

گزارش هفتم آزمایشگاه شبکه های کامپیوتری

اعضای گروه:

پارسا عصمت‌لو

سهیل شهرابی

فهرست مطالب

2.....	فهرست مطالب
3.....	پیش گزارش آزمایش هشتم.....
3.....	سوالات تحلیلی آزمایش هفتم.....
3.....	سوال ۱.....
4.....	سوال ۲.....
4.....	سوال ۳.....
5.....	گزارش آزمایش هفتم.....
5.....	مرحله اول.....
5.....	گام اول.....
6.....	گام دوم.....
6.....	آی پی دهی هاست و نتورک-توضیحات تشریحی.....
6.....	آی پی دهی هاست و نتورک-جدول.....
6.....	گام سوم.....
6.....	تعریف VLAN ها.....
8.....	گام پایانی.....
8.....	بینگ گرفتن.....
9.....	مرحله دوم.....
9.....	گام اول.....
9.....	گام دوم.....
9.....	آی پی دهی هاست و نتورک-توضیحات تشریحی.....
10.....	آی پی دهی هاست و نتورک-جدول.....
10.....	گام سوم.....
10.....	ایجاد اینترفیس های مجازی.....
11.....	گام پایانی.....
11.....	بینگ گرفتن.....

پیش گزارش آزمایش هشتم

سوال ۱

Root Access Points (RAPs)

This access point is connected to the wired network and serves as the “root” or “gateway” to the wired network. RAPs have a wired connection back to a Cisco Wireless LAN Controller. They use the backhaul wireless interface to communicate with neighboring Mesh APs.

Mesh Access Points (MAPs)

The Mesh APs are remote APs that are typically located on rooftops or towers and can connect up to 32 MAPs over a 5GHz backhaul. During bootup, an access point will try to become a RAP if it's connected to the wired network. Conversely, if a RAP loses its wired network connection, it will attempt to become a MAP and will search for a RAP.

AWPP

Each AP runs the Adaptive Wireless Path Protocol (AWPP)—a new protocol designed from the ground up by Cisco specifically for the wireless environment. This protocol allows RAPs to communicate with each other to determine the best path back to the wired network via the RAP. Once the optimal path is established, AWPP continues to run in the background to establish alternative routes back to the RAP just in case the topology changes or conditions cause the link strength to weaken.

This protocol takes into consideration things like interference and characteristics of the specific radio so that the mesh can be self-configuring and self-healing. AWPP actually has the ability to consider all relevant elements of the wireless environment so that the mesh network's functionality isn't disrupted and can provide consistent coverage.

This is pretty powerful considering how truly dynamic a wireless environment is. When there's interference or if APs are added or removed, the Adaptive Wireless Path Protocol reconfigures the path back to the rooftop AP (RAP). Again, in response to the highly dynamic wireless environment, AWPP uses a “stickiness” factor to mitigate routes that ensure that an event, such as a

large truck passing through the mesh causing a temporary disruption, doesn't cause the mesh to change unnecessarily.

سوال ۲

در امنیت ارتباطات بی‌سیم، برخی راهکارها و تکنیک‌ها برای محافظت و افزایش امنیت شبکه‌های بی‌سیم در نظر گرفته شده‌اند. در زیر به برخی از این راهکارها اشاره می‌کنم:

1. استفاده از رمزنگاری (Encryption): استفاده از رمزنگاری برای حفاظت از ارتباطات بی‌سیم بسیار مهم است. این روش با استفاده از الگوریتم‌های رمزنگاری مطمئن، اطلاعات را در حین انتقال از دسترس ناخواسته محافظت می‌کند.
2. شناسایی و احراز هویت (Authentication): در شبکه‌های بی‌سیم، استفاده از مکانیزم‌های شناسایی و احراز هویت برای تایید هویت دستگاه‌ها و کاربران از اهمیت بالایی برخوردار است. مثلاً استفاده از پروتکل‌های مانند WPA2-PSK یا WPA3 برای احراز هویت و دسترسی به شبکه.
3. مدیریت دسترسی (Access Management): این راهکار شامل تنظیمات مربوط به دسترسی و مجوزها می‌شود. مثلاً استفاده از ماکفیلترینگ (MAC Filtering) برای محدود کردن دسترسی به شبکه بر اساس آدرس فیزیکی مک (MAC) دستگاه‌ها.
4. ردیابی و جلوگیری از نفوذ (Intrusion Detection and Prevention): این راهکار شامل استفاده از سیستم‌های ردیابی و جلوگیری از نفوذ است. این سیستم‌ها مانیتورینگ و تشخیص فعالیت‌های ناخواسته یا مخرب در شبکه را انجام می‌دهند و بر اساس قوانین تعیین شده، اقدامات لازم را برای جلوگیری از نفوذ انجام می‌دهند.
5. پنهان‌سازی شبکه (Network Hiding): در این روش، شبکه بی‌سیم به صورت پنهانی و غیرقابل رؤیت برای دستگاه‌ها خارجی قرار می‌گیرد. این کار با کاهش شناسایی و امکان تشخیص شبکه توسط حملات احتمالی موجود در محیط، امنیت را افزایش می‌دهد.
6. فایروال (Firewall): استفاده از فایروال بی‌سیم برای کنترل و مدیریت ترافیک و فیلترینگ بسته‌های داده ورودی و خروجی استفاده می‌شود. این راهکار امکان تشخیص و جلوگیری از حملات ناخواسته را فراهم می‌دهد.

توجه داشته باشید که این راهکارها تنها بخشی از راهکارهای ممکن در امنیت شبکه‌های بی‌سیم هستند و بسته به نیازها و شرایط خاص هر سازمان و محیط، ممکن است راهکارهای دیگری نیز در نظر گرفته شود. همچنین، اجرای صحیح و پیاده‌سازی مناسب این راهکارها نیز از اهمیت بالایی برخوردار است.

سوالات تحلیلی آزمایش هفتم

سوال ۱

802.1Q و ISL دو استاندارد متفاوت برای تگ‌گذاری و سگمنت‌بندی ترافیک شبکه در لایه دوم مدل OSI هستند. تفاوت های اصلی این دو در ذیل آمده است.

1. 802.1Q

- 802.1Q یک استاندارد VLAN است که برای تگ‌گذاری بسته‌های داده در شبکه‌های Ethernet استفاده می‌شود.
- در استاندارد 802.1Q، یک برچسب VLAN به بسته‌های داده اضافه می‌شود تا بتواند در شبکه‌های شناسایی شود و درون شبکه مناسب توزیع شود.
- برچسب 12 VLAN بیتی است و اطلاعات مانند شناسه VLAN و اولویت ترافیک را در خود ذخیره می‌کند.
- استاندارد 802.1Q را می‌توان بر روی تجهیزات شبکه متنوعی نصب کرد و از جمله سوئیچ‌ها و روترها پشتیبانی می‌کند.

2. ISL یا Internal Switch Link

- ISL نیز یک استاندارد سگمنت‌بندی و تگ‌گذاری بسته‌های داده در شبکه‌های VLAN است، اما از یک فریم خاص به نام ISL استفاده می‌کند.
- در استاندارد ISL، برچسب VLAN به بسته‌های داده اضافه می‌شود و اطلاعات مربوط به VLAN و سایر اطلاعات شبکه را درون فریم ISL قرار می‌دهد.
- ISL یک پروتکل ساختگی سیسکو است و از آن به عنوان روش اصلی برای ترافیک VLAN در شبکه‌های سیسکو استفاده می‌شود.
- این استاندارد تقریباً در همه تجهیزات سیسکو قابل پیکربندی است و برای ارتباط بین سوئیچ‌های سیسکو در شبکه‌های VLAN استفاده می‌شود.

به طور خلاصه، 802.1Q یک استاندارد رایج و عمومی تر برای تگ‌گذاری VLAN است که می‌تواند بر روی تجهیزات شبکه متنوعی استفاده شود. از سوی دیگر، ISL یک پروتکل خاص سیسکو است که بیشتر در شبکه‌های سیسکو استفاده می‌شود و بر روی تجهیزات سیسکو پشتیبانی می‌شود.

سوال ۲

خیر. لینک trunk در دو بخش مورد استفاده قرار میگیرد: سویچ-روتر یا سویچ-سویچ هدف اصلی از لینک trunk هدایت فریم ها به vlan هدف است تا در سویچ 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!

سوال ۳

دامنه VTP Domain یا VTP در شبکه های سیسکو استفاده می شود. VTP مخفف VLAN Trunking Protocol است و برای تنظیم و مدیریت VLAN ها در شبکه های سیسکو استفاده می شود. دامنه VTP، مجموعه ای از دستگاه های شبکه است که اطلاعات VLAN را با یکدیگر به اشتراک می گذارند. در زیر کاربردهای دامنه VTP آمده است.

1. همگام سازی VLAN: با استفاده از دامنه VTP، می توان VLAN ها را در سراسر شبکه همگام کرد. یک روتر یا سوئیچ می تواند به عنوان سرور VTP عمل کند و تغییرات در VLAN ها را به سایر دستگاه ها اعلام کند. این کار باعث می شود که تمام دستگاه ها در شبکه به صورت خودکار اطلاعات VLAN را به روز رسانی کنند.
2. افزایش سهولت مدیریت: با استفاده از VTP Domain، مدیران شبکه می توانند تغییرات در VLAN ها را به راحتی اعمال کنند. به جای تنظیم VLAN در هر دستگاه به صورت جداگانه، می توان این تغییرات را در یک سرور VTP اعمال کرده و سایر دستگاه ها به روز رسانی شده را دریافت کنند.
3. امنیت و کنترل دسترسی: با استفاده از دامنه VTP می توان کنترل دسترسی به تغییرات VLAN را مدیریت کرد. با تعریف یک رمز عبور VTP، فقط افراد مجاز می توانند تغییرات را اعمال کنند و از جلوگیری از اعمال تغییرات غیرمجاز جلوگیری می شود.

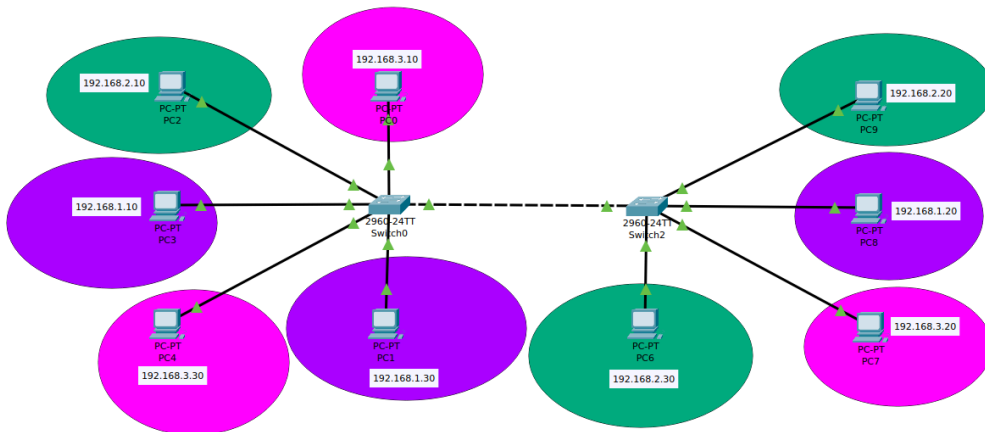
در کل، دامنه VTP در شبکه های سیسکو برای همگام سازی و مدیریت VLAN ها استفاده می شود و باعث افزایش سهولت مدیریت و امنیت شبکه می شود.

گزارش آزمایش هفتم

مرحله اول

گام اول

در گام اول تمامی روترها، سوئیچ ها end device ها و اتصالات میان آنها را مطابق شکل صورت آزمایش در جای خود قرار دادیم. شکل ذیل حالت نهایی است.



گام دوم

آی پی دهی هاست و نتورک-توضیحات تشریحی

در مرحله دوم شروع به اطلاق IP به تک تک دیوایس ها و interface روتر ها به صورت Classfull کردیم. از آنجایی که در این توپولوژی روتری وجود نداشت، تنها ۳ شبکه VLAN تعریف کردیم، شبکه اول 192.168.1.0 شبکه دوم 192.168.2.0 و شبکه سوم 192.168.3.0 می باشد. همچنین هر شبکه

VLAN شامل ۳ هاست است که در آن ها بایت پایانی آی پی برابر ۱۰ یا ۲۰ یا ۳۰ می باشد.

آی پی دهی هاست و نتورک-جدول

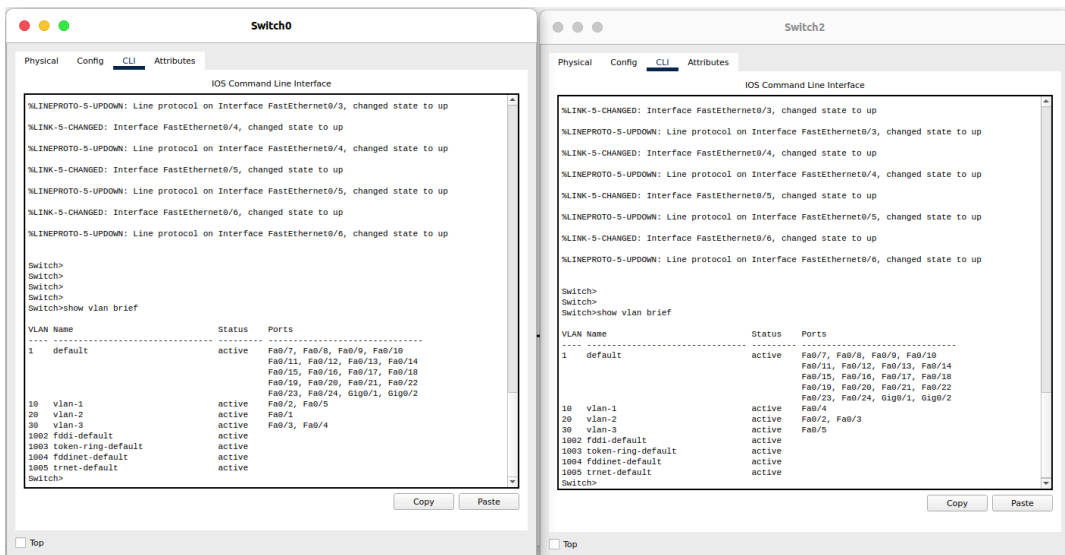
Device name	Ip	Mask	Network	Port	VLAN ID
PC0	192.168.3.10	255.255.255.0	192.168.3.0	FastEthernet0	30
PC1	192.168.1.30	255.255.255.0	192.168.1.0	FastEthernet0	10
PC2	192.168.2.10	255.255.255.0	192.168.2.0	FastEthernet0	20
PC3	192.168.1.10	255.255.255.0	192.168.1.0	FastEthernet0	10
PC4	192.168.3.30	255.255.255.0	192.168.3.0	FastEthernet0	30
PC6	192.168.2.30	255.255.255.0	192.168.2.0	FastEthernet0	20
PC7	192.168.3.20	255.255.255.0	192.168.3.0	FastEthernet0	30
PC8	192.168.1.20	255.255.255.0	192.168.1.0	FastEthernet0	10
PC9	192.168.2.20	255.255.255.0	192.168.2.0	FastEthernet0	20

گام سوم

تعریف VLAN ها

در مرحله سوم شروع کردیم به تعریف VLAN ها در هر سویچ. برای این گام در هر سویچ ابتدا از قسمت VLAN Databases -> Config سه VLAN با id های 10، 20 و 30 تعریف کردیم و پس از آن هاست هایی که در VLAN شماره ۱ بودند را به VLAN ID شماره ۱۰، هاست هایی که در VLAN شماره ۲ بودند را به VLAN ID شماره ۲۰، و هاست هایی که در VLAN شماره ۳ بودند را به VLAN ID شماره ۳۰ متصل کردیم. برای این منظور اگر هاستی از VLAN شماره ۲ به اینترفیس FastEthernet0/1 وصل شده بود، از مسیر Config -> Interfaces -> FastEthernet0/1 -> VLAN آن را از ۱ (شماره VLAN دیفالت) به شماره ۲۰ تغییر دادیم.

پس از انجام این مرحله برای هر دو سوئیچ، اینترفیس هایی که ۲ سویچ را به یکدیگر متصل کرده اند را به حالت Trunk بردیم تا ۲ سوئیچ بسته هایی از هر VLAN را با این اینترفیس برای یکدیگر بفرستند.

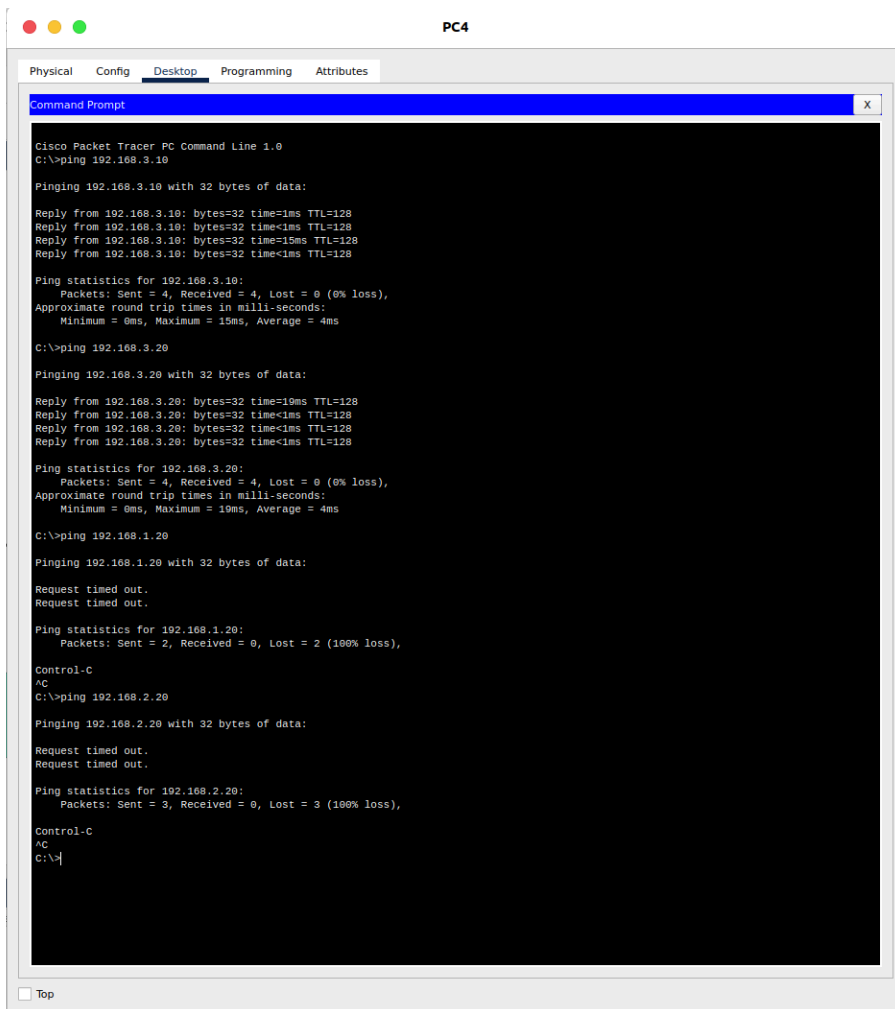


در تصویر بالا خروجی دستور show vlan brief در هر ۲ سویچ نشان داده شده است که هر روتر به کدام اینترفیسی از سویچ صفر یا ۲ متصل شده است.

گام پایانی

پینگ گرفتن

در پایان برای اطمینان از اتصالات و کانفیگ ها هاست های مختلف را پینگ گرفتیم و موفقیت آمیز بود.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time<1ms TTL=128
Reply from 192.168.3.10: bytes=32 time<1ms TTL=128
Reply from 192.168.3.10: bytes=32 time=15ms TTL=128
Reply from 192.168.3.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 4ms

C:\>ping 192.168.3.20

Pinging 192.168.3.20 with 32 bytes of data:

Reply from 192.168.3.20: bytes=32 time=19ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 4ms

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 192.168.1.20:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 192.168.2.20:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

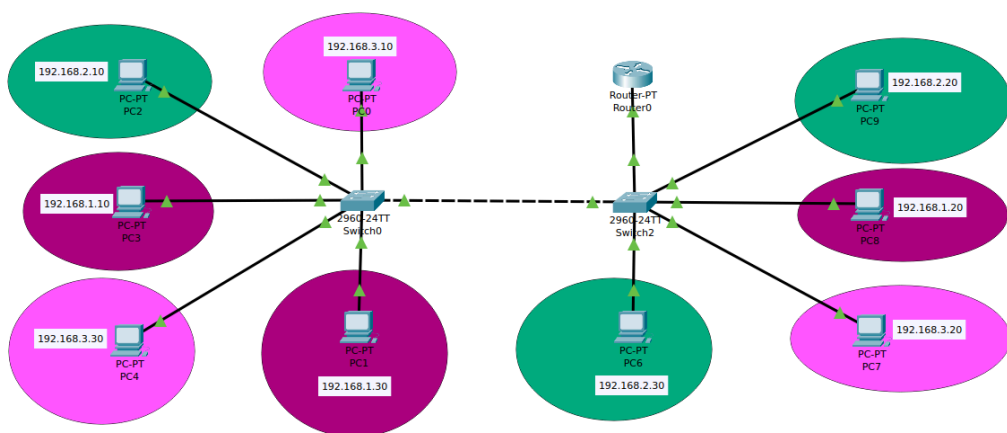
Control-C
^C
C:\>
```

همانطور که در تصویر بالا مشخص است، با هاستی از آی پی 192.168.3.30 در VLAN شماره ۳، هاست های دیگر با آی پی 192.168.3.10 و 192.168.3.20 را پینگ گرفتیم و موفقیت آمیز بود. اما وقتی هاست هایی از VLAN های شماره ۱ و ۲ را پینگ گرفتیم Request Timed out گرفتیم.

مرحله دوم

گام اول

در ابتدا یک روتر جدید را به سوئیچ ۲ متصل کردیم. تصویر توپولوژی جدید در ذیل آمده است.



پس از افزودن روتر، نوع اتصال روتر به اینترفیس سوئیچ را از نوع Trunk قرار می‌دهیم تا مانند قبل تمامی بسته‌ها در هر VLAN به روتر فرستاده شود تا مقصد آن توسط روتر مشخص شود و مسیریابی میان تمامی روترها برقرار شود.

گام دوم

آی پی دهی هاست و نتورک-توضیحات تشریحی

همچنین برای تمامی هاست‌ها یک Default Gateway در نظر گرفته شد تا اگر قصد ping کردن VLAN‌های خارج از VLAN خود داشتیم درخواستمان به روتر برسد، برای هاست‌های درون VLAN ۱ از Default Gateway برابر با 192.168.1.40 برای هاست‌های درون VLAN ۲ از Default Gateway برابر با 192.168.2.40 برای هاست‌های درون VLAN ۳ از Default Gateway برابر با 192.168.3.40 استفاده کردیم.

آی پی دهی هاست و نتورک-جدول

Device name	Ip	Mask	Network	Port	VLAN ID	Default Gateway
PC0	192.168.3.10	255.255.255.0	192.168.3.0	FastEthernet0	30	192.168.3.40

PC1	192.168.1.30	255.255.255.0	192.168.1.0	FastEthernet0	10	192.168.1.40
PC2	192.168.2.10	255.255.255.0	192.168.2.0	FastEthernet0	20	192.168.2.40
PC3	192.168.1.10	255.255.255.0	192.168.1.0	FastEthernet0	10	192.168.1.40
PC4	192.168.3.30	255.255.255.0	192.168.3.0	FastEthernet0	30	192.168.3.40
PC6	192.168.2.30	255.255.255.0	192.168.2.0	FastEthernet0	20	192.168.2.40
PC7	192.168.3.20	255.255.255.0	192.168.3.0	FastEthernet0	30	192.168.3.40
PC8	192.168.1.20	255.255.255.0	192.168.1.0	FastEthernet0	10	192.168.1.40
PC9	192.168.2.20	255.255.255.0	192.168.2.0	FastEthernet0	20	192.168.2.40

گام سوم

ایجاد اینترفیس های مجازی

در پایان یکی از اینترفیس های روتر را بدون آی پی روشن کردیم و پس از آن ۳ اینترفیس مجازی بر روی آن با آی پی های 192.168.1.40، 192.168.2.40 و 192.168.3.40 و همگی با Mask Address 255.255.255.0 ایجاد کردیم، تا VLAN های مختلف بتوانند یکدیگر را پینگ بگیرند.

تمامی دستورات نوشته شده برای روتر در ذیل آمده است:

```
Router en
Router # conf t
Router(config)# interface fa0/1
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config)# interface fa0/1.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.1.40 255.255.255.0
Router(config-subif)# exit
Router(config)# interface fa0/1.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.2.40 255.255.255.0
Router(config-subif)# exit
Router(config)# interface fa0/1.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.3.40 255.255.255.0
Router(config-subif)# exit
```

گام پایانی

پینگ گرفتن



The screenshot shows a virtual machine window titled "PC4" with a "Command Prompt" window open. The Command Prompt displays the output of the "ipconfig" command, showing network configuration for a FastEthernet0 interface. It then shows the results of three ping commands: "ping 192.168.2.20", "ping 192.168.1.20", and "ping 192.168.3.20". All pings are successful, showing 0% loss and 0ms round trip times.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20A:F3FF:FE4D:574D
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.3.30
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::

C:\>ping 192.168.2.20

Pinging 192.168.2.20 with 32 bytes of data:

Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127
Reply from 192.168.1.20: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.20

Pinging 192.168.3.20 with 32 bytes of data:

Reply from 192.168.3.20: bytes=32 time<1ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128
Reply from 192.168.3.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

همانطور که در تصویر بالا مشخص است، خود هاست در VLAN شماره ۳ است با آی پی 192.168.3.30 و توانسته علاوه بر هاست 192.168.3.20، هاست هایی با آی پی 192.168.2.20 و 192.168.1.20 را به ترتیب از VLAN های شماره ۱ و ۲ پینگ بگیرد.