Password Recovery on Cisco Router

ศุทธินี ตันพาณิชย์ เรียบเรียง

สำหรับผู้ที่ใช้งานเร้าเตอร์ซิสโก้อยู่ เกิดพบปัญหาว่าลืมรหัสผ่านต่าง ๆ ในการแอกเซสเข้ามาใช้งานยังตัวเร้าเตอร์โดยตรง เช่น ลืมรหัสผ่านสำหรับพอร์ตคอนโซล (Password Line Console) หรือลืมรหัสผ่านของตัว enable secret หรือ enable password ซึ่งเป็นรหัสผ่านก่อนเข้าสู่การใช้งาน ในโหมด admin หรือที่นิยมเรียกกันทั่วไปคือโหมด enable ถ้าลืมแล้วจะทำอย่างไร วิธีการที่นิยมใช้ทำกัน ก็คือ การทำ “**Password recovery**” นั่นเอง และการทำงานต้องคอนโซลทำที่หน้าเครื่องเท่านั้น และก่อนจะทำการ Recovery จะต้องทำความรู้จักกับค่า Configuration register ก่อน

ค่า Configuration register หรือ ค่า bootstrap คือ ค่าที่ใช้กำหนดว่าจะให้เร้าเตอร์ซิสโก้ไปเรียกค่าคอนฟิคจากที่ใด (nvram หรือ ram) จะเป็นเลขบิต โดยค่า Default ของเร้าเตอร์ทุกตัว คือ 0x2102 สามารถใช้คอมมานด์ show version เพื่อดูค่านี้ได้ โดยข้อความจะแสดงอยู่บรรทัดล่างสุด ว่า Configuration register is 0x2102

0x ที่นำหน้า 2102 นั้นหมายความว่า ตัวเลขที่อยู่หลัง 0x เป็นเลขฐาน 16 ให้ดูบิตที่ 6 จะเป็นการกำหนดว่าจะให้เร้าเตอร์บูตจากอะไร ที่แนะนำคือเลข 0,4 โดย

เลข 0 เป็นการกำหนดให้เร้าเตอร์โหลดคอนฟิคจาก nvram หรือ startup

เลข 4 เป็นการข้ามการโหลดคอนฟิคที่ nvram

ซึ่งการ Recovery Password ต้องเข้ามากำหนดค่า จาก 0x2102 เป็น 0x2142 เพื่อข้ามขั้นตอนการโหลดคอนฟิคจาก nvram ให้ได้

สรุปขั้นตอนในการทำ Password Recovery มีอยู่ 9 ขั้นตอน

1. บูตเร้าเตอร์ใหม่ ด้วยการปิดเปิดสวิตช์ ในขณะที่เร้าเตอร์กำลังบูต ให้ขัดจังหวะการบูตด้วยการกดปุ่ม Ctrl+Break ที่คีย์บอร์ด
2. เปลี่ยนค่า Configuration register ให้เป็นค่า 0x2142
3. รีโหลดเร้าเตอร์ใหม่
4. เข้าสู่โหมด enable หรือ Privileged EXEC
5. ดึงค่าคอนฟิคเดิมที่อยู่ใน nvram หรือ startup มาไว้ที่ ram หรือ running
6. ทำการแก้ไขรหัสผ่านต่าง ๆ
7. เปลี่ยนค่า Configuration register ให้กลับมาเป็นค่า Default (0x2102)
8. เซฟค่าคอนฟิคที่ทำการแก้ไข
9. รีโหลดเร้าเตอร์ใหม่

ตัวอย่างขั้นตอนการทำงานพร้อมคำสั่งที่ใช้งาน ในการ Recovery Password

```
User Access Verification

Password:
Password:
```

กรณีลืมรหัสผ่านคอนโซล (Line Console) จะเห็นว่าเราไม่สามารถเข้ามาใช้งานเร้าเตอร์ได้

1. ทำการปิดเปิดเร้าเตอร์ และในขณะเร้าเตอร์กำลังบูต ให้**กด** Ctrl + Break เพื่อเข้าสู่โหมด Rommon
2. เปลี่ยนค่า Configuration register ให้เป็น 0x2142 โดยใช้คำสั่ง confreg 0x2142
3. รีโหลดเร้าเตอร์ใหม่ ด้วยคำสั่ง boot หรือ reset

```
Self decompressing the image :
##################
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 > boot
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory


Self decompressing the image :
###################################
```

หลังจากเร้าเตอร์บูตขึ้นมาใหม่ เร้าเตอร์ไม่ได้อ่านค่าคอนฟิคจาก nvram จาก Register number ที่เรากำหนดไว้ จะเห็นได้ว่า เราเข้าเร้าเตอร์ได้โดยไม่ติดพาสเวิร์ด จากคอมมานด์พรอมต์ที่ถามว่าต้องการ setup ค่าต่างๆ ให้ตอบ NO

4. เข้าสู่โหมด enable หรือ Privileged EXEC เพื่อเข้าไปแก้ไขค่าคอนฟิคต่าง ๆ ด้วยคำสั่ง enable

```
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>en
Router#
```

5. ดึงค่าคอนฟิคเดิมที่อยู่ใน nvram หรือ startup มาไว้ที่ ram หรือ running เพื่อทำการแก้ไข โดยใช้คำสั่งว่า copy startup-config running-config

ก่อนทำการดึงคอนฟิคกลับมาให้ทำการ

show startup-config เพื่อดูค่าคอนฟิคที่เราทำการเซฟไว้ใน nvram

```
Router#
Router#show startup-config
Using 889 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname jodoi
!
!
!
enable secret 5 $1$mERr$RchIbJiXmCXFtFBZll50l/
enable password 1234
!
!
```

จะเห็นค่าคอนฟิคเดิมที่ทำการเซฟไว้ล่าสุด จะเห็นว่ามีการตั้ง hostname , enable password, enable secret ไว้ และทำการ # show running-config เพื่อดูค่าคอนฟิคปัจจุบัน หรือค่า Default เทียบกันดู

```
Router#show running-config
Building configuration...

Current configuration : 751 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
```

และทำการดึงไฟล์คอนฟิคเดิมกลับมาโดยใช้คำสั่ง # copy startup-config running-config

```
Router#copy startup-config running-config
Destination filename [running-config]?

889 bytes copied in 0.416 secs (2137 bytes/sec)
jodoi#
%SYS-5-CONFIG_I: Configured from console by console

jodoi#
jodoi#
```

จะเห็นว่าเมื่อดึงค่าคอนฟิคเดิมกลับมาแล้ว Hostname จะเปลี่ยน เนื่องจากที่ startup มีการตั้งชื่อ hostname ไว้ ให้ทำการ show startup-config และ show running-config เทียบกันดูจะเห็นว่าค่าคอนฟิคทั้งสองส่วนเหมือนกันแล้ว

6. แก้ไขรหัสผ่านต่าง ดังนี้ ยกตัวอย่าง..

ต้องการเปลี่ยน Password Line Console

jodoi(config) # line console 0

jodoi(config-line) # password 1234

jodoi(config-line) # login

```
jodoi#
jodoi#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
jodoi(config)#line console 0
jodoi(config-line)#password 1234
jodoi(config-line)#login
jodoi(config-line)#exit
jodoi(config)#
```

เปลี่ยนรหัสผ่าน enable password ให้เป็น cisco

jodoi(config) # enable password cisco

กรณีนี้ ต้องการลบ enable secret

jodoi(config) # no enable secret

```
jodoi(config)#enable password 1111
jodoi(config)#no enable secret
jodoi(config)#
```

7. เปลี่ยนค่า Configuration register ให้กลับมาเป็นค่า Default (0x2102) โดยใช้คำสั่ง config-register ตามด้วยค่า register number ที่ต้องการเปลี่ยน คือ 0x2102

jodoi(config) # config-register 0x2102

```
jodoi#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
jodoi(config)#config-register 0x2102
jodoi(config)#exit
jodoi#
%SYS-5-CONFIG_I: Configured from console by console
```

8. เซฟคอนฟิคที่ทำการแก้ไขมาทั้งหมด ด้วยคำสั่ง copy running-config startup-config

jodoi # copy running-config startup-config

```
jodoi#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
jodoi#
```

9. รีโหลดเร้าเตอร์ใหม่ ในโหมดของเร้าเตอร์ปกติ ให้ใช้คำสั่ง reload

jodoi # reload

```
jodoi#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory


Self decompressing the image :
#####################################
```

หลังจากรีโหลดเร้าเตอร์ใหม่แล้ว จะต้องเข้าเร้าเตอร์ได้ด้วย รหัสผ่านที่เราแก้ไข

หวังว่าบทความนี้ จะก่อประโยชน์สำหรับผู้ที่ทำงานอยู่กับอุปกรณ์ Cisco ไม่มากก็น้อยนะคะ

สนับสนุนโดย http://www.jodoi.com

sutthinee@jodoi.com , sutthinee.t@hotmail.com