CISCO CERTIFIED CCNA

CCNA

جزوه

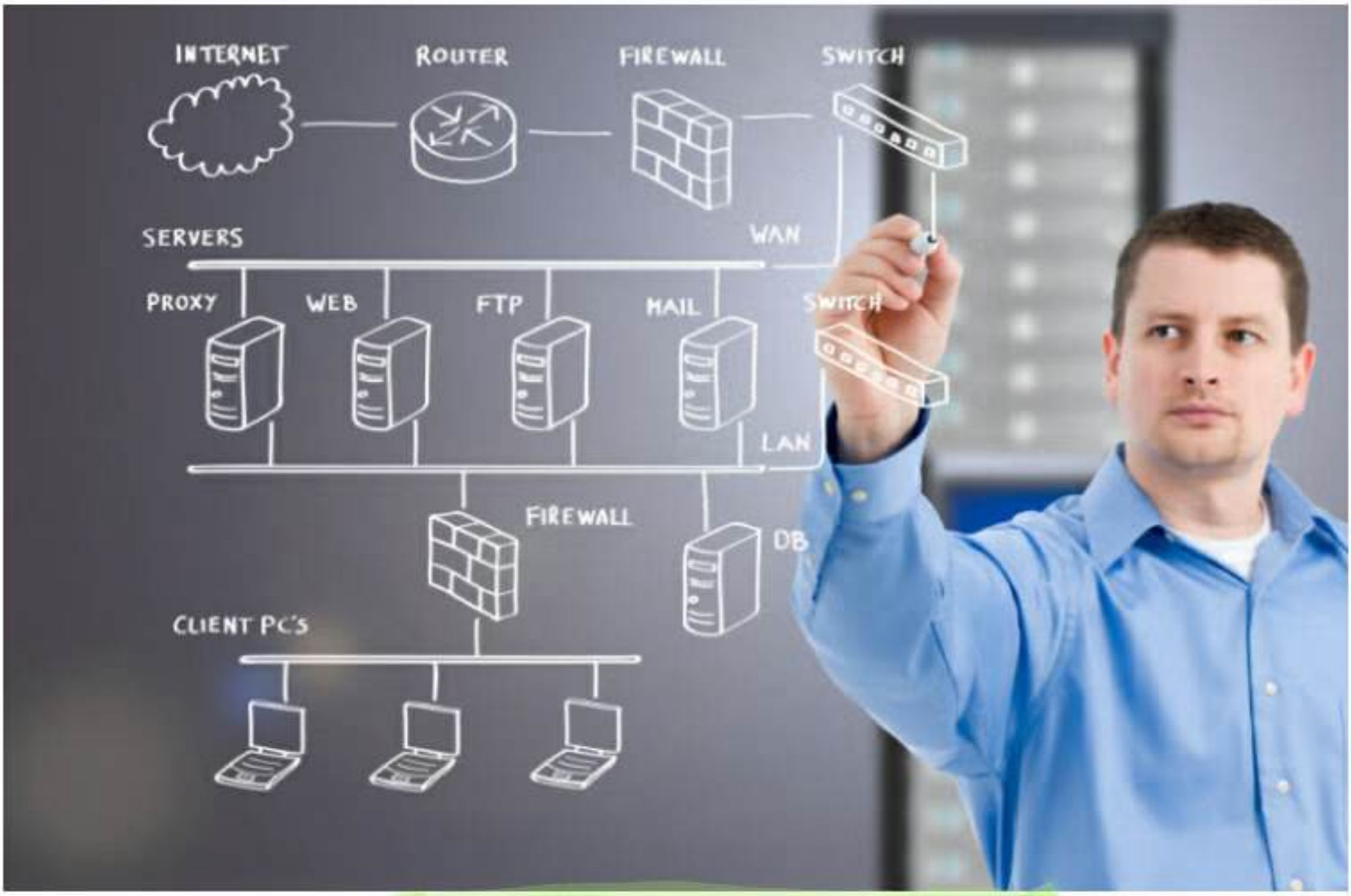
مدرس دوره: مهندس فرزاد حیدری

تهیه کننده: مهندس هوشنگ حشمتی

تابستان ۱۳۹۵

SEMATEC

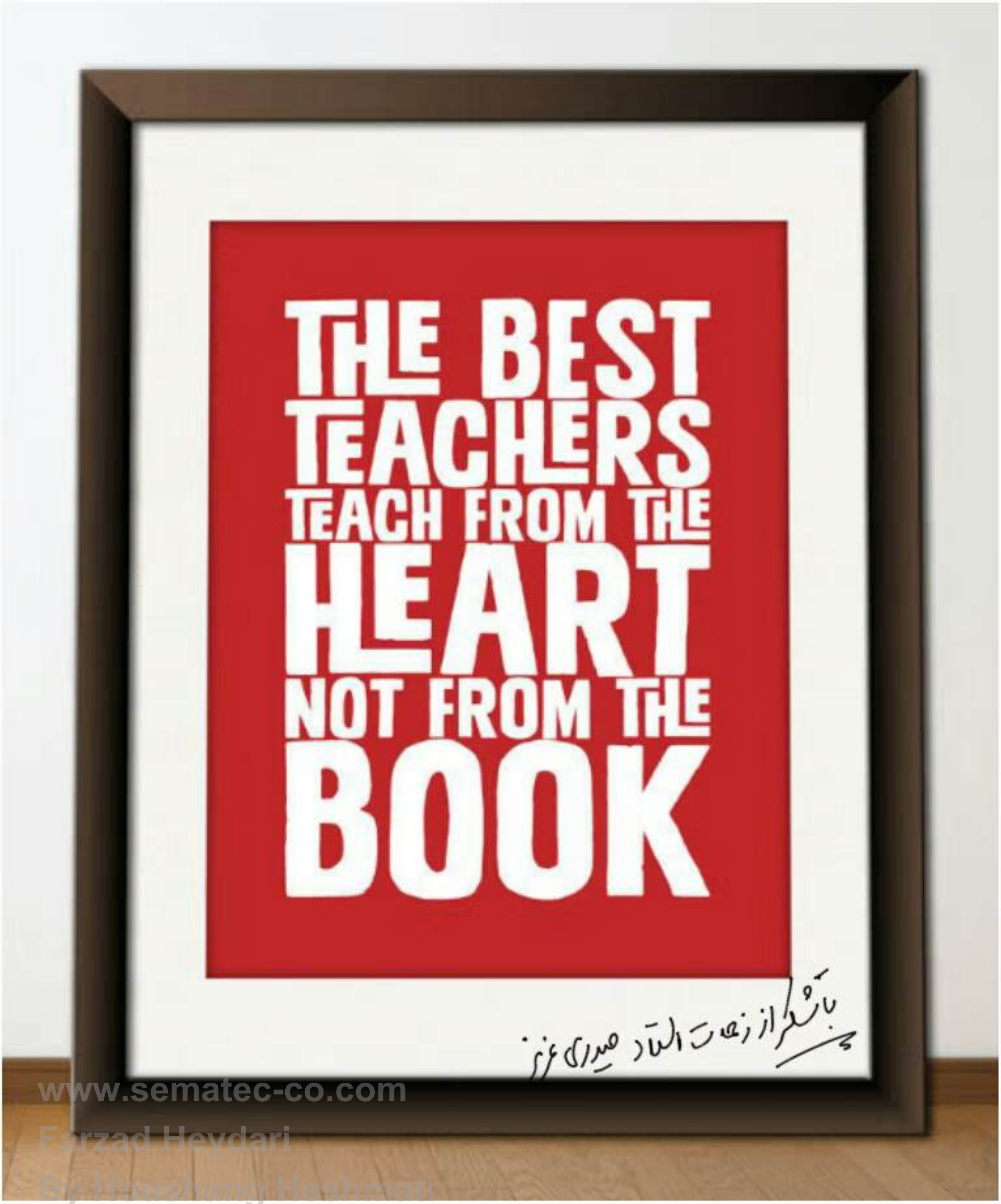
CISCO CERTIFIED CCNA



استاد فرزاد حیدری

گردآورنده هوشنگ حشمتی

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

نرم افزار مورد نیاز :

Cisco packet Tracer Student
6.2.0.0052

Heydari.farzad@gmail.com
استاد فرزاد حیدری

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

یک سوئیچ سیسکو تحویل گرفته ایم و می خواهیم کار با آن را شروع کنیم :

۱) اتصال کابل کنسول :

پشت سوئیچ یک پورت آبی رنگ Rj45 دارد. کابل کنسول هم در جعبه سوئیچ هست. یک سر آن Rj45 و سر دیگر آن پورت قدیمی com دارد. اگر سیستم کامپیوتر شما پورت com نداشت از تبدیل USB های موجود در بازار استفاده کنید :

به کامپیوتر

به سوئیچ

برای وصل شدن به یک نرم افزار کمکی احتیاج دارید که بصورت Free در اینترنت تعدادی هستند ← TeraTerm یا putty

www.senatecisco.com
Farzad Heydari
By Houshang Heshmati

محیط سیستم عامل لوئیچ های سیسکو، حالت command promt است مانند DOS و باید دستورات تایپ شود.

در محیط سیستم عامل سیسکو ۳ مود داریم:

در سمت چپ هر کدام را دیدید مشخص می‌شود در کدام مود هستید

Switch >	Switch #	Switch (config) #
مود اول	مود دوم	مود سوم
	privileged	cofigure terminal
	مانیتورینگ، مدیریت و...	اعمال تغییرات و...

Switch> enable ↵ ورود به مود ۲

Switch# conf t ↵ ورود به مود ۳

Switch(Config)#

از ۲ می‌توانید برای دستورات استفاده کنید

Switch(Config)# Exit ↵ خروج به مود ۲

Switch# disable ↵ خروج به مود ۱

Switch>

هر دستوری را که چند حرف تایپ کنید و بعد کلید Tab را بزنید کامل می‌شود

www.senatec-co.com
Farzad Heydari
By Houshang Heshmati

۲) تغییر نام سوئیچ :

با توجه به اینکه این سوئیچ قرار است بجای اداره یا سازمان استفاده شود و برای دسترسی های بعدی بهتر است (واجب است) نام سوئیچ تغییر کند.

مثلاً اگر سوئیچ سوم در طبقه دوم است که در رک ۲ قرار دارد

SW3F2R2

یا اگر سوئیچ دوم بخش حسابداری طبقه سوم است :

SW2AccountingF3

دستور تغییر نام سوئیچ :

Switch(config)# hostname ------- (نام)

نکته : اگر ابتدای هر دستور No بگذاریم آن دستور لغو (کنسل می شود)

Switch(config)# No hostname SW3F2R2

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

۳) روی پورت کنسول پورد بگذاریم:

اگر شخص دیگری با لپ تاپ به پورت کنسول مانند شما متصل شود می تواند تنظیمات سوئیچ را تغییر دهد. باید روی پورت کنسول پورد ست کنید:

ورود به پورت کنسول
```
Switch(config)# Line Console 0 ↵
```

اعمال پورد
```
Switch(config-ln)# password ------ ↵
```
پورد

برای عمل Login
```
Switch(config-ln)# Login ↵
```

نکته: چرا Line Console 0 ؟ چون یک پورت کنسول بیشتر نداریم بنابراین عدد آن 0 است. اگر سوئیچی داشتیم که دوتا پورت کنسول پشت آن بود می شود

تکته

```
Line console 0
Line console 1
```

حذف پورد
```
Switch(config-ln)# No password ------ ↵
```
پورد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

٤) روی ورود به مود ۲ ، پورد می‌گذاریم :

یعنی اگر شخصی بصورت ریموت یا مخفی به سوئیچ وصل شد
فقط روی مود یک باشد و وارد مود دوم نشود

گاهی کارآموز یا کارمند زیردستی دارید که نمی‌خواهید وارد مود ۲
یا ۳ بشوند پس روی سوئیچ برای ورود به مود ۲ پورد ست می‌کنیم،

Switch (config) # enable password ------
پورد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

۵) ریموت را روی سوئیچ فعال می‌کنیم:

همیشه که لب تاپ به دلت توی طبقه‌ها نمی‌چرخیم باید بتوانیم از اتاق خودمان به سوئیچ‌ها ریموت بشویم.

الف) قابلیت ریموت شدن پیش‌فرض غیرفعال است.

ب) سوئیچ باید IP داشته باشد که پیش‌فرض ندارد.

ج) هر سوئیچ می‌تواند هم‌زمان ۱۶ کاربر داشته باشد که به آن وصل شوند باید برای این کاربرها پسورد بگذارید:

```
Switch(config)# Interface Vlan 1
Switch(config-if)# Ip Address ---------- ----------
                                  Ip        Subnet mask
Switch(config-if)# No shutdown
```

ورود به کارت شبکه سوئیچ

Ip می‌دهیم

کارت شبکه فعال می‌کنیم (از ال shutdown است).

```
Switch(config)# Line vty 0 15
Switch(config-Ln)# password ------
Switch(config-Ln)# Login
```

تعداد کاربران هم‌زمان ریموت

← اعمال پسورد

← جهت لاگ‌این نمودن

یعنی چه تعداد برای یک نفر فقط 0 را بزنید

مثلاً فقط 0 یا مثلاً 0 و 0 یا مثلاً 0 15

www.somatec-co.com
Farzad Heydari
By Houshang Heshmati

برای ریموت شدن باید IP روی لپ تاپ (سیستم) خودمان هم ست باشد (در یک شبکه باشیم)

وارد cmd می‌شویم و ریموت می‌شویم:

C:\> ipconfig /all IP خودتان را ببینید

← با دستور Telnet به سوئیچ وصل می‌شویم

C:\> Telnet 10.0.0.1 مثلا IP سوئیچ می‌باشد

اگر دستور Telnet در محیط cmd کار نمی‌کند باید آن فعال شود:

نکته:

← Control panel

(۱) ← programs

← گوشه بالا سمت چپ Turn windows feature on off

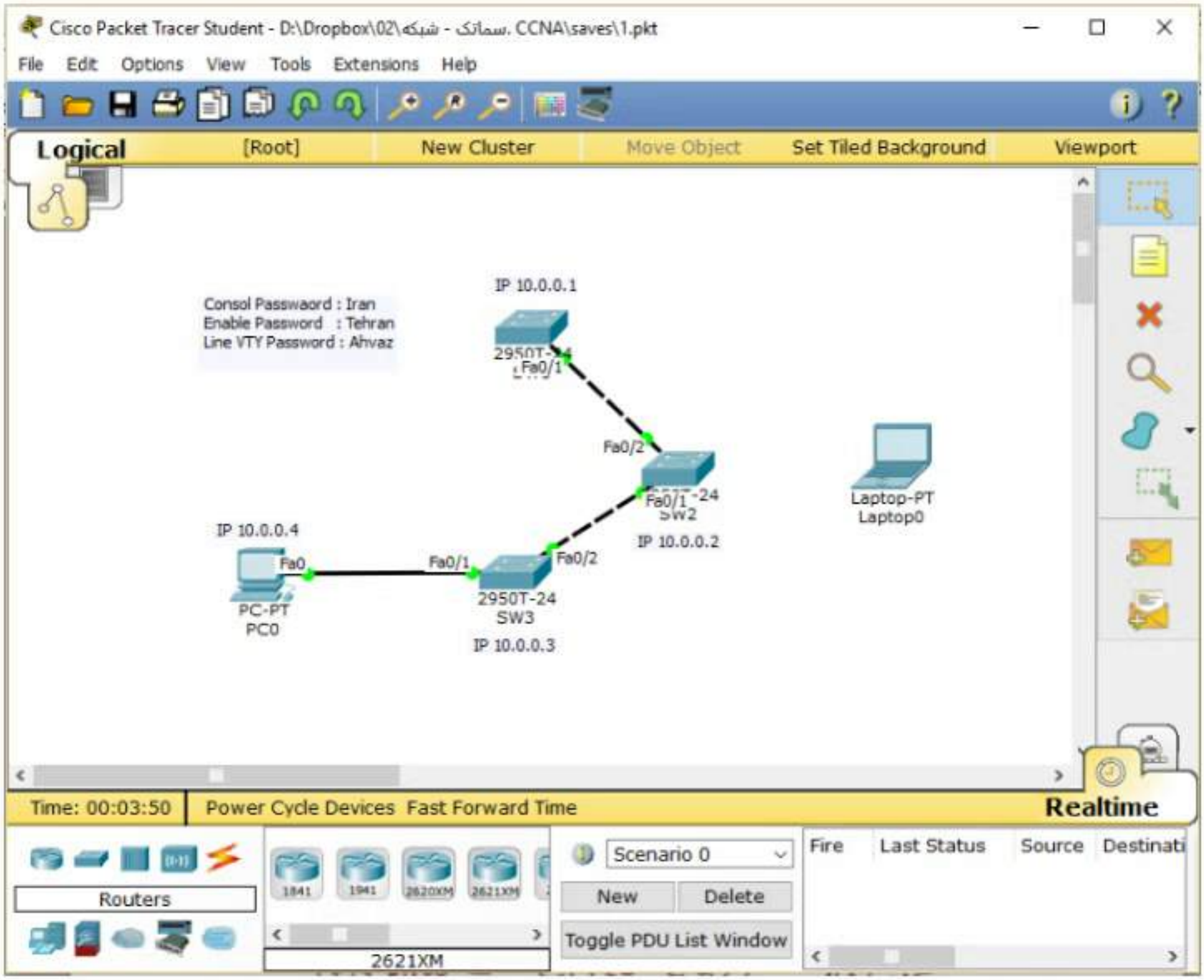
← Telnet client ☐ را پیدا کرده و ✓ بزنید

یا
or

(۲) داخل cmd تایپ کنید

pkgmgr/iu:"Telnet client"

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

جلسه دوم :

چگونه تنظیمات سوئیچ را ذخیره کنیم؟

اگر سوئیچ ریست شود (خاموش روشن شود) همه تنظیمات پاک می‌شود
هر سوئیچ دارای چند حافظه است که ابتدا با آنها آشنا می‌شویم :

۱) RAM به running config معروف است. حافظه موقت است و همه تنظیمات هنگام که سوئیچ روشن است بر روی این حافظه قرار دارد.

۲) Flash معادل HDD است و سیستم عامل سوئیچ (IOS) روی آن نصب است. به صورت اکسترنال هم موجود است.

۳) NVRAM حافظه پاک نشدنی از نوع رم (none volatile) که به Start-up Config معروف است و اگر Save کنیم در این ذخیره می‌شود

www.sarnatec-co.com
Farzad Heydari
By Houshang Heshmati

۴) ROM Read only است و بایوس و فرم روی آن ذخیره شده است.

Switch# show running-config ↵ نمایش محتویات RAM
Switch# show Startup-config ↵ نمایش محتویات NVRAM
Switch# show flash ↵ نمایش IOS

حیات Save کردن اطلاعات و تنظیمات از RAM به NVRAM :

۱) Switch# Copy running-Config Startup-Config ↵
Destination filename [Startup-Config]? سوال می پرسد
اگر q بزنید Save نمی کند. اگر Enter بزنید Save می کند.

۲) یک دستور ساده تر و قدیمی تر هم وجود داشت ولی از روش بالایی استفاده کنید:

Switch# wr ↵ write memory

بدون سوال کردن کپی می کند و احتمال اشتباه زیاد است
در ضمن در امتحان بین المللی wr کار نمی کند.

مانیتورینگ اطلاعات سوئیچ :

یک دستور بسیار مهم که اطلاعات سوئیچ را نشان می دهد. با این دستور همیشه سر و کار خواهید داشت:

www.sematec-co.com
Farzad Heydari
By Houshamang Ashmai

Switch# Show Running-Config
Switch(config)# Do Show RUN ← اگر در مود ۳ بودیم برای که برگردیم مود ۲

- هنگامی که Show Run می‌گیرید پسوردهای ذخیره شده هم نمایش داده می‌شوند. می‌توانیم ذخیره شدن پسوردهای سوئیچ را بصورت Encryption انجام بدهیم تا در Show Run نمایش داده نشوند:

Switch(config)# Service password-encryption ↵

- اگر دستور فوق را با گذاشتن No در ابتدای آن کنسل کنیم پسوردهای قبلی دوباره قابل نمایش نمی‌شوند بلکه پسوردهای جدیدی که ست کنیم دیگر Encryp نمی‌شوند.

* همیشه Service password-Encryption را فعال کنید *

تعریف کاربر برای سوئیچ: username

ابتدا یک کاربر با پسورد می‌سازیم سپس در قسمت‌های مختلف از آن برای ورود استفاده می‌کنیم:

1) Switch(config)# username ..... password ..... ↵
نام کاربری — پسورد

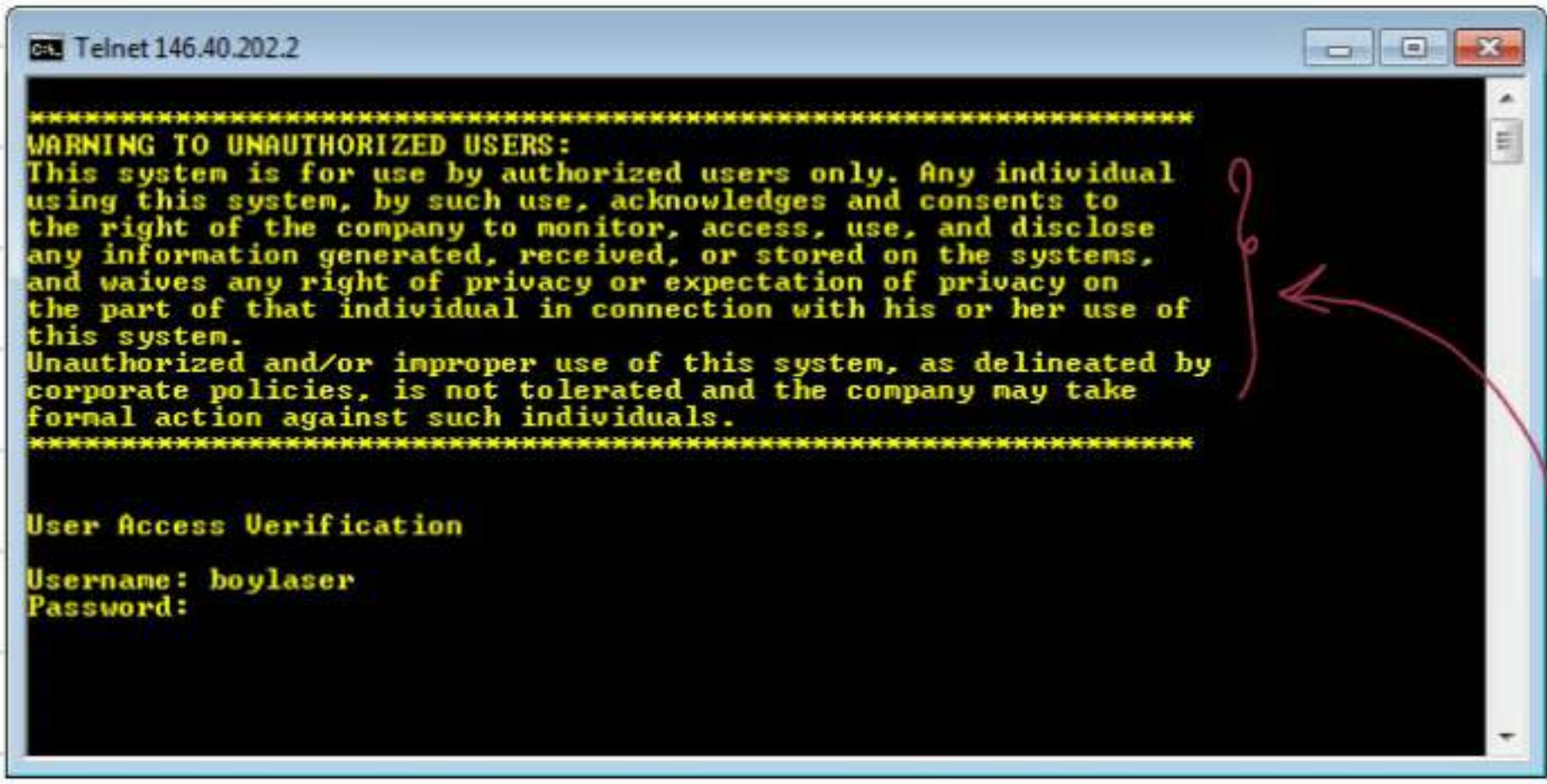
2) Switch(config)# Line vty 0 15 ↵
Switch(Config-line)# Login Local ↵ ← استفاده از username password هنگام Telnet

3) Switch(Config)# Line console 0 ↵
Switch(config-line)# Login Local ↵ ← استفاده از username password هنگام اتصال با کابل Console

www.sematec.co.com
Farzad Heydari
By Houshang Heshmati

اگر username و password تعریف نکرده باشید و login local را بست کنید و از محیط روتر خارج شوید برای همیشه قفل می‌شود. مواظب باشید

Banner



* Banner یک پیغام است که توسط ادمین روی روتر تنظیم می‌شود تا هنگام ورود به آن نمایش داده شود:

۱) در مود ۳ نوشته می‌شود
۲) جزو الزامات امنیتی روتر است
۳) باید تهدیدآمیز باشد
۴) نباید هیچ اطلاعاتی در خصوص اینکه روتر برای کجاست و چه استفاده‌ای دارد، بدهد.

این یک شبکه خصوصی است اگر تلاش کنید که وارد شوید تحت پیگرد قانونی قرار خواهید گرفت.

www.sematec-co.com
Farzad Sayyah
By Hoyshang Ilkhamato

This is a private Network, if you attempt to login you will be prosecuted by goverment

massage of the day

Switch(Config)# banner motd " ↵

{ متن بنر } ↵"

نهایت خط اول
و خط آخر متن خود
یک سطر * بزنید
تا مطلب شما داخل
یک کادر ستاره مانند قرار بگیرد و به چشم بیاید.

۱) این پیغام (motd) قبل از صفحه ورود به لوئیچ نمایش داده می‌شود.

۲) نوع دیگری banner داریم که بعد از ورود به Vty یا اتصال کنسول نمایش داده می‌شود. این پیغام برای کسانی است که جزو شبکه شما هستند و وارد لوئیچ شده‌اند.

Switch(Config)# banner exec " ↵

{ متن بنر } ↵"

مثلاً شماره تماس ادمین
یا اطلاعاتی در خصوص مشکلات
لوئیچ و ...
و خوش آمد گویی به همکاران

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Login Timeout

هنگام اتصال از طریق کنسول یا ریموت (Telnet) اگر بعد از چند دقیقه فعالیتی انجام ندهید از محیط خارج خواهید شد.
این زمان (Time out) را می‌توان تنظیم کرد. بهتر است خیلی کم نباشد و خیلی هم طولانی نباشد. ۳۰ دقیقه زمان مناسبی است.

برای کنسول

```
Switch (Config)# Line Console 0 ↵
Switch(Config-line)# exec_time ..... .....
```

دقیقه ثانیه

برای ریموت

```
Switch (Config)# Line Vty 0 15 ↵
Switch(Config-line)# exec_Time ..... .....
```

دقیقه ثانیه

اگر بجای دقیقه و ثانیه هر دو را صفر بدهید این Timer غیرفعال می‌شود.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Secret

پسورد های ست شده در کوئیچ های Cisco حتی اگر Encryp شده باشند باز هم به راحتی باز می شوند کافی است در اینترنت عبارت Cisco password Cracker را سرچ کنید. هم نرم افزار و هم وب سایت هایی که کد Encrypt شده پسورد را می گیرند و پسورد تحویل می دهند.

درجه بعدی امنیت استفاده از Secret بجای password است.
کلمه عبوری که با استفاده از Secret ساخته شود از مدل MD5 بوده و با هیچ ترفندی بازیابی نمی شود.

Switch(Config)# enable Secret ..... ↵
کلمه عبور

Switch(Config)# username ..... Secret ..... ↵
نام کاربری کلمه عبور

از این به بعد همیشه از Secret استفاده کنید

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Interface

کانفیگ پورت های سوئیچ :

هر پورت روی سوئیچ را می توان جداگانه کانفیگ نمود.

سوئیچ ها بسته به نوع و مدل دارای ۲۴ یا ۴۸ یا ... پورت هستند.
اگر دستور Show Run را بزنید پورت ها، سوئیچ را نمایش می دهد.

انواع پورت ها

1) Ethernet 10 mb/s
۲) fastEthernet 100 mb/s ← Types
۳) Gigabit 1 Gb/s
۴) TenGigabit 10 Gb/s

جهت ورود به هر پورت از دستور زیر استفاده می کنید:

Switch (config) # interface .... / ..... ↵

Type

شماره ماژول

شماره پورت

www.senatec-co.com
Farzad Heydari
By Houshang Heshmati

مثال :

Switch(Config)# interface fastethernet 0/5 ↵

پورت ۵ سوئیچ از نوع fastethenet

Switch(Config)# interface gigabit 0/2 ↵

پورت ۲ سوئیچ از نوع Gig

عدد صفر برای ماژول یعنی پورت fixed هست. یعنی روی مادربرد سوئیچ از اول بوده. اگر سوئیچ پورت کم بیاورد و شما از طریق ماژول به آن پورت اضافه کنید شماره ماژول را بجای صفر می زنید. با دستور show run اطلاعات پورت را می توانید نگاه کنید.

پورت هایی را که استفاده نمی کنید خاموش کنید. پورت به صورت پیش فرض روشن up است.

Switch(config-if)# Shutdown ↵

وقتی وارد یک پورت می شوید

```
Switch#ena
Switch#conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#int
Switch(config)#interface f
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#shu
Switch(config-if)#shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, change
state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
```

ورود

Shutdown

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

می‌توانید روی هر پورت که لازم دارید یک توضیح هم اضافه کنید بعدا اگر ریموت وصل شدید می‌توانید از روی توضیح بفهمید این پورت به چی وصل شده است.

```
Switch(Config)# interface fastEthenet 0/2 ↵
Switch(Config-if)# description Switch3 fast0/3 ↵
```

ورود

مثلاً یک لوپینچ دیگه با پورت فست ۳ خودش وصل شده

```
Switch # Show interface description ↵
```

نمایش توضیحات پورت‌ها

interface	Status	protocal	description
VL1	up	up	
fas0/1	up	up	
fas0/2	up	up	Switch3 fast0/3

بهتر است اینجوری نام‌گذاری کنید: B1F2R18N20

ساختمان طبقه رک نود

می‌توانید سرعت پورت را کاهش بدهید (لازم می‌شود)

```
Switch(Config-if)# Speed 10
Switch(Config-if)# Speed 100
Switch(Config-if)# Speed Auto
```

سرعت را ۱۰ mbps می‌کند

سرعت را ۱۰۰ mbps می‌کند

سرعت را خودش تنظیم می‌کند

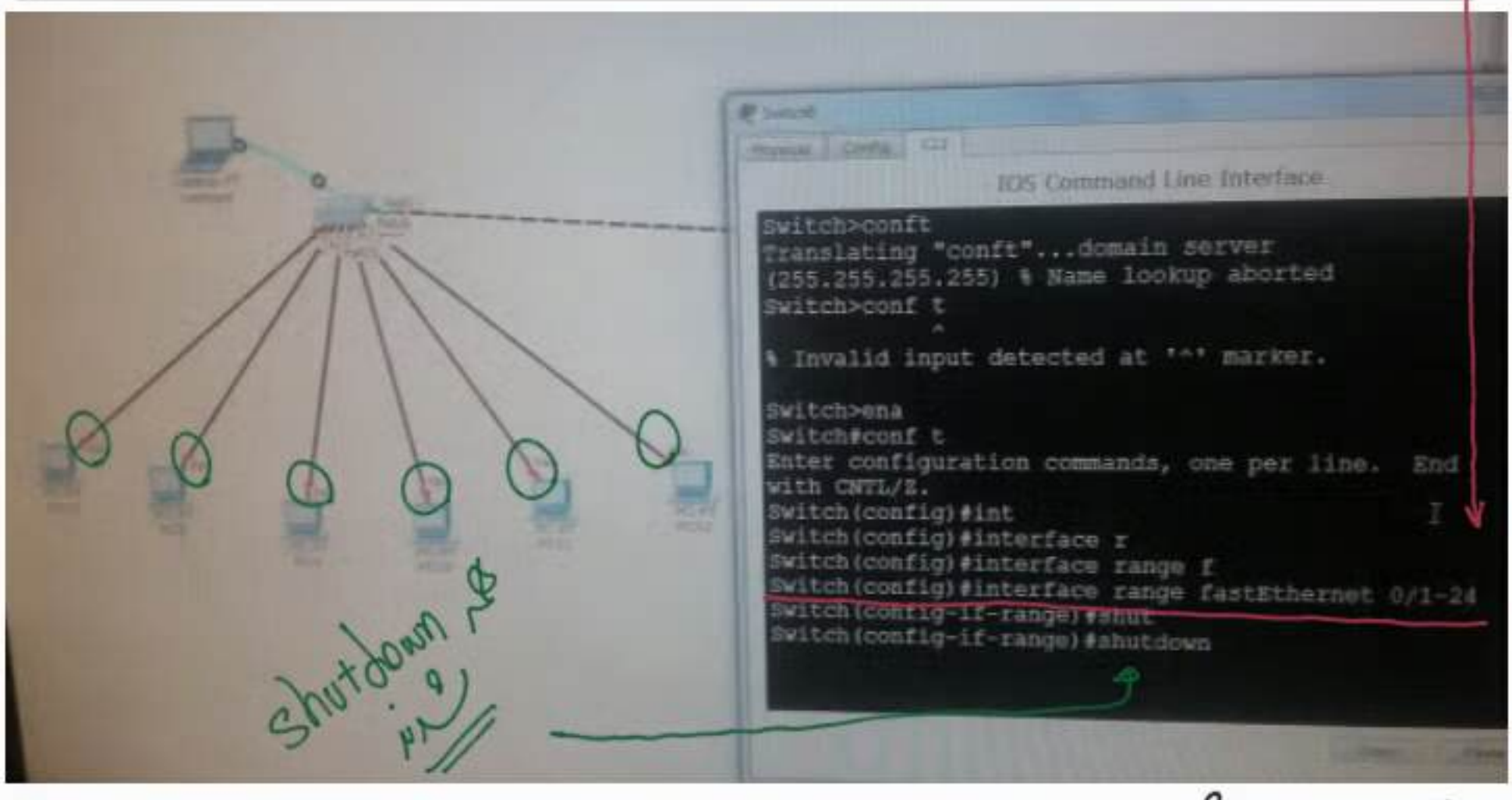
www.shmateo.com
Farzad Heydari
By Houshang Heshmati

خیلی مهم و کاربردی

گاهی می‌خواهید یک دستور روی تعدادی پورت اعمال شود بجای اینکه تک تک پورت ها را دستور بدهید می‌توانید چند پورت را باهم انتخاب کنید و سپس دستور بدهید:

```
Switch(Config)#interface Range fastEthernet 0/1-5
Switch (Config-if -range)#
```

مثلاً یک تا پنج



اگر ترتیب شماره پورت ها پشت سر هم نبود:

```
Switch(Config)#interface Range fastEthernet 0/1 , fastEthernet 0/3
, fastEthernet 0/5
```

با کاما جدا می‌کنیم مثلاً برای ۱ و ۳ و ۵

www.sematec-co.com
Farzad Haydari
By Houshang Heshmati

Macaddress

مک آدرس یک نشانه ۴۸ بیتی (مبنای Hex) روی هر کارت شبکه است که مختص بوده می باشد (unique) و هیچ ۲ کارت شبکه در دنیا دارای یک مک آدرس یکسان نمی باشند.

اصطلاحاً می گویند توسط کارخانه سازنده روی کارت شبکه Burn شده

در سیسکو به مک آدرس BIN (Burn in address) می گویند

در ویندوز به مک آدرس physical address می گویند

۲۴ بایت	۲۴ بایت
نشان شرکت سازنده است OUI	نشان مدل و شماره کارت شبکه است

۶ بیت (۶ رقمی)

برای سیسکو 006052

در ویندوز برای مشاهده مک آدرس کارت شبکه در محیط cmd :

۱) getmac

دو روش دارید

۲) IpConfig /all → physical address می نویسد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

port Security

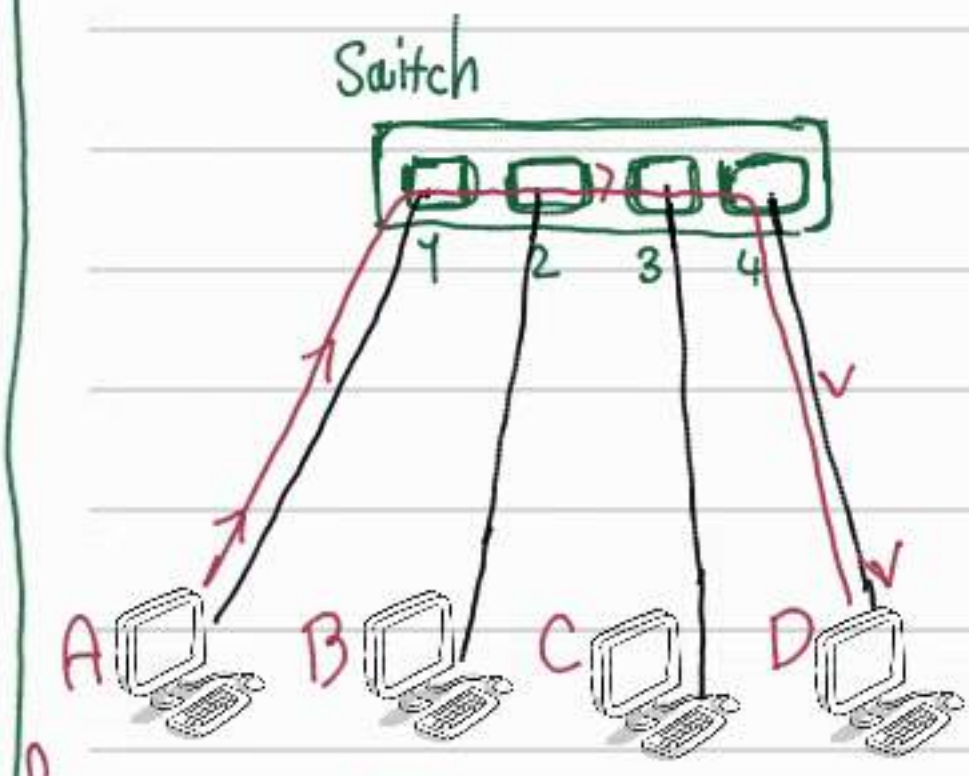
مقدمه :

هاب : آدرس دهی نمی فهمد (layer 1) برای همه پورت می فرستد .

Switch : آدرس دهی می فهمد (layer 2) برای آدرس مشخص می فرستد .

Switch operation

در لایه ۲ باید مک آدرس و مقصد را برای ارسال بسته بزنیم



macaddress table (Switch)

1	A
4	D

وقتی A می فرستد می کند learn

D را ندارد پس درخواست A را بروی همه پورت ها flood می کند و D که جواب می دهد D را (درنمایید learn می کند و به A جواب برمی گردد. (learn می شود)

Source mac
destination mac

Switch # show mac address-table — نمایش جدول مک آدرس لوئیچ

Switch # clear mac address-table — پاک کردن جدول مک آدرس

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

ARP : یعنی مبدا IP می فرستد و از مقصد Mac address می گیرد. (برود کشی)

port Security چیست؟ اگر کامپیوتری را که به سوئیچ وصل است جدا کنیم و یک دستگاه جدید وصل کنیم پورت (Shutdow) خاموش شود.
یعنی mac address کامپیوتر اولی را به سوئیچ معرفی کنیم و اگر mac address عوض شد پورت اتوماتیک خاموش شود.

برای این منظور port Security را روی interface راه اندازی می کنیم

```
Switch(Config-if) # Switchport mode access
Switch(Config-if) # Switchport port-Security
Switch(Config-if)# Switchport port-Security mac-address ----------
```

یعنی این پورت به PC وصل است
امنیتی پورت سیکیوری
مک آدرس دستگاهی که به این پورت وصل است (۲ صفحه قبل یادگرفتید از کی ببینید)

اگر یک دستگاه جدید با mac address جدید وصل شود و پورت خاموش شود باید یکبار پورت را خودمان ببندیم و باز کنیم Shut و No shut.

```
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0060.70
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0001.42
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address 0010.11
!
```

* show run نشون می دهد

www.cmatc.com
Farzad Heydari
By Houshang Heshmati

اگر تعداد کامپیوتر ها زیاد باشد نمی توانیم دانه دانه برای هرکدام mac address وارد کنیم. در این صورت از Sticky استفاده می کنیم.

در این صورت اگر دستور را بزنیم اولین کامپیوتری که به پورت وصل شود macaddress خود را به سوئیچ می دهد.

Switch(Config-if)# Switch port-Security mac-address sticky ↵

ورود به اینترفیس

```
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/7
Switch(config-if)#swi
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#swit
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security
Switch(config-if)#swit
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-
address sti
Switch(config-if)#switchport port-security mac-
address sticky
```

```
nterface FastEthernet0/4
switchport mode access
switchport port-security
switchport port-security mac-address 0010.

nterface FastEthernet0/5
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0000.0C3C.A878
!
interface FastEthernet0/6
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.0FB0.BD5C
!
--More--
```

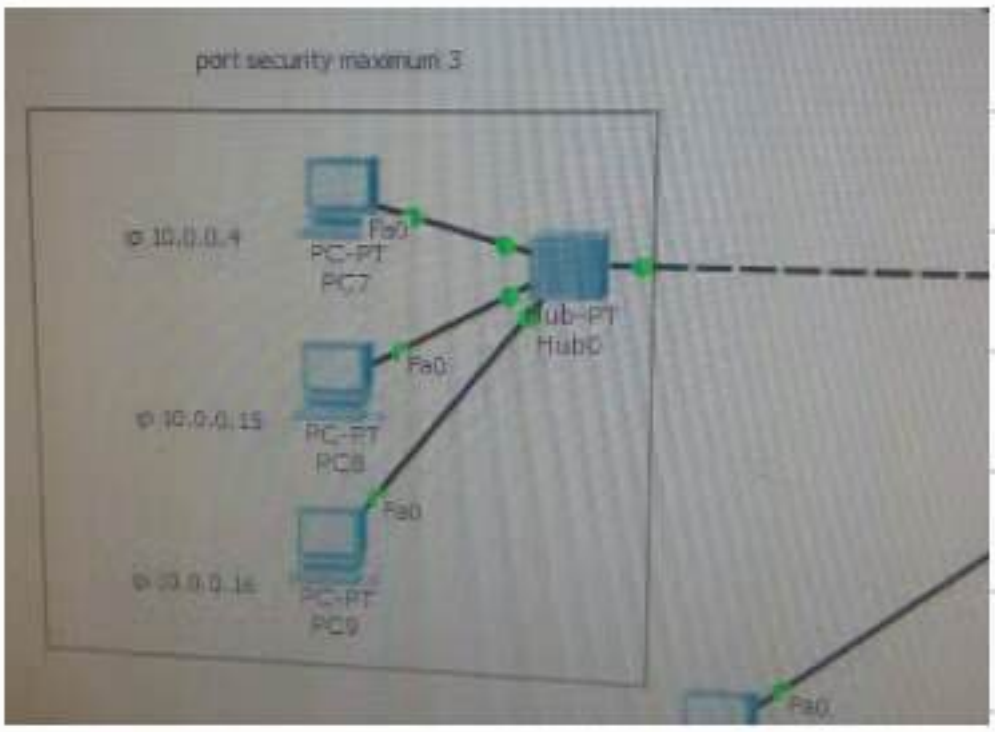
Sticky

در show Run می زند sticky

مثلاً برای یک شرکت کوچک که ۲۴ پورت که بخواهید port Security انجام بدهید:

Switch(Config)# interface Range fastEthernet 0/1-24 ↵
Switch(Config-if)# Switchport mode access ↵
Switch(Config-if)# Switchport port-Security ↵
Switch(Config-if)# Switchport port-Security mac-address sticky ↵

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati



در ایران در بسیاری از ادارات در یک اتاق یک Hub می گذارند و چند کامپیوتر به یک پورت وصل می شوند

می توان برای پورت تعریف کرد که چند تا macaddress را sticky یاد بگیرد و به تعداد مورد نیاز تنظیم کنیم

```
Switch(config-if)# Switchport mode access
Switch(config-if)# Switchport port-Security
Switch(config-if)# Switchport port-Security maxium ------
Switch(Config-if)# Switchport port-Security mac-address sticky
```

show run نمایش می دهد.

```
with CNTL/Z.
Switch(config)#int
Switch(config)#interface fa 0/8
Switch(config-if)#swi
Switch(config-if)#switchport mod acc
Switch(config-if)#switchport mod access
Switch(config-if)#swi
Switch(config-if)#switchport por
Switch(config-if)#switchport port-security
Switch(config-if)#swit
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security max
Switch(config-if)#switchport port-security maximum 3
Switch(config-if)#swi
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-
address sti
Switch(config-if)#switchport port-security mac-
address sticky
```

```
00E0.A3A6.7E5E
!
interface FastEthernet0/8
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0000.0C11.3913
 switchport port-security mac-address sticky
0030.A328.625E
 switchport port-security mac-address sticky
0030.F2A9.3072
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
```

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Violation

می توان پورت را طوری تنظیم کرد که کامپیوتر متجاوز به شبکه و پورت وصل شود و پورت خاموش نشود ولی اطلاعاتی ارسال نشود و اگر کامپیوتر قبلی دوباره به پورت وصل شود کار کند.

Switch(Config-if)# Switchport port-Security violation .....

- Shutdown ← دیفالت : پورت خاموش می شود
- Restrict ← پورت اجازه دسترسی ندارد
- protect ← همان Restrict بدون لاگ

} ۳ تا انتخاب داریم

Switch # Show port-Security ← نمایش مشخصات پورت سیکیورتی

در حالت Restrict هر بار که کامپیوتر متجاوز بسته ای ارسال کند و پورت جلوی آن را بگیرد یک لاگ ثبت می شود (کانتر دارد می شمارد.)
این لاگ در کانفیگ Save می شود برای یک شبکه بزرگ ممکن است خیلی حافظه اشغال شود. اگر ادمین پای کانفیگ نباشد و لاگ را چک نکند بهتر است از protect استفاده شود که لاگ نمی اندازد.

اگر مک آدرس نداده باشیم یا اشتباه وارد شده باشد و ... می توانم حافظه پورت را پاک کنم

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Switch # clear port-Security all

```
switchport port-security

Switch#ena
Switch#conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switch
Switch(config-if)#switchport po
Switch(config-if)#switchport port-security v
Switch(config-if)#switchport port-security violation
re
Switch(config-if)#switchport port-security violation
restrict
Switch(config-if)#
```

```
)#switchport mod acc
)#switchport mod access
)#swith port
)#swithpo
)#swithport
)#swithport PO
)#swithport po
)#swithport port
)#swi
)#switchport po
)#switchport port-security
)#switchport port-security mac
)#switchport port-security mac-address BCAE.C55E.2CI
)#switchport port-security V
)#switchport port-security Violation RE
)#switchport port-security Violation REstrict
)#switchport port-security Violation SHU
)#switchport port-security Violation SHUtdown
)#SHUT
)#SHUTdown
)#NO SHU
)#NO SHUtdown
)#_
```

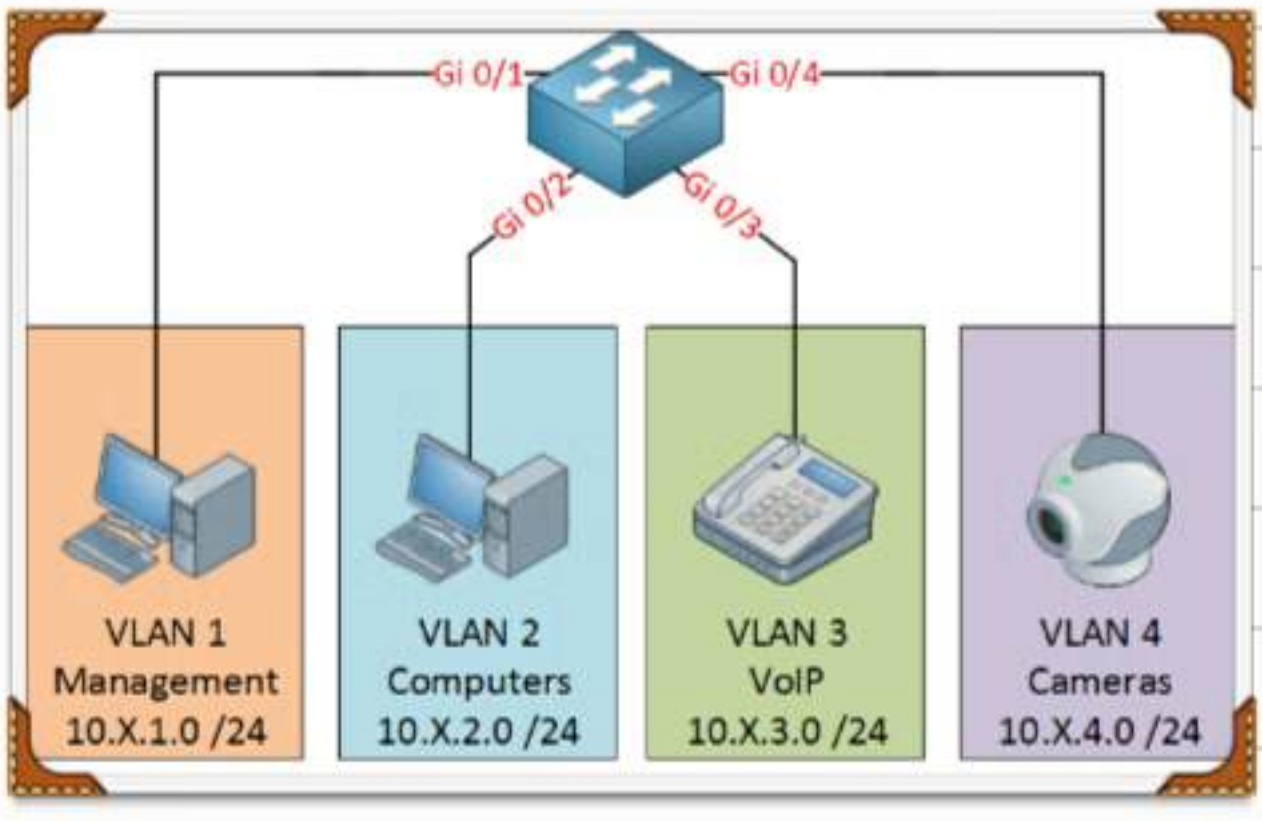
www.sshmatch-co.com
Farzad Heydari
By Houshang Heshmati

خیلی مهم

VLAN

(virtual LAN)

می‌توان روی پورت های سوئیچ، چند شبکه مختلف ساخت که باهم ارتباط نداشته باشند. مثلاً بخش حسابداری و طراحی و مهندسی همه از یک سوئیچ پورت دریافت کنند ولی کامپیوترهای طراحی به کامپیوترهای حسابداری دسترسی نداشته باشند.



در حقیقت روی سوئیچ چند شبکه مجازی می‌سازیم که:

۱) تقسیم‌بندی شبکه‌ها

۲) کوچک کردن برادکست دامین

۳) امنیت و جدا شدن شبکه‌ها

که به هر کدام یک VLAN می‌گوییم که هر کدام می‌شود یک Broadcast domain

ارتباط بین VLAN ها قطع است

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

هر VLAN با VLAN ID مشخص می‌شود که شماره‌ای منحصر به همان vlan است:

VLAN ID

۱) بین صفر و 4095 است

۲) صفر و 4095 رزرو شده است

۳) 1 بعنوان Default است یعنی همه پورت های سوئیچ از اول روی یک vlan با VlanID=1 هستند

۴) 1-1005 برای Normal Vlan

۵) 1002-1005 برای FDDI و Tokken رزرو است.

۶) 1006-4094 برای Extende Vlan است.

یعنی VTP mode transparent است.

چگونه VLAN بسازیم؟

VLAN 1 که دیفالت هست و به آن دست نمی‌زنیم. از ۲ تا 1001 را می‌توانیم بسازیم.

الف) VLAN را می‌سازیم

ب) پورت ها را به vlan خودشان assign می‌کنیم

همه پورت ها بصورت Default عضو VLAN 1 هستند.

شیت ها قبل از خواب ۵ بار تکرار کنید

www.sematec.co.com
Farzad Heydari
By Houshang Heshmati

Switch (config)# VLAN ..... ↵

VLAN ID ↵

بعد از دستور اول وارد vlan می‌شود

Switch (Config-vlan)# name ..... ↵

↵ یک اسم به vlan بدهید

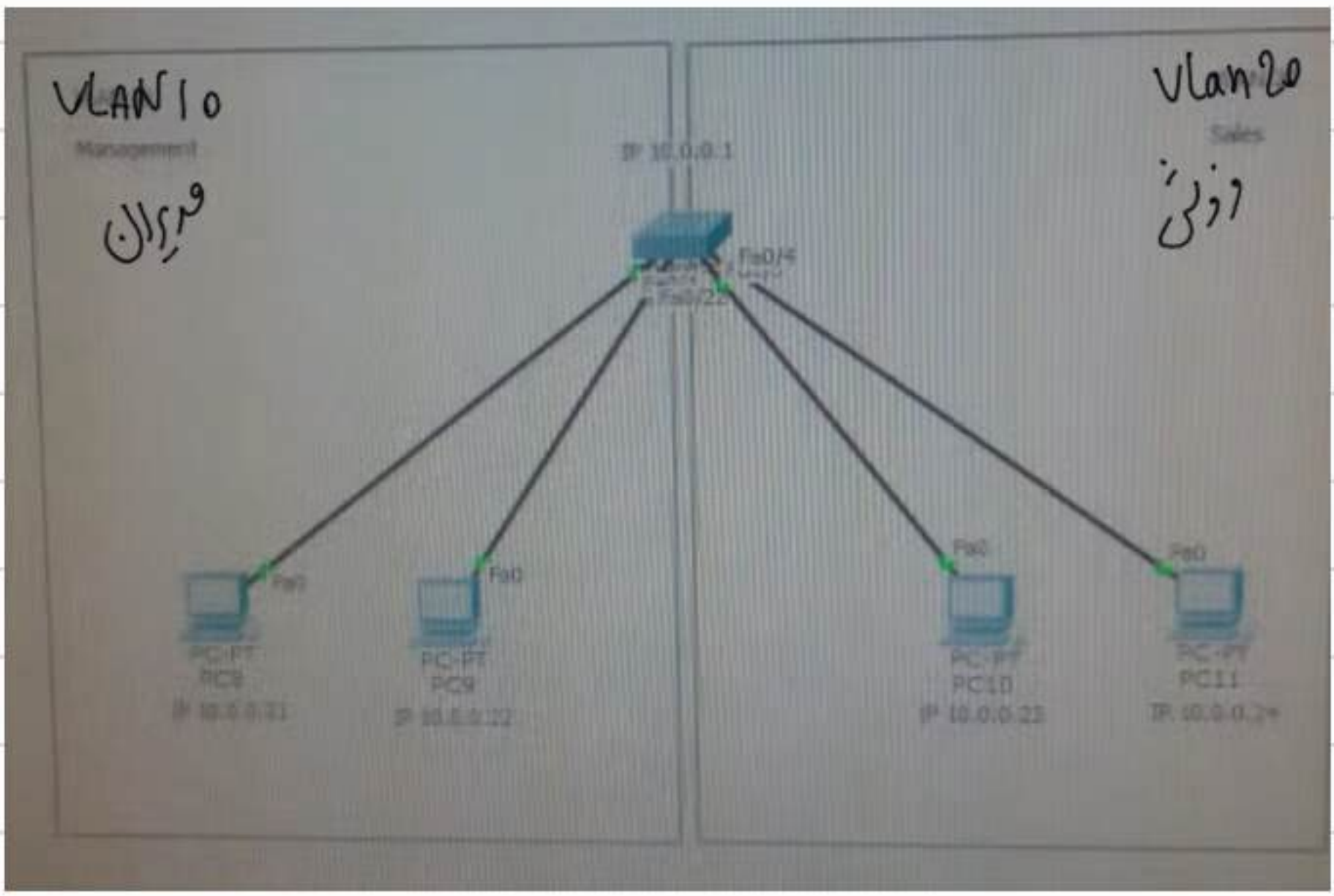
Switch (Config-if)# Switchport access vlan ..... ↵

VLAN ID

داخل interface

Switch# Show vlan Brief ↵

در مود ۲ برای مشاهده vlan ها



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

داخل کانفیگ vlan

```
tch(config)#interface fastEthernet 0/1
tch(config-if)#exit
tch(config)#vlan 10
tch(config-vlan)#name Management
tch(config-vlan)#exit
tch(config)#vlan 20
tch(config-vlan)#name slaes
tch(config-vlan)#exit
itch(config)#intef
itch(config)#intef
itch(config)#intef
itch(config)#inter
itch(config)#interface fas
itch(config)#interface fastEthernet 0/1
itch(config-if)#swi
itch(config-if)#switchport acc
itch(config-if)#switchport access vlan 10
itch(config-if)#exit
itch(config)#interface fastEthernet 0/2
itch(config-if)#switchport access vlan 10
itch(config-if)#exit
itch(config)#interface fastEthernet 0/3
itch(config-if)#switchport access vlan 20
itch(config-if)#exit
itch(config)#interface fastEthernet 0/4
itch(config-if)#switchport access vlan 20
itch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, chan

itch(config-if)#exit
```

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with C
Switch(config)#inte
Switch(config)#interface ra
Switch(config)#interface range fas
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#swi
Switch(config-if-range)#switchport po
Switch(config-if-range)#switchport port-security vl
Switch(config-if-range)#switchport acc
Switch(config-if-range)#switchport access vl
Switch(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
Switch(config-if-range)#exit
Switch(config)#int
Switch(config)#interface ran
Switch(config)#interface range fas
Switch(config)#interface range fastEthernet 0/3-4
Switch(config-if-range)#swit
Switch(config-if-range)#switchport acc
Switch(config-if-range)#switchport access vl
Switch(config-if-range)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
Switch(config-if-range)#exit
```

اگر vlan نباشد خودش ایجاد می‌سازد

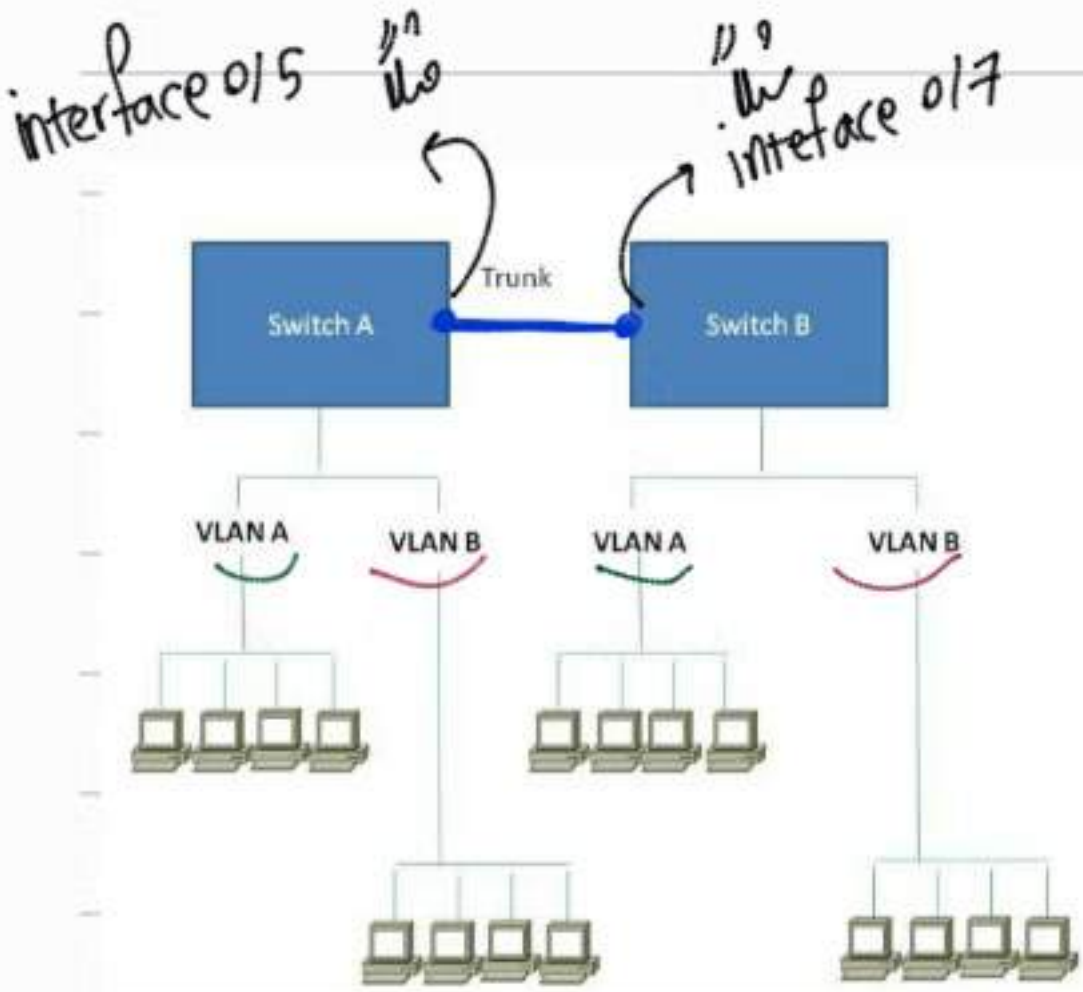
مثلا پورت به یک vlan اختصاص می‌دهیم

این دوتا خیلی مهم هستند ⟹

```
itch#show vlan br
itch#show vlan brief

LAN Name                             Status    Ports
--- ---------------------------------- --------- -------------------------------
    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                               Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                               Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                               Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                               Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                               Gig0/1, Gig0/2
10  Management                       active    Fa0/1, Fa0/2
20  slaes                            active    Fa0/3, Fa0/4
002 fddi-default                     active
003 token-ring-default               active
004 fddinet-default                  active
005 trnet-default                    active
itch#
LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
```

www.samuel-co.com
Farzad Heydari
By Houshang Heshmati

Trunk پورت باید:



می‌توانیم یکی از پورت‌های یک لوئیچ را به یکی از پورت‌های یک لوئیچ دیگر با کابل کراس وصل کنیم

بعد روی هر دو لوئیچ این پورت را پورت Trunk معرفی کنیم

Trunk می‌تواند vlan های دارای vlan ID یکسان را به هم وصل کند.

```
Switch(config-if)# Switchport mode Trunk
```

داخل پورتی که می‌خواهیم ترانک شود (روی هر دو لوئیچ)

```
Switch# Show interfaces trunk
```

نمایش پورت‌های Trunk

```
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#swi
Switch(config-if)#switchport mopd
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode tre
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#exi
```

ساخت

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not prune
Fa0/5       1,10,20
Switch#
```

نمایش روی کدام پورت است

چه vlan هایی وصل شده‌اند.

www.samateo.com
Farzad Haydari
By Houshang Heshmati

پاک کردن یک VLAN :

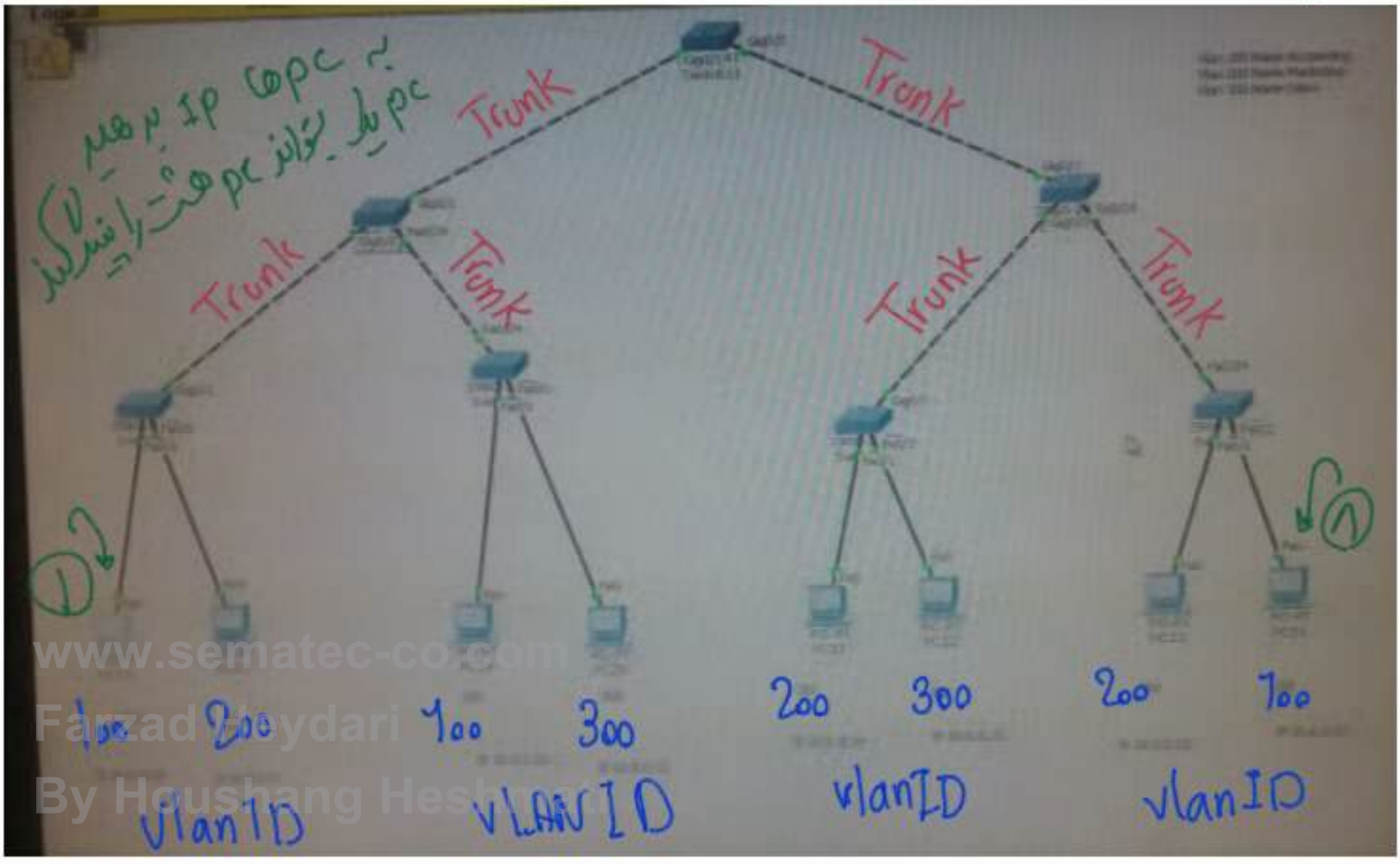
اگر یک vlan را پاک کنید پورت هایی که داخل vlan بوده اند قطع می شوند (غیب می شوند)

باید قبل از پاک کردن vlan همه پورت های آن را عضو VLAN 1 بکنید و بعد اقدام به پاک کردن کنید.

اگر یک vlan ID را پاک کردید و دوباره آن را بسازید پورت ها برمی گردند

Switch(config)# No vlan ..... VLAN ID

تمرین :



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

برای حل تمرین صفحه قبل باید به ۳ نکته زیر توجه کنید:

۱. باید همه سوئیچ ها با پورت Trunk به هم وصل باشند.

۲- پورت gig سوئیچ ها را بعنوان ترانک استفاده کنید

۳- روی همه سوئیچ ها باید همه VLAN ID ها ساخته شده باشند

```
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interfaces tru
Port      Mode         Encapsulation  Status        Native vlan
Gig0/1    on           802.1q         trunking      1
Gig0/2    on           802.1q         trunking      1

Port      Vlans allowed on trunk
Gig0/1    1-1005
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/1    1,100,200,300
Gig0/2    1,100,200,300

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    1,100,200,300
Gig0/2    1,100,200,300
Switch#show vl
Switch#show vlan br
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
100  accounting                       active
200  marketing                        active
300  sales                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

۲ تا پورت gig ترانک

vlan ID های ساخته شده

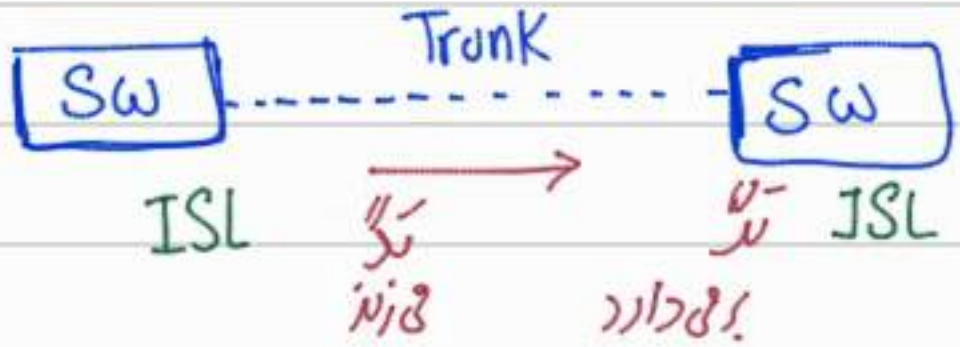
روی سوئیچ ها باید همه vlan ها ساخته شود

پورت های لینک بستند سوئیچ بالا ترانک شده اند.

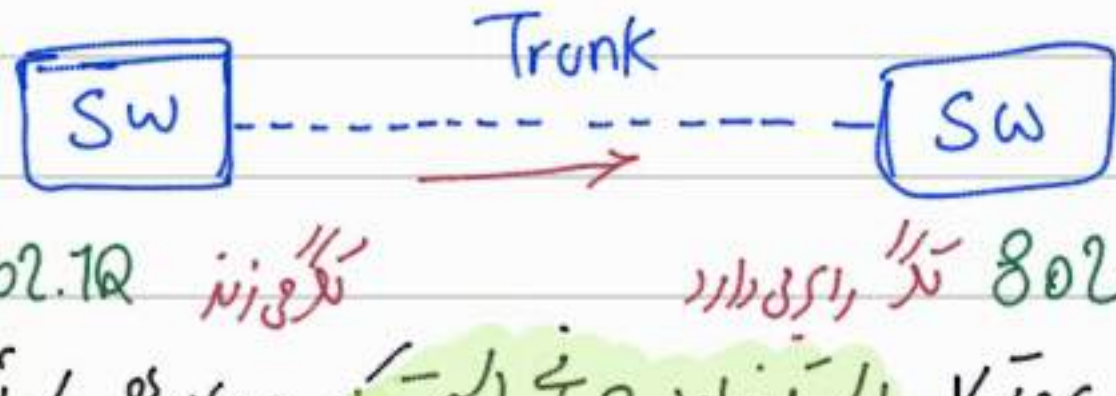
سوئیچ بالایی وسط

www.senatec-co.com
Farzad Heydari
By Houshang Heshmati

پورت ترانک عمل تگ کردن و تگ برداشتن را انجام می دهد:



ISL یک پروتکل قدیمی است که سوئیچ های جدید ندارند. این پروتکل فقط مخصوص سوئیچ های مارک cisco است و برای تگ کردن 30 byte استفاده می کند.



802.1Q یک پروتکل استاندارد جهانی است که بروی همه سوئیچ و مدل های مختلف کار می کند و برای تگ کردن تنها 4 byte استفاده می کند.

علاوه بر این قابلیت پشتیبانی از native vlan را هم دارد.

یادآوری

802.11	وایرلس
802.15	بلوتوث
802.16	وایمکس

⇐ برای اینکه ببینید ترانک از کدام پروتکل استفاده می کند

Switch # show interface Trunk

یکجا نوشته:

Encapsulation

802.1Q

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

اگر از سوئیچ های گران قیمت یا قدیمی استفاده کنید که هر دو پروتکل را دارند باید حتماً به پورت بگویید با کدام پروتکل، ترانک کند وگرنه خطای زیر را خواهید گرفت :

```
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode trun
Command rejected: An interface whose trunk
encapsulation is "Auto" can not be configured
"trunk" mode.
```

Switch(config-if)#Switchport trunk encapsulation ..... ISL یا dot1q

اول این دستور را می زنید بعد ترانک می کنید :

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/
Switch(config)#in
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#swit
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation d
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#swi
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode tru
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

www.farzadheydari.com
Farzad Heydari
By Houshang Heshmati

Native Vlan

در یک سازمان اگر یک vlan دارای کاربران زیادی باشد و ضمنی شلوغ باشد عمل تگ زدن و تگ برداشتن ترافیک باعث کندی شبکه می‌شود.

در کل سوئیچ می‌توانیم به یک (فقط) vlan اجازه بدهیم تا بدون تگ زدن اطلاعات خود را جابه‌جا کنند.

به این عمل Native vlan می‌گویند.

```
Switch (config-if)# Switchport Trunk native-Vlan ------
```
عدد vlan

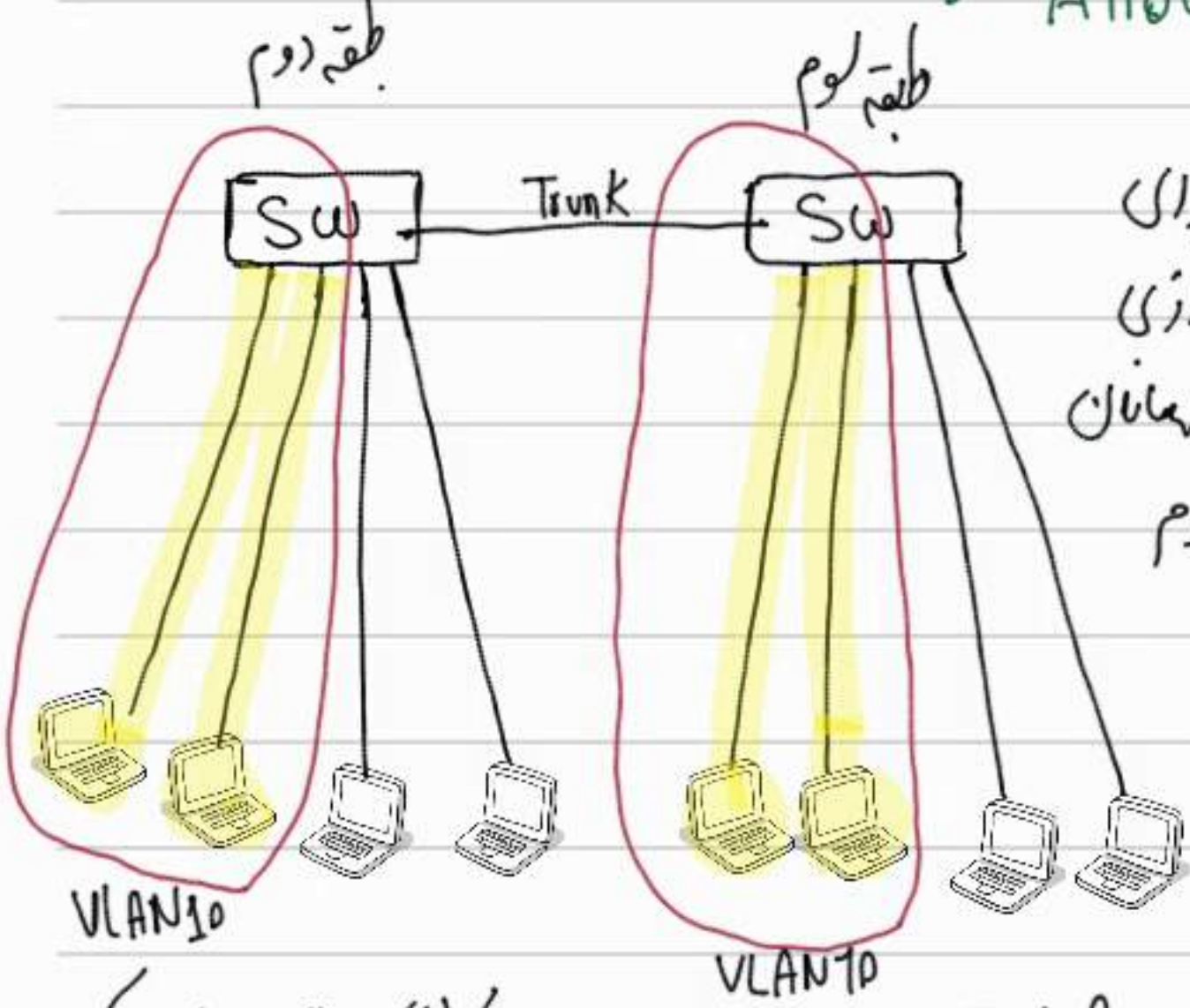
روی هر دو interface هر دو سر Trunk باید این دستور زده شود

روی هر پورت Trunk فقط یک Native vlan داریم

فقط روی 802.1Q هست.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Allowed VLAN :



فرض کنید Vlan 10 را برای مهمانان سازمان راه اندازی کرده اید ولی قرار نیست مهمانان طبقه دوم به مهمانان طبقه سوم دسترسی داشته باشند:

پورت Trunk بصورت default تمام VLAN های با ID یکسان را به هم وصل می کند
با دستورات زیر می توانیم این مورد را تغییر بدهیم:

Switch(Config-if)# Switchport trunk

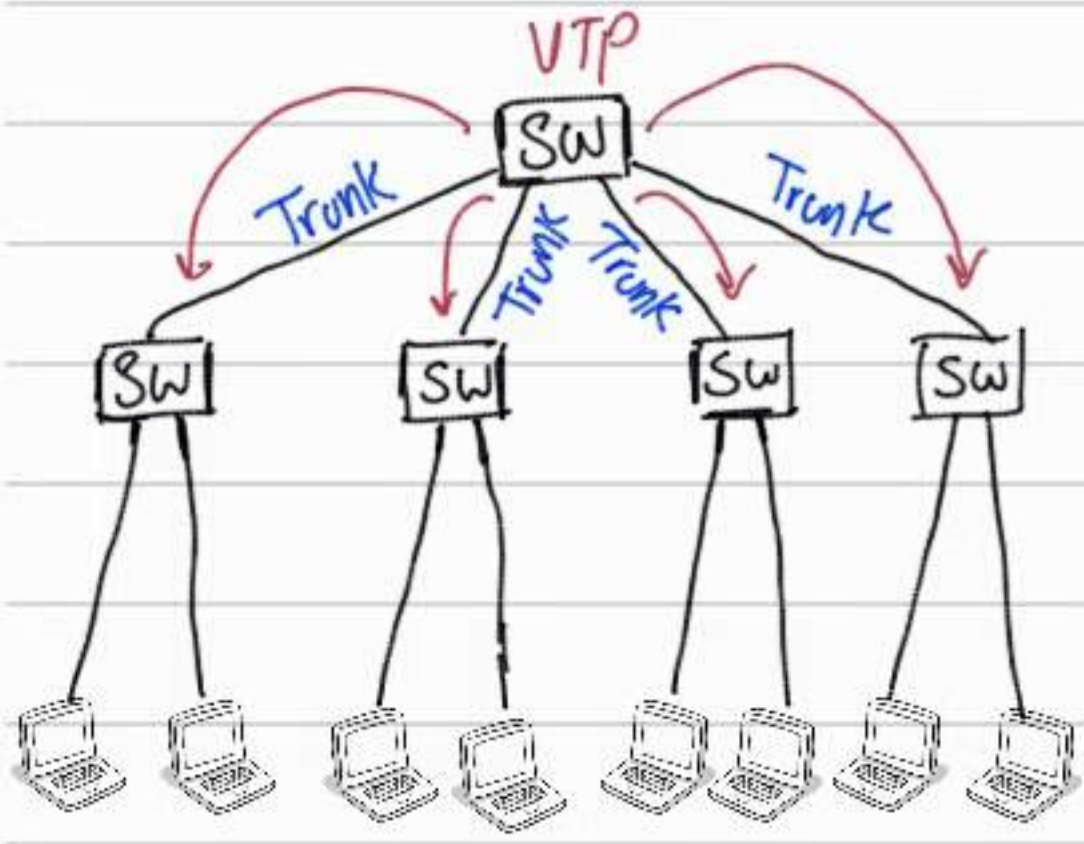
- allowed vlan all — همه vlan ها از ترانک عبور کنند
- allowed vlan add .... (vlan ID) — این vlan هم از ترانک عبور کند
- allowed vlan remove ..... (vlan ID) — این vlan از ترانک عبور نمی کند
- allowed vlan none — هیچ vlan از ترانک عبور نکند
- allowed vlan exept ..... (vlan ID) — بجز این vlan بقیه از ترانک عبور کنند

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

VTP

VLAN Trunking protocol

اگر تعداد سوئیچ ها زیاد باشد و تنظیم تک تک آنها زمان بر شود می توانیم یک سوئیچ مرکزی (سرور) داشته باشیم و تغییرات را روی این سوئیچ اعمال کنیم و روی بقیه سوئیچ ها اعمال شود. برای این منظور باید روی سوئیچ مرکزی VTP اعمال کنیم:



نوع از روی پورت Trunk اعمال می شود برای تعیین VLAN Trunking protocol هست.

ابتدا همه سوئیچ ها را وارد یک domain می کنیم. سپس آنها را به Server و client تقسیم می کنیم (بصورت default همه سوئیچ ها Server هستند) روی سوئیچ که client شده باشد نمی توانیم دستی VLAN بسازیم، بلکه فقط از طریق VTP و از روی سرور می شود.

سپس برای امنیت روی Server ها و client ها پورت می گذاریم و اگر پورت ها یکی باشد می توانند با هم ارتباط برقرار کنند

www.semateg-co.com
Farzad Heydari
By Houshang Heshmati

Switch(Config)# VTP mode .....

یکی از این ۳ تا

- Server
- Transparent
- client

Switch(Config)# VTP domain .....

domain name

Switch (Config)# VTP password .....

password

Switch #show VTP Status

نمایش مشخصات VTP در مود ۲

```
Switch(config)#vtp mo
Switch(config)#vtp mode ser
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp do
Switch(config)#vtp domain Sematec
Changing VTP domain name from NULL to Sematec
Switch(config)#vtp pass
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#vlan 100
Switch(config-vlan)#hos
Switch(config-vlan)#name Accounting
Switch(config-vlan)#exit
```

تغییر نام

Server

```
Switch(config)#vtp mo
Switch(config)#vtp mode cli
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp do
Switch(config)#vtp domain Sematec
Domain name already set to Sematec.
Switch(config)#vtp pass 123
Setting device VLAN database password to 123
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sho vl br

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, Fa0/1
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/2
                                                Fa0/21, Fa0/22, Fa0/23, Gig0/
                                                Gig0/2
100  Accounting                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

client

www.sematec-co.com
Mahdi Heydari
By Houshang Heshmati

```
Switch#sh vt st
Switch#sh vt status
VTP Version                              : 2
Configuration Revision                   : 2
Maximum VLANs supported locally          : 255
Number of existing VLANs                 : 6
VTP Operating Mode                       : Server
VTP Domain Name                          : Sematec
VTP Pruning Mode                         : Disabled
VTP V2 Mode                              : Disabled
VTP Traps Generation                     : Disabled
MD5 digest                               : 0x4A 0xDC 0x36 0xBD 0xC4
Configuration last modified by 0.0.0.0 at 3-1-93 00:09:15
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

نمایش مشخصات VTP

اگر mode را Transparent انتخاب کنیم، اطلاعات سرور روی این سوئیچ اعمال نمی‌شود ولی اطلاعات را از خود عبور می‌دهد و به سوئیچ‌های متصل به خود، می‌رساند. لازم نیست در حالت Transparent نام و پورد بگذاریم

اگر password گذاشته باشیم، سوئیچ‌هایی که password ندارند اطلاعات را دریافت نمی‌کنند و اطلاعات را به سوئیچ‌های متصل به خود انتقال نمی‌دهند.

Configuration Revision

مهمترین بخش VTP همین است. عددی است که سوئیچ‌ها متوجه آپدیت هست یا خیر.
عدد ۲ یعنی ۲ تا کار انجام شده (۱۰۰ vlan ساخته شده و نام account داده شده)
اگر ۴ باشد یعنی ۴ تا کار انجام شده

```
switch>sh vtp sta
VTP Version                              : 2
Configuration Revision                   : 4
Maximum VLANs supported locally          : 255
Number of existing VLANs                 : 7
```

www.sematec-co.com
Azad Heydari
By Houshang Heshmati

چرا خیلی مهم است؟

اگر یک سوئیچ باشد که عدد Revision آن بیشتر از بقیه سوئیچ ها حتی کمی بیشتر باشد تغییرات خود را روی بقیه سوئیچ ها اعمال می‌کند و ناگهان شبکه به فنا می‌رود.

همیشه تحت هر شرایطی هر سوئیچی را که می‌خواهید وارد شبکه بکنید چک کنید عدد Revision آن صفر باشد.

ممکن است سوئیچی قبلاً در شبکه بوده و بدلیلی خارج شده و بعداً دوباره می‌آورید (معمولاً password ها تغییر نمی‌دهند) و وارد شبکه می‌شود و Boom!

- برای صفر کردن عدد Revision سوئیچ یکبار mode سوئیچ را عوض کنید

```
Switch#sh vt sta
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : Sematec
VTP Pruning Mode                : Disable
VTP V2 Mode                     : Disable
VTP Traps Generation            : Disable
MD5 digest                      : 0x56 0x
0x58 0xD3 0xE4 0x40 0xCF
Configuration last modified by 0.0.0.0 at
```

سوئیچ را از شبکه جدا کردیم

این عدد باقی ماند و بعداً دردسر می‌شود

```
Switch(config)#vtp mo
Switch(config)#vtp mode tr
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)#vtp mod
Switch(config)#vtp mode cli
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#do sho vtp st
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : Sematec
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x28 0x24 0x6A 0x1D
Configuration last modified by 0.0.0.0 at 3-1-93 00:23
```

صفر کردن Revision Num

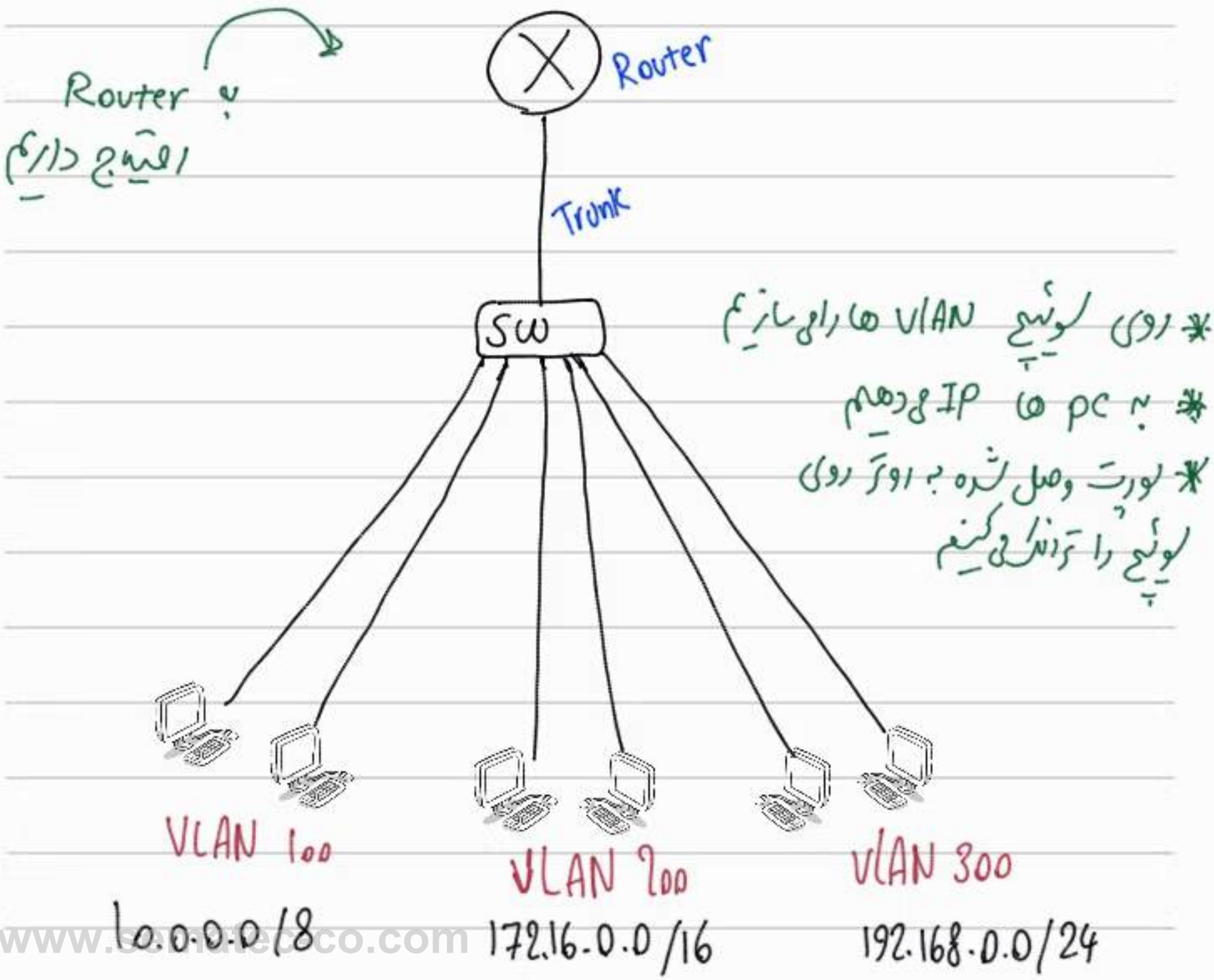
صفر شد

www.sematec.co.com
Farzad Heydari
By Roushang Heshmat

نکته مهم

Inter_VLAN Routing
Router on a Stick

وقتی یک کامپیوتر از vlan 100 بخواهد با یک کامپیوتر از vlan 200 ارتباط پیدا کند باید vlan ها را به هم وصل کنیم بدون اینکه برادکست ها با هم تداخل پیدا کنند:



www.sondeco.com
Farzad Heydari
By Houshang Heshmati

وارد روتر می‌شویم. روتر ضمن پیغام می‌دهد که می‌خواهی تنظیمات Basic را انجام بدهی؟

Would you like to enter Basic management Setup? [yes/no]:

no بزنید و وارد روتر شوید. قبل Switch هست. وارد interface شوید که به سوئیچ وصل است. روتر پورت fastethren کم دارد (۲ تا)

1) Router (config-if) # No shut ↵ پورت روتر خاموش است روشن کنید

همان پورتی که به سوئیچ وصل است

پورتی که به سوئیچ وصل است (Trunk)

2) Router (Config) # interface fastethernet 0/0.100 → VLAN ID

برای هر vlan یک Subinterface بسازید و وارد شوید

3) Router (Config-Subif) # encapsulation dot1Q 100 → VLAN ID

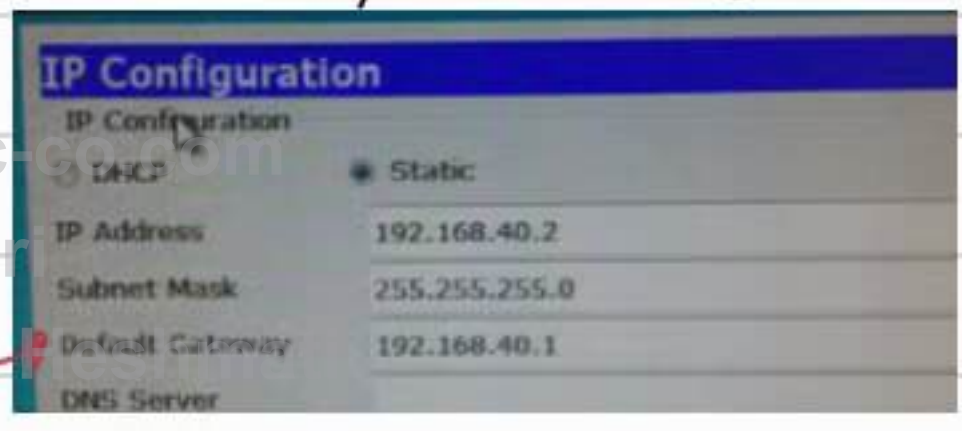
4) Router (Config-Subif) # IP address 10.0.0.1 255.0.0.0

برای آن VLAN یک IP بعنوان default getway تعیین کنید.

معمولاً اولین IP را می‌دهند به default getway

دستورات ۲ و ۳ و ۴ را برای همه VLAN ها تکرار کنید.

سپس روی کامپیوترهای متصل به VLAN ها default getway ها را فعال کنید



www.sematec-co.com
Farzad Heydari
By Houshang Hashemi

```
Router(config)#interface fa
Router(config)#interface fastEthernet 0/0.60
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.60, changed s

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthe

Router(config-subif)#en
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.60.1
% Incomplete command.
Router(config-subif)#ip address 192.168.60.1 255.255.255.
Router(config-subif)#exit
```

روی Router Subinterface 60

```
Router(config)#int
Router(config)#interface fas
Router(config)#interface fastEthernet 0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.40, change

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastE

Router(config-subif)#en
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.40.1
% Incomplete command.
```

روی Router Subinterface 40

```
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vl
Switch(config-if)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
Switch(config-if)#exi
Switch(config)#int
Switch(config)#interface acc
```

ساخت vlan ها روی پورت

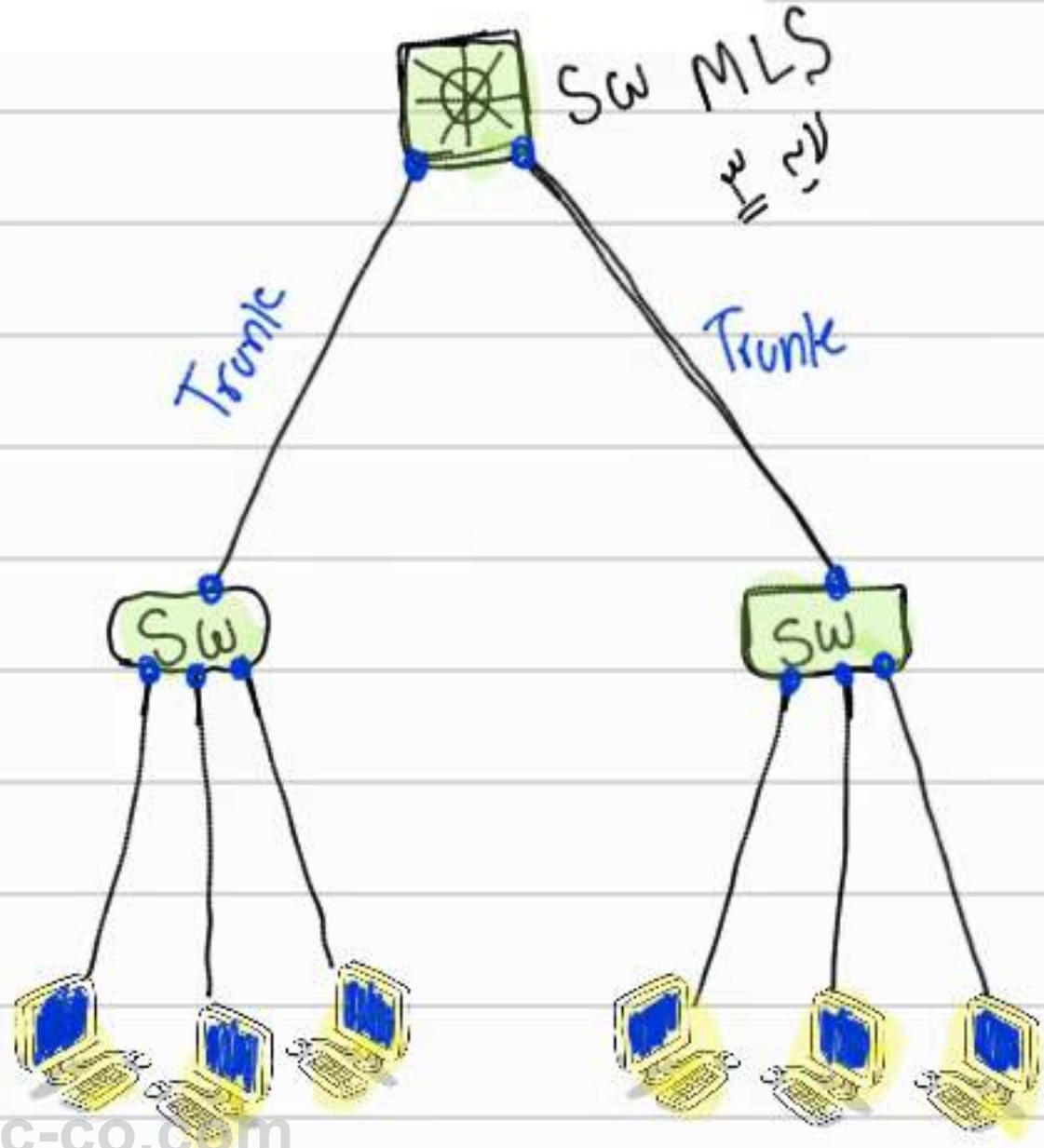
```
Switch(config)#int
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#swi
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

پورت ترانک پورتها

www.cisco-ccna.com
Farhad Heydari
By Houshang Heshmati

امروزه در ادارات و شرکت ها بجای روتر از سوئیچ لایه ۳ (MLS) استفاده می شود. MLS (Multi layer Switch) یعنی این سوئیچ هم در لایه ۲ (Mac address) و هم در لایه ۳ (Ip address) کار می کند و از روتر هم گرانتر هست.

Cisco 3760 (MLS)



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

چگونه از سوئیچ لایه ۳ بجای روتر استفاده کنیم؟

پورت های ترانک راه می سازیم ، VLAN ها راه می سازیم . روی هر interface نماینده VLAN خودش راه می سازیم در داخل نماینده VLAN ، IP می دهیم که بعنوان همان default getway استفاده می شود.

دستور IP Routing را می زنیم تا روتینگ لایه ۳ فعال شود:

```
Switch(Config)# interface vlan ID
Switch(Config-if)# Ip address ----------
Switch(Config)# Ip routing
```

روی MLS ترانک می سازیم VLAN ها راه می سازیم

```
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#vlan 70
```

روی MLS نماینده VLAN ها می سازیم IP می دهیم

```
Switch(config)#interface vlan 60
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, change

Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.60.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#inte
Switch(config)#interface vlan 70
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan70, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan70, changed

Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.70.1 255.255.255.0
Switch(config-if)#exit
```

(MLS) دستور IP routing

```
Switch(config)#ip r
Switch(config)#ip rou
Switch(config)#ip routing
```

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

★★★

DHCP

Dynamic
Host
Configuration
protocol

سرویس DHCP می‌تواند به کامپیوترهای متصل به سوئیچ‌ها به صورت اتوماتیک IP بدهد.

چگونه این سرویس را روی سوئیچ فعال کنیم؟

روی همان سوئیچ MLS لایه ۳ که بقیه وصل بود، باید اعمال کنید: (یا 2960)

برای هر VLAN این دستورات را بزنید:

اول به خودش IP می‌دهید:

```
Switch(Config)# interface vlan 10
Switch(Config-if)# Ip address 192.168.1.1 255.255.255.0
Switch(Config-if)# No shut
```

IP گیت‌وی و DNS سرور

بعد و گوییم IP هایی که رزرو شده است را ندهد:

```
Switch(Config)# Ip DHCP excluded address 192.168.1.1 192.168.1.10
```

خودش یک بود — مثلاً تا ۱۰

```
Switch(Config)# Ip DHCP pool Sale
Switch(dhcp-config)# network 192.168.1.0 255.255.255.0
```

یک مخزن برای IP های سازمان

برای مخزنی که ساختیم محدوده IP و دهیم

```
Switch(dhcp-config)# default-router ------
Switch(dhcp-Config)# dns-Server --------
```

IP گیت‌وی

IP DNS سرور

www.sematec-co.com
Farshad Heydari
By Houshang Heshmati

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vl
Switch(config)#interface vlan 1
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shu

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed stat

Switch(config-if)#exit
Switch(config)#ip dh
Switch(config)#ip dhcp ex
Switch(config)#ip dhcp excluded-address  192.168.1.1 192.168.1.100
Switch(config)#ip dh
Switch(config)#ip dhcp poo
Switch(config)#ip dhcp pool Houshang
Switch(dhcp-config)#netw
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0
Switch(dhcp-config)#def
Switch(dhcp-config)#default-router  192.168.1.1 255.255.255.0

% Invalid input detected at '^' marker.

Switch(dhcp-config)#dns
Switch(dhcp-config)#dns-server 192.168.1.1 255.255.255.0

% Invalid input detected at '^' marker.

Switch(dhcp-config)#exit
```

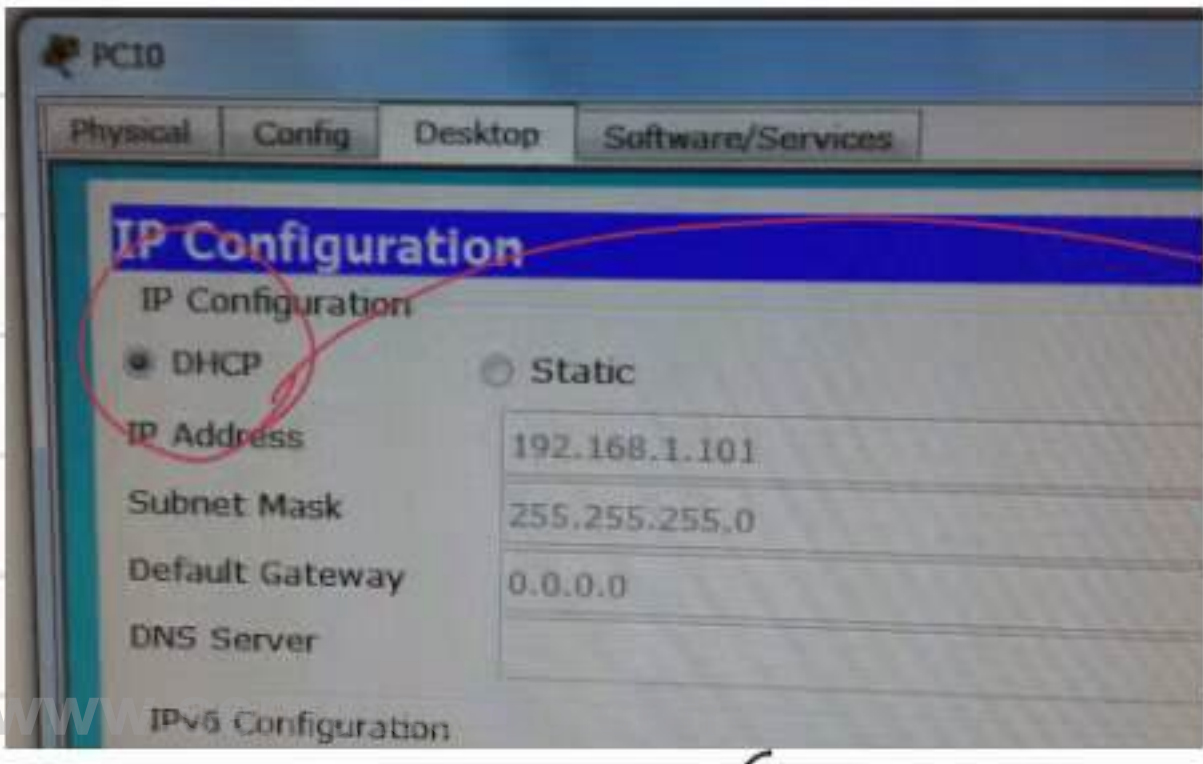
یک VLAN می‌سازیم

داخل VLAN فعال DHCP می‌کنیم

مخزن

default gatway

DNS



DHCP برای IP کامپیوترها انتخاب می‌کنیم

در آخر روی سوئیچ IP routing اعمال می‌کنیم.

www.
Farzad Heydari
By Houshang Heshmati

DTP

Dynamic Trunking protocol

اگر از پروتکل DTP استفاده کنید هرگاه ارتباط بین دو سوئیچ را برقرار کنید
و یک سمت را Trunk کنید سمت سوئیچ دیگر اتوماتیک Trunk می‌شود.
اگر show interface Trunk بگیرید پورت ترانک را با n نمایش
می‌دهد.

مذاکره negotiate

n مخفف

```
... Trunking Dine protocol on interface Fas
Switch>ena
Switch#sho int tr
Switch#sho int trunk
Port        Mode         Encapsulation  Status
Fa0/1       auto         n-802.1q       trunking

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management do
Fa0/1       1

Port        Vlans in spanning tree forwarding state a
Fa0/1       none
Switch#
```

Operational mode

پورت ۲ حالت دارد

- Trunk: همه ترافیک‌ها را عبور می‌دهد عضو Vlan نیست
- access → اتصال END Devies: PC, printer, Server, ...
  فقط ترافیک یک Vlan را عبور می‌دهد.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

حالت سوم هم داریم :

administrative mode (DTp mode)

شامل

- Dynamic Auto
- Dynamic Desirable → اگر down بود یعنی کابل ندارد
- Trunk
- access

برای گزارش گیری از یک پورت :

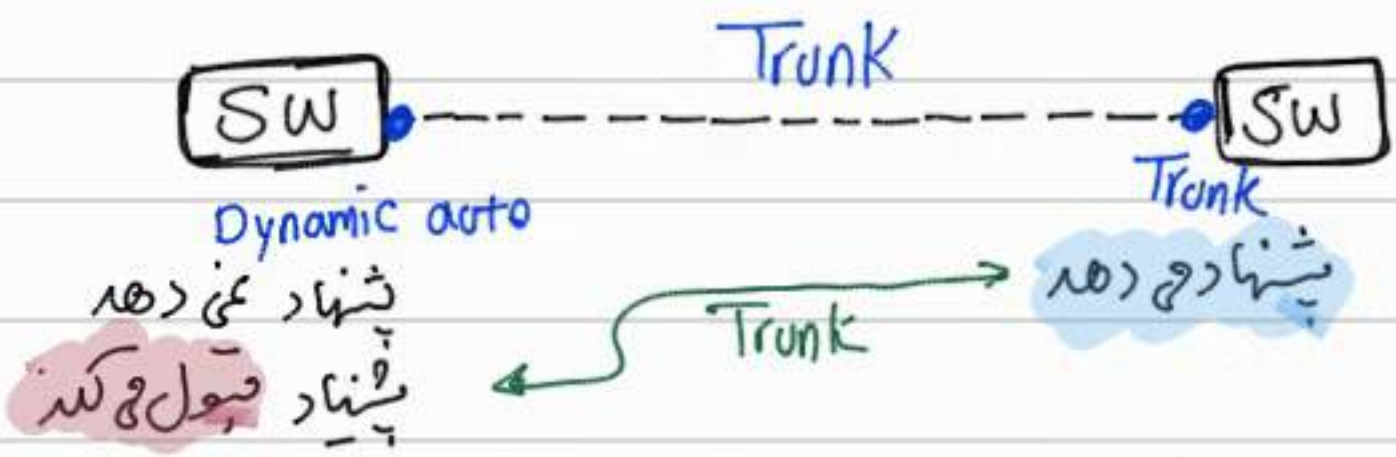
Switch # show interface ...../..... Switchport

Type Number

```
Switch#show interfaces fas 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

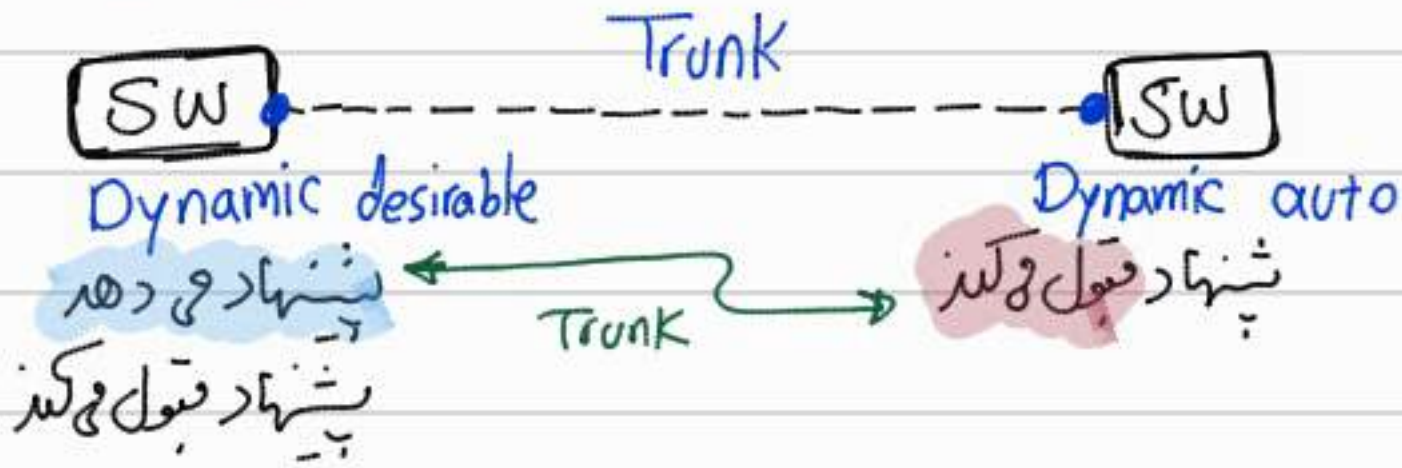
www.samatec.co.com
Farzad Heydari
By Houshang Heshmati

۱

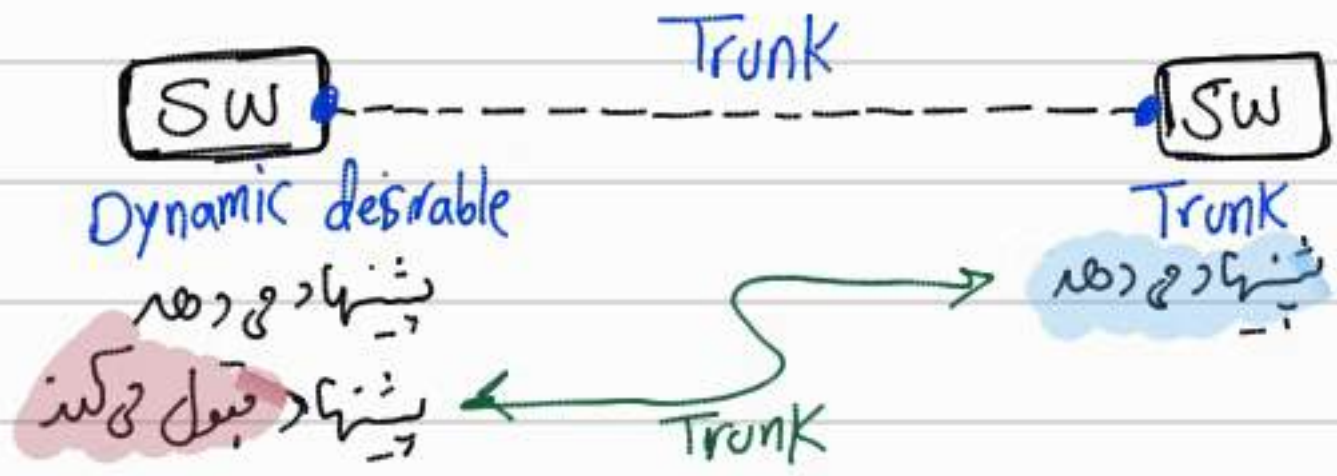


پیشنهاد می دهد یعنی هر ۳۰ ثانیه hello می فرستد و به آن طرف می گوید "بیا ترانک بشویم".

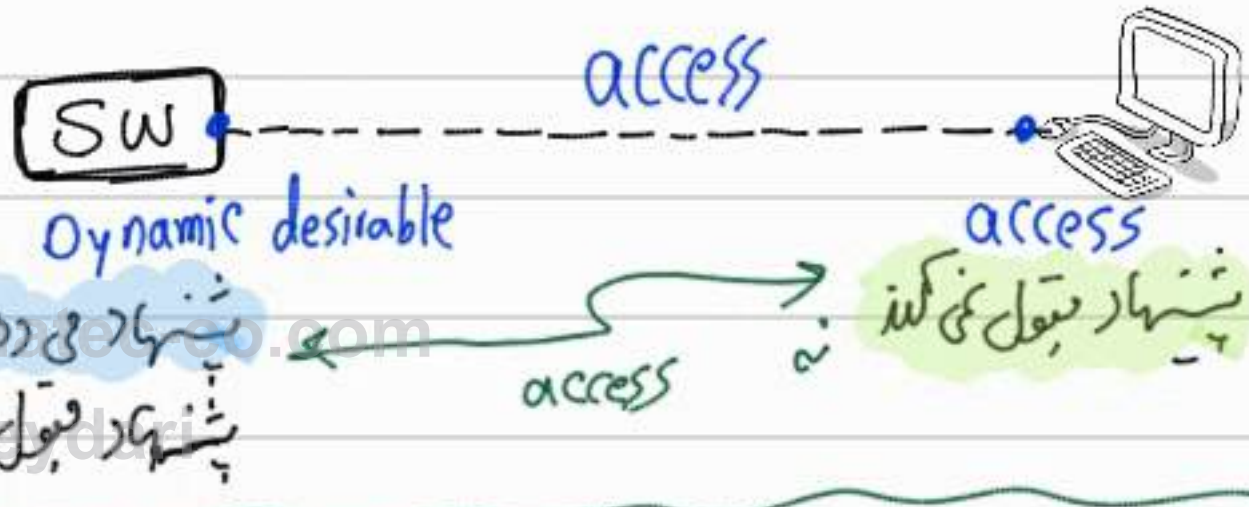
۲



۳



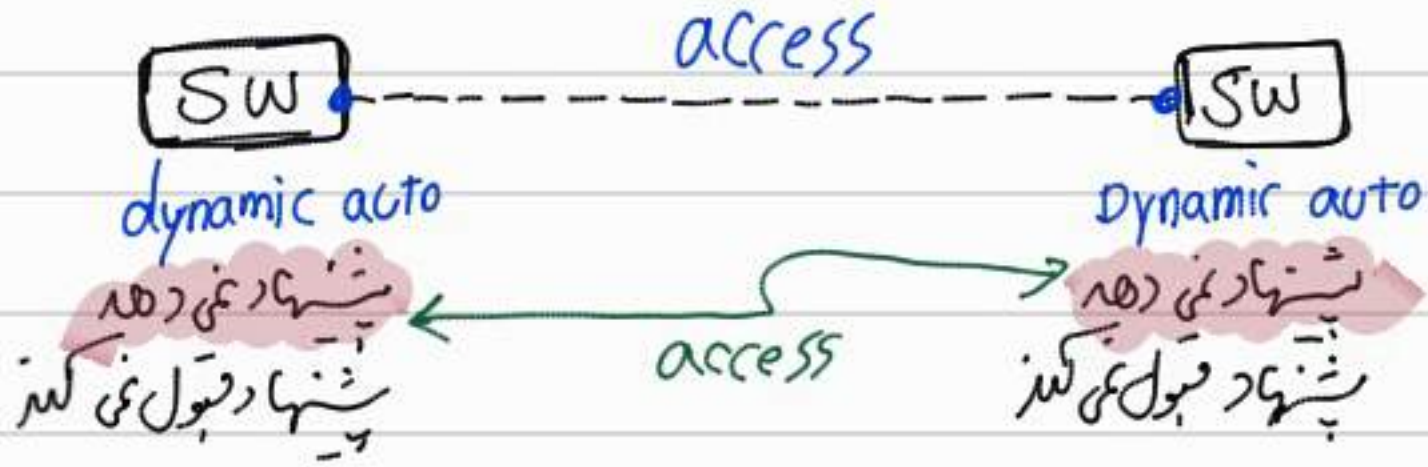
۴



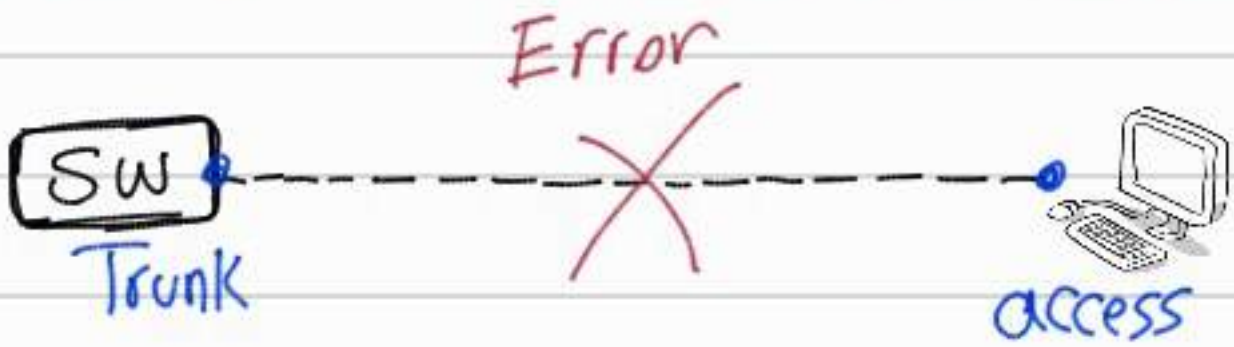
www.semsetech.com
Farzad Nejadari
By Houshang Heshmati

۶

۷



۷



چگونه mode پورت را عوض کنیم؟

Switch (config-if)# switchport mode ----------

- access
- Trunk
- dynamic auto
- dynamic desirable

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

```
Switch#show interfaces fas 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

مثلث Trunk

اگر مود را عوض کنید ۳۰۰ ثانیه (۵ دقیقه) طول می‌کشد که عوض شود

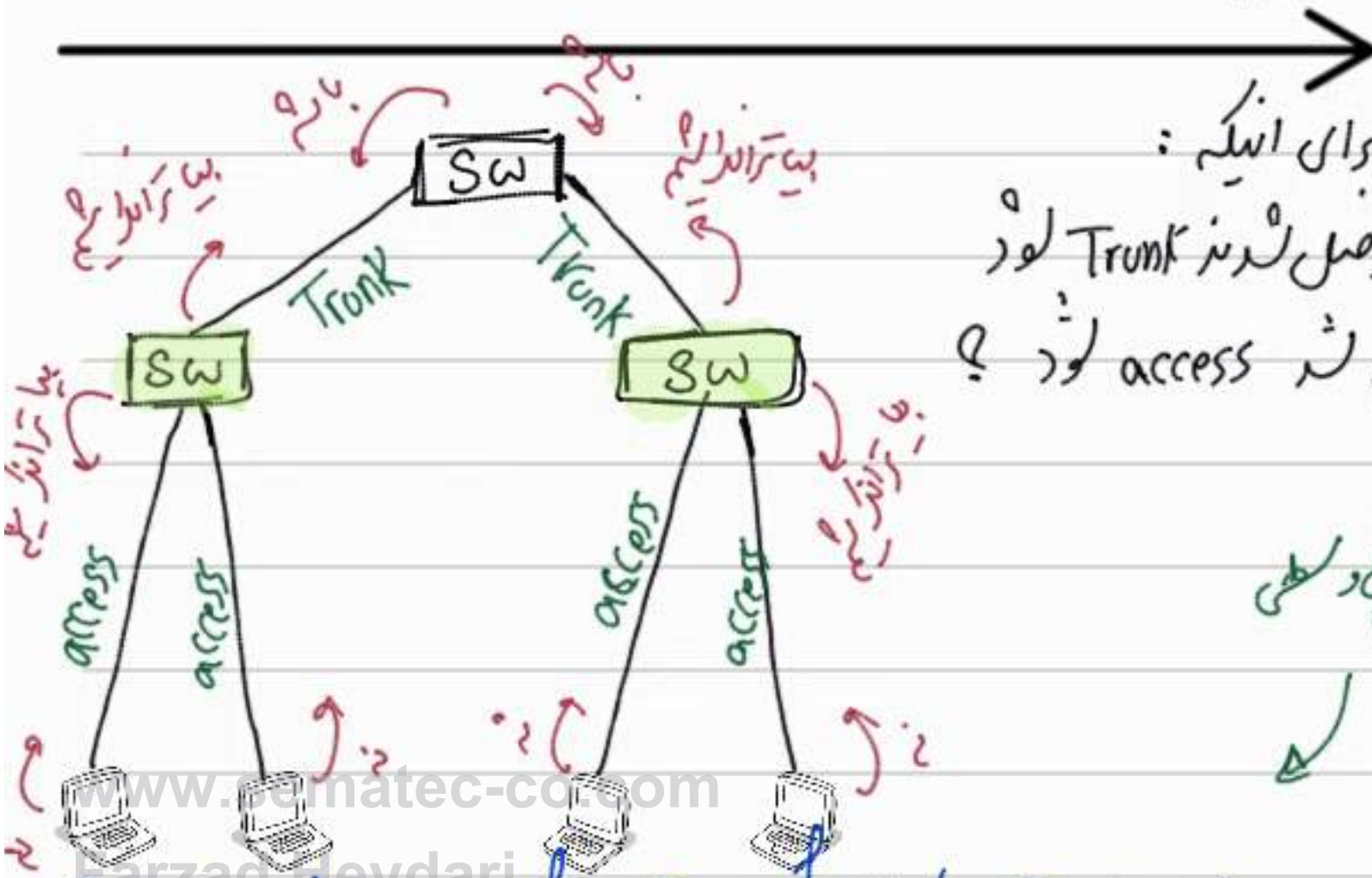
یعنی ممکن است تا پنج دقیقه همچنان access بماند و Trunk نشود

خودآزمایی

کمترین دستور برای اینکه:

هر لوئیچ به هم وصل شدند Trunk شود

هر pc وصل شد access شود؟



روی ۲ تا لوئیچ وسطی

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Switch(Config)# interface Range fastethernet 0/1-24

Switch(Config-if)# Switchport mode dynamic desirable

چند نکته که باید رعایت کنید:

۱) هرجا که End device داریم مثل کامپیوتر، پرینتر و ... حتماً باشد switchport mode access

---

۲) پورت های خالی سوئیچ را حتماً shutdown کنید

```
Switch(Config)# interface range fastEthret 0/10-24 ↵
Switch(config-if)# shutdown ↵
```

قبلاً از پورت ۱۰ تا ۲۴ چیزی وصل نیست

---

۳) جاهایی که End device وصل هستند مثل کامپیوتر و پرینتر و ... حتماً port security و Sticky باشد.

---

۴) از DTP استفاده نکنید (برای محیط آموزشی مناسب است فقط)

---

۵) همیشه به صورت دستی خودتان Trunk کنید Switchport mode Trunk

وقتی دستی Trunk کردید لازم نیست پورت های Trunk برای هم Hello بفرستند و ترافیک ایجاد کنند:

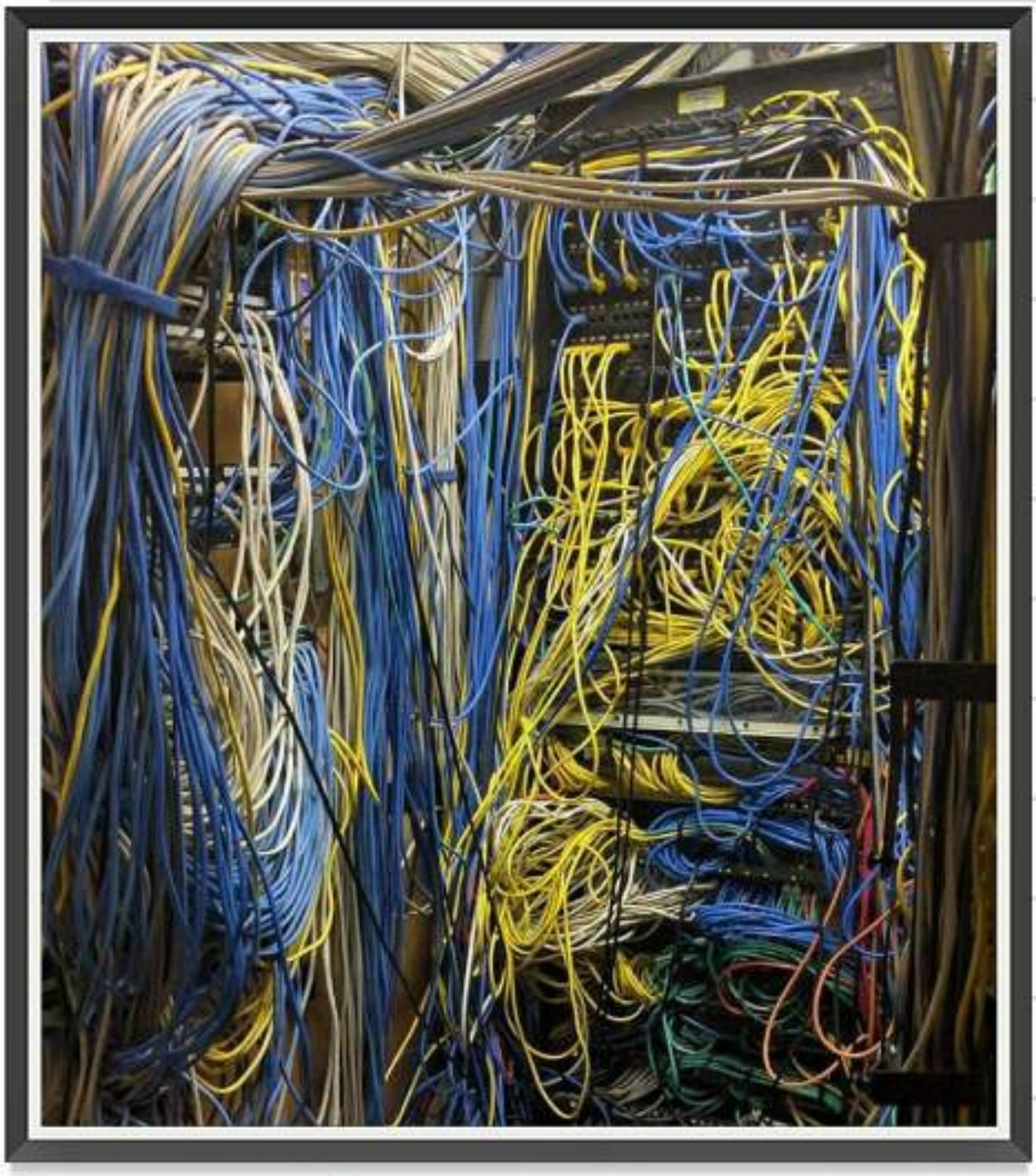
```
Switch(config-if)#switchport mode Trunk ↵
Switch(Config-if)# Switchport nonegotiate ↵
```

برای هم Hello نمی فرستند (مذاکره نمی کنند).

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

CDP

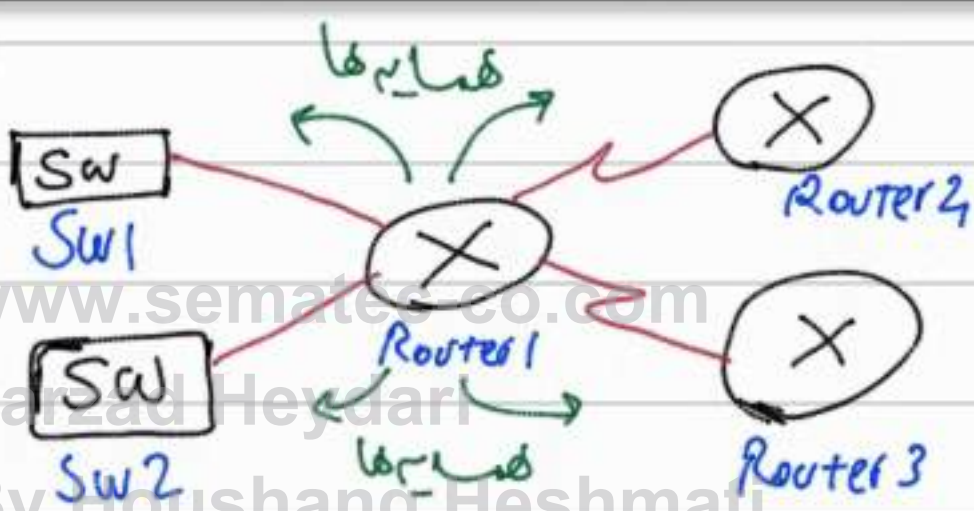
Cisco Discovery protocolo



استفاده شده اید و از شما می خواهند اتاق سرور را مرتب کنید و کابل ها را سر و سامان بدهید بدون اینکه خراب کاری کنید.

وحشت نکنید!

پروتکل CDP می تواند دستگاه های متصل به هم را پیدا کند (همسایه های هر Device را پیدا می کند).



- هر چند ثانیه یکبار برای همه دستگاه ها پروتکل CDP ارسال می شود و از همسایه های مطلع می شود

www.sematec.co.com
Farzad Heydari
By Houshang Heshmati

نکته به این است که روی همه پورت ها پروتکل CDP ارسال می شود و ممکن است برای END Device ها هم فرستاده شود.

به دلایل امنیتی کلا چیزی نباید سمت END Devices ارسال شود.

Switch(Config-if) # No CDP enable روی پورت متصل به End device

```
SW3(config)#intef
SW3(config)#intef fa
SW3(config)#inte
SW3(config)#interface fa
SW3(config)#interface fastEthernet 0/2
SW3(config-if)#no cdp
SW3(config-if)#no cdp enable
SW3(config-if)#
```

به PC وصل بوده

برای استفاده از CDP و مشاهده همسایه های یک دستگاه:

Switch # Show CDP Neighboor ↵

```
SW2#sho cdp n
SW2#sho 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
SW1            Fas 0/1          167          S          2960        Fas 0/2
SW3            Fas 0/2          169          S          2960        Fas 0/1
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
```

به چه دستگاهی

با کدام پورت خودش وصل شده

آن دستگاه چی هست؟

S → Switch

R → Router

P → IP phone

به کدام پورت آن دستگاه وصل شده است.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

جاهایی که امنیت مهم است چون CDP خیلی اطلاعات می دهد کلا CDP را غیرفعال می کنند و هرجا لازم بود CDP را فعال می کنند:

Switch(config)# No CDP run

روی تمام پورت کلا CDP غیرفعال می شود.

می توانید بعد از گرفتن اطلاعات از CDP، نقشه شبکه خود را با نرم افزار جانبی مانند Visio یا Edraw max 7 رسم کنید

CDP از اول فعال است و فقط مخصوص CISCO

اگر برندهای دیگه مثل Hp و ... داشتیم؟

show LLDP Neighboor

برای میکروتک MNDP

در اطلاعاتی که show CDP می دهد یک پارامتر هست به نام Hold time این مدت زمانی است که CDP اطلاعات همسایه را نگه می دارد (180 ثانیه) و هر 60 ثانیه یکبار هم Hello می فرستد.

CDP دقیق تر؟

Switch # show CDP neighboor detail

حتی می گه دیشب شام چی خوردی!

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

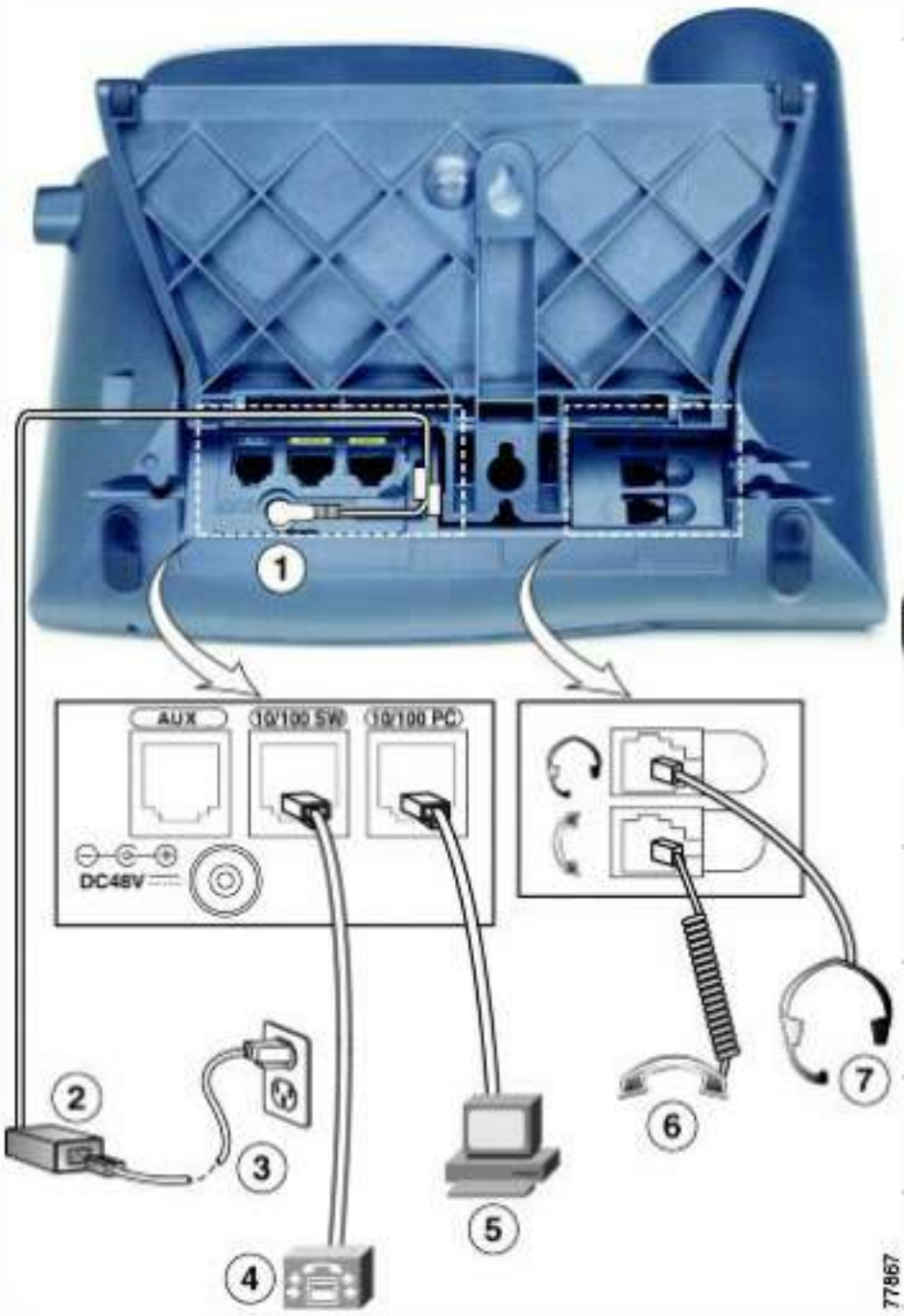
نرم افزارهایی که می توانند اطلاعات CDP را بدزدند (خطرناک)

CDPsnarf

Kali Tool لینوکس

اگر Ip phone در شبکه دارید نباید CDP غیرفعال باشد.

Ip phone :



Ip phone تلفنی است که از بستر شبکه برای تماس استفاده می‌کند و هزینه‌ی برای تماس پرداخت نمی‌کنید

علاوه بر تماس داخلی سازمانی اگر از طریق شبکه به دفتر بندر عباس اتصال دارید می‌توانید با Ipphone داخلی بندر عباس را بگیرید و صحبت کنید

POE هستند (power over Ethernet) برق را از همان کابل شبکه می‌گیرند (سوئیچ باید پورت POE داشته باشد) و می‌توانند از UPS شبکه هم استفاده کنند.

```
Switch#sho cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phon
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port I
IP Phone         Fas 0/1             168        H P       7960
Switch#
```

phone

www.sahatec-co.com
Farzad Heydari
By Houshang Heshmati

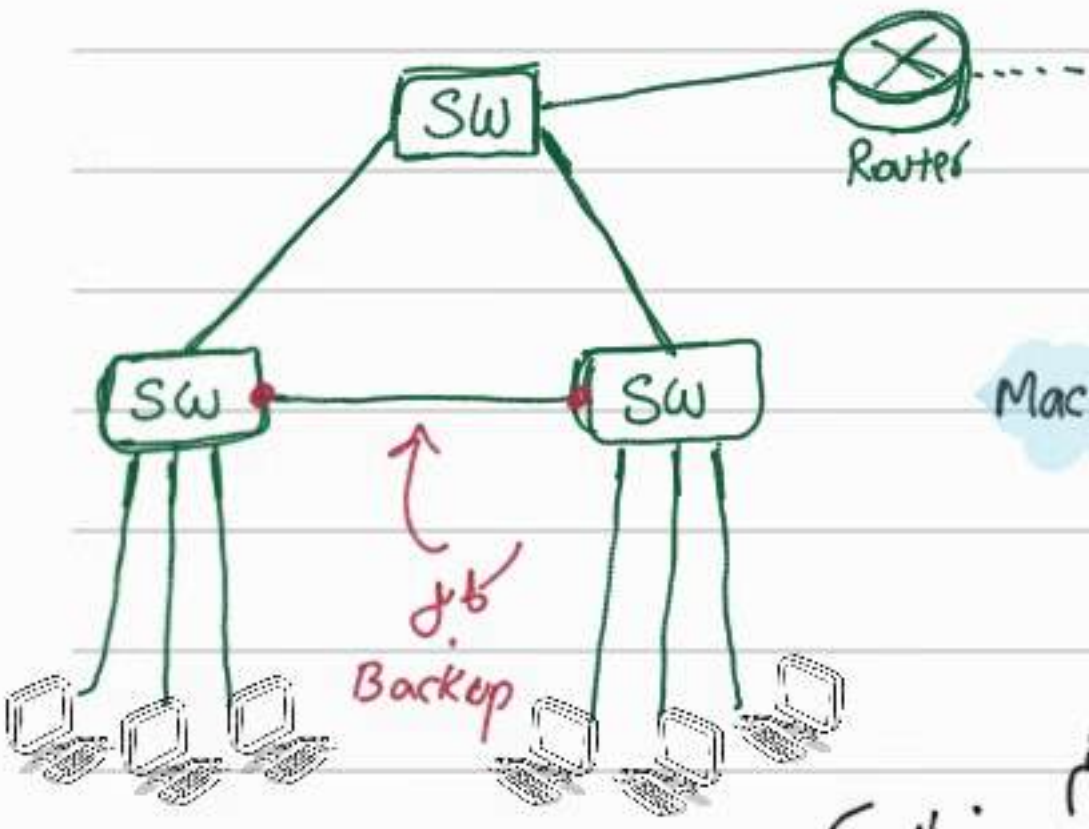
خیلی مهم

STP

Spanning Tree Protocol

حتماً مسلط باشید

معمولاً در شبکه‌ها لینک اضافی جهت Back-up کشیده می‌شود. اتفاق بدی که می‌افتد:



1) Broadcast Storm

لوپینگ هنگ می‌کند

۲) Mac address table instability

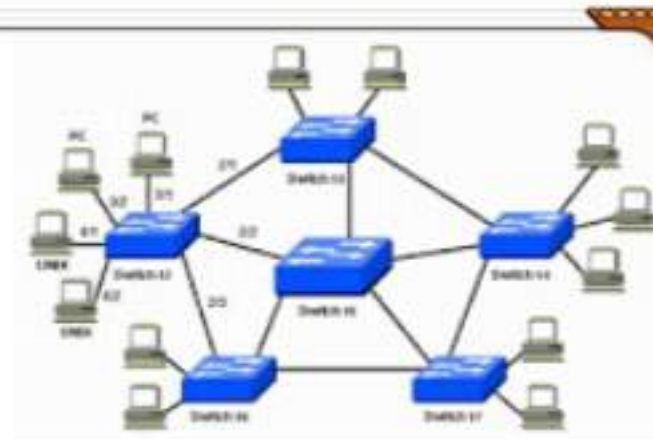
ناپایداری جدول مک آدرس‌ها

۳) Multiple framing

تعداد زیادی frame ایجاد می‌شود که هم آنتی ویروس ایراد می‌گیرد هم لوپینگ در نهایت هنگ می‌کند.

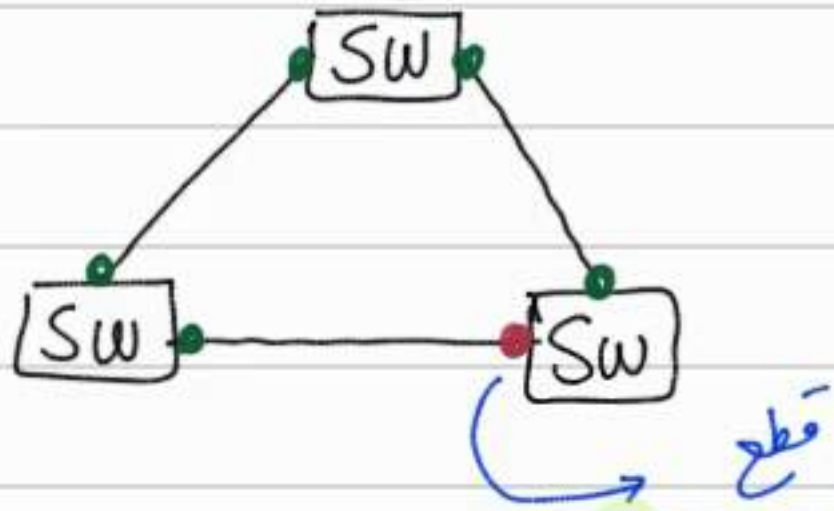
راه حل؟ استفاده از STP (Loop free)

Spanning Tree Protocol (**STP**) is a Layer 2 **protocol** that runs on bridges and switches. The specification for **STP** is IEEE 802.1D. The main purpose of **STP** is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network. Aug 17, 2006



www.semafoc.com
Farzad Heydari
By Houshang Heshmati

راه حل مشکل این است که هر دو لینک با هم وصل نباشند و هر زمان لینک اصلی قطع شد لینک کمکی وصل شود. پروتکل STP دقیقا همین کار را می کند.



اگر ۳ تا لوئیچ را مطابق شکل وصل کنید پروتکل STP یکی از اتصالات را قطع می کند

این پروتکل روی تمام لوئیچ های سیسکو فعال است.

سؤال: چرا STP پورت خاصی را بلاک می کند؟ می توانیم پورت دیگری بلاک کنیم؟

1. Select root bridge — یک لوئیچ را بعنوان رئیس (ریشه) انتخاب می کند
2. Select root port — روی لوئیچ بهترین مسیر تا پورت رئیس را پیدا می کند
3. Select Designated port — پورتی که از لحاظ دیگر بهترین مسیر تا پورت رئیس است

در انتها یک پورت باقی می ماند که آن را بلاک می کند

BID بجای اسم لوئیچ از عدد BID برای معرفی هر لوئیچ استفاده می شود

هر کسی BID کمتری داشته باشد رئیس می شود.

BID عدد = (priority عدد + Mac.address عدد)

priority: بصورت default برای همه (32768)

Mac.address: (مک آدرس لوئیچ)

پس هر لوئیچی مک آدرس کمتری داشته باشد رئیس می شود.

www.sematec-co.com
Fazzdl.loyari
By Housharg Heshmati

این انتخاب اصلاً مناسب نیست و فقط برای این است که شبکه دچار اشکال نشود. چون سوئیچ های خیلی قدیمی تر و ضعیف تر ممکن است Mac address کوچکتری داشته باشند و یک سوئیچ دانون و کلاسه و قدیمی بشود رئیس STP!

برای نمایش اطلاعات STP در سوئیچ:

Switch# show spanning-Tree

سوئیچ 3560

مک آدرس بیشتر

32768+1=32769

عدد priority + شماره vlan

```
Switch#sho spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0000.0CB0.1415
             Cost        19
             Port        2(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000C.8519.B19E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p

Switch#
```

مک آدرس

سوئیچ 2950

رئیس شد

مک آدرس کمتر

32768+1=32769

عدد priority + شماره vlan

```
Switch#sho spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0000.0CB0.1415
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0000.0CB0.1415
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch#
```

www.semateb.com
Farzad Heydari
By Houshang Hedmati

متاسفانه سوئیچ دانون ۲۹۵۰ بجای سوئیچ خفن گرون 3560، رئیس شده

STP اول عدد priority (اولویت) را چک می‌کند و بعد می‌رود سراغ عدد مک آدرس پس می‌توانیم با تغییر عدد priority خودمان ریشه را انتخاب کنیم:

مهم خودتان باید این عملیات را انجام بدهید و ریشه را انتخاب کنید انتخاب پیش‌فرض STP با استفاده از Mac-address بدترین حالت است و فقط برای جلوگیری از loop هست و خیلی نا شیانه است.

عدد priority بصورت default، 32768 است. و بصورت مضربی از 4096 کم و زیاد می‌شود.

Switch(Config)# Spanning-tree vlan ..... priority *4096

vlan شماره

عدد priority مضربی از 4096

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#spa
Switch(config)#spanning-tree vl
Switch(config)#spanning-tree vlan 1 pr
Switch(config)#spanning-tree vlan 1 priority 5
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0      4096   8192   12288 16384 20480 24576 28672
  32768  36864  40960  45056 49152 53248 57344 61440
Switch(config)#spanning-tree vlan 1 priority 20480
Switch(config)#
```

قبول نمی‌کند باید مضربی از 4096 باشد

میگه یکی از اینا را انتخاب کن

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

default خودش (پیش فرض وسط بازه اعداد انتخابی است که جای مانور داشته باشید)

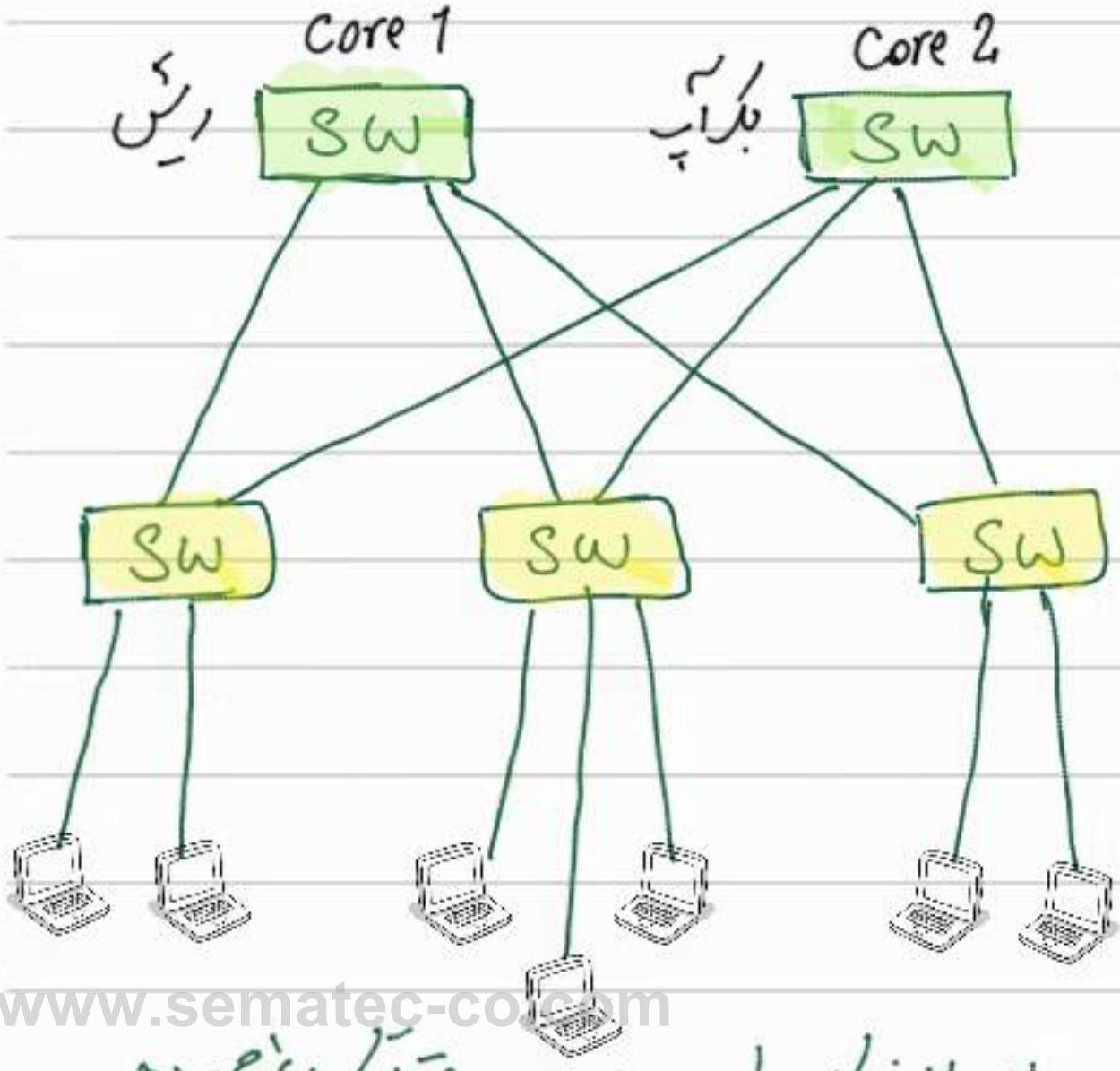
فعلاً برای انتخاب ریشه عدد priority را کم می‌کنیم:

```
Switch# Spanning-Tree vlan 1  36864
```

چرا صفر نمی‌زنیم که کار خودمان را راحت کنیم؟

می‌شود صفر زد و ریشه را انتخاب کرد ولی در شبکه خیلی پیش می‌آید بخواهید ریشه را عوض کنید آن وقت از صفر کمتر که نداریم و دوباره کاری دارید اول باید یک عدد بزرگتر بدهید و در لوپ بعدی یک عدد کمتر.

اگر ریشه (root Bridge) سوخت؟ ترکید؟ منهدم شد؟
باید یک لوپ بعنوان بک‌آپ خودمان انتخاب کنیم:



باید BID Core1 < BID Core2

و

BID Core2 < BID همه Sw ها

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

نترسید، خود سیسکو برای این کار دلسوزی دارد و اتوماتیک انجام می‌دهد.

Switch(Config)# Spanning-Tree vlan vlan ID ..... root primary

روی سوئیچ ریشه (root bridge) می‌زنیم و ریشه می‌شود.

Switch (Config)# Spanning-Tree vlan vlan ID root Secondary

روی سوئیچی که می‌خواهیم بک‌آپ باشد می‌زنیم اگر priority را دستی تغییر داده باشیم

این دستور دو می کار نمی‌کند

```
switch(config)#spanning-tree vlan 1 root primary
switch(config)#sho span
switch(config)#sho span
switch(config)#do sho span
switch(config)#do sho span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     00D0.58D4.C63B
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     00D0.58D4.C63B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/3            Desg LSN 19        128.3    P2p
Fa0/2            Desg LSN 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch(config)#
```

روی سوئیچ root bridge ریشه

BID = 24577

```
witch(config)#spanning-tree vlan 1 root secondary
witch(config)#do sho span
witch(config)#do sho span
LAN0001
 Spanning tree enabled protocol ieee
 Root ID    Priority    24577
            Address     00D0.58D4.C63B
            Cost        38
            Port        1(FastEthernet0/1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay

 Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
            Address     0060.3E73.00D3
            Hello Time  2 sec  Max Age 20 sec  Forward Delay
            Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
```

روی سوئیچ بک‌آپ

BID = 28673

www.samuel-co.com
Farzad Heydari
By Houshang Heshmati

انتخاب بهترین مسیر تا root Bridge :

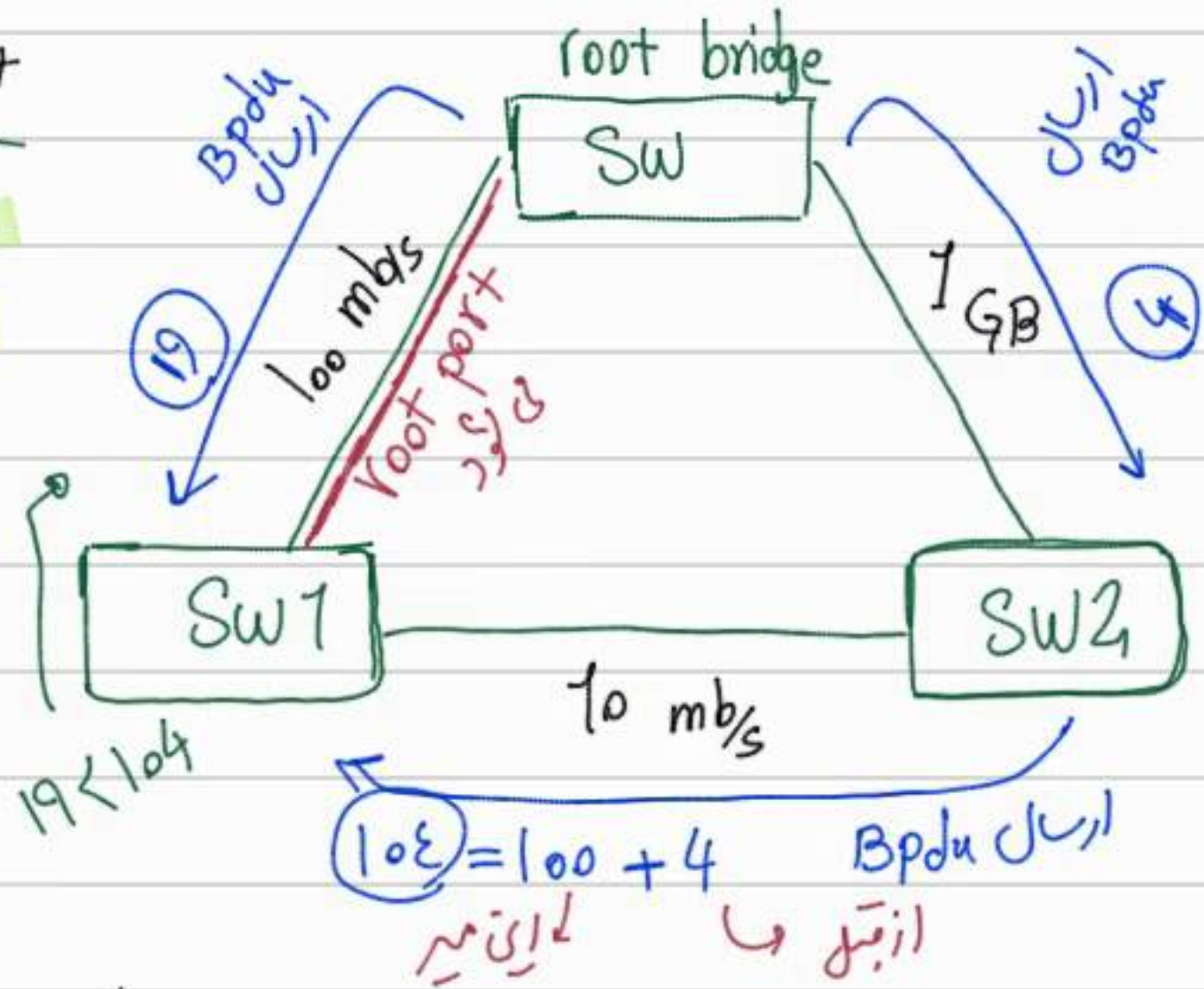
بعد از انتخاب ریشه، دومین کار STP انتخاب بهترین مسیر تا root bridge است.

به ازای هر سوئیچ یک root port داریم :

یکی

root port با کمک جدول هزینه (cost table) محاسبه می‌شود باید حفظ باشید :

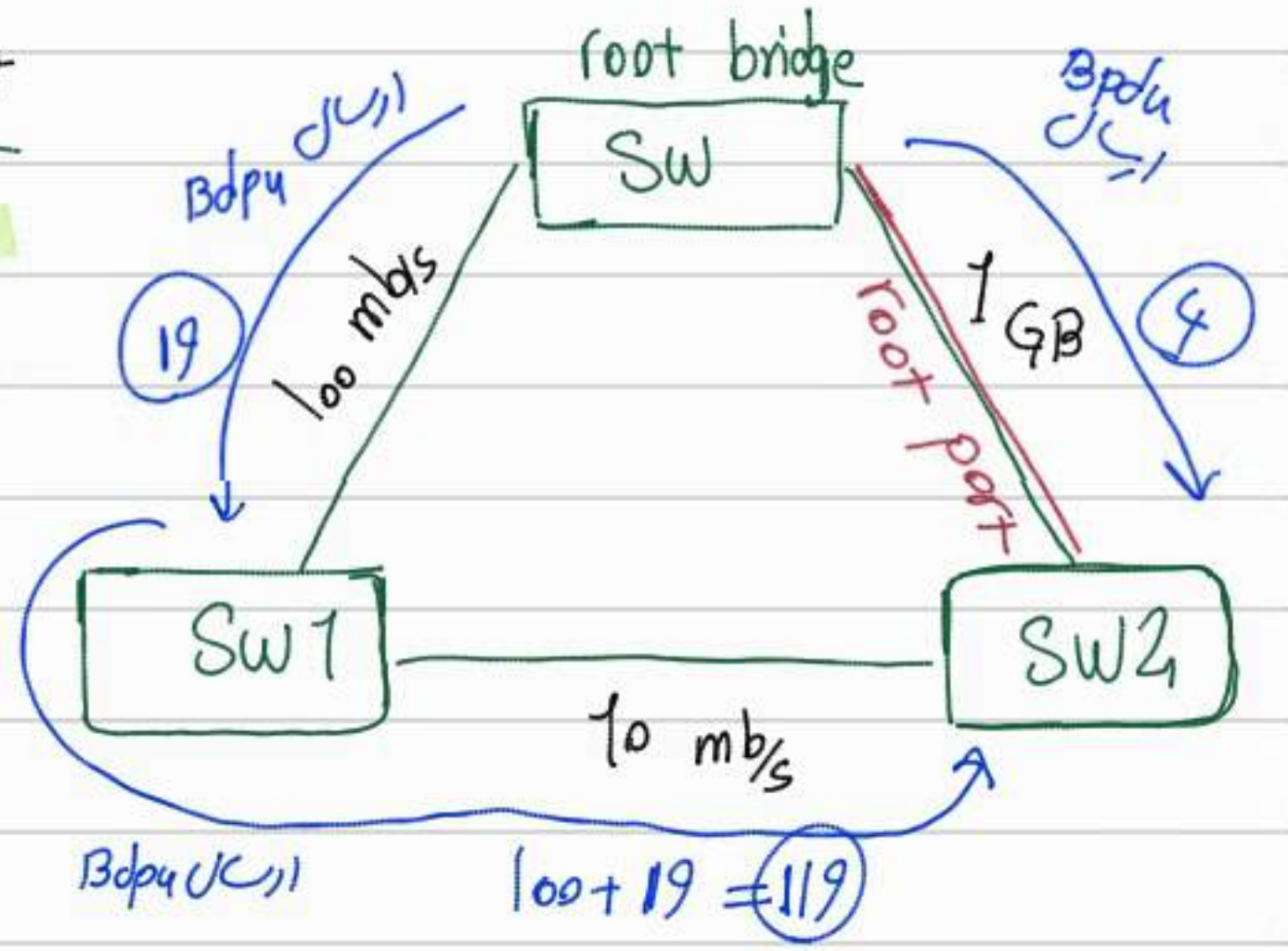
speed	Cost
10 mb/s	100
100 mb/s	19
1 GB	4
10 GB	2
بقیه ↓	1



SW1 برای رسیدن به root bridg ۲ راه دارد. مستقیماً از دلت خودش وصل شود یا از طریق مسیر SW2 برود. برای این کار با کمک ارسال بسته‌های Bpdu میزان cost مسیر را محاسبه می‌کند و مسیر دارای کمترین هزینه را انتخاب می‌کند.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Speed	Cost
10 mb/s	100
100 mb/s	19
1 GB	4
10 GB	2
بقیه ↓	1



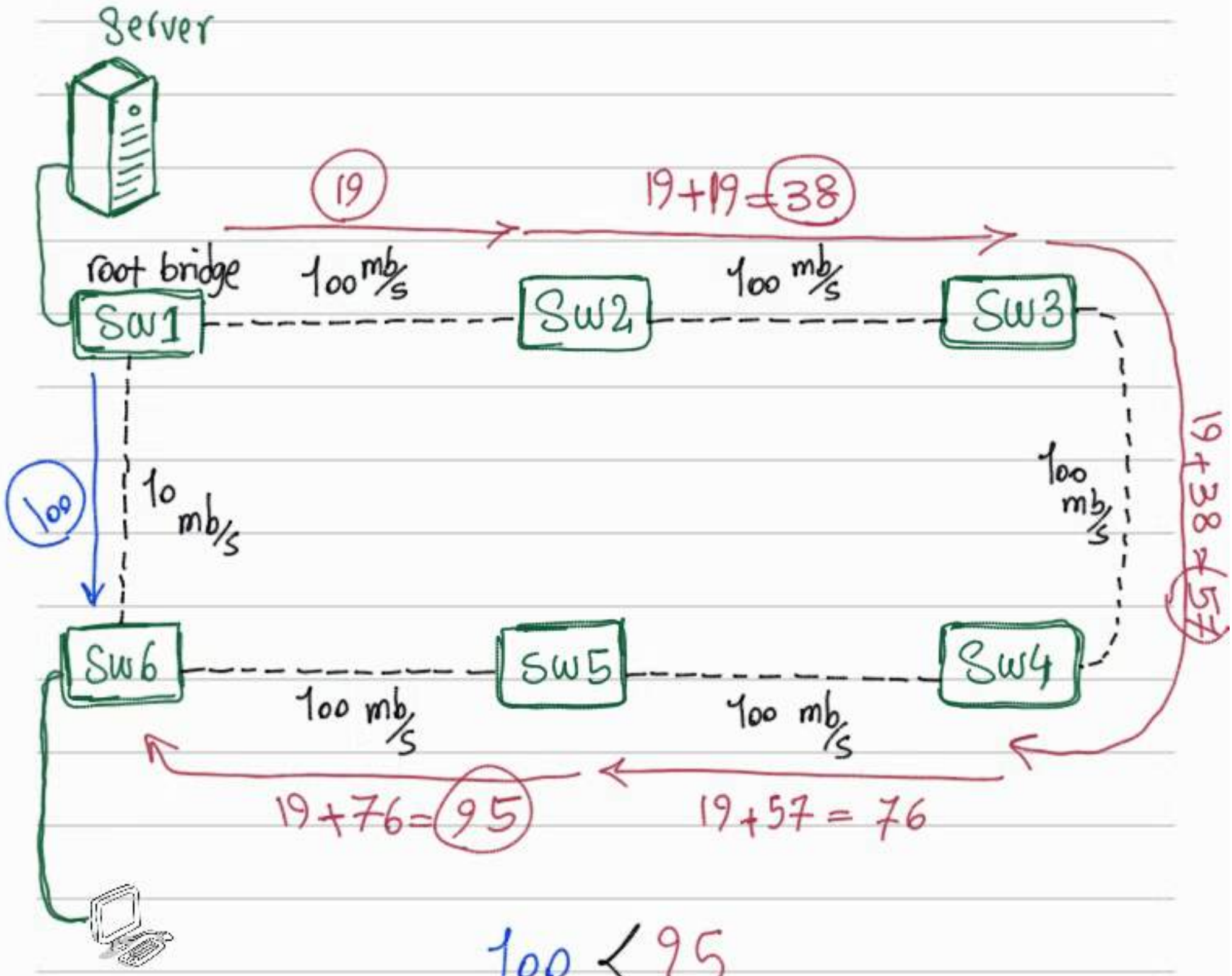
حالا اگر SW2 بخواهد بهترین مسیر تا root bridge پیدا کند؟ چ

Bpdu (بسته های STP): همه سوئیچ‌ها که روشن شوند برای همدیگر bpdu می‌فرستند. هر کسی که می‌فرستد به بقیه می‌گوید من ریشه (root bridge) هستم. وقتی همه فرستادند و ریشه انتخاب شد ریشه برای بقیه Bpdu root می‌فرستد تا بقیه بتوانند مسیر را پیدا کنند.

در Bpdu که ریشه می‌فرستد یک فیلد cost دارد که هزینه مسیر محاسبه می‌شود در آن ذخیره می‌شود.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

root port برای سوئیچ شماره ۶ کدام است؟



$100 < 95$

مسیر قرمز بعنوان root port انتخاب می‌شود.

اگر خواستید در packet Tracer این را آزمایش کنید چون کابل 10 mb/s ندارد روی Interface بروید و سرعت آن کم کنید

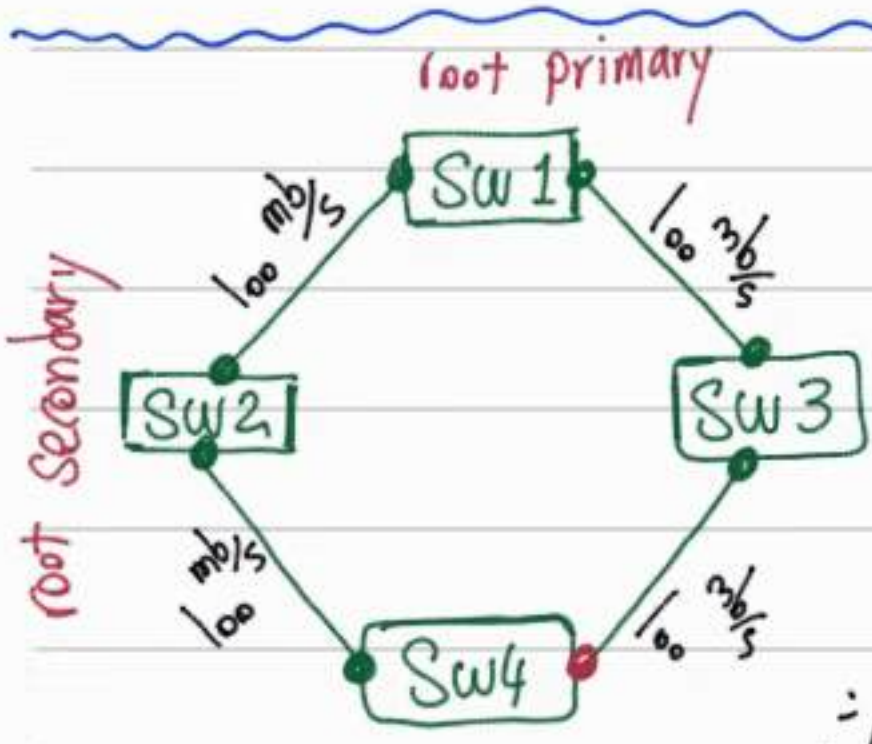
www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

مثال قبل را در packet Tracer بازسازی کردیم. می‌توانیم Cost هر مسیر را بر روی هر پورت ببینیم:

```
Switch>en
Switch#sho spa
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0040.0B96.B6B0
             Cost        57
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  F

  Bridge ID  Priority    32769  (priority 32768 sy
             Address     0090.0C5D.1259
             Hello Time  2 sec  Max Age 20 sec  F
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Switch#
```

root port

برای SW4 در مثال قبلی که خودمان هم 57 برآورد کرده بودیم.



اگر همه مسیرها یکی بودند چی؟

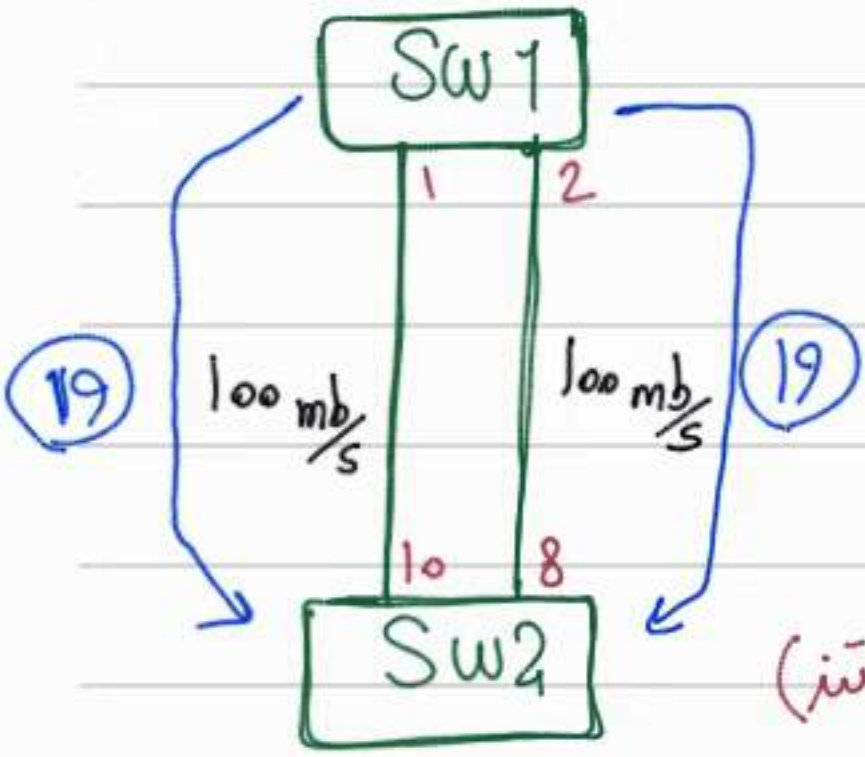
(۱) خودمان روی SW1 دستور root primary می‌زنیم

(۲) اگر بخواهیم از SW4 به سمت SW2 وصل باشد روی SW2 دستور root secondary می‌زنیم.

اگر بخواهیم از SW4 به سمت SW3 وصل باشد روی SW3 root secondary می‌زنیم

www.sematec-co.com
Farzad Heydari
By Hoshang Hashmati

اگر به این شکل بود ؟



Sw1 :
root port ندارد چون خودش root bridge است.

Sw2 :
چون یک لوپ ولی دو پورت است پس BID ها برابرند پس نمی‌شود متوجه شد.

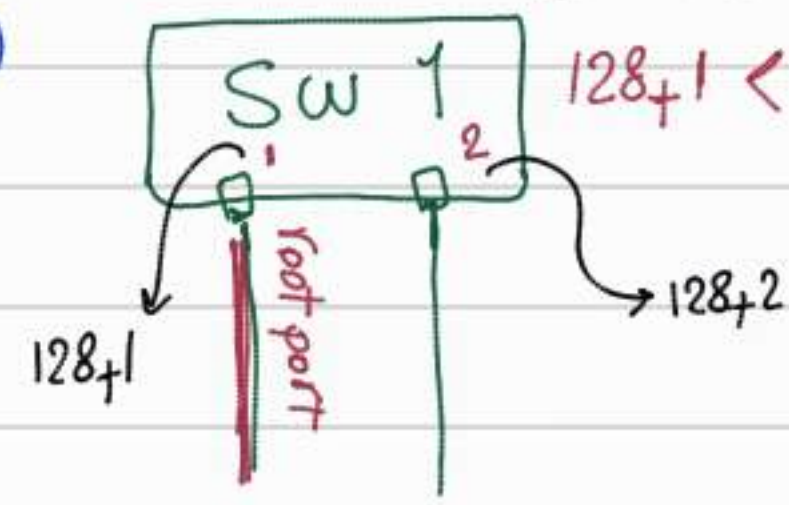
(قرمزها شماره پورت های الصاقی روی لوپ هستند)

معیار جدیدی داریم اگر کار به کشید : Lower Sender PID

(priority + port number)

default = 128
(از صفر تا 240 می‌شود)

شماره پورت



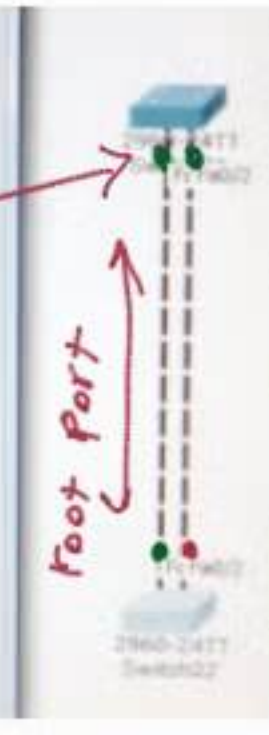
روی لوپ بالا

Switch(Config-if)# Spanning-tree vlan vlan id port-priority عدد

مضرب از 16

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#span
Switch(config)#spanning-tree vl
Switch(config)#spanning-tree vlan 1 roo
Switch(config)#spanning-tree vlan 1 root pr
Switch(config)#spanning-tree vlan 1 root primary
Switch(config)#intr
Switch(config)#int
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#sp
Switch(config-if)#span
Switch(config-if)#spanning-tree vl 1 por
Switch(config-if)#spanning-tree vl 1 port-priority
64
Switch(config-if)#
```

64 < 128

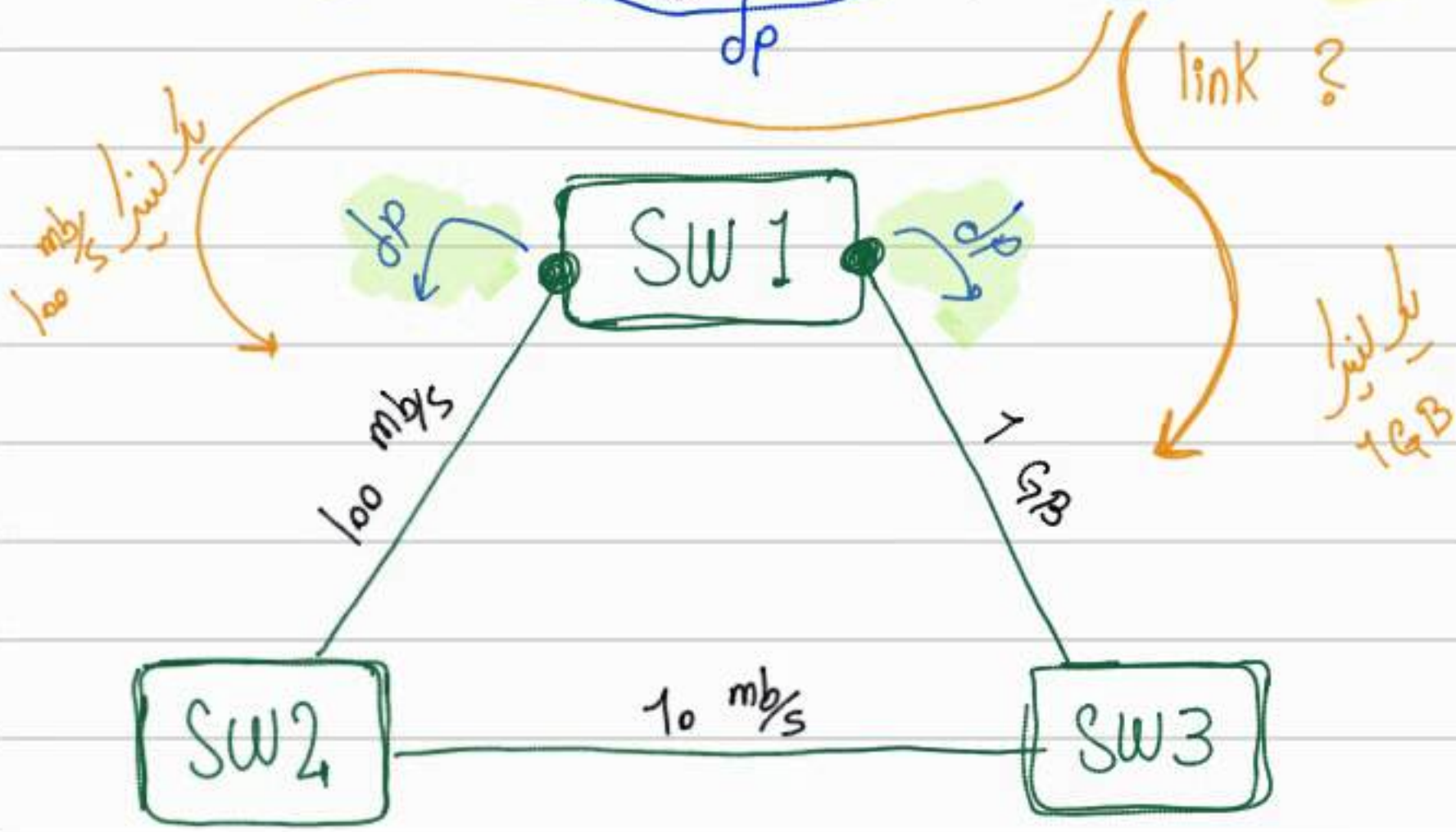


www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

انتخاب designated port (پورت کاندید / نامزد)

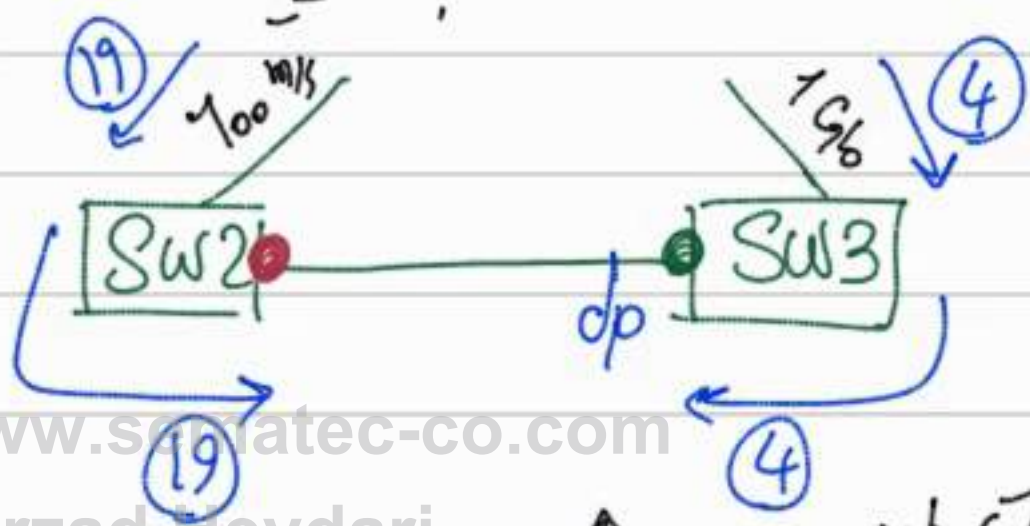
روی هر link باید یک designated port داشته باشیم.

dp



SW1 (Root Bridge): تمام پورت ها designated هست، چون cost تا خودش صفر است.

در لینک پایینی باید ببینیم پورت SW3 dp هست یا پورت لوئیع SW2:



cost را حساب می‌کنیم

dp پورتی می‌شود که مسیر cost کمتری دارد.

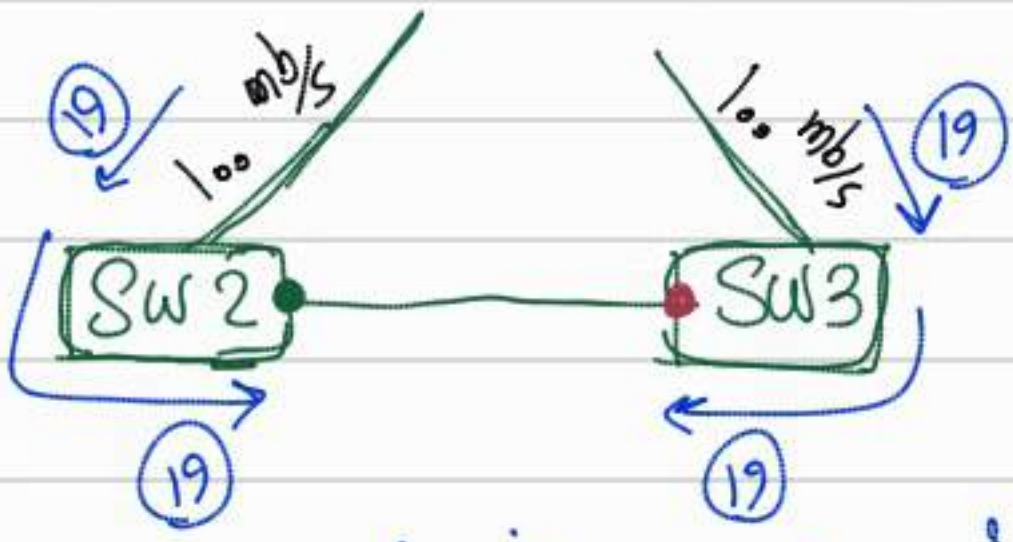
پورتی که روی SW2 بوده چون تقدمی ندارد پس بلاک می‌شود.

www.samatec-co.com
Farzad Heydari
By Houshang Heshmati

```
Switch(config-if)#do sho span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0003.E483.3A29
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 s

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0003.E483.3A29
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 s
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/1            Desg FWD 19        64.1     P2p
Fa0/2            Desg FWD 19        128.2    P2p
Switch(config-if)#
```

root bridge

در root bridge همه پورت‌ها desig هستند



اگر Cost مسیرها یکی بود؟

1) Lowest path cost

2) Lowest Sender Bid

اگر Bid برای Sw2 کمتر باشد، پورت Sw2 می‌شود dp

برای هر port داریم:

Roll: root یا designated یا Alternate (نقش آن) کاربری اش

State: FWD یا BLK یا listening یا Learning یا disable وضعیت آن

هنگام اتصال پورت اول ندرتی است چون STP بلاک می‌کند و چک می‌کند

BLK → listening → Learning → FWD

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Block → listening → learning → Forward

۲ ثانیه ۱۵ ثانیه ۱۵ ثانیه

- تا پورت به مرحله FWD نرسد IP نمی‌گیرد. حتی اگر DHCP داشته باشیم ۳۲ ثانیه اول از IP APIPA استفاده می‌کند تا FWD شود و IP بگیرد.
می‌توانیم تعریف کنیم پورت خاصی از لوپ listening و learning انجام ندهد و سریعاً FWD شود (portfast)

Switch(Config-if) # Spanning-tree portfast

روی پورتی که می‌خواهیم

دقت داشته باشید portfast فقط برای END Device استفاده شود مانند PC و ....
اگر پورتی که به لوپ یا هاب وصل است را portfast کنید دچار loop موقت می‌شوید

می‌توانید روی پورت گارد فعال کنید که اگر بجای END Device به لوپ وصل کرد پورت خاموش می‌شود. برای فعال شدن دوباره پورت باید داخل interface شویم و پورت را shutdown, No shutdown کنیم.

Switch(Config-if) # Spanning-tree bpduguard enable

Switch(Config) # Spanning-tree portfast default ← مود ۳
همه پورت‌ها را portfast می‌کند

Switch(Config) # Spanning-tree portfast bpduguard default ← مود ۳
روی همه پورت‌ها که portfast هست، گارد هم بگذارد.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

به یاد داشته باشید

با اعمال portfast ، STP را متوقف نمی‌کنیم بلکه فقط Listening و learning انجام نمی‌شود.

هنگامی که همه پورت‌ها را portfast می‌کنید پورت Trunk نباید portfast شود. باید روی interface برای ترانک بزنید و :

```
Switch (Config-if) # No spanning tree
```

انواع STP :

STP	802.1d	ieee	تا الان استفاده کردیم
Rapid STP	801.1w		اگر ارتباط قطع شود ۲ ثانیه‌ای وصل می‌شود
MSTP	802.1s		—

کوئیچ‌های سیسکو هر ۳ مدل را دارند :

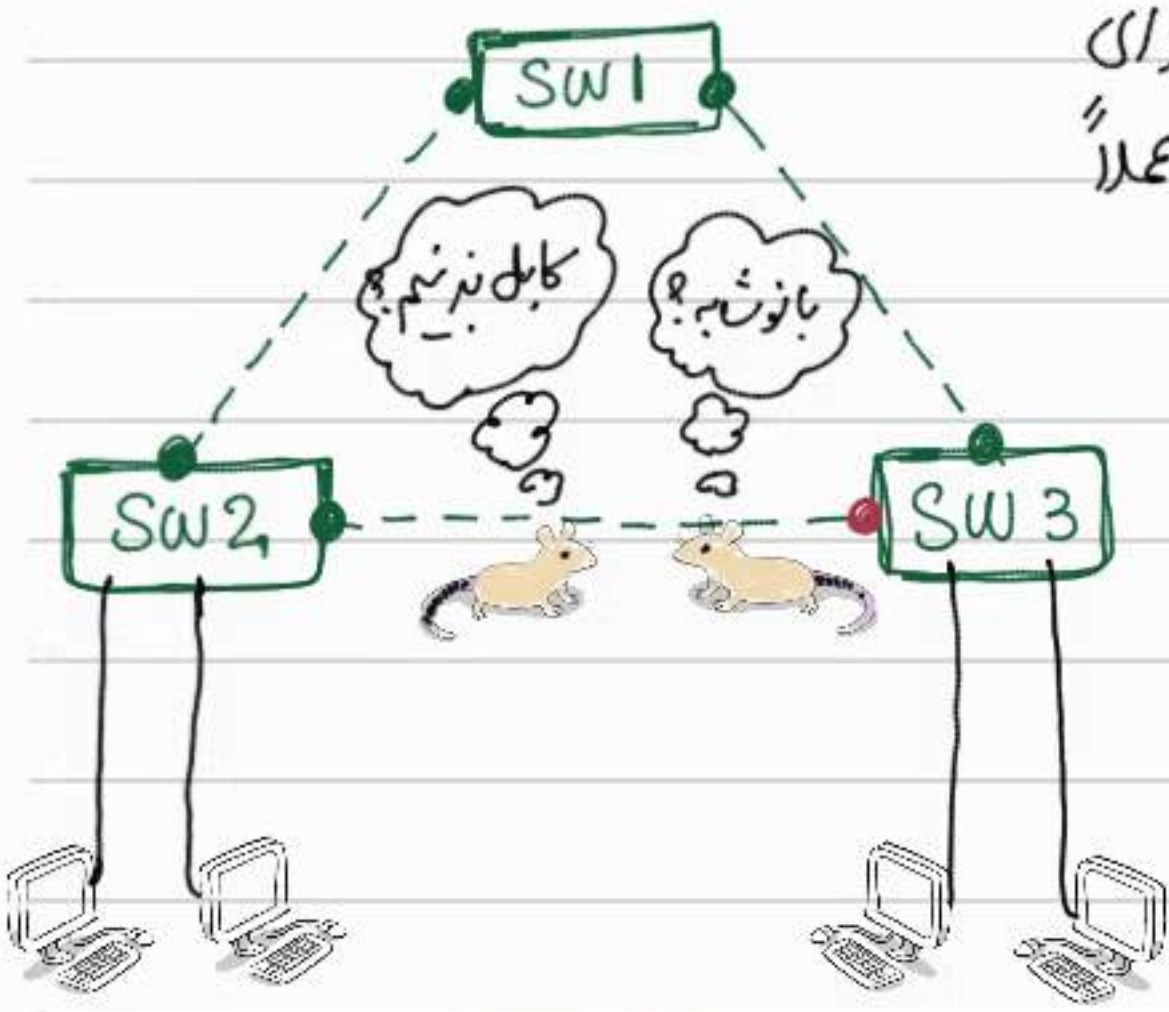
```
Switch (Config) # Spanning-Tree mode ---------
```

- pvst — عادی
- Rapid-pvst — Rapid

در حالت STP عادی اگر لینک قطع شود برای وصل مجدد حدود ۵۰ ثانیه طول می‌کشد در Rapid STP حدود ۲ ثانیه طول می‌کشد.

www.senate-co.com
Farzad Heydari
By Houshang Heshmati

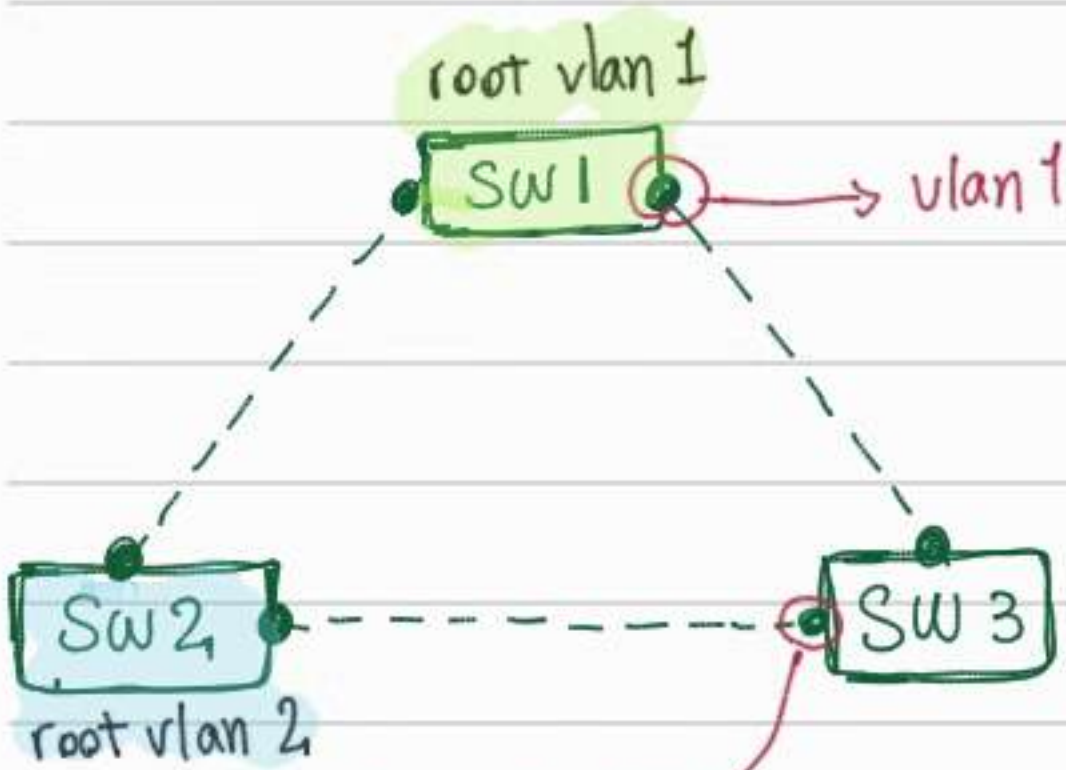
per vlan STP : PVST



کابل بین SW3 و SW2 برای بک آپ کشیده شده است و عملاً بیکار است.

حالا کی بشود که موش بیاد کابل را گاز بزند و قطع بشود تا از بک آپ استفاده کنیم.

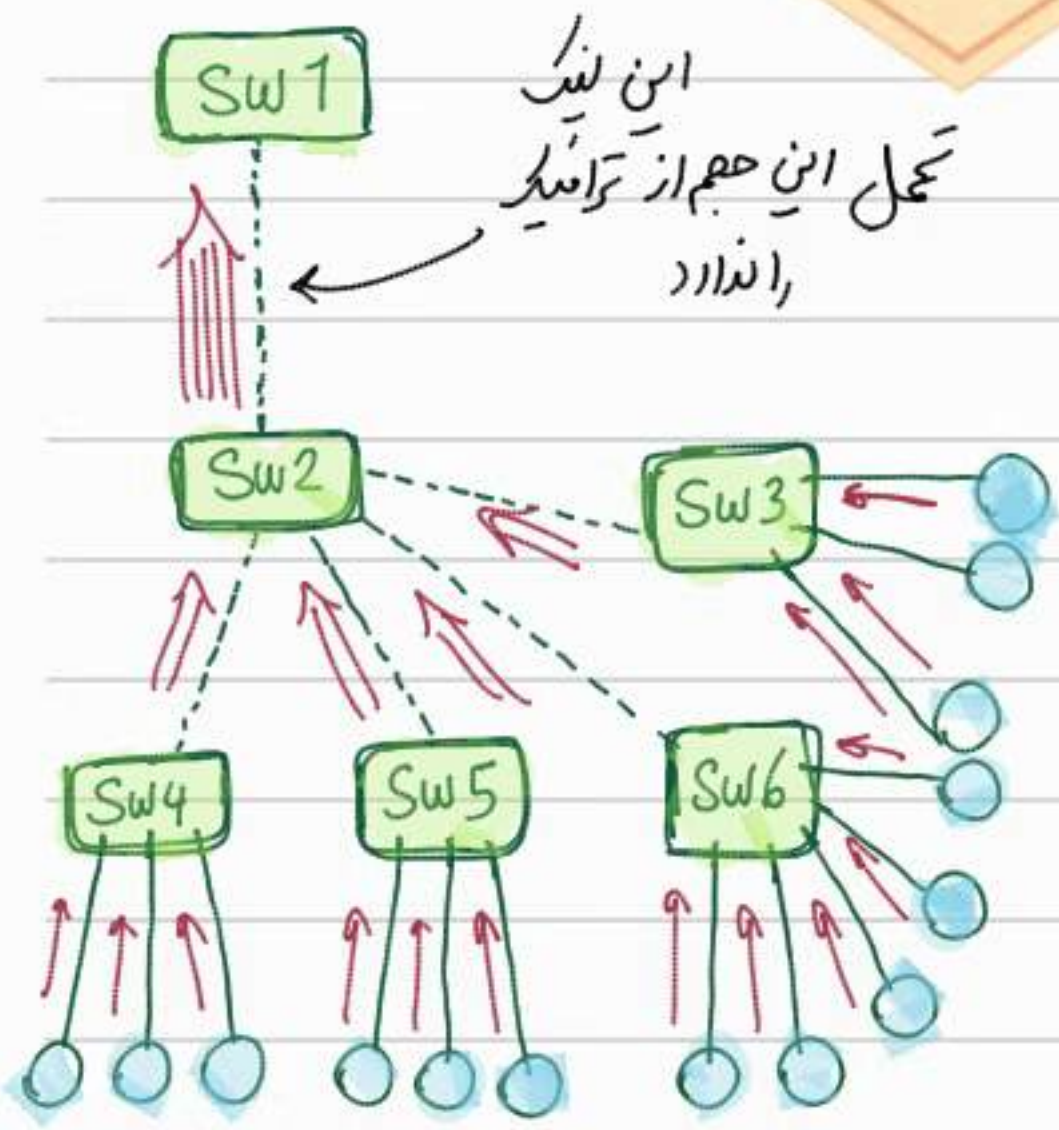
می توانیم با تنظیمات زیر از کابل بک آپ هم استفاده کنیم:



می توانید روی هر SW بزنید show spanning-tree و مشاهده کنید

www.sehatec-co.com
Farzad Heydari
By Houshang Heshmati

Configuring Link Aggregation



این لینک
تحمل این حجم از ترافیک
را ندارد

با استفاده از Aggregation
می‌توانیم چند پورت را با هم جمع
بزنیم و مانند یک پورت استفاده
کنیم

۱) پورت‌های Ethernet نمی‌توان استفاده کرد

۲) سرعت و Type پورت باید یکی باشد fast با fast و gig با gig

۳) حداکثر ۸ پورت با هم aggregation می‌کنند.

۴) mod پورت‌ها باید با هم یکی باشند (Trunk با Trunk)

۵) duplex پورت‌ها باید با هم یکی باشند (auto، half، full)

defaut

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Ether channel

به ۳ روش می‌توانیم aggrigation انجام بدهیم :

① روش دستی (manual) :

باید تعداد پورت‌ها ۲ یا ۴ یا ۸ باشد.

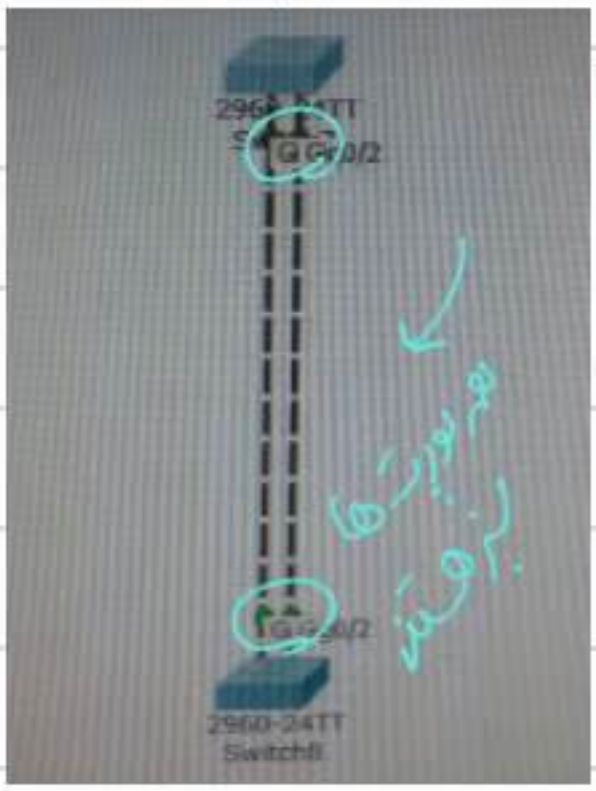
Switch(Config-if-range)# channel-Group ..... mode on
عدد

مهم نیست عدد سوئیچ بالایی با عدد سوئیچ پایینی فرق می‌کند انگار دارید پورت ۴ بالایی را به پورت ۲ پایینی وصل می‌کنید.

Switch(Config)# interface port-channel ..... برای ورود به پورت
عدد

Switch(Config-if)# switchport mode Trunk

Switch # show etherchannel summary




```
Switch(config)#interface ra gig 0/1-2
Switch(config-if-range)#chan
Switch(config-if-range)#chann
Switch(config-if-range)#channeL-G
Switch(config-if-range)#channeL-Group 1 MODE
Switch(config-if-range)#channeL-Group 1 MODE o
Switch(config-if-range)#channeL-Group 1 MODE on
```

سفت

```
Switch(config)#interface po
Switch(config)#interface port-channel 1
Switch(config-if)#swi
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk

Switch(config-if)#
```

ترانک کردم

```
Switch(config)#do sho int tru
Port      Mode         Encapsulation  Status        Na
Po1       on           802.1q         trunking      1

Port      Vlans allowed on trunk
Po1       1-1005

Port      Vlans allowed and active in management domain
Po1       1

Port      Vlans in spanning tree forwarding state and no
Po1       none
Switch(config)#
```

www.semanec-co.com
Farzad Heydari
By Houshang Hesamati

۲) روش pAgp (port aggrigation protocol)

فقط برای سیسکو است و حداکثر ۸ پورت را aggrigation می‌کند.

Switch(config-if-range)# channel-protocol pagp

Switch(config-if-range)# channel-group ..... mode .....

→ auto
→ desirable

۲ تا auto باشند کار نمی‌کند

۲ تا desirable باشند یا یکی auto یکی desirable باشد کار می‌کند

```
Switch(config)#interface ra fa 0/14
Switch(config-if-range)#channel-pr
Switch(config-if-range)#channel-protocol pa
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#chan
Switch(config-if-range)#channel-g
Switch(config-if-range)#channel-group 1 mod
Switch(config-if-range)#channel-group 1 mode on
Command rejected (the interface fa0/14 is ): is already part o
enabled
Switch(config-if-range)#swi
Switch(config-if-range)#switchport mo
Switch(config-if-range)#switchport mode tr
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode de
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1
```

وقتی PAGP هست این را نزنید

خودش پیغام داد

یک سمت desirable بزنید روی سمت دیگر auto بزنید

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

۳) روش سوم LACP :

در این روش ۱۶ پورت را می‌توان aggrigation کرد. اما در نهایت باز ۸ پورت کار می‌کند و ۸ پورت به صورت بک آپ Standby هستند تا اگر یکی از ۸ پورت اصلی قطع شد جایگزین شوند.

Switch(Config-if)# channel-protocol LACP

Switch(Config-if)# channel-group ..... عدد ..... mode .....

active
passive

active پیشنهاد می‌کند و passive پیشنهاد قبول می‌کند. هر دو active باشند وصل می‌شود ولی تعداد Hello ها و بار شبکه بالا می‌رود. بهتر است یک سمت active و سمت دیگر passive.

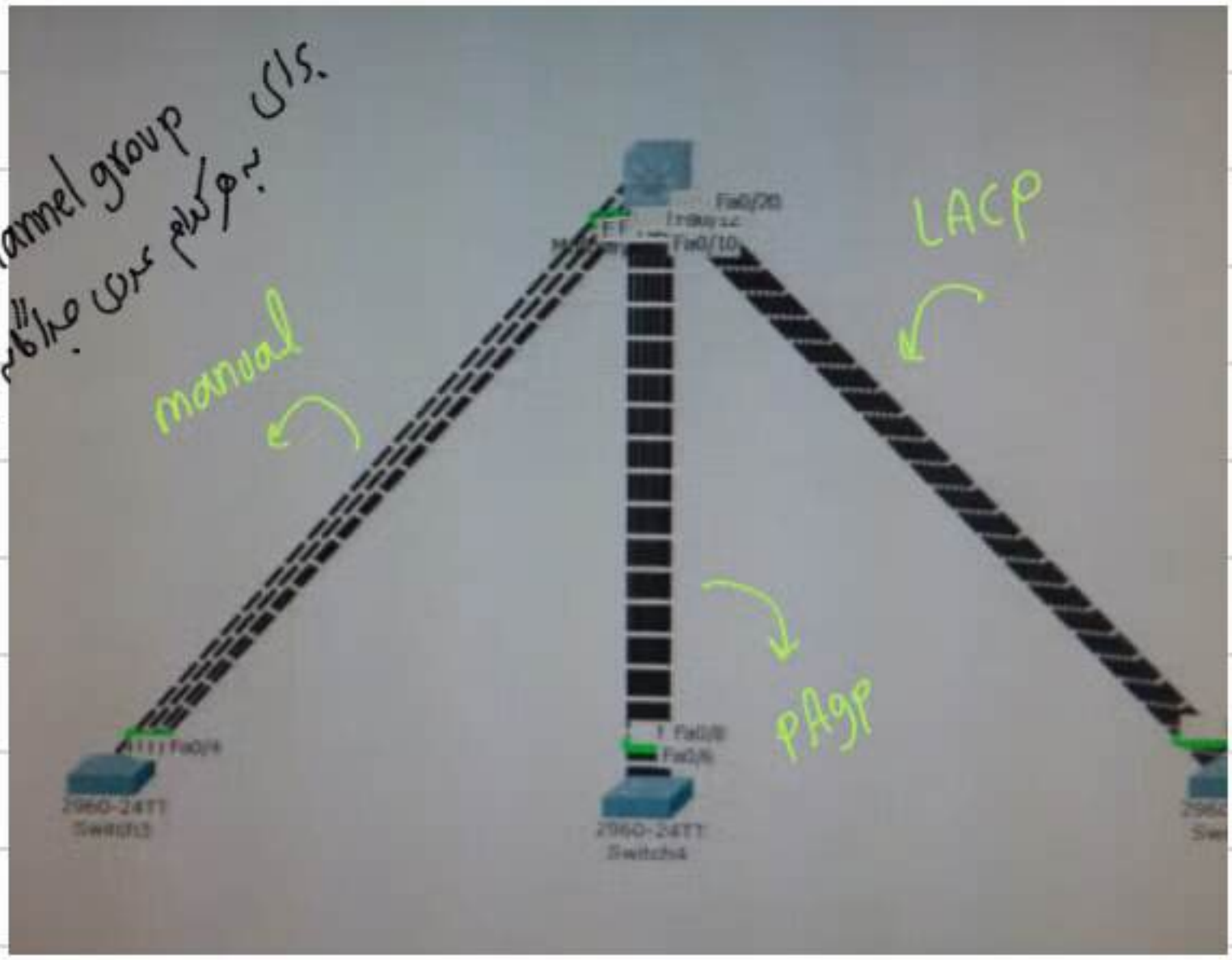
```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface ra
Switch(config)#interface range fa
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#channel-p
Switch(config-if-range)#channel-protocol lacp
Switch(config-if-range)#channel-g
Switch(config-if-range)#channel-group 1 mod
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1
```

حتماً در امتحان بین المللی سؤال دارید ولی در امتحان بین المللی range کار نمی‌کند باید تک تک پورت را بروید و دستور بزنید.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

خیلی فرقی ندارد با کدام دستور aggrigation کنید.

channel group cis.
به هر کدام بدی میخوای بدی




```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#
Switch(config-if-range)#do sho ethe
Switch(config-if-range)#do sho ethe su
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------------------------------------

1      Po1(SU)           -      Fa0/1(P) Fa0/2(P) Fa0/3(P) Fa0/4(P)
2      Po2(SU)           PAgP   Fa0/5(P) Fa0/6(P) Fa0/7(P) Fa0/8(P) Fa0/9(P) Fa0/10(P) Fa0/11(P) Fa0/1
3      Po3(SU)           LACP   Fa0/13(P) Fa0/14(P) Fa0/15(P) Fa0/16(P) Fa0/17(P) Fa0/18(P) Fa0/19(P)
Switch(config-if-range)#
```

manual PAgP LACP

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

با دستور show Ethernet Summary می‌توانید مشخصات aggregate را ببینید:

Su: Layer in use

SSH

Secure SHell

برای ریموت متصل شدن به لوئیچ و روترها از Telnet استفاده نکنید
چون امن نیست. Telnet پورت ها را بصورت clear text ارسال می کند.

باید برای جاهایی که سازمانی هستند و امنیت مهم است از SSH استفاده کنند
IOS لوئیچ باید حتماً قابلیت encryption داشته باشد وگرنه SSH را
ساپورت نمی کند.
اگر دستور show ver را در لوئیچ زدید و K9 بود، می تواند.

```
3825-common-criteria#sh version
Cisco IOS Software, 3800 Software (C3825-ADVENTERPRISEK9-M), Version 12.3(14)T7, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 23-Mar-06 01:17 by pwade

ROM: System Bootstrap, Version 12.3(11r)T1, RELEASE SOFTWARE (fc1)

3825-common-criteria uptime is 17 minutes
System returned to ROM by reload at 17:21:20 UTC Mon Jun 26 2006
System image file is "flash:c3825-adventerprisek9-mz.123-14.T7.bin"
```

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

برای کانفیگ کردن ssh:

۱) به سوئیچ IP می‌دهیم (vlan 1)

۲) Line vty را امن می‌کنیم (login local)

۳) enable secret

4) اسم سوئیچ را عوض می‌کنیم (hostname)

5) اسم دامین به سوئیچ می‌دهیم

6) طول کلید Encryption را زیادتر می‌کنیم

1) Switch(Config)# interface vlan 1
Switch(Config-if)# ip address ...IP... ...subnet...
Switch(Config-if)# No shut

۲) Switch(Config)# Line vty 0 15
Switch(Config-line)# Login Local
Switch(Config-line)# Transport input shh

Telnet غیرفعال می‌شود و فقط shh می‌شود

Switch(Config)# username ...اسم... secret ...کلمه...

3) switch(Config)# enable secret ...کلمه...

4) Switch(Config)# hostname ...اسم...

www.sematec-co.com
Farzad Heydari
By Huawei and Ideahipad

5) Switch(Config)# Ip domain-name ...اسم...

6) Switch(config)# Crypto key generate rsa

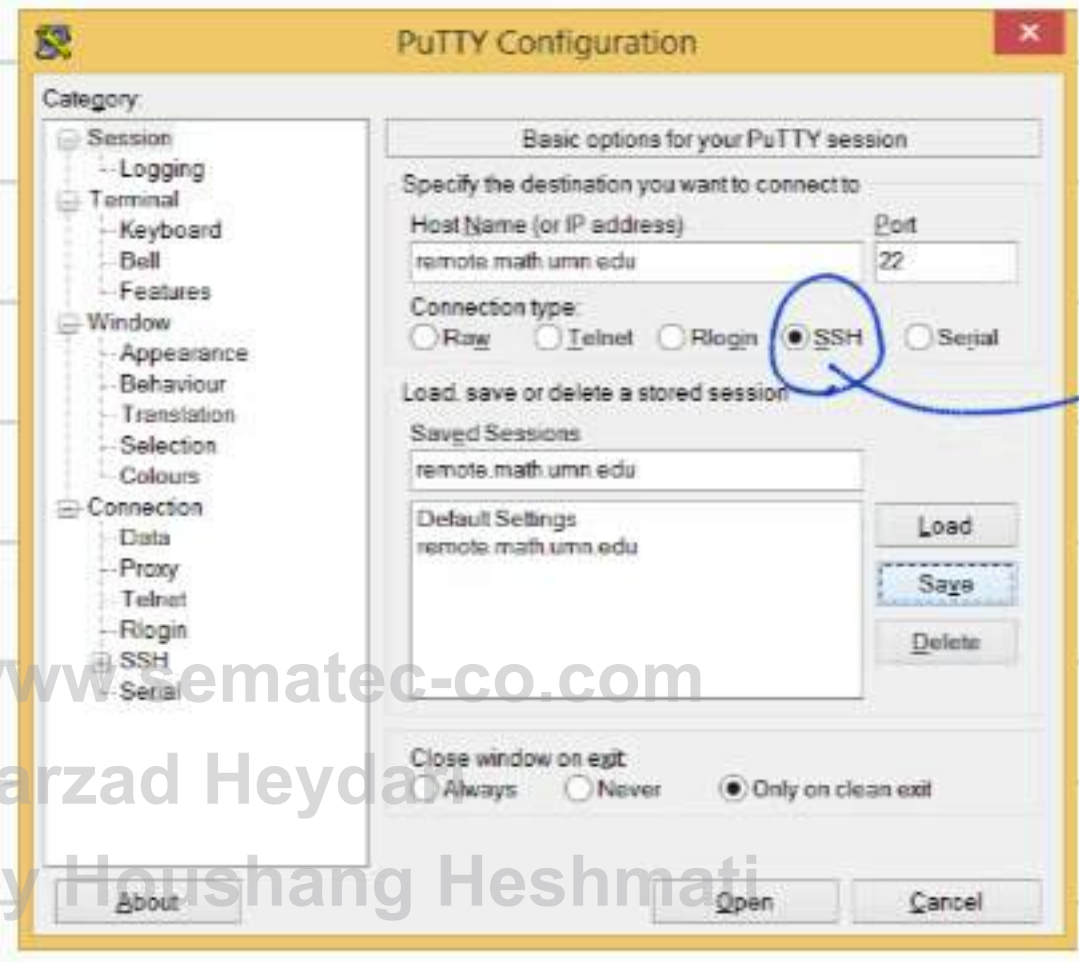
سوال می‌پرسد:

How many bits in modulus [512]: .....

```
router01(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
router01(config)#
router01(config)#
router01(config)#crypto key generate rsa
The name for the keys will be: router01.soundtraining.net
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

router01(config)#
```

منظور 1024 است. هرچی این طول بیشتر باشد، شکستن قفل آن سخت‌تر است.

برای اتصال می‌توانید از نرم‌افزارهای جانبی مانند putty استفاده کنید:

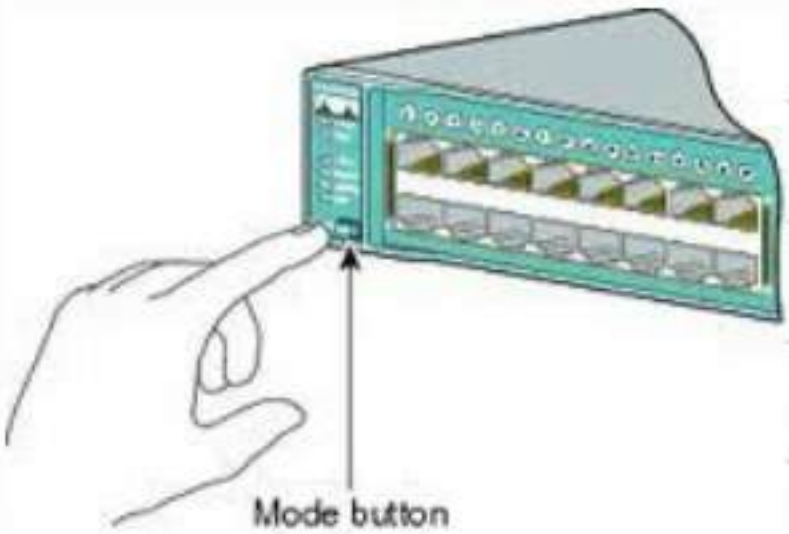


را انتخاب می‌کنیم ssh

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Password Recovery

برای بازیابی پسورد سوئیچ : (باید حتماً دسترسی فیزیکی داشته باشید)



۱) کابل کنسول را وصل می‌کنیم (نرم‌افزار Tera Team)

۲) برق را قطع می‌کنیم و خاموش می‌کنیم

۳) دکمه mode را نگه می‌داریم

۴) سوئیچ را روشن می‌کنیم

Switch :

۵) بجای حالت عادی ، یک مود جدید بالا می‌آید.
یعنی روی Rom نیستیم.

Switch: flash_init

۶) Flash را لود می‌کنیم

Switch: rename flash:config.text flash:peyman

۷) اسم فایلی که پسورد را نگه می‌دارد عوض می‌کنیم

Switch: boot

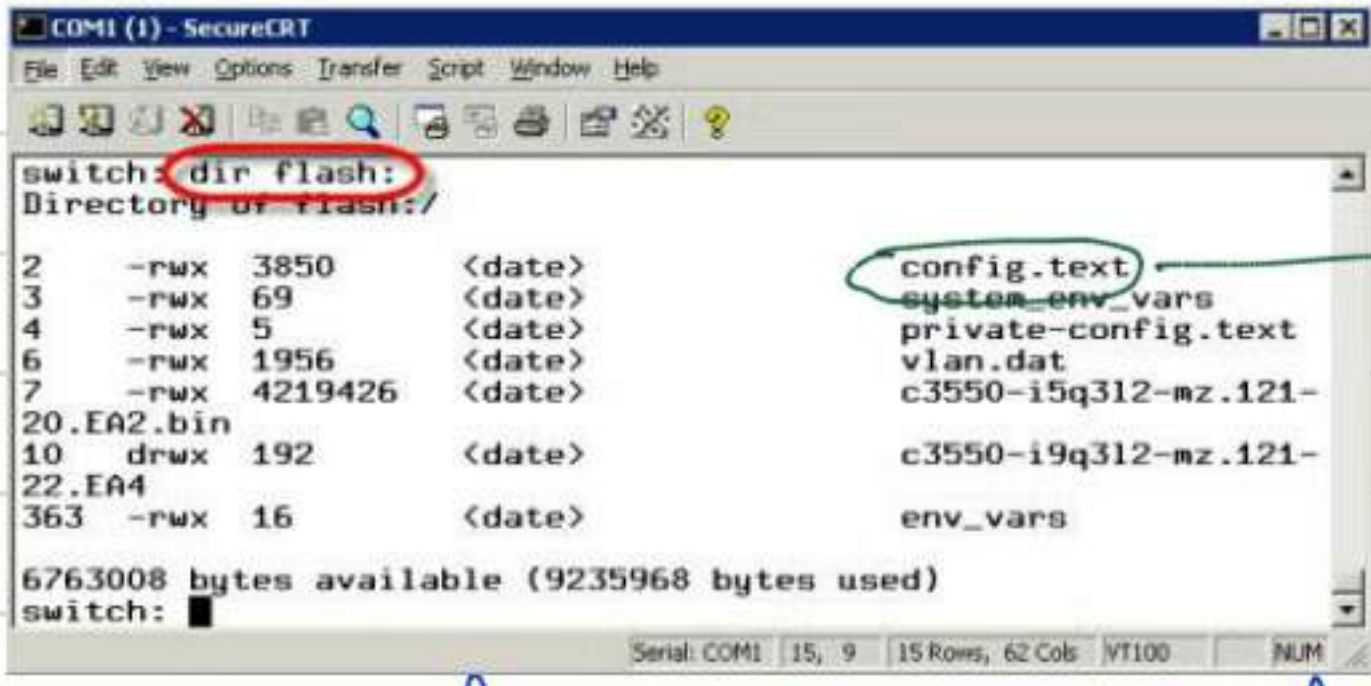
۸) سوئیچ فایل پسورد را نمی‌بیند و لود می‌شود . سوئیچ خام بالا می‌آید

Switch # rename flash:peyman flash:Config.Text

۹) اسم فایل پسورد را دوباره به حالت اول برمی‌گردانیم

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

تحت هیچ شرایطی WR نزنید (save نکنید) نه‌ها می‌رود



یافتن اسم فایل دارای کورد

Switch# copy config.text system:running_config

۱۰) اطلاعات کوئیج را به کوئیج خام برگردانیم همه چی سر جای خودش رفته است. اگر الان show ron بزنید می بینید:

Switch (config) # enable password _____

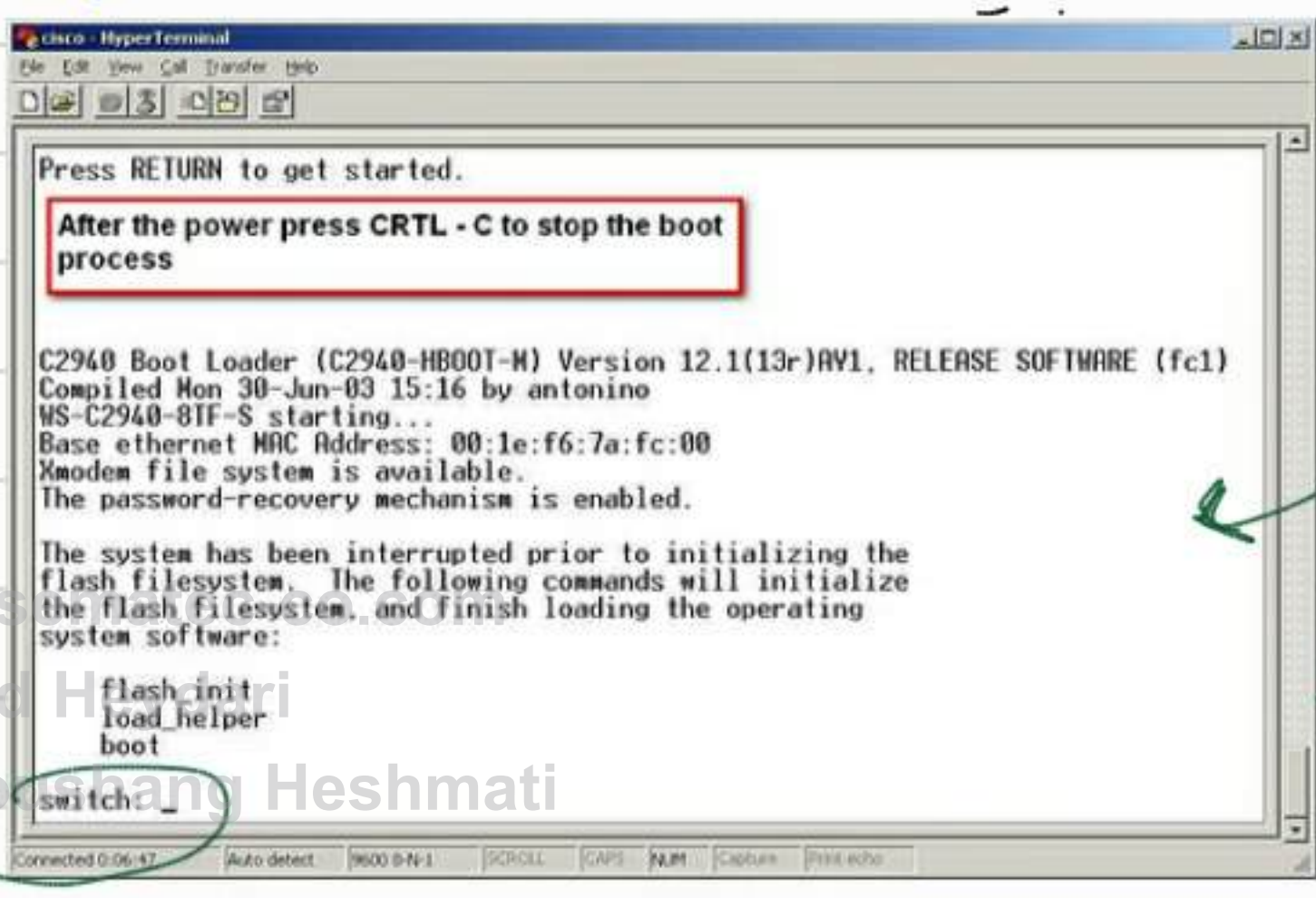
هر چی دوست دارید

Switch (config) # username _____ هر چی دوست دارید password _____ هر چی دوست دارید

۱۱) به مود ۳ بروید و کورد را به هر چی تمایل دارید تغییر بدهید.

Switch # wr

۱۲) حالا wr بزنید.

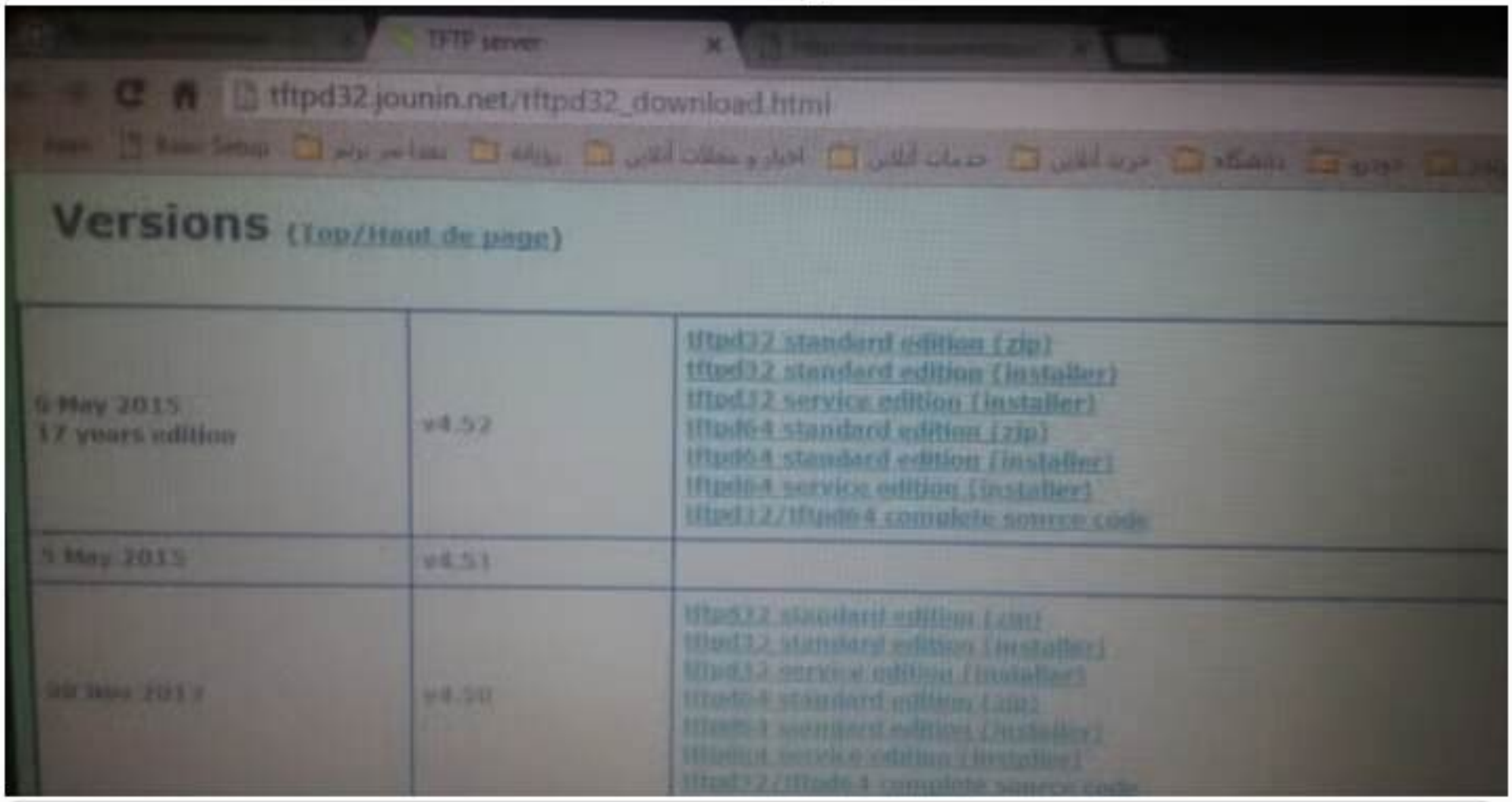


جای خط که جای IOS بالا میآید

www.simplesoft.com
Farzad Hosseini
By Houshang Heshmati

Back up گیری از لوئیچ و آپدیت کردن IOS لوئیچ:

می‌توانید از نرم افزار رایگان که از اینترنت دانلود می‌کنید استفاده کنید



مانند Solarwinds Tftp Server یا Tftpd32 یا ....

هنگامی که روی ویندوز نصب می‌کنید معمولاً یک در درایو یک فولدر به نام Tftproot می‌سازد.

از اینترنت IOS جدید برای لوئیچ خود را می‌گیرید. (حدود ۲۰ مگ هست) از سایت‌های ایرانی دانلود کنید. پس از دانلود فایل را داخل پوشه Tftproot کپی می‌کنید

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

ریموت هم می‌توانید دستور بزنید :

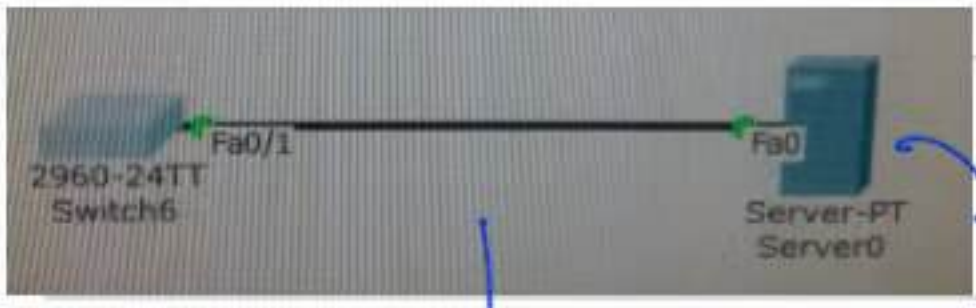
Switch # copy tftp: flash:

address or name of remote host []? IP خودتان را می‌دهید

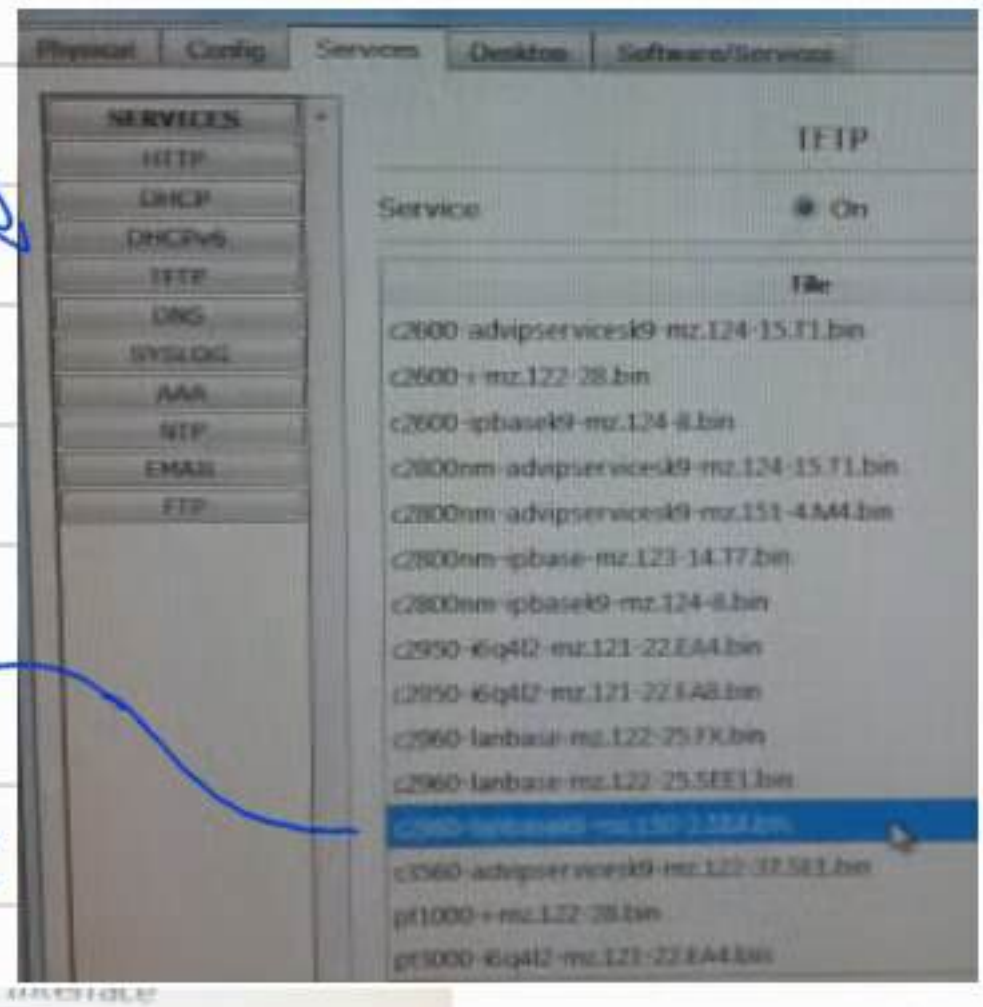
کامپیوتری که فایل روی آن است.

Source filename []? اسم فایل آپ دیت را می‌دهید

Destination filename [اسم فایل]? y یا



برای سناریو یک TFTP Server و سایر



Ctrl+C کپی کنید

```
Vlan1, changed state to up

Switch(config-if)#EXIT
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy tftp: flash:
Address or name of remote host []? 10.0.0.1
Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin
Destination filename [c2960-lanbasek9-
mz.150-2.SE4.bin]?
Accessing tftp://10.0.0.1/c2960-lanbasek9-
mz.150-2.SE4.bin....
Loading c2960-lanbasek9-mz.150-2.SE4.bin from
10.0.0.1:
!!!
```

پس کپی شدن فایل آپدیت که

Switch(config)# boot System flash: ___ اسم فایل آپدیت ___

IOS جدید بوت می شود پس از اینکه اطمینان پیدا کردید همه چی ردیفه و کار می کند و فایل خراب نیست می توانید فایل قبلی را پاک کنید.

Switch(config)# delete flash: ___ اسم فایل قبلی (قدیمی) ___

Switch # show ver ↵ : مشخصات IOS را ببینید

```
!!!
```

Backup گیری :

اول wr بزنید تا همه اطلاعات Save لود پس :

Switch #Copy Startup-Config tftp :

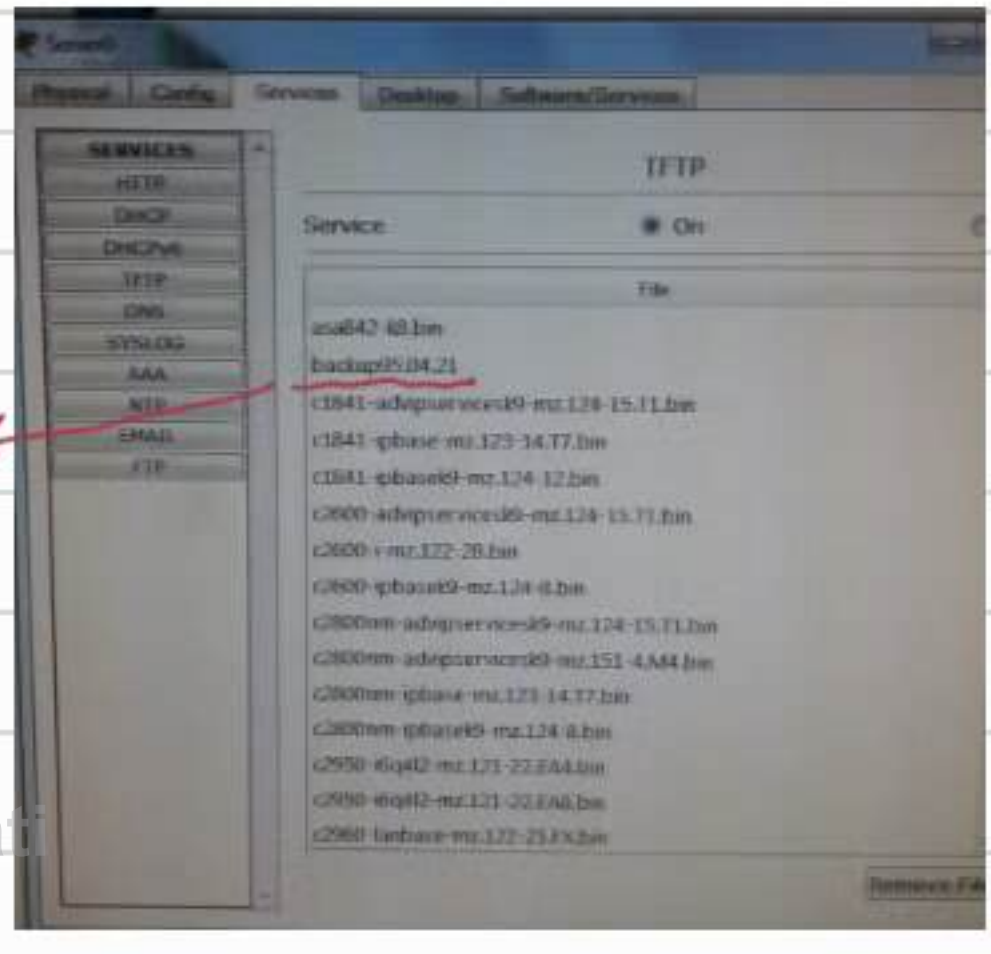
Address or name of remote host[ ]? ----------

Ip سروری که می‌خواهید بک‌آپ ذخیره کنید

Destination filename [Switch-Config]? ----------

اسم فایل بک‌آپ مثلاً Backup95.04

```
Switch#wr
Building configuration...
[OK]
Switch#copy startup-config tftp:
Address or name of remote host []? 10.0.0.1
Destination filename [Switch-confg]? backup95.04.21

Writing startup-config...!!
[OK - 1053 bytes]

1053 bytes copied in 0.028 secs (37607 bytes/sec)
Switch#
```



توی کدوم ذخیره شد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

بازگرداندن بک آپ

Switch # copy tftp: flash:

address or name of remote host [ ]? ---------- Ip

کامپیوتری که فایل روی آن است.

Source filename [ ]? ---------- اسم فایل بک آپ را می‌دهیم

Destination filename [---- اسم فایل]? y یا

بعد فایل کپی شده را به Startup می‌فرستیم.

Switch # copy Flash: Startup-config

Destination filename [Startup-config]?

سوئیچ تمام شد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Router ⊗

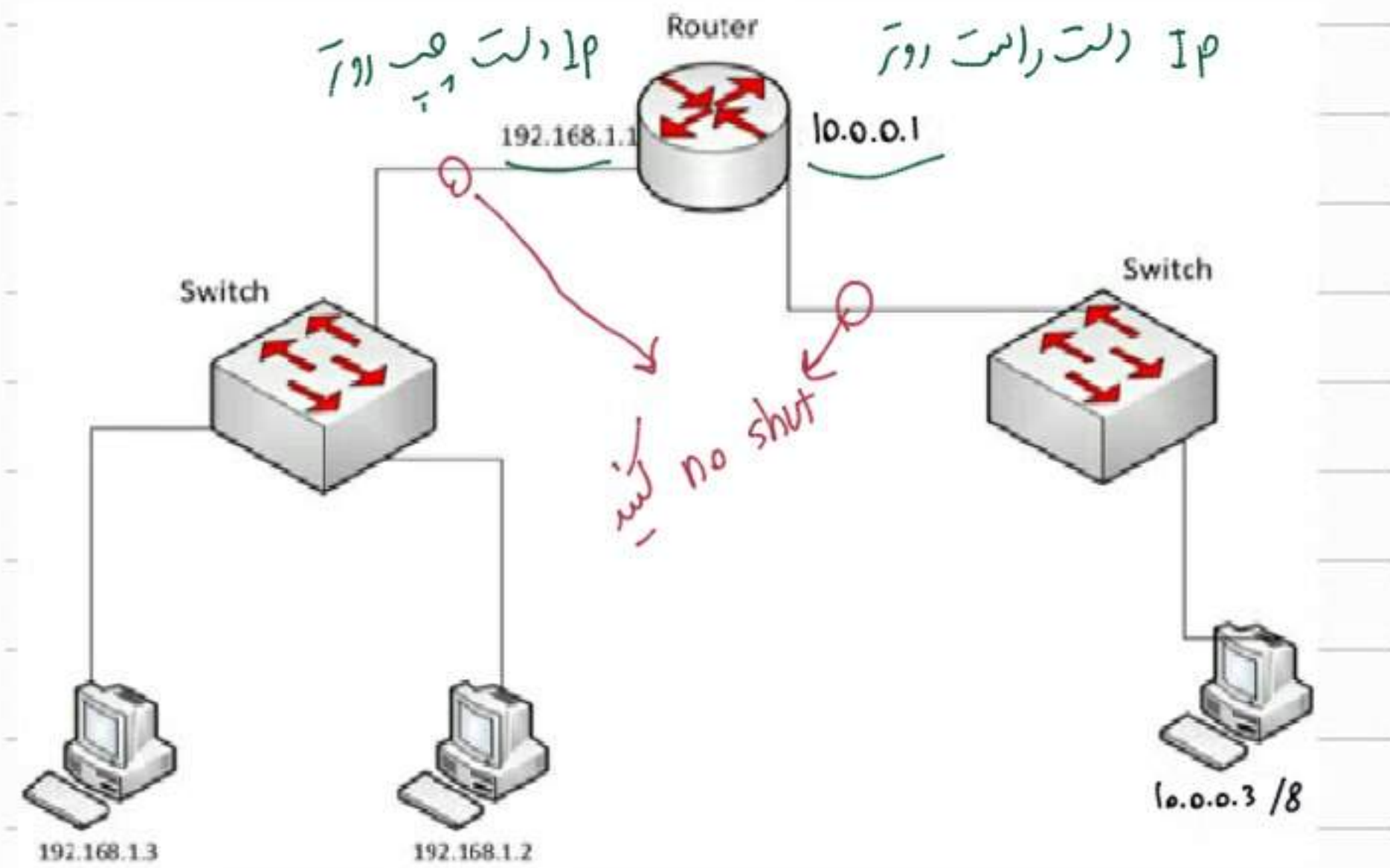
www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

قبل از مطالعه بخش روتر ها" بخش IP و Subneting از دوره Network+ خوب بخوانید.

تفاوت های روتر و سوئیچ

Router	Switch
محدوده کاری Layer 3	Layer 2
ارسال دیتا بروی IP	Mac-address
inter-Network	intra-network
ماژول خاموش روشن دارد on/off	کلید خاموش روشن ندارد
interface 0/0	interface 0/1
modular (به آن ماژول نصب می شود)	Fix and modular
اگر مقصد را نداند بسته را Drop می کند	اگر مقصد را نداند بسته را flood می کند
پورت AUX دارد	پورت AUX ندارد
از اول interface ها خاموش است	از اول interface ها روشن است
Broad cast را Drop می کند	Broad cast را flood می کند
routing table دارد	Mac-address table دارد

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati



هر پورت روتر می‌تواند وارد یک شبکه شود. شکل بالا دلت سمت چپ روتر وارد شبکه 192.168.1.0/24 شده است. دلت سمت راست وارد شبکه 10.0.0.0/8 شده است.

هر دلت روتر IP می‌گیرد. هر IP که به دلت روتر بدهیم برای آن شبکه بعنوان Default Gateway استفاده می‌شود. و روتر می‌تواند شبکه‌های مختلف را به هم وصل کند.

پورت های روتر از اول خاموش است باید هنگام IP دادن No shut هم بکنیم.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

```
Router(config)#interface fa
Router(config)#interface fastEthernet 0/1
Router(config-if)#no
Router(config-if)#no sh
Router(config-if)#no shutdown
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#no
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#exit
```

وارد دلت چپ می‌شویم

IP می‌دهیم

وارد دلت راست می‌شویم

IP می‌دهیم

Router # show Ip route routing نمایش جدول

```
Router#sh
Router#show ip
Router#show ip r
Router#show ip rou
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 are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route.

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
Router#
```

نمایش جدول routing table برای روتر

یعنی متصل به خود روتر

برای ارتباط بین دو تا روتر در شهرهای مختلف می‌توانید از مخابرات (شرکت ارتباطات زیرساخت) تلفن بگیرید خود مخابرات می‌گوید چه ماژولی بخرید و روی روتر نصب کنید

(در cisco packet Tracer) روتر را خاموش کنید و ماژول‌های زیر را اضافه کنید:

WIC → wan interface card چند پورت سریال می‌دهد

NM → Network modual

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

یادآوری و مروری بر IP و Subneting :

IpV4 : 32 بیتی است.

IpV6 : 128 بیتی است.

192.168.1.1 $\xrightarrow{\text{باینری}}$ 11000000.10101000.00000001

ارزش هشت بیت

چگونه بیت‌ها را چ کردیم

128 . 64 . 32 . 16 . 8 . 4 . 2 . 1

192 = 1 + 1 + 0 + 0 + 0 + 0 + 0 + 0 = 192

= 1 1 0 0 0 0 0 0

128 . 64 . 32 . 16 . 8 . 4 . 2 . 1

168 = 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 = 168

= 1 0 1 0 1 0 0 0

کلاس های IP :

کلاس A : بیت اول اوکتت اول صفر است. (از صفر تا 127)

0 0 0 0 0 0 0 0 از صفر

0 1 1 1 1 1 1 1 تا 127

IP 127.X.X.X برای Loopback رزرو شده است. (تست Tcp-ip)

کلا کلاس A رزرو است.

کلاس B : اوکتت اول با 10 شروع می‌شود (از 128 تا 192)

1 0 0 0 0 0 0 0 از 128

1 0 1 1 1 1 1 1 تا 191

Apipa (169.254.X.X) رزرو مایکروسافت برای IP اتوماتیک است.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

کلاس C : اوکتت اول با 110 آغاز می‌شود (از 192 تا 223)

192 از	110 00000
223 تا	110 1111

کلاس D : اوکتت اول با 1110 آغاز می‌شود (از 224 تا 239)

224 از	1110 0000
239 تا	1110 1111

این محدوده برای آدرس های مالتی کست رزرو شده است. (مانند بسته های Hello روی Eigrp)

کلاس E : اوکتت اول با 1111 آغاز می‌شود (از 240 تا 255)

240 از	1111 0000
255 تا	1111 1111

- این محدوده برای کارهای تحقیقاتی و تست رزرو شده است. توسط (IEFF)

IP ها به دو دسته تقسیم می‌شوند : private (برای استفاده داخل شبکه)
public (برای استفاده در اینترنت)

IP های private :
- 10.0.0.0 تا 10.255.255.255
- 172.16.0.0 تا 172.31.255.255
- 192.168.0.0 تا 192.168.255.255

این دسته از IP ها در اینترنت route نمی‌شوند و برای سازمان و شرکت‌ها برای سیستم‌های داخلی می‌توانید استفاده کنید.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

روتر با subnet کار می‌کند.

192.168.1.100 255.255.255.0

مشخص کننده Network — مشخص کننده host

classfull addressing

تعداد هنود در بایتی H که $2^H - 2$ محاسبه تعداد host در یک subnet

A : 255.0.0.0 (8 8 8) $\rightarrow 2^{24} - 2 = 16\,777\,214$ host

B : 255.255.0.0 $\rightarrow 2^{16} - 2 = 655\,534$ host

C : 255.255.255.0 $\rightarrow 2^8 - 2 = 254$ host

هر یک دانه IP ارزش دارد و از حالت classfull استفاده نمی‌شود

: Subnetting

198.1.1.0 / 24 255.255.255.0 $\rightarrow 2^8 - 2 = 254$

ولی اگر 62 کامپیوتر داشته باشیم بجای 254 تا؟

11111111.11111111.11111111.00000000 $2^8 - 2 = 254 \leftarrow /24$

11111111.11111111.11111111.10000000 $2^7 - 2 = 126 \leftarrow /25$

11111111.11111111.11111111.11000000 $2^6 - 2 = 62 \leftarrow /26$ ✓

یعنی از 192.168.1.1/26 تا 192.168.1.62/26

www.sematech.com
Farzad Hayatbakhsh
By Houshang Hoshmati

کلاس C

	تعداد بیت	اگر با کلاس C جمع شود	سابنت		تعداد host
/1	128	124+1	255.255.255.128	/25	126
/2	192	124+2	255.255.255.192	/26	62
/3	224	124+3	255.255.255.224	/27	30
/4	240	124+4	255.255.255.240	/28	14
/5	248	124+5	255.255.255.248	/29	6
/6	252	124+6	255+255.255.252	/30	2
/7	254	124+7	255.255.255.254	/31	—
/8	255	124+8	255.255.255.255	/32	—

کلاس B

	تعداد بیت	اگر با کلاس B جمع شود	سابنت		تعداد host
/1	128	16+1	255.255.128.0	/17	32766
/2	192	16+2	255.255.192.0	/18	16382
/3	224	16+3	255.255.224.0	/19	8190
/4	240	16+4	255.255.240.0	/20	4094
/5	248	16+5	255.255.248.0	/21	2044
/6	252	16+6	255.255.252.0	/22	1022
/7	254	16+7	255.255.254.0	/23	510
/8	255	16+8	255.255.255.0	/24	254

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Ip classless

فعلاً در شبکه‌ای از 10.0.0.0/24 استفاده کردیم و به 14 IP احتیاج داریم

10.0.0.0/24 → 255.255.255.0

00000000 → $2^8-2=254$

1110 0000 → $2^5-2=30$ هنوز زیاد است

1111 0000 → $2^4-2=14$ ✓

4

→ 14 + 124 → 128 → 255.255.255.240

شبکه‌ای که تنها 2 IP داشته باشد؟

10.0.0.0/24 255.255.255.0

خیلی مهم است حفظ باشید برای اتصال نقطه به نقطه (P2P) مانند 2 روتر استفاده می‌شود

11111100 → $2^2-2=2$

6

12 + 124 → 130 255.255.255.252

در شبکه‌ای که 310 کامپیوتر داریم می‌خواهیم از 172.16.0.0 استفاده کنیم

255.255.11111111.00000000 هاست $2^8-2=254$

255.255.11111110.00000000 هاست $2^9-2=510$

255.255.11111100.00000000 هاست $2^{10}-2=1022$

از این استفاده می‌کنیم که کمترین اتلاف IP را داشته باشد.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

اگر در شبکه‌ای با IP 192.168.1.0 تعداد 66 کامپیوتر داشته باشیم

225.225.255.00000000 → $2^8 - 2 = 252$ /24

225.225.255.10000000 → $2^7 - 2 = 127$ ✓ /25

225.225.255.11000000 → $2^6 - 2 = 64$ /26

چون 66 تا می‌خواهیم مجبوریم از بازه دومی استفاده کنیم

شبکه دوبرو چند هاست دارد؟ 172.1.1.1 /20

$32 - 20 = 12$ صفر → $2^{12} - 2 = 4094$ هاست

تعداد بیت‌ها کل

در فرمول $2^h - 2$ چرا از عدد 2 کم می‌کنیم؟

$2^h - 2 =$

2 → Net ID مثل 192.168.1.0 یعنی همه host ها صفر باشند

2 → Broadcast مثل 192.168.1.255 همه host ها یک باشند.

دو تا IP را نمی‌توانیم استفاده کنیم

Net ID و Broadcast در classless IP چگونه محاسبه می‌شود

→

www.somatec-co.com
Farzad Heydari
By Houshang Heshmati

مثلاً برای Ip روبرو، Net ID و Broadcast را حساب کنید:

192.168.1.20 / 28

/28 → 255.255.255.240 $\xrightarrow{\text{از کل}}$ 256 - 240 = 16

پس هر بازه شبکه 16 Ip دارد. یعنی 16 تا 16 تا می‌رویم جلو:

Net ID

192.168.1.0

⋮

192.168.1.15

Broadcast

16 تا

شبکه اول

Net ID

192.168.1.16

⋮

192.168.1.31

Broadcast

16 تا

شبکه دوم

Ip ما در این بازه قرار دارد

Net ID

192.168.1.32

⋮

192.168.1.47

Broadcast

16 تا

شبکه سوم

و الی آخر

www.sematech-co.com
Farzad Heydari
By Houshang Heshmati

مثلاً برای IP روبرو، Net ID و Broadcast را حساب کنید:

192.168.10.50 /27

/27 → 255.255.255.224 $\xrightarrow{\text{از کل}}$ 256 − 224 = 32

پس هر بازه شبکه 32 IP دارد. یعنی 32 تا 32 تا می‌رویم جلو:

Net ID

192.168.10.0

⋮

192.168.10.31

Bro

32 تا

شبکه اول

Net ID

192.168.10.32 → Net ID IP

⋮

192.168.10.63 → Broadcast IP

Bro

32 تا

شبکه دوم

IP ما در این بازه قرار دارد

Net ID

192.168.10.64

⋮

192.168.10.95

Bro

32 تا

شبکه سوم

الی آخر

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

مثلاً برای IP روبرو، Net ID و Broadcast را حساب کنید:

10.14.0.1 /13

/13 → 255.248.0.0 $\xrightarrow{\text{از کل}}$ 256 − 248 = 8

پس هر بازه شبکه 8 IP دارد. یعنی 8 تا 8 تا رو هم طی:

8 تا

10.0.0.0
⋮
10.7.0.0

یک شبکه

8 تا

10.8.0.0 → Net IP
⋮
10.15.0.0 → Broadcast

یک شبکه

IP ما در این شبکه قرار دارد ← 8 < 14 < 15

8 تا

10.16.0.0
⋮
10.23.0.0

یک شبکه

نکته خیلی مهم

در اتصال 2 روتر بهتر است از /30 استفاده شود 10.0.0.1 /30

/30 → 255.255.255.252 $\xrightarrow{\text{از کل}}$ 256 − 252 = 4

پس هر بازه 4 تا 4 جدا می‌شود.

4 تا

10.0.0.0 → Net ID
10.0.0.1
10.0.0.2
10.0.0.3 → Broadcast

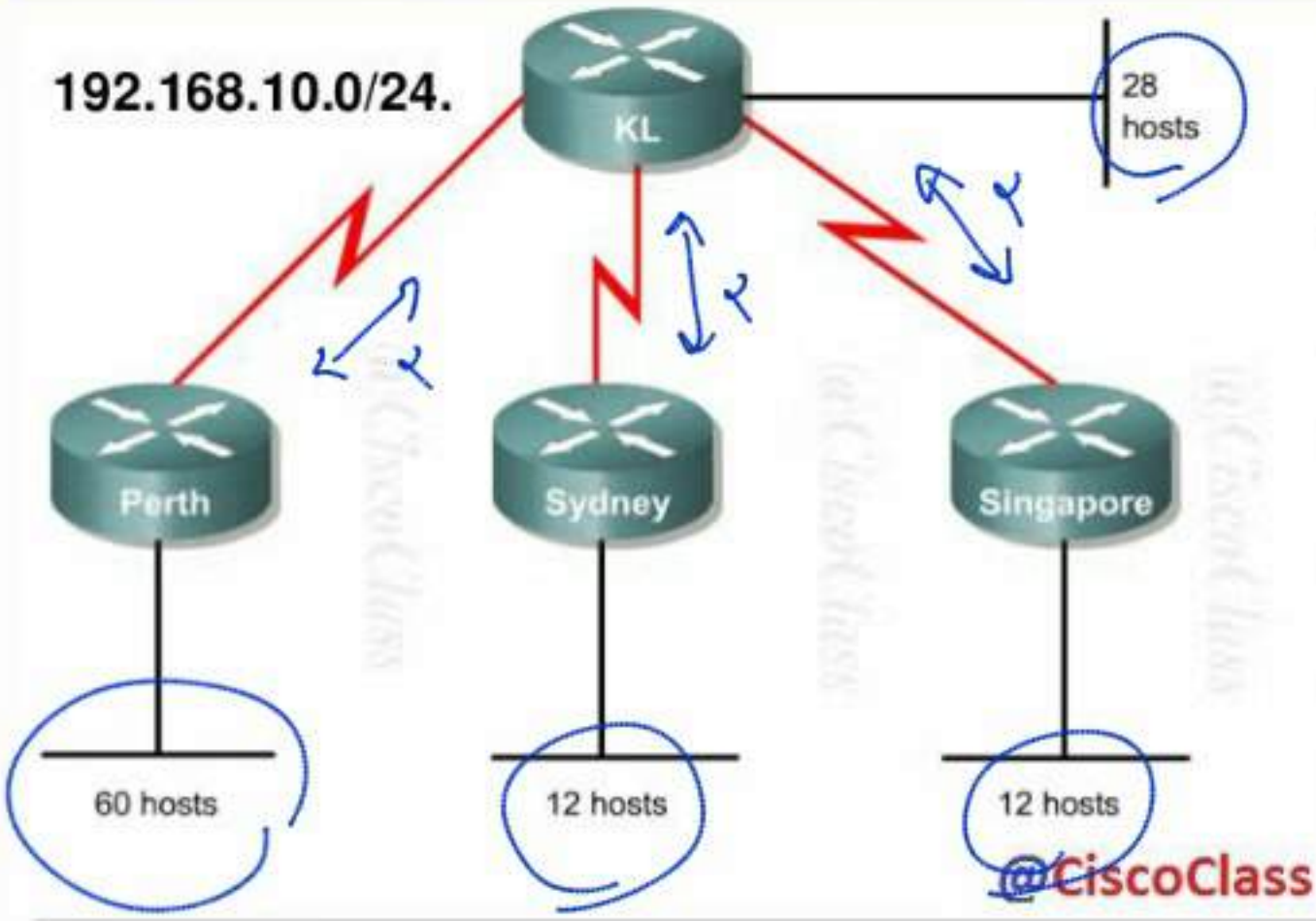
یک شبکه

اگر Net ID یا Broadcast را بجای IP برای روتر برنامه اشتباه شود. IP2 در هر بازه داریم

www.sematec-co.com
Farzad Heydari
By Houshang Hesamat

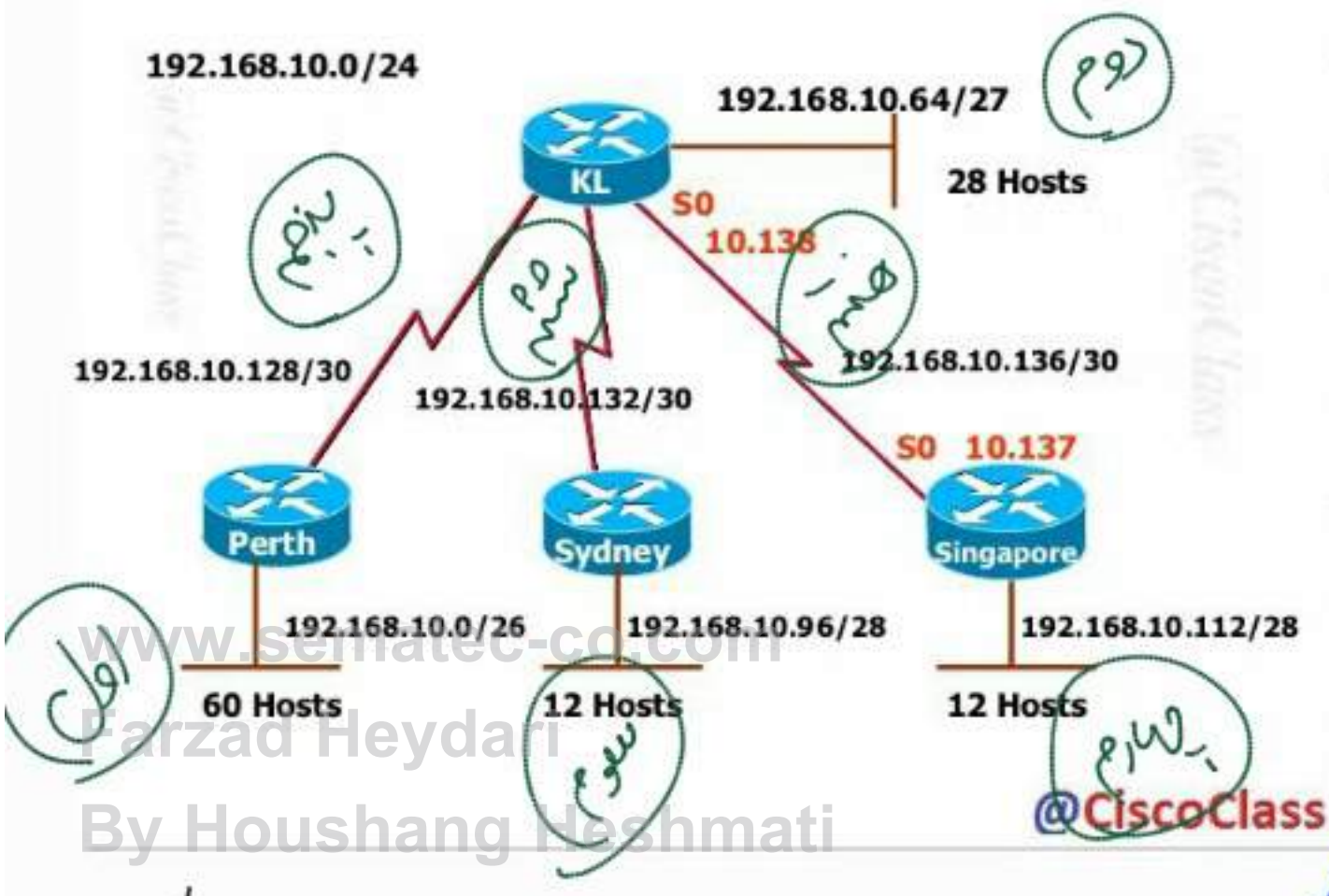
سوال : بازه IP 192.168.10.0/24 را داریم . چگونه بین شبکه های زیر ساخت کنیم ؟ (روترها باید بازه p2p داشته باشند) :

Calculating subnets with VLSM



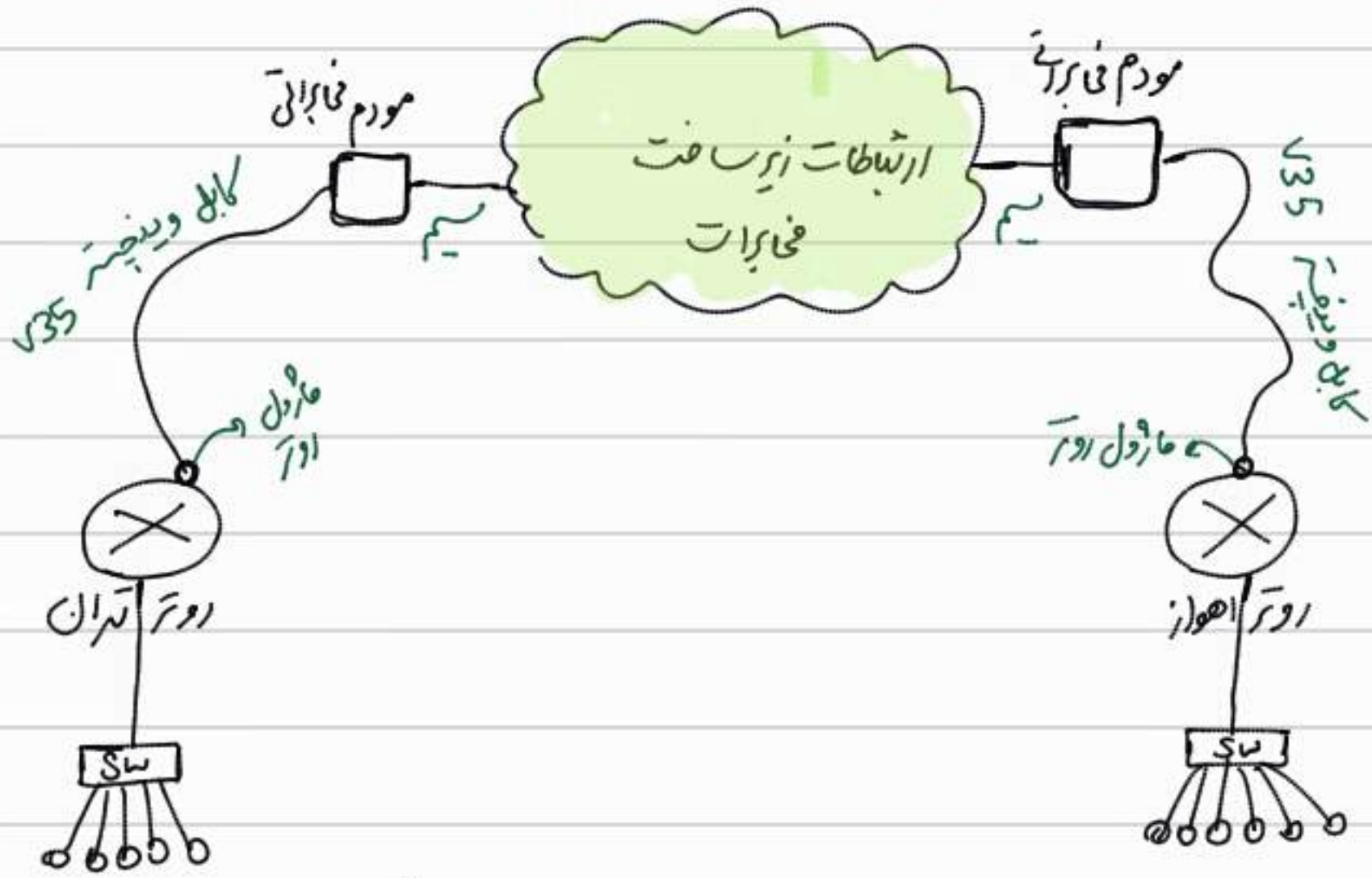
Configuring VLSM

جواب :

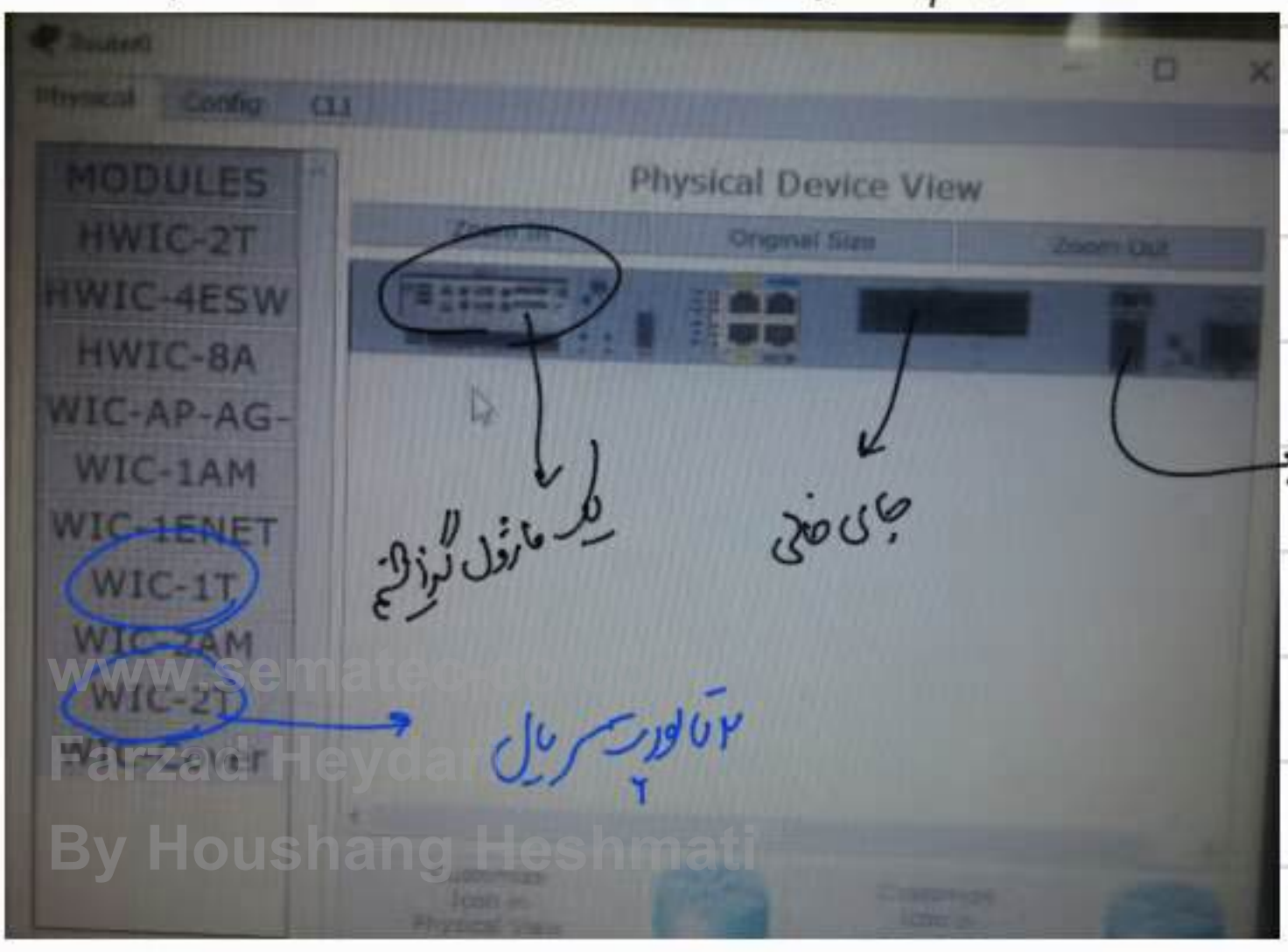


www.senatec-co.com
Farzad Heydari
By Houshang Heshmati

Static Route

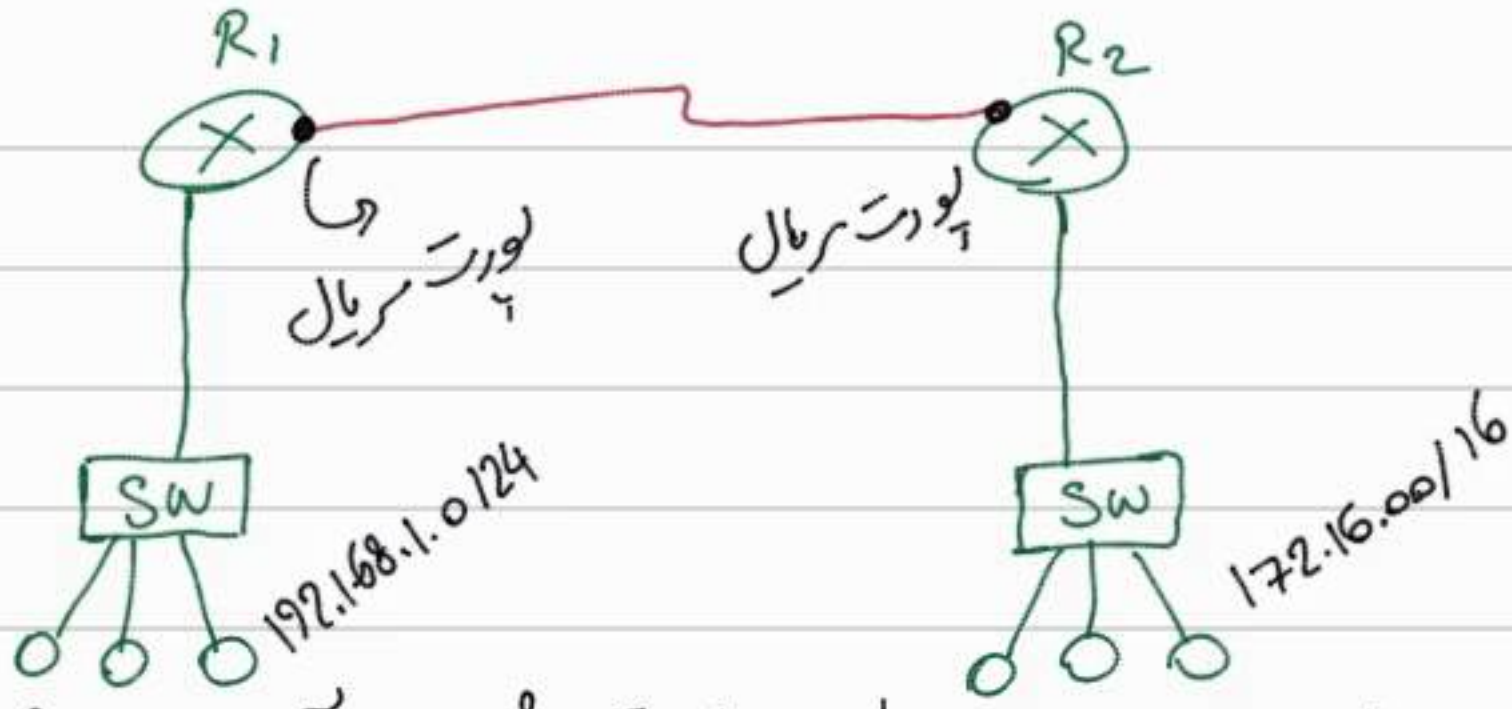


در نرم افزار cisco pactet tracer ، ابتدا روتر را خاموش می‌کنید بعد ماژول اضافه می‌کنید wic2T یا wic1T (پورت سریال اضافه می‌کنند برای اتصال ۲ روتر از پورت سریال استفاده می‌شود.



برای اتصال دو روتر از کابل قرمز که سمت دارد استفاده کنید

www.semateg.com
Farzad Heydari
By Houshang Heshmati



پورت سریال را باید در show run ببینید تا شماره پورت آن را متوجه شوید.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 --More--
```

پورت سریالی که روی روتر هست شماره 0/1/0 هست.

هر بار که یک ماژول پورت سریال اضافه می‌کنید با show run شماره آن را نگاه کنید مانند fast به ترتیب اضافه نمی‌شود.

داخل پورت سریال شوید و به دو روتر IP بدهید (در یادآوری IP یاد گرفتید برای اتصال ۲ روتر از 130 استفاده می‌شود)

سپس به پورت fast که به سمت switch هست وارد شده و IP بدهید دقت کنید IP که می‌دهید برای default Gateway آن بکه استفاده می‌شود

www.sematec.com
Farzad Hoydari
By Houshang Heshmati

```
Router(config)#interface  serial 0/1/0
Router(config-if)#ip ad
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#int
Router(config)#interface fas
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shu
```

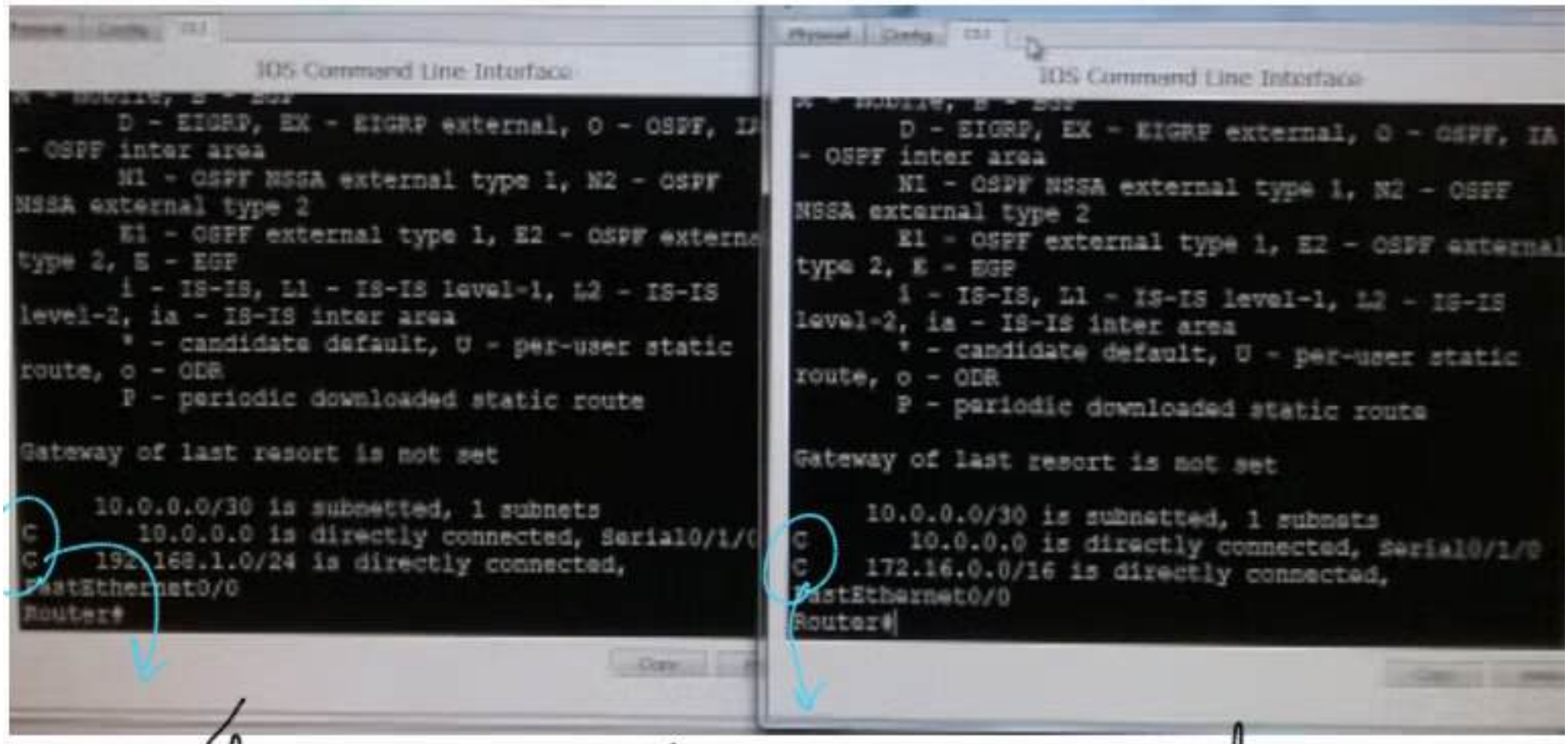
پورت سریال

/30

ورود به پورت متصل به switch

معمولاً یکی می‌دهیم

روی هر روتر show ip route بزنید و ببینید چه مسیرهایی را بلد است؟



C یعنی connected یعنی این دسته روتر متصل است. هر دو روتر به شبکه‌های خودشان متصل هستند و از طریق پورت سریال همدیگر را می‌بینند.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

اتفاقی که می‌افتد این است که کامپیوتر شبکه راستی نمی‌تواند شبکه چپ را ببیند.
چرا؟

روتر شبکه خودش را می‌بیند و دست متصل به روتر بغلی را هم می‌بیند
ولی هنوز نمی‌تواند شبکه روتر بغلی را ببیند.

باید به روتر سمت چپ بگوییم که 172.16.0.0/16 در روتر بغلی است.
و به روتر سمت راست بگوییم که 192.168.1.0/24 در روتر بغلی است.
یعنی یک Static route تعریف کنیم:

router (config)# ip route ....
NetID subnet mask outgoing interface

روتر چپ → router(config)= ip route 172.16.0.0 255.255.0.0 Serial 0/1/0
روتر راست → router(config)= ip router 192.168.1.0 255.255.255.0 Serial 0/1/0

Static route برای شبکه کوچک است که ۴ یا ۵ شبکه بخواهند به هم وصل شوند. چون اگر زیاد شود نمی‌شود روی هر روتر ۱۰۰ خط Static route بنویسید.

بعد از اینکه روی هر router، Static route تعریف کردیم حالا شبکه‌ها می‌توانند با هم ارتباط برقرار کنند.
Show ip route بگیرید:

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

```
Router(config)#ip route 172.16.0.0 255.255.255.0 se
Router(config)#ip route 172.16.0.0 255.255.255.0 serial 0/1/0
Router(config)#do sho ip rou
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
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.0.0 is directly connected, Serial0/1/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Router(config)#
```

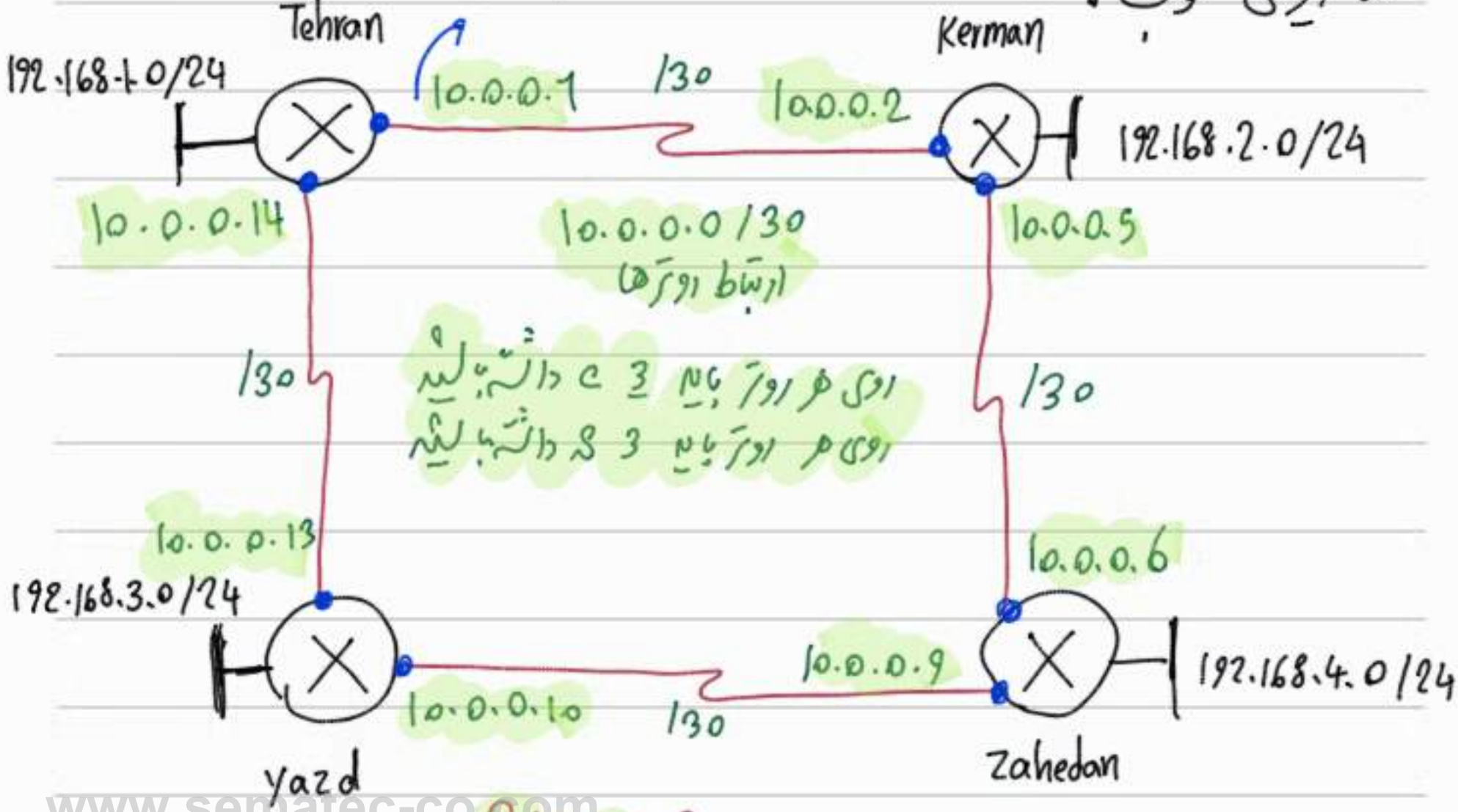
Static route

Static

جدول routing

پرتکلورت سریال دارد باید WIC2T بگذاریم.

سناریوی خوب:



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

10.0.0.0/30 ⟶
- 10.0.0.0
- 10.0.0.4
- 10.0.0.8
- 10.0.0.12

Net 10

```
Router(config)#interface serial 0/1/0
Router(config-if)#ip ad
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to
Router(config-if)#
Router(config-if)#exit
Router(config)#int
Router(config)#interface ser
Router(config)#interface serial 0/1/1
Router(config-if)#ip address 10.0.0.4 255.255.255.252 255.
                                                        ^
% Invalid input detected at '^' marker.

Router(config-if)#ip address 10.0.0.4 255.255.255.252
Bad mask /30 for address 10.0.0.4
Router(config-if)#ip address 10.0.0.14 255.255.255.252
Router(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to do
Router(config-if)#
Router(config-if)#exit
Router(config)#inte
Router(config)#interface fas
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip ad
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

دلت به سمت کرمان

130

Tehran

دلت به سمت یزد

دلت در شبکه خودش

default gateway برای شبکه خودش

```
Router(config)#do sho ip r
% Ambiguous command: "sho ip r"
Router(config)#do sho ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter are
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       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
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
C       10.0.0.12 is directly connected, Serial0/1/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 is directly connected, Serial0/1/0
S    192.168.3.0/24 is directly connected, Serial0/1/1
S    192.168.4.0/24 is directly connected, Serial0/1/0
Router(config)#
```

اول Tehran

متصل

یادگرفته

www.TehranTech.com
Farzad Haydari
By Houshang Heshmati

هنگامی که یک شبکه خارجی را ping می‌کنید و بسته ping از روتر می‌گذرد یک واحد از TTL به ازای عبور از هر روتر کم می‌شود. اگر در یک مسیر از 128 روتر بگذرد بسته Drop می‌شود. اصولا اگر از 128 روتر بگذرد یعنی بسته بین روترها گیر کرده به نمونه ارسال ping به google دقت کنید.

```
C:\Users>cd..

C:\>tracert www.google.com

Tracing route to www.l.google.com [74.125.53.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  modem.Home [192.168.0.1]
  2    24 ms    24 ms    24 ms  ptld-dsl-gw43-235.ptld.qwest.net [
]
  3   100 ms    24 ms    24 ms  ptld-agw1.inet.qwest.net [
]
  4    26 ms    25 ms    24 ms  por-core-01.inet.qwest.net [205.171.130.25]
  5    48 ms    28 ms    28 ms  sea-edge-12.inet.qwest.net [67.14.41.22]
  6    28 ms    28 ms    28 ms  65.122.121.66
  7    28 ms    28 ms    28 ms  66.249.94.212
  8    28 ms    28 ms    28 ms  66.249.94.195
  9    46 ms    35 ms    39 ms  216.239.46.204
 10    35 ms    36 ms    34 ms  216.239.48.139
 11    35 ms    35 ms    35 ms  72.14.232.70
 12    35 ms    35 ms    35 ms  www.google.com [74.125.53.147]

Trace complete.

C:\>_
```

روترها

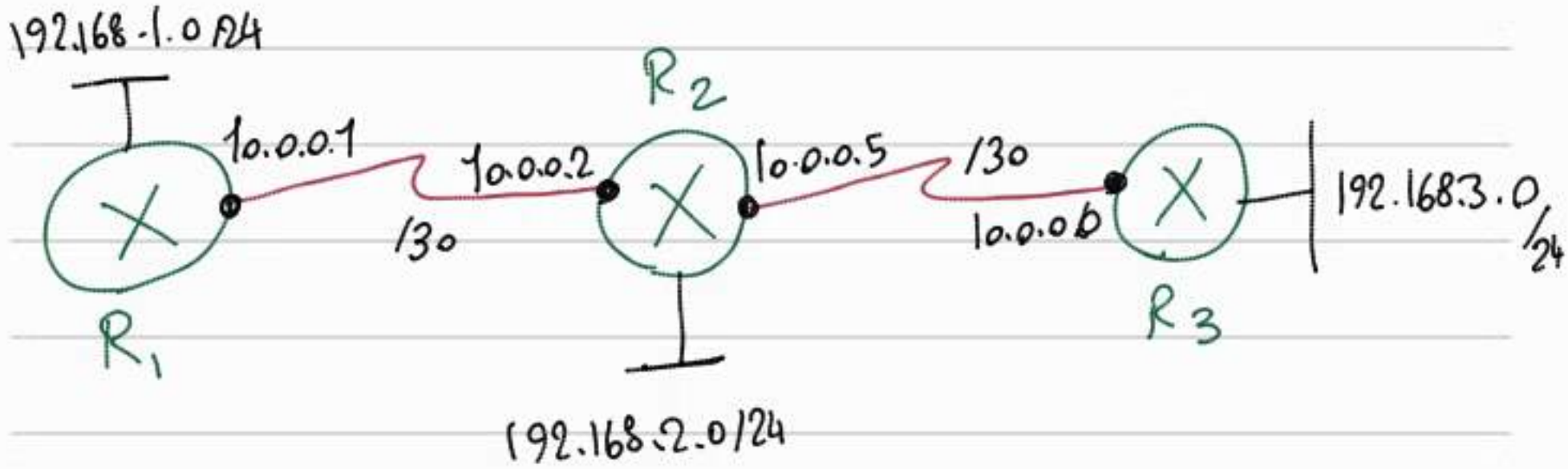
Command Prompt

```
C:\>ping www.google.com

Pinging www.l.google.com [74.125.224.17] with 32 bytes of data:
Reply from 74.125.224.17: bytes=32 time=14ms TTL=52
Reply from 74.125.224.17: bytes=32 time=23ms TTL=52
Reply from 74.125.224.17: bytes=32 time=13ms TTL=52
Reply from 74.125.224.17: bytes=32 time=18ms TTL=52

Ping statistics for 74.125.224.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 23ms, Average = 17ms

C:\>
```

Time To Live

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

روش دوم برای Static routing : Next hop ip address



R1 (Config) # ip route 192.168.2.0 255.255.255.0 10.0.0.2

این شبکه — روی این روتر الت

R2 (Config) # ip route 192.168.1.0 255.255.255.0 10.0.0.1

R2 (Config) # ip route 192.168.3.0 255.255.255.0 10.0.0.6

R3 (Config) # ip route 192.168.2.0 255.255.255.0 10.0.0.5

router (Config) # ip route Net ID Mask Next hop ip

این روش سخت تر است ولی حرفه ای تر است.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

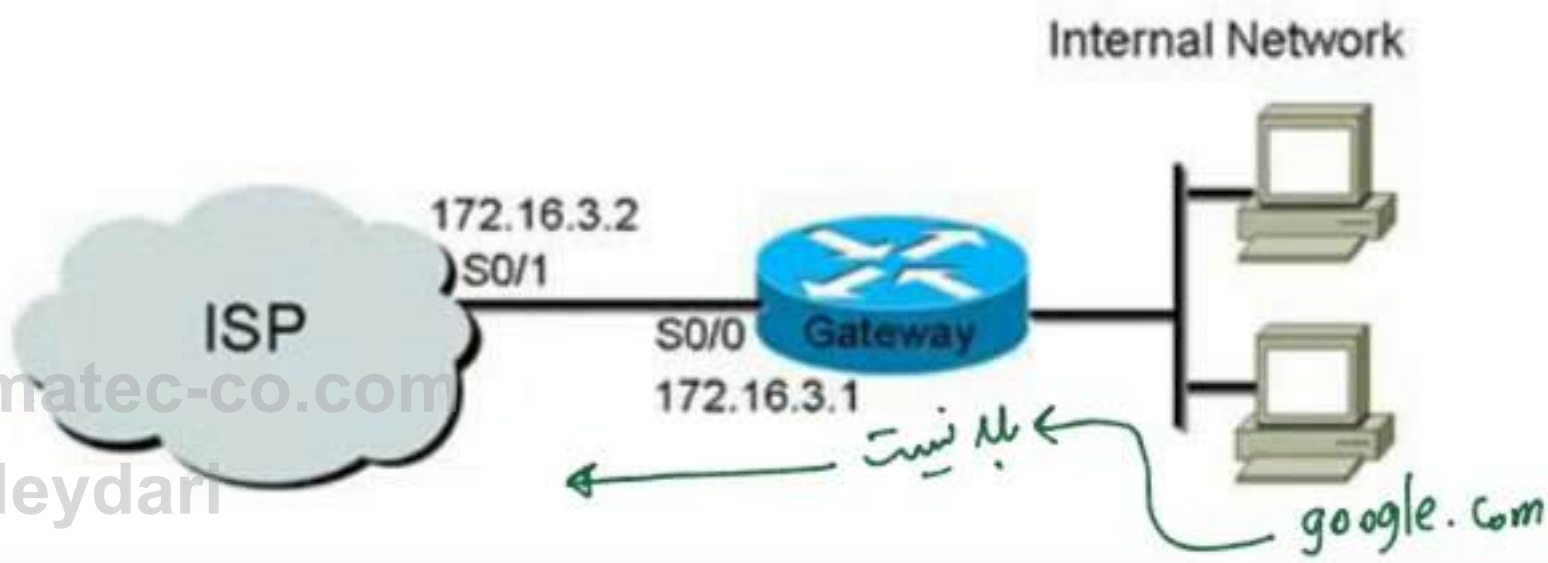
Default Route

هنگام برای روتر بسته‌ای ارسال شود و روتر مقصد را بلد نباشد بسته Drop می‌شود. فرض کنید در شبکه‌ای یک کامپیوتر می‌خواهد Google.com را باز کند وقتی بسته به روتر شبکه می‌رسد خودش نمی‌داند google.com کجاست آن را دراپ می‌کند (Destination host unreachable) برای حل این مشکل:

یک راه این است که آدرس همه وب‌سایت‌ها و مسیر را در Static route به روتر بدهیم (مثلاً چند میلیون خط Static route روی روتر بنویسیم)

راه دوم استفاده از Default route است. یعنی هرچی بلد نبود بفرسته روتر بعدی.

Default Route Example



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

بهتر است بصورت Next hop ip بنویسیم :

Router (Config) # ip router 0.0.0.0 0.0.0.0 ..... Next hop ip

هر ip

با هر subnet mask

البته اگر static route هم نوشته باشیم اول اولویت با آن است یعنی مسیرهای خودش را ارسال می‌کند و اگر مسیری را بلد نبود می‌فرستد به روتر بعدی.

روتر شبکه خودمان

```
Router(config)#interface fast 0/1
Router(config-if)#no shu

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
```

دستی که به روتر ISP وصل است.

/30 امتیاز

default route

روتر ISP که آدرس ها را بلد است

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.2 255.255.255.252
Router(config-if)#no shu

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
Router(config-if)#
```

دستی به روتر شبکه وصل است

امتیاز /30

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Routing Protocol

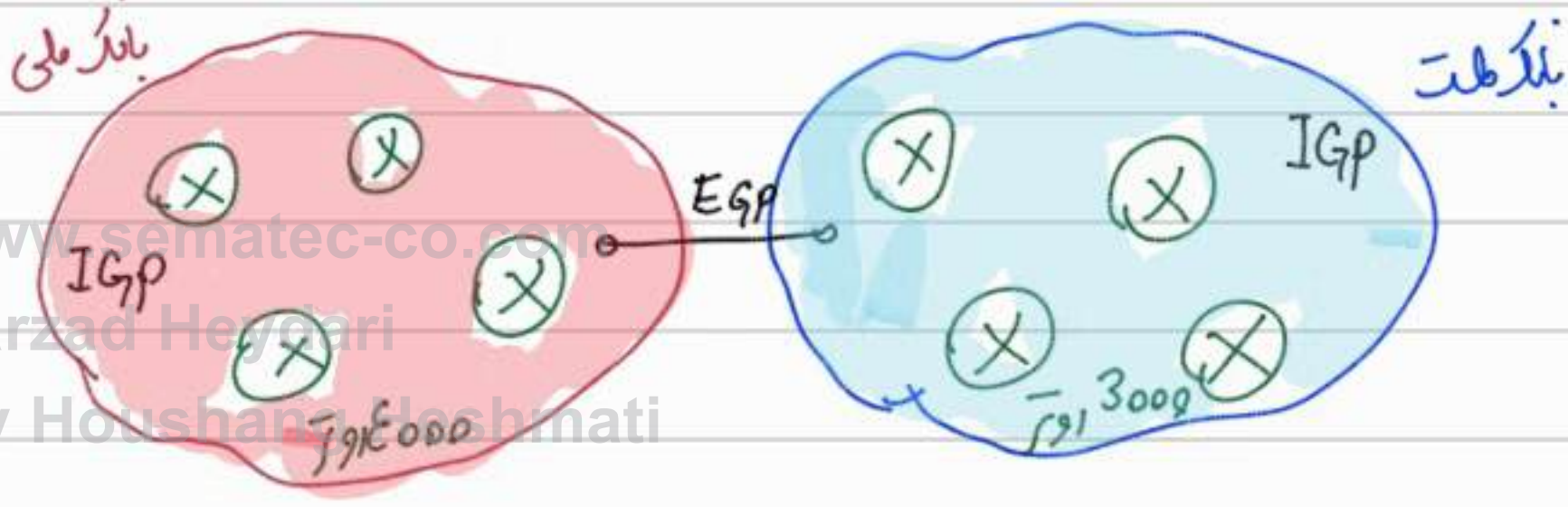
Routing protocol یعنی پروتکل هایی که روترها توسط آنها می توانند با هم ارتباط برقرار کنند و به اصطلاح همسایه بشوند.

برای یک شبکه بزرگ در که تمام شهرهای ایران شعبه دارد و مثلاً 2000 تا روتر دارد نمی شود روی هر روتر 2000 تا Static route نوشت. بعد اگر هم نوشتید مثلاً اگر یک شعبه جدید در یک شهر افتتاح شود باید روی هر 2000 روتر دوباره یک Static route بنویسیم.

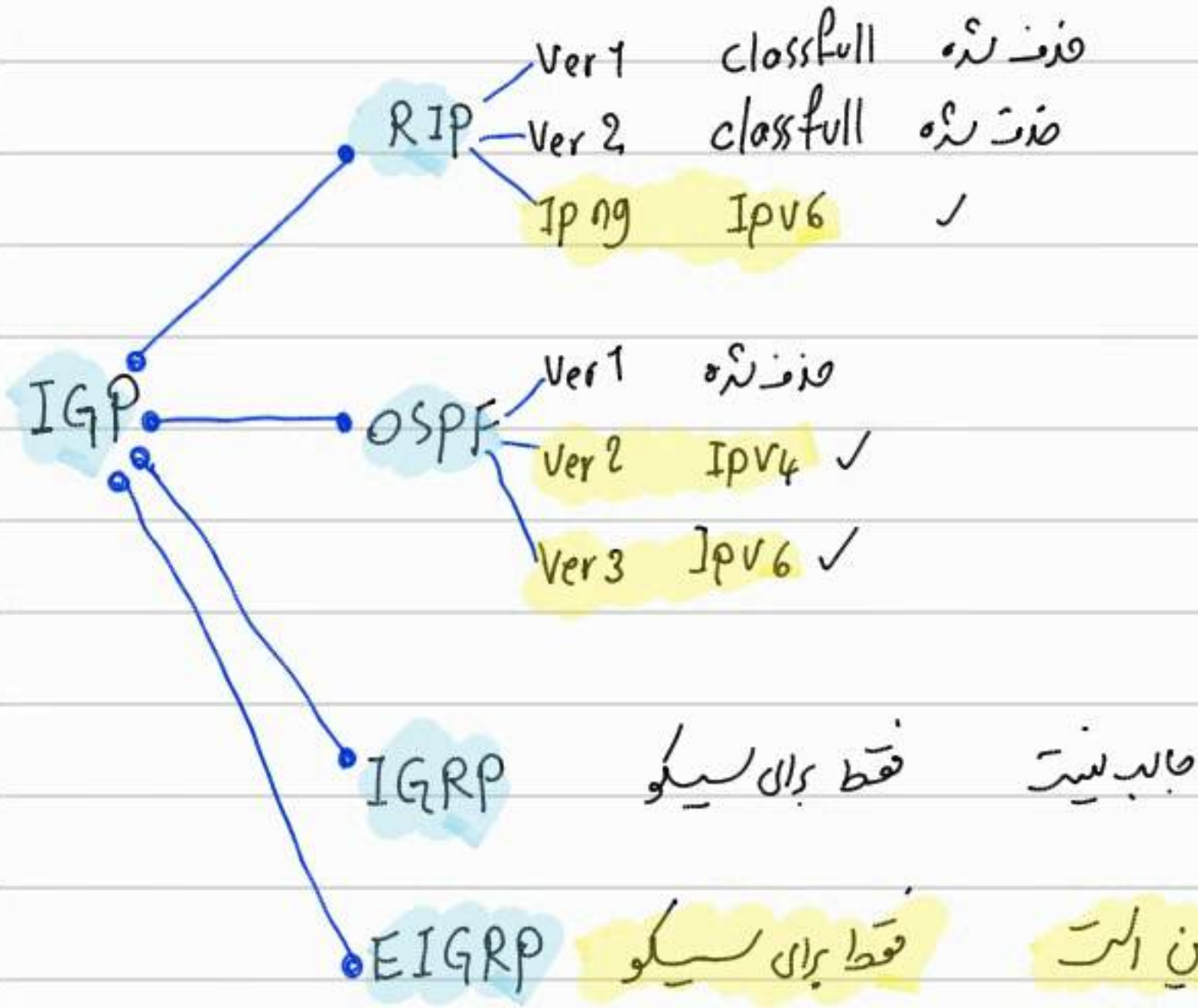
Routing protocol یعنی روترها خودشان با هم ارتباط برقرار کنند و شبکه های خودشان را به هم یاد بدهند (اتوماتیک).

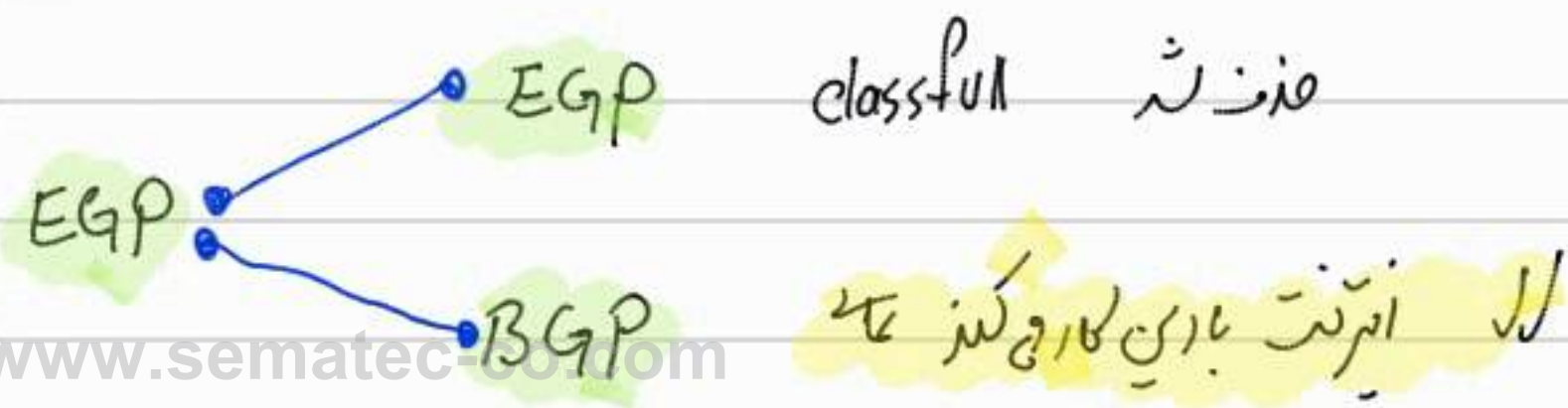
Routing protocols → IGP — شبکه خودمختار (یک شبکه داخلی)

Routing protocols → EGP — بین شبکه ای



www.sematec-co.com
Farzad Heydari
By Houshang Hashmati





www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

EIGRP

EIGRP

Enhanced interior gateway routing protocal

بهترین و سریعترین IGP دنیاست ولی فقط مخصوص CISCO است و روی برندهای دیگر کار نمی کند.

مفهوم wildcard mask :

بعدا مفصل توضیح داده میشود ولی اکنون به این ترتیب حساب کنید.

subnet mask را از 255.255.255.255 کم کنید :

255.255.255.0 /24

255.255.255.255

0.0.0.255 ← wildcard mask

255.255.255.252 /30

− 255.255.255.255

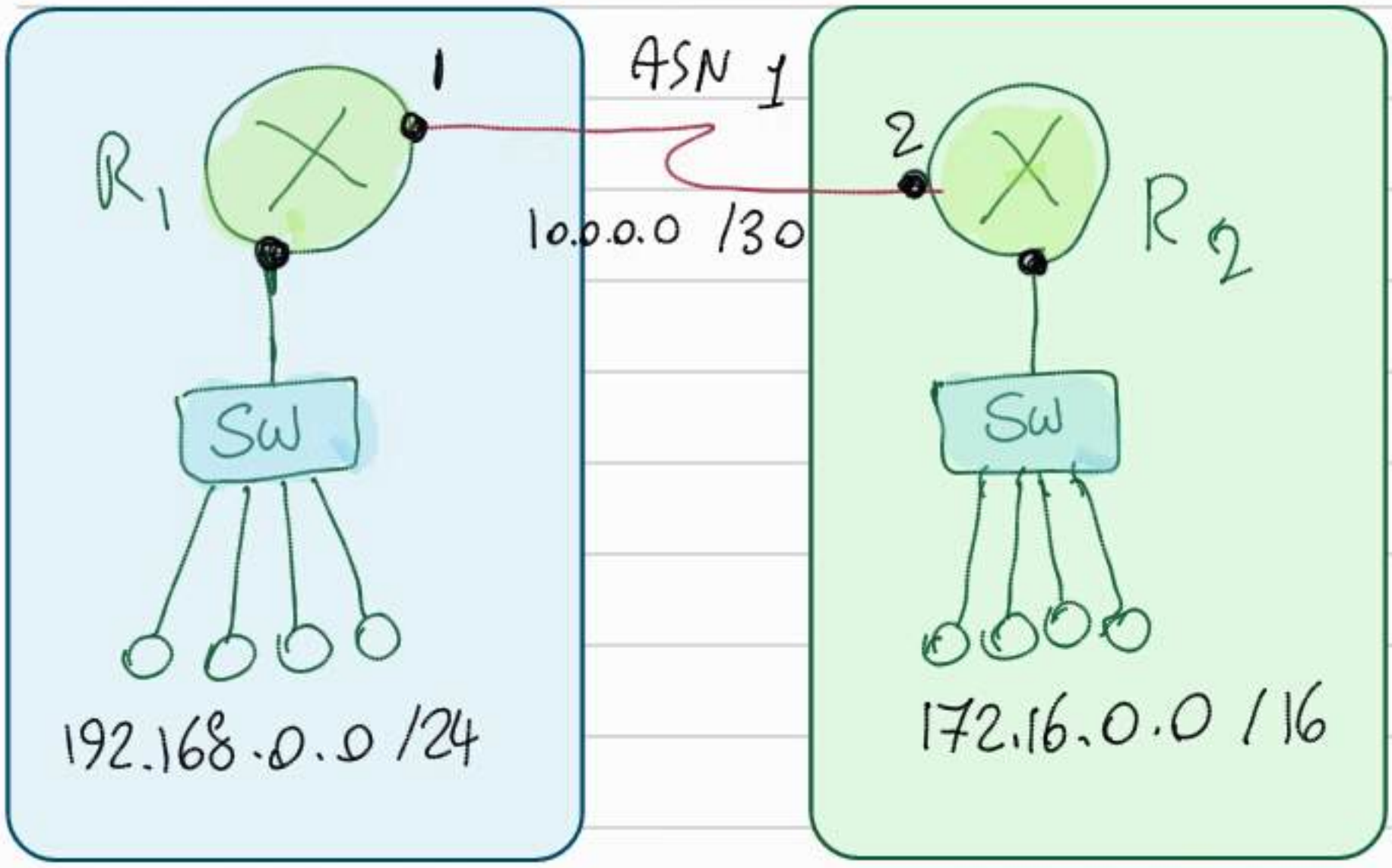
0.0.0.3 ← wildcard mask

ASN :

برای هر IGP می توانید یک عدد بین ۱ تا ۶۵ هزار و خورده ای انتخاب کنید.

روترهایی که در دروی یک ASN یکسان باشند می توانند با هم همسایه شوند.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati



1) Router (Config) # router eigrp ..... ASN عدد

تعریف می‌کنیم کدام پروتکل باشد ← و عدد آن را می‌زنیم

2) Router (Config-router) # network ..... Net ID wildcard mask

← وارد eigrp می‌شود ، شبکه‌هایی که روتر خودش به آنها وصل است را وارد می‌کنیم . در شکل بالا روتر R_1 :

الف) به شبکه 192.168.0.0 وصل است .

ب) و شبکه 10.0.0.0 وصل است .

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

روتر R_1

ورود به eigrp

```
Router(config)#router eigrp 1
Router(config-router)#net
Router(config-router)#network 10.0.0.0 0.0.0.3
Router(config-router)#ne
Router(config-router)#ne
Router(config-router)#network 192.168.1.0 0.0.0.255
Router(config-router)#
```

در هر روتر برای سناریو قبل ۲ شبکه داریم:

- یکی شبکه ای 30 هست و هر دو روتر به هم وصل هستند
- یکی شبکه ای که خود روترها به آن وصل هستند

روتر R_2

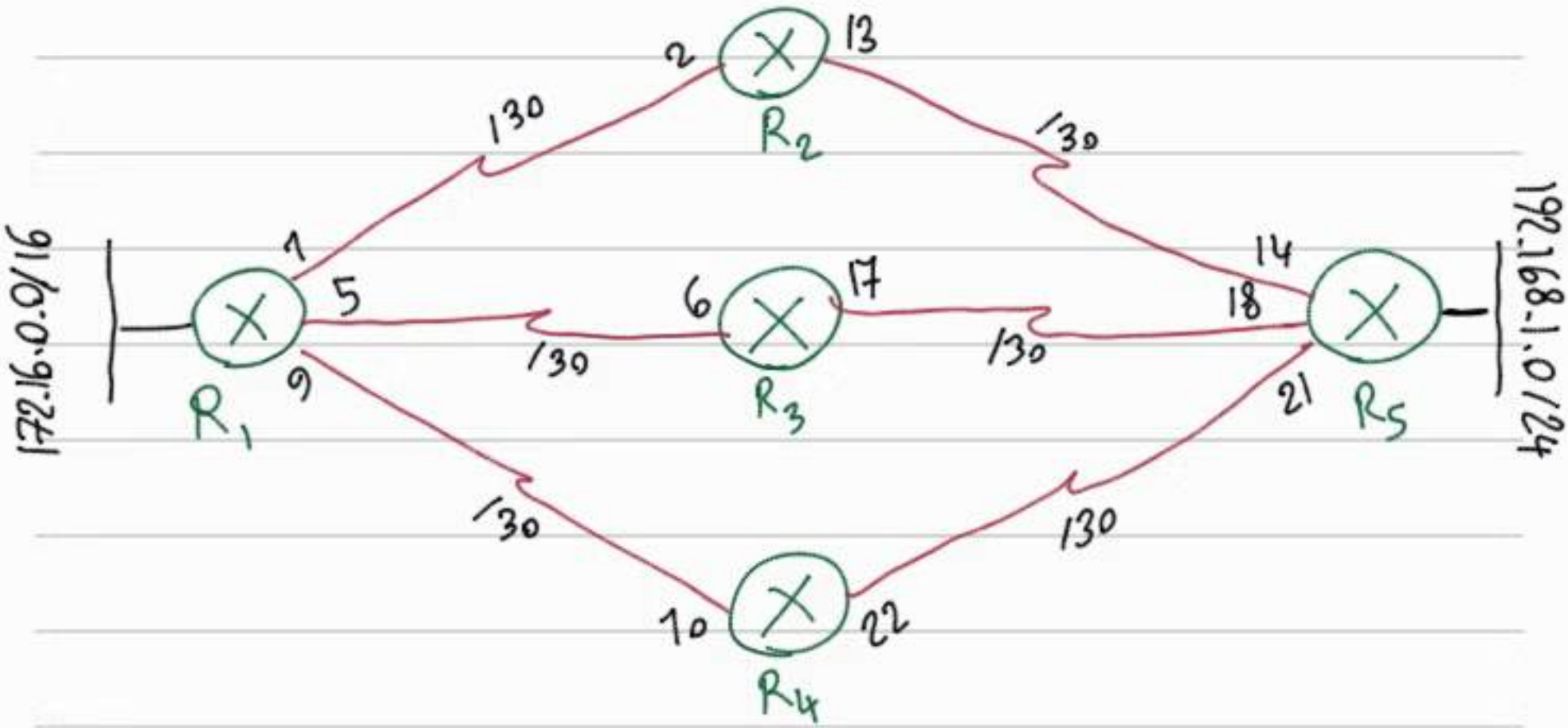
ورود به Eigrp

```
Router(config)#router eig
Router(config)#router eigrp 1
Router(config-router)#net
Router(config-router)#network 10.0.0.0 0.0.0.3
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.0.0.1 (Serial0/1/0) is up: new

Router(config-router)#net
Router(config-router)#network 172.16.0.0 0.0.255.255
Router(config-router)#exit
Router(config)#do sho ip rou
```

```
Router(config)#do sho ip rou
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
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:03:45, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/20514560] via 10.0.0.1, 00:04:03, Serial0/1/0
Router(config)#
```

www.sematec.co.com
Farzad Heydari
By Houshang Heshmati

از روتر R_2 show ip route می‌گیریم. شبکه های خودش و آنهایی که از Eigrp یاد گرفته D می‌زند.



خیلی مهم :

هنگامی که network وارد می‌کنید باید Net.ID همان شبکه را بنویسید

برای ارتباطات دوتایی بین روترها ، هر که 10.0.0.0 می‌شوند این Net.ID فقط برای 10.0.0.1 و 10.0.0.2 هست . مثلاً برای 10.0.0.5 و 10.0.0.6 Net.ID می‌شود 10.0.0.4.

→ 130 Net.ID { 10.0.0.0
10.0.0.4
10.0.0.8
10.0.0.12
⋮

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#inte
Router(config)#interface FAS
Router(config)#interface FASTEthernet 0/0
Router(config-if)#IP ADD
Router(config-if)#IP ADDress 172.16.0.1 255.255.0.0
Router(config-if)#no shu

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, char

Router(config-if)#exit
Router(config)#inte
Router(config)#interface seri
Router(config)#interface serial 0/1/0
Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#exit
Router(config)#inte
Router(config)#interface ser
Router(config)#interface serial 0/1/1
Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.5 255.255.255.252
Router(config-if)#no shu

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#inter
Router(config)#interface ser
Router(config)#interface serial 0/0/0/
                                     ^
% Invalid input detected at '^' marker.

Router(config)#interface serial 0/0/0
Router(config-if)#ip add
Router(config-if)#ip address 10.0.0.9 255.255.255.252
Router(config-if)#no shu
```

اتصال به شبکه خودش

default gateway IP

اتصال به R_2

اتصال به R_3

اتصال به R_4

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

روتر R_1

R1

ورود به Eigrp

4 شبکه - آن وصل است

```
Router(config)#
Router(config)#route
Router(config)#router ei
Router(config)#router eigrp 1
Router(config-router)#net
Router(config-router)#network 10.0.0.0 0.0.0.3
Router(config-router)#netw
Router(config-router)#network 172.16.0.0  0.0.255.255
Router(config-router)#net
Router(config-router)#network 10.0.0.4 0.0.0.3
Router(config-router)#net
Router(config-router)#network 10.0.0.8 0.0.0.3
```

به R2
شبکه خودش
به R3
به R4

روی همه روتر به همین صورت همه شبکه‌های خودشان را در Eigrp خودشان اضافه می‌کنیم شبکه‌ای که به روتر وصل نیست در آن الکی اضافه نکنید

مثلاً روتر R4 به شبکه 10.0.0.0 وصل نیست
روتر R4 به شبکه 172.16.0.0 وصل نیست
← این‌ها را از ERGP باید یاد بگیرد.

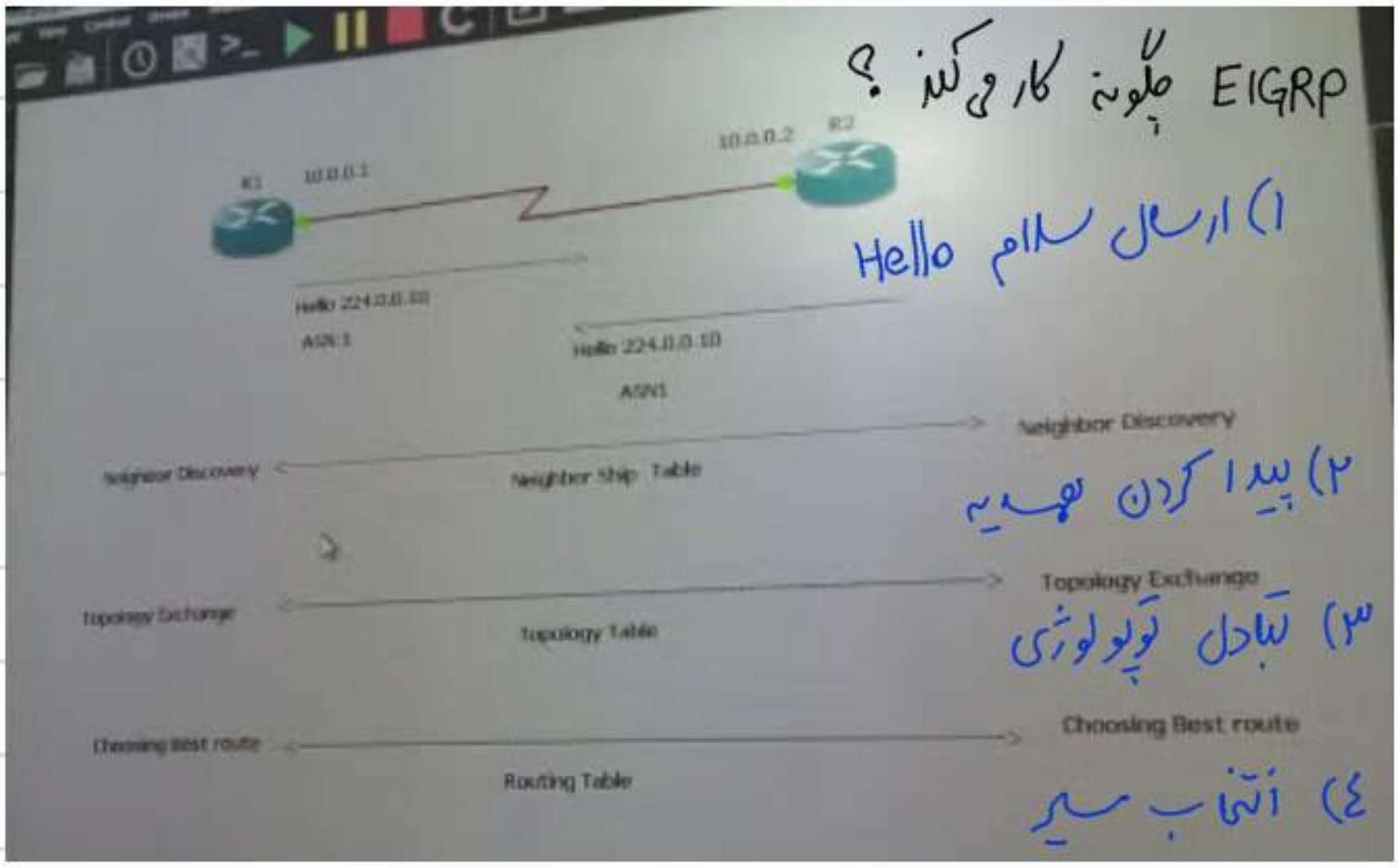
R1

```
Router(config-router)#do sho ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BG
       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 int
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:09:59, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
C       10.0.0.4/30 is directly connected, Serial0/1/1
C       10.0.0.8/30 is directly connected, Serial0/0/0
D       10.0.0.12/30 [90/2681856] via 10.0.0.2, 00:02:54, Serial0/1/0
D       10.0.0.16/30 [90/2681856] via 10.0.0.6, 00:02:33, Serial0/1/1
D       10.0.0.20/30 [90/2681856] via 10.0.0.10, 00:02:03, Serial0/0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
D    192.168.1.0/24 [90/2684416] via 10.0.0.2, 00:01:49, Serial0/1/0
                    [90/2684416] via 10.0.0.6, 00:01:43, Serial0/1/1
                    [90/2684416] via 10.0.0.10, 00:01:35, Serial0/0/0
Router(config-router)#
```

همه شبکه‌ها را یاد گرفته است.

C وصل به خودش
D از Eigrp

www.seryanet.com
Farzad Hayati
By Houshang Hey



IP خالی کست 224.0.0.10 برای EIGRP روتر شده است و روتر با این IP بسته‌های Hello برای روتر های دیگر ارسال می‌کند.

برای مشاهده مشخصات و بررسی Eigrp از دستورات زیر استفاده کنید:

Router # show ip protocols — از کدام پروتکل استفاده شده؟ Eigrp؟

Router # show ip eigrp neighboor — به چه روترهایی وصل هست

Router # show ip eigrp Topology — چه چیزی از کدام روتر یاد گرفته

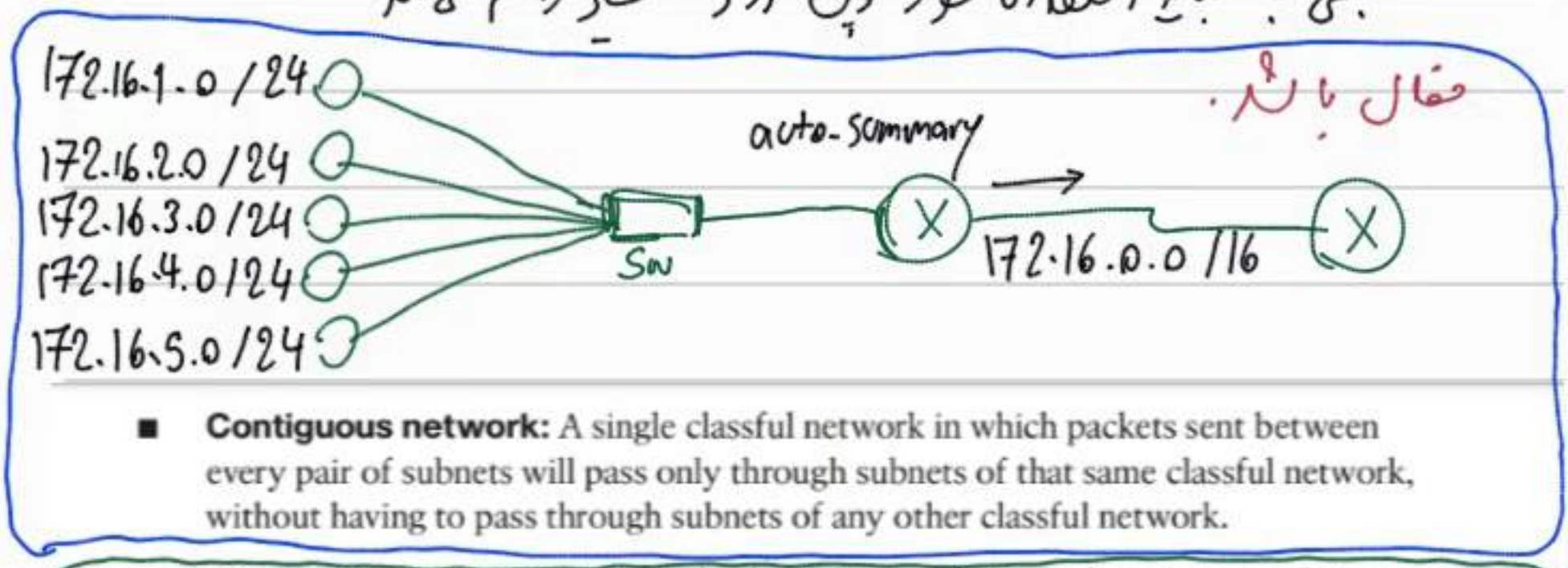
Router # show ip route eigrp — دیدن route های eigrp

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

در CCNP کامل یاد می‌گیرید

Auto-Summary

auto-summary روی Eigrp از ابتدا فعال است و IP های class-less را classfull می‌کند. بعضی جاها خوب است و جدول route بجای چند خط می‌شود یک خط
بعضی جاها نباید استفاده شود چون روتر مسیر را گم می‌کند.

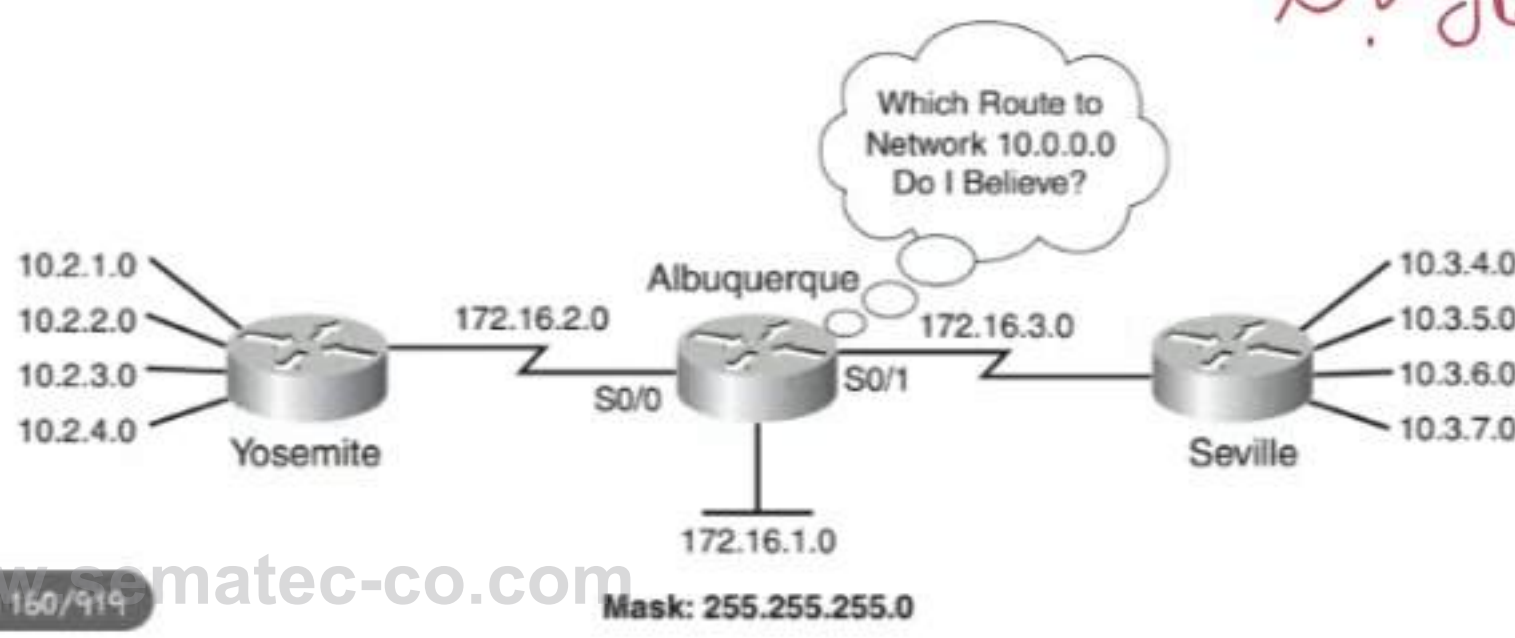


- **Contiguous network:** A single classful network in which packets sent between every pair of subnets will pass only through subnets of that same classful network, without having to pass through subnets of any other classful network.

- **Discontiguous network:** A single classful network in which packets sent between at least one pair of subnets must pass through subnets of a different classful network.

Figure 4-8 shows a classic example of a discontiguous network 10.0.0.0. Subnets of class A network 10.0.0.0 exist on the left and the right, with subnets of class B network 172.16.0.0 in the middle of the internetwork. Following the figure, the problem created by the auto-summary feature is described.

نباید فعال باشد



www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Figure 4-8 *Discontiguous Network 10.0.0.0*

اگر کل subnet ها در یک سمت روتر باشند autosummary باعث
می‌شود جدول route خلاصه و کوچک شود.
ولی اگر subnet ها در هر دو طرف router باشند وقتی auto-summary
جدول route را خلاصه کرد روتر نمی‌داند باید به کدام سمت ارسال کند.
در این حالت باید autosummary را غیر فعال کرد:

```
Router (Config) # router eigrp .....عدد
Router (Config-router) # No auto-Summary
```

معیار روتر برای انتخاب مسیر

با کمک فرمول و مقادیر روبرو:

1) Bandwidth پهنای باند (100 mb/s, 1 Gb, ...)
2) Delay تاخیر: مدت زمانی که بسته از interface خارج می‌شود

$$\rightarrow \left[\left(10^7/\min \text{Bandwidth}\right) + \text{Sum Delay}\right] * 256 = \text{عدد متریک}$$

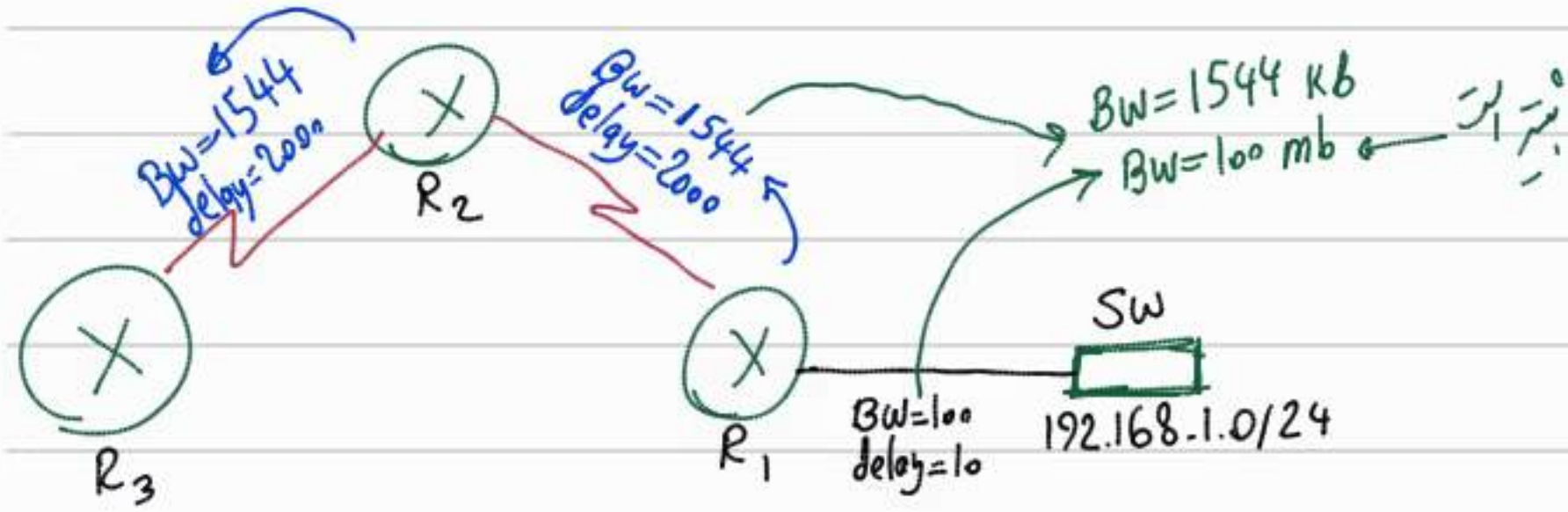
کمترین پهنای باند — جمع همه تاخیرها

هر مسیر که عدد متریک کمتری داشته باشد مسیر بهتری خواهد بود.

```
Router(config)#do sho ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mob
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF i
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA extern
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia
       * - candidate default, U - per-user static route, o -
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
D       10.0.0.4 [90/21024000] via 10.0.0.2, 00:19:39, Serial
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
D       172.16.2.0 [90/21026560] via 10.0.0.2, 00:17:34, Seria
D    192.168.3.0/24 [90/20514560] via 10.0.0.2, 00:19:39, Seri
Router(config)#
```

متریک

www.sematbi-cp.com
Farzad Heydari
By Hossein Ghoreishinia



محاسبه متریک برای R3 اگر بخواهد به لوئیج SW برسد:

$$R_3 \longrightarrow \left[\frac{10^{7}}{1544} + (2000+2000+10)\right] \times 256 = 26844101$$

۶۴۷۶ به سمت پایین گرد می‌شود

نکته: با دستور show interface ...../... Bandwidth و delay را ببینید
Type Num

delay باید قبل محاسبه تقسیم بر ۱۰ شود چون micro/sec هستند.

```
Router1#show int s0/0/0
Serial0/0/0 is administratively down, line protocol is down (disabled)
  Hardware is HD64570
  Internet address is 10.20.30.40/28
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

www.schatec.com
Farzad Heydari
By Houshang Heshmati

Passive Interface

روترها در Eigrp هر ۵ ثانیه یکبار Hello می‌فرستند و ۱۵ ثانیه برای جواب منتظر می‌مانند. اگر جواب دریافت نکنند همسایگی قطع می‌شود (Keep alive)

۵ ثانیه ارسال Hello را Hello interval می‌گویند.

۱۵ ثانیه انتظار پاسخ را hold time می‌گویند.

می‌توانید این مقادیر را تغییر بدهید ولی اگر مقادیر Hello و hold روترها با هم متفاوت باشند Eigrp بهم می‌خورد و همسایگی قطع می‌شود

router (config-if) # ip Hello-interval eigrp ..... ثانیه

router (config-if) # ip hold-time eigrp ..... ثانیه

روی آن لینک روتر که می‌خواهم Hello فرستد

روتر به طور پیش‌فرض بروی همه پورت‌های خود Hello می‌فرستد. بهتر است Hello برای پورت‌هایی که به END Device مانند pc وصل است ارسال نشود چون یک نفوذگر می‌تواند با یک روتر به جای pc وصل شود و با روتر همسایه شده و وارد شبکه شود.

برای این منظور پورت‌هایی که به END Device متصل است را passive می‌کنیم.

پورت passive دیگر Hello دریافت نمی‌کند و به روترهای دیگر اطلاعات می‌دهد.

Router (config-router) # passive-interface ..... / .....

Type — شماره پورت

eigrp داخل

{ passive-interval default — همه پورت‌ها پسیو شوند
{ No passive-interval Serial 0/1/0 — اون یکی پورت که می‌خواهیم پسیو نباشد

برای بهتره

Serial 0/1/0

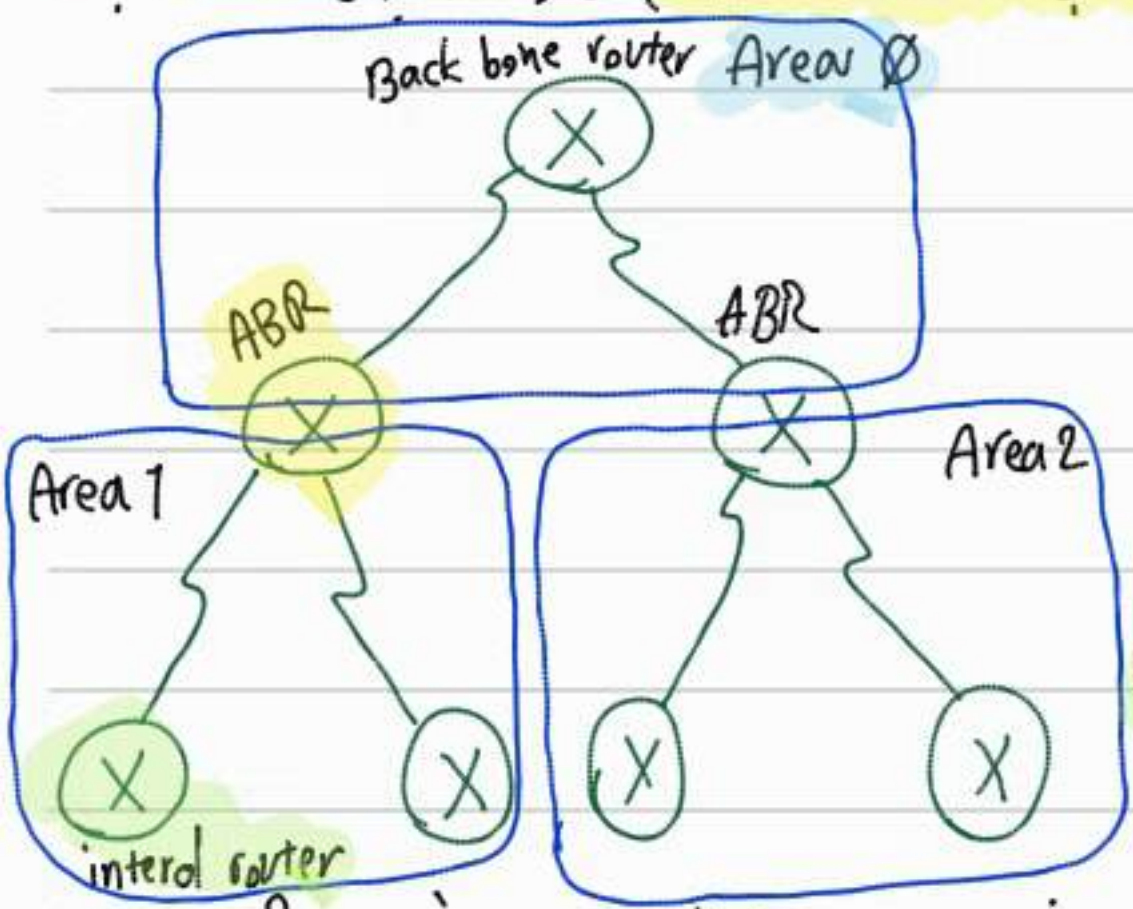
www.dehnatec-co.com
Farzad Heydari
By Houshang Vaseli

OSPF

OSPF
open shortes path first

در ایران خیلی طرفدار دارد چون علاوه بر سیسکو، از برند های دیگر هم (hp و...) پشتیبانی می‌کند.

OSPF باید قبل از ارسال بسته نقشه کل مسیر را بلد باشد و خیلی cpu را اشغال می‌کند (cpu uses) بنابراین در OSPF نقشه کل مسیر را به چند تیکه تقسیم می‌کنیم و هر قسمت را یک area می‌نامیم هر area یک کد عددی دارد هر روتر در OSPF نقشه area مربوط به خودش را بلد است و بسته خود را به روترهای مرز (ABR - روتری که در چند area دست دارد) می‌فرستد برای area بعدی.



* هر area با عددی مشخص می‌شود که بصورت 0.0.0.1 نمایش داده می‌شود برای سیسکو می‌توانید همان 1 را بکار ببرید.

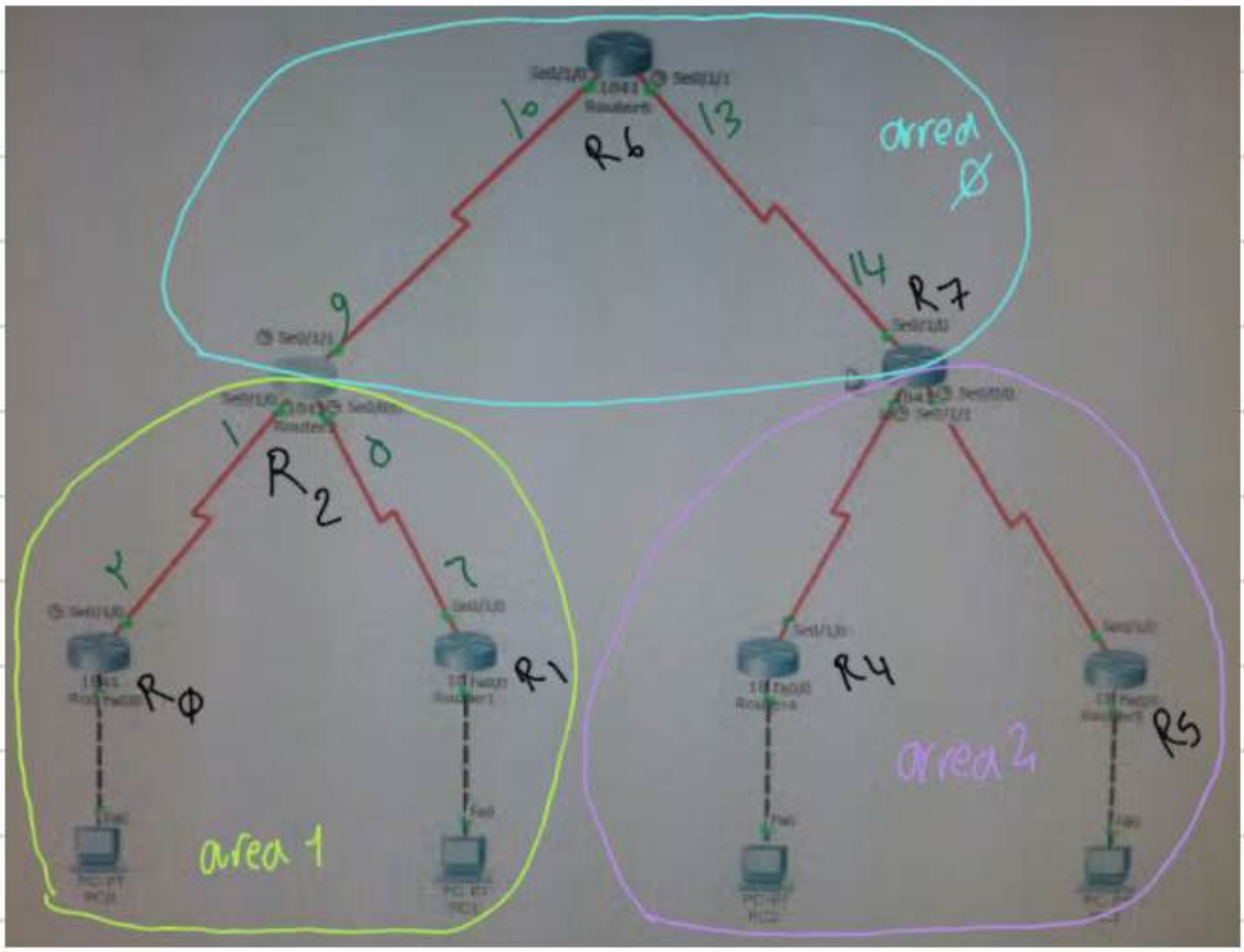
IP مالتی کست 224.0.0.5 برای OSPF رزرو شده و بسته Hello با آن ارسال می‌شود

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

area 0 : Back bone (ستون فقرات) باید حتماً وجود داشته باشد

ABR Router : روترهایی دست های در area های مختلف است.

internal Router : روترهای که همه دست های آن داخل یک area است.



روترهای R_2 و R_7 روترهای مرزی هستند (ABR) چون یک دست در area0 و دست دیگر در area های دیگر دارند.

1) Router (Config) # Router ospf ---------- (proccess ID / شماره ospf)

2) Router (Config-Router) # network ---------- (Net ID) ---------- (wildmask) area ---------- (شماره area)

1) ospf را می‌سازد و داخل ospf می‌شود. شبکه‌های متصل به روتر را با ذکر اینکه در کدام area هستند می‌نویسیم.

www.semotec-co.com
Farzad Heydari
By Houshang Heshmati

area Ø (Backbone) : بعد از IP دادن به interface ها وارد ospf می‌کنیم

```
Router(config)#rout
Router(config)#router os
Router(config)#router ospf 1
Router(config-router)#net
Router(config-router)#network 10.0.0.8 0.0.0.3 are
Router(config-router)#network 10.0.0.8 0.0.0.3 area 0
Router(config-router)#net
Router(config-router)#network
00:15:53: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.9 on Serial0/1/

% Incomplete command.
Router(config-router)#net
Router(config-router)#network 10.0.0.12 0.0.0.3 are
Router(config-router)#network 10.0.0.12 0.0.0.3 area 0
Router(config-router)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, char
00:17:50: %OSPF-5-
```

دلت سمت چپ

دلت سمت راست

روتر وزی R_2 : area Ø : (10.0.0.9)

area 1 : (10.0.0.1) , (10.0.0.9)

```
Router(config-if)#exit
Router(config)#route
Router(config)#router os
Router(config)#router ospf 1
Router(config-router)#netw
Router(config-router)#network 10.0.0.0 0.0.0.3 are
Router(config-router)#network 10.0.0.0 0.0.0.3 area 1
Router(config-router)#net
Router(config-router)#network 10.0.0.
00:12:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Seria
4 0.0.0.3 area
Router(config-router)#network 10.0.0.4 0.0.0.3 area 1
Router(config-router)#network 10.0.0.8 0.0.0.3 area 0
Router(config-router)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

اتصال به R6

اتصال به R1

اتصال به R6

www.setareh-hayeri.com
Setareh Hayeri
By Houshang Heshmati

دستور زیر روترهای داخل همسایگی را نشان می دهد.

Router# Show IP OSPF Neighboor

بعد از اتمام و تنظیم روترها اگر show IP route بگیریم باید همه روترها از همدیگر روت ها را یاد گرفته باشند. مانند شکل زیر

```
[110/257] via 10.0.0.5, 00:00:04, Serial0/1
Router#sho ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inte
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       E1 - OSPF external type 1, E2 - OSPF external type 2, E
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 6 subnets
O       10.0.0.0 [110/128] via 10.0.0.5, 00:12:26, Serial0/1/0
C       10.0.0.4 is directly connected, Serial0/1/0
O IA    10.0.0.8 [110/128] via 10.0.0.5, 00:11:49, Serial0/1/0
O IA    10.0.0.12 [110/192] via 10.0.0.5, 00:10:02, Serial0/1/0
O IA    10.0.0.16 [110/256] via 10.0.0.5, 00:06:12, Serial0/1/0
O IA    10.0.0.20 [110/256] via 10.0.0.5, 00:07:31, Serial0/1/0
O    192.168.1.0/24 [110/129] via 10.0.0.5, 00:12:26, Serial0/1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O IA 192.168.3.0/24 [110/257] via 10.0.0.5, 00:01:31, Serial0/1/0
O IA 192.168.4.0/24 [110/257] via 10.0.0.5, 00:00:22, Serial0/1/0
Router#
```

O IA داخل area دیگری است

C مستقیم وصل است

O داخل همین area است

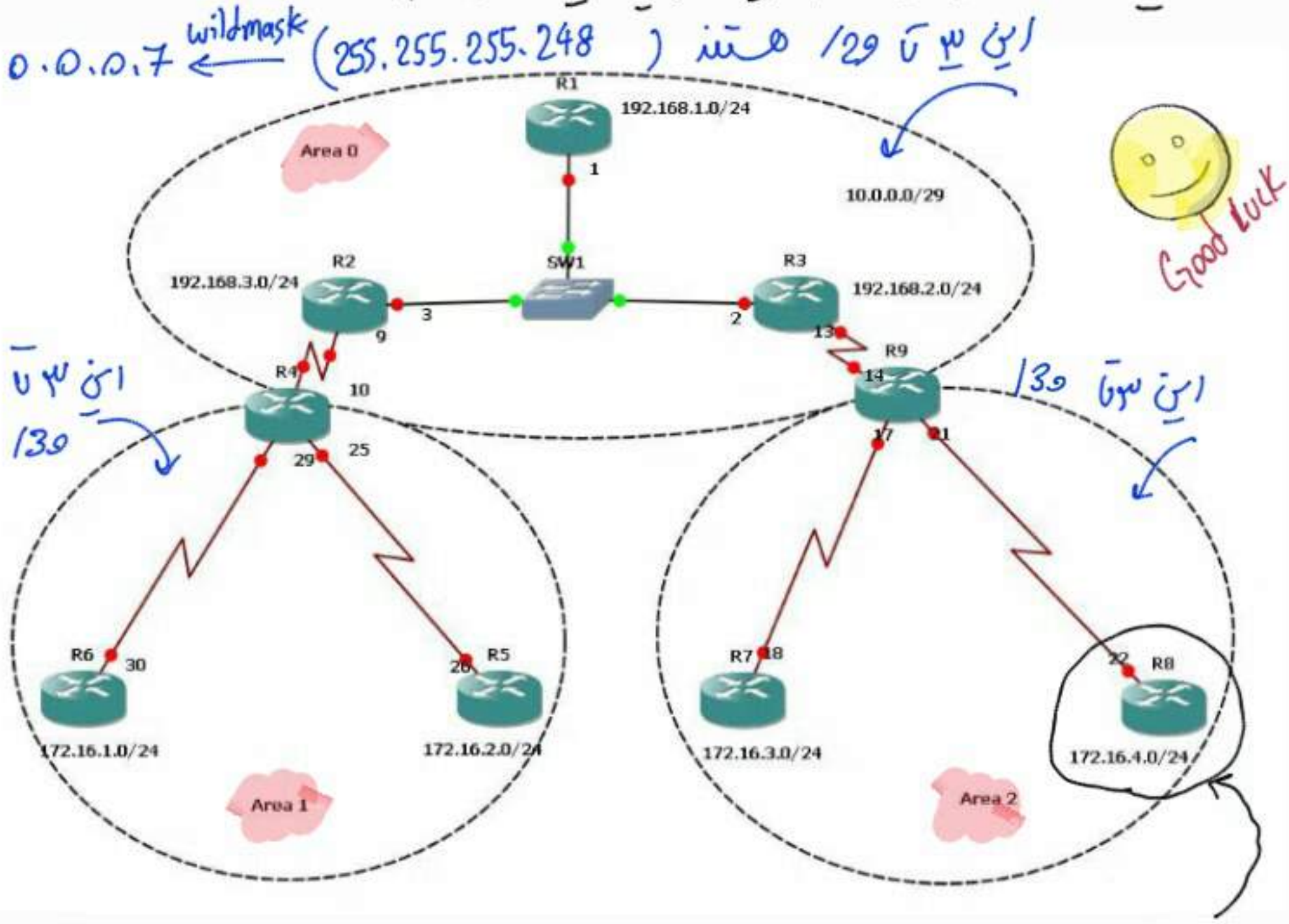
C : یعنی روتر مستقیم به این شبکه وصل است.

O : یعنی ospf یعنی از ospf یاد گرفته است و در همین area است.

O IA : یعنی از ospf یاد گرفته ولی در area دیگری هست.

www.sematec-co.com
Farzad Heydari
By Houshang Héshmati

تمرین : سناریو زیر را بسازید و تمرین کنید. از ospf استفاده شود.



بجای اتصال pc به روترها، روی روترها Loopback بسازید.

Loopback مانند interface هست و در روتر می‌سازید و IP می‌دهید و می‌توانید ping کنید.

```
Router (Config) # interface Loopback ...شماره
Router (Config-if) # IP address 172.16.4.1 255.255.255.0
```

IP بدهید نه NetID چون pc حساب می‌شود

بعد از ساختن Loopback در ospf اضافه کنید

```
router (config-router) # network 172.16.4.0 0.0.0.255 area 2
```

www.sematec-co.com
Farzad Heydari
By Houshang Hashemati

```
router # ping 172.16.4.1
```

← اینجوری ping می‌گیرید

Neighboorship parameters in ospf

دو روتر درصورتی با پروتکل ospf همسایه می‌شوند که موارد زیر رعایت شود:

1) Same area ID — هردو در یک area باشند
2) different Router ID — روتر ID ها با هم فرق کند

router ID چیست؟

در ospf روترها با router ID مشخص می‌شوند و مانند IP ۴ قسمتی است.

چگونه router ID انتخاب می‌شود؟

الف) با دستور توسط ادمین: Router(config-router)# router-id x.x.x.x

ب) بالاترین آدرس Loopback

ج) بالاترین IP که دارد.

```
Router(config)#router ospf 1
OSPF process 1 cannot start. There must be at least one "up" I
Router(config-router)#ro
Router(config-router)#router-id 2.2.2.2
Router(config-router)#
Router(config-router)#
Router(config-router)#exir
                      ^
% Invalid input detected at '^' marker.

Router(config-router)#
Router(config-router)#exit
Router(config)#do sho ip pro

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

Router(config)#
```

اینجا می‌توانید router ID را ببینید

اگر router ID اصلاح شود به هرکدام از روش‌های بالا دیگر تغییر نمی‌کند مگر اینکه ospf ریست شود

Router#clear ip ospf process

دستور reset کردن ospf

www.semanticc.com
Farzad Heydari
By Houshang Heshmati

3) Same Net_ID — هردو در یک شبکه باشند

4) Same Hello_time & Dead interval — زمان ارسال بسته های Hello یکی باشد

۱۰ ثانیه — ۴۰ ثانیه

جهت مانیتورینگ شبکه ospf :

Router # show ip ospf neighboor ← جدول همسایگی ها در ospf

Router # show ip ospf database ← جدول دیتابیس در ospf

Router # show ip router ospf ← فقط روت های ospf

OSPF

محاسبه Metric :

$\frac{10^8}{BW}$ — برحسب b

مثال → $\frac{100,000,000}{1544 \times 1000} \simeq 64$

پورت سریال Serial

Kb به Serial — پورت به BW — Kb به K

مثال → $\frac{100,000,000}{100 \times 1000 \times 1000} = 1$

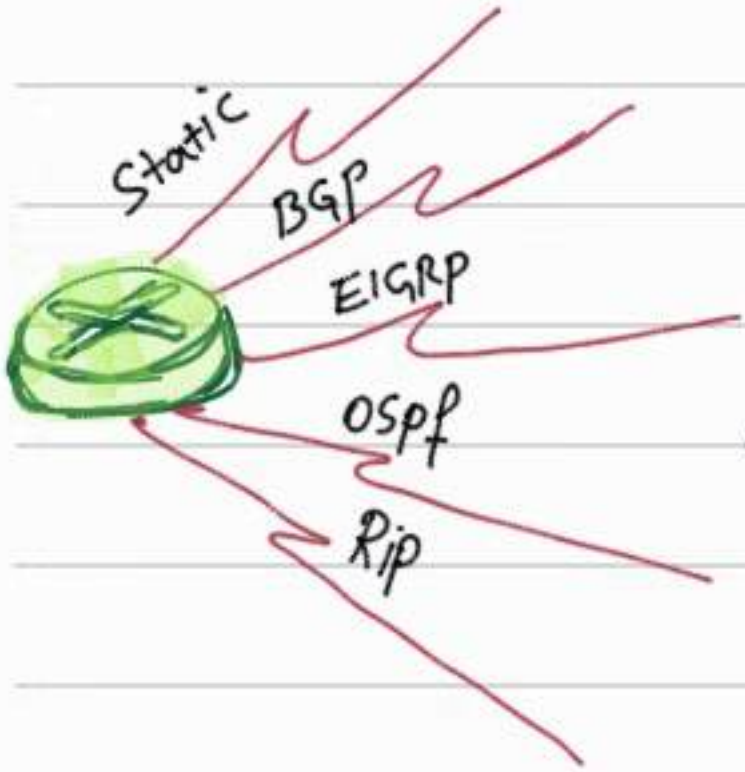
پورت فست fast ethernet

100 mb — پورت fast به BW — Kb به mb — b به Kb

www.cenetec.com
Farzad Heydari
By Houshang Heshmati

برای پیدا کردن BW یک لینک بزنید Router # show interface ... detail

شماره مدل



برای حالت روبرو اولویت با کدام مسیر است؟

در روترها جدولی هست به نام administrative distance که اولویت در آن مشخص شده است.

Type	AD
Connected	∅
Static	1
BGP	20
EIGRP	90
OSPF	110
RIP	120

به خودش وصله

خودمان گفتیم از کدام بره

← بعدا یادی بگیرید

پس اولویت → Static > BGP > Eigrp > OSPF > Rip

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

بسیار کاربردی

خیلی شیرین

ACL
Access Control List

ACL (اکسس لیست) در روترهای سیسکو برای امنیت و فیلتر کردن استفاده می‌شود

نوشتن ACL ۳ قانون طلائی دارد:

قانون اول: ACL را می‌نویسیم و سپس ACL را اعمال می‌کنیم
(Define) (apply)

قانون دوم: اگر در acl چیزی را permit کنیم بقیه deny می‌شوند
از نظر acl همه deny هستند (deny any)

قانون سوم: ترتیب خط‌ها در acl نوشتن، از بالا به پایین است.

مثال ۱
```
deny    mostafa ✓
permit  mostafa ✗
```
خط اول می‌گوید مصطفی deny است
هرچی در خط‌های بعدی بگویید مصطفی permit است دیگر فایده ندارد.

مثال ۲
```
permit  any     ✓
deny    mostafa ✗
```
خط اول گفتیم همه permit هستند
خط دوم نمی‌توانیم مصطفی را deny کنیم چون بالا همه را permit کردیم

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

برای نوشتن acl از wildcard mask استفاده می‌شود:

مثلاً permit 192.168.1.0 0.0.0.255

مثلاً Deny 172.16.0.0 0.0.255.255

صفرها مهم هستند مثلاً یعنی هر IP که با 192.168.1 شروع شود permit

و هر IP که با 172.16 شروع می‌شود deny

اگر بخواهیم یک IP خاص فیلتر شود از wildcard mask 0.0.0.0 استفاده می‌شود.

permit 172.16.4.1 0.0.0.0

مثلاً 0.0.0.3 192.168.1.0 روی ۳ IP اعمال می‌شود

0.0.0.3

0.0.0.00000011

این ۳ IP اعمال می‌شود

01

10

11

چگونه acl بنویسیم و اعمال کنیم؟

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

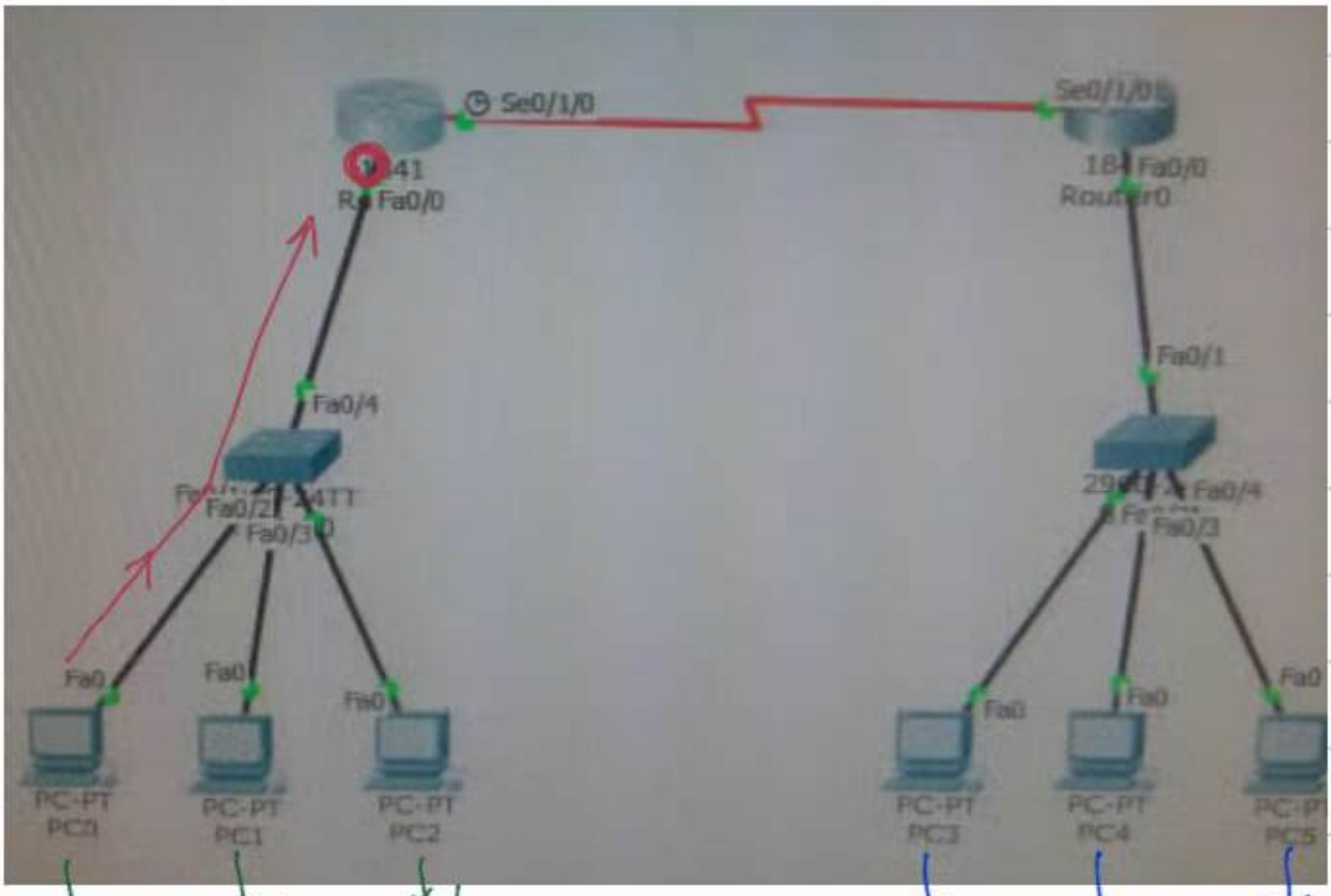
دو نوع ACL داریم :

1) Standard Acl
2) extended Acl

Standard ACL

در Standard Acl فقط می‌توانیم بگوییم IP برود یا نرود

نمی‌توانیم بگوییم به کجا برود، به کجا نرود و چه کند و چه نکند



مدیر 192.168.1.2 | کارمند 192.168.1.3 | کارمند 192.168.1.4 | کارمند | کارمند | کارمند

می‌خواهیم مدیر بتواند به شبکه بغل دسترسی داشته باشد
ولی کارمندان سبز نتوانند کارمندان آبی را ببینند.

www.sematec-co.com
Farzad Heydari
By Houshang Hashmati

Define:

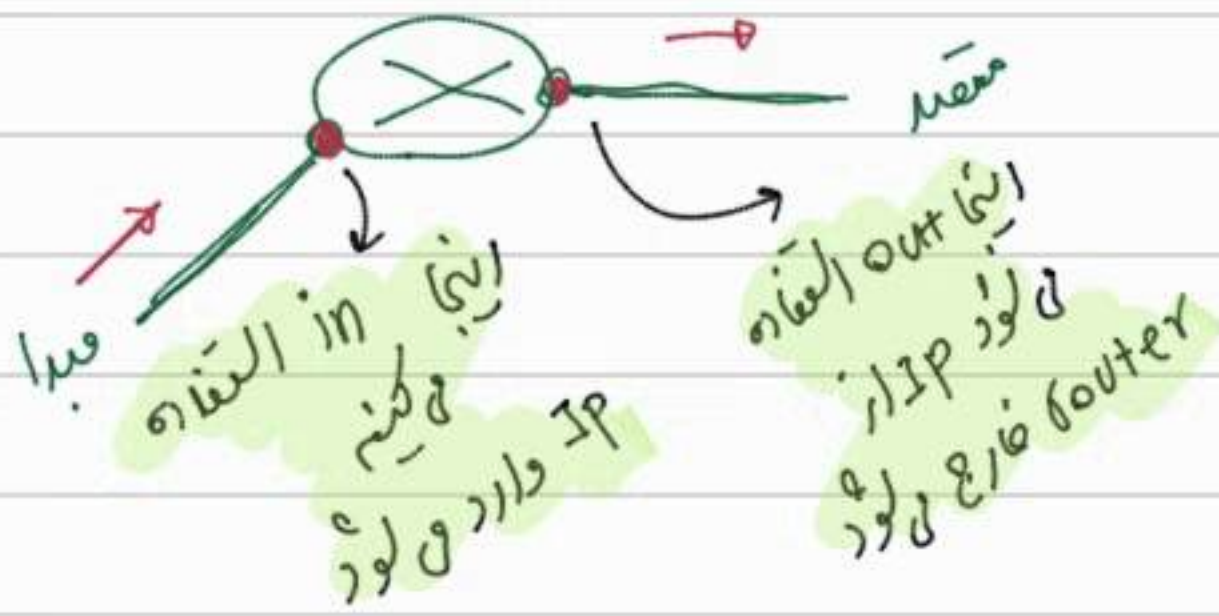
Router(config)# access-list ..... {permit/deny} .... wild card mask
شماره Acl

هر acl با یک شماره مشخص می‌شود که بعدا برای اعمال با شماره‌اش صدا زده می‌شود. شماره acl اگر بین ۱-۹۹ باشد یعنی نوع Standard است.

apply:

Router(config-if)# ip access-group ..... {in / out}
شماره acl

برای اعمال روی دست روتری اعمال می‌کنیم که IP های خواهند از آنجا خارج شوند یا به آن وارد شوند.



قبل از حل مثال صفحه قبل دقت کنید هم کارمندان سبز رنگ هم مدیر برای ورود شبکه بغلی باید به interface fast0/0 روتر وارد شوند. پس می‌توانیم روی آن دست روتر از in اعمال کنیم.

www.sematec.com
Farzad Heydari
By Houshang Heshmati

```
Router(config)#access-list 1 permit 192.168.1.2 0.0.0.0
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#ip acc
Router#conf t
Enter configuration commands, one per line.  End with CNTL
Router(config)#int
Router(config)#interface fas
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip
Router(config-if)#ip ac
Router(config-if)#ip access-group 1 in
Router(config-if)#
```

فقط IP مدیر را permit کردیم

روی دلت روتر رو یم

acl را اعمال کنیم

چرا دو کارمند دیگران را deny نکردیم؟ چون همین که acl بنویسید همه پشت فرض deny می‌شوند ما فقط مدیر را permit می‌کنیم:

اگر بخواهیم فقط مدیر بیرون نرود و بقیه بروند؟

```
router(config)#access-list 1 deny 192.168.1.2 0.0.0.0
router(config)#access-list 1 permit any
```

مدیر را deny کردیم همه هم deny هستند پشت فرض. خط دوم می‌گوییم همه permit هستند (بجز مدیر که خط اول deny شده)

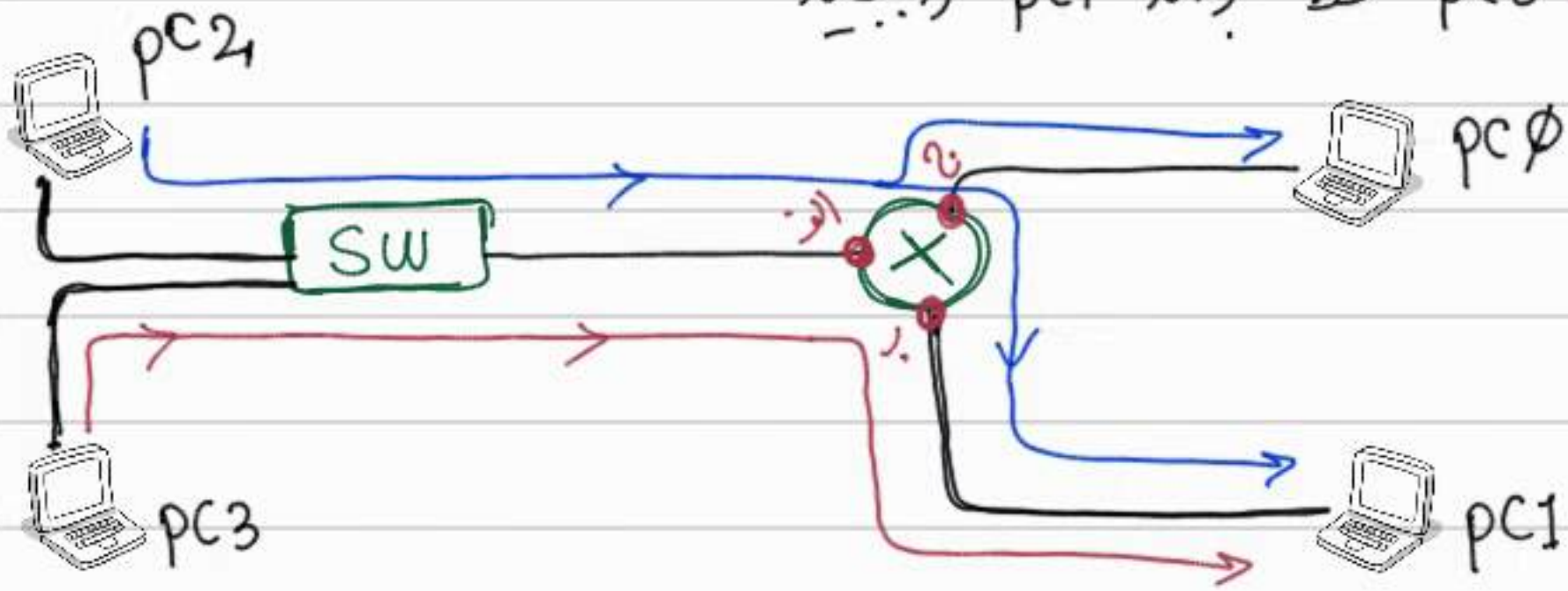
برای نمایش acl از دستور زیر استفاده کنید:

```
router#show access-list
```

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

تمرین: برای سناریوی زیر یک acl یک خطی بنویسید:

* pc2 بتواند pc0 و pc1 را ببیند
* pc3 فقط بتواند pc1 را ببیند



روی دلت ج) روتر که به سمت pc0 می رود acl را اعمال می کنیم

```
Router (config) # access-list 1 permit pc2
Router (config-if) # ip access-group 1 out
```

می نویسیم IP

چرا؟ روی الف و ب هیچ acl ننوشتیم پس همه آزاد هستند بروند و بیایند یعنی pc3 و pc2 می توانند از دلت الف) وارد شوند و از دلت ب به pc1 بروند و pc1 را ببینند.

می ماند اینکه pc3 نتواند pc0 را ببیند
pc2 بتواند pc0 را ببیند

روی دلت ج) روتر acl می نویسیم و اعمال می کنیم همه پیش فرض deny می شوند و فقط به pc2 اجازه خروج می دهیم.

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

چند نکته :

الف) بجای 0.0.0.0 می‌توانیم از عبارت host استفاده کنیم بهتر است.

```
Router (Config)# access-list 1 permit 192.168.1.2 0.0.0.0
Router (Config)# access-list 1 permit host 192.168.1.2
```

هر دو یک معنی می‌دهند

ب) acl فقط برای فیلتر کردن استفاده نمی‌شود بعضی مواقع برای اتصالات و سایت تو سایت (VPN) هم استفاده می‌شود

ج) برای اینکه بعدا یادتون بیاد برای مثلا فلان acl را نوشته‌اید بهتر است آن را بجای عدد با اسم ذخیره کنید (چون عدد نمی‌گذارید باید از عبارت Standard استفاده کنید)

```
Router(Config) # IP access-List Standard .....اسم
Router(Config-Std-nacl) # {permit/deny} ....IP..... wildcar mask
```

وارد acl می‌شوید و می‌توانید خط بنویسید

```
Router(Config-if) # IP access-group .....اسم {out/in}
```

اعمال ← روی interface

چه اسمی؟

مثلاً برای اتصال VPN به سرور بانک acl نوشته‌اید ← VPN2bank

مثلاً دسترسی مدیران به سرورهای فروش ← managersale

www.sematec-co.com
Farzad Heydari
By Mahshang Heshmati

```
Router>
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with
Router(config)#ip acce
Router(config)#ip access-list st
Router(config)#ip access-list standard houshang
Router(config-std-nacl)#perm
Router(config-std-nacl)#permit 192.168.1.2 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#int
Router(config)#interface fa
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group houshang in
Router(config-if)#
```

(بعد از هر خط توضیح همان خط) ۲) ترتیب acl بنویسید برای هر خط یک توضیح بگذارید:

Router(Config)# access-List شماره acl ..... {permit/deny} ..IP..... wildcardmask

Router(Config)# access-List شماره acl ..... remark ..... توضیحات

```
Router(config)#access-list 1 permit host 192.168.1.3
Router(config)#access-list 1 remark Houshang.PC
Router(config)#access-list 1 permit host 192.168.1.4
Router(config)#access-list 1 remark VPN2Bank
Router(config)#
```

```
!
ip flow-export version 9
!
!
!
access-list 1 permit host 192.168.1.2
access-list 1 permit host 192.168.1.3
access-list 1 remark Houshang.PC
access-list 1 permit host 192.168.1.4
access-list 1 remark VPN2Bank
ip access-list standard houshang
 permit 192.168.1.0 0.0.0.255
 permit host 192.168.1.3
!
```

در Show RUN می‌توانید توضیحات را بخوانید

اگر به جای شماره acl اسم دادید و برای توضیحات وقتی وارد acl شدید

Router(config-std-nacl)#remark ..... توضیح

www.ipcisco.com
Farzad Heydari
By Houshang Heshmati

آیا می‌توان acl را ادیت کرد؟

```
RouterX# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

هنگامی از فرمان show accesslist استفاده می‌کنید می‌بینید که خطوط دلخواه شما در acl با شماره ۱۰ تایی از هم جدا شده‌اند. (۱۰، ۲۰، ۳۰، ۴۰، ...)

این برای این است که بین هر دو خط شما ۹ خط جا داشته باشید تا ادیت انجام بدهید:

Router(Config-Std-nacl)# شماره خط {permit/deny} .....

Router(Config-Std-nacl)# No شماره خط

این خط پاک می‌شود

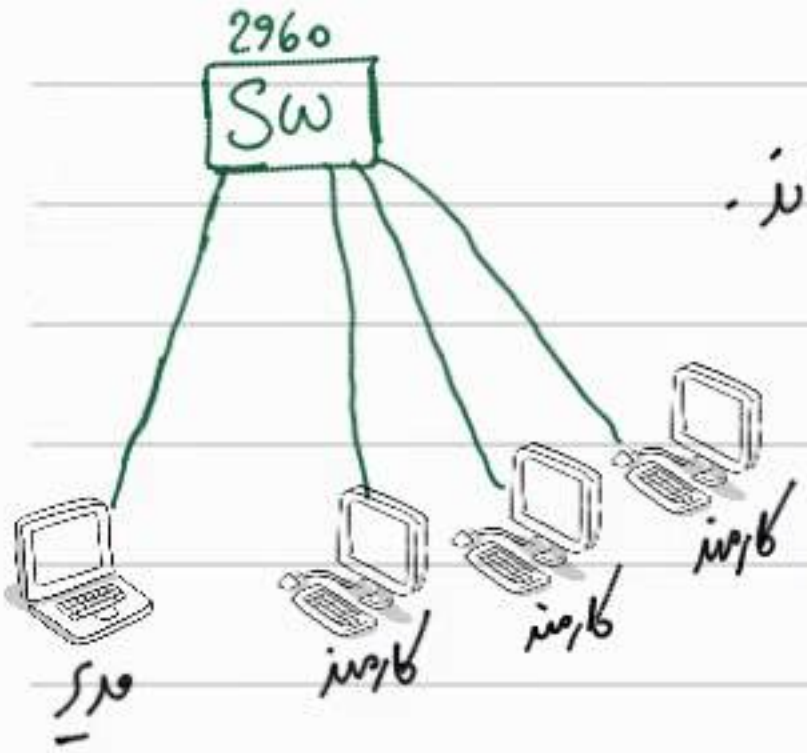
یک خط اضافه می‌کند

```
Router(config)#ip access-list standard 1
Router(config-std-nacl)#12 permit 192.168.1.12
Router(config-std-nacl)#rema
Router(config-std-nacl)#remark khavar
Router(config-std-nacl)#
Router(config-std-nacl)#exit
Router(config)#do sho acc
Standard IP access list 1
    10 permit host 192.168.1.2
    12 permit host 192.168.1.12
    20 permit host 192.168.1.3
    30 permit host 192.168.1.4
Standard IP access list houshang
    10 permit 192.168.1.0 0.0.0.255
    20 permit host 192.168.1.3
```

اگر اسم ندارد و acl شماره‌ای است اینجوری وارد شوید

خط ۱۲ را اضافه کردیم

www.sefiatec-co.com
Farzad Feyda
By Houshang Hashmati



سناریو متداول (با لوئیچ):

فقط مدیر بتواند به بقیه کارمندها Telnet بزند.

برای اعمال در لوئیچ:

Switch (config-if) # access-class ..... {in/out}

```
Switch(config)#inte
Switch(config)#interface vl
Switch(config)#interface vlan 1
Switch(config-if)#ip add
Switch(config-if)#ip address 10.0.0.1 255.0.0.0
Switch(config-if)#no shu

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, ch

Switch(config-if)#exit
Switch(config)#inte
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pass
Switch(config-line)#password 123
Switch(config-line)#login
Switch(config-line)#login
Switch(config-line)#acce
Switch(config-line)#
Switch(config-line)#exit
Switch(config)#ip acc
Switch(config)#ip access-list 1 perm
Switch(config)#ip access-list 1 per
Switch(config)#access-list 1 pe
Switch(config)#access-list 1 pe
Switch(config)#access-list 1 permit host 10.0.0.2
Switch(config)#line
Switch(config)#line VT
Switch(config)#line VTy 0
Switch(config-line)#ACCE
Switch(config-line)#ACCEss-class 1 IN
```

برای رمیوت کردن vty ، Telnet را فعال می‌کنیم

این IP اجازه دارد

روی vty اعمال می‌کنیم

این جوری

چون می‌خواهیم Telnet کنیم پس باید روی Line vty اعمال کرد

www.somagcco.com
Fa
By Houshang Heshmati

برای اعمال فیلتر acl جهت Telnet و ریموت شدن :

۱) بروی کونفیگ باید روی interface line vty اعمال کنید

Switch(Config-line)# access-list شماره acl ..... in

دقت کنید IP نمی نویسیم

اگر IP اول دستور بنویسید یعنی IPV6 می شود.

۲) بروی روتر بروی دست های روتر اعمال می کنید چون به IP دست های روتر ریموت می کوبیم.

در این نوع از acl می توانیم روی مقصد بسته های ارسالی و نوع ترافیک هم نظارت داشته باشیم.

برای شماره گذاری acl از ۱۰۰ تا ۱۹۹ استفاده می کنیم.

Extended ACL
- Source
- Destination
- protocols
  - TCP
  - udp
  - Icmp
  - ospf
  - ⋮

بروی IP می شیند

www.sematec-co.com
Farzad Heydari
By Houshang Hashemat

اگر بجای protocol فقط بزنیم IP یعنی همه پروتکل ها را شامل می شود.

با اسم

```
router(config)# IP access-list extended .....
router(config-ext-nacl)# {permit/deny} ip host ..... host .....
```

IP مبدا — IP مقصد

یعنی همه چی خوبی پروتکل هست.

با عدد

```
router(config)# access-list ..... {permit/deny} ip host ..... host ....
```

شماره acl

IP مبدا — IP مقصد

```
% Incomplete command.
Router(config)#ip acc
Router(config)#ip access-list ex
Router(config)#ip access-list extended houshang
Router(config-ext-nacl)#permi
Router(config-ext-nacl)#permit ip host 192.168.1.2 host 172.16.0.2
Router(config-ext-nacl)#permit ip host 192.168.1.3 host 172.16.0.3
Router(config-ext-nacl)#
```

شبکه اول { مدیر 192.168.1.2 ، معاون 192.168.1.3

شبکه دوم { مدیر 172.16.0.2 ، معاون 172.16.0.3

فقط مدیر شبکه اول فقط مدیر شبکه دوم را ببینند و معاون شبکه اول فقط معاون شبکه دوم را ببینند

```
Router(config)#
Router(config)#inte
Router(config)#interface fas
Router(config)#interface fastEthernet 0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#acc
Router(config-if)#ip
Router(config-if)#ip ac
Router(config-if)#ip access-group 100
% Incomplete command.
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

دقت کنید بعد deny شده اند یعنی هیچ IP هیچ جایی را نمی بیند

www.somatec.com
Farzad Heydari
By Houshang Heshmati

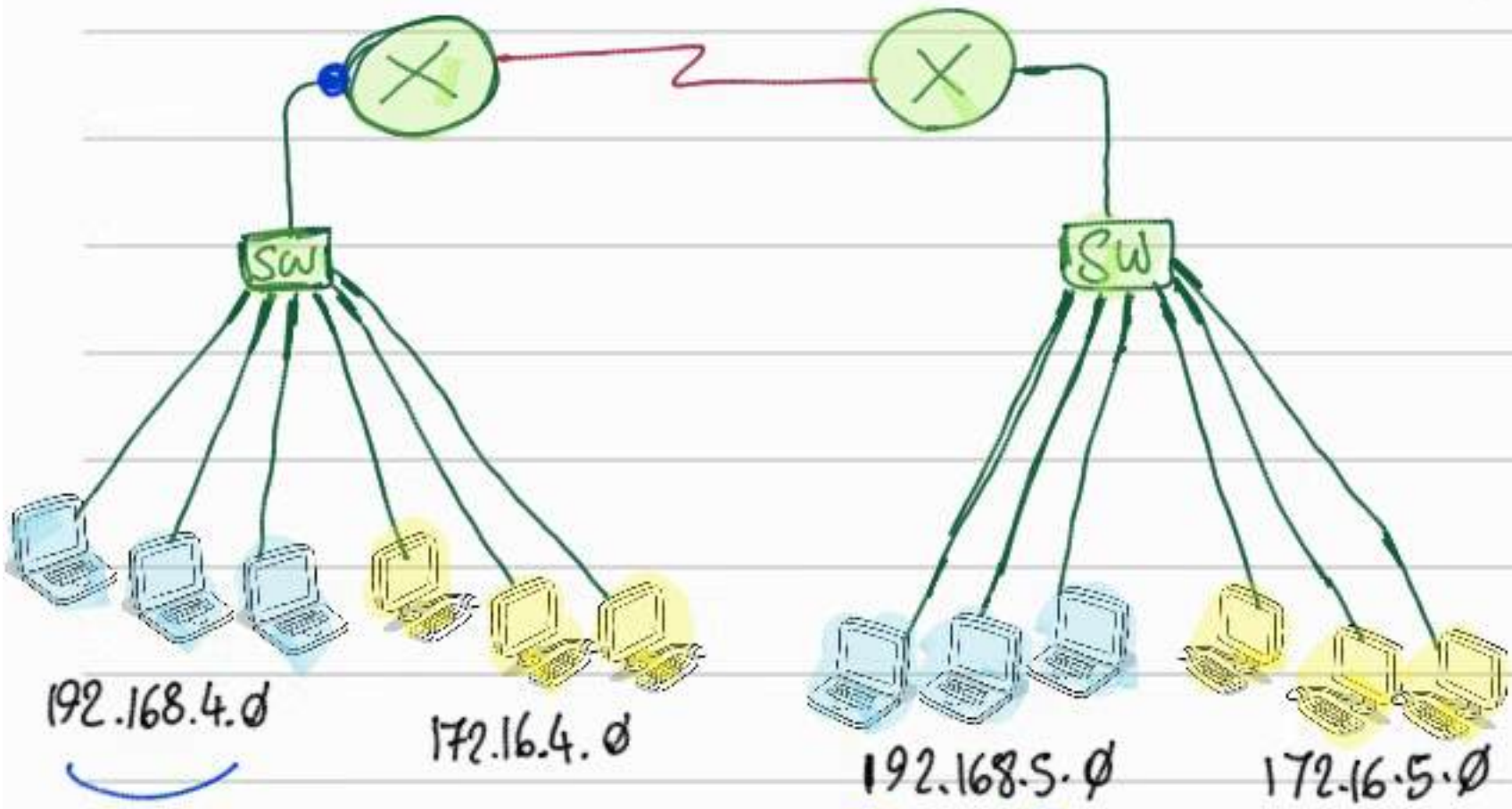
اگر بخواهیم 192.168.1.2 هیچ جایی را نبیند ولی بقیه بتوانند ؟

```
Router(Config)# access-list 100 deny ip host 192.168.1.2 any
Router(Config)# access-list 100 permit ip any any
```

هیچ جا

هر IP هر جایی

* چگونه بگوییم یک شبکه می‌تواند یک شبکه دیگر را ببیند ؟



این شبکه را ببیند

```
Router(Config)# access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255
```

این شبکه این شبکه را ببیند

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

چگونه ای کل access-list بنویسیم

الف) نتوانیم ping بزنیم؟

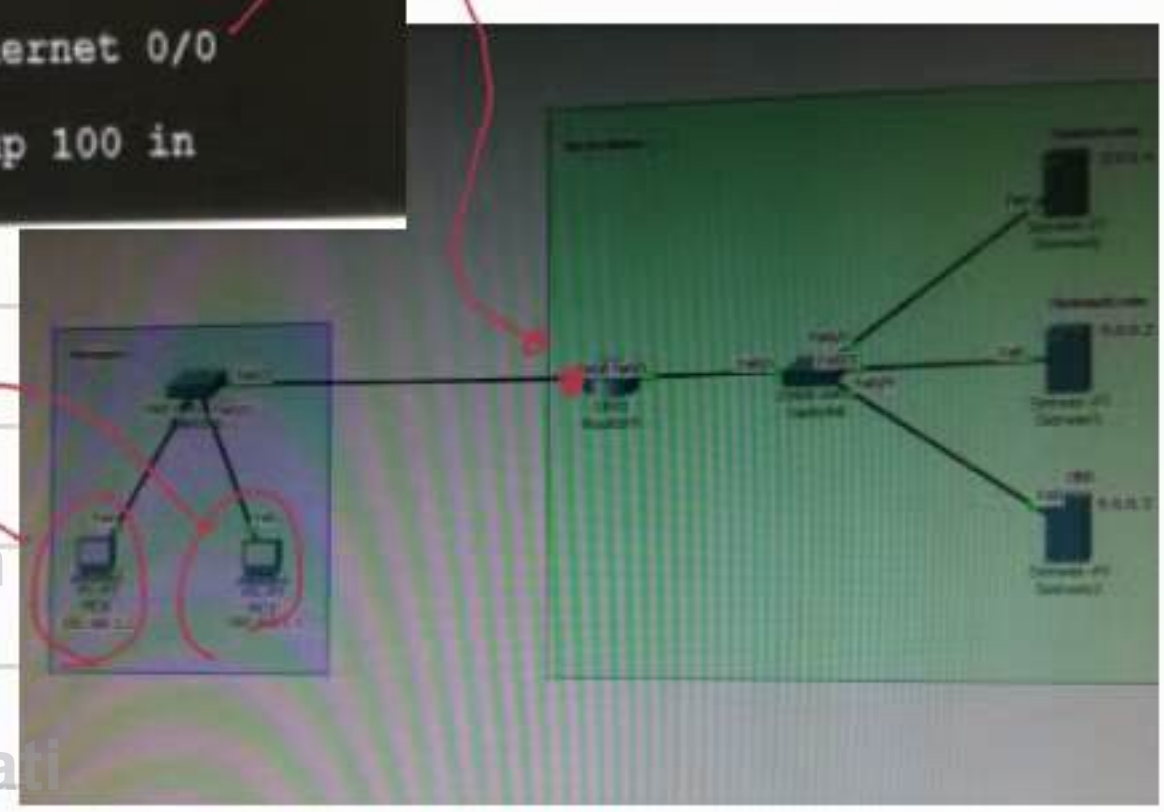
Router(config)# access-list 100 deny icmp any any

icmp را deny کردیم پروتکلی که ping جزء آن است.

Router (Config)# access-list 100 permit IP any any

بقیه IP را باز می‌کنیم. (چون بادلیوز لول، همه چی deny می‌شود).

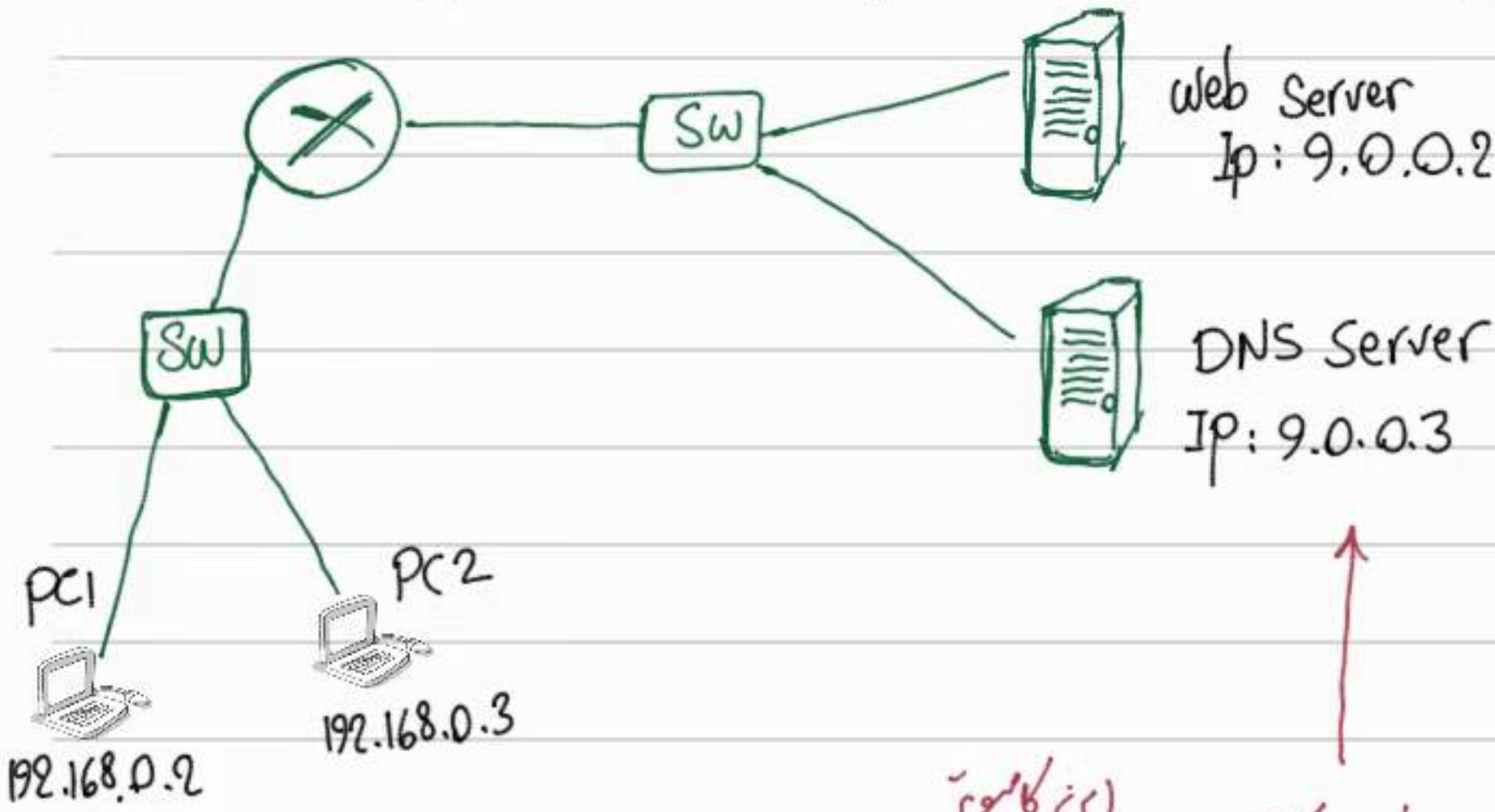
```
Router#conf t
Enter configuration commands, one per line.  End
with CNTL/Z.
Router(config)#acce
Router(config)#access-list 100 den
Router(config)#access-list 100 de
Router(config)#access-list 100 deny ic
Router(config)#access-list 100 deny icmp any any
Router(config)#acc
Router(config)#acc
Router(config)#access-list 100 per
Router(config)#access-list 100 permit ip a
Router(config)#access-list 100 permit ip any an
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#inr
Router(config)#int
Router(config)#interface fa
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 100 in
Router(config-if)#
```



نتوانند سرورها را ping کنند

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

ب) DNS اعمال نشود (وب باز شود ولی فقط با IP):



این کامپیوتر

سرور DNS

router(config)#access_list 100 deny udp host 192.168.0.2 host 9.0.0.3 eq53

پروتکل udp

از پروتکل udp فقط udp53 بسته می‌شود که DNS است.

router(config)#access-list 100 permit ip any any

بجز کامپیوتر PC1 بقیه همه کاری بتوانند بکنند.

دستور کامل Extended acl:

router(config)#access-list acl شماره {permit/deny} protocol SRC IP SRC wc mask [oprator SRC port] DST IP DST wc mask [opertor DST port] [log]

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

ج) چند مثال دیگر :

```
router(config)#access-list 100 deny tcp host 192.168.0.2 host 9.0.0.2 eq 80
```

نتواند وب باز کند (http)

```
router(config)#access-list 100 deny tcp host 192.168.0.2 host 9.0.0.2 eq 443
```

نتواند وب باز کند (https)

د) سؤال درست و صحیح :

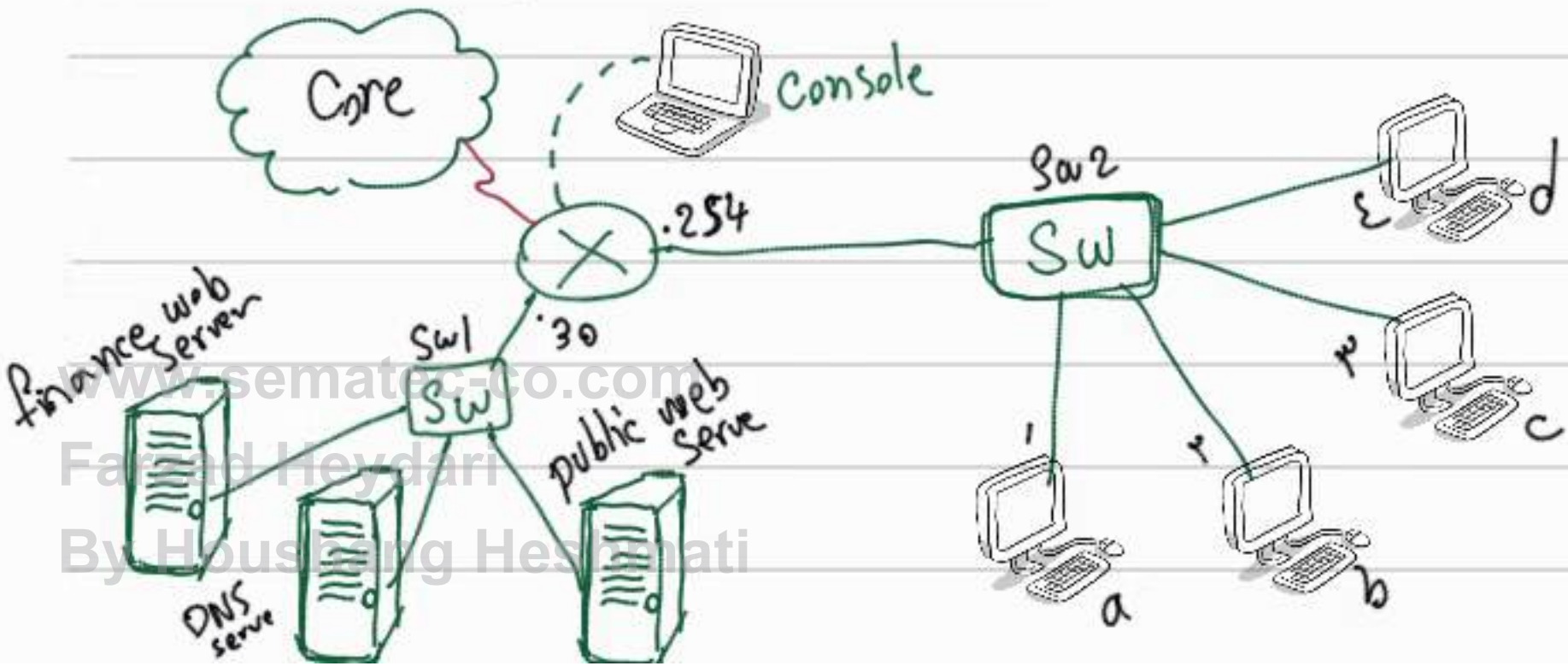
Question

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".
The Core connection uses an IP address of 198.18.196.65
the computers in the Hosts LAN have been assigned addresses of 192.168.33.1-192.168.33.254
Host A 192.168.33.1
Host B 192.168.33.2
Host C 192.168.33.3
Host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 – 172.22.242.30
The Finance Web Server is assigned an IP address of 172.22.242.23.
The Public Web Server is assigned an IP address of 172.22.242.17

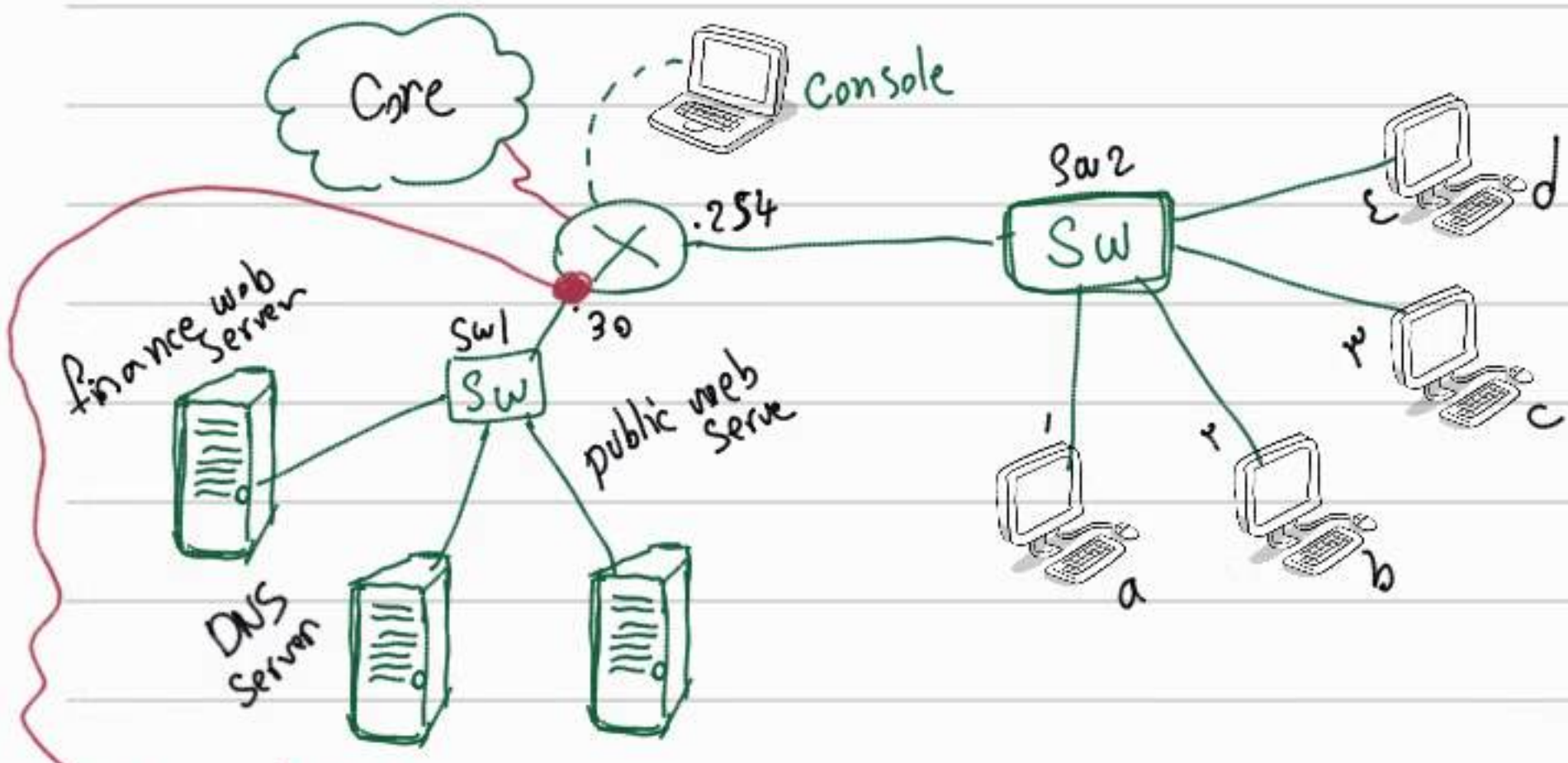


www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

جواب :

```
Router(config)# access-list 100 permit Tcp host 192.168.33.3 host 172.22.242.23 eq 80
Router(config)# access-list 100 deny Tcp any any host 172.22.242.23 eq 80

Router(Config)# access-list 100 permit ip any any
```

خط اول : کامپیوتر e به سرور مالی به صورت web دسترسی پیدا کند.
خط دوم : هیچ کامپیوتر دیگری به صورت web به سرور مالی دسترسی پیدا نکند.
خط سوم : بقیه بتوانند به جاهای دیگر دسترسی داشته باشند.



روی این پورت اعمال می‌شود

```
router(config-if)# ip access-list 100 out
```

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

چرا روی این پورت؟ چرا روی پورت دیگر روتر (که 1 و 2 بنویسیم) اعمال نکردیم؟
چون از Core (اینترنت) هم ممکن است دسترسی پیدا کند باید جلوی آن هم بگیریم.

IP هایی که داخل شبکه های اداری و سازمانی استفاده می‌کنید private هستند و در داخل شبکه جهانی اینترنت route نمی‌شوند. برای ورود به شبکه اینترنت باید از IP های public استفاده کنید.

هنگامی که به اینترنت وصل می‌شوید ISP به pc شما یک IP از نوع public اختصاص می‌دهد که رندوم بوده و در اتصال بعدی از IP دیگری استفاده خواهید کرد.

IP های public خریدنی هستند و اگر تمایل دارید که IP ثابت برای ورود به اینترنت داشته باشید تا همیشه بتوانید به آن وصل شوید (دوربین حفاظتی، سرور، ...) باید از Isp خریداری کنید.

سرویس NAT وظیفه اختصاص دادن IP های public به IP های private شما هنگام ورود به اینترنت بر عهده دارد.

10.0.0.0 /8
172.16.0.0 /16
192.168.0.0 /16

$\xrightarrow{NAT}$ public IP

سرویس NAT روی روتر کانفیگ می‌شود و بر سه حالت است:

1) Static NAT
2) Dynamic NAT
3) Dynamic overload (PAT)

www.sefiatec-co.com
Farzad Haydari
By Houshang Hosmati

Static NAT (1

یک IP از نوع private را به یک IP از نوع public ترجمه می‌کند.

فرض کنید مدیر یک سازمان می‌خواهد از خارج سازمان (منزل خودش یا در سفر) به یکی از سرورهای سازمان دسترسی داشته باشد.

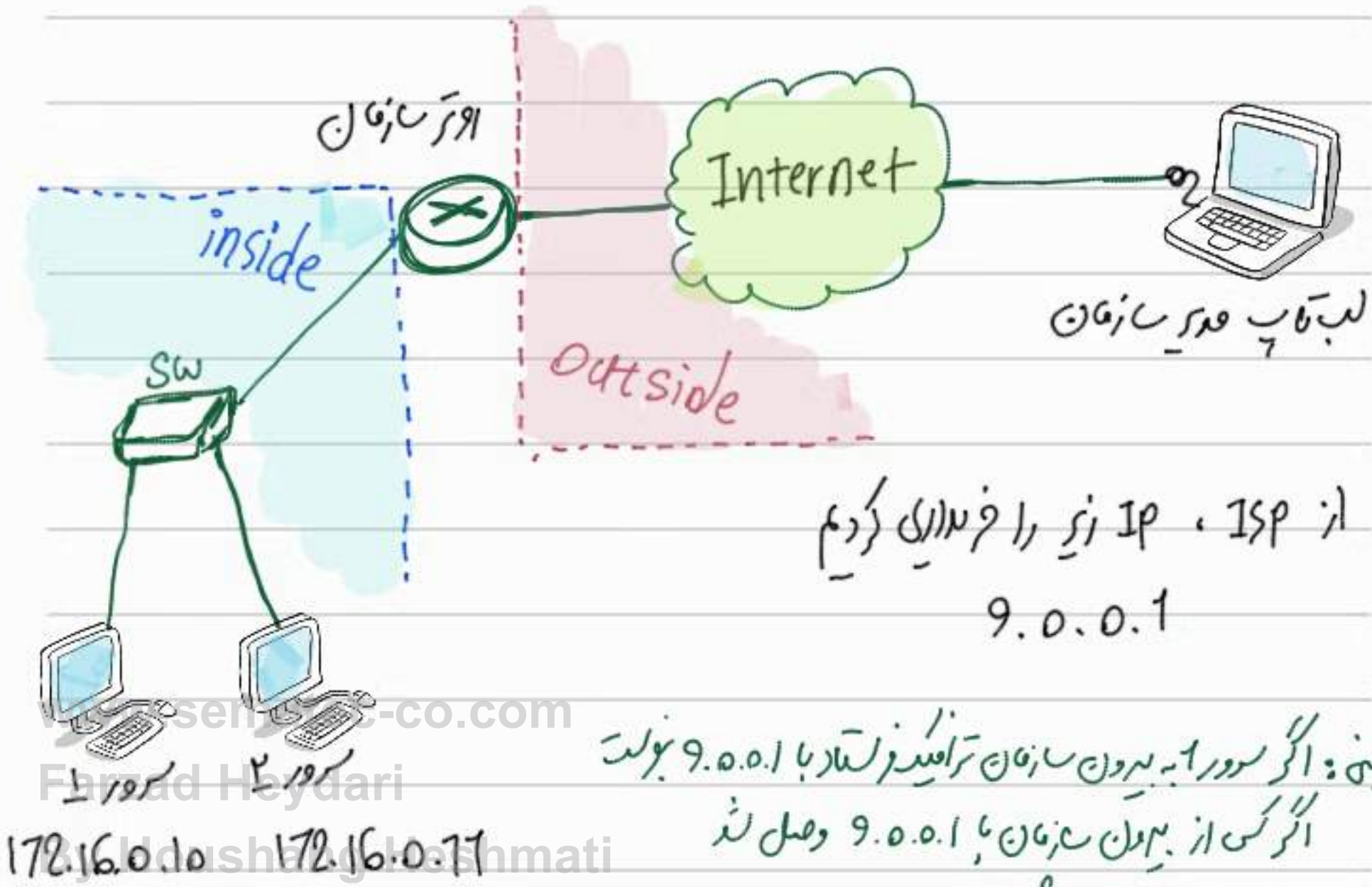
IP سرور مورد نظر 172.16.0.10 می‌باشد ولی مدیر نمی‌تواند از منزل خودش با 172.16.0.10 به سرور وصل شود.

راه حل:

1) یک IP از نوع private خریداری می‌کنید (از ISP خودتان)

2) داخل داخل NAT راه اندازی می‌کنید (inside و outside را مشخص می‌کنیم)

3) IP نوع private را به IP نوع public متصل می‌کنید.



از ISP، IP زیر را خریداری کردیم

9.0.0.1

یعنی: اگر سرور ۱ به بیرون سازمان ترافیک فرستاد با 9.0.0.1 بفرست

اگر کسی از بیرون سازمان با 9.0.0.1 وصل شد به سرور ۱ وصل شود

www.sentec-co.com
Farzad Heydari
Farzad.Heydari@gmail.com

Router (config) # interface ..... Type / num

Router (config-if) # Ip NAT (inside | outside)

باید داخل هر دو دلت روتر تونیم { یک دلت به سمت سازمان ← inside
یک دلت به سمت internet ← outside

Router (Config) # ip NAT inside Source static ..... privet IP ..... public IP

Router # show IP NAT Translation ← جهت گزارش‌گیری

```
Router(config)#interface serial 0/1/1
Router(config-if)#ip nat ins
Router(config-if)#ip nat inside
Router(config-if)#EXIT
Router(config)#
Router(config)#
Router(config)#INTE
Router(config)#INTErface SE
Router(config)#INTErface SErial 0/0/0
Router(config-if)#IP NA
Router(config-if)#IP NAt OU
Router(config-if)#IP NAt OUtside
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#EXIT
Router(config)#ip n
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat ins
Router(config)#ip nat inside so
Router(config)#ip nat inside source s
Router(config)#ip nat inside source static 172.16.0.10 9.0.0.1
Router(config)#do sho ip na tr
Pro  Inside global      Inside local       Outside local
---  9.0.0.2            172.16.0.10        ---

Router(config)#
```

به سمت سازمان ← serial 0/1/1

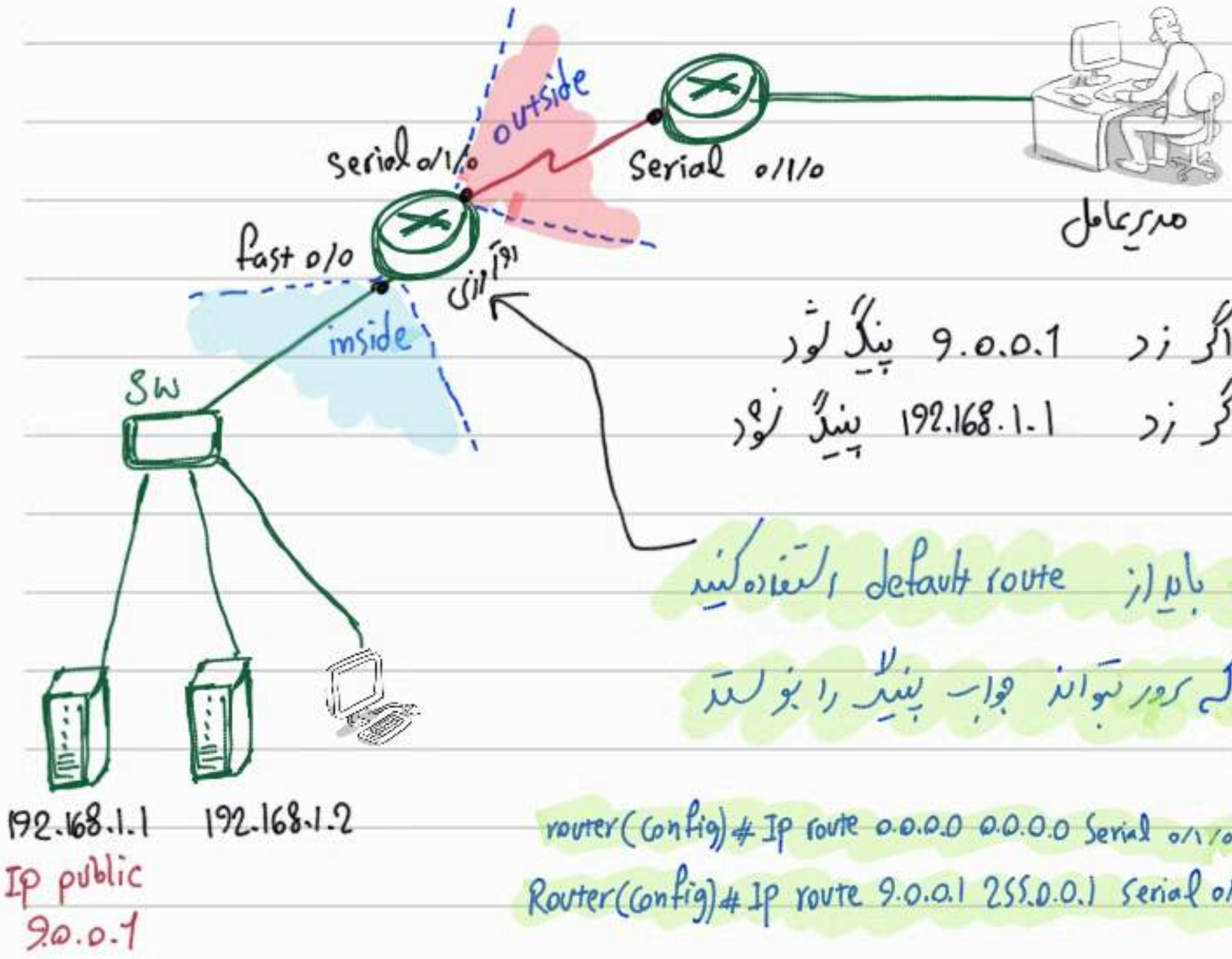
به سمت اینترنت ← serial 0/0/0

IP برای سرور private ↓

IP خریداری شده public ↓

www.somafer.com
Farzad Heydari
By Houshang Heshmati

یک مثال) سناریوی زیر را بسازید: (راهنمایی‌ها به رنگ آبی هستند)



اگر زد 9.0.0.1 پینگ شود

اگر زد 192.168.1.1 پینگ نشود

* باید از default route استفاده کنید که روتر بتواند جواب پینگ را بگیرد

```
router(config)# IP route 0.0.0.0 0.0.0.0 Serial 0/1/0
Router(config)# IP route 9.0.0.1 255.0.0.1 Serial 0/1/0
```

```
Router(config)# interface fastethenet 0/0
Rorter(config-if)# IP NAT inside
Router(config)# interfase Serial 0/1/1
Router(config-if)# IP NAT outside
Router(config)# IP NAT inside Source static 192.168.1.1 9.0.0.1
```

www.sematec-co.com
Powered by Reyvan
By Houshang Heshmati

2) Dynamic NAT :

اگر تعدادی از کاربران بخواهند به اینترنت وصل شوند مثلاً ۶ کاربر در سازمان داریم و ۶ عدد IP هم از نوع public از ISP خریداری کردیم

حالا یک مخزن (pool) برای روتر تعریف می‌کنیم و IPهای public را داخل آن قرار می‌دهیم. هر کدام از ۶ کاربر سازمان که خواست به اینترنت وصل شود از مخزن روتر یک IP می‌گیرد و به اینترنت وصل می‌شود.

مراحل:

۱) inside و outside را مشخص می‌کنیم.

۲) برای روتر Range IPها را برای public و private مشخص می‌کنیم

۳) برای IPهای private یک acl می‌نویسیم

۴) در روتر یک pool از IPهای public تعریف می‌کنیم

```
Router(Config)# interface Type / num
Router(Config-if)# IP NAT {inside|outside}

Router(Config)# access-list acl-num permit Net ID wildcard mask
```

مثال) Router(Config)# access-list 1 permit 192.168.1.0 0.0.0.255

```
Router(Config)# IP Nat pool name start IP End IP netmask mask
```

مثال Route(Config)# IP NAT pool Ali 9.0.0.1 9.0.0.254 netmask 255.255.255.0

```
Router(Config)# IP NAT inside Source list acl-num pool pool name
```

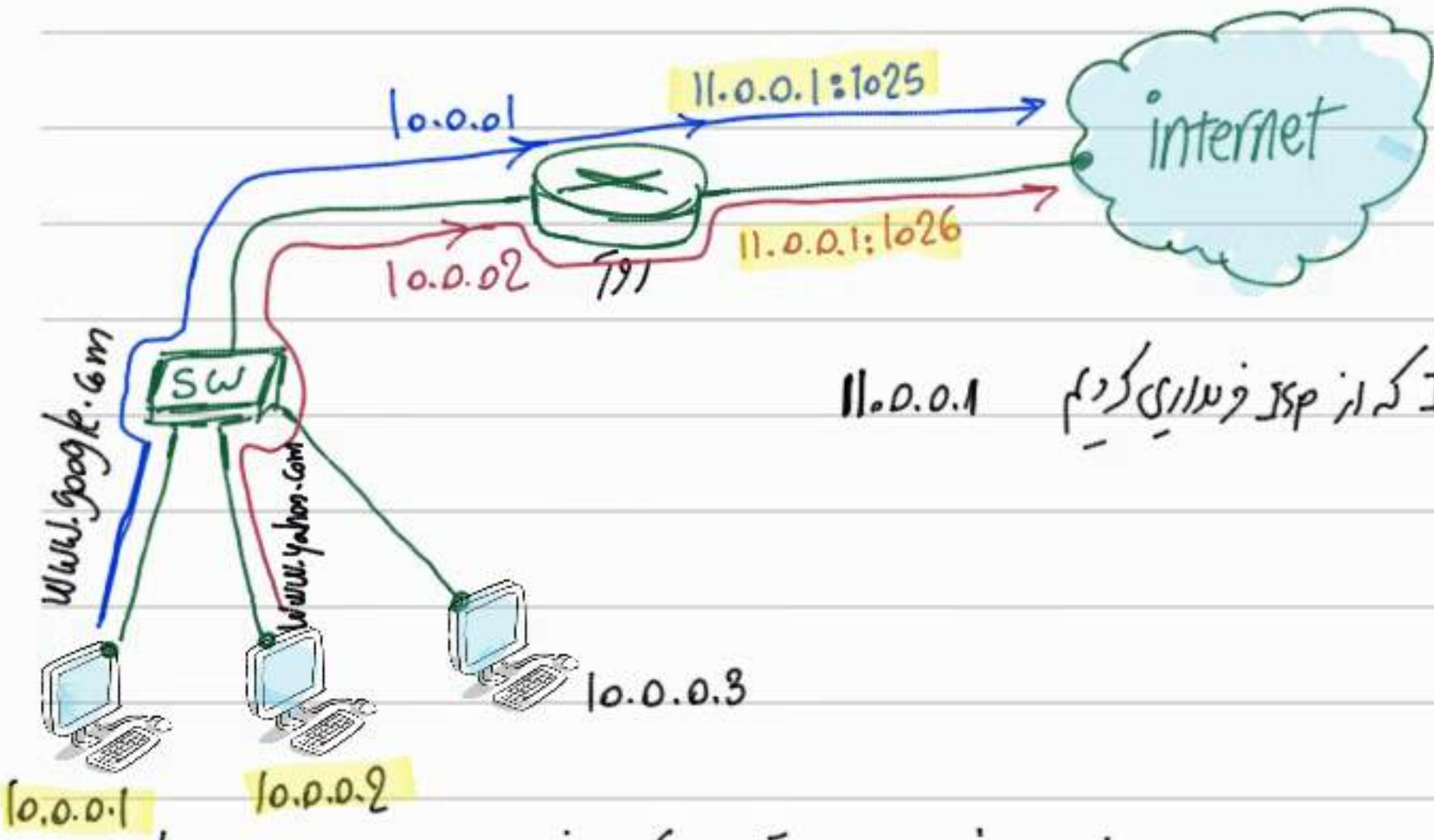
مثال Router(Config)# IP NAT inside Source list 1 pool Ali

www.sematec-co.com
Farzad Heydari
By Farzad Heydari

C3 PAT (dynamic overload) :

این روش کلا IPv4 را نجات داد. به کمک این روش می‌شود کل یک کلاس IP از نوع private را با یک عدد IP از نوع private ، NAT کرد.

در حقیقت IP های private را توسط شماره پورت به اینترنت می‌فرستد



IP که از ISP خریداری کردیم 11.0.0.1

مانند dynamic NAT است فقط با این تفاوت که داخل pool تنها تعدادی یا یک عدد IP وجود دارد و اگر دستور هم overload می‌زنیم.

Router(config)# IP NAT inside source list ..... acl-num pool ..... name overload

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

IPV6

چون تعداد IPهای public مورد استفاده در دنیا زیاد شد (از کامپیوتر و موبایل و سایت گرفته حتی الان یخچال ها IP دارند) کم کم IPV4 تمام شد

IPV6 تعریف شد که 128 bit است.

به صورت زیر می باشد

FE00:0000:0000:0001:0000:0000:0000:0056

که خلاصه می شود

FE00:0:0:1:0:0:0:56

و خلاصه تر

FE00:0:0:1::56

حفالت بکشید، دوره Network+ را مطالعه کنید

* در دستورات هرجا IP داشتید بجای آن IPV6 بزنید
* روی روتر باید فعال شود: Router(config)#IPV6 unicast-routing
* IPV6 کلاس ندارد و subnet mask ندارد و بجای آن prefix length دارد.
* بصورت زیر استفاده می شود 2000::1/64

Router(config)# interface و ...

Router(config-if)# IPV6 address 2000::1/64

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

Router # show Ipv6 Route
Router # show Ipv6 interface brief

گذرنگاری

EigrP

router (Config) # Ipv6 Router eigrp asn
router (Config-rtr) # no shutdown
router (Config-rtr) # router_id X.X.X.X
router (Config-if) # Ipv6 eigrp ASN

---

ospf

router (Config) # Ipv6 ospf process_id
router (Config-rtr) # router_id X.X.X.X
router (Config-if) # Ipv6 ospf process_id area area-id

Rip

router (Config) # Ipv6 rip name
router (Config-if) # Ipv6 rip name enable
router # show ipv6 protocols

---

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati

پایان

با تشکر از زحمات استاد عزیز

استاد: فرزاد حیدری

دوره CCNA

سماتک تابستان 95

www.sematec-co.com
Farzad Heydari
By Houshang Heshmati