaixar a utilização CPU em um IOS Router, mude do Fast/Optimum/NetFlow Switching ao CEF switching. Há algumas advertências para permitir o CEF. A próxima seção discute a diferença entre o CEF e o interruptor rápido, e explica as implicações quando você permite o CEF.

# Cisco Express Forwarding versus Fast Switching

Permita o CEF de aliviar a carga crescente de tráfego causada pelo worm do “código vermelho”. Software release 11.1 () CC, 12.0, e apoio mais atrasado CEF de Cisco IOS® nas Plataformas de Cisco 7200/7500/GSR. O apoio para o CEF em outras Plataformas está disponível no Cisco IOS Software Release 12.0 ou Mais Recente. Você pode investigar mais com a ferramenta de aconselhamento de software.

Às vezes, você não pode permitir o CEF em toda roteadores devido a uma destas razões:

- Memória insuficiente

- Arquitetura de plataforma não suportada
- Encapsulamentos de interface não suportados

## Comportamento e implicações do Fast Switching

Estão aqui as implicações quando você usa o interruptor rápido:

- Esconderijo conduzido tráfego — O esconderijo está vazio até os pacotes dos switch do roteador e povoa o esconderijo.
- O primeiro pacote é processo comutado — O primeiro pacote é comutado por processo, porque o esconderijo está inicialmente vazio.
- Esconderijo granulado — O esconderijo é construído em uma granularidade da entrada a mais específica do Routing Information Base (RIB) parte de uma rede principal. Se o RIB tem /24s para a rede principal 131.108.0.0, o esconderijo está construído com /24s para esta rede principal.
- o esconderijo de /32 é usado — o esconderijo de /32 é usado para equilibrar a carga para cada destino. Quando o esconderijo equilibra a carga, o esconderijo está construído com /32s para essa rede principal.**Nota:** Esses dois últimos problemas podem resultar em um cache imenso que consumiria toda a memória.
- Pôr em esconderijo em limites de rede principais — Com rota padrão, pôr em esconderijo é executado em limites de rede principais.
- O cache ager — O cache ager executa cada minuto e verifica o 1/20th (por cento 5) do esconderijo para ver se há entradas não utilizadas sob condições de memória normais, e 1/4th (25 por cento) do esconderijo em uma condição de memória baixa (200k).

A fim mudar os valores acima, use o **comando ip cache-ager-interval X Y Z**, onde:

- X são número <0-2147483> de segundos entre corridas do ager. Padrão = 60 segundos.
- Y é <2-50> 1/(Y+1) do esconderijo a envelhecer pela corrida (memória baixa). Padrão = 4.
- Z é <3-100> 1/(Z+1) do esconderijo a envelhecer pela corrida (normal). Padrão = 20.

Está aqui uma configuração de exemplo que usa o **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
```

Baseado no ajuste de seu cache ager, alguma porcentagem de sua idade de entradas de cache fora de sua tabela do cache rápido. Quando a idade de entradas rapidamente, uma porcentagem maior da tabela do cache rápido envelhece, e a tabela de cache torna-se menor. Em consequência, o consumo de memória no roteador reduz-se. Uma desvantagem é que o tráfego continua a fluir para as entradas que foram envelhecidas fora da tabela de cache. Os pacotes iniciais são comutados por processo, que causa um ponto curto no consumo de CPU no **IP entrado** até que uma entrada de cache nova esteja construída para o fluxo.

Dos Cisco IOS Software Release 10.3(8), 11.0(3) e mais atrasado, o ager do cache IP são

segurados diferentemente, como explicado aqui:

- **Os comandos ip cache-ager-interval e ip cache-invalidate-delay** estão disponíveis somente se o **comando service internal** é definido na configuração.
- Se o período entre corridas da invalidação do ager é ajustado a 0, o processo de ager está desabilitado inteiramente.
- O tempo é expresso em segundos.

**Nota:** Quando você executa estes comandos, a utilização CPU do roteador aumenta. Use estes comandos somente quando absolutamente necessário.

```
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
```

## Vantagens do CEF

- A tabela do banco de informação de encaminhamento (FIB) é construída com base na tabela de roteamento. Consequentemente a informação de encaminhamento existe antes que o primeiro pacote esteja enviado. O FIB também contém /32 entradas para hosts de LAN conectados diretamente.
- A tabela da adjacência (ADJ) contém a informação reescrita da camada 2 para saltos seguintes e anfitriões conectados diretamente (uma entrada de ARP cria uma adjacência de CEF).
- Não há conceito de envelhecimento de cache com CEF para aumentar a utilização de CPU. Uma entrada MENTIR é suprimida se uma entrada de tabela de roteamento é suprimida.

**Cuidado:** Além disso, uma rota padrão que aponte a uma transmissão ou a uma interface multiponto significa que o roteador envia requisições ARP para cada destino novo. As requisições ARP do roteador criam potencialmente uma tabela de adjacência enorme até o roteador são executado fora da memória. Se o CEF não atribui a memória CEF/DCEF desabilita-se. Você precisará de permitir manualmente outra vez o CEF/DCEF.

## Saída de exemplo: CEF

Está aqui algum exemplo de saída do comando show ip cef summary, essa utilização de memória das mostras. Esta saída é um instantâneo de um servidor de rota do Cisco 7200 com 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
```

## Pontos a serem considerados

Quando o número de fluxos é grande, o CEF consome tipicamente menos memória do que rapidamente comutando. Se a memória é consumida já por um cache de switching rápido, você deve cancelar o cache ARP (através do **comando clear ip arp**) antes que você permita o CEF.

**Nota:** Quando você cancela o esconderijo, um ponto está causado na utilização CPU do roteador.

# Perguntas mais frequentes do “código vermelho” e suas respostas

### Q. Eu uso o NAT, e experimento 100 percentuais de utilização de CPU na entrada IP. Quando eu executo o processador central do proc da mostra, minha utilização CPU é alta no nível de interrupção - 100/99 ou 99/98. Pode isto ser relacionado ao “código vermelho”?

**R.** É fixado recentemente um Bug da Cisco NAT (CSCdu63623 (clientes registrados somente)) que envolva a escalabilidade. Quando houver uns dez dos milhares de fluxos NAT (baseados no tipo de plataforma), o erro causa 100 percentuais de utilização de CPU a processo ou nível de interrupção.

A fim determinar se este erro é a razão, emita o **comando show align**, e verifique se o roteador enfrenta erros de alinhamento. Se você vê erros de alinhamento ou acessos de memória artificiais, emita o **comando show align** um par vezes e veja se os erros estão na elevação. Se o número de erros está na elevação, os erros de alinhamento podem ser a causa da utilização elevada da CPU a nível de interrupção, e não CSCdu63623 do Bug da Cisco (clientes registrados somente). Para mais informação, refira pesquisando defeitos acessos artificiais e erros de alinhamento.

**O comando show ip nat translation** indica o número de traduções ativa. O ponto da fusão para um processador da classe do NPE-300 é aproximadamente 20,000 a 40,000 traduções. Este número varia baseado na plataforma.

Este problema de sobrecarga foi observado previamente por um par clientes, mas após o “código vermelho”, mais clientes experimentaram este problema. A única ação alternativa é executar o NAT (em vez da PANCADINHA), de modo que haja menos traduções ativa. Se você tem uns 7200, use um NSE-1, e abaixe os valores de timeout NAT.

### Q. Eu executo o IRB, e encontro a utilização elevada da CPU no processo de entrada de hybridge. Por que isso acontece? Tem alguma relação com "Código Vermelho"?

**R.** O processo de entrada de hybridge segura todos os pacotes que não puderem ser fast-switched pelo processo IRB. A incapacidade do processo IRB ao fast-switch um pacote pode ser porque:

- O pacote é um pacote de transmissão.
- O pacote é um pacote de transmissão múltipla.
- O destino é desconhecido, e o ARP precisa de ser provocado.
- Está medindo - a árvore BPDU.

A entrada de hybridge encontra problemas se há uns milhares de interfaces Point-to-Point no mesmo grupo de bridge. A entrada de hybridge igualmente encontra edições (mas a um grau inferior) se há uns milhares de VSs na mesma interface multiponto.

Quais são os motivos possíveis para problemas com IRB? Supõe que um dispositivo contaminado com o “código vermelho” faz a varredura de endereços IP de Um ou Mais Servidores Cisco ICM NT.

- O roteador precisa de enviar uma requisição ARP para cada endereço IP de destino. Uma inundação das requisições ARP resulta em cada VC no grupo de bridge para cada endereço que é feito a varredura. O processo ARP normal não causa um problema de CPU. Contudo, se há uma entrada de ARP sem uma entrada da ponte, as inundações de pacotes no roteador destinaram para os endereços para que as entradas de ARP já existem. Isso poderá causar uma alta utilização de CPU, pois o tráfego é comutado pelo processo. Para evitar o problema, aumentar o momento do ponte-envelhecimento (padrão 300 segundos ou minutos 5) de combinar ou exceder o arp timeout (padrão 4 horas) de modo que os dois temporizadores sejam sincronizados.
- O endereço que o host final tenta contaminar é um endereço de broadcast. O roteador faz o equivalente a uma difusão de sub-rede que precisa ser replicada pelo processo HyBridge Input (Entrada de HyBridge). Isto não acontece se o **comando no ip directed-broadcast** é configurado. Do Cisco IOS Software Release 12.0, o **comando ip directed-broadcast** é desabilitado à revelia, que faz com que todos os broadcasts direto de IP sejam deixados cair.
- Está aqui uma nota lateral, não relacionada ao “código vermelho”, e relacionado às arquiteturas IRB:Mergulhe o Multicast 2 e os pacotes de transmissão precisam de ser replicated. Consequentemente, um problema com servidores de IPX que são executado em um segmento de transmissão pode derrubar o link. Você pode usar políticas de assinante para evitar o problema. Para mais informação, refira o x Digital Subscriber Line (xDSL) Bridge Support. Você deve igualmente considerar as listas de acesso da ponte, que limitam o tipo de tráfego permitido passar através do roteador.
- A fim aliviar este problema IRB, você pode usar grupos de bridges múltiplos, e assegura-se de que haja um mapeamento um a um para BVI, subinterfaces e VC.
- O RBE é superior ao IRB porque evita a pilha de Bridging. Você pode migrar ao RBE do IRB. Estes Bug da Cisco inspiram tal migração:CSCdr11146 (clientes registrados somente)CSCdp18572 (clientes registrados somente)CSCds40806 (clientes registrados somente)

## A utilização CPU Q.My é alta a nível de interrupção, e eu recebo resplendores se eu tento um log da mostra. A taxa de tráfego também está um pouco superior ao normal. Que é a razão para este?

**R.** Está aqui um exemplo do **comando show logging** output:

```
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
```

Verifique se você registre ao console. Em caso afirmativo, verifique se haja uns pedidos do HTTP do tráfego. Em seguida, a verificação se há alguma lista de acesso com palavras-chaves do log ou debuga que o IP particular do relógio flui. Se os resplendores estão na elevação, pode ser porque o console, geralmente um dispositivo de 9600 baud, é incapaz de segurar a quantidade de informação recebida. Nesta encenação, as interrupções das inutilizações do roteador e fazem mensagens do console nada mas do processo. A solução é desabilitar o logging de console ou remover o que tipo do registrar execute.

### Q. Eu posso ver tentativas numerosas da conexão de HTTP em meu IOS Router que executa um HTTP-server IP. Isso é devido ao exame de worm "Código vermelho"?

**O A.** “código vermelho” pode ser a razão aqui. Cisco recomenda que você desabilita o **comando ip http server no** IOS Router de modo que não precise de tratar as tentativas de conexão numerosas dos host infectados.

## Soluções

Há as várias ações alternativas que são discutidas nos relatórios formais que discutem a seção do worm do “código vermelho”. Refira os relatórios formais para as ações alternativas.

Um outro método para obstruir o worm do “código vermelho” no Uses Network-Based Application Recognition dos pontos de ingresso de rede (NBAR) e o Access Control Lists (ACLs) dentro do IOS Software em roteadores Cisco. Use este método conjuntamente com as correções recomendadas para servidores IIS de Microsoft. Para obter mais informações sobre deste método, refira a utilização do NBAR e dos ACL para obstruir o worm do “código vermelho” em pontos de ingresso de rede.

## Informações Relacionadas

- Troubleshooting Problemas de Memória
- Troubleshooting de Vazamentos de Buffer
- Troubleshooting de Alta Utilização de CPU em Cisco Routers
- Troubleshooting de Travamentos de Roteador
- Pesquisando defeitos TechNotes - Roteadores
- Troubleshooting do Roteador
- Suporte Técnico e Documentação - Cisco Systems