# CCNA 2013

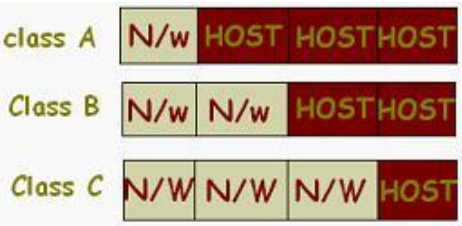
**ویـرایـش 93/05/11**

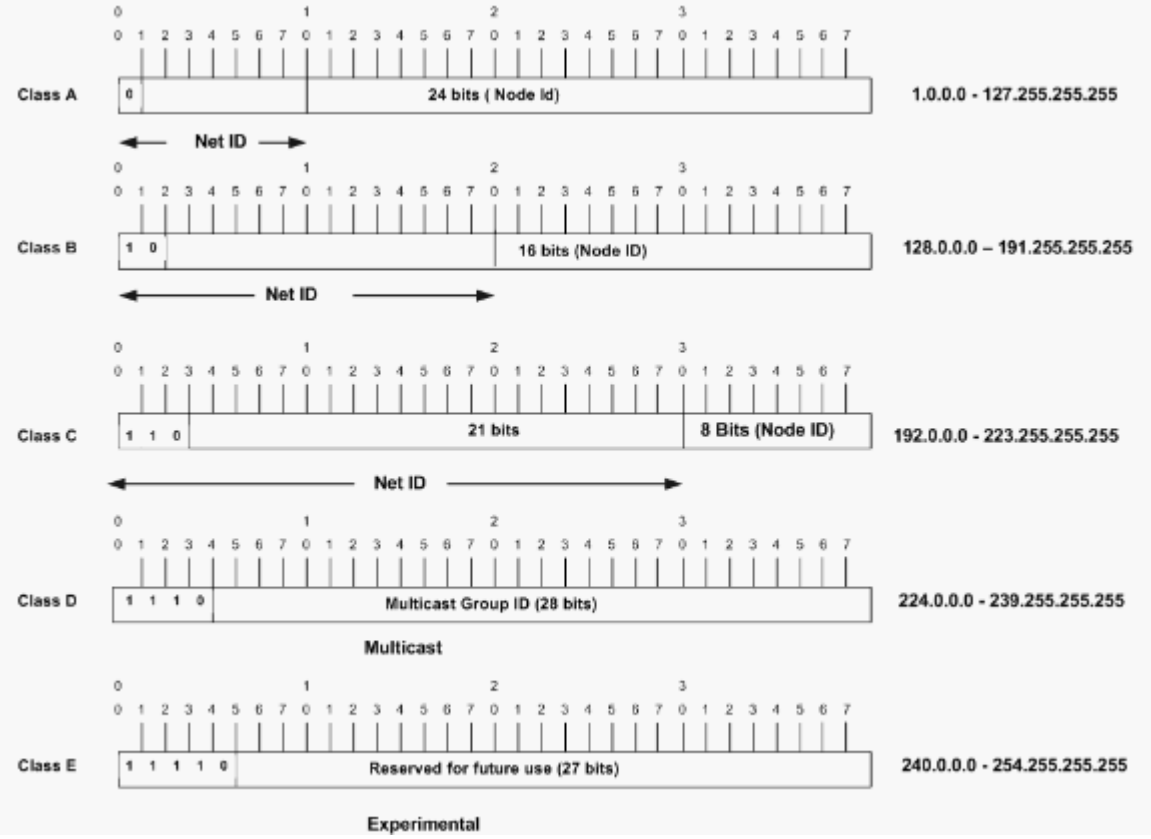
**فهرست مطالب:**

**موضوع:**
**صفحه**

# کلاس های استاندارد IP Address V4

IP Address v4 در 5 کلاس A, B, C, D, E که هریک از آنها شامل دو قسمت شناسه ارتباط NET ID و شناسه کاربر Host ID و یا Node ID میباشد. برای شناسائی آن ها از جدول زیر استفاده مینمائیم:




| Class | 1st Octet Decimal Range | 1st Octet High Order Bits | Network/Host ID (N=Network, H=Host) | Default Subnet Mask | Number of Networks | Hosts per Network (Usable Addresses) |
|---|---|---|---|---|---|---|
| A | 1 – 126* | 0 | N.H.H.H | 255.0.0.0 | 126 ($2^7 - 2$) | 16,777,214 ($2^{24} - 2$) |
| B | 128 – 191 | 10 | N.N.H.H | 255.255.0.0 | 16,382 ($2^{14} - 2$) | 65,534 ($2^{16} - 2$) |
| C | 192 – 223 | 110 | N.N.N.H | 255.255.255.0 | 2,097,150 ($2^{21} - 2$) | 254 ($2^8 - 2$) |
| D | 224 – 239 | 1110 | Reserved for Multicasting | | | |
| E | 240 – 254 | 1111 | Experimental; used for research | | | |

**كلاسهاي E جهت انجام كارهاي آزمايشي و تحقيقاتي استفاده مي شوند.**

**IP:192.168.20.10**
**Mask: 255.255.255.0**

**Network_ID: 192.168.20.0**
**First IP: Net_ID + 1 =** 192.168.20.1
**Last IP: Broadcast -1** = 192.168.20.254
**Broadcast: Next Network – 1=** 192.168.20.255

- **تعداد IP هايي كه در كلاس C مي توانيم براي تجهيزات موجود در شبكه استفاده كنيم:**

255.255.255.**0** ⇨ $2^8 - 2 = \cdots \ldots \ldots$

تعداد دوIP را از آن كم مي كنيم ، زيرا يكي از IP ها مخصوص شبكه است و ديگري مخصوص Broadcast مي باشد و قابل استفاده براي تجهيزات موجود در شبكه نمي باشند. (نمي توان آنها را به تجهيزات شبكه اختصاص داد).

Mask هاي متغيير:
از يك Subnet، Subnetهاي جديد را استخراج مي كنيم.

| Net ID | + Host ID |
|---|---|
| عدد 1 است و ثابت است. | متغير است |

مي توانيم Host ID ها را تغيير دهيم و از بيتهاي آن استفاده كنيم و Subnet جديد ايجاد كنيم.

نوع دوم Mask هاي موجود در شبكه، Maskهاي متغيير مي باشند كه براي حل آنها از سوالات زيراستفاده مي كنيم:

**1- به ازاي IPو Mask داده شده ، چه تعداد شبكه جديد قابل تعريف است:**

$2^{Subnet\ Bits}$

Subnet Bits تعداد بيتهاي متغيير mask مي باشد.

**2- به ازاي هر شبكه جديد چه تعداد Host وجود دارد؟**

$2^{Host\ Bits} - 2$

**3- Net ID شبكه هاي جديد چه مي باشد؟**

$256 - Subnet\ Mask$

**4- آدرس Broadcast براي هر شبكه چيست؟**

$Next\ Subnet - 1$

**5- اولين IP مورد استفاده براي هر شبكه چه مي باشد؟**

$Net\ ID + 1$

**6- آخرين IP مورد استفاده براي هر شبكه چيست؟**

$Broadcast - 1$

- **Example : IP:192.168.10.0 , Mask:255.255.255.192 .**

**S:**

| 255. | 255. | 255. | 192 |
|---|---|---|---|
| | | | 11000000 |

1. $2^2 = 4\ Subnets$
2. $2^6 - 2 = 64 - 2 = 62$ يعني 4 شكبه داريم كه در هر كدام 62 آي پي جاي مي گيرد .
3. $256 - 192 = 64$
4. .

| | A | B | C | D | … |
|---|---|---|---|---|---|
| Net_ID | 0 | 64 | 128 | 192 | … |
| First | 1 | 65 | 129 | 193 | … |
| Last | 62 | 126 | 190 | 254 | … |
| Broadcast | 63 | 127 | 191 | 255 | … |

---

- **Example. IP:192.168.10.0, Mask: 255.255.255.224**

**S:**

| 255. | 255. | 255. | 224 |
|---|---|---|---|
| | | | 11100000 |

1. $2^3 = 8\ Subnets$
2. $2^5 - 2 = 30\ Host$
3. 256-224=32
4. .

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| Net_ID | 32 | 64 | 96 | 128 | 160 | 192 |
| First | 33 | 65 | 97 | 129 | 161 | 193 |
| Last | 62 | 94 | 126 | 158 | 190 | 222 |
| Broadcast | 63 | 95 | 127 | 159 | 191 | 223 |

---

- **Example. IP:192.168.10.0 , Mask: 255.255.255.240**

**S:**

| 255. | 255. | 255. | 240 |
|---|---|---|---|
| | | | 11110000 |

5. $2^4 = 16\ Subnets$
6. $2^4 - 2 = 14\ Host$
7. 256-240=16
8. .

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| Net_ID | 16 | 32 | 48 | | | |
| First | 17 | 33 | | | | |
| Last | 30 | 45 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Broadcast** | **31** | **47** | | | | |

---

- **Example. IP:192.168.10.0 , Mask: 255.255.255.252**

**S:**

| | | | |
|---|---|---|---|
| **255.** | **255.** | **255.** | **252** |
| | | | **11111100** |

9. $2^6 = 64\ Subnets$
10. $2^2 - 2 = 2\ Host$
11. **256-252=4**
12. **.**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| **Net_ID** | **4** | **8** | **12** | **16** | | |
| **First** | **5** | **9** | **13** | | | |
| **Last** | **6** | **10** | **14** | | | |
| **Broadcast** | **7** | **11** | **15** | | | |

---

- **Example:** اگر يك IP بصورت **192.168.10.64** موجود باشد، **Mask** تعريف شده براي آن بصورت **255.255.255.192** است. آيا **Mask** داده شده با توجه به **IP** موجود صحيح است؟ و آيا **IP:192.168.10.68** مي تواند **Net_ID** باشد؟
  - آدرس **Broadcast** براي اين شبكه چيست؟
  - رنج قابل استفاده براي كاربران شبكه چه مي باشد؟

| | | | | |
|---|---|---|---|---|
| **255.** | **255.** | **255.** | **192** | |
| | | | **11000000** | ⇨ **/26** |

1. $2^2 = 4\ Subnets$
2. $2^6 - 2 = 62\ Host$
3. **256-192=64**
4. **.**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| **Net_ID** | **64** | **128** | **192** | | | |
| **First IP** | **65** | **129** | | | | |
| **Last IP** | **126** | **190** | | | | |
| **Broadcast** | **127** | **191** | | | | |

**192.168.10.64**غلط است. زيرا **192.168.10.64**، به عنوان **Net ID** مي باشد و نمي تواند آدرس **IP** سيستمي در شبكه باشد.
**IP:192.168.10.68** نمي تواند **Net_ID** باشد اما مي تواند **IP** يك سيستم باشد.

---

- **Example . IP: 192.168.10.38** و **Mask:255.255.255.24**

**S:**

| | | | | |
|---|---|---|---|---|
| **255.** | **255.** | **255.** | **192** | |
| | | | **11110000** | ⇨ **/28** |

1. $2^4 = 16$ تعداد شبکه هایي که مي توانيم داشته باشيم.
2. $2^4 - 2 = 14$ تعداد تجهيزاتي مي توانيم در هر شبکه داشته باشيم.
3. 256-240=16 طول گامها

| | 1th Subnet | 2th Subnet | 3th Subnet | 4th Subnet | … | 16th ...Subnet |
|---|---|---|---|---|---|---|
| Net_ID: | 0 | 16 | 32 | 48 | … | … |
| First IP: | 1 | 17 | 33 | | … | |
| Last IP: | 14 | 30 | 46 | | … | |
| Broadcast | 15 | 31 | 47 | | … | |

48-1=47

---

- **Example. IP: 192.168.10.13 و Mask:255.255.255.252**

حل:

1. 255-252=3 ⇨$2^2$ ⇨00 ⇨ 11111111. 11111111. 11111111.11111100⇨ /30
2. 8-6=2
3. $2^6 = 64$ تعداد شبکه هایي که مي توانيم داشته باشيم.
4. $2^2 - 2 = 2$ تعداد تجهيزاتي مي توانيم در هر شبکه داشته باشيم.
5. 256-252=4 طول گامها

| | 1th S. | 2th S. | 3th S. | 4th S. | 16th S. |
|---|---|---|---|---|---|
| Net_ID: | 0 | 4 | 8 | 12 | … |
| First IP: | | | 9 | | |
| Last IP: | | | 10 | | |
| Broadcast | | | 11 | | |

---

- **مثال: اگر يك Ip در كلاس C موجود باشد، از چه Mask ي استفاده كنيم تا به ازاي هر شكبه تعداد Host، 35 موجود باشد؟**

| 32< | 35 | <64 |
|---|---|---|
| $2^5$ | | $2^6$ |

**Host<$2^n - 2$**

35<$2^6 - 2$ ⇨ 11111111. 11111111. 11111111.11**000000** تعداد هاست ها ازراست به چپ شمرده مي شود.

به تعداد 6 بيت بايد از سمت راست به چپ شمرده شود و جدا گردد. (صفر مي گذاريم)

| 11111111. | 11111111. | 11111111. | 11000000 |
|---|---|---|---|
| 255. | 255. | 255. | 192 |

---

- **Example. IP: 192.168.20.18, Mask: 255.255.255.224**

**S:**

1. **255-224=31 ⇨$2^5$ ⇨00000 ⇨ 11111111. 11111111. 11111111.11100000 ⇨/27**
2. $2^3 = 8$
3. $2^5 - 2 = 30$
4. **256-224=32**

---

- **Example. IP:172.16.0.0, Mask:255.255.192.0**

**S:**

| 255. | 255. | 192. | 0 |
|---|---|---|---|
| | | 11000000 | 00000000 |

1. $2^2 = 4$
2. $2^{14} - 2 = 16,382$
3. **256-192=64.0**

| Net_ID: | 0.0 | 64.0 | 128.0 | 192.0 | |
|---|---|---|---|---|---|
| Firs_IP: | 0.1 | 64.1 | 128.1 | … | |
| Last_IP: | 63.254 | 127.254 | 192.254 | … | |
| Broadcast: | 63.255 | 127.255 | 191.255 | … | |

| Net_ID: | 64.0 | 128.0 | 192.0 |
|---|---|---|---|
| Firs_IP: | 64.1 | | … |
| Last_IP: | 127.254 | | … |
| Broadcast: | 127.255 | | … |

2 ⇦ 128-1=127

**2 ⇨ صفرها تبديل به يك مي شوند.**

**Net_ID:** 64.**0** ⇨**Broadcast:** 127.**255**

**غير فعال كردن Lookup Mode در روتر:**

**Router(config)#no ip domain-lookup**

| Prefix Format | Decimal | Available Host Addresses |
|---|---|---|
| /8 | 255.0.0.0 | 16777214 |
| /9 | 255.128.0.0 | 8388606 |
| /10 | 255.192.0.0 | 4194302 |
| /11 | 255.224.0.0 | 2097150 |
| /12 | 255.240.0.0 | 1048574 |
| /13 | 255.248.0.0 | 524286 |
| /14 | 255.252.0.0 | 262142 |
| /15 | 255.254.0.0 | 131070 |
| /16 | 255.255.0.0 | 65534 |
| /17 | 255.255.128.0 | 32766 |
| /18 | 255.255.192.0 | 16382 |
| /19 | 255.255.224.0 | 8190 |
| /20 | 255.255.240.0 | 4094 |
| /21 | 255.255.248.0 | 2046 |
| /22 | 255.255.252.0 | 1022 |
| /23 | 255.255.254.0 | 510 |
| /24 | 255.255.255.0 | 254 |
| /25 | 255.255.255.128 | 126 |
| /26 | 255.255.255.192 | 62 |
| /27 | 255.255.255.224 | 30 |
| /28 | 255.255.255.240 | 14 |
| /29 | 255.255.255.248 | 6 |
| /30 | 255.255.255.252 | 2 |

| | Net Mask | Net Mask | Wildcard |
|---|---|---|---|
| .10000000 | /25 | 128 | 127 |
| .11000000 | /26 | 192 | 63 |
| .11100000 | /27 | 224 | 31 |
| .11110000 | /28 | 240 | 15 |
| .11111000 | /29 | 248 | 7 |
| .11111100 | /30 | 252 | 3 |
| .11111110 | /31 | 254 | 1 |

# پروتکل CDP ( Cisco Discovery Protocol )

CDP مخفف Cisco Discovery Protocol یک پروتکل شبکه لایه دو (Data Link) مخصوص سیسکو می باشد که این پروتکل جهت به اشتراک گذاری اطلاعات دستگاههای سیسکو (همانند نسخه سیستم عامل و IP آدرس) که بصورت مستقیم به یکدیگر متصل هستند توسط شرکت سیسکو توسعه یافته است. و این پروتکل در تجهیزات ساخته شده زیر توسط شرکت سیسکو اجرا می شود.

- **Router ها**
- **Bridge ها**
- **Access server ها**
- **Switch ها**

پیامهای CDP از طریق یک دستگاه سیسکو همسایه دریافت می شود و بصورت پیش فرض به هیچ دستگاه دیگری ارسال نمی شود . این به این معنی است که CDP فقط از دستگاههای سیسکو که به صورت مستقیم متصل می باشد عبور می کند .هر دستگاه سیسکو (که CDP را پشتیبانی می کند ) اطلاعات دریافت شده از دستگاههای همسایه را در یک جدول ذخیره می کند که با ساتفاده از دستور show cdp neighbors می توانیم آنرا مشاهده کنیم.

دستگاههای سیسکو پیغامهای CDP را به آدرس مقصد مالتی کاست 01:00:0C:CC:CC:CC ارسال می کنند. پیغامهای CDP در هر 60ثانیه روی اینترفیسهایی که پروتکل دسترسی به زیر شبکه ها Subnetwork Access Protocol ( SNAP) را پشتیبانی میکند ارسال میشود . پشتیبانی از Subnetwork Access Protocol (SNAP) در هر نوع رسانه لایه دو ( data link layer) موجود نمی باشد . مدلهای رسانه ای که CDP را پشتیبانی میکنند عبارتند از:

Ethernet, Token Ring, FDDI, PPP, HDLC, ATM و Frame Relay

پیغام CDP شامل اطلاعات زیر می باشد:

1- نام دستگاه (که با دستور hostname تنظیم شده است )
2- نسخه نرم افزار IOS
3- امکانات سخت افزار (routing/switching)
4- پلت فرم سخت افزار
5- آدرس IP دستگاه
6- اینترفیس که پیام CDP را ایجاد کرده است

دستورات مهم CDP قابل استفاده در IOS
فعال یا غیر فعال کردن CDP در IOS سیسکو:

CDP به صورت پیش فرض در روترهای سیسکو فعال می باشد .اگر شما ترجیح می دهید که این قابلیت را غیر فعال کنید می توانید از دستور no cdp run برای غیر فعال کردن آن و مجدد برای فعال کردن CDP می بایستی از دستور cdp run در وضعیت global configuration استفاده نمایید.

- **RouterX# show cdp neighbors :**

برای دیدن خلاصه ای از دستگاههای سیسکو همسایه می توانیم در privilege mode از این دستور استفاده کنیم.

```
1  Router01#show cdp neighbors
   Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
   S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
   Device ID Local Intrfce Holdtme Capability Platform Port ID
   networkinpersian.com.router02
   Ser 0/0 156 R C2600 Ser 0/0
   networkinpersian.com.switch01
   Fas 0/0 149 S 2950 Fas 0/1
   networkinpersian.com.router01#
```

show cdp neighbors اطلاعات زیر را نمایش می دهد.
نوع دستگاه پیدا شده
نام دستگاه
local تعداد و نوع پورتها یا اینترفیس
برای پورت قابل معتبر است CDP advertisement تعداد ثانیه ای که
شماره محصول دستگاه
شناسه پورت

- **RouterX# show cdp neighbor detail:**

برای دیدن اطلاعات جزئی از دستگاههای سیسکو همسایه میتوانیم در privilege mode از این دستور استفاده کنیم.

```
1  Router#show cdp neighbor detail
   Device ID: networkinpersian.com.router02
   Entry address(es):
   . . .
```

- **RouterX#show cdp interface:**

برای دیدن تنظیمات CDP روی اینترفیس در privilege mode از این دستور استفاده کنیم.

| | |
|---|---|
| | Router**#show cdp interface**<br>FastEthernet0/0 is up, line protocol is up<br>. . . |

---

- **RouterX#show cdp:**

برای دیدن وضعیت CDP در دستگاه سیسکو شما در privilege modeمی توانیم از این دستور استفاده کنیم.

| | |
|---|---|
| 1 | Router**#show cdp**<br>Global CDP information:<br>Sending CDP packets every 60 seconds<br>Sending a holdtime value of 180 seconds<br>Sending CDPv2 advertisements is enabled |

# انواع پسوورد در روتر

1- **Enable Password :** برای برقراری امنیت هنگام ورود به privileged mode استفاده می شود. هنگامی که در user mode فرمان enable را وارد می کنید و می خواهید وارد privileged mode شوید این password پرسیده می شود.

| | |
|---|---|
| 1 | Router (config) # **enable password** **پسورد مورد نظر** |

حال زمانیکه مي خواهيم وارد مد enable شويم از ما پسوورد مي خواهد:

```
Router>en
Password:
```

**تذكر: اين پسورد از امنيت بالايي برخوردار نيست چون در Show Run كاملا نمايش داده مي شود و براي بالا بردن امنيت پسورد مد Enable بايد آنرا رمز نگاري كرد كه از Secret Password بايد استفاده شود.**

---

2- **Secret Password :** همانند enable password می باشد.با این تفاوت با MD5 کد گذاری می شود

| | |
|---|---|
| 1 | Router (config) # **enable secret** **پسورد مورد نظر** |

توجه داشته باشید هنگامی که secret password را تنظیم می کنید، تا زمان فعال بودن secret password به صورت غیر فعال در می آید Enable password و می بایست هنگام ورود به Priviledeg Mode پسورد مربوط به Secret Password را وارد کنید.

---

3- **Telnet Password :** یکی از راههای دسترسی به روتر Virtual Terminal یا همان Telnetمی باشد. بنابراین در صورتیکه به یک روتر Telnet می کنید، می بایست بعد از بررسی و صحت Authentiction ارتباط برقرار شود.

- خط 1: برای تنظیم کردن telnet password وارد global mode شده و فرمان زیر را وارد می کنید:

به ازای هر ارتباط Telnet یک Session برقرار می شود بنابراین به اندازه تعداد Lineهایی که IOS ساپورت می کند می توانید Telnet Session برقرار کنید.

- خط 3: برای دیدن تعداد Line هایی که IOS ساپورت می کند کافی است از Help کمک بگیرید.
- خط7: فرمان بعدی login می باشد. در واقع با این فرمان می گویید که در صورت telnet شدن به این device ، پسورد پرسیده شود.
- خط 8: مرحله آخر تعریف پسورد می باشد:

Router (config-line) # **password** **پسورد مورد نظر**

توجه داشته باشید telnet password قبل از وارد شدنuser به user mode پرسیده می شود.

- خط 9: به کمک فرمان show session می توان تمامی session های برقرار شده و مدت زمان connect بودن هر یک از آنها را مشاهده کرد.
- خط 11: و می توانید به کمک فرمان disconnect ، ارتباط session خاصی را با روتر قطع کرد. برای این منظور کافی است فرمان زیر را به صورت زیر وارد کنید.

| | |
|---|---|
| 1 | Router (config) # **line vty 0 4** |
| 2 | |
| 3 | Router (config-line) # **line vty 0 ?** |
| 4 | <1-4> last line number |
| 5 | <cr> |
| 6 | |
| 7 | Router (config-line) # **login** |
| 8 | Router (config-line) # **password <u>پسورد مورد نظر</u>** |
| 9 | Router # **show session** |
| 10 | |
| 11 | Router # **disconnect connection-number** |

---

4- **AUX Password:** همانطور که می دانید یکی دیگر از راههای برقراری ارتباط remote ، روش استفاده از پورت AUX می باشد. در این روش روتر را از طریق یک مودم به خط dial-up متصل شده است و دسترسی به صورت remote به آن امکان پذیر می باشد AUX password . پسوردی است که قبل از وارد شدن به user modeپرسیده می شود.

| | |
|---|---|
| 1 | Router (config) # **line aux o** |
| 2 | Router (config-line) # **login** |
| 3 | Router (config-line) # **password <u>پسورد مورد نظر</u>** |

---

5- Console password: تنها راه ارتباط با روتر که بدون تنظیم می باشد استفاده از console port است. بنابراین بعد از انجام تنظیمات می توانید روتر را در یک جای ثابت قرار داده و از این به بعد آن را از طریق telnetیا Browser کردن تنظیم کنید.

اما توجه داشته باشید که نداشتن پسورد و محدودیت دسترسی افراد برای adminدردسر ساز می شود.

Console Password، پسوردی است که قبل از وارد شدن به User Modeپرسیده می شود و به صورت زیر تنظیم می شود.

| | |
|---|---|
| 1 | Router (config) # **line console0** |
| 2 | |
| 3 | Router (config-line) # **login** |

| | |
|---|---|
| 4<br>5 | Router (config-line) # **password** **يسورد مورد نظر** |

تنظيمات اضافی پورت Console :

مدت زمان برقراری ارتباط console با روتر یا سوئیچ بدون قطع شدن این ارتباط به صورت پیش فرض ۱۰ دقیقه می باشد. به کمک دستور زیر می توانید مدت زمانی که این ارتباط برقرار می شود را به صورت نامحدود تعریف کنید. در واقع اگر packet ایی برای مدت زمان طولانی از این اینترفیس رد و بدل نشود این ارتباط قطع نخواهد شد.

| | |
|---|---|
| 1 | Router (config) # **line console o** |
| 2 | Router (config-line) # **exec-timeout o o** |

حال اگر بخواهيم براي برقراري امنيت بيشتر، اين زمان را كمتر كنيم تا زمانيكه اگر شخص از پشت سيستم خود بلند شد و براي اينكه شخص ديگري از فرصت استفاده نكند و نتواند Config ها را دستكاري كند زمان را كم مي كنيم كه با اين كار بطور خودكار در زمان تعيين شده روتر از مد Config خارج مي گردد.

| | |
|---|---|
| 1 | Router (config) # **line console 0** |
| 2 | Router (config-line) # **exec-timeout** **دقيقه** **ثانيه** |

يکی ديگر از مشکلاتی که ممکن است با آن مواج شويد، اين است که شما فرمانی را در command prompt روتر يا سوئيچ وارد می کنيد به طور مثال فرمان show run و منتظر نتيجه آن هستيد در اين لحظه پيام جديدی مبنی بر اينکه يکی از اينترفيس ها up شده است ظاهر می شود. بنابراين نمی توانيد تفاوت بين نتيجه فرمان خودتان و پيامی که ظاهر شده را متوجه شويد. به کمک فرمان زير می توانيد به روتر بگوييد پيام جديد را تعد از خروجی فرمان شما نمايش دهد.

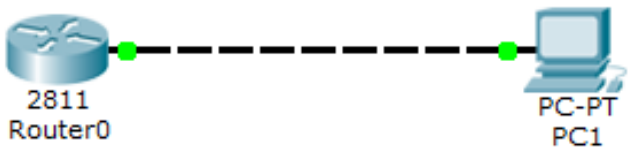
| | |
|---|---|
| 1 | Router (config) # **line console 0** |
| 2 | Router (config-line) # **logging synchronous** |

---

6- براي اينكه باقي پسوردهاي موجود در سيستم را نيز رمز نگاري كنيم از كامند زير استفاده مي كنيم.

| | |
|---|---|
| 1 | Router (config) #**Service Password-encryption** |

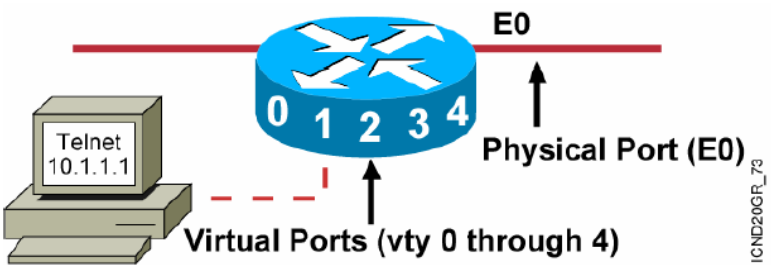
## راه اندازي مكانيزم Telnet:

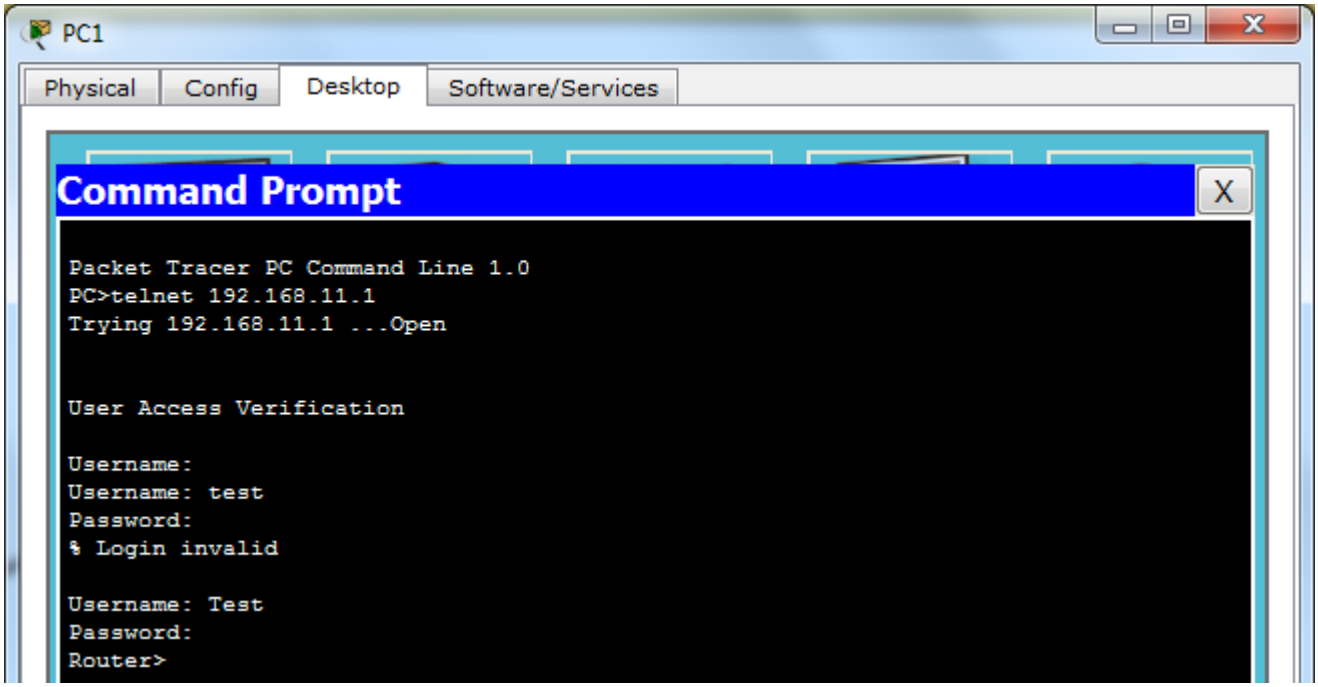



```
1   Router>en
2   Router#conf t
3
4   Router(config)#interface fastEthernet 0/1
5   Router(config-if)#ip address 192.168.11.1 255.255.255.0
6   Router(config-if)#no sh
7
8   Router(config)#username Test password 123
9   Router(config)#line vty 0 4
10  Router(config-line)#login local
11  Router(config-line)#transport input telnet
```

حال مي خواهيم از كامپيوتر مورد نظر از طريق Telnet به روتري كه در آن Telnet را فعال نموديم، وصل شويم.

- صفحه Command prompt را باز مي كنيم.
- IP روتر مورد نظر را به همراه كامند Telnet در خط فرمان مي نويسي move مof.
- بايد توجه داشته باشيم كه به حروف بزرگ و كوچك حساس مي باشد. مثلا در اينجا ما Username را با Testانتخاب نموديم كه حرف T آن بزرگ مي باشد. و همانگونه كه در شكل ofزير مشاهده مي نماييد زمانيكه ما test را با حرف كوچك وارد نموديم پيغام خطا صادر نمود. (Login Invalid).
- زمانيكه پسورد خواست بايد همان پسورد 123 را كه خط username Test password 123 نوشتيم را وارد كنيم.




PC1
Physical
Config
Desktop
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.11.1
Trying 192.168.11.1 ...Open
User Access Verification
Username:
Username: test
Password:
% Login invalid
Username: Test
Password:
Router>

# راه اندازي مكانيزم SSH:

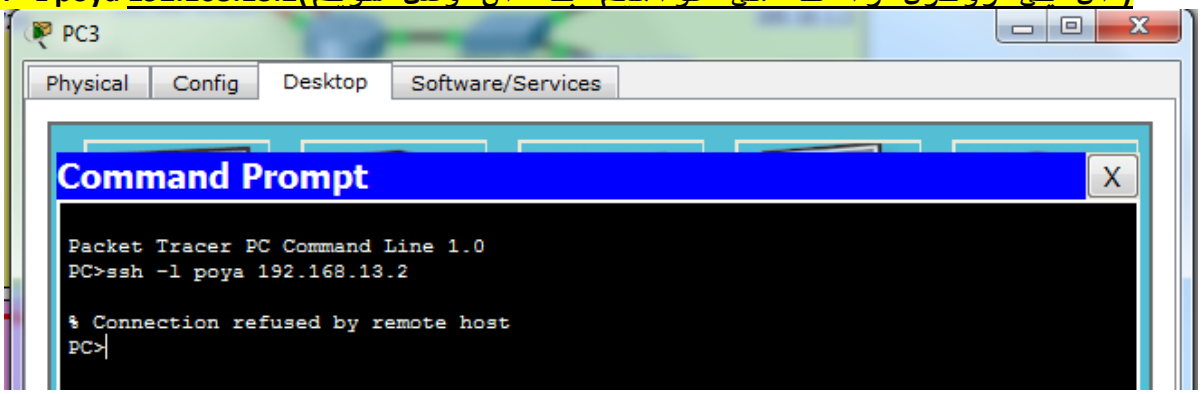
ابتدا SSH را روي روتر مورد نظر فعال مي كنيم:

```
1  R3(config)# hostname TEST
2  TEST(config)# ip domain-name CISCO.com
3  TEST(config)# crypto key generate rsa
4  % You already have RSA keys defined named TEST.CISCO.com .
5  % Do you really want to replace them? [yes/no]:1024
6  TEST(config)# ip ssh version 2
7  TEST(config)# username poya password 123
8
9  TEST(config)# enable secret 12345
10 TEST(config-line)# line vty 0 4
11 TEST(config-line)# login local
12  TEST(config-line)# transport input ssh
```

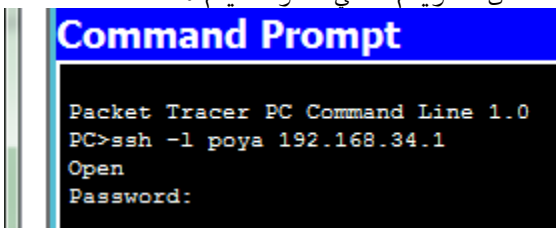
**توضيح كد:**

- خط 3: كليد امنيتي با الگوريتم رمز نگاري RSA
- خط 5: 1024 را وارد مي كنيم براي اينكه طول كليد امنيتي بالا رود و رمز نگاري آن مشگلتر شود.
- خط 6: براي ساپورت طول كليد بزرگتر، بايد وارد Ver2 شويم.
- خط 7: انتخاب نام براي SSH و پسوورد.
- خط 9: انتخاب پسورد مناسبت براي مد enable روتر
- خط 10 الي 12: تنظيمات مربوط به ssh(براي زمانيكه كه كسي مي خواهد از طريق ssh به روتر شماره 3 وصل شود و وارد مد enable شود)

**PC>ssh –L poya 192.168.13.2(آی پی روتری را که می خواهیم به آن وصل شویم)**




و اگر از سيستمهاي ديگر بخواهيم از طريق SSHمتصل شويم مي توانيم.




حال بايد پسورد اول را وارد كنيم: 123

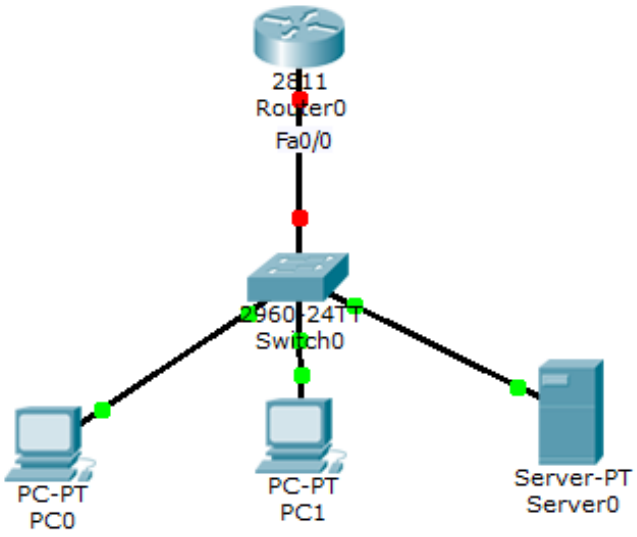
```
PC>ssh -l poya 192.168.34.1
Open
Password:



TEST>en
Password:
```

سپس پسورد enable را وارد مي كنيم : 12345
و وارد مد enable روتر مي شويم .

```
PC>ssh -l poya 192.168.34.1
Open
Password:



TEST>en
Password:
Password:
TEST#
```

# راه اندازي سرويس DHCP

اختصاص اتوماتيك IP به اجزاي شبكه




1- براي شروع كار ابتدا به Interface FastEthernet 0/0 روتر IP اختصاص مي دهيم.

```
1  Router(config)#interface fastEthernet 0/0
2  Router(config-if)#ip address 192.168.10.1 255.255.255.0
3  Router(config-if)#no sh
```

2- راه اندازي DHCP در روتر:

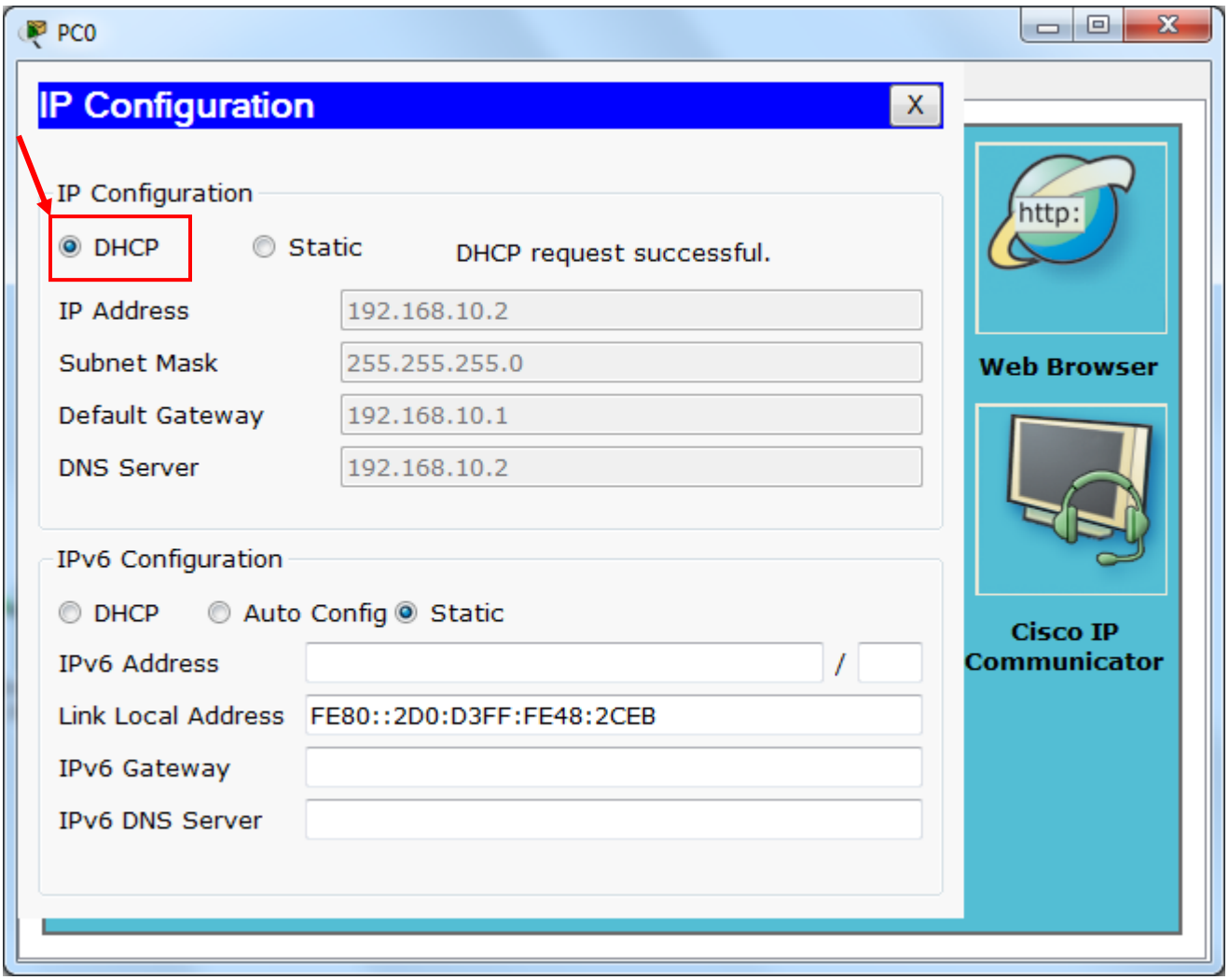
```
1  Router(config)#ip dhcp pool Test
2  Router(dhcp-config)#network 192.168.10.2  255.255.255.0
3  Router(dhcp-config)#default-router 192.168.10.1
4  Router(dhcp-config)#dns-server 192.168.10.2
5
6  Router(config)#ip dhcp excluded-address 192.168.10.4 192.168.10.10
```

- خط 1: بايد مخزني را تعريف كنيم كه كلايتنها بتوانند از آنجا IP دريافت كنند. (Pool درياچه اي از IP هاست.)

  Router(config)#**ip dhcp pool نام دلخواه**

- خط 2: رنج IP ها را تعريف مي كنيم.
- خط 3: تعريف Default Gateway در اينجا Interface FastEthernet 0/0 در نقش Gateway است. و IP اي كه به آن اختصاص داده ايم را بايد در اين قسمت به عنوان Gateway تعريف نماييم.
- خط 4: تعريف Domain Name server (ضروري نيست).
- خط 6: در صورتي كه بخواهيم يكسري از IP ها را از ليست خارج نماييم (مثلا بعضي از IP را به صورت دستي به سيستمها و اجزاي شبكه اختصاص داده ايم) از اين كامند استفاده مي كنيم. و در اينجا رنج بين 4 الي 10 از طريق DHCP به كسي اختصاص داده نمي شود.

و در نهايت بر روي تنظيمات سيستمها و تجهيزات شبكه IP Configuration را بر روي DHCP قرار مي دهيم تا از DHCP آي پي دريافت كند.



# مفاهیم سویچ Switch

Hub برای اتصال دستگاهای مختلف از قبیل رایانه , روتر , چاپگرهای تحت شبکه , دوربین های مدار بسته و .... در شبکه های کابلی مورد استفاده قرار مي گیرد.

در وجه ظاهری، switch همانند جعبه ایست متشکل از چندین درگاه اترنت که از این لحاظ شبیه Hub می باشد, با وجود آنکه هر دو این ها وظیفه برقراری ارتباط بین دستگاه های مختلف را بر عهده دارند , تفاوت از آنجا آغاز می شود که Hub بسته های ارسالی از طرف یک دستگاه را به همه ی درگاه های خود ارسال می کند و کلیه دستگاه های دیگر علاوه بر دستگاه مقصد این بسته ها را دریافت می کنند در حالیکه در Switch ارتباطی مستقیم بین درگاه دستگاه مبدا با درگاه دستگاه مقصد برقرار شده و بسته ها مستقما فقط برای آن ارسال می شود.

این خصوصیت از انجا می آید که Switch می تواند بسته ها را پردازش کند , در Switch های معمولی که به switch layer2 معروفند این پردازش تا لایه دوم مدل OSI پیش می رود و نتیجه این پردازش جدولی است که در Switch با خواندن آدرس سخت افزاری (MAC) فرستنده بسته و ثبت درگاه ورودی تشکیل می شود.

Switch با رجوع به این جدول عملیات آدرس دهی بسته ها در لایه دوم را انجام میدهد , بدین معنا که این جدول مشخص می کند بسته ورودی می بایست فقط برای کدام درگاه ارسال شود.

در شبکه های بزرگ Switch ها جدول های خود را به اشتراک می گذارند تا هر کدام بدانند چه دستگاهی به کدام Switch متصل است و با این کار ترافیک کمتری در شبکه ایجاد کنند.

Switch بطور معمول در لایه دوم مدل OSI کار می کند ولی Switch هایی با قابلیت کارکرد در لایه های مختلف حتی لایه هفتم هم وجود دارد.پرکاربردترین Switch در بین لایه های مختلف بجز لایه دوم می توان به Switch layer3 اشاره کرد که در بسیاری موارد جایگزین مناسبی برای روتر می باشند.

از Switch می توان در یک شبکه خانگی کوچک تا در شبکه های بزرگ با Backbone های چند گیگابایتی استفاده کرد.

برخی مزیت های و قابلیت های:Switch

3- Switch امکان برقراری ارتباط بین ده ها و گاها صدها دستگاه را به طور مستقیم و هوشمند به ما می دهد.
4- Switch امکان برقرای ارتباط با سرعت بسیار بالا را فراهم می کند.
5- Switch امکان نظارت و مدیریت بر عملکرد کاربران را فراهم می کند.
6- switch امکان کنترل پهنای باند مصرفی کاربران را فراهم می کند.
7- Switch امکان تفکیک شبکه به بخش های کوچکتر و مشخص کردن نحوه دسترسی افراد به قسمت های مختلف را فراهم می کند.

8- و ده ها مزیت دیگر

اگر بخواهیم انواع Switch layer2 را فقط نام ببریم از این قرارند :

- Store and forward
- Cut through
- Fragment free
- Adaptive switching

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند شبکه محلی به یکدیگر مورد استفاده قرار می گیرد که باعث افزایش توان عملیاتی شبکه می شود. سوئیچ وسیله ای است که دارای درگاه های متعدد است که بسته ها را از یک درگاه می پذیرد، آدرس مقصد را بررسی می کند وسپس بسته ها را به درگاه مورد نظر " که متعلق به ایستگاه میزبان با همان آدرس مقصد می باشد" ارسال می کند. اغلب سوئیچ های شبکه محلی در لایه پیوند داده های مدل ا اس آی عمل می کند.

سوئیچ ها بر اساس کاربردشان به متقارن "Symmetric" ونامتقارن " Asymmetric" تقسیم می شوند.

در نوع متقارن ، عمل سوئیچینگ بین سگمنت هایی که دارای پهنای باند یکسان هستند انجام می دهد یعنی mbps10 به mbps10 و... سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت هایی با پهنای باند متفاوت انجام می شود.

◄ **پورتهاي سوييچ داراي چهار وضعيت هستند:**

**1- Block: پيش فرض در اين حالت قرار دارد.**
**2- Listen: شناسايي پورتها و... تشكيل Mac Table.**
**3- Learn: ياد مي گيرد**
4- **Send/Receive Forward**

- در سوييچ جدولي به نام Mac Table قرار دارد كه آدرس IP ها به همراه Mac Addressها در آن نگهداري مي شوند.
- مزيت وجود Mac Table: افزايش سرعت و ارتباطات و جلوگيري از Broadcastهاي اضافي است.
- Mac Table زماني پر مي شود كه همه ي پورتها ي آن مشغول باشند.
- ترتيب وضعيت پورتهاي سوييچ:

Block → Listen → Learn → Forward

- چگونه اطلاعاتي از Mac Table حذف مي شود؟ در صورتيكه پورت به صورت فيزيكي خارج شود (قطع شود) يا پورتي را Shut Down كنيم (بصورت منطقي Logical)

- به طور کلي سويچ ها در دو حالت Broadcast مي کنند:

  - زمانيکه مي خواهد اطلاعات از سيستمها ياد بگيرد.
  - زمانيکه سويچ مي خواهد اطلاعاتي را به يك Mac خاص ارسال کند و آدرس سيسم را نداشته باشد ← در سويچ هاي ديگر Broadcast انجام مي دهد تا سيستم مورد نظر خود را پيدا کند.

---

## مفاهيم VLAN

VLANچيست ؟

VLANهمانطور که از نام آن پيداست شبکه LAN مجازي است که Broadcast Domain اصلي سوئيچ را که بصورت يك VLAN وجود دارد (VLAN1) را به چندين Broadcast Domain ديگر مي شکند. به دليل اينکه سوئيچ ها قادر به برقراري ارتباط و Learnکردن از هم هستند لذا چندين پورت از سوئيچ ديگر مي تواند عضو VLAN سوئيچ ما باشد بدون اينکه Broadcast را به سوئيچ ها يا VLAN هاي ديگر منتقل کند. معمولا VLAN براي شبکه هاي بزرگ با ترافيك بالا کاربرد دارد. قبل از اينکه به نحوه تنظيم VLANبپردازم نکاتي را که بايد قبل از اين تنظيمات بدانيد در چند بيان مي کنم.

VLAN-در واقع يك Broadcast Domain مي باشد که توسط سوئيچ ايجاد مي شود.

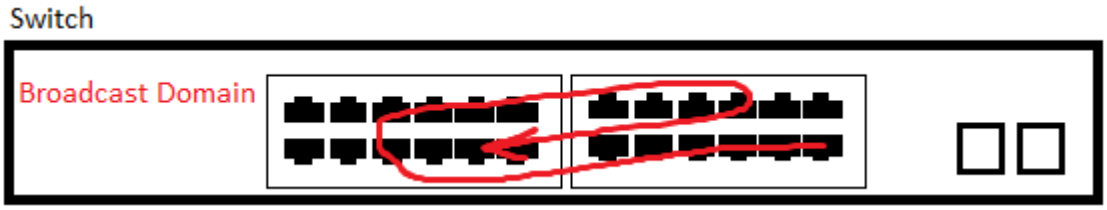
- براي تنظيم VLAN مدير شبکه ابتدا بايد VLAN را ايجاد کند و سپس پورت هاي سوئيچ را به آن مرتبط سازد.
- همه سوئيچ هاي سيسکو داراي يك VLAN بصورت پيش فرض هستند.
- در هر VLAN پورتي به نام Trunk تعريف مي شود که قادر است ترافيك ها VLAN را به خارج يا داخل هدايت کند. اين پورت از پروتکل ISL يا 802.11 qبراي اين کار استفاده مي کند. با کلامي ديگر اين پورت بين چندين VLAN مشترك است و ترافيك کليه آن ها را به سوئيچ يا روتر انتقال مي دهد.
-براي ارتباط چندين VLAN از سوئيچ لايه 3 يا روتر استفاده مي شود.

### مزاياي VLAN:

**1- Segmentation**

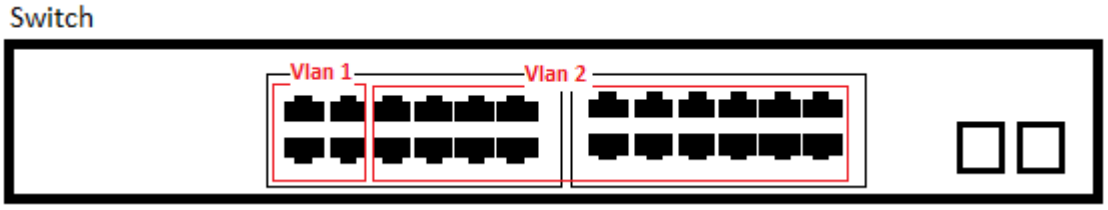
به ازاي تمامي پورتها يك Segment در لايه ي 2 وجود دارد و يك Broadcast Domain وجود دارد.

به ازاي هر VLAN يك Broadcast Domain وجود دارد.




- به صورت پيش فرض به ازاي تمامي پورتهاي سويچ يك Vlan با شماره ي 1 وجود دارد.

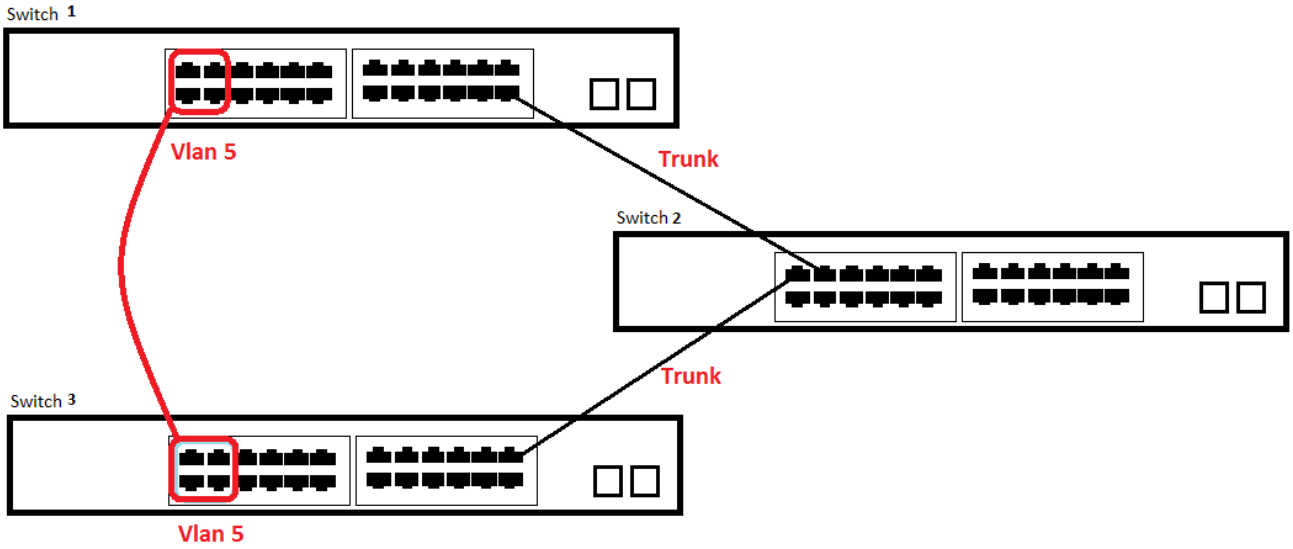
- حال اگر بخواهیم مثلا دوSegment مختلف ایجاد کنیم باید دو Vlan بسازیم. که Vlanآنها جدا مي شود و در نتیجه Broadcast Domain آنها نیز از هم جدا مي گردد.




**2- Flexibility:**

قابلیت انعطاف پذیري در شبکه بوجود مي آید.

- مثلا مي خواهیم دو پورت از یك سویيچ را به پورت سویيچ دیگر در یك Vlan قرار دهیم و آنهایئکه در یك Vlan قرار دارند داراي یك Broadcast هستند.




3- **Security: ایجاد امنیت**

- Mode هاي پورتهاي سویيچ Switch Interface Mode:
  - Access: در حالتي است که سویيچ به PC متصل مي گردد که در حالت پیش فرض در این حالت قرار دارد.
  - Trunk: حالتي است که switch به Switch متصل شده است.

**مدهاي سویيچ نیز شبیه روتر مي باشد:**

1- User exe mode
2- Privilege exe mode
3- Global Config mode

جهت مشاهده ي Vlan هاي موجود در سویيچ از کامند زیر استفاده مي کنیم:

| | |
|---|---|
| 1 | 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
                                                 Gig1/1, Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

## ساخت Vlan

```
1  Switch(config)#vlan 20
2  Switch(config-vlan)#name Test
3
4  Switch(config-vlan)#vlan 30
5  Switch(config-vlan)#name CCNA
6
7  Switch#show vlan b
```

```
Switch#show vlan b

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
                                                 Gig1/1, Gig1/2
20   Test                              active
30   CCNA                              active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- خط 1: ساخت Vlan به شماره 20
- خط 2: اختصاص نام به Vlan شماره 20
- خط 4: ساخت Vlan با شماره 30
- خط 5: اختصاص نام به Vlan شماره 30

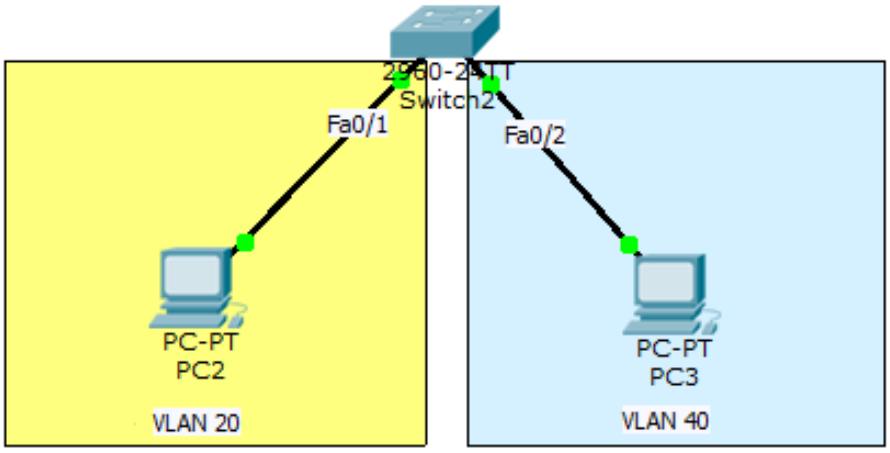
**تذكر: قبل از اينكه پورتهاي سوييچ را به Vlan خاصي اختصاص دهيم بايد ابتدا Vlan را در سوييچ مورد نظر بسازيم (در غير اينصورت با پيغام خطا مواجه مي شويم... % Access VLAN does not exist. Creating vlan) سپس پورتها را در Vlanهاي ساخته شده قرار دهيم.**

**براي حذف Vlan:**

| | |
|---|---|
| 1 | Switch(config)#**no vlan 20** |

## اتصال سويچ به كامپيوتر

**مثال: سناريو ي زير را اجرا كنيد:**




**1- ابتدا بايد VLAN ها را تعريف كنيم:**

| | |
|---|---|
| | Switch(config)#**vlan 20**<br>Switch(config-vlan)#**vlan 40** |

**2- حال وضعيت پورتها را تعريف مي كنيم. چون پورتهاي سويچ به كامپيوتر وصل شده اند ← از نوع Access بايد تعريف گردند.**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode access** |
| 3 | Switch(config-if)#**switchport access vlan 20** |
| 4 | Switch(config-if)#**do sh vl b** |

- خط 1: وارد Interface مربوطه مي شويم.
- خط 2: مد پورت را مشخص مي كنيم. در اينجا چون پورت سويچ به كامپيوتر متصل شده است درنتيجه از نوع Access بايد تعريف گردد.
- خط 3: حال بايد Interface مورد نظر را در Vlan مربوطه (مطابق شكل) قرار دهيم.
- خط 4: خلاصه دستور : Show vlan brief مي باشد.

```
Switch(config-if)#do sh vl b

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
20   VLAN0020                          active    Fa0/1
40   VLAN0040                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

همانگونه که در شکل مي بينم **Interface Fa 0/1** در **Vlan 20** قرار گرفت.

براي **Interface fa 0/2** نيز دقيقا کارهاي بالا را مطابق با سناريو انجام مي دهيم.

| | |
|---|---|
| 1 | Switch(config)#**interface fa 0/2** |
| 2 | Switch(config-if)#**switchport mode access** |
| 3 | Switch(config-if)#**switchport access vlan 40** |
| 4 | Switch(config-if)#**do sh vl b** |

```
Switch(config-if)#do sh vl b

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig1/1, Gig1/2
20   VLAN0020                          active    Fa0/1
40   VLAN0040                          active    Fa0/2
1002 fddi-default                      active
```

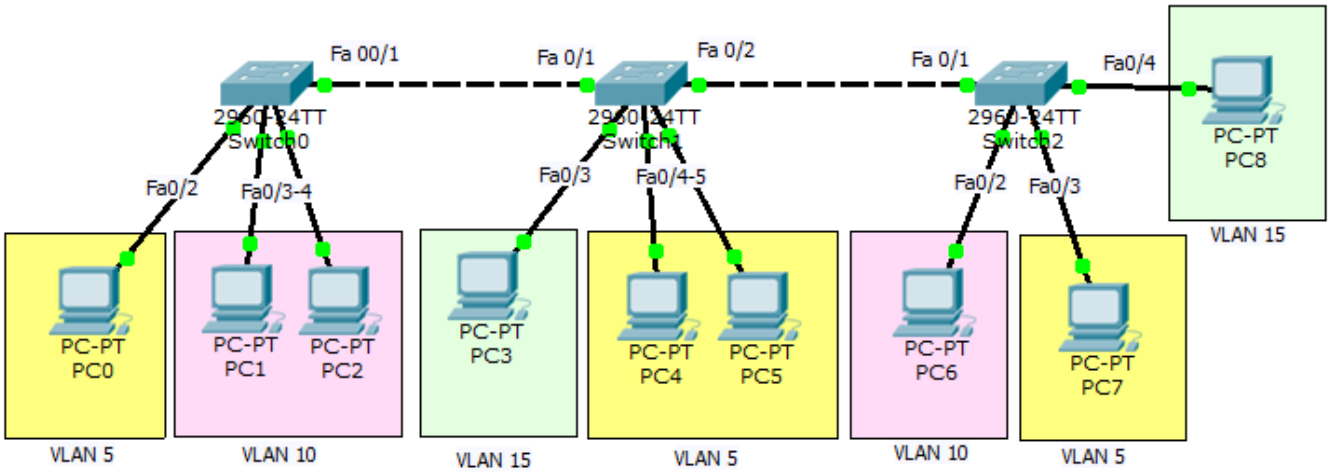
## اتصال سویچ ها با یکدیگر

سویچ ها را باید با کابل Cross به یکدیگر متصل کنیم.
میخواهیم vlanning را بر روی بیشتر از یک سوئیچ داشته باشیم درنتیجه باید ارتباطات بین سوئیچ ها را Trunk تعریف کنیم.

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode trunk** |
| 3 | |
| 4 | Switch#**show interfaces trunk** |


```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
```

## سناريو: سويچ و VLAN:



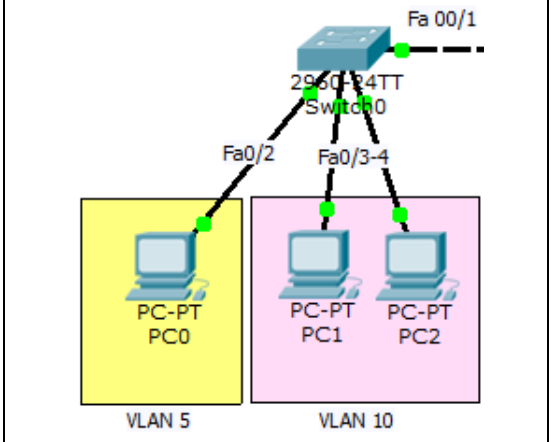

**VLAN 5: 192.168.5.0/24**
**VLAN 10: 192.168.10.0/24**
**VLAN 15: 192.168.15.0/24**

ترتيب اجراي سناريو:

1- ايجاد Vlanها مطابق با سويچ هاي مورد نظر
2- اختصاص پورتهاي Access به ازاي كامپيوترهاي و راه اندازي لينكهاي ترانك
3- اختصاص IP به كامپيوترها و تست ارتباط مابين Vlan هاي هم نام

**Sw0**

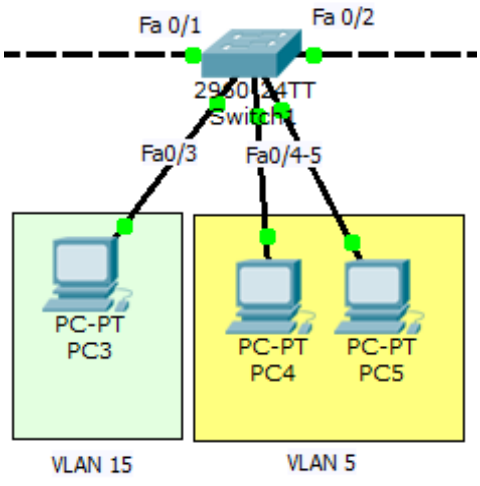
```
1   Switch(config)#vlan 5
2   Switch(config-vlan)#vlan 10
3
4   Switch(config)#interface fastEthernet 0/1
5   Switch(config-if)#switchport mode trunk
6
7   Switch(config)#interface fastEthernet 0/2
8   Switch(config-if)#switchport mode access
9   Switch(config-if)#switchport access vlan 5
10
11  Switch(config)#interface range fastEthernet 0/3-4
12  Switch(config-if-range)#switchport mode access
13  Switch(config-if-range)#switchport access vlan 10
```




```
Switch#show vlan b

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
                                                Gig1/1, Gig1/2
5    VLAN0005                         active    Fa0/2
10   VLAN0010                         active    Fa0/3, Fa0/4
1002 fddi-default                     active
```

**Sw1**

```
1  Switch(config)#interface range fastEthernet 0/1-2
2  Switch(config-if-range)#switchport mode trunk
3
4  Switch(config)#interface fastEthernet 0/3
5  Switch(config-if)#switchport mode access
6  Switch(config-if)#switchport access vlan 15
7
8  Switch(config)#interface range fa 0/4-5
9  Switch(config-if-range)#switchport mode access
10 Switch(config-if-range)#switchport access vlan 5
```

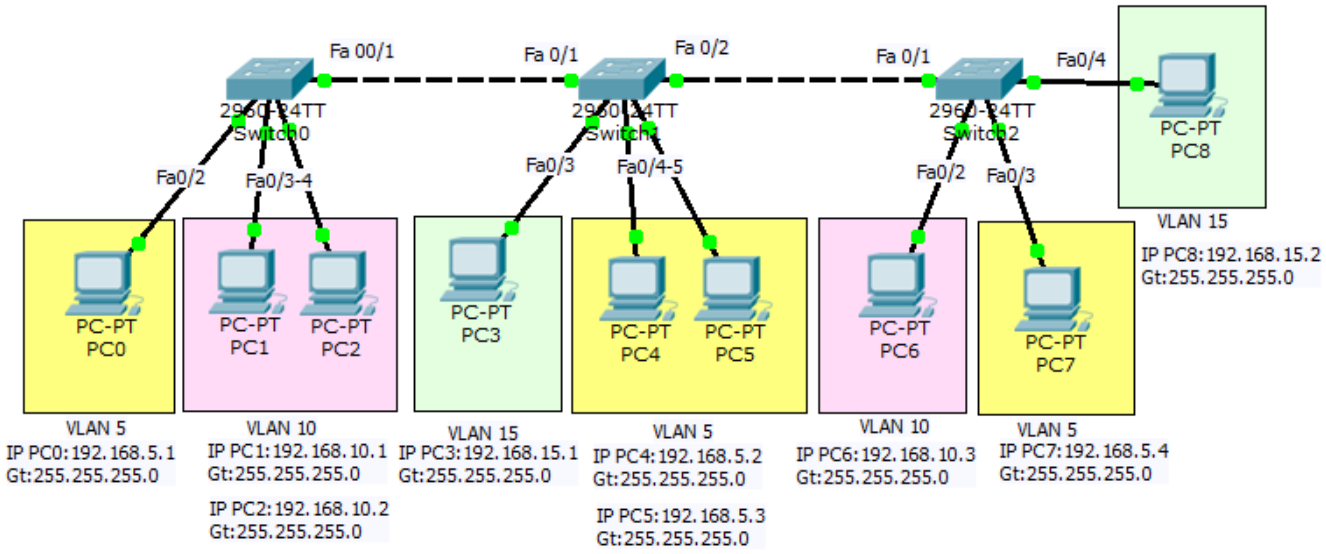



```
Switch#show vlan b

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
5    VLAN0005                         active    Fa0/4, Fa0/5
15   VLAN0015                         active    Fa0/3
1002 fddi-default                     active
```

**Sw2**

```
1  Switch(config)#vlan 10
2  Switch(config-vlan)#vlan 5
3  Switch(config-vlan)#vlan 15
4
5  Switch(config)#interface fa 0/2
6  Switch(config-if)#switchport mode acc
7  Switch(config-if)#switchport access vlan 10
8
9  Switch(config-if)#int fa 0/3
10 Switch(config-if)#switchport mo acc
11 Switch(config-if)#switchport acc vlan 5
12
13 Switch(config-if)#int fa 0/4
14 Switch(config-if)#sw mo acc
15 Switch(config-if)#sw acc vlan 15
```

حال باید به کامپیوترها IP اختصاص دهیم:
تذکر: در IP دادن به کامپیوترها نیاز به تعریف Gateway نداریم چون همه Switch هستند.


Fa 00/1
Fa 0/1
Fa 0/2
Fa 0/1
Fa0/4
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
PC-PT
PC8
VLAN 15
IP PC8:192.168.15.2
Gt:255.255.255.0
Fa0/2
Fa0/3-4
Fa0/3
Fa0/4-5
Fa0/2
Fa0/3
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
VLAN 5
IP PC0:192.168.5.1
Gt:255.255.255.0
VLAN 10
IP PC1:192.168.10.1
Gt:255.255.255.0
IP PC2:192.168.10.2
Gt:255.255.255.0
VLAN 15
IP PC3:192.168.15.1
Gt:255.255.255.0
VLAN 5
IP PC4:192.168.5.2
Gt:255.255.255.0
IP PC5:192.168.5.3
Gt:255.255.255.0
VLAN 10
IP PC6:192.168.10.3
Gt:255.255.255.0
VLAN 5
IP PC7:192.168.5.4
Gt:255.255.255.0

## پروتکل VTP

قرارداد VTP یا VLAN Trunking Protocol برای ساده کردن کار مدیریت VLAN ها توسط شرکت سیسکو ارائه شده است. با استفاده از VTP می توان اقدام به ایجاد و حذف اتوماتیک Vlan ها، بر روی سوئیچ های موجود در شبکه نمود، بدون آنکه عملیات ایجاد و یا حذف نمودن VLANها را بر روی تک تک سوئیچ ها انجام داد. این پروتکل براي زمانيكه تعداد سوييچ هاي ما در شبكه افزايش يابد جهت مديريت Vlanها بسيار مفيد مي باشد.

**سوييچ ها به دو دسته تقسيم مي گردند: Serverو Client.**

- در سوييچ server: بايد Vlan ها را تعريف كنيم.
- در سوييچ Client: Vlan ها به طور اتومات افزوده مي گردد. هر گونه تغييري در Vlanهاي موجود در سوييچ سرور، در سوييچ هاي كلاينت نيز اعمال مي گردد.

به عنوان مثال فرض کنید که شما 5 سوئیچ در اختیار دارید و می خواهید روی همه‌ی آنها vlan 20 یکسان ایجاد نمایید. در این صورت بایستی یک به یک به سوئیچ ها متصل شده و vlan های مورد نظر خود را بر روی آنها ایجاد نمایید. اما هنگامی که شما از قرارداد VTP استفاده کرده و تنظیمات مورد نیاز را اعمال نمایید، هنگامی که بر روی یک سوئیچVLAN ی را ایجاد نمایید، به صورت خودکار این VLAN بر روی تمامی سوئیچ های دیگر نیز ایجاد خواهد شد. لازم به ذکر است که این فرآیند در مورد حذف کردن vlan ها نیز صادق می باشد.

برای اجرای VTP روی سوئیچ ها ابتدا باید یک سوئیچ به عنوان سرور و مابقی سوئیچ ها به عنوان کلاینت انتخاب شوند. به شکل زیر نگاه کنید:

مدهاي VTP:

- Server: پيش فرض تمامي سوييچ ها است.
- Client
- Transparent

**Switch(config)#vtp mode [client | server | transparent]**

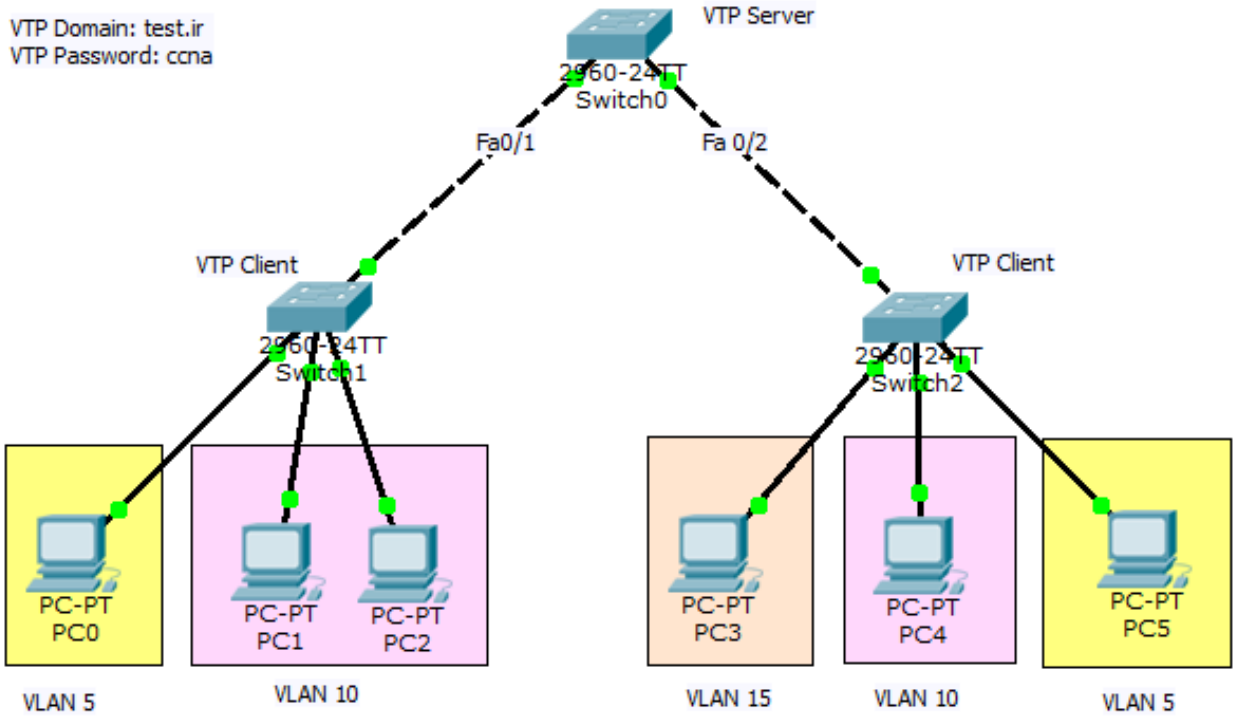
**Switch(config)#vtp domain نام دامنه ی مورد نظر**

**Switch(config)#vtp password پسورد مورد نظر**

**نمايش تغييرات** **Switch# show vtp status**

**اينترفيسهاي از نوع ترانك را نمايش مي دهد.** **Switch# show interface trunk**

## سناریو VTP




**مراحل اجراي سناريو VTP:**

1. اتصال سويچ ها به يكديگر و تعريف لينكهاي ترانك .
2. مشخص نمودن اطلاعات پروتكل VTP مطابق با شكل و ايجان Vlan ها در سويچ سرور
3. مشاهده ي Vlanها در سويچ هاي كلاينت و اختصاص پورتها به ازاي آنها
4. اختصاص IP Add. مطابق با Vlan و تست ارتباط مابين Vlanهاي هم نام.

**Sw0**

| | |
|---|---|
| 1 | Switch(config)#**int range fastEthernet 0/1-2** |
| 2 | Switch(config-if-range)#**switchport mode trunk** |
| 3 | |
| 4 | Switch(config)#**vtp mode server** |
| 5 | Device mode already VTP SERVER. |
| 6 | |
| 7 | Switch(config)#**vtp domain test.ir** |
| 8 | Changing VTP domain name from NULL to test.ir |
| 9 | |
| 10 | Switch(config)#**vtp password ccna** |
| 11 | Setting device VLAN database password to ccna |
| 12 | |
| 13 | Switch(config)#**vlan 5** |
| 14 | Switch(config)#**vlan 10** |

| | |
|---|---|
| 15 | Switch(config)#**vlan 15** |

- خط 1 تا 2: مد لینك بین سویچ ها را مشخص می کنیم که از نوع Trunk است.
- خط 4: Switch 0 را از نوع Server انتخاب می کنیم.
- خط 7: دامنه را تعریف می کنیم.
- خط 10: پسورد دامنه را تعریف می کنیم.
- خط 13 الی 15: Vlan ها را تعریف می کنیم.

حال باید تنظیمات سویچ های کلاینت را انجام دهیم:

**Sw1**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode trunk** |
| 3 | |
| 4 | Switch(config)#**vtp mode client** |
| 5 | Setting device to VTP CLIENT mode. |
| 6 | |
| 7 | Switch(config)#**vtp password ccna** |
| 8 | Setting device VLAN database password to ccna |

**Sw2**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode trunk** |
| 3 | |
| 4 | Switch(config)#**vtp mode client** |
| 5 | Setting device to VTP CLIENT mode. |
| 6 | |
| 7 | Switch(config)#**vtp password ccna** |
| 8 | Setting device VLAN database password to ccna |

```
Switch#show vlan b

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                Gig1/2
5    VLAN0005                         active
10   VLAN0010                         active
15   VLAN0015                         active
```

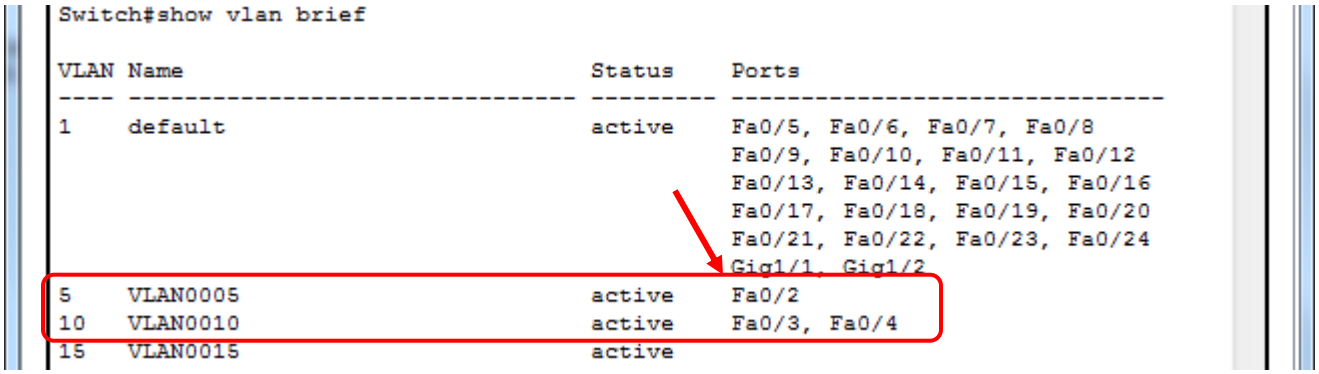
حال می بینیم که Vlan های تعریف شده در سرور به کلاینتها نیز منتقل شده است.

حال می توانیم به راحتی Interface های سویچهای کلاینت را در Vlan های مربوطه قرار دهیم.

**Sw1**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/2** |
| 2 | Switch(config-if)#**switchport mode access** |

```
3  Switch(config-if)#switchport access vlan 5
4
5  Switch(config-if)#int ra fa 0/3-4
6  Switch(config-if-range)#switchport mode access
7  Switch(config-if-range)#switchport access vlan 10
8
9  Switch#show vlan brief
```




و در سويچهاي ديگر نيز به همين صورت كانفيگ ها را انجام مي دهيم.
كانفيگ كلي سويچ 1:

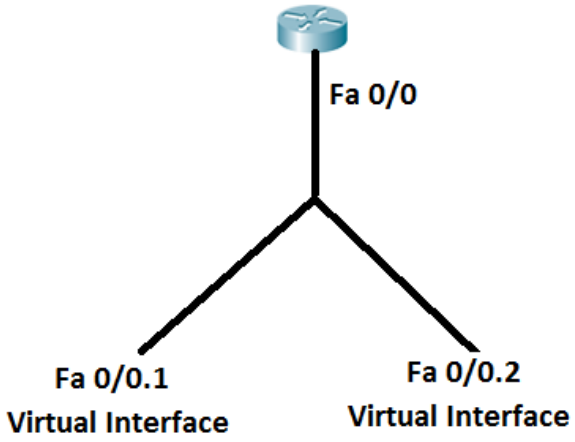
**Sw1**

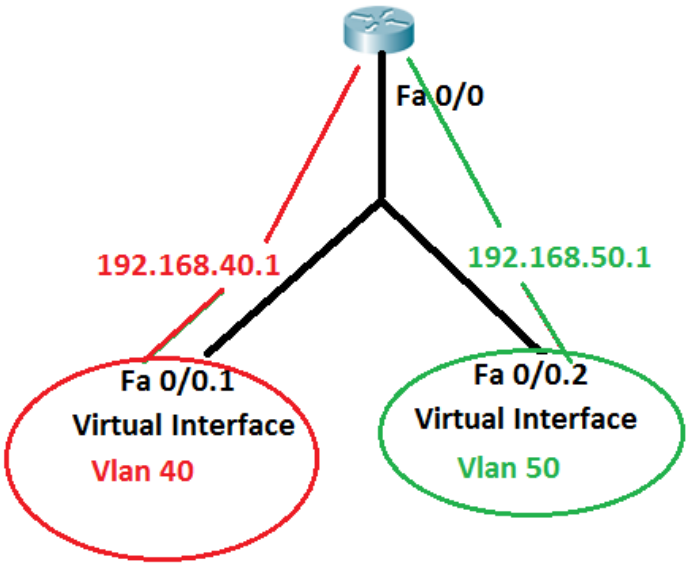
```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch(config)#vtp mode client
5  Setting device to VTP CLIENT mode.
6
7  Switch(config)#vtp password ccna
8  Setting device VLAN database password to ccna
9
10 Switch(config)#interface fastEthernet 0/2
11 Switch(config-if)#switchport mode access
12 Switch(config-if)#switchport access vlan 5
13
14 Switch(config-if)#int ra fa 0/3-4
15 Switch(config-if-range)#switchport mode access
16 Switch(config-if-range)#switchport access vlan 10
17
18 Switch#show vlan brief
```

## اتصال دو Vlan غير هم نام به يكديگر

براي وارد شدن به Vlan هاي متفاوت و انجام مسير يابي:

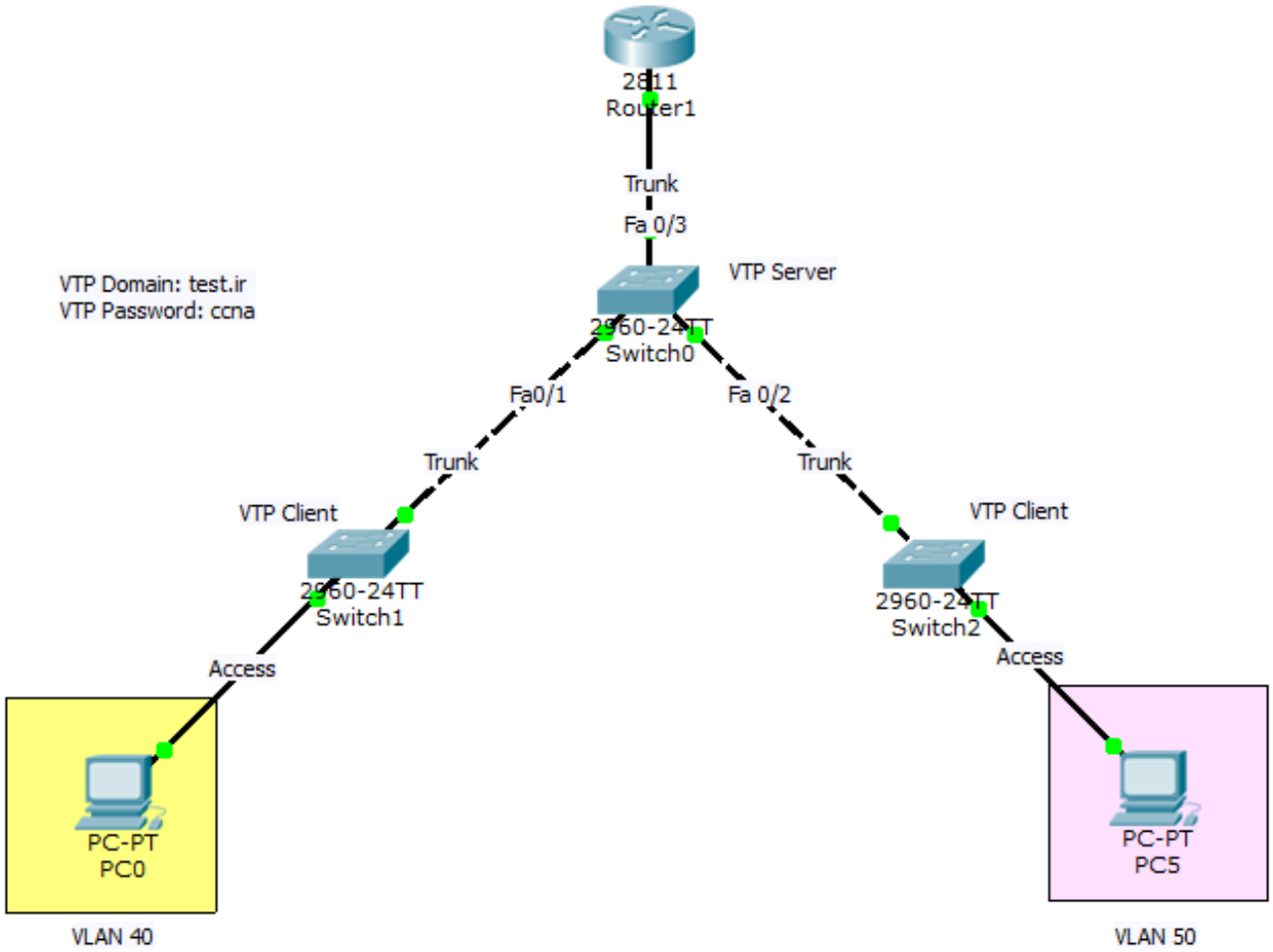
- براي اتصال دو Vlanمتفاوت، نياز به يك روتر داريم. روتر را بايد به سويچ سرور وصل كنيم.
- از تكنيك Sub interface استفاده مي كنيم. يك Interface حقيقي به دو Subinterface تقسيم مي شود. (مثل سه راهي)
- تذكر: در كامپيوترها Gatewaye ما، همان IP اي است كه به پورتهاي مجازي روتر اختصاص داده ايم.




Fa0/0 اينترفيس حقيقي است و
Fa0/0.1 و Fa0/0.2 مجازي است كه رنج IP هايشان با هم متفاوت است.

سناريوي زير را اجرا كنيد. و كاري كنيد كه كامپيوترها همديگر را پينگ كنند.




**Sw0**

```
1  Switch(config)#int range fastEthernet 0/1-2
2  Switch(config-if-range)#switchport mode trunk
3
4  Switch(config)#interface fastEthernet 0/3
5  Switch(config-if)#switchport mode trunk
6
7  Switch(config)#vtp mode server
8  Device mode already VTP SERVER.
9
10 Switch(config)#vtp domain test.ir
11 Changing VTP domain name from NULL to test.ir
12
13 Switch(config)#vtp password ccna
14 Setting device VLAN database password to ccna
15
16 Switch(config)#vlan 50
17 Switch(config)#vlan 40
```

- خط 1 و 2: مانند سناريوهاي قبل پورتهاي بين سويچ ها را از نوع ترانك تعريف مي كنيم.
- خط 4 و 5: پورت بين سويچ و روتر را بايد از نوع Trunk تعريف كنيم.
- باقي تعريف ها همانند سناريوي قبل.

**Sw1:**

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch(config)#vtp mode client
5  Setting device to VTP CLIENT mode.
6
7  Switch(config)#vtp password ccna
8  Setting device VLAN database password to ccna
9
10 Switch(config)#interface fastEthernet 0/2
11 Switch(config-if)#switchport mode access
12 Switch(config-if)#switchport access vlan 40
13
14 Switch#show vlan brief
15
```

**Sw2:**

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Switch(config)#vtp mode client
5  Setting device to VTP CLIENT mode.
6
7  Switch(config)#vtp password ccna
8  Setting device VLAN database password to ccna
9
10 Switch(config)#interface fastEthernet 0/2
11 Switch(config-if)#switchport mode access
12 Switch(config-if)#switchport access vlan 50
13
14 Switch#show vlan brief
```

**Router**

```
1  Router(config-if)#interface fastEthernet 0/0.1
2  Router(config-subif)#encapsulation dot1Q 40
3  Router(config-subif)#ip address 192.168.40.1 255.255.255.0
4
5  Router(config)#interface fastEthernet 0/0.2
6  Router(config-subif)#encapsulation dot1Q 50
```

```
7   Router(config-subif)#ip address 192.168.50.1 255.255.255.0
8
9   Router(config)#interface fastEthernet 0/0
10  Router(config-if)#no sh
11
12  Router(config-if)#
13  %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
14
15  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
16
17  %LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
18
19  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
20
21  %LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
22
23  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up
```

مي خواهيم پورتهاي مجازي را تعريف نماييم.

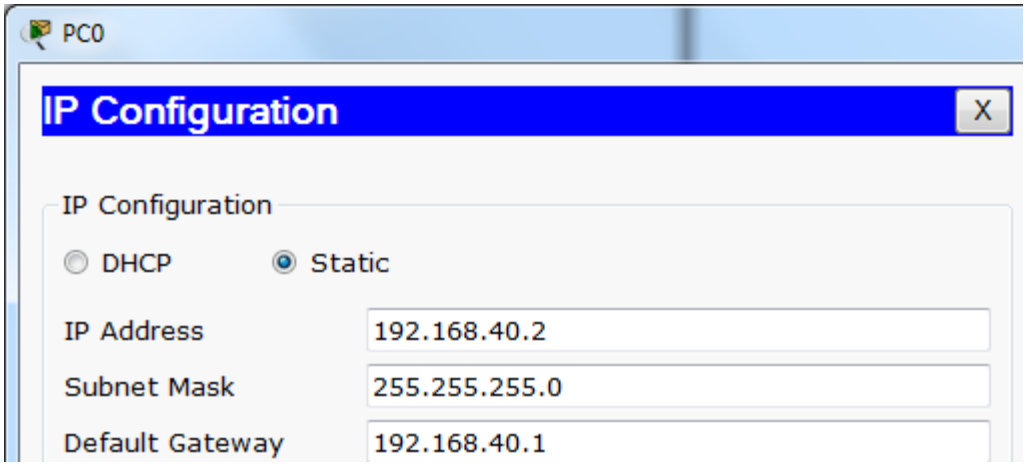
- خط 1 و 5: وارد پورتهاي مجازي مي شويم.
- خط 2و 7: حتما در جلوي هر كدام بايد شماره Vlan ي كه پورت مجازي به آن اتصال دارد را بنويسيم. مثلا پورت مجازي Fa 0/0.1 در Vlan 40 قرار دارد.
- خط 3و 8: IP هر رنج از Vlan ها را به پورتهاي مجازي اختصاص مي دهيم.
- **خط 9: وارد پورت حقيقي روتر مي شويم.**
- **خط 10: No shutdown مي كنيم.**

**توجه: اگر پورت حقيقي را Upنكنيم، پورتهاي مجازي Up نمي شوند. همانطوري كه در خطوط 13 به بعد مشاهده مي فرماييد، 3 پورت را Up مي كند كه شامل يك پورت حقيقي و دو پورت مجازي است.**

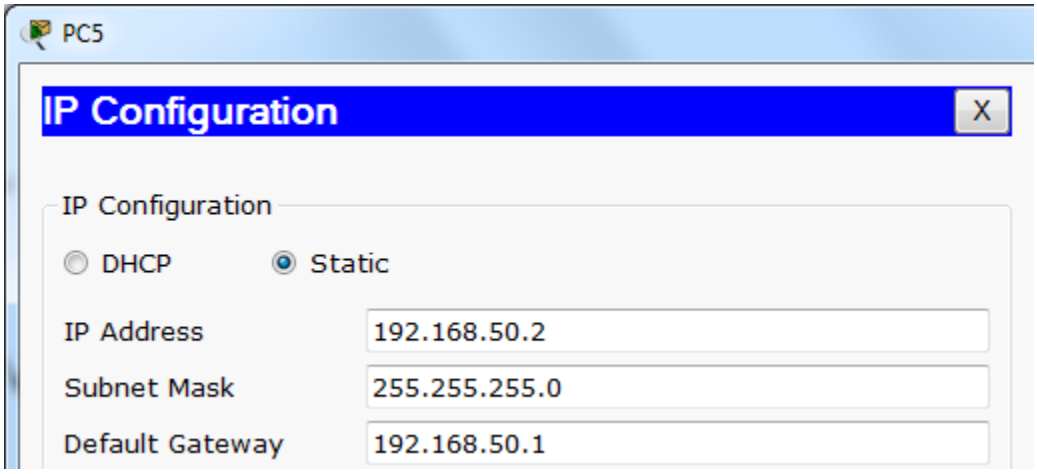
به كامپيوترها IP اختصاص مي دهيم:

**تذكر: Gateway هر كدام از كامپيوترها، IP اي است كه به پورتهاي مجازي روتر اختصاص داده ايم.**

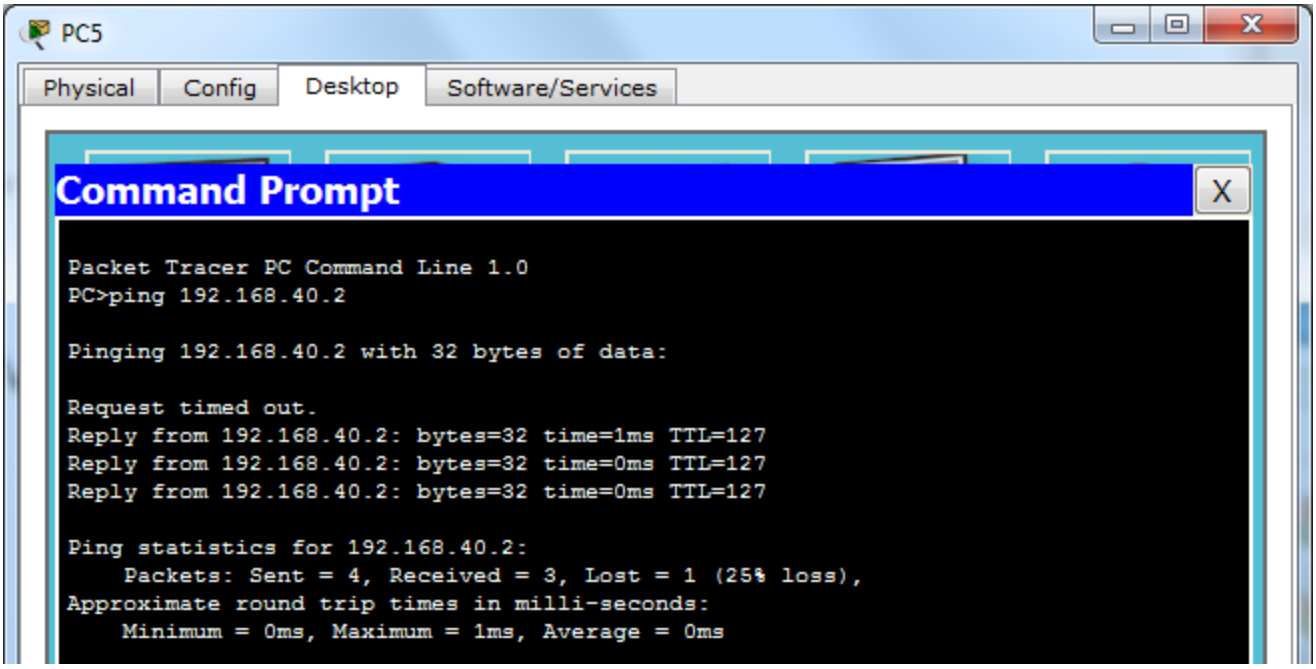
**PC0:**




**PC1:**




حال مي توانيم كامپيوترهاي موجود در دو Vlan مختلف را Ping كنيم:



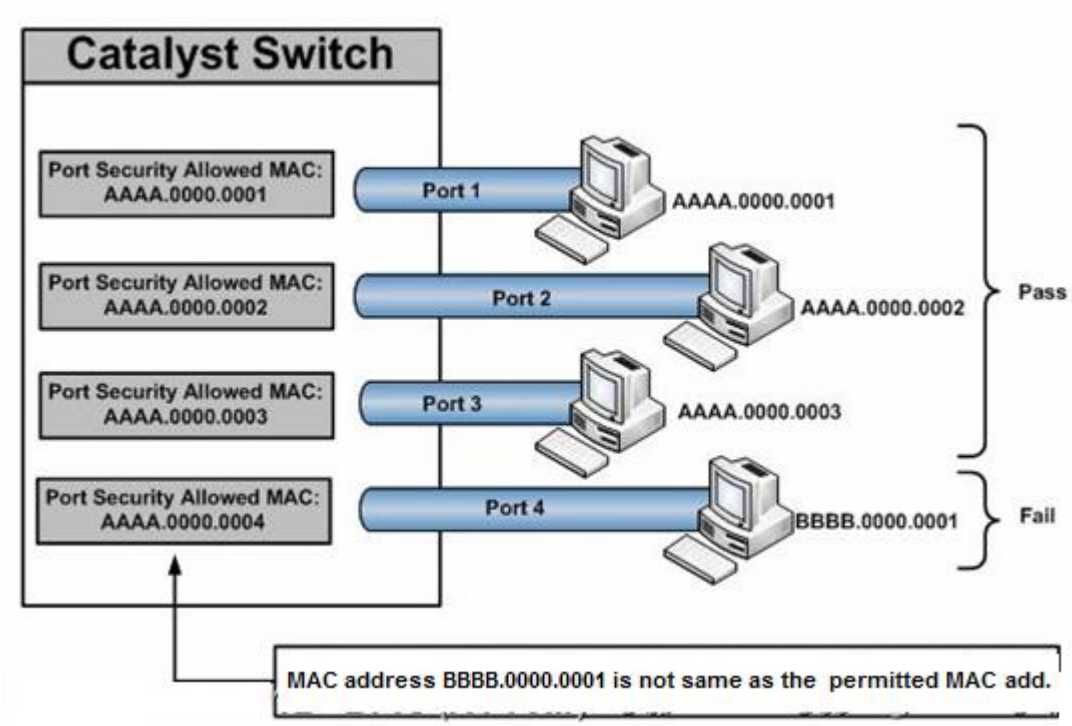
# Port Security

در این قسمت با مفهوم Port Security و اینکه چگونه از این قابلیت سویچ های سیسکو در جهت ایمن سازی سویچ ها و محدود سازی دسترسی به پورت های سویچ شبکه خود استفاده کنیم آشنا خواهیم شد.
یکی از مشکلاتی که مدیران شبکه بسیار با آن درگیر هستند این است که چگونه میتوانند دسترسی های غیر مجاز به شبکه را کنترل کنند ، در واقع مشکل اصلی اینجاست که نمیدانیم چگونه میتوان برای تجهیزات شبکه تعریف کرد که چه کسی بتواند به آنها متصل شود و چه کسی نتواند متصل شود . برای مثال شما نمی خواهید که هر کسی که وارد سازمان شما شد براحتی با استفاده از لپ تاپ خود و متصل کردن آن به یکی از پورت های سویچ شبکه به شبکه شما متصل شده و به منابع شبکه شما دسترسی پیدا کند . شاید با خود بگویید که تمامی پورت های شبکه ما که بر روی دیوار قرار گرفته اند و کامپیوتری به آنها متصل نیست بصورت فیزیکی به سویچ و شبکه متصل نیستند و دیگر جای نگرانی در این خصوص وجود ندارد ، اما اگر شخص کابل کامپیوتر فعالی که مشغول سرویس دهی در شبکه است را از جای خود در آورده و از آن برای اتصال به سویچ و شبکه استفاده کند چطور ؟ این کامپیوتر در ساده ترین حالت ممکن میتواند ویروس ها و کرم های خطرناکی را وارد شبکه ما کند.

**شناخت مبانی Port Security**

در ساده ترین حالت ممکن این قابلیت آدرس سخت افزاری کارت شبکه شما یا همان MACشما را در حافظه ای مربوط به آن پورت ذخیره میکند و فقط به همین آدرس سخت افزاری اجازه ورود به پورت شبکه را میدهد . اگر آدرس سخت افزاری دیگری بخواهد از طریق همان پورت سویچ به شبکه متصل شود ، سویچ آن را بلوکه کرده و اجازه ورود به سیستم را به آن پورت نخواهد داد ، این میتواند غیرفعال کردن پورت سویچ نیز باشد . در شبکه هایی که سیستم های مانیتورینگ یا پایش شبکه راه اندازی شده اند با استفاده از پروتکل SNMP تنظیماتی انجام شده است که بلافاصله بعد از غیرفعال شدن پورت سویچ به سیستم مانیتورینگ اطلاع رسانی می شود و در لاگ این سیستم ثبت می شود.

همیشه انجام تنظیمات امنیتی بر روی شبکه نیاز به سبک سنگین کردن و بررسی درست پیامد های آن دارد . برخی اوقات پیاده سازی امنیت باعث پایین آمدن سهولت کاربری و سخت کردن فعالیت کاری میشود . وقتی شما از قابلیت Port Security استفاده میکنید ، در حقیقت اتصال هر دستگاهی به شبکه را محدود کرده اید و بر حسب آن امنیت خود و شبکه را بالا برده اید . اما همیشه حالت برعکسی هم وجود دارد ، در این حالت از Port Security فقط مدیر شبکه میتواند پورت غیرفعال شده را فعال یا به اصطلاح unlock کند ، و این خود باعث بوجود آمدن دردسرهای مدیریتی زیادی برای مدیر شبکه خواهد شد.




| | |
|---|---|
| 1 | Switch)# **config t** |
| 2 | Switch(config)# **int fa0/5** |
| 3 | Switch(config-if)# **switchport port-security [aging \| mac-address\| maximum\| violation]** |
| 4 | |
| 5 | Switch(config-if)# **switchport mode access** |
| 6 | Switch(config-if)# **switchport security** |
| 7 | Switch(config-if)# **switchport security maximum 1** |
| 8 | Switch(config-if)# **switchport security mac-address sticky** |
| 9 | Switch(config-if)# **switchport security violation [shutdown\| restrict]** |
| 10 | |
| 11 | Switch(config-if)# **switchport security interface FastEthernet 0/5** |

به ازای هر پورت می توان این دستورات را اجرا کرد.

- خط 5: پورتی که می خواهیم در وضعیت Security قرار دهیم باید در مد access باشد.
- خط 6: حال باید Port Security را روی آن فعال کنیم.
- حال که فعال شد باید دو نوع کامند مجاز و غیر مجاز را تعریف می کنیم.
- خط 7: یعنی ماکزیمم فقط یک سیستم را بتوانیم وصل کنیم.
- خط 8: اولین سیستم، سیستمی باشد که اولین بار به آن وصل شده است. به جای Sticky می توانیم Mac Address سیستم مورد نظرمان را وارد کنیم که اگر سیستم دیگری به آن پورت وصل شد نتواند وارد شبکه شود.
- خط 9: در غیر اینصورت پورت را Shutdown / restrict کن. (در حالت Shutdown، پورت مسدود می شود و log را به Admin ارسال می نماید / در حالت Restrict پورت مسدود می شود و log آن به Admin ارسال نمی شود).

- خط 11: دستور Verify، اطلاعات پورت Fasethernet 0/5 را نمایش می دهد.

**جهت پاک کردن کلیه تنظیمات Port Security از کامند زیر استفاده می کنیم.**

| | |
|---|---|
| 1 | Switch#**clear port-security all** |
| 2 | Switch#**reload** |

# دسترسی به سویچ از راه دور

- Telnet
- SSH

Interface های مجازی در سویچ وجود دارد VLAN:

جهت اتصال از طریق Telnet و SSH ابتدا باید به سویچ IP اختصاص دهیم.

- در سویچها Interface مجازی با عنوان Vlan1 وجود دارد.

```
1  Switch#show ip interface b
2  Interface              IP-Address      OK? Method Status                Protocol
3
4  FastEthernet0/1        unassigned      YES manual down                  down
…   …
54 Vlan1                  unassigned      YES manual administratively down down
```

- Vlan1 همان Interface مجازی است. زمانی قابل استفاده است که وجو داشته باشد. جهت اتصال از راه دور به این Interface، IP اختصاص می دهیم.

```
1  Switch(config)#interface vlan 1
2  Switch(config-if)#ip address 192.168.10.1 255.255.255.0
3  Switch(config-if)#no sh
4
5  Switch(config-if)#
6  %LINK-5-CHANGED: Interface Vlan1, changed state to up
7
8  %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

- خط 1: وارد Interface مجازی می شویم.
- خط 2: به آن IP اختصاص می دهیم.
- خط 3: Up می کنیم.

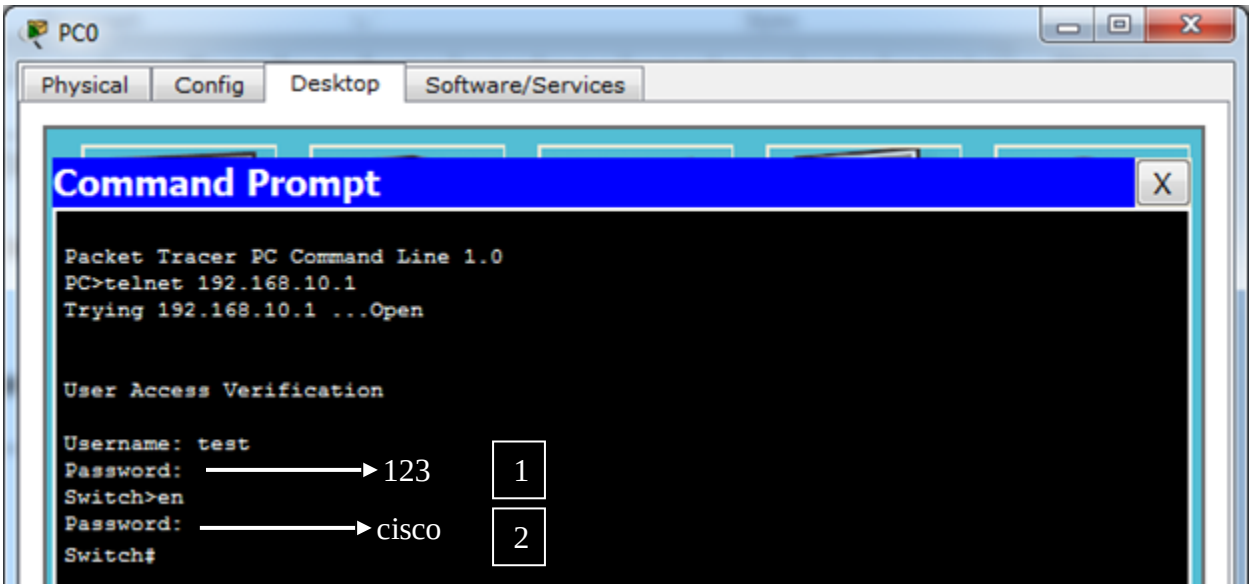
```
1  Switch#show ip interface b
2  Interface              IP-Address      OK? Method Status                Protocol
3
4  FastEthernet0/1        unassigned      YES manual down                  down
…   …
54 Vlan1                  192.168.10.1    YES manual up                    up
```

حال Interface مورد نظر Up شده و سویچ مورد نظر قابل دسترسی از راه دور می باشد.

```
1  Switch(config)#username test password 123
2  Switch(config)#line vty 0 4
3  Switch(config-line)#transport input telnet
```

| | |
|---|---|
| 4<br>5<br>6 | Switch(config-line)#**exit**<br><br>Switch(config)#**enable password <u>cisco</u>** |

- خط 1: تعریف Username و Password جهت اتصال به سویچ. (پسورد شماره 1 مطابق شکل زیر)
- خط 2:
- خط 3: نحوه ی اتصال
- خط 6: تعریف پسورد برای مد Enable سویچ. (پسورد شماره 2 مطابق شکل زیر)



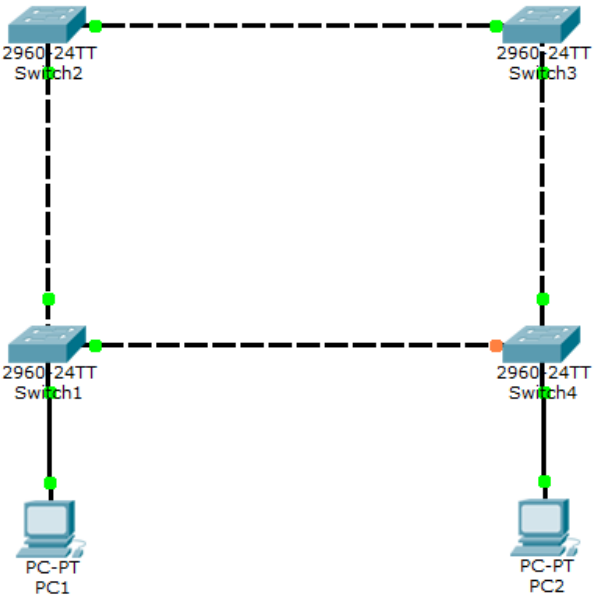
# پروتکل Spanning Tree

پروتکل STP یک پروتکل است که از بوجود آمدن Loop در سوئیچ جلوگیری می کند. منظور از Loop هم این استکه یک بسته از نقطه وارد شبکه شود و در یک حلقه بیفتد و مدام بین سوئیچ های شبکه بچرخد. در این حالت بسته مورد نظر هرگز از بین نخواهد رفت. اگر تعداد این بسته ها زیاد شود مسلما به زودی شبکه پر از این بسته های مزاحم خواهد شد و شبکه را مختل خواهد کرد. (**ایجاد Loop سبب کندي و پايين آمدن كارايي شبكه مي شود و شكبه را Down مي كند.** )

کار پروتکل STP در سوئیچ جلوگیری از بوجود آمدن لوپ در شبکه است. اگر لوپی بوجود نیاید هرگز مشکل فوق اتفاق نخواهد افتاد. چرا؟ چون بسته که از مبدا ارسال می شود به سمت مقصد حرکت کرده و به آن که میرسد یعنی اینکه بسته از بستر فیزیکی شبکه خارج می شود.

- **پورتهاي سوييچ چهار مرحله را طي مي كنند تا به حالت Fwd برسند: Block، Listen، Learn و Fwd.**
- **در دو حالت Sw در شبكه Broadcast انجام مي دهد: 1- موقعي كه روشن مي شود. 2- زمانيكه آدرس مقصد را نمي شناسد.**

پروتکل STP همیشه به صورت پیش فرض بر روی همه سوئیچ ها فعال است و نیاز نیست ما آنرا فعال کنیم.




در این شکل PC1 می خواهد با PC2 ارتباط برقرار کند.
Mac را ارسال مي كند.
يك پكت Broadcast مي كند.
همانطور که در شکل می بینید دو مسیر بین PC1 و PC2 وجود دارد.

- مستقیم از Sw1→Sw4
- از طریقSw1→Sw2→Sw4

يكي از مسيرهاي موجود برا جلوگيري از بوجود آمدن Loop بايد بسته شود. (به اين حالت حلقه بسته مي گويند كه حلقه بسته سبب بوجود آمدن Loop مي شود.)

براي فراگيري روش كار اين پروتكل، در بسیاری از مواقع می توانید با تنظیم و تغییر شبکه باعث عملکرد بهتر این پروتکل شوید.

برای ادامه بحث باید با برخی مفاهیم آشنا بشیم:

- BPDU یا Bridge Protocol Data Unit

سوئیچ های شبکه که بر روي آنها پروتكل STP اجرا شده برای اطلاع از احوال همدیگه از بسته های BPDU استفاده می کنن. دو نوع بسته BPDU تو پروتکل STP وجود داره:

BPDU Configuration: سوئیچ ها از این بسته ها برای محاسباتشان استفاده می کنن.
TCN BPDU: وقتی تغییری بر روی سوئیچی در شبکه رخ دهد برای اعلام تغییرات این مدل بسته را به سوئیچ های دیگه ارسال می کنه تا بروز تغییرات رو اعلام کنه.

- Root Bridge: یکی از سوئچ ها در شبکه به عنوان سوئیچ Root Bridge انتخاب می شود. این سوئیچ تعیین کننده مسیر انتقال بسته ها در شبکه است. مبنای انتخاب Root Bridge تو شبکه Bridge ID است. هر سوئیچ تو شبکه یک Bridge ID منحصر به فرد داره. سوئیچی که Bridge ID آن از همه کمتر باشه به عنوان Root Bridge انتخاب خواهد شد

- Bridge ID .یک مقدار 8 بایتی است که از دو قسمت تشکیل شده:

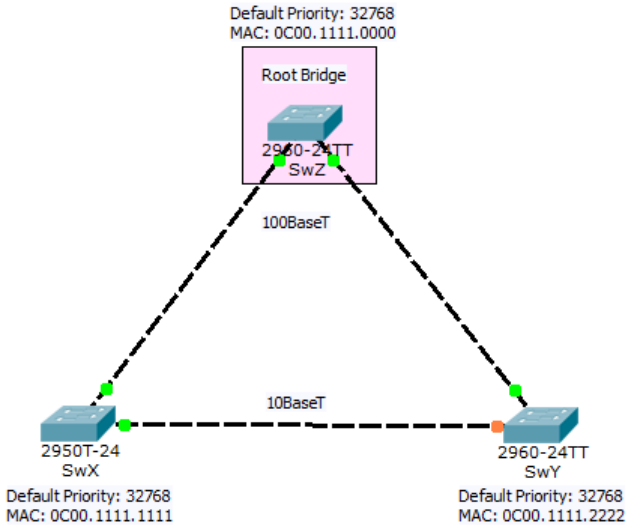
**B.ID= Bridge Priority (2 byte) + Mac Add. (8 byte)**

لحظه اي كه سويچ ها به يكديگر متصل مي شوند، B.ID هايشان را با هم تبادل مي كنند.

**کامند مربوط به مشاهده ي Spanning Tree:**

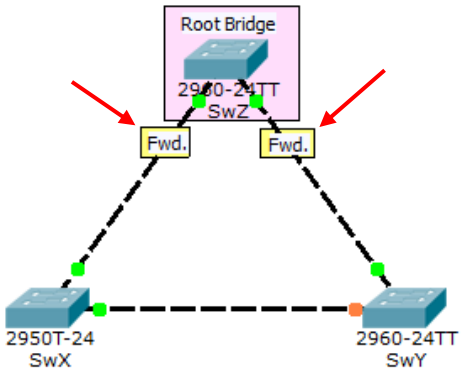
| | |
|---|---|
| 1 | Switch#**Show spanning tree** |

- **قانون اول:** Bridge Priority (اولویت Bridge) عددی بین 0 تا 65535 است. سوئیچی که Bridge Priority آن از سوئیچ های دیگر کمتر باشد به عنوان Root Bridge انتخاب خواهد شد. در صورتی که Bridge Priority همه سوئیچ ها یکسان باشد، از آدرس Mac سوئیچ ها به عنوان الگوی انتخاب استفاده می شود. در این حالت **سوئیچی که آدرس Mac آن از سوئیچ های دیگر کمتر باشد به عنوان Root Bridge انتخاب خواهد شد.**

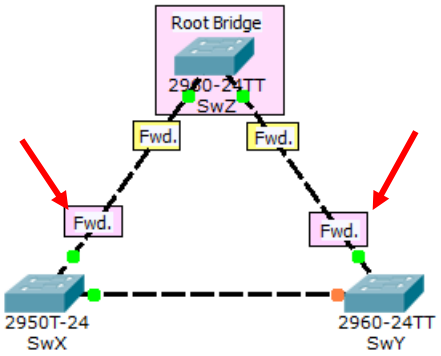



SwZ: $\begin{cases} \text{SwZ: } 32768 + 0C00.1111.0000 \\ \text{SwX: } 32768 + 0C00.1111.1111 \\ \text{SwY: } 32768 + 0c00.1111.2222 \end{cases}$ از همه کوچکتر است و به عنوان Root Bridge انتخاب می شود .

Root Bridge: باید با همه ی سیستمها در ارتباط باشد ← پورتهایش باید در وضعیت .Fwd باشند.

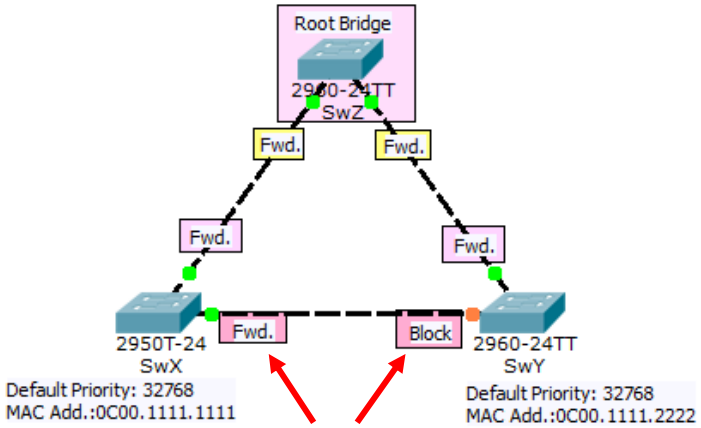


- **قانون دوم:** بين سويچ هاي باقي مانده، آنهاييكه بطور مستقيم به **R.Bridge** متصل هستند پورتهايشان بايد در وضعيت **Fwd** باشد(چون **R.Bridge** بايد با همه در ارتباط باشد.)




- **قانون سوم:** بين سويچ هاي باقي مانده دوباره بايد **B.ID** محاسبه شود.
سويچي كه از همه داراي **B.ID** كوچكتري است پورتش در حالت **Fwd.** قرار مي گيرد .
سويچي كه از همه داراي **B.ID** بزرگتر است پورتش در حالت **Block** قرار مي گيرد .

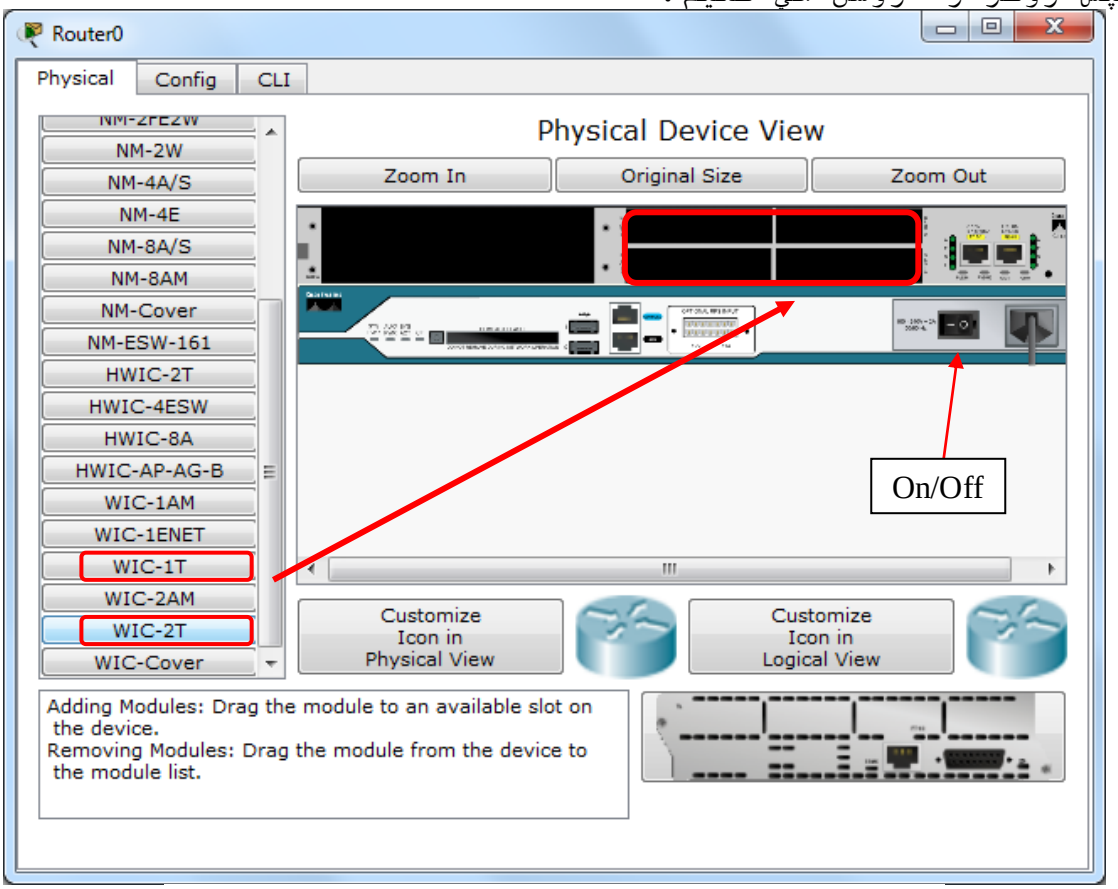
SwX: 32768 + 0C00.1111.1111 *Fwd.*
SwY: 32768 + 0c00.1111.2222 Block

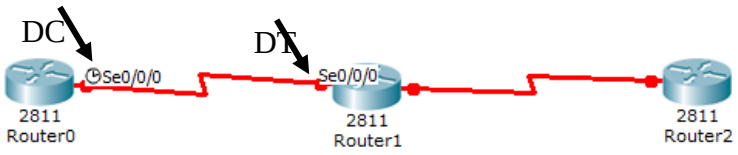



1- پوتهاي R.B ← Desinated Port (پورتهاي برگزيده) گويند.
2- آنهايي كه از جهت فيزيكي به B.R نزديكترند ← Root Port
3- B.Id مقايسه بين B.Id ها و كوچكتر از همه به عنوان ← Desinated Port
4- B.Id مقايسه بين B.Id ها و بزرگتر از همه به عنوان ← Non Desinated Port

# مباني مسير يابي

- اتصال روتر به روتر از كابل Connection Type: Serial DCE
- جهت اتصال روتر به روتر بايد از ماژولهاي WIC-1T (يك پورت سريال در اختيار ما قرار مي دهد) يا WIC-2T (دو پورت سريال در اختيار ما قرار مي دهد) در Packet Tracer استفاده كنيم.
- روتر را خاموش مي كنيم.
- ماژول مورد نظر را در مكان مورد نظر روي روتر درگ & دراپ مي كنيم.
- سپس روتر را روشن مي كنيم.




سمتي كه علامت Clock دارد DCE است و بايد Clock Rate تعريف شود.

**Router 0: (DCE)**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**ip address 192.168.12.1 255.255.255.0** |
| 3 | Router(config-if)#**clock rate 64000** |
| 4 | Router(config-if)#**no sh** |
| | %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down |

تذكر: در اين حالت در سمت اول چون هنوز ارتباط با طرق مقابل برقرار نيست (طرف مقابل Ip ندارد) اجازه نمي دهد لينك Up شود. با پيغام زير مواجه مي شويم.

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

**Router 1:**

```
1   Link R1& R2 (Serial 0/0/0 - DTE)
2   Router(config)#interface serial 0/0/0
3   Router(config-if)#ip address 192.168.12.2 255.255.255.0
4   Router(config-if)#no sh
5   %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
6
7
8   Link R2& R3 (Serial 0/0/1 - DCE)
9   Router(config)#int se 0/0/1
10  Router(config-if)#ip address 192.168.23.1 255.255.255.0
11  Router(config-if)#clock rate 64000
12  Router(config-if)#no sh
13  %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
```

Router3:

```
1   Router>en
2   Router#conf t
3   Router(config)#interface se 0/0/0
4   Router(config-if)#ip add 192.168.23.2 255.255.255.0
5   Router(config-if)#no sh
6
7   Router(config-if)#
8   %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

حال مي بينم كه لينك بين دو روتر Up مي شود. چون به هر دو سمت IP اختصاص داده شده است.
حال مي خواهيم ازRouter1، Router3 را پنگ كنيم. در حالت معمولي نمي توانند همديگر را پينگ كنند. اما در Router2 (كه به هر دو روتر متصل شده است) مي توانيم Router1وRouter3 را پينگ كنيم. در اينحالت بحث روتينگ Routing پيش مي آيد.
روتر جهت اتصال شبكه ها به يكديگر از جدول مسير يابي(Routing Table) استفاده مي كند.
مشاهده ي جدول مسير يابي روتر:

Router 1:

```
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    192.168.12.0/24 is directly connected, Serial0/0/0
Router#
```

Router 2:

```
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    192.168.12.0/24 is directly connected, Serial0/0/0
C    192.168.23.0/24 is directly connected, Serial0/0/1
Router#
```

## انواع مسير يابي

- Dynamic دايناميك
- Static دستي

مسيريابي اتوماتيك:

- در روش Dynamic از Routing Protocol استفاده مي شود.
- روي روترها اجرا مي شود.
- شكبه ها يكديگر را از هم مي پرسند.

## 1- مسير يابي دستي Static

- از طريق Command بايد شبكه ها معرفي شود.

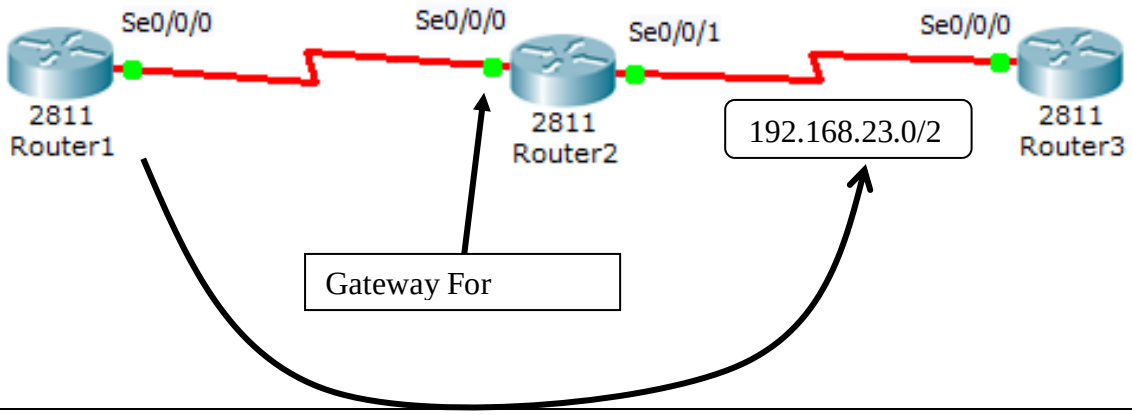
Router(config)#**ip route** شكبه طرف مقابل _ شكبه طرف مقابل Maskشبكه Gateway

در Router 1: مي خواهيم شبكه 192.168.23.0 را معرفي كنيم.

اگه در اين حالت Show Ip Route بگيريم مانند قبل فقط يك شبكه را مي شناسد.

```
C    192.168.12.0/24 is directly connected, Serial0/0/0
Router#
```

براي اين شبكه Gateway ما پورت Serial 0/0/0 Router2 مي باشد.




| | |
|---|---|
| 1 | Router(config)#**ip route 192.168.23.0 255.255.255.0 192.168.12.2** |
| 2 | Router#**show ip route** |

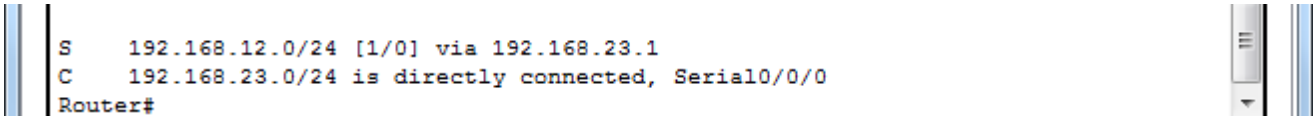
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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    192.168.12.0/24 is directly connected, Serial0/0/0
S    192.168.23.0/24 [1/0] via 192.168.12.2
Router#
```

حال مي بينم كه شبكه طرف مقابل را نيز مي شناسد و حرف S به معناي Static مي باشد.

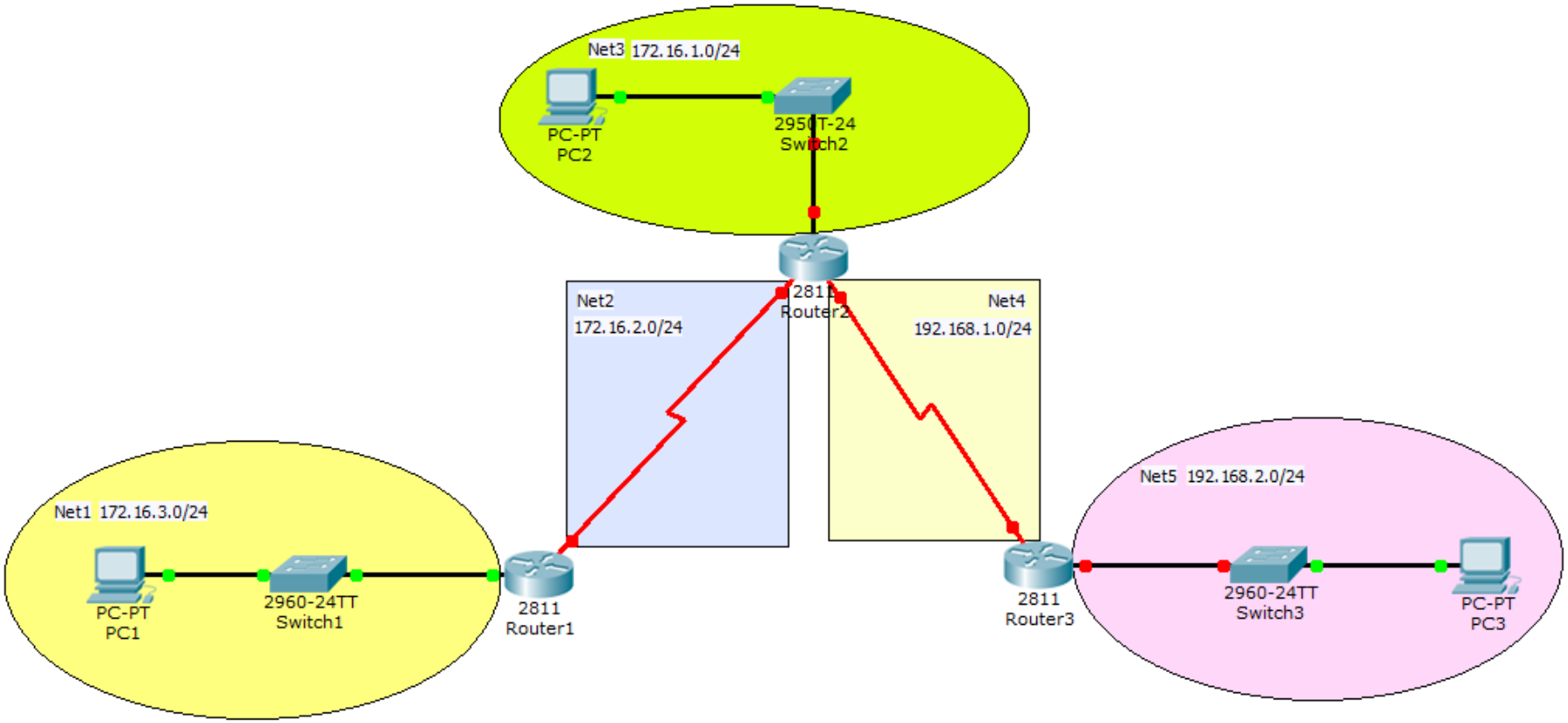
و اين كار را نيز در مورد Router 3 تكرار مي كنيم.

**Router3:**

| | |
|---|---|
| 1 | Router(config)#**ip route 192.168.12.0 255.255.255.0 192.168.23.1** |
| 2 | Router#**show ip route** |



## سناریو : Routing را بصورت Static



به طور کلي ما 5 شبکه داريم که به ترتيب شماره گذاري شده است.

**Net1: 172.16.3.0/24 Net2:172.16.2.0/24 Net3:192.16.1.0/24**
**Net4:192.168.1.0/24 Net5:192.168.2.0/24**

**1- ابتدا به Interface ها IP اختصاص مي دهيم و سپس عمل Routing را انجام مي دهيم.**

**Router1:**

```
1  Router(config)#interface fa0/0
2  Router(config-if)#ip address 172.16.3.1 255.255.255.0
3  Router(config-if)#no sh
4
5  Router(config-if)#int ser 0/0/0
6  Router(config-if)#ip address 172.16.2.2 255.255.255.0
7  Router(config-if)#no sh
```

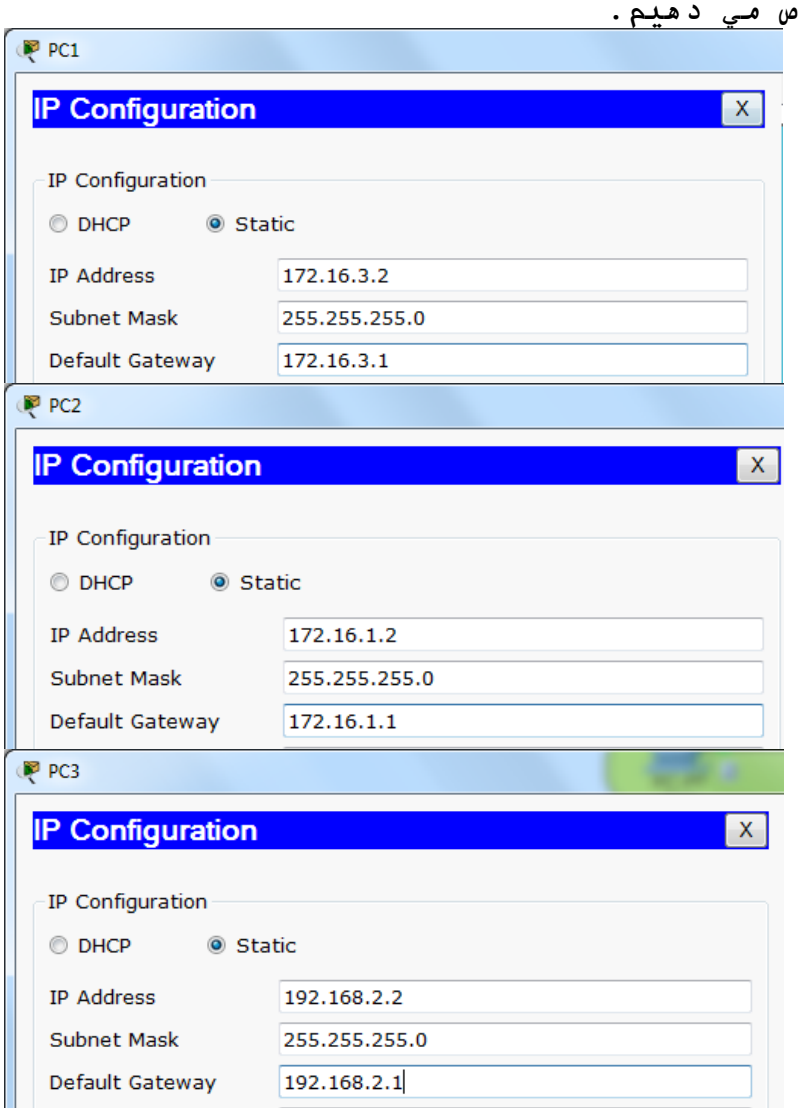
**Router2:**

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 172.16.2.1 255.255.255.0
3  Router(config-if)#clock rate 64000
4  Router(config-if)#no sh
5
6  Router(config-if)#int ser 0/0/1
7  Router(config-if)#ip address 192.168.1.1 255.255.255.0
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no sh
10
11 Router(config-if)#int fa 0/0
12 Router(config-if)#ip add 172.16.1.1 255.255.255.0
13 Router(config-if)#no sh
```

**Router3:**

```
1  Router(config)#interface ser 0/0/0
2  Router(config-if)#ip add 192.168.1.2 255.255.255.0
3  Router(config-if)#no sh
4
5  outer(config-if)#int fa 0/0
6  Router(config-if)#ip add 192.168.2.1
7  Router(config-if)#no sh
```

2- به کامپیوترها نیزIP اختصاص می دهیم.




3- حال باید **Routing** را انجام دهیم.

**Router 1:** به دو شبکه (**Net1**و **Net2**) به صورت مستقیم متصل می باشد. و سه شبکه دیگر (**Net3, Net4, Net5**) را باید به آن معرفی کنیم. برای همه ی این شبکه ها **Gateway** یکسان می باشد **172.16.2.1**.

**Router1:**

| | |
|---|---|
| 1 | Router(config)#**ip route** 172.16.1.0 255.255.255.0 172.16.2.1 |
| 2 | Router(config)#**ip route** 192.168.1.0 255.255.255.0 172.16.2.1 |
| 3 | Router(config)#**ip route** 192.168.2.0 255.255.255.0 172.16.2.1 |

**Router 2:** به سه شبکه (**Net2**و **Net3**و **Net4**) به صورت مستقیم متصل می باشد. و سه شبکه دیگر (**Net5, Net1,**) را باید به آن معرفی کنیم.
برای ارتباط با شبکه ی**Net1**، **Gateway** **172.16.2.2** می باشد.
برای ارتباط با شبکه ی**Net5**، **Gateway** **192.168.1.2** می باشد.

**Router2:**

| | |
|---|---|
| | Router(config)#**ip route** 172.16.3.0 255.255.255.0 172.16.2.2 |
| | Router(config)#**ip route** 192.168.2.0 255.255.255.0 192.168.1.2 |

**Router 3 :** به دو شبکه (**Net4**و **Net5**) به صورت مستقيم متصل مي باشد. و سه شبکه ديگر (**Net3, Net2, Net1**) را بايد به آن معرفي کنيم. براي همه ي اين شبکه ها **Gateway** يکسان مي باشد **192.168.1.1**.

**Router3:**

```
Router(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
Router(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.1
Router(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.1
```

**4- تست ارتباطات**

**Router1: Show IP Route**

```
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.1
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.1
S    192.168.2.0/24 [1/0] via 172.16.2.1
Router#
```

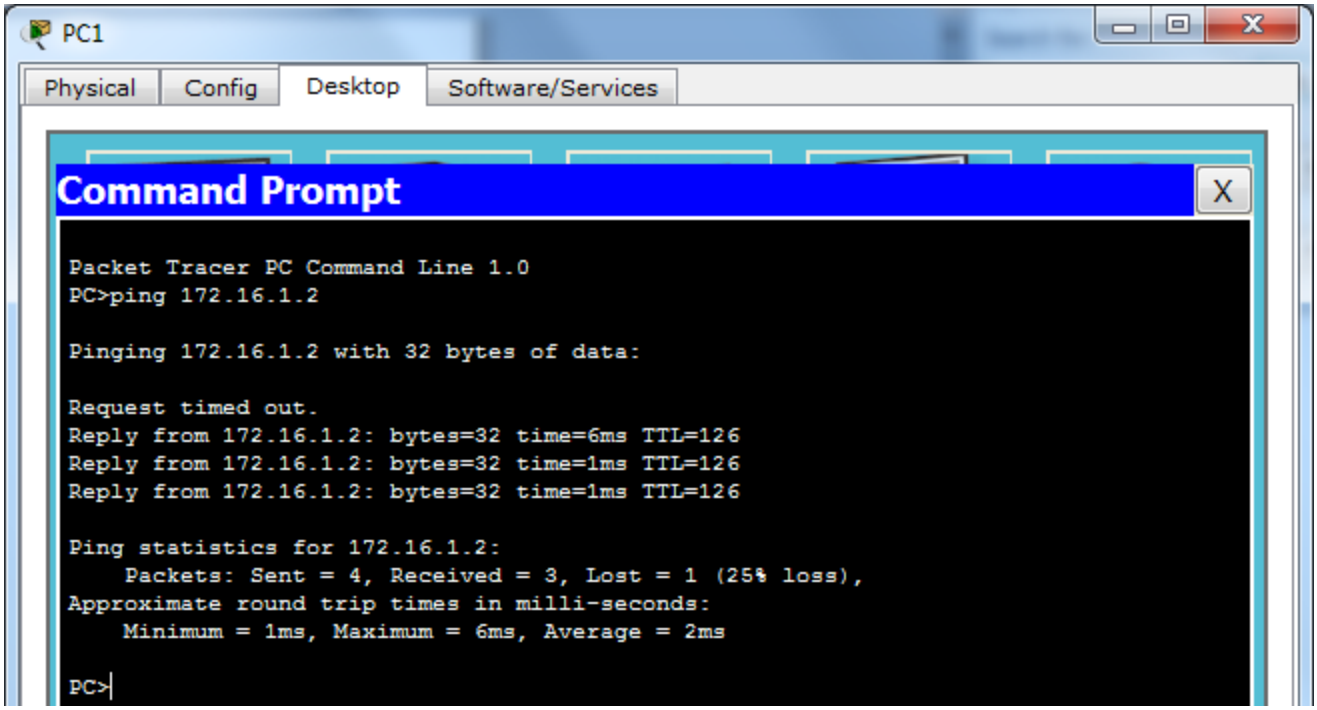
**Router2: Show IP Route**

```
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 [1/0] via 172.16.2.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.2
Router#
```

**Router3: Show IP Route**

```
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 192.168.1.1
S       172.16.2.0 [1/0] via 192.168.1.1
S       172.16.3.0 [1/0] via 192.168.1.1
C    192.168.1.0/24 is directly connected, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router#
```

و يا اينکه مي توانيم کامپيوترهاي هر مجموعه را **Ping** کنيم:
از کامپيوتر **PC1** موجود در شبکه **Net1**، کامپيوتر**PC2** موجود در شبکه **Net3** را **Ping** مي کنيم. همانگونه که مشاهده مي فرماييد کامپيوترها همديگر را مي بينند.




جمع بندي : **Config**هاي انجام شده در روترها.

**Router1:**

```
1   Router(config)#interface fa0/0
2   Router(config-if)#ip address 172.16.3.1 255.255.255.0
3   Router(config-if)#no sh
4
5   Router(config-if)#int ser 0/0/0
6   Router(config-if)#ip address 172.16.2.2 255.255.255.0
7   Router(config-if)#no sh
8
9   Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
10  Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.1
11  Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.1
12
13  Router#Show IP Route
```

**Router2:**

```
1   Router(config)#interface serial 0/0/0
2   Router(config-if)#ip address 172.16.2.1 255.255.255.0
3   Router(config-if)#clock rate 64000
4   Router(config-if)#no sh
5
6   Router(config-if)#int ser 0/0/1
7   Router(config-if)#ip address 192.168.1.1 255.255.255.0
8   Router(config-if)#clock rate 64000
9   Router(config-if)#no sh
10
```

```
11  Router(config-if)#int fa 0/0
12  Router(config-if)#ip add 172.16.1.1 255.255.255.0
13  Router(config-if)#no sh
14
15  Router(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.2
16  Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
17
18  Router#Show IP Route
```

**Router3:**

```
1   Router(config)#interface ser 0/0/0
2   Router(config-if)#ip add 192.168.1.2 255.255.255.0
3   Router(config-if)#no sh
4
5   outer(config-if)#int fa 0/0
6   Router(config-if)#ip add 192.168.2.1
7   Router(config-if)#no sh
8
9   Router(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
10  Router(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.1
11  Router(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.1
12
13  Router#Show IP Route
```

## 2- مسيريابي اتوماتيك Dynamic

**پروتكلهاي مسيريابي اتوماتيك شامل:**

**RIP**

**EIGRP**

**OSPF**

**Summary به معناي** خلاصه سازي شبكه ها كه دو نوع استاتيك(Static) و اتوماتيك(Automatic) مي باشد. كه در پروتكلهاي مسيريابي Rip و EIGRP وجود دارد.

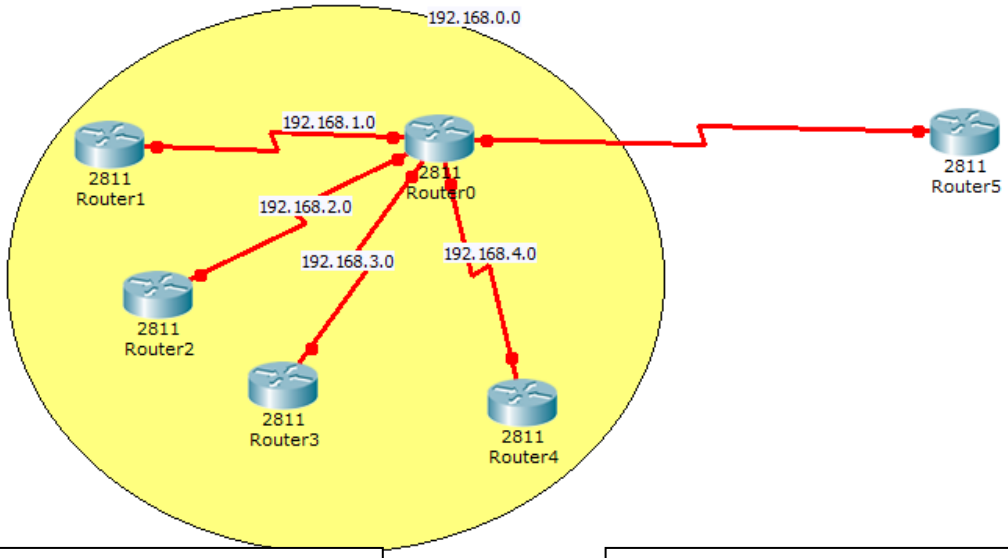
زمانيكه چند IP داريم ← به يك IP واحد تبديل مي كنيم. Supernetting كمتر مي شود. (شبكه ها را خلاصه مي كنيم.)

**مزيت Summary:**

- كمتر حرف مي زنند و در نتيجه ترافيك شبكه كمتر مي شود.
- حجم كمتري ديتا در لينك قرار مي گيرد.
- حجم جدول مسير يابي كم مي شود.

(همانگونه كه مي بينيد Routing Table 1, 2 از لحاظ اندازه بسيار متفاوتند.)

$\begin{cases} IP1 \\ IP2 \\ IP3 \end{cases} \rightarrow IP$ تبديل به يك آي پي مي شوند.




| Routing Table 1 |
|---|
| 192.168.1.0 |
| ..... |
| 192.168.2.0 |
| ..... |

| Routing Table 2 |
|---|
| 192.168.0.0 |
| ..... |

## RIP .1-2

**: Rip Configuration**

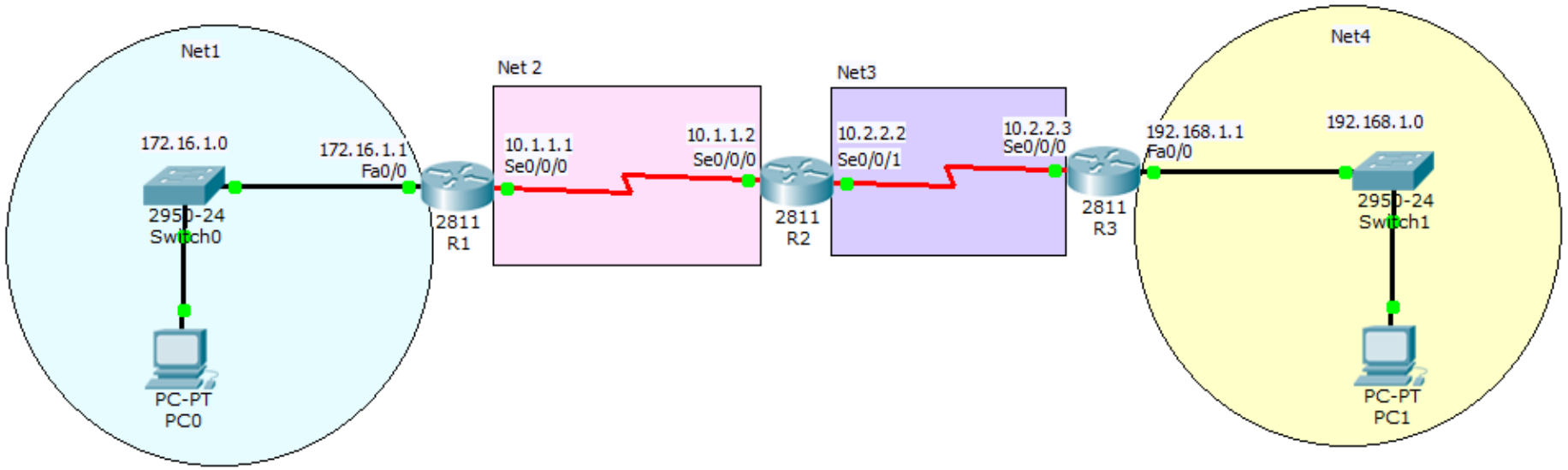
| | |
|---|---|
| 1 | Router(config)#**router rip** |
| 2 | Router(config-router)#**version 2** |
| 3 | Router(config-router)#**no auto-summary** |
| 4 | Router(config-router)#**network ……** |

- خط 1: فعال كردن پروتكل مسير يابي
- خط 2: پيش فرض Ver2 فعال مي باشد.
- خط 3: شبكه ها را به صورت اتوماتيك خلاصه نكن.
- خط 4: معرفي شبكه هايي كه به روتر متصل مي باشند.

**دستورات Verify:**

| | |
|---|---|
| 1 | Router#**show ip protocols** |
| 2 | Router#**show ip route** |
| 3 | Router#**debug ip rip** |
| 4 | Router#**undebug all** |

- خط 1: از طريق اين دستور از Enable بودن پروتكل مطمئن مي شويم.
- خط 2: مشاهده ي جدول مسيريابي
- خط 3: جهت عيب يابي اطلاعات تبادل شده مابين روترها استفاده مي شود. زماني به كار مي رود كه چند شبكه را به هم وصل كرده ايم و ممكن است اشتباه پيش بيايد و بخواهيم چك كنيم كه آيا ارتباط درست برقرار شده است يا خير. در اينحالت Log هارا نمايش مي دهد.
- خط 4: جهت غيرفعال كردن debug.


Net1
172.16.1.0
172.16.1.1
Fa0/0
2950-24
Switch0
PC-PT
PC0
2811
R1
Net 2
10.1.1.1
Se0/0/0
10.1.1.2
Se0/0/0
2811
R2
Net3
10.2.2.2
Se0/0/1
10.2.2.3
Se0/0/0
2811
R3
Net4
192.168.1.1
Fa0/0
192.168.1.0
2950-24
Switch1
PC-PT
PC1

ابتدا به Interface ها IP اختصاص می دهیم. سپس

**Router1:**

| | |
|---|---|
| 1 | Router(config)#**router rip** |
| 2 | Router(config-router)#**version 2** |
| 3 | Router(config-router)#**network 172.16.0.0** |
| 4 | Router(config-router)#**network 10.0.0.0** |

**Router2:**

| | |
|---|---|
| 4 | Router(config)#**router rip** |
| 2 | Router(config-router)#**version 2** |
| 3 | Router(config-router)#**network 10.0.0.0** |

**Router3**:

| | |
|---|---|
| 1 | Router(config)#**router rip** |
| 2 | Router(config-router)#**version 2** |
| 3 | Router(config-router)#**network 192.168.1.0** |
| 4 | Router(config-router)#**network 10.0.0.0** |

از مفهوم COST استفاده می کند.

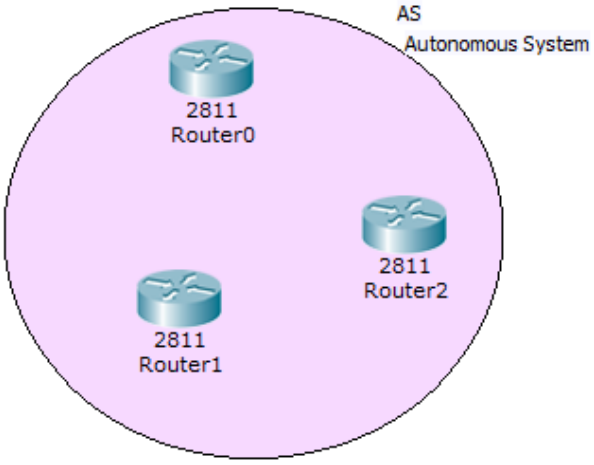
$$Cost = \frac{10^8}{R.Bw}$$

- از الگوریتم درختی برای مسیریابی استفاده می کند.
- ساختار درختی را در یک D.B (Data Base) قرار می دهند و بهترین مسیر را از D.B استخراج می کنند.
- روترها در OSPF به دو دسته تقسیم می شوند: **Single Area** و **Multi Area**
- روترهایی که در یک Area قرار دارند، پکتهایی که به یکدیگر می فرستند LSA Packet نام دارند.
- ساختار فیزیکی اتصال روترها درختی است.
- بطور کلی روترهایی که در یک Area قرار می گیرند 3 نقش اصلی دارند.

1- **DR:** Desinated Router روتری است که اگر تغییری برای یکی از روترها اتفاق بیافتد، آن تغییرات را به بقیه ی روترها می رساند(کنترل و مدیریت محدوده ی داخلی Area)

2- **DBR:** Backup DR پشتیبان DR است به محض خارج شدن DR از شبکه وظیفه ی DR را ادامه می دهد(پشتیبانی را انجام می دهد. )

3- **DROTNER:** روترهای معمولی هستند. که به صورت پیش فرض روترها در این گروه هستند.




2- اگر پیاده سازی Area تکی باشد ← شماره ی Area می تواند عدد دلخواه باشد.

3- اگر Multi Area داشته باشیم ← شماره هر چیز دلخواهی نمی تواند باشد.

**در حالت Multi Area:**

1- ساختار درختی است

2- روترها در اینجا جایگاه خاصی دارند.

a. بعضی ها بالا

b. بعضی ها بین Area ها

c. بعضی ها در قسمت پایین.

## انواع روتر

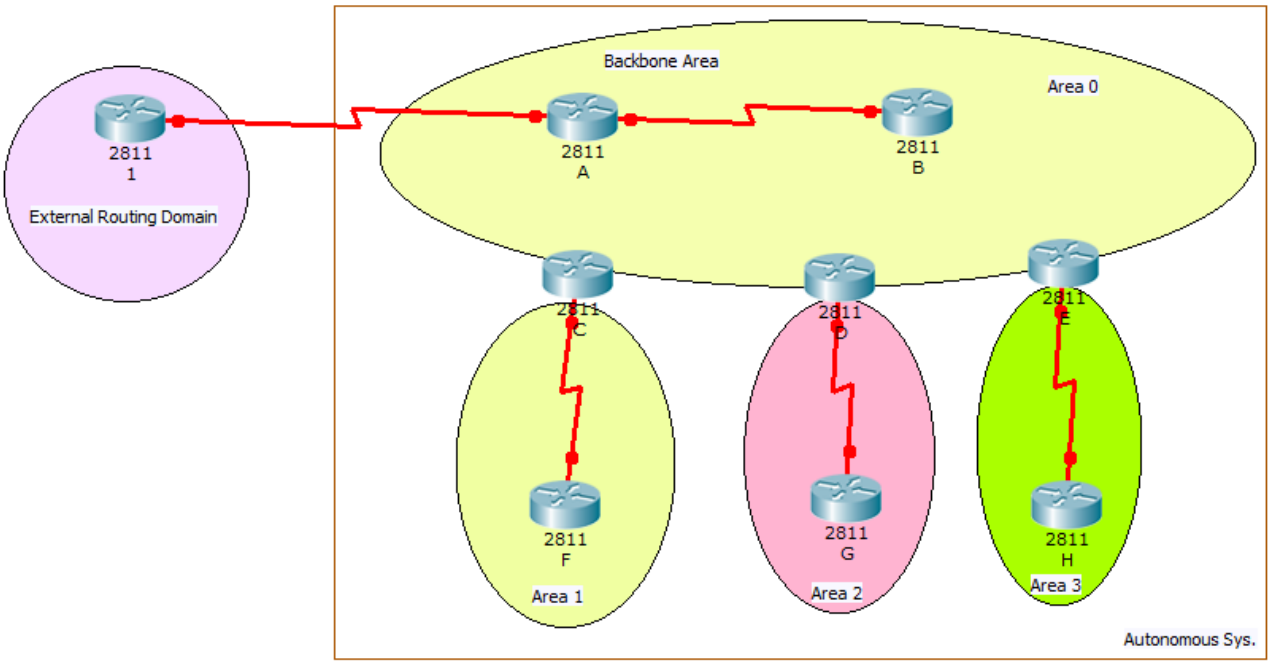
1- **Backbone Router:** Area هایی هستند که در Areaی Backbone با تمام Interface ها یش قرار گرفتند. مثل روتر Aو B.

**ویژگی: همیشه باید دارای شماره ی صفر باشند.**
به دلیل وجود ساختار درختی Area های غیر از صفر باید به Areaهای صفر متصل باشند ← حتما یک Backbone Area داریم.

2- **Internal Router:** روترهایی که با تمامی Interface هایشان در Area های غیر صفر قرار گرفته اند. یعنی باقی روترها در Area های 1و 2و3 مثل روتر H,G,F.

3- **ABR:** Area Border Router- روترهایی که در مرز Areaها قرار گرفتند. مثل روترهای E,D,C.
وظیفه ی اتصال Area های مختلف نسبت به هم را بر عهده دارند.

4- **ASBR:** Autonomous System- مجموعه همه ی Area ها با هم می شوند. **A.S**

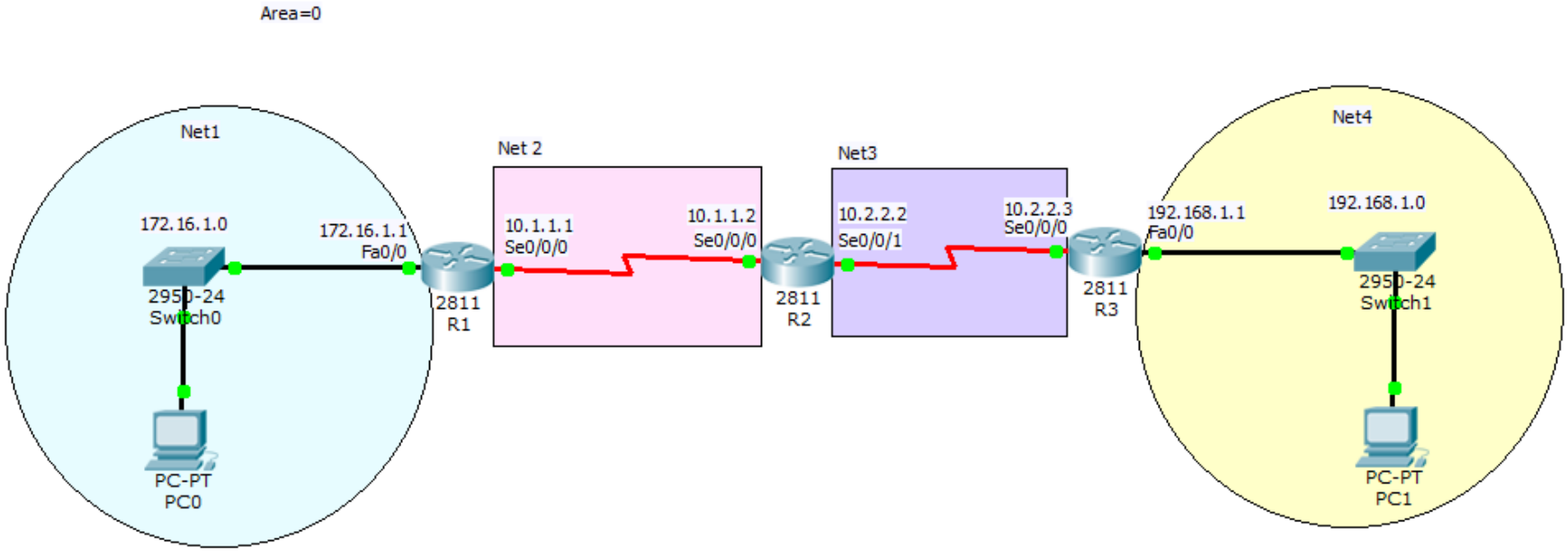



- **Router-ID:** مشخصه ای Unique است که از آن طریق به راحتی می توان روترها را شناسایی کرد.
- **Process-ID:** مشخصه ای است که توسط آن یک پروسس مستقل برای پروتکل OSPF تعریف می شود. عددی دلخواه است که توسط خودمان تعیین می شود.
- **Wildcard:** مربوط به بحث IP-Address هاست. اگر Mask متغیر باشد از 255 کم می کنیم و Wildcard بدست می آید.

Net ID: 192.168.18.0
Mask: 255.255.255.0
Wildcard: 0.0.0.255
Wide Card=255.255.255.255- Net.Mask = 255.255.255.255 – 255.255.255.0 = 0.0.0.255

- **Area-ID:** شماره ی Area است که در سناریو گفته می شود. (دلخواه نیست).

## سنـاریـو : Dynamic Routing with OSPF



**Router1:**

| | |
|---|---|
| 1 | Router(config)#**router ospf 100** |
| 2 | Router(config-router)#**network 10.1.1.1 0.0.0.0 area 0** |
| 3 | Router(config-router)#**network 172.16.1.1 0.0.0.0 area 0** |

- خط 1:

Router ospf ID(شماره ی دلخواه)

- این خط اجباری نیست.

Router(config-router)#**router-id 1.1.1.1(شماره دلخواه اما یونیک)**

- خط 3:

Router(config-router)#**network 10.1.1.0 0.0.0.255 area 0**

یا

Router(config-router)#**network 10.1.1.2 0.0.0.0 area 0**

- خط 3: در این قسمت هم می توان IP Interface هایی که به روتر متصل شده اند را نوشت به همراه Wildcard که در این صورت باید Wildcard: 0.0.0.0 نوشت.
- و یا اینکه Net ID را بنویسیم که در این صورت باید Wildcard:0.0.0.255 را بنویسیم.

**Router 2:**

| | |
|---|---|
| 1 | Router(config)#**router ospf 100** |
| 2 | Router(config-router)#**network 10.1.1.2 0.0.0.0 area 0** |
| 3 | Router(config-router)#**network 10.2.2.2 0.0.0.0 area 0** |

Router3:

| | |
|---|---|
| 1 | Router(config)#**router ospf 100** |
| 2 | Router(config-router)#**network 10.2.2.3 0.0.0.0 area 0** |
| 3 | Router(config-router)#**network 192.168.1.1 0.0.0.0 area 0** |

**دستورات Verify OSPF:**

| | |
|---|---|
| 1 | Router#**show ip protocols** |
| 2 | Router#**show ip route** |
| 3 | Router#**show ip ospf** |
| 4 | Router#**show ip ospf neighbor** |
| 5 | Router#**debug ip ospf events** |
| 6 | Router#**undebug all** |

- خط 2: دیدن جدول مسیریابی مروترهای مربوط ؟؟
- خط 3: با این دستور می توان Process IDو Router ID و تعداد دفعاتی که الگوریتم SPF مورد محاسبه قرار گرفته است قابل مشاهده است.
- خط 4: روترهای مجاور که شامل پروتکل مسیریابی OSPF هستند قابل شناسایی می باشند.
- خط5: دستور عیب یابی.
- خط 6: غیرفعال کردن عیب یابی.

**1:** Router#**show ip protocols**

```
Router#show ip protocols

Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.1 0.0.0.0 area 0
    172.16.1.1 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2              110      00:13:36
    172.16.1.1            110      00:16:20
    192.168.1.1           110      00:13:13
  Distance: (default is 110)
```

2: Router#**show ip route**

```
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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:41:50, Serial0/0/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/129] via 10.1.1.2, 00:38:57, Serial0/0/0
```

3: Router#**show ip ospf**

```
Router#show ip ospf
 Routing Process "ospf 100" with ID 172.16.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
```

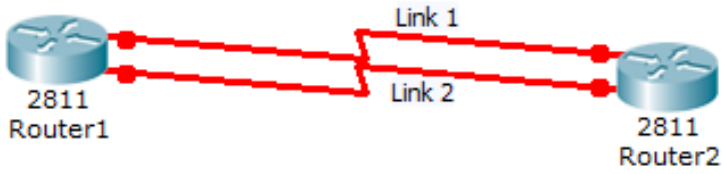
4: Router#**show ip ospf neighbor**

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          0   FULL/  -        00:00:34    10.1.1.2        Serial0/0/0
Router#
```

5: Router#**debug ip ospf events**

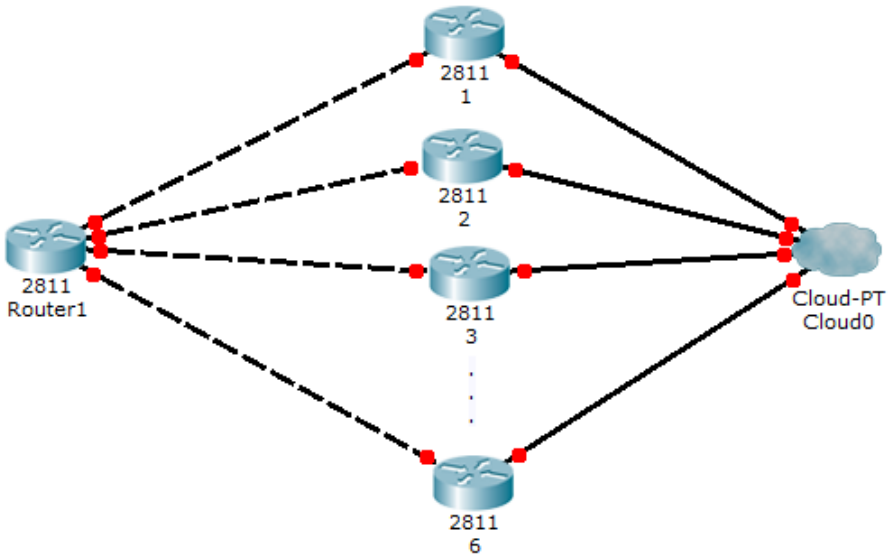
```
Router#debug ip ospf events
OSPF events debugging is on
Router#
01:05:27: OSPF: Rcv hello from 10.2.2.2 area 0 from Serial0/0/0 10.1.1.2

01:05:27: OSPF: End of hello processing
```

باید از لینکهایی که از جهت ارزش، یکسان باشند استفاده کنیم.




| | |
|---|---|
| 1 | Router(config-router)#**maximum-paths <value>** |
| 2 | Router(config-if)#**ip ospf cost <value>** |

یک روتر به 6 روتر در مقابل متصل شده است. می خواهیم بار را بین این 6 لینک تقسیم کنیم.




| | |
|---|---|
| 1 | Router(config)#**interface range fastEthernet 0/1-6** |
| 2 | Router(config-if)#**ip ospf cost 5** |
| 3 | Router(config)#**router ospf 100** |
| 4 | Router(config-router)#**maximum –paths 6** |

- خط 2: عدد 5 به این معناست که ارزش همه ی لینکها 5 می باشد.
- خود روتر به صورت خودکار از 4 لینک استفاده می کند.
- خط 4: خود روتر به صورت خودکار از 4 تا لینک استفاده می کند در حالیکه می خواهیم از همه ی 6 لینک استفاده کنیم.

## OSPF Authentication :

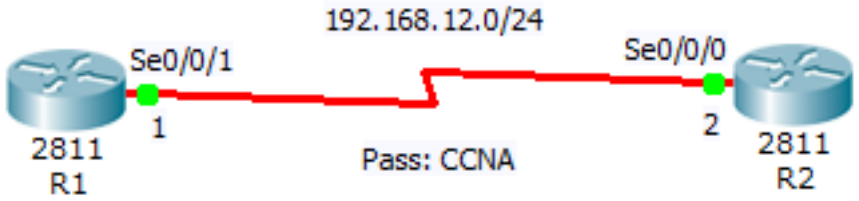
پیاده سازی مکانیزم احراز هویت مابین روترهایی‌که حامل پروتکل OSPF هستند.

- روتری که از بیرون نتواند بیاید و داخل Area ای که OSPF در آن Run شده خودش به شبکه متصل کن.
  - **Plane Test(Simple) :** بدین معناست که در مورد یک رمز شفاف صحبت شود ← امنیت آن پایین است و دیگر کاربرد ندارد. رمزها به راحتی برای یکدیگر بصورت واضح ارسال می شوند.
  - **Message Digest :MD5**، این پروتکل برای رمز نمودن اطلاعات می باشد.

```
1  R1(Config)#interface Serial0/0/0
2  R1(Config-if)# ip ospf authentication-key پسورد مورد نظر
3  R1(Config-if)#ip ospf authentication [message-digest| Null]
4  R1(config-router)#area area-id authentication [message-digest
```

- خط 1: وارد Interface ای می شویم که قرار است بین دو روتر مکانیزم احراز هویت راه اندازی نماییم.
- خط 2: در این خط رمز تعریف می کنیم که باید بین دو روتر مشترک باشد.
- خط 4: Autentication به ازای کل Area است در Multi Area استفاده می شود.

**مثال:**




```
1  R1(Config)#interface Serial0/0/1
2  R1(Config-if)#clock rate 64000
3  R1(Config-if)#ip address 192.168.12.1 255.255.255.0
4
5  R1(Config-if)#ip ospf authentication message-digest
6  R1(Config-if)#ip ospf authentication-key CCNA
```

```
1  R1(Config)#interface Serial0/0/0
2  R1(Config-if)#ip address 192.168.12.2 255.255.255.0
3
4  R1(Config-if)#ip ospf authentication message-digest
5  R1(Config-if)#ip ospf authentication-key CCNA
```

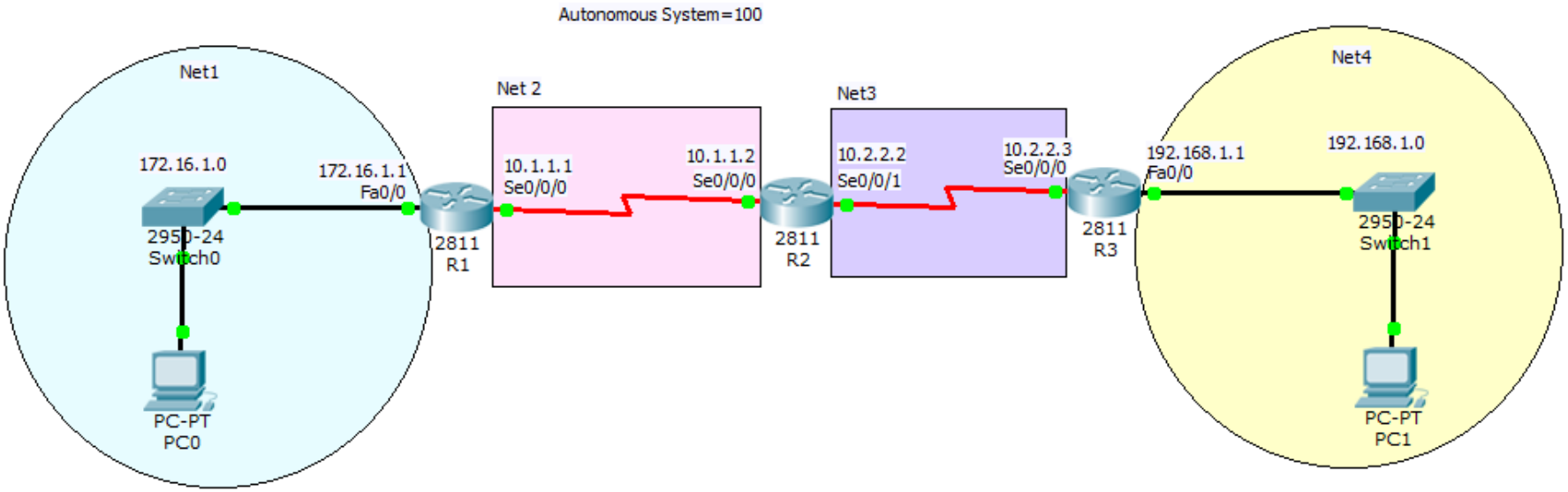
## EIGRP .3-2

- مهمترين مشخصه اش، پروتكل اختصاصي شركت سيسكو است و اگر تجهيزات سيسكو باشد، بهترين عملكرد را دارد.
- VertyFast و Hybrid است.
- پيدايش آن IGRP است كه بهبود يافته است. Enhanced IGRP
- Classless است.
- Update:
  - **Full:** اگر تغييري هم نيافته كل جدول مسير يابي را براي اطرافيان ارسال مي كند← پهناي باند شبكه را اشغال مي كند. (در Rip بدين صورت مي باشد)
  - **Incremental:** ارسال گزارش تغييرات در زماني اتفاق مي افتد كه واقعا تغييري بوجود بيايد و فقط تغييرات را ارسال مي كند ← پهناي باند كمي را اشغال مي كند. (در OSPF بدين صورت مي باشد)
- Load Balancing: ساختال Load به ازاي مسيرهاي با ارزش گذاري يكسان و غيريكسان قابل اجراست. مسيرهاي غير يكسان فقط توسط EIGRP ساورت مي شوند.
- استفاده از Multicastو Uni به جاي ← Broadcast
- VLSM را ساپورت مي كند.
- Summarization نيز انجام مي دهد.
- جداول مسيريابي در پروتكلهاي شكبه ساختارهاي امروزي:
  - Neighbor
  - Topology : شامل همه ي Net هاست
  - Routing ..
- ...
- اصطلاح Successor: بهتريم مسير، را از بين مسيرهاي موجود است.
- Feasible Successor: Backup براي Successor است.

**پياده سازي EIGRP:**

| | |
|---|---|
| 1 | Router(config)# **router eigrp <u>A.S(Autonomous-system)</u>** |
| 2 | Router(config-router)#**network <u>net-number</u>/<u>interface-ip wildcard –Mask</u>** |

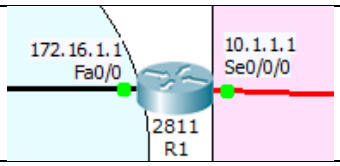
## سنـاریـو : Dynamic Routing with EIGRP



**: Config**

**Router 1:**

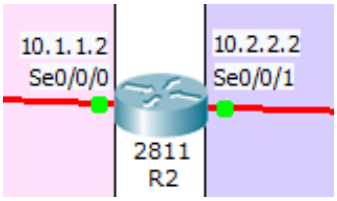
| | |
|---|---|
| 1 | Router(config)#**router eigrp 100** |
| 2 | Router(config-router)#**network 172.16.1.1** |
| 3 | Router(config-router)#**network 10.1.1.1** |




- خط 1: در جلوي EIGRP شماره ي A.S را مي نويسيم.
- خط 2و 3: IP، Interfaceهايي كه مستقيما به روتر متصل شده اند را مي نويسيم.

**Router 2:**

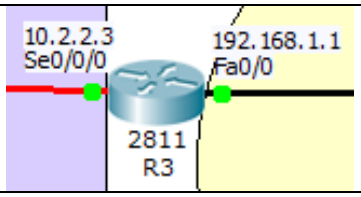
| | |
|---|---|
| 1 | Router(config)#**router eigrp 100** |
| 2 | Router(config-router)#**network 10.1.1.2** |
| 3 | Router(config-router)# |
| 4 | %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor |
| 5 | 10.1.1.1 (Serial0/0/0) is up: new adjacency |
| 6 | |
| 7 | Router(config-router)#**network 10.2.2.2** |




- خط 4: در صورتي كه پروتكل مسير يابي در دو سر لينك برقرار شود. اين پيغام را مي بينيم.

**Router 3:**

| | |
|---|---|
| 1 | Router(config)#**router eigrp 100** |
| 2 | Router(config-router)#**network 10.2.2.3** |
| 3 | Router(config-router)#**network 192.168.1.1** |



دستورات Verify EIGRP :

| | |
|---|---|
| 1 | Router#**show ip route eigrp** |
| 2 | Router#**show ip protocols** |
| 3 | Router#**show ip eigrp interfaces** |
| 4 | Router#**show ip eigrp neighbors** |
| 5 | Router#**show ip eigrp topology** |
| 6 | Router#**show ip eigrp traffic** |
| 7 | Router#**debug ip eigrp** |
| 8 | Router(config)#**interface loopback 1** |
| 9 | Router(config-if)#**ip address** |

1: Router#**show ip route eigrp**

```
Router#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:18:51, Null0
D       10.2.2.0/24 [90/2681856] via 10.1.1.2, 00:15:55, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:18:51, Null0
D    192.168.1.0/24 [90/2684416] via 10.1.1.2, 00:04:03, Serial0/0/0
Router#
```

2: Router#**show ip protocols**

```
Router#show ip protocols

Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
    10.0.0.0/8 for FastEthernet0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
     172.16.0.0
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2        90            1372838
  Distance: internal 90 external 170

Router#
```

3: Router#**show ip eigrp interfaces**

```
Router#show ip eigrp interfaces
IP-EIGRP interfaces for process 100

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0              0        0/0      1236       0/10           0           0
Se0/0/0            1        0/0      1236       0/10           0           0
Router#
```

4: Router#**show ip eigrp neighbors**

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address          Interface      Hold Uptime     SRTT    RTO   Q   Seq
                                    (sec)           (ms)        Cnt Num
0   10.1.1.2         Se0/0/0        13   00:20:08   40      1000  0   5

Router#
```

**5:** Router#**show ip eigrp topology**

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 10.1.1.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 10.0.0.0/8, 1 successors, FD is 2169856
         via Summary (2169856/0), Null0
P 172.16.0.0/16, 1 successors, FD is 28160
         via Summary (28160/0), Null0
```

6: Router#**show ip eigrp traffic**

```
Router#show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 100
  Hellos sent/received: 831/374
  Updates sent/received: 4/3
  Queries sent/received: 0/0
  Replies sent/received:  0/0
  Acks sent/received:  3/4
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0

Router#
```

## Interface Loopback :

بصورت مجازي هستند و به تعداد نامحدود قابل تعريف است و همواره Up مي باشند. مي توانيم به آنها Ip اختصاص دهيم.

| | |
|---|---|
| 1 | Router(config)#**interface loopback 1** |
| 2 | Router(config-if)#**ip address IP Mask** |

- خط 1: Interface Loopback شماره ي 1 را انتخاب كرده ايم.
- خط 2: به آن IP اختصاص مي دهيم.

**انواع پكت ها:**

**1- Hello Packet / Dead time:** يك بازه ي زماني 30 ثانيه اي است كه روتر اطلاعات را هر 30 ثانيه ارسال مي كند يكي از پكت هاي ارسال شده توسط روتر، پكت Hello packet است و روتر انتظار دارد كه روتر مجاور به اين Hello Packet پاسخ دهد اگر بعد از 4 بار ارسال، روترهاي مجاور پاسخ ندهند، روتر اصلي (كه پكت را ارسال كرده) روتر مقابل را از جدول مسيريابي خودش حذف مي كند.

**2- Update Packet:** پكت هايي كه در جهت Update كردن شبكه است.

**3- Query:** ارسال درخواست براي دريافت يك گزارش يا اطلاعات خاص.

**4- Reply:** جواب پكت Query است.

**5- Ack:** همان Delivery است. به لينك TCP/IP عمل مي كند.

## EIGRP Load Balancing :

- به دو دسته:

**1- مسيرهاي با متريك يكسان (ارزشگذاري يكسان):** تا چهار مسير را مي تواند بصورت اتوماتيك Load Balance كند. و خودمان مي توانيم تا 16 مسير را Load Balance كنيم. از طريق دستور Maximum-Paths مي توانيم مقدار مورد نظرمان را وارد كنيم.

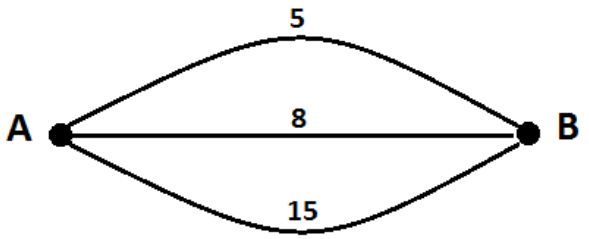
```
Router# maximum-paths 16
```

**2- مسيرهاي با متريك غيريكسان (ارزشگذاري غيريكسان):**

فقط پروتكل EIGRP به آن پرداخته مي شود و Command آن فقط در اين پروتكل وجود دارد.

مثلا: اگر بيش از يك مسير وجود داشته باشد، اعداد متريك 5و8و15 وجود داشته باشد، به صورت پيش فرض بهترين مسير براي رسيدن از A به B، مسير با متريك كوچكتر است يعني 5.

در صورتيكه ترافيك زياد شود تنها مسير 5 از عهده ي عبور اطلاعات بر نمي آيد ← بايد با انجام محاسبات از مسيرهاي ديگر نيز استفاده شود.




Multipier ← از نسبت بزرگترين متريك / كوچكترين متريك بدست مي آيد.

$$Multipier = \frac{\text{بزرگترين متريك}}{\text{كوچكترين متريك}}$$

## EIGRP Authentication :

دو Step اصلي وجود دارد و لزوماً از MD5 استفاده مي كند. (حتما رمزنگاري مي كند)

### 1- تعريف كردن پسورد با Key Chain

يك دسته كليدي است كه يك كليد Select مي شود به آن كليد يك پسورد اختصاص مي دهيم.

```
1  Router(Config)#key chain name-of-chan
2  Router(Config-keyChain)#key key-ID
3  Router(Config-keyChain-key)#key-string text
4  Router(Config-keyChain-key)#accept-lifetime start-time{infinit|end-time|duration-second}
5  Router(Config-keyChain-key)#send-lifetime start-time{infinit|end-time|duration-second}
```

- خط 4: يعني بازه زماني كه در آن كليد از روتر مجاور دريافت شود. (اين خط الزامي نيست)
- خط 5: بازه زماني است كه در آن كليد براي روتر مجاور ارسال مي شود. (اين خط الزامي نيست)
  - **Infinit** ← زمان نامعلوم است
  - **End-time** ←راس ساعتي كه تمام مي شود.
  - **Duration** ← بازه ي زماني تعريف مي شود.

### 2- مكانيزم ارسال كليد:

استفاده از كليدهاي دريافت شده براي ارسال در شبكه.

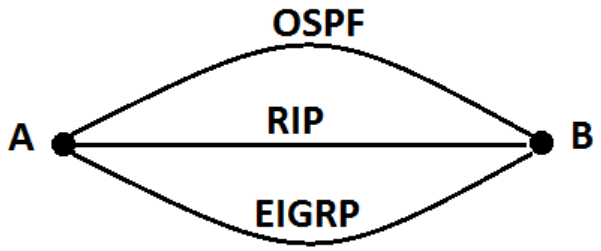
```
1  Router(Config-if)#ip authentication mode eigrp autonomous-system md5
2  Router(Config-if)# ip authentication key chain eigrp autonomous-system name-of-chain
```

```
Keychain test
        Ley-id 1
                Ley-string 123
                        Accept-lifetime 04:00:00 Jan 12006 infinites
```

جهت پياده سازي EIGRP Authentication بايد از نرم افزار Gns3.net استفاده شود.

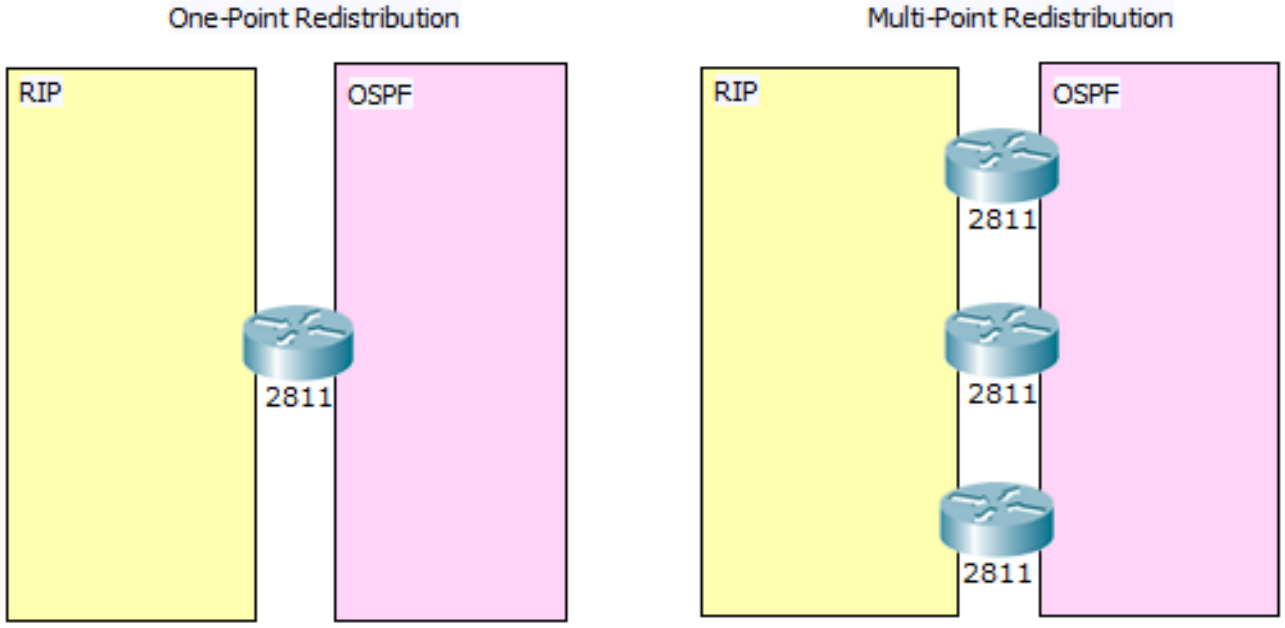
## Redistribution

اگر از نقطه A به B از چند مسير با پروتكلهاي مختلف قابل دسترس بود از طريق اين جدول مسيري انتخاب مي شود كه كمتر باشد.




| | |
|---|---|
| Rip | 120 |
| OSPF | 110 |
| EIGRP | 90 |

هر چقدر عدد كوچكتر باشد↓، اولويت بيشتر است↑.




**1- Rip**

| | |
|---|---|
| 1 | Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value]** |

| | |
|---|---|
| 1 | Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value] [subnets]** |

- **Example**

| | |
|---|---|
| 1 | Router(config)#**router rip** |
| 2 | Router(config-router)#**redistribute ospf 1 metric 3** |

**2- OSPF**

| | |
|---|---|
| 1 | Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value] [subnets]** |

- **Example**

| | |
|---|---|
| 1 | Router(config)#**router ospf 1** |
| 2 | Router(config-router)#**redistribute eigrp 100 subnets metric 10** |

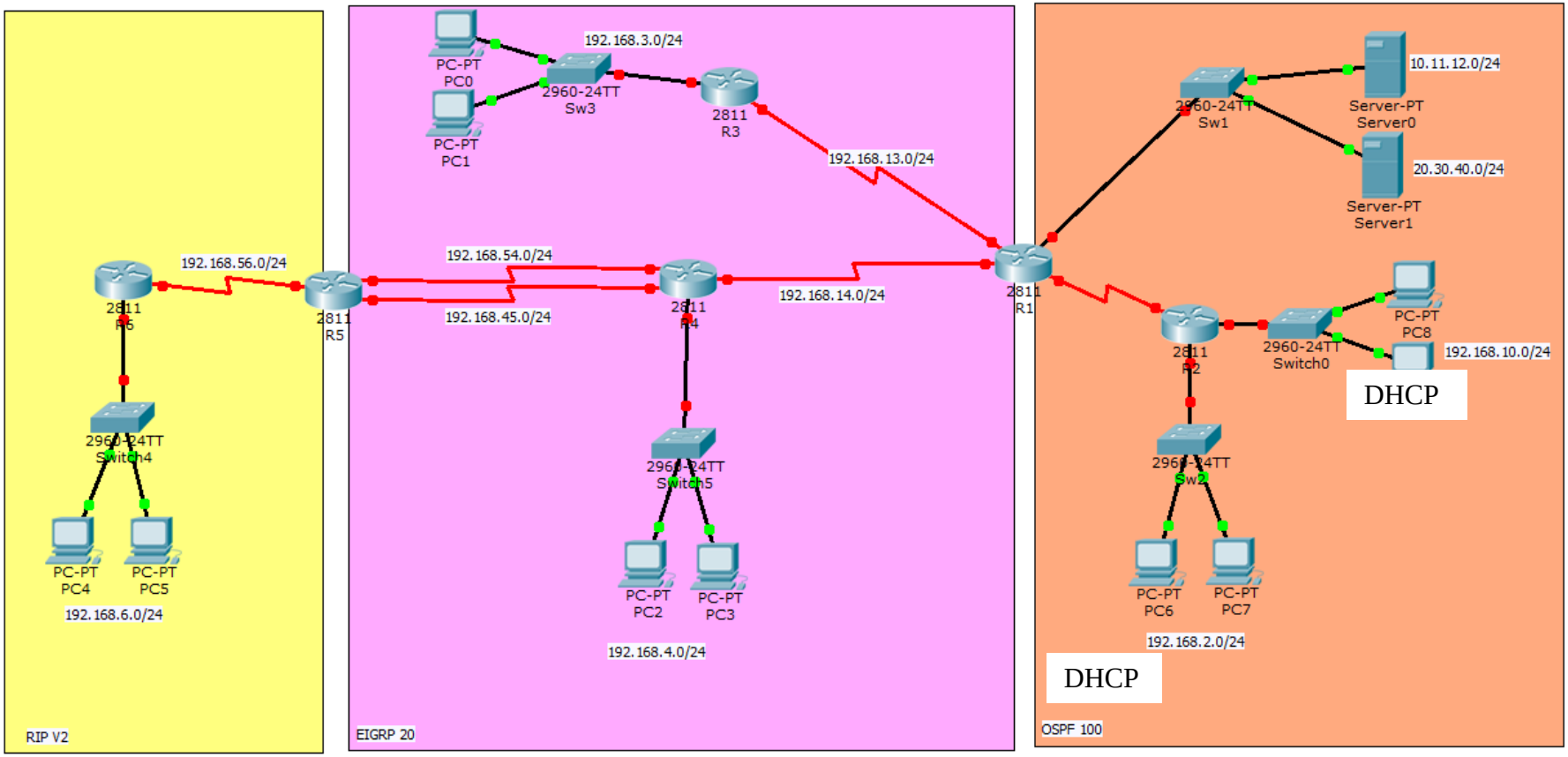
**3- EIGRP**

| | |
|---|---|
| 1 | Router(Config-router)# **redistribiution Protocol [process-id] [Metric metric-value]** |

- **Example**

| | |
|---|---|
| 1 | Router(config)#**router eigrp 100** |
| 2 | Router(config-router)#**redistribute ospf 1 metric 10000 100 255 1 1500** |

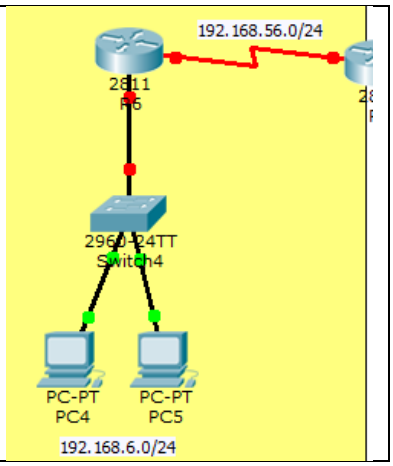
# جلسه 16 : سناریو (IP-DHCP-RIP-EIGRP-OSPF-Redistribution)



## 1- اختصاص IP به Interface هاي روترها

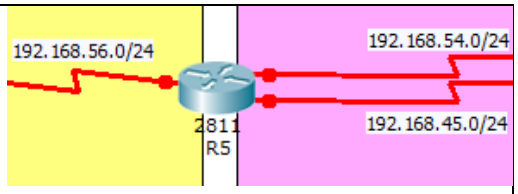
**R6**

| | |
|---|---|
| 1 | Router>**en** |
| 2 | Router#**conf t** |
| 3 | Router(config)#**interface fastEthernet 0/0** |
| 4 | Router(config-if)#**ip address 192.168.6.1 255.255.255.0** |
| 5 | Router(config-if)#**no sh** |
| 6 | |
| 7 | Router(config)#**interface serial 0/0/0** |
| 8 | Router(config-if)#**ip address 192.168.56.2 255.255.255.0** |
| 9 | Router(config-if)#**no sh** |
| 10 | |



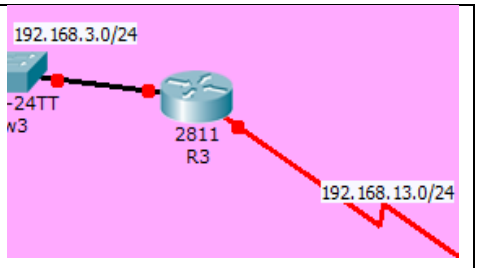

**R5**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/2/0** |
| 2 | Router(config-if)#**ip address 192.168.56.1 255.255.255.0** |
| 3 | Router(config-if)#**clock rate 64000** |
| 4 | Router(config-if)#**no sh** |
| 5 | |
| 6 | Router(config)#**interface serial 0/0/0** |
| 7 | Router(config-if)#**ip address 192.168.54.1 255.255.255.0** |
| 8 | Router(config-if)#**clock rate 64000** |
| 9 | Router(config-if)#**no sh** |
| 10 | |
| 11 | Router(config)#**interface serial 0/0/1** |
| 12 | Router(config-if)#**ip address 192.168.45.1 255.255.255.0** |
| 13 | Router(config-if)#**clock rate 64000** |
| 14 | Router(config-if)#**no sh** |



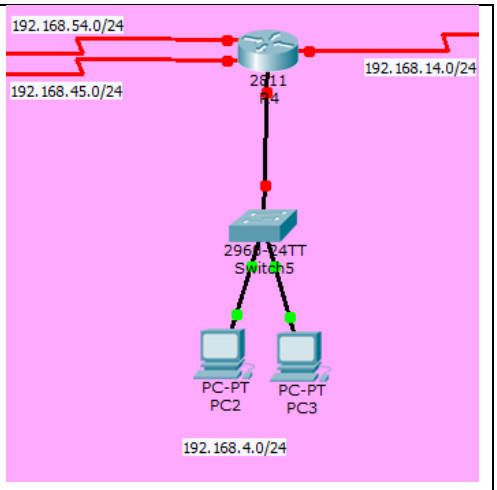

**R3**

| | |
|---|---|
| | Router(config)#**interface fastEthernet 0/0** |
| 2 | Router(config-if)#**ip address 192.168.3.1 255.255.255.0** |
| 3 | Router(config-if)#**no sh** |
| 4 | |
| 5 | Router(config)#**interface serial 0/0/0** |
| 6 | Router(config-if)#**ip address 192.168.13.1 255.255.255.0** |
| 7 | Router(config-if)#**clock rate 64000** |
| 8 | Router(config-if)#**no sh** |



**R4**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**ip address 192.168.54.2 255.255.255.0** |
| 3 | Router(config-if)#**no sh** |
| 4 | |
| 5 | Router(config)#**interface serial 0/0/1** |
| 6 | Router(config-if)#**ip address 192.168.45.2 255.255.255.0** |
| 7 | Router(config-if)#**no sh** |
| 8 | |
| 9 | Router(config)#**interface serial 0/2/0** |
| 10 | Router(config-if)#**ip address 192.168.14.1 255.255.255.0** |
| 11 | Router(config-if)#**clock rate 64000** |
| 12 | Router(config-if)#**no sh** |
| 13 | |
| 14 | Router(config)#**interface fastEthernet 0/0** |
| 15 | Router(config-if)#**ip address 192.168.4.1 255.255.255.0** |
| 16 | Router(config-if)#**no sh** |



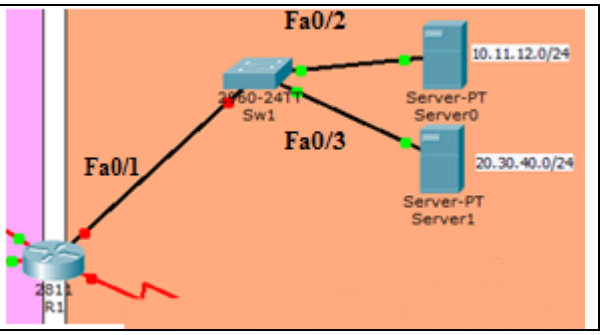

**R1:**

| | |
|---|---|
| 1 | Router(config)#**interface ser** |
| 2 | Router(config)#**interface serial 0/0/0** |
| 3 | Router(config-if)#**ip address 192.168.14.2 255.255.255.0** |
| 4 | Router(config-if)#**no sh** |
| 5 | |
| 6 | Router(config)#**interface serial 0/2/0** |
| 7 | Router(config-if)#**ip address 192.168.13.2 255.255.255.0** |
| 8 | Router(config-if)#**no sh** |
| 9 | |
| 10 | Router(config)#**interface serial 0/0/1** |
| 11 | Router(config-if)#**ip address 192.168.12.1 255.255.255.0** |
| 12 | Router(config-if)#**clock rate 64000** |
| 13 | Router(config-if)#**no sh** |

**2- حال براي ادامه ي كار و تعريف دو رنج IP مختلف روي سويچ بايد روي سويچ دو Vlan بسازيم:**

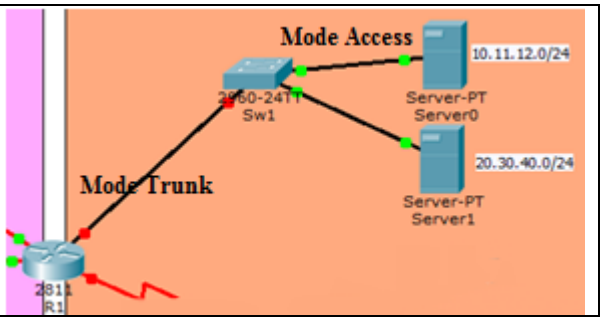
**Sw1**

| | |
|---|---|
| 1 | Switch>**en** |
| 2 | Switch#**conf t** |
| 3 | Switch(config)#**vlan 10** |
| 4 | Switch(config-vlan)#**vlan 20** |
| 5 | |
| 6 | Switch(config)# **interface fastEthernet 0/2** |
| 7 | Switch(config-if)#**switchport mode access** |
| 8 | Switch(config-if)#**switchport access vlan 10** |




- خط 3و 4: تعريف Vlan
- خط 6: قرار دادن interface fastEthernet 0/2 در VLAN10

**Sw1**

| | | |
|---|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/3** |  |
| 2 | Switch(config-if)#**switchport mode access** | |
| 3 | Switch(config-if)#**switchport access vlan 20** | |
| 4 | | |
| 5 | Switch(config)#**interface fastEthernet 0/1** | |
| 6 | Switch(config-if)#**switchport mode trunk** | |



- خط 1 –3: قرار دادن interface fastEthernet 0/3 در VLAN20
- خط 5–6: حال بايد در سويیچ، پورتي كه به روتر متصل شده است را Trunk تعريف كنيم:

سپس بايد به پورتهاي مورد نظر IP اختصاص دهيم:

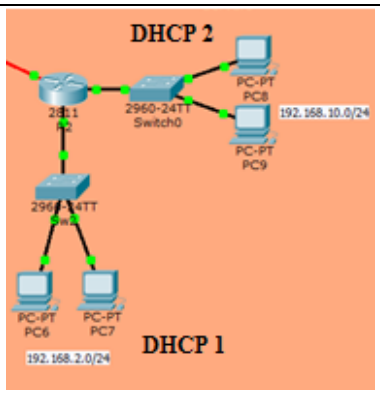
**R1:**

| | |
|---|---|
| 1 | Router(config)#**interface fastEthernet 0/0.1** |
| 2 | Router(config-subif)#**encapsulation dot1Q 10** |
| 3 | Router(config-subif)#**ip address 10.11.12.1 255.255.255.0** |
| 4 | |
| 5 | Router(config)#**interface fastEthernet 0/0.2** |
| 6 | Router(config-subif)#**encapsulation dot1Q 20** |
| 7 | Router(config-subif)#**ip address 20.30.40.1 255.255.255.0** |
| 8 | ~~Router(config-subif)#no sh~~ |
| 9 | |
| 10 | Router(config)#**interface fastEthernet 0/0** |
| 11 | Router(config-if)#**no sh** |
| 12 | Router(config-if)# |
| 13 | %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up |
| 14 | %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up |
| 15 | %LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up |
| 16 | %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up |
| 17 | %LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up |
| 18 | %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up |

- خط 1 –3: اختصاص IP به پورت مجازي كه به سرور اولي متصل شده است.
- خط 5–8: اختصاص IP به پورت مجازي كه به سرور دوم متصل شده است.
- خط 10: توجه: براي فعال كردن پورت حتما بايد كامند no sh را بر روي پورت اصلي بزنيم.

**R2**

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 192.168.12.2  255.255.255.0
3  Router(config-if)#no sh
4
5  Router(config-if)#inter fa0/1
6  Router(config-if)#ip address 192.168.10.1 255.255.255.0
7  Router(config-if)#no sh
8
9  Router(config)#ip dhcp pool test
10 Router(dhcp-config)#network 192.168.2.2 255.255.255.0
11 Router(dhcp-config)#default-router 192.168.2.1
12
13 Router(config)#interface fastEthernet 0/1
14 Router(config-if)#ip address 192.168.10.1 255.255.255.0
15 Router(config-if)#no sh
16
17 Router(config)#ip dhcp pool test2
18 Router(dhcp-config)#network 192.168.10.2 255.255.255.0
19 Router(dhcp-config)#default-router 192.168.10.1
20
```




- خط 9: راه اندازي DHCP 1.
- راه اندازي DHCP 2

## 3- راه اندازي پروتكلهاي مسير يابي بر روي روترها

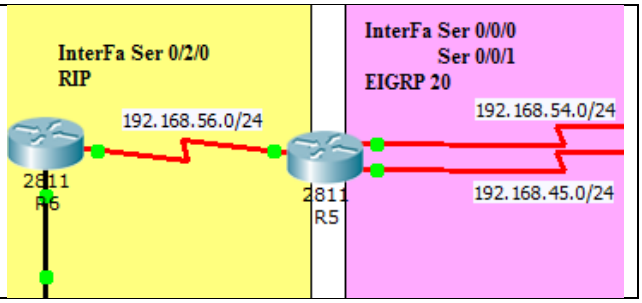
**R6:**

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.6.0
4  Router(config-router)#network 192.168.56.0
```

روتر R5 يك پورت آن در بخش پروتكل RIP قرار دارد و دو پورت ديگر آن در پروتكل EIGRP كه بايد به صورت زير تعريف شود:

**R5:**

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.56.0
4
5  Router(config)#router eigrp 20
6  Router(config-router)#network 192.168.54.0
7  Router(config-router)#network 192.168.45.0
```




- خط 1و2و3: يك Interface روتر R5 داخل Rip است.
- خط 5و6و7: دو Interface ديگر آن در EIGRP است.

**R4:**

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.54.0
```

| | |
|---|---|
| 3 | Router(config-router)#**network 192.168.45.0** |
| 4 | Router(config-router)#**network 192.168.4.0** |
| 5 | Router(config-router)#**network 192.168.14.0** |

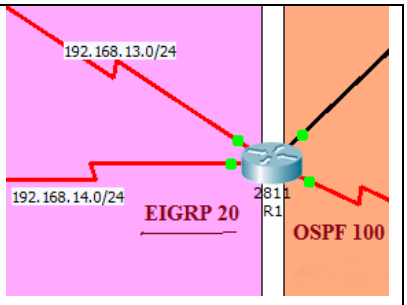
**R3**

| | |
|---|---|
| 1 | Router(config)#**router eigrp 20** |
| 2 | Router(config-router)#**network 192.168.13.0** |
| 3 | Router(config-router)#**network 192.168.3.0** |

روتر 1 نيز مانند روتر 5، در مرز دو پروتكل مسير يابي قرار دارد كه بصورت زير كانفيگ مي گردد:

**R3:**

| | |
|---|---|
| 1 | Router(config)#**router eigrp 20** |
| 2 | Router(config-router)#**network 192.168.13.0** |
| 3 | Router(config-router)#**network 192.168.14.0** |
| 4 | |
| 5 | Router(config)#**router ospf 1** |
| 6 | Router(config-router)#**network 192.168.12.1 0.0.0.0 area 100** |
| 7 | Router(config-router)#**network 10.11.12.0 0.0.0.255 area 100** |
| 8 | Router(config-router)#**network 20.30.40.0 0.0.0.255 area 100** |




**R2:**

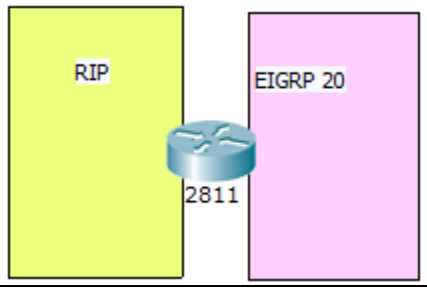
| | |
|---|---|
| 1 | Router(config)#**router ospf 1** |
| 2 | Router(config-router)#**network 192.168.12.2 0.0.0.0 area 100** |
| 3 | Router(config-router)#**network 192.168.2.1 0.0.0.0 area 100** |
| 4 | Router(config-router)#**network 192.168.10.1 0.0.0.0 area 100** |

**4- Config** روترهاي مرزي كه بين دو پروتكل مسير يابي مختلف قرار دارند: **Redistribution**

**حالت اول: Redistribution روتر بين پروتكلهاى مسير يابي RIPو EIGRP:**

**R5:**

```
1  Router(config)#router rip
2  Router(config-router)#redistribute eigrp 20 metric 1
3
4  Router(config)#router eigrp 20
5  Router(config-router)#redistribute rip metric 1 1 1 1 1
```

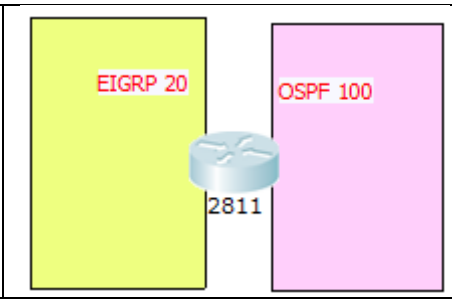



- خط 1و 2: راه اندازي پروتكلهاي redistribute داخل پروتكل RIP
- خط 4و5: راه اندازي پروتكلهاي redistribute داخل پروتكل EIGRP

**حالت دوم: Redistribution روتر بين پروتكلهاى مسير يابي EIGRPو OSPF**

**R1:**

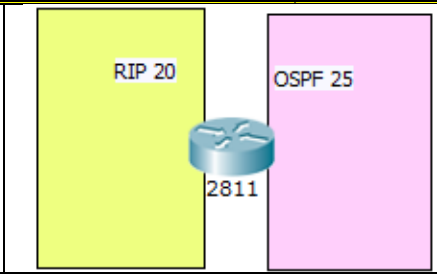
```
1  Router(config)#router eigrp 20
2  Router(config-router)#redistribute ospf 1 metric 1 1 1 1 1
3
4  Router(config)#router ospf 1
5  Router(config-router)#redistribute eigrp 20 metric 1 subnets
```




- خط 1و2: راه اندازي پروتكل redistribute داخل پروتكل EIGRP.
- خط 4و5: راه اندازي پروتكل redistribute داخل پروتكل OSPF.

**حالت سوم: Redistribution روتر بين پروتكلهاي مسير يابي RIPو OSPF:**

```
1  Router(config)#router rip
2  Router(config-router)#redistribute ospf 1 metric 1
3
4  Router(config)#router ospf 1
5  Router(config-router)#redistribute rip metric 1 subnets
```



## Access Control List :

1- Classification : طبقه بندی ترافیک های مختلف شبکه است.
2- Filtering : بعد از اینکه یک ترافیک شناخته می شود از این پس می توان فیلتر را پیاده سازی کرد(چه فیلتر خوب چه فیلتر بد) با کنترل سطح دسترسی سروکار داریم.
یک سری ترافیک Select می کنیم بر حسب نیاز فیلتر می کنیم.

## انواع Access List : (ACL)

**1- استاندارد Standard ACL**

فیلترینگ را به ازای سورس شبکه انجام می دهند. از همان منبع ترافیک را فیلتر می کند. با گسترش شبکه دیگر این راه سخت بوده و در این صورت بتوان بر اساس مبدا (Source) و هم مقصد (Destination) فیلتر کرد.

**2- Extended ACL**

فیلتر بر مبنای منفع و مقصد را گویند. Sourceو Distination.

**طریقه ی نگارش ACL :**

**1- شماره ی ACL (ACL Number)**

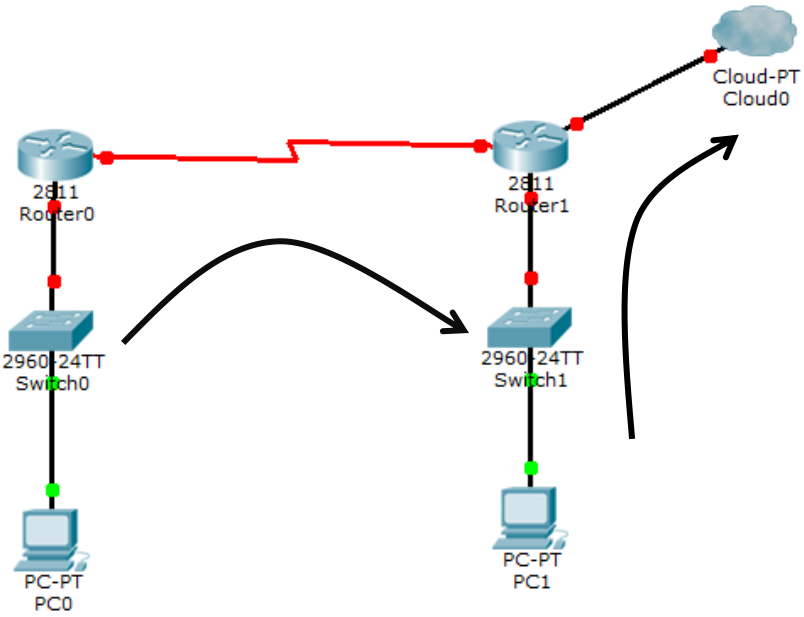
$$ACL\ Number: \begin{cases} 1-99 \\ 1300-1999 \\ 100-199 \\ 200-2699 \end{cases}$$

**2- اسم ACL (ACL Name)**

$ACL\ Name$: نام مورد نظر

## نکات مهم پیاده سازی ACL:

**1- به ازای هر Interface هر پروتکل و هر جهت ارتباطی در شبکه فقط یک ACL قابلیت پیاده سازی دارد.**




a. PC0 به PC1 دسترسی نداشته باشد.
b. PC1 به اینترنت دستری نداشته باشد.

منظور از جهت ← Source به Destination است.
چون مبدا به مقصد این دو تفاوت دارند، باید دو ACL بنویسیم.

| | Source | | Destination |
|---|---|---|---|
| **1.** | PC0 | ↛ | PC1 |
| **2.** | PC1 | ↛ | Internet |

---

**2- در نوشتن ACL ها اولیت بندی حایز اهمیت می باشد، بدین جهت ACL هائیکه در ابتدا نوشته شوند، در ابتدا نیز اجرا می گردد.**

اگر چند خط دستور باشد ← ابتدا خط های اول را اجرا می کند.
اولویت خط 1 بالاتر از خطوط پایینتر است.

ACL 20

---

**3- مکانیزم عملکرد ACL ها بصورت Implicit Deny All می باشد. بدین جهت دسترسی های مورد نیاز باید در قالب Permit در ابتدا معرفی شود.**

که دو حالت دارد:
- Permit
- Deny

**- مبنا را بر اساس deny قرار می دهیم.**

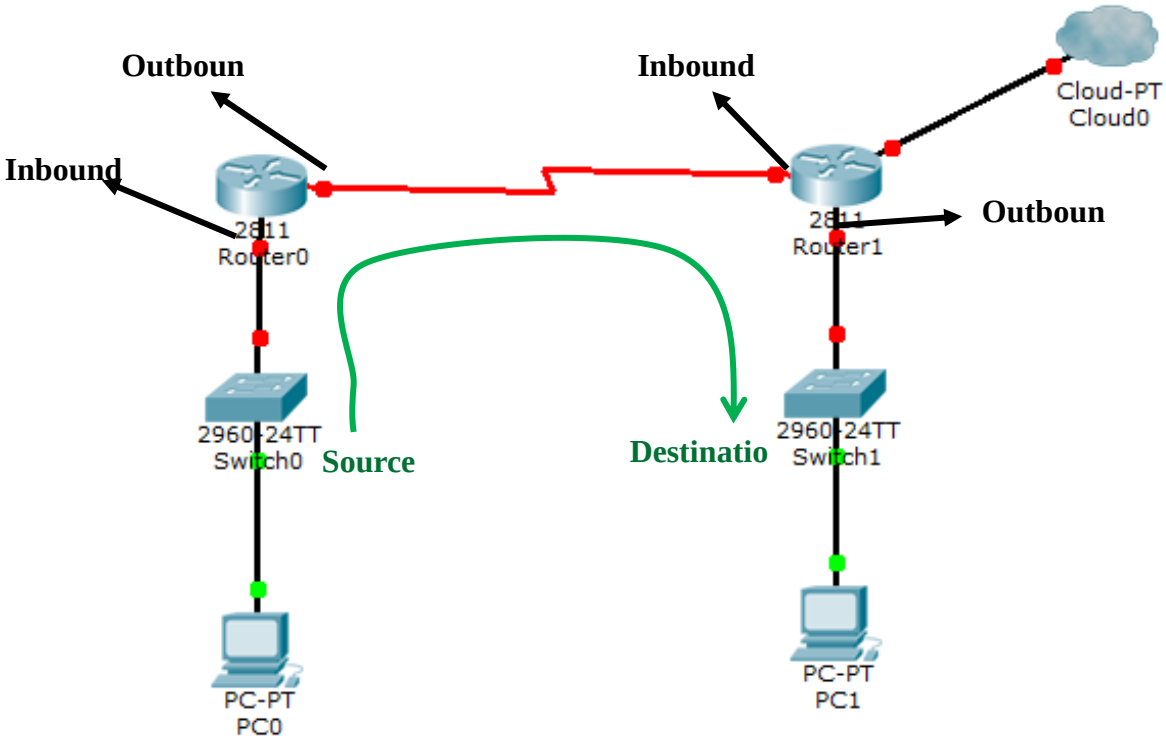
ACL 20

- Permit
- Permt
- Deny all

- سپس آنهائیکه می خواهیم باز باشد را، باز می کنیم. (هر چیزی که نیاز داریم را باز می کنیم).

---

**4- نوشتن ACL ها در مد Config انجام شده، اما اعمال آنها به Interfaceهای روتر در حالت Inbound و یا Outbound قابل اجراست.**



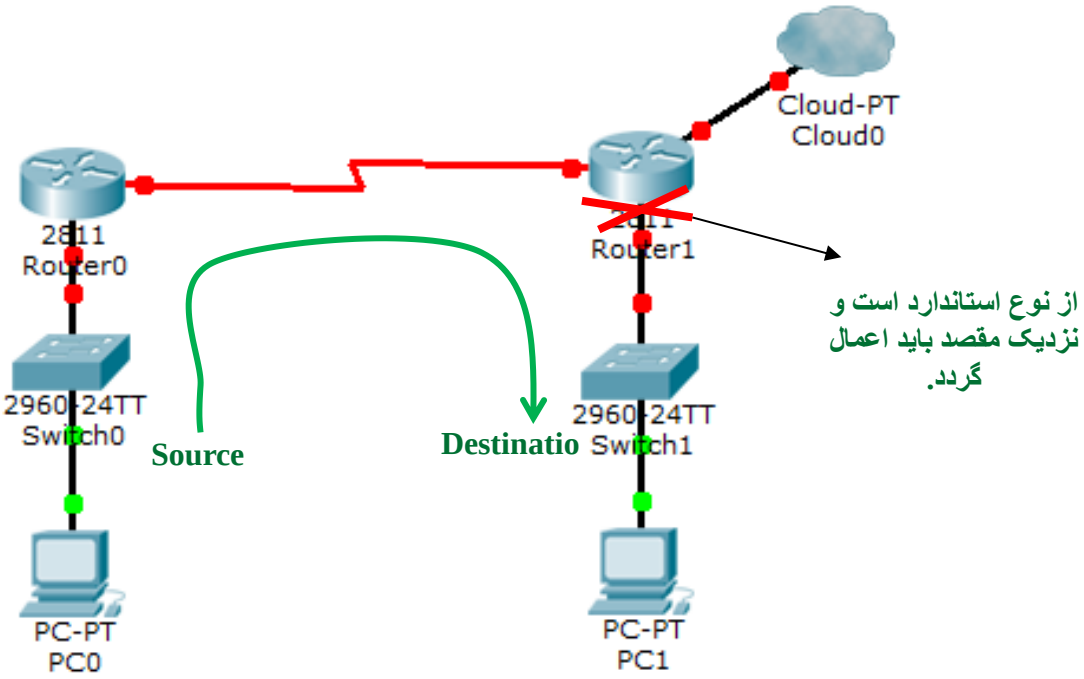

**از مبدا به مقصد حرکت می کنیم و هر Interface که در جهت حرکت ما به روتر وارد شود Inbound است و هر کدام که از روتر خارج گردد Outbound می شود.**

---

**5- برای اِعمال ACL ها در صورتیکه از نوع Extended باشند، آنها را نزدیک به مبدا و در صورتیکه از نوع Standard باشند نزدیک به مقصد اعمال می کنیم.**

- **اگر Standard باشد** ← نزدیک به مقصد چون **مبدا** را نمی توانیم تعیین کنیم.
- **اگر Extended باشد** ← نزدیک مبدا باید تعریف شود.

چون در استاندارد می دانیم که پکت نباید به کجا برسد ← نزدیک مقصد فیلتر می شود از آن مبداعی که آمد نباید به مقصد برسد. زمانیکه چیزی از مبدا مورد نظر ما رسید نباید رد شود .


Cloud-PT
Cloud0
2811
Router0
Router1
از نوع استاندارد است و
نزدیک مقصد باید اعمال
گردد.
2960-24TT
Switch0
Source
Destinatio
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1

## اکسس لیست بر اساس شماره :

### 1- Standard ACL :

تعریف ACL هائیکه با شماره نوشته می شوند :

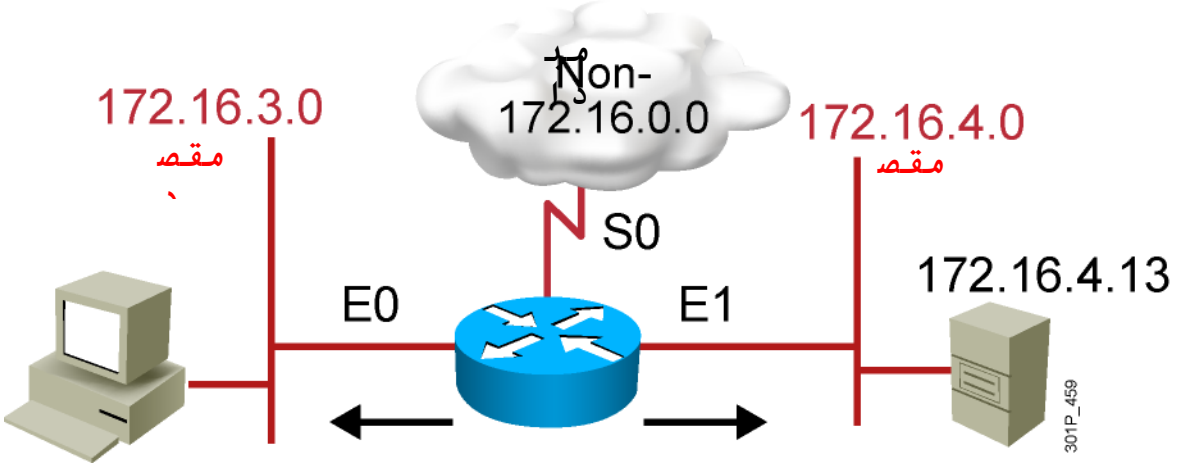
```
1  RouterX(config)# access-list access-list-number {permit | deny | remark} source [mask]
2  RouterX(config-if)# ip access-group access-list-number {in | out}
```

منظور از In همان Inbound و Out همان Outbound می باشد.

---

**مثال: در مثال زیر، امکان دسترسی کاربران از رنج IP:172.16.0.0 نسبت به شبکه مقدور گردیده است.**

- اولویت بندی: کسانیکه IP: 172.16.0.0 دارند ← Permit ( با Wildcard کار می کند)
- بر اساس منطق Firewall ← چیزی برای کسی دیده نشود. ابتدا Permit را اجرا می کند سپس همه را بصورت خودکار می بندد. (Implicit Deny All)



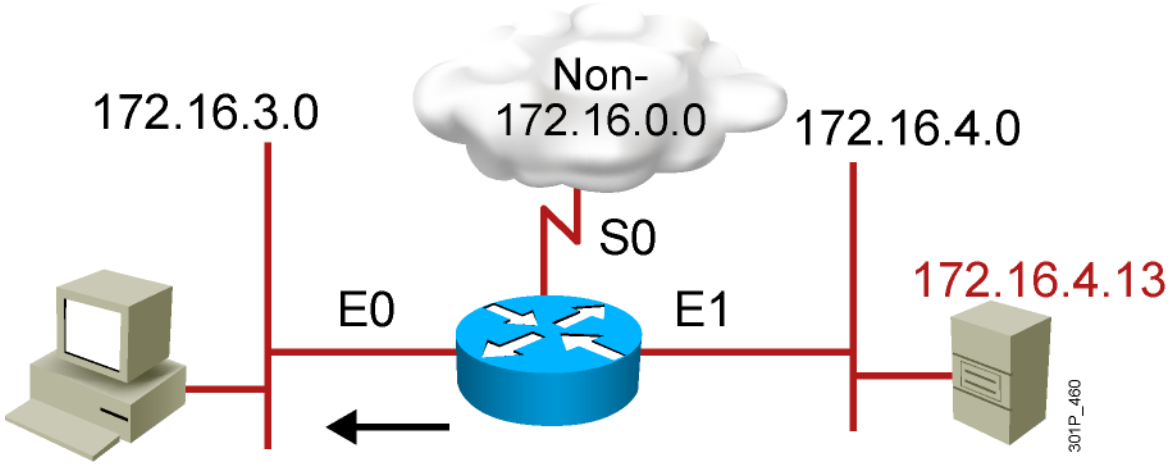

جهت حرکت از سمت ابر (172.16.0.0) به سمت شبکه های 172.16.4.0و 172.16.3.0 می باشد.

```
1  RouterX(config)# access-list 1 permit 172.16.0.0  0.0.255.255
2  (implicit deny all - not visible in the list)
3  (access-list 1 deny 0.0.0.0   255.255.255.255)
4
5  RouterX(config)# interface ethernet 0
6  RouterX(config-if)# ip access-group 1 out
7
8  RouterX(config)# interface ethernet 1
   RouterX(config-if)# ip access-group 1 out
```

خط 2و 3 نوشته نمی شود اما به صورت خودکار اجرا می شود. یعنی زمانیکه ما به 172.16.0.0 دسترسی دادیم به صورت خودکار این دسترسی برای بقیه بسته می شود و به غیر از 172.16.0.0 به بقیه اجازه ی عبور نمی دهد. (Deny All)

---

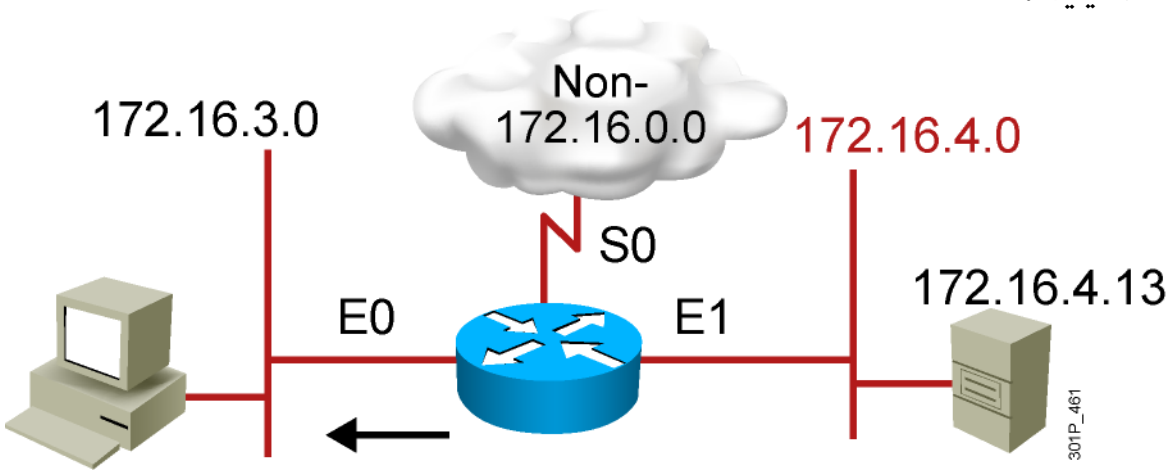
**مثال 2: کاربران شبکه 172.16.3.0 به سرور 172.16.4.13 دسترسی نداشته باشند.**




| | |
|---|---|
| 1 | RouterX(config)# **access-list 1 deny 172.16.4.13 0.0.0.0** |
| 2 | RouterX(config)# **access-list 1 permit 0.0.0.0  255.255.255.255** |
| 3 | **(implicit deny all)** |
| 4 | **(access-list 1 deny 0.0.0.0  255.255.255.255)** |
| 5 | |
| 6 | RouterX(config)# **interface ethernet 0** |
| 7 | RouterX(config-if)# **ip access-group 1 out** |

- خط 1: ابتدا دسترسی را می بندیم.
- خط 2: سپس دسترسی را برای بقیه باز می کنیم.

مثال 3: در مثال زیر دسترسی کاربران شبکه172.16.3.0 به سروربا رنج 172.16.4.0 مسدود نمایید.

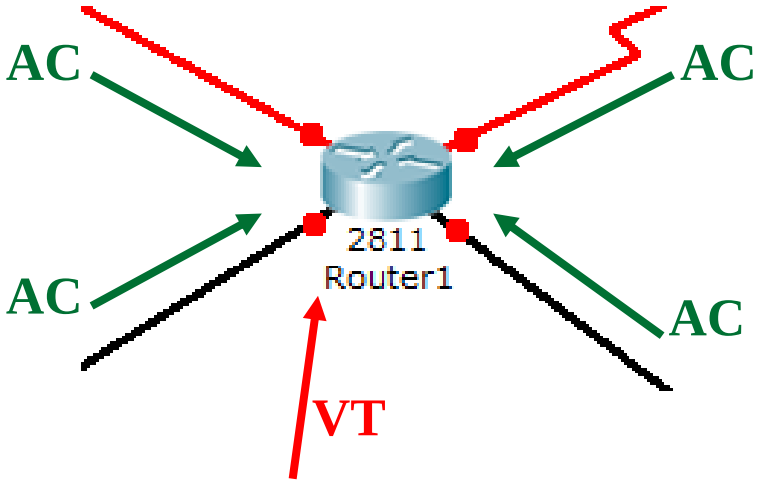



| | |
|---|---|
| 1 | RouterX(config)# **access-list 1 deny 172.16.4.0  0.0.0.255** |
| 2 | RouterX(config)# **access-list 1 permit any** |
| 3 | **(implicit deny all)** |
| 4 | **(access-list 1 deny 0.0.0.0  255.255.255.255)** |
| 5 | |
| 6 | RouterX(config)# **interface ethernet 0** |
| 7 | RouterX(config-if)# **ip access-group 1 out** |

## دسترسی به روتر از راه طریق Telnetو SSH

همان طور که در قبل گفته شده دسترسی به روتر از راه دور به دو صورت Telnet و SSH امکانپذیر می باشد.

برای اینکه نوشتن ACL را برای کسانیکه از راه دور و از طریق هر کدام از Interface های روتر وصل می شوند (باید برای هر جهت یک ACL) تعریف کنیم. ← ACL را باید برای لاین Vty تعریف کنیم.




| | |
|---|---|
| 1 | RouterX(config-line)# **access-class *access-list-number* {in \| out}** |

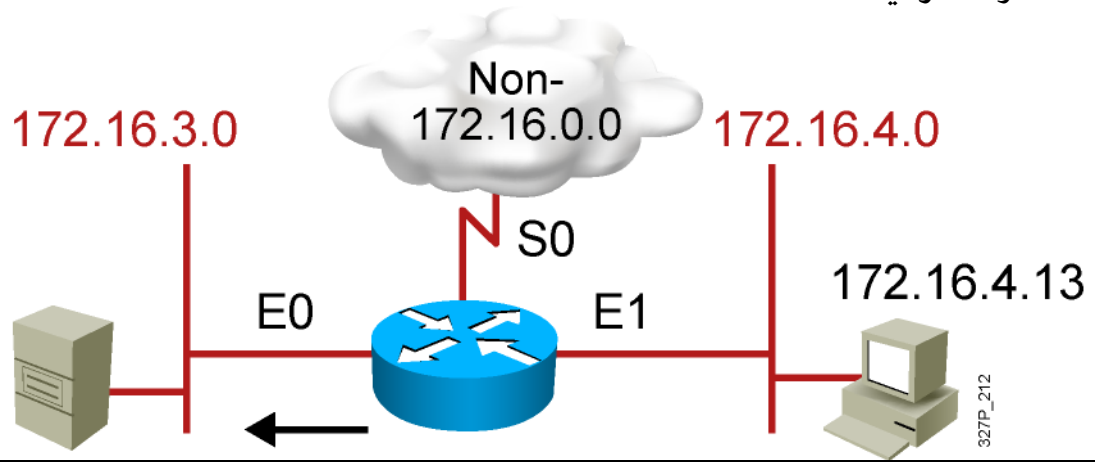
- **Example:**

```
1  access-list 12 permit 192.168.1.0 0.0.0.255
2  (implicit deny any)
3  !
4  line vty 0 4
5   access-class 12 in
```

## Extended ACL -2

```
1  RouterX(config)# access-list access-list-number {permit | deny}
2  protocol source source-wildcard [operator port]
3  destination destination-wildcard [operator port]
4  [established] [log]
5
6  RouterX(config-if)# ip access-group access-list-number {in | out}
```

مثال: در مثال زیر دسترسی کاربران شبکه 172.16.4.0 به سرور FTP در رنج 172.16.3.0 مسدود گردیده است.




```
1  RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
2  RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
3  RouterX(config)# access-list 101 permit ip any any
4  (implicit deny all)
5  (access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
6
7  RouterX(config)# interface ethernet 0
8  RouterX(config-if)# ip access-group 101 out
```

- خط 1و2: دسترسی کاربران با IP:172.16.4.0 (مبدا) ← به سرور FTP با آدرس IP:172.16.3.0 از طریق Interface E0 مسدود شود.
- سپس دسترسی را برای بقیه باز می کند.

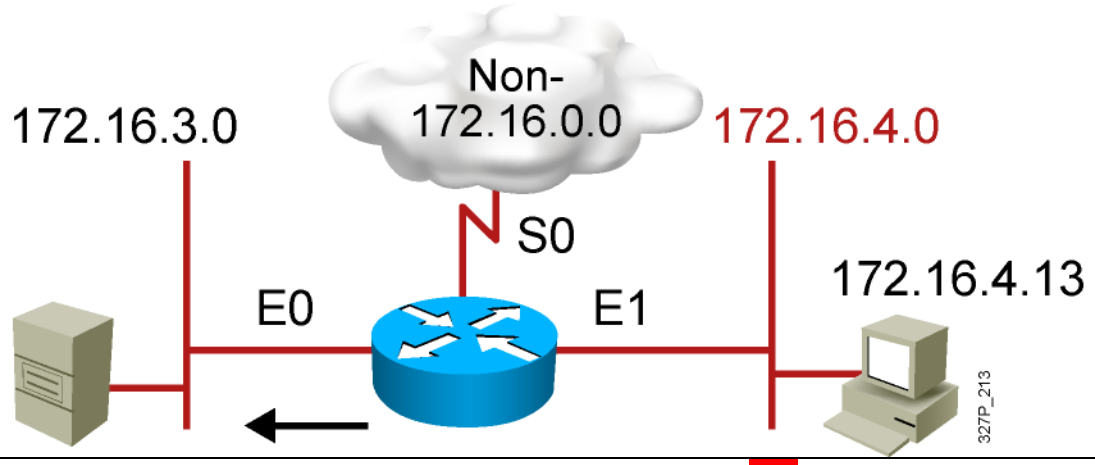
**Ports:**

| | |
|---|---|
| $Web \longrightarrow TCP\ 80$<br>$DNS \longrightarrow TCP\ 53$<br>$Smtp \longrightarrow TCP\ 25$ ارسال میل<br>$Pops \longrightarrow TCP\ 110$ دریافت میل | $Telnet \longrightarrow TCP\ 23$<br>$SSH \longrightarrow TCP\ 22$<br>$FTP \longrightarrow \begin{cases} TCP\ 20 \\ TCP\ 21 \end{cases}$ |

---

مثال 2: در مثال زیر، دسترسی کاربران شبکه به سرور از طریق Telnet مسدود گردیده است.

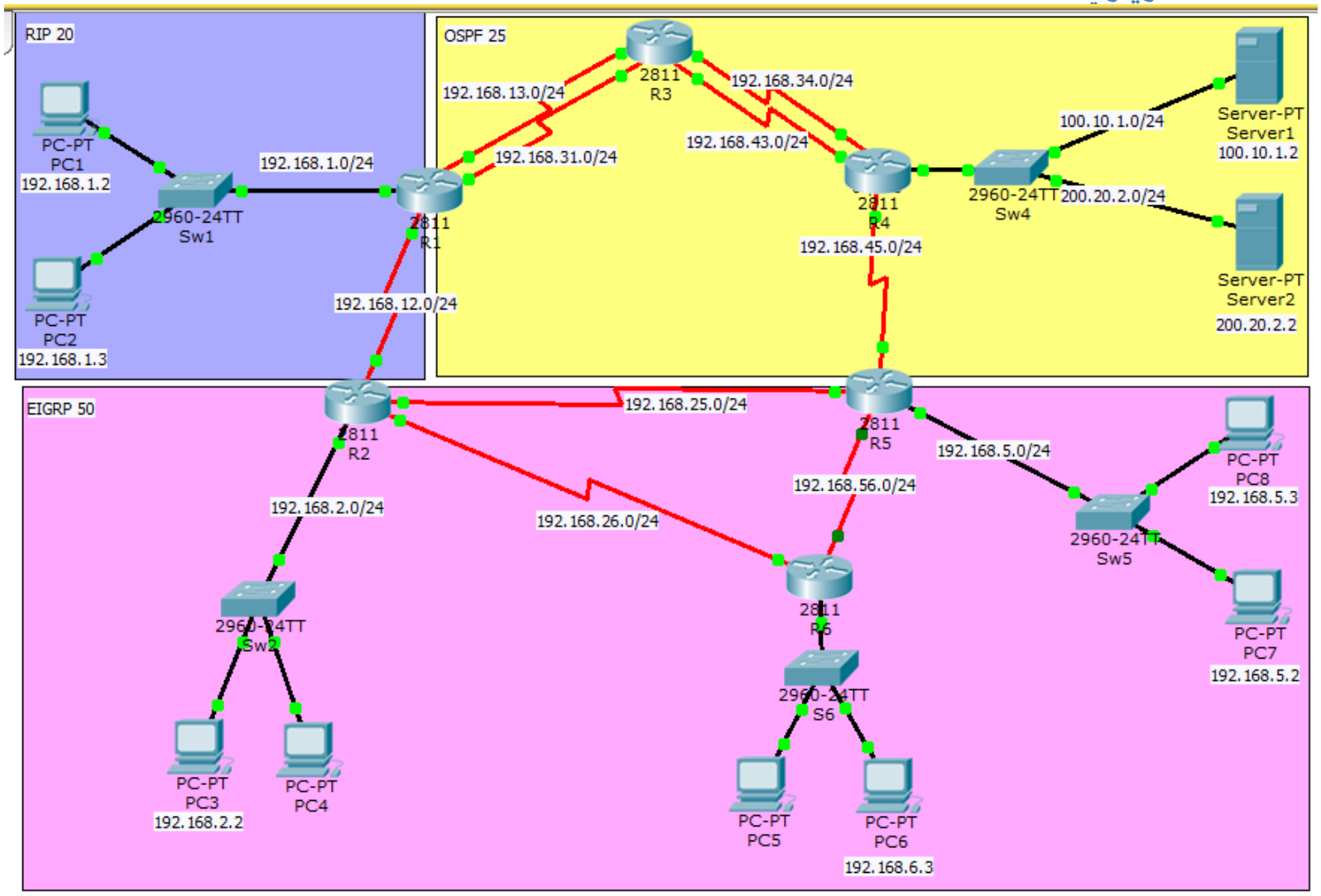
$Telnet \longrightarrow TCP\ 23$




```
1  RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
2  RouterX(config)# access-list 101 permit ip any any
3  (implicit deny all)
4
5  RouterX(config)# interface ethernet 0
6  RouterX(config-if)# ip access-group 101 out
```

- خط 2: به غیر از 172.16.4.0 باقی دسترسی ها به بقیه ی شبکه باز باشد.
- خط 5: فقط روی سرور Telnet نکند.

---


RIP 20
OSPF 25
EIGRP 50
PC-PT PC1
192.168.1.2
2960-24TT Sw1
192.168.1.0/24
2811 R1
PC-PT PC2
192.168.1.3
192.168.13.0/24
192.168.31.0/24
2811 R3
192.168.34.0/24
192.168.43.0/24
2811 R4
192.168.45.0/24
2960-24TT Sw4
100.10.1.0/24
200.20.2.0/24
Server-PT Server1
100.10.1.2
Server-PT Server2
200.20.2.2
192.168.12.0/24
2811 R2
192.168.25.0/24
2811 R5
192.168.5.0/24
192.168.56.0/24
192.168.26.0/24
PC-PT PC8
192.168.5.3
2960-24TT Sw5
PC-PT PC7
192.168.5.2
192.168.2.0/24
2960-24TT Sw2
2811 R6
2960-24TT S6
PC-PT PC3
192.168.2.2
PC-PT PC4
PC-PT PC5
PC-PT PC6
192.168.6.3

**پاسخ سوال 1: دسترسي PC1 نسبت به سرور 1 فقط از طريق وب و نسبت به سرور 2 فقط از طريق پروتكل ICMP مقدور باشد.**

- **بخش اول:** پروتكلها را، فقط از طريق ACL Extended مي توان نوشت ⇐ ACL را بايد در روتر Source ( روتر R1)بنويسيم.

دسترسی PC1 نسبت به سرور 1 فقط از طريق وب(tcp و پورت 80)

| Source | نحوه ي ارتباط | Destination |
|---|---|---|
| PC1→ | Web Browser | → Server 1 |
| 192.168.1.2 | 80 | 100.10.1.2 |

- خط 1: ابتدا فقط دسترسي را براي **مبدا: PC1 (با IP:192.168.1.2)** به **مقصد: Server1 (با IP:100.10.1.2** ) از طريق **TCP** ، باز مي كنيم، كه پورت آن 80 (WWW) است:
- خط 2: سپس بقيه ي دسترسي هاي PC1 به Server1 را مي بنديم.

**بخش دوم :** دسترسي PC1 نسبت به سرور 2 فقط از طريق پروتكل ICMP (Command Prompt) مقدور باشد. (فقط بتواند Ping كند و از طريق مثلا Web browser نتواند باز كند)

| Source | نحوه ي ارتباط | Destination |
|---|---|---|
| PC1→ | Command Prompt | → Server 2 |
| 192.168.1.2 | Permit ICMP | 200.20.2.3 |

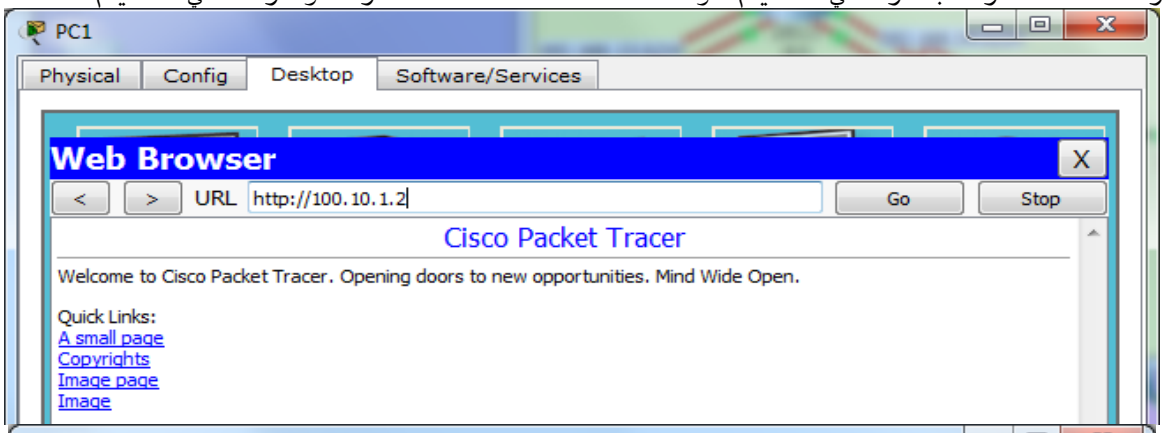
- خط 4: ابتدا دسترسي **ICMP**، را براي **مبدا: PC1 (با IP:192.168.1.2) ، به مقصد: Server2 (با IP:200.20.2.2)** باز مي كنيم:
- خط 5: سپس بقيه ي دسترسي هاي PC1 به Server2 را مي بنديم.
- خط7 : حال دسترسي ها را براي بقيه باز مي كنيم.
- خط 9: سپس اين ACL را در جهت جريان (يعني از سمت مبدا PC1 كه از طريق interface fastEthernet 0/0 روتر R1، به سمت مقصد مي رود) اعمال مي كنيم.
- خط 10: براي اعمال ACL نوشته شده بايد آنرا به Inbound، interface fastEthernet 0/0 روتر R1 اعمال كنيم.

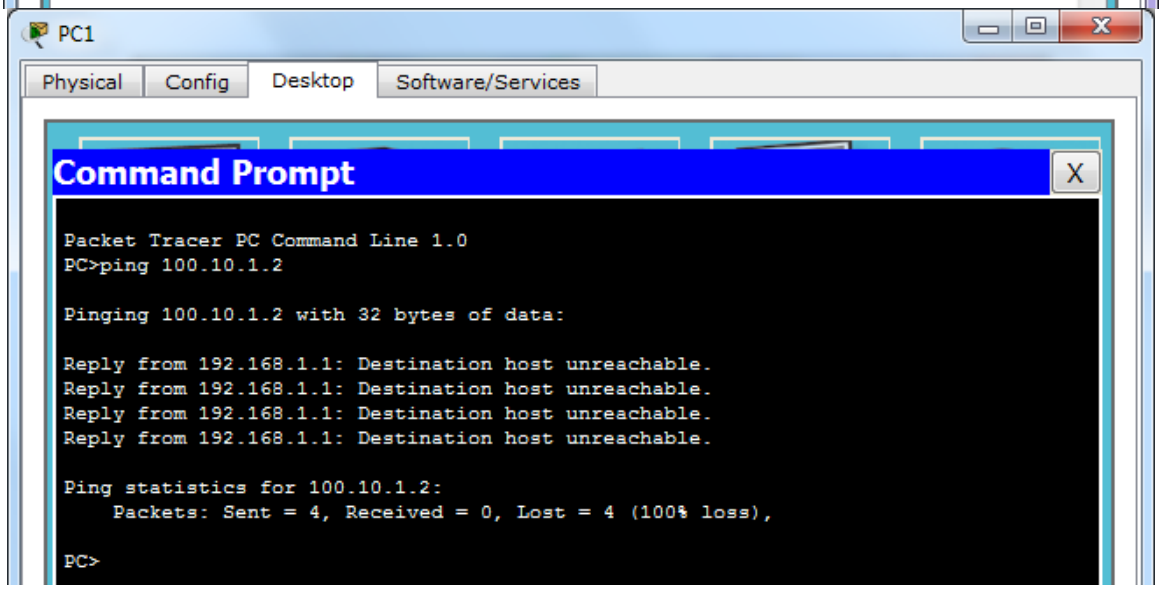
- **كد نوشته شده در روتر R1:**

```
1  R1(config)# access-list 120 permit tcp host 192.168.1.2 host 100.10.1.2 eq 80
2  R1(config)# access-list 120 deny ip host 192.168.1.2 host 100.10.1.2
3
4  R1(config)# access-list 120 permit icmp host 192.168.1.2 host 200.20.2.2
5  R1(config)# access-list 120 deny ip host 192.168.1.2 host 200.20.2.2
6
7  R1(config)# access-list 120 permit ip any any
8
9  R1(config)# interface fastEthernet 0/0
10 R1(config-if)# ip access-group 120 in
```

تست بخش اول:

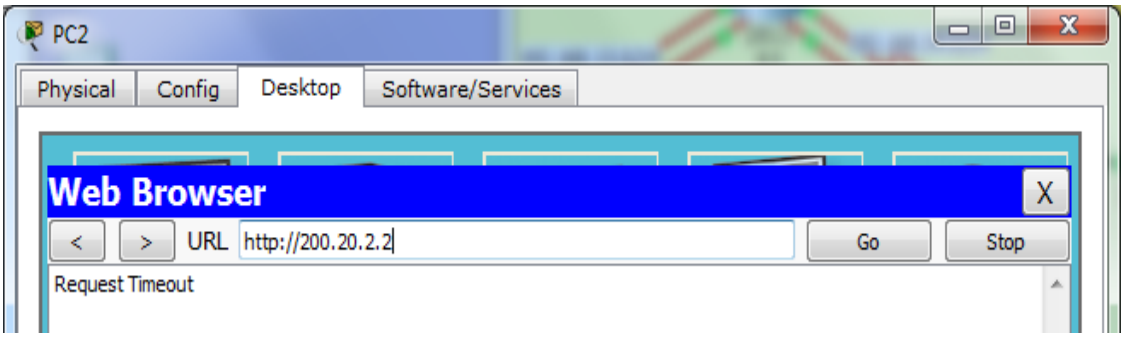
بايد از PC1 به Server1 از طريق Browser دسترسي داشته باشيم، براي اين كار Browser را باز مي كنيم و IPServer1: 100.10.1.2 را وارد مي كنيم:



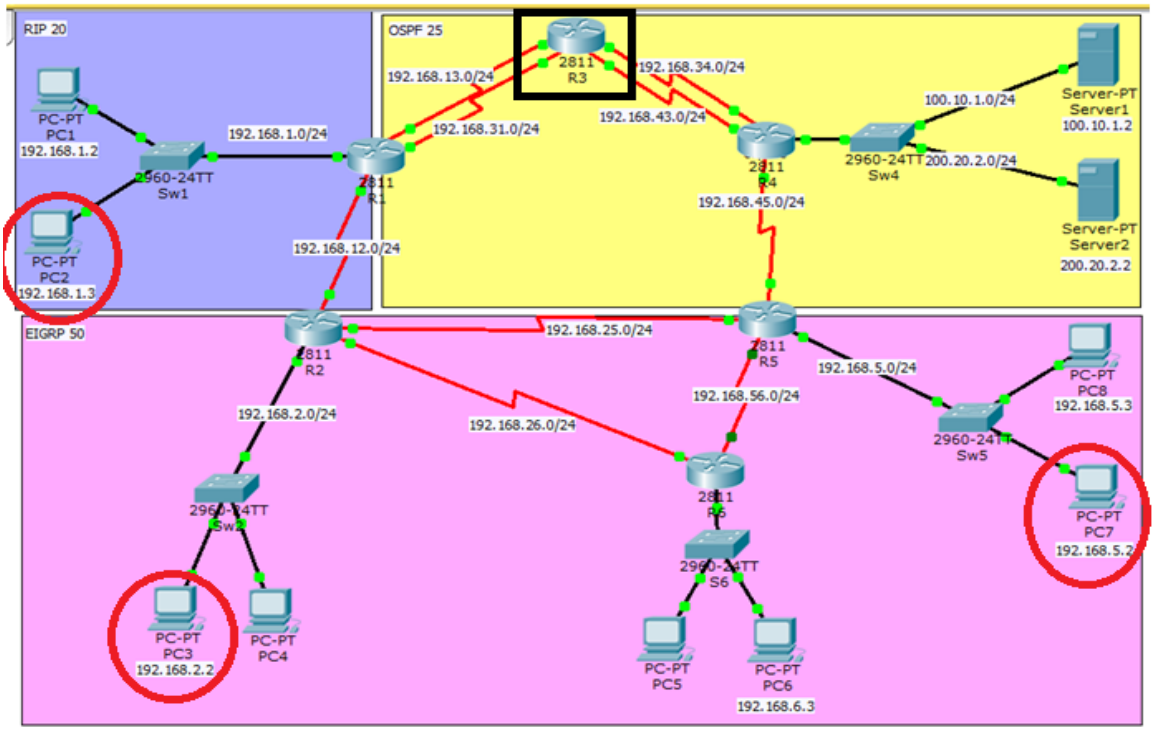

تست بخش دوم:

حال اگر از PC1 بخوهيم Server2 را از طريق Browser باز كنيم. نبايد باز شود:




---

**پاسخ سوال 2: قابليت SSH نسبت به روتر 3 براي PC2، PC3 و PC7 مسدود باشد.**




ابتدا SSH را روي روتر 3 فعال مي كنيم:

| | |
|---|---|
| 1 | R3(config)# **hostname TEST** |
| 2 | TEST(config)# **ip domain-name CISCO.com** |
| 3 | TEST(config)# **crypto key generate rsa** |
| 4 | % You already have RSA keys defined named TEST.CISCO.com . |
| 5 | % Do you really want to replace them? [yes/no]:**1024** |
| 6 | TEST(config)# **ip ssh version 2** |
| 7 | TEST(config)# **username poya password 123** |
| 8 | TEST(config)# **enable secret 12345** |
| 9 | TEST(config-line)# **line vty 0 4** |
| 10 | TEST(config-line)# **login local** |
| 11 | TEST(config-line)# **transport input ssh** |

**توضيح كد:**

- خط 3: كليد امنيتي با الگوريتم رمز نگاري RSA
- خط 4: 1024 را وارد مي كنيم براي اينكه طول كليد امنيتي بالا رود و رمز نگاري آن مشگلتر شود.
- خط 5: براي ساپورت طول كليد بزرگتر، بايد وارد Ver2 شويم.
- خط 6: انتخاب نام براي SSH و پسوورد

PC>**ssh –l poya 192.168.13.2(ip router 3)**

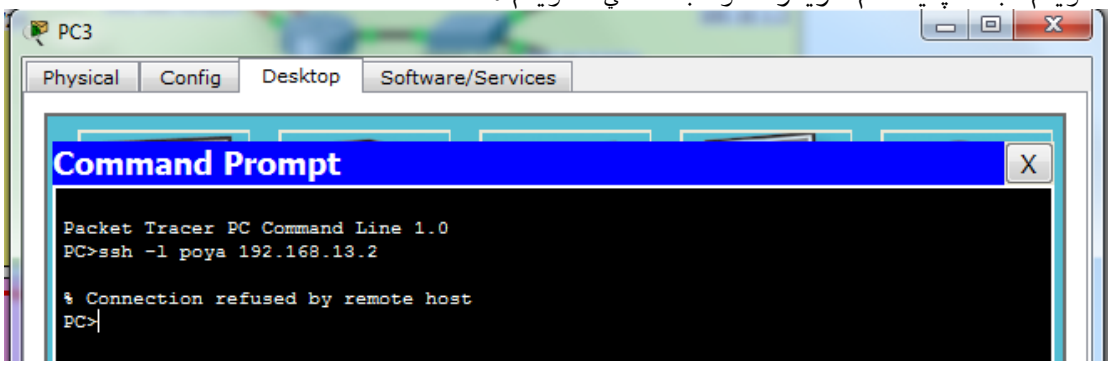
- خط 7: پسورد ورود به مد enable روتر را در اينجا تعريف مي كنيم. (براي زمانيكه كه كسي مي خواهد از طريق ssh به روتر شماره 3 وصل شود و وارد مد enable شود)

حال ACL مورد نظر را مي نويسيم، اين ACL از نوع استاندارد است و بايد آنرا در مقصد (R3) اعمال كنيم:

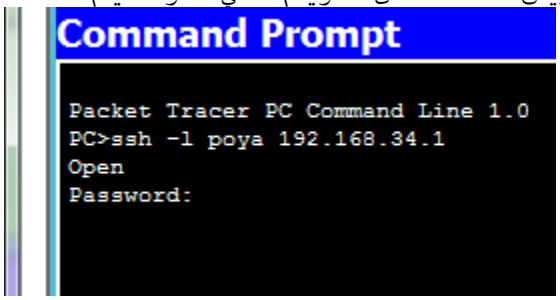
| | |
|---|---|
| 1 | R3(config)#**access-list 20 deny host 192.168.1.3** |
| 2 | R3(config)#**access-list 20 deny host 192.168.2.2** |
| 3 | R3(config)#**access-list 20 deny host 192.168.5.2** |
| 4 | R3(config)#**access-list 20 permit any** |
| 5 | R3(config)#**line vty 0 4** |
| 6 | R3 (config-line)# **access-class 20 in** |

- خط 1و2و3: حال دسترسي ها را براي(PC2(IP: 192.168.1.3 و PC3(IP:192.168.2.2) و PC7(IP:192.168.5.2) مي بنديم.
- خط 4: دسترسي را براي بقيه باز مي كنيم.
- خط 5:
- خط 6: اعمال ACL20 بر روي inbound روتر R3. اجراي دسترسي به دستور Telnet، **access-class مي باشد.**

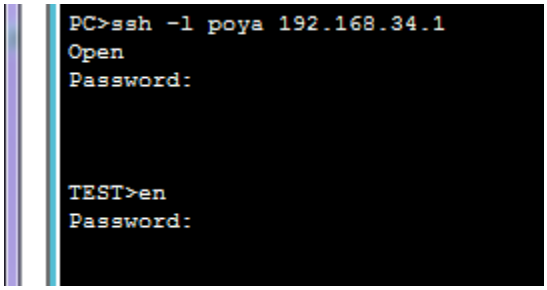
**تست:** حال اگر از سيستم هاي PC3,PC2,PC7 بخواهيم از طريق ssh به روتر R3 وصل شويم با پيغام زير مواجه مي شويم:




و اگر از سيستمهاي ديگر بخواهيم از طريق SSHمتصل شويم مي توانيم.




حال بايد پسورد اول را وارد كنيم: 123



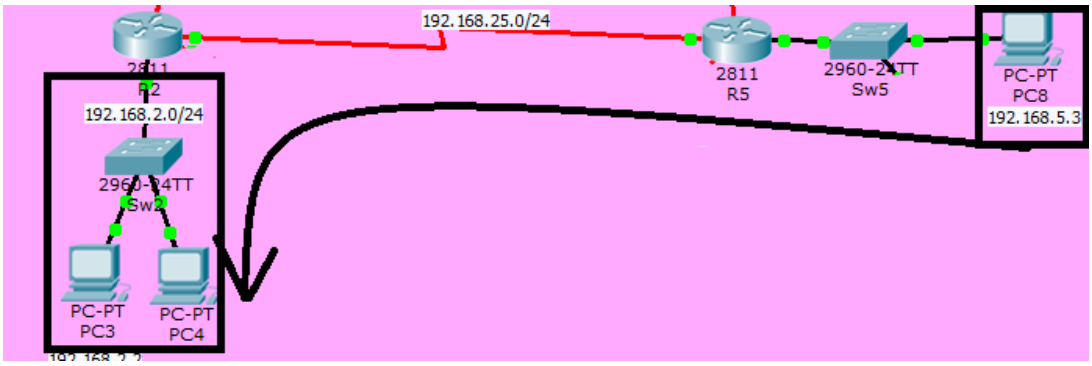

سپس پسورد enable را وارد مي كنيم: 12345

و وارد مد enable روتر مي شويم.

```
PC>ssh -l poya 192.168.34.1
Open
Password:



TEST>en
Password:
Password:
TEST#
```

---

**پاسخ سوال 3: دسترسي PC8 نسبت به كاربران سويچ 2 كلا مسدود باشد.**



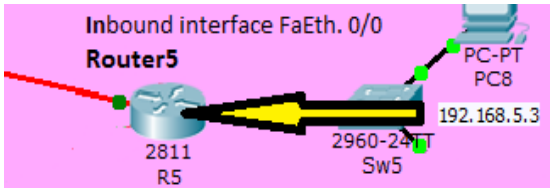

| Source | نحوه ي ارتباط | Destination |
|---|---|---|
| PC8→ | كلا مسدود شود | → Switch 2 |
| 192.168.5.3 | × | 192.168.2.0 |

اين ACL را بصورت Extended مي نويسيم. همانگونه كه در شكل بالا مشاهده مي فرماييد، **مبدا PC8 IP:192.168.5.3** مي باشد و **مقصد شبكه با NET ID:192.168.2.0** و WildCard:0.0.0.255 (چون مقصد Net ID است بايد حتما WildCard را وارد كنيم، اگر مقصد host باشد WildCard ندارد) مي باشد.

- خط 1: ابتدا دسترسي را براي **مبدا: PC8:IP:192.168.5.3** را به **مقصد: شبكه NET ID:192.168.2.0** مي بنديم.
- خط 2: باقي دسترسي ها را باز مي كنيم.
- خط 3و 4: چون مبدا PC8 مي باشد و ACL نوشته شده از نوع Extended است، آنرا بايد در جهت جريان و به ورودي Inbound در interface fastEthernet 0/0 **روتر R5 اعمال كنيم.**

**R5:**

| | |
|---|---|
| 1 | R5(config)#**access-list 150 deny ip host 192.168.5.3 192.168.2.0 0.0.0.255** |
| 2 | R5(config)#**access-list 150 permit ip any any** |
| 3 | R5(config)#**interface fastEthernet 0/0** |
| 4 | R5(config-if)#**ip access-group 150 in** |


Inbound interface FaEth. 0/0
Router5
PC-PT
PC8
192.168.5.3
2811
R5
2960-24TT
Sw5

**پاسخ سوال 4: قابلیت ping از PC6، نسبت به PC2 امکانپذیر نباشد.**

| Source | نحوه ي ارتباط | Destination |
|---|---|---|
| PC8→ | Command Prompt× | → PC2 |
| 192.168.6.3 | Deny ICMP | 192.168.1.3 |

این ACL را نیز از نوع Extended می نویسیم.
**مبدا PC6 IP:192.168.6.3** و **مقصد PC2 IP:192.168.1.3** می باشد و این ACL چون از نوع Extended است باید **در روتر مبدا R6** و ورودي Inbound آن اعمال گردد.

**R6:**

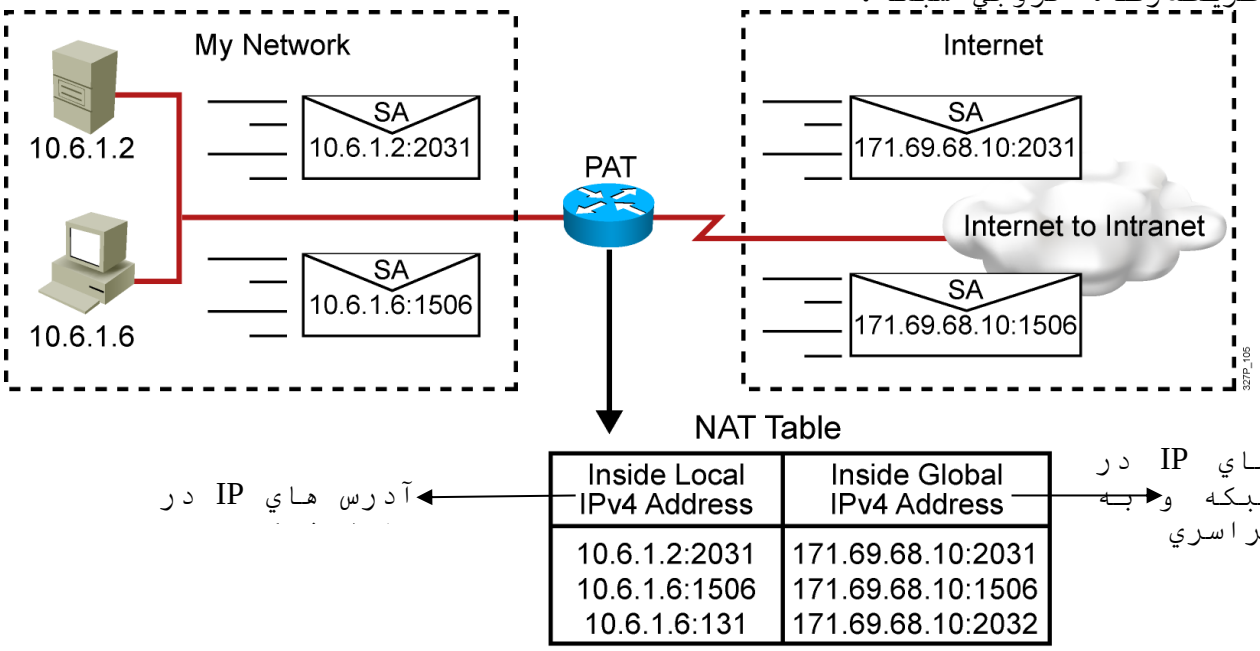
```
1  R6(config)#access-list 180 deny icmp host 192.168.6.3 host 192.168.1.3
2  R6(config)#access-list 180 permit ip any any
3  R6(config)#interface fastEthernet 0/0
4  R6(config-if)#ip access-group 180 in
```

تست ACL نوشته شده:

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# (NAT) Network Access tTeransport

- پنهان سازي رنج IP هاي داخلي شبكه
- تبديل IP هاي Private به Public
- هميشه يك كامپيوتر دخل شبكه مي خواهد به شبكه External وصل شود، از طريقدرگاه خروجي شبكه.



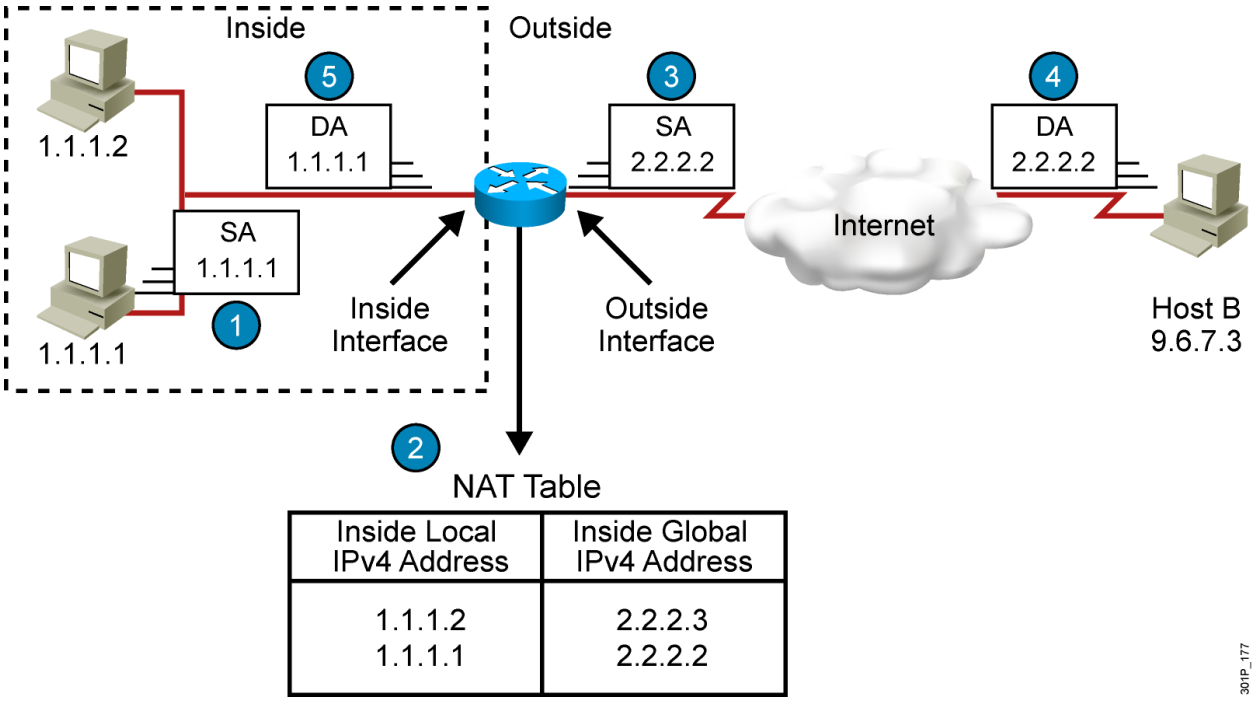

NAT Table

| Inside Local IPv4 Address | Inside Global IPv4 Address |
|---|---|
| 10.6.1.2:2031 | 171.69.68.10:2031 |
| 10.6.1.6:1506 | 171.69.68.10:1506 |
| 10.6.1.6:131 | 171.69.68.10:2032 |

آدرس هاي IP در خارج شبكه و به صورت سراسري

آدرس هاي IP در

- انجام عمل NAT روي روترها توسط عملي به نام Natting مي باشد.
- در روترها يك Nat Table وجود دارد كه مشخص مي كند هر IP به چه چيزي تبديل شده است.

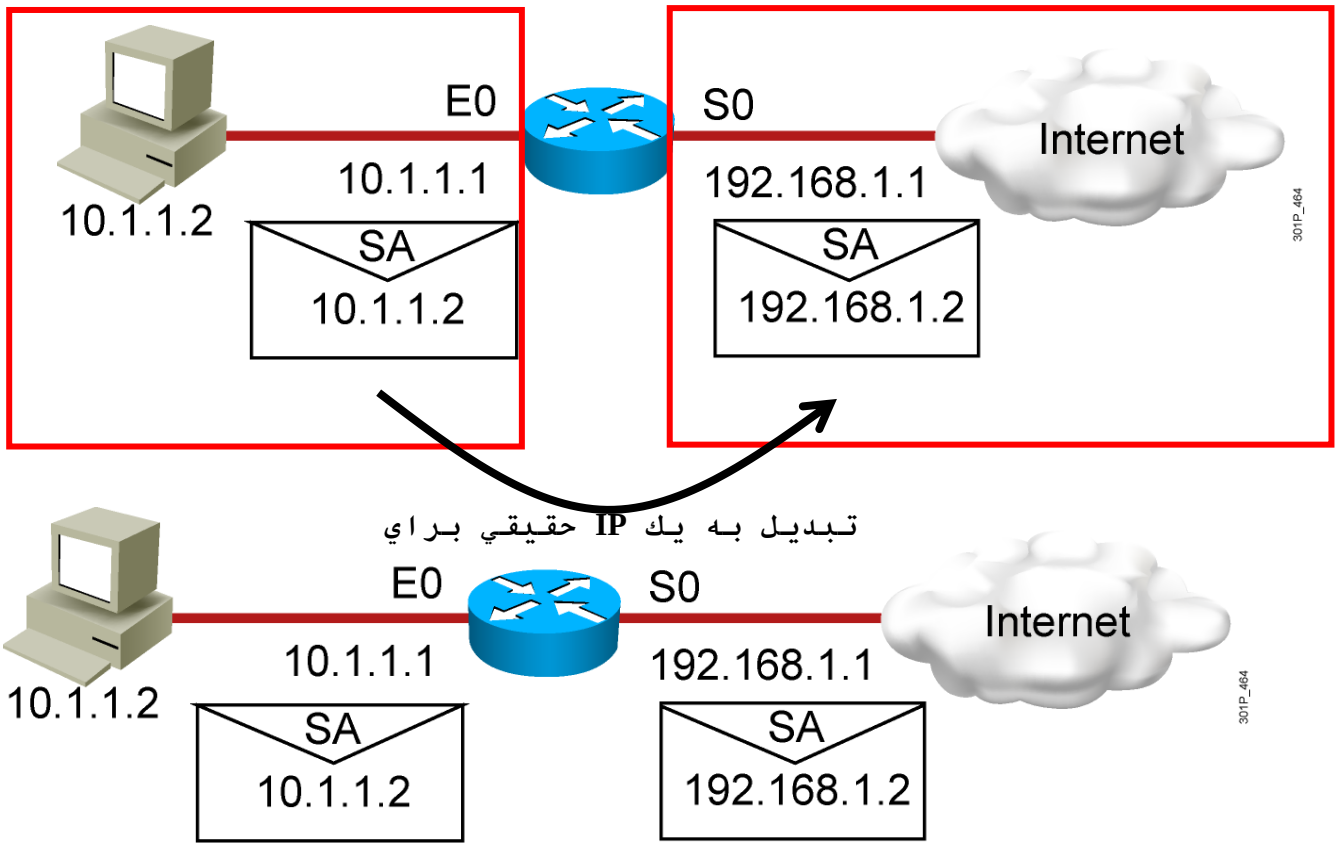


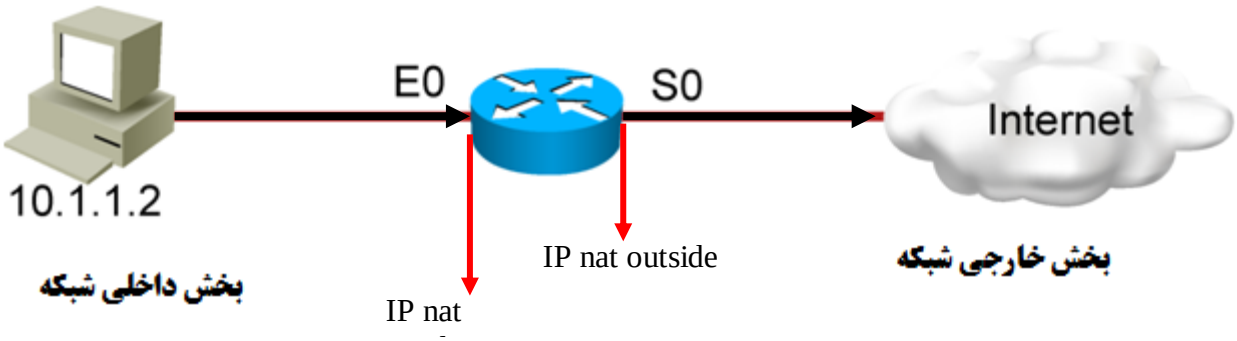
## انواع روشهاي NAT:

### 1- Static Nat:

```
1  RouterX(config)# ip nat inside source static local-ip global-ip
2
3  RouterX(config-if)# ip nat inside
4  RouterX(config-if)# ip nat outside
5
6  RouterX# show ip nat translations
```

- خط 1: انجام عمل تبديل IP هاي داخلي محلي بصورت دستي به آدرسهاي داخلي سراسري.
- خط 3و 4: وارد Interface مي شويم و نوع Interface را انتخاب مي كنيم. Inside /Outside
- خط 6: مشاهده Nat Table (مشاهده ي اينكه آيا Natting انجام مي دهد يا خير)






```
1  RouterX(config)#interface s0
2  RouterX(config-if)# ip address 192.168.1.1 255.255.255.0
3  RouterX(config-if)# ip nat outside
4
5  RouterX(config)#interface e0
6  RouterX(config-if)# ip address 10.1.1.1 255.255.255.0
7  RouterX(config-if)# ip nat inside
8
9  RouterX(config)# ip nat inside source static 10.1.1.2 192.168.1.2

   RouterX# show ip nat translations

      Pro  Inside global   Inside local   Outside local  Outside global
      ---  192.168.1.2     10.1.1.2       ---            ---
```

- خط 9: IP شبکه داخلي 10.1.1.2 ← IP در خارج از شبکه ي داخلي (در شبکه ي سراسري) 192.168.1.2.
- يعني IP:10.1.1.2 در هنگاهي که از شبکه داخلي خارج مي شود به ←IP:192.168.1.2 تبديل شود.
- در اين روش بايد به تعداد کلاينتها IP خريداري/اجاره شود در حال حاضر اين روش استفاده نمي شود چون گران است و ...

## Dynamic NAT -2

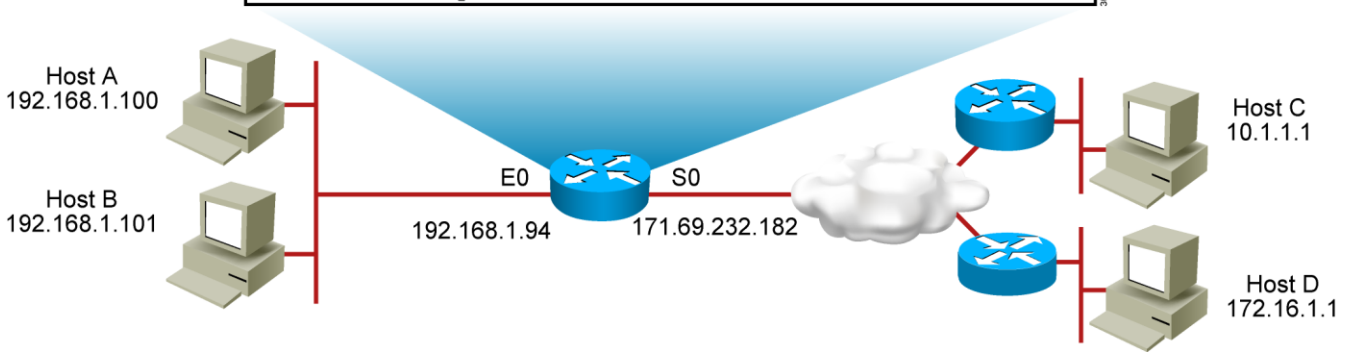
```
1  RouterX(config)# ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
2
3  RouterX(config)# access-list access-list-number permit source [source-wildcard]
4
5  RouterX(config)# ip nat inside source list access-list-number pool name
6
7  RouterX# show ip nat translations
```

- خط 1: معرفي منبعي از آدرسهاي IP جهت اختصاص در زمان مورد نياز.
- خط 3: تعريف ACL استاندارد IP كه اجازه مي دهد كه IP هاي محلي به آدرسهاي جديد تبديل شوند.
- خط 5: ايجاد Dynamic Nat و اختصاص ACLي كه در مرحله ي قبل تعريف كرديم.
- خط 7: مشاهده ي Nat Table.

اگر نتوانيم به ازاي هر كلاينت IP خريداري كرد، مثلا اگر 100 كلاينت داريم و ما فقط 50 IP خريداري كرده باشيم، به تعداد همان 50 نفر مي توانند به بيرون از شبكه متصل شوند از نفر 51 ام بايد منتظر شود كه يك IP خالي شود تا به او IP اختصاص داده شود.

مثال:

```
ip nat pool net-208 171.69.233.209 171.69.233.222 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```




ACL اي كه در اين بخش استفاده مي شود فقط براي Select كردن ترافيك است.

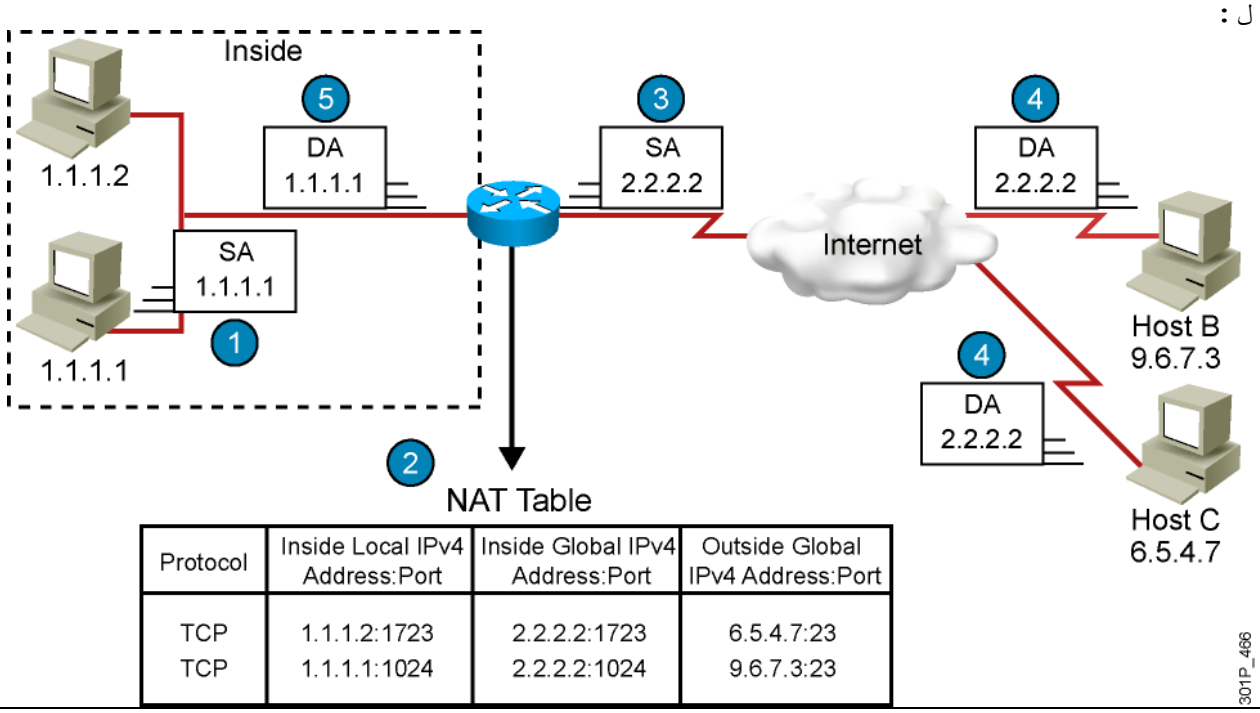
```
1  RouterX# show ip nat translations
2    Pro  Inside global     Inside local      Outside local     Outside global
3    ---  171.69.233.209    192.168.1.100     ---               ---
```

| | | | | | |
|---|---|---|---|---|---|
| 4 | --- | 171.69.233.210 | 192.168.1.101 | --- | --- |

این روش بهتر از روش اول است اما با این حال باز هم IP ها تمام می شود. و باید از روش دیگر استفاده گردد.

## Overloading Port Address Translation –PAT –3

در این روش به جای اینکه IP را به IP، Point کنیم ← IP را به پورتهای روتر Point می کنیم، روتر 65535 پورت دارد.
اگر ما یك روتر داشته باشیم که به عنوان Gatewaye باشد هر کامپیوتر را به یکی از پورتهای روتر Point می کنیم و شماره پورت را به انتهای IP سراسری اضافه می کنیم و در این حالت از یك IP Global می توانیم چند هزار IP جدید ایجاد کنیم.
مثال:

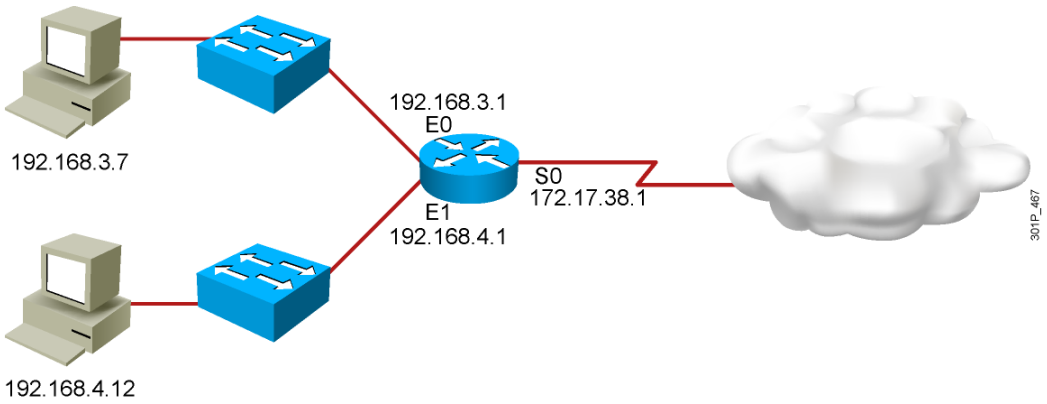



RouterX(config)# **access-list *access-list-number* permit *source source-wildcard***

RouterX(config)# **ip nat inside source list *access-list-number* interface *interface* overload**

RouterX# **show ip nat translations**

مثال:




```
1   RouterX(config)#hostname RouterX
2
3   RouterX(config)#interface Ethernet0
4   RouterX(config-if)#ip address 192.168.3.1 255.255.255.0
5   RouterX(config-if)#ip nat inside
6
7   RouterX(config)#interface Ethernet1
8   RouterX(config-if)#ip address 192.168.4.1 255.255.255.0
9   RouterX(config-if)#ip nat inside
10
11  RouterX(config)#interface Serial0
12  RouterX(config-if)#description To ISP
13  RouterX(config-if)#ip address 172.17.38.1 255.255.255.0
14  RouterX(config-if)#ip nat outside
15
16  RouterX(config)#ip nat inside source list 1 interface Serial0 overload
17
18  RouterX(config)#ip route 0.0.0.0 0.0.0.0 Serial0
19
20  RouterX(config)#access-list 1 permit 192.168.3.0 0.0.0.255
21  RouterX(config)#access-list 1 permit 192.168.4.0 0.0.0.255
22
23  RouterX# show ip nat translations
24      Pro   Inside global        Inside local          Outside local      Outside global
25      TCP   172.17.38.1:1050     192.168.3.7:1050      10.1.1.1:23        10.1.1.1:23
26      TCP   172.17.38.1:1776     192.168.4.12:1776     10.2.2.2:25        10.2.2.2:25
```

خط 23: Nat هاي Active را نمايش مي دهد و Nat table را Refresh مي كند.

**پـاك كـردن Nat Table :**

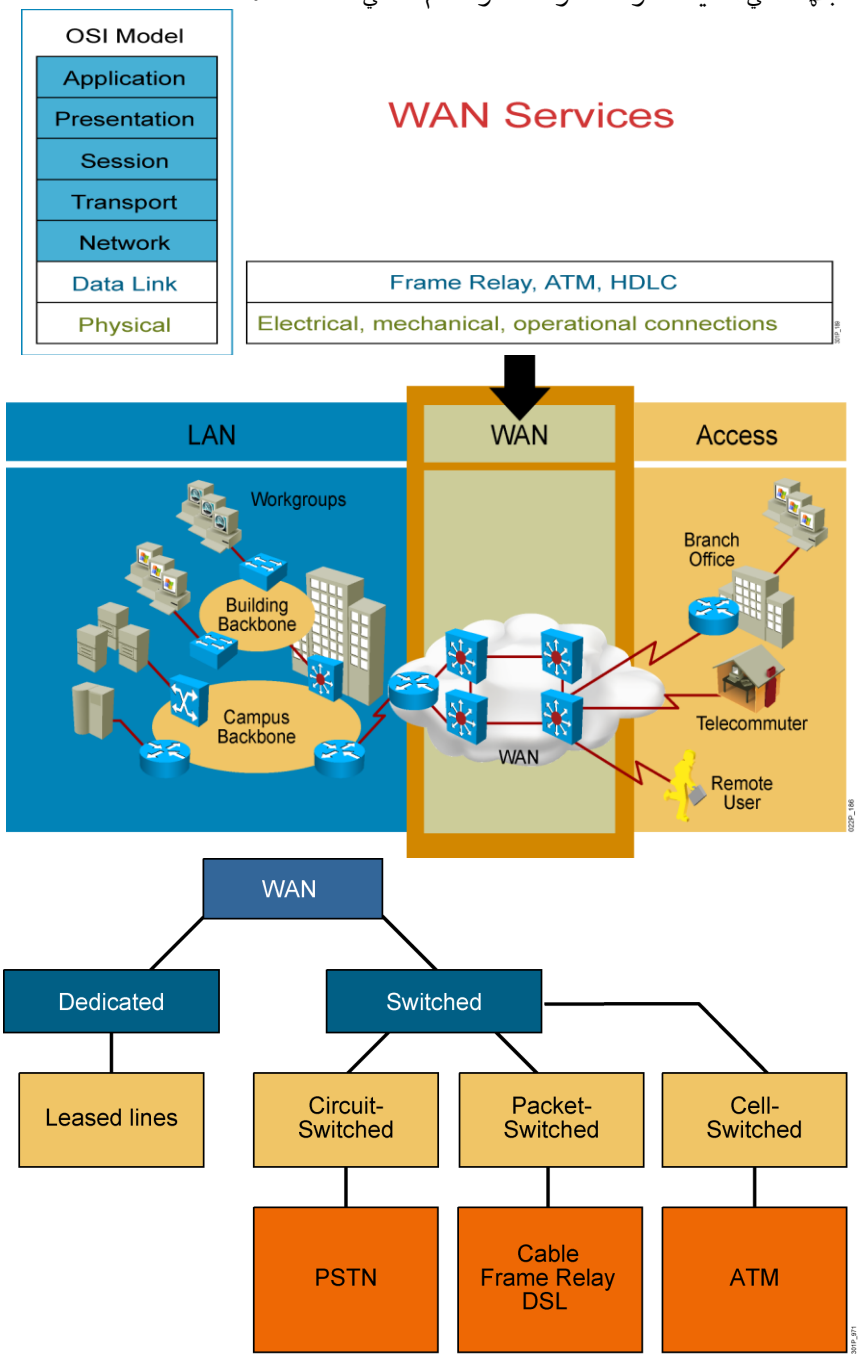
| | |
|---|---|
| 1 | RouterX# **clear ip nat translation** |
| 2 | |
| 3 | RouterX# **clear ip nat translation inside *global-ip* *local-ip* [outside *local-ip* *global-ip*]** |
| 4 | |
| 5 | **RouterX# clear ip nat translation outside *local-ip* *global-ip*** |
| 6 | |
| 7 | RouterX# **clear ip nat translation protocol inside *global-ip* *global-port local-ip* *local-port* [outside** |
| 8 | ***local-ip* *local-port* *global-ip* *global-port*]** |
| 9 | |
| 10 | RouterX# **debug ip nat** |
| 11 | |
| 12 | RouterX# **show ip nat statistics** |

- Line1: Clears all dynamic address translation entries
- Line3: Clears a simple dynamic translation entry that contains an inside translation or both an inside and outside translation.
- Line5: Clears a simple dynamic translation entry that contains an outside translation
- Line7: Clears an extended dynamic translation entry (PAT entry)
- Line10: Displaying Information with show and debug Commands
-

-

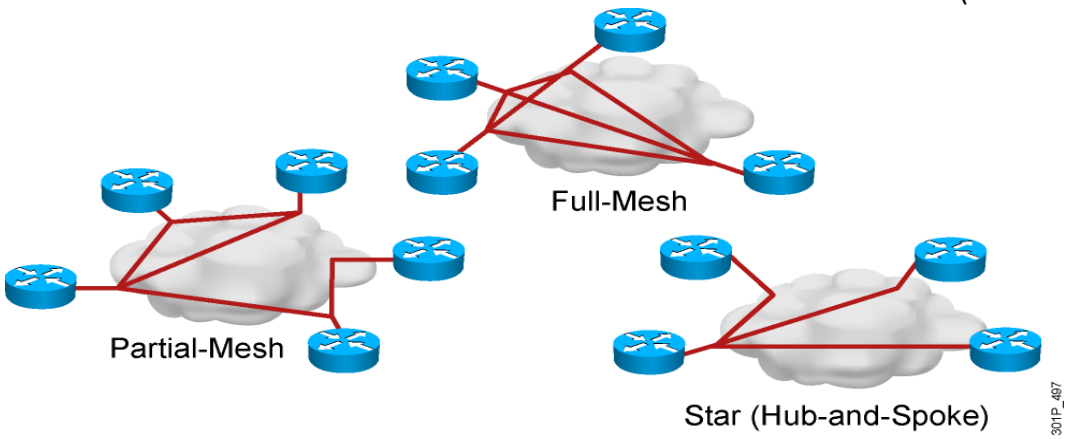
# Wide Area Network –WAN

پروتكلهايي هستند كه در لايه ي Data Link قرار گرفته اند كه بستر اوليه ي دستري به شبكه جهاني اينترنت را فراهم مي كنند.

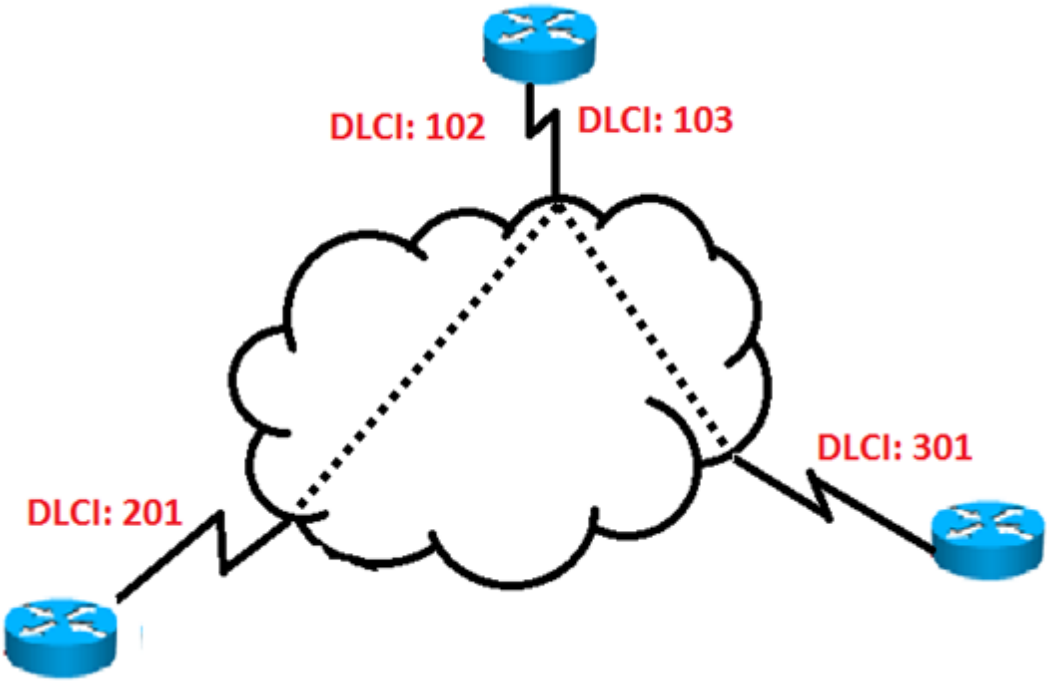


# تپولوژي پياده سازي Frame Relay

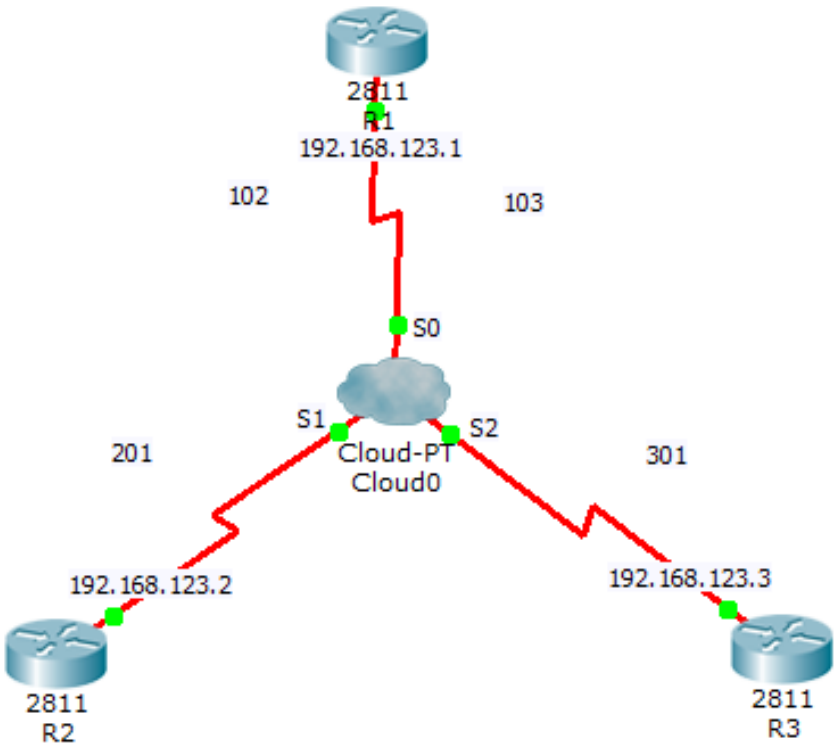
Partial-Mesh-1
Full-Mesh -2
Star(Hub-and-Spoke)-3




مثال: سناريو-




در اين حالت پورت ابر DCE مي شود و با كابل Serial DTE بايد روتر را به ابر وصل كنيم.



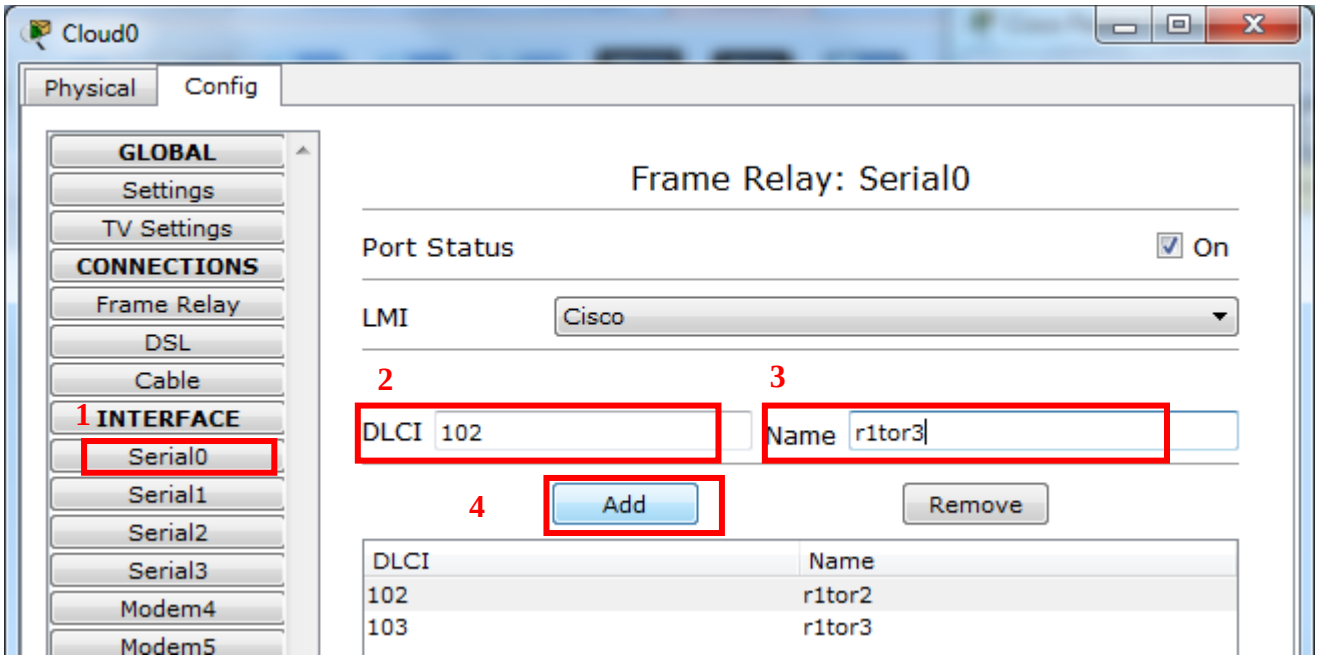

| | |
|---|---|
| 1 | Router(Config)#**Show frame-relay map** |

1- بر روي كليد كرده و **DLCI** را از قسمت **Config** و **Interface** تعريف مي كنيم.

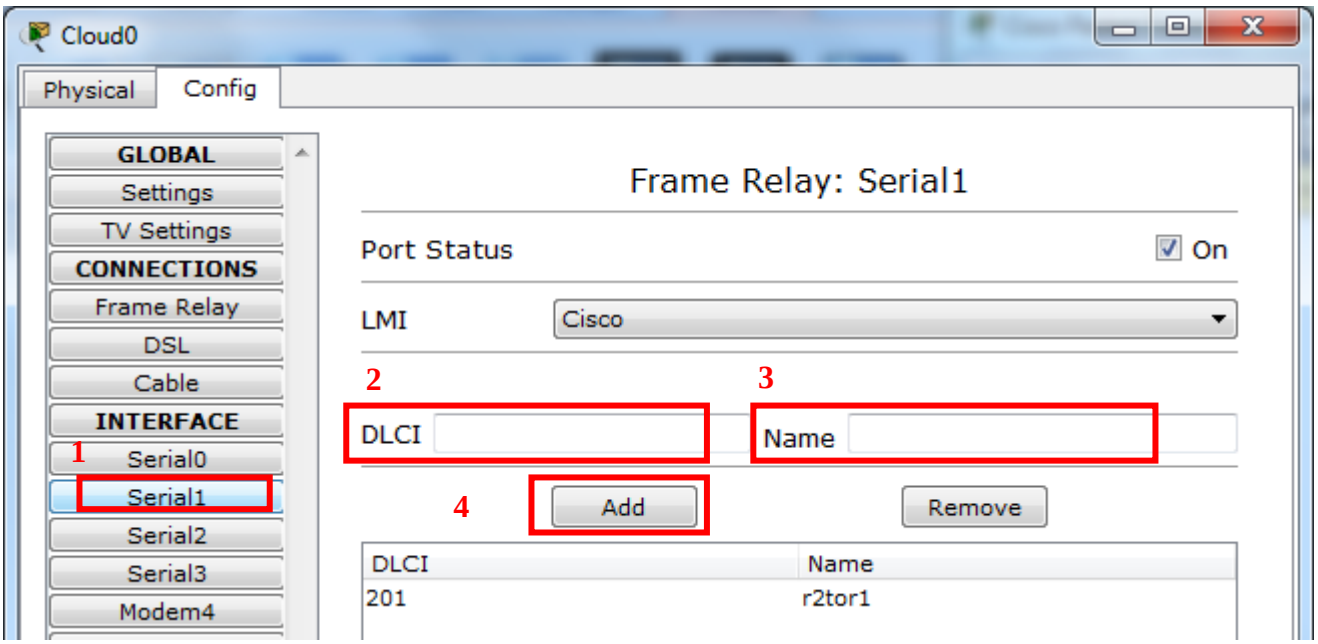
a. **Serial 0** را كليد مي كنيم.

b. **DLCI** هائيكه به پورت سريال ابر متصل هستند را وارد مي كنيم و براي آنها نام انتهاب كرده و سپس در هر مرحله كليد **ADD** با را مي زنيم.

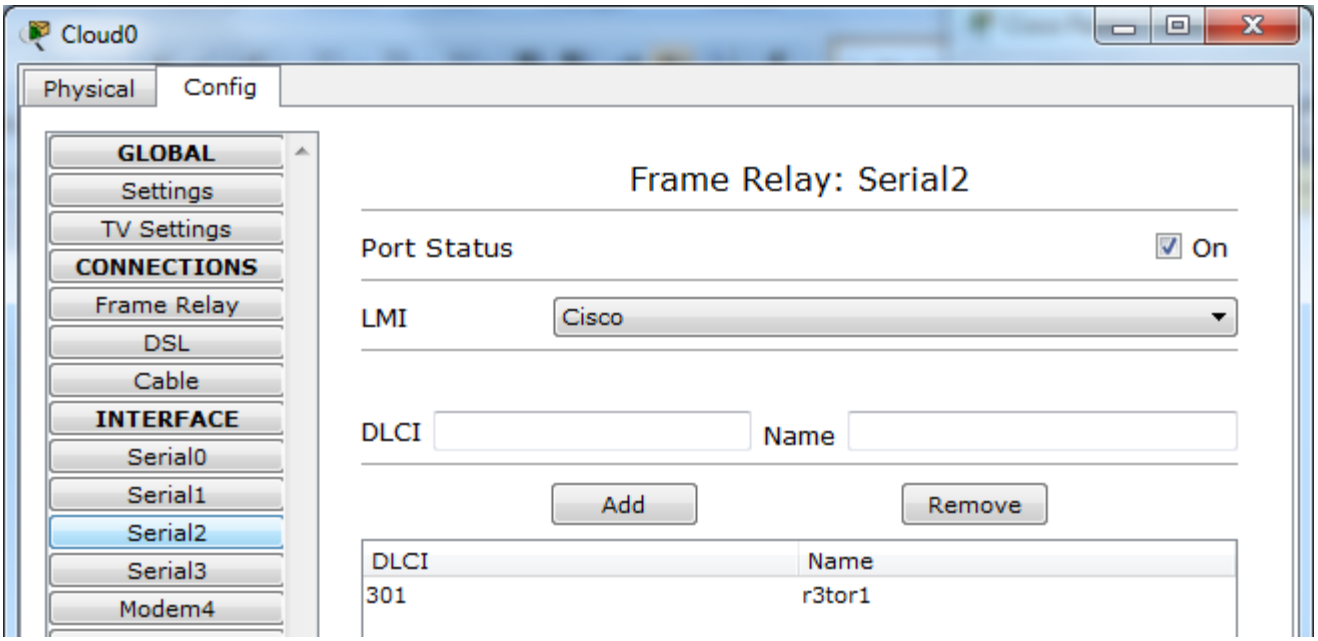
c.



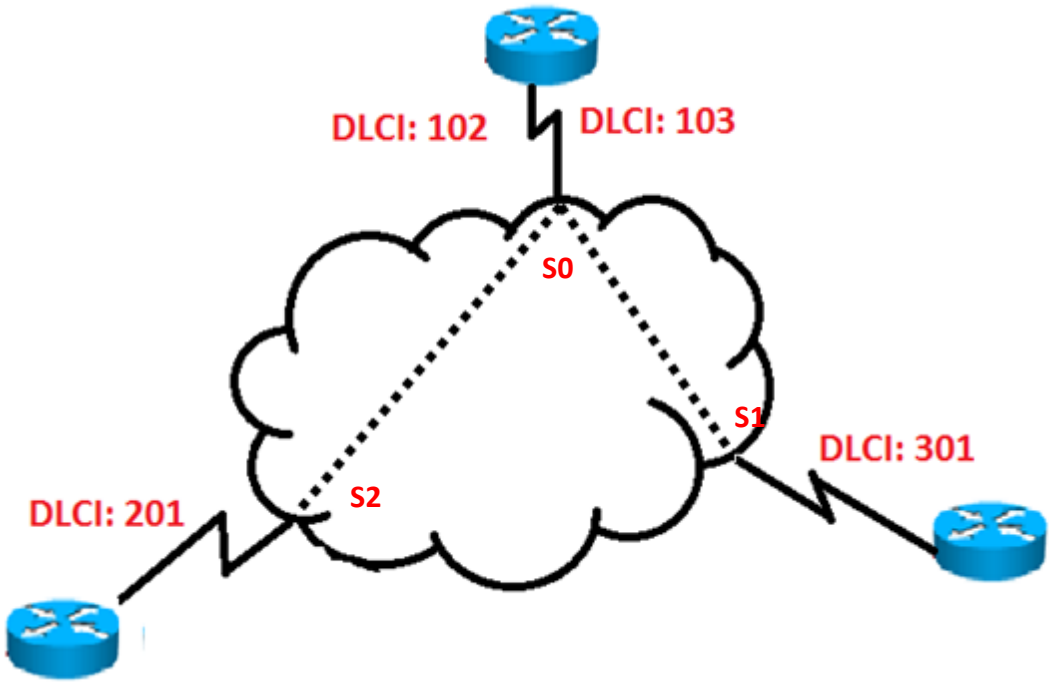

d. و پورت **Serial 1** را كليك كرده و مانند بالا **DLCI** مرتبط به اين پورت را **Add** مي كنيم.

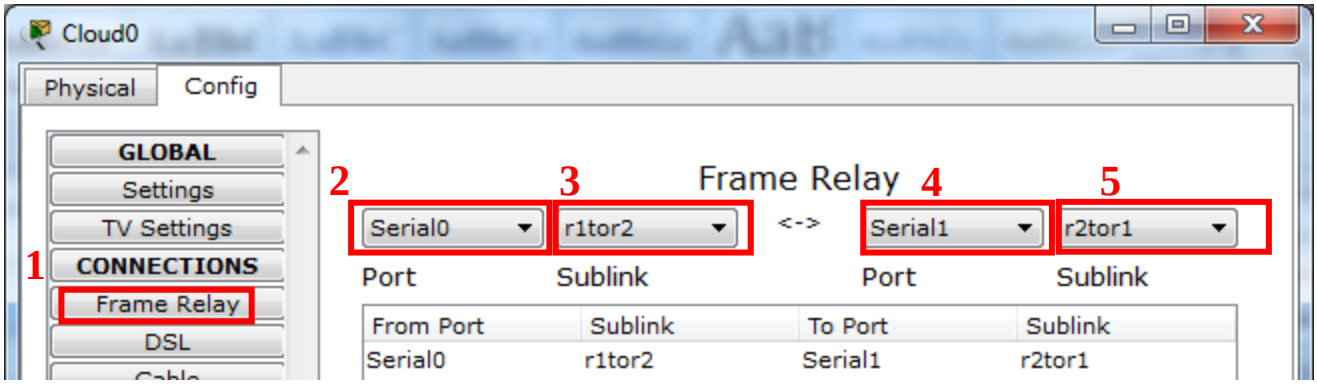


e. و پورت سریال Se2



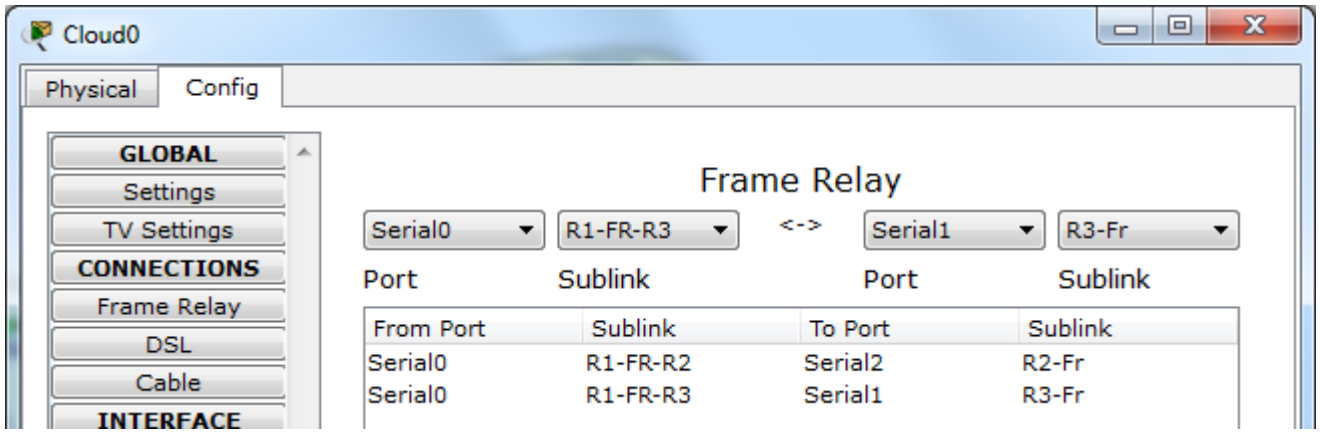

2- مجددا بر روي ابر كليك كرده و Frame Relaye ها را دقيقا مطابق به شكل زير تعريف مي كنيم.






**6. ADD**

در سمت اول از پورت سریال **Se0** ابر با نام **r1tor2** و در سمت دیگر ابر از طریق پورت سریال **Se1** با نام **r2tor1R2-Fr** به روتر **R2** متصل مي شويم.




در سمت اول از پورت سریال **Se0** ابر با نام **r1tor3** و در سمت دیگر ابر از طریق پورت سریال **Se2** با نام **r1tor3** به روتر **R3** متصل مي شويم.

**3-** حال باید روتر ها را **Config** کنیم و به پورتهاي روتر **IP** بدهیم.

**Config** روترها:

**R1**

| | |
|---|---|
| 1 | Router(Config)#**interface Serial0/0/0** |
| 2 | Router(Config-if)#**ip address 192.168.123.1 255.255.255.0** |
| 3 | |
| 4 | Router(Config-if)#**encapsulation frame-relay** |
| 5 | Router(Config-if)#**frame-relay map ip 192.168.123.2 102 broadcast** |
| 6 | Router(Config-if)#**frame-relay map ip 192.168.123.3 103 broadcast** |
| 7 | Router(Config-if)# **frame-relay map ip map ip 192.168.123.1 102** |

**R2**

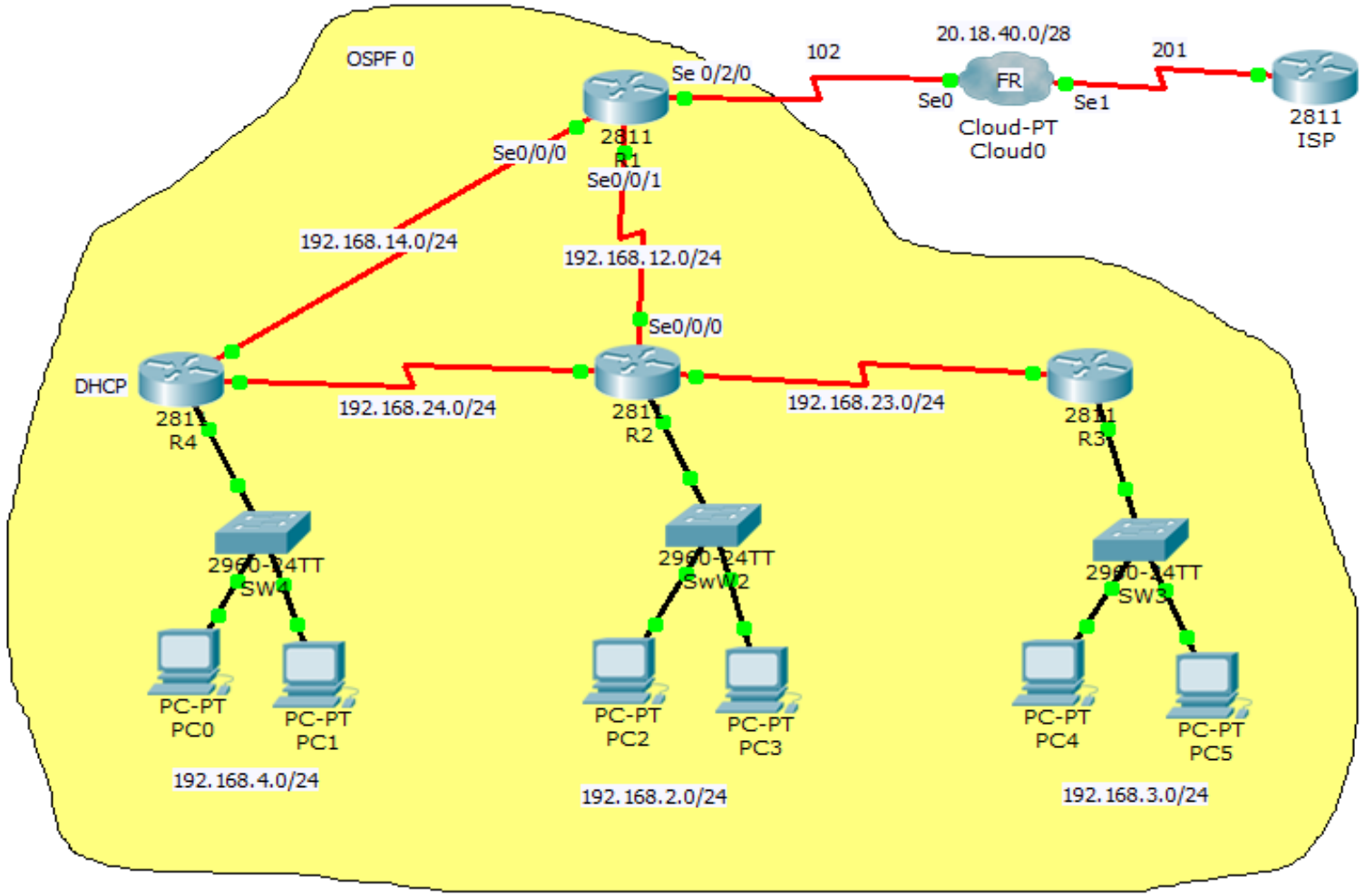
```
1  Router(Config)#interface Serial0/0/0
2  Router(Config-if)#ip address 192.168.123.2 255.255.255.0
3
4  Router(Config-if)#encapsulation frame-relay
5  Router(Config-if)#frame-relay map ip 192.168.123.1 201 broadcast
6  Router(Config-if)#frame-relay map ip 192.168.123.3 201 broadcast
```

**R3:**

```
1  Router(Config)#interface Serial0/0/0
2  Router(Config-if)#ip address 192.168.123.3 255.255.255.0
3
4  Router(Config-if)#encapsulation frame-relay
5  Router(Config-if)#frame-relay map ip 192.168.123.1 301 broadcast
6  Router(Config-if)#frame-relay map ip 192.168.123.2 301 broadcast
```

**نكته: روتر همه را به غير از خودش Ping مي كند، براي اينكه خودش را هم Ping كند بايد يك Map ديگر هم بنويسيم:**

```
1  Router(Config)#interfce serial 0/0/0
2  Router(Config-if)# frame-relay map ip map ip 192.168.123.1 102
3
4  Router#ping 192.168.123.1
```


OSPF 0
Se 0/2/0
102
20.18.40.0/28
201
FR
Se0
Se1
Cloud-PT
Cloud0
2811
ISP
2811
R1
Se0/0/0
Se0/0/1
192.168.14.0/24
192.168.12.0/24
Se0/0/0
DHCP
2811
R4
192.168.24.0/24
2811
R2
192.168.23.0/24
2811
R3
2960-24TT
SW4
2960-24TT
SwW2
2960-24TT
SW3
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
192.168.4.0/24
192.168.2.0/24
192.168.3.0/24

- با توجه به دیاگرام به سوالات زیر پاسخ دهید؟

1. با استفاده از IP هاي داده شده به اختصاص IP پرداخته و در روتر R4 از سرویس DHCP استفاده نمایید.
2. با استفاده از پروتکل هاي Frame-Relay ارتباط روتر R1 با ISP را برقرار نموده و از DLCI هاي داده شده استفاده نمایید (102و 201) .
3. پروتکل مسیریابي OSPF در Area 0 را پیاده سازي کرده و ارتباط R1 با R2 بوسیله ي مکانیزم احراز هویت MD5 راه اندازي شود.
4. با استفاده از مکانیزم PAT دسترسي کاربران سوییچ SW3 را نسبت به ISP فراهم نمایید.

---

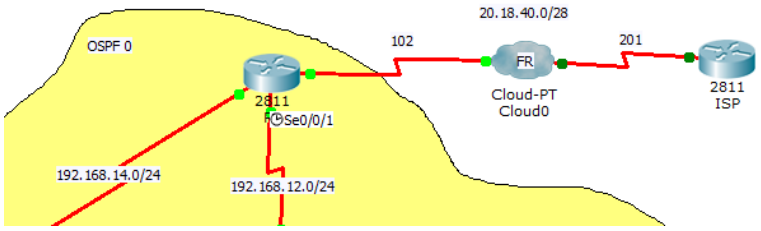
جواب سوال 1: با استفاده از IP هاي داده شده به اختصاص IP پرداخته و در روتر R4 از سرویس DHCP استفاده نمایید.

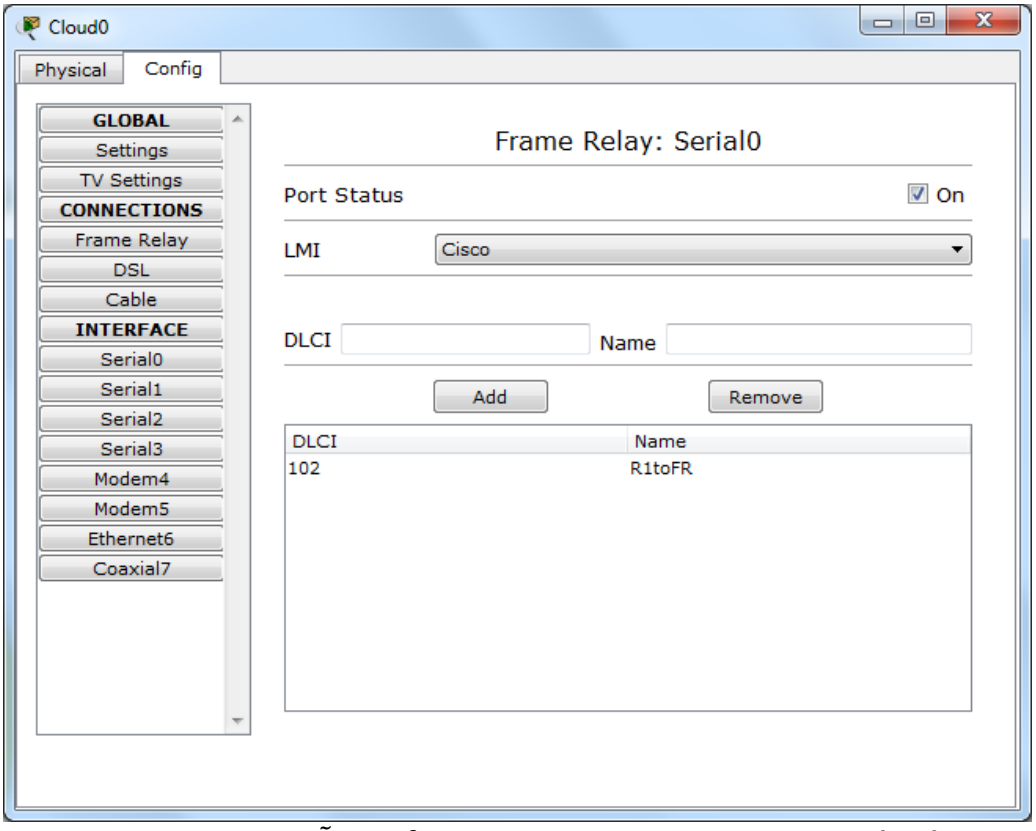
**R4:**

```
1  R4(config)#ip dhcp pool TEST
2  R4(dhcp-config)#network 192.168.4.0 255.255.255.0
3  R4(dhcp-config)# default-router 192.168.4.1
5
6  R4(config)#router ospf 1
7  R4(config-router)# network 192.168.14.1 0.0.0.0 area 0
8  R4(config-router)# network 192.168.24.1 0.0.0.0 area 0
9  R4(config-router)# network 192.168.4.1 0.0.0.0 area 0
```

---

جواب سوال 2: با استفاده از پروتکل هاي Frame-Relay ارتباط روتر R1 با ISP را برقرار نموده و از DLCI هاي داده شده استفاده نمایید (102و 201) .

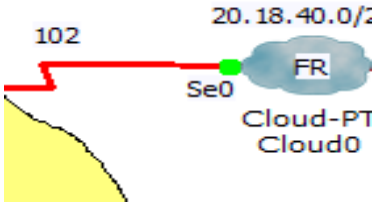




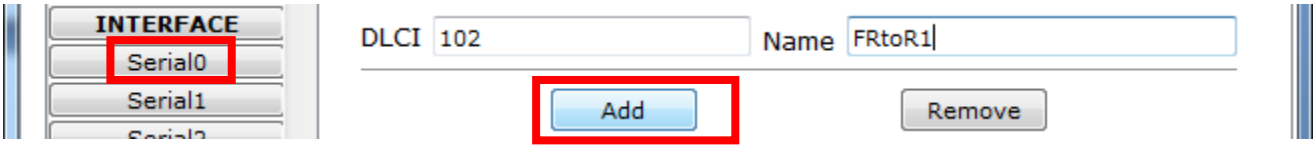

بر روي ابر **Cloud 0** كليك كرده و وارد بخش **Config** آن مي شويم.
**LMI** را چون از تجهيزات **Cisco** استفاده مي كنيم **==> Cisco** انتخاب مي كنيم.


سپس **DLCI** ها را طبق شكل وارد مي كنيم:
از قسمت زير:

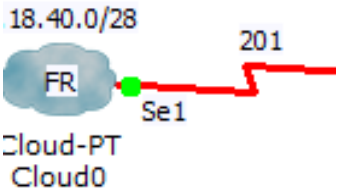
## تنظيمات پورت سريال صفر (Se0) ابر:



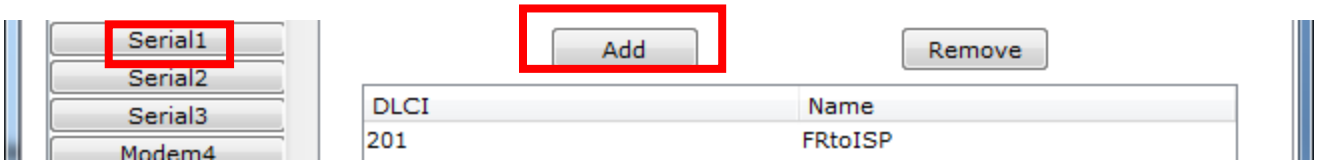

1- Cloud 0> Config> INTERFACE> Serial0
2- DLCI: 102 نام دي ال سي آي مورد نظر را وارد مي كنيم Name: FRtoR1
نام دلخواه را وارد مي كنيم
3- Add



## تنظیمات پورت سریال صفر (Se1) ابر:

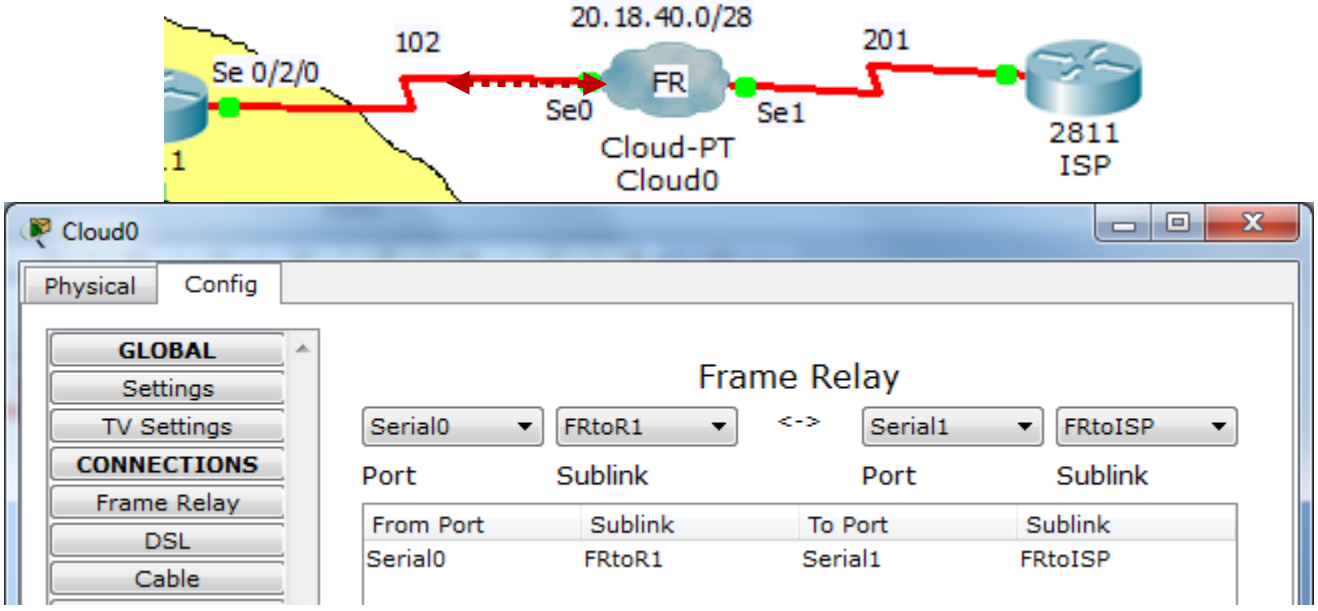



1. Cloud 0> Config> INTERFACE> Serial1
2. DLCI: 201 نام دي ال سي آي مورد نظر را وارد مي كنيم Name: FRtoISP نام دلخواه را وارد مي كنيم
3. Add




## تنظیمات ارتباط Frame Relay

4- Cloud 0> Config>Frame Relay
5- ارتباطات را تعريف مي كنيم.
6- از پورت سريال صفر ابر با مشخصات 102 به پورت سريال 1 ابر با نام 201 متصل شده ايم
7- Add



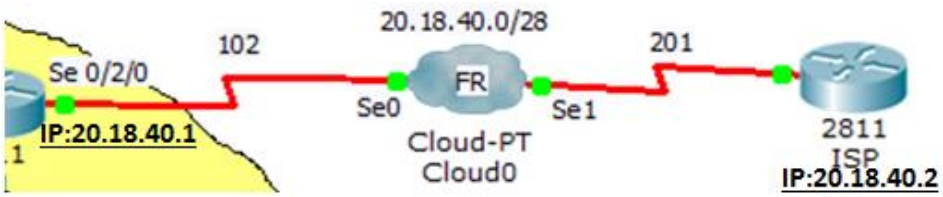

**RI:**

| | |
|---|---|
| 1 | R1(config)#**interface Serial0/2/0** |
| 2 | R1(config-if)#**encapsulation frame-relay** |
| 3 | R1(config-if)# **ip address 20.18.40.1 255.255.255.240** |

| | |
|---|---|
| 4 | R1(config-if)#**frame-relay map ip 20.18.40.2 102 broadcast** |
| 5 | R1(config-if)#**no sh** |
| 6 | |
| 7 | R1(config)#**interface Serial0/0/1** |
| 8 | R1(config-if)#**ip address 192.168.12.1 255.255.255.0** |
| 9 | R1(config-if)#**clock rate 64000** |
| 10 | |
| 11 | R1(config)#**interface Serial0/0/0** |
| 12 | R1(config-if)#**ip address 192.168.14.1 255.255.255.0** |
| 13 | R1(config-if)#**clock rate 64000** |
| 14 | |
| 15 | R1(config)#**router ospf 1** |
| 16 | R1(config-router)# **network 192.168.14.2 0.0.0.0 area 0** |
| 17 | R1(config-router)# **network 192.168.12.1 0.0.0.0 area 0** |
| 18 | R1(config-router)# **network 20.18.40.0 0.0.0.15 area 0** |

**که از طریق آن به سمت مقابل اتصال می IP طرف مقابل** R1(config-if)#**frame-relay map ip یابیم DLC broadcast**

- خط 4: بدین معناست که روتر R1 از طریق DLCI: 102 به ISP با IP:20.18.40.2 متصل شده است.
- ما از روتر 1، با استفاده از DLC:102 به ISP:20.18.40.2 ارتباط داریم.



**ISP:**

```
1  ISP(config)#interface Serial0/0/0
2  ISP (config-if)#ip address 20.18.40.2 255.255.255.240
3  ISP (config-if)#encapsulation frame-relay
4  ISP (config-if)#frame-relay map ip 20.18.40.1 201 broadcast
```

---

**جواب سوال 3: پروتكل مسيريابي OSPF در Area 0 را پياده سازي كرده و ارتباط R1 با R2 بوسيله ي مكانيزم احراز هويت MD5 راه اندازي شود.**

تنظيمات روتر 1:

**R1:**

```
1  R1(Config)#router ospf 1
2  R1(config-router)#network 192.168.14.2 0.0.0.0 area 0
3  R1(config-router)#network 192.168.12.1 0.0.0.0 area 0
4  R1(config-router)# network 20.18.40.0 0.0.0.15 area 0
5
6  R1(Config)#interface Serial0/0/1
7  R1(Config-if)# ip ospf authentication-key CCNA
8  R1(Config-if)#ip ospf authentication message-digest
```

تنظيمات روتر 2 نيز همانند بالاست:

**R2**

```
1  R2(Config)#router ospf 1
2  R2(config-router)#network 192.168.23.1 0.0.0.0 area 0
3  R2(config-router)#network 192.168.12.2 0.0.0.0 area 0
4  R2(config-router)#network 192.168.24.2 0.0.0.0 area 0
5  R2(config-router)#network 192.168.2.1 0.0.0.0 area 0
6
7  R1(Config)#interface Serial0/0/0
8  R1(Config-if)# ip ospf authentication-key CCNA
9  R1(Config-if)#ip ospf authentication message-digest
```

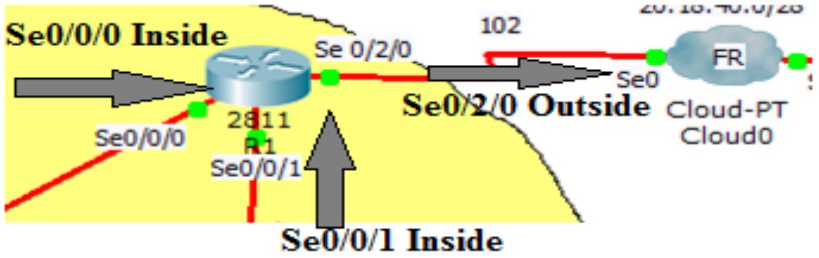
---

**جواب سوال 4: با استفاده از مکانیزم PAT دسترسي کاربران سویيچ SW3 را نسبت به ISP فراهم نمایید.به ترتیب:**

1. نوشتن ACL

R1(config)#**access-list 1 permit 192.168.3.0 0.0.0.255**

2. تعریف insideو Outeside ها در روتر 1




3. نوشتن دستور PAT:

| | |
|---|---|
| 1 | R1(config)#**interface Serial0/2/0** |
| 2 | R1(config-if)#**ip nat outside** |
| 3 | R1(config)#**interface Serial0/0/1** |
| 4 | R1(config-if)#**ip nat inside** |
| 5 | R1(config)#**interface Serial0/0/0** |
| 6 | R1(config-if)#**ip nat inside** |
| 7 | |
| 8 | R1(config)#**access-list 1 permit 192.168.3.0 0.0.0.255** |
| 9 | R1(config)#**ip nat inside source list 1 interface Serial0/2/0 overload** |

# پروتكلهاي WAN

$$\textbf{\textit{Serial Interface}}: \begin{cases} HDLC \\ PPP \begin{cases} Chap \\ PAP \end{cases} \end{cases}$$

- **HDLC:** به صورت پيش فرض روي پورتهاي سريال Run مي باشد.
- **Chap:** امنيت بالايي دارد تمامي رمزها، Encrypt شده هستند.
- **PAP:** امنيت پايييني دارد و چون پسوردهايي كه بين روترها تبادل مي گردد بدون رمز نگار است و به علت امنيت پايينش از آن استفاده نمي شود.
- مزيت PPP، Feature هاي بيشتري را نسبت به HDLC ساپورت مي كند. مثل Authentication.

- **Configuration HDLC Encapsulation:**

```
RouterX(config-if)# encapsulation hdlc
```

- **Configuration PPP Encapsulation:**

```
RouterX(config-if)# encapsulation ppp
```

- **Configuration PPP and Authentication:**

```
1  RouterX(config-if)# encapsulation ppp
2
3  RouterX(config)# hostname name
4  RouterX(config)# username name password password
5  RouterX(config-if)# ppp authentication {chap | chap pap | pap chap | pap}
```

- خط 1: فعال كردن PPP
- خط 2: انتخاب نام براي روتر
- خط 3: انتخاب يوزر و پسورد براي روتر (كه Username همان Hostname روتر مقابل است) و پسورد بين دو روتري كه مي خواهيم PPP راه اندازي نماييم مشترك مي باشد.
-

## PPP and CHAP Configuration Example


```
1  RouterX(config)# hostname RouterX
2  RouterX(config)# username RouterY
3  password 1234
4
5  RouterX(config)# int serial 0
6  RouterX(config-if)# ip address 10.0.1.1
7  255.255.255.0
   RouterX(config-if)# encapsulation ppp
   RouterX(config-if)# ppp authentication chap
```

```
1  RouterY(config)# hostname RouterY
2  RouterY(config)# username RouterX
3  password 1234
4
5  RouterY(config)# int serial 0
6  RouterY(config-if)# ip address 10.0.1.1
7  255.255.255.0
   RouterY(config-if)# encapsulation ppp
   RouterY(config-if)# ppp authentication chap
```

- خط 1: نام روتر را تعريف مي كنيم.
- خط 3: در قسمت يوزرنيم، نام روتر مقابل را مي نويسم و در قسمت پسورد، پسورد مشترك بين دو روتر انتخاب مي كنيم.
- خط 4: به پورتهاي طرفين IP اختصاص مي دهيم.

### خطا يابي PPP

```
1   RouterX# show interface s0
2   Serial0 is up, line protocol is up
3    Hardware is HD64570
.    Internet address is 10.140.1.2/24
.    MTU
24   LCP Open
     Open: IPCP, CDPCP
     …

30  RouterX# debug ppp authentication
    4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
    4d20h: Se0 PPP: Treating connection as a dedicated line
    4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
    4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from ”left"

    RouterX# debug ppp negotiation
```

- خط 24: چك كردن مكانيزم Authentication PPP.
- خط 30: براي Debug كل پروتكل PPP.

## Virtual Private Network –VPN

- ايجاد يك كانكشن امن در يك بستر نا امن (مثل WAN) را گويند.
- پياده سازي VPN با دو مدل Device قابل انجام شدن است:

- **VPN**: $\begin{cases} Firewall \begin{bmatrix} Hard(ASA, SSG) \\ Soft(ISA, TMG) \end{bmatrix} \\ Router \rightarrow K9 \end{cases}$

- **مزيت هاي استفاده از VPN:**
  1- كاهش هزينه ها
  2- قابليت رشد و گسترش شبكه
  3- ايجاد امنيت

- **انواع روشهاي پياده سازي VPN:**
  1- **Site to Site VPN:** 80% به اين روش است. دو شبكه ي كاملا مستقل از طريق يك كانكشن WAN به هم متصل مي شوند.
  2- **Remote Access VPN:** استفاده از يك نرم افزار جانبي جهت اتصال به سرور (مثل VPN هايي كه در ايران براي عبور از فيلترينگ استفاده مي شود.)
  و يا Cisco Easy VPN: نرم افزار رايگاني است كه شركت سيسكو ارائه داده است.
- **Web VPN:** استفاده از VPN با استفاده از SSL (كه براي ايمن سازي سرويس هاي وب مثل سايت بانكها است كه روي Browserها اجرا مي گردد.)
-
- در راه اندازي VPN پروتكل جامعي كه استفاده مي شود IPSec است. IPSec از مجموعه عملكرد يكسري پروتكل امنيني است.
- پروتكلهايي كه به آن اشاره مي شود:
  1- Confidentiality: محرمانگي داده ها
  2- Data Integrity: يكپارچگي و تضمين سلامت داده ها در رسيدن به مقصد
  3- Authentication: احراز هويت
  4- Antireplay Protection: تصديق فرستنده ي واقعي

- **Encryprion Algorithms: الگوريتمهاي رمز نگاري**
- جهت محرمانگي (محرمانه نگه داشته داده ها) از الگوريتمهاي رمزنگاري استفاده مي شود.

تفاوت الگوريتمهاي رمز نگاري در طول كليد آنهاست

$$\begin{cases} 1.DES & 56\ bit \\ 2.3DES & 3 \times 56\ bit \\ 3.RSA & 512\ bit \\ 4.AES & 128\ bit \end{cases}$$

- بعد ازتعريف الگوريتمهاي رمز نگاري، الگوريتمهاي Key Exchang بوجود آمد كه عمل رد و بدل كردن كليدها بين مبدا و مقصد (دو نقطه) را انجام مي دهد. يكي از اين الگوريتمها كه عمل تبادل را انجام مي دهد، Diffie-Hellman مي باشد.

$$\begin{cases} ?.??? \\ ?.??? \\ ?.??? \\ ?.??? \end{cases}$$

- **Integrity : تضمين سلامت داده ها**

زمانيكه داده بين مبدا و مقصد رد و بدل مي گردد بايد مطمئن شويم كه داده ي ارسال شده به صورت درست و بدون دستكاري به مقصد مي رسد.
بايد كاري كنيم اگر بخواهيم داده اي را از نقطه ي A به نقطه ي Bانتقال دهيم در صورتي كه داده تغيير كند ← گيرنده بفهمد كه اين داده تغيير كرده است. در اين حالت ما از الگوريتمهاي Hashing استفاده مي كنيم.

[illegible]: $\begin{cases} 1. \text{[illegible]} - \text{[illegible]}5 \\ 2. \text{[illegible]} - \text{[illegible]}1 - 1 \end{cases}$ [illegible] $g$ [illegible]

- **Authentication، احراز هويت**

- دو معيار و بحث كلي در دنيا در اين بخش موجود است. PSK و CA.

**انواع كليدهاي رد و بدل شده بين مبدا و مقصد.** $\begin{cases} \text{[illegible]} \\ \text{[illegible]} \end{cases}$ [illegible] → [illegible] **1.**

- يك پسورد (رمز ارتباطي) تعريف مي كنيم (جهت ورود به نقطه ي مورد نظر)
- الگوريتمهايي كه از اين دو دسته (Public Keyو Private Key) استفاده مي كنند به دو دسته تقسيم مي شوند.

- $\begin{cases} \text{[illegible]} \\ \text{[illegible]} - \text{[illegible]} \end{cases}$ → [مبدا] [illegible] $r$ [illegible] ⟶ [مقصد] [illegible]

- A-Semetric دو كليدي است. در مبدا با Public key قفل مي شود.
- كليد همراه بسته ارسال مي گردد كه اين روش خطرناك است و گيرنده با كليد شخصي اش بسته را باز مي كند .

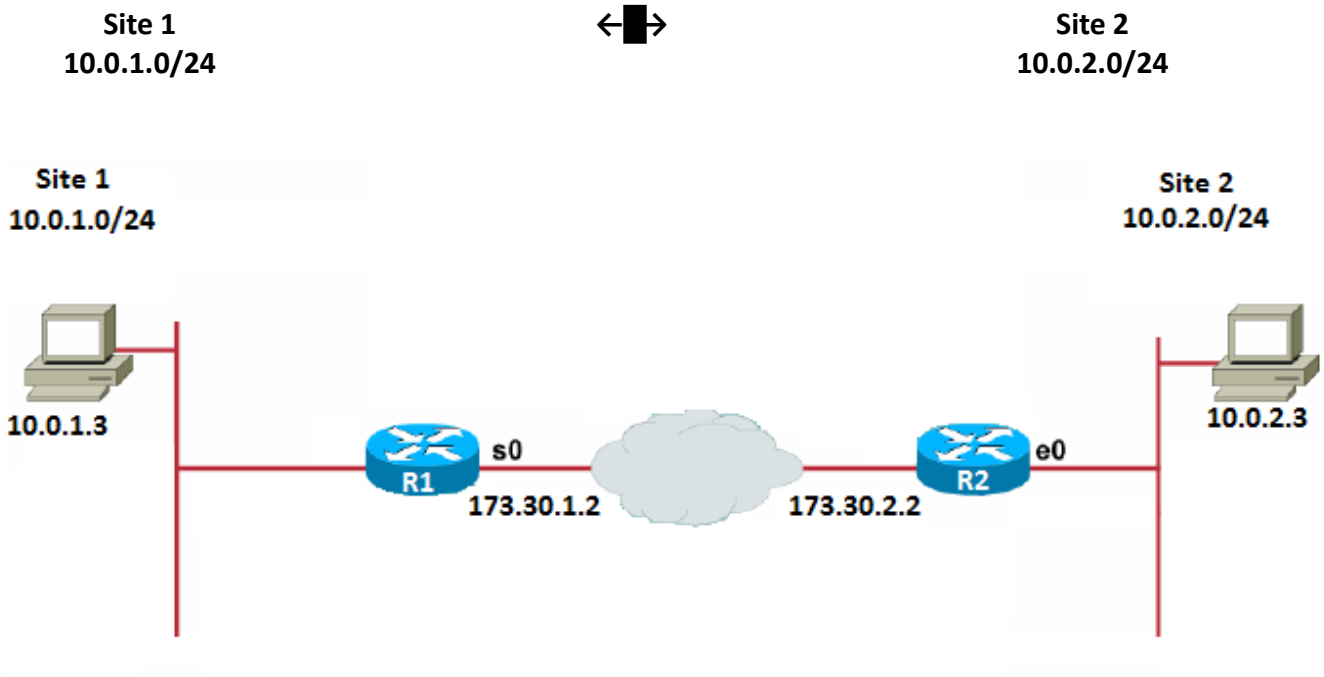
**2.** [illegible] ⟶ [illegible] [illegible]

- Certification : تاريخ Expire در آن قرار دارد. درخواست كننده نيز وجود دارد.

## پیاده سازی IPSec:

5 مرحله دارد.

**1- نوشتن ACL متناسب براي ارتباط سايتها نسبت به هم.**




**R1:**

| | |
|---|---|
| 1 | Router(Config)#**Access-list 110 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255** |

**R2:**

| | |
|---|---|
| 1 | Router(Config)#**Access-list 120 permit ip 10.0.2.0 0.0.0.255** |

اين ACL صرفا جهت كنترل ترافيك است.
شماره ي ACL ها در روتر نياز نيست شبيه به هم باشد.

---

**2- نوشتن Policy امنيتي براي مشخص نمودن پروتكلهاييكه در IPSec مي خواهيم از آنها استفاده كنيم.**

| | |
|---|---|
| 1 | Router(Config)#**Crypto isakmp policy *priority*** |

Priority: شماره ي اولويت است. در زمانيكه چند Policy وجود داشته باشد اولويت اجراي Policy ها را بر اساس اين شماره تعيين مي كند.

**Router 1, 3:**

| | |
|---|---|
| 1 | Router(Config)#**Crypto isakmp policy *110*** |
| 2 | Router(Config-isakmp)#**authentication pre-share** |
| 3 | Router (config-isakmp)#**encryption aes 256** |
| 4 | Router (config-isakmp)#**group 1** |
| 5 | Router (config-isakmp)#**hash md5** |

| | |
|---|---|
| 6 | Router (config-isakmp)#**lifetime 86400** |

در هر دو روتر باید عینا Policyیکسان بنویسیم.

---

**3-تعریف رمز متناسب مابین روترها**

Router(config)#**crypto isakmp key رمز مناسب address IPمقابل**

**R1**

| | |
|---|---|
| 1 | R1(config)#**crypto isakmp key cisco123 address 172.30.2.2** |

بعد از address باید ip اینترفیس روتر مقابل را بنویسیم. 173.30.2.2

**R2**

| | |
|---|---|
| 1 | R2(config)# **crypto isakmp key cisco123 address 173.30.1.2** |

---

**4- تعریف Transfprm Set: مکانیزمي است که Header داده را مشخص مي کنیم.**

**R1:**

| | |
|---|---|
| 1 | RouterX(config)#**crypto ipsec transform-set *MYSET(ccna)* esp-aes 128** |

**R2:**

| | |
|---|---|
| 1 | RouterY(config)#**crypto ipsec transform-set *OtherSET* esp-aes 128** |

- نام طرفین مي تواند همسان باشد.
- طول کلید طریفین (عددي که در جلوي esp-aes نوشته شده است) باید یکسان باشد.

**R1,R2:**

| | |
|---|---|
| 1 | RouterX(config)#**crypto ipsec transform-set cisco123 esp-aes 128** |

---

**5- تعریف Crypto Map:**

**R1, R2:**

| | |
|---|---|
| 1 | R1(config)#**crypto map MYMAP 10 ipsec-isakmp** |
| 2 | R1(config-crypto-map)#**match address 101** |
| 3 | R1(config-crypto-map)#**set peer 172.30.2.2 ~~default~~** |
| 4 | R1(config-crypto-map)#**set pfs group1** |
| 5 | R1(config-crypto-map)#**set transform-set (MYSET) ccna** |
| 6 | R1(config-crypto-map)#**set security-association lifetime seconds 86400** |

- خط 1: اسم دلخواه انتخاب مي کنیم که در جلوي آن برایش اولویت تعریف مي کنیم که در صورتي که از چند Crypto استفاده کردیم سیستم بداند که اولویت اجرا به چه ترتیبي است.
- خط 2: باید شماره ي ACL نوشته شده را در جلوي آن بنویسیم.
- خط 3: در قسمت IP Set peer سمت مقابل را مي نویسیم . نوشتن Defualt نیاز نیست. در جایي که Slave /Master داشته باشیم نیاز است.

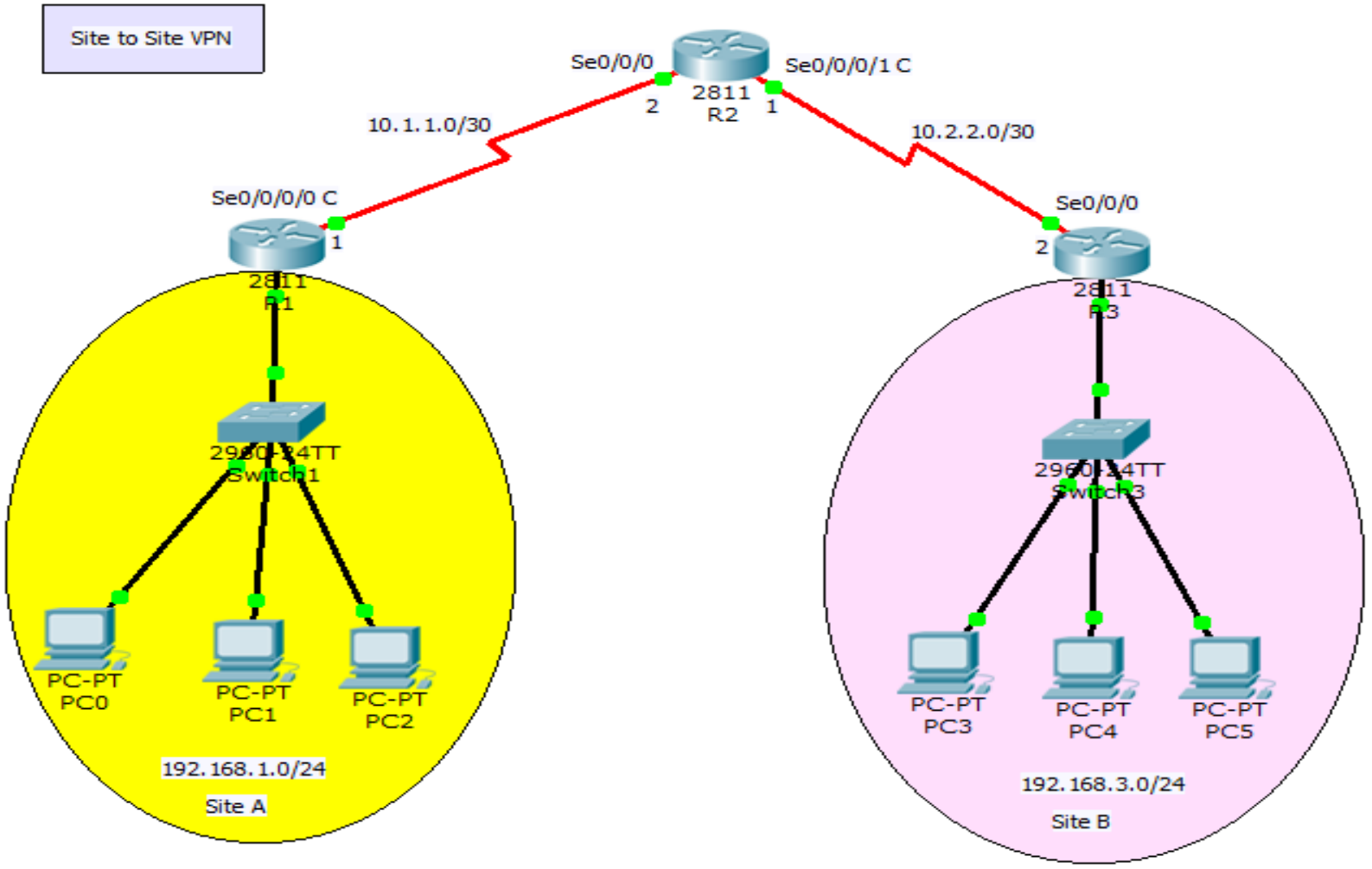
---

**6- اعمال Crypto Map نوشته شده به پورت مورد نظر.**

**R1, R2:**

| | |
|---|---|
| 1 | R1, R3(config)#**interface <u>Interface</u>** |
| 2 | Router(config-if)#**crypto map <u>MYMAP</u>** |
| 3 | *Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON |

## جلسه 23-سناریو VPN Site to Site



- **با توجه به دیاگرام فوق ارتباط روتر 1 با روتر 3 را با استفاده از VPN Site to Site راه اندازي كنيد. (پروتكل مسير يابي به صورت دلخواه)**

**پروتكل مسير يابي را در اينجا Rip انتخاب نموده ايم.**

```
1  R1(config)#router rip
2  R1(config-router)#version 2
3  R1(config-router)#network 192.168.1.0
4  R1(config-router)#network 10.1.1.0
```

**R2**

```
1  R2(config)#router rip
2  R2(config-router)#version 2
3  R2(config-router)#network 10.1.1.0
4  R2(config-router)#network 10.2.2.0
```

**R3**

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 10.2.2.0
4  Router(config-router)#network 192.168.3.0
```

---

**1. ابتدا ACL(Access List) مناسب را جهت ارتباط سايتها نسبت به هم مي نويسيم.**

**R1**

```
1  R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

آي پي : 0.0.0.255 IP Source: 192.168.1.0 و سپس 0.0.0.255 IP Des:192.168.3.0 به همراه Widcard مناسب مي نويسيم.

- در روتر مقابل نيز ACL مورد نظر را مي نويسيم:

**R3**

```
1  R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

- اين ACL جهت كنترل ترافيك است.

---

**2. نوشتن Policy امنيتي براي مشخص نمودن پروتكلهائيكه در IPsec مي خواهيم از آنها استفاده كنيم. در هر دو روتر R1و R3 كد زير را مي نويسيم:**

**R1, R3**

```
1  R1,R3 (config)#crypto isakmp policy 10
2  R1,R3 (config-isakmp)#authentication pre-share
3  R1,R3 (config-isakmp)#encryption aes 256
4  R1,R3 (config-isakmp)#group 1
5  R1,R3 (config-isakmp)#hash md5
6  R1,R3 (config-isakmp)#lifetime 86400
```

---

**3. تعريف رمز مناسب مابين روترهاي R1, R3.**

Router(config)#**crypto isakmp key** رمز مناسب **address** آی پی مقابل

**R1**

```
1  R1(config)#crypto isakmp key minush address 10.2.2.2
```

**بعد از address بايد ip اينترفيس روتر مقابل را بنويسيم. 10.2.2.2**

**R3**

```
1  R3(config)#crypto isakmp key minush address 10.1.1.1
```

---

**4. تعريف Transform Set مناسب.**

**R1**

```
1  R1(config)#crypto ipsec transform-set ccna esp-aes 128
```

**R3**

```
1  R3(config)#crypto ipsec transform-set ccna esp-aes 128
```

---

**5. تعريف Crypto Map**

```
1  R1(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer  and a valid access list have been
3  configured.
4  R1(config-crypto-map)#match address 101
5  R1(config-crypto-map)#set peer 10.2.2.2
6  R1(config-crypto-map)#set pfs group?
7  group1  group2  group5
8  R1(config-crypto-map)#set pfs group1
9  R1(config-crypto-map)#set transform-set ccna
   R1(config-crypto-map)#set security-association lifetime seconds 86400
```

**R3**

```
1  R3(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer  and a valid access list have been
3  configured.
4  R3(config-crypto-map)#match address 101
5  R3(config-crypto-map)#set peer 10.1.1.1
6  R3(config-crypto-map)#set pfs group1
7  R3(config-crypto-map)#set transform-set ccna
   R3(config-crypto-map)#set security-association lifetime seconds 86400
```

---

**6. اعمال Crypto Map نوشته شده به پورت سريال خروجي روتر مورد نظر (در پورت سريال Se0/0/0 روترهاي R1, R3)**

**R1, R3:**

```
1  R1, R3(config)#interface serial 0/0/0
2  Router(config-if)#crypto map vpn
3  ERROR: Crypto Map with tag vpn does not exist.
4
5  R1,R3(config-if)#crypto map VPN
6  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

---

**7. تست تانل ايجاد شده: ابتدا از كامپيوترهاي سايت A، كامپيوترهاي سايت B را Ping مي كنيم و بالعكس.**

سپس با استفاده از دستور زير چك مي كنيم كه ارتباط بين دو سايت برقرار مي باشد يا نه؟

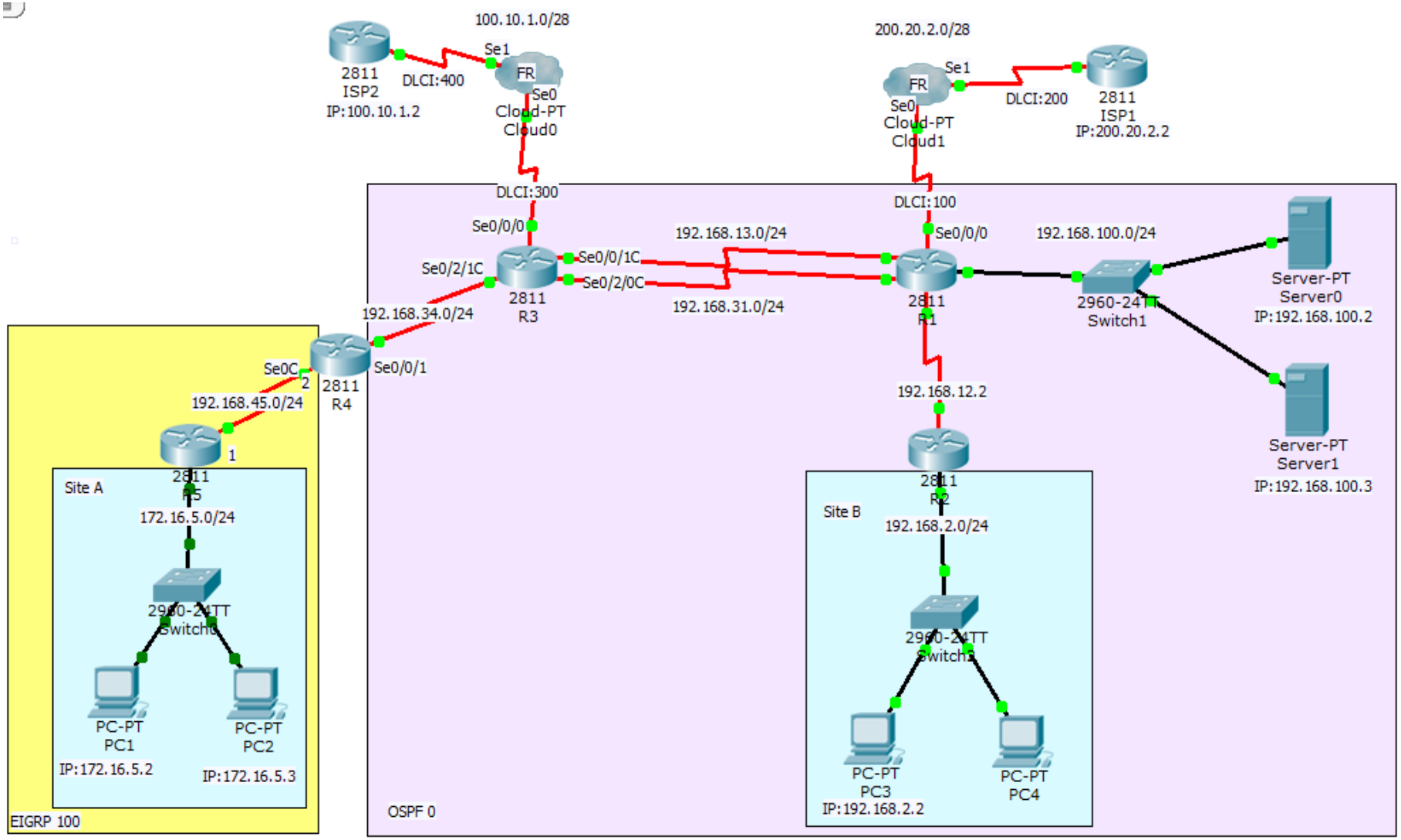
```
1.  R1#show crypto ipsec sa
.   …
.   interface: Serial0/0/0
.      Crypto map tag: VPN, local addr 10.1.1.1
.
.     protected vrf: (none)
.     local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
.     remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
.     current_peer 10.2.2.2 port 500
.      PERMIT, flags={origin_is_acl,}
.     #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
.     #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
.   …
```

در صورتي كه تانل برقرار شده باشد و پكت ها بعد از ping بين دو سايت رد و بدل شده باشند بايد مقادير

**pkts encaps, pkts encrypt, pkts decaps, pkts decrypt.**

صفر نباشند.

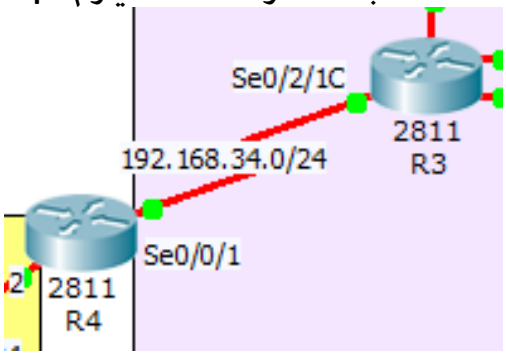
## PPP, Frame Relay, Redistribution, Pat, ACL, VPN -23 سناریو جلسه



با توجه به سناريوي زير به سوالات پاسخ دهيد.

1- با Ip هاي داده شده به اختصاص IP پرداخته و ار پروتكل PPP براي ارتباط Router 3 با Router 4 به همراه مكانيزم Chap استفاده كنيد:
2- از پروتكل Frame Relay استفاده نموده و ارتباط Router 1 و Router 3 را با ISP هاي 1 و 2 با استفاده از اطلاعات داده شده راه اندازي نماييد.
3- با استفاده از پروتكلهاي مسير يابي داده شده، مطابق با ديا گرام به پياده سازي مسيريابي پرداخته و در روتر Redistribution 4 استفاده نماييد.
4- دسترسي PC1 نسبت به ISP1 و دسترسي PC3 نسبت به ISP2 را از طريق PAT مقدور نماييد.
5- دسترسي PC2 را نسبت به Server1 كلا مسدود و از طريق Server 2 به طريق Web مقدور نماييد.
6- از مكانيزم VPN Site to site به روش IPsec ارتباط سايت A و B را برقرار كنيد.

**جواب سوال 1:** با Ip هاي داده شده به اختصاص IP پرداخته و ار پروتکل PPP براي ارتباط Router 3 با Router 4 به همراه مکانيزم Chap استفاده کنيد:




**R3:**

| | |
|---|---|
| 1 | Router(config)#**hostname R3** |
| 2 | R3(config)#**username R4 password 1234** |
| 3 | R3(config)#**interface serial 0/2/1** |
| 4 | R3(config-if)#**encapsulation ppp** |
| 5 | R3(config-if)#**ppp authentication chap** |
| 6 | R3(config-if)#**no sh** |

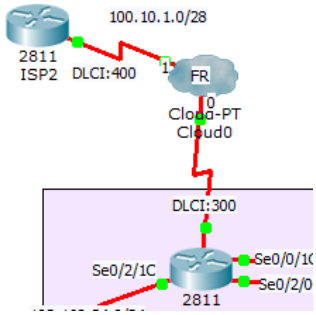
**R4:**

| | |
|---|---|
| 1 | Router(config)#**hostname R4** |
| 2 | R4(config)#**username R3 password 1234** |
| 3 | R4(config)#**interface serial 0/0/1** |
| 4 | R4(config-if)#**encapsulation ppp** |
| 5 | R4(config-if)#**ppp authentication chap** |
| 6 | R4(config-if)#**no sh** |

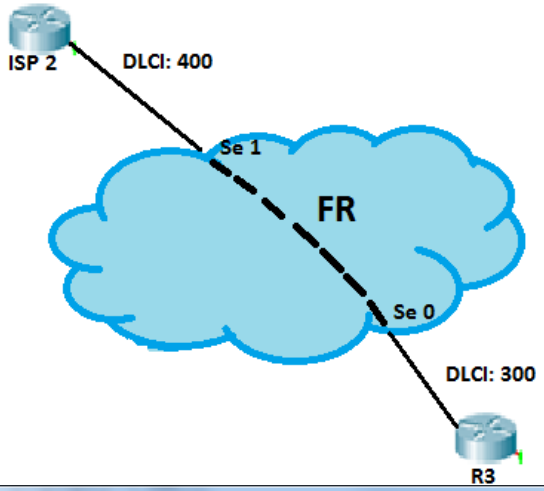
در دوسمت يسورد مشترک وارد مي نام روتر مقابل password Router(config)#username کنيم

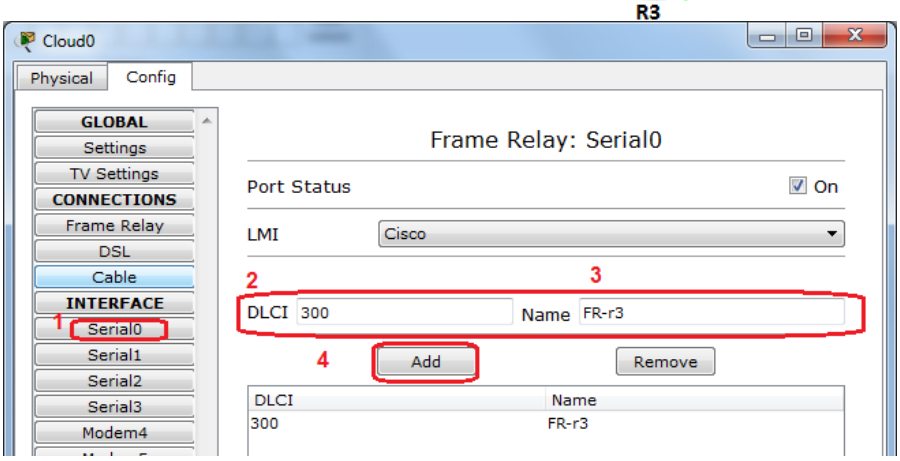
---

**جواب سوال 2:** از پروتکل Frame Relay استفاده نموده و ارتباط Router 1 و Router 3 را با ISP هاي 1 و 2 با استفاده از اطلاعات داده شده راه اندازي نماييد.

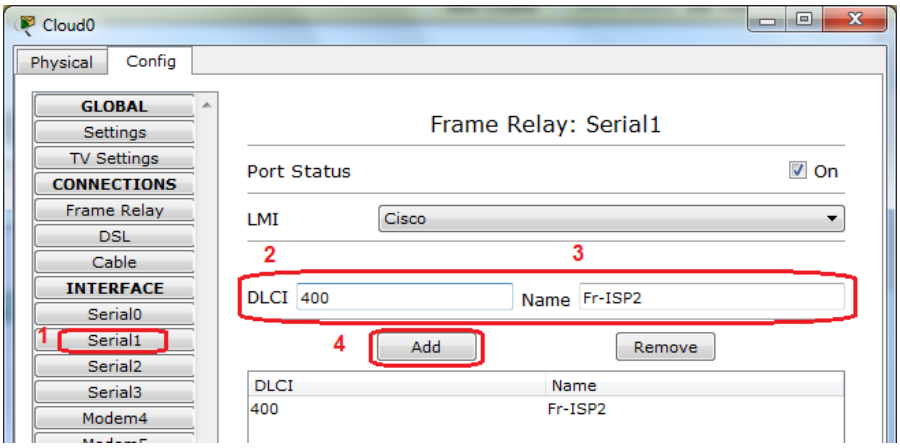



- با توجه به شکل مي بينيم که DLCI 300، از طريق Interface Serial 0 ابر، به ابر متصل شده است و تنظيمات مربوطه را مطابق شکل زير وارد مي کنيم.

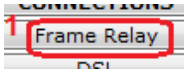



- با توجه به شکل می بینیم که DLCI 400، از طریق Interface Serial 1 ابر، به ابر متصل شده است.

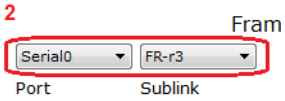



- حال باید ارتباط را برقرار کنیم، همانگونه که در شکل می بینم:

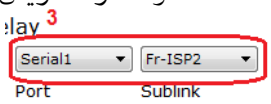



1- وارد قسمت Frame Relay می شویم.

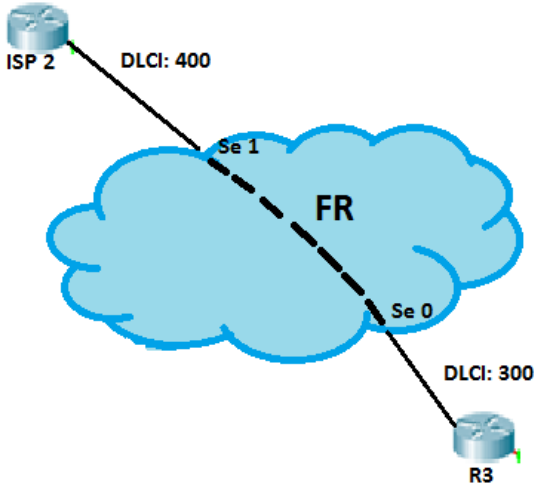
2- روتر R2 از طریق Interface serial 0 به Fr (ابر)متصل شده ایم.

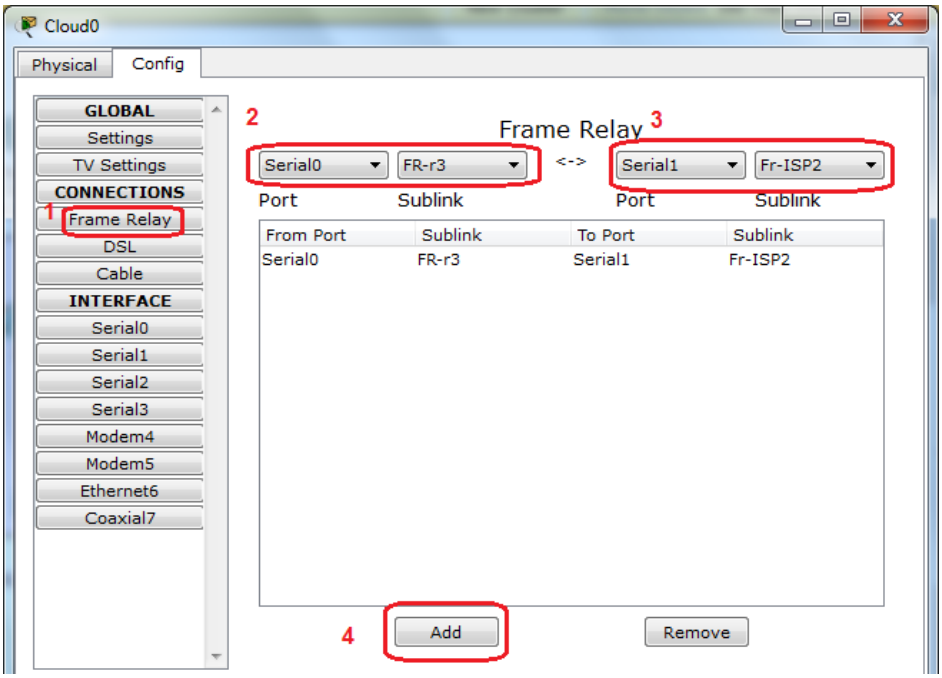


3- و از طریق Interface serial 1 ازFR (ابر) به ISP 2 متصل شده ایم.




4- در قسمت پایین پنجره کلید Add را می زنیم.




**R3:**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**encapsulation frame-relay** |
| 3 | Router(config-if)#**ip address 100.10.1.1 255.255.255.240** |
| 4 | Router(config-if)#**frame-relay map ip 100.10.1.2 300 broadcast** |
| 5 | Router(config-if)#**no sh** |

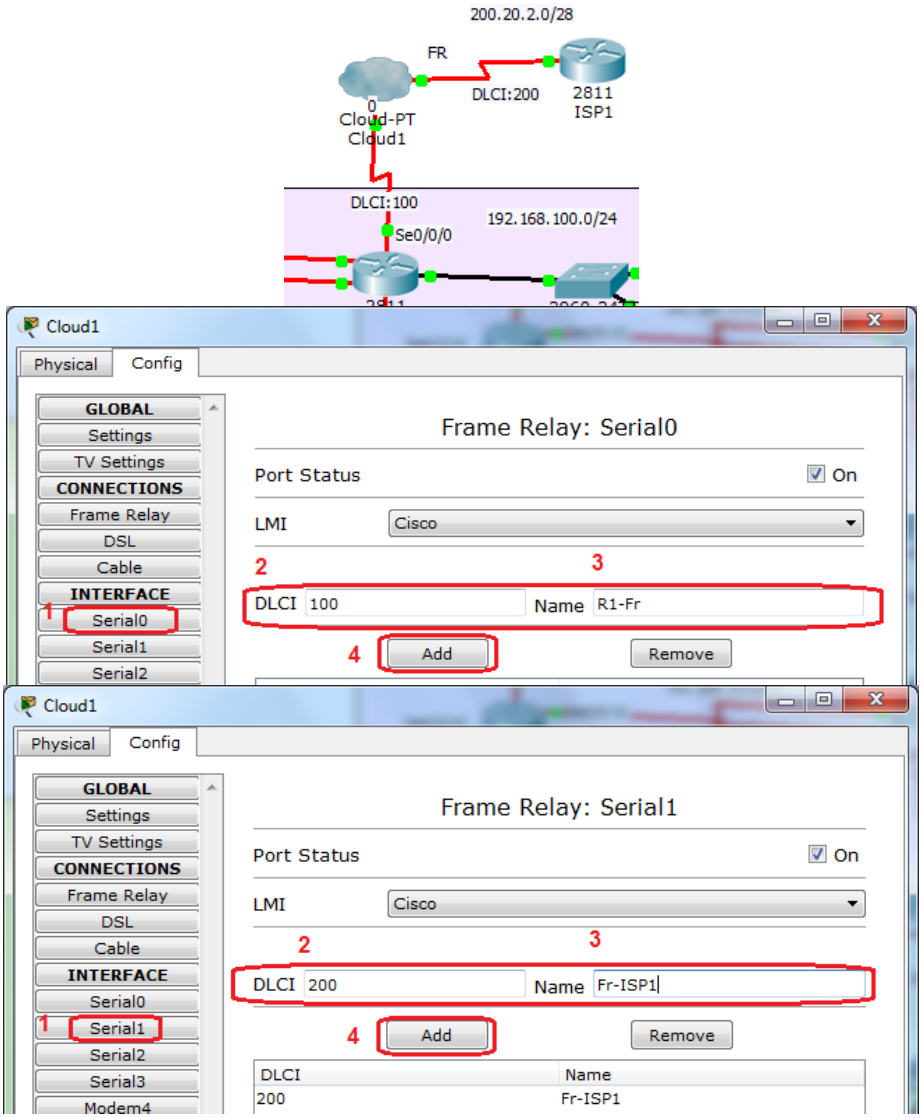
**ISP2:**

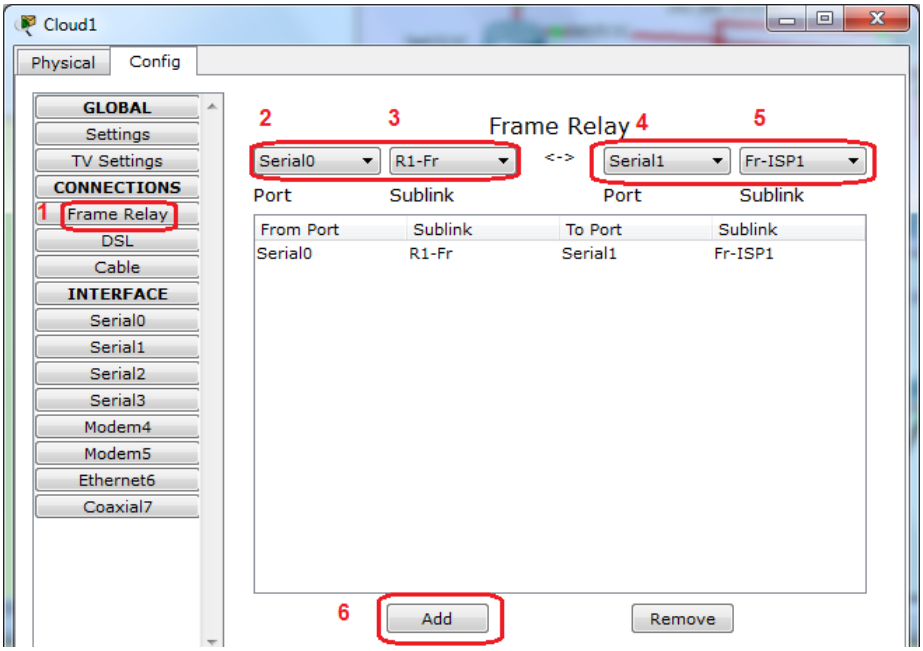
| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**encapsulation frame-relay** |
| 3 | Router(config-if)#**ip address 100.10.1.2 255.255.255.240** |

| | |
|---|---|
| 4 | Router(config-if)#**frame-relay map ip <u>100.10.1.1</u> <u>400</u> broadcast** |
| 5 | Router(config-if)#**no sh** |

Router(config-if)#**frame-relay map ip** **<u>آی پی سمت مقابل</u>** **<u>مبدا</u>DLCI broadcast**

براي قسمت دوم، عينا مشابه بالا عمل مي كنيم:






**R1:**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**encapsulation frame-relay** |
| 3 | Router(config-if)#**ip address 200.20.2.1 255.255.255.240** |
| 4 | Router(config-if)#**frame-relay map ip 200.20.2.1 200 broadcast** |
| 5 | Router(config-if)#**no sh** |

**ISP1:**

| | |
|---|---|
| 1 | Router(config)#**interface serial 0/0/0** |
| 2 | Router(config-if)#**encapsulation frame-relay** |
| 3 | Router(config-if)#**ip address 200.20.2.2 255.255.255.240** |
| 4 | Router(config-if)#**frame-relay map ip 200.20.2.1 200 broadcast** |
| 5 | Router(config-if)#**no sh** |

**جواب سوال 3:** با استفاده از پروتکلهاي مسير يابي داده شده، مطابق با دياگرام به پياده سازي مسيريابي پرداخته و در روتر **4 Redistribution** استفاده نماييد.

راه اندازي پروتکل هاي مسير يابي:

**R1:**

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 192.168.13.2 0.0.0.0 area 0
3  Router(config-router)#network 192.168.31.2 0.0.0.0 area 0
4  Router(config-router)#network 200.20.2.0 0.0.0.15 area 0
5  Router(config-router)#network 192.168.12.1 0.0.0.0 area 0
6  Router(config-router)#network 192.168.100.1 0.0.0.0 area 0
```

**R2:**

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 192.168.12.2 0.0.0.0 area 0
3  Router(config-router)#network 192.168.2.1 0.0.0.0 area 0
```

**R3:**

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 192.168.34.2 0.0.0.0 area 0
3  Router(config-router)#network 192.168.13.1 0.0.0.0 area 0
4  Router(config-router)#network 192.168.31.1 0.0.0.0 area 0
5  Router(config-router)# network 100.10.1.0 0.0.0.15 area 0
```

**R4:**

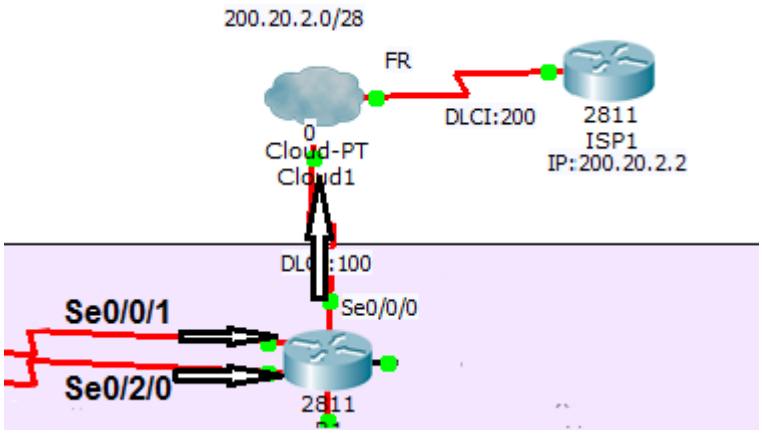
```
1  Router(config)#router eigrp 100
2  Router(config-router)#network 192.168.45.0
3  Router(config-router)# redistribute ospf 1 metric 1 1 1 1 1
4
5  Router(config)#router ospf 1
6  Router(config-router)#network 192.168.34.1 0.0.0.0 area 0
7  Router(config-router)# redistribute eigrp 100 metric 1 subnets
```

**R5:**

```
1  Router(config)#router eigrp 100
2  Router(config-router)#network 192.168.45.0
3  Router(config-router)#network 172.16.5.0
```

**جواب 4: دسترسي PC1 نسبت به ISP1 و دسترسي PC3 نسبت به ISP2 را از طريق PAT مقدور نماييد.**

PC1: 172.16.5.2 ISP1:200.20.2.1




**دسترسي PC1 نسبت به ISP1**

**R1:**

```
1  R1(config)#interface serial 0/0/0
2  R1(config-if)#ip nat outside
3
4  R1(config-if)#int ser 0/0/1
5  R1(config-if)#ip nat inside
6
7  R1(config-if)#int ser 0/2/0
8  R1(config-if)#ip nat inside
9
10 R1(config)#access-list 1 permit 172.16.5.2 0.0.0.0
11 R1(config)#ip nat inside source list 1 interface serial 0/0/0 overload
```

**دسترسي PC3 نسبت به ISP2**

**R3:**

```
1  R3(config)#access-list 1 permit 192.168.2.2 0.0.0.0
2  R3(config)#interface serial 0/2/0
3  R3(config-if)#ip nat inside
4
5  R3(config-if)#interface serial 0/0/1
6  R3(config-if)#ip nat inside
7
8  R3(config-if)#interface serial 0/0/0
9  R3(config-if)#ip nat outside
```

**جواب سوال 5: دسترسي PC2 را نسبت به Server1 كلا مسدود و از طريق Server 2 به طريق Web مقدور نماييد.**

| Source | Access | Destination |
|---|---|---|
| PC2: **172.16.5.3** | **Block** | Server1: **192.168.100.2** |
| PC2: **172.16.5.3** | **Web** | Server2: **192.168.100.3** |

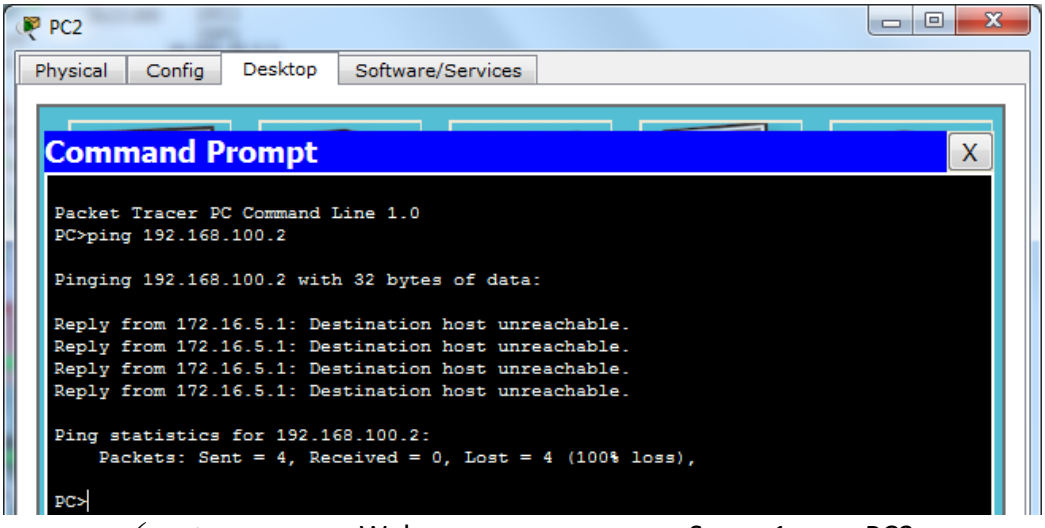
Access List را از نوع Extended مي نويسيم ← بايد در روتر نزديك به Source (مبدا) يعني روتر R5 نوشته شود.
ابتدا دسترسي هايي كه جزئي هستند را مي نويسيم.

```
1  Router(config)#access-list 100 permit tcp host 172.16.5.3 host 192.168.100.3 eq 80
2  Router(config)#access-list 100 deny ip host 172.16.5.3 host 192.168.100.3
3
4  Router(config)#access-list 100 deny ip host 172.16.5.3 192.168.100.2 0.0.0.0
5  Router(config)#access-list 100 permit ip any any
6
7  Router(config)#interface fastEthernet 0/0
8  Router(config-if)#ip access-group 100 in
```

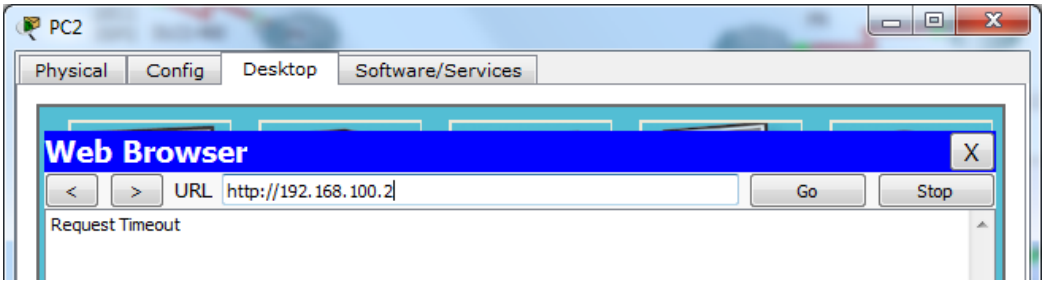
- خط 1: ابتدا دسترسي PC2 را به Server2 از طريق وب باز مي كنيم.
- خط 2: باقي دسترسي هاي PC2 به Server2 را مي بنديم.
- خط 4: كليه ي دسترسي هاي PC2 به Server1 را مي بنديم.
- خط 5: دسترسي را براي باقي سيستم ها باز مي كنيم.
- خط 7: وارد Interface روتر مبدا مي شويم.
- خط 8: و ACL نوشته شده را به ورودي Interface روتر نزديك به مبدا (يعني روتر R5) اعمال مي كنيم.

حال تست مي كنيم:

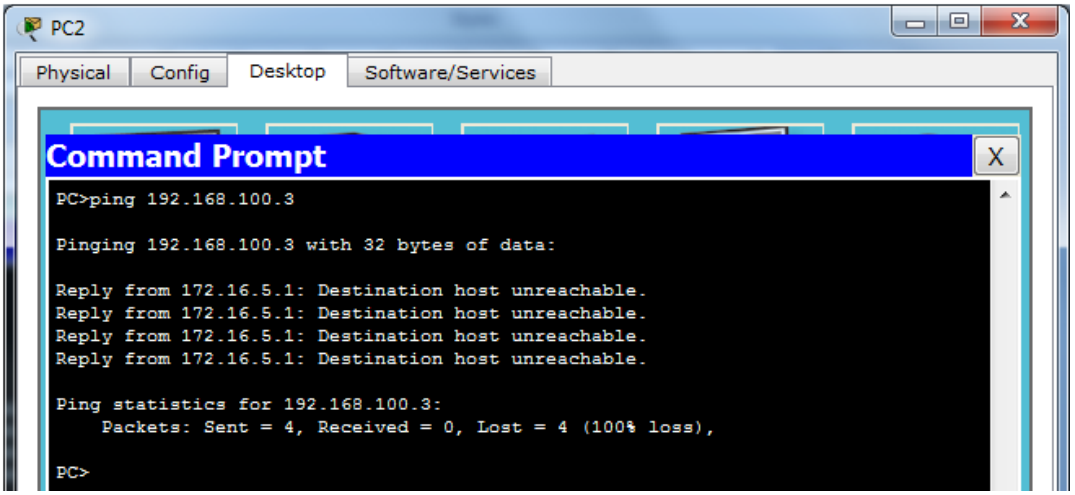
- دسترسي از PC2 به Server1 بايد از طريق Command بسته باشد. ✓



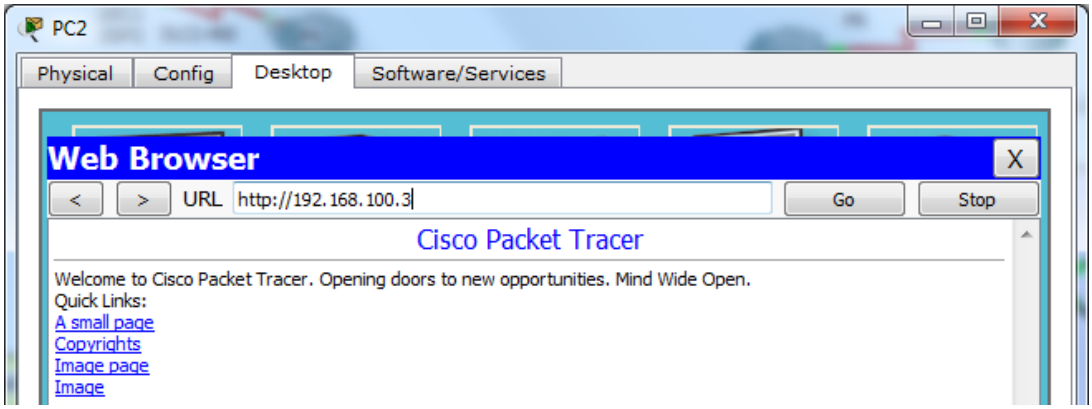

- دسترسي از PC2 به Server1 بايد از طريق Web بسته باشد. ✓



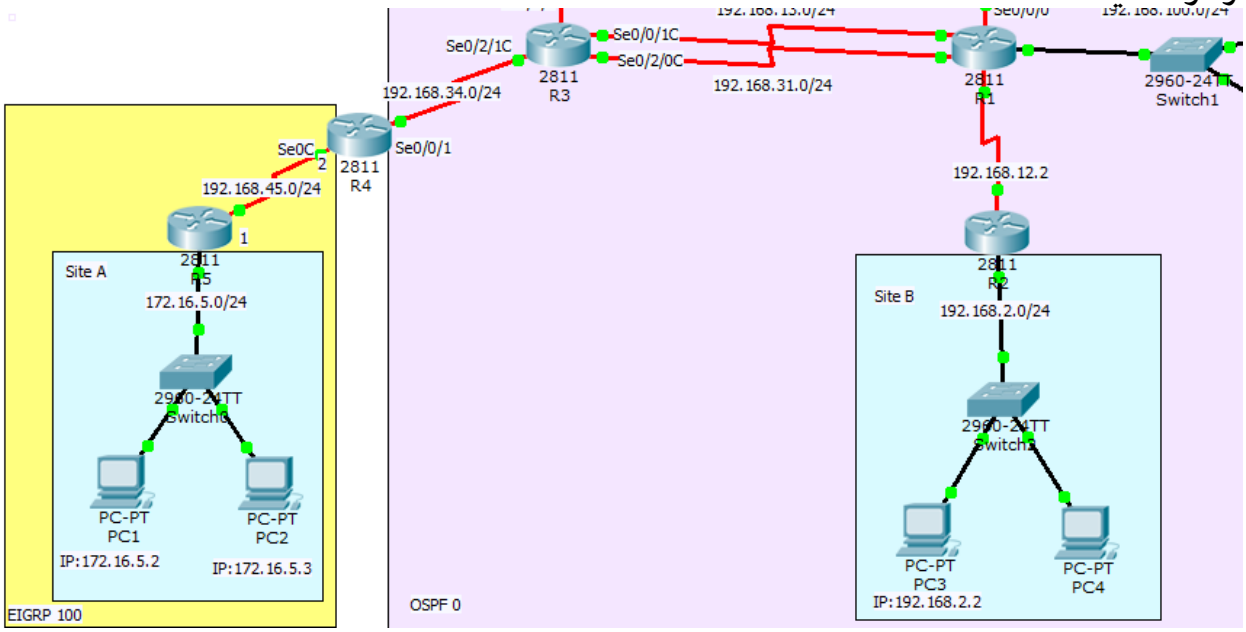

- دسترسي از PC2 به Server2 بايد از طريق Command بسته باشد. ✓




- دسترسي از PC2 به Server2 بايد از طريق Web باز باشد. ✓



**جواب سوال 6: از مکانیزم VPN Site to site به روش IPsec ارتباط سایت A و B را برقرار کنید.**




1- راه اندازي پروتكل هاي مسير يابي كه در بخش 1 راه اندازي شده است.

2- نوشتن ACL مناسب در روترهاي متصل به سايتها (روتر R5 متصل به سايت A و روتر R2 متصل به سايت B)

**R5:**

| | |
|---|---|
| 1 | Router(config)#**access-list 102 permit ip 172.16.5.0 0.0.0.255 192.168.2.0 0.0.0.255** |

Router(config)#**access-list 102 permit ip** ا مبد _ مقصد

**R2:**

| | |
|---|---|
| 1 | Router(config)#**access-list 102 permit ip 192.168.2.0 0.0.0.255 172.16.5.0 0.0.0.255** |

3- نوشتن Policy امنيتي براي مشخص نمودن پروتكلهايي كه در IPsec مي خواهيم از آنها استفاده كنيم. در هر دو روتر R5 و R2 كد زير را مي نويسيم:

**R2, R5:**

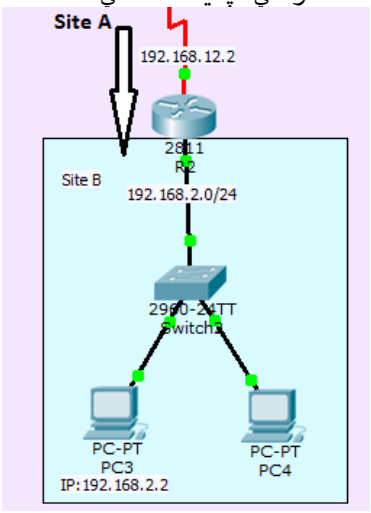
| | |
|---|---|
| 1 | Router(config)#**crypto isakmp policy 10** |
| 2 | Router(config-isakmp)#**authentication pre-share** |
| 3 | Router(config-isakmp)#**encryption aes 256** |
| 4 | Router(config-isakmp)#**group 1** |
| 5 | Router(config-isakmp)#**hash md5** |
| 6 | Router(config-isakmp)#**lifetime 86400** |

4- تعريف رمز مناسب و مشترك بين روترهاي R5 و R2 (روترهاي متصل به سايتهاي مورد نظر)

**R5**:

```
Router(config)#crypto isakmp key pari address 192.168.12.2
```

آي پي Interface روتر مقابل (Inbound) كه از طريق آن سايت A وارد روتر سمت مقابل مي شود و به سايت B دسترسي پيدا مي كند.




در سمت ديگر هم عينا به روش بالا Config مي كنيم:

**R2**

```
Router(config)#crypto isakmp key pari address 192.168.45.1
```

5- تعريف Transform Set مناسب:

**R2, R5:**

```
Router(config)#crypto ipsec transform-set ccna esp-aes 128
```

6- تعريف Crypto Map:

**R5:**

```
1  Router(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer
3        and a valid access list have been configured.
4  Router(config-crypto-map)#match address 102
5  Router(config-crypto-map)#set peer 192.168.12.2
6  Router(config-crypto-map)#set pfs group1
7  Router(config-crypto-map)#set transform-set ccna
8  Router(config-crypto-map)#set security-association lifetime seconds 86400
```

**R2:**

```
1  Router(config)#crypto map VPN 10 ipsec-isakmp
2  % NOTE: This new crypto map will remain disabled until a peer
3        and a valid access list have been configured.
4  Router(config-crypto-map)#match address 102
5  Router(config-crypto-map)#set peer 192.168.45.1
6  Router(config-crypto-map)#set pfs group1
7  Router(config-crypto-map)#set transform-set ccna
8  Router(config-crypto-map)#set security-association lifetime seconds 86400
```

7- اعمال Crypto Map نوشته شده به پورت سريال خروجي روترهاي مورد نظر:

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#crypto map vpn
3  ERROR: Crypto Map with tag vpn does not exist.
4
5  Router(config-if)#crypto map VPN
6  *Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

نكته: حتما بايد به نام Map نوشته شده دقت كنيم. ما در بالا نام Map را VPN (كليه حروف بزرگ هستند) گذاشته ايم و همانگونه كه در خط 3 مشاهده مي نماييد زمانيكه نام مورد نظر را به حروف كوچك نوشتيم پيغام خطا صادر كرد.

8- تست تانل ايجاد شده: براي اينكه اطلاع پيدا كردن از اينكه تانل ايجاد شده درست كار مي كند و پكت ها بين اين دو سايت ارسال مي شوند يا نه ابتدا از هر سايت كامپيوترهاي سايت مقابل را پينگ مي كنيم. سپس با استفاده از Command زير تانل را چك مي كنيم.

```
1  Router#show crypto ipsec sa
.
.  …
10   #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 0
11   #pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 0
.  …
.
```

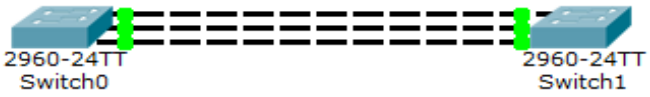
در صورتيكه تانل برقرار باشد و پكت ها بعد از ping كردن، بين دو سايت رد و بدل شده باشد اين مقادير **pkts encaps** ، **pkts encrypt** ، **pkts decaps** و **pkts decrypt** نبايد صفر باشد، در صورتيكه صفر باشد نشان دهنده ي اين است كه تانل ايجاد نشده است.

# EtherChannel Technology

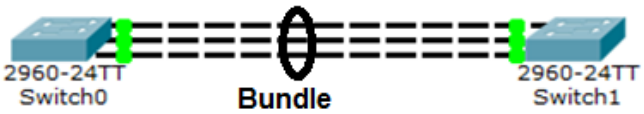
➢ **ساختار EtherChannel در پورت سويچ:**

- در سويچ هاي لايه 2 و لايه 3 به منظور يكپارچه سازي تمامي لينك هاي سوئيچ، براي استفاده از حداكثر ظرفيت ارتباطي مورد استفاده قرار مي گيرد.
- به صورت صورت پيش فرض اگر بين دو سويچ چند مسير وجود داشته باشد(يعني Loopداشته باشيم)، سيستم بصورت اتوماتيك يك مسير را باز مي گذارد و بقيه مسيرها را بلاك مي كند، براي اينكه جلوي بلاك شدن را بگيريم، بايد باقي مسيرهاي موجود را با ادغام (Bundle) كنيم.


- همانگونه كه در شكل مي بينم فقط يكي از مسيرها باز است(دو سمت ارتباط به رنگ سبز است) و دو لينك ديگر تنها يك سر لينك سبز است و سر ديگر ارتباط بلاك (به رنگ نارنجي در آمده) شده است.
- حال اگر اين لينكها را با هم ادغام كنيم ارتباط كليه ي مسيرهاي ادغام شده برقرار مي گردد.




- لينك هاي ادغام شده (Bundle) شده به صورت زير نمايش داده مي شود.




- ادغام چندين پورت سويچ بعنوان يک Logical Link راEtherchannel يا Aggregation يا Bundlingمی نامند كه ميتوانند از 2 تا 8 پورت را با هم ادغام كنند.
- پورت های كه ميخواهند ادغام شوند بايد عضو يک Vlan باشند اگر بعنوان Trunkبخواهند استفاده شوند بايد پورت ها در حالات trunk باشند و حتی Speed و از نظر Duplex آنها بايد يكسان باشند.
- ترافيک به طور مساوی روی لينک ها فرستاده نمی شود بر اساس الگوريتم از يک لينک خاص فرستاده می شوند الگوريتم می تواند.
- EtherChannel Negotiation Protocols، دارای 3 پروتكل است: **LACP –1** **PAGP –2** **Without –3**

| mode | SW1 | SW2 |
|---|---|---|
| **LACP** | Active | Passive |
| **PAGP** | Auto | Desirable |
| **Without** | On | On |

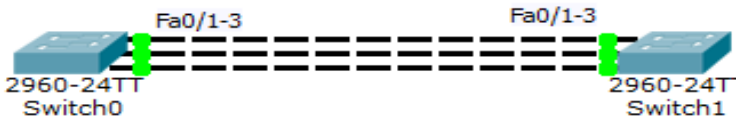
**PAGP:** اين پرو تكل توسط شركت سيسكو ارائه شده است دارای mode 2 است:

- Auto: در اين حالت سويچ به پيغامها یPAGP جواب ميدهد يعنی صبر ميكند تا از او خواسته شود اما ارتباط برقرار نمی شود.
- Desirable: در اين حالت سويچ يک پيغام جهت برقراری ارتباط می فرستد.

نکته: اگر هر دو سمت سویچ در حالت Auto باشند Etherchannel برقرار نمی شود.

**LACP:** توسط IEEE ارائه شده و در انحصار سیسکو نیست لذا بقیه تولیدکنندگان از LACP بصورت استاندارد 802.3ad استفاده میکنند. تا 16 پورت را میتوان در یک Etherchannel گنجاند اما 8 پورت Active و 8 پورت دیگر بقیه بصورت Standby در می آیند و دارای mode 2 است.

- Passive: سویچ صبر میکند تا از او خواسته شود جهت برقراری Etherchannel
- Active: سویچ یک پیغام می فرستد جهت برقراری Etherchanne




Switch 0:

```
1  Switch0(config)#interface port-channel 2
2  Switch0(config-if)#no sh
3
4  Switch0(config)#interface range fastEthernet 0/1-3
5  Switch0(config-if-range)#channel-group 2 mode active
```

Switch 1:

```
1  Switch1(config)#interface port-channel 2
2  Switch1(config-if)#no sh
3
4  Switch1(config)#interface range fastEthernet 0/1-3
5  Switch1(config-if-range)#channel-group 2 mode desirable
```

**Switch0:**

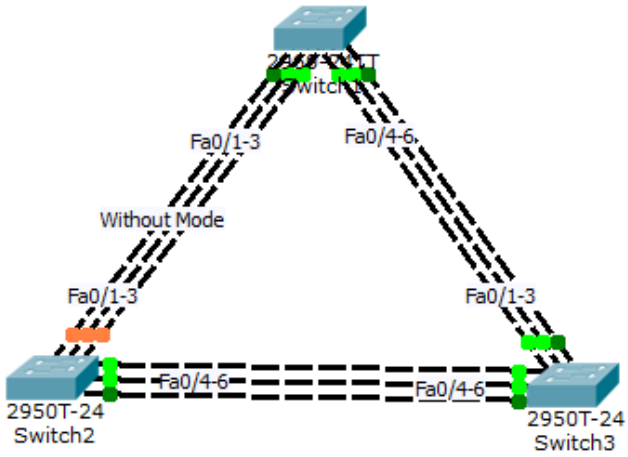
- خط 1: (در اینجا شماره 2) شماره ی دلخواه
  Switch0(config)# interface port-channel
- خط 4: وارد Interface هایي مي شويم كه مي خواهيم در يك گروه قرار دهيم.
- خط 5: مد مورد نظر (در اینجا Active) mode شماره اي كه در خط 1 انتخاب كرده بوديم
  Switch0(config-if-range)# channel-group

**Switch1:**

- خط 1: دقيقا با همان شماره اي كه در سويچ مقابل انتخاب كرده ايم را بايد وارد كنيم (كه در اينجا شماره 2 را انتخاب كرده ايم).
- خط 5:

مد طرف مقابل مطابق جدول (در اینجا desirable) شماره اي كه در خط 1 سويچ اول انتخاب كرده بوديم
Switch1(config-if-range)# channel-group

## سناريو: راه اندازي ساختار EtherChannel




**1- Without Mode:**

**Switch 1 , Port FE 0/1-3**

**Switch 2 , Port FE 0/1-3**

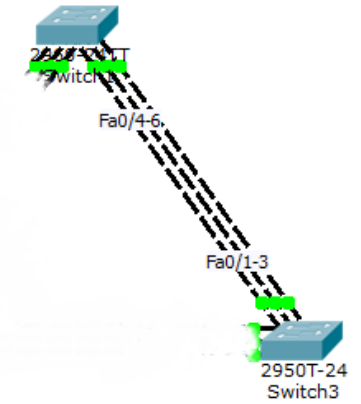
| | |
|---|---|
| 1 | Switch1(config)#**interface port-channel 1** |
| 2 | Switch1(config-if)#**no sh** |
| 3 | |
| 4 | Switch1(config)#**interface range fastEthernet 0/1-3** |
| 5 | Switch1(config-if-range)#**channel-group 1 mode on** |
| | sw2-port 0/1-3 |
| 1 | Switch2(config)#**interface port-channel 1** |
| 2 | Switch2(config-if)#**no sh** |
| 3 | |
| 4 | Switch2(config)#**interface range fastEthernet 0/1-3** |
| 5 | Switch2(config-if -range)#**channel-group 1 mode on** |


**2- PAGP Mode:**

**Switch 1 - Port FE 0/4-6**

**Switch 3 - Port FE 0/1-3**

| | |
|---|---|
| | Sw1- port0/4-6 |
| 1 | Switch1(config)#**interface port-channel 2** |
| 2 | Switch1(config-if)#**no sh** |
| 3 | |
| 4 | Switch1(config)#**interface range fastEthernet 0/4-6** |
| 5 | Switch1(config-if-range)#**channel-group 2 mode auto** |
| | Sw3- port 0/1-3 |
| 1 | Switch(config)#**interface port-channel 2** |
| 2 | Switch(config-if)#**no sh** |



| | | |
|---|---|---|
| 3<br>4<br>5 | Switch(config)#**interface range fastEthernet 0/1-3**<br>Switch(config-if-range)#**channel-group 2 mode desirable** | |

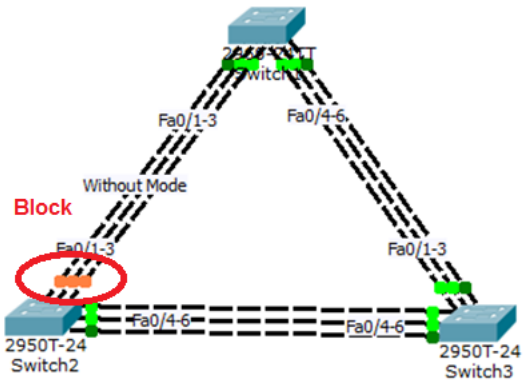
**3- LACP**

**Switch 2 - Port FE 0/4-6**

**Switch 3 - Port FE 0/4-6**

| | | |
|---|---|---|
| | Sw2-port-0/4-6<br>1 Switch2(config)#**interface port-channel 3**<br>2 Switch2(config-if)#**no sh**<br>3<br>4 Switch2(config)#**interface range fastEthernet 0/4-6**<br>5 Switch2(config-if-range)#**channel-group 3 mode passive** |  |
| | Sw 3-port0/4-6<br>1 Switch3(config)#**interface port-channel 3**<br>2 Switch3(config-if)#**no sh**<br>3<br>4 Switch3(config)#**interface range fastEthernet 0/4-6**<br>5 Switch3(config-if-range)#**channel-group 3 mode active** | |

همانطوریکه در شکل اول می بینید به علت به وجود آمدن دور (Loop) ، خود سیستم یکی از مسیرها را مسدود می کند(که در اینجا لینک ارتباطی بین Sw1 و Sw2 را مسدود کرده است.

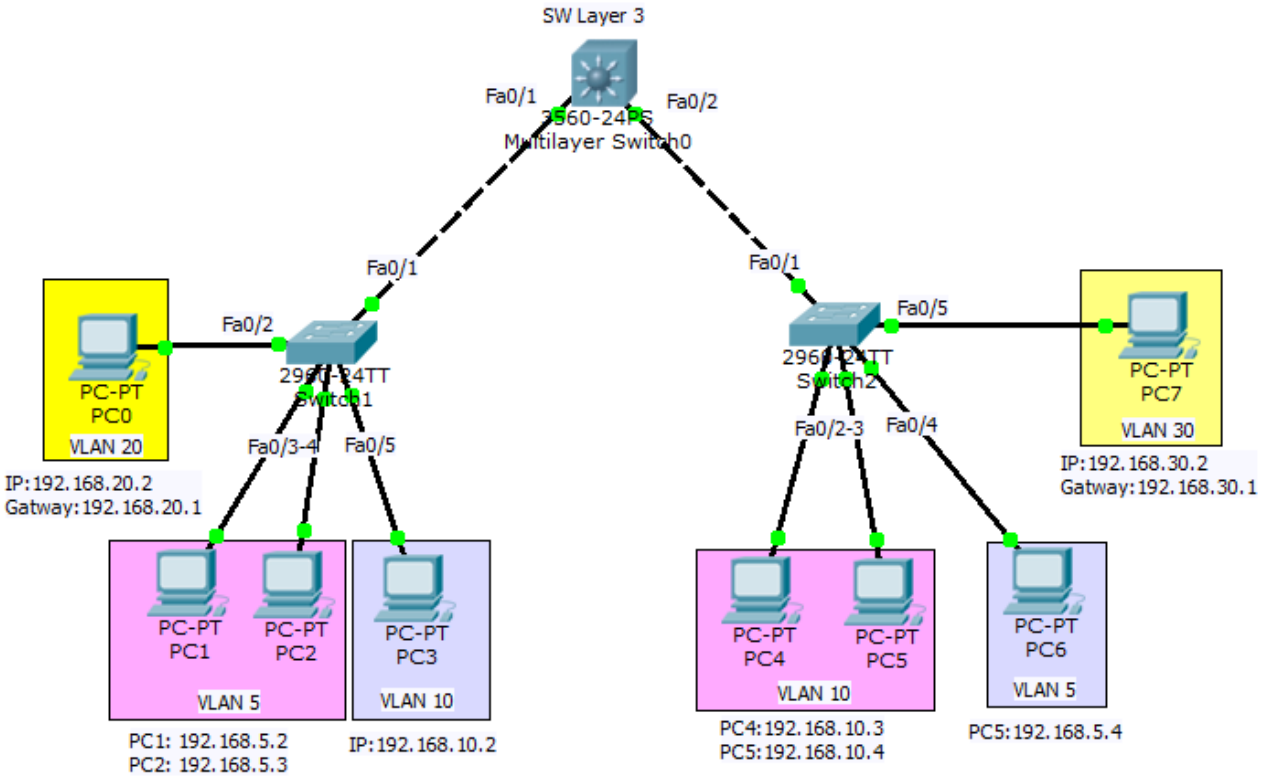



| mode | SW1 | SW2 |
|---|---|---|
| **LACP** | Active | Passive |
| **PAGP** | Auto | Desirable |
| **Without** | On | On |

## سناريو : سويچ لايه 3- VLAN-VTP

- ساختار زير را به گونه اي تنظيم نماييد كه Vlan 20 بتواند Vlan 30 را Ping كند.
- سويچ بالا از نوع سويچ لايه 3 باشد.
- Vtp راه اندازي نماييد. Domain: **cisco.com** و Pass: **ccna**
- رنج IP هاي زير:

Vlan 5: 192.168.5.0/24
Vlan 10: 192.168.10.0/24
Vlan 20: 192.168.20.0/24
Vlan 30: 192.168.30.0/24




**مراحل كار:**

1. **برقراري لينك هاي ترانك بين سويچ ها: ارتباط بين دو سويچ بايد از نوع Trunk تعريف كنيم.**

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport trunk encapsulation dot1q
3  Switch(config-if)#switchport mode trunk
4
5  Switch(config)#interface fastEthernet 0/2
   Switch(config-if)#switchport trunk encapsulation dot1q
   Switch(config-if)#switchport mode trunk
```

براي اينكه در سويچ لايه 3 بخواهيم پورتي را از نوع ترانك تعريف كنيم بايد كامندهاي زير را بنويسيم:
خط 1 الي 7:

Sw3(config)#**interface fastEthernet** **شماره ی اینترفیس مورد نظر**
Sw3(config-if)#**switchport trunk encapsulation dot1q**
Sw3(config-if)#**switchport mode trunk**

**Sw1 , Sw2:**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode trunk** |

**2. تعریف Vtp ( سویچ سرور و سویچ کلاینت ) :**

سویچ لایه ي 3 در اینجا (سویچ بالا) به عنوان سرور است:

**Sw Layer3:**

| | |
|---|---|
| 1 | Switch(config)#**vtp mode server** |
| 2 | Switch(config)#**vtp domain cisco.com** |
| 3 | Switch(config)#**vtp password ccna** |

دو سویچ دیگر به عنوان کلاینت هستند( در این حالت دیگر نیاز نیست Vlan ها را در هر یك از سویچ ها تعریف کنیم و Vlan ها را فقط در سویچ سرور تعریف مي کنیم) :

**Sw 1, Sw2:**

| | |
|---|---|
| 1 | Switch(config)#**vtp mode client** |
| 2 | Switch(config)#**vtp password ccna** |

**3. تعریف Vlan ها در سویچ سرور (سویچ لایه 3) :**

| | |
|---|---|
| 1 | Switch(config)#**vlan 5** |
| 2 | Switch(config-vlan)#**vlan 10** |
| 3 | Switch(config-vlan)#**vlan 20** |
| 4 | Switch(config-vlan)#**vlan 30** |

مشاهده ي Vlan ها در سویچ هاي کلاینت:

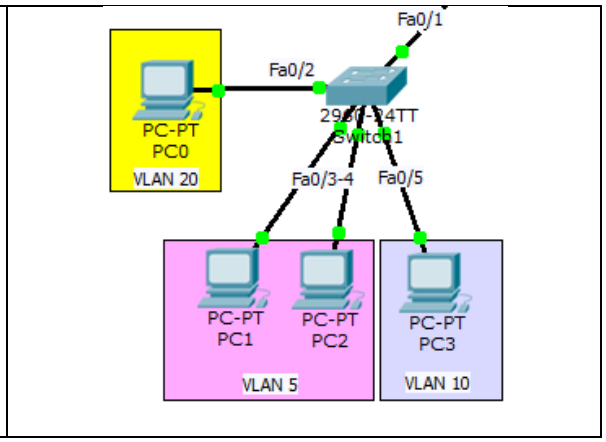
**Sw1, Sw2:**

| | |
|---|---|
| 1 | Switch#**show vlan b** |

قرار دادن کامپیوترها در Vlanهاي مورد نظر:

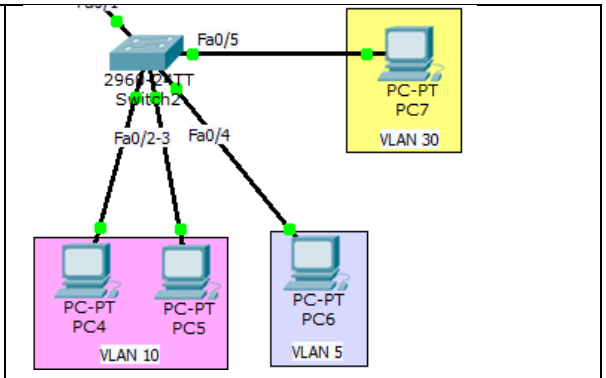
**Sw1:**

| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/2** |
| 2 | Switch(config-if)#**switchport mode access** |
| 3 | Switch(config-if)#**switchport access vlan 20** |
| 4 | |
| 5 | Switch(config)#**interface range fastEthernet 0/3-4** |
| 6 | Switch(config-if-range)#**switchport mode access** |
| 7 | Switch(config-if-range)#**switchport access vlan 5** |
| 8 | |
| 9 | Switch(config)#**interface fastEthernet 0/5** |
| 10 | Switch(config-if)#**switchport mode access** |
| 11 | Switch(config-if)#**switchport access vlan 10** |

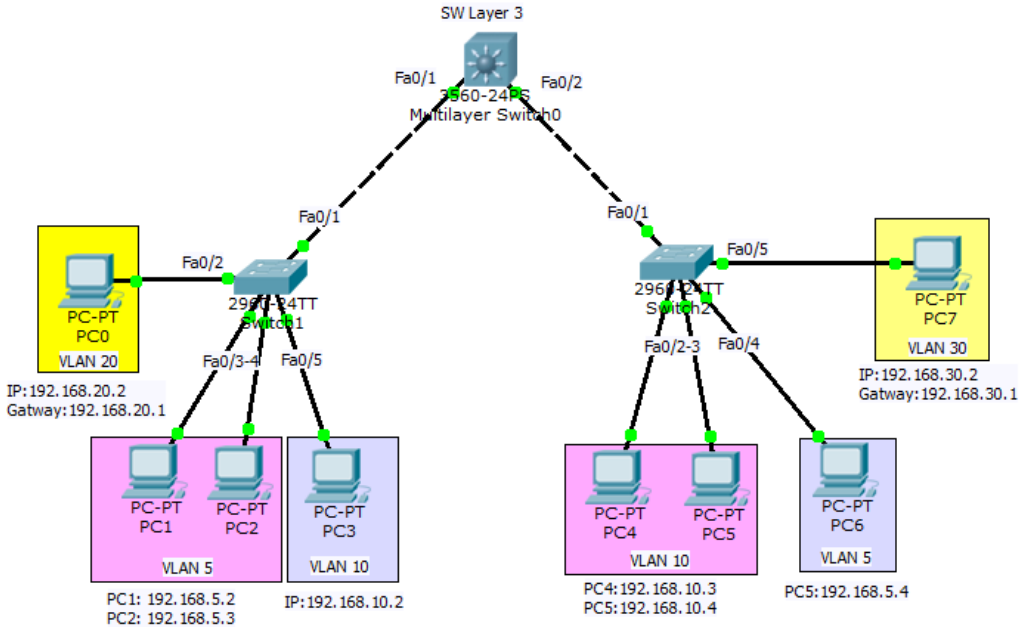



**Sw 3:**

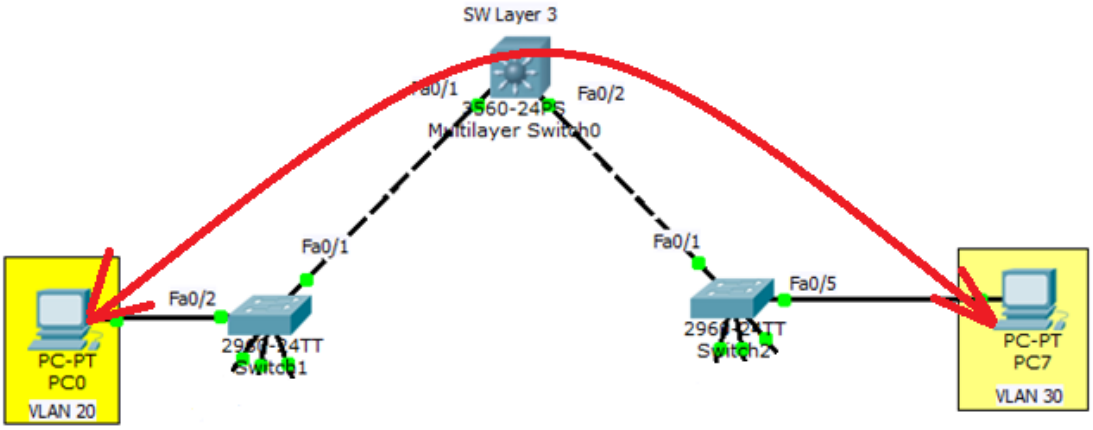
| | |
|---|---|
| 1 | Switch(config)#**interface fastEthernet 0/5** |
| 2 | Switch(config-if)#**switchport mode access** |
| 3 | Switch(config-if)#**switchport access vlan 30** |
| 4 | |
| 5 | Switch(config)#**interface fastEthernet 0/4** |
| 6 | Switch(config-if)#**switchport mode access** |
| 7 | Switch(config-if)#**switchport access vlan 5** |
| 8 | |
| 9 | Switch(config)#**interface range fastEthernet 0/2-3** |
| 10 | Switch(config-if-range)#**switchport mode access** |
| 11 | Switch(config-if-range)#**switchport access vlan 10** |




حال به کامپیوتر ها IP مي دهيم:




**4. ايجاد Interface Vlan :**




**Sw Layer3:**

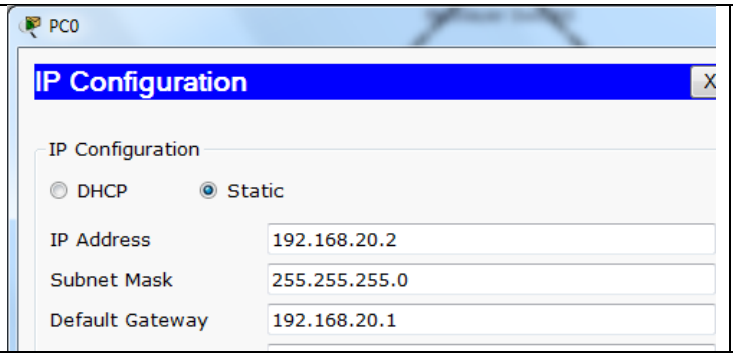
| | |
|---|---|
| 1 | Switch(config)#**interface vlan 20** |
| 2 | Switch(config-if)#**ip address 192.168.20.1 255.255.255.0** |
| 3 | |
| 4 | Switch(config)#**interface vlan 30** |
| 5 | Switch(config-if)#**ip address 192.168.30.1 255.255.255.0** |
| 6 | |
| 7 | Switch(config)#**ip routing** |

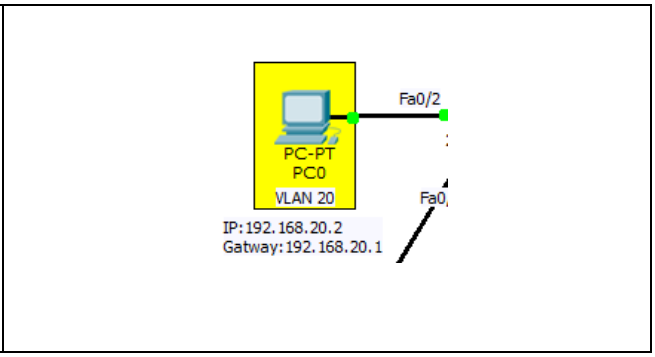
خط 1: براي اينكه دو Vlan با رنج Ip هاي متفاوت را با هم اتصال دهيم بايد ابتدا يك Interface مجازي بسازيم .

خط 2: سپس به اين Interface ساخته شده IP اختصاص مي دهيم. كه اين IP را بايد به عنوان Gateway كامپيوترهاي موجود در Vlan ها ي مربوطه تعريف كنيم :

تعريف Interface Vlan مجازي براي Vlan 20 :

Switch(config)#**interface vlan 20**
Switch(config-if)#**ip address 192.168.20.1 255.255.255.0**




خط 7: سپس با كامند Ip routing ارتباط بين اين دو Vlan غيرهمنام برقرار مي گردد .

**Sw Layer 3:**

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport trunk encapsulation dot1q
3  Switch(config-if)#switchport mode trunk
4
5  Switch(config)#interface fastEthernet 0/2
6  Switch(config-if)#switchport trunk encapsulation dot1q
7  Switch(config-if)#switchport mode trunk
8
9  Switch(config)#vtp mode server
10 Switch(config)#vtp domain cisco.com
11 Switch(config)#vtp password ccna
12
13 Create VLAN:
14 Switch(config)#vlan 5
15 Switch(config-vlan)#vlan 10
16 Switch(config-vlan)#vlan 20
17 Switch(config-vlan)#vlan 30
18
19 Creat Interface VLAN:
20 Switch(config)#interface vlan 20
21 Switch(config-if)#ip address 192.168.20.1 255.255.255.0
22 Switch(config)#interface vlan 30
23 Switch(config-if)#ip address 192.168.30.1 255.255.255.0
24 Switch(config)#ip routing
```

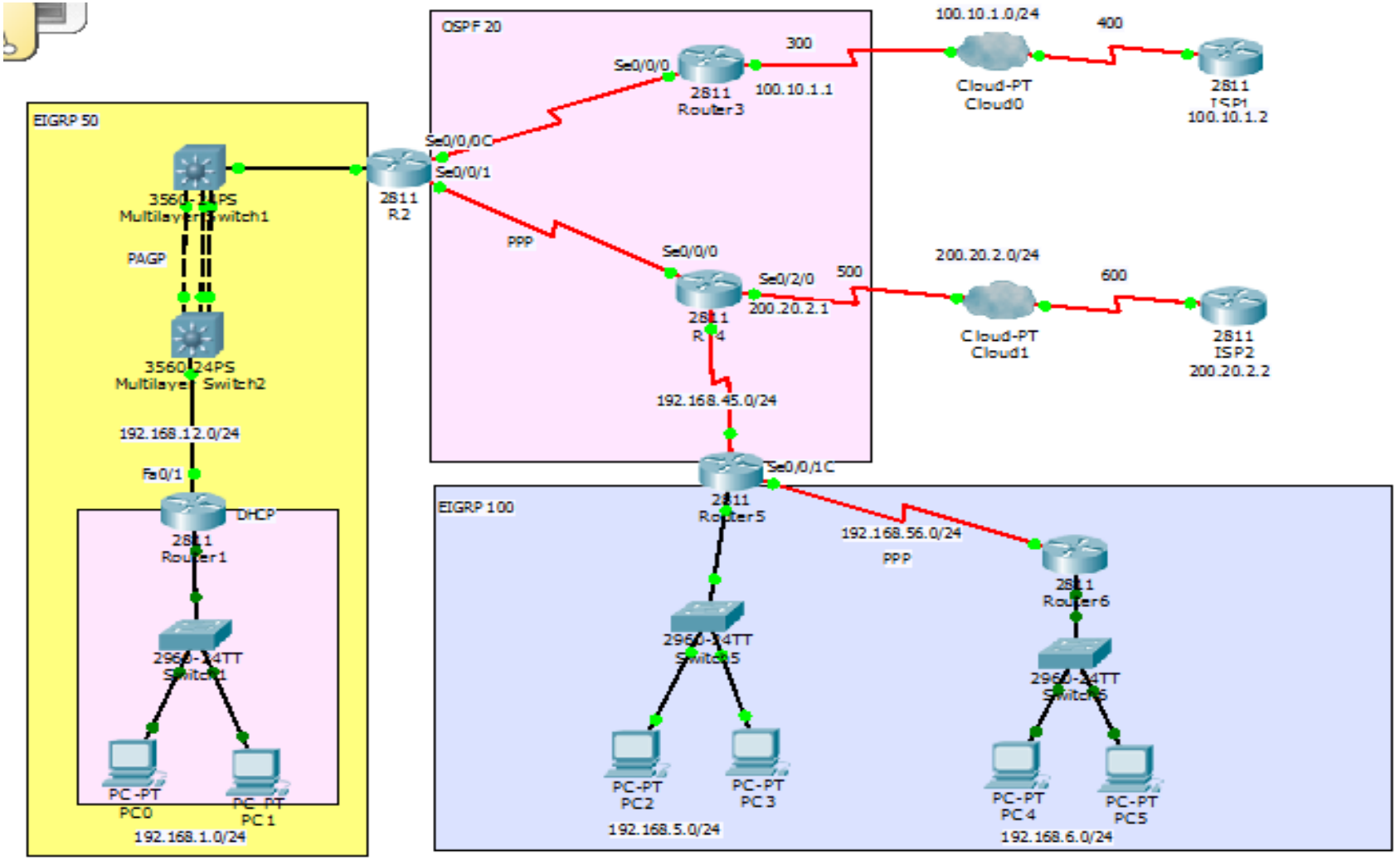
**Sw1:**

```
1  Switch(config)#interface fastEthernet 0/1
2  Switch(config-if)#switchport mode trunk
3
4  Define VTP:
5  Switch(config)#vtp mode client
6  Switch(config)#vtp password ccna
7
8  View VLAM:
9  Switch#show vlan b
10
11 Assign Vlan to interfases:
12 Switch(config)#interface fastEthernet 0/2
13 Switch(config-if)#switchport mode access
14 Switch(config-if)#switchport access vlan 20
15
16 Switch(config)#interface range fastEthernet 0/3-4
17 Switch(config-if-range)#switchport mode access
18 Switch(config-if-range)#switchport access vlan 5
19
```

| | |
|---|---|
| 20 | Switch(config)#**interface fastEthernet 0/5** |
| 21 | Switch(config-if)#**switchport mode access** |
| 22 | Switch(config-if)#**switchport access vlan 10** |

**SW2**

| | |
|---|---|
| 1 | witch(config)#**interface fastEthernet 0/1** |
| 2 | Switch(config-if)#**switchport mode trunk** |
| 3 | |
| 4 | Define VTP: |
| 5 | Switch(config)#**vtp mode client** |
| 6 | Switch(config)#**vtp password ccna** |
| 7 | |
| 8 | Assign Vlan to interfases: |
| 9 | Switch(config)#**interface fastEthernet 0/5** |
| 10 | Switch(config-if)#**switchport mode access** |
| 11 | Switch(config-if)#**switchport access vlan 30** |
| 12 | |
| 13 | Switch(config)#**interface fastEthernet 0/4** |
| 14 | Switch(config-if)#**switchport mode access** |
| 15 | Switch(config-if)#**switchport access vlan 5** |
| 16 | |
| 17 | Switch(config)#**interface range fastEthernet 0/2-3** |
| 18 | Switch(config-if-range)#**switchport mode access** |
| 19 | Switch(config-if-range)#**switchport access vlan 10** |


OSPF 20
EIGRP 50
EIGRP 100
100.10.1.0/24
400
300
Se0/0/0
2811
Router3
100.10.1.1
Cloud-PT
Cloud0
2811
ISP1
100.10.1.2
Se0/0/0C
Se0/0/1
2811
R2
PAGP
PPP
Se0/0/0
Se0/2/0
500
200.20.2.1
200.20.2.0/24
600
Cloud-PT
Cloud1
2811
ISP2
200.20.2.2
192.168.45.0/24
Se0/0/1C
2811
Router5
192.168.56.0/24
PPP
2811
Router6
2960-24TT
Switch5
2960-24TT
Switch6
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
192.168.5.0/24
192.168.6.0/24
3560-24PS
Multilayer Switch1
3560-24PS
Multilayer Switch2
192.168.12.0/24
Fa0/1
DHCP
2811
Router1
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
192.168.1.0/24

**با توجه به دیاگرام به سوالات پاسخ دهید:**

**سوال 1: با IP های داده شده به اختصاص آدرسها پرداخته و سرویس DHCP در روتر 1 پیاده سازی گردد.**

**س 2: ارتباط سویچ های 1 با 2 را با استفاده از پروتکل PAGP پیاده سازی نمایید.**

**س 3: با استفاده از پروتکل PPP ارتباط روتر 2 با 4 و روتر 5 با 6 را راه اندازی نموده و مکانیزم احراز هویت Chap استفاده گردد.**

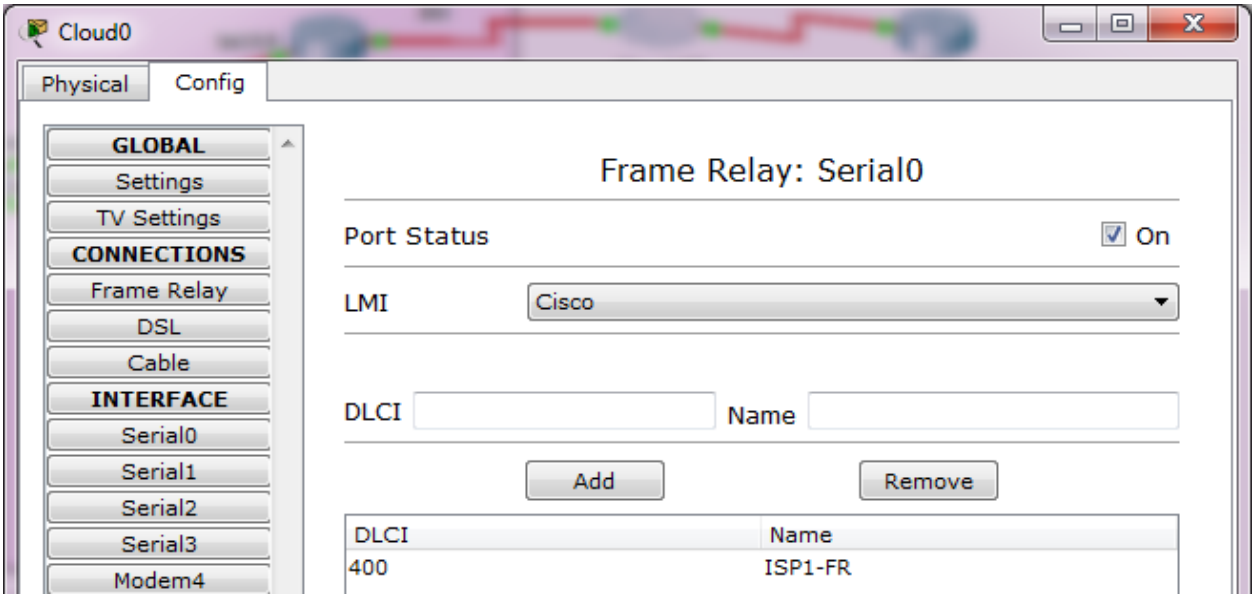
**س 4: پروتکل های مسیریابی مطابق با دیاگرام را پیاده سازی نموده و برای ارتباط روتر 2 با 4 از مکانیزم MD5 با پسورد CCNA و برای ارتباط روتر 2 با 3 از مکانیزم MD5 با پسورد CCNA استفاده نمایید.**

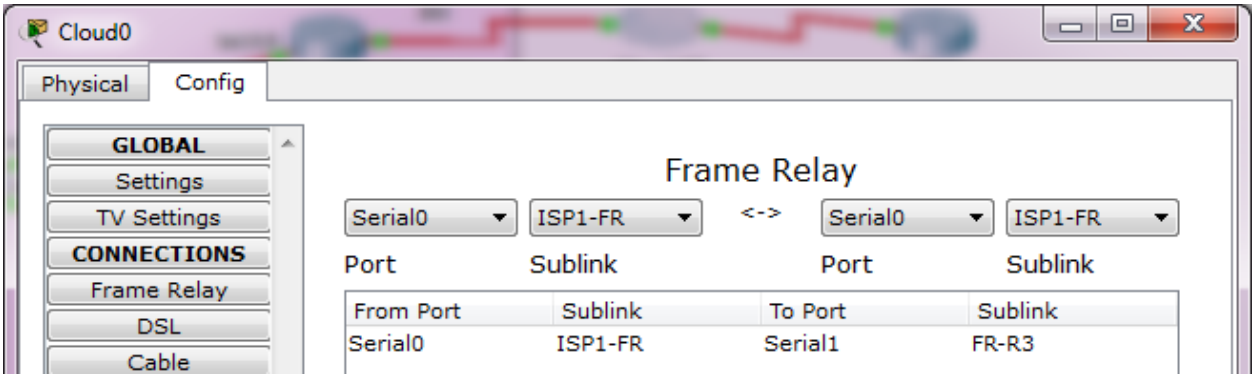
**س 4: دسترسی روترهای 3 و 4 را با ISP برقرار نموده و دسترسی کاربران سویچ 10 را به هر دوی اینها مقدور نمایید.**

---

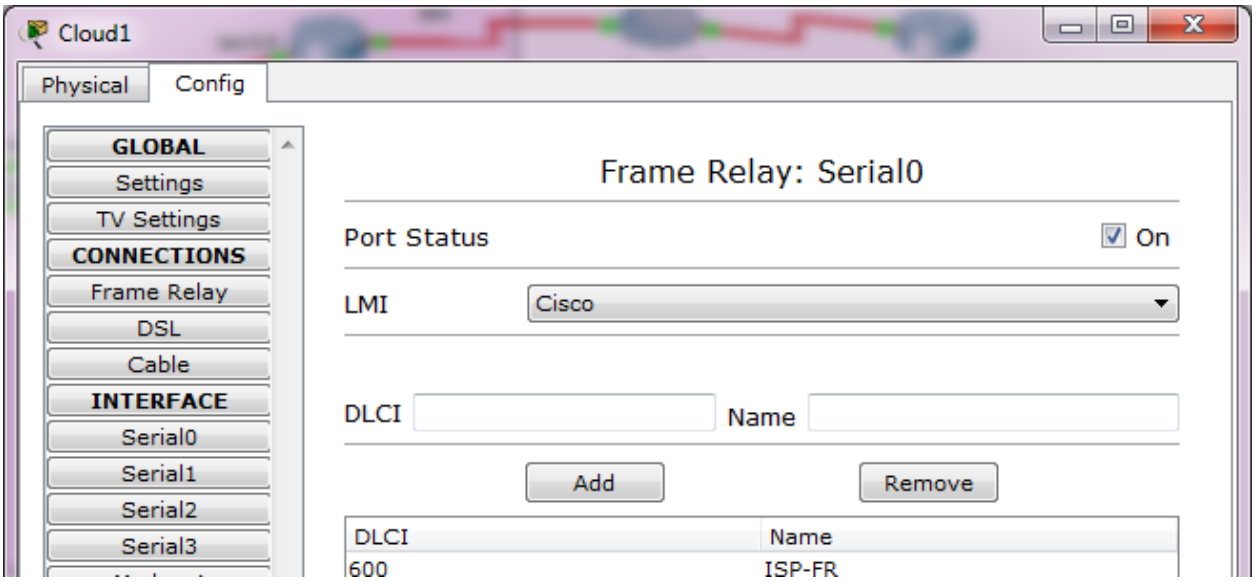
ج 1:

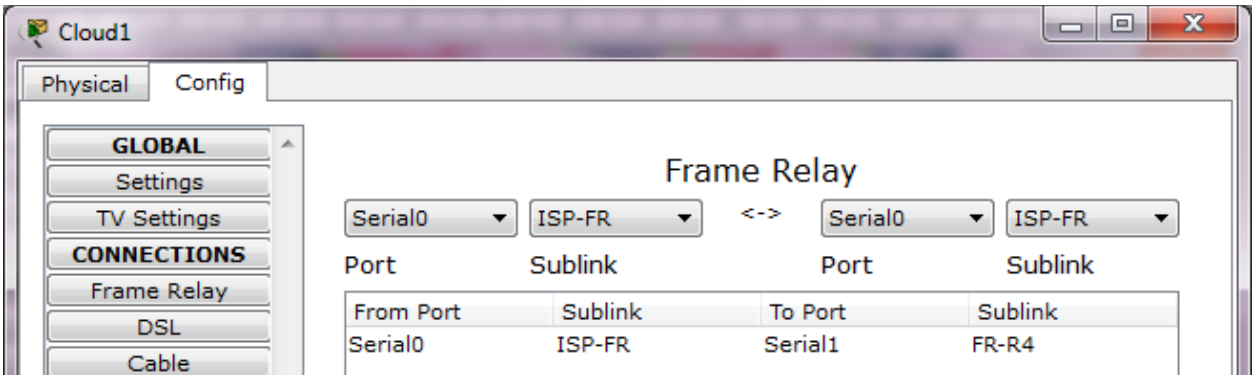
**Cloud 0:**






**Cloud1:**




ج 1:

**R1:**

```
ip dhcp pool test
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 !
interface FastEthernet0/1
```

```
 ip address 192.168.12.1 255.255.255.0
```

**R2:**

```
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
!
!interface Serial0/0/0
 ip address 192.168.23.1 255.255.255.0
  clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.24.1 255.255.255.0
  clock rate 64000
!
```

**R3:**

```
interface Serial0/0/0
 ip address 192.168.23.2 255.255.255.0
 !
interface Serial0/0/1
 ip address 100.10.1.1 255.255.255.0
 !
```

**R4:**

```
hostname R4
!
interface Serial0/0/0
 ip address 192.168.24.2 255.255.255.0
 !
interface Serial0/0/1
 ip address 192.168.45.1 255.255.255.0
 clock rate 64000
!
interface Serial0/2/0
 ip address 200.20.2.1 255.255.255.0
!
```

**R5:**

```
interface FastEthernet0/0
 ip address 192.168.5.1 255.255.255.0
 !
interface Serial0/0/0
 ip address 192.168.45.2 255.255.255.0
!
interface Serial0/0/1
 ip address 192.168.56.1 255.255.255.0
  clock rate 64000
!
```

**R6:**

```
interface FastEthernet0/0
 ip address 192.168.6.1 255.255.255.0
 !
interface Serial0/0/0
 ip address 192.168.56.2 255.255.255.0
```

**ISP1:**

```
interface Serial0/0/0
 ip address 100.10.1.2 255.255.255.0
```

**ISP2:**

```
interface Serial0/0/0
 ip address 200.20.2.2 255.255.255.0
```

ج2: ارتباط با سویچ های 1 با 2 را با استفاده از پروتکل PAGP پیاده سازی نمایید.

**SW1:**

```
interface FastEthernet0/2
 channel-group 1 mode desirable
!
interface FastEthernet0/3
 channel-group 1 mode desirable
!
interface FastEthernet0/4
 channel-group 1 mode desirable
```

**SW2:**

```
interface FastEthernet0/2
 channel-group 1 mode auto
!
interface FastEthernet0/3
 channel-group 1 mode auto
!
interface FastEthernet0/4
 channel-group 1 mode auto
```

ج3: با استفاده از پروتکل ppp ارتباط روتر 2 با 4 و روتر 5 با 6 را راه اندازی نموده و مکانیزم احراز هویت چپ استفاده گردد.

**R2:**

```
hostname R2
!
username R4 password 0 1234
!
!interface Serial0/0/0
 ip ospf authentication message-digest
 ip ospf authentication-key ccna
 !
interface Serial0/0/1
 encapsulation ppp
 ppp authentication chap
 ip ospf authentication message-digest
 ip ospf authentication-key ccnp
```

**R4:**

```
hostname R4
!
username R2 password 0 1234
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
 ip ospf authentication message-digest
 ip ospf authentication-key ccnp
 ip nat inside
```

---

**R5, R6:**

**R5:**

```
hostname R5
!
username R6 password 0 1234
!
interface Serial0/0/1
 encapsulation ppp
 ppp authentication chap
```

**R6:**

```
hostname R6
!
username R5 password 0 1234
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
```

---

**ج4: پروتکل های مسیریابی مطابق با دیاگرام را پیاده سازی نموده و برای ارتباط روتر 2 با 4 از مکانیزم MD5 با پسورد CCNA و برای ارتباط روتر 2 با 3 از مکانیزم MD5 با پسورد CCNA استفاد هنمایید.**

**R1:**

```
router eigrp 50
 network 192.168.1.0
 network 192.168.12.0
```

**R2:**

```
hostname R2
!
username R4 password 0 1234
!
```

```
!interface Serial0/0/0
 ip ospf authentication message-digest
 ip ospf authentication-key ccna
 !
interface Serial0/0/1
 encapsulation ppp
 ppp authentication chap
 ip ospf authentication message-digest
 ip ospf authentication-key ccnp
!
router eigrp 50
 redistribute ospf 1 metric 1 1 1 1 1
 network 192.168.12.0
 !
router ospf 1
 redistribute eigrp 50 metric 1 subnets
 network 192.168.24.1 0.0.0.0 area 20
 network 192.168.23.1 0.0.0.0 area 20
```

**R3:**

```
!
interface Serial0/0/0
 ip ospf authentication message-digest
 ip ospf authentication-key ccna
 ip nat inside
!
interface Serial0/0/1
encapsulation frame-relay
 frame-relay map ip 100.10.1.2 300 broadcast
 ip nat outside
!
router ospf 1
 log-adjacency-changes
 network 192.168.23.2 0.0.0.0 area 20
 network 100.10.1.1 0.0.0.0 area 20
!
ip nat inside source list 1 interface Serial0/0/1 overload!
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

**R4:**

```
hostname R4
!
username R2 password 0 1234
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
 ip ospf authentication message-digest
 ip ospf authentication-key ccnp
 ip nat inside
!
interface Serial0/2/0
 encapsulation frame-relay
 frame-relay map ip 200.20.2.2 500 broadcast
 ip nat outside
!
router ospf 1
 network 192.168.24.2 0.0.0.0 area 20
 network 192.168.45.1 0.0.0.0 area 20
 network 200.20.2.1 0.0.0.0 area 20
!
ip nat inside source list 1 interface Serial0/2/0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

**R5:**

```
hostname R5
!
username R6 password 0 1234
!
interface Serial0/0/1
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
router eigrp 100
 redistribute ospf 1 metric 1 1 1 1 1
 network 192.168.5.0
 network 192.168.56.0
 !
router ospf 1
 redistribute eigrp 100 metric 1 subnets
 network 192.168.45.2 0.0.0.0 area 20
```

**R6:**

```
hostname R6
!
username R5 password 0 1234
!
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
!
router eigrp 100
 network 192.168.6.0
 network 192.168.56.0
```

**ISP1:**

```
interface Serial0/0/0
 ip address 100.10.1.2 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 100.10.1.1 400 broadcast
```

**ISP2:**

```
interface Serial0/0/0
 ip address 200.20.2.2 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 200.20.2.1 600 broadcast
```

---

**ج5: دسترسی روترهای 3 و 4 را با ISP برقرار نموده و دسترسی کاربران سویچ 10 را به هر دوی اینها مقدور نمایید.**

**R3:**

```
!
interface Serial0/0/0
 ip ospf authentication message-digest
 ip ospf authentication-key ccna
 ip nat inside
!
interface Serial0/0/1
encapsulation frame-relay
 frame-relay map ip 100.10.1.2 300 broadcast
 ip nat outside
!
ip nat inside source list 1 interface Serial0/0/1 overload!
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

**R4:**

```
interface Serial0/0/0
 encapsulation ppp
 ppp authentication chap
 ip ospf authentication message-digest
 ip ospf authentication-key ccnp
 ip nat inside
!
interface Serial0/2/0
 encapsulation frame-relay
 frame-relay map ip 200.20.2.2 500 broadcast
 ip nat outside
!
ip nat inside source list 1 interface Serial0/2/0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

**R5:**

```
hostname R5
!
username R6 password 0 1234
!
interface Serial0/0/1
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
router eigrp 100
 redistribute ospf 1 metric 1 1 1 1 1
 network 192.168.5.0
 network 192.168.56.0
 !
router ospf 1
 redistribute eigrp 100 metric 1 subnets
 network 192.168.45.2 0.0.0.0 area 20
```

**R6:**

```
hostname R6
!
username R5 password 0 1234
!
interface Serial0/0/0
 encapsulation ppp
```

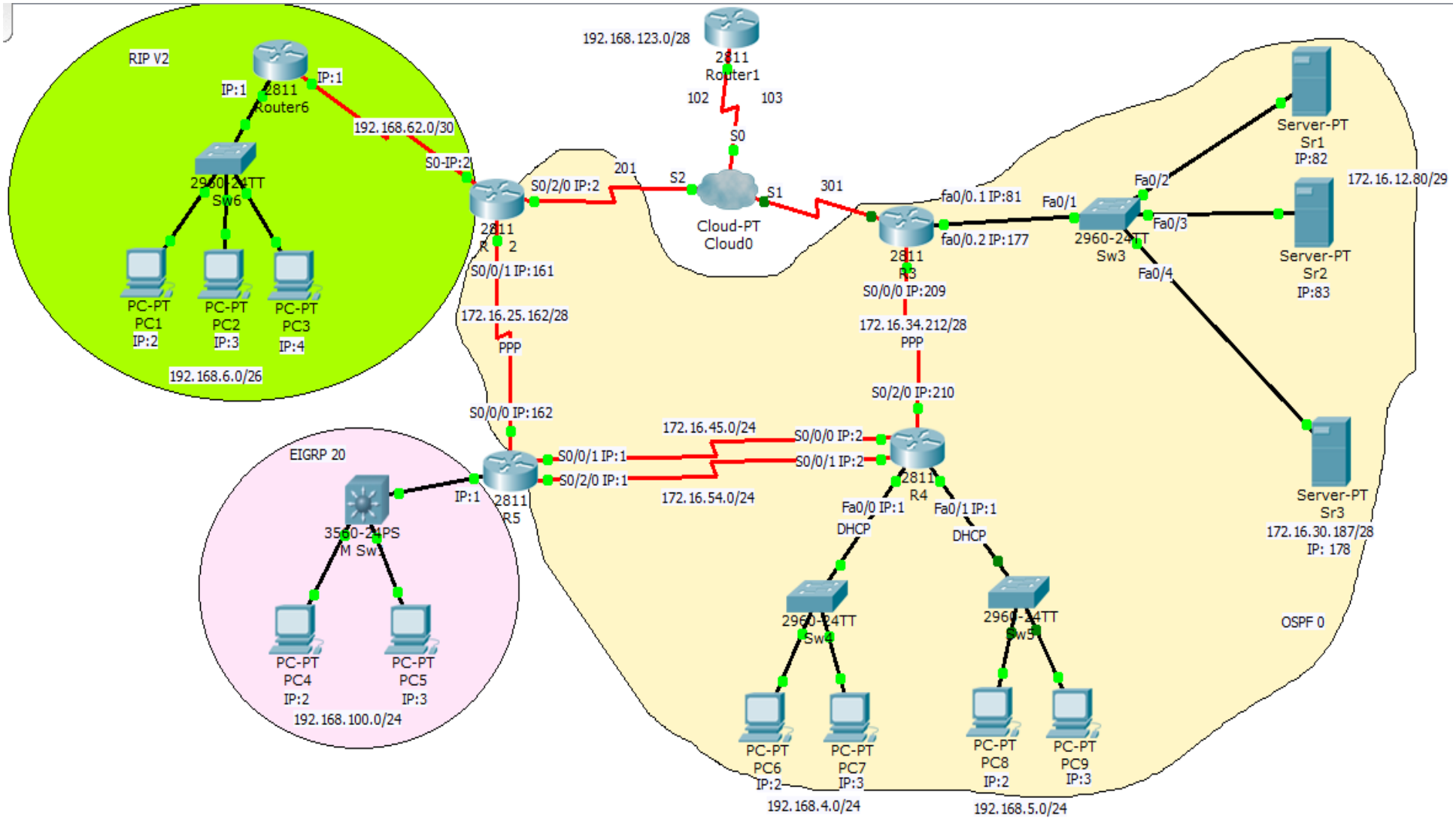
```
 ppp authentication chap
!
router eigrp 100
 network 192.168.6.0
 network 192.168.56.0
```

**ISP1:**

```
interface Serial0/0/0
 ip address 100.10.1.2 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 100.10.1.1 400 broadcast
```

**ISP2:**

```
interface Serial0/0/0
 ip address 200.20.2.2 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 200.20.2.1 600 broadcast
```


RIP V2
IP:1
2811
Router6
IP:1
192.168.62.0/30
S0-IP:2
2960-24TT
Sw6
PC-PT
PC1
IP:2
PC-PT
PC2
IP:3
PC-PT
PC3
IP:4
192.168.6.0/26
192.168.123.0/28
2811
Router1
102
103
S0
201
S2
Cloud-PT
Cloud0
S1
301
S0/2/0 IP:2
2811
R
2
S0/0/1 IP:161
172.16.25.162/28
PPP
S0/0/0 IP:162
EIGRP 20
IP:1
3560-24PS
M Sw
PC-PT
PC4
IP:2
PC-PT
PC5
IP:3
192.168.100.0/24
2811
R5
S0/0/1 IP:1
S0/2/0 IP:1
172.16.45.0/24
172.16.54.0/24
S0/0/0 IP:2
S0/0/1 IP:2
2811
R4
Fa0/0 IP:1
DHCP
Fa0/1 IP:1
DHCP
2960-24TT
Sw4
2960-24TT
Sw5
PC-PT
PC6
IP:2
PC-PT
PC7
IP:3
192.168.4.0/24
PC-PT
PC8
IP:2
PC-PT
PC9
IP:3
192.168.5.0/24
fa0/0.1 IP:81
fa0/0.2 IP:177
2811
R3
S0/0/0 IP:209
172.16.34.212/28
PPP
S0/2/0 IP:210
Fa0/1
2960-24TT
Sw3
Fa0/2
Fa0/3
Fa0/4
Server-PT
Sr1
IP:82
Server-PT
Sr2
IP:83
172.16.12.80/29
Server-PT
Sr3
172.16.30.187/28
IP: 178
OSPF 0

س1: با استفاده از IP هاي داده شده به اختصاص آدرسها پرداخته و در روتر 4 سرويس DHCP براي سوييچ هاي 4و 5 پياده سازي گردد.

س 2:از پروتكل PPP براي ارتباط روتر 3 با 4 و روتر 2 با 5 استفاده شده و از ارتباط روتر 3 با 4 با مكانيزم احراز هويتChap پياده سازي گردد.
س 3: براي روتر هاي R3,R2,R1 پروتكلهاي Frame relay به روش ها؟؟؟ اسپك پياده سازي شده و از DLCI هاي داده شده استفاده گردد.
س4: پروتكلهاي مسيريابي مطابق شكل پياده سازي گردد و براي ارتباط روتر 3 و 4 از مكانيزم MD5 استفاده گردد.

س 5: دسترسي PC1 به سرور 1 از طريق Web و به سرور 2 از طريق پروتكل ICMP و نسبت به سرور 3 كلا مسدود باشد.
س 6: قابليت SSH نسبت به روتر 2 براي PC2,5,6 كلا مسدود باشد.

**ج 1: با استفاده از IP هاي داده شده به اختصاص آدرسها پرداخته و در روتر 4 سرويس DHCP براي سويچ هاي 4و 5 پياده سازي گردد.**

ابتدا Subnetها را محاسبه مي كنيم.

**Sw6:**

**192.168.6.0/27**

**S:**

| | | | |
|---|---|---|---|
| 8 | 8 | 8 | 3 |
| 255. | 255. | 255. | 224 |
| 11111111 | 11111111 | 11111111 | 11100000 |

**Net-ID: 192.168.6.0**
**Net-Mask: 255.255.255.224**

255-31=224

---

**R1,R3:**

**192.168.123.0/28**

**S:**

| | | | |
|---|---|---|---|
| 8 | 8 | 8 | 4 |
| 255. | 255. | 255. | 240 |
| 11111111 | 11111111 | 11111111 | 11110000 |

**Net-ID: 192.168.123.0**
**Net-Mask: 255.255.255.240**

255-15=240

---

**R1,R6:**

**192.168.62.0/30**

**S:**

| | | | |
|---|---|---|---|
| 8 | 8 | 8 | 6 |
| 255. | 255. | 255. | 224 |
| 11111111 | 11111111 | 11111111 | 11111100 |

**Net-ID: 192.168.62.0**
**Net-Mask: 255.255.255.252**

255-3=252

---

**R2,R5:**

**172.16.25.162/28**

**S:**

| | | | |
|---|---|---|---|
| 8 | 8 | 8 | 4 |
| 255. | 255. | 255. | 240 |
| 11111111 | 11111111 | 11111111 | 11110000 |

**Net-ID: 172.16.25.160**
**Net-Mask: 255.255.255.240**

255-15=240

1. $2^4 = 16\ Subnets$
2. $2^4 - 2 = 14\ Host$

3. $256 - 240 = 16\ Step$
4. .

| Step 16 | 16×0 | 16×1 | 16×2 | | 16×10 | 16×11 |
|---|---|---|---|---|---|---|
| Net_ID | 0 | 16 | 32 | | 160 | 176 |
| First | | | | | 161 | |
| 2th | | | | | 162 | |
| Last | | | | | 174 | |
| Broadcast | | | | | 175 | |

---

**R3,R4:**

**172.16.34.212/28**

**S:**

| 8 | 8 | 8 | 4 |
|---|---|---|---|
| 255. | 255. | 255. | 240 |
| 11111111 | 11111111 | 11111111 | 11110000 |

**Net-ID: 172.16.25.208**
**Net-Mask: 255.255.255.240**

255-15=240

1. $2^4 = 16\ Subnets$
2. $2^4 - 2 = 14\ Host$
3. $256 - 240 = 16\ Step$
4. .

| Step 16 | 16×0 | 16×1 | 16×2 | | 16×13 | 16×14 |
|---|---|---|---|---|---|---|
| Net_ID | 0 | 16 | 32 | | 208 | 224 |
| First | | | | | 209 | |
| … | | | | | 212 | |
| Last | | | | | 222 | |
| Broadcast | | | | | 223 | |

---

**Server 1, Server2:**

**172.16.12.80/29**

**S:**

| 8 | 8 | 8 | 4 |
|---|---|---|---|
| 255. | 255. | 255. | 248 |
| 11111111 | 11111111 | 11111111 | 11111000 |

**Net-ID: 172.16.12.80**
**Net-Mask: 255.255.255.248**

255-7=248

1. $2^5 = 32\ Subnets$
2. $2^3 - 2 = 6\ Host$
3. $256 - 248 = 8\ Step$
4. .

| Step 16 | 8×0 | 8×1 | 8×2 | … | 8×10 | 8×11 |
|---|---|---|---|---|---|---|
| Net_ID | 0 | 8 | 18 | … | 80 | 88 |
| First | | | | … | 81 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **…** | | | | … | | |
| **Last** | | | | … | **86** | |
| **Broadcast** | | | | … | **87** | |

---

**Server3**

**172.16.30.187/28**

**S:**

| | | | |
|---|---|---|---|
| 8 | 8 | 8 | 4 |
| 255. | 255. | 255. | 240 |
| 11111111 | 11111111 | 11111111 | 11110000 |

**Net-ID: 172.16.30.176**

**Net-Mask: 255.255.255.240**

255-15=240

1. $2^4 = 16\ Subnets$
2. $2^4 - 2 = 14\ Host$
3. $256 - 240 = 16\ Step$
4. .

| **Step 16** | **16×0** | **16×1** | **16×2** | | **16×11** | **16×12** |
|---|---|---|---|---|---|---|
| **Net_ID** | 0 | 16 | 32 | | **176** | 192 |
| **First** | | | | | **177** | |
| **…th** | | | | | **187** | |
| **Last** | | | | | **…** | |
| **Broadcast** | | | | | **191** | |

---

**اختصاص IP به Interface ها :**

**R6**

```
1  Router(config)#interface fastEthernet 0/0
2  Router(config-if)#ip add 192.168.6.1 255.255.255.224
3  Router(config-if)#no sh
4
5  Router(config)#interface serial 0/0/0
6  Router(config-if)#ip address 192.168.62.1 255.255.255.252
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no sh
```

**R2:**

```
1  Router(config)#interface serial 0/0/0
2  Router(config-if)#ip address 192.168.62.2 255.255.255.252
3  Router(config-if)#no sh
4
5  Router(config-if)#inte ser 0/0/1
6  Router(config-if)#ip address 172.16.25.161 255.255.255.240
```

```
8  Router(config-if)#clock rate 64000
9  Router(config-if)#no sh
```

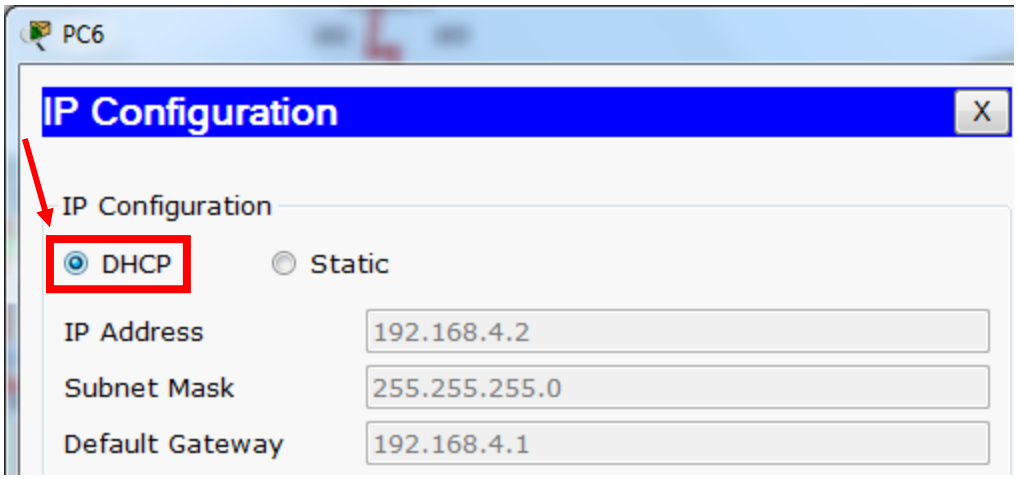
**R5:**

```
1  Router(config-if)#int fa 0/0
2  Router(config-if)#ip add 192.168.100.1 255.255.255.0
3  Router(config-if)#no sh
4
5  Router(config)#interface serial 0/0/0
6  Router(config-if)#ip address 172.16.25.162 255.255.255.240
8  Router(config-if)#no sh
9
10 Router(config-if)#in ser 0/0/1
11 Router(config-if)#ip add 172.16.45.1 255.255.255.0
12 Router(config-if)#clock rate 64000
13 Router(config-if)#no sh
14
15 Router(config-if)#int ser 0/2/0
16 Router(config-if)#ip add 172.16.54.1 255.255.255.0
17 Router(config-if)#clock rate 64000
18 Router(config-if)#no sh
```

**R4**

```
1  Router(config)#int ser 0/0/0
2  Router(config-if)#ip add 172.16.45.2 255.255.255.0
3  Router(config-if)#no sh
4
5  Router(config-if)#int ser 0/0/1
6  Router(config-if)#ip add 172.16.54.2 255.255.255.0
8  Router(config-if)#no sh
9
10 Router(config-if)#int ser 0/2/0
11 Router(config-if)#ip add 172.16.34.210 255.255.255.240
12 Router(config-if)#no sh
13
14 Router(config-if)#int fa 0/0
15 Router(config-if)#ip add 192.168.4.1 255.255.255.0
16 Router(config-if)#no sh
17
18 Router(config-if)#int fa 0/1
19 Router(config-if)#ip add 192.168.5.1 255.255.255.0
20 Router(config-if)#no sh
21
22 DHCP Sw4
23 Router(config)#ip dhcp pool Test1
24 Router(dhcp-config)#network 192.168.4.2 255.255.255.0
```

```
25  Router(dhcp-config)#default-router 192.168.4.1
26
27  DHCP Sw5
28  Router(config)#ip dhcp pool Test2
29  Router(dhcp-config)#network 192.168.5.2 255.255.255.0
30  Router(dhcp-config)#default-router 192.168.5.1
```




**SW3:**

```
1   Switch(config)#vlan 10
2   Switch(config-vlan)#vlan 20
3
4   Switch(config)#interface range fa 0/2-3
5   Switch(config-if-range)#switchport mode access
6   Switch(config-if-range)#switchport access vlan 10
8
9   Switch(config)#int fa 0/4
10  witch(config-if)#switchport mode access
11  Switch(config-if)#switchport access vlan 20
12
13  Switch(config-if)#int fa 0/1
14  Switch(config-if)#switchport mode trunk
15
```

**R3:**

```
1   Router(config)#interface ser 0/0/0
2   Router(config-if)#ip add 172.16.34.209 255.255.255.240
3   Router(config-if)#clock rate 64000
4
5   Router(config-if)#interface fastEthernet 0/0.1
6   Router(config-subif)#encapsulation dot1Q 10
8   Router(config-subif)#ip add 172.16.12.81 255.255.255.248
9
10  Router(config)#interface fastEthernet 0/0.2
```

```
11  Router(config-subif)#encapsulation dot1Q 20
12  Router(config-subif)#ip add 172.16.30.177 255.255.255.240
13
14  Router(config)#interface fa 0/0
15  Router(config-if)#no sh
```

---

**ج 2:از پروتکل PPP براي ارتباط روتر 3 با 4 و روتر 2 با 5 استفاده شده و از ارتباط روتر 3 با 4 با مکانیزم احراز هویتChap پیاده سازي گردد.**

**R3⇨R4: PPP Protocol & Chap Authentication**

**R3:**

```
1  Router(config)#hostname r3
2  r3(config)#username r4 password 123
3
4  r3(config)#interface serial 0/0/0
5  r3(config-if)#encapsulation ppp
6  r3(config-if)#ppp authentication chap
7  r3(config-if)#no sh
```

**R4:**

```
1  Router(config)#hostname r4
2  r4(config)#username r3 password 123
3
4  r4(config)#interface se 0/2/0
5  r4(config-if)#encapsulation ppp
6  r4(config-if)#ppp authentication chap
7  r4(config-if)#no sh
```

**R2⇨R5: PPP Protocol**

**R2:**

```
1  Router(config)#hostname r2
2  r2(config)#username r5 password 123
3
4  r2(config)#int ser 0/0/0
5  r2(config-if)#encapsulation ppp
6  r2(config-if)#no sh
```

**R5:**

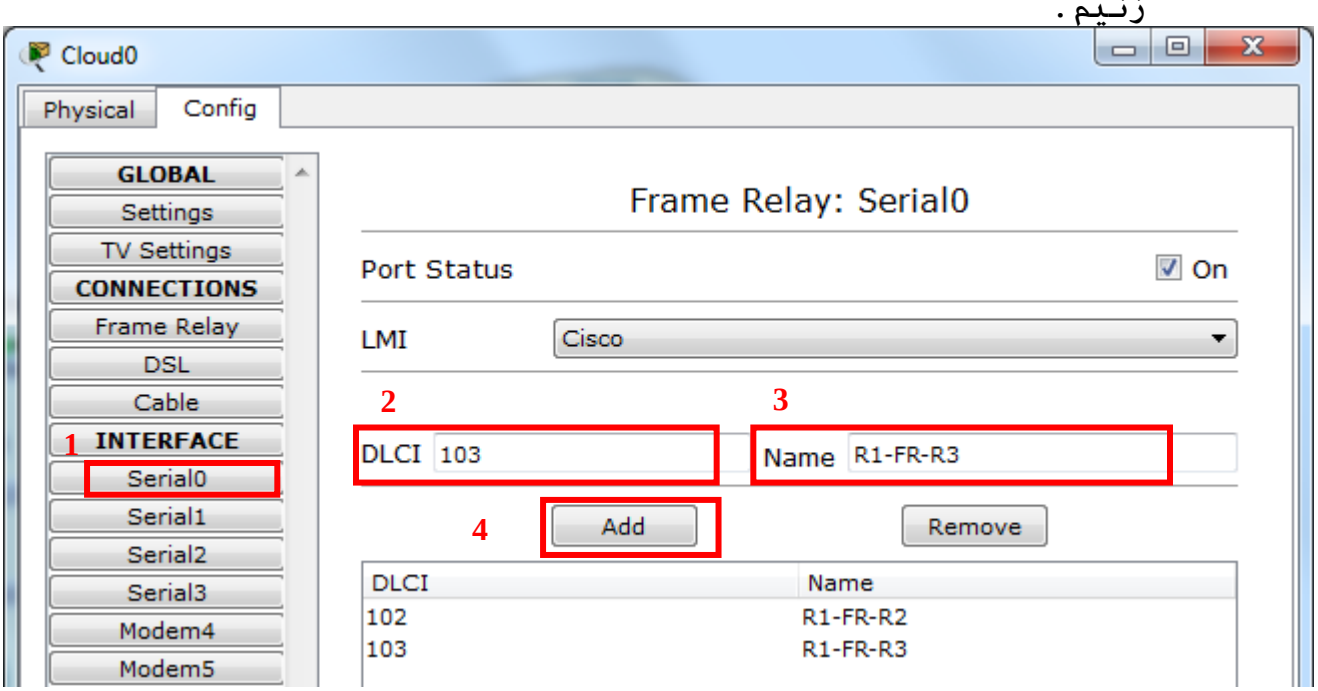
```
1  Router(config)#hostname r5
2  r5(config)#username r2 password 123
3
4  r5(config)#int ser 0/0/0
5  r5(config-if)#encapsulation ppp
6  r5(config-if)#no sh
```

---

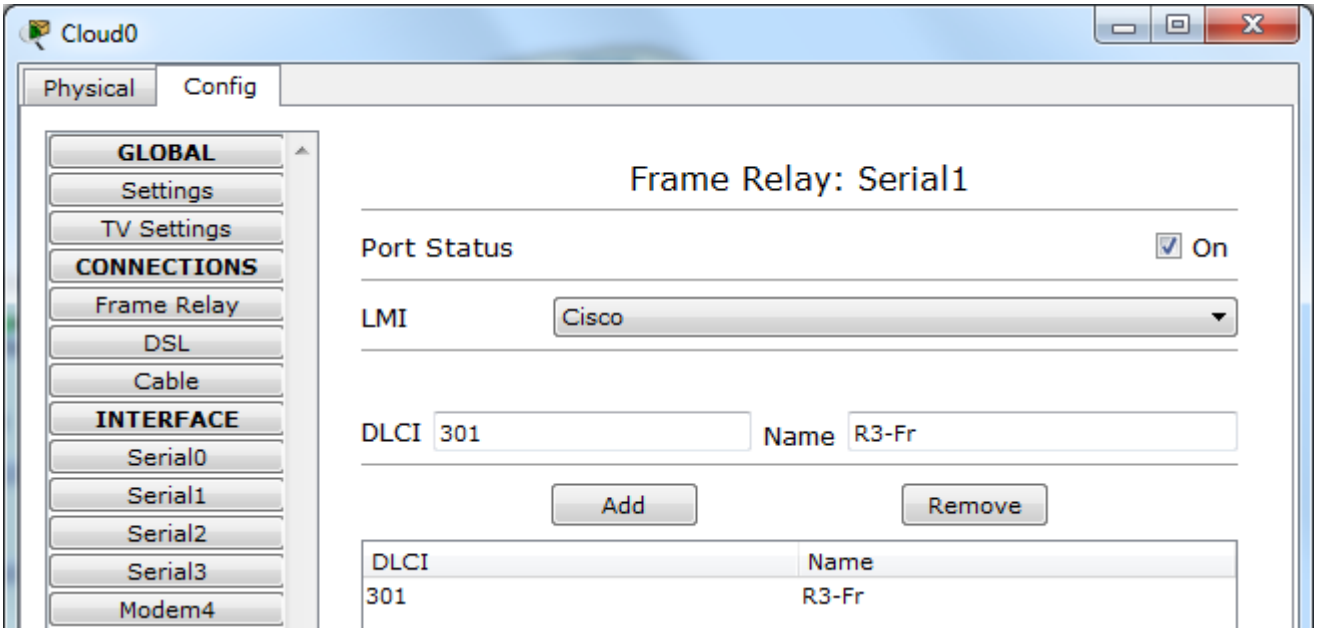
ج 3: براي روتر هاي R3,R2,R1 پروتكلهاي Frame relay به روش ها؟؟؟ اسپك پياده سازي شده و از DLCI هاي داده شده استفاده گردد.

ب 1- بر روي ابر كليک كرده و DLCI را از قسمت Config و Interface تعريف مي كنيم.

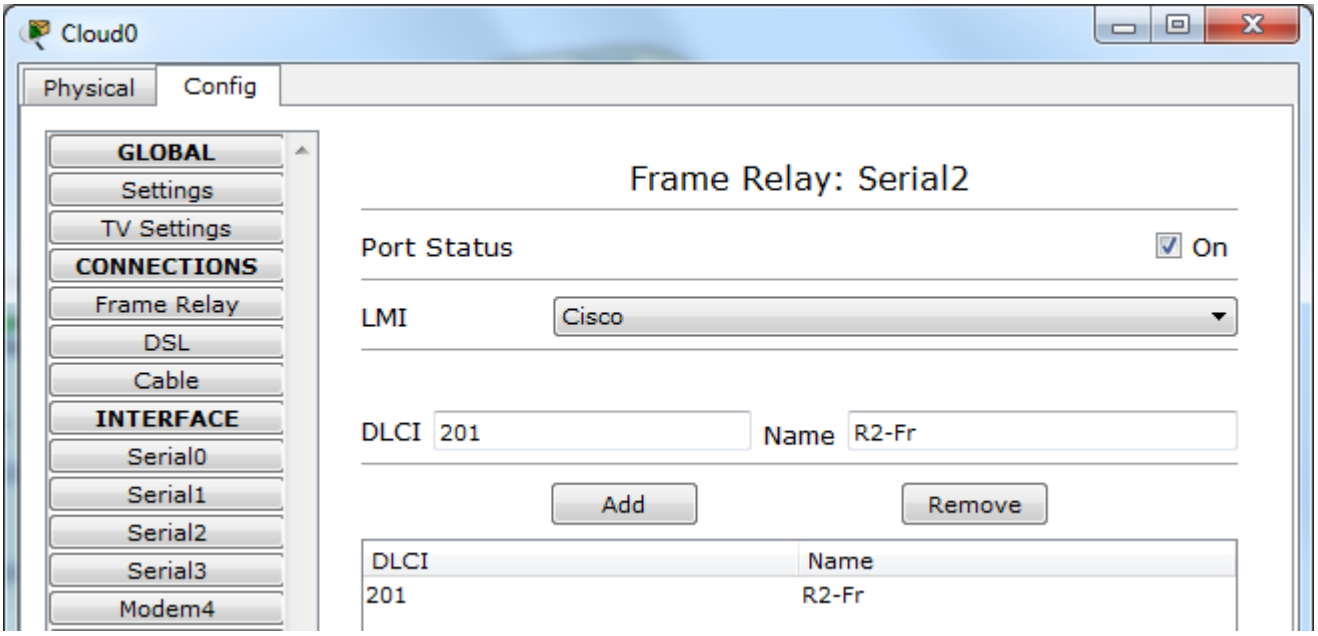
a. Serial 0 را كليک مي كنيم.
b. DLCI هائيكه به پورت سريال ابر متصل هستند را وارد مي كنيم و براي آنها نام انتخاب كرده و سپس در هر مرحله كليد ADD را مي زنيم.



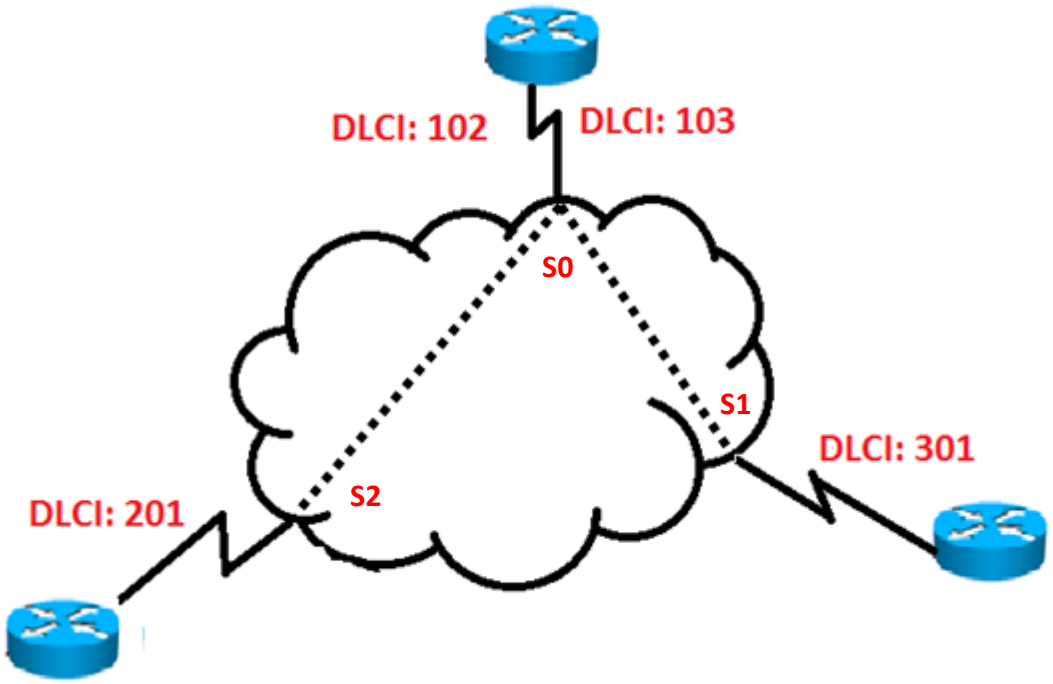

c. و پورت Serial 1 را كليك كرده و مانند بالا DLCI مرتبط به اين پورت را Add مي كنيم.

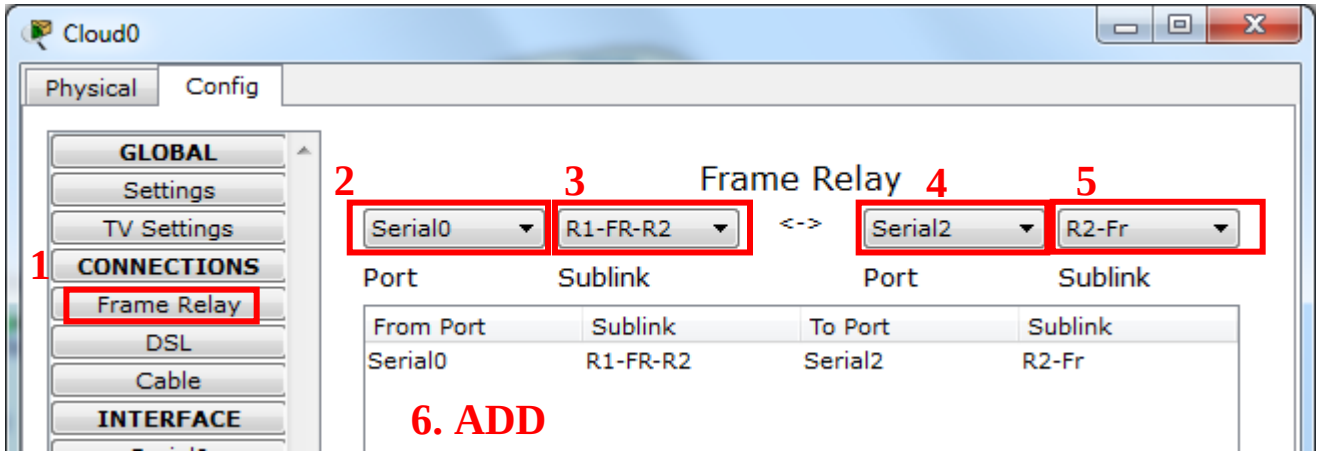



**d.** و پورت سریال **Se2**

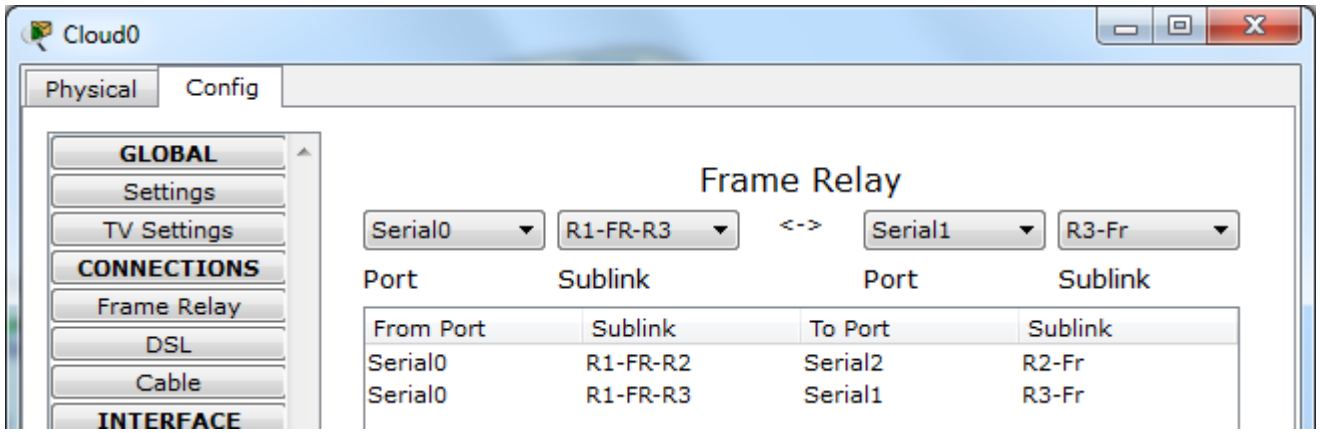



ب 2- مجددا بر روي ابر كليک كرده و **Frame Relaye** ها را دقيقا مطابق به شكل زير تعريف مي كنيم.




در سمت اول از پورت سریال **Se0** ابر با نام **R1-FR-R2** و در سمت دیگر ابر از طریق پورت سریال **Se2** با نام **R2-Fr** به روتر **R2** متصل مي شويم.



در سمت اول از پورت سریال **Se0** ابر با نام **R1-FR-R3** و در سمت دیگر ابر از طریق پورت سریال **Se1** با نام **R3-Fr** به روتر **R3** متصل مي شويم.

ب3- حال بايد روتر ها را **Config** كنيم و به پورتهاي روتر **IP** بدهيم.

**R1:**

```
1  Router(config)#interface se 0/0/0
2  Router(config-if)#encapsulation frame-relay
3  Router(config-if)#ip address 192.168.123.1 255.255.255.240
4
5  Router(config-if)#frame-relay map ip 192.168.123.3 103 broadcast
6  Router(config-if)#frame-relay map ip 192.168.123.2 102 broadcast
7  Router(config-if)#no sh
```

**R3:**

```
1  r3(config)#int ser 0/0/1
2  r3(config-if)#encapsulation frame-relay
3  r3(config-if)#ip address 192.168.123.3 255.255.255.240
4
5  r3(config-if)#frame-relay map ip 192.168.123.1 301 broadcast
6  r3(config-if)#no sh
```

**R2:**

```
1  r2(config)#int ser 0/2/0
2  r2(config-if)#encapsulation frame-relay
3  r2(config-if)#ip address 192.168.123.2 255.255.255.240
4
5  r2(config-if)#frame-relay map ip 192.168.123.2 201 broadcast
6  r2(config-if)#no sh
```

---

**ج 4: پروتكلهاي مسيريابي مطابق شكل پياده سازي گردد و براي ارتباط روتر 3 و 4 از مكانيزم MD5 استفاده گردد.**

**راه اندازي Dynamic Routing:**

**R6:**

```
1  Router(config)#router rip
2  Router(config-router)#ver 2
3  Router(config-router)#network 192.168.6.0
4  Router(config-router)#network 192.168.62.0
```

**R2:**

```
1  Router(config)#router rip
2  Router(config-router)#version 2
3  Router(config-router)#network 192.168.62.0
4
5  Router(config)#router ospf 1
6  Router(config-router)#network 172.16.25.161 0.0.0.15 area 0
7  Router(config-router)#network 192.168.123.2 0.0.0.15 area 0
8  Router(config-router)#redistribute rip metric 1 subnets
9
10 Router(config)#router rip
11 Router(config-router)#version 2
12 Router(config-router)#redistribute ospf 1 metric 1
```

- خط 6و7: محاسبه ي Wildcard ، Interface Se0/0/1 :

**Wildcard=255.255.255.255 - NetMask**
**Wildcard= 255.255.255.255 - 255.255.255.240=0.0.0.15**

**R5:**

```
1  Router(config)#router eigrp 20
2  Router(config-router)#network 192.168.100.0
3
4  Router(config)#router ospf 1
5  Router(config-router)#network 172.16.25.162 0.0.0.15 area 0
6  Router(config-router)#network 172.16.45.1 0.0.0.0 area 0
7  Router(config-router)#network 172.16.54.1 0.0.0.0 area 0
8  Router(config-router)#redistribute eigrp 20 metric 1 subnets
9
10 Router(config)#router eigrp 20
11 Router(config-router)#redistribute ospf 1 metric 1 1 1 1 1
```

**R4:**

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 172.16.45.2 0.0.0.0 area 0
3  Router(config-router)#network 172.16.54.2 0.0.0.0 area 0
4  Router(config-router)#network 192.168.4.1 0.0.0.0 area 0
5  Router(config-router)#network 192.168.5.1 0.0.0.0 area 0
6  Router(config-router)#network 172.16.34.210 0.0.0.15 area 0
```

**R3:**

```
1  Router(config)#router ospf 1
2  Router(config-router)#network 172.16.12.81 0.0.0.7 area 0
3  Router(config-router)#network 172.16.30.177 0.0.0.15 area 0
4  Router(config-router)#network 192.168.123.3 0.0.0.15 area 0
5  Router(config-router)#net 172.16.34.209 0.0.0.15 area 0
```

**: Md5 Authentication**

**R3:**

```
1  r3(config)#interface serial 0/0/0
2  r3(config-if)#ip ospf authentication-key ccna
3  r3(config-if)#ip ospf authentication message-digest
```

**R4:**

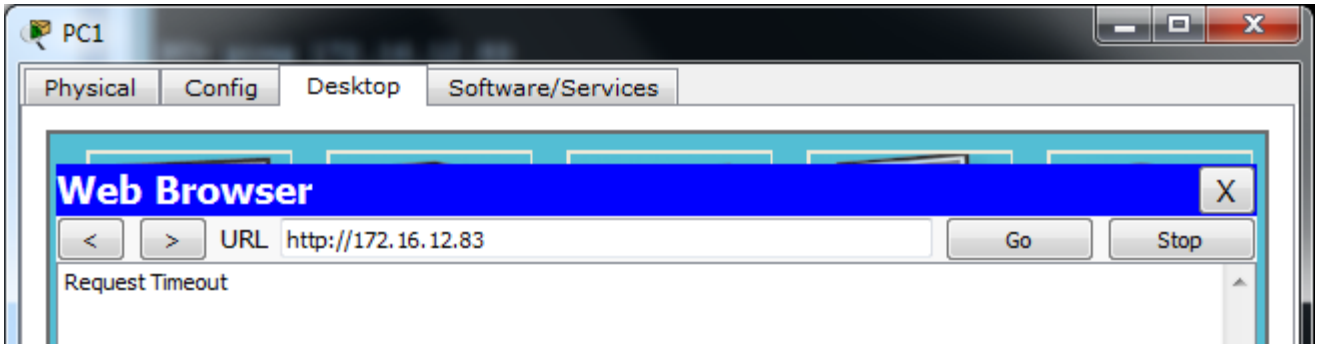
```
1  r4(config)#interface serial 0/2/0
2  r4(config-if)#ip ospf authentication-key ccna
3  r4(config-if)#ip ospf authentication message-digest
```

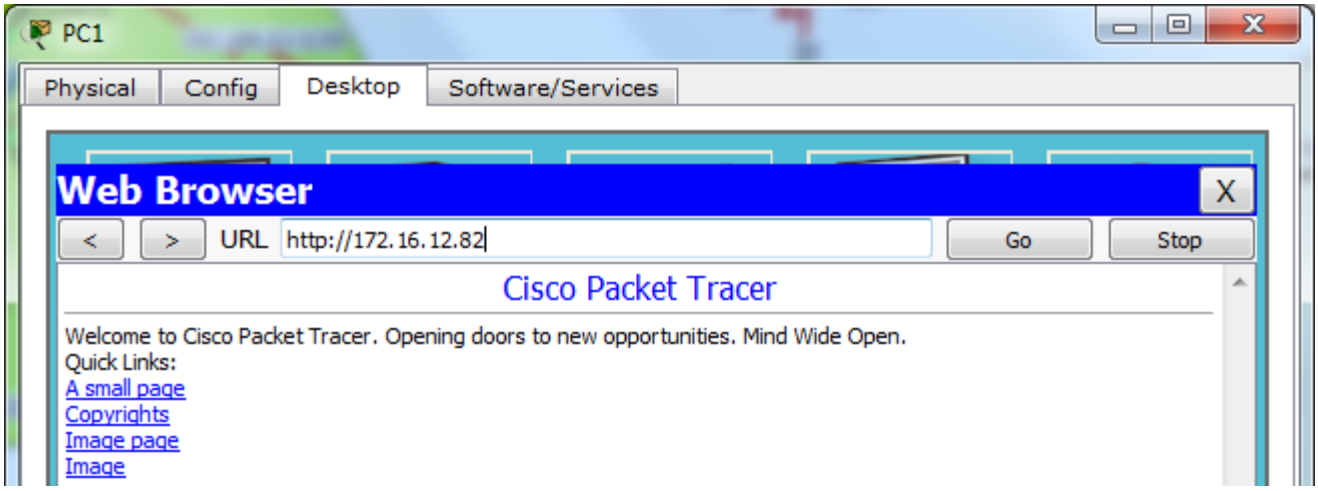
---

**ج 5- دسترسي PC1 به سرور 1 از طريق Web و به سرور 2 از طريق پروتكل ICMP و نسبت به سرور 3 كلا مسدود باشد.** (بخش 1- خط 1و2) (بخش 2- خط 4و5) (بخش 3- خط 7)

**R6:**

```
1  Router(config)#access-list 180 permit tcp host 192.168.6.2 host 172.16.12.82 eq 80
2  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.12.82
3
4  Router(config)#access-list 180 permit icmp host 192.168.6.2 host 172.16.12.83
5  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.12.83
6
7  Router(config)#access-list 180 deny ip host 192.168.6.2 host 172.16.30.178
8
9  Router(config)#access-list 180 permit ip any any
10
11 Router(config-if)#inter fa 0/0
12 Router(config-if)#ip access-group 180 in
```






و . . .

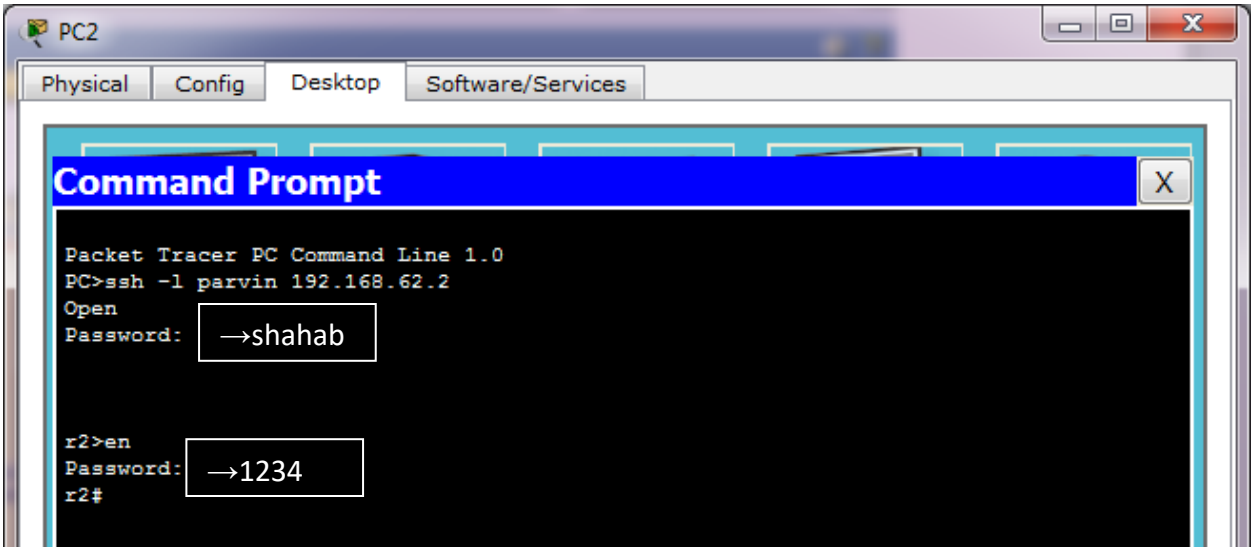
---

**ج 6:** قابلیت SSH نسبت به روتر 2 براي PC2,5,6 کلا مسدود باشد.

ب1. ابتدا SSH را بر روی روتر فعال می کنیم:

```
1   r2(config)#ip domain-name cisco.com
2   r2(config)#crypto key generate rsa
3   The name for the keys will be: r2.cisco.com
4   Choose the size of the key modulus in the range of 360 to 2048 for your  General Purpose Keys.
5   Choosing a key modulus greater than 512 may take  a few minutes.
6   How many bits in the modulus [512]: 1024
7   % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
8
9   r2(config)#ip ssh version 2
10  r2(config)#username parvin password shahab
11  r2(config)#enable secret 1234
12  r2(config)#line vty 0 4
13  r2(config-line)#login local
14
15  r2(config-line)#transport in
    r2(config-line)#transport input ssh
```

**PC2>ssh –L parvin 192.168.62.2**



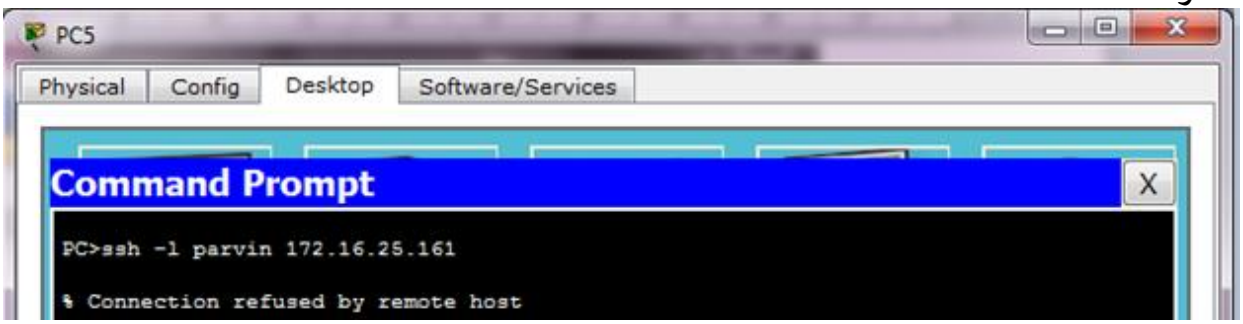

ب2. حال **ACL** مورد نظر را جهت بستن دسترسی **PC** ها از نوع استاندارد می نویسیم که آنرا باید در مقصد (یعنی روتر **R2** اعمال نماییم):

**IP PC2:192.168.6.3**
**IP PC5:192.168.100.3**
**IP PC6:192.168.4.2**

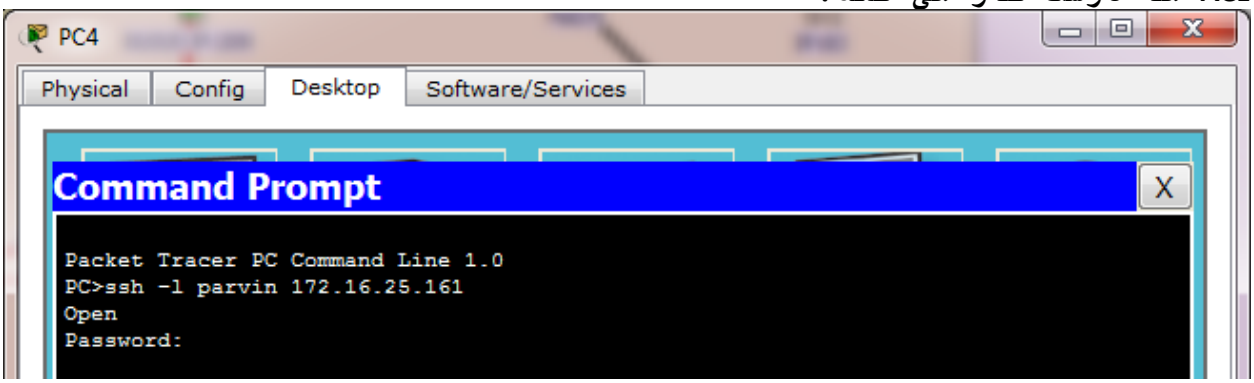
**R2:**

| | |
|---|---|
| 1 | r2(config)#**access-list 20 deny host 192.168.6.3** |
| 2 | r2(config)#**access-list 20 deny host 192.168.100.3** |
| 3 | r2(config)#**access-list 20 deny host 192.168.4.2** |
| 4 | r2(config)#**access-list 20 permit any** |
| 5 | |
| 6 | r2(config)#**line vty 0 4** |
| 7 | r2(config-line)#**access-class 20 in** |

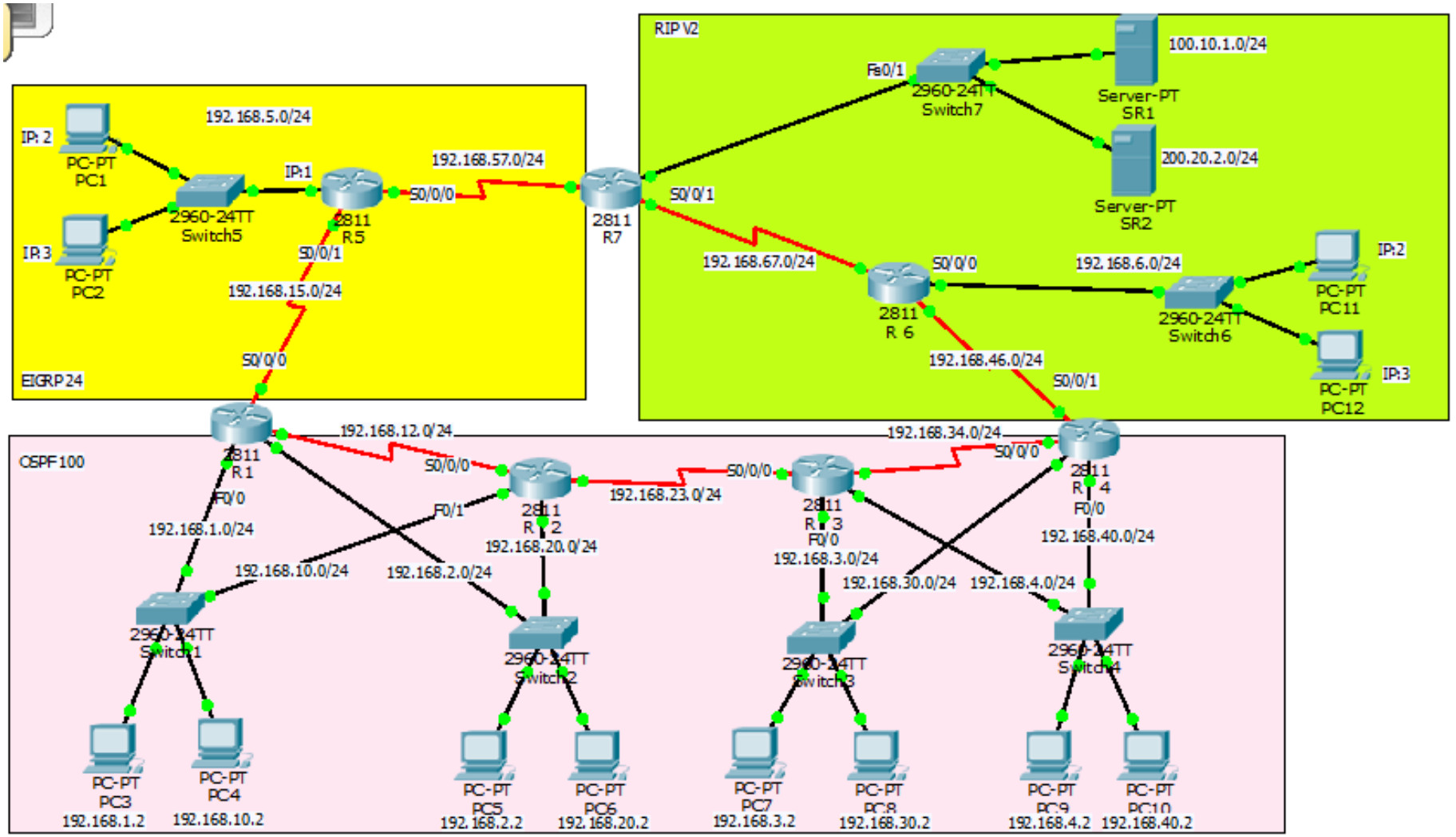
ب3. تست از PC5:




در حالیکه از PC4 بخواهیم از طریق SSh به روتر R2 وصل شویم، می شود در نتیجه ACL ما درست کار می کند.



# سناریو جلسه 29: V.Interface – SSH-Telnet-ACL و . . .



س 1: با استفاده از IP های داده شده ، ارتباط اولیه شبکه را راه اندازی نموده و پروتکل های مسیریابی را مطابق با شکل پیاده سازی نمایید.
س 2: دسترسی PC2 نسبت به Server 1 فقط از طریق Web مقدور باشد.
س 3: دسترسی PC 1 نسبت به Server 1,2 فقط از طریق پروتکل ICMP مسدود باشد.
س 4: دسترسی کاربران SW1 / SW6/SW3 از طریق SSH نسبت به Router 7 مسدود باشد.
س 5: قابلیت Telnet نسبت به Server 1 فقط برای PC12 مقدور باشد.

---

ج 1- اختصاص IP: با استفاده از IP های داده شده ، ارتباط اولیه شبکه را راه اندازی نموده و پروتکل های مسیریابی را مطابق با شکل پیاده سازی نمایید.

**R1:**

```
1   R1(config)#int ser 0/0/0
2   R1 (config-if)#ip add 192.168.15.2 255.255.255.0
3   R1 (config-if)#no sh
4
5   R1 (config-if)#int ser 0/0/1
6   R1 (config-if)#ip  add 192.168.12.1 255.255.255.0
7   R1 (config-if)#clo rat 64000
8   R1 (config-if)#no sh
9
10  R1(config)#int fa 0/0
11  R1 (config-if)#ip add 192.168.1.1 255.255.255.0
12  R1(config-if)#no sh
13
14  R1(config)#int fa 0/1
15  R1 (config-if)#ip add 192.168.2.1 255.255.255.0
16  R1(config-if)#no sh
```

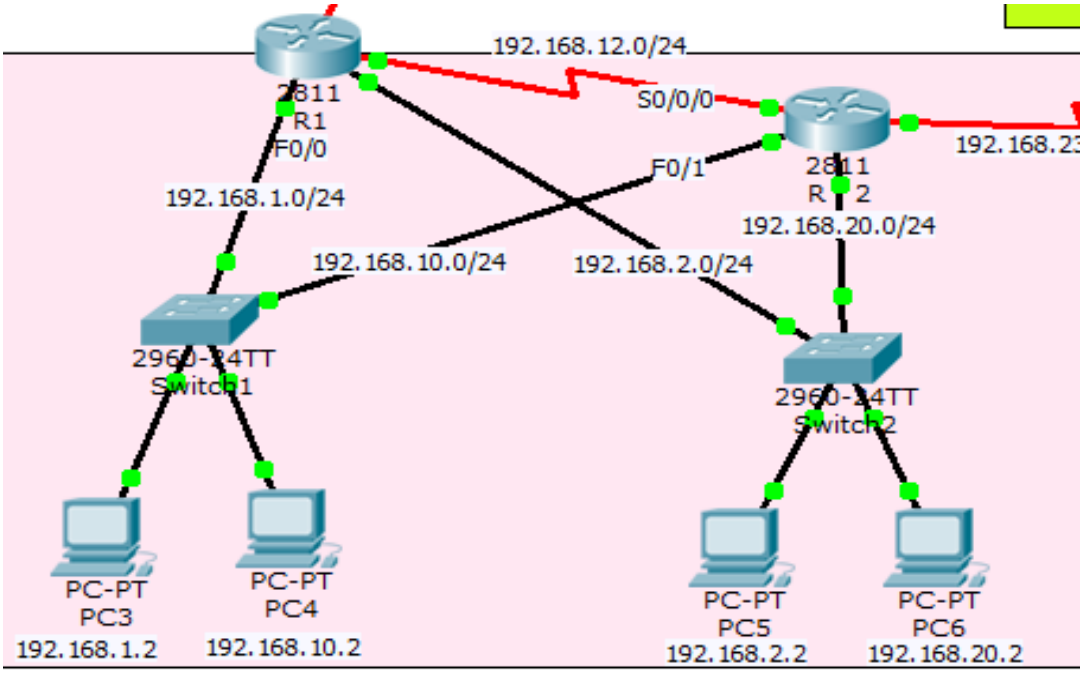
**R2:**

```
1   Router(config)#int ser 0/0/0
2   Router(config-if)#ip add 192.168.12.2 255.255.255.0
3   Router(config-if)#no sh
4
5   Router(config-if)#int ser 0/0/1
6   Router(config-if)#ip add 192.168.23.1 255.255.255.0
7   Router(config-if)#clock rat 64000
8   Router(config-if)#no sh
9
10  R2(config)#int fa 0/0
11  R2(config-if)#ip address 192.168.20.1 255.255.255.0
12  R2(config-if)#no sh
13
14  R2(config-if)#int fa 0/1
15  R2(config-if)#ip add 192.168.10.1 255.255.255.0
16  R2(config-if)#no sh
```

این قسمت که بصورت ضدربدر IP داده شده است نیز به هر کدام از Interface های روتر مطابق شکل IP اختصاص می دهیم و به هر کدام از PC ها نیز مطابق با آنچه خواسته شد می توان IP اختصاص داد.

**PC3:** **IP: 192.168.1.2** **Gateway: 192.168.1.1**
**PC4:** **IP: 192.168.10.2** **Gateway: 192.168.10.1**

**PC5:** **IP:192.168.2.2** **Gateway:192.168.2.1**
**PC6:** **IP:192.168.20.2** **Gateway:192.168.20.1**




**R3:**

```
1   R3(config)#int ser 0/0/0
2   R3(config-if)#ip add 192.168.23.2 255.255.255.0
3   R3(config-if)#no sh
4
5   R3(config-if)#int ser 0/0/1
6   R3(config-if)#ip add 192.168.34.1 255.255.255.0
7   R3(config-if)#no sh
8
9   R3(config)#int fa 0/0
10  R3(config-if)#ip add 192.168.3.1 255.255.255.0
11  R3(config-if)#no sh
12
13  R3(config-if)#int fa 0/1
14  R3(config-if)#ip add 192.168.4.1 255.255.255.0
15  R3(config-if)#no sh
```

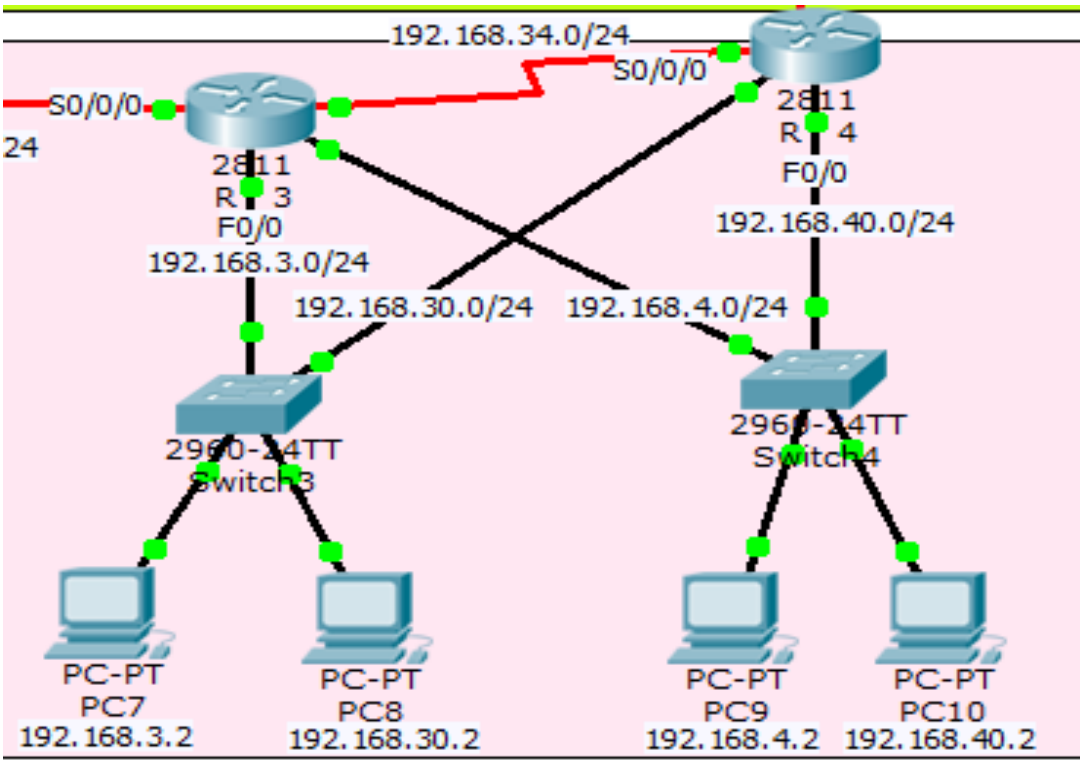
**R4**

```
1   Router(config)#int ser 0/0/1
```

```
2   Router(config-if)#ip add 192.168.46.2 255.255.255.0
3   Router(config-if)#no sh
4
5   Router(config-if)#int ser 0/0/0
6   Router(config-if)#ip add 192.168.43.2 255.255.255.0
7   Router(config-if)#no sh
8
9   R4(config)#int fa 0/0
10  R4(config-if)#ip add 192.168.40.1 255.255.255.0
11  R4(config-if)#no sh
12
13  R4(config-if)#int fa 0/1
14  R4(config-if)#ip add 192.168.30.1 255.255.255.0
15  R4(config-if)#no sh
```

**PC7: IP: 192.168.3.2 Gateway: 192.168.3.1**
**PC8: IP: 192.168.30.2 Gateway: 192.168.30.1**

**PC9: IP: 192.168.4.2 Gateway: 192.168.4.1**
**PC10: IP: 192.168.40.2 Gateway: 192.168.40.1**




**Redistribution:**

**R5:**

```
1   R5(config)#router eigrp 24
2   R5(config-router)#network 192.168.5.0
```

| | |
|---|---|
| 3 | R5(config-router)#**network 192.168.15.0** |
| 4 | R5(config-router)#**network 192.168.57.0** |

**R7:**

| | |
|---|---|
| 1 | R7(config)#**router eigrp 24** |
| 2 | R7 (config-router)#**network 192.168.57.0** |
| 3 | |
| 4 | R7 (config)#**router rip** |
| 5 | R7 (config-router)#**v 2** |
| 6 | R7 (config-router)#**network 192.168.67.0** |
| 7 | R7 (config-router)#**net 100.10.1.0** |
| 8 | R7 (config-router)#**net 200.20.2.0** |
| 9 | R7(config-router)#**redistribute eigrp 24 metric 1** |
| 10 | |
| 11 | R7 (config)#**router eigrp 24** |
| 12 | R7(config-router)#**redistribute rip metric 1 1 1 1 1** |

**R6:**

| | |
|---|---|
| 1 | R6(config)#**router rip** |
| 2 | R6(config-router)#**v 2** |
| 3 | R6(config-router)#**net 192.168.6.0** |
| 4 | R6(config-router)#**net 192.168.46.0** |
| 5 | R6(config-router)#**net 192.168.67.0** |

**R2:**

| | |
|---|---|
| 1 | R2(config)#**router ospf 1** |
| 2 | R2(config-router)#**network 192.168.23.0 0.0.0.255 area 100** |
| 3 | R2(config-router)#**network 192.168.12.0 0.0.0.255 area 100** |
| 4 | R2(config-router)#**network 192.168.10.0 0.0.0.255 area 100** |
| 5 | R2(config-router)#**network 192.168.20.0 0.0.0.255 area 100** |

**R3:**

| | |
|---|---|
| 1 | R3(config)#**router ospf 1** |
| 2 | R3(config-router)#**network 192.168.23.0 0.0.0.255 area 100** |
| 3 | R3(config-router)#**network 192.168.34.0 0.0.0.255 area 100** |
| 4 | R3(config-router)#**network 192.168.3.0 0.0.0.255 area 100** |
| 5 | R3(config-router)#**network 192.168.4.0 0.0.0.255 area 100** |

**R1:**

| | |
|---|---|
| 1 | R1(config)#**router eigrp 24** |
| 2 | R1(config-router)#**net 192.168.15.0** |
| 3 | |
| 4 | R1(config-router)#**router ospf 1** |
| 5 | R1(config-router)#**net 192.168.1.0 0.0.0.255 area 100** |
| 6 | R1(config-router)#**net 192.168.12.0 0.0.0.255 area 100** |
| 7 | R1(config-router)#**net 192.168.2.0 0.0.0.255 area 100** |

```
8  R1(config-router)#redistribute eigrp 24 metric 1 subnets
9
10 R1(config)#router eigrp 24
11 R1(config-router)#redistribute ospf 1 metric 1 1 1 1 1
```

**R4:**

```
1  R4(config)#router rip
2  R4(config-router)#v 2
3  R4(config-router)#net 192.168.46.0
4
5  R4(config)#router ospf 1
6  R4(config-router)#net 192.168.34.0 0.0.0.255 area 100
7  R4(config-router)#net 192.168.40.0 0.0.0.255 area 100
8  R4(config-router)#net 192.168.30.0 0.0.0.255 area 100
9  R4(config-router)#redistribute rip metric 1 subnets
10
11 R4(config)#router rip
12 R4(config-router)#v 2
13 R4(config-router)#redistribute ospf 1 metric 1
```

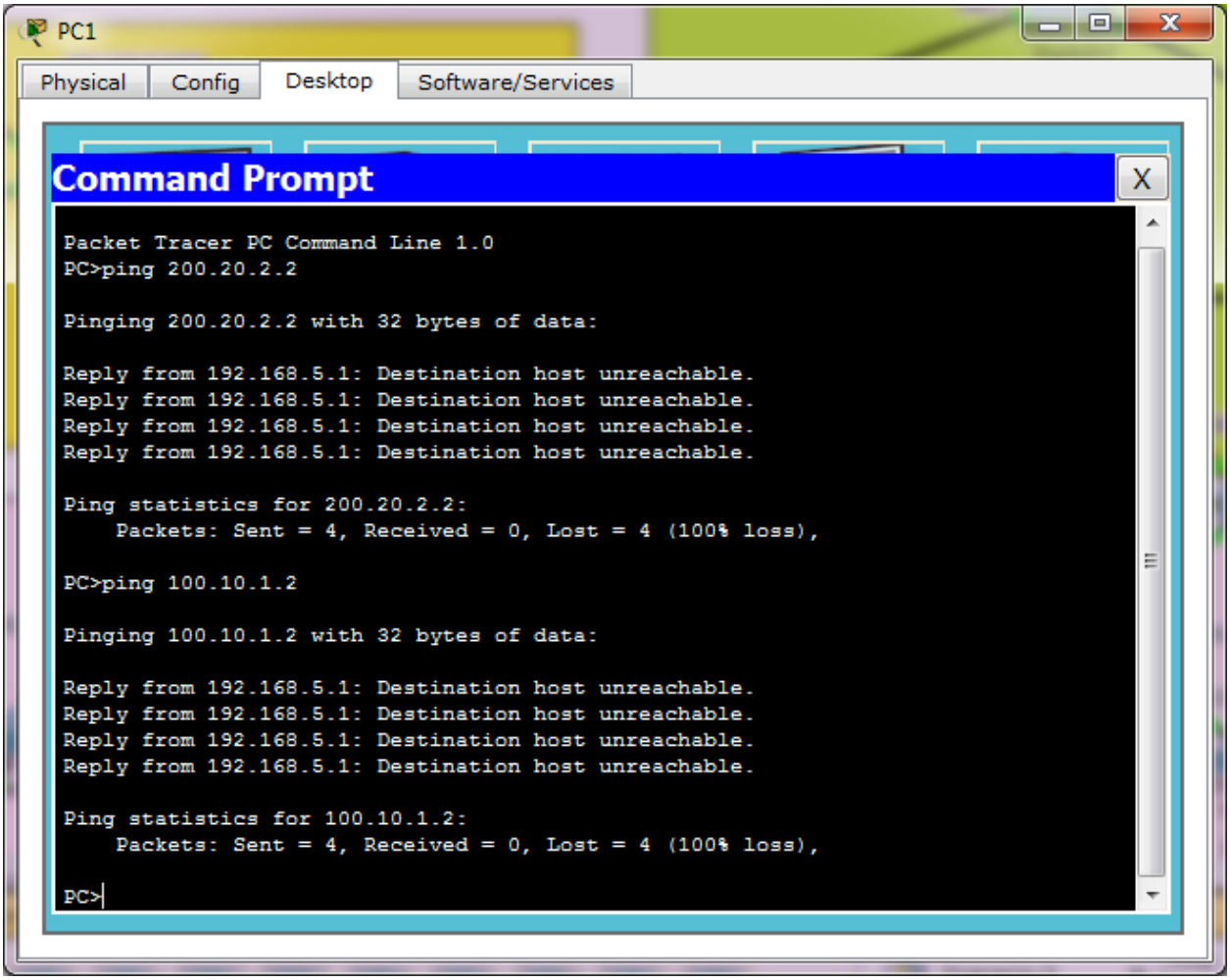
---

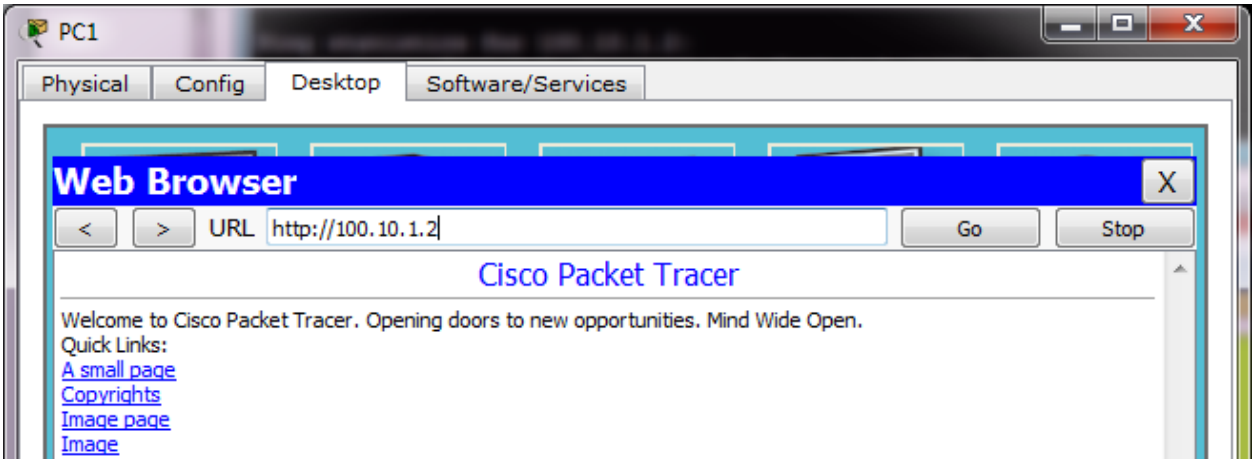
**ج 2: دسترسي PC1 نسبت به Server 1,2 فقط از طريق Web مقدور باشد.**

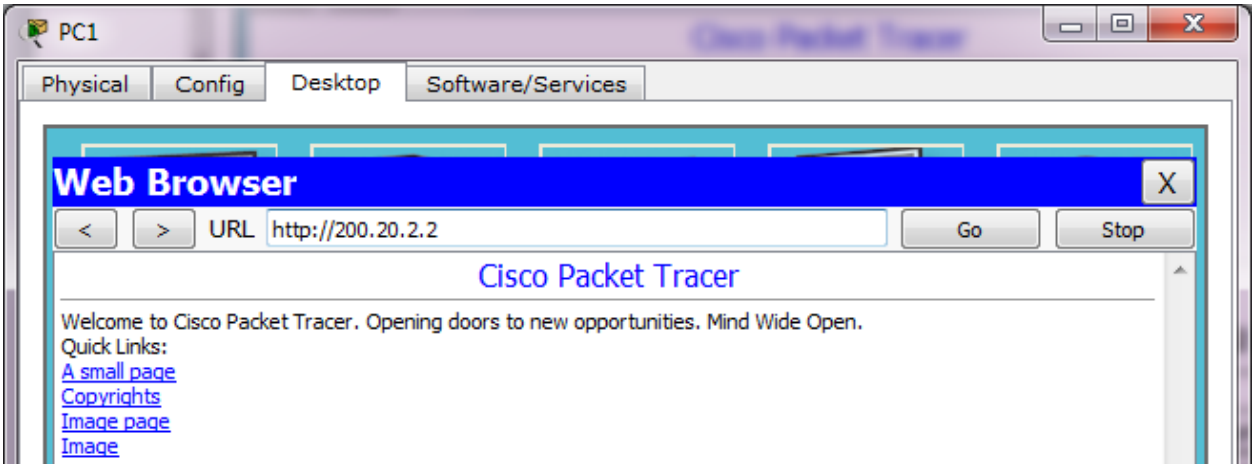
| Source | Access Type | Destination | In |
|---|---|---|---|
| PC 1 | Web | Server 1,2 | Near Source |
| 192.168.5.2 | Permit TCP … Eq80 | 100.10.1.2 | R5-Inbound Fa0/0 |
| 192.168.5.2 | Permit TCP … Eq80 | 200.20.2.2 | R5-Inbound Fa0/0 |

**R5:**

```
1  R5(config)#access-list 120 permit tcp host 192.168.5.2 host 100.10.1.2 eq 80
2  R5(config)#access-list 120 deny ip host 192.168.5.2 host 100.10.1.2
3
4  R5(config)#access-list 120 permit tcp host 192.168.5.2 host 200.20.2.2 eq 80
5  R5(config)#access-list 120 deny ip host 192.168.5.2 host 200.20.2.2
6
7  R5(config)#access-list 120 permit ip any any
8
9  R5(Config)#inte fa 0/0
10 R5(Config-if)#ip access-group 120 in
```


PC1
Physical
Config
Desktop
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 200.20.2.2
Pinging 200.20.2.2 with 32 bytes of data:
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Ping statistics for 200.20.2.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 100.10.1.2
Pinging 100.10.1.2 with 32 bytes of data:
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Ping statistics for 100.10.1.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>


PC1
Physical
Config
Desktop
Software/Services
Web Browser
URL
http://100.10.1.2
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image




---

**س 3:** دسترسی **PC 1** نسبت به **PC11** فقط از طریق پروتکل **ICMP** مسدود باشد.

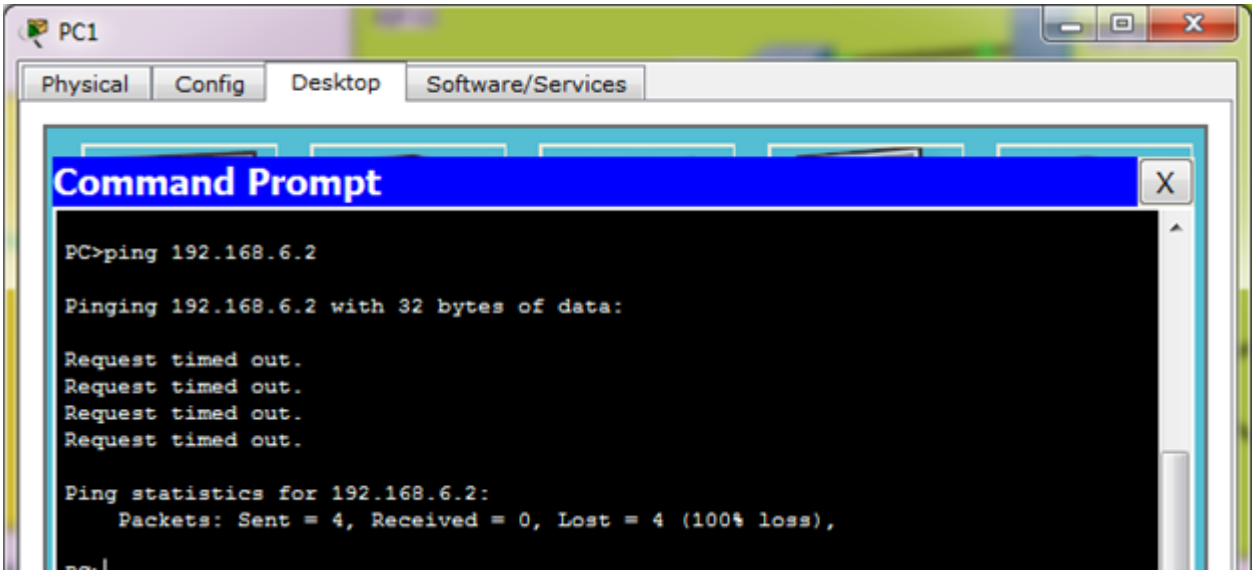
نکته بسیار مهم: در این قسمت مبدا با سوال قبل دقیقا یکسان است اما مقصد ها یکسان نیست و باید در اینجا نیز **ACL Extended** بنویسیم و قاعدتا در روتر مبدا و روی **Inbound Interface Fa 0/0 R5** باید اعمال کنیم. اما اگر این کار را بکنیم **ACL** جدید روی **ACL** ای که برای سوال قبل نوشتیم **Over write** می شود و ← اشتباه است و باید راه حل دیگری بیابیم.

| Source | Access Type | Destination | In |
|---|---|---|---|
| PC 1 | Deny ICMP | PC11 | Near Source |
| 192.168.5.3 | Deny ICMP | 100.10.1.2 | ~~R5-Inbound Fa0/0~~ |

برای اینکه این مشکل حل گردد جای مبدا و مقصد را عوض می کنیم که مشکل حل می شود و **ACL** را بر روی روتر **R6** و **Inbound Interface Fa 0/0** اعمال می کنیم.

| Source | Access Type | Destination | In |
|---|---|---|---|
| PC11 | Deny ICMP | PC 1 | Near Source |
| 192.168.6.2 | Deny ICMP | 192.168.5.2 | R6-Inbound Fa0/0 |

```
1  R6(config)#access-list 150 deny icmp host 192.168.6.2 host 192.168.5.2
2  R6(config)#access-list 150 permit ip any any
3
4  R6(config)#interface fa 0/0
5  R6(config-if)#ip access-group 150 in
```




**س 4:** دسترسی کاربران **SW1** / **SW6/SW3** از طریق **SSH** نسبت به **Router 7** مسدود باشد.

ابتدا باید **SSH** را باید در روتر **R7** فعال کنیم. (مثل تمرینهای قبل)

**R7:**

```
1   R7(config)#ip domain-name cisco.com
2   R7(config)#crypto key generate rsa
3   The name for the keys will be: R7.cisco.com
4   Choose the size of the key modulus in the range of 360 to 2048 for your
5    General Purpose Keys. Choosing a key modulus greater than 512 may take
6    a few minutes.
7
8   How many bits in the modulus [512]: 1024
9   % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
10
11  R7(config)#ip ssh version 2
12  R7(config)#username parvin password shahab
13  R7(config)#enable secret 123456
14  R7(config)#line vty 0 4
15  R7(config-line)#login local
16  R7(config-line)#transport input ssh
```

در اینجا سوییچ **Sw1**و **Sw3** دو **IP** دارد.

**IP SW1: 192.168.1.0, 192.168.10.0**
**IP SW3: 192.168.3.0, 192.168.30.0**
**IP Sw6: 192.168.6.0**

**R7:**

```
1   R7(config)#access-list 10 deny 192.168.1.0 0.0.0.255
2   R7(config)#access-list 10 deny 192.168.10.0 0.0.0.255
3
4   R7(config)#access-list 10 deny 192.168.3.0 0.0.0.255
```

```
5   R7(config)#access-list 10 deny 192.168.30.0 0.0.0.255
6
7   R7(config)#access-list 10 deny 192.168.6.0 0.0.0.255
8
9   R7(config)#access-list 10 permit any any
10
11  R7(config)#line vty 0 4
12  R7(config-line)#access-class 10 in
```

**و یا اگر فقط بخواهیم یک کامپیوتر را از کاربر یک سویچ ببندیم: مثلا یکی از IPهای سویچ SW1 را ببندیم:**

```
1   R7(config)#access-list 10 deny host 192.168.1.2
```

---

**س 5: قابلیت Telnet نسبت به روتر R1 فقط برای PC12 مقدور باشد.**
**ابتدا Telnet را بر روي روتر R1 فعال مي كنيم.**

```
1   R1(config)#username test password 123
2   R1(config)#line vty 0 4
3   R1(config-line)#login local
4   R1(config-line)#transport input telnet
```

**سپس ACL را مي نويسيم و دسترسي PC12 را به R1 از طريق Telnet باز مي كنيم.**

```
1   R1(config)#access-list 25 permit host 192.168.6.3
2   R1(config)#line vty 0 4
3   R1(config-line)#access-class 25 in
```