# آزمایشگاه شبکه های کامپیوتری



مدرس استاد مجید اسدپور نویسنده مهدی گران

# سناريو اول

### •-عنوان: عملكرد پروتكل 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 مقصد را نداشته باشد ، پروتکل Arp یک فریم با آدرس IP مقصد و آدرس FFFF.FFF،Mac 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 – 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 بررسیی 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 و VirtualMachine مربوط به VirtualMachine ها هستند .

WIRESHARK The World's Most Popular Network Protocol Analyzer Version 1.10.6 (v1.10.6 from master-1.10)					
Capture	Files				
<ul> <li>Interface List         Lysist of the capture interfaces             counts incoming packets)     </li> <li>Start         Choose one or more interfaces to capture from, then Start     </li> <li>VirtualBox Host-Only Network         Bluetooth Network Connection         Ethernet 2         Ethernet         Wi-Fi         VMware Network Adapter VMnet8         VMware Network Adapter VMnet1     </li> <li>Capture Options         Start a capture with detailed options     </li> </ul>	<ul> <li>Popen Open a previously captured file</li> <li>Open Recent:</li> <li>Sample Captures A rich assortment of example capture files on the wiki</li> </ul>				
١-	شکل ۱				
ِت کلیک کنید. کل زیر وارد کنید .	پس از انتخاب اینترفیس مورد نظر برروی دکمه استار ۲- در Command Prompt فرمان ping را به ش				

### 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 باز گردید ، همانگونه که در شکل ۳-۱ مشاهده می کنید در قسمت Arp ، Filter را تایپ کرده و Enter را بزنید .

Filter	r: a	rp		¥	Expression.	Clear Apply Save
No.		Time	Source	Destination	Protocol	Length Info
ſ	76	132.461156	Vmware_c0:00:08	Broadcast	ARP	42 who has 192.168.1.15? Tell 192.168.1.12
1	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 گفت ہمی شــود در یک Boradcast Domain هســتند.و ســیســتم هایی که در یک Boradcast Domain باشـند با یکدیگر ، شـبکه Lan تشـکیل 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 – arp جدول Arp سیستم خود را مشاهده کرده و نتیجه هر دو حالت را با هم مقایسه کنید.

### سناريو دوم

--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 تعدی کنید :

Vlar	Mac Address	Туре	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 از این ورت 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	Туре	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 FFF.FFF.FFF 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 request در فریم Arp request می مقصد را FFF.FFF.FFF.

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.

**نکته ۵:** برای آنکه مانند شکل شماره پورت روی هر پورت متصل برچسب گذاری شود ، از منو Always show Port برید و تیک گزینه 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 Ip Configuration ، Desktop را انتخاب کنید.



شکل ۲-۰

۳- مانیتورینگ و رفع اشکال :

- را انتخاب کرده و از تب CommandPrompt ، Desktop را انتخاب کرده و دستور Arp cach 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
   ۱۰- دستور Arp –a را بر روی سیستم ها اجرا کنید.در شکل ۲-۰ ،
   جدول 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 دسته 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

•-عنوان : طراحی شبکه های Lan

۱-خلاصه : در این سناریو با نحوه طراحی شبکه های محلی با استفاده از سویچ های Access و Distribution و Distribution و Distribution و Core



شکل ۰–۳

**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 Distribution ، Access ، 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 ۱–۳

قدرت پردازشی هریک از سویچ های Core ، Distribution ، Access 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.
- Show mac سویچ ، پس ورود به مد Enable ، فرمان Mac + برای مشاهده جدول 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 ؟

# سناريو شماره ۴

•-عنوان : پیاده سازی (Vlan د 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 :



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 Discard ، Router 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 شکل ۲-۴ را ، که یک شبکه در حالت بدون VLAN و VLAN نشان می دهد ، در نظر بگیرید .









شکل ۲-۴

نکته ( : 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.

نکته ۲ : 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 به سویچ اعلام می کنیم
   ۷- دستور به سویچ اعلام می کنیم
   ۷- دستور 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.

نکته ۲: 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 1 VLAN خارج کرده و به عضویت VLAN 2 در آوردیم .پورت های ۰/۴ و ۷/۲ در VLAN پیش فرض خود یعنی VLAN 1 مانده اند .

نکته ٤ : به ازای هر VLAN در سویچ یک MAC Table ایجاد می شود . هنگامی که سویچ فریمی را دریافت کند ، تنها در VLAN ، MAC Table 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

# سناريو شماره ۵

### •-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 .



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 ، PCO و PC2 در VLAN 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 Fa0/3 سویچ ۳۵۶۰ و همچنین پورتهای Fa0/3 ،

SWICHO 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 .

پيکربندي سويچ 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 .
 ۴- دستور not را وارد کنید تا از Subcommand مربوط به vlan خارج شوید .
 ۶- دستور not را وارد کنید تا یک it vlan با ID ، ۲ ایجاد شود .
 ۶- دستور exit را وارد کنید تا یک not vlan با ID ، ۲ ایجاد شود .
 ۶- دستور exit را وارد کنید تا از subcommand مربوط به vlan خارج شوید .
 ۶- دستور it vlan و ۴ را انجام دهید ولی اینبار یک vlan با ID ، ۳ ایجاد کنید تا اینترفیس مورد .
 ۶- در مد it vlan را وارد کنید تا از itterface fastEthernet را وارد کنید تا اینترفیس مورد .

- ۷- دستور switchport trunk encapsulation dot1 وارد کنید.
  - ۸– دستور switchport mode trunk وارد کنید .
- وارد کنید تا بتوانیم ترافیک vlan2,3 را عبور switchport trunk allowed vlan 2,3 –۹ وارد کنید. دهیم.
- ۱۰− دستور Exit را وارد کنید. مراحل ۶ تا ۸ را برای 10 interface fastEthernet تکرار کنید.

پیکربندی سویچ swich0 :

- در این سویچ پورت TRUNK، Fa0/3 است. و پورت های Fa0/1 و Access ، Fa0/2 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 .
- یا بتوانیم ترافیک vlan2,3 را عبور switchport trunk allowed vlan 2,3 –۸ را عبور دهیم.

پیکربندی سویچ swich1 :

۱- در این سویچ نیز پورت TRUNK، Fa0/3 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 دستور trunk د 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.

# سناریو شماره ۶

### •-عنوان : Static Routing

۱-خلاصه: در این سناریو با مفاهیم پایه ای مسیریابی آشنا خواهید شد .سپس می آموزید که چگونه یک Router را پیکربندی کرده و جدول مسیریابی آن را بطور Static ایجاد کنید.



شکل ۱-۰

**۲-توضیح:** میدانیم هنگام ارسال یک IP ، Packet مقصد و Subnet مبدا با هم And میشوند . چنانچه نتیجه این And برابر با Netid مبدا شد ، مقصد Packet در داخل شبکه و در غیر اینصورت مقصد در یک شبکه دیگر است و باید بسته تحویل Gateway داده شود .

سوال اصلی اینجاست، در نهایت کدام Device مسئولیت تبادل Packet بین دو شبکه متفاوت را به عهده دارد ؟ پاسخ Router است . Router ها مسئولیت ارتباط بین دو شبکه متفاوت را بر عهده می گیرند . آنها بهترین مسیر ممکن را از طریق الگوریتم های مسیریابی آموخته و جداول مسیریابی خود را با استفاده از پروتکل ها مسیریابی ایجاد خواهند کرد.

Router ها برای آنکه بتوانند به درستی وظیفه مسیریابی را به انجام برسانند ، نیازمند پیکربندی هستند. بر خلاف سویچ ها که میتوانستند بدون پیکربندی ارتباط لایه دویی پیکربندی هستند. بر خلاف سویچ ها که میتوانستند بدون پیکربندی ارتباط لایه دویی سیستم های یک شبکه را برقرار کنند . مهم ترین چیزی که یک Router باید بداند جداول مسیریابی است ، که بدون آن Router قادر به مسیریابی نیست . هر رکورد از جدول مسیریابی به Subner خواهد گفت که به ازای هر Subnet مقصد ، او Packet را زر کند . مهم از که می واند به ازای هر Subnet مقصد . مواند از کدام از کدام از کند . مهم ترین چیزی که یک Inter می از کرام از کرام از کند . مهم ترین چیزی که میتوانست . مواند از کرام از کرام می واند از کرام می می واند . مهم ترین چیزی که می واند . مواند از کرام مسیریابی است . می می واند گفت که به ازای هر Subnet مقصد . Subnet را زر کرام از کرام Subnet خود Subnet کند .

برای مثال ، شکل زیر یک رکورد از جدول مسیریابی Router را نشان می دهد .

مقصد	اينترفيس خروجي	روتر بعدی
192.168.3.0/24	Fastehernet0/0	10.10.12.1

اما سوال اینجاست که یک Router چگونه جداول مسیریابی خود را ایجاد می کند؟ برای ایجاد جداول مسیریابی بطور کلی دو روش وجود دارد :

-Static -۱ در این روش کلیه مسیرهای ممکن باید بطور دستی به Router داده شود.

۲– Dynamic در این روش ،Router با استفاده از الگوریتم ها و پروتکل های مسیریابی ، مسیرهای ممکن را می آموزد و سپس با توجه به پارامترهای مختلف ، فقط بهترین مسیر را برای هر مقصد ، در جدول مسیریابی خود درج میکند.

در این سناریو به StaticRouting خواهیم پرداخت . در این روش به ازای هر مقصد ، مسیر آن در تمام روترها بطور دستی وارد شود .

نکته ( : یک Router ، مسیر مربوط به Subnet هایی که بطور مسیقیم به Interface آن متصل هسیتند را اتوماتیک می آموزد و در جدول مسیریابی خود وارد میکند . به چنین مسیرهایی ، مسیرهای Connected گفته می شود.

شـبکه ۶-۰ را در نظر بگیرید ، می خواهیم شـبکه تهران با subnet آدرس ، ۱۹۲,۱۶۸,۳,۰/۲۴ بتواند با مازندران و اصفهان ارتباط داشـته باشـد. بنابراین باید به ازای مقصـدی با ۱۹۲,۱۶۸,۳,۰/۲۴ در جدول مسـیریابی هر سه Router رکورد ایجاد شود. با توجه به نکته گفته شده برای Router تهران این مسیر توسط Router بطور خودکار در جدول درج می شود.زیرا جزء مسیرهای Router می د محسـوب می شود. رکورد اضافه شده برای شهر تهران را به ترتیب در جدول مسیریابی هر سه Router ، تهران ، مازندران و اصفهان مشاهده می کنید.

مقصد	اينترفيس خروجي	روتر بعدی
192.168.3.0/24	Gig0/0	Connected
مقصد	اينترفيس خروجي	روتر بعدی
192.168.3.0/24	Se0/0/0	10.10.11.2
مقصد	اينترفيس خروجي	روتر بعدی
192.168.3.0/24	Se0/0/0	10.10.12.2

حال اگر بخواهیم هر سه استان تهران ، مازندران و اصفهان با یکدیگر ارتباط داشته باشند جدول مسیریابی برای هر سه شهر تهران ، مازندران و اصفهان ، به ترتیب برابر است با:

مقصد	اينترفيس خروجي	روتر بعدی
192.168.1.0/24	Se0/0/0	10.10.11.1
192.168.2.0/24	Se1/0/0	10.10.12.1
10.10.11.0/30	Se0/0/0	Connected
10.10.12.0/30	Se1/0/0	Connected
192.168.3.0/24	Gig0/0	Connected
مقصد	اينترفيس خروجي	روتر بعدی
192.168.1.0/24	Se0/0/0	10.10.11.2
192.168.2.0/24	Se0/0/0	10.10.11.2
10.10.11.0/30	Se0/0/0	Connected
192.168.1.0/24	Gig0/0	Connected
مقصد	اينترفيس خروجي	روتر بعدی
192.168.1.0/24	Se0/0/0	10.10.12.2
192.168.2.0/24	Se0/0/0	10.10.12.2
10.10.12.0/24	Se0/0/0	Connected
192.168.2.0/24	Gig0/0	Connected

برای ایجاد یک رکورد جدید در جدول مسیریابی Router شما می توانید از دستور ip route به صورت ip oute یک رکورد جدید در جدول مسیریابی Router شما می توانید از دستور iproute destinationSubnet destination استفاده کنید.برای مثال برای ایجاد سطر اول از جدول مسیریابی Router تهران ، دستور زیر را وارد می کنیم :

iproute 192.168.1.0 255.255.255.0 10.10.11.1

برای حذف یک مسیر ، کافیست به ابتدای دستور no ، ip route اضافه کنید .برای مثال مسیری که در صفحه قبل ایجاد کردیم با دستور زیر حذف می شود:

no iproute 192.168.1.0 255.255.255.0 10.10.11.1

۳-پیکربندی:

۱-۳- ابتدا باید به تمام Interface های هر سه روتر IP اختصاص دهیم. وارد مد enable شده و سپس در محیط آن آشنا شده اید و سپس در محیط configure ، دستورات زیر را که در سناریو های قبلی با آن آشنا شده اید وارد کنید.

#### **Tehren router**

Tehran(config)#interface gigabitEthernet 0/0 Tehran(config-if)#ip address 192.168.3.1 255.255.255.0 no shutdown exit Tehran(config)# interface serial 0/0/0 Tehran(config-if)#ip address 10.10.11.2 255.255.255.252 no shutdown exit Tehran(config)#interface interface serial 0/0/1 Tehran(config-if)#ip address 10.10.12.2 255.255.255.252 no shutdown exit **Mazandaran router** 

# Mazandaran (config)#interface gigabitEthernet 0/0 Mazandaran (config-if)#ip address 192.168.1.1 255.255.255.0 no shutdown exit

Mazandaran (config)# interface serial 0/0/0 Mazandaran (config-if)#ip address 10.10.11.1 255.255.255.252 no shutdown exit **Esfahan router** Esfahan (config)#interface gigabitEthernet 0/0 Esfahan (config-if)#ip address 192.168.2.1 255.255.255.0 no shutdown exit Esfahan (config)# interface serial 0/0/0 Esfahan (config)# interface serial 0/0/0

no shutdown

exit

۲-۳- حال با استفاده از دستور ip route جداول مسیریابی را برای هر سه router ایجاد خواهیم کرد:

### **Tehren router**

Tehran(config)#ip route 192.168.1.0 255.255.255.0 10.10.11.1 Tehran(config)#ip route 192.168.2.0 255.255.255.0 10.10.12.1

### Mazandaran router

Mazandaran (config)#ip route 192.168.3.0 255.255.255.0 10.10.11.2 Mazandaran (config)#ip route 192.168.2.0 255.255.255.0 10.10.11.2

#### **Esfahan router**

Esfahan (config)#ip route 192.168.2.0 255.255.255.0 10.10.12.2 Esfahan (config)#ip route 192.168.1.0 255.255.255.0 10.10.12.2

**تذکر :** همانطور که قبلا گفته شد ، مسیرهای Connected بطور اتوماتیک توسط Router در جدول مسیریابی درج می شوند و نیازی به وارد کردن این مسیرها نیست .برای مثال در Router تهران نیازی به وارد کردن دستور ip route مقصد 192.168.3.0 نداریم.

۴-مانیتورینگ و رفع اشکال :

 برای مشاهده جدول مسیریابی Router از دستور show ip route استفاده کنید .برای مثال شکل زیر نتیجه دستور show ip route را برای Router مازندران نشان می دهد.حرف C در ابتدای هر خط ، بیانگر مسیرهای connected است. و حرف S مسیرهای Static ، یعنی مسیرهایی را که بطور دستی وارد کردیم نمایش می دهد.

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

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.10.11.0/30 is directly connected, Serial0/0/0 L 10.10.11.1/32 is directly connected, Serial0/0/0 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.1.0/24 is directly connected, GigabitEthernet0/0 L 192.168.1.1/32 is directly connected, GigabitEthernet0/0 S 192.168.2.0/24 [1/0] via 10.10.11.2 S 192.168.3.0/24 [1/0] via 10.10.11.2

شکل ۶–۱

 برای اینکه از برقراری اتصال بین سیستم ها هر سه شبکه مطمئن شوید ، از دستور ping استفاده کنید .چنانچه اتصال برقرار نبود از دستور tracert بر روی کامپیوتر ، یا معادل آن بر روی Router ،یعنی traceroute استفاده کنید.با دستور traceroute در سناریو بعدی آشنا خواهید شد.

شکل ۶–۲ اجرای دستور tracert بر روی pc0 در subnet مازندران را نشان می دهد.که برای تست اتصال با pc2 در subnet تهران استفاده شده است.هر یک از IP ها متعلق به interface یک روتر یا یک pc یا ...است که در اصطلاح به آن hope گفته می شود.چنانچه جدول مسیریابی به درستی ایجاد نشده باشد یا به هر دلیل نقطه ای از مسیر دچار اختلال شده باشد ، packet در pop مورد نظر گیر می کند . برای مثال ، شکل۶–۳، نتیجه دستور tracert را پس از حذف مسیر مربوط به subnet مقصد ، 192.168.3.0 نشان می دهد که از router مازندران حذف شده است.

مشاهده می کنید که packet در hope اول ،که اینترفیس router مازندران را نشان می دهد گیر کرده است .

PC>tra	PC>tracert 192.168.2.2						
Tracing route to 192.168.2.2 over a maximum of 30 hops:							
1	0 ms	0 ms	0 ms	192.168.1.1			
3	1 ms	12 ms	1 ms	10.10.12.1			
Trace	complete.	10 ms	13 ms	192.100.2.2			

شکل ۶-۲

PC≻tra	PC>tracert 192.168.3.2				
Tracin	ng route t	to 192.168.	3.2 over a	maximum of 30 hops:	
		0	0	400 400 4 4	
1	1 ms	u ms	u ms	192.168.1.1	
2	0 ms	*	0 ms	192.168.1.1	
3	*	0 ms	*	Request timed out.	
4	0 ms	*	0 ms	192.168.1.1	
5	*	0 ms	*	Request timed out.	
6	10 ms	*	0 ms	192.168.1.1	
7	*	1 ms	*	Request timed out.	
8	1 ms	*	0 ms	192.168.1.1	
9	*	0 ms	*	Request timed out.	
10	0 ms	*	0 ms	192.168.1.1	

# <sup>شکل ۶</sup>-۳ **سناریو شماره ۷**

### +-عنوان : Static Routing در محيط GN3

**۱-خلاصه:** در این سناریو ، با کمی تغییرات بر روی سناریو ۶ ، آن را در GN3 پیاه سازی خواهیم کرد. و با مفهوم اینترفیس loopback و همچنین مسیر های default آشنا خواهید شد.



شکل ۰–۷

**۲-توضیح :**در سناریوهای مربوط به Routing ، میتوان برای افزایش سادگی و سرعت طراحی در محیط شــبیه سـازی ، Swich و Host را از سـناریو حذف کرد و بجای آن از اینترفیس loopback استفاده کرد.

Ioopback interface -۲-۱ اینترفیس loopback ، اینترفیسی است مجازی ، که برای تست و رفع اشکال به کار می رود.این اینترفیس همیشه بطور پیش فرض up است ، و نه تنها بر روی تجهیزات شــبکه ، بلکه بر روی host ها نیز اســتفاده می شــود.برای مثال اگر اینترفیس loopback 0 بـا آدرس 192.168.3.1 را بر روی Router ایجاد کنیم ، همانند آن اســت که شـبکه ای با Host ، subnet به Router متصـل اسـت ، که در آن یک Host با آدرس 192.168.3.1 وجود دارد.این اینترفیس نقش host های که در سناریو ۶ وجود داشت را ایفا می کند .

**نکته :** شـما می توانید به تعداد بسـیار زیادی اینترفیس loopback ایجاد کنید.برای مثال برای ایجـاد اینترفیس loopback 0 در Router از دسـتور interface loopback 0 در محیط config استفاده خواهید کرد.

**Default route**-۲-۲ همانطور که پیش تر گفته ایم ، Router پس از دریافت Default route و در IP، مقصد آن را با هر یک از مسیر های موجود در جدول مسیریابی خود مقایسه می کند و در صورت وقوع یک match ، آن را از interface مربوطه forward خواهد کرد.

اگر Router نتواند به ازای IP مقصد packet ، در جدول مسیریابی ، مسیری پیدا کند ، packet را از مسیری که default route مشخص میکند ، forward خواهد کرد .به عبارتی به ازای هر IP مقصدی با router رخ می دهد.اگر router نتواند در جدول مسیریابی خود به ازای IP مقصد ، مسیری پیدا کند و default route هم وجود نداشته باشد ، discard ، packet خواهد شد.

**نکته :** خط زیر نحوه ایجاد یک default route را نشان می دهد :

Router(config):ip route 0.0.0.0 255.255.255.255 10.10.11.1

یعنی اگر برای packet ، مسیری یافت نشد ، برای هر IP مقصدی ، بسته را به سمت router با 10.10.11.1 ، IP هـدایـت کن.توجـه کنید که default router آخرین مسیری اسـت که router به آن رجوع می کند. حال که با مفهوم default route آشنا شدید با یک مثال کاربرد آن را شرح می دهیم.



شکل ۱–۷

R1 ، Router در شــکل ۱–۷ را در نظر بگیرید .تنها یک مسـیر خروجی از طریق subnet وجود دارد.فرض کنید می خواهیم ، R1 از همین مسیر به اینترنت و هزاران subnet دیگر مرتبط شود .پس باید به ازای هر subnet مقصد یک مسیر در جدول مسیریابی R1 ایجاد کنیم.یعنی هزاران مسیر ایجاد کنیم ، درحالی که می دانیم تمامی packet ها ، با هر IP مقصدی در نهایت باید از طریق forward ، s0/1 شوند.اینجاست که default route کار را ساده خواهد کرد.

default route به R1 خواهد گفت اگر مسیری به ازای مقصد مورد نظر یافت نشد آن را از forward ، s0/1 کند .

### ۲-۳–دستور Ping و ۲-۳

این دو دستور برای رفع اشکال و تست برقراری اتصال استفاده می شود.که معادل آنها را بر روی pc قبلا بررسی کردیم.و در router هم این دو دستور همان کار مشابه را انجام می دهند.فقط هنگام استفاده از این دو دستور به این نکته توجه داشته باشید :packet که برای تست توسط این دستور تولید می شود ، I مبدا آن ، Interface خروجی Router است.و به دلیل آنکه شما به ازای این I در تعاو می مسیری تعریف نکردید ، بسته قادر به عبور نخواهد بود و به ازای این مسیری تعریف می معادل آن ، Router در ستور می در است.و به دازای این I در یا می دهند.فقط یا در یا می دو دستور به این نکته توجه داشته باشید این کار مشابه را انجام می دهند.فقط بو این دستور تولید می شود ، I مبدا آن ، Interface خروجی Router است.و به دلیل آنکه شما به ازای این IP در Router های میانی مسیری تعریف نکردید ، بسته قادر به عبور نخواهد بود و پیام شکست مواجه می شوید.برای آنکه این دو دستور درست وظیفه خود را به انجام برسانند لازم

است تا source مربوط به ping ، packet و trace route را مشخص کنید.برای مثال بر روی R1 ، Router با اینترفیس loopback ، از 192.168.2.1 به مقصد 192.168.1.1 ، از دستور ping و trace route بصورت زیر استفاده می کنیم:

ping 192.168.1.1 source 192.168.2.1

trace route 192.168.1.1 source 192.168.2.1

۳-پیکربندی:

۳−۱− در محیط پیکربندی ، برای هر Router ، اینترفیس loopback ایجاد کنید و به آن و اینترفیس loopback ایجاد کنید و به آن و اینترفیس ها Router مطابق شکل ۰۹-۲ ، IP اختصاص دهید.توجه کنید router استفاده شده در این سناریو از سریc3700 است.

#### **Tehren router**

Tehran(config)#interface loopback 0 Tehran(config-if)#ip address 192.168.3.1 255.255.255.0 Exit

Tehran(config)# interface fastEthernet 0/0 Tehran(config-if)#ip address 10.10.11.2 255.255.255.252 no shutdown exit

Tehran(config)#interface fastEthernet 0/1 Tehran(config-if)#ip address 10.10.12.2 255.255.255.252 no shutdown exit

#### Mazandaran router

Mazandaran (config)#interface loopback 0 Mazandaran (config-if)#ip address 192.168.1.1 255.255.255.0 Exit

Mazandaran (config)# interface fastEthernet 0/0 Mazandaran (config-if)#ip address 10.10.11.1 255.255.255.252 no shutdown exit

### **Esfahan router**

Mazandaran (config)#interface loopback 0 Mazandaran (config-if)#ip address 192.168.2.1 255.255.255.0 Exit

Esfahan (config)# interface interface fastEthernet 0/0 Esfahan (config-if)#ip address 10.10.12.1 255.255.255.252 no shutdown exit

۲−۲ – با توجه به اینکه هر سه subnet باید با هم ارتباط داشته باشند جداول مسیریابی را برای هر سـه Router ایجاد کنید.توجه کنید جداول مسیریابی در این سـناریو دقیقا همانند سـناریو قبلی است.

### **Tehren router**

Tehran(config)#ip route 192.168.1.0 255.255.255.0 10.10.11.1

Tehran(config)#ip route 192.168.2.0 255.255.255.0 10.10.12.1

#### Mazandaran router

Mazandaran (config)#ip route 192.168.3.0 255.255.255.0 10.10.11.2 Mazandaran (config)#ip route 192.168.2.0 255.255.255.0 10.10.11.2

#### **Esfahan router**

Esfahan (config)#ip route 192.168.2.0 255.255.255.0 10.10.12.2 Esfahan (config)#ip route 192.168.1.0 255.255.255.0 10.10.12.2

### ۴-مانیتورینگ و رفع اشکال :

- برای مشاهده IP اختصاص داده شده و همچنین وضعیت up یا down بودن interface
   ها از دستور show ip interface brief در محیط enable ، استفاده کنید.
- در محیط enable از دستور show ip router برای مشاهده جدول مسیریابی router
   استفاده کنید.
- از دستور ping و trace route برای عیب یابی و تست برقراری اتصال استفاد کنید.نتیجه این دو دستور را بر روی Router اصفهان در دو شکل زیر مشاهده خواهید کرد.



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