



10 | 案例篇：系統的軟中斷CPU使用率升高，我該怎麼辦？

JeriChen



案例：反向代理服務器 Nginx

- 文中範例：模擬DOS攻擊, 類型為 Syn Flood
 - `hping3 -S -p 80 -i u100 192.168.0.30`
 - 每隔100微秒發送一個TCP封包(SYN)到 192.168.0.30 port 80
 - `watch -d cat /proc/softirqs`
 - 判斷軟中斷類型：網絡接收

sar -n DEV 1 (-n 分析輸出網絡設備狀態統計信息/ DEV 報告網絡設備的統計訊息)

```
01:35:01      IFACE  rxpck/s  txpck/s   rxkB/s   txkB/s   rxcmp/s   txcmp/s  rxmcst/s   %ifutil
01:35:02    docker0  5390.80 10780.46  231.64   568.50     0.00     0.00     0.00     0.00
01:35:02      eth0 10789.66  5400.00  421.58   306.84     0.00     0.00     0.00     0.00
01:35:02 veth5912ce8  5390.80 10780.46  305.34   568.50     0.00     0.00     0.00     0.05
01:35:02         lo    0.00    0.00    0.00    0.00     0.00     0.00     0.00     0.00
```

- 報告的時間
- IFACE：網卡名稱
- rxpck/s：每秒接收的數據包總數
- txpck/s：每秒傳輸的數據包總數
- rxkB/s：每秒接收的字節(byte)總數
- txkB/s：每秒傳輸的字節(byte)總數
- rxcmp/s：每秒接收壓縮數據包總數
- txcmp/s：每秒傳輸壓縮數據包的總數
- rxmcst/s：每秒接收的群播(multicast)數據包總數
- %ifutil：網絡接口使用率



tcpdump -i eth0 -n tcp port 80 (確認是什麼樣的網路, 從那裡來的)

```
01:30:18.303424 IP 172.31.37.238.80 > 18.181.199.69.56173: Flags [S.], seq 3915598523, ack 2130737668, win 64240, options [mss 1460], length 0
```

- 從 18.181.199.69:56173 發送到 172.31.37.238:80
- Flags [S] 則表示這是一個 SYN包



案例：php-fpm 佔用大量的 CPU

- 壓力測試
 - `ab -c 10 -n 10000 http://52.195.2.110/example.php`
 - 併發 10 個請求測試 nginx 效能, 總共測試 10000 個請求



思考

最後，我想請你一起來聊聊，你所碰到的軟中斷問題。你所碰到的軟中問題是這種類型，是不是這個案例中的小包問題？你又是怎麼分析它們的來源並解決的呢？



參考資料

- Ubuntu manuals
 - <http://manpages.ubuntu.com/manpages/trusty/man1/sar.sysstat.1.html>
- Linux SAR 指令大全
 - <https://www.twblogs.net/a/5cd38884bd9eee67a77f1005>
- Linux strace
 - https://linuxtools-rst.readthedocs.io/zh_CN/latest/tool/strace.html