آزمایشگاه شبکه های کامپیوتری

مدرس استاد مجید اسدپور

نویسنده مهدی گران

سناریو اول

۰-عنوان : عملکرد پروتکل Arp

۱- خلاصه: در این آزمایش به نحوه عملکرد پروتکل Arp و کاربرد آن در بدست آوردن Mac address نودهای موجود در شبکه خواهیم پرداخت .

	Time	Source	Destination	Protocol	Length	Info
25	24.8799500	Vmware_c0:00:08	Broadcast	ARP	42	who has 192.168.1.15? Tell 192.168.1.12
26	24.8805090	Vmware_de:33:b6	Vmware_c0:00:08	ARP	42	192.168.1.15 is at 00:0c:29:de:33:b6
28	24.8813820	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.12? Tell 192.168.1.15
29	24.8814400	Vmware_c0:00:08	Vmware_de:33:b6	ARP	42	192.168.1.12 is at 00:50:56:c0:00:08
40	28.9759160	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
41	29.5625620	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
42	30.5616040	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
43	31.9791890	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
44	32.5617420	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
45	33.5618620	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
46	37.9798210	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
47	38.5623240	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
48	39.5624460	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
49	50.9868210	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
50	51.5629010	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15
51	52.5618710	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.15

شکل ۰-۱

۲- توضیح : هدف از این سناریو آشنایی با عملکرد پروتکل Arp است. برای آنکه یک فریم از فرستنده بدست گیرنده ای در همان شبکه محلی برسد ، باید علاوه بر داشتن Ip مقصد ، آدرس Mac مقصد را نیز داشته باشیم. وظیفه پروتکل Arp بدست آوردن آدرس Mac مقصد با استفاده از آدرس Ip آن است.

۲-۱-نحوه عملکرد Arp : هنگامی که فرستنده آدرس Mac مقصد را نداشته باشد ، پروتکل Arp یک فریم با آدرس Ip مقصد و آدرس Mac،FFFF.FFFF.FFFF را به کل شبکه Broadcast می کند.

هر نود در شبکه ، پس از دریافت این بسته ، آدرس Ip مقصد آن را با آدرس Ip خودش مقایسه می کند اگر برابر بود ، یک فریم Arp reply به آدرس Ip و Mac فرستنده می فرستد و همچنین در این بسته Mac خود را نیز قرار می دهد.فرستنده با دریافت فریم ، آدرس Mac موجود در آن را در جدولی قرار می دهد تا در مراجعات بعدی نیاز به تکرار مراحل Arp نباشد .

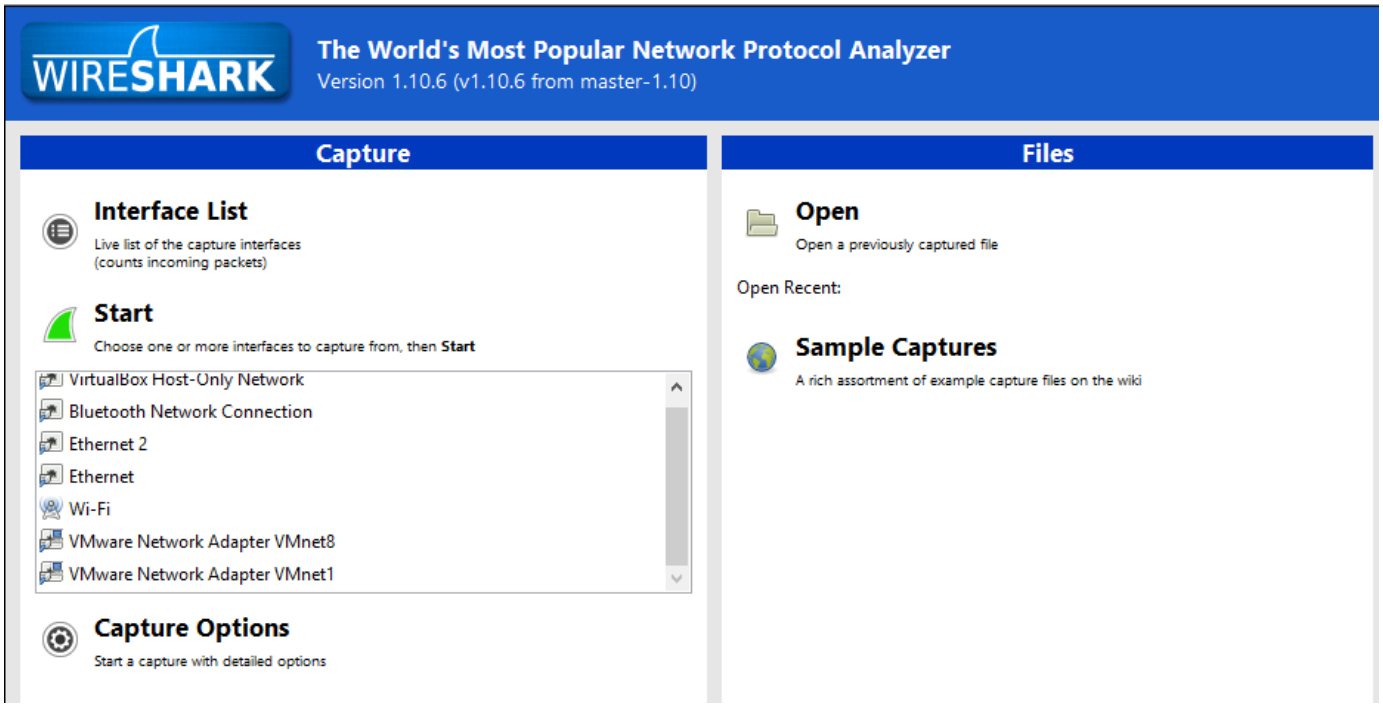
نکته ۱: برای اجرای پروتکل Arp نیاز به هیچگونه پیکربندی در سویچ و سیستم های انتهایی نیست و هرگاه که نیاز به بدست آوردن آدرس Mac سیستمی در شبکه باشد این پروتکل بطور اتوماتیک اجرا می شود.

نکته ۲: در یک کامپیوتر آدرسهای Mac نودهایی که به آنها فریم ارسال شده در جدولی به نام Arp Cache در حافظه Ram نگهداری می شود ، این بدان معناست که با هربار خاموش کردن سیستم این جدول پاک خواهد شد ، همچنین در زمان روشن بودن سیستم نیز ، این جدول بصورت پریودیک پاک خواهد شد که این زمان در سیستم عاملهای مختلف و Device های مختلف متفاوت است.در سیستم عامل ویندوز برای مشاهده این جدول از فرمان Arp –a استفاده می کنیم. برای آگاهی بیشتر از کلیه پارامترهای دستور Arp می توانید به لینک زیر مراجعه کنید.یا اینکه با تایپ arp راهنمای کامل پارامترهای این دستور را مشاهده کنید.

http://technet.microsoft.com/en-us/library/cc786759(v=ws.10).aspx

برای درک بهتر Arp ، این پروتکل را در نرم افزار WireShark مورد بررسی قرار خواهیم داد . که مراحل انجام سناریو به شرح زیر است :

۱- مطابق شکل ۱-۱ در صفحه اول برنامه WireShark ، لیست اینترفیس های سیستم خود را مشاهده خواهید کرد .اینترفیسی را که از طریق آن به شبکه Lan خود متصل هستید انتخاب کنید . اگر به یک شبکه Lan واقعی دسترسی ندارید ، می توانید اینترفیس VirtualMachine خود را نیز انتخاب کنید.در شکل ۱-۱ اینترفیس های VMnet8 و Vmnet1 و VirtualBox Host-Only Network مربوط به VirtualMachine ها هستند .



شکل ۱-۱

پس از انتخاب اینترفیس مورد نظر برروی دکمه استارت کلیک کنید.

۲- در Command Prompt فرمان ping را به شکل زیر وارد کنید .

Ping DestinationIpAddress

آی پی سیستم مورد نظر را جایگزین DestinationIpAddress در دستور کنید.

```
C:\Windows\system32>ping 192.168.1.15

Pinging 192.168.1.15 with 32 bytes of data:
Reply from 192.168.1.98: Destination host unreachable.
Reply from 192.168.1.11: Destination host unreachable.
Reply from 192.168.1.15: bytes=32 time=2ms TTL=128
Reply from 192.168.1.15: bytes=32 time<1ms TTL=128
```

شکل ۲-۱

همانطور که در شکل ۲-۱ مشاهده می کنید در دو خط اول پاسخ ping مقصد unreachable اعلام شد ، چرا که Mac مقصد در Arp chach سیستم موجود نبود اما در همین زمان پروتکل arp وارد عمل شده و Mac مقصد را بدست آورده و جدول Arp chach سیستم ، بروز رسانی شد. بگونه ای که در دو خط بعدی مشاهده می کنید بسته به دست مقصد رسیده است .

۳-به برنامه WireShark بازگردید ، همانگونه که در شکل ۳-۱ مشاهده می کنید در قسمت Filter ، Arp را تایپ کرده و Enter را بزنید .

Filter: arp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
76	132.461156	Vmware_c0:00:08	Broadcast	ARP	42	who has 192.168.1.15? Tell 192.168.1.12
77	132.461717	Vmware_de:33:b6	Vmware_c0:00:08	ARP	42	192.168.1.15 is at 00:0c:29:de:33:b6
79	132.462623	Vmware_de:33:b6	Broadcast	ARP	42	who has 192.168.1.12? Tell 192.168.1.15
80	132.462686	Vmware_c0:00:08	Vmware_de:33:b6	ARP	42	192.168.1.12 is at 00:50:56:c0:00:08

شکل ۳-۱

در خط اول شکل ۳-۱ مشاهده خواهید کرد پیام Arp request به مقصد Broadcast ، مبنی بر اینکه کدام سیستم در شبکه دارای آی پی ۱۹۲,۱۶۸,۱,۱۵ است ارسال شد .در خط دوم خواهید دید که سیستم مورد نظر Mac خود را در قالب یک پیام Arp response باز می گرداند .

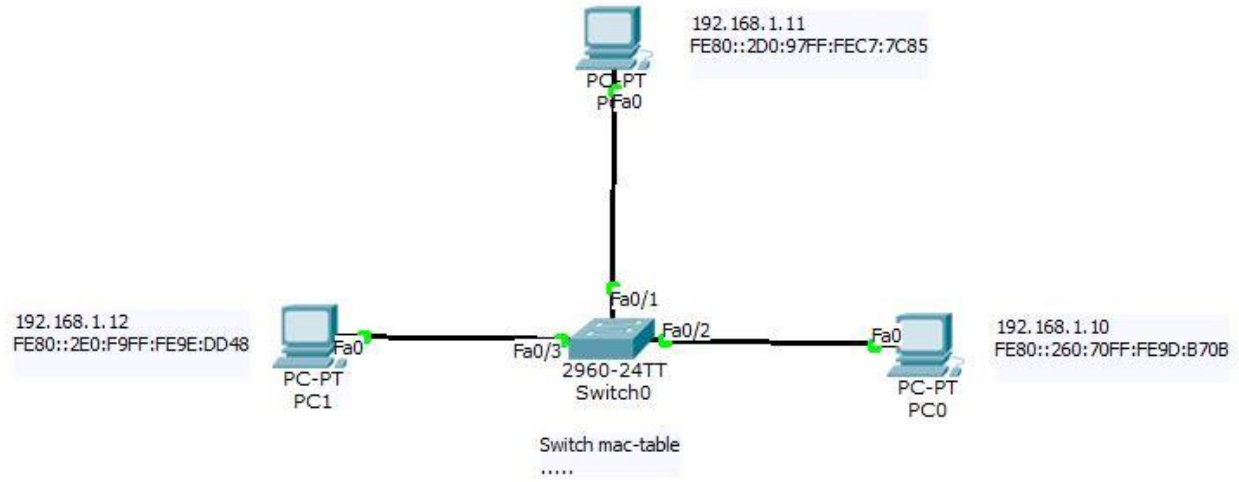
نکته ۳: به سیستم هایی که قادر به دریافت فریم Broadcast یک دیگر باشند ، اصطلاحا گفته می شود در یک Boradcast Domain هستند.و سیستم هایی که در یک Boradcast Domain باشند با یکدیگر ، شبکه Lan تشکیل می دهند. توجه کنید که Router فریم Boradcast را از خود عبور نمی دهد.بنابراین شعاع یک Boradcast Domain ، محدود به موقعیت Router در شبکه است .

۳- مانیتورینگ و رفع اشکال : برای آنکه تغییرات جدول Arp سیستم خود را مشاهده کنید ، قبل و بعد دستور ping با استفاده از دستور arp –a جدول Arp سیستم خود را مشاهده کرده و نتیجه هر دو حالت را با هم مقایسه کنید.

سناریو دوم

۰-عنوان : نقش سویچ در شبکه

۲-خلاصه : در این سناریو خواهیم دید که یک سویچ چگونه با یادگیری آدرس فیزیکی لایه دو (Mac address) ندهای شبکه ، به هدایت فریم ها می پردازد و انتشار بسته های Flooding را ، بطور قابل توجه ای کاهش خواهد داد تا منجر به افزایش کارایی شبکه شود.



شکل ۰-۲

۲-توضیح : وظیفه اصلی سویچ در شبکه هدایت فریم ها در شبکه به سمت مقصد مورد نظر است. بدون وجود سویچ یک فریم ، به دست تمام سیستم های موجود در Boradcast domain خواهد رسید. در آن صورت هر کارت شبکه پس از دریافت آن بسته باید بررسی کند که مالک آن بسته هست یا خیر ، برای این کار ، کارت شبکه به پردازنده وقفه خواهد داد .حال تصور کنید فریم های زیادی در شبکه ارسال شود آنگاه زمان قابل توجهی از Cpu گرفته می شود و کارایی سیستم های شبکه و خود شبکه کاهش می یابد.

اما یک سویچ چگونه می تواند مشکلات گفته شده در بالا را حل کند ؟ اساس کار سویچ یک جدول به نام Mac table است.این جدول کل دانش سویچ از شبکه است.برای آنکه مفهوم این جدول را بهتر درک کنید به جدول mac زیر که متعلق به یک سویچ است توجه کنید :

Vlan	Mac Address	Type	Ports
1	0060.709d.b70b	DYNAMIC	Fa0/2
1	00d0.97c7.7c85	DYNAMIC	Fa0/1

برای مثال معنای سطر اول از این جدول برای سویچ این است که ، اگر فریمی را با آدرس مک مقصد 0060.709d.b70b دریافت نمود باید آن را از پورت شماره ۰/۲ خارج کند . چرا که تنها سیستم متصل به این پورت دارای مک 0060.709d.b70b است ، یا قبلا سیستمی با این مک از این پورت فریم را به سویچ داده است .

سویچ این جدول را چگونه می آموزد ؟ برای آموختن مک آدرس های هرسیستم ، سویچ و سیستم های شبکه نیاز به هیچگونه پیکربندی ندارد .برای مثال اگر سویچ از پورت شماره 0/3 خود یک فریم با آدرس مک مبدا 00e0.f99e.dd48 را دریافت کند و به ازای این مک رکوردی در جدول نباشد ، جدول را بصورت زیر به روز رسانی خواهد کرد .

Vlan	Mac Address	Type	Ports
1	0060.709d.b70b	DYNAMIC	Fa0/2
1	00d0.97c7.7c85	DYNAMIC	Fa0/1
1	00e0.f99e.dd48	DYNAMIC	Fa0/3

توجه: سویچ در دو صورت فریم دریافتی را Flood خواهد کرد ، حالت اول زمانی است که سویچ نداند فریمی با مک مقصد مورد نظر را به کدام پورت خود هدایت کند . به عبارتی رکوردی به ازای آن مک وجود نداشته باشد.در این صورت فریم را به تمام پورت های خود می فرستد یا به عبارتی flood می کند. حالت دوم زمانی است که که فریمی با مک مقصد FFFF.FFFF.FFFF را دریافت کند.آنگاه در می یابد که یک فریم مربوط به Broad cast را دریافت کرده است و آن را به تمام پورت های خود می فرستد. بخاطر دارید که پروتکل Arp در فریم Arp request مک مقصد را FFFF.FFFF.FFFF قرار می داد.

برای درک بهتر عملکرد یک سویچ ، مطابق شکل ۰-۱ ، یک شبکه Lan را در محیط Cisco packet tracer پیاده سازی می کنیم ، مراحل کار :

۱- از یک سویچ Catalyst 2960 استفاده کنید.

سه کامپیوتر را با استفاده از کابل Straight به ترتیب به پورت های 0/1,0/2,0/3 سویچ متصل کنید .

نکته ۳ : در سویچ های ۲۹۶۰ ، شماره پورت از 0/1 شروع می شود و پورت ۰/۰ نداریم.

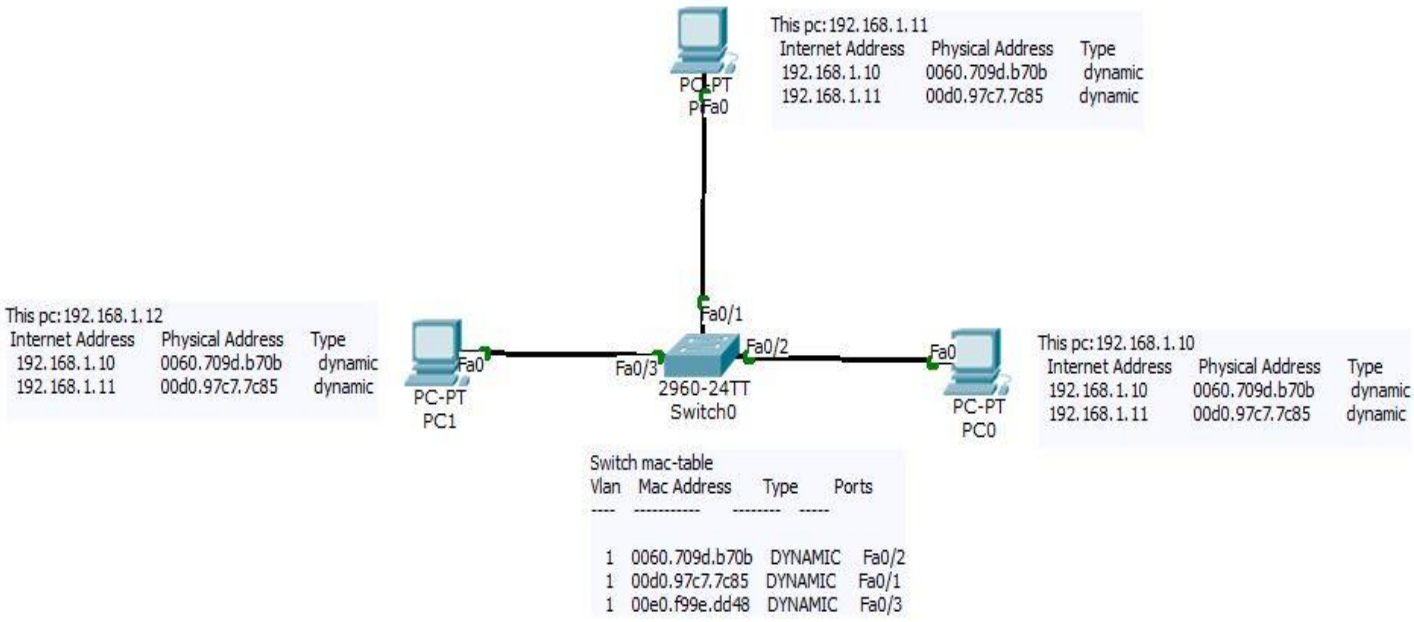
نکته ٤: برای آگاهی از اینکه هر دو گره در شبکه را با چه نوع کابلی به هم متصل کنید به جدول شماره یک انتهای جزوه مراجعه کنید.

نکته۵: برای آنکه مانند شکل شماره پورت روی هر پورت متصل برچسب گذاری شود ، از منو بالای برنامه به مسیر Option>Preferences بروید و تیک گزینه Always show Port Lables را فعال کنید.

۴-مطابق شکل ۱-۰ به هر کامپیوتر یک آدرس Ip با Subnetmask ، ۲۵۵,۲۵۵,۲۵۵,۰ اختصاص دهید .برای انجام این کار پس از کلیک بر روی کامپیوتر مورد نظر می توانید از یک کدام از دو مسیر زیر استفاده کنید:

مسیر اول : از تب Config به مسیر Interface>FastEthernet بروید.

مسیر دوم: از تب Desktop ، Ip Configuration را انتخاب کنید.



شکل ۲-۰

۳- مانیتورینگ و رفع اشکال :

۱- بر روی یک pc کلیک کرده و از تب Desktop ، CommandPrompt را انتخاب کرده و دستور Arp –a را اجرا کنید مشاهده خواهید کرد که جدول Arp cach خالیست. زیرا هنوز هیچ فریمی بین سیستم ها رد و بدل نشده.

۲- دستور Ping را اجرا کرده و به دو سیستم دیگر Ping کنید ، این کار را برای تمام pc ها انجام دهید .حال مجددا دستور Arp –a را بر روی سیستم ها اجرا کنید.در شکل ۲-۰ ، جدولَ Arp cach هر سیستم را کنار آن نوشته ایم.

۳- بر روی سویچ کلیک کرده ، به تب CLI بروید. با تایپ Enable در خط فرمان وارد مد Enable شوید و برای مشاهده جدول Mac سویچ ، فرمان Show mac address-table را تایپ کنید.

حال سوال اینجاست ، چه اتفاقی رخ داده است ؟ چرا با اجرای دستور Ping جدول Arp سیستم ها و جدول Mac سویچ تغییر کرده است ؟

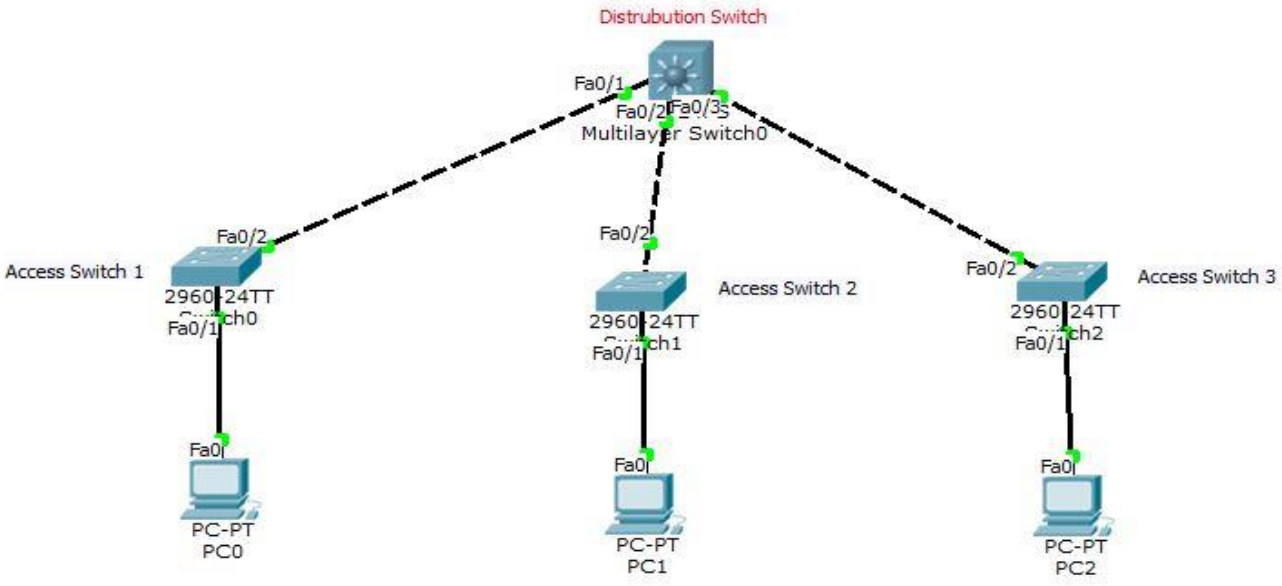
ابتدا یادآوری مختصری در رابطه با Ping خواهیم داشت ، این دستور که معمولا برای تست برقراری اتصال بین دوسیستم در شبکه بکار می رود ، یک بسته داده به آی پی مشخص شده در دستور می فرستد ، سیستم مورد نظر پس از دریافت این بسته ، مجدا آن را به فرستنده بر می گرداند.فرستنده با دریافت بسته آگاه خواهد شد که اتصال با مقصد برقرار است .

پیش تر اشاره شد برای آنکه فرستنده ای بتواند بسته ای را ، به دست مقصدی در شبکه محلی خودش بفرستد نیازمند آن است که آدرس Ip و Mac مقصد را بداند .دستور Ping هم که نیاز به ارسال بسته دارد از این قاعده مستثنی نیست .به علت اینکه تا قبل دستور Ping هیچ بسته ای بین مبدا و مقصد رد و بدل نشده فرستنده آدرس Mac مقصد را نمی داند.اینجاست که قبل از ارسال بسته توسط Ping ، پروتکل Arp وارد عمل شده ،Mac مقصد را بدست آورده و جدول Arp chach سیستم را به روز رسانی خواهد کرد تا در ارسالهای بعدی ، از آن استفاده کند.حال بسته توسط Ping قادر به ارسال خواهد شد.

سناریو شماره ۳

۰-عنوان : طراحی شبکه های Lan

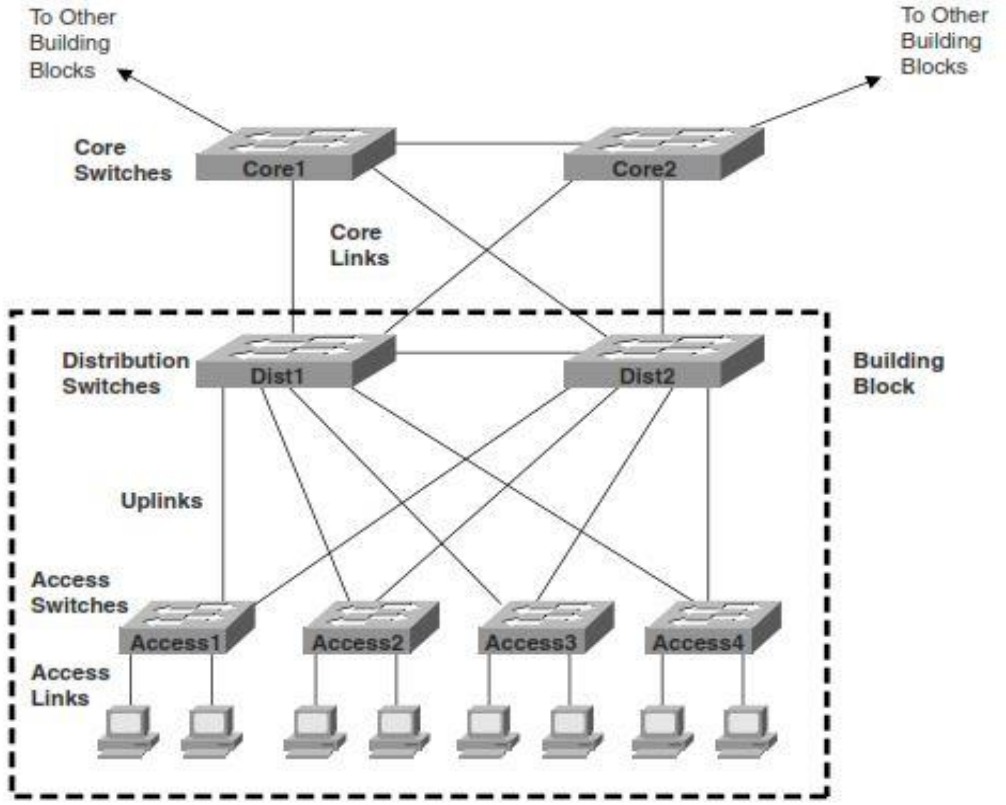
۱-خلاصه : در این سناریو با نحوه طراحی شبکه های محلی با استفاده از سویچ های Access و Distribution وCore آشنا خواهید شد . همچنین جزئیات بیشتری در مورد سویچ ها را بررسی خواهیم کرد.



شکل ۳-۰

۳-تشریح : در این سناریو قصد داریم تا شما را با چند واژه در ادبیات سیسکو آشنا کنیم که در طراحی شبکه های محلی بسیار بکار برده خواهد شد. سویچ ها در شبکه ، در موقعیت های مختلفی قرار داده میشوند و بر همین اساس بار پردازشی متفاوتی به آنها تحمیل خواهد شد. ما سویچ را از لحاظ موقعیت شان در شبکه به سه دسته تقسیم خواهیم کرد .

دسته اول سویچ ها به سیستم های انتهایی شبکه متصل می شوند .دسته دوم نیز بین سایر سویچ ها اتصال برقرار می کنند و دسته سوم نیز در بالاترین سطح وظیفه اتصال سویچ های دسته ی دوم را به عهده دارند. سویچ های دسته اول و دوم و سوم را به ترتیب سویچ Access ، Distribution ، Core می نامیم .رعایت این دسته بندی به ما کمک خواهد کرد بار پردازشی بطور مناسبی در شبکه توزیع شده و کارایی شبکه افزایش یابد.



شکل ۴-۱

قدرت پردازشی هریک از سویچ های Access ، Distribution ، Core با یکدیگر متفاوت است و سویچ های سطوح بالاتر قدرت و قیمت بیشتری دارند . با این دسته بندی ما می توانیم بزرگترین شبکه های Lan را با کارایی مناسبی ، طراحی کنیم .

مراحل پیاده سازی سناریو شکل ۳-۱ به شرح زیر است :

۱- با استفاده از سویچ های ۳۵۶۰ و ۲۹۶۰ شبکه محلی شکل 3-0 را پیاده سازی کنید .
۲- به هر یک از سیستم های pc-0 و pc-1 و pc-2 به همان روش که در سناریو دوم گفته شد، به ترتیب آدرسهای ۱۹۲,۱۶۸,۱,۱۰ و ۱۹۲,۱۶۸,۱,۱۱ و ۱۹۲,۱۶۸,۱,۱۲ را اختصاص دهید.

۴-مانیتورینگ و رفع اشکال :

۳- دستور Ping را اجرا کرده و به دو سیستم دیگر Ping کنید ، این کار را برای تمام سیستم ها انجام دهید . و سپس دستور Arp –a را بر روی سیستم ها اجرا کنید.
۴- برای مشاهده جدول Mac سویچ ، پس ورود به مد Enable ، فرمان Show mac address-table را تایپ کنید.

بررسی کنید :

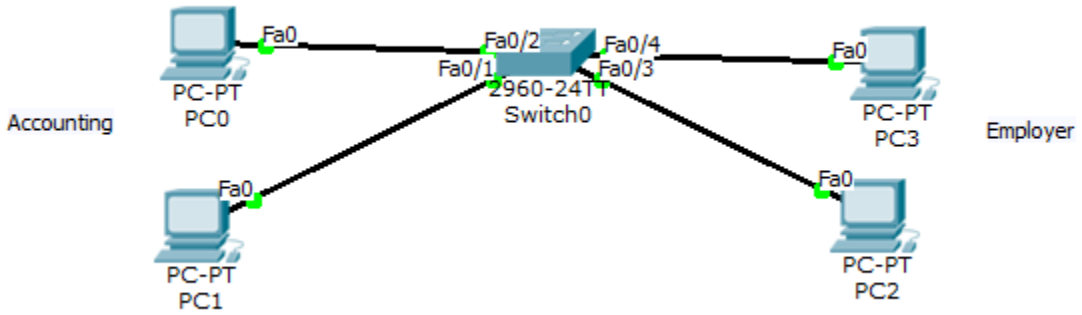
جدول Mac سویچ نسبت به سناریو اول چه تفاوتی دارد ؟

آیا یک سویچ فقط باید مک سیستم های متصل به پورت های خود را بیاموزد ؟

سناریو شماره ۴

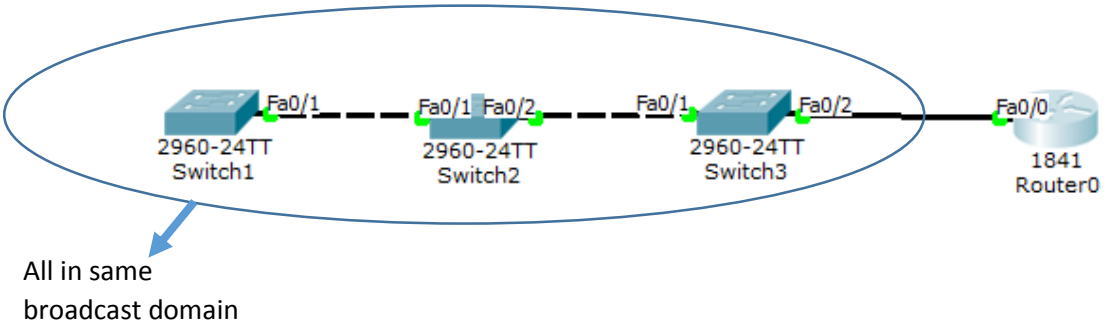
۰-**عنوان :** پیاده سازی Virtual LANS(Vlan)

۱-**خلاصه :** در این سناریو با مفهوم Vlan و کاربردهای آن در شبکه ها کامپیوتری آشنا خواهید شد و مراحل پیاده سازی آن را می آموزید.



شکل ۰-۴

۲-**توضیح :** پیش تر گفته بودیم وقتی یک فریم به مقصد Broadcast به دست سویچ برسد ، سویچ آن را روی تمامی پورت های خود Forward خواهد کرد . بنابراین فریم به دست تمام سیستم هایی که در یک Broadcast domain هستند می رسد . شبکه فرضی شکل صفحه بعد را در نظر بگیرید :



شکل ۱-۴

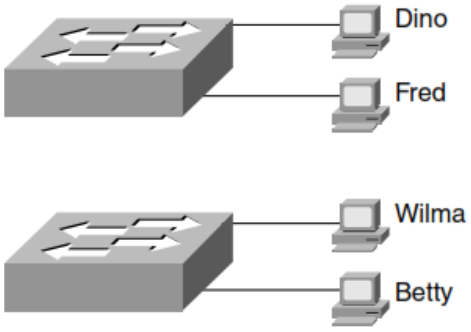
در شبکه شکل ۱-۴ ، سویچ های ۱ و۲ و۳ همگی در یک Broadcast domain قرار دارند . و فریم Boradcast به دست تمامی سیستم های متصل به این سه سویچ می رسد . تا در نهایت توسط Router ، Discard شود .حال تصور کنید به هریک از این سه سویچ ، ۲۴ سیستم متصل باشد . در این صورت ممکن است فریم های حاصل از Broadcast حجم قابل توجهی از ترافیک را به شبکه تحمیل کند .و در نهایت منجر به کندی شبکه و کاهش کارایی شود .

علاوه بر این ، به راحتی می توان با نرم افزارهایی مانند packet snnifer ها ، از محتویات ترافیک عبوری در بخش های مختلف شبکه مطلع شد. برای مثال شبکه ی شکل ۰-۴ را تصور کنید که سیستم های مالی و سیستم های کارمندان همگی در یک شبکه هستند ، حال اگر کارمند بازیگوشی داشته باشید که بخواهد با یک نرم افزار packt snnifer اطلاعات مالی شما را که در داخل شبکه رمزنگاری نشده ،Snnif کند ، شما کاملا بی دفاع خواهید بود .

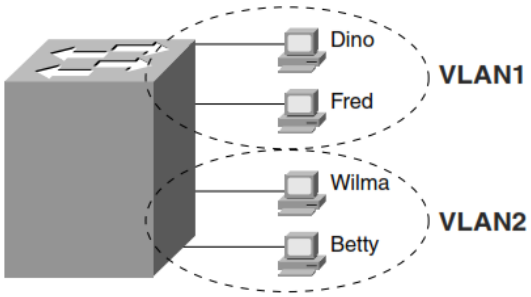
بنظر می رسد برای برطرف کردن مشکلات گفته شده ، باید یک Broad cast Domain بزرگ را به چند Broadcast Domain کوچتر تقسیم کرد تا ترافیک ها محدودتر شود و به کل شبکه سرایت نکند. از طرفی میدانیم ایجاد Broadcast Domain جدید ، با Router امکان پذیر است .وظیفه اصلی Router مسیریابی است .آیا معقول و بصرفه بنظر می رسد که تنها برای ایجاد Boradcast domain بیشتر ، Router خریداری کنیم ؟

مشکلات مطرح شده در بالا و بسیاری از مشکلات دیگر باعث شده تا مفهومی به نام Virtual LAN مطرح شود . با استفاده از پیاده سازی Vlan ما می توانیم بر روی یک سویچ چندین Boradcast Domain داشته باشیم . یا به عبارتی چندین Vritual LAN داشته باشیم. تنها سیستمهایی که

در یک Virtual LAN هستند می توانند با هم مبادله ی ترافیک داشته باشند، به عبارتی در عمل دقیقا ما دو LAN مجزا خواهیم داشت . برای درک بهتر مفهوم Vlan ، شبکه شکل۲-۴ را ، که یک شبکه در حالت بدون VLAN و VLAN نشان می دهد ، در نظر بگیرید .



Two Broadcast Domains and No VLANs



Two VLANs using One Switch

شکل ۲-۴

نکته۱ : پورتی که فقط در یک VLAN عضویت داشته باشد ، پورت Access نامیده می شود .

حال که با مفهوم VLAN آشنا شده اید ، زمان آن رسید است که شبکه شکل ۰-۴ را پیاده سازی کنیم.در این شبکه سیستم های مربوط به حساب داری (Accounting) در سمت چپ و سیستم های کارمندان در سمت راست تصویر ، و همگی متصل به یک سویچ هستند .هدف این است که با ایجاد دو شبکه مجازی بر روی سویچ ، از Boradcast فریم در تمام شبکه جلوگیری کنیم . به عبارتی می خواهیم سیستمهای حسابداری در یک VLAN و سیستمهای کارمندان در یک VLAN باشند .تمرکز ما در این سناریو VLAN بندی تنها با پورت ACCESS است . به عبارتی می خواهیم هر پورت تنها متعلق به یکی از VLAN ها باشد .

۳-پیکربندی : مراحل پیکربندی سویچ ۲۹۶۰ به شرح ذیل است :

۱- وارد محیط CLI شده دستور enable را وارد کنید.

۲- دستور configure terminal را وارد کنید تا وارد محیط پیکربندی سویچ شوید.

۳- دستور vlan 2 را وارد کنید تا یک vlan با ID ، ۲ ایجاد شود .

نکته۲ : تمام سویچ های سیسکو یک VLAN پیش فرض به نام ۱ دارند .که تمامی پورت سویچ در آن عضو هستند .

۴- دستور exit را وارد کنید تا از Subcommand مربوط به Vlan خارج شوید .

۵- مجددا دستور مربوط به مرحله دوم را وارد کنید تا به محیط مربوط به پیکربندی سویچ وارد شوید.

۶- دستور interface fastEthernet 0/2 را وارد کنید تا پورت شماره ۰/۲ سویچ برای پیکربندی انتخاب شود .

۷- دستور switchport mode access را وارد کنید .با این دستور به سویچ اعلام می کنیم که می خواهیم این پورت تنها عضو یک VLAN باشد .به مفهوم پورت ACCESS و TRUNK در نکته ۱ این سناریو توجه کنید.

۸- دستور switchport access vlan 2 را وارد کنید . با این دستور به سویچ اعلام می کنید که پورت ۰/۲ را در vlan 2 قرار دهد .

۹- دستور exit را وارد کنید.

نکته۳ : در صورتی که نوع دسترسی به پورت ACCESS اعلام شود ، با عضو کردن سویچ در یک VLAN ، عضویت سویچ در VLAN قبلی آن ، به طور اتوماتیک لغو خواهد شد.

۱۰-مراحل ۶ تا ۹ را برای پورت شماره ۰/۱ نیز انجام دهید.

با مراحل بالا ما پورتهای ۰/۱ و ۰/۲ را از عضویت VLAN 1 خارج کرده و به عضویت VLAN 2 در آوردیم .پورت های ۰/۴ و ۰/۳ در VLAN پیش فرض خود یعنی VLAN 1 مانده اند .

نکته٤ : به ازای هر VLAN در سویچ یک MAC Table ایجاد می شود . هنگامی که سویچ فریمی را دریافت کند ، تنها در MAC Table ، VLAN مربوط به پورت دریافتی به جستجو می پردازد .

۴-مانیتورینگ و رفع اشکال :

۱-برای مشاهده اطلاعات اینکه هر پورت متعلق به کدام است VLAN ، در محیط enable دستور show vlan brief را وارد کنید.

۳-برای آنکه مشاهده کنید هر Vlan جدول Mac address مربوط بخودش را دارد ، وارد محیط enable شده و دستور show mac-address-table را وارد کنید.

همانند شکل زیر مشاهده خواهید کرد که در ستون Vlan شماره Vlan مربوط به هر سطر درج شده است.

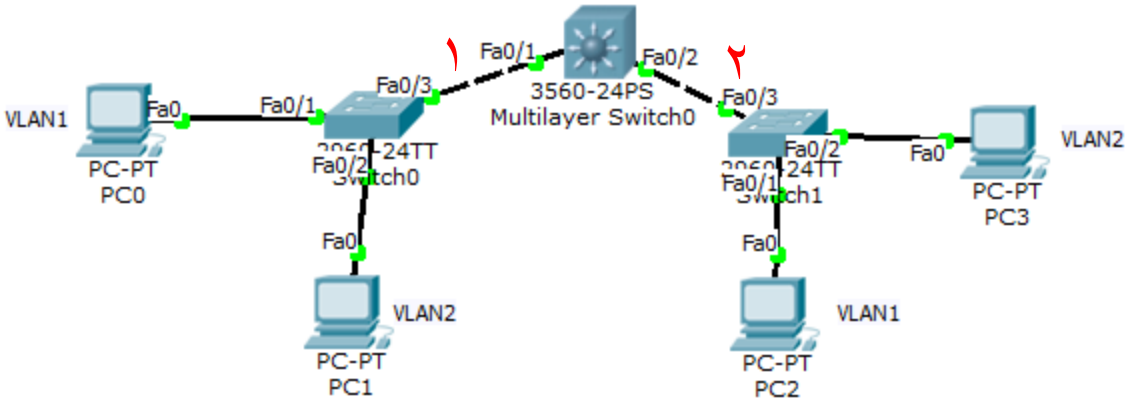
Vlan	Mac Address	Type	Ports
1	0007.ec26.648d	DYNAMIC	Fa0/1
1	00d0.588a.55cc	DYNAMIC	Fa0/2
2	0006.2ade.196a	DYNAMIC	Fa0/4
2	0090.2146.1985	DYNAMIC	Fa0/3

شکل ۳-۴

سناریو شماره ۵

۰-عنوان : VLAN Trunking

۱-خلاصه : در این سناریو با کاربرد پورت TRUNK و دلایل استفاده از آن آشنا خواهید شد .سپس نحوه پیاده سازی آن بر روی سویچ را می آموزید .



شکل ۰-۵

۲-توضیح : گاهی در شبکه ممکن است سیستم های عضو یک VLAN همگی متصل به یک سویچ نباشند.و از طریق چند سویچ بهم مرتبط شوند . برای مثال در شکل ۰-۵ ، PC0 و PC2 در VLAN1 هستند ولی به سویچ های متفاوتی متصل اند .مجددا شکل ۰-۵ را مشاهده کنید.

سیستم هایی که عضو یک VLAN هستند باید قادر به برقراری ارتباط لایه دو باشند .و بنظر می رسد تنها راه ارتباط سیستم ها عضو یک VLAN استفاده از لینک های ۱ و۲ سویچ ۳۵۶۰ است.حال سوال اصلی اینجاست ، پورت Fa0/1 و Fa0/2 سویچ ۳۵۶۰ و همچنین پورتهای Fa0/3 ،

SWICH0 و SWICH1 باید عضو کدام VLAN باشد؟ اگر عضو VLAN2 باشد ، ترافیک VLAN3 را عبور نمی دهد.

و اگر عضو VLAN3 باشد ترافیک VLAN2 را عبور نمی دهد.بنظر می رسد برای آنکه ما بتوانیم ترافیک هر دو VLAN را ، از پورت های ذکر شده عبور دهیم ، نیازمند آن هستیم تا این پورتها هم زمان قادر به عضویت در دو VLAN باشند . به چنین پورتی ،TRUNK گفته می شود .

نتیجه گیری : به پورتی که در بیش از یک VLAN عضویت داشته باشد ، پورت TRUNK گفته می شود .

اما مشکل بسیار مهمی که مطرح می شود این است ، اگر یک پورت عضو دو یا چند Vlan باشد ، سویچ از کجا بفهمد فریم دریافتی متعلق به کدام VLAN است ؟ برای رفع این مشکل، سویچ ارسال کننده فریم از پورت TRUNK ، برچسبی یا tag را به فریم اضافه می کند که نشان دهنده شماره vlan مربوطه است.سویچی که فریم را از پورت TRUNK خود دریافت می کند با خواندن این tag به شماره VLAN مربوط به فریم پی خواهد برد .

۳-پیکربندی : بطور کلی پورت Fa0/1 و Fa0/2 سویچ ۳۵۶۰ و همچنین پورتهای Fa0/3 ، SWICH0 و SWICH1 باید TRUNK باشد .

پیکربندی سویچ ۳۵۶۰ :

۱- وارد محیط CLI شده دستور enable را وارد کنید.
۲- دستور configure terminal را وارد کنید تا وارد محیط پیکربندی سویچ شوید.
۳- دستور vlan 2 را وارد کنید تا یک vlan با ID ، ۲ ایجاد شود .
۴- دستور exit را وارد کنید تا از Subcommand مربوط به Vlan خارج شوید .
۵- مجددا مراحل ۳ و ۴ را انجام دهید ولی اینبار یک VLAN با ID ، ۳ ایجاد کنید.
۶- در مد configure ، دستور interface fastEthernet 0/1 را وارد کنید تا اینترفیس مورد نظر برای پیکربندی انتخاب شود.

۷- دستور switchport trunk encapsulation dot1 وارد کنید.
۸- دستور switchport mode trunk وارد کنید .
۹- switchport trunk allowed vlan 2,3 وارد کنید تا بتوانیم ترافیک vlan2,3 را عبور دهیم.
۱۰- دستور Exit را وارد کنید. مراحل ۶ تا ۸ را برای interface fastEthernet 0/2 تکرار کنید.

پیکربندی سویچ swich0 :

در این سویچ پورت Fa0/3 ،TRUNK است. و پورت های Fa0/1 و Fa0/2 ، Access هستند.

۱- وارد محیط CLI شده دستور enable را وارد کنید.
۲- دستور configure terminal را وارد کنید تا وارد محیط پیکربندی سویچ شوید.
۳- دستور vlan 2 را وارد کنید تا یک vlan با ID ، ۲ ایجاد شود .
۴- دستور exit را وارد کنید تا از Subcommand مربوط به Vlan خارج شوید .
۵- مجددا مراحل ۳ و ۴ را انجام دهید ولی اینبار یک VLAN با ID ، ۳ ایجاد کنید.
۶- در مد configure ، دستور interface fastEthernet 0/3 را وارد کنید تا اینترفیس مورد نظر برای پیکربندی انتخاب شود.
۷- دستور switchport mode trunk وارد کنید .
۸- switchport trunk allowed vlan 2,3 وارد کنید تا بتوانیم ترافیک vlan2,3 را عبور دهیم.

پیکربندی سویچ swich1 :

۱- در این سویچ نیز پورت Fa0/3 ،TRUNK است. و پورت های Fa0/1 و Fa0/2 ، Access هستند. و مراحال پیکربندی عینا" شبیه سویچ swich0 است.

۴-مانیتورینگ و رفع اشکال :

۱-برای مشاهده پورت های TRUNK هر سویچ ، در محیط enable دستور show interfaces trunk را وارد کنید.

۲-برای مشاهده اطلاعات اینکه هر پورت متعلق به کدام است VLAN ، در محیط enable دستور show vlan brief را وارد کنید.

۳-برای تست برقراری اتصال بین سیستم های موجود در یک VLAN ، از دستور ping استفاده کنید.

جدول ١-٠

If Device A Has A:	And Device B Has A:	Then Use This Cable:
Computer COM port	Console of router/switch	Rollover
Computer NIC	Switch	Straight-through
Computer NIC	Computer NIC	Crossover
Switch port	Router's Ethernet port	Straight-through
Switch port	Switch port	Crossover (check for uplink button or toggle switch to defeat this)
Router's Ethernet port	Router's Ethernet port	Crossover
Computer NIC	Router's Ethernet port	Crossover
Router's serial port	Router's serial port	Cisco serial DCE/DTE cables