

دانشگاه سمنان

دانشکده مهندسی برق و کامپیوتر

درجه تحصیلی: کارشناسی

Network Lab Documentary

گردآورندگان:

پرنیان شاکریان

استاد:

دکتر غزاله مصطفائی

سال تحصیلی: 1403 - 1402

فهرست مطالب

[computer network 1](#_Toc167451982)

[Packet Tracer 1](#_Toc167451983)

[switch 4](#_Toc167451984)

[VLAN 5](#_Toc167451985)

[بهینه سازی 10](#_Toc167451986)

[VTP 12](#_Toc167451987)

[امنیت شبکه 21](#_Toc167451988)

[port security 21](#_Toc167451989)

[دستورات 22](#_Toc167451990)

[Shutdown and Restrict 25](#_Toc167451991)

[Router 29](#_Toc167451992)

[Routing Information 33](#_Toc167451993)

### computer network

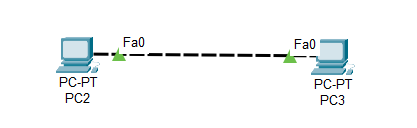
در شبکه‌های کامپیوتری به دلیل هزینه‌های فراوان و پیچیدگی نمیتوان تمامی قطعات و device‌های موردنیاز را تهیه کرد. به این منظور از شبیه‌ساز ها برای آموزش و یادگیری استفاده می‌کنیم. 2 نوع از شبیه‌ساز‌های مهم شامل موارد زیر می‌باشد:

1. Simulator: برنامه ریزی شده تا کار مشخصی را انجام دهد. مانند Packet Tracer
2. Emulator: به هنگام کار یا آن از منابع سیستم استفاده می‌کند. مانندGNS3 و EVE

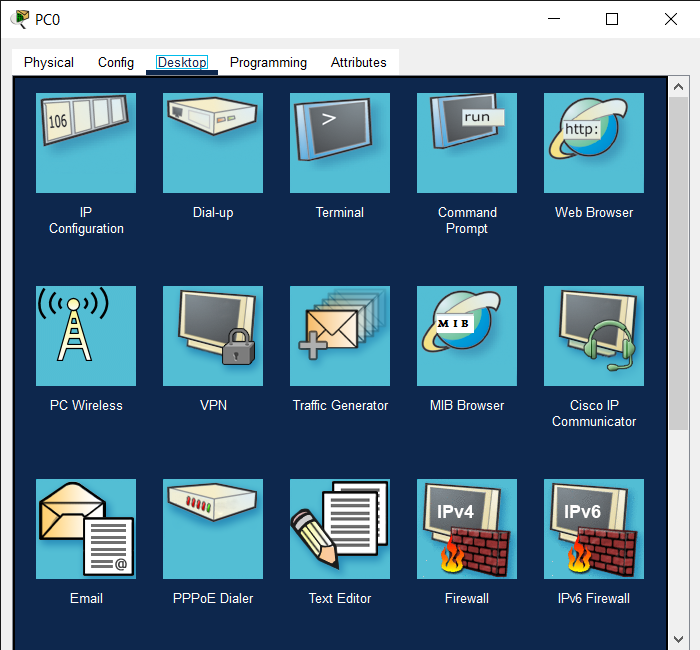
Packet Tracer یک ابزار شبیه‌سازی است که توسط Cisco Systems طراحی شده و به کاربران اجازه می‌دهد تا توپولوژی‌های شبکه‌ را ایجاد نمایند. کاربران در این نرم افزار می‌توانند انواع پیکربندی روترها و سوئیچ های سیسکو را با استفاده از یک رابط خط فرمان (CLI) شبیه سازی کنند. این نرم‌افزار عمدتاً توسط دانشجویان آکادمی شبکه‌های سیسکو به عنوان یک ابزار آموزشی برای یادگیری مفاهیم اساسی CCNA استفاده می‌شود. در پنل Packet Tracer می‌توانیم ابزارهای مورد نیاز خود را برای طراحی و ساخت یک شبکه انتخاب نماییم. Category های مشخص شده در انتهای نرم‌افزار شاملnetwork devices، end devices، connections و غیره می‌شود. در سری آزمایش‌های خود بیشتر با 3 بخش نام برده شده کار خواهیم داشت.

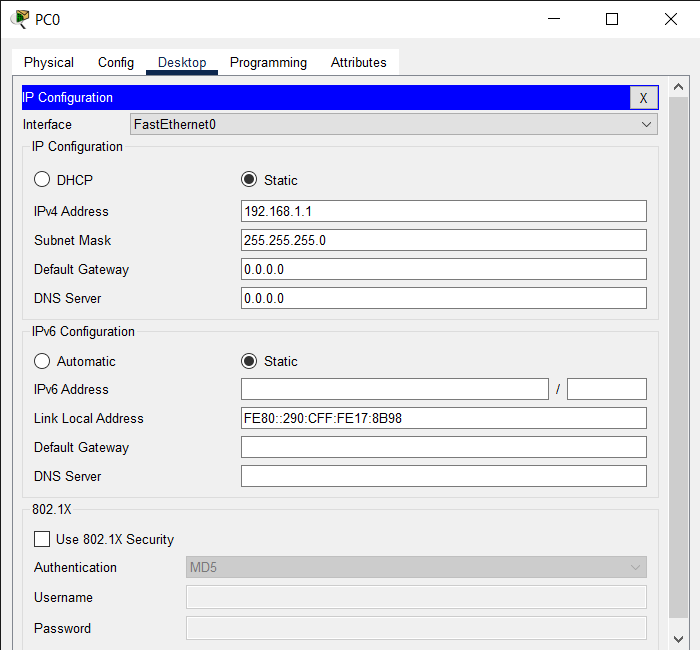


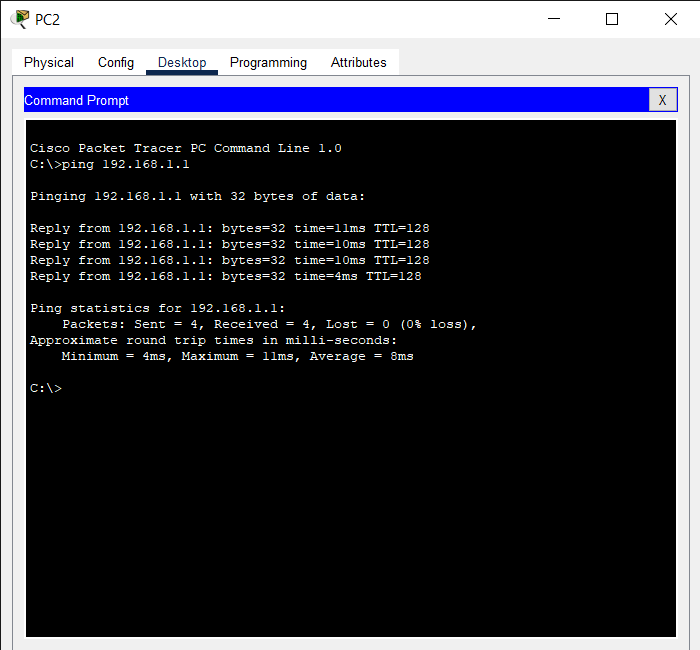
در اولین فعالیت خود ساده‌ترین نوع پیکربندی را خواهیم ساخت. ابتدا وارد بخش end devices شده و دو عدد PC انتخاب می‌کنیم سپس PC ها را توسط کابل اتصال از قسمت connections به هم وصل خواهیم کرد. (بهتر است از کابل automat استفاده شود.)



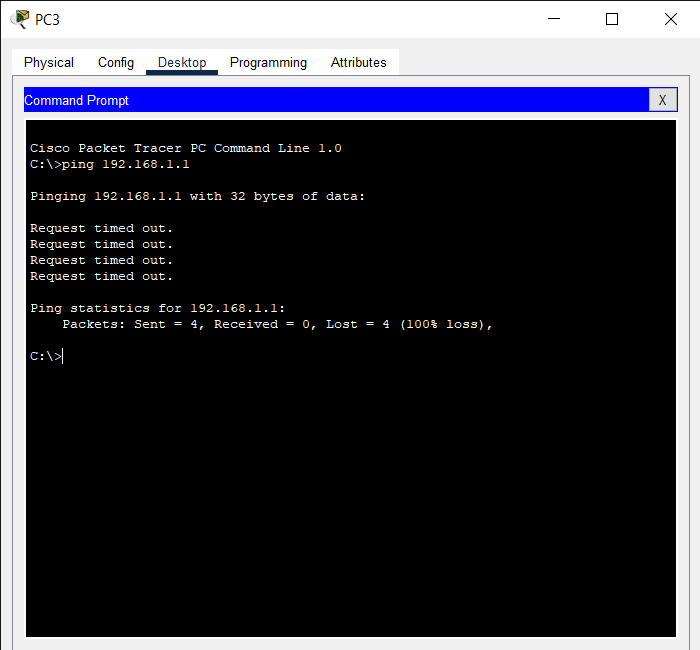
بر روی PC ها به ترتیب کلیک کرده و در قسمت ip configuration آدرس ip را مشخص می‌کنیم. پس از وارد کردن آدرس ip سایر قسمت‌ها به طور خودکار پر می‌شوند. ( از آدرس های 192.168.1.1، 192.168.1.2 و ... استفاده می‌کنیم.) پس از انجام مراحل فوق به قسمت command prompt رفته و با کمک دستور ping تست می‌کنیم که ارتباط در شبکه برقرار شده باشد.







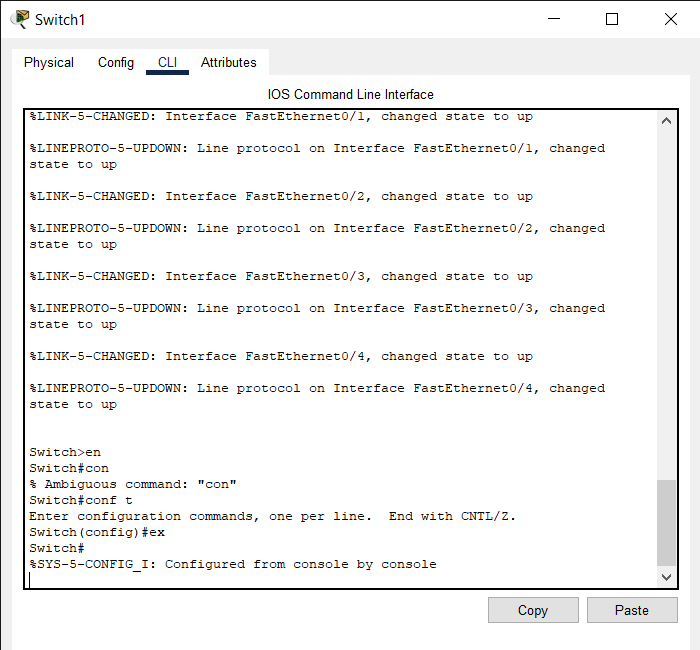
در صورتی که تمامی مراحل به درستی طی شده باشند، هنگامی که در قسمت command prompt از pc دیگر ping می‌گیریم ارتباط در شبکه برقرار می‌شود و پیام reply نمایش داده خواهد شد. اگر pc ها نتوانند ping یکدیگر را دریافت کنند به این معنا است که ارتباطی بین دو pc برقرار نشده و پیام request timeout نمایش داده می‌شود.

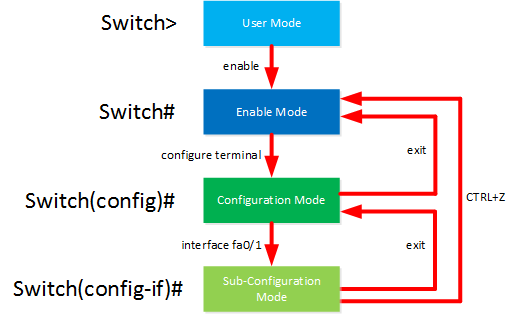


### switch

در ادامه switchهای لایه دو را بررسی خواهیم کرد. ابتدا 4 عدد PC انتخاب کرده، آدرس ip های هر کدام را مشخص و توسط کابل به switch2960 وصل می‌کنیم. پس از ping گرفتن از pcها و اطمینان از عملکرد صحیح آن‌ها بر روی switch کلیک کرده و محیط CLI را باز و شروع به نوشتن دستورات می‌کنیم(با زدن ؟ دستورات موجود نمایش داده می‌شود). محیط CLI دارای 3 نوع mode می‌باشد:

1. user mode: اولین mode که با زدن دکمه enter مشاهده می‌شود. (کمترین سطح دسترسی)
2. privilege mode: دومین mode که با تایپ en وارد شده و با # نشان داده می‌شود.
3. config mode: سومین mode که با دستور conf t وارد می‌شویم. (استفاده از ex برای بازگشت)

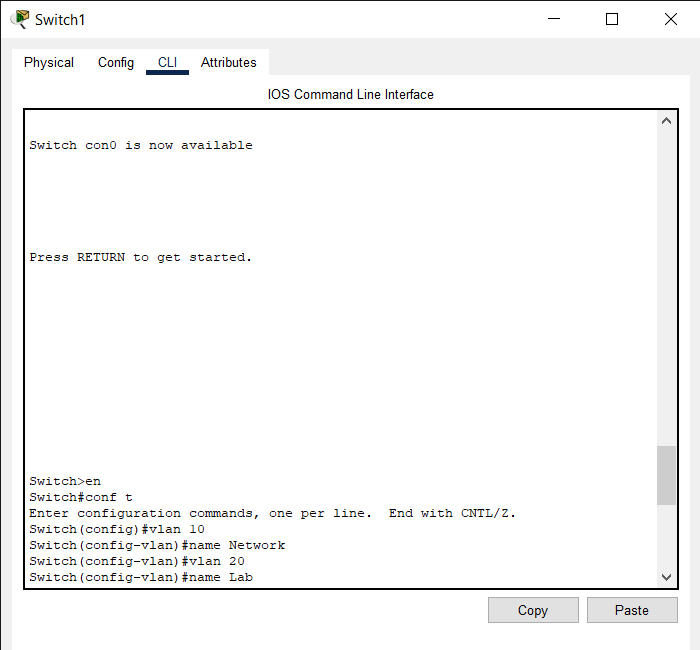




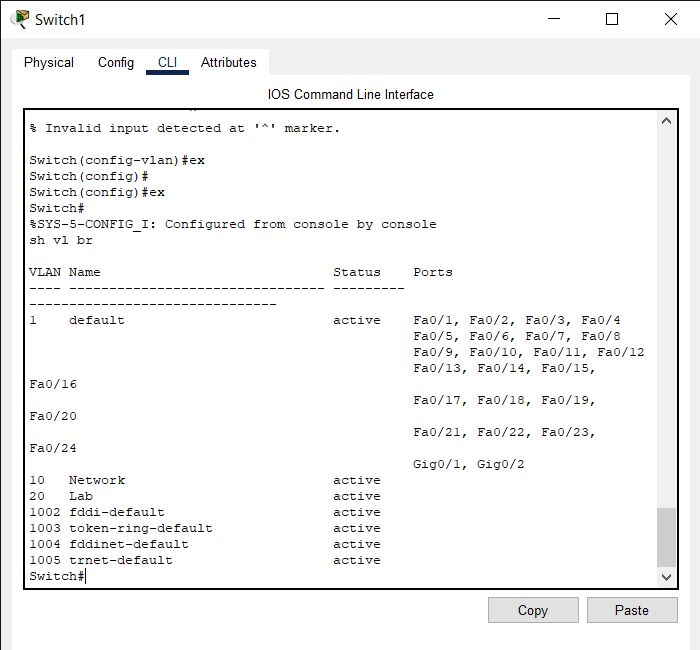
### VLAN

در مرحله بعد با مفهوم و نحوه تعریف VLAN آشنا خواهیم شد. virtual local area network یک اتصال مجازی است که چندین دستگاه و Node را از شبکه‌های محلی مختلف به یک شبکه منطقی متصل می‌کند. VLANها به مدیران شبکه اجازه می‌دهند تا Hostها را با یکدیگر گروه بندی کنند. برای مثال مدیر شبکه می‌خواهد که در یک سازمان، سیستم‌های 1 تا 10 به اطلاعات بخش X دسترسی داشته باشند اما سیستم های شماره 11 تا 20 به این اطلاعات دسترسی نداشته باشند. سیستم هایی که به اطلاعات یکسانی دسترسی دارند، در یک VLAN قرار گرفته و می‌توانند Ping یکدیگر را داشته باشند و داده را انتقال دهند.VLANها به دستگاه‌ها اجازه می‌دهند از کابل بندی شبکه فیزیکی به صورت اشتراکی استفاده کرده و در عین حال از تعامل مستقیم با یکدیگر جلوگیری کنند.

برای تعریف VLAN ابتدا باید وارد config mode شویم و شماره‌های توافقی 10، 20، 30، ... را خواهیم داد (توجه شود که هر شماره تنها می‌تواند به یک VLAN اختصاص داده شود). در ادامه برای هر کدام از VLANها name مورد نظر را تعریف می‌کنیم.

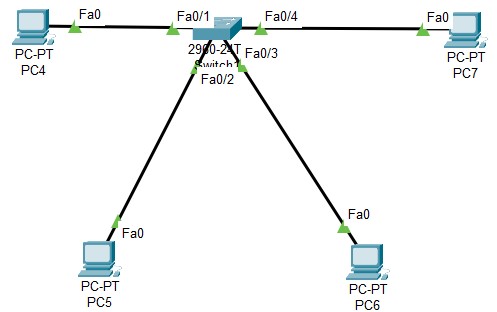


برای اطمینان از تعریف VLAN خود وارد user mode شده و دستور sh vl br را اجرا می‌کنیم. همان طور که مشاهده می‌شود اسم و شماره VLANهایی که مشخص کرده‌ایم نمایش داده شده است. active به این معنی است که VLANها فعال هستند و می‌توانند انتقال داده داشته باشند.

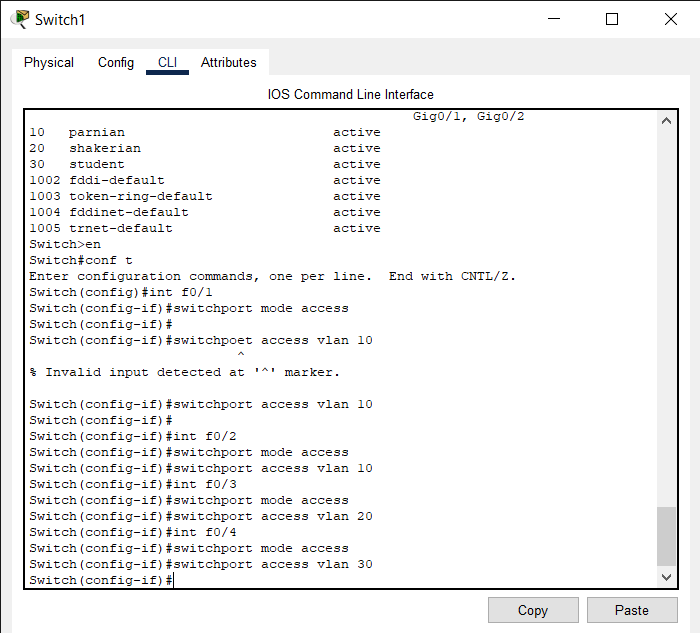


virtual local area network یک اتصال مجازی است که چندین دستگاه و Node را از شبکه های محلی مختلف به یک شبکه منطقی متصل می‌کند. switchها دستگاه‌های ارتباطی هستند که وظیفه انتقال داده‌ها بین دستگاه‌ها را به عهده می‌گیرند. هنگامی که بسته‌های اطلاعاتی از یک دستگاه به دستگاه دیگر ارسال می‌شود ممکن است به همزمانی با اطلاعاتی دیگر از دستگاه دیگر برخورد کند. در این صورت امکان از بین رفتن اطلاعات یا دیر رسیدن اطلاعات به دستگاه مقصد وجود دارد. در این موارد وجود سوئیچ‌ها کمک می‌کند تا اطلاعات با نظم و بدون از بین رفتن به مقصد خود برسند. switch پورت‌های مختلفی دارد که می‌توانیم هرکدام از بخش‌های مجزا یک سازمان را به این پورت‌ها که در vlan های switch ایجاد کرده‌ایم بدهیم.

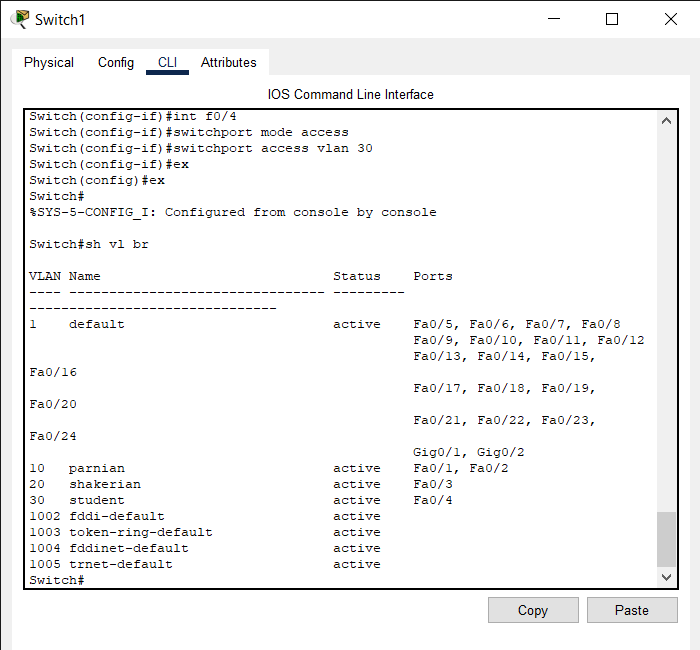
ابتدا 4 عدد PC یا laptop انتخاب کرده، و توسط کابل به switch2960 وصل می‌کنیم. بر روی PC ها به ترتیب کلیک کرده و در قسمت ip configuration آدرس ip را مشخص می‌کنیم. پس از انجام مراحل فوق به قسمت command prompt رفته و با کمک دستور ping تست می‌کنیم که ارتباط در شبکه برقرار شده باشد.

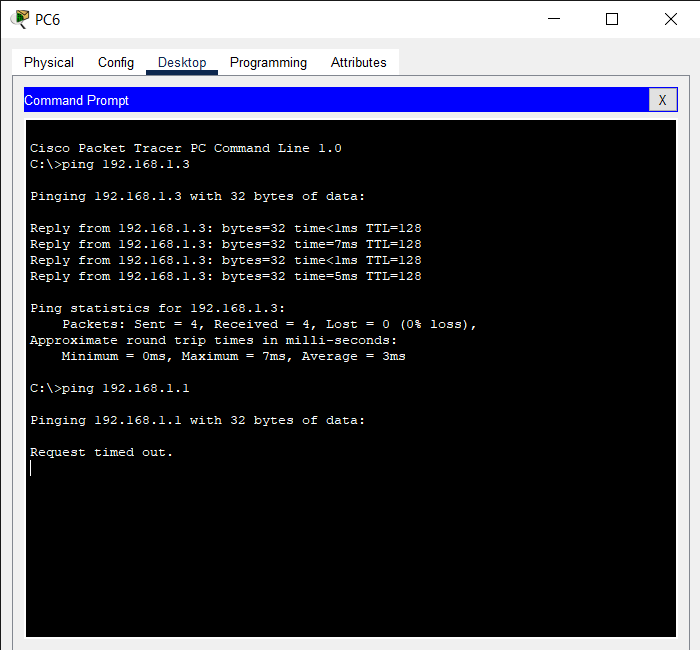


برای تعریف VLAN وارد config mode شده و شماره‌های توافقی را خواهیم داد. در ادامه برای آن name تعریف می‌کنیم و برای اطمینان از تعریف VLAN خود وارد user mode شده و دستور sh vl br را اجرا می‌کنیم. در ادامه می‌خواهیم PC‌ 4 و 5 در یک بخش مجزا قرار گرفته و به یکدیگر دسترسی داشته باشند اما PC‌ 6 و 7 به بقیه دسترسی نداشته باشند. طبق توضیحات فوق PC‌هایی که در یک VLAN قرار گرفته‌اند به اطالعات یکسانی دسترسی داشته و می‌توانندPing یکدیگر را داشته باشند ولی PC‌هایی که در این VLAN قرار ندارند، شبکه خارجی محسوب شده و نمی توانند به این اطالعات دسترسی داشته باشند. به این ترتیب با کمک دستورات زیر هرکدام از PC‌ها را به VLAN مخصوص خود داده و وقتی ping از pc شماره 6 بگیریم باید درست نشان دهد ولی برای pc شماره 4 را request timeout بزند.

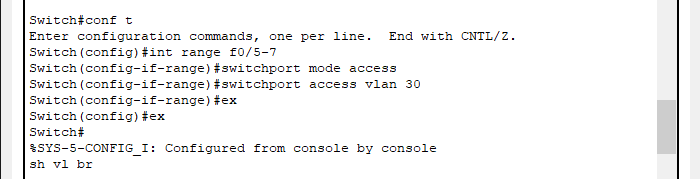


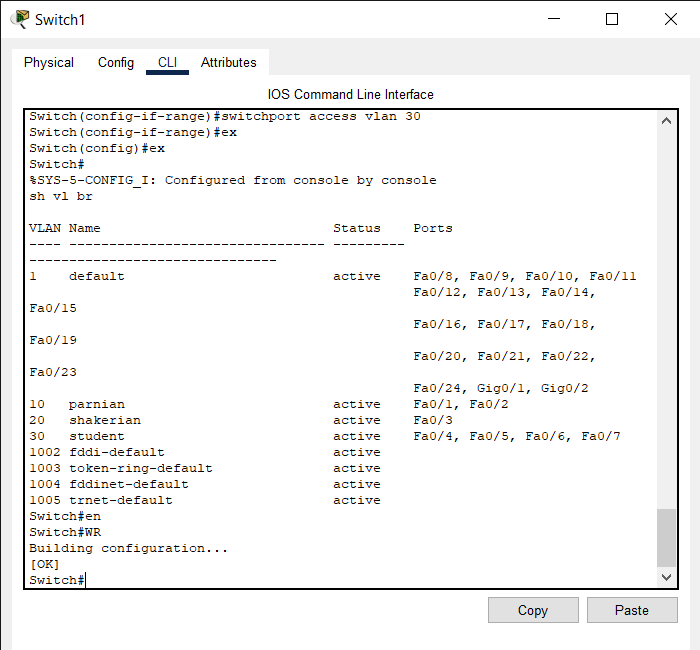
دستور switchport mode accessدر سوئیچ های سیسکو برای پیکربندی یک رابط به عنوان یک پورت دسترسی استفاده می‌شود تا مشخص کند که رابط باید به عنوان یک پورت دسترسی عمل کند، که تنها برای یک VLAN، ترافیک را حمل می‌کند.





حال اگر بخواهیم تعدادی از Portها، درون یک VLAN ببریم می‌توانیم از دستور range استفاده کنیم. دستور int range در سیسکو برای پیکربندی چندین رابط به طور همزمان استفاده می‌شود و به ما این امکان را می‌دهد تا به جای پیکربندی هر رابط به صورت جداگانه، پیکربندی را برای طیف وسیعی از رابط ها وارد کنیم. البته می‌توانیم هر کدام را تک به تک نیز در VLAN قرار دهیم اما وقت گیر خواهد بود. برای اعمال این دستور وارد config mode شده، دستور int range را وارد کرده و بازه port هایی را که می‌خواهیم درون یک VLAN مشخص قرار دهیم را وارد می‌کنیم. رنج Ip یا subnet، یک مجموعه از آی پی های عمومی(Public Ip) متوالی است. اندازه و تعداد range Ip را سابت نت مسک (Subnet Mask) تعیین می‌کند و تعداد آی پی ها را محدود می‌کند.

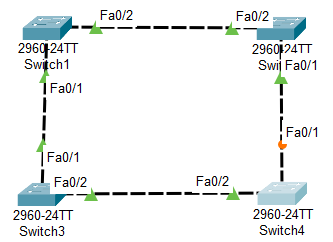




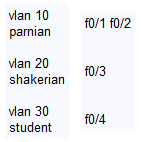
در آخر برای save تمام تغییراتی که در config اعمال کرده‌ایم دستور WR را در mode privilege وارد می‌کنیم.

### بهینه سازی

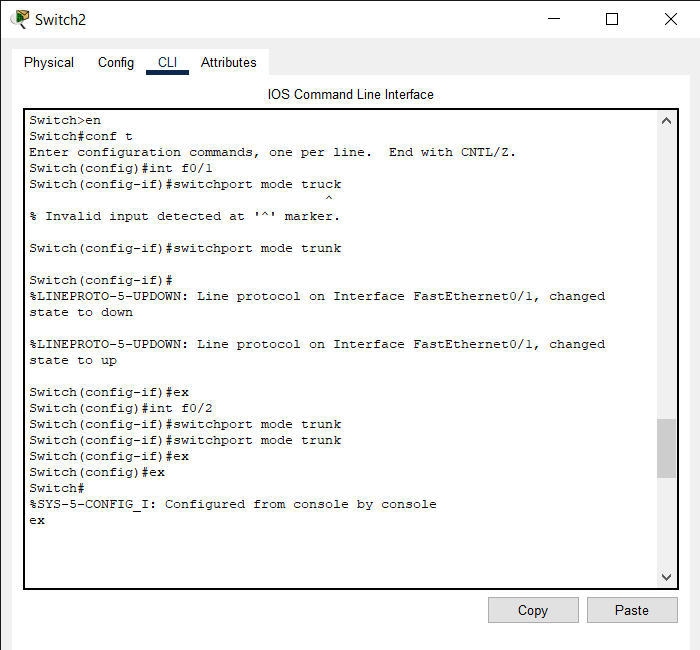
در ادامه سعی داریم که شبکه درون یک سازمان را بهینه کنیم. از آزمایش‌های گذشته دریافتیم که اگر نخواهیم برای هر بخش سازمان خود switch جدا بذاریم و port‌هایی را هدر دهیم باید از vlan استفاده کنیم و اگر بخواهیم در بخش‌هایی از vlan عملیاتی انجام دهیم باید برای تعریف آن‌ها، روی همه switch ها دستورات لازم را بزنیم. حال فرض کنید 10 بخش مجزا داریم؛ باید برای هر قسمت تعریفات را تک به تک اعمال کنیم در صورتی که تعریف آن‌ها روی هر تعداد switch که داریم برای هه 10 تا vlan مشترک است. پس بهتر است این عمل مشترک را فقط یکبار انجام دهیم. جدا از آن اگر در شبکه تعدادvlan ها تغییر کند، باید روی همه switchها موارد نخواسته را پاک کرده و دقت کنیم که درست انجام دهیم چون ممکن است سیستم کل شبکه خراب شود. برای انجام آزمایش ابتدا طبق تصویر شبکه خود را با کمک 4 عدد switch خواهیم بست.



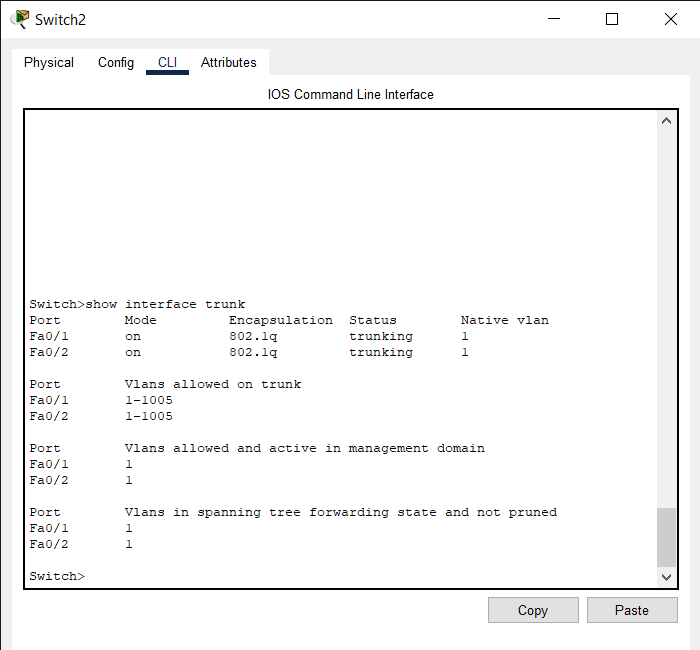
به منظور ارتقاء نظم و خوانایی با استفاده از place note مشخصات هر یک از VLAN‌ها را درج می‌کنیم.



پس از وصل switchها با کابل auto باید trunk هر پورت switch را مشخص کنیم. به این منظور به ترتیب روی هر switch زده و دستورات زیر را برای faهای خود در configuration mode وارد می‌کنیم. دستور "switchport mode trunk" برای پیکربندی یک رابط به عنوان پورت ترانک در سیسکو استفاده می شود تا مشخص کند که رابط باید به عنوان یک پورت ترانک عمل کرده و ترافیک داده را برای چندین VLAN حمل کند.



برای اطمینان از صحت عملیات خود دستور sh vl br را وارد می‌کنیم یا موس را روی هر switch نگه داشته تا برای دو پورت تعیین شده کلمه up را ببینیم.

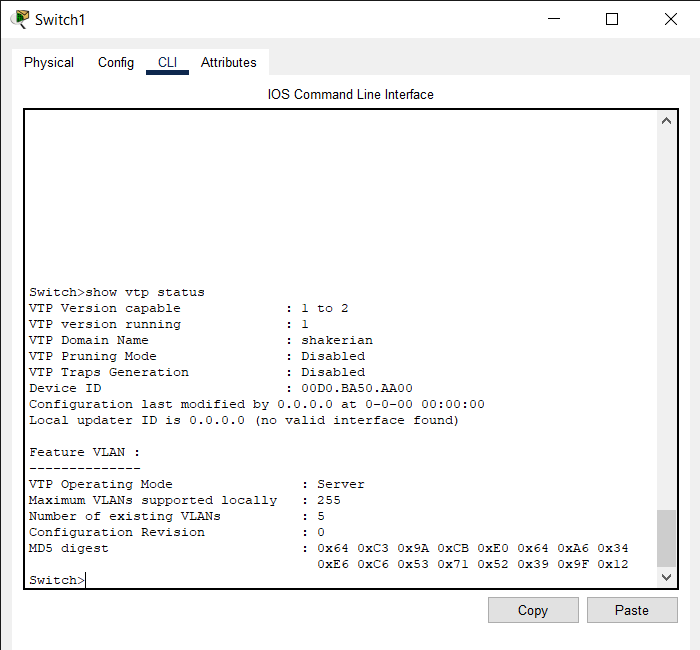
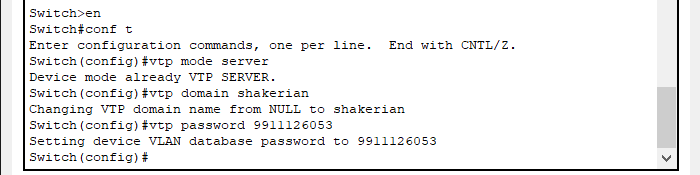


### VTP

پس از فعال کردن پورت ها باید نوع switchهای شبکه را مشخص کنیم. یکی از switchها به عنوان server و بقیه client در نظر گرفته می‌شوند. برای مشخص کردن نوع هر switch از دستورات VTP استفاده می‌کنیم. (نام domain و password متغییر است.)

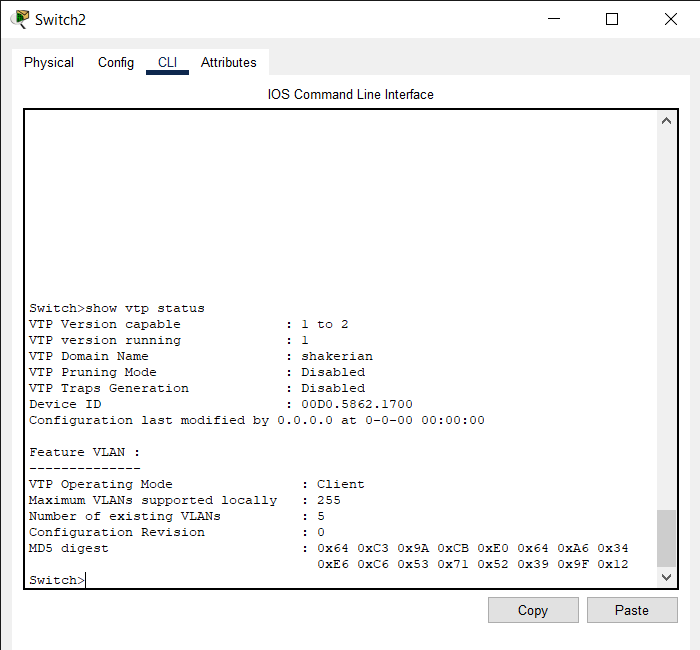
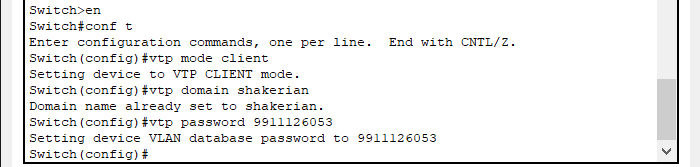
دستورات برای مشخص نمودن server:

1. vtp mode server: با این دستور یکی از سوئیچ ها را تبدیل به سرور می‌کنیم.
2. vtp domain name: با این دستور برای دامنه نام موردنظر را قرار می‌دهیم
3. vtp password xxx: با این دستور رمز موردنظر را مشخص می‌کنیم.

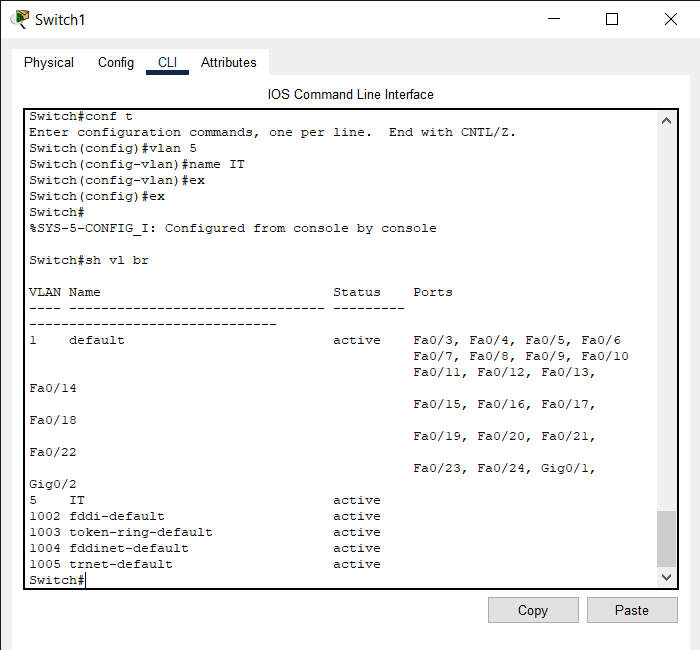


3 switch باقی مانده را تبدیل به client می‌کنیم. دستورات برای مشخص نمودن client مشابه دستورات ذکر شده در بالا می‌باشند:

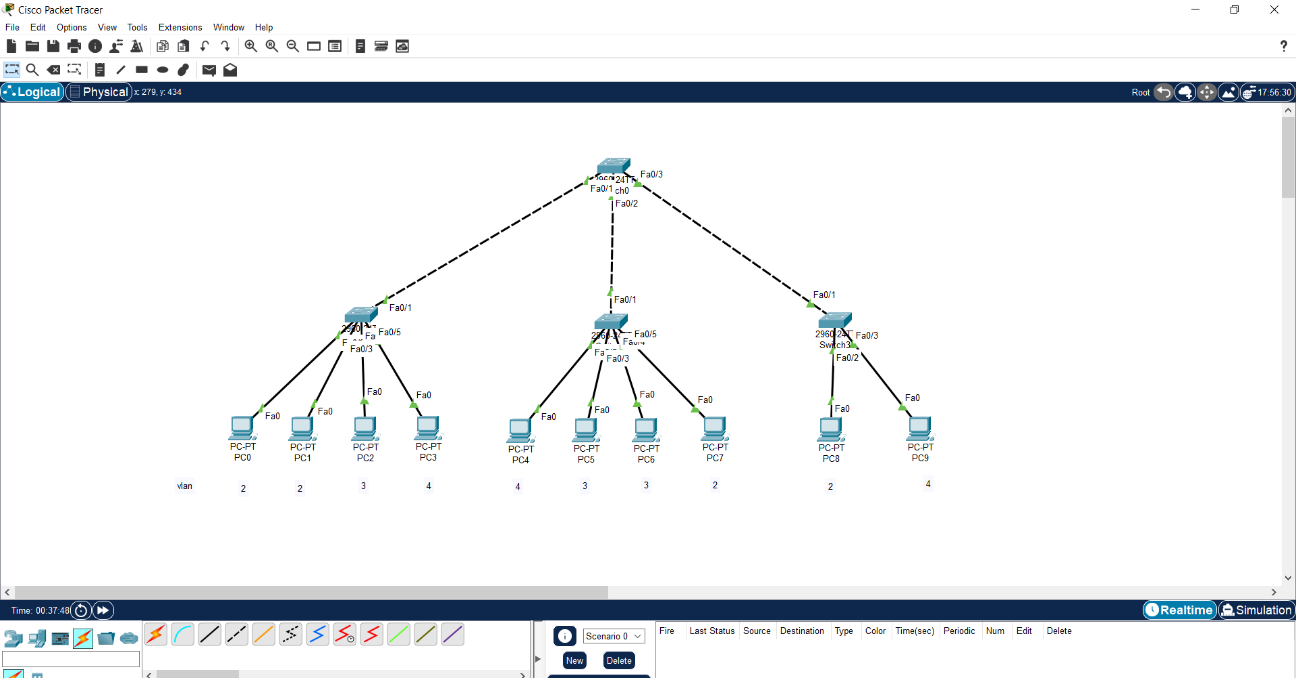
1. vtp mode client: با این دستور سوئیچ ها را تبدیل به کلاینت می‌کنیم.
2. vtp domain name: با این دستور برای دامنه نام موردنظر را قرار می‌دهیم
3. vtp password xxx: با این دستور رمز موردنظر را مشخص می‌کنیم.



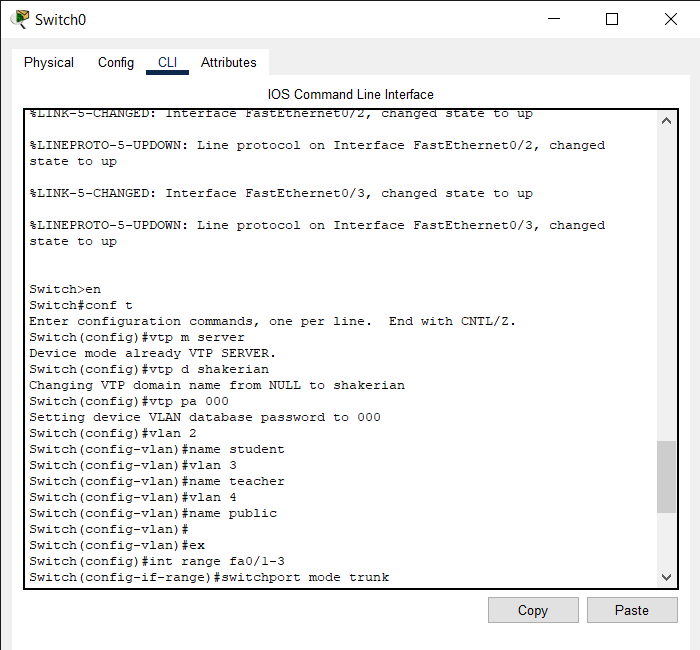
در آخر برای آنکه مطمئن شویم که شبکه ما درست کار می‎کند یک تست انجام می‌دهیم. برای تعریف vlan ها لازم نیست در همه switchها دستورات را واردکنیم بلکه تنها در سوئیچ سرور دستورات را اعمال خواهیم کرد. برای تست به vlan یک اسم و شماره می‌دهیم و سپس در یکی از switchها sh vl br خواهیم گرفت. اگر کلاینت و سرورها را درست به هم متصل کرده باشیم و شبکه درست کار کند نام و شماره vlan وارد شده را باید نشان دهد.



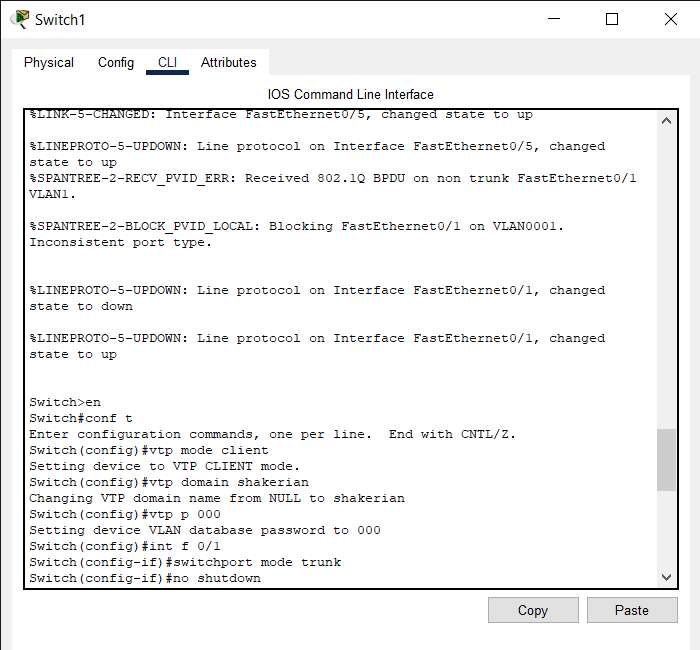
در آزمایش قبل که نمونه ساده تری از مدل VTP را مشاهده کردیم یکی از switchها را به server و 3 تای دیگر را به client تبدیل کردیم. این روش باعث می‌شد که دیگر لازم نباشد Vlanهای موجود برای هر switch را تعریف کنیم بلکه هر Vlan سرور برای بقیه کلاین ها نیز قابل مشاهده باشد. در آزمایش چهارم سعی داریم که نمونه پچیده تری از شبکه‌های متشکل از switchها و Vlanها را بسازیم. به این منظور از 4 switch استفاده کرده که switch اولی server و سه‌تای دیگر client می‌باشند. به دوتا کلاینت اول 4 pc و به کلاینت سوم 2 عدد pc متصل میکنیم تا شبکه‌ای به شکل زیر تشکیل گردد:

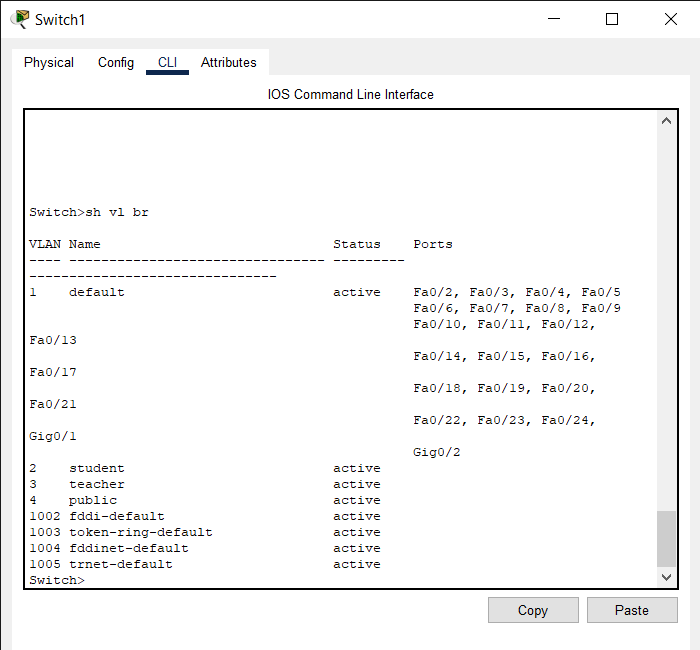
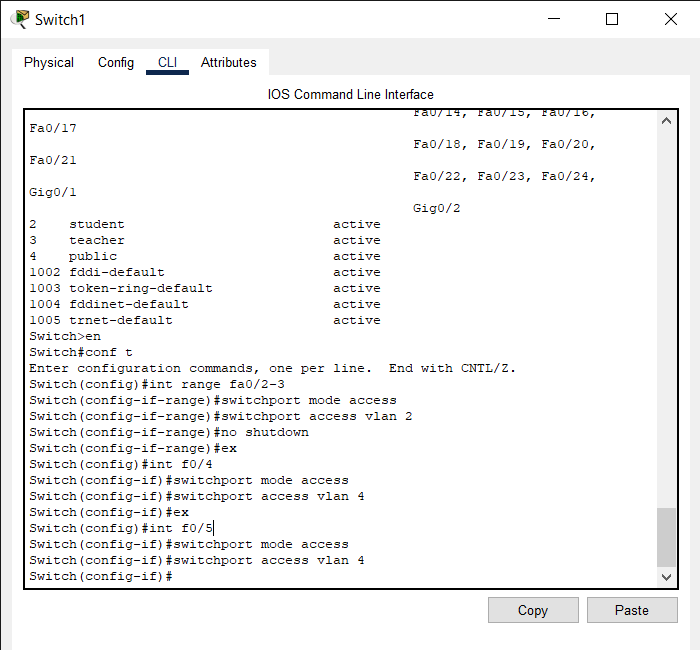


وارد CLI switch می‌شویم. وارد مود config شده و switch را طبق دستورات نوشته شده در آزمایش سوم به سرور تبدیل می‌کنیم. Domain و رمز را هم برای آن تعریف خواهیم کرد. سپس vlanهای خود را تعریف کرده و در ادامه پورت‌ها را مشخص می‌کنیم. از مود config خارج شده و trunk سرور را اعمال می‌کنیم در آخر no shutdown را خواهیم زد تا از خاموش شدن پورت‌ها جلوگیری کنیم:

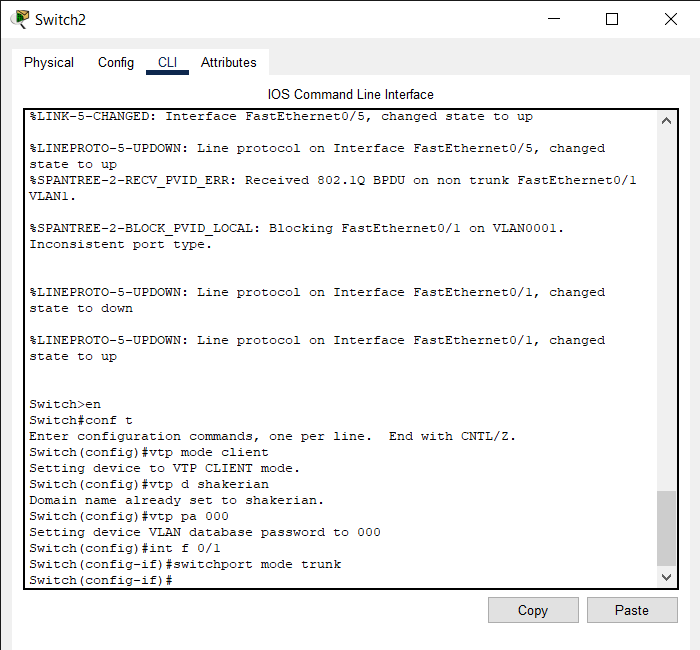


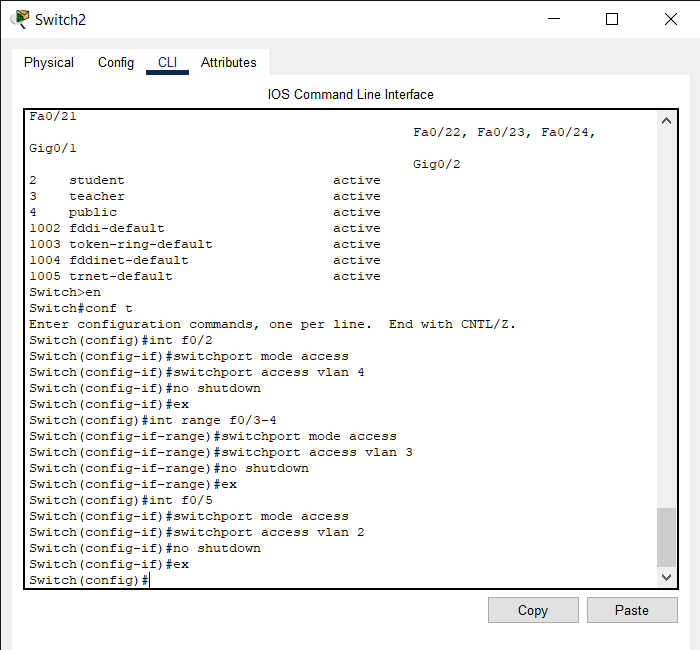
حال وارد switch کلاینت شماره 1 می‌شویم. تمام مراحل فوق را برای این switch هم انجام می‌دهیم ولی دقت شود که switch کلاینت ست شده و در mode user چک شود که تمام تغییرات اعمال شود:



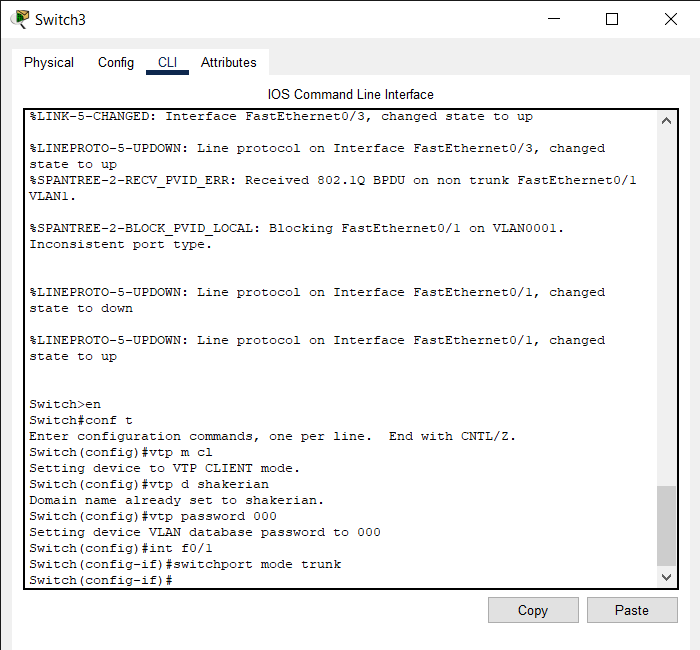


وارد switch کلاینت شماره 2 می‌شویم و تمام مراحل فوق را برای این switch هم انجام می‌دهیم:

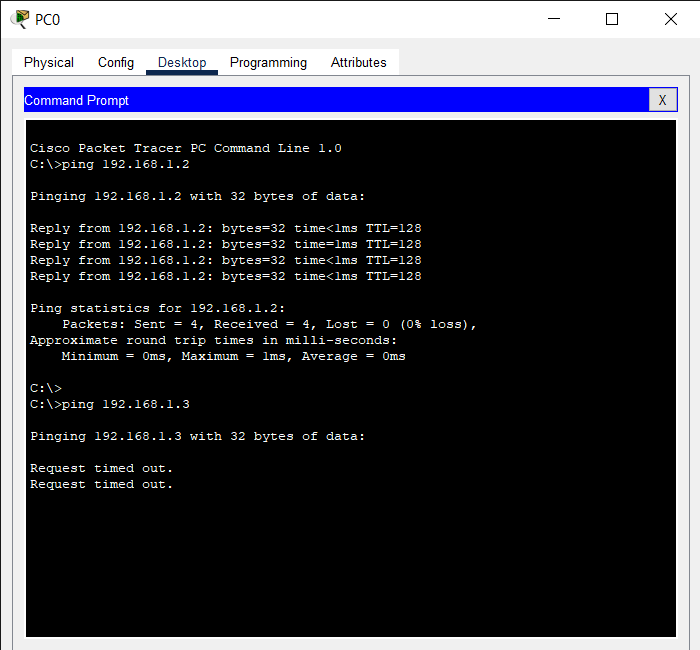




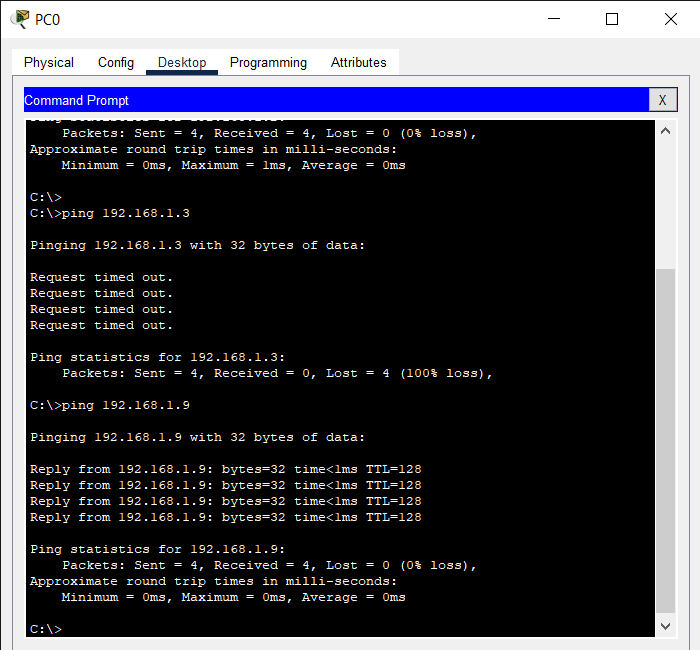
وارد switch کلاینت شماره 3 که آخرین switch است شده و تمام مراحل فوق را برای این switch هم انجام می‌دهیم:



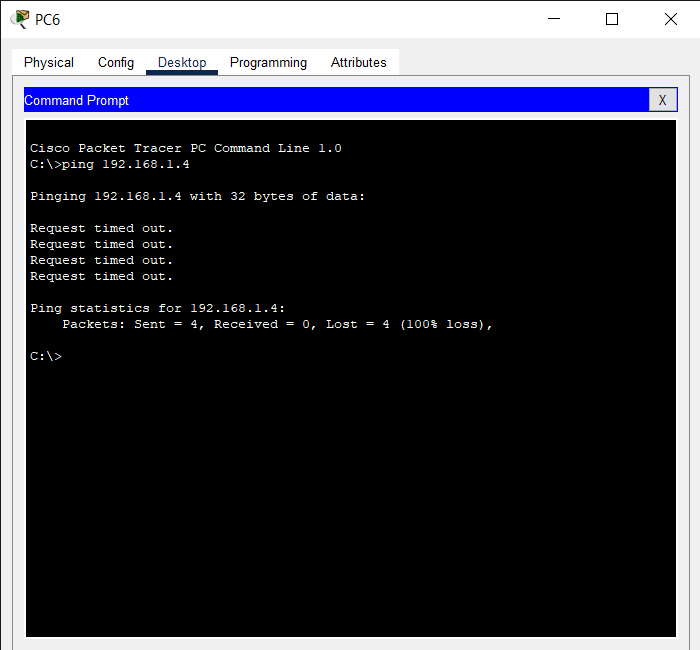
به Pcها آدرس IP می‌دهیم. همه Pcهایی که در یک Vlan هستند باید ping هم را داشته باشند. PCهایی که در یک Vlan نیستند نیز نباید ping هم را داشته باشند. طبق خواسته آزمایشpc0 و pc8 باید ping هم را داشته باشند. ولی pc6 و pc3 نباید ping هم را داشته باشند.



پس بررسی برای اطمینان از صحت شبکه خود، pcهای مورد نظر را آزمایش می‌کنیم در ping بین pc0 و pc8 با آدرس ip 192.168.1.9 همان طور که مشاهده می‌شود replyداده است چون در یک VLAN می‌باشند.



اما در ping بین pc6 و pc3 با آدرس ip 192.168.1.4 همان طور که مشاهده می‌شود request timeout داده است چون در دو VLAN متفاوت می‌باشند.



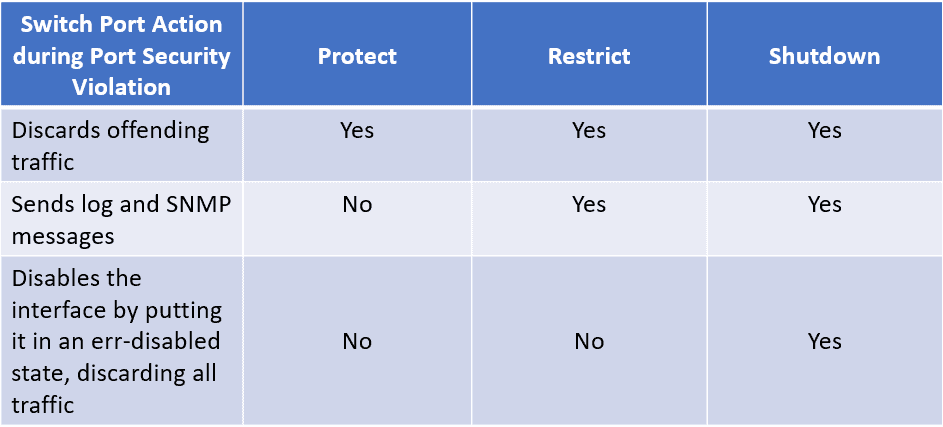
### امنیت شبکه

در ادامه مسائل امنیت شبکه را مورد بررسی قرار خواهیم داد. در امنیت شبکه چه رویکرد حمله و یا رویکرد دفاع داشته باشیم، اولین مسئله‌ای که مورد توجه قرار می‌گیرد بحث امنیت فیزیکی شبکه است. به عنوان مثال یک switch را تصور کنید که یه فلش مخرب به آن وصل شود و در شبکه یه سازمان ایجاد اختلال کند؛ پس برای جلوگیری از ایجاد این قبیل مشکلات، در ایمن سازی شبکه اولین گام افزایش امنیت فیزیکی می‌باشد چرا که اگر امنیت شبکه یک سازمان ضعیف باشد به هنگام حملات مخرب، شبکه دچار مشکالت مختلفی مانند از کار افتادن سیستم سازمان، افشاء اطالعات محرمانه و یا دستکاری در داده‌ها می‌شود.

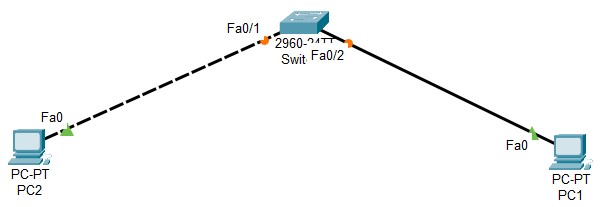
### port security

در این راستا شرکت سیسکو شرایط و قابلیتی را به نام port security ایجاد کرده است. به این صورت هر device که به پورت وصل می‌شود ادرس مک مختص به خود را دارد، حال مسئول شبکه به پورت‌ها دستور می‌دهد فقط آدرس مک‌های مشخصی trust هستند. یعنی می‌دانیم در شبکه، این سیستم‌ها اجازه وصل شدن را دارند. بدین ترتیب از دسترسی دستگاه های غیر مجاز به شبکه و ایجاد مشکالت ناشی مانند سرقت اطالعات و آلوده کردن شبکه جلوگیری می‌کند. روشی دیگر نیز وجود دارد که به جای آدرس مک سیستم‌ها پورت‌ها را به گونه‌ای برنامه‌ریزی کنیم که ادرس مک هر تعداد device که به پورت وصل شد را یاد گرفته و اگر جز این deviceها هر device دیگری به پورت وصل شد، آن‌ها را قبول نکند. اگر سیستم‌های جدید بخواهند وصل شوند باید آدرس مکشان ابتدا learn و سپس ذخیره شود. در گام بعدی روی device هایی که trust نیستند چه عملیاتی انجام دهند؟ در Switchهای سیسکو 3 روش مقابله با این مشکلات وجود دارد:

1. Shutdown: اگر آدرس مکی وارد پورت شود که trust نباشد پورت خاموش شده و وظیفه مدیر شبکه است تا آن را درست کند.
2. روش دوم پورت رو Shutdown نمی‌کند بلکه پورت همچنان روشن بماند تا مرتب مجبور به کانفیگ نباشد اما data را که از مک ناشناس گرفته است drop کند.
3. روش آخر data را drop کند و در ادامه log بیندازد تا ادمین شبکه بتواند بخواند.



در ادامه شبکه‌ای مانند شکل زیر متشکل از یک switch و 2 عدد pc خواهیم ساخت:



### دستورات

ابتدا باید mode پورت ها را از dynamic به Access تغییر می‌دهیم. وارد مود config شده و دستور زیر را وارد می‌کنیم:

Switch(config-if)#switchport mode access

سپس port security را فعال خواهیم کرد:

Switch(config-if)#switchport port-security

در ادامه تعداد max دستگاه‌های مجازی که می‌خواهیم به پورت دهیم را مشخص کرده و سپس آدرس‌های مک را تعیین می‌کنیم که به دو صورت انجام می‌شود:

Switch(config-if)#switchport port-security maximum 1

1)Switch(config-if)#switchport port-security mac-address

2)Switch(config-if)#switchport port-security mac-address sticky

(اگر pc قبلاً به پورت سوئیچ وصل شده باشد و سپس فرمان max پورت را پیکربندی کنیم، آدرس MAC رایانه فعلی متصل در تعداد max گنجانده خواهد شد. بنابراین، نمی‌توان دو pcدیگر را بدون تجاوز از حد مجاز وصل کرد بلکه فقط می‌توانیم یک pc دیگر را بدون ایجاد نقض امنیتی متصل کنیم.)

(در حالت sticky نیاز به وارد کردن آدرس مک نیست زیرا خود سوئیچ آدرس را از روی بسته دریافتی برمیدارد.)

حال 3 حالتی را که در ابتدای داک اشاره کرده‌ایم مشخص می‌کنیم (در اینجا گزینه shutdown را انتخاب می‌کنیم):

Switch(config-if)#switchport port-security violation ?

1)Protect

2)Restrict

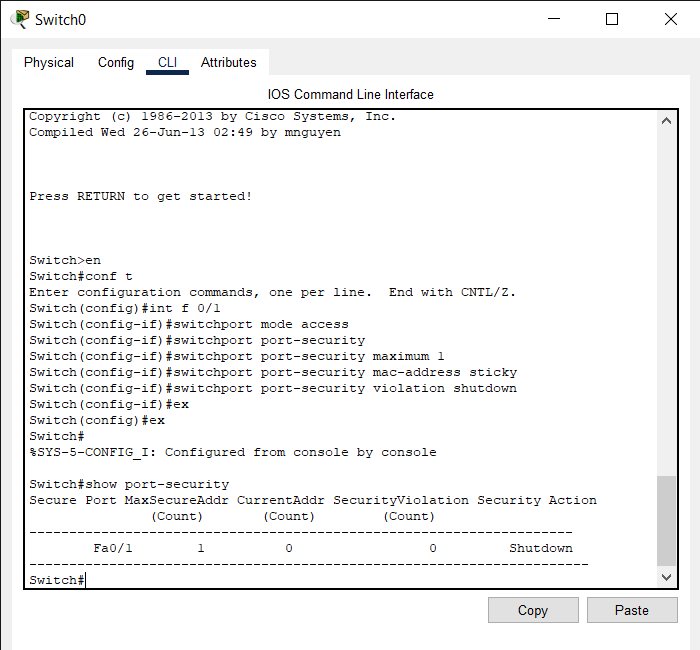
3)Shutdown

حالت shutdown، درگاه switch را در حالت غیرفعال کردن خطا در هنگام وقوع نقض امنیتی قرار می‌دهد:

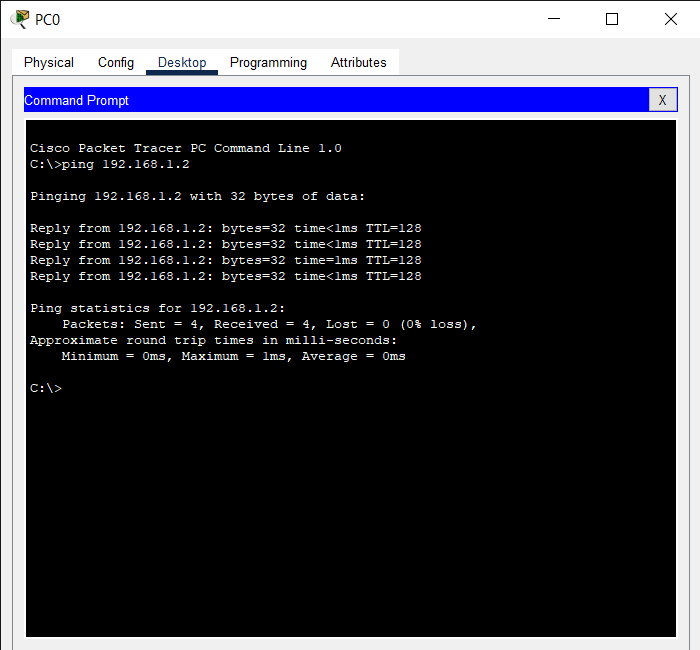
1. Detection of Violation: نقض امنیتی زمانی رخ می‌دهد که تعداد آدرس‌های MAC در یک پورت از حداکثر پیکربندی بیشتر شود، یا زمانی که یک دستگاه غیرمجاز تلاش کند از طریق پورت به شبکه متصل شود.
2. Error-Disabled State: پس از تشخیص نقض، switch بلافاصله پورت را در حالت غیرفعال خطا قرار داده و تمام ترافیک به و از آن را متوقف می کند.
3. Logging and Notifications: switch پیامی را ایجاد می‎‌کند تا نشان دهد که پورت به دلیل نقض امنیتی بسته شده است. این گزارش به مدیران شبکه کمک می‌کند تا علت نقض را تشخیص دهند.
4. Recovery: مدیر شبکه باید به صورت دستی پورت را با استفاده از دستورات خاموش و بدون خاموش کردن دوباره فعال کند. در صورت پیکربندی، switch می‌تواند به طور خودکار سعی کند پورت را از حالت غیرفعال پس از یک دوره مشخص بازیابی کند.

در آخر جهت مشاهده و بررسی تغییرات اعمال شده از دستور زیر استفاده می‎کنیم:

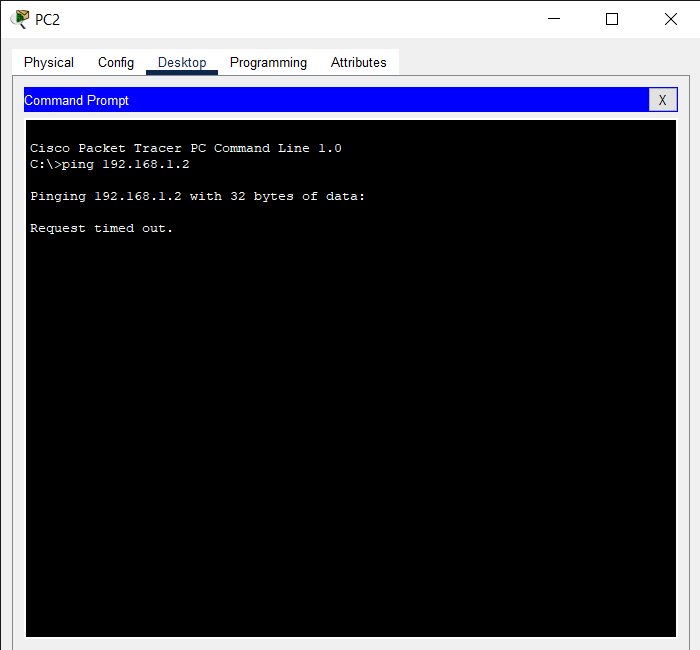
Switch#show port-security



حال اگر یک pc به switch وصل کنیم و آدرس ip دهیم و ping بگیریم آدرس مک را learn کرده و نمایش خواهد داد.

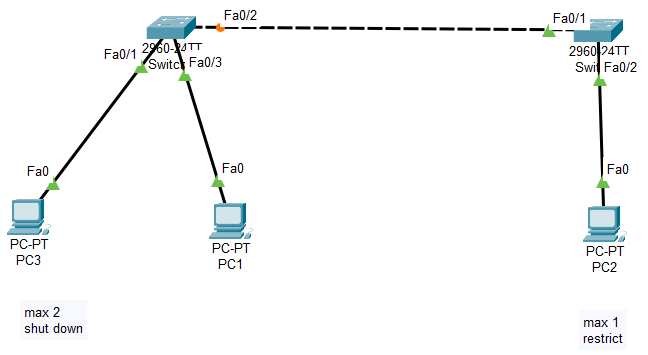


ولی اگر pc را پاک کنیم و یک Pc جدید قرار دهیم و دوباره Ping بگیریم request timeout می‌دهد.

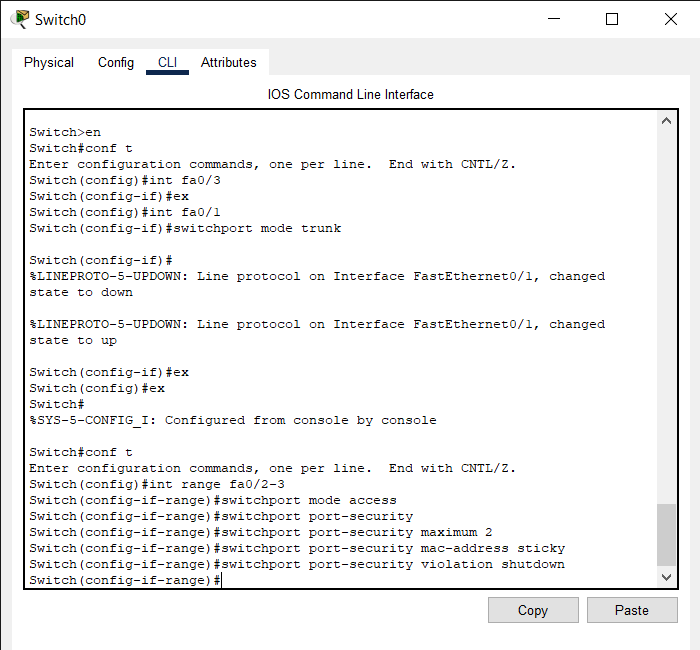


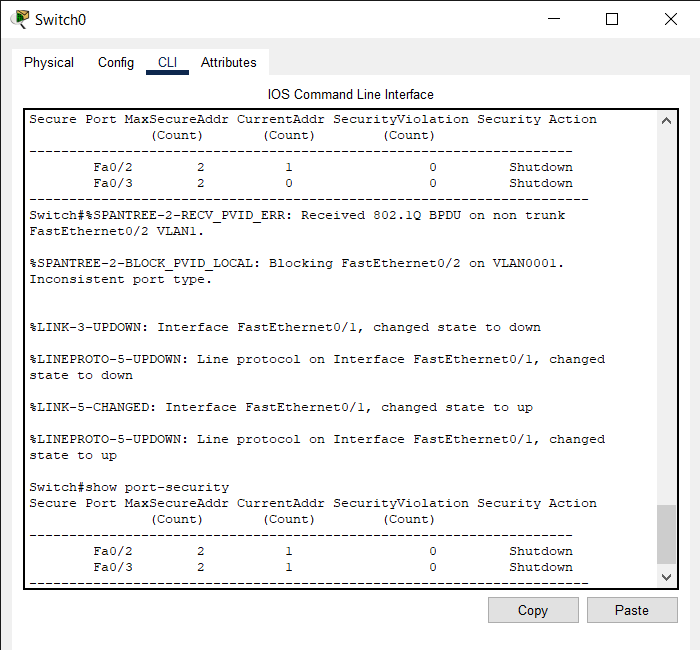
### Shutdown and Restrict

حال برای به کارگیری مفاهیم فوق سناریو زیر را خواهیم ساخت:

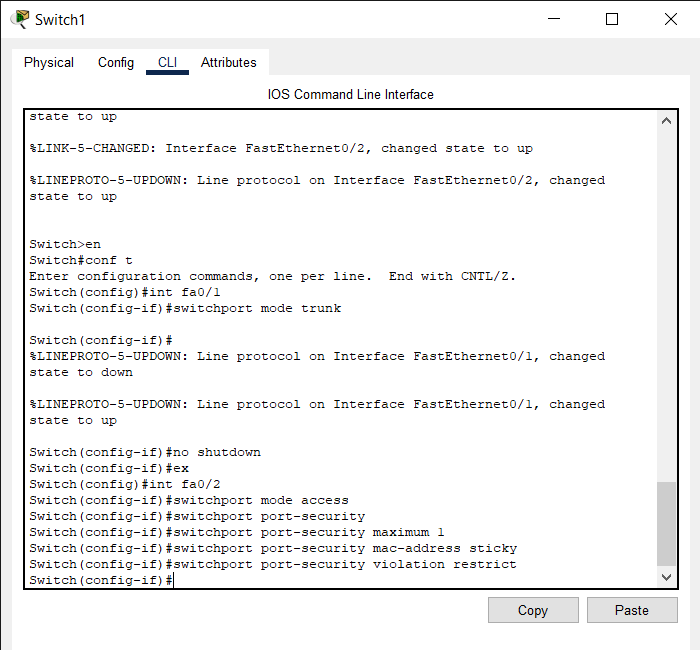


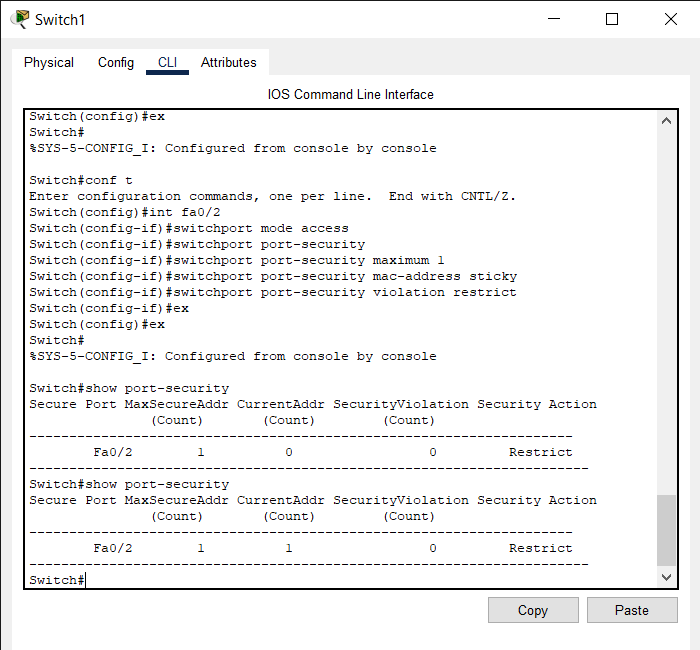
ابتدا پورت trunk را برای switch فعال کرده تا ارتباط بین pcها دو طرف سوئیچ برقرار شود. سپس مقدار max که می‌خواهیم به switch وصل شود را تعیین می‌کنیم. switch آدرس‌های مک را به روش sticky learn کرده و در صورت ورود یک pc خارجی که از پیش تعیین نشده است shutdown خواهد شد.



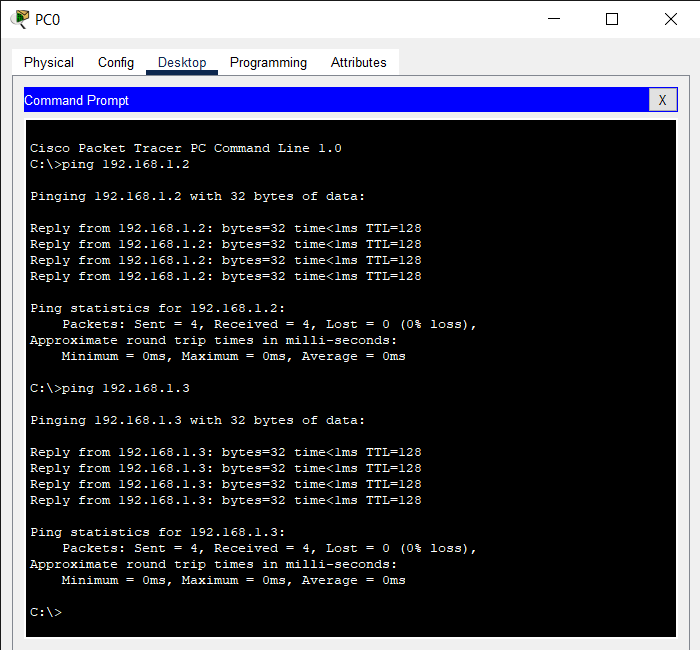


تمامی مراحل فوق را برای switch دوم نیز اعمال خواهیم کرد با این تفاوت که مقدار max که برای این switch تعیین می‎کنیم 1 خواهد بود، همچنین حالت دفاعی که به هنگام ورود یک سیستم ناشناخته خواهد گرفت از نوع restrict تنظیم می‌شود.

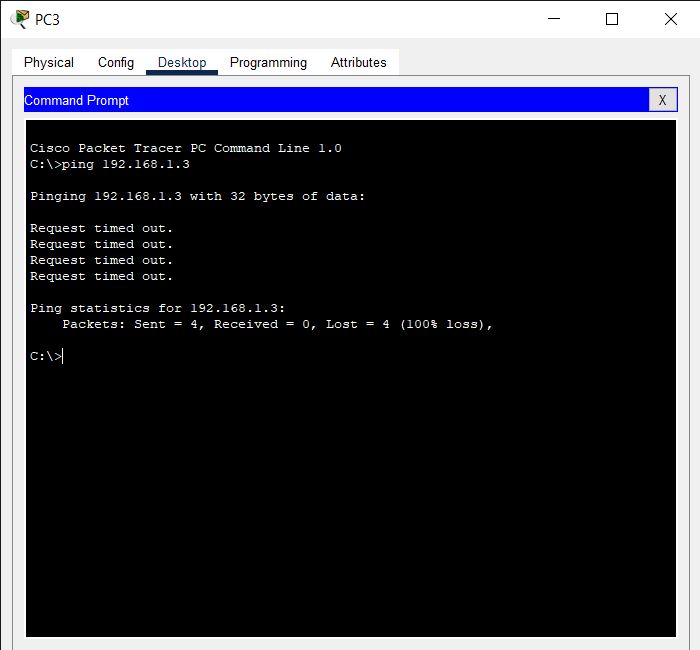




حال از pc0 با آدرس ip 192.168.1.1 به pc1 و pc2 با آدرس ip 192.168.1.2 و 192.168.1.3 ping گرفته و باید به درستی کار کند و پیام reply را نشان دهد.



بعد از اطمینان از صحت شبکه خود حالا pc0 را حذف کرده و pc جدید را به switch اول وصل می‌کنیم و دوباره از pc2 ping خواهیم گرفت که باید request timeout را نشان دهد زیرا آدرس مک سیستم‌های ورودی از تعداد max که برای switch تعیین کرده بودیم بیشتر خواهد شد.



### Router

در آزمایش سری ششم مبحث Router را مورد بررسی قرار خواهیم داد. در شبکه مسیریاب یاRouter دستگاهی از تجهیزات رایانه‌ای است که بسته‌های داده را در یک شبکه برای رسیدن به مقصدشان، هدایت می‌کند. مسیریابی در لایه سوم مدل مرجع OSI رخ می‌دهد. Router جهت اتصال دو یا چند شبکه محلی به هم یا اتصال چندین خط شبکه بزرگ به هم مورد استفاده قرار می‌گیرند و می‌تواند انواع مختلف شبکه را به هم وصل کند.

Static routing

Static routing یا مسیریابی استاتیک نوعی از مسیریابی است که دستگاه روتر با استفاده از Routeهایی که در Routing Table آن دارد و بصورت دستی در روتر Learn یا تعریف شده است بسته اطلاعاتی را به سمت مقصد هدایت میکند. در بسیاری از موارد static routeها به صورت دستی توسط مدیر شبکه در Routing Table روتر پیکربندی میشوند. بر خلاف مسیریابی داینامیک یا Dynamic routing مسیریابی استاتیک ثابت بوده و تا زمانیکه تغییری در ساختار فیزیکی شبکه (مانند اضافه شدن یا حذف شدن یک روتر از شبکه) بوجود نیامده است بدون تغییرات باقی می‌مانند.

مزایای:

1. از static routing می‌توان برای تعیین یک مسیر پیش‌فرض خروج بسته اطلاعاتی در صورت نبود آدرس مقصد آن بسته در Routing Table روتر استفاده کرد.
2. Static routing را میتوان زمانی که Dynamic routing در دسترس نباشد استفاده کرد به این معنا که یک Backup routing یا بهتر است بگوییم به عنوان یک مکمل استفاده کرد.
3. از static routing میتوان به عنوان یک کمک برای انجام عملیات Routing از یک پروتکل مسیریابی به پروتکل مسیریابی دیگر بهره برد (Routing Redistribution)

معایب:

1. Human error: در بسیاری از موارد static route ها بصورت دستی در روتر تعریف می‌شود که این خود مستعد بروز اشتباهات فردی است. اگر تنها یک Route به اشتباه در روتر وارد شود عملیات مسیریابی در کل شبکه از کار می افتد.
2. Fault toleranc: مسیریابی استاتیک از قابلیت fault tolerant یا تحمل خرابی پشتیبانی نمیکند. به این معنا که اگر یکی از روترها در شبکه خراب شود یا تغییری در ساختار فیزیکی شبکه ایجاد شود دیگر ترافیک قابل مسیریابی در شبکه نمیشود. در نتیجه شبکه غیر قابل استفاده شده و تا زمانیکه مشکل برطرف نشده باشد کل شبکه فلج خواهد ماند.
3. Administrative distance: مسیر های استاتیک بر dynamic route تقدم دارند.Static route ها ممکن است مانع از کارکرد مناسب پروتکل های مسیریابی شوند.
4. Administrative overhead: مسیر های استاتیک در هر روتر باید بصورت دستی پیکربندی شود. اگر تعداد روترها در شبکه زیاد باشد این پیکربندی ها مدت زمان زیادی صرف میکند.

در ادامه یک مثال از نحوه پیکربندی Static routing در روترهای سیسکو میزنیم. در محیط CLI یا خط فرمان روتر سیسکو ابتدا با دستور Enable وارد Enable mode شویم:

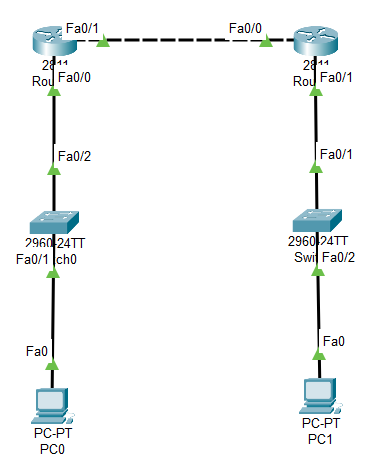
Router> enable

Router# configure terminal

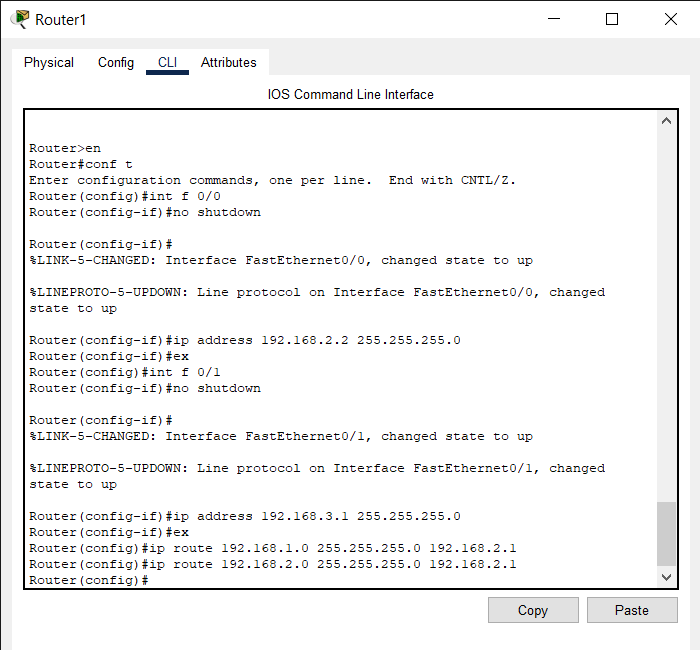
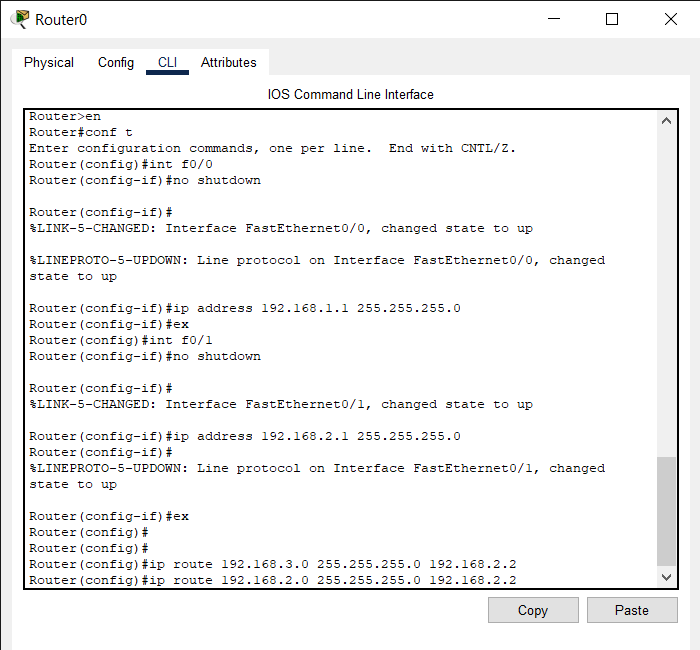
Router(config)# interface s0/0/0

Router(config)# ip route 10.10.20.0 255.255.255.0 192.168.100.1

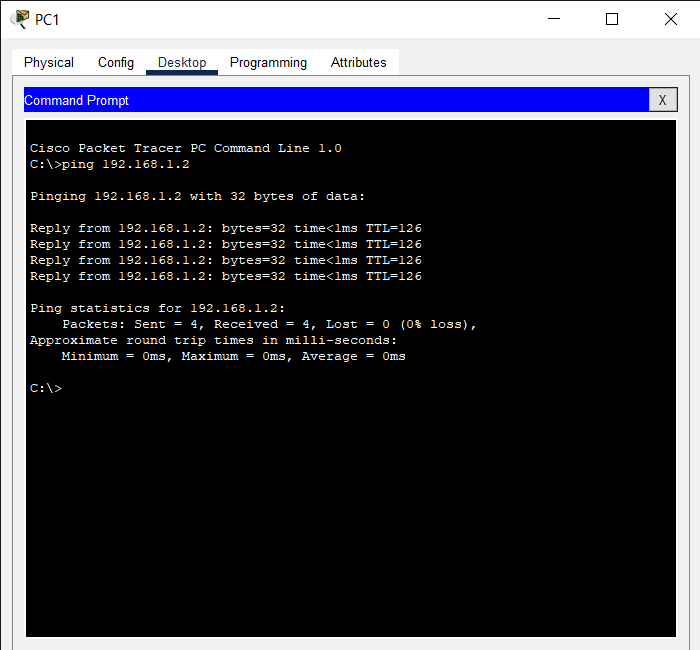
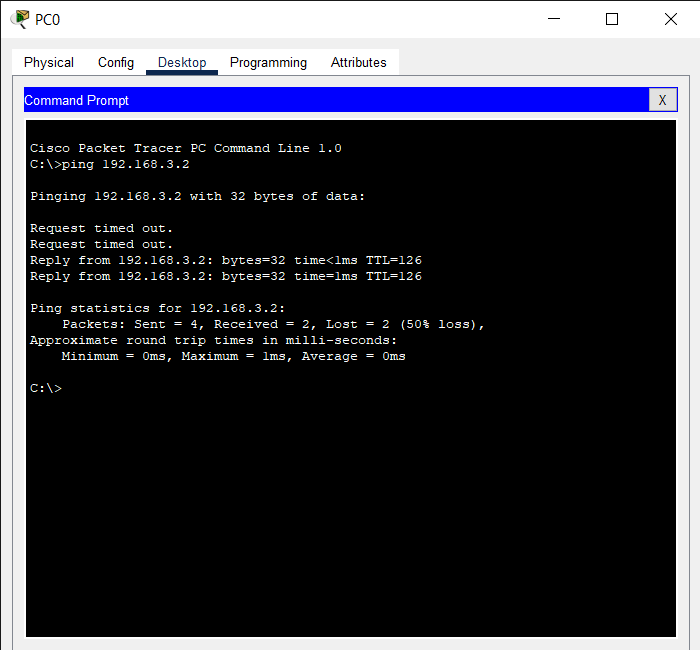
آدرس 10.10.20.0 همان آدرس Destination یا مقصدی است که بسته اطلاعاتی قصد رسیدن به آن را دارد و آدرس 192.168.100.1 آدرس IP اینترفیسی است که بسته های اطلاعاتی میتوانند از آن عبور کنند به این آدرس Default-Gateway نیز میگویند. برای آزمایش داده های خود یک شبکه به شکل زیر را خواهیم ساخت:



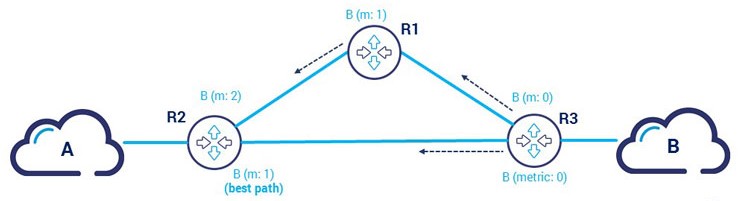
به pcها آدرس ip و gateway داده و در هر روتری تمام آدرس‌های شبکه ها را معرفی می‌کنیم. هر ناحیه در شبکه که با دایره قرمز مشخص شده‌اند رنج آدرس ip خود را دارند که باید در روتر شناخته شوند تا دو pc بتوانند با یکدیگر تبادل اطلاعات کنند. پس به ترتیب در هر روتر آدرس های gateway را مانند شکل زیر وارد خواهیم کرد.



سپس به ترتیب از pcها ping خواهیم گرفت که باید به درستی کار کند.



Routing Information به اختصار (RIP) یکی از خانواده پروتکل‌های مسیریابی IP است که برای توزیع اطلاعات مسیریابی در یک سیستم Autonomousطراحی شده است. RIP یک پروتکل distance-vector می‌باشد. در یک پروتکل مسیریابی vector، روترها اطلاعات دسترسی به شبکه را با نزدیکترین همسایگان خود مبادله میکنند. به عبارت دیگر، روترها مجموعه address prefixes را که می‌توانند به آن‌ها برسند و آدرس هاپ بعدی که برای رسیدن به آن مقصد باید ارسال شود را به یکدیگر ارسال می‌کنند. هر روتر جدول مسیریابی خود را با لیستی از شبکه‌های متصل به خود راه اندازی می‌کند.



به صورت دوره‌ای، هر روتر کل محتویات جدول مسیریابی خود را در تمام اینترفیس های فعال شده با RIP تبلیغ می‌کند. هر زمان که یک روتر RIP چنین تبلیغاتی را دریافت می‌کند، تمام مسیرهای مناسب را در جدول مسیریابی خود قرار می‌دهد و شروع به استفاده از آن برای ارسال بسته ها می‌کند. این فرایند تضمین می‌کند که هر شبکه متصل به هر روتر در نهایت برای همه روترها شناخته می‌شود. اگر یک روتر به تبلیغات یک مسیر ادامه ندهد، در نهایت آن مسیر را به پایان می رساند و ارسال بسته ها را بر روی آن متوقف می‌کند. وقتی تصمیم می‌گیرید کدام یک از دو نسخه مسیری را در جدول مسیریابی برنامه ریزی کنید، مسیرهای کوتاهتر را به مسیرهای طولانی ترجیح می دهند. با استفاده از دستورات زیر در قسمت CLI روترها بر اساس سناریو آموزش IP های اینترفیس های روتر رو اختصاص میدهیم:

Router(config)#interface fastehernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial0/0

Router(config-if)#ip address 10.10.10.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

بعد از اختصاص IP ها بر روی اینترفیس روترها حال نوبت به کانفیگ ارتباط شبکه‌ها و روترها باهم با استفاده از پروتکل RIP هست که برای انجام این کار نیز دستورات زیر را بر روی روترها انجام میدهیم:

Router(config)#router rip

Router(config-router)#net

Router(config-router)#network 172.16.88.0

Router(config-router)#network 10.10.10.0

Router(config-router)#exit

در rip نیز همانند شبکه بالا پیکربندی را انجام داده و دستورات زیر را در ادامه خواهیم زد:

