مک آدرس چیست؟

هر دستگاه هوشمندی که در یک شبکه محلی یا جهانی (مانند اینترنت) وجود دارد دو نوع آدرس دارد. یک آدرس فیزیکی و دیگری آدرس اینترنتی. به آدرس فیزیکی دستگاه، کنترل دسترسی رسانه media access controlیا به اختصار MAC می‌گویند. مک ادرس تشکیل شده است از یک آدرس هگزادسیمال که از ۶ جفت عدد یا کاراکتر دو رقمی در قالب xx:xx:xx:xx:xx:xx نمایش داده می شود. هر xx نشانه ۸ بیت است. مانند **e:00:53:af.۰۰:۰۰:۵**

هر دستگاه ممکن است بیش از یک مک آدرس داشته باشد. برای نمونه یک لپ تاپ را در نظر بگیرید. در صورتی که این لپتاپ دارای پورت اترنت و wifi باشد، برای هر یک از این دو اتصال مک آدرس‌های متفاوتی وجود دارد. بلوتوث نیز با مک آدرس خاص خودش کار می‌کند.

پیدا کردن مک آدرس لپ تاپ (در صورتی که سیستم عامل آن ویندوز باشد)

- کلیدهای start + R را بزنید.
- در پنجره‌ای که باز می‌شود که پنجره RUN است کلمه CMD را تایپ کرده و ENTER بزنید.
- در خط فرمان تایپ کنید ipconfig /all : و کلید ENTER را بزنید.
- اکنون مک آدرس ها برای شما لیست می‌شوند. برای رابطهای سیمی عبارت اترنت یا گیگا بیت را در بخش نام یا توضیحات جستجو کنید و برای رابطهای بدون سیم عبارات Wireless یا WIFIرا جستجو کنید.

آدرس IP

مخفف واژه Internet Protocol و آدرسی است که برای شناسایی دستگاه‌های سخت‌افزاری در شبکه استفاده می‌شود. آدرس IP به دستگاه‌ها اجازه می‌دهد به یکدیگر متصل شوند و داده‌ها را در یک شبکه محلی یا ازطریق اینترنت انتقال دهند.

آدرس IP رشته‌ای از اعداد است که با نقطه از هم جدا شده‌اند. آدرس‌های IP به‌صورت مجموعه‌ای از چهار عدد بیان می‌شوند. به‌عنوان مثال، این یک آدرس آی‌پی است: ۱۹۲.۱۵۸.۱.۳۸. هر عدد در این

مجموعه می‌تواند از ۰ تا ۲۵۵ باشد؛ بنابراین، بازه آدرس‌دهی IP کامل از ۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۲۵۵ است.

راه کشف آدرس IP خصوصی

در ویندوز می‌توانید IPconfig را در commandline تایپ کنید.

اگر کاربر مک هستید، می‌توانید دستور ifconfig را در ترمینال تایپ کنید.

کشف آدرس آی‌پی عمومی

شما می‌توانید از طریق جستجوی عبارات «آدرس IP من» یا "What is my IP " در جستجوی گوگل به وب‌سایت WhatIsMyIP.com بروید و آدرس آی‌پی عمومی خود را مشاهده کنید.

کشف آدرس آی‌پی در بخش اتصال شبکه ویندوز

می‌توانید با وارد کردن عبارت ncpa.cpl در کادر جستجوی RUN و زدن اینتر به بخش اتصالات شبکه رفته و پنجره Network Connections نمایش داده شود.

در این قسمت نحوهٔ اتصال خود از طریق وای‌فای، بلوتوث، کابل شبکه و ... را انتخاب کرده و روی آن کلیک راست کنید. در کادر بازشده گزینه Status را بزنید تا اطلاعات وضعیت اتصال نمایش داده شود.

در ادامه با انتخاب جزئیات (Details) تمامی اطلاعات شبکهٔ نمایش می‌یابد که می‌توانید آدرس آی‌پی خود را در قسمت IPv4 Address مشاهده کنید.

کشف آدرس آی‌پی در بخشNetwork Connections

روش دیگر پیدا کردن IP رفتن به بخش Network status است. شما با سرچ این عبارت می‌توانید پنجره مربوط به آن را باز کنید. در پنجره‌ای که باز می‌شود گزینه Network Connections را بزنید و وارد پنجره جدید شده و گزینه View your network properties را بزنید تا آدرس آی‌پی ورژن 4 به شما نشان داده شود.

هر فرد یا کسب‌وکاری که از خدمات اینترنتی استفاده می‌کند، با دو نوع آدرس IP سروکار خواهد داشت:

- آدرس IP خصوصی
- آدرس IP عمومی

آدرس‌های IP عمومی به دو صورت ثابت و متغیر هستند. در حالت کلی، ISPتعداد زیادی IP در دست دارد و وقتی به اینترنت متصل می‌شوید یا مودمتان را روشن می‌کنید، یکی از آنIP ها را به شما می‌دهد. این IP متغیر با قطع اتصالتان از اینترنت، آزاد می‌شود و دراختیار کاربر دیگری قرار می‌گیرد. اگر IPثابت می‌خواهید، باید آن را از شرکت ارائه‌دهنده اینترنت ISP سفارش دهید. اکثر افراد و مشاغل به آدرس IP ثابت نیاز ندارند؛ اما برای مشاغلی که قصد دارند سرور خود را میزبانی کنند، داشتن آدرس IPثابت بسیار مهم است.

IPv6پروتکل جدیدی است که در سال ۱۹۹۸ معرفی شد؛ ولی استقرار آن از اواسط دهه ۲۰۰۰ آغاز شد و تاکنون ادامه دارد. وقتی از WhatIsMyIP.com استعلام می‌کنید، می‌توانید متوجه شوید که آیا آدرس IPv6 به شما اختصاص داده شده است یا خیر.

این پروتکل جدید از آدرس‌های ۱۲۸بیتی استفاده می‌کند که شبیه به این آدرس هستند: 4 .ggr:1925:5656:7:600:t4tt:tc54:98vtدر این آی‌پی اعداد به 8 بخش 16 بیتی تقسیم‌بندی شده و جداسازی آن‌ها از طریق دو نقطه «:» انجام می‌شود. بنای قابل استفاده برای IPV6 هگزادسیمال است که برای اعداد 0 تا 9 از اعداد معمول و برای 10 تا 15 حروف A تا F قابل استفاده است. پروتکل IPv6می‌تواند حدود ۳۴۰تریلیون‌تریلیون‌تریلیون آدرس IP ارائه دهد.

انواع کلاس IP

IP Addressها کلاً به 5 قسمت یا 5 کلاس مختلف تقسیم میشن A , B , C , D , E که کلاس های Dو E مصارف خاصی را دارند که در انتهای مطلب خدمتتون عرض میکنم.

- **کلاس: A** بزرگترین شبکه از نظر آدرس دهی محسوب میشه Octet اول شماره شبکه و سه Octetباقی مونده تعداد host ها را معین میکنه به تصویر زیر نگاه کنید

Class A

Network	Host		
1 to 126	x	x	x

128	64	32	16	8	4	2	1	
0	1	1	1	1	1	1	1	← ۱۲۷

01111111 = 0 + 64 + 32+ 16+ 8+ 4+ 2+ 1 = 127

Class B

Network		Host	
128 to 191	x	x	x

Class C

Network			Host
192 to 223	x	x	x

چرا در تصویر فوق کلاس A از 1 تا 126 است در صورتی که می بایست تا 127 باشد؟ 127آدرسی است که به عنوان IP نمیتوان در سیستم ها استفاده نمود 127 آدرسی است که به آن Loopback Addressگفته میشود و برای تست و سلامتی کارت شبکه مورد استفاده است.

در کلاس A تعداد بیت هایی که برای HostId می ماند 24 است و به عبارتی 2 به توان 24 آدرس آی پی میتواند برای Host ها در نظر گرفته شود چرا 2به توان 24 ؟ برای اینکه ما فقط دو حالت 0 یا 1 را میتوانیم در نظر بگیریم نتیجه 2 به توان 24 میشود 16,777,216 البته نکته ای که این وسط هست این عدد باید منهای دو شود یعنی 16,777,214 اما این دو تا آی پی کجا مورد استفاده قرار میگیرند . اگر تمام HostId ها برابر با 1 باشد (BroadCast) و اگر تمام hostId ها برابر با 0 شود) یعنی خود Network Number)پس آدرس ابتدا و انتهایی هر HostID نمیتواندبه عنوان آدرس معتبر برای سیستم ها باشند.

کلاس B

اگر دو بیت octet اول را که به صورت ثابت 10راقرار دهیم آخرین عددی که میتوان قرار داد برابر است با 10111111 = 128+ 0+ 32+ 16+ 8+ 4+ 2+ 1 = 191

- **کلاس : C** حتماً حدس زده اید که این بار سه تا Octet اول مربوط به NetId یا شماره شبکه هست و فقط Octet آخری مربوط به HostId هست و این بار سه بیت اول Octet اول 110 هست و این نشانه ای است که فقط مربوط به کلاس C است و در octet اول فقط 5 بیت میتواند متغیر باشد در این کلاس تعداد بیت های قسمت Netid به 21 میرسد و تعداد Hostid به دو به توان 8 منهای دو 254 آدرس است.

کلاس : D آدرس کلاس D برای **Multicasting**استفاده میشود.224 تا 239

کلاس : E در این کلاس وضعیت چهار بیت اول 1111 است این کلاس برای کار های تحقیقاتی و تجربی محیا شده است: 240 تا 254

سیستم ها براي تشخيص تعلق يا عدم تعلق به يك شبكه از مفهومي به نام Subnet Mask استفاده مي كند. به اين صورت كه تمام بيت هاي Network را 1 و تمام بيت هاي Host را 0 در نظر مي گيرد تا Subnet maskرا بسازد. در نظر داشته باشید که هر کلاسی که ما میتونیم ازشون به عنوان یک آدرس استفاده کنیم یک SubnetMask استاندارد داره به عبارت دیگر هر ip دارای یک SubnetMask است و برای کلاس هایی که در بالا گفته شد این SubnetMask ها به صورت استاندارد زیر هستند:

Standard Subnet Masks:

Class A : 255.0.0.0

Class B : 255.255.0.0

Class C: 255.255.255.0

مثال

IP: 192.168..1.2
Subnet mask: 255.255.255.0

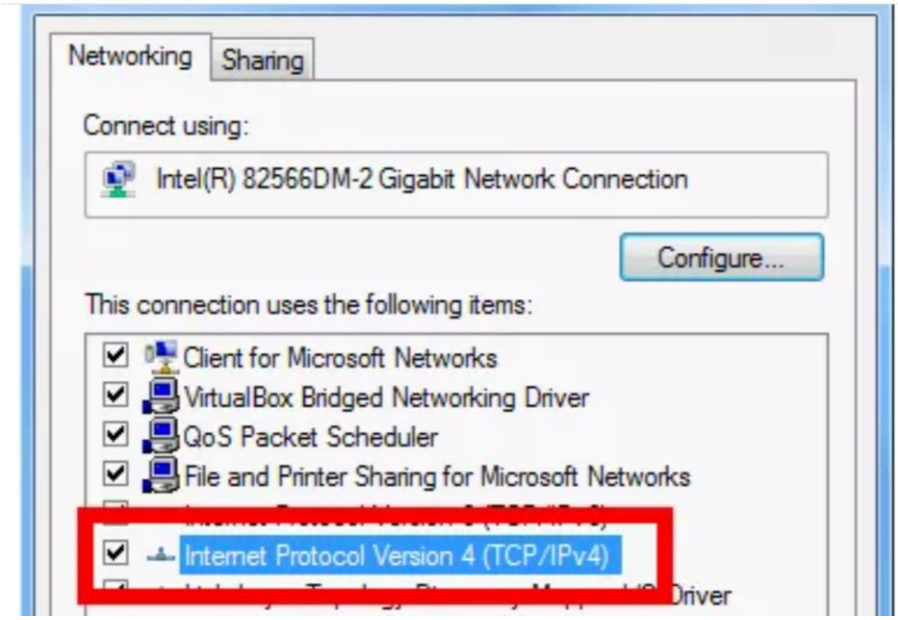
IPهادر صوورت قابل نمایش هستند

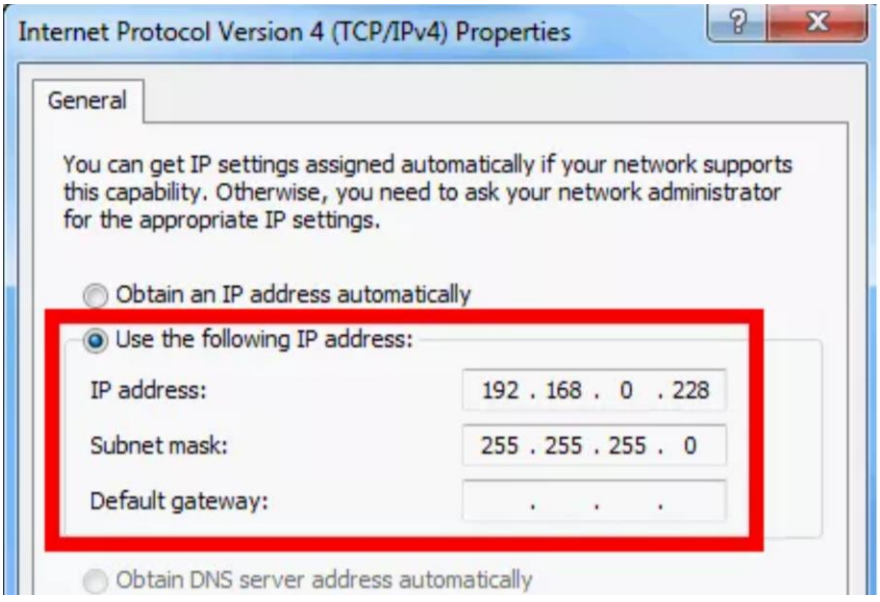
1. subnet mask format
2. prefix format

```
192.168.1.2/24
```

چطور SubnetMask آدرس آی پی را متوجه شویم ؟

توی Run دستور ncpa.cpl رو وارد کنید تا به قسمت تنظیمات کارت شبکه خودتون وارد بشید و از اونجا از یکی از کارت شبکه هاتون یا روی گزینه Local Area Connection راست کلیک کرده و propertiesبگیرید و وارد تنظیمات IP ورژن 4 بشید. بعد از این که Octet 4 آی پی های خوتون رو وارد کردید کلید TAB رو بزنید تا به صورت خودکار Subnet mask آی پی خودتون رو مشاهده کنید.





فرآیند سابنتینگ Subnettingچیست؟

سابنتینگ یا Subnetting به فرآیند انجام دادن محاسبات بر روی آدرسهای IP و اختصاص دادن آدرس هایی با محدوده بزرگتر یا کوچکتر گفته می شود که معمولا متخصصین حوزه زیرساخت به ویژه سیسکو به این محاسبات نیاز دارند و یک نیاز عمومی در تخصص شبکه محسوب نمی شود.

اگر بخواهیم به صورت ساده تر بیان کنیم یعنی شکستن یک شبکه بزرگ به شبکه های کوچکتر برای مدیریت بهتر و راحت تر.

subnettingیک سازمان را قادر می‌سازد تا پیچیدگی شبکه را آسان کند و با افزودن زیرشبکه‌ها بدون راه اندازی شبکه جدید، ترافیک شبکه را کاهش دهد. گاهی اوقات در شبکه های بسیار بزرگ نیاز است که شبکه های آنها از هم جدا باشند تا یکدیگر را برای موارد امنیتی و حفاظتی نبینند. در اینصورت subnettingاست که به کمک آنها می‌آید و راه را آسان می‌کند.

مزایای subnetting عبارتند از:

- کاهش حجم ترافیک شبکه
- تعداد دلخواه کاربران در سازمان از مزایای اصلی آن است. هر سازمان با هر تعداد کاربری می تواند فعال باشد.
- ایجاد لایه های امنیتی

جالب است بدانید سایت هایی وجود دارند که به صورت آنلاین برای شما این کار را انجام می‌دهند و نیازی نیست که شما مدتها زمان برای این کار بگذارید.

تقسیم شبکه باSubnetting

مثال شبکه ای را بیان می کنیم که در آن سابنتینگ درست صورت نگرفته در نتیجه شبکه عملکرد درستی نخواهد داشت . به شکل زیر دقت کنید : همانگونه که می بینید در این شبکه یک کامپیوتر Clientو یک کامپیوتر Server و یک) Router با رنگ نارنجی مشخص شده) داریم که توسط سوییچ به هم متصل شده است . در نگاه اول شاید فکر کنید که این شبکه مشکلی ندارد و درست آی پی دهی شده است . آی پی کلاینت ۱۹۲.۱۶۸.۱۰.۱۰۱ و آیپی سرور ۱۹۲.۱۶۸.۱۰.۲۰۱ و آیپی روتر ۱۹۲.۱۶۸.۱۰.۲۰۰ می باشد . مشکل این شبکه کجاست ؟ سابنت ماسک ۲۵۵.۲۵۵.۲۵۵.۲۴۸ اگر بخواهیم با استفاده از این سابنت ماسک شبکه را آی پی دهی کنیم نتیجه کار متفاوت خواهد بود.

Client : 192.168.10.101

Server : 192.168.10.201

Router : 192.168.10.200

Subnet Mask : 255.255.255.248

برای مشاهده مشکل بایستی آیپی سرور , کلاینت و رورتر را به باینری تبدیل کنیم:

Client : 11000000.10101000.00001010.01100101

Server : 11000000.10101000.00001010.11001001

Router : 11000000.10101000.00001010.11001000

Subnet Mask : 11111111.11111111.11111111.11111000

ملاحظه می کنید که Subnet ID که با رنگ نارنجی و Host ID با رنگ آبی و Network ID مجموعه رنگ سبز و نارنجی می باشد . اکنون اگر کمی در سابنت آیدی دقت کنیم ملاحظه می کنید که سابنت آیدی کامپیوتر کلاینت (۰۱۱۰۰) با سرور و روتر (۱۱۰۰۱) متفاوت است .می دانید این به چه معنی است ؟ درست مثل اینکه کامپیوتر کلاینت ما در شبکه دیگری قرار دارد.

با استفاده از فرمول هایی که در درس گذشته بیان کردیم این شبکه 8-2=6 کامپیوتر یا هاست را آیپی دهی می کند . یعنی قادر به آیپی دهی ۶ کامپیوتر هستیم . پس چرا در شکل زیر ۸ آیپی را نشان داده ایم ؟ آیپی اول از این هشت آیپی یعنی ۱۹۲.۱۶۸.۱۰.۰ سابنت آیدی ما می باشد و آیپی آخر از این هشت آیپی یعنی ۱۹۲.۱۶۸.۱۰.۷ برودکست آیپی می باشد و بقیه ۶ آیپی دیگر از ۱۹۲.۱۶۸.۱۰.۱ تا ۱۹۲.۱۶۸.۱۰.۶ آیپی های کامپیوتر های شبکه ما می باشند.

11000000.10101000.00001010. 00000000 >> 192.168.10.0

11000000.10101000.00001010. 00000001 >> 192.168.10.1

11000000.10101000.00001010. 00000010 >> 192.168.10.2

11000000.10101000.00001010. 00000011 >> 192.168.10.3

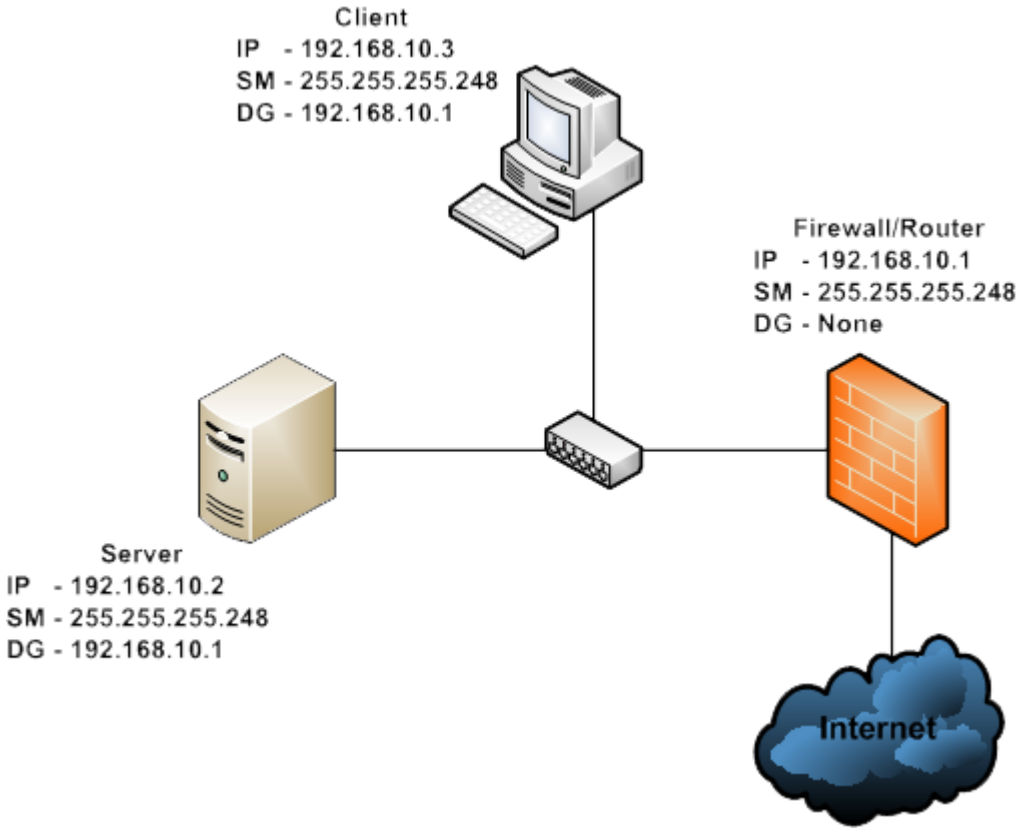
11000000.10101000.00001010. 00000100 >> 192.168.10.4

11000000.10101000.00001010. 00000101 >> 192.168.10.5

11000000.10101000.00001010. 00000110 >> 192.168.10.6

11000000.10101000.00001010. 00000111 >> 192.168.10.7

ملاحظه می کنید که در شکل زیر آیپی های شبکه را اصلاح کردیم و سه آدرس آیپی که در یک سابنت(زیر شبکه) وجود دارند را اختصاص دادیم.



اکنون که کامپیوتر های شبکه را به شیوه CIDR آیپی دهی (آدرس دهی بدون کلاس. کردیم , برای نشان دادن آدرس آیپی و سابنت ماسک دو راه داریم روش اول همان روشی است که تاکنون از آن استفاده می کردیم . مثلا می نوشتیم برای مثال بالا می نوشتیم : ۱۹۲.۱۶۸.۱۰.۱ ۲۵۵.۲۵۵.۲۵۵.۲۴۸ بله مشکلی ندارد روش درستی است ولی اگر بخواهیم کمی حرفه ای تر برخورد کنیم , بایستی با استفاده از روش دوم که CIDR Notation که به معنی نشانه گذاری در CIDR می باشد بنویسیم . برای مثال بالا و با استفاده از روش دوم به این صورت می نویسیم : ۲۹/۱۹۲.۱۶۸.۱۰.۱

ساب نت ماسک ما در این جا ۲۵۵.۲۵۵.۲۵۵.۲۴۸ بود . از کجا به عدد ۲۹ رسیدیم ؟ باز هم با تبدیل به باینری . برای این منظور سابنت ماسک را به باینری تبدیل می کنیم:
۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۰۰۰
اکنون تعداد بیت های یک را می شماریم که می شود ۲۹

روتر ، سوئیچ و هاب

یک سوئیچ شبکه(Switch) ، دستگاه‌ها را در یک شبکه کامپیوتری به همدیگر متصل می‌کند. سوئیچ‌ها از آدرس Mac برای ارسال داده‌ها به مقصد درست استفاده می‌کنند. سوئیچ در لایه‌ی 2 (لایه‌ی پیوند داده) فعالیت می‌کند.

روتر، یک یا چند زیرشبکه‌ی منطقی را به هم وصل می‌کند به طوری که دیگر نیازی به اتصال رابطهای فیزیکی روتر به تک‌تک آن‌ها نباشد. یکی از دلایل گسترش استفاده از روتر، ضرورت اتصال یک شبکه به چندین شبکه‌ی دیگر اینترنت یا دیگر سایت‌ها در عصر حاضر است. اغلب سوئیچ لایه 3 با روتر قابل تعویض است.

هاب که تکرار کننده (repeater) نیز نامیده می‌شود، نسبت به سوئیچ‌ها، پیش پا افتاده‌تر هستند به طوری که اطلاعات مشابه را به تمامی پورت‌ها ارسال می‌کنند ولی سوئیچ‌ها از روی آدرسی که روی بسته قرار دارد مقصد را تعیین می‌کنند و بسته را فقط به آنجا می‌فرستند. هاب‌ها ترافیکی دریافتی را مدیریت نمی‌کنند، آن‌ها فقط اطلاعات را از یک پورت ورودی دریافت می‌کنند و آن را به تمامی پورت‌ها ارسال می‌کنند.

سوییچ

روتر

تکرارگر یا ریپیتر (Repeater) یه دستگاه کوچیک تو شبکه هست که وظیفه تقویت و باز ارسال سیگنال‌های دریافتی از تجهیزات دیگه شبکه‌رو به عهده دارد. **تکرارگر یا ریپیتر تو شبکه به کمک سیگنال‌ها میاد و با تقویت ان‌ها باعث میشه سیگنال‌ها قوی و در مسافت بیشتری ارسال بشوند**

نواع تکرارگر های (ریپیتر های) شبکه رو میشه به دسته‌های پایین تقسیم کرد:

- با توجه به انواع سیگنال‌هایی که تولید می‌کنن:
  -1تکرارگرهای آنالوگ
  -2تکرارگرهای دیجیتال
- با توجه به شبکه‌هایی که به هم متصل میشن:
  -1تکرارگرهای سیمی
  -2تکرارگرهای بی‌سیم
- با توجه به دامنه شبکه‌های محلی که به هم متصل میشن:
  1تکرارگرهای محلی(local repeater)
  2تکرارگرهای راه دور(remote repeater)

تکرارگرها معمولاً برای اتصال بین دو شبکه محلی (LAN) مورد استفاده قرار می‌گیرن

کاربردهای تکرارگر (ریپیتر) شبکه

1. وقتی که می‌خواهید **خارج از فضای خانه،** مثل حیاط هم به سیگنال وای‌فای دسترسی داشته باشید.
2. یا مثلا وقتی **بین روتر و اتاقتان مانعی وجود دارد** که اجازه دریافت سیگنال شبکه وای‌فای رو نمیدهد
3. و اگر نقاطی تو خانه یا دفتر کار هست که **از روتر خیلی دوره و سیگنال‌ها ضعیفند** یا اصلا دسترسی ندارید.

پل یا بریج(Bridge)

بریج دو پورتی است که حداکثر دو سگمنت را به هم متصل یا یک شبکه را به دو سگمنت تقسیم می‌کند. **بریج** دو مزیت مهم دارد:

1. می‌تواند آدرس‌های مک گره‌های شبکه را یاد بگیرد و آن‌ها را در حافظه‌اش ذخیره کند.
2. می‌تواند شبکه را دست‌کم به دو بخش یا اصطلاحا دو سگمنت جداگانه تقسیم کند.

درنتیجه، وقتی گره‌ای برای گره دیگری در شبکه پیغام می‌فرستد، **بریج** می‌تواند آدرس مک گره مقصد را که در پیغام درج شده است بخواند و تشخیص دهد که گره مقصد در کدام سگمنت جای گرفته است. پس از آن، **بریج** پیغام دریافتی از گره مبدا را فقط به سگمنتی می‌فرستد که گره مقصد در آن جای دارد. در این‌صورت، ترافیک شبکه‌ای با دو سگمنت، به نصف کاهش می‌یابد، زیرا از پخش یا اصطلاحا flooding فریم در سگمنت نامربوط جلوگیری می‌شود

سناریوها

تعریف شبکه ساده با سوییچ

در این سناریو دو کامپیوتر و یک سوییچ بر روی صفحه قرار میگیرد. با استفاده از ابزار connection و انتخاب automatically choose connection type دو کامپیوتر را به سوییچ متصل می کنیم. برای تنظیم ip کامپیوترها بر روی کامپیوتر کلیک می کنیم و در تب desktop گزینه ip configurationرا انتخاب می کنیم. آدرس های ip زیر را برای دو کامپیوتر انتخاب کنید. هر دو آدرس در یک زیر شبکه هستند، بنابر این به را حتی در شبکه دو کامپیوتر برای یکدیگر قابل دسترسی هستند.

آدرس ip اولی

192.168.1.1

Subnet mask

255.255.255.0

آدرس ip دومی

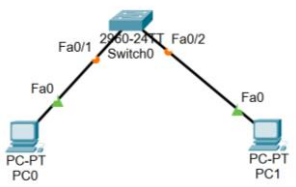
192.168.1.2

Subnet mask

255.255.255.0

برای مشخص نمودن اینکه آیا دو کامپیوتر به یکدیگر دسترسی دارند یا خیر؟ روی کامپیوتر کلیک کنید و گزینه command prompt را انتخاب می کنیم و در کامپیوتر اول دستور ping به کامپوتر دوم را اعمال می کنیم. اگر ارتباط برقرار باشد، خروجی reply است در غیر این صورت .time out

ping 192.168.1.2



سناریوی دوم

آموزشVLan

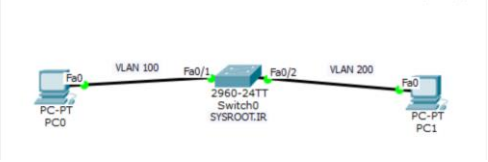
VLANچیست؟

VLANمخفف Virtual Local Area Network هست. یعنی شبکه محلی مجازی، هر شبکه محلی برای خودش تنها یک محدوده Broadcast داره که ترافیک محدوده خودش رو در در این محدوده نگه میداره و اگر شما بتونید بصورت مجازی یک شبکه محلی ایجاد کنید در حقیقت تونستید یک محدوده Broadcast یازمانی که در دامین باشیم Broadcast Domain ایجاد کرده‌ایم و در این حالت ترافیک شبکه به حالت کنترل شده می‌شود.

فرض می‌کنیم که شبکه ما دارای تعدادی سرور و تعدادی کامپیوتر می‌باشیم که 10 کامپیوتر در طبقه اول و 10 کامپیوتر در طبقه دوم می‌باشد می‌خواهیم تنظیماتی انجام دهیم که سیستم‌های طبقه اول و دوم و سرورها همگی در Vlan مجزا باشند.

دلایل طراحیVLAN

- بالا بردن امنیت شبکه و کنترل دسترسی‌ها
- بهینه سازی ترافیک شبکه با کنترل پهنای، جهت بالا بردن سرعت شبکه
- مدیریت آسان برای Policy های سازمان



سناریوی ما خیلی ساده هست، میخواهیم دو PC را در دو Vlan 100 و Vlan 200 قرار دهیم .برای ساخت VLAN 100 که یک VLAN جدید هست از دستور زیر استفاده میکنیم

Switch(config)#vlan 100

و برای تغییر نام آن از دستور زیر

Switch(config-vlan)#name sysroot-100

سپس با دستورات زیر به ترتیب اول وارد اینترفیس مورد نظر می شویم سپس ان اینترفیس را در مود(access) قرار می دهیم و در آخر آن اینترفیس رو به VLAN 100 اضافه میکنیم

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 100

همین کار را برای اینترفیس دوم هم انجام می دهیم

Switch(config)#interface fastEthernet 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 200

با دستور Show Vlan میتوانیم چک کنیم که اینترفیس ها به درستی در VLan مورد نظر قرار گرفته اند

همچنین با دستور زیر میتوانید اطلاعات کاملتری از اینترفیس خود داشته باشید

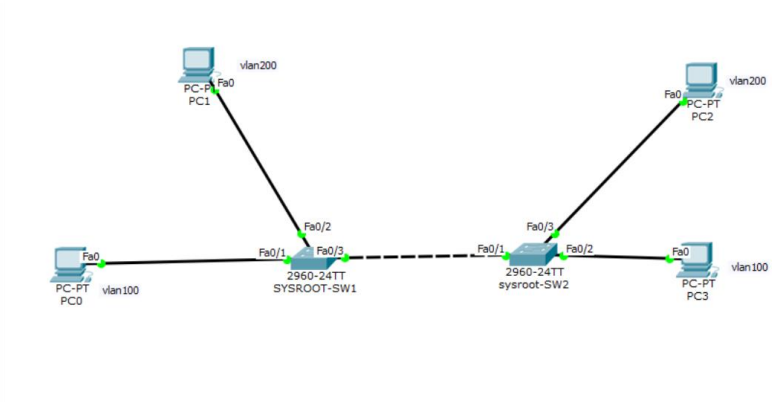
Switch#show interfaces fastEthernet 0/1 switchport

تعریفTrunk

شما می توانید کامپیوتری در VLAN 100 در سویچ MALI داشته باشید که بعد از جدا کردن از سیستم و بردن آن به طبقه دهم و اتصال به سویچ MODIRIYAT همچنان در همان 100 VLANقرار داشته باشد !!

یک پورت ترانک یا Port Trunk در واقع پورتی است که وظیفه آن انتقال ترافیک VLAN هایی است که سویچ به آنها دسترسی دارد ، به فرآیندی که در آن ترافیک VLANها می تواند به سویچ دیگر از طریق پورت Trunk منتقل شود نیز Trunking گفته می شود. پورت های Trunkهر Frame را با استفاده از یک برچسب شناسایی منحصر به فرد که در اصطلاح Tagگفته می شود علامت گذاری می کند ، معمولترین نوع برچسب ها یا Tag های مورد استفاده ISLیا Inter-Switch Link برچسب همچنین و 802.1 Qبرچسب Trunking باشد.

به این نکته توجه کنید که یک پورت اترنت یا می تواند یک Port Access باشد یا یک Port Trunkو نمی تواند بصورت همزمان هر دو کار را انجام بدهد ، بنابراین به پورتی که به عنوان Trunk تعریف شده است کامپیوتری را نمی توانید متصل کنید .



دقیقا مثل سناریوی قبلی برای سوئیچ دوم نیز تمام دستورات قبلی را میزنیم

```
Switch(config)#interface fastEthernet 0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 100

Switch(config)#interface fastEthernet 0/3

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 200
```

خب حالا با استفاده از دستور Switchport Mode Trunk اقدام به تغییر Interface به حالت Trunkمی کنیم. بنا به مدل سوئیچی که استفاده می کنید، ممکن است با اروری مشابه با این ارور برخورد کنید. می توانیم نوع Encapsulation Trunk را نیز تغییر دهیم. مابین Encapsulation 1q.802یا Isl Encapsulation یکی را انتخاب کنید. با استفاده از دستور زیر آن را به 1 802.qتغییر میدهیم .

Switch(config-if)#switchport trunk encapsulation dot1q

نکته: در پکت تریسر دستور بالا لازم نمی باشد فقط کافی است در هر دو سوئیچ دستور زیر را وارد کنیم تا هر دو در مود Trunk قرار بگیرند

Switch(config-if)#switchport mode trunk

در وهله اول اگر شما دستور Show Vlan را اجرا کنید، نمی توانید Interface مربوط به Trunkرا ببینید. این مسئله طبیعی می باشد زیرا دستور Show Vlan تنها Interfaceهایی را نمایش می دهد که در حالت Access قرار دارند و Trunk Interfaces را نمایش نمی دهد

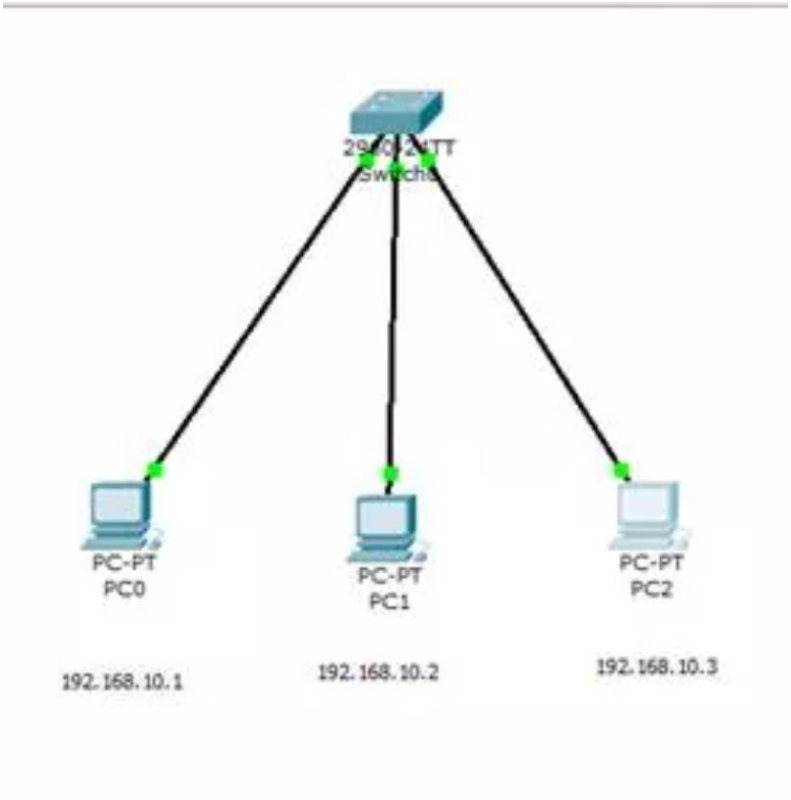
Switch#show interfaces trunk

درصورتی که بخواهیم فقط یک تعداد Vlan از Trunk ما عبور کنن میتوانیم با دستور زیر Vlanهای مجاز خودمون رو به هر دو سوئیچ معرفی کنیم

Switch(config-if)#switchport trunk allowed vlan 100,200

سناریوی 3

آموزش portsecurity



برروی سویچ کلیک کرده و به قسمت CLI سویچ رفته و دستورات زیر را برای بر قراری port securityدرج می کنیم.ما در اینجا port security را بر روی اینتر فیس های 1 تا 3 اجرا کرده ایم.

```
Switch>enable
Switch#conf terminal
Switch(config)#interface range fastEthernet 0/1 – 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
```

خوب حالا با توجه به اینکه maximum را برای پورت ها عدد یک قرار داده ایم طبیعتا باید یک mac آدرس را بیشتر نشناسند و در صورتی که پورت اینتر فیس 1 تا 3 به دستگاهی با

macمتفاوت وصل شد طبق violation که تعریف کرده ایم باید shutdown شده و کابل اینترفیس آن در این نرم افزار به رنگ قرمز در بیاید.و ارتباط با دیگر سیستم ها قطع شده و دیگر اجازه بازگشت به شبکه را نداشته باشد.خوب ما دراینجا یک لپ تاپ اضافه کرده ایم و در ابتدا برایش یک ip تنظیم کرده ایم . 192.168.10.5

حالا کابل اینترفیس 0/1 *را از pc 0 جدا کرده و به لپ تاپ وصل کرده ایم چون mac این لپ تاپ با mac موجود در جدول mac-address سویچ مغایرت دارد وما اجازه اتصال فقط یک mac را به هر port داده ایم ، پس طبیعتا پورت اینترفیس 0/1* را shutdown می کند و اجازه ارتباط با دیگر pc ها را نمی دهد.

انواع violation

Protect

Restrict

Shut down

Violation restrict اجازه وصل شدن غیر مجاز را می گیرد ولی interface قطع نمیشود.

violation restrictهم مانند protect هست با این تفاوت که mac سیستم متخلف را به مدیر شبکه اعلام می کند , واجازه فعالیت دوباره اش را در شبکه می دهد.اما در violation shutdownاگر بخواهیم به پورت متخلف اجازه فعالیت دوباره بدهیم ابتدا وارد اینترفیس پورت متخلف می شویم (یعنی کابل از حالت قرمز رنگ به حالت سبز و عادی بر می گردد) و دستورات زیر را وارد می کینیم:

```
Switch(config)#int fa 0/2
Switch(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
Switch(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

ویا از دستور زیر استفاده می کنیم

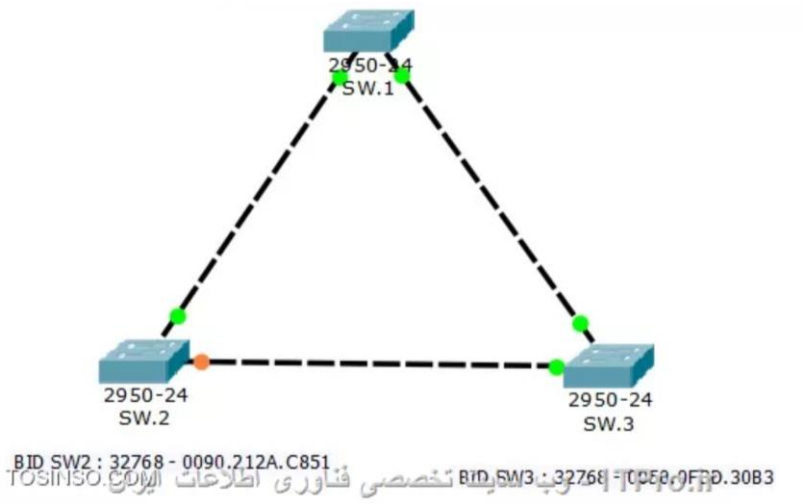
switch#clear port-security sticky interface fastethernet

با این دستور آدرس های مکی که توسط این اینترفیس یادگرفته شده است و در فایل running configهست حذف می شود.

منبع

https://cisco.tosinso.com/fa/articles/40429/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-%D9%BE%D9%88%D8%B1%D8%AA-%D8%B3%DA%A9%DB%8C%D9%88%D8%B1%DB%8C%D8%AA%DB%8C-(-Port-Security-)-%D8%AF%D8%B1-%D9%BE%DA%A9%D8%AA-%D8%AA%D8%B1%DB%8C%D8%B3%D8%B1

سناریوی چهارم



در مرحله اول سوئیچ روت انتخاب میشود : سوئیچ با کمترین BID به عنوان سوئیچ اصلی یا همان ROOT BRIDGE مشخص می شود.تمام پورتهای این سوئیچ در نقش DESIGNATED PORT و وضعیت FORWARD قرار می گیرد.

مقادیر BID به شرح زیر می باشد:

BID SW1 : 32768 .(0001.43EC.9121)

BID SW2 : 32768 .(0090.212A.C851)

BID SW3 : 32768 .(0050.0F3D.30B3)

همانطور که مشخص است هر 3 سوئیچ در مقدار PRIORITY یکسان هستند که عدد آن 32768 است.در ادامه قیاس BID کوچکتر ، مقادیر مک با هم مقایسه می شوند ، توجه شود که این مقدار در مبنای 16 می باشد . برای اینکه این مقدار رو بصورت دهدهی دیده تا کارمان در قیاس راحت شود (می توانیم آنرا از طریق ماشین حساب به دهدهی تبدیل کنیم).

(0001)16=(1)10

(0090)16=(144)10

(0050)16=(120)10

مرحله دوم پروتکلSTP

در بین تمام سوئیچ های باقی مانده فقط یک پورت و نزدیکترین پورت به سوئیچ روت ، به عنوان پورت اصلی (ROOT PORT) انتخاب می شود .معیار نزدیکی براساس COST است COST مفهومی گره خورده به خود اینترفیس پورت سوئیچ است که COST آن طبق سرعت محاسبه می شود .در این مرحله سوئیچ روت انتخاب شده و پورتهای سوئیچ روت همگی DESIGANATED PORTهستند.مکانیزم پروتکل STP با FORWARD کردن BPDUها نقش پورت ها و در این قسمت ، ROOT PORT را مشخص میکند.

انتخاب نقش پورت ها که در وضعیت forwarding هستند براساس 3 معیار است:

COSTکمتر

BRIDGE IDکمتر

PORT IDکمتر

پورتی که حلقه بوجود می آورد در حالت بلاک شده است.

```
Switch#SHOW SPANning-tree

VLAN0001

  Spanning tree enabled protocol ieee

  Root ID    Priority    32769

             Address     0003.E4A0.E208

             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     0003.E4A0.E208

             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

             Aging Time  20
```

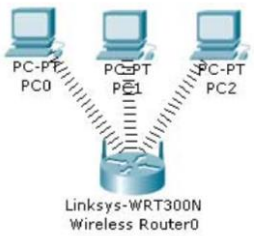
HELLO TIME

سوئیچ ROOT BRIDGE هر 2 ثانیه یکبار (HELLO TIME) بسته BPDU را روی همه پورت هایش ارسال می کند.هدف از ارسال دوره ای BPDU تشخیص تغییرات توپولوژی شبکه است.

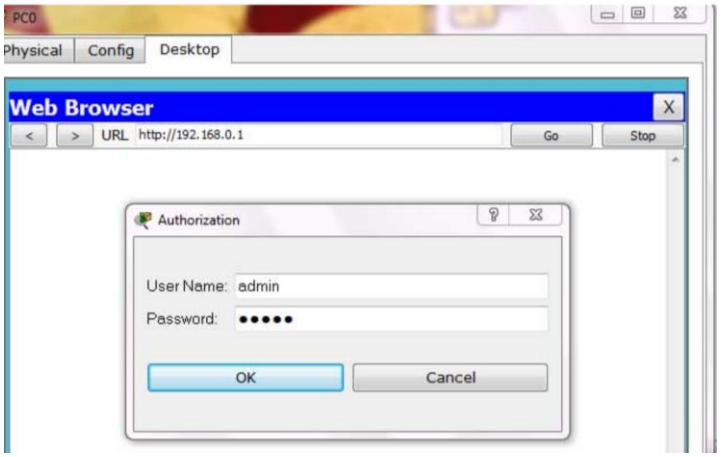
منبع

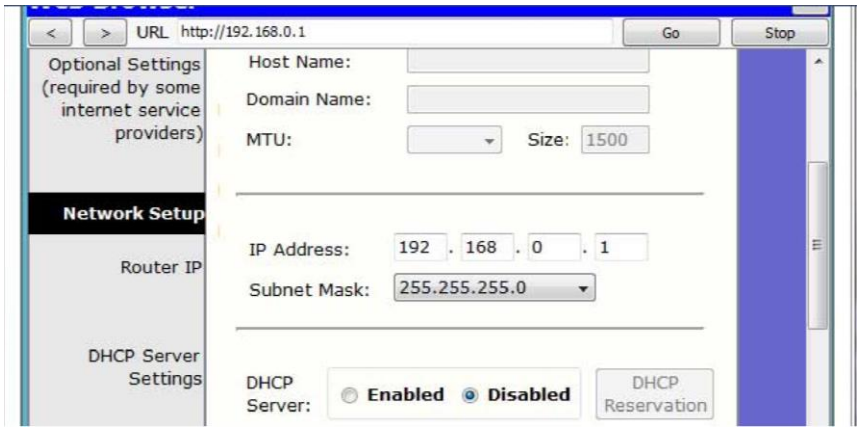
https://cisco.tosinso.com/fa/articles/34827/%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-STP-(Spanning-Tree)-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%DA%AF%D9%88%D9%86%D9%87-%DA%A9%D8%A7%D8%B1-%D9%85%DB%8C%DA%A9%D9%86%D8%AF%D8%9F

آموزش راه اندازی DHCP با روتر بی سیم



PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1

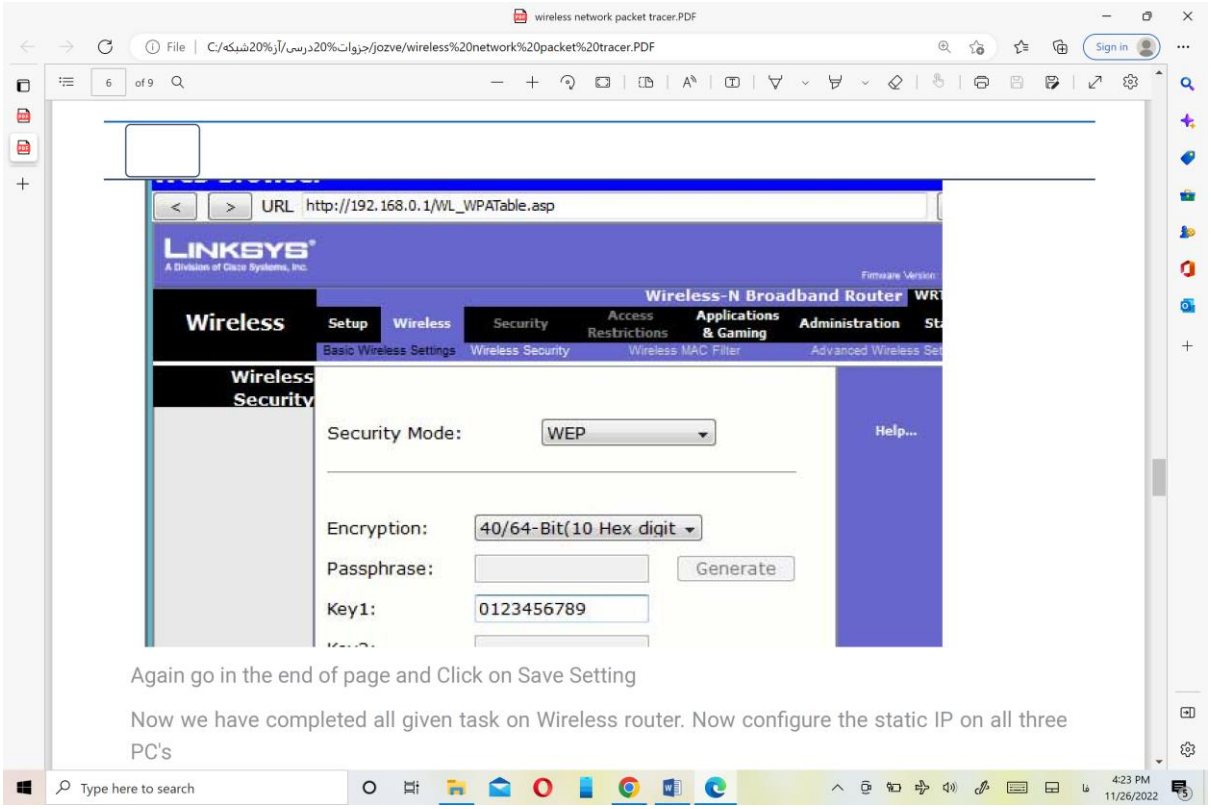

PC0
Physical
Config
Desktop
Web Browser
URL http://192.168.0.1
Go
Stop
Authorization
User Name: admin
Password:
OK
Cancel


URL http://192.168.0.1
Go
Stop
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size: 1500
Network Setup
Router IP
IP Address: 192 . 168 . 0 . 1
Subnet Mask: 255.255.255.0
DHCP Server Settings
DHCP Server: Enabled Disabled
DHCP Reservation


URL http://192.168.0.1/Management.asp
Go
Stop
Wireless-N Broadband Router WRT300N
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Management
Log
Diagnostics
Factory Defaults
Firmware Upgrade
Management
Router Access
Router Password:
Re-enter to Confirm:
Help...

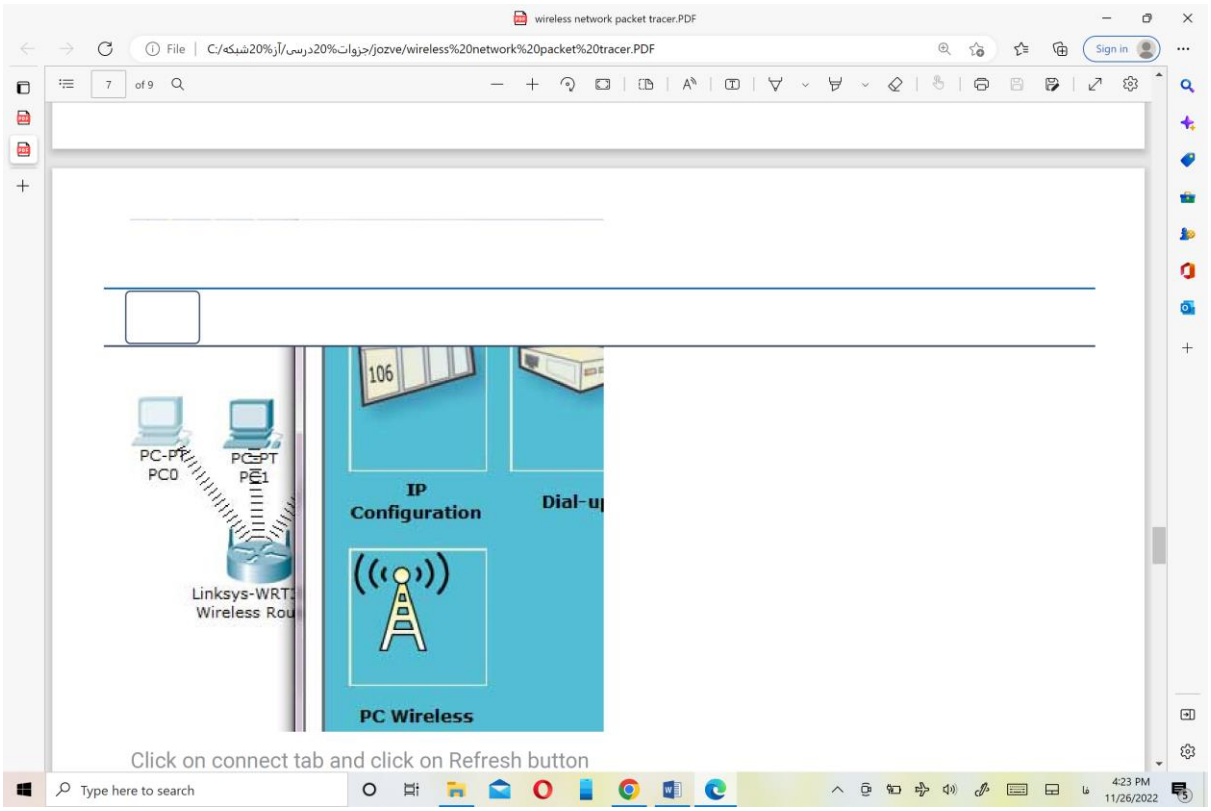

URL http://192.168.0.1/Wireless_Basic.asp
Go
Stop
Wireless-N Broadband Router
WRT300N
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Help...
Network Mode:
Mixed
Network Name (SSID):
MotherNetwork
Radio Band:
Auto
Wide Channel:
Auto
Standard Channel:
Auto


PC0
Physical
Config
Desktop
Web Browser
URL http://192.168.0.1/WL_WPATable.asp
LINKSYS
Wireless-N Broadband Router
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Wireless Security
Help...
Security Mode:
Disabled
Disabled
WEP



Again go in the end of page and Click on Save Setting

Now we have completed all given task on Wireless router. Now configure the static IP on all three PC's

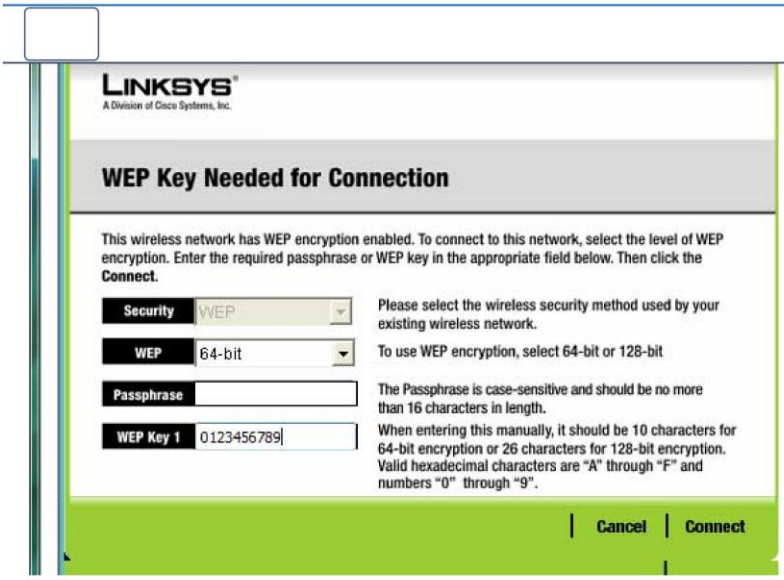


Click on connect tab and click on Refresh button

wireless network packet tracer.PDF

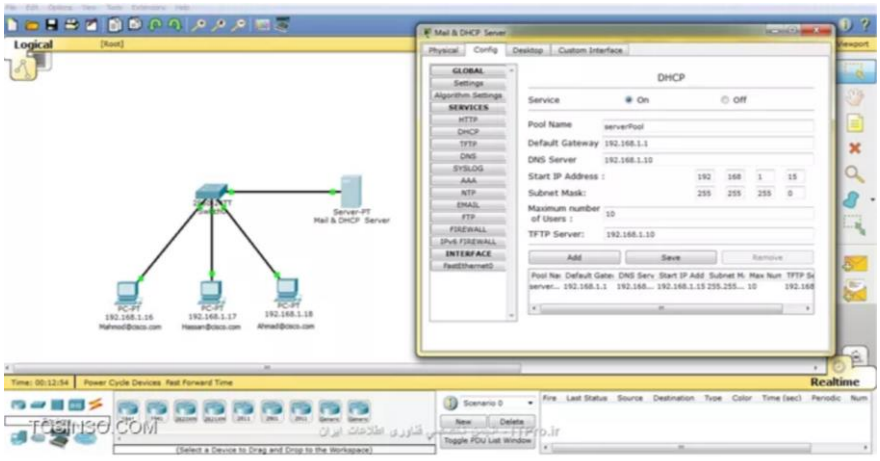
Click on connect tab and click on Refresh button

wireless network packet tracer.PDF



It will connect you with wireless router.

آموزش راه اندازی DHCP و ایمیل سرور در پکت تریسر



1. سرور
2. سوییچ 2960
3. کامپیوتر

ارتباطات را با کابل Straight برقرار نموده و به سرور ip 192.168.1.10 می دهیم و برای باقی سیستم ها در این سناریو جهت سهولت در کار از DHCP استفاده می نماییم که برای این کار ابتدا بر

روی سرور کلیک کرده به قسمت Config رفته و سرویس DHCP را به حالت ON قرار بدهید و در قسمت Pool Name نام DHCP سرور را وارد کنید که بطور پیش فرض ServerPool است که در این سناریو از همین نام استفاده می کنیم و در قسمت بعد Default Gateway ادرس IP Gatewayشبکه را وارد می کنیم که بصورت اتوماتیک به کلیه سیستم ها نیز اعمال می شود و در قسمت بعد Start IP Address اولین ادرس IP که به سیستم اعمال می شود تعریف می کنیم که در این سناریو از شبکه 192.168.10.0/24 که اولین ادرس IP در این شبکه از 15 شروع شده است و در قسمت بعد subnet mask شبکه را وارد می کنیم 255.255.255.0 در قسمت بعد بیشترین تعداد userها تعیین می گردد که در این سناریو 10 عدد استفاده شده است.

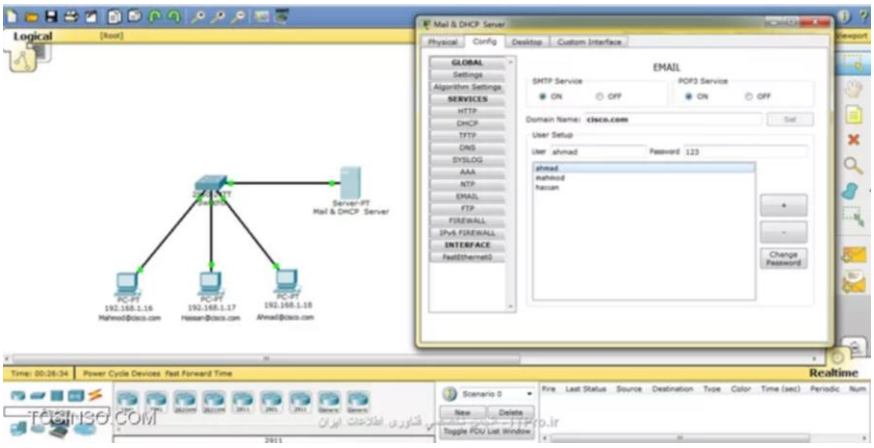
کلیه تنظیمات برای DHCP Server اعمال شده است و با زدن کلید Save سرویس مورد نظر فعال می شود و می توانید به کامپیوتر ها مراجعه کنید و در انجا به تنظمیات IP Configuration بروید و از DHCP استفاده کنید که بطور اتوماتیک ادرس IP و سایر ادرسها ارایه می شود.

برای سیستم های دیگر نیز این کار را انجام بدهید تا ادرس IP انها اعمال شود . حال برای راه اندازی Mail Serverبر روی سرور کلیک می کنید و قسمت Email رفته و سرویس های Pop3 , STP را در حالت ON قرار دهید و در قسمت Domain Name نام دامین که قرار است سرویس ایمیل را ارایه کند را وارد می کنیم که دراین سناریو از Cisco.com استفاده شده است و در قسمت بعد USER Setupنوبت به تعریف نام کاربری و رمز عبور برای ایمیل های کاربران می رسد که در این سناریو کاربران زیر با رمز عبور تعریف شده اند:

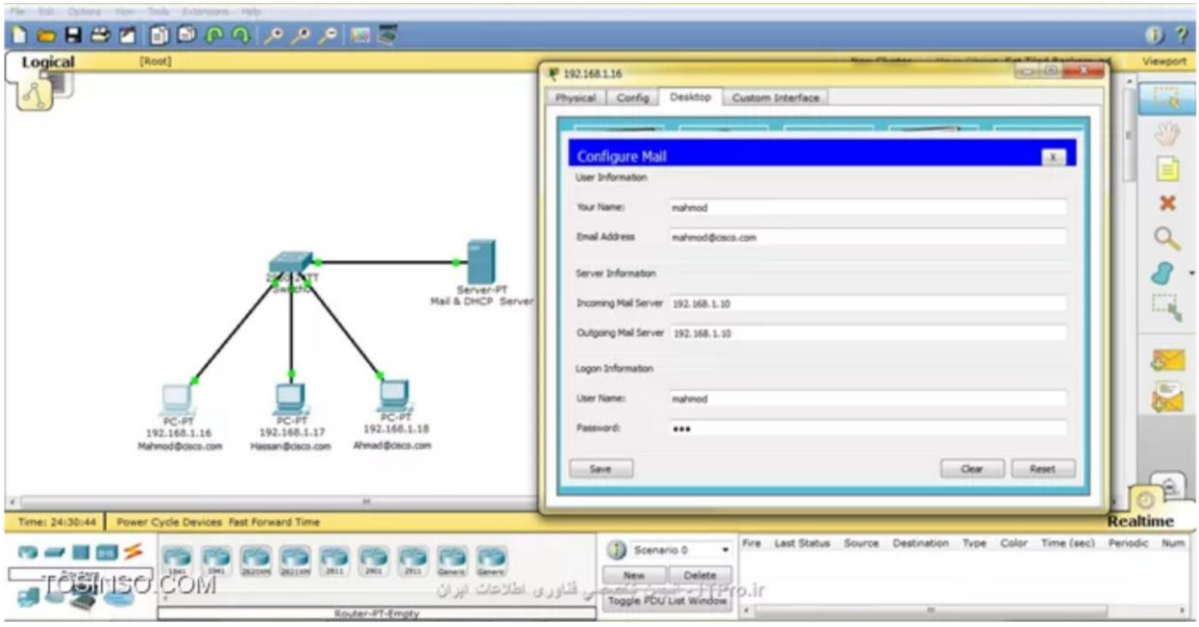
Ahmad 123

Mahmod 456

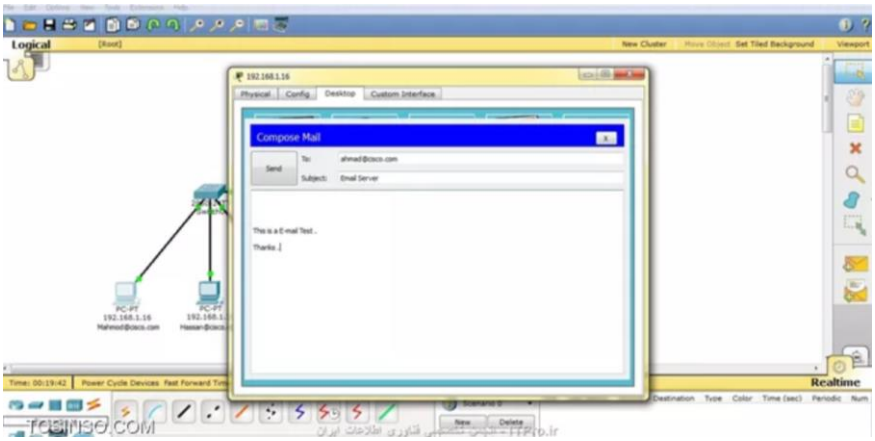
Hassan 789



سرویس ایمیل به صورت کامل فعال و نوبت به اعمال تنظیمات در کامپیوترهای کاربران شده است .
برای این کار ابتدا بر روی کامپیوتر کلیک کرده و به قسمت Desktop رفته و بعد بر روی email کلیک می کنیم و سرویس ایمیل را بصورت زیر تنظیم کنید



آدرس ایمیل و نام در قسمت User Information وارد میشود و آدرس 192.168.1.10 جهت ارسال و دریافت ایمیل در قسمت Server Information وارد شود و در انتها User & Pass وارد می شود هم چنین برای سایر سیستم ها نیز این کار را انجام دهید .سرویس ایمیل فعال شده است و کافی است در Mail Browserبا زدن دکمه Compose ایمیلی را آماده کنید و زدن دکمه Send آن را برای کاربر مورد نظر ارسال کنید که ما از کاربر Mahmod به کاربر Ahmad ایمیل می زنیم و پاسخ آن را از Ahmadدریافت می کنیم

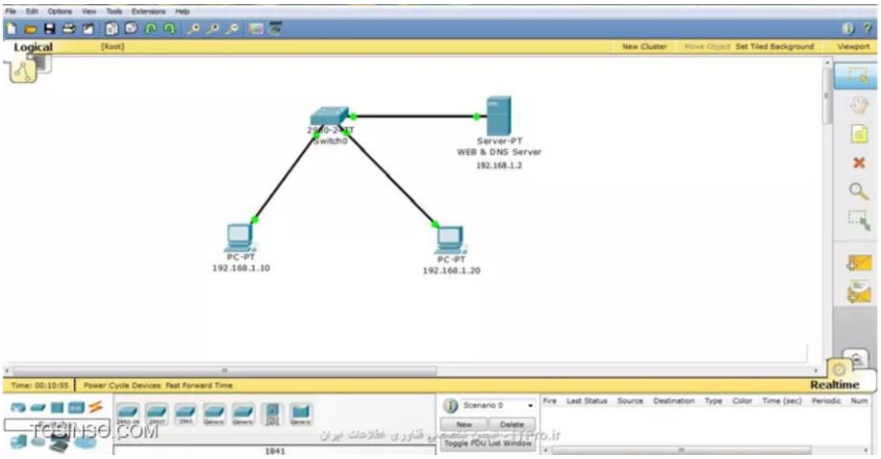


https://cisco.tosinso.com/fa/articles/43277/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-%D8%A7%DB%8C%D9%85%DB%8C%D9%84-%D8%B3%D8%B1%D9%88%D8%B1-%D8%AF%D8%B1-%D9%BE%DA%A9%D8%AA-%D8%AA%D8%B1%DB%8C%D8%B3%D8%B1-(Packet-Tracer)

آموزش راه اندازی وب سرور و DNS سرور در پکت تریسر

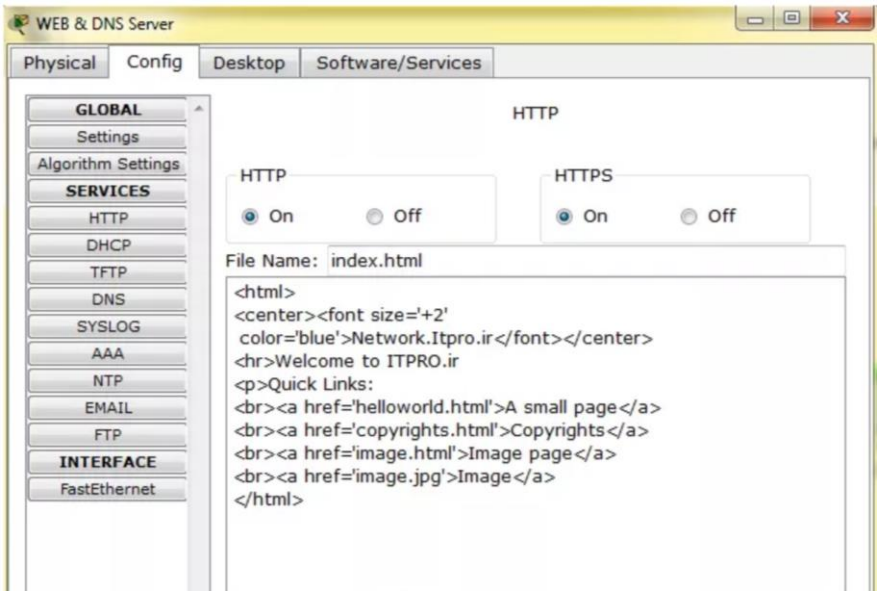
1. سوییچ 2960 سیسکو
2. PC
3. سرورWEB & DNS

در گام نخست ارتباط بین سوییچ و سایر Device ها را با کابل Straight برقرار می کنیم.

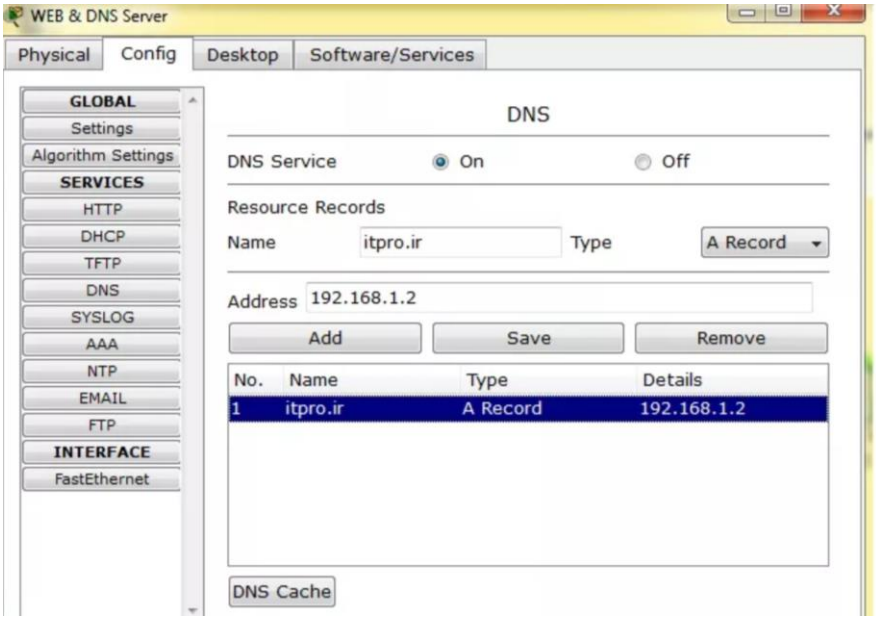


در ادامه به SERVER یک IP بصورت دستی اختصاص می دهیم 192.168.1.2

- برای فعال کردن WEB Server روی سرور کلیک کرده و از قسمت Config گزینه HTTPرا انتخاب می کنیم ، حال دو گزینه HTTP و HTTPS را روی On قرار می دهیم تا WEB Server بر روی سرور مورد نظر فعال شود.



- در ادامه برای فعال کردن DNS Server از قسمت Config گزینه DNS را انتخاب می کنیم و برای فعال کردن DNS Service گزینه On را انتخاب می کنیم و در قسمت Name نام مورد نظر وب سایت را وارد کرده و در قسمت Address ادرس آن را وارد کرده و گزینه ADDرا انتخاب می کنیم.



- آدرس pc ها را به صورت دستی تعیین می کنیم.

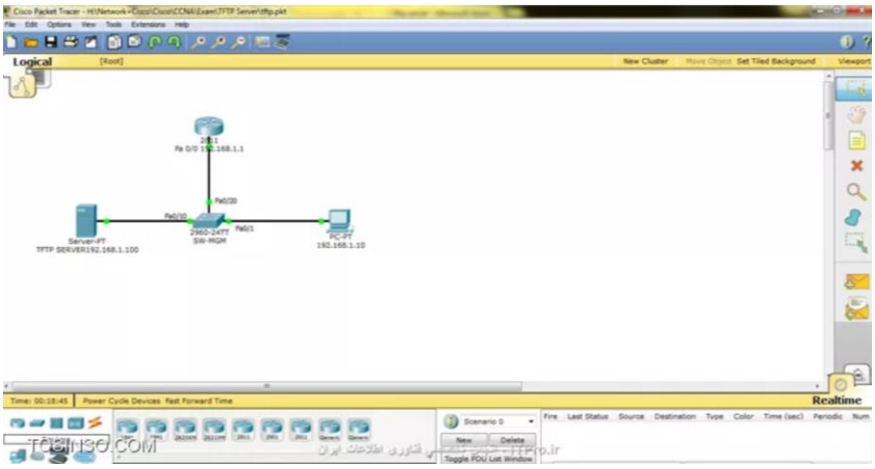
روی یکی از PC ها کلیک کرده و وارد Browser آن می شویم و آدرس 192.168.1.2 را وارد می کنیم و یک وب سایت با نام Network.tosinso.com نمایش داده می شود هم چنین می توان به جای آدرس IP وب سایت نام آن یعنی tosinso.com را وارد نماییم.

https://cisco.tosinso.com/fa/articles/41981/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-%D9%88%D8%A8-%D8%B3%D8%B1%D9%88%D8%B1-%D9%88-DNS-%D8%B3%D8%B1%D9%88%D8%B1-%D8%AF%D8%B1-%D9%BE%DA%A9%D8%AA-%D8%AA%D8%B1%DB%8C%D8%B3%D8%B1

آموزش راه اندازی TFTP سرور در پکت تریسر

1. **روتر 2811 سیسکو**
2. **سوییچ 2960 سیسکو**
3. **کامپیوتر**

4. سرور جهتTFTP



حال به محیط CLI روتر رفته

R1>enable

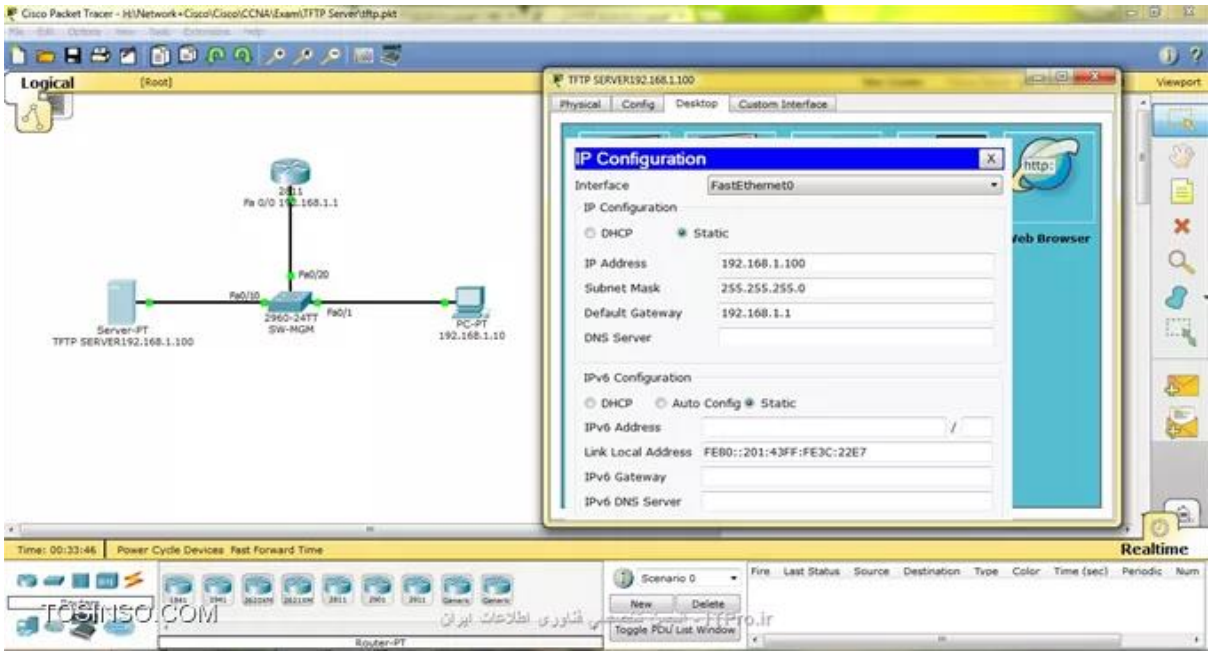
R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#interface fastEthernet 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown



تنظیمات سرور را به صورت شکل بالا انجام دهید.

پس از اعمال تنظیمات اولیه و تست گرفتن از Device ها در شبکه می توان عملیات انتقال فایل از روتر به سرور TFTP و بالعکس را انجام دهیم برای این مراحل زیر را انجام می دهیم .در اولین گام وارد محیط CLI روتر می شویم و با دستور Show Version در محیط Privilage Mode ورژن روتر را می توان مشاهده نمود.

و با دستور Show Flash نیز می توانید فلش روتر را مشاهده نمود.

R1#show flash

System flash directory:

File Length Name/status

3 50938004 c2800nm-advipservicesk9-mz.124-15.T1.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

[51193823 bytes used, 12822561 available, 64016384 total]

63488K bytes of processor board System flash (Read/Write)

حال با دستور Copy می توان انواع مختلف انتقال بین TFTP و روتر را بسته به نیاز انتخاب نموده و فایل مورد نظر را جابجا کرد:

R1#copy ?

flash: Copy from flash: file system

ftp: Copy from ftp: file system

running-config Copy from current system configuration

startup-config Copy from startup configuration

tftp: Copy from tftp: file system

همانطور که در بالا مشاهده می کنید حالت های مختلف انتقال فایل نشان داده شده است که ما میخواهیم یک فایل را از TFTP به روتر اضافه و برعکس آن را انجام دهیم .برای این کار ابتدا فایل فلش را از روتر به TFTP انتقال می دهیم مراحل زیر را دنبال کنید:

R1#copy flash: tftp:

Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin

Address or name of remote host []? 192.168.1.100

Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]? cisco2811R1.bin

Writing c2800nm-advipservicesk9-mz.124-15.T1.bin...!!!!!!!!

[OK - 50938004 bytes]

50938004 bytes copied in 4.52 secs (11269000 bytes/sec)

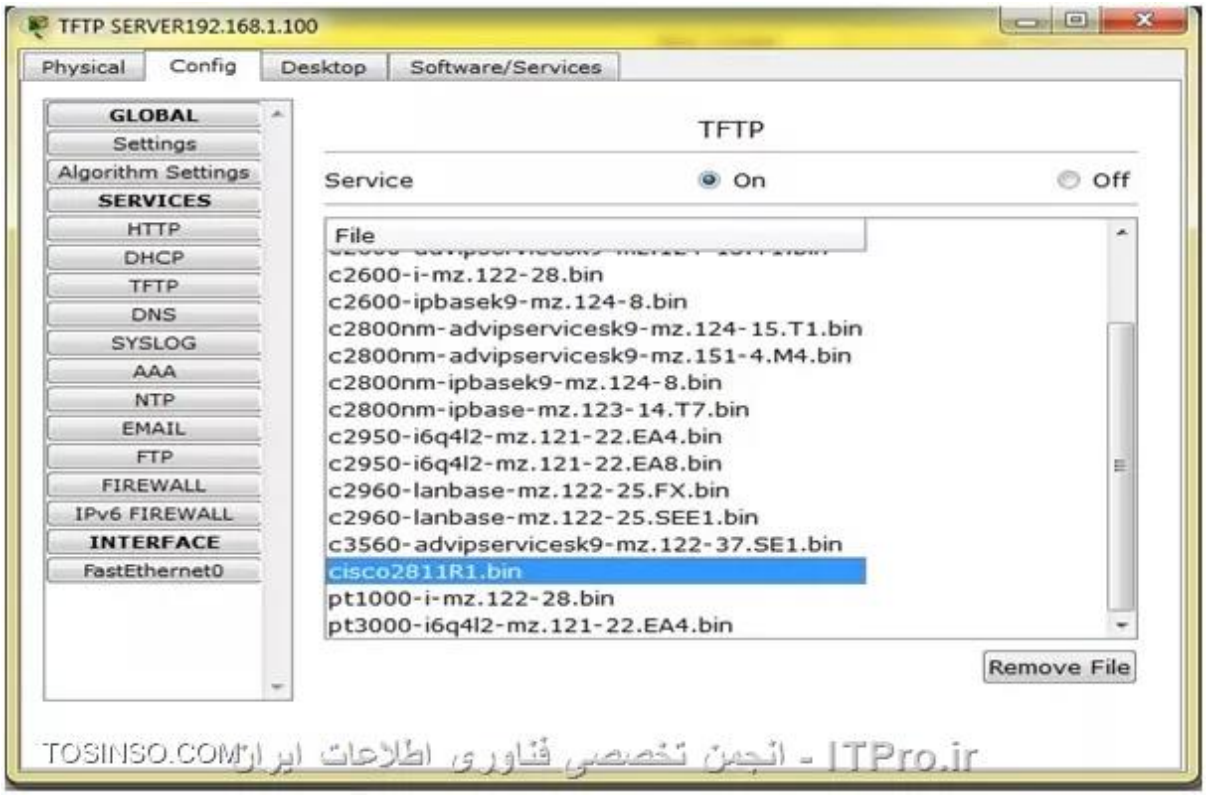
پس از وارد کردن دستور Copy در خط بعد اسم فایل داخل فلش را برای انتقال وارد می کنیم (Source Filename)و در خط بعد ادرس IP سرور TFTP را باید در داخل شبکه وارد نماییم که ما از ادرس IP 192.168.1.100 برای سرور در این سناریو استفاده نموده ایم.

Address or name of remote host []? 192.168.1.100

و در خط بعد از شما می پرسد با چه اسمی باید فایل مورد نظر را ذخیره نماید ؟ که پیش فرض را داخل کروشه نمایش می دهد به این معناست که اگر اسم وارد نشود بازدن کلید Enter اسم پیش فرض اعمال میشود.

Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]? cisco2811R1.bin

در نهایت مشاهده می کنید که انتقال فایل به درستی انجام و در تصویر زیر نمایش داده می شود.



و حالا برعکس این کار را انجام می دهیم یعنی از TFTP به Flash انتقال می دهیم:

R1#copy tftp: flash:

Address or name of remote host []? 192.168.1.100

Source filename []? c1841-ipbasek9-mz.124-12.bin

[Destination filename [c1841-ipbasek9-mz.124-12.bin ?

Accessing tftp://192.168.1.100/c1841-ipbasek9-mz.124-12.bin...

Loading c1841-ipbasek9-mz.124-12.bin from 192.168.1.100: !!!!!!!!!!!!!!!!!

[OK - 16599160 bytes

16599160 bytes copied in 1.431 secs (2595568 bytes/sec(

حال با نمایش از فلش می توان مشاهده نمود که فایل 4 را اضافه نموده ایم:

R1#sh flash:

System flash directory:

File Length Name/status

4 16599160 c1841-ipbasek9-mz.124-12.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

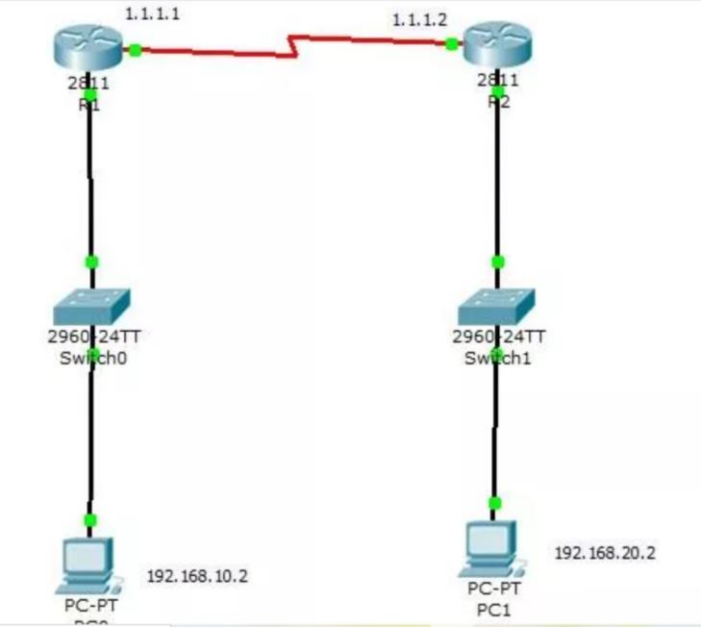
[16854979 bytes used, 47161405 available, 64016384 total]

63488K bytes of processor board System flash (Read/Write)

شما با استفاده از سناریو می توانید روشهای دیگر انتقال فایل را از سوییچ و روترهای سیسکو نیز انجام بدهید ، هم چنین با استفاده از Telnet می توانید از کامپیوتر وارد روتر شوید و از انجا مراحل انتقال فایل را انجام بدهید

https://cisco.tosinso.com/fa/articles/43436/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-TFTP-%D8%B3%D8%B1%D9%88%D8%B1-%D8%AF%D8%B1-%D9%BE%DA%A9%D8%AA-%D8%AA%D8%B1%DB%8C%D8%B3%D8%B1-(Packet-Tracer)

سناریو راه اندازی Static Route



ابتدا آدرس های ip دو کامپیوتر را تعیین می کنیم.

خوب حالا به قسمت cli روتر R1رفته و دستورات زیر را می نویسیم

```
Router>enable
Router#conf terminal
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
```

اینتر فیس سریال 000

```
R1(config)#interface Serial000
R1(config-if)#ip address 1.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000
```

از دستور clock rate برای سمتDCE سرویس دهندهاستفاده می کنیم. برای استفاده از این اتصال SERIAL DCEدر نرم افزار ابتدا باید روتر را خاموش کرده و ماژول WIC-1T را به آن اضافه نمود و دوباره روتر را روشن می کنیم.

حالا به سراغ روتر R2 می رویم و تنظیمات اینترفیس ها را مانند روتر R1 انجام می دهیم.

```
Router>enable
Router#conf terminal
Router(config)#hostname R2
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
```

اینترفیس سریال 300

```
R2(config)#interface Serial030
R2(config-if)#ip address 1.1.1.2 255.255.255.0
R2(config-if)#no shutdown
```

خوب تا اینجا فقط تنظیمات اولیه را انجام دادیم و هنوز بین pc ها ارتباط برقرار نیست.برای استفاده از static routing از دستور زیر استفاده می کنیم

روتر R1

```
R1(config)#ip route 192.168.20.0 255.255.255.0 serial 000
```

البته به جای استفاده از اینترفیس سریال در آخر دستور می شود ip را که برای روتر R2 تنظیم شده نیز استفاده کرد

```
R1(config)#ip route 192.168.20.0 255.255.255.0 1.1.1.2
```

وبرای روتر R2

```
R2(config)#ip route 192.168.10.0 255.255.255.0 serial 030
```

البته به جای استفاده از اینترفیس سریال در آخر دستور می شود ip را که برای روتر R1 تنظیم شده نیز استفاده کرد

```
R2(config)#ip route 192.168.10.0 255.255.255.0 1.1.1.1
```

حالا ارتباط بین دو کامپیوتر را با ping تست می کنیم.

منبع

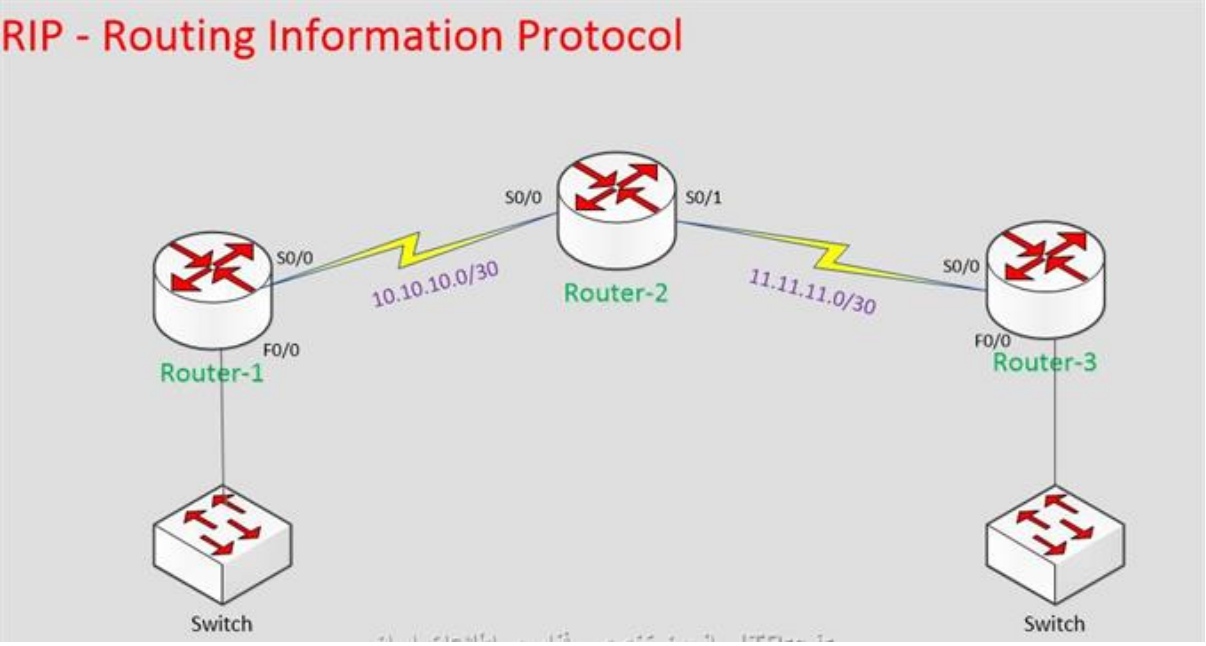
https://cisco.tosinso.com/fa/articles/38655/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B3%D9%86%D8%A7%D8%B1%DB%8C%D9%88-%D8%B1%D8%A7%D9%87-%D8%A7%D9%86%D8%AF%D8%A7%D8%B2%DB%8C-Static-Route-%DB%8C%D8%A7-%D8%B1%D9%88%D8%AA-%D8%AF%D8%B3%D8%AA%DB%8C-%D8%AF%D8%B1-Packet-Tracer

پیاده سازی پروتکل مسیریابی RIP

پروتکل Rip از نوع Vector Distanceمی باشد و به طور کلی از الگوریتم مسیر یابی Bellmanfordاستفاده می کند. این الگوریتم بسیار سبک است و به همین دلیل Load بسیار کمی روی CPU و RAM روتر می اندازد

مشخصات پروتکل مسیریابی.

Administrative Distance (AD) = 120 Metric = Hop Countدر Table Routing با حرف R نشان داده می شود Infinite Metric = 16 .



اختصاص Address IP برای اینترفیس های روتر Serial و Fast Ethernet با استفاده ازدستورات زیردرقسمت CLI روترها بر اساس سناریو آموزش IP های اینترفیس های روتر رواختصاص میدیم :

آموزش-پیاده-سازی-پروتکل-مسیریابی -

ها بر روی اینترفیس روترها حال IP بعد از اختصاص RIP پیاده سازی پروتکل مسیریابی هست که برای RIPنوبت به کانفیگ ارتباط این ۲ شبکه و روترها باهم با استفاده از پروتکل Router-1: :انجام این کار نیز دستورات زیر را بر روی روترها انجام میدیم

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)#clock rate 64000

Router(config-if)#no shutdown

Router(config-if)#exit :

Router(config)#interface serial0/0

Router(config-if)#ip address 10.10.10.2 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial0/1

Router(config-if)#ip address 11.11.11.1 255.255.255.0

Router(config-if)#clock rate 64000

Router(config-if)#no shutdown

Router(config-if)#exit

Router-3

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 11.11.11.2 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Router-1

Router(config)#router rip

Router(config-router)#network 172.16.88.0

Router(config-router)#network 10.10.10.0

Router(config-router)#exit

Router-2 Router(config)#router rip

Router(config-router)#network 11.11.11.0

Router(config-router)#network 10.10.10.0

Router(config-router)#exit

Router-3 Router(config)#router rip

Router(config-router)#network 192.168.1.0

Router(config-router)#network 11.11.11.0

Router(config-router)#exi

پیاده سازی **OSPF**

روی روترهای سیسکو با توجه به **Link state** بودن این پروتکل مسیریابی به نسبت دارای پیچیدگی بیشتری از پروتکل های **Distance Vector** است و شما با استفاده از دستورات زیر و قالب دستوری زیر می توانید این پروتکل را روی روترهای خود پیاده سازی کنید:

ITPRO-Router(config)# router ospf process_ID

ITPRO-Router(config-router)# network network_id wildcard_mask area area_#

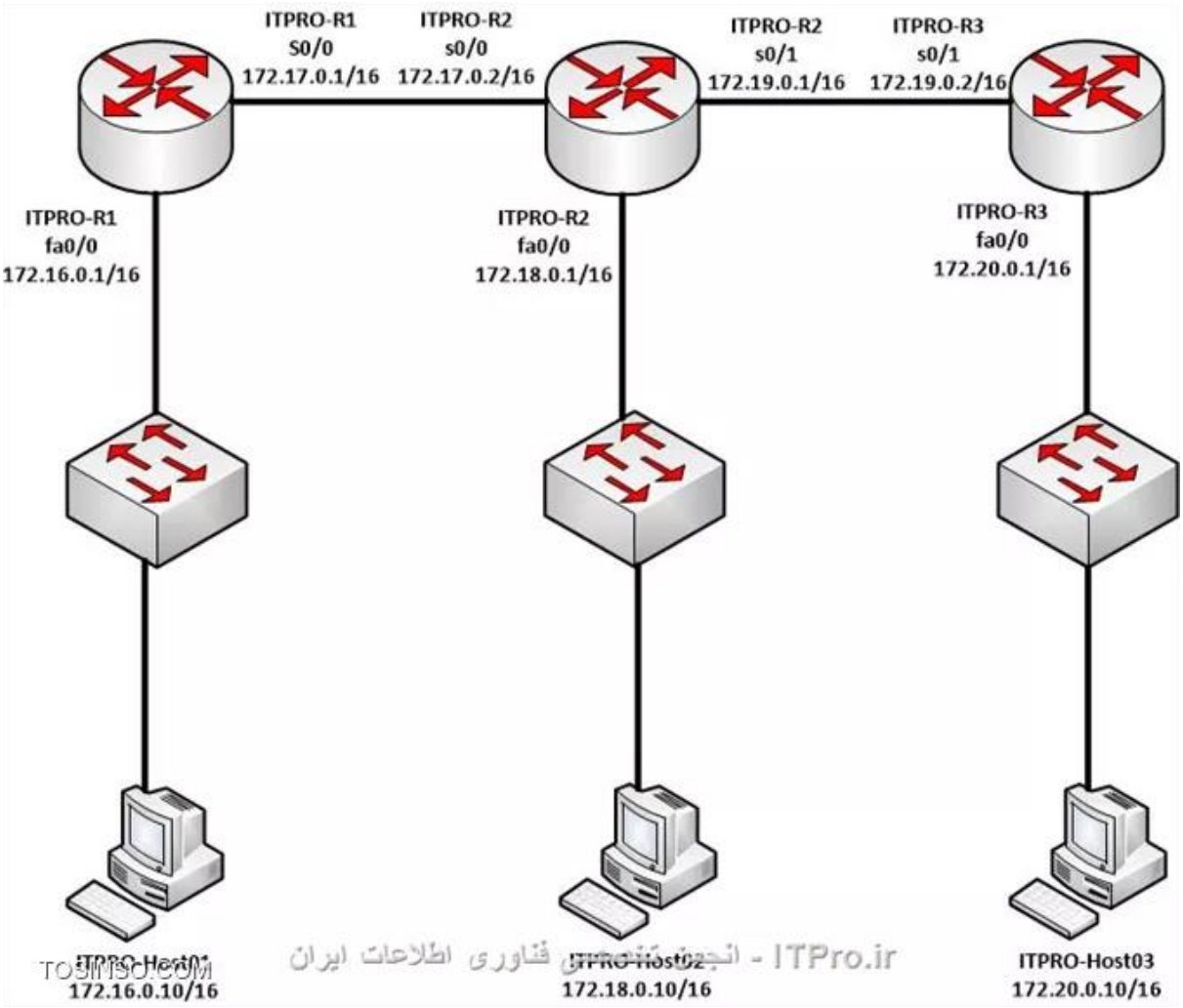
نکات مهم در خصوص دستور OSFP بالا

- **Process_ID** : در مثال بالا گزینه **process_ID** یک عدد در محدوده 1 تا65535 است که مشخص کننده OSPF Process ID یا شناسه فرآیند های پروتکل مسیریابی **OSPF** است. در

واقع OSPF Process ID یک عدد منحصر به فرد است که بر روی روتر قرار می گیرد که مجموعه ای از تنظیمات و پیکربندی های **OSPF** را در خود نگه می دارد و همه آنها را در یک Process یا فرآیند خاص اجرا می کند.

- **Wildcard Mask** : گزینه **wildcard_mask** در مثال بالا در واقع حالت inverse شده subnetmaskاست . اگر octet در حالت wildcardmask بصورت عدد 0 باشد به معنی این است که Octet هایی که در شبکه وجود دارند می بایست دقیقا با مسیری که تعریف شده است برابری کنند. از طرفی دیگر اگر در این قسمت عدد 255 قرار بگیرد به معنی این است که شما به عددی که در octed شبکه وجود دارد توجهی نخواهید داشت. ترکیب network و wildcard maskبه شکل 192.168.10.0 0.0.0.0 فقط محدوده آدرس 192.168.10.0 را قبول می کند و هیچ شبکه دیگری قابل قبول نخواهد بود.
- **Area Number** : گزینه **Area Number** #_در مثال بالا به منزله **Area Number** می باشد . **Area Number** همیشه یا بهتر بگوییم معمولا در شبکه های کوچک عدد صفر یا 0 است ، اما برای شبکه های بزرگتر **Area Number** ها هم بایستی به گونه ای طراحی شوند که بتوانند تمامی routing update هایی که از Area 0 دریاف می شود را پشتیبانی کنند

سه عدد روتر ، سه عدد سویچ و سه عدد Host داریم که با سه محدوده آدرسی دهی متفاوت به هم متصل شده اند:



ITPRO-R1>enable

ITPRO-R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ITPRO-R1 (config)#router ospf 1

ITPRO-R1 (config-router)#network 172.16.0.0 0.0.255.255 area 0

ITPRO-R1 (config-router)#network 172.17.0.0 0.0.255.255 area 0

ITPRO-R1 (config-router)#exit

ITPRO-R1 (config)#exit

ITPRO-R1#

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور **copy running-config startup-config** را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود.

انجام تنظیمات مربوط به پروتکل OSPF روی روتر ITPRO-R2

با استفاده از دستور زیر به پورت کنسول **ITPRO-R2** متصل شوید و تنظیمات **OSPF** را روی آن انجام دهید. دستورات مربوط به پیکربندی **OSPF** را در ابتدای مقاله عنوان کردیم شما می توانید به پاراگراف اول همین آموزش مراجعه کنید. با استفاده از دستور **network** همانطور که در تصویر پایین مشاهده می کنید ما فقط لینک هایی که بصورت مستقیم به روتر متصل شده اند را به آن معرفی می کنیم ، دستورات زیر را می توانید بدون کمی و کاستی در روتر خود وارد کنید:

ITPRO-R2>

ITPRO-R2>enable

ITPRO-R2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ITPRO-R2(config)#router ospf 1

ITPRO-R2(config-router)#network 172.17.0.0 0.0.255.255 area 0

ITPRO-R2(config-router)#network 172.18.0.0 0.0.255.255 area 0

ITPRO-R2(config-router)#network 172.19.0.0 0.0.255.255 area 0

ITPRO-R2(config-router)#exit

ITPRO-R2(config)#exit

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور **copy running-config startup-config** را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود.

انجام تنظیمات مربوط به پروتکل OSPF روی روتر ITPRO-R3

با استفاده از دستور زیر به پورت کنسول **ITPRO-R3** متصل شوید و تنظیمات **OSPF** را روی آن انجام دهید. دستورات مربوط به پیکربندی **OSPF** را در ابتدای مقاله عنوان کردیم شما می توانید به پاراگراف اول همین آموزش مراجعه کنید. با استفاده از دستور **network** همانطور که در تصویر پایین مشاهده می کنید ما فقط لینک هایی که بصورت مستقیم به روتر متصل شده اند را به آن معرفی می کنیم ، دستورات زیر را می توانید بدون کمی و کاستی در روتر خود وارد کنید:

```
ITPRO-R3>enable
ITPRO-R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ITPRO-R3(config)#router ospf 1
ITPRO-R3(config-router)#network 172.19.0.0 0.0.255.255 area 0
ITPRO-R3(config-router)#network 172.20.0.0 0.0.255.255 area 0
ITPRO-R3(config-router)#exit
ITPRO-R3(config)#exit
ITPRO-R3#
```

فراموش نکنید که بعد از وارد کردن دستورات بالا در انتها دستور **copy running-config startup-config** را در **enable mode** بزنید تا تنظیمات شما روی روتر بصورت دائمی ذخیره شود و بعد از restart شدن روتر تنظیمات از بین نرود.

مشاهده Routing Table های موجود روی ITPRO-R1

بعد از وارد کردن دستورات بالا برای پیاده سازی پروتکل OSPF در روتر **ITPRO-R1** با استفاده از دستور **show ip route** در این روتر شما می توانید خروجی routing table موجود در این روتر را به شکل زیر مشاهده کنید:

```
ITPRO-R1>enable
ITPRO-R1#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 area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
  C    172.16.0.0/16 is directly connected, FastEthernet0/0
  C    172.17.0.0/16 is directly connected, Serial0/0
  O    172.18.0.0/16 [110/65] via 172.17.0.2, 00:26:31, Serial0/0
  O    172.19.0.0/16 [110/128] via 172.17.0.2, 00:26:21, Serial0/0
  O    172.20.0.0/16 [110/129] via 172.17.0.2, 00:24:54, Serial0/0
```

در خروجی دستورات بالا کاراکتر O در ابتدای خط مربوط به routing table ها به معنی این است که مسیری که پیدا شده است از طریق پروتکل مسیریابی Open Shortest Path First یا OSPF شناسایی شده است و کاراکتر C به معنی اتصال مستقیم یا directly connected می باشد.

مشاهده Routing Table های موجود روی ITPRO-R2

بعد از وارد کردن دستورات بالا برای پیاده سازی پروتکل OSPF در روتر **ITPRO-R2** با استفاده از دستور **show ip route** در این روتر شما می توانید خروجی routing table موجود در این روتر را به شکل زیر مشاهده کنید:

```
ITPRO-R2>enable
ITPRO-R2#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 area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
O    172.16.0.0/16 [110/65] via 172.17.0.1, 00:30:20, Serial0/0
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
C    172.19.0.0/16 is directly connected, Serial0/1
O    172.20.0.0/16 [110/65] via 172.19.0.2, 00:28:08, Serial0/1
```

در خروجی دستورات بالا کاراکتر O در ابتدای خط مربوط به routing table ها به معنی این است که مسیری که پیدا شده است از طریق پروتکل مسیریابی **Open Shortest Path First** یا **OSPF** شناسایی شده است و کاراکتر C به معنی اتصال مستقیم یا directly connected می باشد.

مشاهده Routing Table های موجود روی ITPRO-R3

بعد از وارد کردن دستورات بالا برای پیاده سازی پروتکل OSPF در روتر **ITPRO-R3** با استفاده از دستور **show ip route** در این روتر شما می توانید خروجی routing table موجود در این روتر را به شکل زیر مشاهده کنید:

```
ITPRO-R3>enable
ITPRO-R3#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 area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
O    172.16.0.0/16 [110/129] via 172.19.0.1, 00:29:43, Serial0/1
O    172.17.0.0/16 [110/128] via 172.19.0.1, 00:29:43, Serial0/1
O    172.18.0.0/16 [110/65] via 172.19.0.1, 00:29:43, Serial0/1
C    172.19.0.0/16 is directly connected, Serial0/1
C    172.20.0.0/16 is directly connected, FastEthernet0/0
```

در خروجی دستورات بالا کاراکتر O در ابتدای خط مربوط به routing table ها به معنی این است که مسیری که پیدا شده است از طریق پروتکل مسیریابی Open Shortest Path First یا OSPF شناسایی شده است و کاراکتر C به معنی اتصال مستقیم یا directly connected می باشد.

اطمینان از عملکرد درست و تست ارتباط بین شبکه ها با استفاده از دستور Ping

برای اینکه مطمئن شویم که پروتکل مسیریابی **Open Shortest Path First یا OSPF**به درستی کار می کند از طریق دستور ping از ITPRO-Host01 که دارای آدرس IP به شکل 16//172.16.0.10 است ITPRO-Host03 که دارای آدرس IP به شکل 16//172.20.0.10 است را ping می کنیم در صورتیکه عملیات با موفقیت مانند خروجی زیر انجام شد کار به درستی انجام شده است و OSPF پیاده سازی شده است:

C:\>ping 172.20.0.10

Pinging 172.20.0.10 with 32 bytes of data:

Reply from 172.20.0.10: bytes=32 time=172ms TTL=125

Reply from 172.20.0.10: bytes=32 time=188ms TTL=125

Reply from 172.20.0.10: bytes=32 time=157ms TTL=125

Reply from 172.20.0.10: bytes=32 time=188ms TTL=125

Ping statistics for 172.20.0.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 157ms, Maximum = 188ms, Average = 176ms