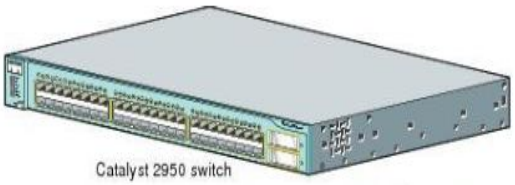
کارگاه شبکه های کامپیوتر
VLAN کردن سوئیچ
مسیریابی ROUTER

مدرس: مهندس علی زواره

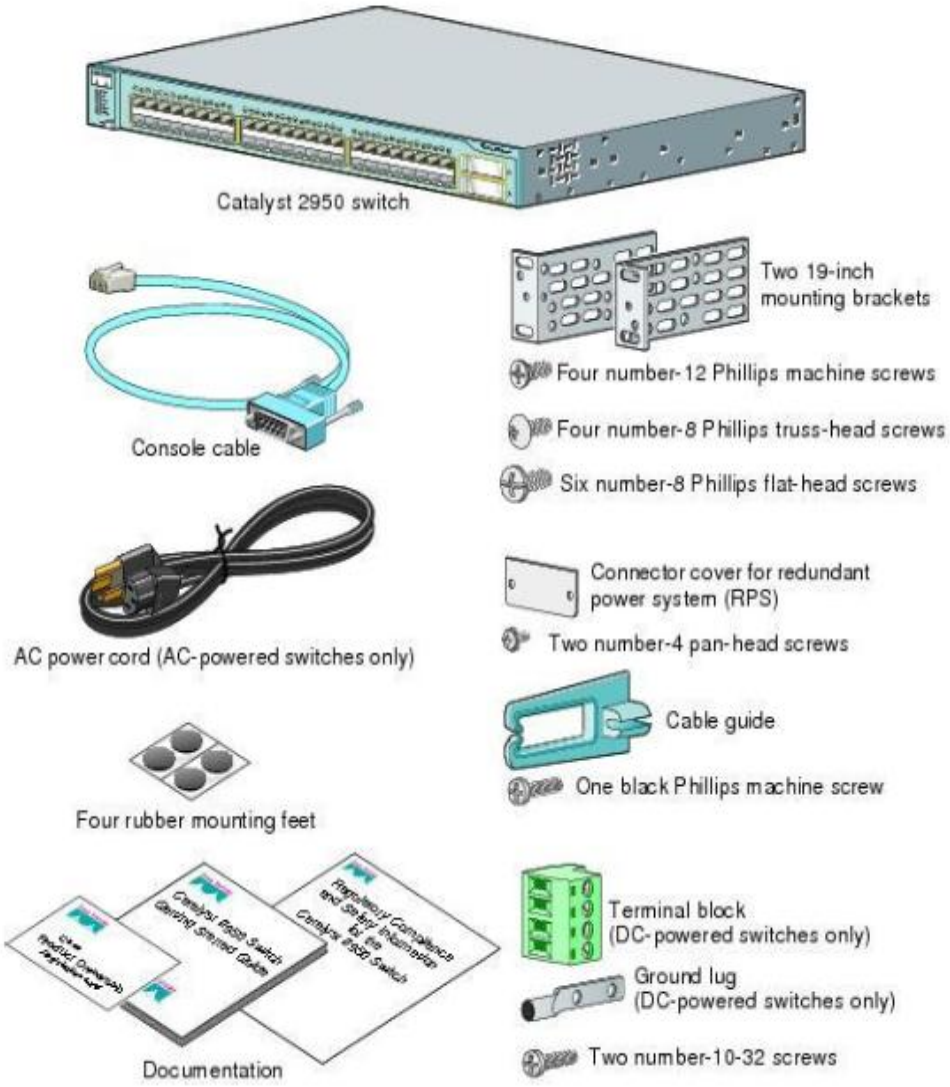
سوئیچ لایه دو



نگاهی به سوئیچ ۲۵۹۰

سوئیچ ها در انواع مختلفی وجود دارند ۸و۱۶و۲۴و۲۶و۴۸ پورت و ... وجود دارند که بنا به نیاز خود یکی از این مدل ها را تهیه می کنیم، سوئیچ ها در انواع سرعت های ۱۰، ۱۰۰، ۱۰۰۰ و ۱۰۰۰۰ مگابایتی وجود دارند و سیستم عامل های آنها مانند روترها IOS می باشد که اولین IOS آن مدل ۱/۱۲ بوده است.

زمانی که یک سوئیچ روشن می شود به حالت post می رود و در این مرحله تمام سخت افزار آن تست می شود و اگر یکی از پورت ها مشکلی داشت به رنگ کهربایی در می آید و اگر هیچ کدام مشکل نداشتند. همه آنها یک بار چشمک زده و اعلام آمادگی می کنند بعد از این کار سوئیچ به دنبال فایل IOS میگردد و وقتی فایل مورد نظر را پیدا کرد وارد مد CLI می شود.



چراغ های سوئیچ ها

سوئیچ ها از چراغ هایی تشکیل شده اند و این چراغ ها به ۴ نوع تقسیم می شوند:

Port status Led

روی این سوئیچها به ازای هر پورتی که وجود دارد یک چراغ چشمک زن هم وجود دارد که این چراغ به رنگ های مختلف نمایانگر می شود که هر رنگ آن را با هم مورد بررسی قرار می دهیم:

رنگ		علت
سبز		به این پورت کابلی متصل شده است اما فعال نشده است.
سبز چشمک زن		این پورت فعال و در حال ارسال و دریافت اطلاعات است
سبز و	**کهربایی**	در این حالت collision در سوئیچ رخ داده است
کهربایی		در این حالت پورت Disable شده اما به صورت دستی

OFF	به پورت کابلی متصل نشده است

Port Mode Led

در این حالت دو نوع چراغ وجود دارد:

UTL LED : این چراغ های نشان دهنده پهنای باند مصرفی در سوئیچ می باشند.

STST LED : زمانی که سوئیچ روشن شود این چراغ هم روشن می شود.

FDUP LED: در این حالت پورت ها در دو حالت Half-duplex و Full-duplex قرار دارند و اگر چراغ پورت خاموش باشد یعنی در حالت Half-duplex قرار دارد و اگر روش باشد و سبز در حالت Full-duplex قرار دارد.

100 یا Speed led : این چراغ نشان دهنده سرعت یک پورت می باشد که اگر خاموش باشد یعنی از ۱۰ مگابایت استفاده می کند و اگر روشن و سبز باشد یعنی از حداکثر سرعت استفاده می کند.

انواع مدهای سوئیچ

سوئیچ ها مانند روتر ها دارای سه مد user و privilege و Global و دستور ورود به این مدها مانند روترها می باشد.

```
Switch> en
Switch# conf t
Switch(config)#
```

بررسی VLAN (Virtual Link)

وقتی چندین کامپیوتر را به یک سوئیچ متصل می کنید آنها به راحتی می توانند با هم ارتباط داشته باشند و از منابع شبکه استفاده کنند، اما تعداد زیاد کامپیوترها می تواند حجم کاری سوئیچ را افزایش دهند، یعنی اینکه تمام سوئیچ ها در یک منطقه کاری با هم در ارتباط هستند و امنیت در این نوع شبکه ها بسیار پایین می آید ولی می توان با تقسیم یک منطقه به چندین منطقه امنیت را افزایش و ترافیک شبکه را به راحتی کنترل کرد.

یک مثال بزنم، شما مدیر شبکه یک شرکت هستید و این شرکت از سه بخش: حسابداری، فروش، اداری تشکیل شده است و می خواهید این چند اتاق را توسط سوئیچ به هم شبکه کنید که با متصل کردن همه کامپیوترهای این اتاق ها آنها به هم متصل می شوند و می توانند به منابع شبکه دسترسی داشته باشند با این کار ترافیک روی سوئیچ افزایش پیدا می کند چون همه این کامپیوترها در یک Broadcast Domain قرار دارند و امنیت در این شبکه به خاطر دسترسی همگان به همه اطلاعات پایین می آید، شما که مدیر شبکه هستید باید کاری انجام دهید که این اتاق ها از هم جدا شوند. مثلاً کامپیوتر اتاق حسابداری را نتوانند با اتاق اداری ارتباط برقرار کند. خوب این کار توسط VLAN انجام می شود که همه کامپیوتر های اتاق حسابداری را می توان در یک منطقه قرار داد و با هم در ارتباط باشند و با اتاق های دیگر نتوانند در ارتباط باشند.

ایجاد VLAN

برای ایجاد یک VLAN در سوئیچ وارد مد Global شده و دستور زیر را وارد می کنید:

```
Switch (config)# vlan ?
<1-1005> ISL VLAN IDs 1-1005
```

همانطور که مشاهده می کنید بعد از تعریف vlan علامت سوال قرار دادیم که به ما تعداد vlan های قابل ایجاد را نمایش می دهد یعنی می توانیم از ۱ تا ۱۰۰۵ عدد vlan در یک سوئیچ تعریف کنیم، توجه داشته باشید که vlan 1 را نمی توانید ایجاد کنید چون به صورت پیش فرض تمام پورت های سوئیچ در این vlan قرار دارد و به خاطر همین است که تمام پورت ها با هم در ارتباط هستند.

```
Switch (config)# vlan 20
Switch (config-vlan)# name Tehran
```

در این دستور Vlan شماره ۲۰ تعریف شده است و بعد از آن یک اسم از طریق دستور name به آن نسبت دادیم برای مشاهده vlan از دستور زیر استفاده می کنیم:

```
Switch # show vlan brief
Switch#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, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
20 Tehran active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

قرار دادن پورت ها داخل vlan مورد نظر

این کار به دو صورت انجام می پذیرد:

Static

این روش به صورت دستی میباشد و می توانیم هر پورتی را در vlan مورد نظر خود قرار دهیم، این روش یکی از امن ترین روش ها می باشد.

Dynamic

در این روش نسبت دادن پورت به یک vlan از طریق دستی صورت نمی گیرد بلکه از طریق یک سرور مرکزی با نام VMPS (Vlan Membership Policy Server) ایجاد شده و مدیریت می شوند.

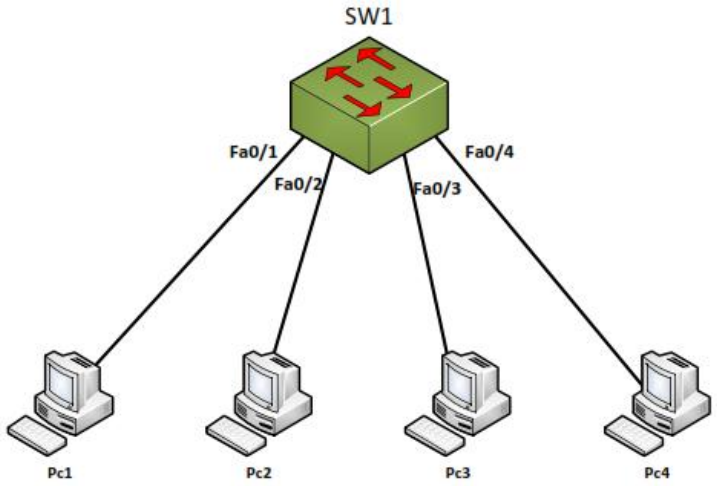
هر پورت سوئیچ از دو مد تشکیل شده است: mode Access و mode Trunk

که بطور پیش فرض در مد access قرار دارند و برای ایجاد vlan باید در این مد باشیم.

ایجاد VLAN

یک سوئیچ و چهار Pc متصل به آن ایجاد نمایید.

طبق جدول زیر IP های زیر را به کامپیوتر دهید:



Station	IP Address	Subnet Mask
Pc1	192.168.1.1	255.255.255.0
Pc2	192.168.1.2	255.255.255.0
Pc3	192.168.1.3	255.255.255.0
pc4	192.168.1.4	255.255.255.0

تنظیمات کامپیوترها برای VLAN

PC1
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switch mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
PC2
Switch(config)#int f0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
PC3
Switch(config)#int f0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex
PC4
Switch(config)#int f0/4
Switch(config-if)#switchport access vlan 20
Switch(config-if)#ex

وضعیت VLAN ایجاد شده با دستور show vlan brief

Switch#show vlan brief
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active 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
Gig0/1, Gig0/2
10 VLAN0010 active Fa0/1, Fa0/2
20 VLAN0020 active Fa0/3, Fa0/4
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

وضعیت دستور ping از pc1 به pc4 قبل و بعد از VLAN

قبل از VLAN

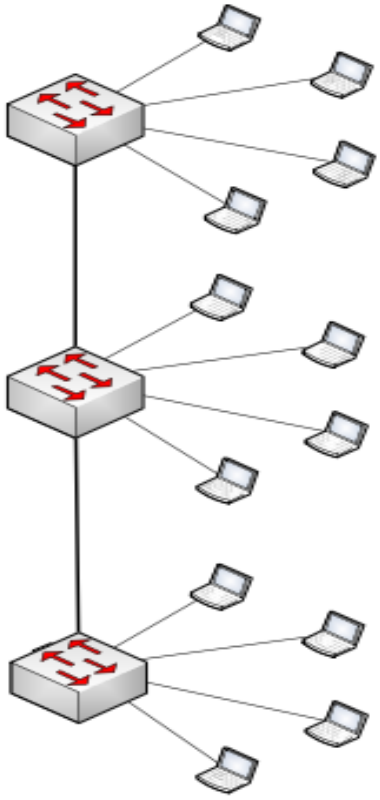
PC>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=2ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

بعد از VLAN

PC>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.

Trunk Mode

با یک مثال مفهوم Trunk را توضیح می دهیم. فکر کنید یک ساختمان سه طبقه داریم و در هر طبقه از یک سوئیچ برای شبکه کردن کامپیوترها استفاده شده است و تمام سوئیچ ها به هم متصل شده اند، نکته مهم در این قسمت این است که در هر طبقه برای هر بخش یک vlan تعریف شده است و پورت ها را داخل vlan مورد نظر قرار می دهید، ولی یک مشکل اینجا و جود دارد و این است که سوئیچ باید با vlan های دیگر در طبقات مختلف در ارتباط باشند. برای حل این مشکل باید از Trunk استفاده کرد.



Tag زدن روی فریم ها

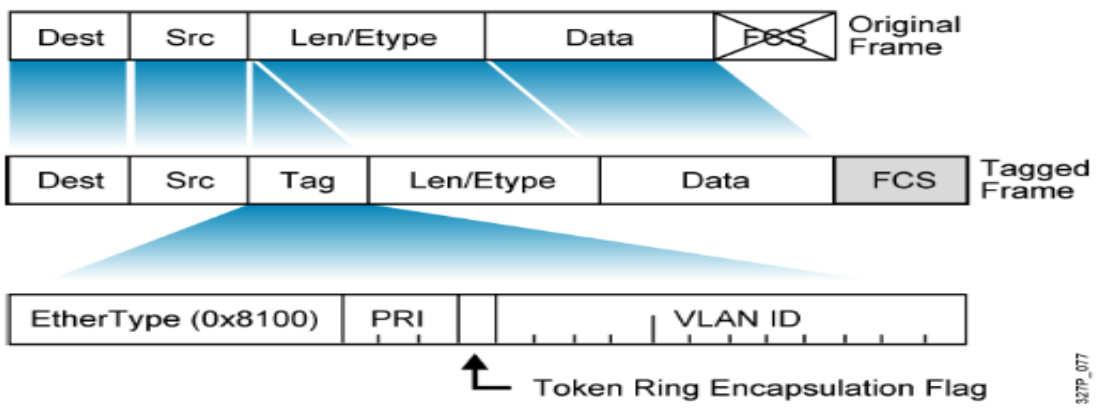
برای انتقال Vlan ها در مد Trunk دو روش وجود دارد که از طریق آن یک Vlan شناسایی می شود:

ISL (Inter-Switch Link Protpcol)

802.1 Q

روش ISL: یک استاندارد برای بسته بندی فریم ها برای انتقال در یک مسیر یا همان Trunk که این استاندارد مختص شرکت سیسکو بوده و به صورت پیش فرض در دستگاههای لایه دوم این شرکت فعال می باشد. این پروتکل بطور پیش فرض در سویچ های شرکت سیسکو فعال می باشد.

روش 802.1 Q: یک استاندارد Open Source می باشد و مختص شرکت خاصی نیست و اگر در شبکه خود از سوئیچ های شرکت های متفاوت استفاده می کنید برای برچسب زدن روی فریم ها باید از این استاندارد استفاده کنید. این پروتکل ساختار فریم ها را به کل تغییر می دهد.



فعال سازی پروتکل 802.1 Q

برای فعال کردن این پروتکل باید وارد interface مورد نظر شوید و دستور زیر را وارد کنید:

```
Switch(Config-if)# switchport mode trunk
Switch(Config-if)# switchport trunk encapsulation dot1q
```

با اجرای این دستورات یک سوئیچ تمام Vlan ها را برچسب گذاری کرده و از خود عبور می دهد.

فعال سازی پروتکل 802.1 Q

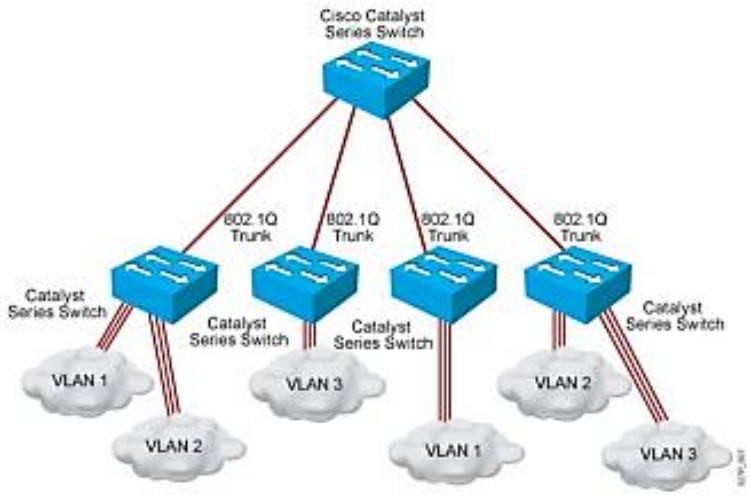
شاید شما بخواهید به سوئیچ بگویید که فقط Vlan های خاصی از وی عبور کنند برای این منظور از دستور زیر استفاده می کنیم:

```
Switch(Config-if)# switchport trunk allowed Vlan 10
```

با اجرای این دستور فقط Vlan 10 حق عبور را دارد و بقیه Vlan ها از این سوئیچ عبور نمی کنند. پس یک پورت در سوئیچ زمانی trunk می شود که بخواهد Vlan ها را بین دو دستگاه سوئیچ جابجا کنند.

به شکل زیر توجه کنید:

در این شکل سوئیچ ها به هم متصل شده اند و سوئیچ هایی که در زیر قرار دارند از Vlan های مختلفی تشکیل شده اند برای ارتباط Vlan1 به Vlan1 در سوئیچ دیگر باید پروتکل Trunk را روی پورتهای سوئیچ که به سوئیچ اصلی متصل است اجرا کنیم و بعد 802.1 Q را راه اندازی کنیم تا عملیات برچسب گذاری روی Vlan ها را انجام دهد.



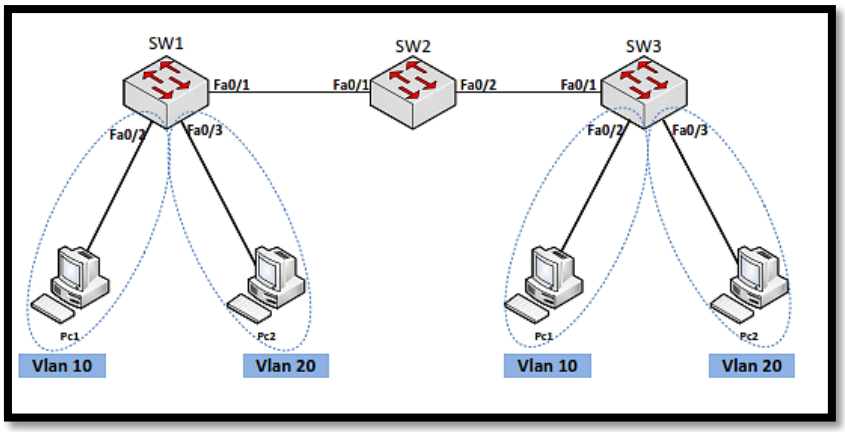
Native Vlan

همانطور که قبلاً گفتیم در تمام سوئیچ ها Vlan 1 وجود دارد و قادر به ایجاد و یا حذف آن نیستیم ولی وقتی چندین سوئیچ را با پروتکل 802.1 Q، Trunk می کنید در زمان انتقال Vlan 1 بین سوئیچ ها روی آنها هم برچسب گذاری می شود و همین کار باعث استفاده بیش از حد از پهنای باند شبکه می شود و برای جلوگیری از این کار باید روی پورتی که Trunk شده است دستور زیر را وارد کنیم:

```
Switch(Config-if)# switchport trunk native Vlan 1
```

با این کار Vlan1 در پروتکل Trunk انتقال داده نمی شود.

مثال ۴



Station	IP Address	Subnetmask
Pc1	192.168.1.1	255.255.255.0
Pc2	192.168.1.2	255.255.255.0
Pc3	192.168.1.3	255.255.255.0
pc4	192.168.1.4	255.255.255.0

بعد از این که Ip Address را در pc ها وارد کردیم نوبت به تعریف Vlan در سوئیچ می باشد.

مراحل تعریف Vlan

در داخل هر یک از سوئیچ Vlan های ۱۰ و ۲۰ را به صورت زیر تعریف می کنیم:

```
Switch(config)#vlan 10
Switch(config)#vlan 20
```

بعد از تعریف vlan باید پورت متصل به pc را داخل vlan های مشخص شده قرار دهیم، مثلاً pc1 باید در vlan 10 قرار بگیرد برای اینکار وارد سوئیچ شده و بعد وارد interface 0/2 که به pc1 متصل است می شویم و آن را طبق دستور زیر داخل vlan10 قرار می دهیم:

```
Switch(config)# int fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config)# int fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
```

بعد از اینکه این کار را انجام داده اید یک ping از pc1 به pc3 بگیرید و مطمئن باشید جواب نمی گیرید، به خاطر اینکه پروتکل Trunk روی پورت های سوئیچ فعال نشده و به خاطر همین ارتباط برقرار نمی شود. وارد sw1 شوید و پورتی که به طرف sw2 می رود را Trunk کنید:

```
Switch(config)# int fa0/1
Switch(config-if)# switchport mode trunk
```

بعد از این کار مدل برچسب گذاری روی فریم ها را باید مشخص کنید که ISL باشد یا 802.1Qوجود که در برنامه Packet Tracer به صورت پیش فرض dot1q می باشد و ISL وجود ندارد که این کار بعید بود از شرکت سیسکو چون در سوئیچ ۲۹۵۰ استاندارد ISL وجود ندارد، که مختص سیسکو است. بقیه پورت های متصل به سوئیچ های دیگر را Trunk کنید:

SW2:

```
Switch(config)# int fa0/1
Switch(config-if)# switchport mode trunk
Switch(config)# int fa0/2
Switch(config-if)# switchport mode trunk
```

SW3:

```
Switch(config)# int fa0/1
Switch(config-if)# switchport mode trunk
```

بعد از این کار ارتباط بین Vlan ها برقرار می شود و Pc1 با Pc3 با هم ارتباط برقرار می کنند.

بعد از این مثال سوالی که برای شما ایجاد می شود که اگر تعداد سوئیچ ها زیاد باشد و ما بخواهیم داخل هر کدام از سوئیچ ها vlan تعریف کنیم کار بسیار وقت گیری است، آیا روش دیگری هم وجود دارد؟

بله، روش دیگری هم وجود دارد که می توانیم در یک سوئیچ با هر سوئیچی در شبکه vlan تعریف کند و این vlan ها به صورت خودکار وارد سوئیچ دیگر می شوند که به این روش Vlan Trunking Protocol (VTP) می گویند.

دستورات محیط CLI برای روتر

هنگام ورود به محیط CLI از طریق کابل کنسول توسط برنامه ترمینال Terminal ابتدا بعد از جواب No دادن به setup mode وارد مد کاربری می شویم و به شکل Router> خط فرمان دیده می شود.

با فرمان Enable یا En واد مد privilege می شویم که خط فرمان بصورت Router# دیده می شود. برای برگشت به مد قبلی می توان از فرمان Exit استفاده کرد.

برای ورود به مد Global باید از دستور زیر استفاده کرد:

```
Router# configure terminal یا Conf T
Router(config)#
```

برای بازگشت به مد privilege می توان از کلیدهای Ctrl+Z استفاده کرد.

مشاهده وضعیت اینترفیس های روتر

یا خلاصه آن بصورت دستور زیر

```
Router# show ip interface brief
Router#sho ip int bri
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet0/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
```

همانطور که ملاحظه می کنید روتر انتخاب شده ما دارای دو اینترفیس صفر و یک می باشد که در حالت خاموش down می باشد.

دستور دادن IP به اینترفیس های روتر

برای آدرس دادن به اینترفیس روتر باید به مد Global برویم بعد با دستورات زیر وارد پورت اینترفیس بشویم و آدرس دهی خود را انجام دهیم.

```
Router(config)# interface FastEthernet 0/0
```

بعد از اجرای دستور بالا وارد پورت اینترفیس می شویم دستور خلاصه بالا به صورت int fa 0/0 میباشد.

Router(config-if)# ip address 192.168.1.1 255.255.255.0

بعد از دادن آدرس آی پی باید اینترفیس مربوطه را روشن یا به عبارت دیگر فعال نمود.

Router(config-if)#No Shutdown

توجه: بعد از انجام دستورات بالا اگر از دستور show protocols یا sho ip int bri استفاده کنیم آدرس داده شده به اینترفیس مشاهده میشود و وضعیت آن از down به up تغییر می کند.

راههای دسترسی به روتر و رمزگذاری آن

راههای دسترسی به روتر از طریق پورت Consol و پورت Aux و Telnet می باشد. برای امنیت ورود به روتر می توان راههای ورود را رمزگذاری و پسورد دار نمود.

دستور ورود به کنسول و رمز گذاری آن

Router#conf t
Router(config)#
Router(config)#Line consol 0
Router(config-line)#password 123
Router(config-line)#login برای فعال شدن پسورد باید این دستور اجرا شود

Ctrl+z

بعد از اجرای این دستور متوجه می شوید که پسوردی که دادید قابل مشاهده است Router# show running-config .

برای مشاهده نشدن پسورد بجای دستور Password از secret استفاده کنید البته اول باید دستور قبلی را حذف کرد که با دستور no password بر می گردد.

Router(config-line)# no password
Router(config-line)#secret 123
Router(config-line)#login

برای ورود به قسمت privilege نیز می توان پسورد گذاشت دستورات آن بصورت زیر است:

Router# conf t
Router(config)# enable secret 123
Ctrl+Z
Router# show running-config

حال می توانید مشاهده کنید که رمز قرار داده شده در مد privilege قادر به نمایش نمی باشد.

enable secret 5 1mERr$3HhIgMGBA/9qNmgzccuxv0

ورود از طریق AUX

Router#conf t
Router(config)# line aux 0
Router(config-line)# secret 123
Router(config-line)#login

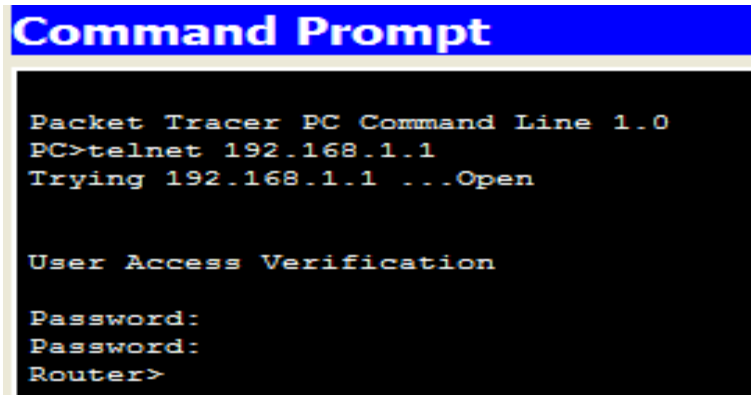
ورود از طریق Tel Net

برای ورود از راه دور از طریق یک کامپیوتر توسط نرم افزار Telnet پورتهای مجازی vty را فعال می کنیم.

یک روتر و یک کامپیوتر را با کابل cross به هم اتصال دهید و ip روتر را 192.168.1.1 قرار دهید

Router# conf t
Router(config)# int fa 0/0
Router(config-if)# ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

```
Router(config-if)# exit
Router(config)#line vty ?
Router(config)#line vty 0 15
Pass 123
login
```



و بعد به کامپیوتر رفته و ip آنرا 192.168.1.2 قرار دهید.

به قسمت CMD رفته و دستورات زیر را وارد کنید:

telnet 192.168.1.1

کد کردن تمام رمزها

```
Router# conf t
Router(Config)#service password-encryption
```

جلوگیری از رفته به مد user در اثر باز بودن و کار نکردن خط CLI این دستور در کنسول انجام می شود.

```
Router(Config-line)# Exec-timeout 0 0
```

جلوگیری از نشان دادن اطلاعات اضافه مانند فعال شدن یک پورت یا اجرای یک پروتکل

```
Router(Config-line)#logging synchronous
```

جلوگیری از جستجوی دستور اشتباه در روتر

```
Router(Config)# no ip domain-lookup
```

ذخیره و حذف اطلاعات بر روی NVRAM

```
Router# copy  running-config  statrup-config
Router# erase startup-config
```

ذخیره تغییرات و تنظیمات بر روی سرور

تنظیم IP Server :192.168.1.2

```
Router# conf t
Router(config)# int fa 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut down
Router# Copy running-config tftp
myhome#copy running-config tftp
Address or name of remote host []? 192.168.1.2
Destination filename [myhome-confg]? worker
Writing running-config....!!
[OK - 732 bytes]
732 bytes copied in 3.05 secs (240 bytes/sec)
```

فرمان Hostname- تغییر نام روتر

```
Router# Conf t
Router(config)#hostname melat_S15
Melat_S15#
```

فرمان banner-نمایش پیام زمان ورود به روتر

```
Router# conf t
Router(config)#banner ?
```

login Set login banner هنگام ورود از طریق تل نت است

هنگام ورود به کنسولmotd Set Message of the Day banner

```
Router(config)#banner motd @
Enter TEXT message. End with the character '@'.
Hello World@
Router(config)#banner login @
Enter TEXT message. End with the character '@'.
Welcome @
```

فرمان Description

برای نوشتن توضیحات بر روی اینترفیس روتر استفاده می شود.

```
Router(config-if)# desception OUR CITY ARE OUR HOME
```

فرمان Clock set

تنظیم ساعت و تاریخ روتر

```
Router(config)# clock set 10:05:04 19 nov 2016
```

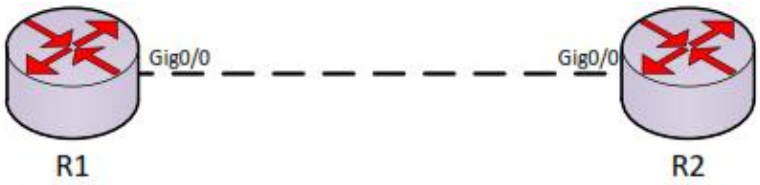
مسیریابی (IP Routing)

Routing

Routing یا مسیریابی، روشی است برای انتخاب مسیرهای شبکه های غیر محلی، برای انتقال اطلاعات از شبکه ای دیگر که این کار توسط پروتکل های مسیریابی انجام می شود. در مسیریابی بهترین و کوتاه ترین مسیر برای رسیدن اطلاعات مشخص می شود که این کار توسط جدول Routing مشخص شده و مسیر انتخاب می شود.

Routing Table

در این شکل دو روتر به هم متصل شده اند، IP هایی که به آنها داده شده در رنج ۱۹۲,۱۶۸,۱,۰ است که همانطور مشاهده می کنید، این IP به عنوان شبکه محلی روتر(رنگ قرمز) ثبت شده است یک کلمه C اول IP مشاهده می کنید که نشان دهنده Connected بودن آن می باشد البته هر حروفی که اینجا می نویسد در بالای آن کلمه مربوط به آن نوشته شده است.



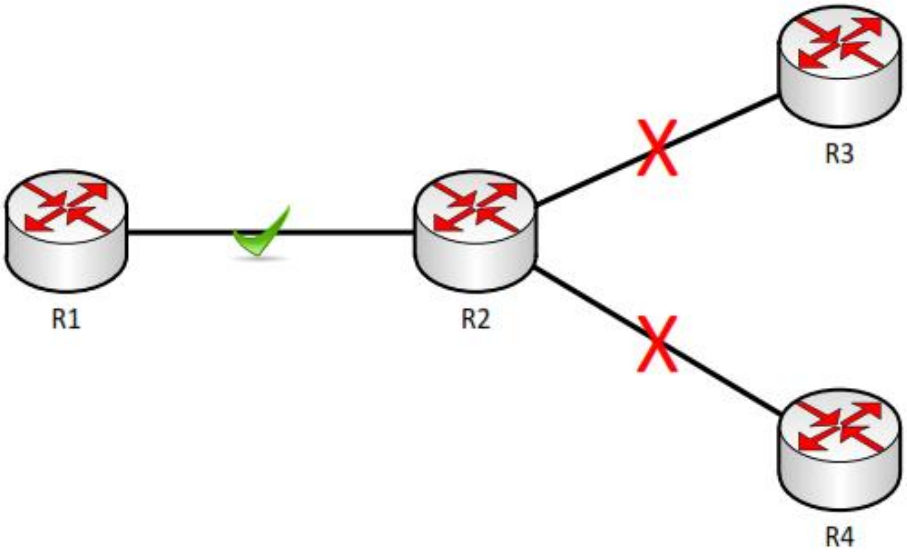

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     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
```

معرفی شبکه های غیر محلی به روتر

همانطور که در شکل می بینید R1 از اطلاعات شبکه ای که به وی متصل است خبر دارد اما از اطلاعات شبکه های دیگر در روترهای دیگر خبری ندارد، برای حل این مشکل دو راه کار وجود دارد، برای معرفی شبکه های غیر محلی به روترها:

Static Route

Dynamic Routing



۱- Static Route

استاتیک روت به دو روش می باشد:

IP Route

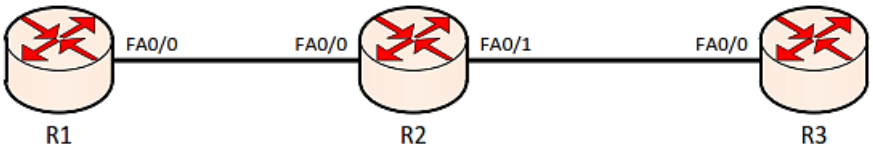
Default Route

روش IP Route

در این روش شبکه های غیر محلی را به صورت دستی به روتر معرفی می کنیم و مسیر حرکت را مشخص می کنیم. معرفی و حذف در این روش در شبکه های بزرگ بسیار وقت گیر و خسته کننده است و کمتر در این نوع شبکه ها استفاده می شود.

مثال ۱

سه روتر وارد صفحه کنید و آنها را با کابل cross به هم متصل کنید، مانند شکل Ip های روتر ها به صورت جدول فوق وارد نمایید.



تنظیمات اینترفیس روترها		
R1	F 0/0	192.168.1.1
R2	F 0/0	192.168.1.2
	F 0/1	192.168.2.1
R3	F 0/0	192.168.2.2

۱-۱- روش IP Route حالت Static Routing

برای اینکه متوجه بشوید به روترها درست IP داده ایم از دستور Ping استفاده می کنیم در روتر R1 به حالت Privileged رفته و دستور زیر را اجرا کنید:

Router# ping 192.168.1.2

نتیجه کار پیام زیر می شود که علامت تعجب (!!!!.) نشانه وصل بودن است. اگر به IP 192.168.2.2 دستور ping بگیریم متوجه می شویم که وصل نیستیم و نیاز به Routing داریم.

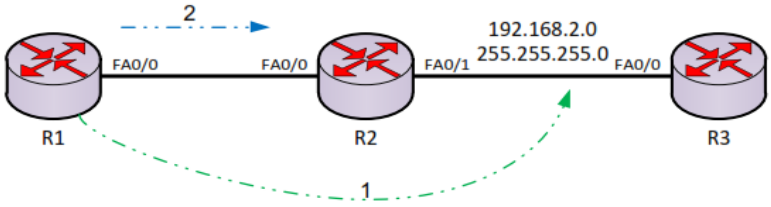
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

دستور IP ROUTE

در روتر R1 وارد مد گلوبال می شویم و دستور زیر را وارد می کنیم:

Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.2

اینگونه بخوانید برو به شبکه 192.168.2.0 با 255.255.255.0 subnet mask و از 192.168.1.2 عبور کن.

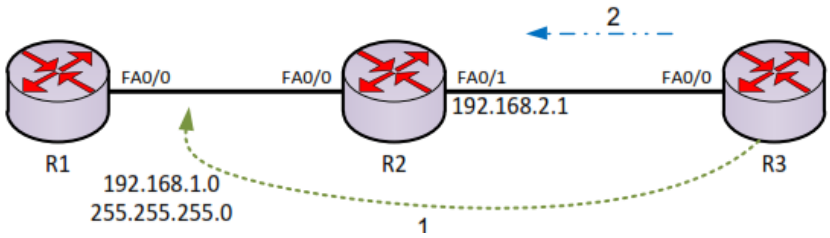


دستور IP ROUTE

در روتر R3 وارد مد گلوبال می شویم و دستور زیر را وارد می کنیم:

Router(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.1

اینگونه بخوانید برو به شبکه 192.168.1.0 با 255.255.255.0 subnet mask و از 192.168.1.2 عبور کن.



دستور IP ROUTE

حالا اگر از روتر R1 به روتر R3 با IP 192.168.2.2 دستور ping را انجام دهیم ارتباط برقرار است.

```
Router# ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms
```

برای نمایش جدول روتینگ از دستور Show IP Route در مد Privileged روتر R3 استفاده کنید.

همانطور که مشاهده می کنید لیست شبکه های متصل به روتر را با حرف C مشخص کرده و شبکه ای که با حرف S مشخص شده همان شبکه Static است که به صورت دستی تعریف شده است.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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

C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 192.168.1.2
```

۲-۱- روش Default Routeحالت Static Routing

اگر تعداد شبکه زیاد باشد استفاده از روش IP Route بسیار وقت گیر خواهد بود لذا از طریق این روش می توان روترها را به هم معرفی کرد و نیاز به معرفی تک تک شبکه ها نیست فقط به روتر می گوییم هر چیزی که نمی دانی را بفرست به روتر کناری.

در ادامه کار قبلی ابتدا با دستور No IP Route مقدار دهی قبلی را پاک نمایید.

```
Router(config)# no ip route 192.168.2.0 255.255.255.0 192.168.1.2
Router(config)# no ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

در روتر R1 :

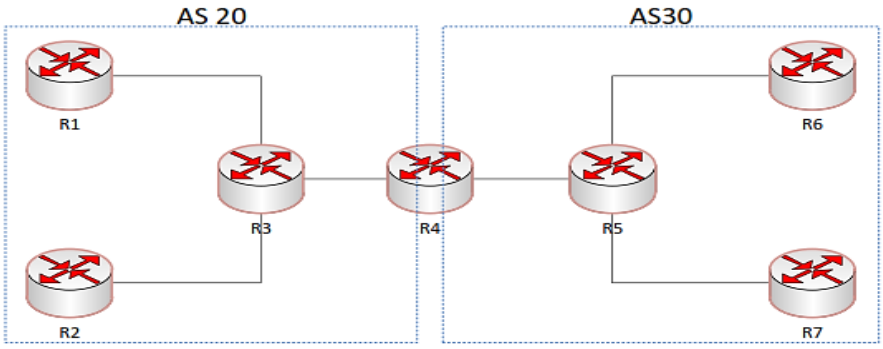
```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

در روتر R3:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

AS (Autonomous System)

اصطلاح AS (Autonomous System)- به مجموعه ای از روترها که در یک ناحیه قرار دارند می گویند. تعداد AS می تواند عددی بین ۱ تا ۶۵۵۳۵ می باشد.



انواع پروتکلهای مسیریابی

پروتکلهای مسیریابی دو دسته می باشند:

IGPs (Interior Gateway Protocol)
EGPs (Exterior Gateway Protocol)

پروتکلهای IGPs

به روتینگ پروتکلهایی که داخل یک AS کار می کنند و با هم در ارتباط هستند مانند پروتکلهای IGRP, RIP, EIGRP, OSPF پروتکلهای IGPs گفته می شود.

پروتکلهای EGPs

به روتینگ پروتکلهایی که می توانند AS های مختلف را به هم ارتباط دهند مانند پروتکل BGP پروتکل های EGPs گفته می شود که به آنها روترهای مرزی هم گفته می شود.

۲- روش Dynamic Routing

این روش بصورت دستی انجام نمی شود و از Routing Protocols استفاده می کنند. به سه روش انجام می پذیرد:

Distance Vector (بردار مسافت)

Link State (وضعیت اتصال)

Hybrid (ترکیبی)

Distance Vector (بردار مسافت)

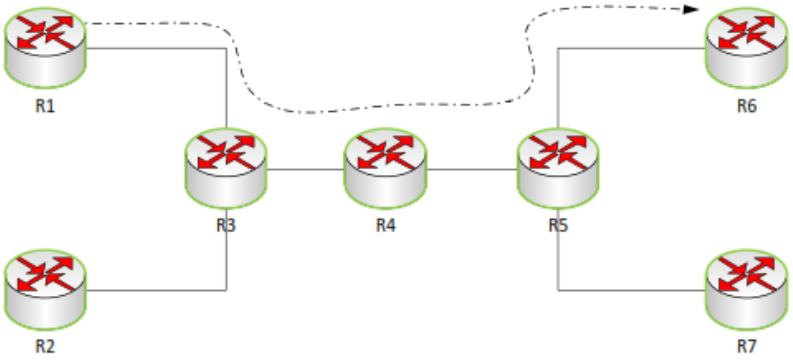
به پروتکل هایی گفته می شود که فقط و فقط با روتر کناری خود در ارتباط هستند و تمام اطلاعات خود را به روتر کناری خود منتقل و دریافت می کنند.

دراین پروتکلها اگر روتری، روتر کناری خود را بشناسد، می تواند بهترین مسیر را از روتر کناری خود دریافت کند، روتینگ پروتکل های IGRP و RIP این نوع هستند. الگوریتمی که این نوع پروتکل ها با آن کار می کنند Bellman_Ford می باشد که ویژگی های آن بصورت زیر است:

ساخت جدول Routing برای آدرس های شبکه

شناسایی شبکه های متصل به آن و ثبت در جدول

انتقال اطلاعات این جداول به صورت کلی در زمان مشخص که به آن Periodic Update می گویند.



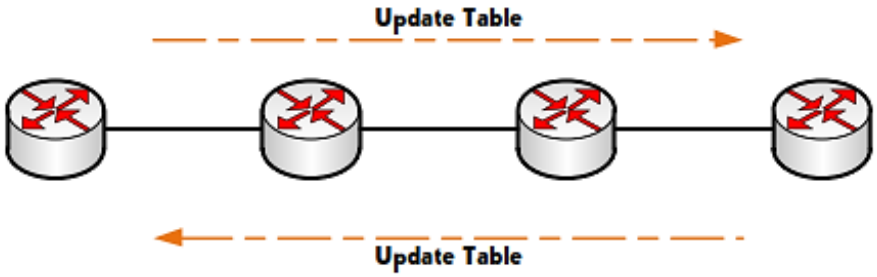
طرز کار پروتکل Distance Vector

این نوع پروتکل در جدول روتینگ خود ابتدا، شبکه های Connect به خود را درج می کنند

و بعد از ارتباط با روترهای دیگر بهترین مسیر را انتخاب و در جدول خود درج می کنند.

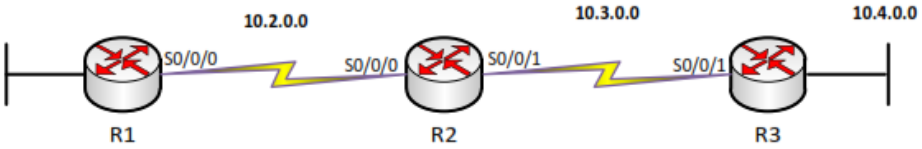
روترها جداول خود را به صورت Broadcast به روتر مجاور خود می فرستند که در پروتکل RIP به IP 255.255.255.255 و در پروتکل IGRP به IP 224.0.0.9 فرستاده می شود

و بعد روتر در پاسخ به روتری که Update فرستاده اطلاعات جدول خود را بصورت Unicast به این روتر می دهد و به همین صورت همه روترها از کل شبکه موجود با خبر می شوند.



متریک (Metric) یا Hop Count

در جدول روتینگ معیاری وجود دارد بنام متریک *که تعداد روترهای سر راه برای رسیدن به شبکه مورد نظر را مشخص می کند.* در یک پروتکل مشخص، برای رسیدن به یک شبکه اگر تعداد روترهای سر راه ۳ تا باشد، متریک می شود ۳ و به این هم توجه داشته باشید که هرچی متریک کمتر، مسیر بهتر و سریعتر می باشد و همان مسیر انتخاب می شود.



Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Convergence Time

به مدت زمانی گفته می شود که یک روتر به حالت پایدار می رسد و تمام شبکه های خود و اطراف خود را می شناسد و در جدول خود ثبت می کند.

بعد از این که روتر به حالت پایدار رسیده و جدول روتینگ خود را کامل کرده در طی زمان های مشخص تمام جدول روتینگ خود را به صورت Full Update به روتر های دیگر ارسال می کند، تغییری در جدول این روتر صورت بگیرد چه نگیرد این Update ارسال می شود. به این روش ارسال اطلاعات که در طی زمان مشخص صورت می گیرد می گویند. Periodic Update که این یکی از مهمترین ویژگی پروتکل های Distance Vector می باشد.

پروتکل RIP (Routing Information Protocol)

این پروتکل یک از محبوب ترین پروتکل های روتینگ و یک از قدیمی ترین آنها هم است.

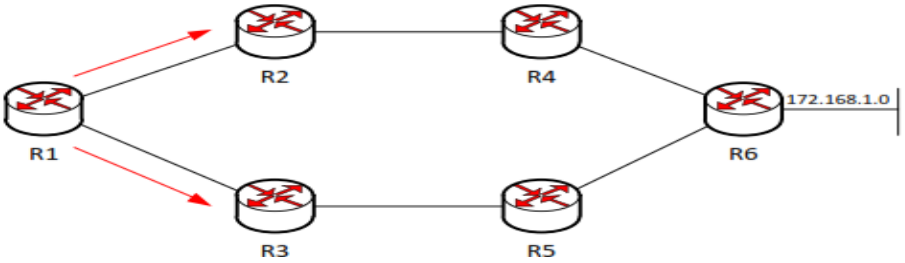
این پروتکل زیر مجموعه پروتکل های Distance Vector می باشد، و یک پروتکل IGPs می باشد

در داخل یک AS(Autonomous System) کار می کنند.

این پروتکل مخصوص شبکه های کوچک می باشد و در شبکه های بزرگ بالای ۱۵ روتر کاربرد ندارد یا به عبارتی دیگر حداکثر متریک آن ۱۵ می باشد.

یکی دیگر از ویژگی های این پروتکل این است که جدول روتینگ را به صورت کامل(Broadcast) در فواصل زمانی ۳۰ ثانیه به دیگر روترها ارسال می کند که به آن periodic Update می گویند.

یکی دیگر از ویژگیهای پروتکل RIP استفاده بهینه از شبکه است یا Load Balancing می باشد اگر دو مسیر با متریک یکسان داشته باشد اطلاعات را بر روی هر دو مسیر انتقال می دهد واین امر باعث افزایش کارایی شبکه می شود.



تفاوت پروتکل های Ver1 و RIP Ver2

پروتکل RIP بر دونوع می باشد:

RIP Version 1 (subnet mask را به همراه Net ID نمی فرستد.)

RIP Version 2

RIP V1	RIP V2
Classful	Classless
Broadcast based	User Multicast 224.0.0.9
No Support VLSM	Support VLSM

No authentication	Allows for MD5 authentication
No Supports for discontiguous networks	Supports discontiguous networks

راه اندازی پروتکل RIP

Router(Config)# Router RIP

Router(Config-router)# Network Network number

برای راه اندازی پروتکل RIP به صورت زیر عمل می کنیم:

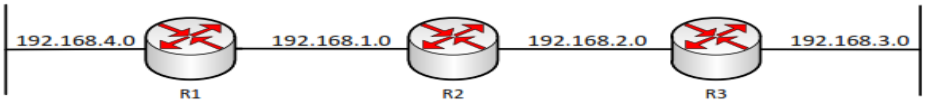
ابتدا وارد قسمت Global می شویم.

با دستور Router RIP پروتکلRIP بر روی روتر راه اندازی می شود.

بعد از آن باید شبکه های متصل به روتر را به آن معرف می کنیم.

مثال ۲

Packet Tracer را اجرا کرده و ۳ روتر مانند شکل زیر به صفحه اضافه کنید و آنها را از طریق کابل به هم متصل کنید و طبق شکل آدرس دهی کنید.



دستورات راه اندازی پروتکل RIP

R1

Router(Config)#router RIP

Router(Config-router)#network 192.168.1.0

Router(Config-router)#network 192.168.4.0

R2

Router(Config)#router RIP

Router(Config-router)#network 192.168.1.0

Router(Config-router)#network 192.168.2.0

R3

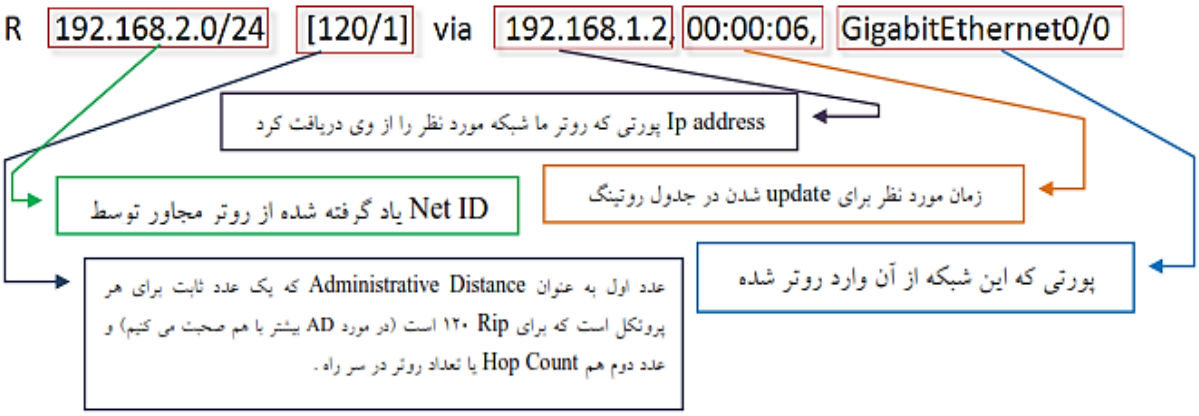
Router(Config)#router RIP

Router(Config-router)#network 192.168.2.0

Router(Config-router)#network 192.168.3.0

نتیجه دستور Show Ip route در روتر R1

```
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

     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
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
R    192.168.3.0/24 [120/2] via 192.168.1.2, 00:00:01, GigabitEthernet0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/1
L       192.168.4.1/32 is directly connected, GigabitEthernet0/1
```



تایمرها در پروتکل RIP

Update Timer

این زمان همان زمان periodic update می باشدو هر ۳۰ ثانیه یک بار، کل جدول روتینگ را به صورت Broadcast به ip 255.255.255.255 می فرستد، البته در پروتکل RIP Ver2 به صورت Multicast و به IP 224.0.0.9 می فرستد.

Invalid Timer

این تایمر زمانی اجرا می شود که در مورد یک شبکه هیچ گونه اطلاعاتی در زمان ۹۰ ثانیه دریافت نکند به حالت Hold رفته و در جدول روتینگ مقابل این شبکه جمله Possibly Down را درج می کند.

Hold down Timer

این تایمر با تایمر Invalid Timer با هم کار می کنند، هر موقع در مورد یک شبکه متریک بی نهایت را دریافت کند به حالت hold رفته و جمله Possibly down را در کنار آن شبکه در جدول روتینگ درج می کند و زمان آن ۱۸۰ ثانیه می باشد.

Flush Timer

این تایمر قاتل شبکه هایی است که بعد از ۲۷۰ ثانیه که تمام تایمرهای بالا به کار خود پایان دادن اگر update برای شبکه مورد نظر نرسد آن را از لیست یا همان Routing Table حذف می کند.

تغییر زمانهای تایمر بروز رسانی جدول روتر

```
Router# router RIP
Router(config-router)#timers basic ?
<0-4294967295> interval between updates
Router(config-router)#timers basic 10 ?
<1-4294967295> invalid
Router(config-router)#timers basic 10 50 ?
<0-4294967295> hold down
Router(config-router)#timers basic 10 50 90 ?
<0-4294967295> flush
Router(config-router)#timers basic 10 50 90 130
```

فرمان Debug

این فرمان برای کنترل و عیب یابی به کار می رود و برای فعال کردن آن برای پروتکل RIP دستور زیر را در مد Privileged وارد می کنیم:

```
Router# Debug IP RIP
```

برای غیرفعال کردن دستور Debug از دستور زیر استفاده می کنیم:

```
Router# no debug all
```

```
Router#
Router#
Router#
Router#
Router#
Router#debug ip rip
RIP protocol debugging is on
Router#RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
RIP: ignored v1 packet from 192.168.1.2 (illegal version)
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (192.168.1.1)
RIP: build update entries
      192.168.4.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/1 (192.168.4.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
```

راه اندازی پروتکل RIP Version 2

یکی از ویژگیهای مهم RIP V2 این است که classless و VLSM را پشتیبانی می کند و بهره دهی شبکه را افزایش می دهد.

برای اینکه در پروتکل RIP از این Version استفاده کنید در داخل RIP دستور version 2 را وارد کنید، مانند زیر عمل کنید:

Router(config)# router RIP

Router(config-router)# version 2