# ใช้ AAA แต่ User/Pass เดิม



## ทำอย่างไร เปิด AAA แล้ว Telnet/Console ไม่ได้

ในหลักสูตร CCNA กล่าวถึงการตั้งค่าพาสเวิร์ดสำหรับล็อกอินในการเทอมินัล (หรือเรียกว่า Console) กับการเทอมินัลแบบเวอร์ช่วล (เช่น การ Telnet หรือ Secure Shell) ไว้ว่า

- ถ้าไม่ได้ตั้งค่าพาสเวิร์ดสำหรับล็อกอินไว้ การ เวอร์ช่วลเทอมินัลจะถูกปฏิเสธเนื่องจากถือว่าเป็นการสื่อสารแบบ In-Band (ผ่านเครือข่ายแลนหลัก หรือใช้แบนด์วิธร่วมกับการสื่อสารทั่วไปในเครือข่าย ซึ่งง่ายต่อการโจรกรรมข้อมูล ) ไม่เหมือนกับการเทอมินัลหรือต่อพอร์ทคอนโซลที่เป็นแบบ Out-of-Band (ใช้สายแยก หรือเครือข่ายแยกจากเครือข่ายหลักต่างหาก)
- การตั้งพาสเวิร์ดสำหรับล็อกอินเวลาคอนโซลหรือเวอร์ช่วลเทอมินัลเบื้องต้นนั้น จะใช้คำสั่ง password (พาสเวิร์ดที่ต้องการ) และปิดท้ายด้วยคำสั่ง login โดยไม่กำกับเงื่อนไขเพิ่มเติมทั้งในโหมดไลน์คอนโซล และไลน์เวอร์ช่วลเทอมินัล ดังตัวอย่าง

```
Router(config)# line con 0
Router(config-line)# password ranetconsolepassword   <-- ตั้งค่าพาสเวิร์ดสำหรับไลน์คอนโซล
Router(config-line)# login
Router(config-line)# line vty 0 4
Router(config-line)# password ranettelnetpassword    <-- ตั้งค่าพาสเวิร์ดสำหรับไลน์เวอร์ช่วลเทอมินัล
Router(config-line)# login
```

จะได้ว่า เมื่อ คอนโซลหรือเวอร์ช่วลเทอมินัล เราท์เตอร์จะถามเฉพาะพาสเวิร์ด ก่อนอนุญาตให้เข้าสู่โหมด User ดังนี้

```
User Access Verification
Password: (ตอนพิมพ์จะไม่แสดงตัวอักษร)
```

แต่ในทางปฏิบัติ เรานิยมตั้งค่าเป็นแบบ User/Pass (เรียกว่าแบบ Local คือเป็น user/pass ที่ประกาศไว้ลอยๆ บนโหมดโกลบัลคอนฟิกในเราท์เตอร์ ฟีเจอร์ไหนที่ต้องการนำไปใช้งานก็ให้อ้างถึงข้อมูล user/pass แบบ “local”) มากกว่า เนื่องจากสามารถตรวจสอบได้ว่าใครกำลังเทอมินัลเข้าอุปกรณ์ หรือแก้ไขคอนฟิกได้ (ไม่ว่าใช้คำสั่ง show user หรือจะดูจาก Syslog) โดยมีแนวทางการตั้งค่าดังนี้

```
Router(config)# username ranetuser password ranetpass
Router(config)# line con 0
Router(config-line)# login local
Router(config-line)# line vty 0 4
Router(config-line)# login local
```

*ตั้งค่า **user/pass** แบบ **Local** จะตั้งกี่ **Account** ก็ได้*

*ตั้งค่าให้ใช้ **user/pass** แบบ **Local** ที่ตั้งไว้*

จะได้ว่า เมื่อคอนโซลหรือเวอร์ช่วลเทอมินัล เราท์เตอร์จะถามทั้ง Username และพาสเวิร์ด ก่อนอนุญาตให้เข้าสู่โหมด User ดังนี้

```
User Access Verification
Username: ranetuser
Password: (ตอนพิมพ์จะไม่แสดงตัวอักษร)
```

จากการใช้ User/Pass แบบ Local ทำให้สามารถติดตามความเคลื่อนไหวของผู้ที่เทอมินัลเข้าอุปกรณ์ได้ เช่น การใช้คำสั่ง show user เพื่อให้แสดงผู้ที่ล็อกอินเข้ามาอยู่ในปัจจุบัน ดังนี้

```
Router# show user
    Line          User       Host(s)          Idle       Location
*  0 con 0       ranetadmin  idle             00:00:00
```

หรือจะตรวจสอบประวัติ หรือ Log ที่เกี่ยวข้องกับการกระทำของ User ที่สนใจได้ ด้วยการตั้งค่าให้บันทึก Log บนแรมของเราท์เตอร์ เพื่อสามารถอ่าน Log ที่เก็บไว้ได้ผ่านคำสั่ง show logging ดังนี้

```
Router(config)# logging buffered
Router(config)# exit
*Apr  4 15:31:19.739: %SYS-5-CONFIG_I: Configured from console by ranetadmin on console
Router# show logging
Syslog logging: enabled (1 messages dropped, 0 messages rate-limited,
            0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 12 messages logged, xml disabled, filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
    Buffer logging: level debugging, 1 messages logged, xml disabled, filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
No active filter modules.
    Trap logging: level informational, 16 message lines logged
Log Buffer (4096 bytes):
*Apr  4 15:31:19.739: %SYS-5-CONFIG_I: Configured from console by ranetadmin on console
```

*ตั้งค่าให้เก็บ **(Buffer) Log** ไว้บนเราท์เตอร์ส่วนหนึ่ง*

*แสดงชื่อ **Username** ด้วย!*

***Syslog** ที่แสดงขึ้น*

*ใช้คำสั่งให้แสดงการตั้งค่าเกี่ยวกับ **Log** และ **Log** ที่บัฟเฟอร์ไว้บนเราท์เตอร์*

*แสดงขนาดบัฟเฟอร์ และรายการ **Log** ที่บัฟเฟอร์ไว้*

การตั้งค่าพาสเวิร์ดเป็นค่าหรืออากิวเมนท์หลังคำว่า “password” ไม่ว่าจะเป็นพาสเวิร์ดที่ตั้งค่าในโหมดไลน์ต่างๆ หรือพาสเวิร์ดแบบ Local ก็ตาม จะไม่ถูกเข้ารหัสโดยดีฟอลท์ (ถือเป็นพาสเวิร์ดระดับ 0; Unencrypt/Cleartext) เราสามารถใส่คำสั่งที่บังคับให้เปลี่ยนรูปแบบพาสเวิร์ดที่ปรากฏบนคอนฟิกในที่ต่างๆ ให้เข้ารหัสในระดับ 7 (HIDDEN) ด้วยคำสั่ง service password-encryption ดังนี้

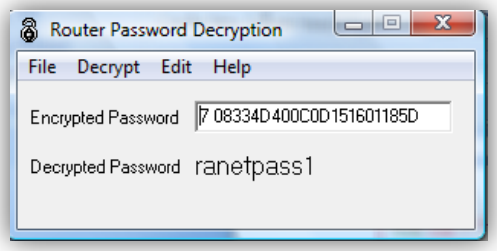
```
Router# show running-config
(ละข้อความ)
!
username ranetuser1 password 0 ranetpass1
username ranetuser2 password 0 ranetpass2
(ละข้อความ)
line con 0
 password ranetconsolepassword
 login
line vty 0 4
 password ranettelnetpassword
 login
(ละข้อความ)
Router# configure terminal
Router(config)# service password-encryption
Router(config)# end
Router# show running-config
!
username ranetuser1 password 7 08334D400C0D151601185D
username ranetuser2 password 7 8334D400C0D151601185E
(ละข้อความ)
line con 0
 password 7 08334D400C0D06181C1803082F3B253B20222D0103
 login
line vty 0 4
 password 7 08334D400C0D11121E0509103A2A373B243A3017
 loginc
```

*สังเกตพาสเวิร์ดเริ่มต้นที่ยังไม่ถูกเข้ารหัส บางครั้งจะมีเลข **0** กำกับเพื่อแสดงให้เห็นว่าเป็นแบบ **ClearText***

*คำสั่งที่ให้เข้ารหัสพาสเวิร์ดทุกตำแหน่ง (หลังคำว่า **“password”**) ให้เข้ารหัสแบบ **7***

*พาสเวิร์ดที่เข้ารหัสแบบ **7** แล้ว โดยมีเลข **“7”** นำหน้า*

แต่ถึงแม้จะเข้ารหัสแบบ 7 แล้ว ปัจจุบันก็มีทั้งโปรแกรมและเว็บไซต์ต่างๆ บริการถอดรหัสออกมาเป็น ClearText ได้โดยง่าย เช่น โปรแกรม Router Password Decryption ที่มากับชุดโปรแกรม Solarwind เป็นต้น *(หรือลองเสิร์ชในกูเกิ้ลด้วยคำว่า Decrypt Password Cisco ดู)*




*ภาพหน้าตาของโปรแกรม Router Password Encryption ที่ทำให้ถอดรหัสพาสเวิร์ดที่เข้ารหัสแบบ 7 ได้อย่างง่ายดาย*

ด้วยเหตุนี้ ซิสโก้จึงคิดอัลกอริทึมในการเข้ารหัสใหม่ เป็นการเข้ารหัสแบบ 5 (หรือทำ Hashing แบบ MD5) ซึ่งถ้าไม่ใช่อุปกรณ์ของซิสโก้ที่มีฐานข้อมูลใ นการทำ Hash เหมือนกันแล้วจะไม่สามารถถอดรหัสได้เลย และใช้คำอากิวเมนท์คำว่า "secret" แทน "password" กำกับในคำสั่ง (ทำนองเดียวกับการใช้ enable secret แทน enable password) ดังตัวอย่างต่อไปนี้

```
Router(config)# username ranetuser secret ranetpass
Router(config)# end
Router# show running-config
(ละข้อความ)
username ranetadmin secret 5 $1$mERr$BpCh1ChM40AQG87NihRA9.
```

***ใช้คำว่า Secret แทน Password***

***พาสเวิร์ดที่ถูก Hashing แบบ MD5 จะมีเลข 5 นำหน้า (เหมือนบนคำสั่ง enable secret)***

นอกจากการกำหนด User/Pass แบบ Local จะมีประโยชน์ด้านการยืนยันตน (Authentication) และการบันทึกความเคลื่อนไหวของแต่ละ User ผ่าน Log หรือที่เรียกว่า Accounting แล้ว ยังสามารถกำหนดสิทธิ์ (Privilege) ของผู้ใช้แต่ละบัญชี ที่เรียกว่า Authorization ได้ด้วย โดยกำกับอากิวเมนท์คำว่า privilege ข้างหลังชื่อ User ตามด้วยตัวเลขที่แสดงอำนาจเป็นสเกลตั้งแต่ 0 – 15 โดยที่

- 0 (ไม่ค่อยได้ใช้) บังคับให้ใช้ได้แค่ enable, disable, exit, help, logout
- 1 (Prompt เป็น Router>) แทนสิทธิ์ของผู้ใช้พื้นฐานในโหมด User (ต้องใช้คำสั่ง enable ถึงเข้าโหมดสิทธิ์สูงสุด)
- 15 (Prompt เป็น Router#) แทนสิทธิ์หรืออำนาจเต็ม คือ สามารถล็อกอินเข้ามายังโหมดอีนาเบิลได้เลยโดยไม่ต้องผ่านโหมด User ก่อน ดังตัวอย่างต่อไปนี้

```
Router(config)# username ranetuser3 privilege 15 secret ranetpass3
```

ซึ่งเมื่อล็อกอินด้วย user: ranetuser3 ก็จะเข้าสู่โหมดอีนาเบิลทันที ดังนี้

```
User Access Verification
Username: ranetuser3
Password: (ตอนพิมพ์จะไม่แสดงตัวอักษร)
Router#  <-- เข้าโหมดอีนาเบิลได้เลย เพราะตั้งค่า Privilege = 15
```

ถึงแม้จะมีการเข้ารหัสพาสเวิร์ดในข้อมูลการตั้งค่า หรือคอนฟิกแล้วก็ตาม ถ้ามีการทำสำรองข้อมูลการตั้งค่าเหล่านี้ไว้ด้านนอก คนอื่นก็สามารถนำพาสเวิร์ดที่เข้ารหัสนี้ไปใช้ประโยชน์ได้ เนื่องจากเมื่อนำคอนฟิกนี้มาใช้บนอุปกรณ์ซิสโก้อีก อุปกรณ์ดังกล่าวก็สามารถถอดรหัสพาสเวิร์ดเหล่านี้ได้เหมือนกัน *(เช่น เมื่อ copy บรรทัด "username ranetadmin secret 5 $1$mERr$BpCh1ChM40AQG87NihRA9." ไปใส่ในโหมดโกลบัลคอนฟิกของอุปกรณ์อีกตัวหนึ่ง ก็สามารถใช้ user: ranetadmin และ pass: ranetpass ได้เช่นกัน)*

ดังนั้น ด้วยเหตุผลด้านความปลอดภัยสูงสุด ซิสโก้จึงแนะนำให้เปิดใช้โปรโตคอล AAA *(ย่อมาจาก Authentication (การยืนยันตน) Authorization (การให้อำนาจในการใช้งาน) Accounting (การบันทึกประวัติการใช้งาน) ซึ่งมักใช้คู่กับ AAA Server ที่แยกออกมาต่างหาก ซึ่งอาจเป็นเซิร์ฟเวอร์ควบคุมการยืนยันตนโดยเฉพาะ อย่าง RADIUS หรือ TACACS+ Server หรือจะเป็นเซิร์ฟเวอร์ที่ให้บริการ AAA ครบวงจร อย่าง Cisco Secure ACS ก็ได้)* ทั้งนี้เนื่องจากเป็นการบังคับใช้ฐานข้อมูลที่เกี่ยวข้องกับบัญชีผู้ใช้เหล่านี้ด้านนอกอุปกรณ์

โดยเมื่อเปิดใช้โปรโตคอล AAA ด้วยคำสั่ง aaa new-model การล็อกอินเข้าอุปกรณ์ทุกเส้นทางทั้งการคอนโซลหรือเวอร์ช่วลเทอมินัลจะถูกล็อกทันที และจะดำเนินการตามการตั้งค่าของ AAA เป็นศูนย์กลางเท่านั้น

**จึงเป็นที่มาของปัญหาที่กล่าวถึงในครั้งนี้ (เข้าเรื่องเสียที!)**

หลังจากเปิดใช้ aaa แล้ว ฐานข้อมูลทั้งสามด้าน โดยเฉพาะการยืนยันตน จะไม่สามารถใช้ค่าที่ตั้งไว้เดิมไม่ว่าแบบใด (ที่ไม่ได้ตั้งค่าออกมาจาก aaa แล้ว) ได้ หรือแม้แต่เส้นทางที่ไม่เคยตั้งค่าพาสเวิร์ด (เช่น ถ้าก่อนหน้าไม่ได้ตั้งพาสเวิร์ดเข้าคอนโซล เมื่อเปิด AAA แล้ว ก็ถูกล็อกไปด้วย) ดังตัวอย่างนี้

```
Router(config)# aaa new-model          <-- ใช้คำสั่งเปิดการทำงาน AAA บนเราท์เตอร์

(เผลอทิ้งไว้จนเลย Timeout ทำให้โดนบังคับล็อกเอาต์ออกมาโดยยังไม่ได้ตั้งค่า aaa เกี่ยวกับการยืนยันตัวตน)

User Access Verification
Username: ranetuser3
Password: (ตอนพิมพ์จะไม่แสดงตัวอักษร)
% Authentication failed   <-- ถึงใช้ user/pass เดิม ก็ไม่สามารถ Telnet/Console ได้อีกแล้ว
```

ซึ่งบางครั้งการเปิดใช้ AAA อาจต้องการใช้แค่ส่วนของ Authorization หรือ Accounting แต่ไม่ได้ต้องการล็อกการยืนยันตนไปด้วย หรือบางครั้ง ตั้งค่า Accounting ให้ไปใช้ฐานข้อมูลของ RADIUS server ด้านนอก แต่เกิดเหตุที่ทำให้ไม่สามารถติดต่อกับเซิร์ฟเวอร์นั้นได้ชั่วคราว ทำให้ไม่สามารถ Telnel/Console เข้าอุปกรณ์ดังกล่าวได้เลย

จึงควรใช้คำสั่งตั้งค่า aaa authentication ของการล็อกอินให้ไปใช้ฐานข้อมูลแบบ Local ด้วยโดยดีฟอลท์ (เหมือนสำรองการทำงานไว้ในกรณีที่ ถ้าติดต่อกับฐานข้อมูลที่เคยตั้งค่าสำหรับการ Authentication เดิมไม่ได้ ให้เปิดโอกาสให้ยังใช้ User/Pass เดิมที่ตั้งค่าไว้แบบ Local เช่น เป็นรหัสผ่านที่รู้เฉพาะแอดมินตัวจริงเท่านั้น เป็นต้น)

ใช้คำสั่ง aaa authentication login default local เพื่อให้ใช้ User/Pass แบบ Local ได้ทั้งทาง Console หรือ Telnet ที่โดนล็อกได้ดังตัวอย่างนี้

```
Router(config)# aaa authentication login default local   <-- ใช้คำสั่งเปิดจาก AAA ให้ใช้ User/Pass แบบ Local กับการเทอมินัลเข้าทุกเส้นทางได้โดยดีฟอลท์ (คือ นำไปใช้ได้แม้ไม่ได้ตั้งค่าบนโหมดไลน์นั้นๆ ว่าให้ใช้ User/Pass ชุดนี้)
Router(config)# end
Router# exit

User Access Verification
Username: ranetuser3
Password: (ตอนพิมพ์จะไม่แสดงตัวอักษร)
Router>   <-- ใช้ user/pass เดิมเข้ามาได้แล้ว (แต่สังเกตว่าค่า Privilege ที่ตั้งไว้ยังไม่มีผลตามนั้น)
```