

به نام خدا



آزمایشگاه شبکه و امنیت

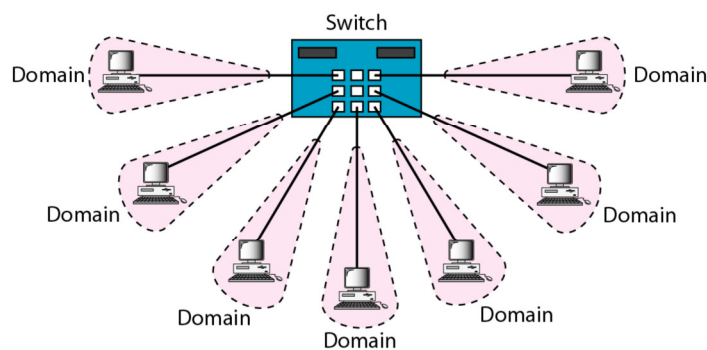
آشنایی با سویچ های سیسکو



گردآوری و تنظیم: سید علی سنایی

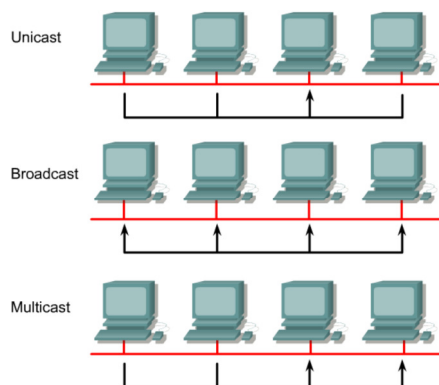
با نظارت دکتر علی فانیان

سوییچ یک تجهیز لایه دو است که وظیفه هدایت فریم های Ethernet را برعهده دارد. سوییچ ها بر خلاف هاب با محدود کردن ناحیه تصادم بین میزبان و پورت سوییچ، کارایی شبکه را بالاتر می‌برند. از سوی دیگر سوییچ امکان مدیریت قوی‌تر بر روی فریم‌ها و ایزوله کردن ترافیک بین قسمت های مختلف یک شبکه از یکدیگر را فراهم می‌سازد.



اگر چه سوییچ سبب کوچک سازی نواحی تصادم می‌گردد اما همچنان همه میزبان ها در یک ناحیه همه پخشى قرار دارند. به هر حال انواع ارسال در یک شبکه اترنت توسط سوییچ پشتیبانی می‌شود.

- تک پخشى (Unicast): ارتباط بین مبدا و یک مقصد مشخص
- چند پخشى (Multicast): ارتباط بین مبدا و چند مقصد مشخص
- همه پخشى (Broadcast): ارتباط بین مبدا و همه آدرس مقصد های قابل دسترسی



ارتباط بر روی لینک اترنت به دو صورت انجام می گیرد

❖ Half Duplex: ارتباط یکطرفه است به این معنا که به صورت همزمان دریافت و ارسال انجام نمی گیرد. به منظور

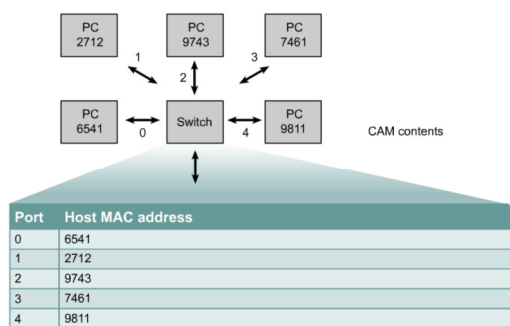
مدیریت تصادم از CSMA/CD استفاده می شود.

❖ Full Duplex: ارتباط دو طرفه است. داده به صورت هم زمان می تواند ارسال و دریافت شود. بازده این روش بالاتر

است.

سوییچ با استفاده از جدول آدرس های MAC، فریم های مربوط به مقصد مشخص را به سمت پورت مربوطه

هدایت می کند.



وظایف اساسی یک سوییچ را می توان به صورت زیر خلاصه کرد:

- هدایت فریم
- فیلتر کردن فریم
- یادگیری آدرس های MAC
- اجتناب از ایجاد loop با استفاده از STP

هدایت و فیلتر کردن فریم ها:

سوییچ آدرس MAC مقصد را بررسی می کند

❖ اگر آدرس مقصد همه پخش، چند پخش و یا تک پخش ناشناس باشد. فریم را بر روی همه پورت ها

به جز پورتی که از آن فریم را دریافت کرده است، ارسال می کند.

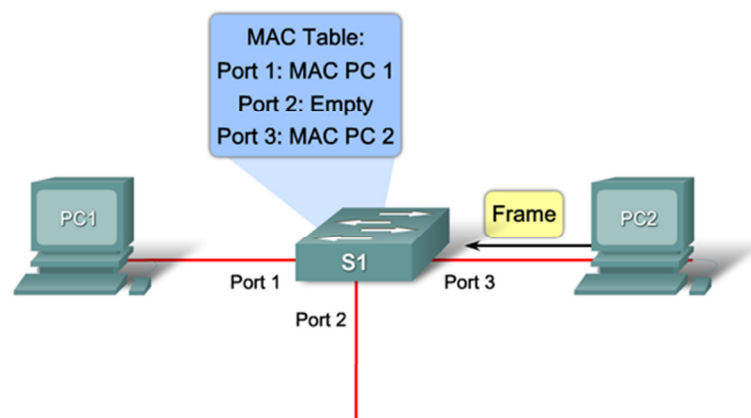
❖ اگر آدرس مقصد یک آدرس تک پخش شناخته شده باشد.

- اگر آدرس مقصد با آدرس مبدأ متفاوت باشد، فریم به سمت پورت مربوطه هدایت می‌شود.
- اگر آدرس مقصد با آدرس مبدأ یکسان بود، فریم فیلتر شده و هدایت نمی‌گردد.

یادگیری آدرس MAC

سوییچ آدرس مبدأ و پورتهای که فریم را دریافت کرده است را چک می‌کند.

- ❖ اگر این آدرس قبلاً در جدول آدرس‌های MAC موجود نبود، این آدرس را و پورتهای که از آن، این آدرس را یاد گرفته است. در جدول قرار می‌دهد و تایمر آن را بر روی صفر قرار می‌دهد.
- ❖ اگر آدرس در جدول موجود باشد، تایمر آن را صفر می‌کند.



Managing MAC Address Table

```
switch#show mac-address-table
```

Mac Address Table

Vlan	Mac Address	Type	Ports
1	000c.7671.7534	DYNAMIC	Fa0/2
1	0013.e809.7695	DYNAMIC	Fa0/2
1	0017.9a51.d339	DYNAMIC	Fa0/2
1	0019.5b0a.a951	DYNAMIC	Fa0/2
1	0060.b0af.7be4	DYNAMIC	Fa0/2

Total Mac Addresses for this criterion: 5

`mac-address-table static <MAC address> vlan {1-4096, ALL} interface interface-id`

اجتناب از ایجاد loop با استفاده از STP

سوییچ با استفاده از STP و مسدود کردن برخی از پورت ها مانع از ایجاد دور در شبکه می گردد.

? سوال 1: نحوه عملکرد STP در سوییچ به چه صورتی است؟

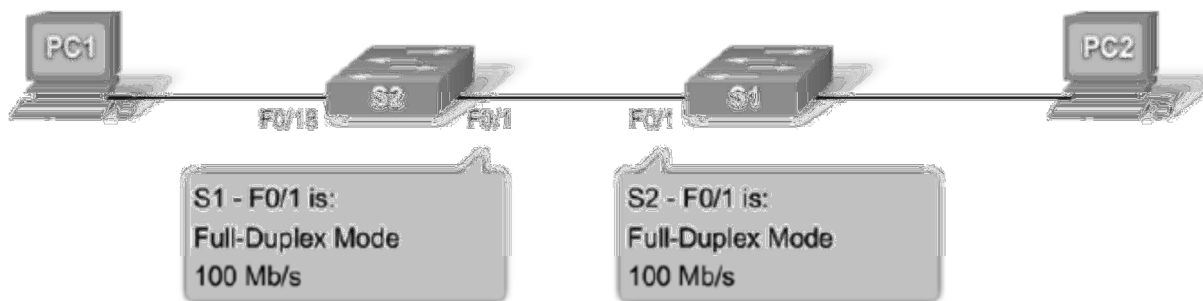
روشای هدایت فریم

❖ Store-and-forward: کل فریم را دریافت می کند و پس از آن، ارسال می کند. (سرعت پایین ولی دقت بیشتر)

❖ Cut-through: بخشی از فریم که دریافت شد شروع به ارسال می کند. (سرعت بالاتر ولی دقت کمتر)

? سوال 2: سوییچ لایه سه چیست؟

پیکربندی سوییچ



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#configure terminal
Enter the interface configuration mode.	S1(config)#Interface fastethernet 0/1
Configure the interface duplex mode to enable AUTO duplex configuration	S1(config-if)#duplex auto
Configure the interface duplex speed and enable AUTO-speed configuration.	S1(config-if)#speed auto
Return to privileged EXEC mode.	S1(config-if)#end
Save the running configuration to the switch start-up configuration.	S1#copy running-config startup-config

با استفاده از دستور زیر می توان دسته ای از اینترفیس ها را پیکربندی کرد.

```
#configure terminal
```

```
(switch-config)#interface range fastEthernet 0/1-10
```

با استفاده از دستورات زیر می توان تنظیمات سویچ را بررسی کرد.

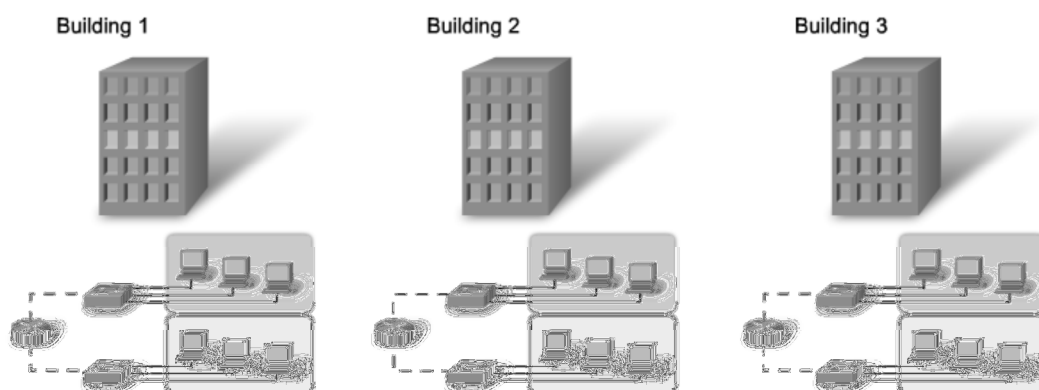
Cisco IOS CLI Command Syntax	
Displays interface status and configuration for a single or all interfaces available on the switch.	<code>show interfaces [interface-id]</code>
Displays contents of startup configuration.	<code>show startup-config</code>
Displays current operating configuration.	<code>show running-config</code>
Displays information about flash file system.	<code>show flash</code>
Displays system hardware and software status.	<code>show version</code>
Displays the MAC learning table.	<code>show mac-address-table</code>

سوال 3: چند نمونه از حملات امنیتی به سویچ را بیان و راه های مقابله با آنها را معرفی کنید؟

شبکه های محلی مجازی (VLAN)

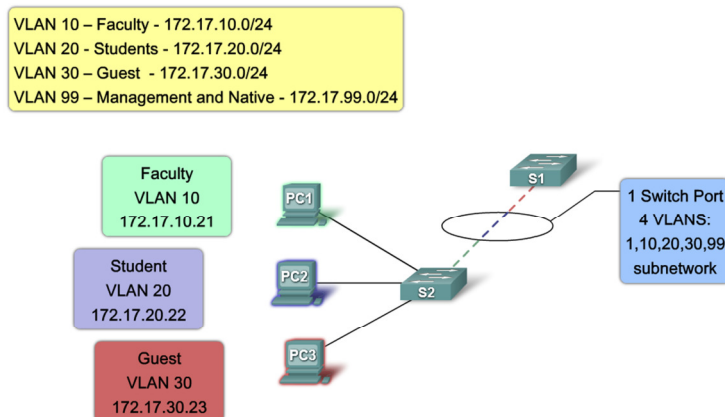
شبکه های محلی مجازی این امکان را برای مدیر شبکه فراهم می سازند که گروه بندی های مختلفی بین دیوایس های مختلفی که از یک زیرساخت مشترک استفاده می کنند، ایجاد کند. بنابراین می توان میزبان های مختلفی که متصل به یک سویچ هستند را به چندین قسمت گوناگون بر اساس کاربرد و یا سطح دسترسی تقسیم نمود. VLAN محسنات زیر را در شبکه ایجاد می کند:

- امنیت
- صرفه جویی در هزینه
- کارایی بالاتر
- مدیریت ساده تر و باکیفیت تر شبکه



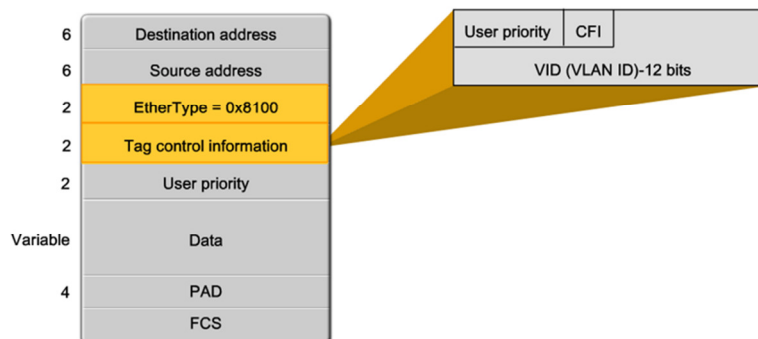
Ethernet Trunk

ترافیک چندین VLAN را از یک خط عبور می دهد.



IEEE 802.1Q

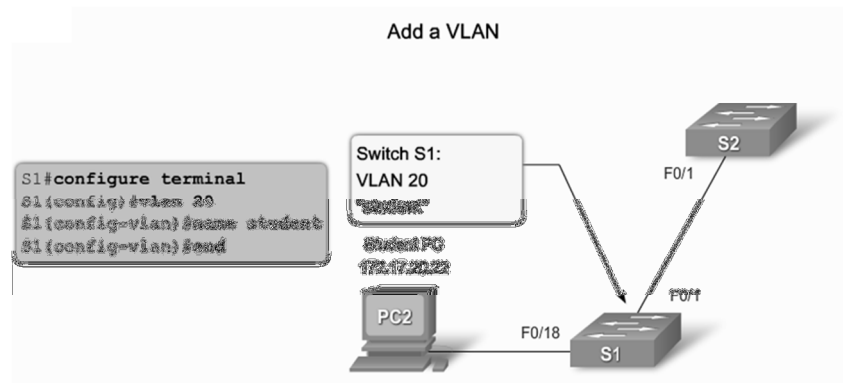
به منظور مشخص نمودن آنکه فریم ارسالی که از روی لینک ترانک عبور می کند، از سوی کدام VLAN است یک tag به فریم اضافه می گردد. این جاگذاری tag بر مبنای استاندارد IEEE 802.1Q انجام می گیرد.



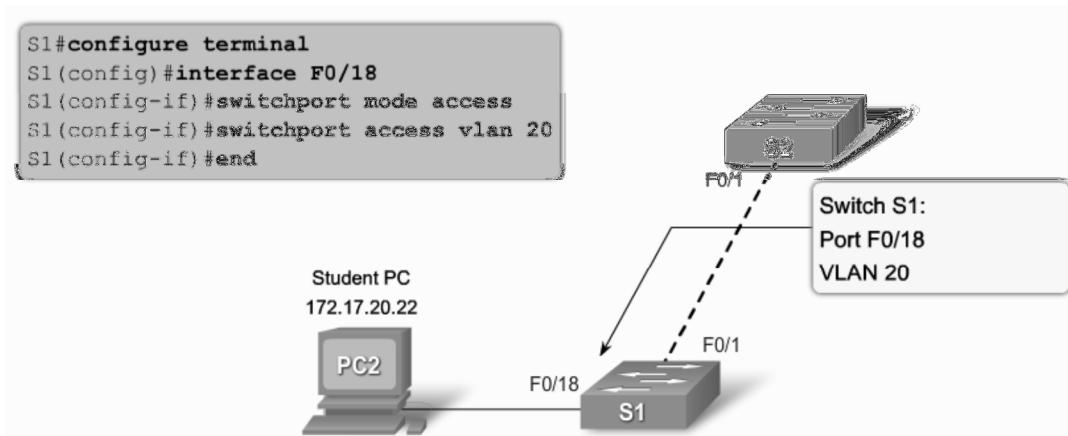
مراحل تنظیم VLAN و Trunk

1. ایجاد VLAN
2. تخصیص پورت های سویچ به VLAN ها به صورت استاتیک
3. بررسی پیکربندی VLAN
4. فعال کردن ترانک بر روی اتصالات بین سویچ ها
5. بررسی پیکربندی ترانک

1. ایجاد VLAN



2. تخصیص پورت‌های سویچ به VLAN ها به صورت استاتیک



3. بررسی پیکربندی VLAN

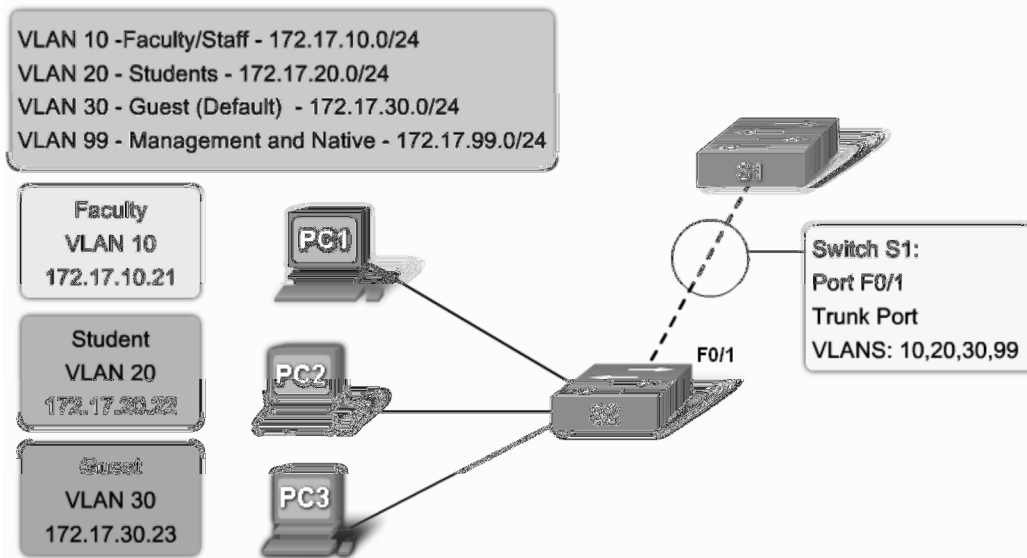
```

S1#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, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
20	student	active	Fa0/18
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

S1#

4. فعال کردن ترانک بر روی اتصالات بین سویچ ها



```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan add 10,20,30
S1(config-if)#end
```

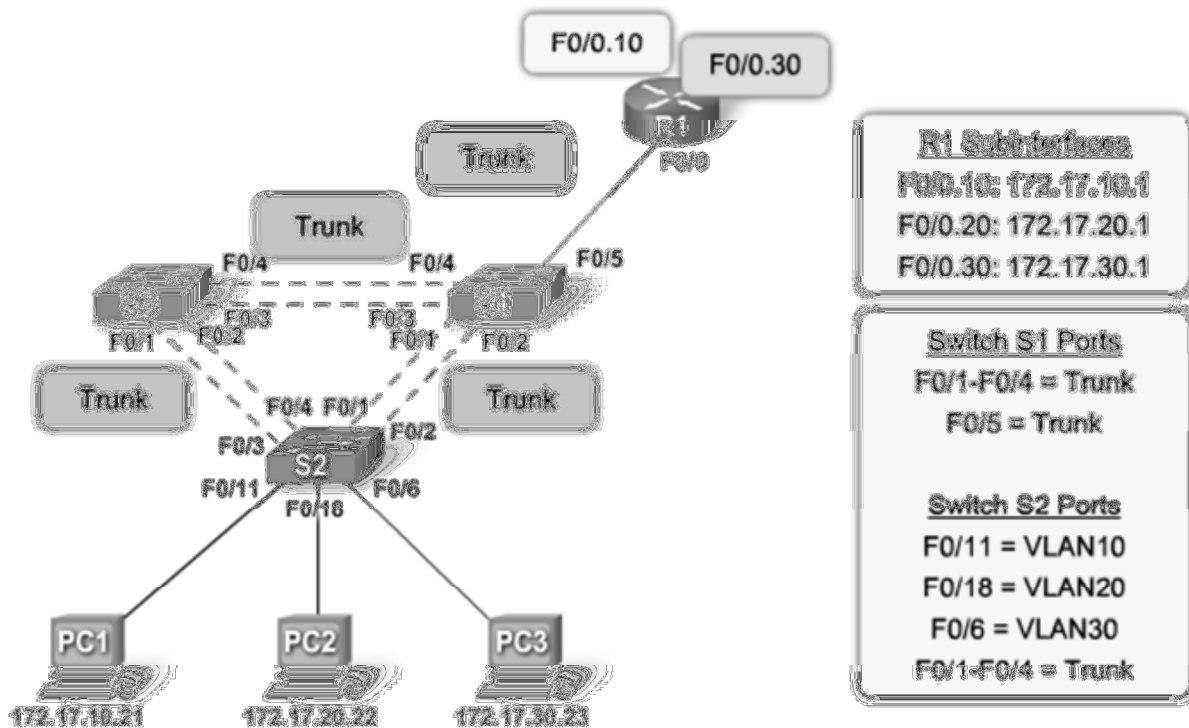
#show interfaces trunk

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
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: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

--More--
```

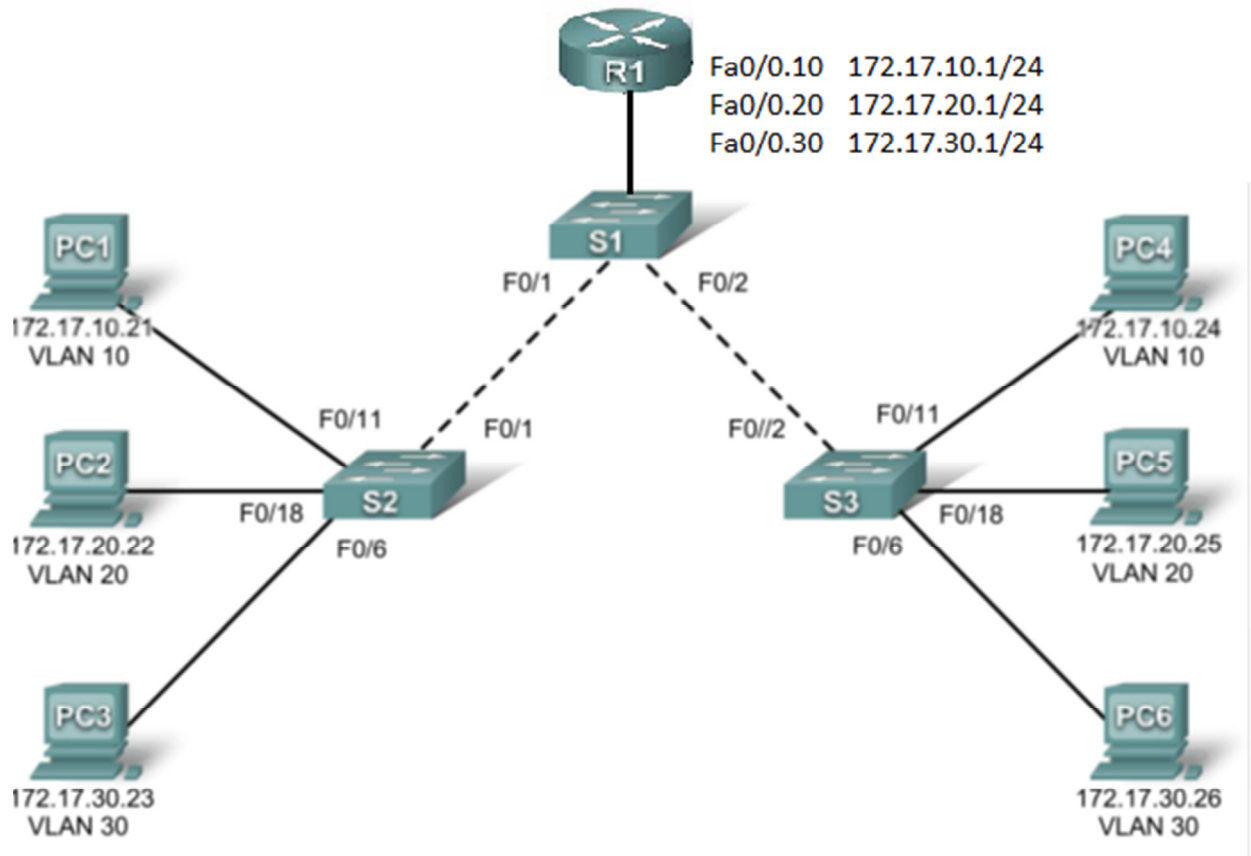
مسیریابی بین شبکه های محلی مجازی

به دلیل آنکه هر یک از VLAN ها زیر شبکه خاص خود را دارند. میزبان های بر روی VLAN های مختلف به یکدیگر دسترسی ندارند. بدین منظور بایستی با استفاده از یک مسیریاب، مسیریابی بین شبکه های محلی مجازی فراهم گردد. بدین منظور بایستی inter-vlan-routing بر روی مسیریاب به صورت زیر پیکربندی گردد.



```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface f0/0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
R1(config-if)#end
R1#
```

دستور کار آزمایش



1. سناریوی فوق را ببندید. (آدرس IP همه کامپیوترها را روی شبکه 172.17.10.0 /24 قرار دهید)
2. سویچ ها را نام گذاری کنید.
3. اطلاعات پیش فرض سویچ را با دستورات مناسب بررسی کنید.
4. آیا کامپیوترها به یکدیگر دسترسی دارند؟ چرا؟
5. اکنون آدرس های IP کامپیوترها را مانند شکل تنظیم کنید.
6. VLAN های نشان داده شده را ایجاد کنید.
7. وضعیت VLAN ها را بررسی کنید.

8. پورت های Truck را فعال کنید

9. آیا کامپیوترها به یکدیگر دسترسی دارند؟ کدام کامپیوترها به یکدیگر دسترسی دارند؟ چرا؟

10. مسیریابی بین VLAN ها را بر روی مسیریاب تنظیم کنید.

11. آیا همه کامپیوترها به یکدیگر دسترسی دارند؟

12. جدول آدرس های MAC را بررسی کنید.