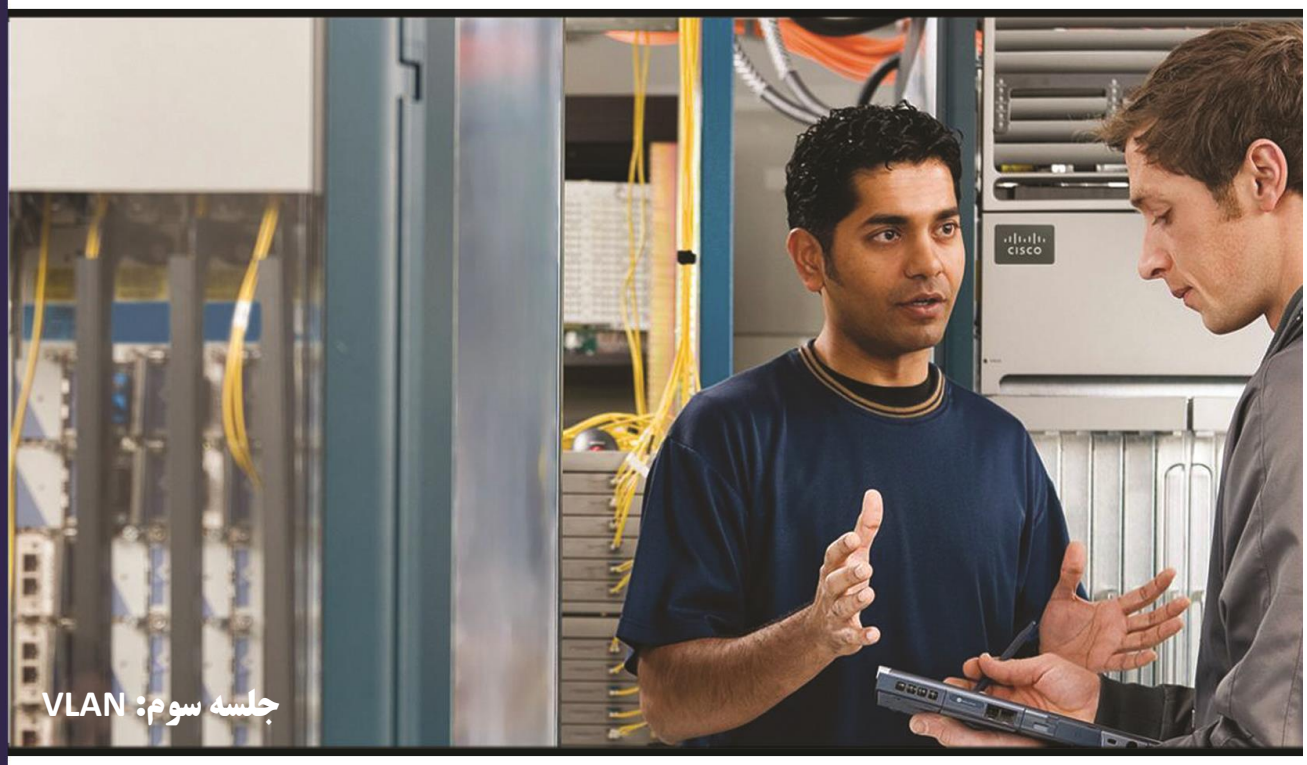
مبانی اولیه سیسکو

CCNA

CISCO CERTIFIED
CCNA
Security



جلسه سوم: VLAN

✔ آموزش کامل Routing & Switching

✔ به همراه سناریو

نویسنده: مهندس امیرحسین خالقی

فهرست

پیشگفتار

سپاس پروردگار را که این امکان را داد که تا باز بتوانیم مجموعه ای پر مطلب و پر فهم را کمتر از یک سال بنویسیم.

این کتاب با توجه به سرفصل های کتاب CCNA ICND 1 & ICND 2 برای علاقه مندان به شبکه و سیسکو نوشته شده است. در تهیه این کتاب سعی بر آن شده است تا فهم مطالب و مباحث به صورت روان و گیرا مطرح گردد.

در ابتدای کتاب سر فصل مطالب قید شده است. در انتهای هر فصل سناریویی طراحی شده که می تواند در فهم و یادگیری سریع تر شما کمک کند. توصیه می شود که این سناریو ها حتما کار شود. در انتهای کتاب به بررسی نمونه سوالات آزمون Cisco پرداخته ایم.

درصورت هرگونه مشکل در این کتاب میتوانید با ایمیل نویسنده (info@akhaleghi.ir) تماس حاصل فرمایید تا با بررسی آن بتوانیم کتابی کامل و با زبان فارسی در اختیار شما دوستان و همکاران ارجمند قرار دهیم.

در پایان از تمامی عزیزانی که ما را در تهیه و تنظیم این کتاب یاری نموده اند کمال تشکر را داریم.

باشد که موثر باشیم ....

امیرحسین خالقی

فصل سوم : Vlan

Vlan که مخفف شده ی عبارت Virtual Lan می باشد یکی از جدیدترین و جالبترین تکنولوژی های شبکه است که اخیرا مورد توجه بیشتری قرار گرفته است. رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گران قیمت بدون از دست دادن کارایی و امنیت ، اهمیت و ضرورت توجه بیشتر به VLANرا مضاعف نموده است.

به منظور ایجاد VLAN، به یک سوئیچ لایه دو که این تکنولوژی را حمایت نماید ، نیاز می باشد . تعدادی زیادی از افرادیکه جدیدا با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفا می بایست به منظور فعال نمودن VLAN ، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند . (برداشتی کاملا" اشتباه !) . با توجه به این که در شبکه های VLAN، میلیون ها محاسبات ریاضی انجام می شود ، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است ، استفاده گردد (دقت در زمان تهیه یک سوئیچ)، در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده ، وجود نخواهد داشت .

هر VLAN که بر روی سوئیچ ایجاد می گردد ، به منزله یک شبکه مجزا می باشد . بدین ترتیب برای هر VLAN موجود یک Broadcast domain جداگانه ایجاد می گردد. پیام های Broadcast ، به صورت پیش فرض ، از روی تمامی پورت هائی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند . ویژگی فوق ، یکی از مهمترین دلایل متداول شدن VLAN در شبکه های بزرگ امروزی است.

- **دستورات Vlan**

در خط اول ما دستور Vlan را فراخوانی کرده و Vlan 2 را ساخته ایم. اگر ؟ بگیریم میبینیم که میتوانیم برای این Vlan نام بگذاریم و یا آن را پاک کنیم.

```
amirSW(config)#vlan 2
amirSW(config-vlan)#?
VLAN configuration commands:
  exit  Apply changes, bump revision number, and exit mode
  name  Ascii name of the VLAN
  no    Negate a command or set its defaults
amirSW(config-vlan)#exit
amirSW(config)#interface fastEthernet 0/1
amirSW(config-if)#switchport access vlan 2
```

سپس با استفاده از دستور آخر interface 1 را عضو Vlan 2 کرده ایم.

در حالت کلی Port های ما بصورت زیر می باشد:

Access, Trunk, Dynamic Auto, Dynamic Desirable

جدول آن بصورت زیر می باشد:

❊	A	T	DD	DA
A	A	A	A	A
T	A	T	T	T
DD	A	T	T	T
DA	A	T	T	A

به طور کلی Trunk یعنی اجازه ی عبور را به همه بده و Access یعنی اجازه عبور را فقط به یک نفر بده!

نکته : Port بین سوییچ ها همیشه باید Trunk باشد و Port بین سوییچ و PC باید Access باشد.

برای تغییر وضعیت پورت ها ابتدا وارد آن پورت شده و مانند زیر عمل میکنیم:

```
amirSW(config)#interface fastEthernet 0/1
amirSW(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
amirSW(config-if)#switchport mode trunk
```

برای مشاهده ی وضعیت Port ها میتوان از Command زیر استفاده کرد:

```
amirSW(config-if)#do 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, Gig1/1
                                                Gig1/2
2    VLAN0002                         active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
amirSW(config-if)#
```

همانطور که مشاهده میکنید ما پورت ۰/۱ را عضو VLan2 کرده ایم.

نکته: تمامی Port ها به صورت Default عضو Vlan1 هستند

همچنین می توان از Command های ، Show interface Trunk و نیز Show running-config برای دیدن interface های Trunk استفاده کرد.

نکته: برای دیدن ادامه (more) میتوان هم از Enter به صورت سطری و از Space به صورت ستونی استفاده کرد.

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

Current configuration : 1020 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
 --More-- |
```

برای اینکه محدوده ای از Port ها رو انتخاب کنیم (مثلا از پورت ۱ تا ۵ را میخواهیم تا اعمال مشابهی مثل عضو کردن همه آنها در یک Vlan بر روی آنها اعمال کنیم) میتوانیم از Command زیر استفاده کنیم :

```
amirSW(config)#interface range fastEthernet 0/1 -5
amirSW(config-if-range)#
```

نکته : برای خاموش و یا روشن کردن Port های سوییچ و روتر (تمامی روتر ها به صورت Default ، Port هایشان خاموش است) بصورت زیر عمل می کنیم:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#sh
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively do
wn
Switch(config-if)#no sh
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
Switch(config-if)#
```

همچنین برای امنیت بیشتر میتوانیم پورت هایی که خالی هستند را خاموش کرده و یک Vlan جدا درست کنیم و آنها را عضو آن کنیم.

- **Native Vlan**

مفهوم Native Vlan در شرایطی معنا پیدا میکند که پورت در حالت Trunk باشد و از پروتکل 802.1Q استفاده کند. بر اساس تعریفی که ما از Vlan و dot1q در Trunkداریم پکت هایی که در یک لینک trunk منتقل میشوند دارای tag با شماره Vlan مربوطه هستند. حال در صورتی که یک پکت به صورت بدون تگ از یک لینک خارج شود و یا به سوییچ سمت مقابل برسد آن پکت را سوییچ به درون یک Vlan که به نام Native Vlan می گویند فرستاده و به صورت پیش فرض در Vlan شماره ۱ قرار میدهد.

به معنای دیگر در صورتی که Native Vlan بر روی یک پورت به صورت مثال پورت ۱ تعریف شده باشد در صورتی که پکتی از آن پورت وارد سوییچ شود و دارای tag مربوط به Vlan ها نباشد آن را جزو پکتهای مربوط به Vlan 1 در عملیات سوییچینگ به حساب میاورد.

اگر Native VLAN در دو سمت ترانک بین دو سوییچ متفاوت تنظیم شده باشد، CDP آنرا کشف و گزارش می کند. CDP پروتکل سیسکو است که بین دستگاه های سیسکو ارتباط برقرار کرده و همسایگان را به هم معرفی می کند.

در زیر از دستور اول جهت تنظیم Native VLAN روی یک لینک ترانک استفاده می شود و از دستور دوم روی ترانک جهت اجازه عبور یا جلوگیری از عبور ترافیک یک یا چند VLAN خاص، می توان استفاده کرد:

```
amirSW(config)#interface fastEthernet 0/1
amirSW(config-if)#switchport trunk native vlan 1005
amirSW(config-if)#switchport trunk allowed vlan 1-3
```

دستور بالا روی ترانک فوق تنها VLAN ۱ تا ۳ را اجازه می دهد.

می توان VLAN 1 را روی ترانک Disable یا غیر فعال کرد، اما ترافیک CDP, Spanning Tree و VTP بصورت خودکار روی VLAN1 به هر حال عبور خواهد کرد (چه بخواهید یا نخواهید) این عملکرد را VLAN1 Minimization می گویند.

نکته : توصیه می شود جهت بالا بردن امنیت از VLAN1 برای هیچ ترافیکی در شبکه استفاده نکنید. (پورتی را در این VLAN قرار ندهید.)

Vtp -

وقتی شما از Vlan در شبکه تان استفاده می کنید ، می بایست Vlanها را روی تک تک سوئیچ ها تعریف نمایید. حال حساب کنید که شما یک شبکه بزرگ دارید با چندین Vlan و چندین سوئیچ ...

تعریف این همه Vlan روی این همه سوئیچ بسیار زمان بر است .حال به فرض که شما این کار را انجام دادید چند وقت بعد یه بخش دیگه در شرکت ایجاد میشود و این یعنی یک Vlan جدید لازم دارید و مجدد باید این Vlan جدید رو روی تک تک سوئیچ ها تعریف کنید ....

پروتکل Vtp کار شما را راحت کرده است ، بدین صورت که شما روی همه سوئیچ ها پروتکل Vtp رو فعال می کنید. سپس یکی از سوئیچ ها را بعنوان Vtp server تنظیم می کنید و بقیه سوئیچ ها را بعنوان Vtp client . بعد فقط کافی است که Vlan ها را فقط روی سوئیچی که Vtp server است تعریف کنید. پروتکل Vtp کلیه اطلاعات را به بقیه سوئیچ ها منتقل می کند.

```
amirSW(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
amirSW(config)#vtp domain AMkhaleghi
Changing VTP domain name from NULL to AMkhaleghi
amirSW(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
amirSW(config)#vtp password ?
  WORD  The ascii password for the VTP administrative domain.
amirSW(config)#vtp password 123
Setting device VLAN database password to 123
amirSW(config)#vtp version ?
  <1-2>  Set the adminstrative domain VTP version number
amirSW(config)#vtp version 2
amirSW(config)#
```

نکته : شرط Vtp ، Trunk بودن بین سوییچ ها می باشد.

Vtp Domain همان نام Domain است. Vtp Mode اگر Server باشد هم اطلاعات میگیرد و هم اطلاعات می دهد اگر Client باشد یعنی فقط اطلاعات می دهد و اگر transparent باشد یعنی اطلاعات را عبور میدهد اما روی خود تاثیری ندارد.

Vtp Password اگر پسورد بگذاریم بر روی هر یک از سوییچ ها باید پسورد بدهیم تا اطلاعات وارد شود. (برای امنیت آن این کار را باید انجام دهیم).
Vtp Version ورژن آن ۲ است.

میتوان با Command زیر اطلاعات Vtp را مشاهده کرد:

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : Cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE8 0x6F 0x31 0xAA 0xE5 0xAB 0xC5 0xDB
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:30
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#show vtp password
VTP Password: 123
```

نکته: چگونه Vlan ها و Vtp ها را پاک کنیم؟!!!

Vlan ها درون فایلی به نام Vlan.dat درون فلش ذخیره شده اند. اطلاعات Vtp هم در آنجا می باشد! راهکار برای پاک کردن آن:

ابتدا پورتهای سوییچ که به سوییچ متصل است را قطع کنید (چون اگر Vtp داشته باشید دوباره Vlan ها بر میگردد!) سپس در تمامی سوییچ ها فایل Vlan.dat را از درون فلش به طریقه زیر پاک کرده و Reload می کنیم:

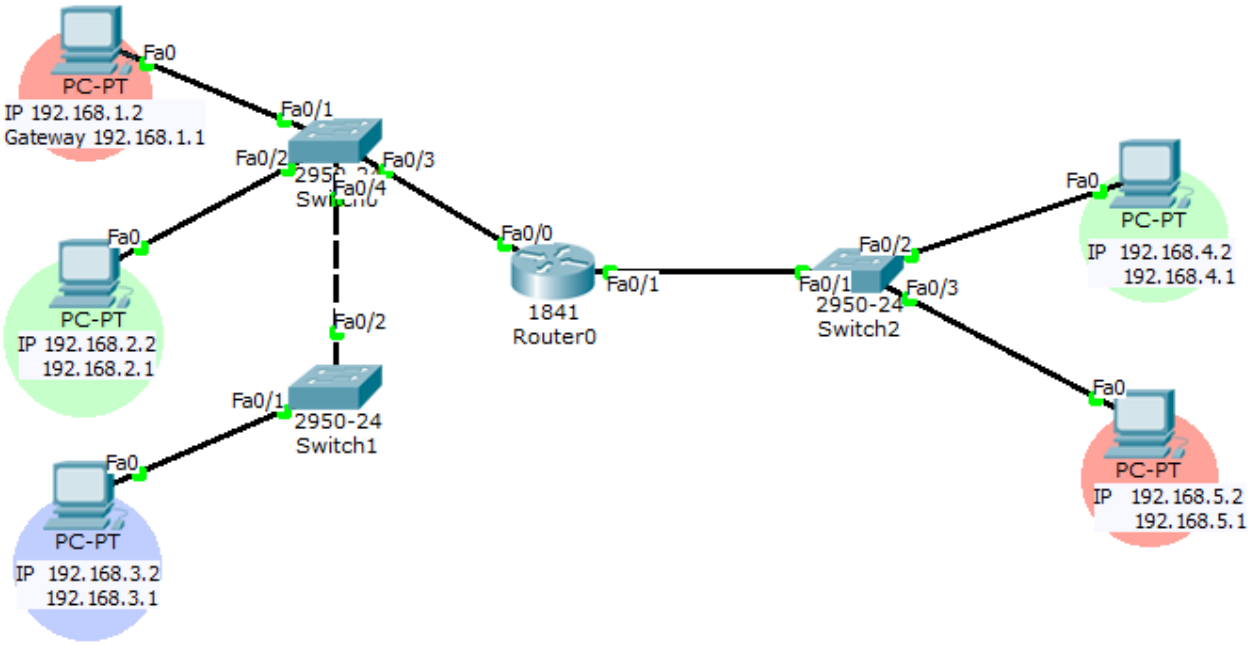
```
Switch#show flash:
Directory of flash:/

    1  -rw-     3058048          <no date>  c2950-i6q412-mz.121-22.EA4.bin
    2  -rw-         556          <no date>  vlan.dat

64016384 bytes total (60957780 bytes free)
Switch#del
Switch#delete fl
Switch#delete flash:
Delete filename []?vlan.dat
Delete flash:/vlan.dat? [confirm]
```

سپس تمامی Vlan ها درون یک سوییچ که Server هست میسازیم و پورتها را متصل کرده و Trunk می کنیم.

سناریو :



شکل فوق را در نرم افزار Cisco Packet Tracer پیاده سازی کنید و عملیات زیر را بر روی آن انجام دهید.

۱- Ip و Default Gateway ها را بر روی سیستم ها Set کنید.

۲- بین سوییچ ۰ و ۱ Vtpبرقرار کنید.

۳- Vlan ها را بسازید. (سه Vlan باید بسازیم)

۴- Port های متصل به روتر را Trunk کنید.

۵- بر روی روتر Inter Vlan Routing راه اندازی کنید.

Ping کنید. تمای PC های شبکه باید Ping هم را داشته باشند در غیر اینصورت مراحل فوق را به دقت بررسی کنید