

การทำ Password Recovery on Cisco Switch

สำหรับคนที่ทำงานทางสาย Network นะคะ ที่ขอลืม password ในการเข้าไป config อุปกรณ์ จากบทความที่แล้วเกี่ยวกับการ Recovery Router cisco คราวนี้เป็นของ Switch บ้างนะคะ

Step การ Password Recovery ต่อไปนี้สามารถทำได้ทั้ง Cisco Catalyst Layer 2 รุ่น 2900XL/3500XL, 2940, 2950/2955, 2960 , 2970 Series และ Cisco Catalyst Layer 3 รุ่น 3550, 3560 และ 3750 Series

Step Password Recovery

1. เสียบสาย console และเปิด terminal เช่น Hyper Termians เพื่อ console เข้า switch โดยผ่าน port console โดย Set ค่า terminal ดังนี้

- Bits per second (baud): 9600
- Data bits: 8
- Parity : None
- Stop bits: 1
- Flow Control :Xon/Xoff

เพิ่มเติม ในการ console ในแต่ละอุปกรณ์ มีค่าแตกต่างกัน ต้องศึกษา Data sheet ของ Product นั้นๆ

2. ถอดปลั๊กของ Switch ออก
3. กดปุ่ม Reset (หน้าเครื่อง) ค้างไว้ ในระหว่างที่เสียบปลั๊ก Switch เข้าไปใหม่ ค้างไว้ประมาณ 10 วินาที แล้วปล่อย ก็จะสามารเข้า switch ได้แล้ว

Switch:

4. พิมพ์ flash_init

Switch : flash_init

Issue the **flash_init** command.

```
switch: flash_init
Initializing Flash...
flashfs[0]: 143 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2729472
flashfs[0]: Bytes available: 883200
flashfs[0]: flashfs fsck took 86 seconds
....done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:

!--- This output is from a 2900XL switch. Output from
!--- other switches will vary slightly.
```

5. พิมพ์ load_helper

Switch : load_helper

Switch :

6. พิมพ์ dir flash: จะเห็นไฟล์ config.text ซึ่งไฟล์ config ต่างๆ จะถูกเก็บไว้ที่ไฟล์นี้

Switch : dir flash:

Issue the **dir flash:** command.

Note: Make sure to type a colon ":" after the **dir flash**.

The switch file system is displayed:

```
switch: dir flash:
Directory of flash:/
 2  -rwx 1803357  <date>          c3500xl-c3h2s-mz.120-5.WC7.bin

!--- This is the current version of software.

 4  -rwx 1131    <date>          config.text

!--- This is the configuration file.

 5  -rwx 109     <date>          info
 6  -rwx 389    <date>          env vars
 7  drwx 640    <date>          html
18  -rwx 109    <date>          info.ver
403968 bytes available (3208704 bytes used)
switch:

!--- This output is from a 3500XL switch. Output from
!--- other switches will vary slightly.
```

7. ในการเปิด switch ขึ้นมาใช้งาน switch จะทำการโหลดข้อมูลจากไฟล์ config.text ขึ้นมาก่อน ดังนั้นถ้าเกิดมีการ set password ไว้แล้วไม่ทราบว่าเป็น password อะไร ก็ไม่สามารถเข้ามาใช้งานได้ ดังนั้น

7.1 กรณีที่ต้องการเก็บ config เดิมไว้ด้วย ให้ทำการเปลี่ยนชื่อไฟล์เป็นชื่ออื่นก่อน เพื่อที่จะได้โหลดไฟล์นั้นขึ้นมาใหม่ เพื่อทำการแก้ไข config นั้นๆ

Switch : rename flash:config.text flash:config.old

หมายเหตุ เมื่อทำข้อ 7.1 เสร็จแล้ว ทำข้อ 8 – 13 ต่อได้เลยค่ะ

7.2 กรณีที่ไม่ต้องการเก็บ config เดิมไว้ ก็สามารถลบได้เลยค่ะ

Switch : delete flash:config.text

หมายเหตุ เมื่อพิมพ์ delete flash:config.text เสร็จแล้ว ทำขั้นตอนที่ 8 (ทำการ boot Switch) ทีเดียวก็เป็นอันเสร็จสิ้นขั้นตอนการ hack switch แล้วค่ะ และสามารถเข้า switch ได้แล้วค่ะ โดยจะไม่หลงเหลือ config เก่าอยู่เลย

8. พิมพ์ boot

Switch : boot

Issue the **boot** command to boot the system.

```
switch: boot
Loading "flash:c3500xl-c3h2s-mz.120-5.WC7.bin"...#####
#####
#####
File "flash:c3500xl-c3h2s-mz.120-5.WC7.bin" uncompressed and installed, entry po
int: 0x3000
executing...

!--- Output suppressed.
!--- This output is from a 3500XL switch. Output from other switches
!--- will vary slightly.
```

9. หลังจาก boot เสร็จแล้ว ให้พิมพ์ no ซ้ำมาก่อน เนื่องจากเราจะทำการ config เอง

Enter "n" at the prompt to abort the initial configuration dialog.

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]: n

!--- Type "n" for no.

Press RETURN to get started.

!--- Press Return or Enter.

Switch>
```

10. พิมพ์ enable เพื่อเข้าสู่ enable mode (เป็น admin)

Switch>enable

Switch#

11. ทำการเปลี่ยนชื่อไฟล์ config.old กลับมาเป็น config.text เหมือนเดิม เพื่อใช้ในการดึงไฟล์ config เก่ากลับมาด้วย

Switch# rename flash:config.old flash:config.text

12. copy config ต่างๆ มาไว้ที่ Ram

switch#copy flash:config.text system:running-config

SW-1#

//จะสังเกตเห็น config เดิมมาแล้ว เนื่องจาก hostname เปลี่ยน

13. ทำการแก้ไข password ต่างๆ เป็นของเราตามต้องการ

SW-1#conf t

SW-1(config)#enable password new password ---> ใส่ password ที่เราต้องการ

SW-1(config)#enable secret new password ---> ใส่ password ที่เราต้องการ

SW-1(config)#line vty 0 4

SW-1(config)#password new password ---> ใส่ password ที่เราต้องการ

SW-1(config)#login

SW-1(config)#line con 0

SW-1(config)#password new password ---> ใส่ password ที่เราต้องการ

SW-1(config)#login

14. เมื่อแก้ไข password ต่างๆ แล้ว อย่าลืม save config ด้วยนะคะ

SW-1#copy running-config startup-config

เสร็จแล้วคราวนี้ก็สามารถเข้า switch โดยเป็น password ของเราได้แล้วค่ะ แล้วอย่าลืม password อีกนะคะ ^_^

เรียบเรียงโดย
พัชรินทร์ ดั่งสิงคำ
<http://www.jodoi.com>

แหล่งอ้างอิง :

http://www.cisco.com/en/US/products/hw/switches/ps628/products_password_recovery09186a0080094184.shtml