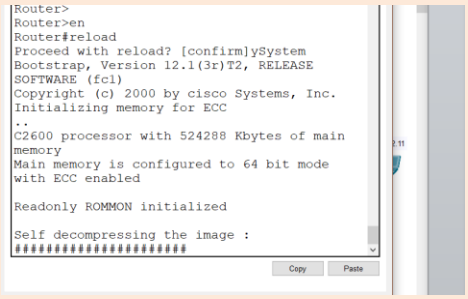
CCNA for Cyber Security

مدرس : استاد عباس ولی زاده

دانشجو : محمدرضا مختاریان

دستور Reload این دستور برای این است که به تنظیمات اولیه برگردد البته اگر زمانی که این دستور را استفاده میکنیم از قبل کانفیگی داشته باشیم از ما سوال می کند آیا ذخیره می کنی که با yes , no جواب می دهیم سپس دستگاه شروع به Reload می کند



روتر در درون خودش یک سیستم عامل دارد که یک فایل فشرده هست با پسوند bin که زمانی که بوت می شود به شکل # یا @ میباشد که یعنی داره از حالت فشرده فایل bin را خارج می کند و به حافظه موقت رم انتقال می دهد در اصل روتر روشن می کنیم وارد وارد فرایند به نام POST میشود یعنی Power On Self Test را داریم یعنی خودشو چک میکنه همه چه اوکی باشد سپس بصورت پیش فرض سراغ Bootstrap که معادل بایوس است تو Bootstrap نوشته شده که فایل bin از کجا بخون در روتر یه حافظه داریم به نام NVRAM که با قطع جریان برق اطلاعات پاک نمی شود اگر کانفیگی داشته باشیم در این حافظه ذخیره میشود و زمانی که لازم باشد یه نسخه از این کانفیگ تو رم کپی می کند این فرایندی که زمانی کانفیگ تو NVRAM هست Startup Config هست و وقتی در رم کپی می کند Runig config اگر به هر دلیلی نتواند فایل bin را پیدا کند که بوت شود به این صورت می نویسد : Router که باید به روش های اون فایل بهش مسیریابی یا بارگذاری کنیم

Security کردن Router یا Switch (امن کردن لاین کنسول)

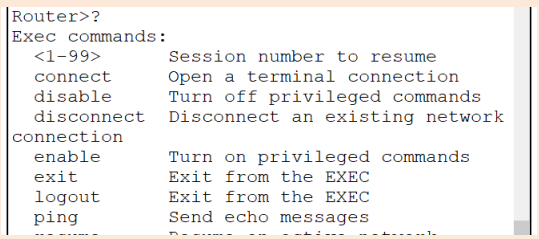
زمانی که Router بالا می آید از ما سوال می کند : (که ما در جواب no را وارد میکنیم)

Would you like to enter the initial configuration dialog? [yes/no]:

سپس وارد چنین محیطی می شود

در عکس بالا به محیطش میگن User Mod می باشد

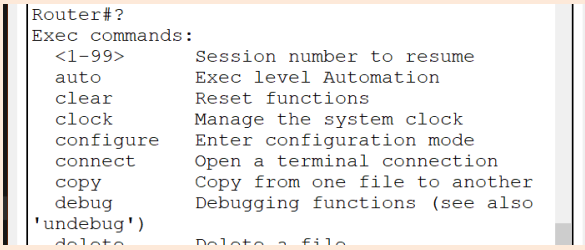
با گذاشتن یک علامت ؟ می توانیم ببینیم چه command های می توان در محیط User Mod بزنیم (این command ها در محیط واقعی بیشتر است)



Command enable

با استفاده از این Command می توانیم وارد محیط Privileged بشویم که علامت # دارد معمولا دستوراتی که برای مانیتورینگ هستن اینجا وارد می کنیم (مثلا command به نام show Arp)

اگر دوباره علامت ? را بگذاریم Command هایی که در این محیط میتوان زد را برای ما لیست می کند که با زدن Enter خط به خط طی می کند و با زدن Space صفحه به صفحه طی می کند



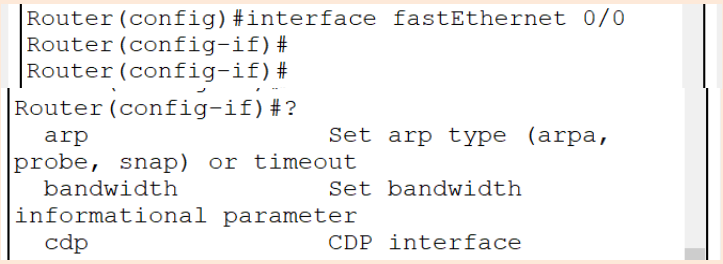
نکته : اگر در سیسکو برای نوشتن دستور تا جای که دستور مشابه باشد با زدن TAP میتوانیم کاملش کنیم البته باید یونیک باشد اگر مشابهی هم داشت برای ما لیست می کند که بهش میگن آتو کامپلیت

Command Configure terminal

برای اینکه از محیط Privileged یک مد بالاتر بریم وارد این مد میشویم که بهش میگن Global Mod

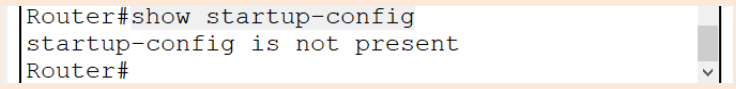
Command interface gigabitEthernet x/x/x - interface fastEthernet 0/0

با این دستور می توانیم که وارد یکی از کانکتورهای Router مورد نظر بشویم که اگر علامت ? را وارد کنیم تمام دستوراتی که در این محیط میتوان زد را ببینیم



Command show startup-config

با این Command می توانیم محتویات NVRAM را ببینیم (در این مثال هیچ کانفیگی انجام نشده است)



Command Show running Config

در این دستور هر کانفیگی که در RAM است را نشان می دهد که بصورت اولیه به این نحو می باشد (تین کانفیگ ما انجام ندادیم و بصورت پیش فرض وجو دارد ، اگر همین کانفینگ پایین را کپی بگیریم در نت پد انگار یه بکاپ گرفتیم از دستگاه)

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

```
Current configuration : 929 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface Serial0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1
```

```
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet1/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

امن کردن Router - Security Router

لاین کنسول را امن کردن

1- وارد محیط یوزر مد می شویم : enable

2- وترد محیط Privileged می شویم
3- سپس Command line console میشویم
4- برای اینکه ببینیم چند تا console داریم جلوی دستور 3 یک علامت سوال می گذاریم : line console ?
5- نکته : با دیدن <cr> یعنی اجازه داری Enter بزنی
6- حالا که مثلا line console 0 را انتخاب کردیم وارد اون لاین می شویم

```
Router(config)#line console ?
  <0-0>  First Line number
Router(config)#line console
% Incomplete command.
Router(config)#line console 0
Router(config-line)#
```

7- حالا باید دستور Password با مقدارش وارد کنیم
8- سپس برای اینکه این دستور تثبیت شود از دستور login استفاده می کنیم

```
Router(config-line)#password 123456
Router(config-line)#logi
Router(config-line)#login
```

9- حالا هر وقت با کنسول وارد شویم از ما پسورد می خواهد

Command Show users

این دستور کاربرانی که یوزر دارند را نشان می دهد

چطور میتوان کانفیگی که انجام دادیم را در NVRAM ذخیره کنیم ؟

با نوشتن دستور Copy running-config starup-config یعنی هرچی در حافظه RAM است به NVRAM انتقال بده بعد که این دستور زدیم از ما اسم میخواهد اگر Enter بزنیم اسم پیش فرض ذخیره می شود و اگر اسمی خودمان بخواهیم تایپ و سپس Enter را می زنیم

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

اگر دستور show startup config را بزنیم مقدار پسورد بصورت clear text ذخیره شده است

نکته : اگر بخواهیم Password را برداریم به چه صورت است ؟ دوباره وارد line console 0 می شویم و دستور no password را می زنیم و سپس دستور no login هم استفاده میکنیم تا در RAM چیزی نماند

نکته مهم : اگر در مد بالاتر از Privileged باشیم اگر دستورات Privileged مثل show run بزنیم کار نمی کند ولی میتوانیم با نوشتن do اول دستور این دستورات را در مدهای بالاتر استفاده کنیم مثال :

```
Router(config-line)#do show run
Building configuration...

Current configuration : 936 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

چطور می توانیم یک یوزر ایجاد کنیم ؟

1- در محیط کنسول دستور login local را وارد می کنیم

```
Router(config-line)# login local
Router(config-line)#
```

2- حالا یک مد پایین تر میایم و وارد مد Global می شویم

```
Router(config)#username admin password 123
Router(config)#
```

نکته : با دستور end میتوانی یهو از مدی به مد Privileged وارد شویم یا با کلید Ctrl + z

نکته دوم و مهم : میتوانیم زمانی که یوزر میسازیم بجای نوشتن پسورد بنویسیم secret که هش قوی تری دارد مثال :

Username admin secret 123

3- سپس دستور starup-config Copy running-config را استفاده میکنیم تا ذخیره شود البته می توانیم ذخیره کنیم بنویسیم write memory یا می توانیم بنویسیم write me یا می توانیم بنویسیم wr

```
Router>show users
    Line       User       Host(s)              Idle
Location
*  0 con 0     admin      idle                 00:00:00

  Interface    User               Mode         Idle     Peer
Address
Router>
```

چطور سطح دسترسی را ببینیم ؟

با نوشتن دستور Show Privileged می توان سطح دسترسی را ببینیم

```
Router>show  privilege
Current privilege level is 1
Router>enable
Router#show
Router#show pr
Router#show pri
Router#show privilege
Current privilege level is 15
Router#
```

نکته : اگر show running-config بنویسیم در کانفیگ هم یوزر و هم پسورد به صورت clear text می باشد

چطور در مد Privileged میتوانیم پسورد وارد کنیم ؟

1- ابتدا وارد مد Global میشویم با دستور enable
2- سپس دتور enable password سپس مقدار پسورد را میدهیم مثل : enable password 123 - نکته مهم : میتوانیم به جای پسورد از secret استفاده کنیم یعنی ..... enable secret مثلا : enable secret 123
3- حتما ذخیره کنیم برای ذخیره سریع wr
4- حالا باید از کانفیگ یک بکاپ بگیریم پس با دستور show running-config دستور را در note pad ذخیره میکنیم

چطور پسورد ها را Encrypt کنیم ؟

1- با command service password Encryption اینکار انجام میشود (نکته : در محیط Global انجام شود)
2- ولی اینکار باز هم Decrypt میشود کافیه در گوگل سرچ کنیم password 7 cisco
3- برای اینکه این command را لغو کنیم کافیه بنویسیم : no service password Encryption
4- نکته : وقتی پسورد را بر میداریم در فایل show running-config که فایل RAM است هنوز می باشد

نکته : برای اینکه در محیط Privilegeمشکل هنگی داشتم مثلا سیسکو یک لاگ انداخت که با نوشته های ما به مشکل برخورد از کلید ترکیبی Ctrl + R استفاده میکنیم که مشکل حل میشود (این مشکل در دنیای واقعی می باشد فقط) ، ولی در کل برای اینکه جلوی این مشکل را بگیریم وارد مد Global میشویم با دستور Conf t سپس دستور line console 0 را تایپ می کنیم و بعد از آن دستور logging synchronous را تایپ می کنیم

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#lin
Switch(config)#line co
Switch(config)#line console 0
Switch(config-line)#logg
Switch(config-line)#logging sy
Switch(config-line)#logging synchronous
Switch(config-line)#
```

مشکل برطرف کردن اینکه اگر در سوئیچ سیسکو واقعی مدت زمان اسکرین سرور را بیشتر کنیم که اگر پسرود داشت از ما دوباره نخواهد

مراحل :

1- ابتدا وارد محیط Global میشویم با دستور conf t
2- سپس وارد لاین کنسول دستگاه می شویم با دستور line console 0
3- در ادامه با استفاده از دستور exec-timeout مینویسیم (اگر جلوی این دستور ؟ بنویسیم یک help)
4- اگر عدد را بدهیم سپس ؟ بگذاریم به ما نشان میدهد می توانیم ثانیه هم بگذاریم و با زدن اینتر تایید میکنیم (ضمنا اعداد به دقیقه است)

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#lin
Switch(config)#linco
Switch(config)#line co
Switch(config)#line console 0
Switch(config-line)#
Switch(config-line)#
Switch(config-line)#exe
Switch(config-line)#exec-t
Switch(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes

Switch(config-line)#exec-timeout 10 ?
  <0-2147483>  Timeout in seconds
  <cr>

Switch(config-line)#exec-timeout 10
```

نکته : حالا اگر با دستور Show running-config نگاه کنیم به کانفیگ دستگاه با این دستور میبینیم در لاین های کنسول هیچ دستوری ست نشده زیرا دستور exect-timeout از دستورات پیش فرض سیسکو هستند (همان طور که میبینیم در سیسکو مثل لینوکس میتوانیم | کنیم و یک کات از خروجی بگیریم – خط قرمز)

```
Switch(config-line)#do sh run | begin line con 0
line con 0
 exec-timeout 10 1
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
end
```

نکته مهم : اگر بخواهیم که هیچ وقت سیسکو به حالت اسکرین سرور نرود باید از نهی No استفاده کنیم در دستور exect-timeout این دستور فقط برای محیط lab هست

```
Switch(config-line)#no exec-timeout
Switch(config-line)#
Switch(config-line)#
```

چطور میتوانیم وقتی یوزری لاگین میکند مثلا وارد مد Privilege 15 کنیم یعنی enable نخواهد برای یوزر خاصی

مراحل :

1- ابتدا وارد مد Privilege میشویم با دستور en
2- در ادامه وارد مد Global میشویم با دستور conf t

3- سپس با دستور username xxxx Privilege xx secret xx میویسیم (جای x اعداد و حروف مناسب میگذاریم)

```
Switch(config)#username admin privilege 15 secret 1234
Switch(config)#do sh
Switch(config)#do show run | begin con 0
line con 0
!
line vty 0 4
 login
line vty 5 15
```

نکته مهم : یکی از نکاتی که برای نفوذ گر مهم است پیدا کردن ورژن سویچ یا روتر است که براساس ورژنی که دارد از تکنیک آسیب پذیری خاص اون ووژن استفاده کند پس به روز بودن دستگاه مهم است

دسترسی به لاین کنسول از راه دور

چطور می توانیم Interface ها را یک روتر یا سوئیچ را ببینیم ؟

مراحل :

1- وارد مد Privilege بشویم با دستور enable
2- سپس دستور show ip interface brief (دستور brief برای این هست که خروجی را مرتب نشان دهد البته میتوانیم اختصار هم بنویسیم یعنی br)

```
Router#show ip interface br
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up
up
GigabitEthernet0/1     192.168.1.1     YES manual up
up
Vlan1                  unassigned      YES unset
administratively down down
Router#
```

چطور به یک روتر IP بدیم ؟

مراحل :

1- ابتدا امن سازی مد ها را تعریف میکنیم
2- وارد محیط Global میشویم
3- سپس در محیط Global باید وارد اون interface بشویم که می خواهیم گت وی اون تعریف کنیم یعنی با این دستور

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#
```

4- حالا وارد اون interface شدیم سپس باید دستور no sht down بزنیم و بعد باید ip و ساب نت مکس را بدهیم

```
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
```

5- با دستور description می توانیم توضیحاتی در مورد اینترفیس ست شده بدهیم تا در run config درج شود برای نوشتن این دستور باید در مد interface باشیم (البته اطلاعات برای هکر ایجاد میشود دقت شود برای استفاده از این دستور)

```
Router(config-if)#description link-to-lan-192-168-1
Router(config-if)#
```

```
Router(config-if)# do show run | begin interface
interface GigabitEthernet0/0
 description Link To Lan 192.168.1/24
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
```

- Exclude چیست ؟ زمانی که در مد Privilege هستیم با نوشتن دستور show ip interface brief برای ما لیست اینتر فیس ها را نشان میدهد

```
Router#show ip interface br
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up
up
GigabitEthernet0/1     192.168.1.1     YES manual up
up
Vlan1                  unassigned      YES unset
administratively down down
```

- حالا می خواهیم کلمه که دورش قرمز کشیده شده است را از سرچ در بیاریم بدین صورت با دستور Exclude اینکار را انجام می دهیم

```
Router#show ip interface br | exclude un
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up
up
GigabitEthernet0/1     192.168.1.1     YES manual up
up
Router#
```

دستور پر کاربر در Router

دستور show ip route برا این هست که خروجی جدول که روتر در خودش دارد را نشان میدهد

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0

Router#
```

❖ یک مثال برای امن کردن سوئیچ و روتر تمامی مراحل در تصویر است :

```
Switch#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#us
Switch(config)#username admin1 sec
Switch(config)#us
Switch(config)#username admin1 sec
Switch(config)#username admin1 secret 12
Switch(config)#en
Switch(config)#ena
Switch(config)#enable sec
Switch(config)#enable secret 12
Switch(config)#lo
Switch(config)#lin
Switch(config)#line con
Switch(config)#line console 0
Switch(config-line)#log
Switch(config-line)#login local
```

ارتباط از راه دور با Switch AND Router با استفاده از پروتکل Telnet

این پروتکل با استفاده از پورت 23 ارتباط را برقرا میکند در کل پروتکل امنی نیست

مراحل :

1- برای اینکه به Router وصل بشویم با استفاده از پروتکل Telnet (tcp – po 23) باید از لاین مجازی روتر استفاده کنیم برای دیدن این لاین وارد مد Global میشویم

2- سپس دستور line vty مینویسیم در انتها یک ؟ میگذاریم تا ببینیم چند تا لاین اجازه استفاده میدهد

```
Router(config)#line vty ?
  <0-15>  First Line number
Router(config)#line vty
% Incomplete command.
Router(config)#
```

3- در این مثال می خواهیم دو نفر همزمان به این روتر Telnetبزنن

```
Router(config)#line vty 0 1
Router(config-line)#
```

4- حالا تعریف می کنیم که login local باشد

```
Router(config-line)#login local
Router(config-line)#
```

5- قبل استفاده از Telnet باید اگر Secret در مد Privilege گذاشته باشیم چون اگر نباشد تا یه حد استفاده از Telnet را میدهد پس در مد Global دستور en secret را میدهیم

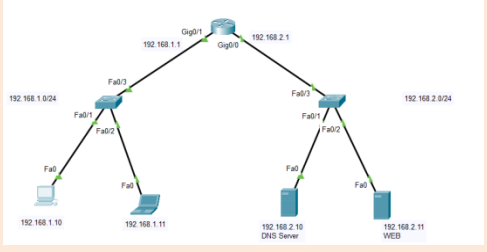
```
Router(config)#no enable secret
Router(config)#
```

از کلاینت 192.168.1.10 به روتر 192.168.1.1 یک Telnet زدیم

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: admin1
Password:
Router#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#
```



```
Router#show users
    Line       User       Host(s)              Idle       Location
   0 con 0     admin1     idle                 00:03:20
*134 vty 0     admin1     idle                 00:00:00 192.168.1.10

  Interface    User               Mode         Idle     Peer Address
Router#
```

نکته : اگر دستور show run configبگیریم و محدود کنیم با پایپ به vty متوجه میشویم که دو مدل vty دارد یکی 0 1 و دیگری 2 4 در صورتی که ما فقط 0 1را ست کردیم اگر 16 تا هم ست کنیم برای ست کردن 16 دستگاه بازم 2 4 را نشان میدهد علت این هست در ورژن های مختلف سیسکو احتمال ساپورت این نوع کانفیگ برای 2 4 هست یعنی ما اگر فایل کانفیگ را در دستگاه دیگه کپی کنیم بتواند جواب دهد

```
Router#show running-config | begin vty
line vty 0 1
 login local
line vty 2 4
 login
!
!
!
end


Router#
```

چطور Telnet را در ویندوز 10 فعال کنیم ؟

1- ابتدا کلید win + r = appwiz.cpl را میزنیم وارد پنجره programs and featuers میشویم بر روی Turn Windows features or off میشویم و تیک Telnet را می زنیم

نکته : روشی برای چک کردن پورت های باز با استفاده از Telnet

Telnet ip target port target

با استفاده از دستور بالا و دادن ip مورد نظر و پورت مورد نظر اگر کلا صفحه سیاه شد یعنی پورت باز هست وگرنه پورت بسته است

چطور switch را با استفاده از Telnet وصل بشویم ؟

1- همان طور که می دانیم سوئیچ نمی تواندip بگیرد ما باید یک vln مجازی درست کنیم
2- اگر دستور show ip interface را استفاده کنیم میبینیم در لیست ip ها جدول سوئیچ یک vlan داریم
3- با استفاده از دستور interface vlan 1 را در مد Global مینویسیم
4- حالا باید interface را با دستور no shut down روشن کنیم

```
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#no sh
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, changed state to up

Switch(config-if)#
```

5- حالا می توانیم به این اینترفیس مجازی ip بدهیم با دستور ip add

```
Switch(config-if)#ip address 192.168.2.2
255.255.255.0
```

6- حالابا استفاده از دستور show run میبینیم مچ شده است یا نه اگر مچ باشد پس سوئیچ را می توانیم پینگ کنیم

```
interface Vlan1
 ip address 192.168.2.2 255.255.255.0
!
!
```

7- وارد مد Globalمیشویم سپس دستور line vty 0 میزنیم که یک نفر مصل بشه
8- در ادامه login local یعنی برو از یورزر و پسورد که ست کردم استفاده کن
9- نکته : اگر الان کسی از شبکه که یک سوئیچ دیگر دارد بخواهد این سوئیچ را که بهش ip با vlan مجازی دادیم ارتباط برقرار نمیشود علت این هست که سوئیچ هیچ اطلاعاتی از این ip ندارد پس باید دستور زیر را بنویسیم در مد Global

Ip default-geteway ip address geteway - مثال ip default-geteway 192.168.1.1

معنی دستور بالا در سوئیچ این هست که اگر کسی از تو سوالی پرسید که بلد نبودی برو از 192.168.1.1 بپرس

10- نکته دوم : ما می توانیم با دستور ip name-server و بعد نام ip از موارد که دستوری به اشتباه زده شده و سویچ براد کست میکند از این DNS که دادیم بپرسد در تصویر اول یه دستور الکی برای مثلا هنگ کردن و در تصویر دوم یک DNS Server ست کردیم تا هنگ نباشد ضمنا اگر DNS Server ست نکردیم میتوانیم کلید ctr+shift+6 بزنیم

```
Translating "asdqrdf"...domain server (255.255.255.255) % Name lookup aborted
Switch#
```

```
Switch(config)#ip name-server 192.168.1.10
```

نکته : در محیط واقعی اگر کامندی اشتباه بود تلنت نزن با دستور no ip domain –lookup از اینکار جلوگیری میشود فقط نرم افزار پکت تریسیر پیش فرض این کامند فعال است

چطور Router – switch را ریست فکتوری کنیم ؟

با نوشتن دستور زیر :

Erase startup-config

چطور SSH را برای Router ست کنیم

1- ابتدا باید برای اینترفیس ها Router باید ip ست کنیم یعنی دستورات زیر را وارد کنیم براساس معماری شبکه

```
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#int g 0/0/1
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

Router(config-if)#
Router(config-if)#ip add 192.168.2.1 255.255.255.0
```

2- حالا باید یک مایش از اینترفیس ها بگیریم تا متوجه بشیم درست هست همیشه هر کاری میکنیم باید چک کنیم تا به ترابل شوت کمتری بر بخوریم

```
Router#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.2.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
Router#
```

3- حالا باید اسم دستگاه Router را عوض کنیم با دستور host name

```
Router(config)#hostname r1
r1(config)#
r1(config)#
```

4- حالا بهش یک دامین معرفی میکنیم با دستور ip domain-name

```
r1(config)#ip domain-name ravin.com
r1(config)#
r1(config)#
```

5- حالا دقت کنیم از ترکیب اسم که دادیم و دامین که تشکیل FQDN را میدهند یک کلید می سازیم بادستور crypto key generate rsa

```
r1(config)#crypto key generate rsa
```

6- نکته : RSA یک نوع الگوریتم است

این دستور در محیط واقعی به این صورت است

```
r1(config)#crypto key generate rsa modulus 1024
```

7- وقتی این دستور میزنیم برای ما یک کلید درست میکند فقط نوع رمز نگاری کلید را می پرسد از 360 – 2048 که هرچی بیشتر بزنیم منابع دستگاه بیشتر درگیر میشود

```
r1(config)#crypto key generate rsa
The name for the keys will be: r1.ravin.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

r1(config)#
*Mar 1 0:8:51.47: %SSH-5-ENABLED: SSH 1.99 has been enabled
r1(config)#
```

8- حالا دقت کنیم برای ما ssh را فعال کرد

9- نکته مهم : در اینجا زده SSH 1.99 یعنی می توان از SSH ورژن 1 استفاده کن تا SSH ورژن 2 یعنی اگر هکر از ورژن 1 که آسیب پذیر هست بیاد میتواند نفوذ کند پس باید به Router بفهمانیم مثلا فقط از ورژن 2 استفاده کن با استفاده از دستور :

Ip ssh version 2

```
r1(config)#ip ssh version 2
r1(config)#
```

10- سپس دستورات زیر را برای ایمن سازی استفاده میکنیم

R1(config)#username admin secret 123

R1(config)#ena

R1(config)#enable seq

R1(config)#enable se

R1(config)#enable secret 12

R1(config)#int vlan 10(har vlan dar scenario metavand bashad)

R1(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

R1(config-if)#ip address 192.168.10.2 255.255.255.0

R1(config-if)#line vty 0

R1(config-line)#login local

R1(config-line)#transport input ssh

نکته : هر ip می توانیم بدهیم ما بالا 10.2 استفاده شده است

11- سپس باید تعریف کنیم فقط باید از ssh استفاده بشود با استفاده از دستور transport input ssh اینکار میکنیم (مهم)

12- چطور از دستور ssh برای وصل شدن به Router استفاده کنیم (قسمت قرمز یوزر نیم و قسمت زرد آی پی دستگاه است)

یک مثال برای تنظیم SSH در Router(command های مربوطه که باید بزنیم بجز ip که براساس سناریو میدیم)

1) Enable
2) Conf t
3) Int g 0/0/0
4) No sh
5) Ip add 192.168.1.1 255.255.255.0
6) Exit
7) Int gig 0/0/1
8) No sh
9) Ip add 192.168.2.1 255.255.255.0
10) Exit
11) Hostname R1
12) Ip domain –name r1.ir
13) Crypto key generate rsa
14) 1024
15) Username admin secret 123
16) Enable secret 123
17) Line vty 0

18) Login local
19) Transport input ssh
20) End
21) Wr

روتر Core با سوئیچ Distribution و سوئیچ Access

مدل شبکه‌ای کمپانی سیسکو شامل لایه هسته، لایه توزیع و لایه دسترسی است. بنابراین، شبکه در این لایه‌ها با نام‌های مختص به خود مانند روتر Core و سوئیچ Distribution و سوئیچ Access شناخته می‌شوند.

مقایسه سوئیچ Core با سوئیچ Distribution و سوئیچAccess

مدل شبکه‌ای کمپانی سیسکو شامل لایه هسته، لایه توزیع و لایه دسترسی است. بنابراین، شبکه در این لایه‌ها با نام‌های مختص به خود مانند سوئیچ Coreو سوئیچ Distribution و سوئیچ Access شناخته می‌شوندسوئیچ Core چیست؟

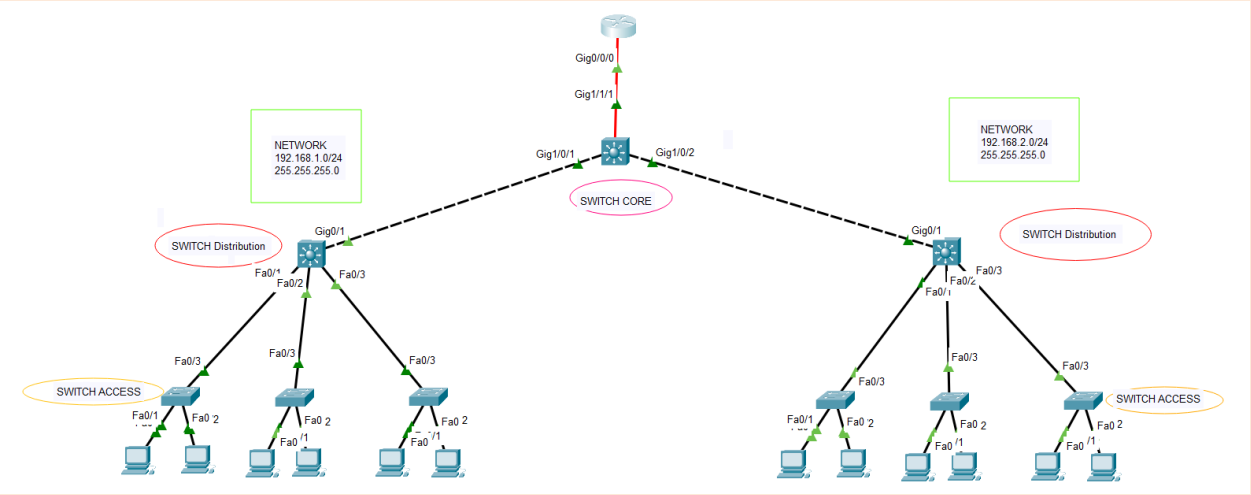
سوئیچ Core نوع خاصی از سوئیچ شبکه نیست. این کلمه به سوئیچ داده‌ای اشاره دارد که در پایه یا هسته فیزیکی یک شبکه قرار دارد. بنابراین باید یک سوئیچ با ظرفیت بالا باشد تا بتواند به عنوان Gateway در خدمت شبکه WAN یا اینترنت باشد. در یک کلام سوئیچ Core نقطه تجمیع نهایی شبکه را فراهم می کند و اجازه می‌دهد تا ماژول‌های مختلف در کنار هم کار کنند

سوئیچ Distribution چیست؟

سوئیچ Distribution به طور مشابه در لایه توزیع یا همان Distribution فعالیت می‌کند. از بالا به سوئیچ Core و از رده‌ی پایین‌تر به سوئیچ Accessمتصل است. سوئیچ Distribution به عنوان پلی بین سوئیچ لایه Core و سوئیچ لایه دسترسی عمل می کند. علاوه بر این، سوئیچ لایه توزیع اطمینان حاصل می‌کند که بسته‌ها یا همان پکت‌های داده به طور پیوسته بین VLAN و Subnet در شبکه سازمانی تبادل داشته باشند. یک سوئیچ Distribution به طور معمول می‌تواند با سرعت ۱۰ گیگابیت بر ثانیه فعالیت کند.

سوئیچ Access چیست؟

سوئیچ Access به طور کلی در لایه دسترسی فعالیت می‌کند. این سوئیچ برای اتصال بیشتر دستگاه‌ها به شبکه مورد استفاده قرار می‌گیرد. در نتیجه به طور معمول دارای پورت‌های زیاد با ظرفیت بالا است ،سوئیچ‌های Access به طور معمول اترنت گیگابیتی هستند و به صورت مستقیم با اینترنت عمومی ارتباط دارند. این سوئیچ‌ها اغلب در دفاتر، اتاق‌های سرور کوچک و مراکز تولید محتوا استفاده می‌شود. سوئیچ مدیریتی و سوئیچ غیر مدیریتی هر دو می‌توانند به عنوان سوئیچ Access فعالیت داشته باشند



کاربرد AAA در سیسکو چیست؟ چگونه AAA سیسکویی راه اندازی کنیم؟

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 هویت کاربر می باشد . این بخش از سرویس AAA ، مجاز بودن و یا غیر مجاز بودن دسترسی کاربر را تعیین می کند.
- ✓ Authorization:این بخش بعد از احراز هویت کاربر (Authentication)اجازه دسترسی به منابع را به کاربر خواهد داد و سطوح دسترسی کاربر را تعیین خواهد کرد.
- ✓ Accounting: این بخش بعد از احراز هویت کاربر(Authentication) و هچنین بعد از Authorization اعمال خواهد شد و دسترسی کاربر را بررسی و همچنین مدت و مقدار دسترسی کاربر را تعیین می کند.
- ✓ سرویس AAA جهت انجام وظایف خود یعنی Authentication,Authorization,Accounting نیاز به تصدیق کاربر بر اساس Username خواهد داشت.شما همچنین میتوانید AAA را به گونه ای پیکربندی کنید که از Username های تعریف شده به صورت Local بر روی استفاده نمایید.

Cisco ISE چیست؟ معرفی نسل جدید سیستم احراز هویت و کنترل دسترسی

سیستم احراز هویت سیسکو (Cisco Identity Services Engine) یا به اختصار ISE یک راه‌حل جدید برای کنترل دسترسی به شبکه است. این سیستم برای تصمیم‌گیری در مورد مجاز بودن دسترسی کاربران و اینکه چه سطح دسترسی به هر یک از آن‌ها داده شود، به سیاست‌های شبکه استناد می‌کند.

کلیه دستگاه‌های بی‌سیم و سیمی می‌توانند تحت کنترل این برنامه امنیتی پیچیده به شبکه متصل شوند. به‌علاوه امکان احراز هویت، اعتبارسنجی و حسابرسی (AAA) از طریق پروتکل RADIUS فراهم می‌شود. به زبان ساده شرکت‌ها می‌توانند با این پلتفرم احراز هویت، دسترسی به شبکه و امنیت آن را چندین برابر بهبود ببخشند. کلیه اطلاعات به‌صورت بلادرنگ جمع‌آوری می‌شود و مدیر شبکه بر اساس آن‌ها تصمیمات حاکمیتی را اتخاذ می‌کند.

مهمترین ویژگی‌های cisco ise چیست؟

اگر بخواهیم به برخی از مهمترین ویژگی‌های سیسکو ISE اشاره کنیم، اولین مورد ادغام پروتکل) AAA احراز هویت، اعتبارسنجی و حسابرسی) با وضعیت سلامتی تجهیزات کاربران و Profiler در یک دستگاه است ، مدیریت جامع دسترسی Guest را برای مدیر سیسکو، سرپرستان اسپانسر یا هر دو فراهم می‌کند پشتیبانی از شناسایی کاربران، پروفایل‌سازی، جاگذاری کاربران در شبکه مبتنی بر سیاست و نظارت بر دستگاه‌های اندپوینت در شبکه از دیگر ویژگی‌های سیسکو ISE است. فعال‌سازی سیاست‌های منسجم که خدمات را همانجا که لازم است ارائه می‌کند ، استفاده از قابلیت‌های اجرایی پیشرفته از جمله دسترسی به گروه امنیتی (SGA) و لیست‌های کنترل دسترسی گروه امنیتی.(SGACL) پشتیبانی از مقیاس‌پذیری جهت پشتیبانی از سناریوهای استقرار برای محیط‌های اداری کوچک تا محیط‌های سازمانی بزرگ.

TACACSو مدیریت دستگاه

یکی از مهمترین موارد استفاده سیسکو ISE کنترل دسترسی اداری به دستگاه‌های زیرساخت شبکه مثل روترها و سوئیچ‌ها است. با استفاده از +TACACSنوع دستوراتی که مجازند در این دستگاه‌ها اجرا شوند را می‌توان در صورت لزوم برای مدیران شبکه‌های مختلف تنظیم و محدود کرد

زمانی که یک کاربر وارد شبکه می‌شود و تغییراتی روی آن ایجاد می‌کند، +TACACS گزارش‌های از تمام افرادی که وارد سیستم شده اند، زمان ورود آن‌ها و تغییراتی که اعمال کرده‌اند ثبت می‌کند.

vlanچیست ؟ کاربرد vlan بندی در شبکه چیست

میخواهم با یک مثال بسیار ساده بگویم که یک vlan چیست ؟

فرض کنید در یک شرکتی که می‌کنید ۱۰۰ نفر کارمند دارد. بخش هایی که در این مجموعه وجود دارد شامل: بخش بازاریابی، حراست، منابع انسانی، حسابداری و... است. هزاران سند و مدرک در این شرکت موجود است و قرار نیست که همه ۱۰۰ نفر کارمند همه اطلاعات را ببینن ،

می‌دانیم که در شبکه می‌توانیم اطلاعات را دسته بندی و دسترسی هایی ایجاد کنیم که همه اطلاعات را نبینند. اما راه بهتری وجود دارد که منطقی تر است. یعنی vlan بندی. چرا که اینجا سناریو به این شکل است ، استراتژی ما در این شرکت به این طریق است که ما می‌خواهیم فقط بچهای گروه

حراست به پرونده های استخدامی دسترسی داشته باشند و دیگر هیچکس نتواند آن داده ها را ببیند. برای اینکار بهترین راه داشتن وی لن است، vlan ها گروه بندی‌های منطقی هستند که دستگاهای های فیزیکی شبکه همانند سوئیچ، کامپیوتر و لپ تاپ و... درون آن قرار می‌گیرند. این گروه بندی در سوئیچ ایجاد می‌شود و می‌تواند تغییرات بزرگ و اساسی در شبکه ها ایجاد کند.

اگر ساده تر بخواهیم تعریف کنیم شما شبکه محلی خود را به راحتی می‌بینید و می‌توانید کابل ها و دستگاه های آن را لمس کنید. اما در این مدل شبکه مجازی لمس برخی از قسمتهای آن امکان پذیر نیست و نمی‌توانید فیزیکی آن را ببینید و با ذهن باید آن را درک کنید و با دستورها با آن سروکار دارید.

کارایی و مزیت vlan چیست ؟

در اکثر شبکه های بزرگ با تعداد کارمندان زیاد که سیاستهای شبکه‌ای خاصی را می‌طلبد نیاز است که یک هوش مدیر شبکه پشت آن باشد تا بهترین سود از کارایی از پسیو و اکتیو سیستم های مجموعه را ببرند.

VLAN ها به شما امکان می دهند شبکه خود را به راحتی تقسیم بندی کنید. شما می توانید کاربرانی را که اغلب با یکدیگر در یک VLAN مشترک ارتباط هستند، صرف نظر از مکان فیزیکی که قرار دارند، گروه بندی کنید.

ترافیک شبکه ها به شدت کاهش پیدا می‌کند.

ترافیک هر گروه که تعیین کرده باشید تا حد زیادی در VLAN قرار دارد و باعث کاهش ترافیک اضافی و بهبود کارایی کل شبکه می شود.

مدیریت VLAN ها آسان است. شما می توانید به سرعت هر سیستم و یا نود شبکه را اضافه یا تغییر دهید و سایر تغییرات شبکه را از طریق رابط مدیریت به صورت وب به جای انجام دهید.

VLAN ها باعث افزایش عملکرد می شوند .پهنای باند را با محدود کردن ترافیک پخش در سراسر شبکه آزاد می کند.

VLAN ها امنیت شبکه را افزایش می دهند .VLAN ها مرزهای مجازی ایجاد می کنند که فقط از طریق روتر قابل عبور است. بنابراین، می توانید از اقدامات امنیتی استاندارد مبتنی بر روتر برای محدود کردن دسترسی به VLAN استفاده کنید.

چه زمانیvlan ها کاربردی خواهند بود؟

دقت داشته باشید که بهتر است VLAN زمانی استفاده شود که بیش از 200 دستگاه روی LAN خود داشته باشید.

هنگامی که ترافیک زیادی در شبکه LAN دارید، مفید است. در غیر اینصورت گیج کننده خواهد بود.

VLAN زمانی ایده آل است که گروهی از کاربران به امنیت بیشتری احتیاج داشته باشند یا انتقال اطلاعات آنها کاهش یافته باشد.

زمانی استفاده می شود که کاربران در یک دامین پخش نباشند.

یک سوئیچ را به چند سوئیچ تبدیل کنید.

معایب vlan بندی چیست؟

اگر فردی که این کار را به صورت حرفه ای بلد نباشد انجام دهد یک بسته می تواند از یک VLAN به دیگری نشت کند بسته اطلاعاتی ممکن است منجر به حمله سایبری شود داده ها ممکن است یک ویروس را از طریق یک شبکه منطقی کامل منتقل کند برای کنترل حجم کار در شبکه های بزرگ به یک روتر اضافی نیاز دارید در زمینه همکاری با مدیران شبکه و عوض کردن متخصصین شبکه در زمان‌های مختلف با مشکلاتی زیادی روبرو خواهید شد یک VLAN نمی تواند ترافیک شبکه را به سایرVLAN ها ارسال کند

VLANچگونه اطلاعات را ارسال می‌کند؟

VLAN ها در شبکه با یک عدد شناسایی می شوند.

یک محدوده معتبر از 1تا 4094 است. در یک سوئیچVLAN ، پورت ها را در شماره VLAN مشخص قرار می‌دهید.

سپس سوئیچ با توجه به اطلاعاتی که ارسال می‌شود از پورت خاص با شماره وی لن خاص اجازه می دهد تا داده ها بین وی لن ها ارسال شوند.

ممکن است در یک شبکه بزرگ از یک سوئیچ استفاده شده باشد، باید راهی برای ارسال ترافیک بین دو سوئیچ وجود داشته باشد.

راهکاری که برای ارتباط بین دو سوییچ وجود دارد این است که یک پورت به هر سوئیچ شبکه با یک VLAN تعریف کنیم و با یک کابل به هم وصل کنیم.

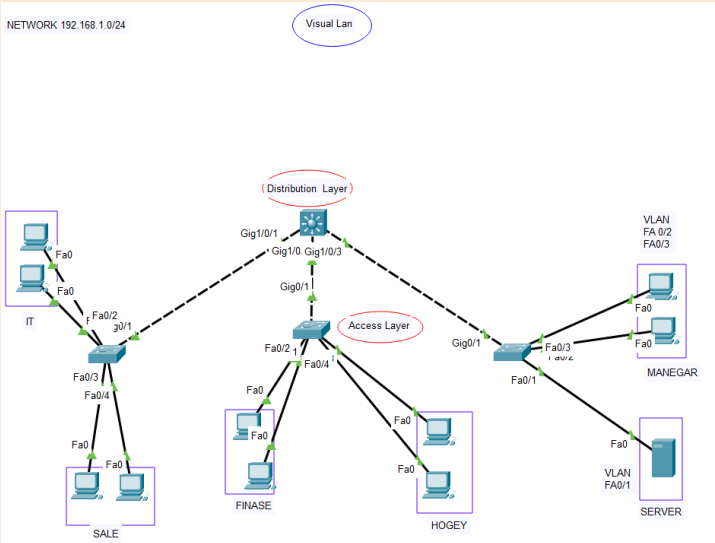
vlanچیست و چه کاربردی دارد ؟

زمانی که در یک شبکه تعداد دستگاه‌ها و کارمندان مجموعه زیاد می‌شود و ترافیک شبکه بالا می‌رود برای کنترل کردن این ترافیک بهتر است که سوئیچ های مجموعه را بخش بندی کرد و هر بخش شرکت را در یک طبقه مشخص شده در سوئیچ قرار داد. مثلا سکشن بازاریابی را در قطعه مشخص شده در سوئیچ قراردهیم و همینطور قسمت های مختلف را در بخش های مختلف. به این کار وی لن بندی گفته می‌شود.

نکته : ما می توانیم برای تفیک تمامی واحد ها که چندین END POINT دارند با IP شبکه ها را جدا کنیم ولی زمانی که برادکست زده میشود در لایه دو اتفاق می افتد و باعث میشود منابع زیادی درگیر شود پس راه کار خوبی نیست

راه اندازی سناریو VLAN بندی کردن

1- در این سناریو ما می خواهیم قسمت Server و Manegar را VLAN بندی کنیم که FA/01 تا FA0/3 به سوئیچ مورد نظر وصل هستند



2- وارد مد Privileged می شویم و تایپ میکنیم Show vlan Brief تا لیست اینتر فیس ها رانشنان دهد در vlan مربوطه بصورت پیش فرض تمامی اینترفیس ها در vlan 1 هستند که بهش میگن Native Vlan می گویند ، پسری Vlan داریم که با (قرمز) نشان دادیم نباید استفاده شوند کل Vlan هایی که داریم از 1 تا 4090 می باشد

```
Switch>
Switch>EN
Switch#sh
Switch#show vl
Switch#show vlan br
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

3- ابتدا در محیط Global باید Vlan 10 مثلا برای Server بسازیم با دستور vlan 10 (تو دنیای واقعی تا exit ندی ساخته نمی شود)

```
Switch#show vlan br
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   VLAN0010                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

4- سپس وارد vlan 10میشویم در مد Global با نوشتن دستور vlan 10 سپس به vlan 10یک name می دهیم چون برای Server هست همین نام را می دهیم

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Server
Switch(config-vlan)#do sho vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Server                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

5- حالا باید اینترفیسی که میخواهیم به vlan بدهیم با دستور interface range fastEthernet 0/1

6- سپس دستور switchport access vlan 10 را میدهیم – نکته : برای این vlan 10 چون می خواهیم Server در این vlan باشد

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   Server                            active    Fa0/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

7- حالا می خواهیم vlan قسمت manger را بدهیم

```
Switch(config)#interface fastEthernet 0/2-3
                                      ^
% Invalid input detected at '^' marker.

Switch(config)#int
Switch(config)#interface ra
Switch(config)#interface range fas
Switch(config)#interface range fastEthernet 0/2-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport ac
Switch(config-if-range)#switchport access vla
Switch(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch(config-if-range)#do sh vlan brief
```

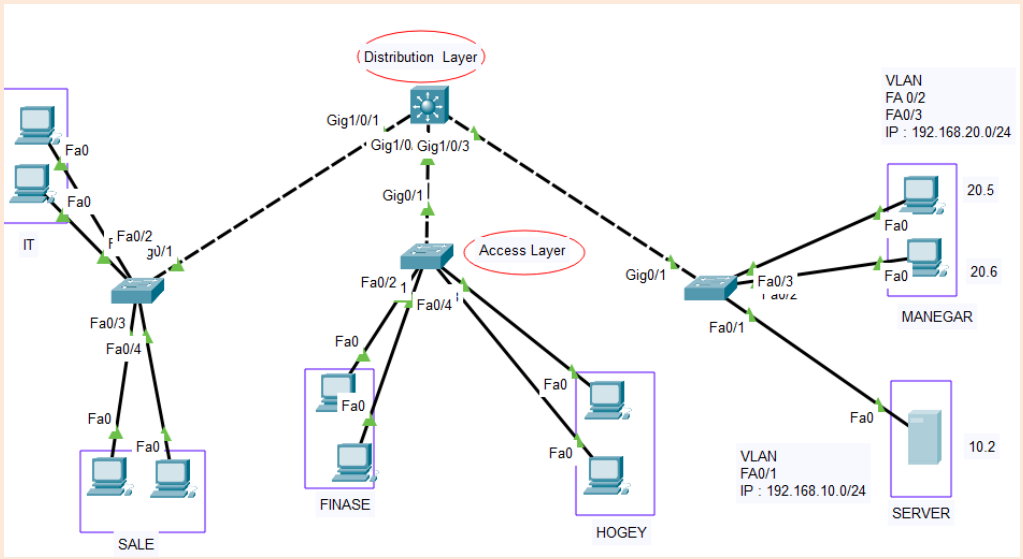
8- درسته از قبل vlan 20نساختیم ولی با دستور فوق مستقیم ساخته می شود
9- حالا یک خروجی نمایش میگیرم تا vlan manager ساخته شده است

```
Switch(config)#vlan 20
Switch(config-vlan)#name manager
Switch(config-vlan)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   Server                           active    Fa0/1
20   manager                          active    Fa0/2, Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch(config-vlan)#
```

10- حالا قسمت manager بهش IP میدهیم
11- و سپس قسمت server بهش IP میدهیم

نکته : زمان VLAN بندی هر قسمت شبکه جدا باشند احمقانه ترین کار این هست تو یک شبکه باشند



Trunk تعریف

به عنوان کسی که در حوزه شبکه فعالیت میکند حتما میدانید که ما مفهومی به نام VLAN داریم که پورت های سویچ ها را از هم تفکیک و ترافیک آنها را مجزا می کنیم و در وهله اول باید به این موضوع توجه کنید که شما می توانید VLAN هایی به یک اسم و با یک ID مشترک در سویچ های مختلف شبکه داشته باشید که ترافیک این سویچ ها در این پورت ها برای VLAN مورد نظر ایزوله است!!

پس این طرز فکر را از ذهنتان بیرون بیندازید که VLAN فقط مختص یک سویچ و پورت های آن است و بس!!

شما می توانید کامپیوتری در VLAN 100 در سویچ MALI داشته باشید که بعد از جدا کردن از سیستم و بردن آن به طبقه دهم و اتصال به سویچ MODIRIYATهمچنان در همان VLAN 100 قرار داشته باشد !! اما چطور ممکن است که ما همچنان در یک VLAN باشیم و با کامپیوترهایی در سویچ های دیگر در همان VLAN صحبت کنیم ؟ شما می توانید با استفاده از یک پورت به عنوان شاه پورت ترافیک سویچ های مختلف به هم را مدیریت و آنها را به هم متصل کنید به این شاه پورت در اصطلاح فنی پورت Trunk گفته می شود.

پورت Trunk چیست

یک پورت ترانک یا Trunk Port در واقع پورتی است که وظیفه آن انتقال ترافیک VLAN هایی است که سویچ به آنها دسترسی دارد ، به فرآیندی که در آن ترافیک VLAN ها می تواند به سویچ دیگر از طریق پورت Trunk منتقل شود نیز Trunking گفته می شود. پورت های Trunk هر Frameرا با استفاده از یک برچسب شناسایی منحصر به فرد که در اصطلاح Tag گفته می شود علامت گذاری می کند ، برای مثلا برچسبی بر روی یک Frame قرار می گیرد که مشخص کننده این است که این Frame متعلق به VLAN 100 می باشد ، البته برچسب های متنوعی وجود دارند که بر اساس پروتکل های مورد استفاده در سویچ متفاوت هستند ، معمولترین نوع برچسب ها یا Tag های مورد استفاده در Trunking برچسب 802.1Qو همچنین برچسب Inter-Switch Link یا ISL می باشد. این برچسب ها یا Tag ها زمانی کاربرد دارند که ترافیک بین سویچ ها جابجا می شوند. با استفاده از این مکانیزم و برچسب ها هرگاه یک Frame از سویچ خارج شود با توجه به برچسب مورد نظر ، مشخص می شود که قرار است به کجا هدایت شود و مسیر مشخصی را طی خواهد کرد و به VLAN مورد نظر ما هدایت می شود ، به این نکته توجه کنید که یک پورت اترنت یا می تواند یک Access Port باشد یا یک Trunk Port و نمی تواند بصورت همزمان هر دو کار را انجام بدهد ، بنابراین به پورتی که به عنوان Trunk تعریف شده است کامپیوتری را نمی توانید متصل کنید. نکته جالبتر در خصوص پورت های Trunk این است که برخلاف پورت های Accessیا دسترسی ، این پورت ها می توانند همزمان به عضویت چندین VLAN در بیایند و به همین دلیل است که می توانند ترافیک های VLAN های مختلفی را همزمان هدایت کنند.

همانطور که گفتیم برای اینکه پورت ترانک ما به درستی بتواند ترافیک های VLAN های مختلف را هدایت کند با استفاده از پروتکل 802.1Qهر کدام از Frame هایی که از پورت های مختلف سویچ دریافت می شوند را برچسب گذاری یا Tag می زند. به این فرآیند 802.1 Q Encapsulation نیز گفته می شود. در این روش Tag مورد نظر و مربوط به VLAN مورد نظر بر روی Header بسته یا Frame اطلاعاتی ما قرار می گیرد. محتویات این برچسب یا Tag مشخص کننده VLAN ای است که Frame از آن وارد سویچ شده است ، این فرآیند باعث می شود که هرگاه ترافیک از پورت های Trunk یک سویچ عبور می کنند مشخص باشد که قرار است به کدام VLAN وارد شوند و همزمان می توان چندین Frame از VLAN های مختلف را درون یک Trunk Port هدایت کرد. بصورت پیشفرض همه ترافیک VLAN های مختلف به سمت همه Trunk Port ها هدایت می شوند اما شما می توانید این روند را تغییر بدهید و طراحی خاص خودتان را در سویچ ها پیاده سازی کنید.

مراحل راه اندازی Trunk

1- ابتدا بهتر است که اسم دو سوئیچ را عوض کنیم پس سوئیچ اول در مد Global با دستور Switch-1 hostename می گذاریم و سوئیچ دوم را با دستور Switch-2 hostename می گذاریم

2- سپس وارد مد interface Gig 0/1 که به Switch-1 هست وارد می شویم.

```
Switch-1(config)#interface gigabitEthernet 0/1
Switch-1(config-if)#
```

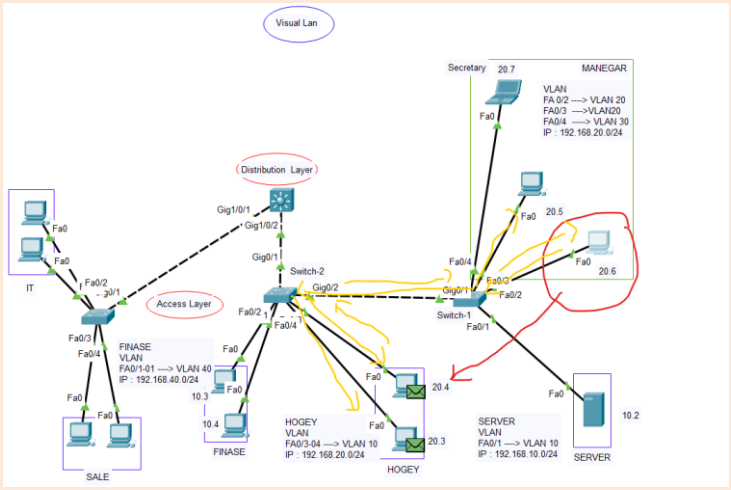
3- سپس دستور switchport mode trunk را مینویسیم

```
Switch-1(config-if)#switchport mode trunk
Switch-1(config-if)#
```

4- نکته بعضی دستگاه ها دستور 3 قبول نمی کنن از دستور زیر استفاده می کنیم

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#
```

5- حالا وارد مد Privileged می شویم و دستور Show interface trunk میزنیم



در شکل بالا می بینیم که از 192.168.20.6 یک بسته به سمت 192.168.20.4 که اول سوئیچ برادکست زده (خط زرد) و چون در یک vlan هستند سوئیچ فقط برای این محدوده می فرستند و با ساتفاده از Trunk می گویم که فقط بسته به این سمت فرستاده شود و برادکست که برای همه میرود برای همه نفرستد

نکته مهم : تنها vlan که tag نمی خوره در هنگام trunk وی لن Native است ما باید وی لن Native را اسمشو عوض کنیم که پیش فرض اسمش 1 هست از نظر امنیتی مهم است وقتی اسم وی لن Native به مثلا 99 تغییر دهیم هنگام Trunk وی لن مذکور Tag می خورد

نکته مهم 2 : اگر سوئیچی به فرض داریم که از 24 پورت اینترفیس 5 تا اینترفیس استفاده می کنیم مابقی اینتر فیس ها داخل بشویم و shut down کنیم سپس حتما Native وی لن اسمشو عوض کنیم چون باعث حمله vlan hopping می شود

چطور می توان بفهمیم که چه اینترفیس های وصل هستند و فعالن :

با دستور show int status لیستی از تمامی پورت های سوئیچ با وضعیتش میدهد - سپس با دستور interface range fastEthernet 0/5-24 اینترفیس هایی که لازم نداریم خاموش کردیم

چطور اسم Vlan Native را عوض کنیم ؟

1- وارد مد Global می شویم با دستور conf t
2- سپس اینترفیس مربوطه انتخاب میکنیم مثله int g 0/1
3- سپس با دستور switchport trunk native vlan 99 که 99 اسمی هست که ما به vlan دادیم پیش فرضش 1 بود

```
Switch-2#
Switch-2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native
vlan
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
```

```
Switch-2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native
vlan
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/2      1-1005
```

VLAN hoppingچیست و چگونه باعث آسیب‌پذیری‌های امنیتی شبکه می‌شود؟

VLAN hoppingروشی برای حمله به منابع شبکه یک VLAN با ارسال بسته‌ها به پورتی است که معمولاً از یک سیستم پایانی، قابل دسترسی نیست. هدف اصلی این نوع حمله دسترسی بهVLAN های دیگر در همان شبکه است درVLAN hopping ، عامل تهدید ابتدا باید حداقل در یک VLANشبکه نفوذ کند. این امر مجرمان سایبری را قادر می‌سازد تا پایگاهی از عملیات را برای حمله به دیگرVLAN های متصل به همان شبکه ایجاد کنند.

VLAN hoppingچگونه باعث آسیب‌پذیری‌های امنیتی شبکه می‌شود؟

آسیب‌پذیری‌های VLAN به ویژگی‌های کلیدی آن‌ها مربوط می‌شود، از جمله:

قادر ساختن مدیران شبکه برای پارتیشن‌بندی یک شبکه سوئیچ شده برای مطابقت با الزامات عملکردی و امنیتی سیستم‌های خود بدون نیاز به استفاده از کابل‌های جدید یا ایجاد تغییرات قابل توجه در زیرساخت شبکه بهبود عملکرد شبکه با گروه‌بندی دستگاه‌هایی که مرتبا با یکدیگر ارتباط برقرار می‌کنند ایجاد امنیت در شبکه‌های بزرگ‌تر با فعال‌سازی کنترل بیشتر بر دسترسی دستگاه‌ها با یکدیگر VLANها با تفکیک کاربران، به بهبود امنیت کمک می‌کنند زیرا کاربران فقط می‌توانند به شبکه‌هایی دسترسی داشته باشند که مربوط به نقش‌های آنهاست. علاوه بر این، رصورتی‌که مهاجمان خارجی به یک VLAN دسترسی داشته باشند، تنها در همان شبکه خواهند بود.

حملات VLAN hopping چگونه انجام می‌شوند؟

یک حمله VLAN hopping می‌تواند به یکی از دو روش زیر انجام شود:

1- double tagging(برچسب‌گذاری دوگانه)

حملات double tagging زمانی اتفاق می‌افتند که عوامل تهدیدtag ها را در فریم اترنت اضافه و تغییر دهند. این رویکرد امکان ارسال بسته‌ها را از طریق هر VLAN به عنوان VLAN بدون tag بومی، در ترانک فراهم می‌کند و از چند سوییچ که tag ها را پردازش می‌کنند، بهره می‌برد.هکر با ارسال فریم‌هایی با دو تگ Q802.1، داده‌ها را از طریق یک سوییچ به سوییچ دیگر ارسال می‌کند: یکی برای سوییچ مهاجم و دیگری برای سوییچ قربانی این عمل باعث می‌شود سوییچ قربانی فکر کند که فریمی برای آن در نظر گرفته شده است. سپس سوییچ هدف فریم را به پورت قربانی می‌فرستد. اکثر سوییچ‌ها، tagبیرونی را فقط قبل از ارسال فریم به تمام پورت‌های VLAN بومی حذف می‌کنند. به عنوان مثال، اگر یک سوییچ شبکه برای autotrunking تنظیم شده باشد، مهاجم آن را به سوییچی تبدیل می‌کند که گویا برای دسترسی به تمامVLAN های مجاز در پورت ترانک دائما به ترانک نیاز دارد. از آنجایی که کپسوله کردن بستهٔ برگشتی غیرممکن است، این سوء استفاده امنیتی اساساً یک حمله یک طرفه است و تنها در صورتی امکان‌پذیر است که هکر عضوی از همان VLAN trunk link باشد.

کانفیگ کردن راه کار های امنیتی

1- با دستور show interfaces fastEthernet 0/1 switchport اطلاعات جامعی از این اینتر فیس بگیریم (در اینجا وارد اینتر فیس 1/0 شدیم)

```
Switch-1#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 10 (Server)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
 --More--
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(1), with Switch-2 GigabitEthernet0/2 (99).
```

اطلاعات مواردی که از نمایش دستور بالا برای اینترفیس گرفته شده است (همان عکس بالا است)

1) Switchport: Enabled (یعنی سویچ پورت لایه دو است فقط کابل وصل شود فعال میشود)
2) Administrative Mode: dynamic auto (مد ها رانشان میدهد که access , trunk ادمین تصمیم میگیرد)
3) Operational Mode: static access (یعنی الان اینترفیس به سیستمی وصل است که دو حالت دارد یا access یا trunk)
4) Administrative Trunking Encapsulation: dot1q
5) Operational Trunking Encapsulation: native
6) Negotiation of Trunking: On
7) Access Mode VLAN: 10 (Server)
8) Trunking Native Mode VLAN: 1 (default)
9) Voice VLAN: none
10) Administrative private-vlan host-association: none
11) Administrative private-vlan mapping: none
12) Administrative private-vlan trunk native VLAN: none
13) Administrative private-vlan trunk encapsulation: dot1q
14) Administrative private-vlan trunk normal VLANs: none
15) Administrative private-vlan trunk private VLANs: none
16) Operational private-vlan: none

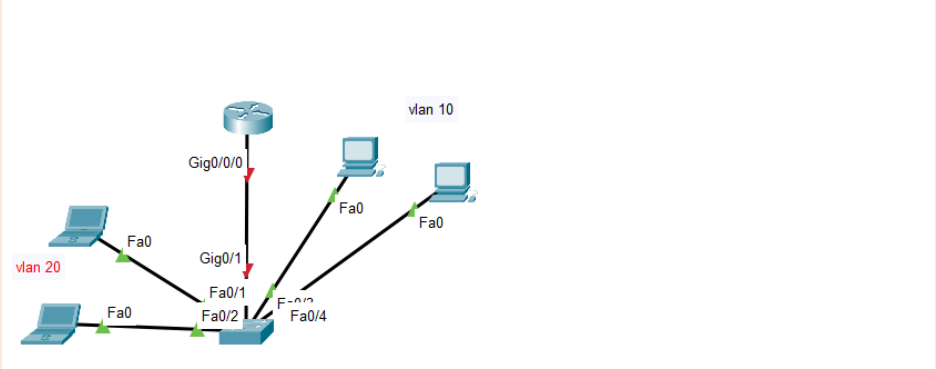
17) Trunking VLANs Enabled: All
18) Pruning VLANs Enabled: 2-1001
19) Capture Mode Disabled
20) Capture VLANs Allowed: ALL
21) Protected: false
22) نکته : یک اینترفیس که access است عضو دو وی لن باشد یکی دیتا وی لن یکی ویس وی لن
23) نکته : اگر اینترفیس trunk باشد عضو بیش از یک وی لن است

نکته مهم : ما با دستور switchport mode name mode morde nazar (access, auto , trunk) می توانیم بفهمیم که اینترفیس مربوطه رو چه مدی است اگر اینترفیس مربوطه روی auto باشد نفوذگر می تواند با ابزار (Yersinia) بوسیله پروتکل DTP (که برای ایجاد Trunk این پروتکل استفاده می شود) از اینترفیس و سویچ مربوطه بخواهد trunk شویم و چون اینتر فیس روی مد auto است به راحتی قبول میکند و این باعث میشود ترافیک سازمان از این قسمت آسیب پذیر شود ما باید اینترفیس سمت end point ها بزنیم switchport mode access یا switchport mode host پس تو سناریو قبلی که داشتیم آموزش trunk ایجاد میکردیم فقط برای یک سویچ trunk کردیم این نکته مهم است باید باید دو سوئیچ trunk شود و وقتی که اون سوئیچ هم با دستور switchport trunk زدیم در ادامه اش دستور switchport nonegotiate را حتما می زنیم (باید این دستور پروتکل DTP جلوش گرفته میشود) پس این دستور برای دو سوئیچ دستور switchport nonegotiate میزنیم حتما

(ROAS) Router One A Stick

در این مبحث می خواهیم Port Security راه اندازی کنیم تا Enter Vlan Routing انجام بدهیم ، یعنی یک روتر که یک اینترفیس واقعی دارد اون اینترفیس را به چند اینترفیس مجازی تبدیل کنیم

1- در سناریو که داریم یک سوئیچ و یک روتر و دوتا vlan به نام های 10و20



2- ابتدا سوئیچ را به نحو زیر کانفیگ می کنیم

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int ra fa 0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if-range)#
```

3- همان طور که مشاهده می کنیم به ما اعلام می کند که vlan10 وجو نداشت ولی ساختم
4- اگر در سناریو ببینیم یک vlan20 هم داریم که به کانفیگ اون را انجام می دهیم