آزمایش ۷

سید عباس میرقاسمی

پیش گزارش:

۱. این که یک شبکه Flat است به چه معناست؟
یعنی در شبکه تنها از یک آدرس دامنه برای برادکست استفاده میکنیم.
۲. VLAN ها چگونه مدیریت شبکه را آسان تر میکنند؟
مواردی که در کتاب گفته شده است:

- با تنظیم یک پورت در VLAN ای که میخواهیم، میتوانیم جابجایی و اضافه کردن و تغییرات در شبکه را برای خودمان آسان تر کنیم.
- می توان افراد را دسته بندی کرد و به هرکدام دسترسی های مختلف داد. همچین تنها افراد داخل یک vlan با یکدیگر در ارتباط اند.
- VLAN یک دسته بندی گروه بندی کاربران است که توسط خودمان ایجاد شده است. و خاصیت های محلی کاربر در نظر گرفته نمیشود(مستقل از مکان فیزیکی)
- امنیت شبکه افزایش پیدا میکند.
- تعداد دامنه برادکست شده زیاد میشود ولی اندازه آن ها کوچک تر می شود.

۳. Static vlans با dynamic vlans چه تفاوتی دارد؟
در static، ادمین شبکه باید vlan ها را با در نظر گرفتن پورت سویچ مشخص کند، ولی در dynamic ما مک آدرس و شماره vlan های مرتبط به یکدیگر را در دیتابیس شبکه ذخیره میکنیم. در نهایت خود سیستم سویچ و پورت هایش را برای ما تنظیم میکند.
۴. پارامترهایی که پویایی درdynamic vlan بر اساس آنها ایجاد میشوند کدامند؟
مک آدرس- پروتوکل ها- برنامه ها
۵. مفاهیم زیر را توضیح دهید:
a. Access port:

یک پورت دسترسی فقط به یک VLAN تعلق دارد و ترافیک آن را حمل می کند. ترافیک هم در قالب های بومی بدون هیچ گونه برچسب گذاری VLAN دریافت و ارسال می شود. هر چیزی که به یک پورت دسترسی می رسد به سادگی به VLAN اختصاص داده شده به پورت تعلق دارد. بنابراین، فکر می کنید اگر یک پورت دسترسی یک بسته برچسب گذاری شده، مانند برچسب گذاری شده IEEE 802.1Q را دریافت کند، چه اتفاقی می افتد؟ آن بسته به سادگی حذف می شود. اما چرا؟ خوب، از آنجایی که یک پورت دسترسی به آدرس منبع نگاه نمی کند، بنابراین ترافیک برچسب گذاری شده را می توان فقط در پورت های ترانک ارسال و دریافت کرد. با یک پیوند دسترسی، می توان به آن VLAN پیکربندی شده پورت اشاره کرد. هر دستگاهی که به پیوند دسترسی متصل است از عضویت در VLAN بی خبر است - دستگاه فقط فرض می کند که بخشی از همان دامنه پخش است، اما تصویر بزرگی ندارد، بنابراین توپولوژی فیزیکی شبکه را اصلا درک نمی کند.
اطلاعات خوبی که باید بدانید این است که سوئیچ ها هرگونه اطلاعات VLAN را قبل از ارسال به یک دستگاه پیوند دسترسی از فریم حذف می کنند. به یاد داشته باشید که دستگاه های پیوند دسترسی نمی توانند با دستگاه های خارج از VLAN خود ارتباط برقرار کنند مگر اینکه بسته مسیریابی شود. و شما فقط می توانید یک پورت سوئیچ ایجاد کنید که یک پورت دسترسی یا یک پورت ترانک باشد – نه هر دو. بنابراین باید یکی یا

دیگری را انتخاب کنید و بدانید که اگر آن را به یک پورت دسترسی تبدیل کنید، آن پورت را می توان فقط به یک VLAN اختصاص داد. یک پورت دسترسی را می توان تنها به یک VLAN اختصاص داد. امروزه، اکثر سوئیچ ها به شما اجازه می دهند یک VLAN دوم را به یک پورت دسترسی در یک پورت سوئیچ برای ترافیک صوتی خود اضافه کنید. به آن صدای VLAN می گویند. VLAN صوتی قبلاً VLAN کمکی نامیده می شد که به آن اجازه می داد در بالای VLAN داده قرار گیرد و هر دو نوع ترافیک را از طریق یک پورت امکان پذیر می کرد. اگرچه از نظر فنی این نوع پیوند متفاوتی در نظر گرفته می شود، اما همچنان فقط یک پورت دسترسی است که می تواند هم برای VLANهای داده و هم برای VLANهای صوتی پیکربندی شود. این به شما امکان می دهد هم یک تلفن و هم یک دستگاه رایانه شخصی را به یک پورت سوئیچ متصل کنید، اما همچنان هر دستگاه را در یک VLAN جداگانه داشته باشید.

b. Trunk port

پورت های ترانک می توانند به طور مشابه چندین VLAN را در یک زمان حمل کنند. پیوند ترانک یک پیوند نقطه به نقطه ۱۰۰ یا ۱۰۰۰ مگابیت در ثانیه بین دو سوییچ، بین سوئیچ و روتر، یا حتی بین سوئیچ و سرور است و ترافیک چندین VLAN را از ۱ تا ۴۰۹۴ در یک زمان حمل می کند. اگرچه واقعاً فقط تا ۱۰۰۵ است مگر اینکه با VLAN های توسعه یافته استفاده کنید. ترانک می تواند یک مزیت واقعی باشد زیرا با آن، می توانید یک پورت واحد را به طور همزمان بخشی از یک دسته کامل از VLAN های مختلف کنید. این یک ویژگی عالی است زیرا می توانید پورت ها را به گونه ای تنظیم کنید که یک سرور در دو دامنه پخش جداگانه به طور همزمان داشته باشند تا کاربران شما مجبور نباشند برای ورود به سیستم و دسترسی به آن از یک دستگاه لایه ۳ (روتر) عبور کنند. یکی دیگر از مزایای ترانک هنگام اتصال سوئیچ ها به چشم می خورد. پیوندهای ترانک می توانند مقادیر مختلفی از اطلاعات VLAN را در سراسر پیوند حمل کنند، اما به طور پیش فرض، اگر پیوندهای بین سوئیچ های شما ترانک نشده باشند، فقط اطلاعات VLAN پیکربندی شده در آن پیوند جابه جا می شوند. خوب است بدانید که همه VLAN ها اطلاعات را روی یک پیوند ترانک شده ارسال می کنند، مگر اینکه هر VLAN را با دست پاک کنید، و نگران نباشید، من به شما نشان خواهم داد که چگونه VLAN های جداگانه را از یک ترانک پاک کنید. همه هاست های متصل به سوئیچ ها می توانند به همه پورت ها در VLAN خود ارتباط برقرار کنند، زیرا پیوند ترانک بین آنها وجود دارد. به یاد داشته باشید، اگر از یک لینک دسترسی بین سوئیچ ها استفاده کنیم، این شناسایی VLAN ها به تنها یک VLAN اجازه می دهد تا بین سوئیچ ها ارتباط برقرار کند. همانطور که می بینید، این هاست ها از پیوندهای دسترسی برای اتصال به سوئیچ استفاده می کنند، بنابراین آنها فقط در یک VLAN ارتباط برقرار می کنند. این بدان معناست که بدون روتر، هیچ میزبانی نمی تواند خارج از VLAN خود ارتباط برقرار کند، اما آنها می توانند داده ها را از طریق پیوندهای ترانک شده به هاست های روی سوئیچ دیگری که در همان VLAN پیکربندی شده است ارسال کنند.

c. Frame Tagging

همانطور که می دانیم، می توانیم VLAN های خود را طوری تنظیم کنیم که بیش از یک سوئیچ متصل را پوشش دهد. این قابلیت انعطاف پذیر و پر قدرت احتمالاً مزیت اصلی برای پیاده سازی VLAN است. اما می تواند تا حدی پیچیده باشد - حتی برای یک سوئیچ - بنابراین باید راهی برای هر یک وجود داشته باشد تا همه کاربران و فریم ها را در حین پیگیری آنها دنبال کند. فابریک سوییچ و VLAN ها را سفر کنید. وقتی می گویم «سوئیچ فابریک»، فقط به گروهی از سوئیچ ها اشاره می کنم که اطلاعات VLAN یکسانی دارند. و این دقیقاً جایی است که برچسب فریم وارد صحنه می شود. این روش شناسایی فریم به طور منحصر به فرد یک شناسه تعریف شده توسط کاربر را به هر فریم اختصاص می دهد. گاهی اوقات مردم از آن به عنوان "VLAN ID" یا حتی "color" یاد می کنند. نحوه کار به این صورت است: هر سوئیچ که فریم به آن می رسد باید ابتدا شناسه VLAN را از تگ فریم شناسایی کند. سپس با مشاهده اطلاعات موجود در آنچه به عنوان جدول فیلتر شناخته

می شود، متوجه می شود که با قاب چه کاری انجام دهد. اگر فریم به سوییچی برسد که پیوند ترانک شده دیگری دارد، فریم به خارج از درگاه پیوند ترانک ارسال می شود. هنگامی که فریم به خروجی رسید که توسط جدول جلو/فیلتر به عنوان پیوند دسترسی مطابق با شناسه VLAN قاب تعیین می شود، سوئیچ شناسه VLAN را حذف می کند. این به این دلیل است که دستگاه مقصد می تواند فریم ها را بدون نیاز به درک شناسایی VLAN آنها دریافت کند. نکته دیگر در مورد پورت های ترانک این است که آنها از ترافیک برچسب گذاری شده و بدون برچسب به طور همزمان پشتیبانی می کنند (اگر از ترانکینگ Q۸۰۲.۱ استفاده می کنید که در مورد آن صحبت خواهیم کرد. در بخش بعدی). به پورت ترانک یک درگاه VLAN ID (PVID) پیش فرض برای VLAN اختصاص داده می شود که تمام ترافیک بدون برچسب به آن منتقل می شود. این VLAN همچنین VLAN بومی نامیده می شود و به طور پیش فرض همیشه VLAN 1 است (اما می توان آن را به هر شماره VLAN تغییر داد). به طور مشابه، هر ترافیک بدون برچسب یا برچسب شده با شناسه VLAN NULL (تخصیص نشده) متعلق به VLAN با PVID پیش فرض پورت (دوباره، VLAN 1 به طور پیش فرض). بسته ای با شناسه VLAN برابر با PVID پیش فرض پورت خروجی بدون برچسب ارسال می شود و فقط می تواند با میزبان ها یا دستگاه های موجود در VLAN 1 ارتباط برقرار کند. تمام ترافیک VLAN دیگر باید با یک برچسب VLAN ارسال شود تا در یک VLAN با اون تگ خاص ارتباط برقرار کند.

۶. VTP چیست و چه ویژگی هایی دارد؟

سیسکو این مورد را نیز ایجاد کرد. اهداف اساسی پروتکل ترانکینگ VLAN (VTP) مدیریت تمام VLANهای پیکربندی شده در یک اینترنت سوئیچ شده و حفظ ثبات در سراسر آن شبکه است. دامنه. در اینجا لیستی از برخی از ویژگی های جالب VTP ارائه شده است:

- پیکربندی یکسان VLAN در تمام سوئیچ ها در شبکه
- ترانک VLAN روی شبکه های مختلط، مانند اترنت به ATM LANE یا حتی FDDI
- ردیابی و نظارت دقیق VLAN ها
- گزارش پویا از VLAN های اضافه شده به تمام سوئیچ ها در دامنه VTP
- افزودن VLAN Plug and Play

قبل از اینکه بتوانید VTP را برای مدیریت VLAN های خود در سراسر شبکه دریافت کنید، باید یک سرور VTP ایجاد کنید. همه سرورهایی که نیاز به اشتراک گذاری اطلاعات VLAN دارند باید از یک نام دامنه استفاده کنند و یک سوئیچ می تواند در یک زمان فقط در یک دامنه باشد. بنابراین اساساً این بدان معناست که یک سوئیچ تنها در صورتی می تواند اطلاعات دامنه VTP را با سایر سوئیچ ها به اشتراک بگذارد که در همان دامنه VTP پیکربندی شده باشند. اگر بیش از یک سوئیچ در یک شبکه متصل هستید، می توانید از یک دامنه VTP استفاده کنید، اما اگر همه سوئیچ های خود را فقط در یک VLAN دارید، فقط نیازی به استفاده از VTP ندارید. به خاطر داشته باشید که اطلاعات VTP بین سوئیچ ها فقط از طریق پورت ترانک ارسال می شود. سوئیچ ها اطلاعات دامنه مدیریت VTP و همچنین شماره ویرایش پیکربندی و تمام VLAN های شناخته شده با هر پارامتر خاص را تبلیغ می کنند. اما چیزی به نام حالت شفاف VTP نیز وجود دارد. در آن، می توانید سوئیچ ها را طوری پیکربندی کنید که اطلاعات VTP را از طریق پورت های ترانک ارسال کنند، اما به روزرسانی اطلاعات را نپذیرند یا پایگاه داده VTP خود را به روزرسانی کنند. اگر کاربرانی دارید که پشت سرتان سوئیچ هایی را به دامنه VTP شما اضافه می کنند، می توانید رمزهای عبور اضافه کنید، اما فراموش نکنید - هر سوئیچ باید با یک رمز عبور راه اندازی شود.و همانطور که می توانید تصور کنید، این مشکل کوچک می تواند از نظر اداری دردسر واقعی باشد! سوئیچ ها هر VLAN اضافه شده را در تبلیغات VTP شناسایی می کنند، سپس آماده ارسال اطلاعات روی پورت های ترانک خود با VLAN جدید تعریف شده در داخل می شوند. به روزرسانی ها به عنوان شماره های نسخه ارسال می شوند که شامل اعلان به اضافه یک می شوند. هر بار که سوئیچ شماره نسخه بالاتری را می بیند، می داند اطلاعاتی که دریافت می کند جدیدتر است، بنابراین پایگاه داده موجود را با آخرین اطلاعات بازنویسی می کند.

برای انتقال اطلاعات VLAN بین سوئیچ ها، باید این سه الزام را برای VTP بدانید:

- نام دامنه مدیریت VTP هر دو سوییچ باید یکسان تنظیم شود.
- یکی از سوئیچ ها باید به عنوان سرور VTP پیکربندی شود.
- هیچ روتری لازم نیست.

۷. درباره ی مدهای VTP توضیح دهید.

- server

این حالت پیش فرض برای همه سوئیچ های Catalyst است. برای انتشار اطلاعات VLAN در سراسر آن دامنه حداقل به یک سرور در دامنه VTP خود نیاز دارید. همچنین مهم است: سوئیچ باید در حالت سرور باشد تا بتواند VLAN ها را در دامنه VTP ایجاد، اضافه و حذف کند.اطلاعات VTP باید در حالت سرور تغییر کند و هر تغییری که در یک سوئیچ در حالت سرور ایجاد شود در کل دامنه VTP تبلیغ می شود. در حالت سرور VTP، تنظیمات VLAN در NVRAM ذخیره می شوند.

- client

در حالت کلاینت، سوئیچ ها اطلاعات را از سرورهای VTP دریافت می کنند، اما به روز رسانی را نیز ارسال و دریافت می کنند، بنابراین به این ترتیب مانند سرورهای VTP رفتار می کنند. تفاوت این است که آنها نمی توانند VLAN ها را ایجاد، تغییر یا حذف کنند. به علاوه، هیچ یک از پورت های سوئیچ کلاینت را نمی توان به یک VLAN جدید اضافه کرد، قبل از اینکه سرور VTP به سوییچ مشتری از VLAN جدید اطلاع دهد. همچنین خوب است بدانید که اطلاعات VLAN ارسال شده از یک سرور VTP در NVRAM ذخیره نمی شود، این مهم است زیرا به این معنی است که اگر سوئیچ ریست یا بارگذاری مجدد شود، اطلاعات VLAN حذف می شود. در اینجا یک نکته وجود دارد: اگر می خواهید یک سوئیچ تبدیل به یک سرور شود، ابتدا آن را به یک مشتری تبدیل کنید تا تمام اطلاعات صحیح VLAN را دریافت کند، سپس آن را به یک سرور تغییر دهید که خیلی راحت تراست! بنابراین اساساً، یک سوئیچ در حالت مشتری VTP، تبلیغات خلاصه VTP را ارسال کرده و آنها را پردازش می کند. این سوئیچ پیکربندی VTP را در پیکربندی در حال اجرا ذخیره نمی کند، و آن را در NVRAM ذخیره نمی کند. سوئیچ هایی که در حالت کلاینت VTP هستند فقط اطلاعات VTP را یاد می گیرند و به آنها منتقل می کنند.

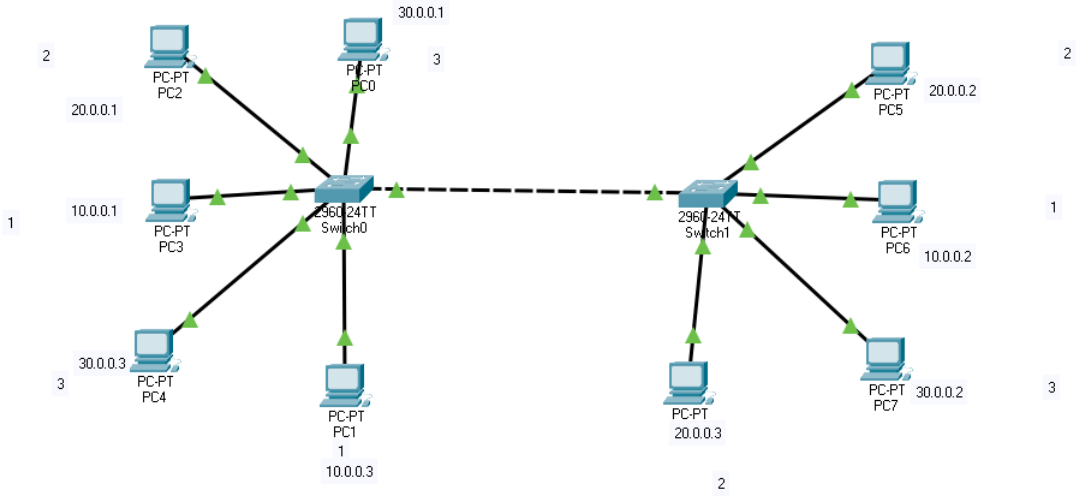
- transparent

سوئیچ ها در حالت شفاف در دامنه VTP شرکت نمی کنند یا پایگاه داده VLAN آن را به اشتراک نمی گذارند، اما همچنان تبلیغات VTP را از طریق پیوندهای ترانک پیکربندی شده ارسال می کنند. آنها می توانند VLAN ها را ایجاد، اصلاح و حذف کنند زیرا پایگاه داده خود را نگه می دارند - یکی را از سوییچ های دیگر مخفی نگه می دارند. با وجود نگهداری در NVRAM، پایگاه داده VLAN در حالت شفاف در واقع فقط به صورت محلی قابل توجه است. هدف کل حالت شفاف این است که به سوئیچ های راه دور اجازه دهد تا پایگاه داده VLAN را از یک سوئیچ پیکربندی شده توسط سرور VTP از طریق سوئیچی دریافت کنند که در همان تخصیص VLAN شرکت نمی کند.

گزارش تکلیف:

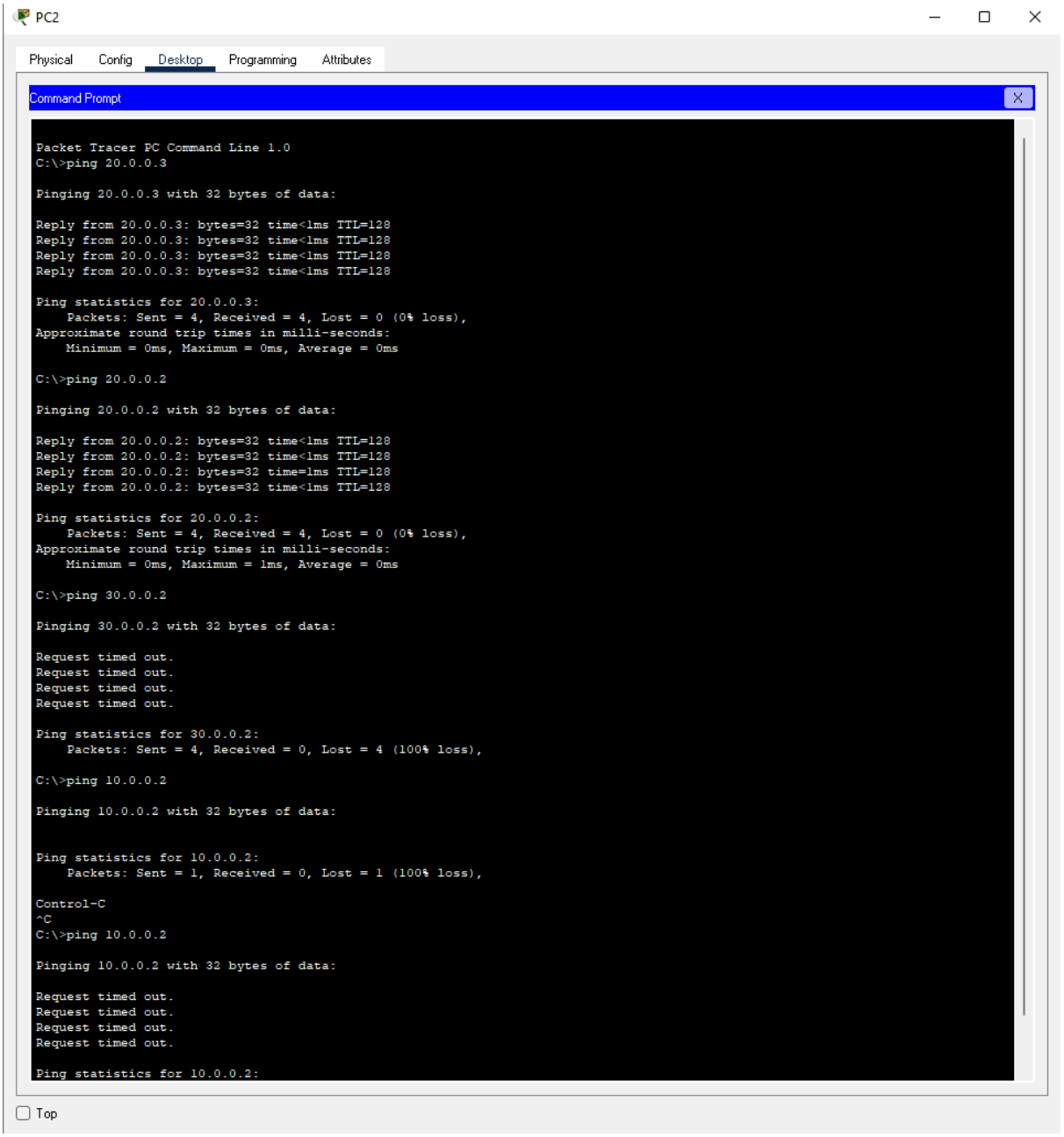
۱- حالت اول:

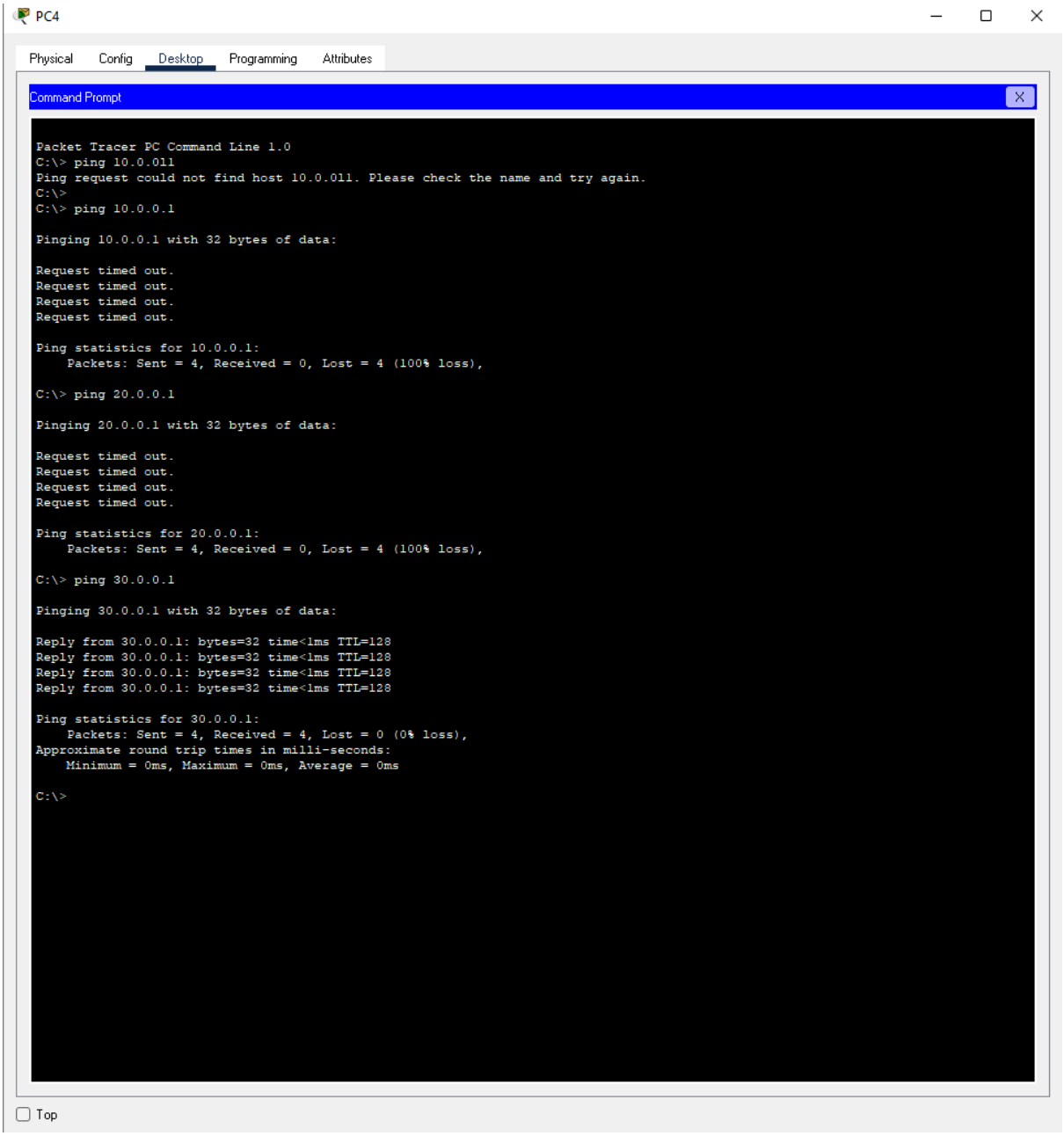
با توجه به نکات گفته شده در سر کلاس، شبکه را سرهم بندی کردیم:



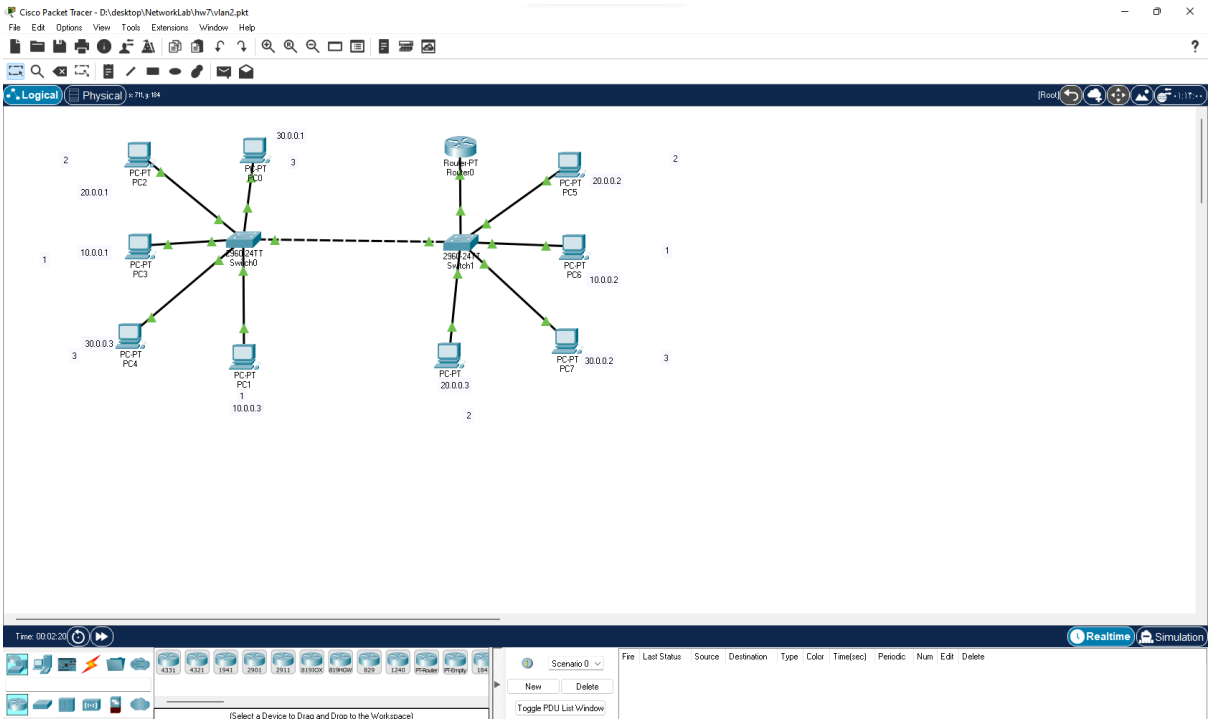
همان طور که در تصویر مشاهده میکنید. Network ip های هر end device نوشته شده است.

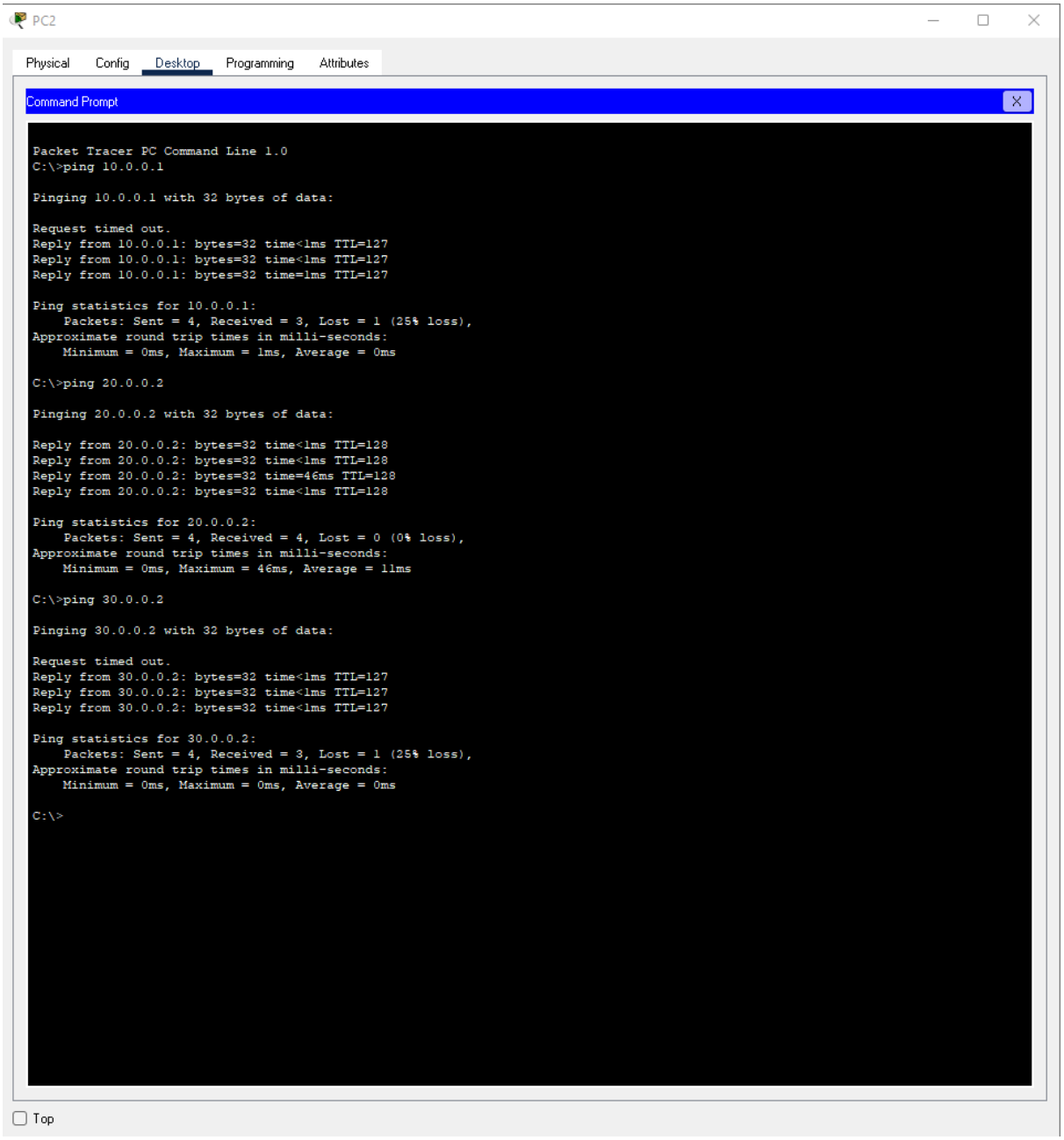
حال که تنظیمات را در سویچ ها انجام دادیم، بین end device هایمان تست ping میگیریم.


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.3
Pinging 20.0.0.3 with 32 bytes of data:
Reply from 20.0.0.3: bytes=32 time<1ms TTL=128
Reply from 20.0.0.3: bytes=32 time<1ms TTL=128
Reply from 20.0.0.3: bytes=32 time<1ms TTL=128
Reply from 20.0.0.3: bytes=32 time<1ms TTL=128
Ping statistics for 20.0.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 20.0.0.2
Pinging 20.0.0.2 with 32 bytes of data:
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Reply from 20.0.0.2: bytes=32 time=1ms TTL=128
Reply from 20.0.0.2: bytes=32 time<1ms TTL=128
Ping statistics for 20.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 30.0.0.2
Pinging 30.0.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 30.0.0.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Ping statistics for 10.0.0.2:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.0.2:
Top



۲- حال دستوراتی که در کلاس گفته شد را برای روتری که به شبکه اضافه کردیم را تنظیم میکنیم


Cisco Packet Tracer - D:\desktop\NetworkLab\hw7\vlan2.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
PC-PT PC2
PC-PT PC0
30.0.0.1
Router-PT Router0
PC-PT PC5
20.0.0.2
20.0.0.1
10.0.0.1
PC-PT PC3
2960-24TT Switch0
2960-24TT Switch1
PC-PT PC6
10.0.0.2
30.0.0.3
PC-PT PC4
PC-PT PC1
10.0.0.3
PC-PT 20.0.0.3
PC-PT PC7
30.0.0.2
Time: 00:02:20
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete



همانطور که مشاهده میکنید از دستگاه pc2 به هر شبکه دسترسی داریم.

سوالات:

۱- پروتکلهای Q.802۱ و ISL را با هم مقایسه کنید.

- پروتکل Q.802۱ از محصولات کنوانسیون IEEE است:
  - حداکثر از ۴۰۹۶ vlan را پشتیبانی میکند که تعداد بالاتری نسبت به پروتکل isl دارد.
  - در انکپسوله سازی تعدادی تگ که هر کدامشان ۴ بایت است به فریم اصلی اضافه میشود.
  - به فریم های vlan های محلی تگ اضافه نمیکند.
  - نسبت به isl سربار کمتری دارد.
- پروتکل ISL از محصولات شرکت CISCO است:
  - حداکثر ۱۰۰۰ vlan را پشتیبانی میکند.
  - براساس انکپسوله سازی یک هدر اضافی روی همان فریم اصلی کار میکند.

- این پروتکل فریم های vlan های محلی را نیز تگ میزند.
- به خاطر اضافه کردن تگ به فریم ها، سربار زیادی روی شبکه دارد و خیلی کم استفاده میشود.

۲- آیا لینک trunk میتواند بین دو روتر وجود داشته باشد؟ توضیح دهید.

خیر. لینک trunk در دو بخش مورد استفاده قرار میگیرد: سوییچ-روتر یا سوییچ-سوییچ

هدف اصلی از لینک trunk هدایت فریم ها به vlan هدف است تا در سوییچ هدف دریافت شود. حال اگر لینک trunk را بین دو روتر قرار دهیم، vlan ای در این بین وجود ندارد که فریم ها به آن سمت هدایت شوند. پس انجام این کار درست و دارای منطق نیست!

۳- کاربرد VTP Domain؟

VLAN management domain، شامل یک یا چند سوییچ متصل به همدیگر است که زیر مجموعه یک مسئولیت اداری هستند و به اصطلاح VTP domain name برای آن ها ثابت و مشترک است. کاربردی اصلی آن در زمانی است که سویچ تصمیم میگیرد به هنگام تبادل اطلاعات بین vlan ها ، بر اساس نام دامنه تبلیغات را انجام دهد یا نه، حال کلاینت هایی که در یک vtp domain هستند می توانند با یکدیگر اطلاعات مبادله کنند.