**روش های اتصال به Device:**

اولین روش اتصال از طریق پورت serial RS-232:

- معمولا در کانفیگ اولیه از این روش استفاده میشه چون محدودیت حضور فیزیکی در کنار Device هست. برد اتصال سریال هم نمیتونه زیاد باشه. معمولا بیشتر از ۱۵ متر نیست.
- وقتی Device از دسترس خارج میشود از این روش استفاده میشود.
- وقتی نیاز به password recovery باشد از طریق سریال متصل میشویم.
- کابل console معمولا همراه device هست ولی اگر نداشتیم میشه درست کرد. یک کابل شبکه برمیداریم و بصورت rollover وصل میکنیم. ۱ به ۸، ۲ به ۷، ۳ به ۶، ۴ به ۵، ۵ به ۴، ۶ به ۳، ۷ به ۲ و ۸ به ۱ وصل میشه و یکی از پین های DB9 خالی میمونه.

دومین روش اتصال از طریق VTY:

- باید حتما دستگاه IP ست شده باشد
- باید حتما Telnet سرور و SSH سرور روی دستگاه کانفیگ شده باشد
- با یک Terminal میتوان وصل شد
- Telnet نا امن و SSH امن است
- همه دستگاه ها SSH را ساپورت نمیکنن
- حداکثر ۱۶ نفر میتونن به این دستگاه متصل بشن

سومین روش برای Router ها قابلیت Auxiliary:

- پورت AUX روتر را به مودم DSL متصل میکنیم و PC خودمان را نیز از طریق یک مودم DSبه تلفن وصل میکنیم. با شماره گیری خط تلفن مقصد به روش هایی میتوان به روتر متصل شد.

چهارمین روش از طریق نرم افزار NMS:

**محیط های پیکربندی:**

محیط Usermode:

- با علامت > نشان داده میشود.
- در این محیط نمی توان Configuration انجام داد.
- با ساخت username برای افراد مختلف میتوان در این محیط اقدام به ورود با user های مختلف کرد.
- دروازه برای ورود به Device
- امکان خراب کاری در این محیط وجود ندارد
- Command های مهم مانند: enable – ping – show – telnet - terminal

محیط Enablemode:

- با دستور enable وارد این محیط میشویم
- با علامت # نشان داده میشود
- مانیتورینگ (با دستورات show)، رفع اشکال (با دستور Ping و ... ) و مدیریت تا حدودی (با دستورات Copt و Erase و ...)
- Backup گرفتن و Restore و ... در این بخش است
- Command های مهم مانند: cd – copy – clock – debug – enable – erase – traceroute – config - show

محیط Global Config Mode:

- با دستور config terminal وارد می شویم
- علامت این محیط (config)# است
- خود تنظیمات در این محیط نیست بلکه در context Mode انجام میشود
- بسته به command خاص و نیاز خاص وارد context های خاص میشویم

محیط context mode:

- بسته به command فرق دارد

**شروع راه اندازی اولیه سوئیچ:**

۱- ابتدا از طریق کابل Console و از طریق یک Terminal یا Putty به دستگاه متصل می شویم.

۲- تنظیم زمان دستگاه:

```
Switch> enable
Switch# clock set 17:15:00 25 June 2017
```

نیازی به تنظیم timezone نیست

۳- تنظیم اسم دستگاه:

```
Switch# config terminal
Switch(config)# hostname SW-1
```

۴- ست کردن پسورد برای دستگاه:

پسورد برای اتصال سریال

```
Switch(config)#line console 0
Switch(config-line)#password <…>
Switch(config-line)#login
Switch(config-line)#exit
```

پسورد برای وexitرود به محیط Enable

```
Switch(config)#enable password/secret <…>
```

telnet-ssh برای دسترسی از طریق usernameساختن چند

```
Switch(config)#username USER1 privilege 15 secret/password <…>
```

فعال کردن Telnet یا SSH

```
Switch(config)#line vty 0 15
Switch(config-line)#transport input <telnet/ssh/all/none>
Switch(config-line)#exit
```

دسترسی از طریق telnet اگر فقط یک پسورد بخواهیم (در این حالت حتما باید پسورد enable هم داشته باشیم)

```
Switch(config)#line vty 0 15
```

```
Switch(config-line)#password <...>
Switch(config-line)#login
```

اگر بخواهیم از username های ساخته شده استفاده کند

```
Switch(config)#line vty 0 15
 Switch(config-line)#login local
```

فعال کردن SSH:

برای فعال کردن ssh حتما باید Hostname و DomainName سوئیچ عوض شده باشد. بصورت دیفالت نام سوئیچswitch است و Domainname نیز ست نشده است.

```
Switch(config)#hostname SW1
SW1(config)#ip domain-name test.local
```

حال باید برای اتصال از طریق ssh اقدام به ساخت key کنیم:

کمترین سایز key ها ۳۶۰ بیت و بیشترین 2048بیت است. ۱۰۲۴ بیت مقدار مناسبی است.

```
SW1(config)#crypto key generate rsa
How many bits in the modules [512]: 1024
```

با دستور زیر میتوان key های ساخته شده را مشاهده کرد

```
SW1# show crypto key mypubkey rsa
```

**چک کردن تنظیمات کلی Switch:**

- در محیط enable mode با دستور show running-config میتوان تنظیمات انجام شده در محیط global config mode را مشاهده کرد. در این تنظیمات نوع دسته بندی و تنظیمات پورت ها را میتوان دید. همچنین مسیر های ارتباطی console و vty را نیز میتوان دید. اگر برای console و vty از password استفاده کرده باشیم در این بخش بصورت plain text نشان میدهد.
- با دستور show ip interface brief میتوان کلیت وضعیت interface های فیزیکی و مجازی را دید. برای پورت های فیزیکی IP ها بصورت unassigned هستند و برای vlan ها اگر IPاست شده باشد نشان میدهد. همینطور status پورت ها نیز نشان داده میشود.
- با دستور show interface status میتوان اطلاعات دیگری مانند وضعیت دقیق تر پورت و vlan هر اینترفیس فیزیکی را مشاهده کرد. این دستور اطلاعات پورت های فیزیکی را نشان میدهد.

- با دستور show vlan brief میتوان اطلاعات کلی vlan ها . همچنین اینترفیس هایی که در هر vlan هستند نشان داده میشود.

**تنظیم IP بر روی switch:**

درسوئیچ های لایه ۲ مانند 2960 و 2950 نمیتوان بر روی اینترفیس ها IP تنظیم کرد. به خاطر ماهیت لایه ۳ بودن IP باید برروی یک پروتوکل لایه ۳ تنظیم شود.VLAN ماهیت لایه ۳ دارد و برای اینکار IP برروی vlan ست میشود.

ساخت vlan و تنظیمات آن:

Switch#conf terminal

Switch(config)#interface vlan 100

Switch(config-if)#description “xxxxxxx”

Switch(config-if)#no shutdown (اگر قبلا دستی خاموش شده باشد)

Switch(config-if)# ip address 192.168.10.xxx 255.255.255.xxx

نکته: وقتی یک vlan میسازیم، تا وقتی به پورت فیزیکی خاصی Assign نشده باشد با دستور show vln brief نشان داده نمیشود ولی در show ip int briefe میتوان این vlanرا دید. وقتی این vlan به یک پورت فیزیکی خاص متصل شد آن وقت در vlan brief نیز دیده میشود.

تنظیمات interface های فیزیکی:

Switch(config)#interface fastether/gigabit 1/0/1 (در ۲۹۶۰)

Switch(config)#interface fastether/gigabit 0/1 (در ۲۹۵۰ و ۳۵۶۰)

Switch(config-if)#no shutdown

اگر بخواهیم Access باشد و به PC وصل شود

Switch(config-if)#switchport mode access/trunk/dynamic

Switch(config-if)#switchport access vlan <xxx>

Switch(config-if)#description “xxxxxxxxx”

Switch(config-if)#duplex auto (default)

اگر بخواهیم trunk باشد و به switch دیگری یا router یا سروری وصل باشد

Switch(config-if)#switchport mode trunk

اضافه کردن یک vlan به vlan های مجاز به دسترسی از این پورت

Switch(config-if)#switchport trunk allowed vlan add <…>

همه vlan ها مجاز هستند بجز اینها

Switch(config-if)#switchport trunk allowed vlan except

اجازه به همه vlan ها برای دسترسی به این پورت

Switch(config-if)#switchport trunk allowed vlan all

**نکته**: در سوئیچ های لایه ۳ به بالا قبل از اینکه mode پورت را trunk کنید باید نوع encapsulation trunk را مشخص کنید:

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#switchport mode trunk

**امن کردن پورت های سوئیچ Port Security**:

- وقتی بخواهیم MAC های مجاز روی پورت هارا مشخص کنیم
- وقتی بخواهیم تعداد حداکثر MAC مجاز روی یک پورت را معلوم کنیم
- میتوانیم بگوییم در صورت بروز تخلف سوئیچ چه کاری انجام دهد

- این یک قابلیت برای پورت های Access است

دستورات:

Switch(config)#interface gigabit 1/0/1

Switch(config-if)#switchport mode access

تا این دستور را نزنیم port security فعال نمیشود

Switch(config-if)#switchport port-security maximum <...>

اگر اینجا عدد ۱ گذاشته شود فقط همزمان یک PC یا NIC می تواند به آن متصل شود. معمولا برای امنیت بیشتر این عدد را روی ۱ میگذارند تا نتوان به این پورت switch دیگری وصل کرد

Switch(config-if)#switchport port-security MAC-address <xxxx.xxxx.xxxx>

فرمت MAC باید بصورت بالا باشد. مانند b5c0.50d6.25j8

Switch(config-if)#switchport port-security violation <shutdown/restrict/protect>

**حالت shutdown**: پورت کلا disable میشود و وضعیت پورت به حالت err-disabled می رود.

**حالت restrict**: پورت فعال می ماند ولی packet های مربوط به MAC غیر مجاز drop میشوند. یعنی اگر روی پورتی MAC خاصی ست شده باشد و یک کامپیوتر با MAC غیر مجاز وصل شود، packet هایی که از این سیستم غیرمجاز آمده باشد drop میشود ولی اگر سیستم اولیه دوباهر وصل شود پورت کار میکند. همچنین سوئیچ تعداد بسته های غیرمجاز را برای Syslog server یا سرور monitoring بر روی پروتکل SNMP می فرستد.

**حالتprotect** : مانند حالت restrict است ولی هیچ log نمی اندازد.

**DHCP Configuration on Router**

```
enable
configure terminal
interface fastethernet 0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
exit
service dhcp
ip dhcp pool RouterPool
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 4.2.2.4
ip dhcp exclude-address 192.168.0.100 192.168.0.200
```