سیسکو به پارسی

مدیریت روتر سیسکو – آموزش مقدماتی

نوشته:
شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian
انجمن سیسکو به پارسی http://forum.shafagh.com

Console به روتر

ابتدایی ترین راه مدیریت و تنظیم روتر سیسکو استفاده از کنسول است. پهنای باند کنسول سیسکو بصورت قراردادی ۹۶۰۰ بیت در ثانیه است. این Baudrate از طریق تنظیمات قابل تغییر است.

جهت اتصال به روتر از طریق پورت کنسول به راهنمای نحوه اتصال به روتر سیسکو مراجعه کنید.

از دیگر راههای اتصال به روتر AUX، TELNET، SNMP و HTTP است. از طریق این متدها میتوان تنظیمات روتر را بررسی و تغییر داد. پورت AUX در کنار Console قرار دارد (گاهی زیر آن). این پورت، درگاه Auxiliary (امداد) نام دارد و در زمانیکه که از راه دور نیاز به دسترسی به سیسکو داشتیم با اتصال خط تلفن به یک مودم خارجی (External MODEM) و نهایتا اتصال مودم به این پورت متصل شده و تنظیمات را از راه دور بررسی و انجام میدهیم.

روش های اتصال و مدیریت روتر بوسیله Console و AUX را OOB یا Out Of Band Management مینامند. در این مدل ارتباط فیزیکی برای مدیریت دستگاه از کانال Data مجزا است و از پورت جداگانه برای مدیریت استفاده میشود که در همه زمان قابل دسترس است حتی اگر روتر در حال Restart باشد میتوان پروسه را روی کنسول دید. اما برای دسترسی به روش های مدیریتی In-band باید روتر برای این کار تنظیم شده باشد. بطور مثال برای Telnet کردن به روتر باید یک پورت دستگاه به شبکه متصل باشد، باید IP داشته و IP آن قابل دسترس و علاوه بر آن Password روی آن تنظیم شده باشد.

Cisco in Persian

Telnet به روتر

برای اینکه از راه دور (اینترنت یا شبکه IP) بتوانیم به روتر وصل شویم از دو پروتکل Telnet و SSH میتوان استفاده کرد. Telnet از TCP Port 23 و SSH از TCP Port 22 استفاده میکند. فرق Telnet با SSH در این است که Telnet بصورت Clear Text بسته ها را ردوبدل میکند و اگر هکری روی خط شنود داشته باشد میتواند بسته های مبادله شده را بخواند و حتی تغییر دهد در حالیکه SSH از رمزنگاری (Encryption) استفاده میکند.

برای Telnet کردن به روتر، روتر باید IP و Password داشته باشد برای تعریف پسورد چنین میکنیم:

۱. ابتدا یک IP به روتر اختصاص میدهیم و در صورتیکه به شبکه های دیگر وصل است از IP Route استفاده میکنیم تا دسترسی محیا گردد. (برای اختصاص IP به قسمت: چگونه به روتر IP اختصاص دهیم رجوع کنید.)
۲. برای روتر Enable Secret تعریف کنید.
۳. در صورتیکه برای روتر Telnet Password تعریف نکرده باشید هنگام Telnet با پیغام زیر مواجه میشوید: (برای Telnet کردن به روتر از دستور Telnet در Windows یا Linux استفاده میکنیم.)

```
Password required, but none set
```

۴. برای تنظیم Password مخصوص Telnet:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco123
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
```

حال با Telnet به روتر با صفحه Login مواجه میشویم:

```
User Access Verification

Password:
Router>
```

قبلا عنوان کردیم که Console و Auxiliary را روش های Out-of-Band Management و Telnet و SSH را از آنجا که همراه با دیتا به روتر راه پیدا میکنند، In-Band Management مینامیم .

از همین روش برای تعریف Password برای Console و AUX میتوان استفاده کرد:

```
Router(config)#line con 0
Router(config-line)#password ciscoconsolepass
Router(config-line)#login
Router(config-line)#exit
Router(config)#line aux 0
Router(config-line)#password ciscoauxpass
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
```

لازم به ذکر است که این پسورد در هنگام ورود به User-mode پرسیده میشود و جهت ورود به Privilege-mode به رمزی دیگر که قبلا به آن اشاره شد، بنام Enable Secret نیاز داریم. برای دیدن کل تنظیمات:

```
Router# show run
Building configuration...

Current configuration : 1236 bytes
!
version 12.4
no service password-encryption
!
enable secret 5 $1$WAXk$C4WDTvAcx34KZ2O2zvnne.
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
```

Cisco in Persian

```
!
line con 0
 password ciscoconsolepass
 login
line aux 0
 password ciscoauxpass
 login
line vty 0 4
 password cisco123
 login
!
end
```

همانطور که در تنظیمات میبینیم روتر پسورد ها را بصورت Clear-text (خوانا) نشان میدهد و بدین صورت دیدن پسورد برای کسی که دسترسی به تنظیمات دارد بسیار ساده است. البته Secret به صورت رمزنگاری شده ثبت میشود که از خصوصیات MD5 در Enable Secret است. (این الگوریتم یک طرفه و غیر قابل برگشت است.) برای این که رمزهای دیگر نیز در Configuration بصورت رمزنگاری شده نشان داده شوند، از دستور زیر استفاده میکنیم:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)#exit
Router#show run
!
service password-encryption
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
!
enable secret 5 $1$WAXk$C4WDTvAcl34KZ2O2zvnne.
!
line con 0
 password 7 02050D4808090C2E425D0615000713181F
 login
line aux 0
 password 7 0822455D0A1604020A1B0D1739
 login
line vty 0 4
 password 7 030752180500701E1D
 login
!
end
```

Cisco in Persian

ایجاد کاربر درون روتر

تعریف یک کاربر و رمز آن بسادگی یک خط دستور است:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#username test password test
```

میتوان چندین کاربر با سطوح مختلف دسترسی تعریف کرد. در مثال بالا سطح دسترسی کاربر در حد User-mode است و در صورتیکه Secret را بداند میتواند به Privilege-mode دست یابد در مثال زیر کاربری با سطح دسترسی عالی تعریف میکنیم:

```
Router(config)#username admin privilege 15 password admin123
```

سپس، برای این که به روتر بگوییم در زمان وصل شدن کاربر از طریق Telnet بجای Telnet password از لیست کاربران (که در مثال بالا تنظیم کردیم) استفاده کند، این گونه عمل میکنیم:

```
Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#exit
```

Cisco in Persian

سپس امتحان میکنیم:

```
Command Prompt>telnet 192.168.100.1

User Access Verification

Username: test
Password: test
Router>
```

و این بار با کاربر admin امتحان میکنیم:

```
Command Prompt>telnet 192.168.100.1

User Access Verification

Username: admin
Password: admin123
Router#
```

تفاوت در این است که کاربر admin در مد Enable وارد شد و نیاز به Secret ندارد چون در زمان تعریف سطح دسترسی Privilege 15 را به او دادیم. اگر در زمان تمرین روتر شما بدین صورت عمل نکرد، IOS قدیمی دارید و باید توسط AAA Authorization این عملکرد تعریف گردد که بعدا به آن میپردازیم.

چند نکته در مورد Telnet

پیام هایی که روتر به کاربر میدهد به دو دسته Syslog و Debug تقسیم میشوند. Syslog خود دارای مراتب متفاوتی است. Debug نوعی Syslog است که در زمان عیب یابی میتوانیم آنرا فعال کنیم.

وقتی به روتر از طریق کنسول وصل میشویم پیام های Syslog و Debug روی صفحه در زمان خود ظاهر میشوند. اما زمانی که به روتر Telnet کردیم برای دیدن این پیام ها و پدیدار شدن آنها روی صفحه باید دستور زیر را وارد کنیم:

```
Router# terminal monitor
```

این دستور ترمینال (Telnet) را به حالت مونیتورینگ در آورده و پیام های سیستم را به ما نشان میدهد. اگر ظهور پیام ها در زمان وارد کردن دستورات برایمان آزار دهنده است از دستور زیر استفاده میکنیم تا اختلالی در زمان تایپ کردن برای ما ایجاد نکند:

```
Router(config)# line vty 0 4
Router(config-line)# logging synchronous
```

دستور فوق پیام های سیسکو را تنها در زمان مناسب نشان میدهد. از دیگر دستورات مهم استفاده از Exec-timeout است. روتر به صورت default یک ارتباط Telnet را پس از ۱۰ دقیقه (اگر غیر فعال باشد) قطع میکند با دستور فوق میتوان زمان بیشتری به کاربر داد تا مجبور نباشد دوباره به روتر Telnet و Login کند.

```
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 0 0
```

Cisco in Persian

تعریف DNS برای روتر

وقتی یک IP را داخل روتر بدون هیچ دستوری تایپ کنیم روتر سعی میکند به آن IP، Telnet کند:

```
Router#
Router#10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
```

اگر یک FQDN یا نام (بجای IP مثلا cisco.example.com) را وارد کنیم روتر ابتدا تلاش میکند تا آن نام را به IP تبدیل کرده (از DNS سوال میکند) و سپس به آن Telnet کند. جهت تنظیم DNS برای روتر از دستور زیر استفاده میکنیم:

```
Router(config)#ip name-server 192.168.100.201 192.168.100.202
```

در مثال بالا دو DNS سرور برای روتر تنظیم کردیم تا هرگاه توسط Ping، Traceroute و یا ابزاری های دیگر، FQDN ی را صدا زدیم روتر برای ترجمه اسم به IP از این DNS استفاده کند.

خیلی از اوقات (حتما برای شما هم پیش آمده) که در زمان کار با روتر دستورات را اشتباه تایپ کرده و روتر بعنوان یک نام FQDN سعی میکند به آن اشتباه تایپی Telnet کند و بدین صورت وقت زیادی را تلف میکند برای اینکه از شر این موضوع خلاص شویم دو راه داریم:

Cisco in Persian

۱. Telnet کردن از داخل روتر را ببندیم بدین معنی که وقتی به روتر Telnet کردیم نتوانیم از روتر به IP ی دیگری Telnet کنیم و اجازه Telnet از روتر به بیرون را از آن بگیریم:

```
Router(config)#line vty 0 4
Router(config-line)#transport output none
```

۲. یا اینکه، استفاده از DNS را برای روتر ممنوع کنیم. بدین صورت روتر تلاش نمیکند اسمها را به IP تبدیل کند:

```
Router(config)#no ip domain-lookup
```