az shabake 1

Thursday, December 10, 2020 6:23 PM

نشان دادن دستورات قابل استفاده در mode (حالتی) که در آن قرار داریم:
?

نشان دادن دستوراتی که با e شروع می شوند:
e?

نشان دادن پارامتر های دستور show:
show ?

ورود از حالت User EXEC به حالت Privileged EXEC (حالت enable):
enable

نشان دادن تنظیمات موجود در ram:
show running-config

ورود از حالت Privileged EXEC به حالت Global config. (حالت global):
configure terminal

تغییر hostname سویچ به sw1:
hostname sw1

برگشتن به حالت قبلی (enable):
exit

نشان دادن تنظیمات موجود در ram:
show running-config
(مشاهده می کنیم که hostname تغییر کرده است)

سیو کردن تنظیمان موجود در ram در nvram:
copy running-config startup-config
یا
write memory
یا
wr
(همواره در صورت reboot کردن سویچ، تنظیمات vram بارگذاری می شوند)

نشان دادن تنظیمات موجود در vram:
show startup-config

ورود از حالت enable به حالت global:
configure terminal

ورود از حالت global به حالت Interface config. پورت fastEthernet 0/1:
interface fastEthernet 0/1

برگشتن به حالت قبلی (global):
exit

ورود از حالت global به حالت Line config. پورت کنسول 0:
line console 0

پسورد تعیین کردن برای پورت کنسول و فعال کردن login به کمک پسورد: (1)
password 123
login

برای سیو کردن تنظیمات در vram باید به حالت enable برویم.
برای این که از mode فعلی خارج نشویم، می توانیم از do کمک بگیریم
(فقط برای اجرا کردن دستورات حالت enable به هنگام حضور در حالتی دیگر):
do wr

ساخت user-pass (در حالت global می سازیم):
username nima password 123

برداشتن پسورد پورت کنسول و غیر فعال کردن login به کمک پسورد
(در حالت Line config. پورت کنسول 0 می زنیم):
no password
no login

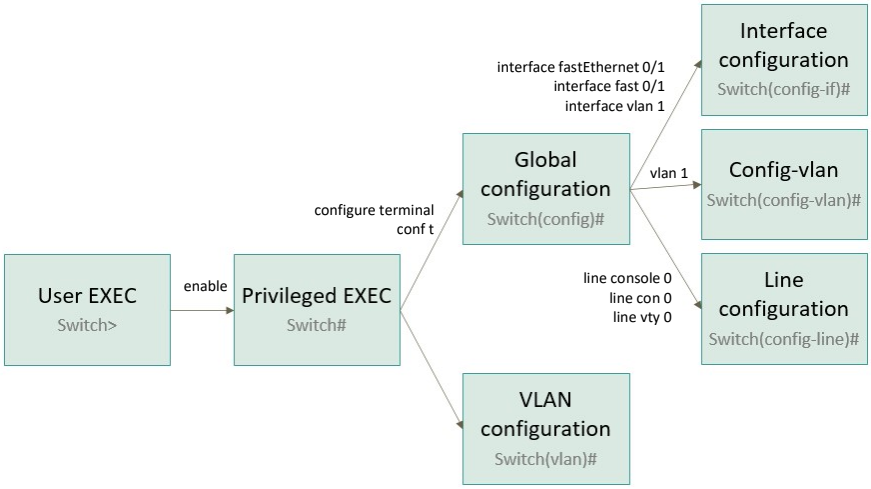
فعال کردن login به کمک user-pass برای پورت کنسول (در حالت Line config. پورت کنسول 0 می زنیم):
login local

حذف user-pass (در حالت global می زنیم):
no username nima

ساخت user-pass امن (در حالت global می سازیم):
username nima secret 123
(در این حالت پسورد ها encrypt می شوند)

reboot کردن سویچ (در حالت enable می زنیم):
do reload

نکته: برای logout کردن از کنسول از دستور logout استفاده می کنیم.



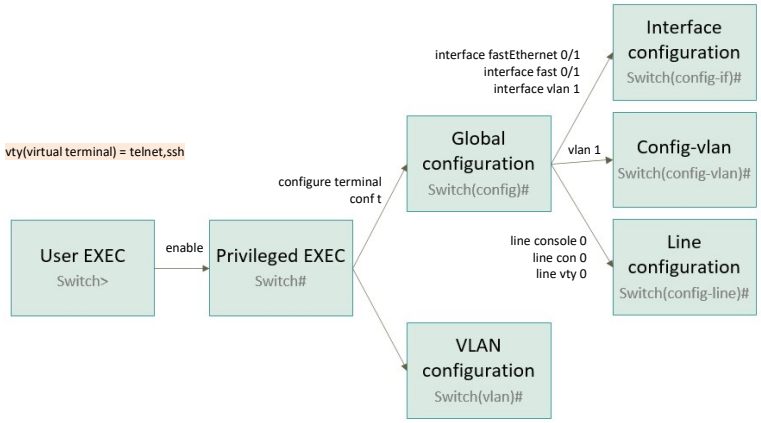
(1) توجه: پسورد (های) مربوط به console port نیز به صورت plain text در config فایل سویچ ذخیره می شوند.
برای حل این مشکل به کمک دستور زیر سرویس password-encryption را در سویچ فعال می کنیم:
service password-encryption

برای تعیین کردن یک پسورد برای "ورود به حالت enable" از دستورات زیر استفاده می کنیم:
(در حالت global می زنیم)
enable secret <password>

روش دیگری نیز برای تعیین کردن یک پسورد برای ورود به حالت enable وجود دارد و آن استفاده از دستور زیر است:
enable password <password>
ولی استفاده از این روش توصیه نمی شود زیرا پسورد را به صورت plain text در config فایل سویچ ذخیره می کند
در حالی که روش بالا، پسورد را در قالب هش MD5 ذخیره می کند.

az shabake 2

Monday, December 14, 2020 4:15 PM



در حالت user عملا هیچ غلطی نمی توانیم بکنیم و عملا فقط برای این ساخته شده است تا به کمک دستور enable به حالت enable رفته و سیستم از ما یک پسورد بپرسد.
در حالت enable نیز بغیر از show های ابتدایی هیچ غلطی نمی توانیم بکنیم.

در حالت global می توانیم کار های کلی مربوط به سویچ، مثل ذخیره کردن config فایل ها، تغییر نیم سویچ، show های بدرد بخور و... را انجام دهیم.
از حالت global می توانیم وارد 4 نوع interface یا پورت یا لاین سویچ شده و آن ها را تنظیم کنیم:

- پورت (لاین) های کنسول
- پورت (لاین) های vty
- پورت های ethernet (fa 0/1)
- vlan interface ها

دستور vlan 1 برای ورود به تنظیمات vlan است و درصورتی که vlan وجود نداشته باشد، آن را ساخته و سپس وارد تنظیمات آن می شود.
کاربرد آن به عنوان مثال تغییر نام vlan مورد نظر است:

```
name ACCOUNTING
```

مشاهده vlan ها به همراه نام آن ها و پورت های موجود در آن ها (در enable):

```
do show vlan brief
```

دستور interface vlan 1 برای ورود به vlan interface شماره 1 است.

Backup گرفتن از startup-config و running-config در TFTP سرور:
فرض می کنیم که IP آدرس TFTP سرور 192.168.1.100 است.
حال برای این که بتوانیم فایل های موجود در یک سویچ را به یک TFTP سرور کپی کنیم، باید به سویچ IP دهیم.
چگونه؟
توجه داشته باشید که interface های یک سویچ، لایه 2 ای هستند و به آن ها port می گویند و قابلیت IP گرفتن ندارند.
فرض کنید که در یک سویچ، دو VLAN با ID های 1 و 2 وجود دارد.
(VLAN شماره 1 به شکل پیشفرض در تمام سویچ ها وجود دارد و تمام port ها به شکل پیشفرض در آن قرار دارند)
در یک سویچ، 4 نوع interface یا پورت وجود دارد:

- پورت (لاین) های کنسول
- پورت (لاین) های vty
- پورت های ethernet
- vlan interface ها

از بین چهار interface بالا فقط vlan interface ها و vty ها مجازی اند.
نکته بسیار مهمی که باید به آن توجه کنید این است که (بر خلاف 3 پورت دیگر که لایه 2 ای اند)، vlan interface ها لایه 3 ای اند و قابلیت IP گرفتن دارند.
حال فرض می کنیم که TFTP سرور به یکی از پورت های موجود در VLAN شماره 1 سویچ متصل است. پس به VLAN interface شماره 1 یک IP می دهیم.
برای پیکربندی کردن VLAN interface شماره 1 به کمک دستور زیر وارد حالت interface config، VLAN interface شماره 1 می شویم:

```
enable
configure terminal
interface vlan 1
no shutdown
```

حال یک IP آدرس برای آن تعیین می کنیم:

```
ip address 192.168.1.10 255.255.255.0
```

(توصیه می شود همواره IP را به vlan شماره 1 دهیم زیرا نمی توان آن را پاک کرد)

حال به کمک دستور زیر مشاهده می کنیم که vlan interface شماره 1، up است و ip دارد (در enable):

```
do show ip interface brief
```

برای Backup گرفتن از دستور زیر استفاده می کنیم (در حالت global می زنیم):

```
copy running-config tftp://192.168.1.100/my-backup
copy startup-config tftp://192.168.1.100/my-backup
```

برای Restore کردن نیز از دستور زیر استفاده می کنیم (در حالت global می زنیم):

```
copy tftp://192.168.1.100/my-backup startup-config
```

az shabake 3

Sunday, December 20, 2020 4:25 PM

برای فعال کردن telnet در سویچ، مراحل زیر را دنبال می کنیم:

```
enable
configure terminal
line vty 0
login local
exec-timeout 10
```

توجه1: از user-pass های ساخته شده در مراحل قبل برای login کردن استفاده می شود.
یاداوری: تمام لاین های vty (0 تا 15) به شکل پیشفرض در حالت login قرار دارند. یعنی اگر یک پسورد برای پورت تعیین کرده باشیم، به کمک آن می توانیم به پورت مذکور، login کنیم.
به کمک دستور login local، لاین vty شماره 0 را به حالت login local تغییر دادیم. یعنی به هنگام login کردن به این پورت، باید یکی از user-pass های موجود در سویچ را وارد کنیم.

توجه2: در مراحل قبل یک IP برای vlan interface شماره 1 تعیین کردیم.
IP ای که برای vlan interface شماره 1 درنظر می گیریم باید از رنج IP کامپیوتر های موجود در همین vlan باشد
زیرا کامپیوتر های موجود در vlan شماره 2 نمی توانند به سویچ ssh بزنند مگر این که یک router وجود داشته باشد و یا این که سویچ پیشرفته باشد خودش عمل routing را انجام دهد (شکل زیر).

توجه3: دستور exec-timeout برای این است که اگر کاربر به مدت 10 دقیقه idle باشد، سیستم نشست را خاتمه دهد.
برای غیر غعال کردن آن از دستور no exec-timeout استفاده می کنیم.

توجه4: به شکل پیشفرض در سویچ ها، 2 لاین کنسول و 16 لاین vty وجود دارد که لاین (پورت) های vty مجازی اند و به شکل پیشفرض غیر فعال اند. در سناریوی بالا فقط لاین vty شماره 0 را فعال کردیم که فقط یک user به شکل هم زمان می تواند به آن متصل شود. در صورتی که بخواهیم چند user به شکل هم زمان به سویچ متصل شوند، لاین های vty بیشتری را فعال می کنیم.

حال telnet را به ssh تغییر می دهیم (در global):

```
hostname sw1
ip domain-name mylab.local
crypto key generate rsa
line vty 0
transport input ssh
```

همانطور که مشاهده کردید، در قدم اول یک fqdn برای سویچ تعیین کرده، سپس یک rsa key ساخته (برای finger print؟) و در نهایت وارد لاین 0 vty شده و ssh را فعال کردیم.

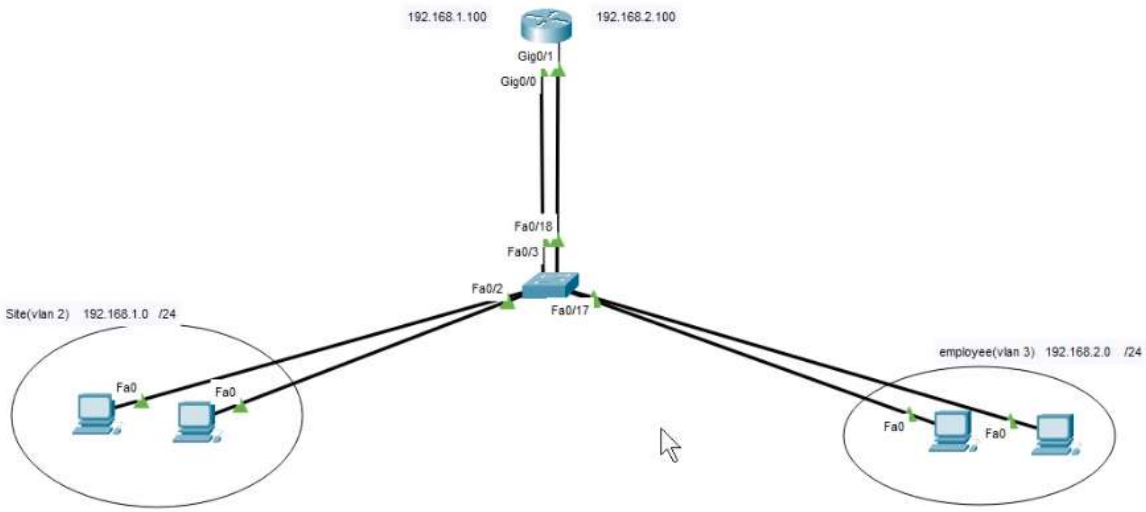
کلید ساخته شده را مشاهده می کنیم (در enable):

```
do show crypto key mypubkey rsa
```

یاداوری:برداشتن پسورد پورت کنسول و غیر فعال کردن login به کمک پسورد
(در حالت .Line config پورت کنسول 0 می زنیم):

```
no password
no login
```

```
-->
line vty 1 15
no login
(تست نشده)
```



az shabake 4

Sunday, December 27, 2020 4:36 PM

برای ساختن و منتقل کردن یک پورت به یک VLAN، مراحل زیر را دنبال می کنیم:
enable
configure terminal
interface fastEthernet 0/2

حال به کمک دستور زیر، interface انتخاب شده (در این مورد fast 0/2) را در VLAN (مثلا) 24 قرار می دهیم:
switchport access vlan 24
(بقیه interface ها در VLAN پیشفرض یا همان 1 باق می ماند)
(با وارد کردن دستور بالا، در صورتی که VLAN 24 وجود نداشته باشد، به شکل خودکار ساخته خواهد شد)

دستور vlan 1 برای ورود به تنظیمات vlan است و درصورتی که vlan وجود نداشته باشد، آن را ساخته و سپس وارد تنظیمات آن می شود.
کاربرد آن به عنوان مثال تغییر نام vlan مورد نظر است:
name ACCOUNTING

مشاهده vlan ها به همراه نام آن ها و پورت های موجود در آن ها (در enable):
do show vlan brief

دستور interface vlan 1 برای ورود به vlan interface شماره 1 است.

هدف از ساخت VLAN های مختلف، کوچک کردن broadcast domain و کاهش بار شبکه است.

برای عضو کردن تعدادی از پورت ها به شکل هم زمان در VLAN شماره 24 از دستورات زیر استفاده می کنیم:
interface range fastEthernet 0/1-9
switchport mode access
switchport access vlan 24
do wr
do show vlan brief

به کمک دستور switchport mode access، port mode پورت های انتخابی را از حالت پیشفرض dynamic به حالت access تغییر دادیم.
سوال: تفاوت port mode های dynamic، access و trunk در چیست؟
جواب در قسمت بعد.

az shabake 5

Saturday, October 10, 2020 7:17 PM

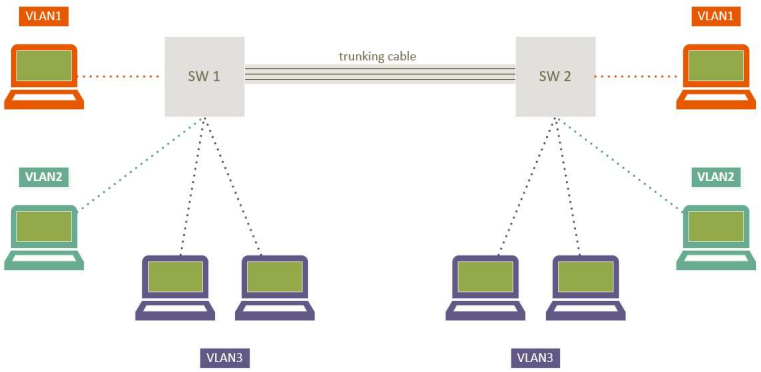
در حالت پیشفرض برای وصل کردن دو سویچ به یکدیگر تنها کافیست که یک از پورت های سویچ الف را به یک از پورت های سویچ ب متصل کنیم (ترجیحا پورت های Gig).
سوال: اگر تعدادی VLAN بر روی سویچ الف و تعدادی VLAN بر روی سویچ ب تعریف شده باشد، تکلیف چیست؟
جواب: فرق نمی کند. فقط در این گونه مواقع، trunking وارد عمل می شود.
عملکرد trunking بدین صورت است که وقتی یک سویچ می خواهد تعدادی frame را (از طریق trunking cable) به سویچ دیگر بفرستد، یک tag یا برچسب VLAN ID به frame ها اضافه می کند و وقتی frame مورد نظر به سویچ مقصد رسید، سویچ مقصد این tag را حذف کرده و حال می داند که frame متعلق به کدام VLAN است.

توجه1: پورت های یک سویچ می توانند دارای سه حالت access، trunk و dynamic باشند که به شکل پیشفرض در حالت dynamic قرار دارند.
کاربرد dynamic این است که اگر پورت به یک کامپیوتر وصل شود، به شکل خودکار در حالت access و اگر به یک سویچ وصل شود، به شکل خودکار در حالت trunk قرار می گیرد.

نکته1: trunking باید روی پورت های اتصال دهنده دو سویچ فعال شود (خودکار یا دستی) و protocol مورد استفاده برای trunking در هردو سویچ باید یکی باشد (ترجیحا 802.1q).

نکته2: trunking port موجود در یک سویچ به شکل پیشفرض عضو تمام VLAN های موجود در سویچ است.

نکته3: access port ها فقط می توانند عضو یک VLAN باشند.



برای مشاهده کردن trunking port ها یا همان trunking interface ها از دستور زیر استفاده می کنیم (در enable):
do show interface trunk

همچنین به کمک دستور زیر می توانیم hostname سویچ ها، کامپیوتر ها و پرینتر هایی که به سویچ ما متصل اند را مشاهده کنیم (در enable):
do show cdp neighbor
به عنوان مثال در تصویر زیر، سویچ SW2 به پورت Fas 0/2 سویچ ما متصل است و الی آخر:

```
Device ID       Local Intrfce
SW2             Fas 0/2
SW3             Fas 0/3
HOST_2          Fas 0/1
```

در صورتی که به تشخیص خودکار سویچ ها (تشخیص خودکار حالت access و یا trunk توسط حالت dynamic پورت ها)
علاقه ای نداشته باشیم و بخواهیم پورت مورد نظر (در این مورد gig 0/1) را به شکل دستی در حالت trunk قرار دهیم، مراحل زیر را دنبال می کنیم:
enable
configure terminal
interface gigabitEthernet 0/1

حال protocol مورد نظر برای trunking (در این مورد 802.1q) را انتخاب می کنیم:
(البته مقدار پیشفرض نیز همین است)
switchport trunk encapsulation dot1q

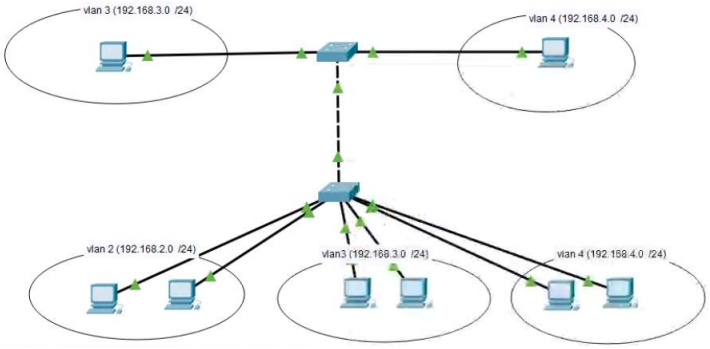
سپس gig 0/1 را از حالت dynamic به حالت trunk تغییر می دهیم.
بدین معنا که از این پورت فقط برای trunking می توان استفاده کرد:
switchport mode trunk

تا به اینجا gig 0/1 به شکل پیشفرض عوض تمام VLAN ها است و اجرا کردن دستور زیر optional است.
ولی در صورتی که بخواهیم gig 0/1 فقط عضو تعداد محدودی از VLAN ها باشد، می توانیم از دستور زیر استفاده کنیم:
switchport trunk allowed vlan 1,2,3,4
دستور بالا درواقع باعث می شود که فقط ترافیک VLAN های مشخص شده از سویچ خارج شوند و وقتی کاربرد دارد که به عنوان مثال VLAN شماره 5 در سویچ همسایه وجود نداشته باشد و ارسال کردن ترافیک های با برچسب VLAN ID شماره 5 به این سویچ بیهوده باشد.

همچنین می توانیم از دستور زیر استفاده کنیم:
switchport trunk allowed vlan except 6
یعنی gig 0/1 عضو تمام VLAN ها است بغیر از VLAN شماره 6

برای اطلاعات بیشتر:
switchport trunk allowed vlan ?

یاداوری:
برای مشاهده کردن trunking port ها یا همان trunking interface ها از دستور زیر استفاده می کنیم (در enable):
do show interface trunk



نیما احمدوند