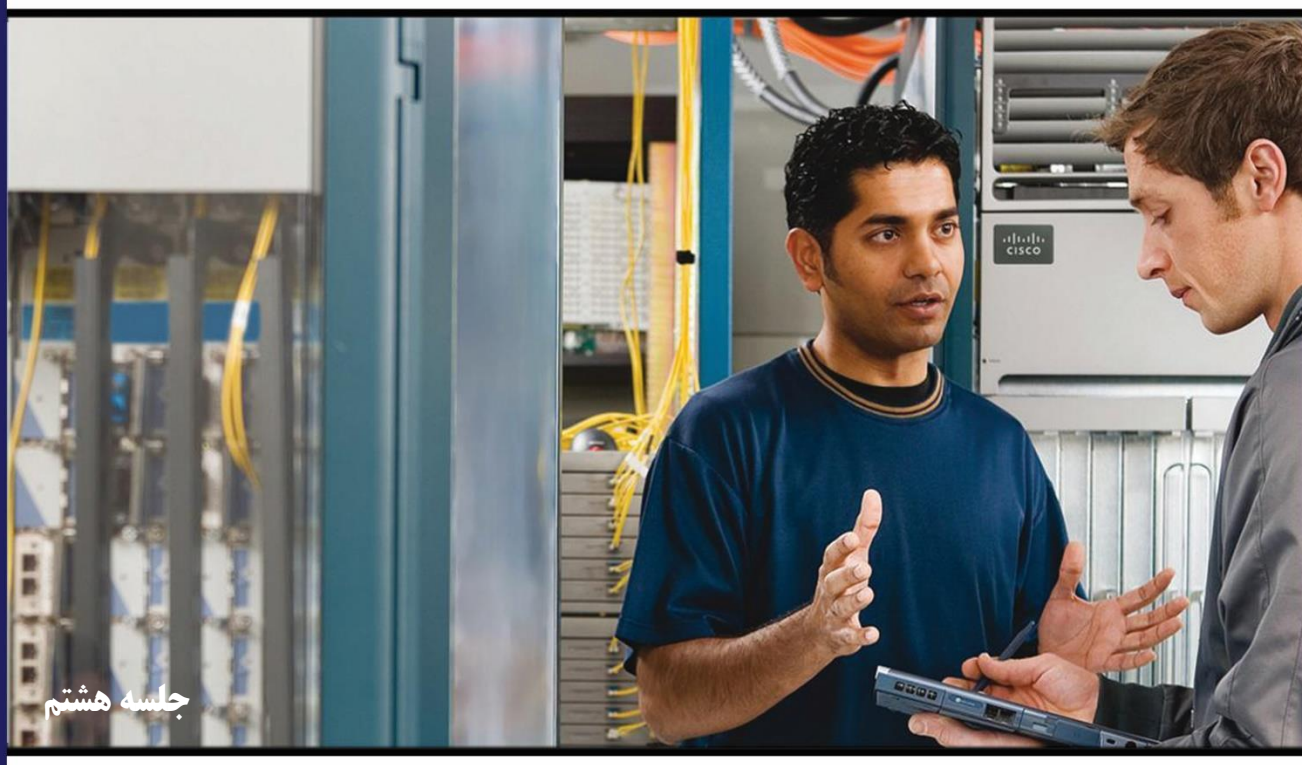
مبانی اولیه سیسکو

CCNA

CISCO CERTIFIED
CCNA
Security



✓ آموزش کامل Routing & Switching

✓ به همراه سناریو

نویسنده: مهندس امیرحسین خالقی

فهرست

پیشگفتار

سپاس پروردگار را که این امکان را داد که تا باز بتوانیم مجموعه ای پر مطلب و پر فهم را کمتر از یک سال بنویسیم.

این کتاب با توجه به سرفصل های کتاب CCNA ICND 1 & ICND 2 برای علاقه مندان به شبکه و سیسکو نوشته شده است. در تهیه این کتاب سعی بر آن شده است تا فهم مطالب و مباحث به صورت روان و گیرا مطرح گردد.

در ابتدای کتاب سر فصل مطالب قید شده است. در انتهای هر فصل سناریویی طراحی شده که می تواند در فهم و یادگیری سریع تر شما کمک کند. توصیه می شود که این سناریو ها حتما کار شود. در انتهای کتاب به بررسی نمونه سوالات آزمون Cisco پرداخته ایم.

درصورت هرگونه مشکل در این کتاب میتوانید با ایمیل نویسنده (info@akhaleghi.ir) تماس حاصل فرمایید تا با بررسی آن بتوانیم کتابی کامل و با زبان فارسی در اختیار شما دوستان و همکاران ارجمند قرار دهیم.

در پایان از تمامی عزیزانی که ما را در تهیه و تنظیم این کتاب یاری نموده اند کمال تشکر را داریم.

باشد که موثر باشیم ....

امیرحسین خالقی

DHCP :

DHCP یا (Dynamic Host Configuration Protocol) یکی از سرویسهای بسیار مهم و پرکاربرد سیستم عاملهای مایکروسافت است. این سرویس امکان تعریف آدرس IP و دیگر تنظیمات مورد نیاز کامپیوتر های سرویس گیرنده (Client) بطور اتوماتیک را فراهم می آورد. میدانیم که در صورت ازدیاد تعداد کامپیوتر های سرویس گیرنده در شبکه های بزرگ مدیریت این شبکه ها بسیار سخت و زمان بر میباشد. همچنین تعریف و مدیریت تنظیماتی آدرسی این کامپیوترها نیز بطبع سخت خواهد شد.

سرویس DHCP این امکان را به مدیر شبکه میدهد تا تمامی تنظیمات و آدرسهای مورد نیاز که باید به سرویس گیرنده ها تعلق گیرد را در DHCP Server به صورت متمرکز انجام دهد و این سرور هم با استفاده از روشی که در اینجا توضیح داده شده است ، این آدرسها را به کامپیوترهای فاقد آدرس ارسال و در اختیار آنها قرار دهد. حال این سرور با دیگر تنظیماتی که در اختیار مدیر شبکه میگذارد امکان مدیریت آسان را به ایشان میدهد.

فرض میکنیم که مدیریت یک شبکه در اختیار ما قرار داده شده است. ابتدا باید برای ارتباط صحیح مابین کامپیوترهای شبکه و همچنین در صورت نیاز ارتباط این شبکه با شبکه های دیگر آدرسهای مورد نیاز را در اختیار این کامپیوتر ها قرار دهیم. تصمیم گرفتیم این کار را با سرویس DHCP انجام دهیم. ابتدا باید طراحی آدرسها را انجام دهیم و سپس باید سرویس DHCP را فعال کنیم.

الف) DHCP در روترها:

برای فعال کردن DHCP در روتر به صورت زیر عمل میکنیم:

ابتدا باید بصورت زیر Pool بسازیم :

(جلوی Pool یک نام انتخاب میکنیم)

سپس به صورت زیر عمل می کنیم:

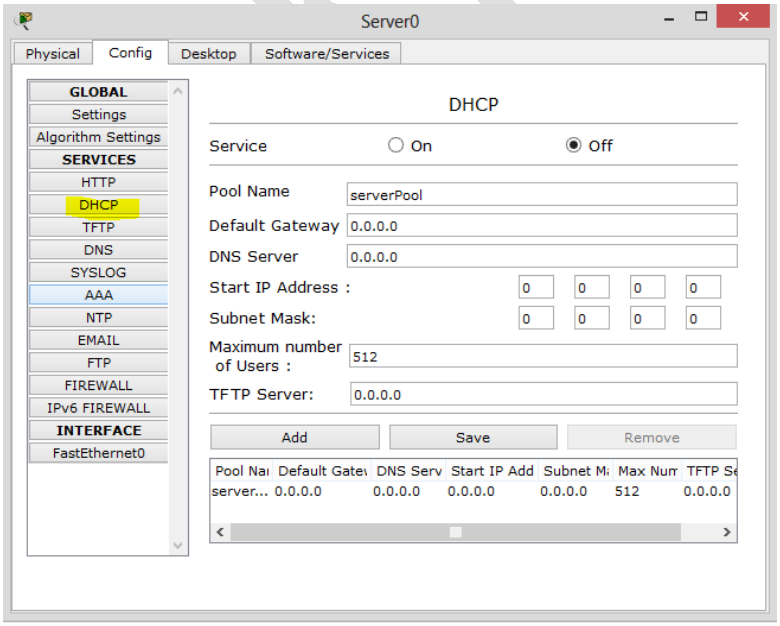
```
Router(config)#ip dhcp pool vlan2
Router(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
Router(dhcp-config)#network 192.168.2.2 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns 4.2.2.4
```

پس از آن اگر بر روی PC IP Configuration آن را بر روی DHCP بگذاریم میبینیم که به صورت اتومات IP گرفت.

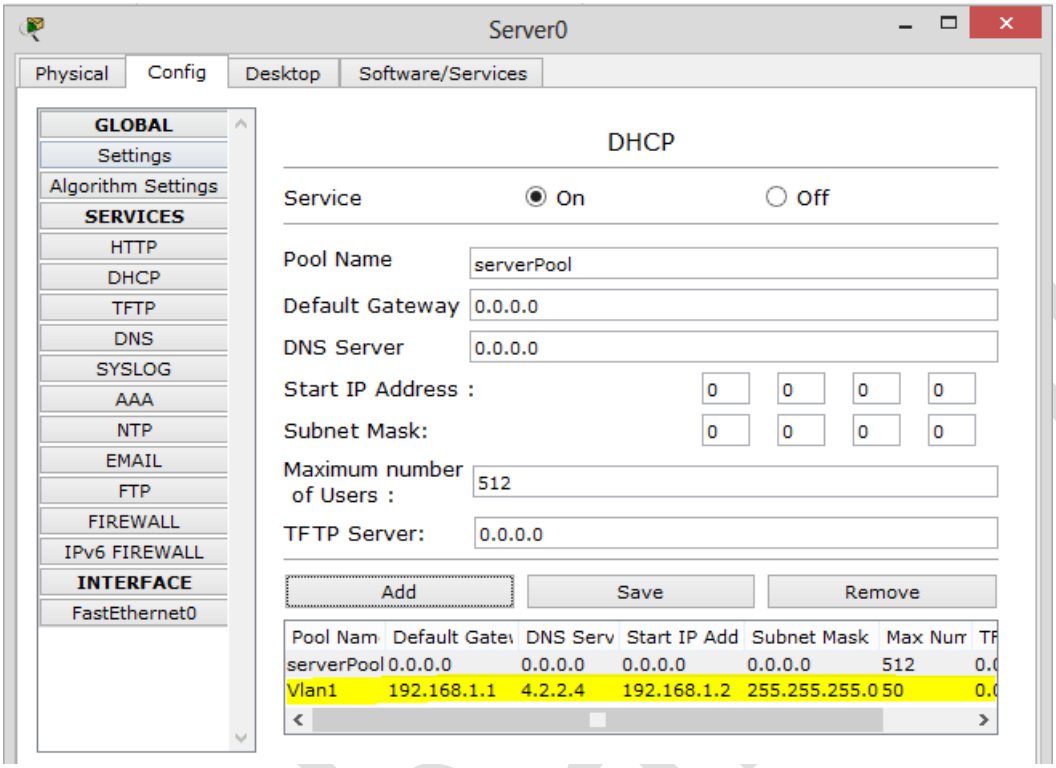
ب) DHCP Server :

برای فعال کردن آن بر روی سرور واقعی لازم است کتاب MCITP را بخوانید اما در اینجا (در محیط Packet Tracer) به صورت زیر عمل میکنیم:

یک سرور انتخاب میکنیم و وارد محیط Config DHCP آن می شویم:



- ✓ اول از همه Service آن را On می کنیم.
- ✓ سپس Pool name را انتخاب کرده و بعد DNS , Gateway را انتخاب میکینیم.
- ✓ Start IP اولین IP که شروع شود به همراه Subnet mask آن را وارد میکنیم.
- ✓ Maximum number یعنی بیشترین تعدادی که IP بدهد ودر آخر Add می کنیم.



سپس بر روی Sub interface ها ip helper-address میگذاریم. بدین معنا که برای گرفتن IP از DHCP از فلان IP بپرس!

```
Router(config)#interface fastEthernet 0/1.3
Router(config-subif)#ip helper-address 192.168.4.2
```

و تمام. حال مشاهده میکنید که تمام PC ها از IP DHCP میگیرد.

تذکر مهم : فراموش نشود که همیشه اگر بیش از ۱ Vlan بر روی روتر داشتیم باید از Inter Vlan Routing استفاده کنیم و اگر هم یک Vlan بود باید Gateway آن را بر روی Interface روتر Set کنیم همچنین اگر DHCP Server داشتیم باید Gateway آن بر روی Interface مربوطه Set شود.

DNS :

کلمه DNS ، مخفف Domain Name System یا "سیستم نام دامنه" است. سیستم نام دامنه (DNS) یک سیستم پایگاه داده است که نام کامل دامنه یک کامپیوتر را به یک آدرس IP ترجمه میکند.

کامپیوترهای موجود در یک شبکه برای اتصال به یکدیگر از آدرسهای IP استفاده می کنند، ولی به یاد داشتن آدرس های IP کامپیوترهای یک شبکه برای افرادی که قصد اتصال به آنان را دارند بسیار دشوار است. مثلا به خاطر سپردن نام دامنه www.Google.com بسیار ساده تر از به خاطر سپردن

آدرس IP نظیر آن (۷۴,۱۲۵,۲۳۲,۱۲۸) است. به همین علت اغلب ما برای اتصال به سایت ها، نام دامنه آن را وارد می کنیم. لذا DNS به شما امکان می دهد تا به جای استفاده از آدرس های عددی IP برای اتصال به یک کامپیوتر خاص در شبکه ای دیگر (یا برای دسترسی به یک سرویس راه دور)، با به کارگیری نام دامنه ای که به خاطر آوردن آن برای شما راحت تر است به آن کامپیوتر متصل شده یا از آن سرویس بهره بگیرید.

هر سازمانی که دارای یک شبکه کامپیوتری است حداقل مجهز به یک سرور مرکزی است که پرس و جوهای DNS را کنترل و سازماندهی می کند. این سرور که Name Server نامیده می شود فهرستی از همه آدرس های IP اختصاص داده شده به کامپیوترهای موجود در آن شبکه را نگه می دارد. این سرور همچنین آدرس های IP آن دسته از کامپیوترهای خارج از شبکه را که اخیرا مورد دسترسی قرار گرفته اند نیز نگه می دارد. هر کامپیوتر در هر شبکه باید مکان تنها یک Name Server را بداند.

زمانی که کامپیوتر شما درخواست یک آدرس IP را می کند، بسته به اینکه آدرس IP درخواست شده در محدوده شبکه محلی شما قرار دارد یا خیر یکی از این سه حالت رخ می دهد:

حالت اول : اگر آدرس IP درخواست شده به طور محلی ثبت شده است (مثلا این آدرس متعلق به یکی از کامپیوترهای شبکه سازمان شماست) مستقیما پاسخی را از یکی از Name Server های محلی فهرست شده در تنظیمات Workstation خود دریافت خواهید داشت. در این حالت معمولا دریافت پاسخ یا خیلی کم طول می کشد یا به صورت کاملا بلادرنگ صورت می گیرد.

حالت دوم : اگر آدرس IP درخواست شده به صورت محلی ثبت نشده است (مثلا این آدرس متعلق به کامپیوتری در خارج شبکه سازمان شماست) ولی شخصی در سازمان شما اخیرا به همان آدرس IP رجوع کرده و به سایت نظیر آن متصل شده است، آنگاه Name Server آدرس IP را از سیستم ذخیره سازی کش خود بازیابی خواهد کرد (کش= حافظه ای محدود که بخشی از آدرسهای IP که اخیرا مورد مراجعه قرار گرفته اند را در خود نگه می دارد). مجددا در این حالت هم معمولا دریافت پاسخ یا خیلی کم طول می کشد یا به صورت کاملا بلادرنگ صورت می گیرد.

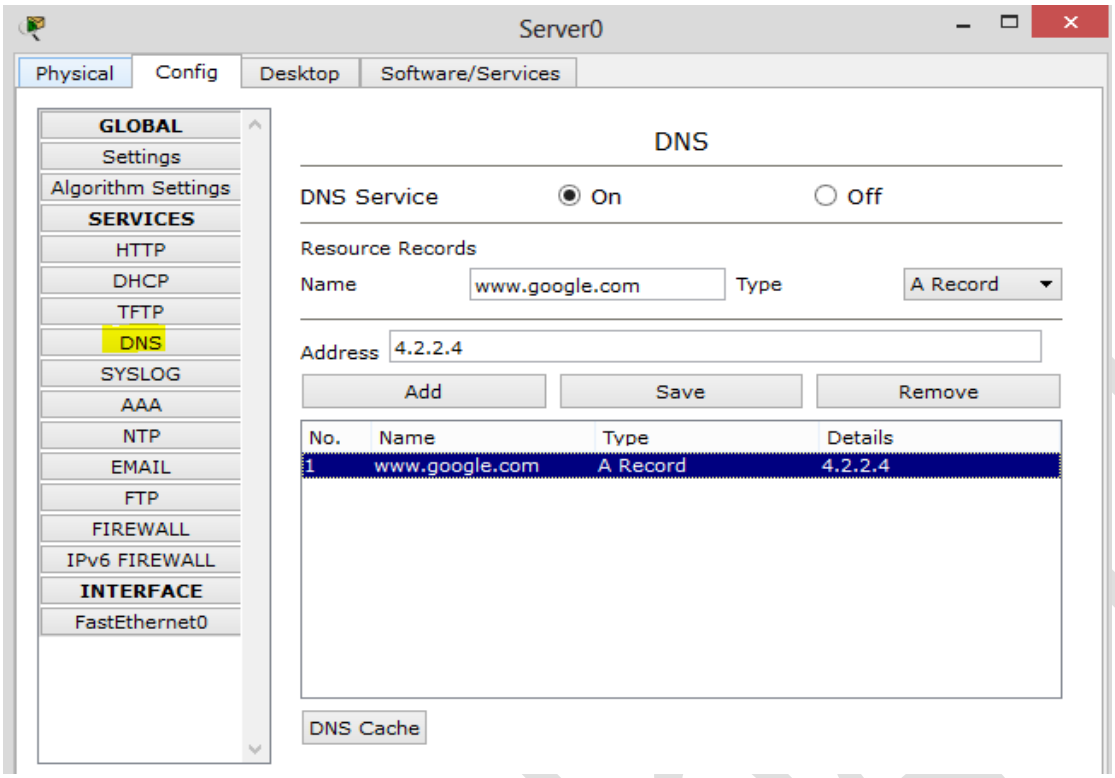
حالت سوم : اگر آدرس IP درخواست شده به صورت محلی ثبت نشده است و شما اولین کسی هستید که در یک بازه زمانی خاص اطلاعاتی از سیستم مورد نظر را درخواست کرده اید، (از ۱۲ ساعت تا یک هفته پیش) آنگاه Name Server محلی به جای Workstation شما جستجو را انجام خواهد داد. این جستجو ممکن است شامل پرس و جو از دو یا چند Name Server دیگر در هر مکان راه دور دیگری باشد. این پرس و جوها ممکن است از یک ثانیه تا بیشتر به طول انجامد (بسته به آنکه اتصال شما به شبکه راه دور چه کیفیتی دارد و با چند Name Server بایستی ارتباط برقرار شود)

برخی اوقات به خاطر پروتکل Lightweight مورد استفاده در DNS ، ممکن است پاسخی دریافت نکنید. در چنین شرایطی Workstation یا نرم افزار Client شما ممکن است تا زمان دریافت پاسخ به تکرار پرس و جوی خود ادامه دهد یا ممکن است پیام خطایی دریافت کنید.

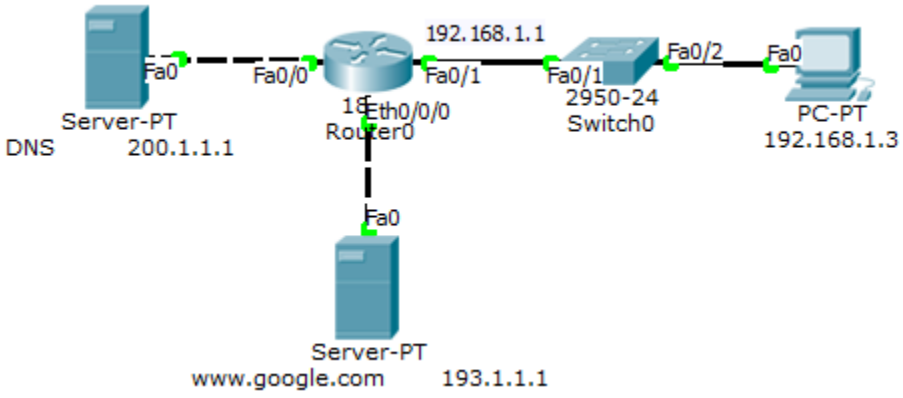
زمانی که از برنامه ای مثل Telnet برای اتصال به کامپیوتری دیگر استفاده می کنید، احتمالا برای برقراری این اتصال به جای تایپ کردن آدرس کامپیوتر مورد نظر، نام دامنه آن را وارد می کنید. برنامه Telnet نام دامنه ای که توسط کاربر تایپ شده است را دریافت کرده و با به کارگیری یکی از روشهایی که در بالا گفته شد و به کمک Name Server ، آدرس IP نظیر آن را به دست می آورد.

به عنوان مثال می توان DNS را مانند یک دفترچه تلفن الکترونیکی برای یک شبکه کامپیوتری در نظر گرفت، به طوری که اگر نام کامپیوتر مورد نظر را بدانید، Name Server آدرس IP نظیر آن را جستجو کرده و می یابد.

اما چگونگی کار DNS در Cisco Packet Tracer بدین گونه است که یک سرور انتخاب کرده و از محیط Config آن DNS را انتخاب می کنیم:



ابتدا آن را On کرده سپس نام دلخواه را انتخاب میکنیم و در قسمت Name می نویسیم بعد از آن Address دلخواه آن را مینویسیم وبعد Add میکنیم. لازم به ذکر است که همانند DHCP این تنظیمات با محیط سرور واقعی متفاوت است و برای تنظیمات در سرور واقعی بهتر است کتاب MCITP را بخوانید.



پس از آن مطابق شکل مقابل یا خودش و یا یک سرور دیگر را به عنوان سایت می گذاریم IP می دهیم و اگر از داخل PC سایت www.google.comرا چک کنیم میبینیم برایمان صفحه باز میکند!

اما یک نکته:

همان طور که میدانید ما در هر روتر دو Fastehternet Port داریم و اگر تعداد بیشتری نیاز داشته باشیم باید ماژول آن را نصب کنیم که آموزش آن را در کتاب آموزش Cisco Packet Tracer داده ایم.

در اینجا چون ما ماژول Ethernet گذاشته ایم باید در دستور آن بگوییم Interface Ethernet 0/0/0

Telnet:

تِلنت : شبکه‌ای است که در اینترنت و بخش‌های داخلی استفاده می‌شود. این شبکه در سال ۱۹۶۹ توسعه یافت و RFC 15 در آن استفاده شد. استاندارد آن به صورت IETFSTP8 می‌باشد. مشتریان می‌توانند از سیستم UNIX به مدت چندین سال استفاده کنند، بیشتر تجهیزات شبکه‌ای و OSکه TCP/IP دارند حامی Telnet هستند. اخیرا Secure Shell از دسترسی راه دور برای Unix استفاده می‌کند. این اصطلاح به برقراری روابط Telnetو TCP اشاره دارد. در واقع سرور می‌تواند از یک رمز عبور استفاده کند، یک کاربر می‌تواند سیستم سرور Unix را ساده کند و مانند کلید عمل نماید. به عنوان مثال کاربر می‌تواند پست الکترونیکی خود را در مدرسه کنترل کند، به این طریق می‌تواند ارتباطات کامپیوتری را با سرور برقرار کرد. در این حالت باید اطلاعات و اجرای سیستم‌عامل از راه دور در نظر گرفته شوند .

در سیستمهای زیادی، سرویس گیرنده می‌تواند از جلسات تعاملی TCP استفاده نماید. در این زمینه جلسات Telnet در واقع TCP خام را با ۲۵۵ بایت عرضه می‌کنند. Telnet یک پروتکل سرویس دهنده و سرویس گیرنده است و براساس انتقال ارتباطی عمل می‌کند. این TCP بر روی Port ۲۳ است. اگر چه telnet می‌تواند TCP/IP را بر NCP اجرا کند. پروتکل‌ها چند پسوند دارند و هر یک استاندارد اینترنت می‌باشند. IETF به STD ۲۷ اشاره می‌کند. STB ۳۲ نیز در تعریف پسوندها کاربرد داشته‌است. دیگر پسوندهای IETF یک استاندارد هستند.

وقتی Telnet در سال ۱۹۶۹ طراحی شد بیشتر کاربرهای شبکه درحوزه‌های کامپیوتر موسسات آکادمیک، یا در تسهیلات تحقیق دولتی و خصوصی فعال بودند. در این محیط(سال ۱۹۶۹) امنیت خیلی مورد توجه نبود تا اینکه سال ۱۹۹۰ انفجار پهنای باند شد. با افزایش تعداد مردم در دسترسی به اینترنت، و با توسعه، تعدادی تلاش می‌کنند تا به سرویس دهنده‌های دیگر نفوذ (crack) کنند که (سرویس دهنده‌ها) به طور متناوب رمزگذاری شدند حتی بیشتر از یک ضرورت. کارشناسان ایمنی مانند موسسه Sans و اعضای Compos معتقدند که استفاده از Telnet برای ثبت راه دور می‌تواند در شرایط عادی متوقف شود. این به دلایل زیر گزارش شده‌است.

Telnet نمی‌تواند رمزبرداری داده‌های ارسال شده را انجام دهد .بنابراین می‌توان روابط را با یک رمز عبور رشد داد. این عامل دسترسی به یک ردیاب است. آنها بین دو میزبان قرار دارند و Telnet می‌تواند بسته‌ها را با اطلاعات کافی عرضه کند. برنامه‌های کمکی مانند Tcdump و Wireshark از این نوع هستند. این نوع فرآیندهای اجرایی Telnet می‌توانند بدون طرح اعتبارسازی توصیف شوند. بنابراین باید ارتباطات بین دو میزبان برقرار شوند. در Telnet چندین آسیب پذیری نیز دیده شده است. این نوع نقایص در استفاده پروتکل Telnet زیاد هستند به خصوص در اینترنت و پروتکل SSHکه ابتدا در سال ۱۹۹۵ گزارش شد.

SSH می‌تواند قابلیت Telnet را افزایش دهد. این اعتبارسازی کلیدی می‌تواند متضمن دسترسی به ادعاهای واقعی باشد. این پروتکل‌ها تعمیم Telnetهستند و می‌توانند اعتبار sasl و امنیت TLS را به دنبال داشته باشند. با این وجود بیشتر این فرآیندها حامی این تعمیم نمی‌باشند. علاه به اجرای SSH می‌تواند کافی باشد. مزیت اصلی TLS- TENET شامل توانایی استفاده از گواهینامه سرور می‌باشد. آنها دارای کلید ذخیره می‌باشند. در SSH ضعفهای کاربر باید به خوبی شناخته شوند.

در واقع Telnet و SSH کاربرد آن در این است که ما بتوانیم هرکجا که هستیم از طریق یک PC به روتر و سوییچ و ... به راحتی متصل شویم.

برای استفاده از Telnet هم باید روی ویندوز و هم روی روتر و سوییچ فعال شود. در ویندوز به صورت زیر عمل میکنیم:

- ✓ به Control Panel رفته و Uninstall a program را انتخاب می کنیم.
- ✓ سمت چپ گزینه ی Turn Windows features on or off را انتخاب می کنیم.
- ✓ تیک گزینه ی Telnet را زده و Ok می کنیم و میگذاریم نصب گردد.

اما در محیط روتر و یا سوییچ به صورت زیر عمل میکنیم:

```
Router(config)#line vty 0
Router(config-line)#login local
Router(config-line)#no login
Router(config-line)#login
```

- ✓ ابتدا روی Interface , IP میگذاریم
- ✓ دیواره های Secret را میسازیم و پسورد گذاری می کنیم.
- ✓ Command های زیر را در روتر یا سوییچ وارد می کنیم:

یکی از مواردی که با رنگ زرد نمایش داده شده را انتخاب میکنیم که Login Local برای استفاده از User name & Password به صورت همزمان و Login برای استفاده از Password به صورت تنها و no Login برای خاموش کردن Telnet می باشد.

سپس در سیستم مورد نظر Cmd را باز کرده و به صورت زیر عمل میکنیم:

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Username: amir
Password:
Router>
```

User & Pass را وارد کرده همان طور که در شکل میبینم وارد روتر شدیم و تمام عملیاتی که انجام میدادیم را در اینجا هم میتوان انجام داد.

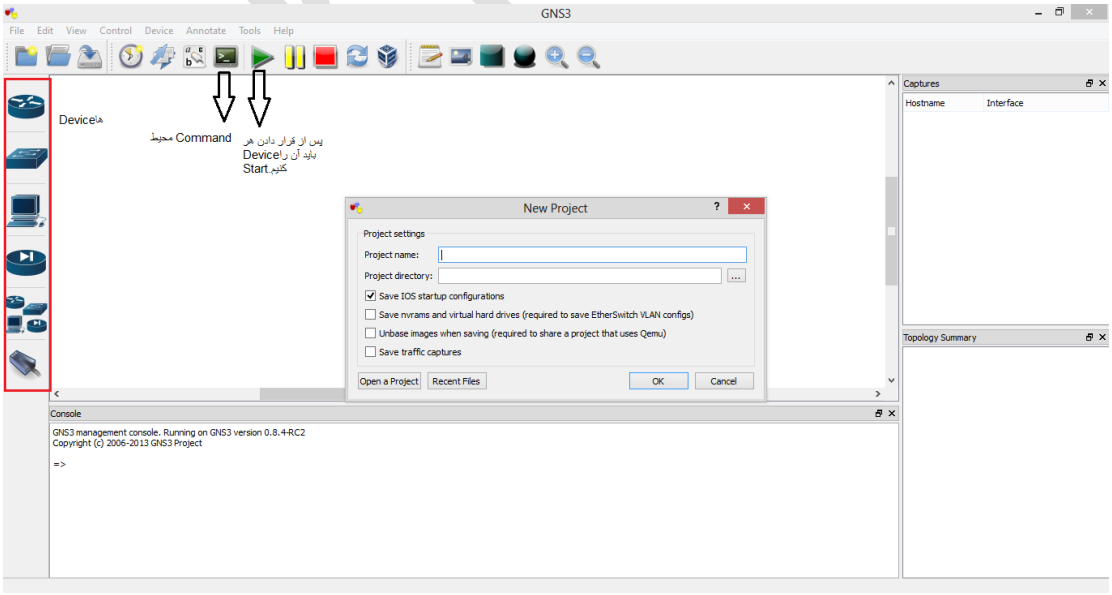
GNS3 :

دو نوع سیمولاتور هایی که در این زمینه استفاده می شوند عبارتند از:

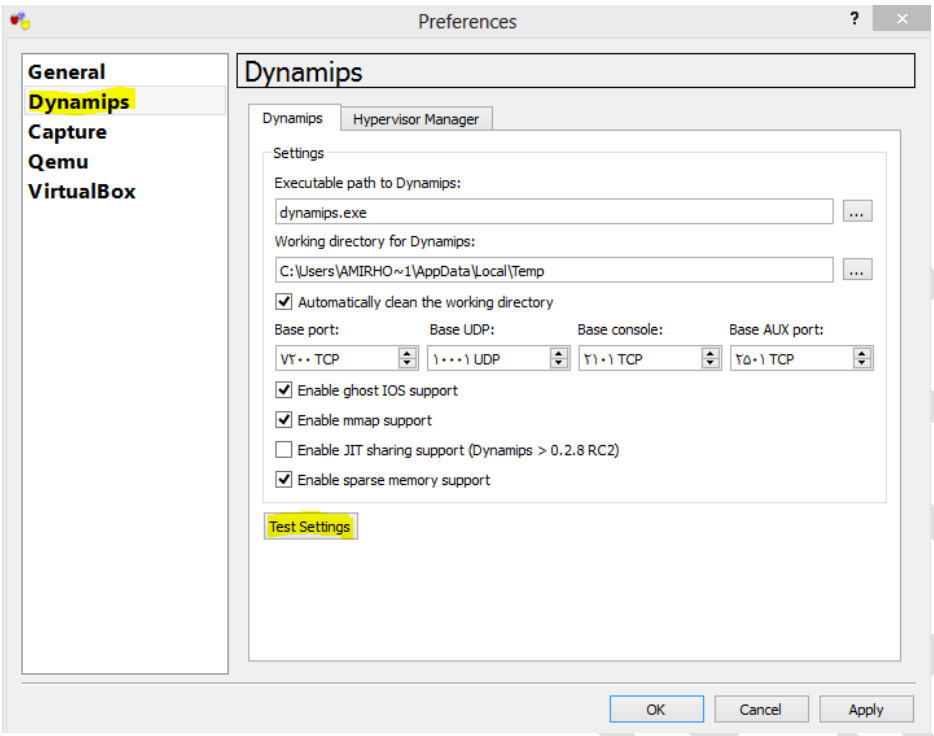
- ✓ نرم افزار GNS که ما در این آموزش از این نرم افزار استفاده می کنیم.
- ✓ نرم افزار Packet Tracer

هر دو شبیه ساز خوب هستند . اما GNS یک جورایی از شبیه سازی فاصله گرفته و دقیقا یک روتر واقعی رو پیاده سازی می کند.

نصب کردن خیلی ساده ای دارد و مثل باقی نرم افزار های کامپیوتری با چند تا Next نصب می شود. پس از نصب موقع اجرای نرم افزار با صفحه زیر روبرو خواهید شد.

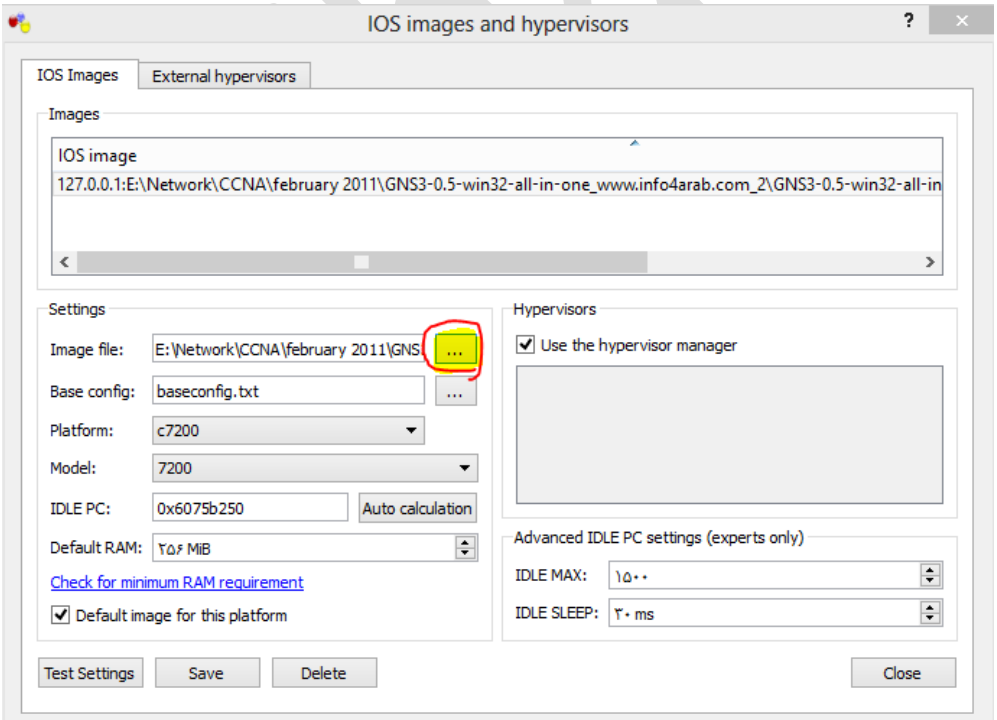


به محیط Edit Preferences بروید. در اینجا برای شروع به کار نرم افزار باید ۲ کار انجام دهید:



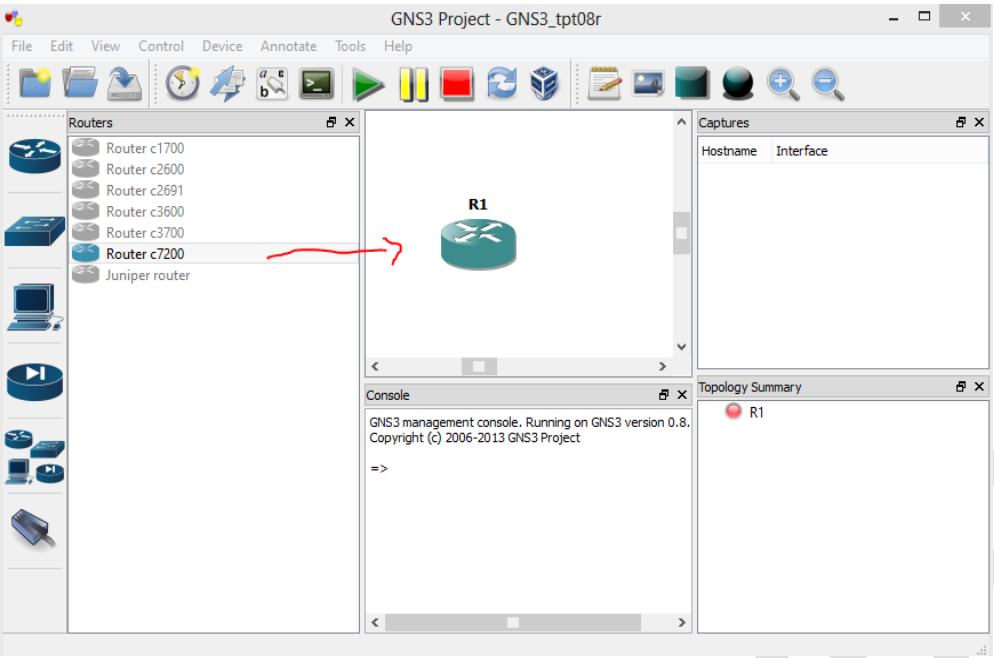
قسمت Dynamips رو باید چک کنیم بر روی Test Setting کلیک کنید.اگر Successfully نداد در قسمت working directory خودتون یک جای دیگه یک فولدر بسازید و به برنامه معرفی کنید و بعد دوباره Test رو بزنید تا successfully دهد.

بعد از این که عملیات با موفقیت انجام شده در همین پنجره فوق ok می زنیم و به Edit IOS images and hypervisors می رویم. در این قسمت باید IOS به برنامه معرفی کنیم. همانطور که در شکل زیر می بینید در قسمت مشخص شده باید IOS مربوطه را به نرم افزار بدهیم که پسوند bin دارد.



بدون IOS روتر در داخل نرم افزار کار نخواهد کرد و این گام اجباری هست .بعد از معرفی IOS ، حالا ذخیره می کنیم .

چون IOS ما مدل ۷۲۰۰ بوده حالا می توانیم روتر ۷۲۰۰ رو بکشیم به داخل صفحه و برروی آن کار کنیم. مطابق شکل زیر:



دقت کنید مشکلی که در این میان وجود دارد ، بحث پردازش سنگینی که این نرم افزار بر روی CPU می اندازد است. جهت حل این مشکل ، پس از start کردن روتر مطابق شکل بالا، برروی روتر راست کلیک می کنیم و گزینه Idle PC رو انتخاب می کنیم. سپس از پنجره ظاهر شده قسمت علامت دار را انتخاب کرده و OK میکنیم.

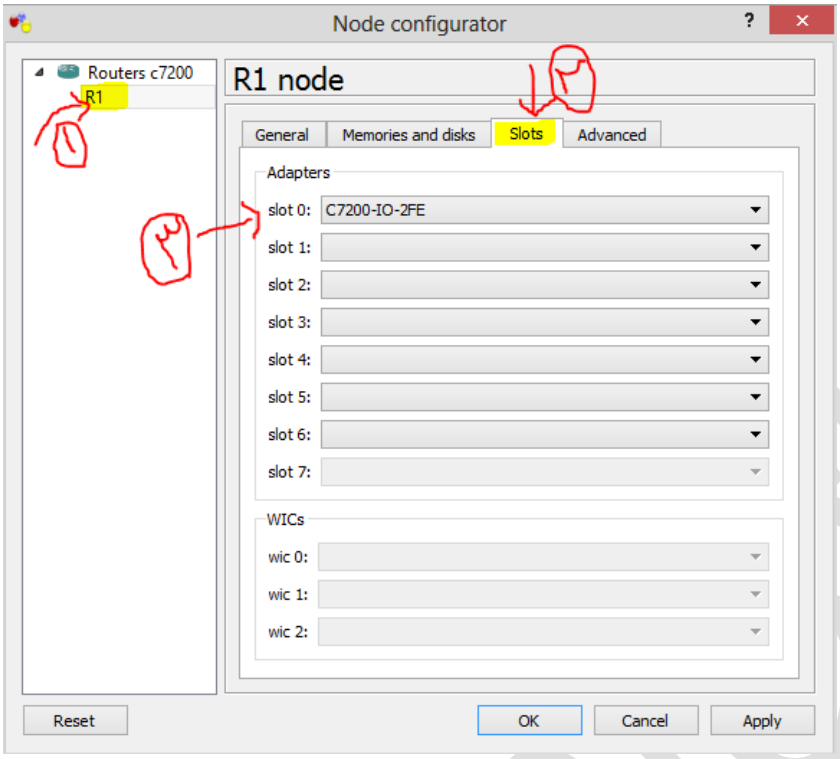
خب .حالا میرسیم سر کانفیگ روترمون. که البته این کار رو از پورت کنسول انجام میدهیم. جهت این کار بر روی روتر راست کلیک کرده و گزینه Console رو انتخاب می کنیم .پنجره مشکی رنگ داس ظاهر می شود و منتظر می شویم تا روتر آماده به کار شود.

اگر کانفیگ های اولیه بر روی دستگاه وجود نداشته باشد ، در روترهای واقعی ، وارد محیطی به نام Setup Mode می شود. در این محیط به صورت پرسش پاسخی کانفیگ های اولیه را از شما می پرسد. بعنوان مثال اسم روتر چی باشد . ست کردن پسورد و ...

البته شما با زدن حرف N یا همون No می توانید به روتر بگویید که تمایل به استفاده از محیط Setup Mode را ندارد و این محیط رو رد کنید. پس از زدن یکی دوتا Enter ، وارد روتر شده و شما می توانید کانفیگ های خود را بر روی روتر اعمال کنید. بقیه تنظیمات همه همانند روتر موجود در Cisco Packet Tracer است که قبلا به شما آموزش دادیم!

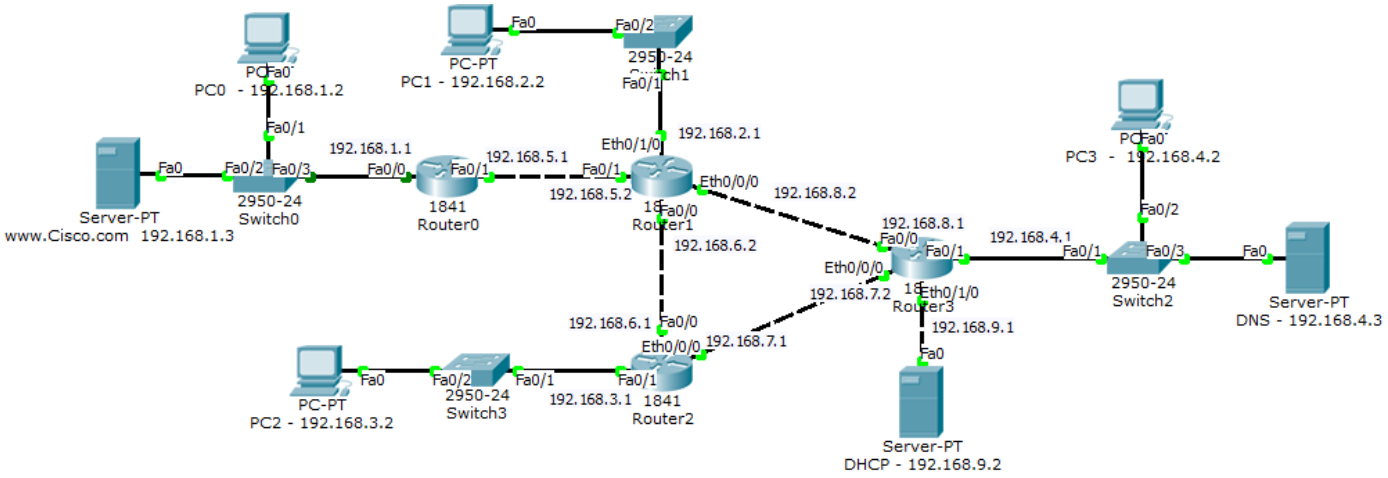
نصب ماژول:

- ✓ بر روی روتر راست کلیک کرده و configure را می زنیم:
- ✓ ابتدا R1 را انتخاب کرده و در تب Slots از بین Slot ها ماژول خود را انتخاب می کنیم.
- ✓ بعد از آن OK می کنیم.



نکته: توجه داشته باشید که حتما Device خاموش باشد.

سناریو ۶:



شکل فوق را در نرم افزار Cisco Packet Tracer پیاده سازی کنید و عملیات زیر را بر روی آن انجام دهید.

۱- ابتدا Portهای سوییچ ها را عضو Vlan کنید.

۲- ارتباط بین سوییچ و روتر را Trunk کنید.

۳- بر روی روتر ها IP و Gateway ؛ Set کنید.(مطابق شکل)

۴- Telnetرا بر روی روترها فعال کنید.

۵- تمامی شرایط امنیتی که قبلا گفته شده را بر روی تمامی Device ها برقرار کنید.

۶- EIGRP را بر روی تمامی روترها فعال کنید.

۷- DHCP را فعال کنید طوری که تمام PC ها و سرور ها (DHCP, DNS, Site) از DHCP ؛ IP بگیرند.

۸- DNS را فعال کنید طوری که تمامی PC ها سایت Cisco.com را ببینند.

۹- Telnet را بر روی روتر ها فعال کرده و از بیرون به آن وصل شوید.

۱۰- Ping کنید. تمای PC های شبکه باید Ping هم را داشته باشند در غیر اینصورت مراحل فوق را به دقت بررسی کنید.