

Open NTP server 的問題

- **NOTICE** 2019/11/27 網路協進會報告，自2020/02/11(二)起，比照 **open DNS** 的處理，若偵測為 **open NTP server** 將自動阻斷其IP，請使用者務必修正問題，以免網路遭阻斷。阻斷處理，詳「[不當網路資訊](#)」
- 為幫助本校使用者防治 open NTP server 的問題，2019/05/17 本頁面上線，以提供更多相關資料。
- 由於軟體及設備種類繁多，歡迎知悉某特定軟體或設備其修正方法者，能不吝提供資料，嘉惠眾人，詳：[網路設備](#)

問題概述

- Open NTP server 指伺服器(或資訊設備)對外公開且不限使用對象提供 NTP 網路對時服務，可能產生以下問題：
 1. 暴露於外界，容易被攻擊或平白損耗系統及網路資源
 2. 容易被外界利用，成為發動 **DDoS** 網路攻擊的一員
 3. 因系統資訊揭露，衍生入侵問題
- 關於利用 NTP 的反射放大攻擊(reflection and amplification attack)請參閱此連結 [NTP amplification attack](#)

偵測系統

NEW 為防治 open NTP server 問題，協助處理校園內電腦或資訊設備，因設定不慎而可能遭攻擊者利用來發動網路攻擊，故本組建置 open NTP server 偵測系統，並將偵測結果提供各單位網管，以便轉知其使用者參考[建議作法](#)來修正設定及自行檢測問題是否解決，藉以減少本校網路內 open NTP server 的數量。

最近七天內偵測結果

- **NOTICE** 若已存在本清單的 IP 地址，至少需等待至隔日系統重新偵測，通過後時才會移除，故擬移出本清單者，請先用下方的「[即時檢測服務](#)」，檢查確認該 IP 地址已無問題後，隔日應可自清單中移除。

更新時間 Wed Feb 11 13:27:00 2026 Asia/Taipei

序號	單位	IP 位址	偵測時間	備註
總計 0 筆記錄				

即時檢測服務

NEW 為方便本校使用者自行檢測其電腦或網路設備是否具有 **open NTP server** 的問題，特建置此即時的檢測服務，目前限由本校 IP 位址來進行檢測。(2019/05/14上線試用)

檢測 open NTP server IP 位址: . . .

- **NOTICE** 檢測前請先確認目標 IP 位址的電腦或設備狀態為開機且網路連線正常，以免影響檢測結果。

檢測說明

- 採用 <http://openntpproject.org/> 的偵測方法，若有類似以下輸出結果，則表具有 **open NTP server** 問題
 - 不應回覆 **NTP** 查詢

```
Check open ntp for the target IP 140.114.XX.XX
Time: Tue May 14 15:06:28 2019

check_open_ntp: 140.114.XX.XX
check open ntp server with (140.114.XX.XX,,)

Command: (/sbin/ntpq -c rv 140.114.XX.XX; /sbin/ntpdc -n -c
monlist 140.114.XX.XX)

STDOUT: 6
  associd=0 status=062c leap_none, sync_ntp, 2 events, clock_step,
  version="4", processor="unknown", system="UNIX", leap=00,
  stratum=3,
  precision=-10, rootdelay=, rootdisp=, refid=118.163.81.61,
  reftime=e084df98.d4395a58 Tue, May 14 2019 14:32:56.829,
  clock=e084e775.028f5c30 Tue, May 14 2019 15:06:29.010,
  peer=39323,
  tc=10, mintc=3, offset=, frequency=, sys_jitter=, clk_jitter=,
  clk_wander=

STDERR: 1
140.114.XX.XX: timed out, nothing received
***Request timed out

Is 140.114.XX.XX an open ntp server?
ANSWER: YES for 140.114.XX.XX
```

- 若類似以下輸出結果，表不具有 **open NTP server** 問題
 1. 無 **NTP** 回應，若電腦已開且網路已通，則此機無問題。

```
Check open ntp for the target IP 140.114.63.253
Time: Tue May 14 15:11:28 2019

check_open_ntp: 140.114.63.253
check open ntp server with (140.114.63.253,,)

Command: (/sbin/ntpq -c rv 140.114.63.253; /sbin/ntpdc -n -c
monlist 140.114.63.253)

STDOUT: -1

STDERR: 3
140.114.63.253: timed out, nothing received
***Request timed out
```

```
140.114.63.253: timed out, nothing received
***Request timed out

Is 140.114.63.253 an open ntp server?
ANSWER: NO for 140.114.63.253
```

建議作法

防火牆作法

- 以防火牆來限制 NTP 查詢，預設攔阻 123/udp 的封包，再針對開放服務範圍的 IP 位址來開放服務，這種作法效益最好。
 - **NOTICE**用外部閘道型防火牆來保護內部所有資訊設備的方法甚為簡便，但考慮到閘道型防火牆總有需 bypass 或下線的時候，所以平時最好還是將每部資訊設備本身的安全防護做好來。

NTP 軟體

- 常見 NTP 軟體(<http://www.ntp.org/>) 的設定檔 ntp.conf 以下以例子簡單說明存取控制(access control) 如需詳細資料，請自行參閱：<https://www.eecis.udel.edu/~mills/ntp/html/accopt.html#restrict>
 - 以下這一行設定：預設拒絕所有的查詢

```
restrict default ignore
```

- 以下這一行設定：許可服務範圍 140.114.0.0/255.255.0.0 的查詢(query) 但拒絕其 modify 與 trap

```
restrict 140.114.0.0 mask 255.255.0.0 nomodify notrap
```

- 完成設定重新啟動 ntpd 服務後，若非服務範圍內對 NTP 伺服器 140.114.xx.xx 送出查詢，就會看到以下回應逾期的訊息。

```
# /sbin/ntpq -c rv 140.114.xx.xx
140.114.xx.xx: timed out, nothing received
***Request timed out
```

NTP client

- 若設定 140.114.63.1 與 140.114.64.1 為其 NTP 對時的伺服器(server) 除開放自身 127.0.0.1 查詢外，其餘關閉，則設定檔 ntp.conf 的參考設定如下：

```
restrict default ignore

server 140.114.63.1
restrict 140.114.63.1 mask 255.255.255.255 nomodify noquery notrap
```

```
server 140.114.64.1
restrict 140.114.64.1 mask 255.255.255.255 nomodify noquery notrap

restrict 127.0.0.1 nomodify notrap
```

- 完成設定重新啟動 ntpd 服務

```
# ntpq -c peers 127.0.0.1
      remote           refid      st t when poll reach  delay
offset jitter
=====
=====
*140.114.64.1      216.239.35.0      2 u  124  256  377   0.181
1.043  0.400
+140.114.63.1      140.114.63.132    3 u   52  256  377   0.141
0.881  0.220
```

網路設備

NOTICE 有些網路設備（如：無線網路開道器、IP分享器、或路由器）本身可能具有 open NTP server 問題，需適當調整設定或以防火牆來處理，由於網路設備的類型繁多，若您知悉某裝置該如何處理，歡迎提供設備廠牌、型號、軟(韌)體版本、及其設定方式的畫面，寄至 [mucheng @ cc.nthu.edu.tw](mailto:mucheng@cc.nthu.edu.tw) 以利製成以下網頁，嘉惠眾人，格式及文字可參考以下作法，謝謝!

Cisco 網路設備

- **NEW** Cisco WS-C2960-24PC-L 網路交換器：避免 open NTP server 問題之設定方式請參考下圖，本資料感謝網路系統組林平梓小姐提供(2019/05/29)。

廠牌：Cisco
 型號：Cisco WS-C2960-24PC-L Switch
 軟(韌)體版本：version 12.2(55)SE12
 open NTP server 解法如下：

```
C2960_PoE#conf t
Enter configuration commands, on per line. End with CNTL/Z.
C2960_PoE(config)#access-list 99 permit 140.114.63.1
C2960_PoE(config)#access-list 99 permit 140.114.64.1
C2960_PoE(config)#access-list 99 deny any
C2960_PoE(config)#ntp access-group serve-only 99
C2960_PoE(config)#exit
```

- **NEW** Cisco WS-C3750G 網路交換器 (版本:12.2(55)SE12) 避免 open NTP server 問題之設定方式請參考以下指令，本資料感謝網路系統組陳文城先生提供(2019/05/31)。

- 指令參考網址
https://www.cisco.com/en/US/products/ps6017/products_command_reference_chapter09186a008087ab11.html#wp1010372

```
SW#conf t
SW(config)#ip access-list standard 98
SW(config-std-nacl)# deny any

SW(config)#ip access-list standard 99
SW(config-std-nacl)# permit host 140.114.63.1
SW(config-std-nacl)# permit host 140.114.64.1
SW(config-std-nacl)# deny any
SW(config)#exit

SW(config)#ntp server 140.114.64.1
SW(config)#ntp server 140.114.63.1
SW(config)#ntp access-group peer 99
SW(config)#ntp access-group serve 98
SW(config)#ntp access-group query-only 98
SW(config)#end
SW#wr
```

```
SW#sh ntp associations
```

address	ref clock	st	when	poll	reach	delay
offset disp						
+~140.114.64.1	140.114.63.132	3	169	1024	377	0.8
-0.01 0.1						
*~140.114.63.1	140.114.63.132	3	21	1024	377	0.5
-0.34 0.3						

* master (syncd), # master (unsyncd), + selected, - candidate,
~ configured

HPE 網路設備

- **NEW** HPE 1920 8G PoE+ (180W) 網路交換器：避免 open NTP server 問題之設定方式請參考下圖，本資料感謝網路系統組林平梓小姐提供(2019/05/29)。

廠牌：HPE
型號：HPE 1920 8G PoE+ (180W) Switch (JG922A)
軟(韌)體版本：version 5.20.99, Release 1116
open NTP server 解法如下：

```
<140.114.X.X>_cmdline-mode on
All commands can be displayed and executed. Continue? [Y/N]Y
Please input password:***** (Jinhua1920unauthorized)
Warning: Now you enter an all-command mode for developer's testing, some
commands may affect operation by wrong use, please carefully use it with our
engineer's direction.
<140.114.X.X>system-view
System View: return to User View with Ctrl+Z.
[140.114.X.X]acl number 2001
[140.114.X.X-acl basic 2001]rule 0 permit source 140.114.63.1 0
[140.114.X.X-acl basic 2001]rule 1 permit source 140.114.64.1 0
[140.114.X.X-acl basic 2001]rule 5 deny source any
[140.114.X.X-acl basic 2001]ntp-service access synchronization 2001
[140.114.X.X-acl basic 2001]save (force)
[140.114.X.X-acl basic 2001]quit
[140.114.X.X]quit
```

參考資料

- [Open NTP Project](#)
- [NTP amplification attack](#)
- [NTP can be abused to amplify denial-of-service attack traffic](#)

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/ntp:open_ntp



Last update: **2020/02/11 14:16**