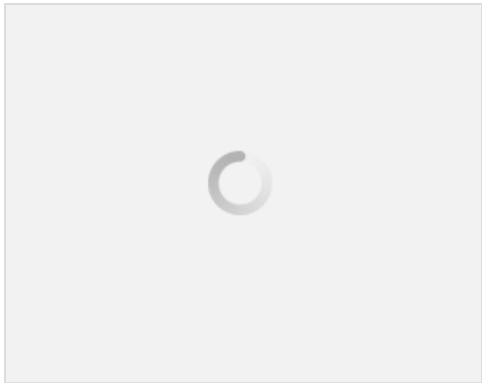
آموزش راه اندازی AAA در روتر سیسکو و امن کردن AAA در سیسکو (نسخه PDF)

با سلام ، سرویس AAA برگرفته از Authentication,Authorization,Accounting که از این سرویس جهت احراز هویت و تعیین سطوح دسترسی و نظارت به دسترسی و مدت دسترسی کاربر استفاده می شود.

- **Authentication**: وظیفه این بخش احراز هـویت کـاربر می باشـد . این بخش از سـرویس AAA ، مجـاز بودن و یـا غیر مجاز بودن دسترسی کاربر را تعیین می کند.
- **Authorization**: این بخش بعـد از احراز هـویت کـاربر(Authentication) اجـازه دسترسـی به منابع را به کاربر خواهـد داد و سـطوح دسترسی کاربر را تعیین خواهد کرد.
- **Accounting**: این بخش بعـد از احراز هویت کـاربر(Authentication) و هچنین بعـد از Authorization اعمال خواهد شد و دسترسـی کاربر را بررسی و همچنین مدت و مقدار دسترسی کاربر را تعیین می کند.

سرویس AAA جهت انجـام وظایف خود یعنی Authentication,Authorization,Accounting نیـاز به تصـدیق کاربر بر اساس Username خواهد داشت.شـما همچنین میتوانید AAA را به گـونه ای پیکربنـدی کنیـد که از Username هـای تعریف شـده به صورت Local بر روی اسـتفاده نمایید.



گام ۱ : پیکربندی hostname بر روی Router۱

```
Router#conf t

Router(config)#hostname Router1

Router1(config)#
```

گام ۲ : پیکربندی تنظیمات IP Address روی اینتر فیس های Router۱

```
Router1(config)#int fa0/0

Router1(config-if)#ip add 192.168.1.1 255.255.255.0

Router1(config-if)#no sh

Router1(config-if)#ex

Router1(config)#int s0/0/0
```

```
Router1(config-if)#ip add 10.1.1.1 255.255.255.252

Router1(config-if)#clock rate 64000

Router1(config-if)#no sh
```

گام ۳ : پیکربندی Default Route بر روی Router۱

در این مرحله با پیکربندی یک Default Route کلیه ترافیکی که مقصد آنها خارج از شبکه ۱۹۲.۱۶۸.۱.۰ می باشد به هر مقصدی از یک مسیر پیش فرض به سمت Router۲ به آدرس ۱۰.۱.۱.۲ ارسال خواهد شد.

```
Router1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

گام ۴ : پیکربندی hostname برروی Router۲

```
Router#conf t

Router(config)#hostname Router2

Router2(config)#
```

گام ۵ : پیکر بندی تنظیمات IP Address روی اینتر فیس های Router۲

```
Router2#conf t

Router2(config)#int s0/0/0

Router2(config-if)#ip add 10.1.1.2 255.255.255.252

Router2(config-if)#no sh

Router2(config-if)#ex

Router2(config)#int s0/0/1

Router2(config-if)#ip add 10.2.2.1 255.255.255.252

Router2(config-if)#clock rate 64000

Router2(config-if)#no sh
```

گام ۶ : پیکربندی Static Route برروی Router۲

```
Router2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1

Router2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.2
```

گام ۷ : پیکربندی hostname برروی Router۳

```
Router#conf t

Router(config)#hostname Router3

Router3(config)#
```

گام ۸ : پیکر بندی تنظیمات IP Address روی اینتر فیس های Router۳

```
Router3#conf t

Router3(config)#int fa0/0

Router3(config-if)#ip add 192.168.3.1 255.255.255.0

Router3(config-if)#no sh

Router3(config-if)#ex

Router3(config)#int s0/0/0

Router3(config-if)#ip add 10.2.2.2 255.255.255.252

Router3(config-if)#no sh
```

گام ۹ : پیکربندی Default Route بر روی Router۳

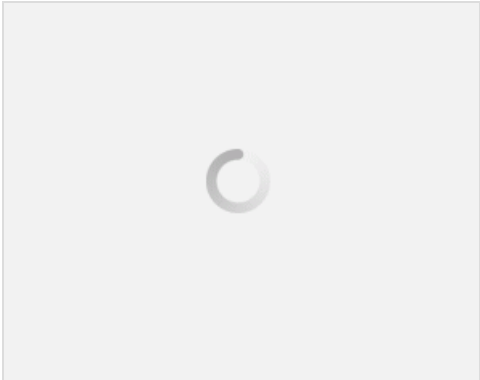
در این مرحله با پیکربندی یک Default Route کلیه ترافیکی که مقصد آنها خارج از شبکه ۱۹۲.۱۶۸.۳.۰ می باشد به هر مقصدی از یک مسیر پیش فرض به سمت Router۲ به آدرس ۱۰.۲.۲.۱ ارسال خواهد شد.

```
Router3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

گام ۱۰: بررسی اتصال بین Server۱ و PC۱

```
SERVER>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
```

```
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
```



گام ۱۱ : پیکربندی حداقل طول پسورد برای تمامی پسوردهای Router

```
Router#conf t

Router(config)#security passwords min-length 4
```

در دستور بالا حداقل پسورد برای تمامی پسوردهای روتر مقدار ۴کاراکتر در نظر گرفته شده است(در این حالت نمی توان روی روتر پسورد کمتر از طول ۴ کاراکتر تنظیم نمود)

گام ۱۲ : اعمال رمزگذاری(Encryption) برروی پسوردهای Clear text

کلمات رمز برای ورود به مدهای AUX,Console,Telnet که برروی روتر تنظیم می شود به صورت Clear text (رمز قابل مشاهده) می باشد.به عبارتی این رمزها در فایل پیکربندی روتر به صورت متن ساده قابل مشاهده می باشند که از نظر امنیتی باید به صورت رمزگذاری(Encryption) در فایل پیکربندی روتر نگهداری شود که برای این منظور از دستور زیر برروی Routerهای سیسکو استفاده میکنیم.

```
Router#conf t

Router(config)#service password-encryption
```

گام ۱۳ : پیکربندی هشدارهای امنیتی در زمان دسترسی به روتر(Login Warning banner)

قصد داریم یک Warning Massage برای کاربران غیر مجاز (unauthorized) که قصد دسترسی به مد پیکربندی روتر را دارند تعیین کنیم که این پیام قبل از دسترسی کاربر به Login Prompt یا همان User Mode نمایش داده می شود.برای این منظور از MOTD banner استفاده می کنیم.

```
Router#conf t

$Router(config)#banner motd $Unauthorized access
```

گام ۱۴ : تعریف User Account و Password روی Router

```
Router#conf t

Router(config)#username itpro password cisco
```

گام ۱۵ : تعریف User Account و Password روی Router به صورت Secret Password

```
Router#conf t

Router(config)#username itpro secret ccna123
```

گام ۱۶ : استفاده از User Accountهای Local روتر برای دسترسی به صورت Console به Router

```
Router#conf t

Router(config)#line console 0

Router(config-line)#login local

Router(config-line)#exit
```

گام ۱۷ : استفاده از User Accountهای Local روتر برای دسترسی به صورت Telnetبه Router

```
Router1#conf t

Router(config)#line vty 0 4

Router(config-line)#login local

Router(config-line)#exit
```

گام ۱۸ : پیکربندی Local Authentication با استفاده از سرویس AAA برروی Router۳

در این حالت میخواهیم سـرویس AAA را بر روی روتر فعـال و پیکربنـدی نمـاییم به طوری که سـرویس AAA برای احراز هـویت و تعیین سطوح دسترسی از Username های Local که بر روی روتر تعریف شده استفاده نمایید.اولین مرحله فعال نمودن سرویس AAA با استفاده از دستور زسر می باشد.

```
Router3#conf t

Router3(config)#aaa new

Router3(config)#aaa new-model
```

دومین مرحله استفاده از سرویس AAA برای احراز هویت در زمـان Login با استفاده از Usernameهای Local که بر روی روتر تعریف شـده

اند می باشد.برای این منظور از دستور زیر استفاده میکنیم.

```
Router3(config)#aaa authentication login default local
```

سومین مرحله شما باید به صورت Local برروی روتر Username تعریف کنید که سرویس AAA برای احراز هویت از آن استفاده می کند.

```
Router3(config)#username itpro privilege 15 secret Cisco123
```

گام ۱۹ : استفاده از سرویس AAA برای دسترسی به صورت Telnet

```
Router3#conf t

Router3(config)#line vty 0 4

Router3(config-line)#login authentication default

Router3(config-line)#exit
```

گام ۲۰ : استفاده از سرویس AAA برای دسترسی به صورت Console

```
Router3#conf t

Router3(config)#line Console 0

Router3(config-line)#login authentication default

Router3(config-line)#exit
```

گام ۲۱ : عیب یابی AAA با استفاده از توانمندی Debug

```
Router3#debug aaa authentication
```

مطلب اصلی