處理「紅色代碼」蠕蟲引起的mallocfail和CPU使用率高的問題

目錄

簡介

本檔案介紹「紅色代碼」蠕蟲及其在Cisco路由環境中可能引起的問題。本文還提供防止蠕蟲感染的技術，以及指向描述蠕蟲相關問題解決方案的相關建議的連結。

「Code Red」蠕蟲利用Microsoft Internet Information Server(IIS)5.0版的Index Service中的漏洞進行攻擊。當「Code Red」蠕蟲感染主機時，會導致主機探測並感染一系列隨機的IP地址，從而導致

網路流量急劇增加。如果網路中有備援連結和/或未使用思科快速轉送(CEF)來交換封包，則問題尤其嚴重。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

「紅色代碼」蠕蟲如何感染其他系統

「紅色代碼」蠕蟲會嘗試連線到隨機生成的IP地址。每個受感染的IIS伺服器都可以嘗試感染同一組裝置。您可以追蹤蠕蟲的來源IP位址和TCP連線埠，因為它沒有偽裝。單播反向路徑轉發(URPF)無法抑制蠕蟲攻擊，因為源地址是合法的。

討論「紅色代碼」蠕蟲的建議

以下建議介紹「紅色代碼」蠕蟲，並說明如何修補受蠕蟲影響的軟體：

- 思科資安顧問諮詢：「紅色代碼」蠕蟲 — 客戶影響
- 遠端IIS索引伺服器ISAPI擴展緩衝區溢位
- .ida "紅色代碼"蠕蟲
- 認證？建議CA-2001-19「Code Red」蠕蟲利用IIS索引服務DLL中的緩衝區溢位

症狀

以下是表示Cisco路由器受「紅色代碼」蠕蟲影響的症狀：

- NAT或PAT表中大量的流（如果您使用NAT或PAT）。
- 網路中出現大量ARP請求或ARP風暴（由IP地址掃描引起）。
- IP Input、ARP Input、IP Cache Ager和CEF進程佔用過多記憶體。
- ARP、IP Input、CEF和IPC中的CPU使用率高。
- 如果使用NAT，則中斷級別的CPU使用率較高，而流量率較低；或者IP輸入中的進程級別的CPU使用率較高。

記憶體不足或中斷級別的CPU利用率持續高(100%)，可能導致Cisco IOS®路由器重新載入。重新載

入是由進程引起的，該進程由於應力條件而發生異常。

如果您懷疑站點中的裝置感染了「紅色代碼」蠕蟲或它是「紅色代碼」蠕蟲的目標，請參閱相關資訊部分，以獲取有關如何解決遇到的任何問題的其他URL。

識別受感染的裝置

使用流交換識別受影響裝置的源IP地址。在所有介面上配置ip route-cache flow，以記錄路由器交換的所有資料流。

幾分鐘後，發出show ip cache flow 命令以檢視記錄的條目。在「紅色代碼」蠕蟲感染的初始階段，蠕蟲會嘗試自我複製。當蠕蟲向隨機IP地址傳送HT請求時，就會發生複製。因此，必須查詢目標埠為80(HT., 0050（十六進位制）)的快取流條目。

show ip cache flow | include 0050命令顯示具有TCP埠80（0050以十六進位制表示）的所有快取條目：

```
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
```

如果您發現具有相同源IP地址、隨機目標IP地址[1]、DstP = 0050(HTTP)和Pr = 06(TCP)的條目數量異常多，則可能找到了受感染的裝置。在此輸出範例中，來源IP位址為193.23.45.35，且來自VLAN1。

[1]「紅色代碼」蠕蟲的另一個版本（稱為「紅色代碼II」）不選擇完全隨機目的IP地址。相反，「紅色代碼II」保留IP地址的網路部分，並選擇該IP地址的隨機主機部分進行傳播。這使得蠕蟲可以在同一個網路中更快地自我傳播。

「紅色代碼II」使用以下網路和掩碼：

```
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)
```

排除的目標IP地址為127.X.X.X和224.X.X.X，不允許二進位制八位數是0或255。此外，主機不會嘗試重新感染自己。

如需詳細資訊，請參閱紅色代碼(II) 。

有時，無法運行netflow來檢測「紅色代碼」感染嘗試。這可能是因為您運行的代碼版本不支援netflow，或者因為路由器沒有足夠的記憶體或過度碎片來啟用netflow。思科建議您不要在路由器上

有多個輸入介面且只有一個輸出介面時啟用netflow，因為會在輸入路徑上執行netflow記帳。在這種情況下，最好在唯一的輸出介面上啟用IP計量。

注意：ip accounting 命令會禁用DCEF。請勿在要使用DCEF交換的任何平台上啟用IP記帳。

```
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
```

在show ip accounting命令輸出中，查詢嘗試將資料包傳送到多個目標地址的源地址。如果受感染的主機處於掃描階段，它會嘗試建立到其他路由器的HTTP連線。因此您會看到嘗試訪問多個IP地址。大多數連線嘗試通常會失敗。因此，您只看到少量資料包被傳輸，每個資料包的位元組數都很少。在本示例中，20.1.145.49和20.1.104.194可能受到感染。

在Catalyst 5000系列和Catalyst 6000系列上執行多層交換(MLS)時，您必須執行不同的步驟以啟用netflow計量並追蹤感染。在配備了Supervisor 1多層次交換功能卡(MSFC1)或SUP I/MSFC2的Cat6000交換器中，預設會啟用基於netflow的MLS，但流量模式是僅目的地模式。因此，不會快取源IP地址。您可以使用Supervisor上的set mls flow full 命令，啟用「全流」模式以追蹤受感染的主機。

對於混合模式，請使用**set mls flow full**命令：

```
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.
```

對於本地IOS模式，請使用mls flow ip full 命令：

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

啟用「全流」模式時，將顯示一條警告，指示MLS條目大幅增加。增加的MLS條目對您的網路已經感染了「紅色代碼」蠕蟲的影響在短期內是合理的。該蠕蟲導致您的MLS條目過多且呈上升趨勢。

要檢視收集的資訊，請使用以下命令：

對於混合模式，請使用**set mls flow full**命令：

```
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.
```

在本機IOS模式下，使用**mls flow ip full**命令：

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

啟用「全流」模式時，將顯示一條警告，指示MLS條目大幅增加。增加的MLS條目對您的網路已經感染了「紅色代碼」蠕蟲的影響在短期內是合理的。該蠕蟲導致您的MLS條目過多且呈上升趨勢。

要檢視收集的資訊，請使用以下命令：

對於混合模式，請使用show mls ent 命令：

```
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
-------------- -------------- ----- ------ ------ ----------------- ---- ----
---- --------- --------- ---------- ----------- -------- --------
```

注意：所有這些欄位均在「全流」模式下填寫。

對於本地IOS模式，請使用**show mls ip**命令：

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

確定攻擊中涉及的源IP地址和目標埠時，可以將MLS設定為「僅目標」模式。

對於混合模式，請使用set mls flow destination 命令：

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

在本機IOS模式下，使用mls flow **ip destination命**令：

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

Supervisor(SUP)II/MSFC2組合會受到保護，不會受到攻擊，因為會在硬體中執行CEF交換，且會維護netflow統計資訊。因此，即使在「紅色代碼」攻擊期間，如果您啟用全流模式，由於交換機制更快，路由器也不會被淹沒。在SUP I/MFSC1和SUP II/MSFC2上啟用全流模式和顯示統計資訊的命令相同。

預防技術

使用本節所列的技術，將「紅色代碼」蠕蟲對路由器的影響降至最低。

阻止流向埠80的流量

如果在您的網路中可行，防止「紅色代碼」攻擊的最簡單方法是阻止所有流量流向埠80（WWW的公認埠）。建立存取清單，以拒絕目的地為連線埠80的IP封包，並將其傳入到面對感染來源的介面上。

減少ARP輸入記憶體使用

當靜態路由指向廣播介面時，ARP輸入會消耗大量記憶體，如下所示：

```
ip route 0.0.0.0 0.0.0.0 Vlan3
```

預設路由的每個資料包都會傳送到VLAN3。但是，沒有指定下一跳IP地址，因此路由器會傳送目的IP地址的ARP請求。除非禁用代理ARP，否則該目標的下一跳路由器會使用自己的MAC地址進行應答。來自路由器的回覆會在ARP表中建立一個額外的條目，其中資料包的目的IP地址對映到下一跳MAC地址。「紅色代碼」蠕蟲將資料包傳送到隨機IP地址，為每個隨機目標地址新增新的ARP條目。在ARP輸入過程中，每個新的ARP條目會消耗越來越多的記憶體。

不要建立到介面的靜態預設路由，尤其是當介面是廣播（乙太網/快速乙太網/GE/SMDS）或多點（幀中繼/ATM）時。 任何靜態預設路由都必須指向下一跳路由器的IP地址。將預設路由更改為指向下一跳IP地址後，使用**clear arp-cache**命令清除所有ARP條目。此命令可修復記憶體利用率問題。

使用Cisco Express Forwarding(CEF)交換

為了降低IOS路由器上的CPU使用率，請從快速/最佳/Netflow交換更改為CEF交換。啟用CEF時需要注意幾點。下一節將討論CEF和快速交換之間的差異，並解釋啟用CEF時的影響。

Cisco快速轉送與快速交換

啟用CEF可緩解「紅色代碼」蠕蟲導致的流量負載增加。Cisco IOS®軟體版本11.1(CC)、12.0和更高版本在Cisco 7200/7500/GSR平台上支援CEF。Cisco IOS軟體版本12.0或更高版本支援其他平台上的CEF。您可以使用Software Advisor工具進一步進行調查。

有時，您無法在所有的路由器上啟用CEF，原因如下：

- 記憶體不足
- 不受支援的平台架構
- 不支援的介面封裝

快速交換行為及其影響

以下是使用快速交換時的含義：

- 流量驅動快取 — 快取為空，直到路由器交換資料包並填充快取。
- 第一個資料包是進程交換 — 第一個資料包是進程交換，因為快取最初是空的。
- 粒度快取 — 快取構建於主網中最具體的路由資訊庫(RIB)條目部分的粒度上。如果RIB主網路131.108.0.0有/24s ，則快取將使用/24s構建主網路。
- 使用/32快取 — /32快取用於平衡每個目標的負載。當快取平衡負載時，該主網路使用/32構建

快取。**注意：**上兩個問題可能會導致佔用所有記憶體的巨大快取。
- 在主網路邊界處快取 — 使用預設路由，在主網路邊界處執行快取。
- 快取管理器 — 快取管理器每分鐘運行一次，並檢查第1/20(5%)個快取，以查詢在正常記憶體條件下未使用的條目，以及在低記憶體條件(200k)下第1/4(25%)個快取。

要更改上述值，請使用**ip cache-ager-interval X Y Z**命令，其中：

- X是老化器運行2147483間的秒數。預設值= 60秒。
- Y是每次運行（低記憶體）要老化的<2-50> 1/(Y+1)個快取。 預設值= 4。
- Z是每次運行（正常）要老化的<3-100> 1/(Z+1)個快取。 預設值= 20。

以下是使用**ip cache-ager 60 5 25的組態範例**。

```
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
```

根據快取記憶體器設定，快取記憶體條目中一部分會從快速快取記憶體表中過期。當條目快速老化時，快速快取表中較大部分會老化，快取表會變小。因此，路由器上的記憶體消耗會降低。缺點是流量繼續流向快取表中老化的條目。初始資料包採用進程交換，這會導致**IP Input**中的CPU消耗量出現短暫峰值，直到為流構建新的快取條目。

自Cisco IOS軟體版本10.3(8)、11.0(3)和更新版本起，IP快取處理器的處理方式有所不同，如下所述：

- 只有在配置中定義**service internal**命令時，**ip cache-ager-interval**和**ip cache-invalidate-delay**命令才可用。
- 如果老化器失效運行之間的時間段設定為0，則完全禁用老化器進程。
- 時間以秒表示。

注意：執行這些命令時，路由器的CPU利用率會增加。僅在絕對必要時使用這些命令。

```
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
```

CEF的優點

- 轉發資訊庫(FIB)表是根據路由表構建的。因此，轉發第一個資料包之前存在轉發資訊。FIB還包含直連LAN主機的/32條目。
- 鄰接關係(ADJ)表包含下一跳和直連主機的第2層重寫資訊（ARP條目建立CEF鄰接關係）。
- 沒有使用CEF的快取器概念來提高CPU利用率。如果刪除了路由表條目，則會刪除FIB條目。

注意：同樣，指向廣播或多點介面的預設路由意味著路由器為每個新目標傳送ARP請求。來自路由器的ARP請求可能會建立一個巨大的鄰接表，直到路由器記憶體耗盡。如果CEF無法分配記憶體，則CEF/DCEF會禁用自身。您將需要再次手動啟用CEF/DCEF。

輸出示例：CEF

以下是show ip cef summary命令的一些輸出範例，顯示記憶體使用情況。此輸出是採用Cisco IOS軟體版本12.0的Cisco 7200路由伺服器的快照。

```
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
```

注意事項

當流數量較大時，CEF通常比快速交換消耗更少的記憶體。如果快速交換快取已佔用記憶體，則必須在啟用CEF之前清除ARP快取(通過**clear ip arp**命令)。

注意：清除快取時，路由器的CPU利用率會急劇上升。

「紅色代碼」常見問題及其答案

問：我使用NAT，在IP輸入中體驗到100%的CPU使用率。當我執行show proc cpu時，我的CPU使用率在中斷級別很高 — 100/99或99/98。這是否與「紅色代碼」有關？

答：最近修復了一個涉及可擴充性的NAT Cisco錯誤(CSCdu63623(僅限註冊客戶)。當有數以萬計的NAT流（根據平台型別）時，該錯誤會導致進程或中斷級別的100%的CPU利用率。

若要判斷此錯誤是否為原因，請發出**show align**命令，並驗證路由器是否遇到對齊錯誤。如果確實看到對齊錯誤或虛假記憶體訪問，請發出**show align**命令幾次，然後檢視錯誤是否增加。如果錯誤數量在上升，對齊錯誤可能是中斷級別CPU使用率較高的原因，而不是思科錯誤CSCdu63623(僅限

註冊客戶)。 如需詳細資訊，請參閱疑難排解虛假存取和對齊錯誤。

show ip nat translation命令顯示活動轉換的數量。NPE-300級處理器的崩潰點大約是2萬到4萬次轉換。此數字因平台而異。

此崩潰問題以前由幾個客戶發現，但在「紅色代碼」之後，更多客戶遇到過此問題。唯一的解決方法是運行NAT（而不是PAT），以便減少活動轉換。如果您有7200，請使用NSE-1，然後降低NAT超時值。

問：我運行IRB，在HyBridge輸入過程中遇到高CPU使用率。為什麼會發生這種情況？是否與「紅色代碼」相關？

A. HyBridge Input進程處理IRB進程無法快速交換的任何資料包。IRB進程無法快速交換資料包的原因可能是：

- 此封包是廣播封包。
- 封包是多點傳送封包。
- 目的地未知，需要觸發ARP。
- 有跨距樹狀目錄BPDU。

如果同一網橋組中有數千個點對點介面，HyBridge輸入會遇到問題。如果同一多點介面中有數千個VS，HyBridge輸入也會遇到問題（但程度較小）。

IRB出現問題的可能原因是什麼？假設感染了「紅色代碼」的裝置會掃描IP地址。

- 路由器需要為每個目的IP地址傳送ARP請求。對於掃描的每個地址，網橋組中的每個VC上都會產生大量ARP請求。正常的ARP進程不會導致CPU問題。但是，如果存在不帶網橋條目的ARP條目，路由器會向目的地址中已經存在ARP條目的資料包泛洪。這會導致CPU使用率高，因為流量是進程交換的。為了避免此問題，請增加網橋老化時間（預設300秒或5分鐘）以匹配或超過ARP超時（預設4小時），以便兩個計時器同步。
- 終端主機嘗試感染的地址是廣播地址。路由器執行的子網廣播相當於HyBridge輸入過程需要複製的子網廣播。如果設定了**no ip directed-broadcast**命令，則不會發生這種情況。自Cisco IOS軟體版本12.0起，**ip directed-broadcast**命令預設為停用，這會導致所有IP導向型廣播被捨棄。
- 下面是與「紅色代碼」無關並與IRB架構相關的註釋：需要複製第2層組播和廣播資料包。因此，在廣播網段上運行的IPX伺服器出現問題會導致鏈路關閉。可以使用訂戶策略避免此問題。如需詳細資訊，請參閱x數位使用者線路(xDSL)橋接器支援。您還必須考慮網橋存取清單，這些清單會限制允許通過路由器的流量型別。
- 為了緩解此IRB問題，可以使用多個網橋組，並確儲存在針對BVI、子介面和VC的一對一對映。
- RBE優於IRB，因為它完全避免了橋接堆疊。您可以從IRB遷移到RBE。這些思科錯誤激發了這些遷移：CSCdr1146(僅限註冊客戶)CSCdp18572(僅限註冊客戶)CSCds40806(僅限註冊客戶)

問：在中斷級別我的CPU使用率很高，如果我嘗試顯示日誌，我會收到刷新資訊。流量速率也只是稍高於正常水準。原因是什麼？

A.以下是**show logging**命令**輸出**的範例：

```
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
```

檢查您是否登入到控制檯。如果是，請檢查是否存在流量HTTP請求。接下來，檢查是否有包含日誌關鍵字的存取清單或監控特定IP流的偵錯。如果刷新率上升，可能是由於控制檯（通常是9600波特裝置）無法處理接收到的資訊量。在這種情況下，路由器會禁用中斷，除處理控制檯消息外不執行任何操作。解決方案是禁用控制檯日誌記錄或刪除您執行的任何型別的日誌記錄。

問：在運行ip http-server的IOS路由器上，我可以看到許多HTTP連線嘗試。這是因為「紅色代碼」蠕蟲掃描嗎？

A.「紅色代碼」可能是原因。思科建議您在IOS路由器上禁用**ip http server**命令，以便它無需處理來自受感染主機的無數連線嘗試。

因應措施

討論「紅色代碼」蠕蟲病毒的建議一節中討論了各種解決方法。請參考參考諮詢以獲得解決方法。

另一種在網路入口點阻止「Code Red」蠕蟲的方法在Cisco路由器的IOS軟體中使用基於網路的應用識別(NBAR)和訪問控制清單(ACL)。將此方法與推薦的Microsoft IIS伺服器修補程式結合使用。有關此方法的詳細資訊，請參閱使用NBAR和ACL在網路入口點阻止「紅色代碼」蠕蟲。

相關資訊

- **記憶體問題故障排除**
- **排除緩衝區洩漏故障**
- **疑難排解思科路由器 CPU 高使用率的問題**
- **路由器崩潰故障排除**
- **疑難排解技術筆記 — 路由器**
- **路由器故障排除**
- **技術支援與文件 - Cisco Systems**