بنام خدا

دانشگاه علم و صنعت ایران- دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری-آزمایش ۷

Port Security & PoE

نام خانوادگی و نام	شماره دانشجوئی	شماره آزمایش	آدرس آیمیل	PK.Tracer Ver	تلفن)اختياري)
مرشدزاده یگانه	۹۶۵۲۱۴۸۸	8	yegmor@gmail.com	Ver 6.2	

این آزمایش در قالب یک Case Study می‌باشد.

تذکر : قالب نامگذاری سوئیچ‌ها، کامپیوترها و نیز قراردادن مشخصات دانشجو درباکس با استفاده از Place Note براساس آنچه که قبلا گفته شد و نیز قالب نامگذاری فایل DOCX و عنوان زیر برای ارسال ایمیل ضروری است:

eMail subject : NetLab8-Class14

❖ بخش اول : CDP – Cisco Discovery Protocol (۵۰ نمره)

1- این پروتکل را با ذکر منبع تعریف، اینکه متعلق به چه شرکتی است و محدودیت‌های استفاده از آن را بنویسید ؟ (در زیر همین قسمت)

این یک پروتکل اختصاصی لایه دو که مستقل از رسانه ها و دستگاه ها و شبکه است که بر روی دستگاه های سیسکو اجرا میشود که توسط Cisco Systems ارائه شده است.

این قابلیت را به برنامه های شبکه میدهد که به طور مستقیم از دستگاه های متصل نزدیک باخبر شوند. این پروتکل مدیریت دستگاه های سیسکو را تسهیل میبخشد به واسطه یافتن این دستگاه ها و مشخص کردن اینکه چگونه config شده‌اند و اجازه دادن به سیستم برای استفاده کردن از پروتکل های لایه شبکه متفاوت برای یاد گرفتن یکدیگر.

این پروتکل برای به اشتراک گذاشتن اطلاعات سایر تجهیزات سیسکو که به طور مستقیم متصل شده اند به مانند ورژن سیستم عامل و آدرس IP استفاده میشوند.

پیش نیاز برای استفاده از این پروتکل این است که تمام interface ها باید از هدر های Subnetwork Access Protocol (SNAP) پشتیبانی بکنند.

این پروتکل محدودیت های زیر را دارد:

- این پروتکل تنها بر روی دستگاه های سیسکو اجرا میشود.
- این پروتکل بر روی Frame Relay multipoint subinterfaces پشتیبانی نمیشوند.
- اگر یک همسایه بر روی interface ای که فعال شده است با CDP، هیچ آدرس IP ای نداشته باشد آن گاه آدرس IP یک interface دیگر آپدیت خواهد شد به عنوان آدرس IP برای interface که آدرس IP نداشت.
- این پروتکل تنها بر روی interface های مستقیما متصل کار میکند.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x

https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol

2- با استفاده از دو سوئیچ لایه ۲ ، استفاده از پروتکل CDP را نشان دهید.

راهنمائی : در Packet Tracer ، دو سوئیچ و به هر سوئیچ سه کامپیوتر متصل و آدرس IP کامپیوترها را از یک آدرس شبکه انتخاب کنید. سپس با دستور mac-address-table clear در دو سوئیچ جدول mac را خالی کنید (منتظر aging نشوید). تمام عملیاتی که انجام می‌دهید (از قبیل انتخاب دامنه IP برای کامپیوترها) را در زیر همین قسمت بنویسید.

PC-000D.BD5C.1938: 172.16.8.1/24

PC-00D0.5887.6EB0 : 172.16.8.2/24

PC-00D0.5881.0310 : 172.16.8.3/24

PC-0001.C954.673B : 172.16.8.6/24

PC-0090.0C1D.A08E : 172.16.8.7/24

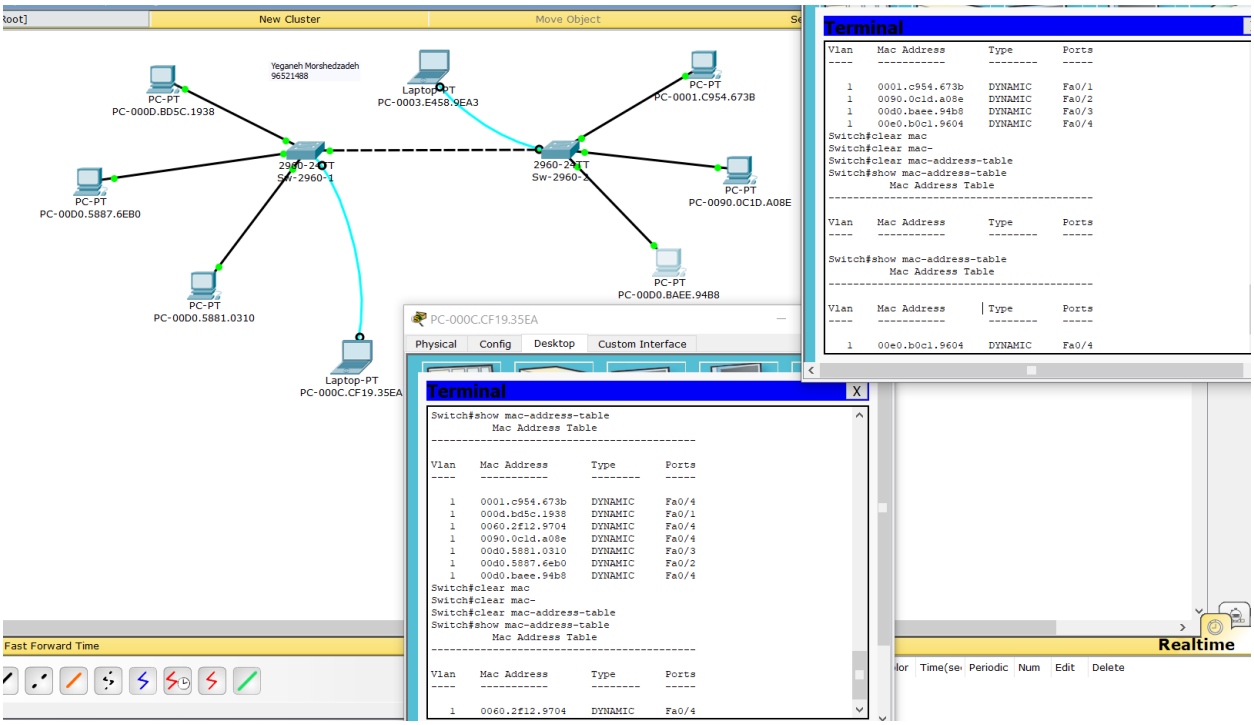
PC-00D0.BAEE.94B8 : 172.16.8.8/24

PC-000C.CF19.35EA: 172.16.8.10/24

PC-0003.E458.9EA3: 172.16.8.11/24

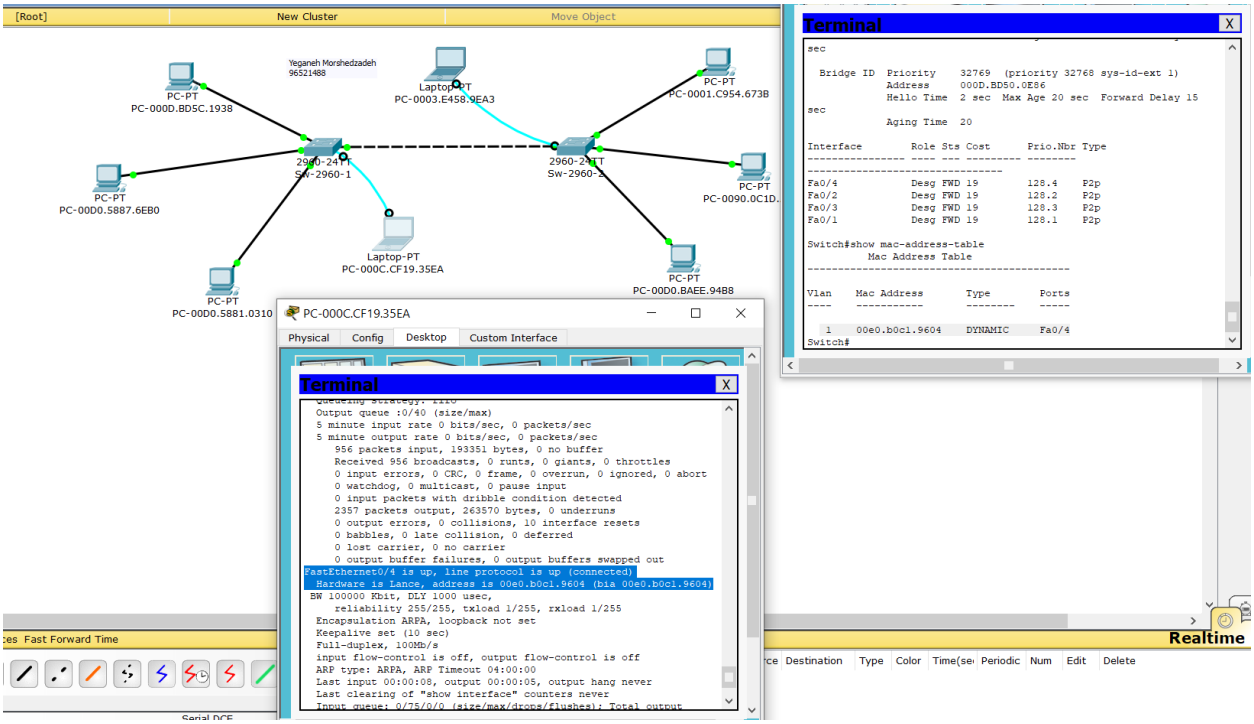
در ترمینال سوییچ با دستور en به حالت privileged میرویم و سپس دستورات جدول آدرس مک را میزنیم.

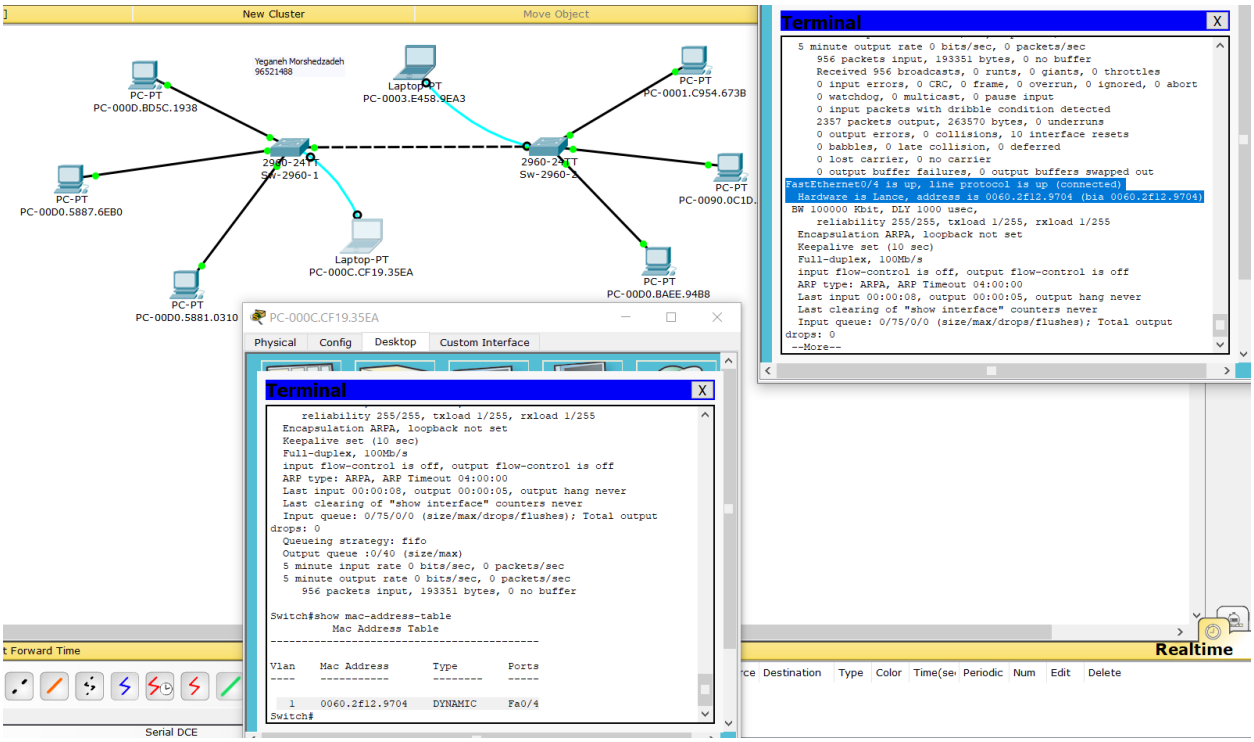
3- تصویری از Packet Tracer با مشخص بودن همه کامپیوترها و نیز خروجی دستوری که مشخص کننده جدول mac است را در زیر همین قسمت قرار دهید.



4- به نظر شما تنها سطری که در جدول mac هریک از سوئیچ‌ها می‌بینید مربوط به کدام Device است و با چه پروتکلی این اطلاعات توسط سوئیچ بدست می‌آید.

این سطر ها مربوط به آدرس مک interface هایی که با کابل سوییچ ها را بهم متصل کردند که در اینجا fast ethernet 0/4 دو طرف به این امر اختصاص داده شده است. این دو سوییچ با استفاده از CDP اطلاعات زیادی را رد و بدل میکنند. بسته های مربوط به این پروتکل پیوسته در حال تبادل بین سوییچ ها هستند و از این طریق خود سوییچ ها ارتباطات را آغاز و بسته ها را رد و بدل میکنند.





تذکر : در یادگیری آدرس MAC اینترفیس‌های متصل به پورت‌های سوئیچ، شروع کننده Learning ، سوئیچ نمی‌باشد در صورتیکه در مورد CDP، شروع کننده یادگیری MAC دستگاه متصل روی پورت اتصال، سوئیچ می‌باشد.

❖ **بخش دوم : VTP – VLAN Trunking Protocol (۶۰ نمره)**

1- پروتکل VTP را با ذکر منبع تغریف کنید.

این پروتکل یک پروتکل لایه دو است که پایداری configuration را در VLAN ها نگهداری میکند به واسطه مدیریت کردن addition(اضافات) deletion(پاک شده ها) و نامگذاری مجدد VLAN ها در داخل یک VTP domain.

VTP به حداقل میرساند misconfiguration ها و configuration هایی که ناپایدار (inconsistence) هستند که میتواند مشکلاتی من جمله نام های VLAN تکراری، جزئیات نادرست نوع VLANو بهم خورد Security را منتج شود.

با VTPمیتوان به صورت مرکزی تغییرات configuration را بر روی یک یا چند دستگاه شبکه اعمال کرد و آن تغییرات به صورت اتوماتیک به تمام سایر دستگاه های شبکه ای که در شبکه هستند اطلاع رسانی میشود.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/vtp.pdf

2- VTP Domain را تعریف کنید.

یک VTP Domain (و یا VLAN Management domain) تشکیل شده است از یک یا چند دستگاه شبکه که به اشتراک میگذارند نام VTP domain یکسانی را و با trunk ها بهم متصل (interconnected) هستند.

3- انواع VTP Modes را تعریف کنید.

- Server:

در این حالت شما میتواند VLANها را بسازید، اطلاح و حذف کنید و همچنین سایر پارامتر های Configuration را برای تمام VTP domain مشخص کنید. VTP serverها configuration مربوط به VLANخودشان را به سایر دستگاه های شبکه که در VTP domainیکسانی هستند، تبلیغ میکنند و VLAN configurationخودشان را با سایر

دستگاه های شبکه بر مبنای تبلیغ های دریافت شده از لینک های trunk میتوانند synchronize کنند.

- Client:

مشابه VTP serverها هستند با این تفاوت که در این حالت شما نمیتواند VLANهای بر روی یک VTP client را بسازید، اطلاح و حذف کنید.

- Transparent:

دستگاه های VTP transparent در VTP شرکت نمیکنند و این دستگاه ها VLAN configurationها را تبلیغ نمیکند و خود را با VLAN configuration که به واسطه تبلیغات دریافتی هستند، synchronize نمیکند. هرچند در VTPورژن دو یک دستگاه شبکه transparentتبلیغات VTPدریافتی را از پورت Trunking lanخود forward میکند.

- Off:

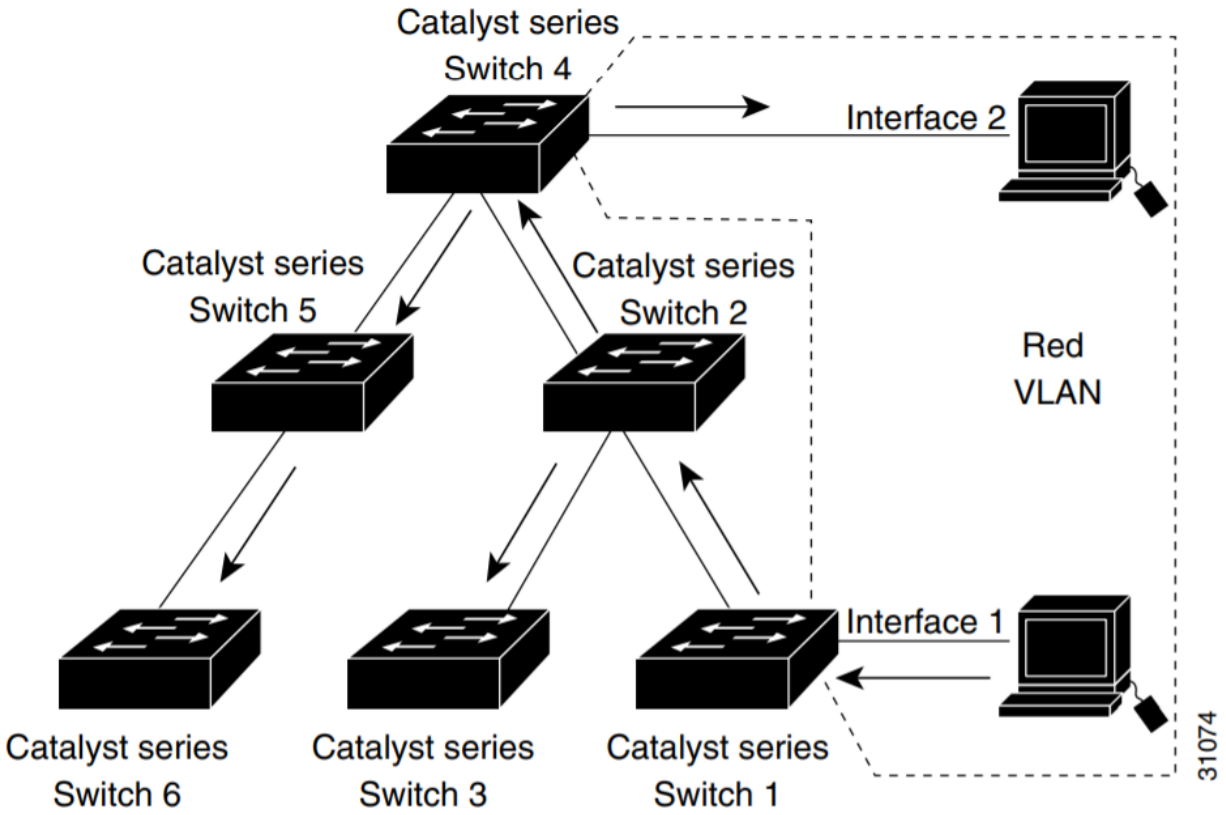
در این حالت یک دستگاه شبکه به مشابه یک دستگاه VTP transparent عمل میکند به جز اینکه تبلیغات VTP را forward نمیکند. که این همان حالتی است که اصلا سوییچ را هیچگونه تنظیمی نکنیم.

4- VTP Pruning را تعریف و تفاوت آن را در صورت Enable و Disable بودن توضیح دهید.

با VTP Pruning میتوان به واسطه کاهش دادن ترافیک flooded غیر ضروری (به مانند broadcastو multicast و ناشناس و flooded unicast بسته ها) bandwidth شبکه را بهبود داد. با VTP Pruning میتوان با محدود کردن ترافیک flooded به سمت آن لینک های trunk ای که ترافیک باید استفاده کند تا به دستگاه های شبکه مناسب دسترسی پیدا کند، bandwidth در دسترس را افزایش داد.

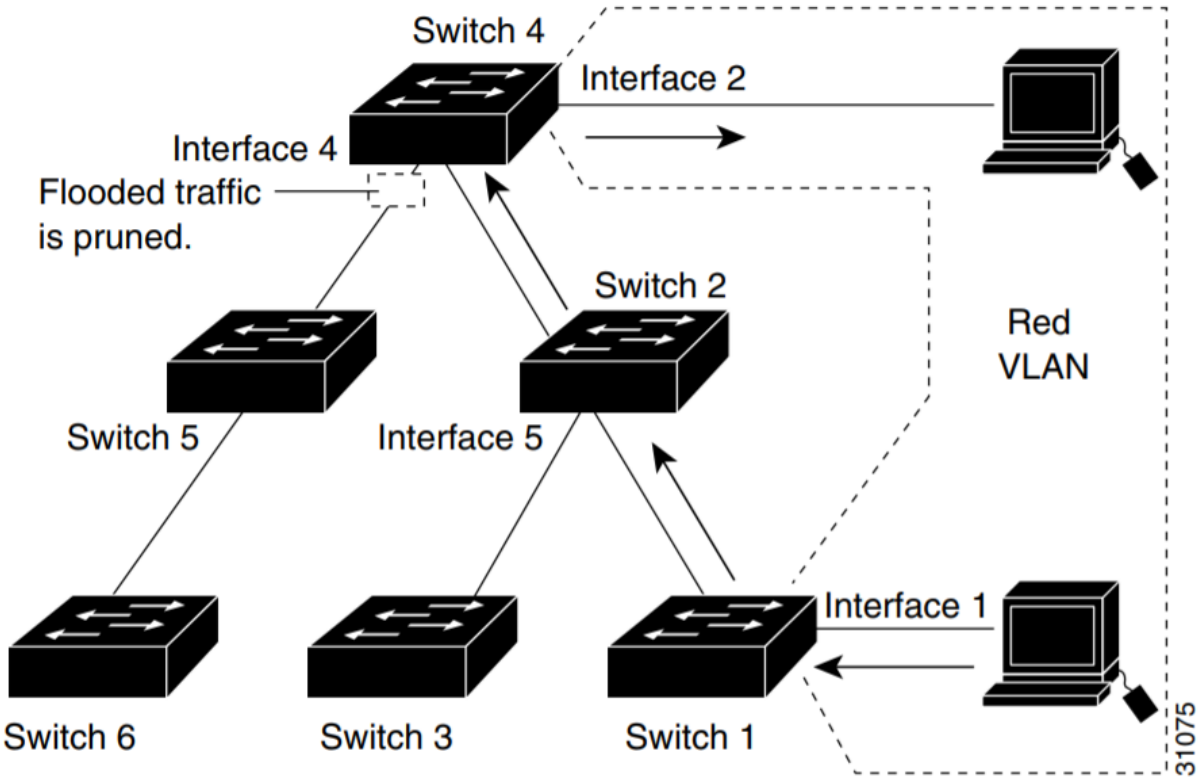
در شکل زیر میتوان یک switched networkکه در ان VTP Pruningفعال نیست را مشاهده کرد. در Interface شماره یک در شبکه ، سوییچ ۱ و پورت ۲ در سوییچ ۴ به VLAN قرمز اختصاص داده شده اند. هنگامی که یک broadcast از سمت hostکه به سوییچ یک متصل شده است ارسال شود، سوییچ یک broadcastرا floodمیکند و در نتیجه تمام دستگاه های شبکه در شبکه آن را دریافت میکنند حتی با وجود اینکه سوییچ های ۳و ۵ و ۶ هیچ پورتی در VLAN قرمز ندارند.

Figure 25-1 Flooding Traffic without VTP Pruning



در شکل زیر نیز میتوان همان switched networkکه در آن VTP Pruningفعال است را مشاهده کرد. ترافیک broadcast از سوییچ یک دیگر به سوییچ های ۳ و۵ و۶ forward نمیشود زیرا که ترافیک برای VLAN قرمز است که بر روی پورت های ۵ سوییچ ۲ و پورت ۴ سوییچ ۴ pruned شده است.

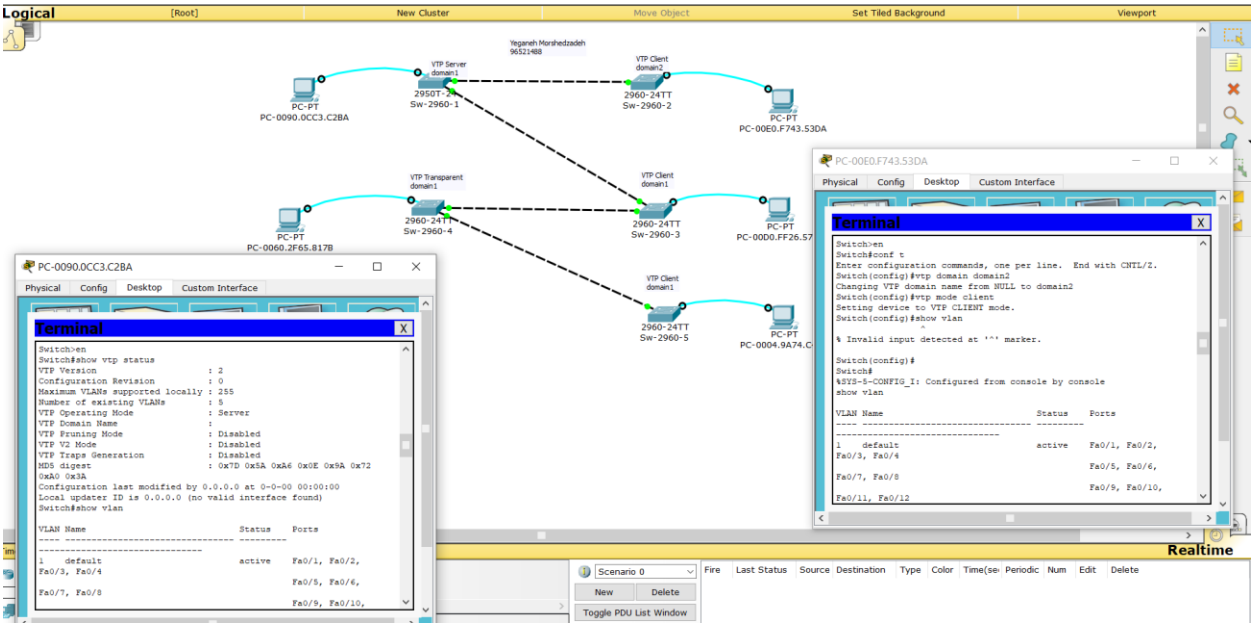
Figure 25-2 Flooding Traffic with VTP Pruning

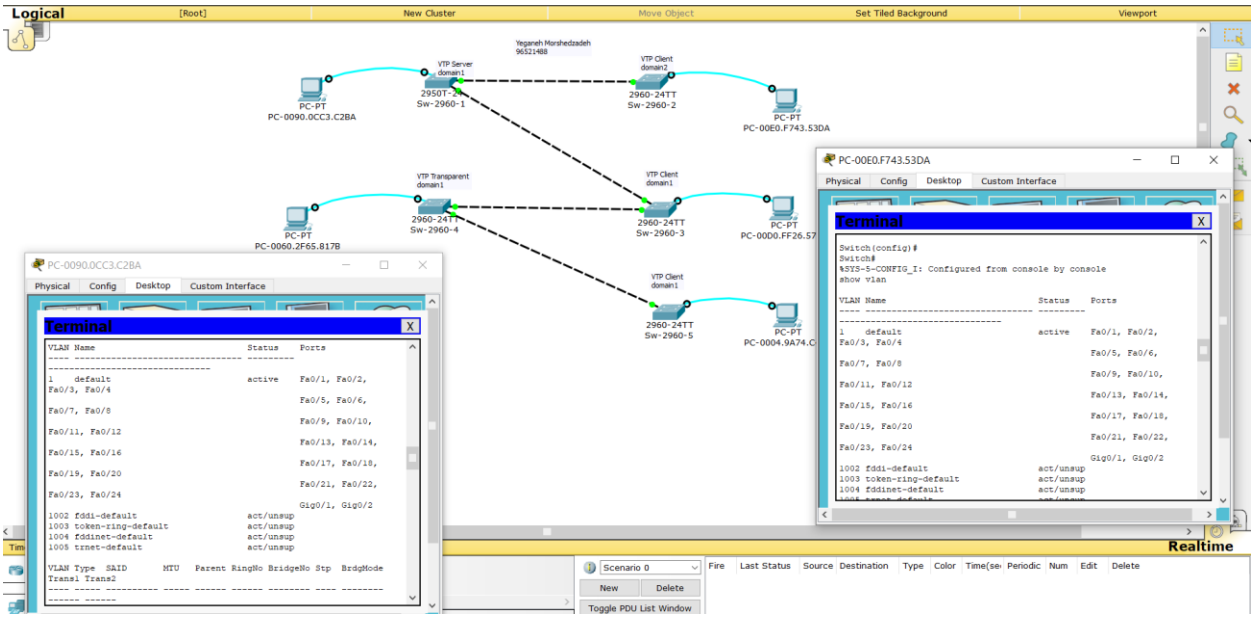


5- یک سناریو در Packet Tracer با استفاده از حداقل چهار سوئیچ طراحی کنید که نمایانگر استفاده از VTP باشد. این سناریو کافیست Domain و Modeهای VTP را پوشش دهد. مراحل انجام سناریو در Packet Tracer به همراه حداقل اضافه و کم کردن یک VLAN و گرفتن تصویر Packet Tracer بگونه‌ای که علاوه بر سوئیچ‌ها و کامپیوترها، شامل پنجره CLI و دستورات و خروجی باشد، در زیر همین قسمت اضافه کنید.

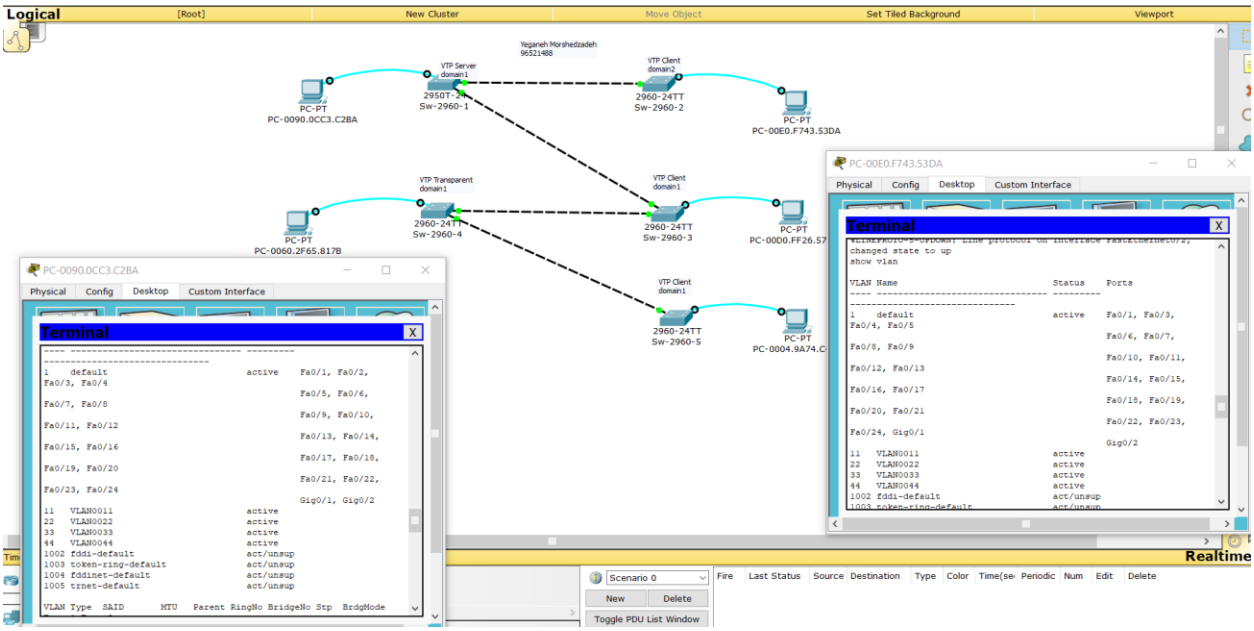
- Client mode

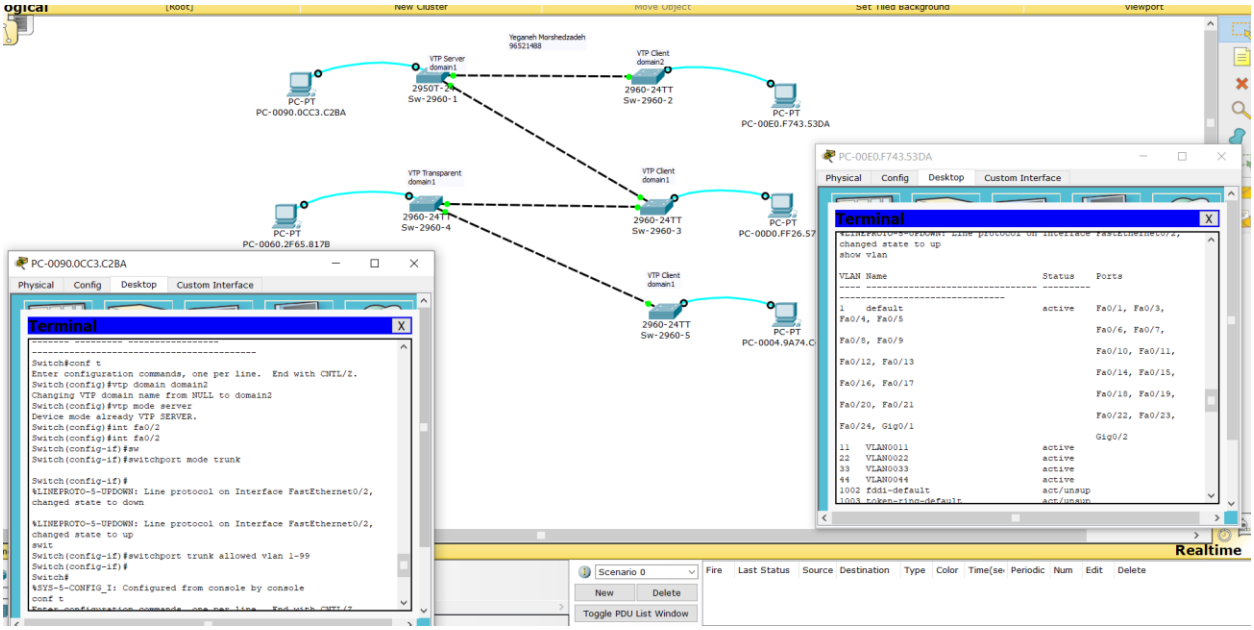
در حالت اولیه که هنوز تنظیمات را اعمال نکردیم vlan ها و وضعیت VTPبه صورت زیر است:

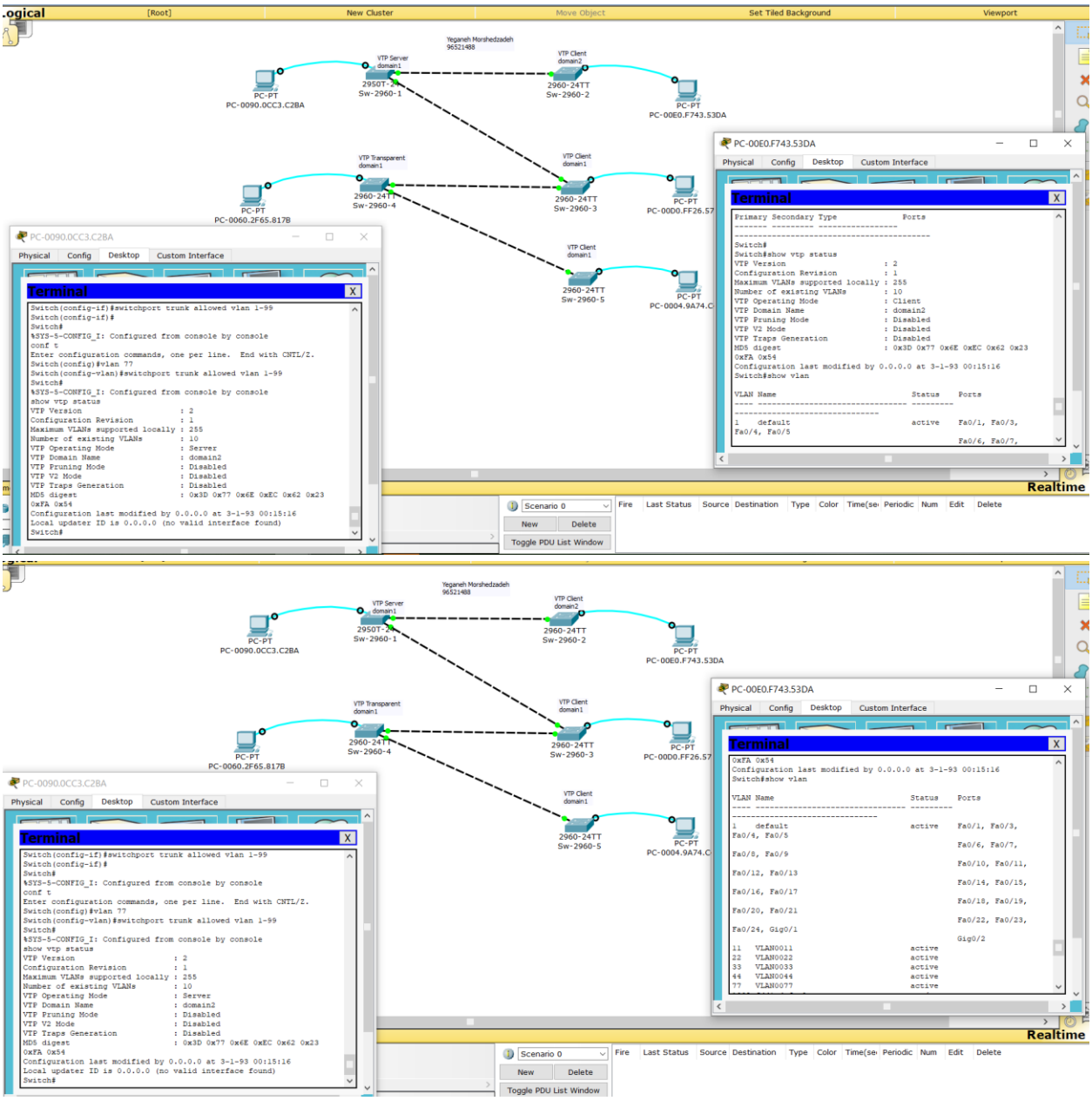




سپس پس از ایجاد تعدادی VLANبر روی سوییچ شماره یک و تنظیم این سوییچ به عنوان سرور VTP و تنظیم پورت اتصالی بین سوییچ بین ۱ و۲ به عنوان trunk link و همچنین تنظیم سوییچ ۲ به عنوان VTP Client وضعیت شبکه به صورت زیر میشود:


Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Yeganeh Morshedzadeh
96521488
VTP Server
domain1
2950T-24
Sw-2960-1
VTP Client
domain2
2960-24TT
Sw-2960-2
PC-PT
PC-0090.0CC3.C2BA
PC-00E0.F743.53DA
VTP Transparent
domain1
2960-24TT
Sw-2960-4
VTP Client
domain1
2960-24TT
Sw-2960-3
PC-0060.2F65.817B
PC-00D0.FF26.57
2960-24TT
Sw-2960-5
PC-0004.9A74.C
PC-0090.0CC3.C2BA
Physical
Config
Desktop
Custom Interface
Terminal
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
Gig0/1, Gig0/2
11 VLAN0011 active
22 VLAN0022 active
33 VLAN0033 active
44 VLAN0044 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode
PC-00E0.F743.53DA
changed state to up
show vlan
VLAN Name Status Ports
1 default active Fa0/1, 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, Gig0/1
Gig0/2
11 VLAN0011 active
22 VLAN0022 active
33 VLAN0033 active
44 VLAN0044 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(se
Periodic
Num
Edit
Delete

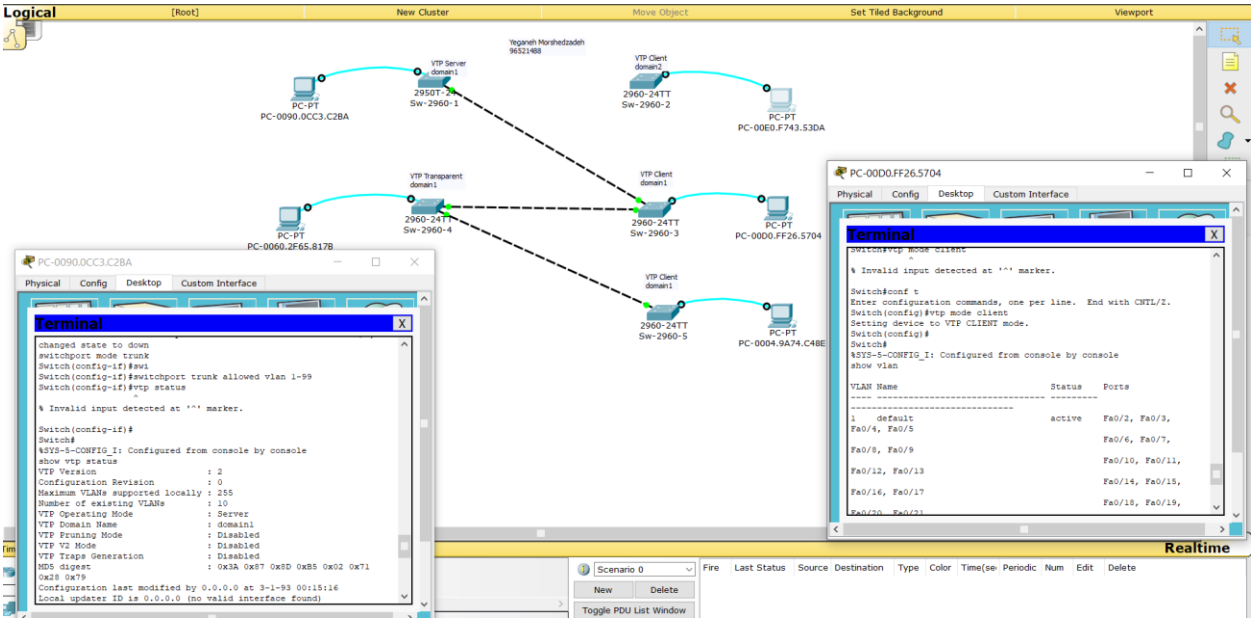

Yeganeh Morshedzadeh
96521488
VTP Server
domain1
2950T-24
Sw-2960-1
VTP Client
domain2
2960-24TT
Sw-2960-2
PC-PT
PC-0090.0CC3.C2BA
PC-00E0.F743.53DA
VTP Transparent
domain1
2960-24TT
Sw-2960-4
VTP Client
domain1
2960-24TT
Sw-2960-3
PC-0060.2F65.817B
PC-00D0.FF26.57
2960-24TT
Sw-2960-5
PC-0004.9A74.C
PC-0090.0CC3.C2BA
Physical
Config
Desktop
Custom Interface
Terminal
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp domain domain2
Changing VTP domain name from NULL to domain2
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#int fa0/2
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
swit
Switch(config-if)#switchport trunk allowed vlan 1-99
Switch(config-if)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console
conf t
PC-00E0.F743.53DA
changed state to up
show vlan
VLAN Name Status Ports
1 default active Fa0/1, 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, Gig0/1
Gig0/2
11 VLAN0011 active
22 VLAN0022 active
33 VLAN0033 active
44 VLAN0044 active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(se
Periodic
Num
Edit
Delete



همان طور که مشاهده شد ما تنظیمات VLANها را تنها بر روی سوییچ ۱ انجام دادیم و با اعمال تنظیمات VTPتوانستیم همین VLANها را برای سوییچ ۲ اعمال کنیم. در این مثال سوییچ ۱ و۲ بر روی domain2 بودند. در حقیقت که هنگامی که سوییچ ۲ را بر روی domain2که از قبل سرور بر روی آن تنظیم شده بود، تنظیم کردیم، configurationها به این سوییچ منتقل شد.

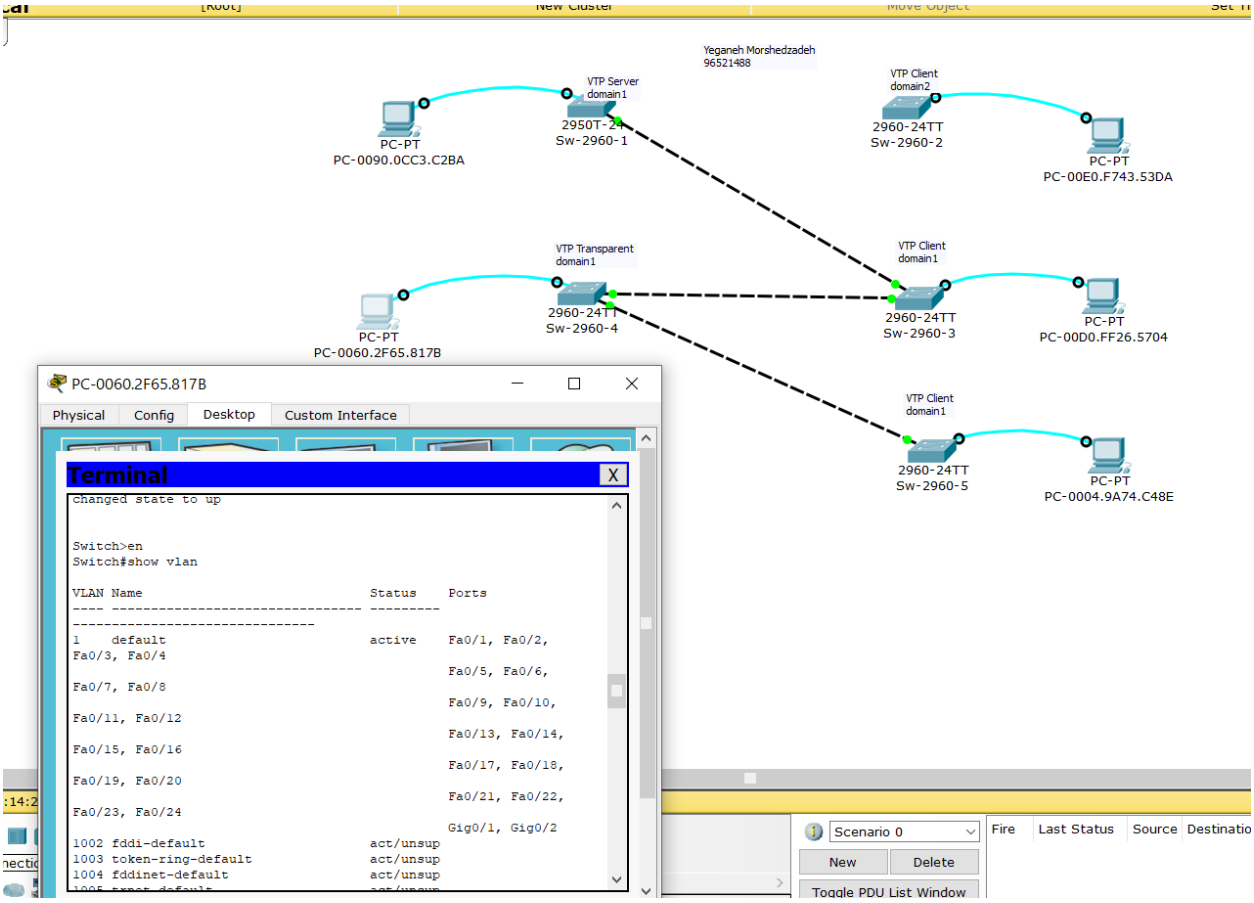
- Transparent mode

در اینجا نیز مشابه قسمت قبل domain1 را ساخته و سرور را بر روی این دامنه تنظیم میکنیم. همچنین سوییچ ۳ را در حالت clientتنظیم میکنیم و پورت اتصال fastethernet0/1 را در حالت trunk قرار داده و پس از آن سوییچ ۳ نیز vlanهای سرور را نیز خواهد داشت.

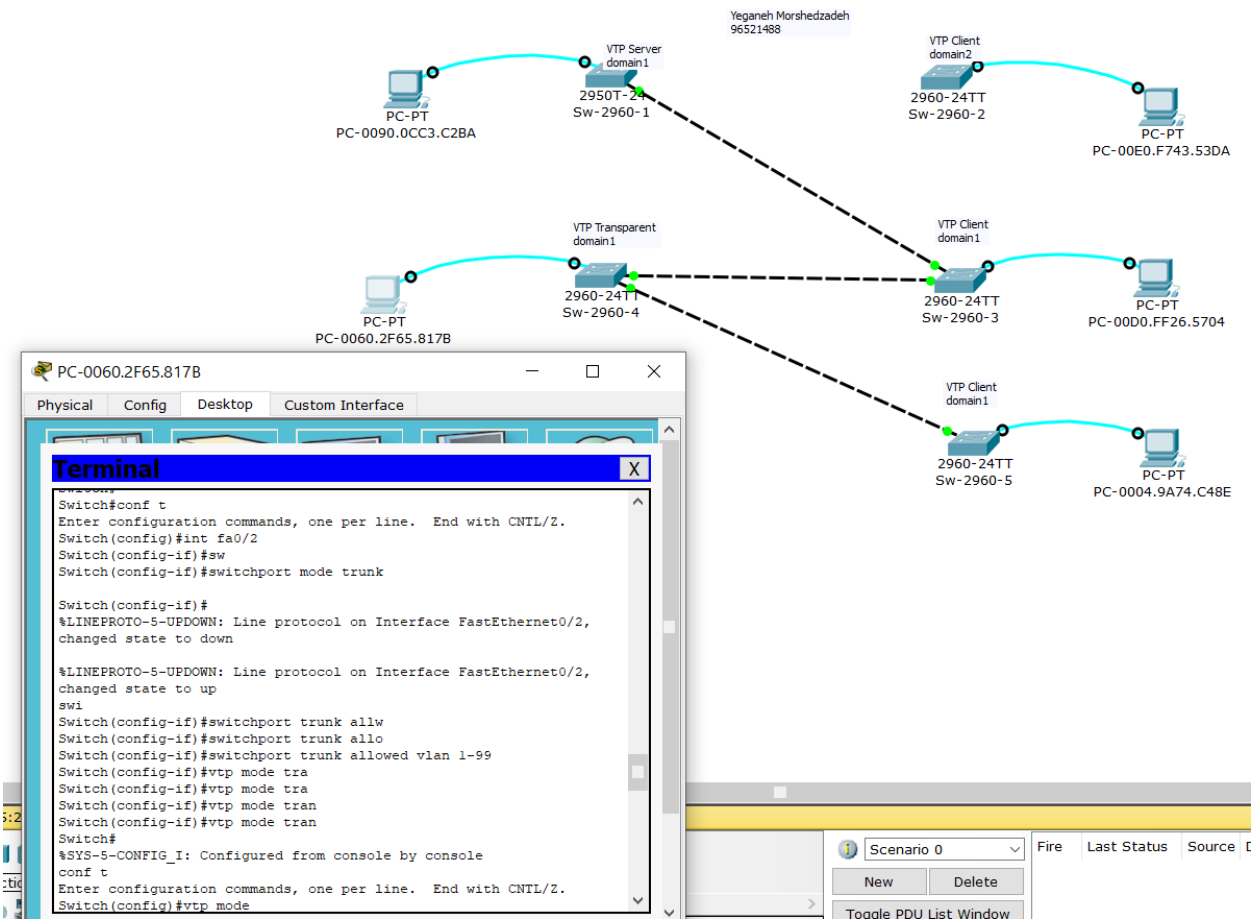


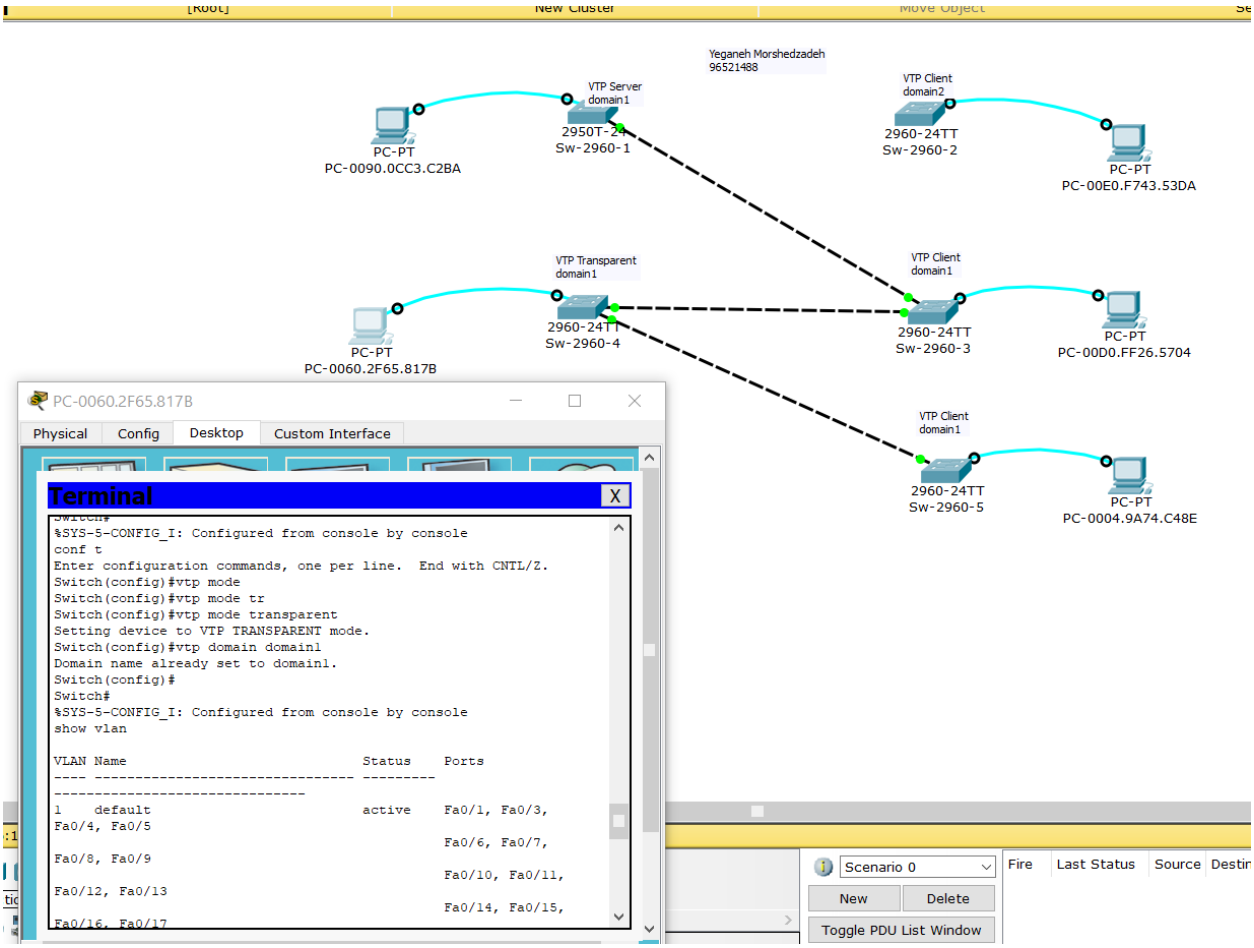
حال سوییچ ۴ را بر روی حالت transparentتنظیم میکنیم. مشاهده میشود که قبل و بعد از این تنظیمات، VLANهای این سوییچ (۴) هیچ تغییری نکرده و یعنی configuration ها را با خود synchronize نکرده است.

سوییچ ۴ قبل از تنظیمات:

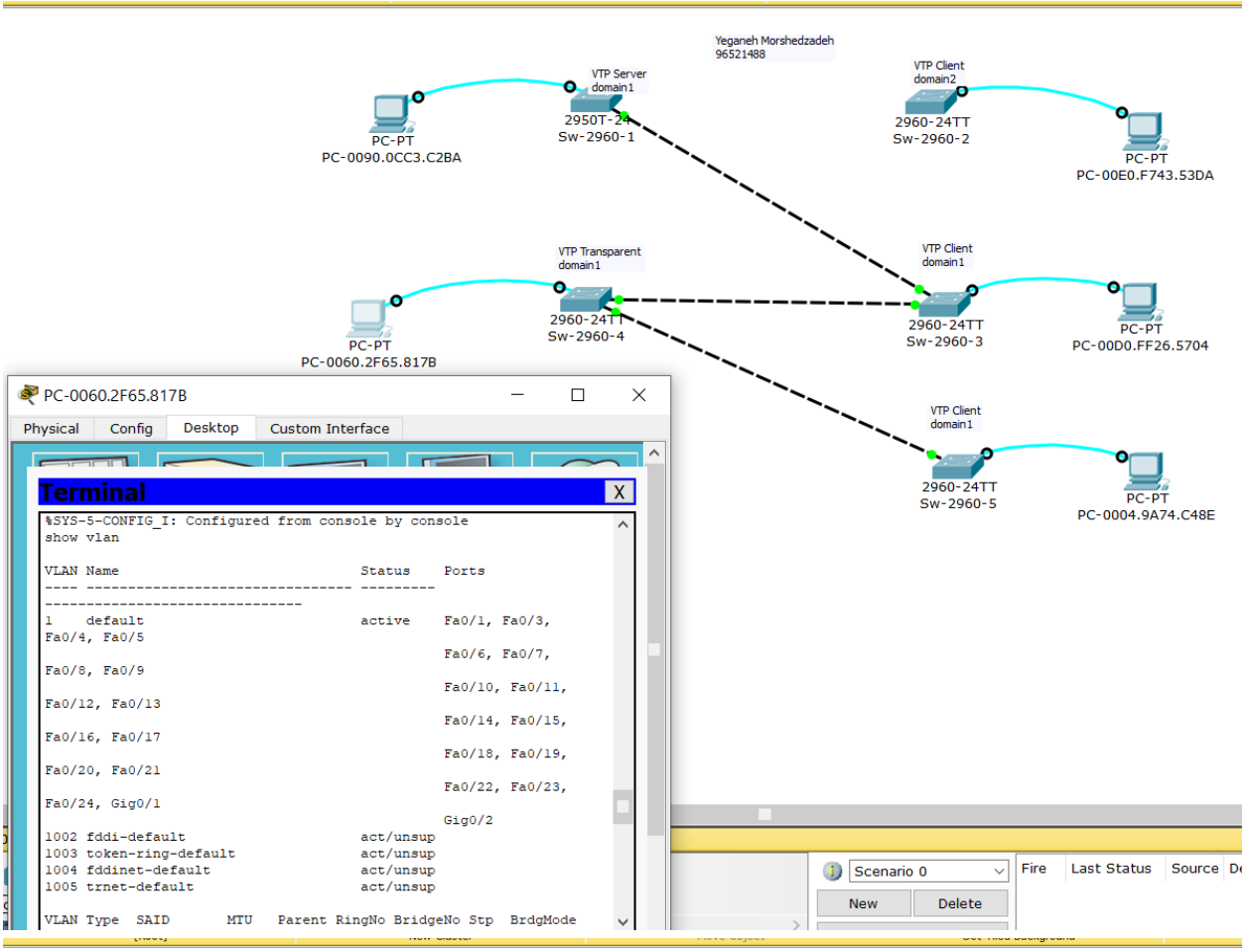


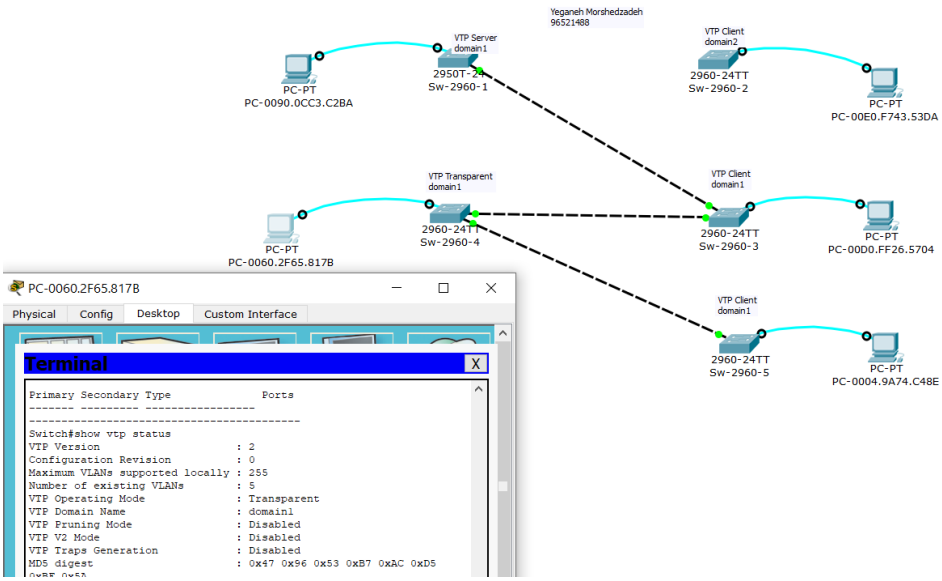
تنظیمات برای سوییچ ۴:


Yeganeh Morshedzadeh
96521488
VTP Server
domain1
2950T-24
Sw-2960-1
VTP Client
domain2
2960-24TT
Sw-2960-2
PC-PT
PC-0090.0CC3.C2BA
PC-PT
PC-00E0.F743.53DA
VTP Transparent
domain1
2960-24TT
Sw-2960-4
VTP Client
domain1
2960-24TT
Sw-2960-3
PC-PT
PC-0060.2F65.817B
PC-PT
PC-00D0.FF26.5704
VTP Client
domain1
2960-24TT
Sw-2960-5
PC-PT
PC-0004.9A74.C48E
PC-0060.2F65.817B
Physical
Config
Desktop
Custom Interface
Terminal
X
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#sw
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
swi
Switch(config-if)#switchport trunk allw
Switch(config-if)#switchport trunk allo
Switch(config-if)#switchport trunk allowed vlan 1-99
Switch(config-if)#vtp mode tra
Switch(config-if)#vtp mode tra
Switch(config-if)#vtp mode tran
Switch(config-if)#vtp mode tran
Switch#
%SYS-5-CONFIG_I: Configured from console by console
conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp mode
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source



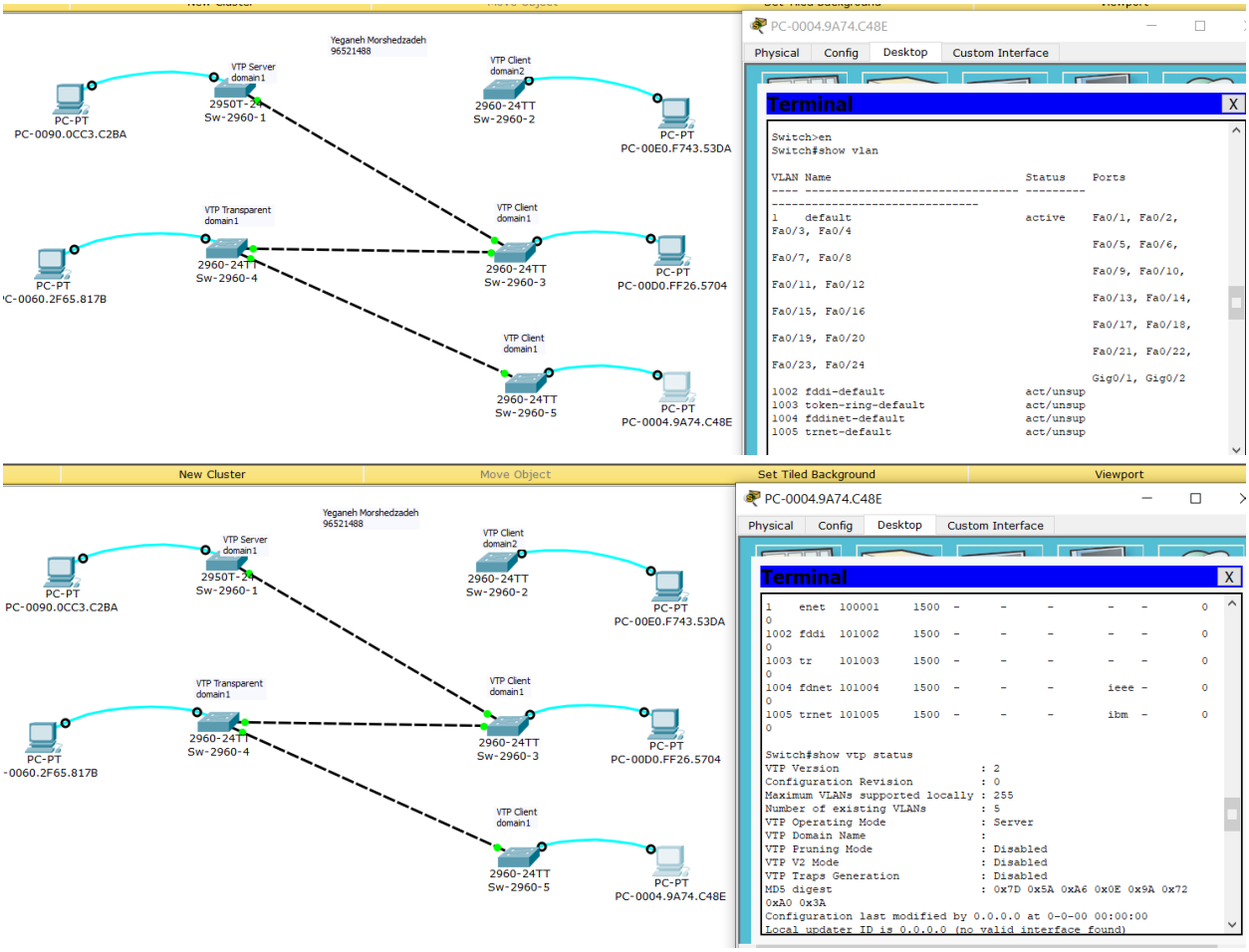
سوییچ ۴ بعد از تنظیمات:


Yeganeh Morshedzadeh
96521488
VTP Server
domain1
2950T-24
Sw-2960-1
VTP Client
domain2
2960-24TT
Sw-2960-2
PC-PT
PC-0090.0CC3.C2BA
PC-PT
PC-00E0.F743.53DA
VTP Transparent
domain1
2960-24TT
Sw-2960-4
VTP Client
domain1
2960-24TT
Sw-2960-3
PC-PT
PC-0060.2F65.817B
PC-PT
PC-00D0.FF26.5704
VTP Client
domain1
2960-24TT
Sw-2960-5
PC-PT
PC-0004.9A74.C48E
PC-0060.2F65.817B
Physical
Config
Desktop
Custom Interface
Terminal
%SYS-5-CONFIG_I: Configured from console by console
show vlan
VLAN Name Status Ports
1 default active Fa0/1, 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, Gig0/1
Gig0/2
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode
Scenario 0
New
Delete
Fire
Last Status
Source

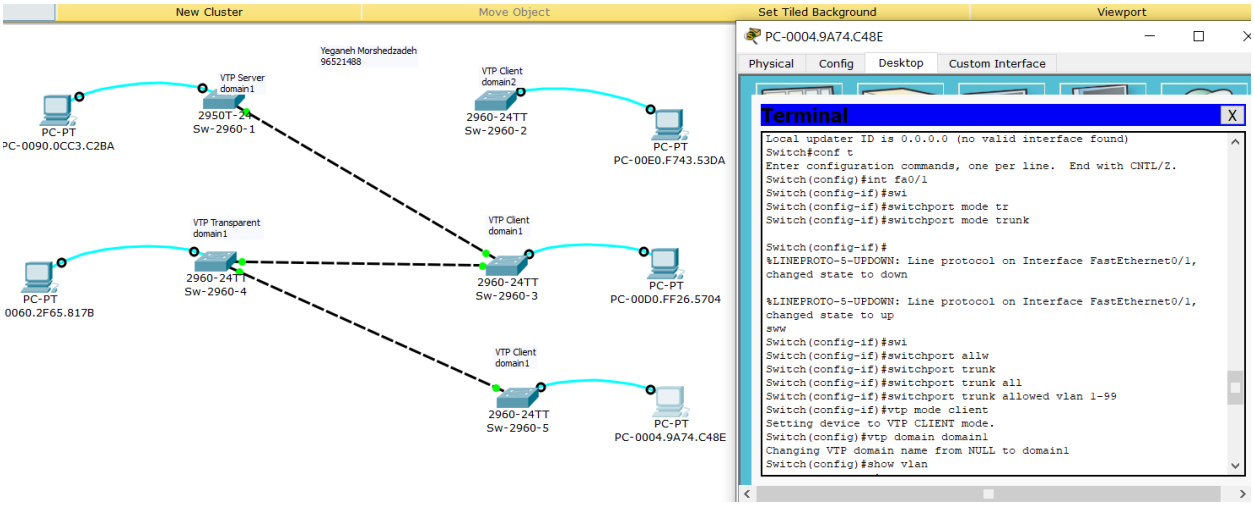

Yeganeh Morshedzadeh
96521488
VTP Server
domain1
2950T-24
Sw-2960-1
VTP Client
domain2
2960-24TT
Sw-2960-2
PC-PT
PC-0090.0CC3.C2BA
PC-PT
PC-00E0.F743.53DA
VTP Transparent
domain1
2960-24TT
Sw-2960-4
VTP Client
domain1
2960-24TT
Sw-2960-3
PC-PT
PC-0060.2F65.817B
PC-PT
PC-00D0.FF26.5704
VTP Client
domain1
2960-24TT
Sw-2960-5
PC-PT
PC-0004.9A74.C48E
PC-0060.2F65.817B
Physical
Config
Desktop
Custom Interface
Terminal
Primary Secondary Type Ports
Switch#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Transparent
VTP Domain Name : domain1
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x47 0x96 0x53 0xB7 0xAC 0xD5

حال در ادامه بررسی میکنیم که آیا توانسته این اطلاعات را به سوییچ شماره ۵ که در حالت clientتنظیم شده است برساند یا خیر

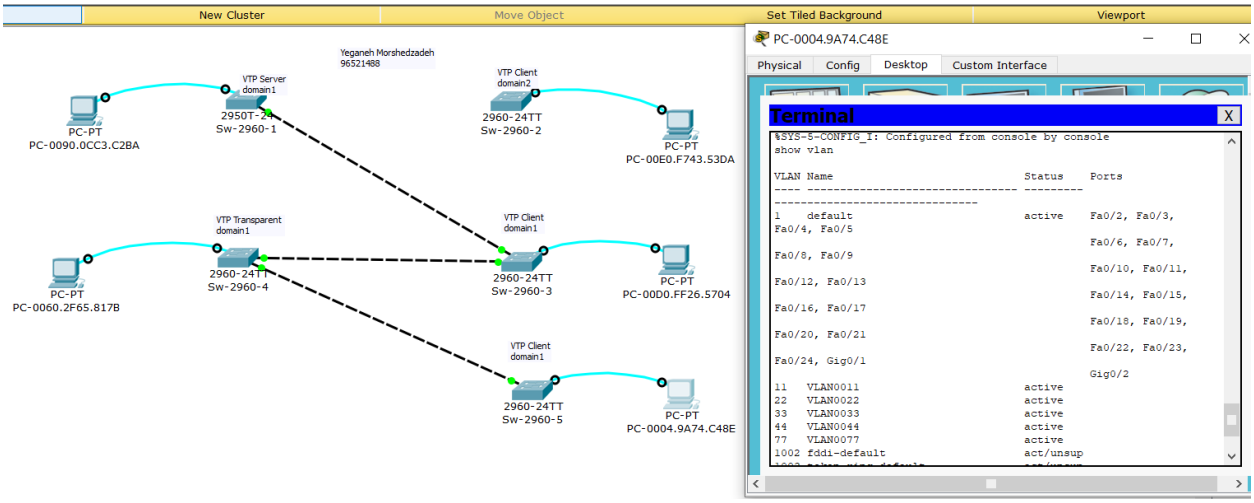
سوییچ ۵ قبل از تنظیمات:



تنظیمات برای سوییچ ۵:



سوییچ ۵ بعد از تنظیمات:

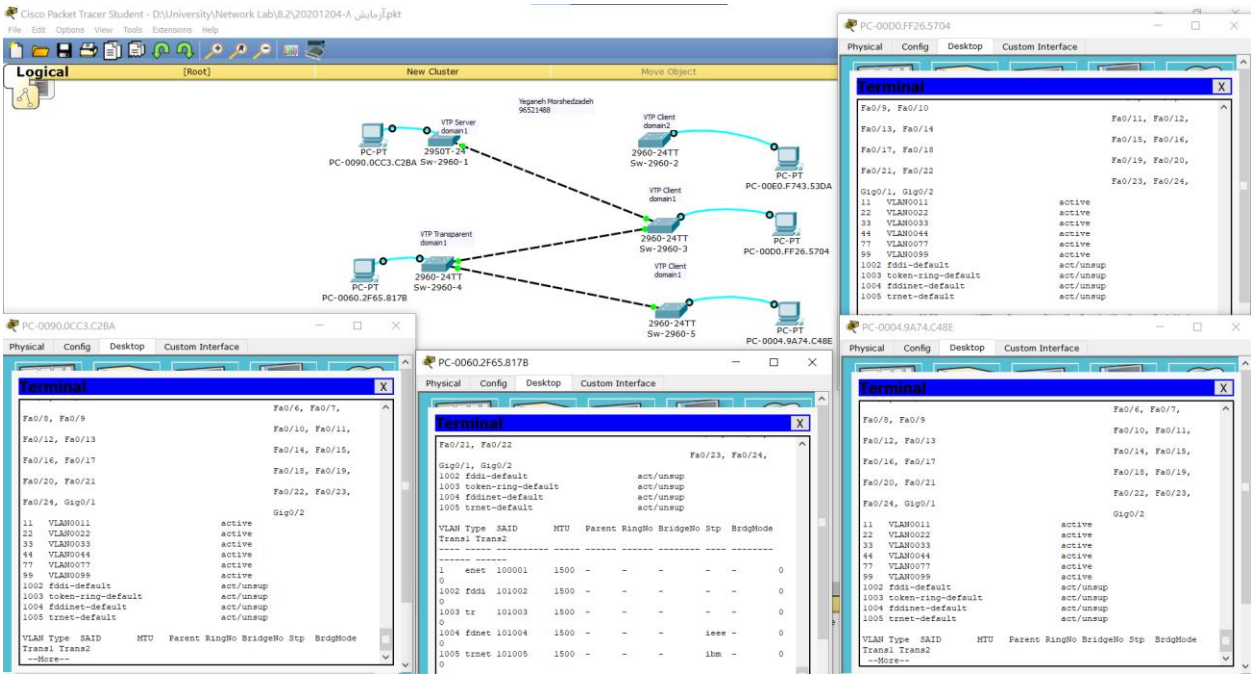


همان طور که مشاهده شده این سوییچ ها در domain1قرار گرفتند و در حالت clientهم اطلاعات را در شبکه تبلیغ میکردند و هم خودشان configurationهای خود را با اطلاعات دریافتی از VTP server هماهنگ میکردند. در حالت transparent نیز سوییچ configuration را برای خود اعمال نمیکند ولی اطلاعات را در شبکه پخش میکند از همین خاطر سوییچ ۵ نیز توانست از vlanهای تنظیم شده در server باخبر شود.

حالت off نیز همان حالت عادی شبکه بدون هیچ تنظیمی است که نه اطلاعات VLANرا رد و بدل میکند و نه از اطلاعات و configuration های دریافتی تاثیر میپذیرد و تنها خود میتواند با دستورات به صورت مستقیم VLANهای خود را اصلاح، ایجاد و حذف کند.

لازم به ذکر است که در حالت client نمیتوان VLANها را ایجاد، اصلاح و حذف کرد.

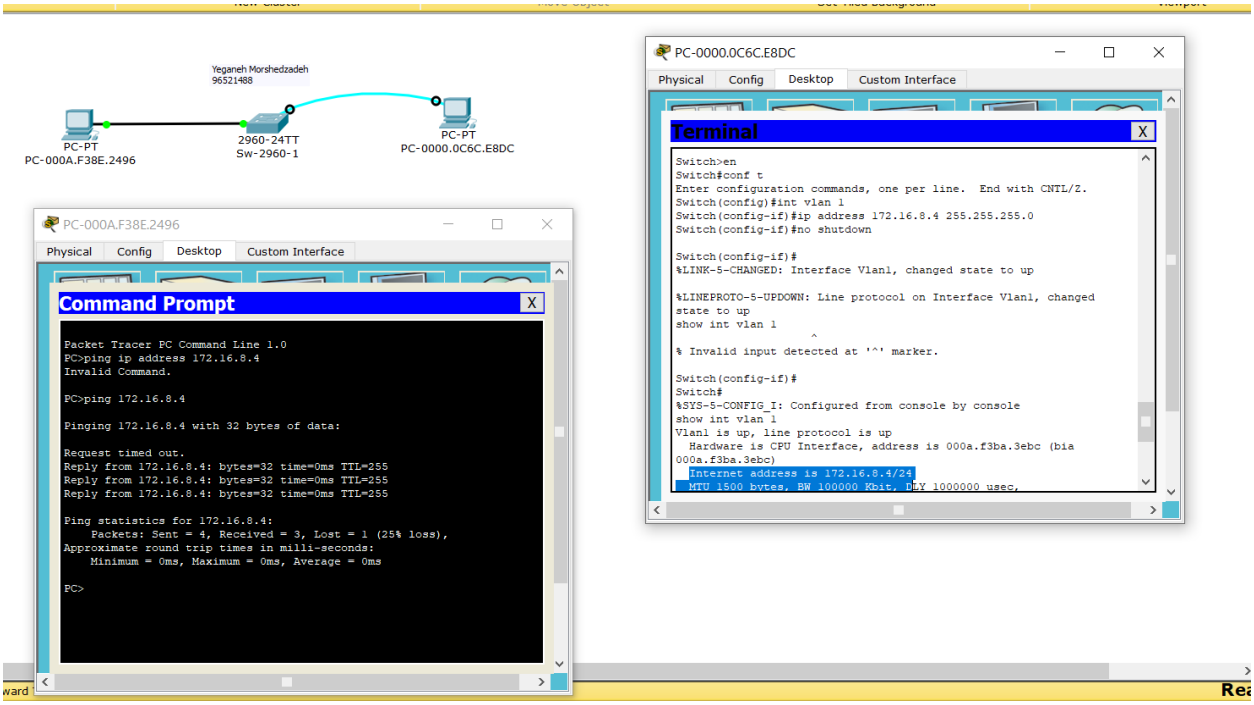
مشاهده میشود که با اضافه کردن vlan99 در VTP server سوییچ های clientنیز این VLAN را در خود تنظیم کردند ولی سوییچ transparentاین کار را نکرد ولی اطلاعات را به سوییچ ۵ رساند.



❖ بخش سوم : چگونگی تخصیص IP به سوئیچ لایه ۲ (۴۰ نمره)

1- یک راه‌کار جهت اختصاص IP به سوئیچ لایه ۲ ارائه کنید. تمام مراحل انجام کار در زیر توضیح داده شود. ضمنا همه مراحل در محیط Packet Tracer انجام و در نهایت تصویری از Packet Tracer به همراه پنجره CLI که تمامی دستورات و خروجی آن را شامل می‌شود بایستی در زیر همین قسمت اضافه شود.

راهنمائی : بعد از اختصاص IP به سوئیچ بایستی بتوانید از یک کامپیوتر به آن Ping کنید. در تصویر بند ۱ بایستی خروجی دستور Ping به سوئیچ نیز مشخص باشد.



https://geek-university.com/ccna/assign-the-switch-ip-address/

ارزیابی آزمایش :

براساس نمره درج شده در جلوی هر بخش.

کپی علاوه بر حذف نمره هریک از کپی کنندگان، به همان اندازه نمره منفی برای کپی‌کنندگان منظور خواهد شد.

با آرزوی توفیق

عباس عزیز جلالی