Password Recovery on Cisco Router

วรเดช อ่อนละมัย (อ.คิว) เรียบเรียง

สำหรับผู้ที่ใช้งานเร้าเตอร์ Cisco อยู่ก็จะทราบกันดีอยู่แล้วว่าเราจะต้องทำการตั้ง Password ไว้เพื่อเพิ่มความปลอดภัยให้กับเร้าเตอร์ ของเรา และบางครั้งผู้ดูแลระบบหนึ่งคนนั้นก็มีหน้าที่ในการดูแลเร้าเตอร์ มากกว่าหนึ่งตัวอยู่แล้ว และเร้าเตอร์ แต่ละตัวนั้นก็ต้องมีการตั้ง Password ที่แตกต่างกัน และด้วยเหตุนี้บางครั้งจึงพบปัญหาเรื่องการลืม Password ขึ้นหรือบางครั้งเราเข้าไปทำงานในองค์กรณ์ใหม่ แล้วผู้ดูและ คนเก่าไม่ได้บอก Password ไว้ให้เรา หรือบางครั้งเราอาจจะซื้อเร้าเตอร์ มือสองมาแล้วไม่ได้มีการ Clear Config เก่าที่อยู่ในเครื่องออกก็อาจจะติด Password ที่มีมาในเครื่อง ดังนั้นการที่เราจะทำการเข้าไป Config หรือแก้ไขค่าต่างๆ ใน Router ตัวนั้นๆ ก็มีทางเดียวก็คือเราต้องทำการ Recovery Password เข้าไปนะครับ ซึ่งในบทความนี้ผมก็จะมาสาธิตวิธีการทำ Password Recovery ให้ดูกันนะครับ และก่อนที่จะทำการ Recovery Password เราต้องทำความรู้จักกับค่า Configuration register กันก่อนนะครับ

ค่า Configuration register หรือค่า Boot strap คือ ค่าที่ใช้ในการกำหนดว่าจะให้เร้าเตอร์ ไปเรียกค่า Config จากที่ (Nvram หรือ Ram) และจะเป็นเลขบิต โดยค่า Default ของ Router ทุกตัว คือ 0x2102 สามารถใช้คอมมานด์ Show verison เพื่อดูค่านี้ได้ โดยข้อความจะแสดงอยู่บรรทัดล่างสุด ว่า Configuration register 0x2102

0x ที่นำหน้า 2102 นั้นหมายความว่า ตัวเลขที่อยู่หลัง 0x เป็นเลขฐาน 16 ให้ดูบิตที่ 6 จะเป็นการกำหนดว่าให้เร้าเตอร์ บูตจากอะไรที่แนะนคือเลข 0 , 4 โดย

เลข 0 เป็นการกำหนดให้ เร้าเตอร์ ไปโหลด Config จาก Nvram หรือ startup

เลข 4 เป็นการข้ามการโหลด Config ที่ Nvram

ซึ่งการ Recovery Password ต้องเข้ามากำหนดค่า Configuration register จาก 0x2102 ให้เป็น 0x2142 เพื่อข้ามขั้นตอนการโหลด Config จาก Nvram ให้ไปโหลดที่ Ram แทนนะครับ

ขั้นตอนการทำ Password Recovery มีอยู่ 9 ขั้นตอนด้วยกัน ดังนี้

1. บูตเร้าเตอร์ ใหม่ ด้วยการปิดเปิดสวิตช์ ในขณะที่ Router กำลัง boot ให้ขัดจังหวะการ Boot ด้วยการ กดปุ่ม Ctrl+Break ที่คัย์บอด
2. เปลี่ยนค่า Configuration register ให้เป็นค่า 0x2142
3. รีโหลดเร้าเตอร์ ใหม่
4. เข้าสู้โหมด enable หรือ Privileged EXEC
5. ดึงค่า Config เดิมที่อยู่ใน Nvram หรือ Stratup มาไว้ที่ Ram หรือ Running
6. ทำการแก้ไข Password ต่างๆ
7. เปลี่ยนค่า Configuration register ให้กลับมาเป็นค่า Default (0x2102)
8. Save Config ที่ทำการแก้ไขใหม่
9. รีโหลดเร้าเตอร์ ใหม่อีกครั้ง

ตัวอย่างขั้นตอนการทำงานพร้อมคำสั่งที่ใช้งาน ในการทำ Password Recovery

```
Press RETURN to get started!


################################################
####         This is Jodoi-Router            ####
####     Contact Mr.Woradet  Oonlamai        ####
####      E-mail Woradet@jodoi.com           ####
####         Tel. 092-5699592                ####
################################################

User Access Verification

Password:
```

จากภาพผมจำลองว่าผมลืม Password Console ถ้าในการทำงานจริงเราลืม Password Console เราจะไม่สามารถทำอะไรกับเร้าเตอร์ ได้เลยครับ เราต้องทำ Password Recovery อย่างเดียวนะครับโอเครครับ เรามาเริ่มกันเลยครับ ทำตามขั้นตอนดังนี้นะครับ

1.ทำการปิดเปิดเร้าเตอร์ และในขณะที่เร้าเตอร์ กำลัง Boot นั้นให้ กด Ctrl + Break เพื่อเข้าสู่โหมด Rommon

2.ให้ทำการเปลี่ยนค่า Configuration register เป็น confreg 0x2142

3.ทำการรีโหลดเร้าเตอร์ 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 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
####################################
```

หลังจากที่เร้าเตอร์บูต ขึ้นมาใหม่เร้าเตอร์ จะไม่อ่านค่า Config จาก Nvram เพราะว่าเราได้ทำการเปลี่ยนค่า Configuration register จาก 0x2102 เป็น 0x2142 แล้ว ซึ่งตอนนี้เร้าเตอร์ มันจะไปถึงค่า Config ที่ Ram แทนมันก็จะดึงค่า config ที่เป็น Default ขึ้นมาแทนเหมือนกับว่ายังไม่ได้มีการ Config ใดใดเลย เพราะฉะนั้นตอนนี้ Password ต่างๆมันก็จะไม่ถูกเรียกขึ้นมาทำการ Authentication ดูตามภาพด้านล่างเลยนะครับ

```
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)


         --- System Configuration Dialog ---

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


Press RETURN to get started!



Router>
Router>
```

4. ให้ทำการเข้าสู้โหมด Admin หรือ Privileged EXEC เพื่อเข้าไปแก้ไข Config ต่างๆ ด้วยการใช้คำสั่ง enable

```
Press RETURN to get started!



Router>
Router>en
Router#
```

5.ทำการดึง Config เดิมที่อยู่ที่ Nvram หรือ Startup มาไว้ที่ ram หรือ running เพื่อทำการแก้ไข โดยใช้คำสั่ง copy startup-config running-config

ก่อนที่เราจะทำการ ดึง Config กลับมาให้ใช้คำสั่ง

Show startup-config เพื่อดู Config เก่าที่เราทำการ Save ไว้ใน Nvram ก่อนนะครับ

```
Router#show startup-config
Using 1136 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Jodoi-Router
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password 1234
!
```

จะเห็นค่า Config เดิมที่ได้ Config ไว้นะครับ และจะเห็นว่ามีการ ตั้ง enable password, enable secret ไว้ด้วยนะครับ ซึ่งมันจะมี Config มากกว่านี้นะครับ แต่ผมขอโชว์ให้ดูแค่นี้นะครับ หลังจากที่เราทำการ Show startup-config

ดูแล้ว ให้ทำการ # Show running-config เพื่อดูค่า Config ปัจจุบันหรือค่า Default เพื่อเปรียบเทียบดูนะครับ

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

Current configuration : 691 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
```

จากภาพจะเห็นว่าค่า Config ต่างๆ จะเป็นค่า Default นะครับ หลังจากนั้นให้ทำการ ดึงไฟร์ Config เก่ามาที่ Running โดยใช้คำสั่ง #copy startup-config running-config

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

1136 bytes copied in 0.416 secs (2730 bytes/sec)
Jodoi-Router#
%SYS-5-CONFIG_I: Configured from console by console

Jodoi-Router#
Jodoi-Router#
```

จะเห็นว่าเมื่อทำการดึง Config เก่ากลับมาแล้ว Hostname จะเปลี่ยนไปเนื่องจาก Config เก่าได้มีการ Config hostname ไว้ หลังจากนั้นให้ทำการ Show startup-config และ Show running-config ดูอีกครั้งจะเห็นว่าค่า Config ทั้งสองจะเหมือนกันแล้ว

6.แก้ไข Password ต่างๆ จาก Config เดิมเราจะเห็นว่าเราไม่สามารถทำการแก้ไขค่า Config ใดใดได้เลยเพราะติด Password Line console ดังนั้น เราก็ต้องเข้าไปแก้ไข Password ตรงนี้ก่อนนะครับ หรือ จะลบมันออกก็ได้นะครับหากไม่ต้องการใช้งานมันแล้ว แต่ก็จะทำให้มีความปลอดภัยลดน้อยลงอีกขั้นนึงนะครับ แล้วแต่ความเหมาะสมในการทำงานนะครับ

```
Jodoi-Router(config)#line console 0
Jodoi-Router(config-line)#password 1234
Jodoi-Router(config-line)#login
Jodoi-Router(config-line)#
```

จากภาพผมได้ทำการแก้ไข Password Line console ผมก็ตั้งให้ยากๆหน่อยเอา 1234 ละกันอิอิ
เมื่อทำการเปลี่ยน Password Line console แล้วนะครับ ผมก็จะทำการเปลี่ยน Password enable และทำการลบ enable secret ทิ้งนะครับ ซึ่งในการทำงานจริง ควรจะตั้ง Password enable ไว้ด้วยนะครับ แต่เคสนี้เป็นเคสตัวอย่างนะครับ ซึ่งผมจะทำการลบ enable secret ทิ้งไปนะครับ

เปลี่ยน enable password ให้เป็น Cisco

Jodoi-Router(config)#enable password 1234

ลบ enable secret

Jodoi-Router(config)#no enable secret

```
Jodoi-Router(config)#
Jodoi-Router(config)#enable password 1234
Jodoi-Router(config)#no enable secret
Jodoi-Router(config)#
```

ให้ทำการแก้ไขแค่ Password ต่างๆนะครับ ส่วน Config อื่นๆไม่ต้องไปแก้ไขอะไรนะครับ เพราะเราต้องการแค่ recovery password นะครับ

7.หลังจากที่ทำการเปลี่ยน Password แล้วให้ทำการเปลี่ยนค่า Configuration register ให้กลับมาเป็นค่า Default (0x2102) โดยใช้คำสั่ง config-register 0x2102 ตามภาพด้านล่างนี้นะครับ

Jodoi-Router(config)#config-register 0x2102

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Jodoi-Router(config)#config-register 0x2102
Jodoi-Router(config)#
```

8.ทำการ Save Config ที่เราแก้ไขมาทั้งหมด โดยใช้คำสั่ง copy running-config startup-config

Jodoi-Router#copy running-config startup-config

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

9. ให้ทำการ รีโหลดเร้าเตอร์

Jodoi-Router#reload

```
Jodoi-Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
##############
```

หลังจากที่ รีโหลดเร้าเตอร์ใหม่แล้ว เราจะต้องเข้าเตอร์ได้ด้วย Password ใหม่ที่เราทำการแก้ไขไปแล้วนะครับสำหรับการทำ Password Recovery ก็มีขั้นตอนการทำเพียงเท่านี้นะครับ ก้พยายามฝึกบ่อยๆนะครับจะได้จำได้ รับรองว่าได้ใช้จริงๆแน่ๆครับ และผมหวังว่าบทความนี้จะเป็นประโยชน์ต่อผู้ที่ได้เข้ามาอ่านนะครับ และถ้าหากผิดพลาดประการใดผมต้องขออภัยมา ณ ที่นี้ด้วยนะครับ ขอบคุณครับ