|  |  |  |
| --- | --- | --- |
|  | دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران) | F:\Arm\AKUT.svg.png |

دستور کار آزمایشگاه شبکه‌های کامپیوتری

مسئول آزمایشگاه:

دکتر مسعود صبایی

پاییز 97



**فهرست مطالب**

[فصل 1: مقدمه 1](#_Toc525336870)

[1- آشنایی با تجهیزات شبکه و کابل‌کشی 2](#_Toc525336871)

[1-1- هدف آزمایش 2](#_Toc525336872)

[1-2- مطالب مقدماتی 2](#_Toc525336873)

[1-2-1- تجهیزات شبکه 2](#_Toc525336874)

[1-2-2- کابل‌کشی 12](#_Toc525336875)

[1-3- قطعات و ابزارهای موردنیاز 17](#_Toc525336876)

[1-4- شرح آزمایش 18](#_Toc525336877)

[2- ابزارهای مدیریت شبکه‌های کامپیوتری 21](#_Toc525336878)

[2-1- هدف آزمایش 21](#_Toc525336879)

[2-2- شرح آزمایش 21](#_Toc525336880)

[2-2-1- مشاهده تنظیمات آدرس IP واسط‌های شبکه 21](#_Toc525336881)

[2-2-2- استفاده از برنامه‌های خط فرمان 22](#_Toc525336882)

[2-2-3- ارزیابی ارتباط با سیستم‌های دیگر با استفاده از ابزارهای Ping و Tracert 23](#_Toc525336883)

[2-2-4- استفاده از ابزار Ping Plotter 25](#_Toc525336884)

[3- آشنایی با نرم‌افزار Wireshark 28](#_Toc525336885)

[3-1- هدف آزمایش 28](#_Toc525336886)

[3-2- مطالب مقدماتی 28](#_Toc525336887)

[3-3- قطعات و ابزارهای موردنیاز 31](#_Toc525336888)

[3-4- شرح آزمایش 31](#_Toc525336889)

[3-4-1- لایه‌بندی پروتکل‌ها 31](#_Toc525336890)

[3-4-2- کار با فیلتر کننده بسته‌ها 32](#_Toc525336891)

[فصل 2: لایه کاربرد 36](#_Toc525336892)

[1- راه‌اندازی سرویس‌های Web و FTP 37](#_Toc525336893)

[1-1- هدف آزمایش 37](#_Toc525336894)

[1-2- قطعات و ابزارهای موردنیاز 37](#_Toc525336895)

[1-3- شرح آزمایش 37](#_Toc525336896)

[1-3-1- تنظیمات سرور Web 38](#_Toc525336897)

[1-3-2- تنظیمات سرور FTP 44](#_Toc525336898)

[1-3-3- پروتکل HTTP 48](#_Toc525336899)

[1-3-4- پروتکل FTP 48](#_Toc525336900)

[2- کار با کاربردهای Web، DNS، سوکت و پویش سرویس‌ها 50](#_Toc525336901)

[2-1- هدف آزمایش 50](#_Toc525336902)

[2-2- فعالیت‌های قبل از آزمایش 50](#_Toc525336903)

[2-3- قطعات و ابزارهای موردنیاز 50](#_Toc525336904)

[2-4- شرح آزمایش 50](#_Toc525336905)

[2-4-1- کارکرد DNS 50](#_Toc525336906)

[2-4-2- مشاهده و تخصیص پورت‌های لایه انتقال با استفاده از ابزار Netstat 52](#_Toc525336907)

[2-4-3- کارکرد Web 53](#_Toc525336908)

[2-4-4- پویش سرویس‌ها 54](#_Toc525336909)

[فصل 3: لایه انتقال 56](#_Toc525336910)

[1- تحلیل TCP با استفاده از Wireshark 57](#_Toc525336911)

[1-1- هدف آزمایش 57](#_Toc525336912)

[1-2- فعالیت‌های قبل از آزمایش 57](#_Toc525336913)

[1-3- شرح آزمایش 57](#_Toc525336914)

[فصل 4: لایه شبکه 64](#_Toc525336915)

[1- آشنایی با شبیه‌ساز Boson Netsim 65](#_Toc525336916)

[1-1- هدف آزمایش 65](#_Toc525336917)

[1-2- مطالب مقدماتی 65](#_Toc525336918)

[1-2-1- انواع حافظه در تجهیزات سیسکو 67](#_Toc525336919)

[1-2-2- اتصال از طریق کابل سریال 69](#_Toc525336920)

[1-2-3- پروتکل CDP 70](#_Toc525336921)

[1-3- قطعات و ابزارهای موردنیاز 70](#_Toc525336922)

[1-4- شرح آزمایش 70](#_Toc525336923)

[1-4-1- تنظیمات مقدماتی 70](#_Toc525336924)

[1-4-2- اختصاص آدرس IP به واسط‌های شبکه 74](#_Toc525336925)

[1-4-3- اتصال به مسیریاب از طریق Telnet 77](#_Toc525336926)

[1-4-4- تنظیمات پروتکل CDP 77](#_Toc525336927)

[2- آشنایی با مکانیسم NAT و پروتکل DHCP 79](#_Toc525336928)

[2-1- هدف آزمایش 79](#_Toc525336929)

[2-2- مطالب مقدماتی 79](#_Toc525336930)

[2-3- شرح آزمایش 82](#_Toc525336931)

[2-3-1- مکانیسم NAT 82](#_Toc525336932)

[2-3-2- پروتکل DHCP 85](#_Toc525336933)

[3- آشنایی با شبیه‌ساز GNS3 88](#_Toc525336934)

[3-1- هدف آزمایش 88](#_Toc525336935)

[3-2- مطالب مقدماتی 88](#_Toc525336936)

[3-2-1- معرفی GNS3 88](#_Toc525336937)

[3-2-2- مسیریابی 97](#_Toc525336938)

[3-3- قطعات و ابزارهای موردنیاز 99](#_Toc525336939)

[3-4- فعالیت‌های قبل از آزمایش 99](#_Toc525336940)

[3-5- شرح آزمایش 100](#_Toc525336941)

[3-5-1- مسیریابی ایستا 100](#_Toc525336942)

[3-5-2- مسیریابی RIPv2 101](#_Toc525336943)

[4- آشنایی با پروتکل مسیریابی OSPF 104](#_Toc525336944)

[4-1- هدف آزمایش 104](#_Toc525336945)

[4-2- مطالب مقدماتی 104](#_Toc525336946)

[4-3- فعالیت‌های قبل از آزمایش 107](#_Toc525336947)

[4-4- قطعات و ابزارهای موردنیاز 107](#_Toc525336948)

[4-5- شرح آزمایش 108](#_Toc525336949)

[4-5-1- دستور کار اول 108](#_Toc525336950)

[4-5-2- دستور کار دوم 110](#_Toc525336951)

[5- کار با شبیه‌سازی GNS3 115](#_Toc525336952)

[5-1- هدف آزمایش 115](#_Toc525336953)

[5-2- فعالیت‌های قبل از آزمایش 115](#_Toc525336954)

[5-3- قطعات و ابزارهای موردنیاز 115](#_Toc525336955)

[5-4- شرح آزمایش 115](#_Toc525336956)

1. مقدمه
   1. آشنایی با تجهیزات شبکه و کابل‌کشی
      1. هدف آزمایش

هدف از انجام این آزمایش آشنایی دانشجویان با روش­های استاندارد کابل­کشی و شبکه­بندی است.

* + 1. مطالب مقدماتی

یک کابل ارتباطی، صدا، داده، ویدیو، سیگنال‏های هشدار و ... را در طول شبکه حمل می‏کند. با اطمینان می‏توان گفت که نیازمندی به پهنای باند، با توجه به گسترش روزافزون کاربردهای مختلف، مدام در حال افزایش است. دنیای فناوری اطلاعات در یک دهه‏ی گذشته، اهمیت کابل‏کشی ساختاریافته و قابل‌اطمینان را به‌خوبی دریافته است. اهمیت این موضوع از یک طرف و رشد انفجاری تقاضا برای پهنای باند بیشتر از طرف دیگر باعث شده است تا تعداد افرادی که نیازمند فراگیری مفاهیم پایه‏ی کابل‏کشی هستند به شدت افزایش یابد.

هدف از انجام این آزمایش آشنایی با طراحی یک سیستم کابل­کشی ساختاریافته و اتصال گره‏ها و ایجاد یک شبکه‏ی ارتباطی است. مطالبی که در ادامه مطرح خواهند شد عبارت‏اند از:

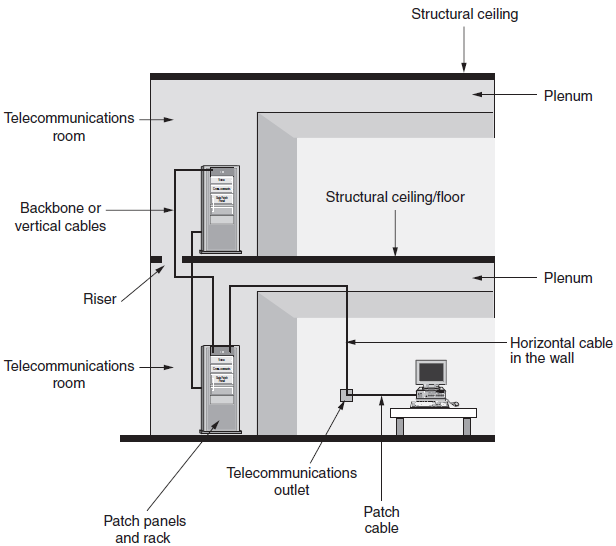
* معرفی تجهیزات به کار رفته در یک شبکه‏ی ارتباطی
* انواع مختلف کابل‏های شبکه و تفاوت‏های آن‏ها
* قوانین و نکات مهم برای طراحی یک سیستم کابل‏کشی
  + - 1. تجهیزات شبکه
         1. کابل‌های افقی

بر اساس استاندارد ANSI/TIA-568-C.2 برای پیاده‏سازی کابل‏های افقی معمولاً از چهار زوج سیم‏ به هم تابیده‏ی بدون محافظ[[1]](#footnote-1) (UTP) 100 اهمی که از جنس مس هستند استفاده می‏شود. طبق این استاندارد امکان پیاده‏سازی کابل‏های افقی با استفاده از فیبر نوری چندحالته‏ی 125/5.62 میکرون یا 125/50 میکرون‏ نیز وجود دارد. برای انتقال داده و صوت بر بستر شبکه، استفاده از کابل‏های هم‏محور[[2]](#footnote-2) (Coaxial) به‌عنوان کابل افقی مناسب نیست.

* + - * 1. کابل‌های Backbone

برای پیاده‏سازی کابل‏های Backbone می‏توان از زوج سیم به هم تابیده‏ی محافظ دار[[3]](#footnote-3) (STP)، UTP یا Screened Twisted Pair (ScTP) 100 اهمی استفاده کرد. از فیبر نوری چندحالته‏ی 125/5.62 میکرون یا 125/50 میکرون‏ و یا فیبر نوری تک‏حالته‏ی 125/3.8 میکرون نیز می‏توان استفاده کرد. برای ارتباطات Backbone استفاده از کابل‏های STP و هم‏محور 150 اهمی مجاز نیست. به دلیل محدودیت مسافت در کابل‏های مسی (STP, UTP, ScTP)، استفاده از فیبر نوری به‌عنوان رسانه‏ی انتقال در Backbone ترجیح داده می‏شود.

‏شکل (1-1) مؤلفه‏های معمول یک محیط کابل‏کشی ساختاریافته را نشان می‏دهد.

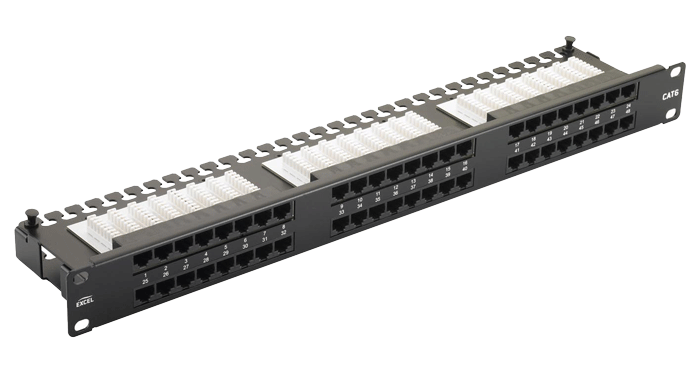


مولفه‌های یک محیط کابل‌کشی ساختاریافته

در این شکل، Plenum به فضای بین سقف کاذب و سقف اصلی اتاق اطلاق می‌شود که برای تهویه هوا و عبور کابل‌ها استفاده می‌شود. همچنین Riser عموما یک فضای ایجاد شده بین طبقات مختلف است که می‌توان کابل‌ها را از یک طبقه به طبقه دیگر انتقال داد.

* + - * 1. Patch Panel

وظیفه اصلی Patch Panel این است که بین نقاط انتهایی کابل­های شبکه و تجهیزات شبکه­ای (هاب، سوئیچ، مسیریاب، ...) قرار گرفته و مانع اتصال مستقیم کابل­های شبکه به تجهیزات ­شود. مهم­ترین مزیت استفاده از Patch Panel عدم آسیب به کابل­های اصلی شبکه و نظم بخشیدن به کابل­کشی است که باعث ردیابی و رفع سریع اشکالات می­شود. کابل­های اصلی شبکه به پشت Patch panel متصل می­شوند و از طریق سوکت Patch Panel و Patch Cord ها به سوییچ، مسیریاب و سایر تجهیزات متصل می‏شوند. Patch Panel در ابعاد مختلف و تعداد پورت متفاوت به بازار عرضه می‌شوند. لازم به ذکر است که Patch Panel باید متناسب با کابل به­کار رفته در سیستم انتخاب شود، زیرا در صورت عدم تطابق، سیگنال حامل داده را تضعیف خواهد کرد. ‏شکل (1-2) Patch Panel با 48 پورت را نشان می‏دهد.



یک Patch Panel

* + - * 1. Patch Cord

Patch Cord کابل‌هایی هستند که برای برقراری ارتباط بین نقاط انتهایی کابل‏های افقی و تجهیزات شبکه (مانند سوییچ و هاب) در Patch Panel و یا برقراری ارتباط بین دستگاه‏های انتهایی (مانند رایانه و پرینتر) و پریز ارتباطی[[4]](#footnote-4) استفاده می‏شود. Patch Cord ها آن بخش از کابل‏کشی شبکه‏اند که به راحتی قابل رویت هستند. به دلیل همین قابل رویت و در دسترس بودن، Patch Cord ها لینک‏های ضعیف یک سیستم کابل‏کشی محسوب می‏شوند. Patch Cord ها انعطاف‏پذیر ساخته می‏شوند تا در مقابل پیچ‏خوردگی‏ها و قطع و وصل‏های مداوم به دستگاه‏ها و تجهیزات شبکه مقاوم باشند. با اینکه Patch Cord ها در شرایط بسیار خاص و دقیق ساخته می‏شوند، اما تضمین کارایی آن‏ها در یک شبکه‏ی ارتباطی دشوار است.

* + - * 1. مجرای سیم

مجرای سیم[[5]](#footnote-5) یک لوله است که می‏تواند فلزی یا غیرفلزی، انعطاف‏پذیر یا سفت و سخت باشد. از مزایای استفاده از مجرای سیم این است که ممکن است چنین مجرایی از قبل در محل کابل‏کشی موجود باشد (برای اتصالات و کابل‏کشی‏های قبلی)، درنتیجه عبور کابل‏های جدید از آن چندان زمان‏بر نخواهد بود؛ اما از طرفی فضای داخلی مجرای سیم محدود است و ممکن است کافی نباشد. توصیه می‏شود که مجرای سیم طبق نیازمندی‏های فعلی تنها بین %40 تا %60 اشغال شود تا امکان افزایش ظرفیت شبکه و کابل‏کشی‏های بیشتر در آینده وجود داشته باشد.

طبق استاندارد TIA-569-C، از مجرای سیم می‏توان برای هدایت هر دو نوع کابل در شبکه (افقی و Backbone) استفاده کرد. ‏شکل (1-3) و ‏شکل (1-4) نمونه‏هایی از مجرای سیم هستند.



نمونه‌ای از مجرای سیم



نمونه‌ای دیگر از مجرای سیم

* + - * 1. سینی کابل

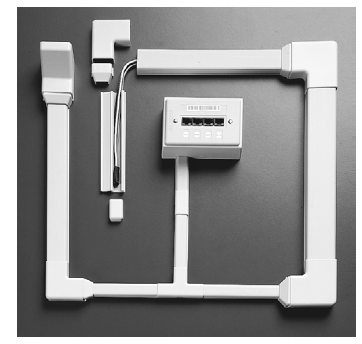
به‌عنوان جایگزینی برای مجرای سیم، می‏توان از سینی کابل[[6]](#footnote-6) برای هدایت سیم‏ها استفاده کرد. سینی‏های کابل معمولاً قفسه‏های سیمی هستند که برای تحمل وزن تعداد زیادی کابل طراحی شده‏اند. کابل‏ها به سادگی روی این سینی‏ها قرار می‏گیرند و به راحتی قابل دسترس هستند. همین باعث ساده‏تر کردن کار عیب‏یابی می‏شود. طبق استاندارد TIA-569-C سینی‏های کابل قابل استفاده برای هدایت هر دو نوع کابل افقی و Backbone هستند. ‏شکل (1-5) یک نمونه سینی کابل به همراه کابل‌های داخلش را نشان می‌دهد.



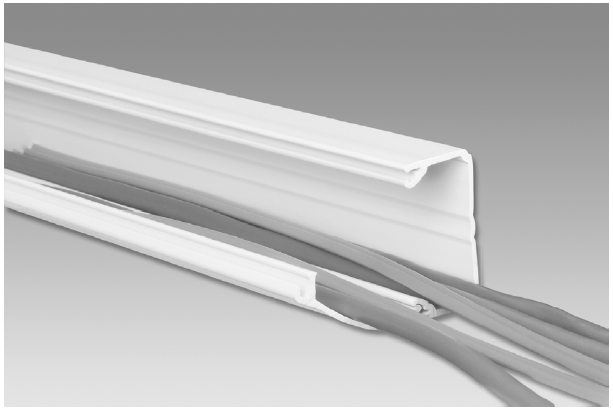
نمونه‌ای از سینی کابل

* + - * 1. داکت

داکت نوع خاصی از مجرای سیم است که برای کابل‏کشی افقی روی سطوح استفاده می‏شود. داکت‏ها معمولاً به‏صورت ماژولار ساخته می‏شوند. از داکت برای کابل‏کشی روی سطوح دیوارهایی که امکان هدایت کابل از داخل آن‏ها وجود ندارد استفاده می‏شود. ‏شکل (1-6) و ‏شکل (1-7) نشان د‏هنده‏ی سیستم داکت‏کشی است.



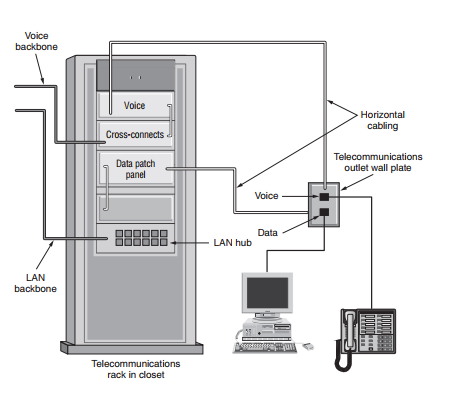
یک سیستم ماژولار داکت کشی



داکت عبوری از یک سطح با تعدادی کابل

* + - * 1. پریز ارتباطی

پریز ارتباطی ارتباط بین تجهیزات انتهایی و رک‌ها را تسهیل می‌کند. طراح شبکه، پریزها را به رک‌ها متصل می‌کند و تجهیزات انتهایی صرفا به پریز متصل می‌شوند. یک نمونه از پریزهای ارتباطی در ‏شکل (1-8) و ‏شکل (1-9) آورده شده است.



ارتباط تجهیز انتهایی به رک از طریق پریز



یک نمونه پریز ارتباطی

* + - * 1. رک

رك[[7]](#footnote-7)ها به شما کمک می‏کنند تا زیرساخت کابل‏کشی خود را نظم دهید. ارتفاع آن معمولا می‏تواند بین 39 اینچ تا 84 اینچ و پهنای آن 19 تا 23 اینچ باشد. در 60 سال اخیر، رک‏ها با پهنای 19 اینچ بسیار مورد استفاده قرار گرفته‏اند. این رک‏ها، رک 19 اینچی یا رکEIA[[8]](#footnote-8) نامیده می‏شوند.

به طور کلی سه نوع رک وجود دارد:

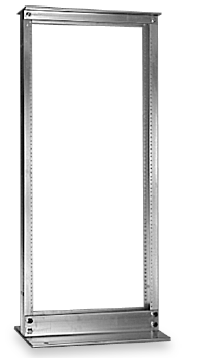
* رک‏های دیواری[[9]](#footnote-9)
* رک‏های ایستاده[[10]](#footnote-10)
* کابینت‏های کاملاً تجهیز شده[[11]](#footnote-11)

برای شبکه‏بندی‏های کوچک و مکان‏هایی با محدودیت فضایی، رک‏های دیواری بهترین انتخاب هستند. قبل از نصب رک‏های دیواری، باید از بودن فضای کافی برای باز کردن پنل جلویی رک اطمینان حاصل کرد. ‏شکل (1-10) یک رک دیواری را نشان می‏دهد.

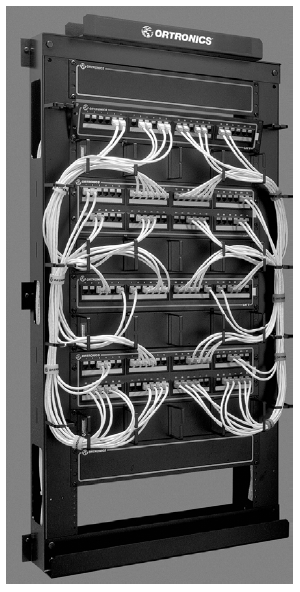


نمونه‌ای از رک دیواری

رک‏های ایستاده (یا رک‏های 19 اینچی یا EIA) متداول‏ترین نوع رک‏های مورداستفاده هستند. این رک‏ها بر اساس استاندارد EIA/ECA-310-E (مربوط به سال 2005) طراحی و ساخته شده‏اند. این رک‏ها بین 39 اینچ تا 84 اینچ ارتفاع دارند. طراحی رک‏های ایستاده به گونه‏ای است که امکان کار کردن با قسمت جلویی و پشتی تجهیزات نصب‌شده وجود دارد. هنگام نصب رک ایستاده، باید بین دیوار و رک، فضای کافی برای جاسازی تجهیزات وجود داشته باشد (عمق تجهیزات معمولاً بین 6 اینچ تا 18 اینچ است). همچنین باید فضای کافی برای فردی که با تجهیزات کار خواهد کرد، در پشت رک در نظر گرفته شود (حداقل 12 اینچ تا 18 اینچ). همچنین باید از استحکام رک روی زمین برای جلوگیری از سقوط آن اطمینان حاصل کرد. در این رک‏ها می‏توان از ابزار مدیریت کابل[[12]](#footnote-12)، خصوصاً زمانی که تعداد کابل‏ها زیاد است استفاده کرد. ‏شکل (1-11) و ‏شکل (1-12) نمونه‏هایی از رک‏های اسکلتی (ایستاده) را نشان می‏دهند.



یک فریم اسکلتی 19 اینچی (رک ایستاده)



رک ایستاده The Ortronics Mighty Mo II با مدیریت کابل، نصب‌شده روی دیوار

تجهیزات داخل رک محدود به Patch Panel و تجهیزات ارتباطی (سوییچ و مسیریاب) نمی‏شوند. سرورها ازجمله تجهیزات رایج نصب‌شده در رک هستند. قفسه‏های ابزار، قفسه‏ی مانیتور و قفسه‏ی کیبورد هم ازجمله سایر تجهیزات قابل نصب در رک هستند. ‏شکل (1-13) نمونه‏ای از این قفسه‌ها است.



نمونه‌هایی از قفسه برای رک‏های 19 اینچی

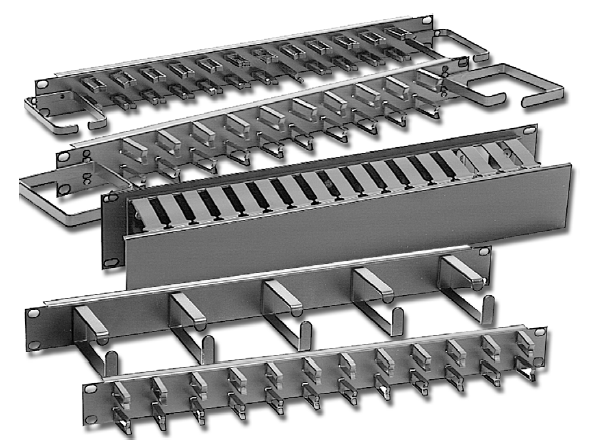
کابینت‏های کاملاً تجهیز شده، گران‌ترین گزینه برای انتخاب است. این کابینت‏ها امکان قفل درهای کابینت و فراهم کردن امنیت تجهیزات داخلی را دارند. این رک‏ها می‏توانند بسیار ساده و یا بسیار تجهیز شده (مثل سیستم خنک‏کننده‏ی داخلی و سیستم حفاظت از تداخل الکترومغناطیسی) باشند. ‏شکل (1-14) یک کابینت را نشان می‏دهد.



یک کابینت کاملاً تجهیز شده

* + - * 1. لوازم جانبی مدیریت کابل

این لوازم به مدیریت و نظم‏بخشی به کابل‏های ارتباطی، خصوصاً در رک‏هایی که فاقد ابزار مدیریت سیم هستند، کمک می‏کنند. ازجمله‌ی این ابزار می‏توان به آویزهای کابل[[13]](#footnote-13) در قسمت جلو و یا پشت تجهیزات نصب‌شده در رک اشاره کرد. ‏شکل (1-15) ابزار مدیریت کابل را نشان می‏دهد.



ابزار مدیریت کابل محصول MilesTek

* + - 1. کابل‌کشی
         1. قوانین

در کابل‌کشی قوانینی وجود دارد که برخی از آن‌ها را مرور می‌کنیم:

* برای کابل‌کشی افقی حداکثر طول کابل 90 متر باشد به علاوه اینکه طول Patch Cord های مورد استفاده در داخل قفسه‌های مخابراتی[[14]](#footnote-14) نباید بیشتر از 5 متر شود.
* کابل‌های حامل داده را هرگز نباید به هم پیوند زد، اگر کابلی در نقطه‌ای دچار مشکل شد با کابل جدید جایگزین شود. اگر سیم‌های کابل آسیب دیده‌اند کابل را تعویض کنید.
* کابل‌ها را مستقیما روی سقف قرار ندهید، از سینی کابل، قلاب J[[15]](#footnote-15)، نردبان افقی[[16]](#footnote-16) و یا روش‌های دیگر استفاده کنید.
* زمانی که در سیستم کابل‌کشی از داده و صدا پشتیبانی می‌شود برای خطوط صوتی از Patch Panel های مجزا استفاده کنید.
* تاباندن محکم کابل باعث آسیب کابل و سیم‌های آن می‌شود همچنین برای جلوگیری از آسیب دیدن کابل‌ها، آن‌ها را در مسیر منابع تولید گرما مثل لوله‌های آب گرم و شوفاژ قرار ندهید.
* کابل‌های حامل داده نباید با کابل برق در یک مجرای سیم قرار گیرند. اگر مجبور شوید که کابل‌های داده و برق یکدیگر را قطع کنند این کار باید با زاویه درستی انجام شود.
  + - * 1. استاندارد کابل‌کشی ANSI/TIA-568-C

در اواسط دهه 80 میلادی کمبود یک استاندارد مربوط به سیم‌کشی مخابراتی توسط سازندگان تجهیزات، پیمانکاران، مصرف‌کنندگان و تولیدکنندگان احساس شد. تا قبل از آن تمامی سیم‌کشی‌های ارتباطی به صورت شخصی و غالبا تک منظوره انجام می‌شده است. انجمن صنعت ارتباطات کامپیوتر (CCIA) از اتحادیه صنعت الکترونیک[[17]](#footnote-17) (EIA) درخواست توسعه یک استاندارد کابل‌کشی و ساخت‌یافته را کرد که در سال 1991، EIA و انجمن صنعت مخابرات[[18]](#footnote-18) (TIA) اولین نسخه‌ی استاندارد کابل‌کشی مخابراتی ساختمان‌های تجاری را تحت عنوان ANSI/TIA/EIA-568 به چاپ رساند. این استاندارد چندین بار بازنگری و به‌روزرسانی شده است. در سال 1995 استاندارد ANSI/TIA/EIA-568-A چاپ شد و در سال‌های بعد مواردی به این نسخه اضافه شد به عنوان مثال استاندارد TIA/EIA-568-A-5 نیازمندی‌های مربوط به کابل UTP Category 5e را قبل از اینکه نسخه کامل بعدی استاندارد بتواند چاپ شود را پوشش می‌داد. در سال 2001 یک بروز رسانی از استاندارد تحت عنوان ANSI/TIA/EIA-568-B منتشر شد. سرانجام در سال 2009 نسخه قبلی به‌روزرسانی شد و تمام اصلاحات آن به یک استاندارد جدید با نام ANSI/TIA-568-C به وجود آمد. در حال حاضر هم TIA به‌روزرسانی این نسخه و چاپ ANSI/TIA-568-D را مدنظر دارد.

استاندارد ANSI/TIA-568-C شامل دو الگوی سیم‌کشی برای استفاده از کابل‌های UTP و سوکت[[19]](#footnote-19) های (RJ-45 و RJ-11) است. این استاندارد ترتیب سیم‌های کابل UTP را برای اتصال به پین[[20]](#footnote-20) های سوکت بیان می‌کند که با T568A و T568B شناخته می‌شوند. در ‏جدول (1-1) جزئیات این دو استاندارد بیان شده است.

استانداردهای T568A و T568B

|  |  |  |  |
| --- | --- | --- | --- |
| T568A | | T568B | |
| رنگ | شماره پین | رنگ | شماره پین |
| سفيد-سبز | 1 | سفید-نارنجی | 1 |
| سبز | 2 | نارنجی | 2 |
| سفيد-نارنجي | 3 | سفید-سبز | 3 |
| آبي | 4 | آبی | 4 |
| سفيد-آبي | 5 | سفید-آبی | 5 |
| نارنجي | 6 | سبز | 6 |
| سفيد-قهوه‌اي | 7 | سفید-قهوه‌ای | 7 |
| قهوه‌اي | 8 | قهوه‌ای | 8 |

دو الگوی سیم‌کشی برای کابل‌های UTP وجود دارد که طبق یکی از این قراردادها باید سیم‌کشی را انجام دهیم، T568A و T568B. این دو الگو تقریباً یکسان هستند به‌جز جفت 2 و 3 که جابه‌جا می‌شوند. T568B بیشتر در موارد تجاری استفاده می‌شود اما طبق ANSI/TIA-570-B توصیه می‌شود از پیکربندی T568A برای موارد مسکونی استفاده شود. پیکربندی T568A با طرح‌های سیم‌کشی که معمولاً برای سیستم‌های صدا استفاده می‌کردند مانند USOC سازگار است. ‏جدول (1-2) برخی از کاربردهای رایج و پین‌های استفاده‌شده در آن‌ها را نشان می‌دهد.

‏شکل (1-16) نحوه اتصال سیم‌های کابل UTP را طبق استانداردهای T568A و T568B بر روی پین‌های سوکت نشان می‌دهد. ‏شکل (1-17) به‌صورت واضح سیم‌های رنگی متناسب با هر پین را نمایش داده است.

* + - * 1. تفاوت سوکت‌های RJ-45 و RJ-11

دودسته اصلی از سوکت[[21]](#footnote-21) ها (نام دیگر آن‌ها پلاگ هست) برای اتصال به کابل‌های زوج سیم به هم تابیده استفاده می‌شود: RJ-45 و RJ-11.

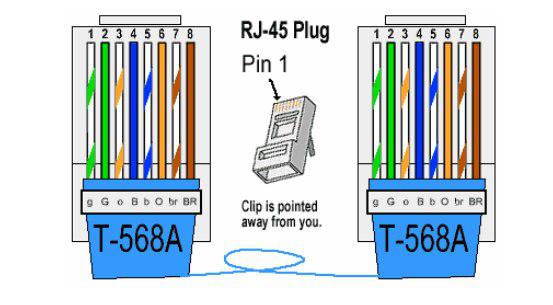
این دو سوکت اساساً مشابه هستند به‌جز آن‌که RJ-45 سیم‌های بیشتری را داخل خودش جا می‌دهد، علاوه بر این اندکی از RJ-11 نیز بزرگ‌تر است. سوکت‌های RJ-11 و RJ-45 در ‏شکل (1-18) نشان داده شده‌‌اند. سوکت‌های RJ-11 شش position دارند اما به‌جای شش سطح تماس فلزی با دو سطح تماس فلزی پیکربندی‌شده‌اند دلیل این کار صرفه‌جویی در هزینه برای کاربردهای تلفنی است که تنها نیاز داریم دو سیم تماس داشته باشند.

جفت کردن کابل‌های UTP متناسب با کاربردها

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| پین 7 و 8 | پین 4 و 5 | پین 3 و 6 | پین 1 و 2 | کاربرد |
| - | ارسال/دریافت | - | - | Analog voice |
| Power | دریافت | ارسال | Power | ISDN |
| - | - | دریافت | ارسال | 10Base-T (802.3) |
| - | دریافت | ارسال | - | Token Ring (802.5) |
| - | - | دریافت | ارسال | 100Base-TX (802.3u) |
| دوطرفه | دوطرفه | دریافت | ارسال | 100Base-T4 (802.3u) |
| دوطرفه | دوطرفه | دوطرفه | دوطرفه | 100Base-VG (802.12) |
| دریافت | Optional | Optional | ارسال | FDDI (TP-PMD) |
| دریافت | Optional | Optional | ارسال | ATM User Device |
| ارسال | Optional | Optional | دریافت | ATM Network Equipment |
| دوطرفه | دوطرفه | دوطرفه | دوطرفه | 1000Base-T (802.3ab) |
| دوطرفه | دوطرفه | دوطرفه | دوطرفه | 10GBase-T (802.3an) |

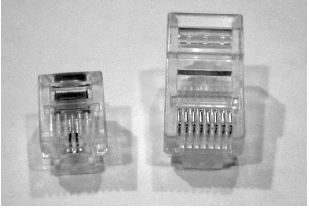


نحوه اختصاص سیم‌ها به پین‌های سوکت



سیم‌های رنگی متناسب با هر پین سوکت RJ-45

از RJ-11 به دلیل سادگی و اندازه کوچکی که دارند برای تلفن‌های خانگی و تجاری استفاده می‌شود اما از RJ-45 با توجه به تعداد سیم‌هایی که پشتیبانی می‌کند در کاربردهای LAN استفاده می‌شود. اخیراً توصیه می‌شود که برای کاربردهای تلفنی هم از RJ-45 استفاده شود چون قابلیت‌های RJ-11 را نیز پشتیبانی می‌کند.



به ترتیب از راست سوکت RJ-45 و RJ-11

نکته: دو سر انتهایی Patch Cord های مستقیم[[22]](#footnote-22) با استانداردهای مشابه سیم‌کشی می‌شوند به‌عبارت‌دیگر برای هر دو سر انتهایی یا از استاندارد T568-A یا T568-B استفاده می‌شود.Patch Cord مستقیم PC را به پریز ارتباطی و Patch Panel را به تجهیزات شبکه مانند هاب، سوئیچ و روتر متصل می‌کند. برای Patch Cord های متقاطع[[23]](#footnote-23) یکسر انتهایی با استاندارد T568-A و سر دیگر با استاندارد T568-B سیم‌کشی می‌شود. برای شبکه‌های Ethernet، Patch Cord های متقاطع مستقیماً PC ها را بدون واسطه هیچ تجهیز شبکه‌ای به هم متصل می‌کند. برای اتصال هاب‌ها، سوئیچ‌ها و روترها به یکدیگر، متناسب به نوع تجهیزات در طرفین یا یک کابل مستقیم یا یک کابل متقاطع موردنیاز است.

* + 1. قطعات و ابزارهای موردنیاز

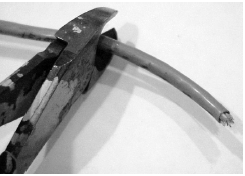
تجهیزات موردنیاز برای انجام این آزمایش به همراه عکس آن‌ها در ‏جدول (1-3) نشان داده شده است.

تجهیزات موردنیاز

|  |  |  |
| --- | --- | --- |
| نام تجهیز | مقدار موردنیاز | عکس |
| رشته كابل CAT5 | مقدار لازم |  |
| سوكت RJ-45 | برای هر کابل دو عدد |  |
| آچار Crimp یا آچار پرس | یک عدد |  |
| Tester شبكه | یک عدد |  |
| سیم‌چین | یک عدد |  |
| کابل لخت کن | یک عدد |  |

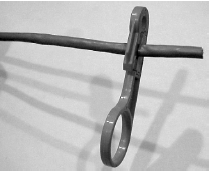
* + 1. شرح آزمایش

1. . با استفاده از سیم‌چین کابل را به‌اندازه دلخواه برش دهید، دقت کنید که کابل را باید 3 اینچ (7.62 سانتی‌متر) بیشتر از طول کابل پچ نهایی برش بزنید (‏شکل (1-19)).



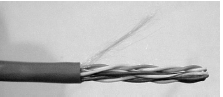
برش کابل

1. با استفاده از کابل لخت کن پوسته‌ی کابل را جدا می‌کنید به این صورت که کابل لخت کن را حدود 1.5 اینچ (3.81 سانتی‌متر) از انتهای کابل قرار دهید و کابل لخت کن را دو بار دور کابل بچرخانید (‏شکل (1-20)).



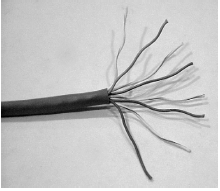
لخت کردن کابل

1. پوسته کابل را جدا کنید تا سیم‌های داخلی کابل مشخص شود، اگر jacket slitting cord که مانند نخ‌های سفید است، نمایان شد، آن‌ها را از سیم‌ها جدا کنید (‏شکل (1-21)).



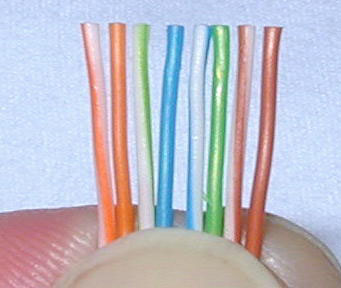
کابل لخت شده

1. تمامی سیم‌های داخلی را صاف کنید و آن‌ها را کاملاً از هم جدا کنید به صورتی که بتوان تمامی آن‌ها مانند ‏شکل (1-22) را مشاهده کرد.



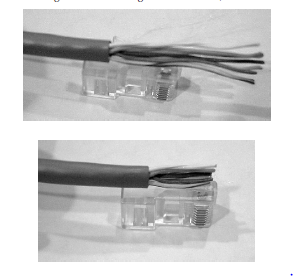
جداسازی سیم‌های داخلی

1. هرکدام از سیم‌ها را مطابق با یکی از استانداردهای گفته‌شده در ‏جدول (1-2) مانند ‏شکل (1-23) مرتب کنید.



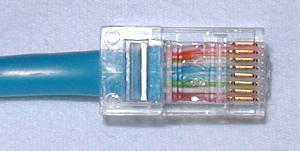
مرتب‌سازی رنگ‌ها بر اساس استاندارد T568B

1. سیم‌های داخلی را مرتب کنید به صورتی که انتهای همگی آن‌ها در یک خط قرار بگیرند، اطمینان حاصل کنید که مانند ‏شکل (1-24) پوسته‌ی کابل داخل سوکت RJ-45 قرار گیرد.



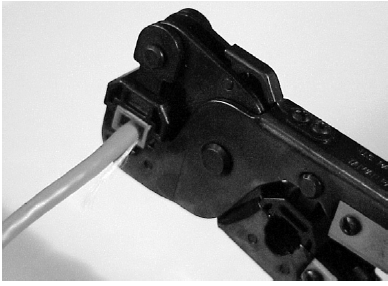
مرتب کردن سیم‌های داخلی

1. سیم‌ها را داخل سوکت کنید و دقت کنید که تمامی سیم‌ها با پین‌های سوکت در تماس باشند در غیر این صورت آن‌ها را بیرون بکشید، مرتب کنید و مجدداً امتحان کنید. به علت این‌که این مرحله آخرین گام قبل از پرس کردن با آچار Crimp هست، در انجام این مرحله دقت کنید (‏شکل (1-25)).



نحوه قرارگیری صحیح سیم‌های داخلی در سوکت

1. طبق ‏شکل (1-26) سوکت و کابل را داخل آچار Crimp قرار دهید، دسته آچار را محکم فشار دهید تا به انتها برسد و در حدود سه ثانیه با فشار نگه‌دارید.



پرس کردن سوکت

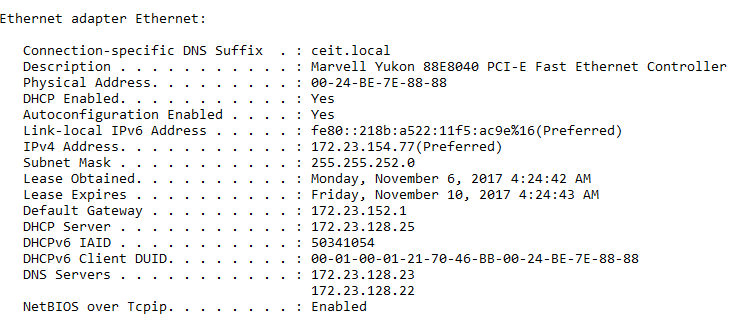
1. پس از آنکه پرس را انجام دادید، سوکت را از آچار Crimp جدا کنید. بررسی کنید تا همه سیم‌ها با پین‌های متناظر خود به‌درستی پرس شده‌اند. اگر سوکت به‌درستی پرس نشده باشد باید آن را برش دهید و تمامی مراحل را از ابتدا انجام شود.
   1. ابزارهای مدیریت شبکه‌های کامپیوتری
      1. هدف آزمایش

هدف از این آزمایش آشنایی با ابزارهای مدیریت شبکه‌های کامپیوتری و نحوه عیب‌یابی و رفع خطاهای شبکه است.

مطالبی که در این آزمایش پوشش داده می‌شود عبارت‌اند از:

* مشاهده تنظیمات آدرس IP واسط‌های شبکه
* استفاده از برنامه‌های خط فرمان شامل Ping، Tracert
* استفاده از ابزار Ping plotter
  + 1. شرح آزمایش
       1. مشاهده تنظیمات آدرس IP واسط‌های شبکه

با استفاده از دستور ipconfig /all اطلاعات مربوط به تنظیمات پروتکل IP واسط‌های سیستم شما لیست خواهند شد. این اطلاعات شامل آدرس IP سیستم، ماسک شبکه، آدرس دروازه[[24]](#footnote-24) شبکه، آدرس فیزیکی واسط‌ها و آدرس سرور DNS است و به تفکیک واسط‌ها نمایش داده خواهد شد. این دستور را می‌توانید در محیط CMD اجرا کنید. نمونه‌ای از خروجی این دستور در ‏شکل (1-27) نمایش داده ‌شده است.



خروجی دستور ipconfig /all

توضیحات بخش‌های مهم ‏شکل (1-27) در ‏جدول (1-4) بیان شده‌اند. بسیاری از مشکلات رایج در اتصال به شبکه ناشی از اختصاص نیافتن آدرس IP مناسب است. در این حالت در اغلب موارد در بخش IPv4 Address، آدرس‌هایی که با عبارت 169 شروع می‌شوند را مشاهده خواهید کرد. همچنین پاسخ‌گو نبودن سرورهای DNS از مشکلات رایج دیگر است. در این حالت می‌توانید سرورهای DNS را Ping کنید تا از دسترس بودن آن‌ها اطمینان حاصل کنید. درنهایت آدرس دروازه شبکه را نیز Ping کنید تا مطمئن شوید می‌توانید با آن ارتباط داشته باشید.

توضیحات بخش‌های مختلف خروجی دستور ipconfig /all

|  |  |
| --- | --- |
| بخش | توضیحات |
| Description | توضیحات مربوط به واسط شبکه |
| Physical Address | آدرس فیزیکی واسط شبکه |
| DHCP | آیا آدرس IP به واسط شبکه از طریق پروتکل DHCP اختصاص می‌یابد. اگر جواب Yes است باید آدرس DHCP Server مشخص شده باشد. |
| IPv4 Address | آدرس IP نسخه 4 واسط شبکه |
| IPv6 Address | آدرس IP نسخه 6 واسط شبکه |
| DNS Server | آدرس مربوط به سرورهای DNS |
| Default Gateway | آدرس IP مربوط به دروازه شبکه |
| Subnet Mask | به همراه آدرس IP، آدرس شبکه‌ای که واسط شبکه شما در آن قرار دارد را مشخص می‌کند. |

با استفاده از دستور ipconfig /release آدرس IP مربوط به واسط مشخص‌شده، رها خواهد شد. پس از این دستور باید ipconfig/renew را نیز اجرا کنید تا آدرس‌های جدید به واسط‌های شما اختصاص پیدا کند.

* + - 1. استفاده از برنامه‌های خط فرمان

برنامه‌های خط فرمان مانند Ping، Netstat و Tracert از برنامه‌های موجود در سیستم‌عامل خانواده ویندوز هستند که امکانات مدیریتی و اشکال‌زدایی شبکه را به کاربر می‌دهند. برای دیدن گزینه‌های هر دستور می‌توانید از /? بعد از دستور استفاده کنید. به عنوان مثال با استفاده از دستور ping/? خروجی ‏شکل (1-28) در خط فرمان چاپ می‌شود.

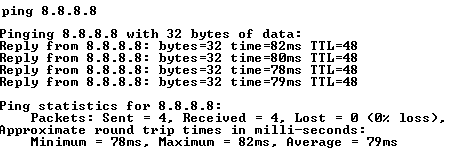
به نظر شما سوییچ –l چیست و چگونه عمل می‌کند؟



خروجی دستور ping/?

* + - 1. ارزیابی ارتباط با سیستم‌های دیگر با استفاده از ابزارهای Ping و Tracert

با استفاده از ابزار Ping می‌توانید ارتباط با سیستم‌های دیگر را ارزیابی کنید. در جلوی دستور Ping باید آدرس IP سیستمی که می‌خواهید ارتباط با آن را آزمایش کنید قرار دهید. به عنوان مثال، دستور Ping 8.8.8.8 یکی از آدرس‌های IP متعلق به شرکت Google را Ping می‌کند. خروجی این دستور در ‏شکل (1-29) نمایش داده ‌شده است. با استفاده از این دستور می‌توانید وضعیت اینترنت خود را نیز بسنجید. همان‌گونه که مشاهده می‌کنید میانگین زمان رفت و برگشت بسته‌ها، 79 میلی‌ثانیه است که نسبتا مناسب است. این تاخیر معمولا باید زیر 1 ثانیه باشد. همچنین تمام بسته‌ها باید دریافت شده باشند. در ‏شکل (1-29) مشاهده می‌کنید که هر چهار بسته ارسالی، دریافت شده‌اند. دریافت نکردن هر یک از بسته‌ها می‌تواند نشان از وجود مشکل در شبکه باشد.



خروجی دستور ping 8.8.8.8

با استفاده از CMD، دستورات زیر را اجرا کنید:

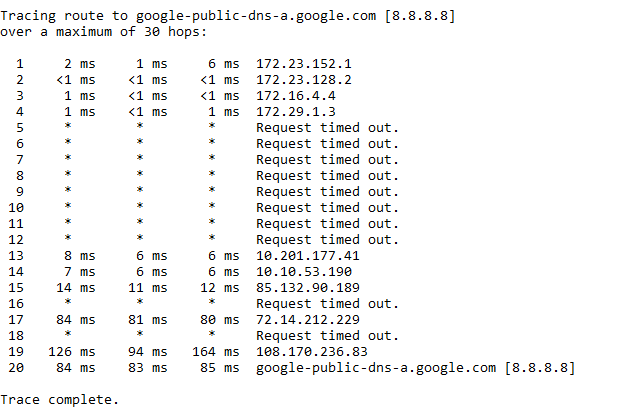
ping aut.ac.ir

ping google.com

چه تفاوتی بین میانگین زمان رفت و برگشت برای این دو آدرس وجود دارد؟ به نظر شما این اختلاف از کجا ناشی می‌شود؟ دستور ping dolat.ir را نیز اجرا کنید و میانگین زمان رفت و برگشت را مقایسه کنید.

همان‌گونه که مشاهده کردید Ping بعد از ارسال و دریافت چهار پیغام قطع می‌شود. دستوری پیدا کنید که ارسال و دریافت پیغام را بدون توقف ادامه دهد.

اصول عملکرد ابزار Tracert مشابه ابزار Ping است. با استفاده از ابزار Tracert می‌توانید مسیر عبور بسته‌های خود تا رسیدن به مقصد را مشاهده کنید؛ بنابراین اگر در جایی در این مسیر، شبکه قطع باشد می‌توانید آن را شناسایی کنید. خروجی این دستور در ‏شکل (1-30) داده شده است.



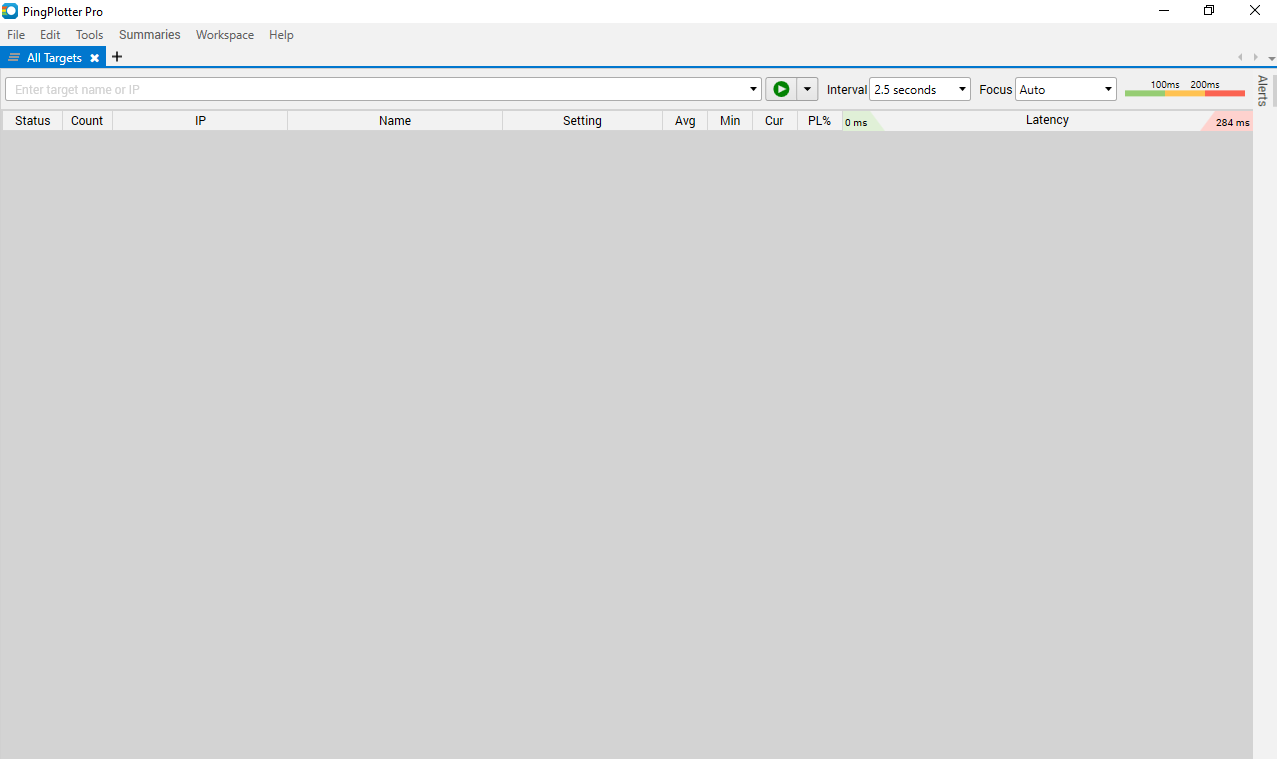
خروجی دستور tracert

همان‌گونه که در این شکل مشاهده می‌شود، ستون اول از سمت چپ، بیانگر گام‌های عبور بسته است. هر گام بیانگر یک مسیریاب است. سه ستون بعدی بیانگر زمانی است که بین ارسال و دریافت بسته طول کشیده است. درنهایت ستون اول از سمت راست بیانگر آدرس IP مسیریاب در آن گام است.

دستور tracert google.com، tracert facebook.com و tracert aut.ac.ir را اجرا کنید. آخرین آدرس IP که در خروجی هر سه دستور مشاهده می‌کنید و ارتباط آن‌ها با ورودی دستور tracert را مشخص کنید. به نظر شما چرا در خروجی tracert facebook.com در بعضی از گام‌ها به‌جای آدرس IP مسیریاب‌ها، Request timeout قرار گرفته است؟ آخرین آدرس IP در خروجی مربوط به facebook چه ارتباطی با facebook دارد.

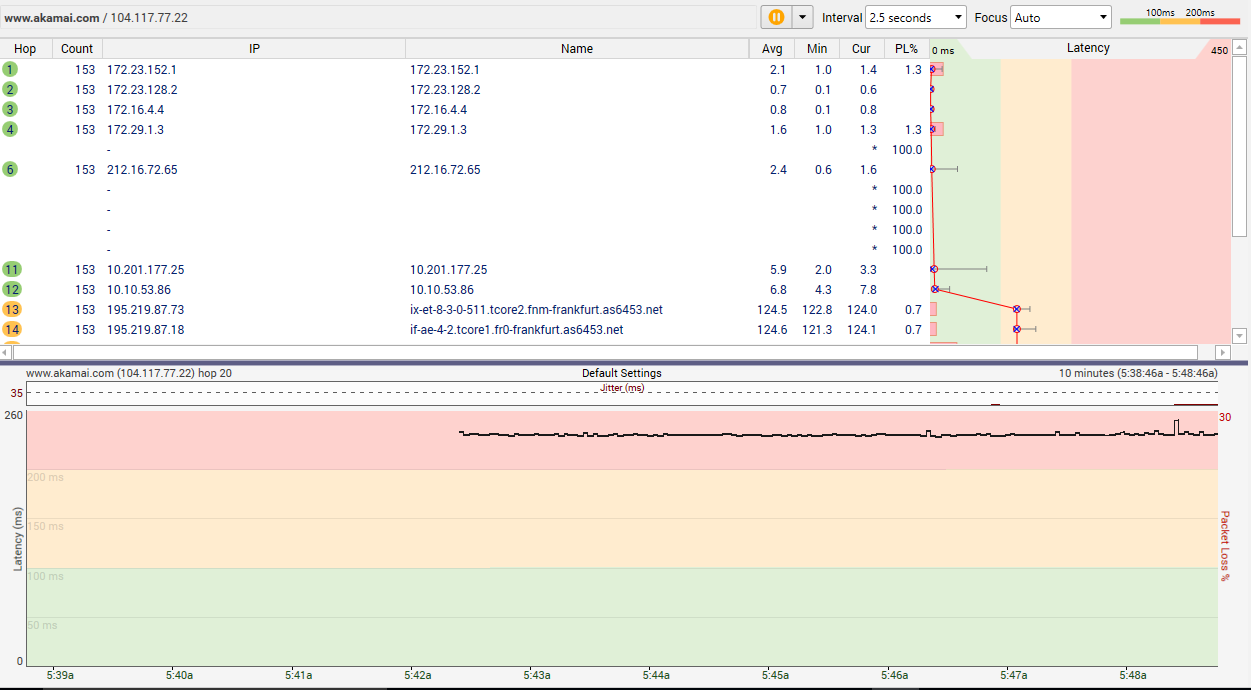
* + - 1. استفاده از ابزار Ping Plotter

اگرچه دستورات گفته شده امکان بررسی وضعیت شبکه را ممکن می‌سازد، اما با ابزارهای دیگری نیز می‌توان تغییرات وضعیت شبکه را به صورت کاراتر مشاهده کرد. یکی از این ابزارها، Ping Plotter است. نمایی از این ابزار در ‏شکل (1-31) نمایش داده شده است.



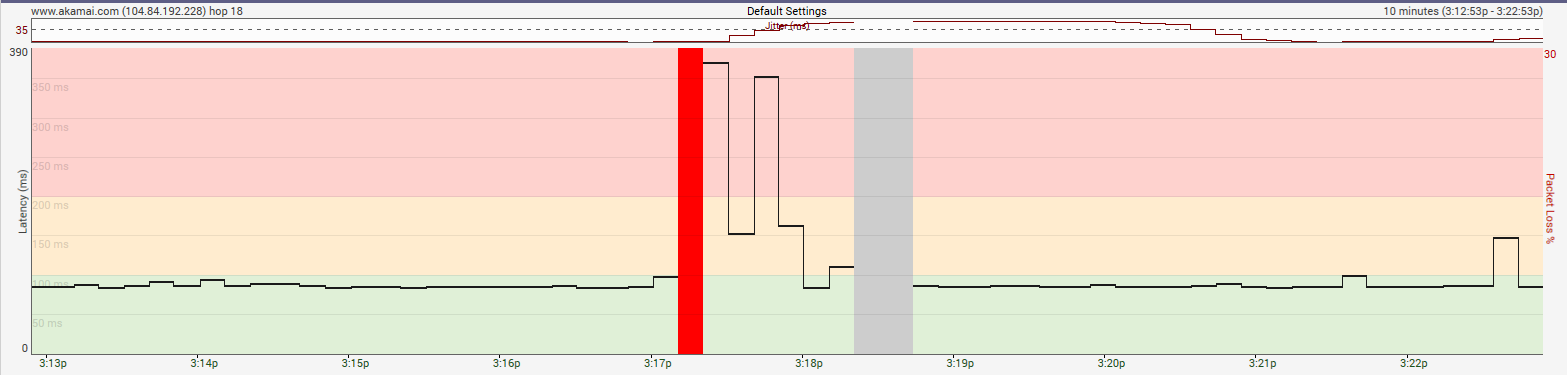
نمایی از ابزار Ping Plotter

با استفاده از این ابزار می‌توان وضعیت تاخیر لینک‌های شبکه را نظارت کرد. برای این کار از منو، File را انتخاب کرده سپس بر روی New Target کلیک می‌کنیم و یک مقصد را انتخاب می‌کنیم. همان‌طور که در ‏شکل (1-32) مشاهده می‌شود برنامه Ping Plotter با Ping کردن دائم مقصد، وضعیت تاخیر بسته‌های دریافتی را نظارت می‌کند.



صفحه کلی

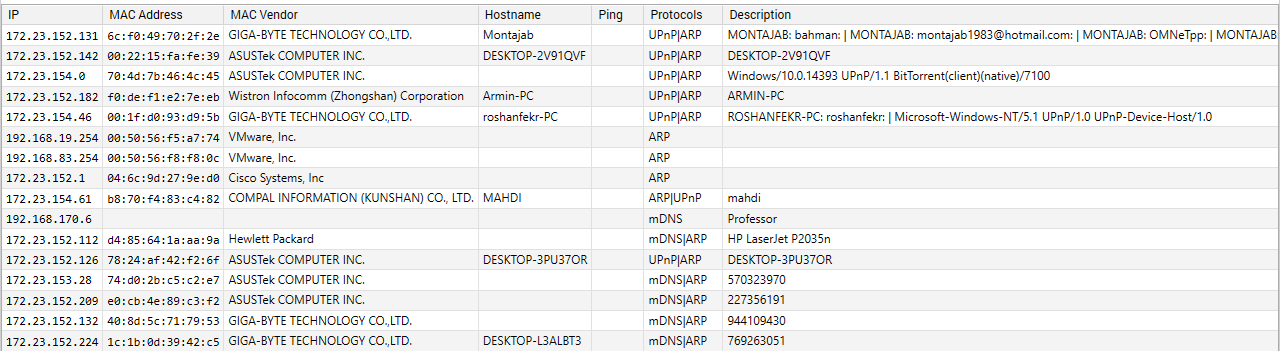
همان‌گونه که در شکل بالا مشاهده می‌شود، تعداد گام‌های بسته تا مقصد نیز نمایش داده شده است. در پنجره پایین نمودار تاخیر بسته‌ها در طول زمان را مشاهده می‌کنید. تصویر دیگری از این صفحه در ‏شکل (1-33) نمایش داده شده است.



نمودار تاخیر بسته‌های دریافتی

مشاهده می‌شود که تاخیر بسته‌ها در ساعت 3:17 بعد از ظهر به صورت ناگهانی افزایش پیدا کرده است. در صورتی که نمودار تاخیر بسته‌ها در شبکه شما به صورت غیرمعمول بالاتر از ناحیه سبزرنگ باشد، نشان دهنده وجود مشکل در شبکه است.

از دیگر امکانات برنامه Ping Plotter می‌توان قابلیت لیست کردن سیستم‌های موجود در شبکه را نام برد. برای این کار از منوی Tools، بخش Local Network Discovery را انتخاب کنید. نمونه خروجی در ‏شکل (1-34) نمایش داده شده است.



نمونه‌ای از خروجی local network discovery

همان‌گونه که در این شکل مشاهده می‌کنید، آدرس IP، آدرس MAC، اسم سیستم و توضیحات آن در هر ردیف نمایش داده شده است.

با استفاده از ipconfig و ping plotter آدرس فیزیکی دروازه شبکه و یکی از دوستان خود را پیدا کنید.

* 1. آشنایی با نرم‌افزار Wireshark
     1. هدف آزمایش

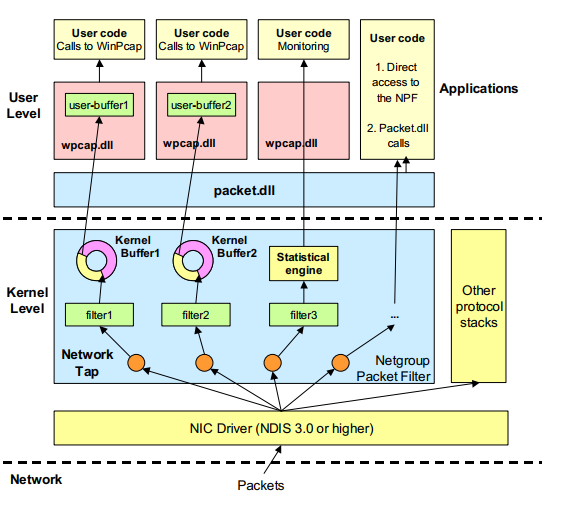
هدف از این آزمایش آشنایی با نرم‌افزار Wireshark و بررسی پروتکل‌ها در لایه مختلف معماری TCP/IP است.

* + 1. مطالب مقدماتی

برنامه Wireshark تحلیل‌کننده پروتکل و شنود کننده ارتباط متن‌باز بر روی سیستم‌عامل‌های خانواده ویندوز و لینوکس است که به شما اجازه می‌دهید ترافیک شبکه خود را تحلیل کنید. پروژه‌ی Wireshark در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد. این پروژه در سال ۲۰۰۶ به Wireshark تغییر نام داد. این نرم‌افزار توسط چهارچوب Qt و با زبان C/C++ نوشته شده است. این برنامه قادر به تحلیل برخط بیش از 1000 پروتکل در نسخه 1.10.6 است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه‌های شنود و تحلیل دیگر مانند TCPdump، Microsoft Network Monitor است. خروجی این برنامه می‌تواند به‌صورت XML،CSV،PostScript یا Plaintext باشد.

در سیستم‌عامل خانواده ویندوز، برنامه Wireshark شنود بسته‌ها با استفاده از کتابخانه‌ Winpcap انجام می‌دهد. معماری نرم‌افزار Winpcap در ‏شکل (1-35) نمایش داده شده است. همان‌گونه که در این شکل مشخص است، برنامه Winpcap از دو بافر یکی در سطح کرنل و دیگری در سطح کاربر، یک ماشین فیلتر کننده که فیلترهایی را به بسته‌ها اعمال می‌کند و همچنین دو فایل wpcap.dll و packet.dll که اینتفریس‌های این برنامه را ارائه می‌کنند تشکیل شده است.

در ابتدا کاربر می‌تواند فیلترهایی را مشخص کند که این فیلترها توسط Netgroup Packet Filter(NPF) به دستوراتی ترجمه می‌شوند که توسط فیلترها بر روی بسته‌ها اعمال می‌شوند. به عنوان مثال کاربر می‌تواند یک فیلتر را به صورت «صرفا بسته‌های پروتکل UDP دریافت شوند» تعریف کند. بسته‌ها پس از اینکه توسط گرداننده شبکه، از واسط شبکه خوانده شدند جمع‌آوری می‌شوند؛ بنابراین کارایی Winpcap وابسته به گرداننده شبکه است. همچنین مشخص است که صرفا یک کپی از بسته‌ها توسط Winpcap دریافت می‌شود و بسته‌ها هم‌زمان می‌توانند پشته پروتکلی سیستم‌عامل که در شکل با نام Other protocol stack مشخص شده است را طی کنند.



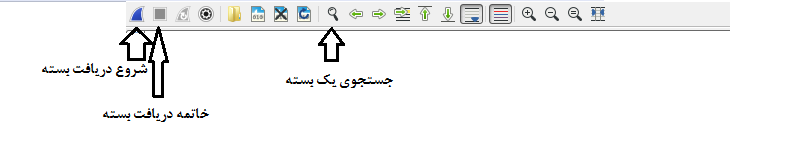
معماری نرم‌افزار Wireshark

برای کار با برنامه Wireshark ابتدا باید واسط شبکه‌ای که قرار است بسته‌ها از آن دریافت شوند مشخص شود. پس از باز کردن برنامه صفحه‌ای مشابه ‏شکل (1-36) نمایش داده می‌شود.



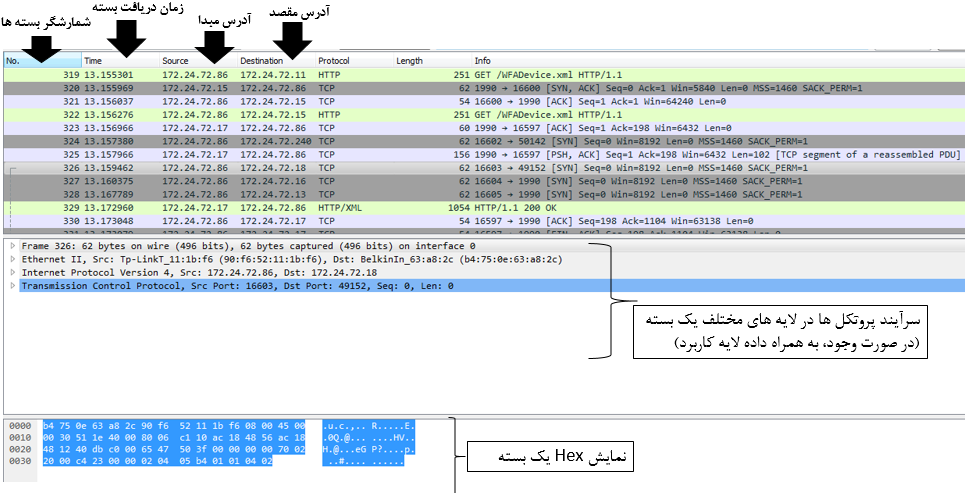
صفحه اول برنامه

واسط شبکه‌ای که به اینترنت متصل است را انتخاب کنید. در ادامه برنامه شروع به دریافت بسته‌ها از کارت شبکه می‌کند. معمولا هر سطر یک بسته را نشان می‌دهد. همان‌گونه که مشاهده می‌کنید بسته‌ها با رنگ‌های مختلف نمایش داده شده‌اند. قوانین رنگ گذاری Wireshark از بخش View->Coloring rules قابل دسترس است. اجزای مختلف منوی ابزار Wireshark در ‏شکل (1-37) نمایش داده شده است.



منوی ابزار

هر زمان که خواستید می‌توانید با استفاده از کلیدهای CTRL+E یا دکمه قرمز رنگ در نوار ابزار، شنود بسته‌ها را متوقف کنید. با دوباره فشردن CTRL+E، Wireshark دوباره شروع به شنود بسته‌ها می‌کند. همچنین این کار می‌تواند با استفاده از دکمه آبی رنگ در نوار ابزار نیز انجام شود. در نوار وضعیت نیز می‌توانید تعداد بسته‌های دریافت شده را مشاهده کنید. بخش‌های مهم محیط اصلی Wireshark در ‏شکل (1-38) نمایش داده شده است.



بخش‌های مهم نرم‌افزار wireshark

* + 1. قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

* برنامه Wireshark نسخه 2 به بعد
* یک کامپیوتر با سیستم‌عامل ویندوز 7 به بعد با دسترسی به اینترنت
  + 1. شرح آزمایش

در تمام بخش‌های آزمایش، واسطی که با آن دسترسی به اینترنت دارید را برای شنود بسته انتخاب کنید.

* + - 1. لایه‌بندی پروتکل‌ها

شروع به شنود بسته‌ها کنید. به اینترنت وارد شوید، شروع به وب گردی کنید و پس از گذشت سه دقیق شنود را متوقف کنید.

به یک بخش دلخواه از بسته‌های شنود شده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آن‌ها را یادداشت کنید.

یک بسته را به‌دلخواه انتخاب کنید. مشخص کنید که چه پروتکل‌هایی در لایه‌های مختلف آن استفاده شده است. ترتیب قرارگیری بیت‌ها داخل بسته چه ارتباطی با لایه‌های مختلف دارد؟ اندازه فریم لایه دو این بسته چقدر است؟ اندازه بسته لایه 3 چقدر است؟

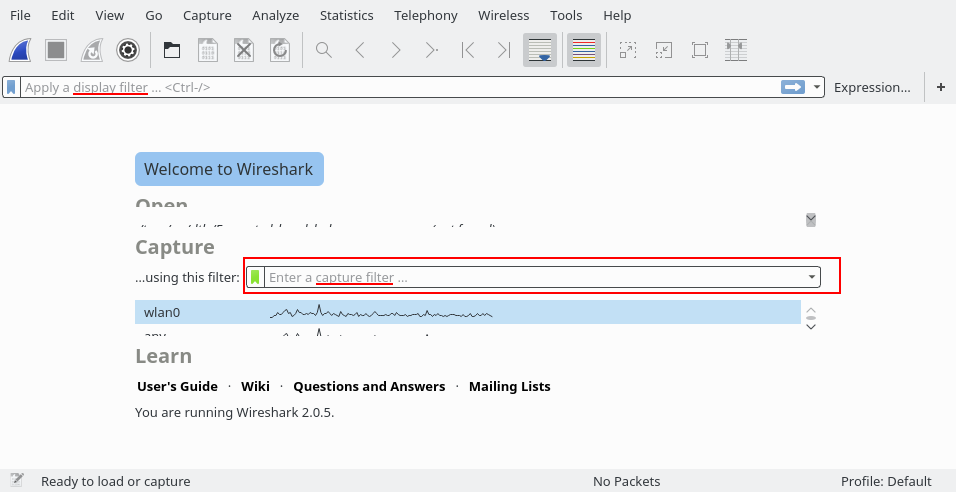
آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Network،Transport و Application باشند؟ این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

از یکی از بسته‌ها بخش مربوط به پروتکل Internet Protocol(IP) را پیدا کنید. Checksum پروتکل IP را پیدا کنید و آن را یادداشت کنید.

از یکی از بسته‌ها بخش مربوط به پروتکل Transport Control Protocol(TCP) و یا User Datagram Protocol(UDP) را پیدا کنید. عدد مربوط به Port مبدا و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدا و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

* + - 1. کار با فیلتر کننده بسته‌ها

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Capture Filter است و نوع دیگر Display Filter. Capture Filter قبل از شروع به شنود بسته مقداردهی می‌شود و در حقیقت همان فیلتری است که توسط NPF بر روی بسته‌های دریافت شده از گرداننده شبکه اعمال می‌گردد؛ بنابراین این فیلتر بر جمع‌آوری بسته‌ها تاثیر می‌گذارد. در مقابل Display Filter صرفا مربوط به فیلتر کردن بسته‌های جمع‌آوری شده است. با استفاده از Display Filter می‌توان تعدادی از بسته‌های جمع‌آوری شده را مشخص کرد که در پنجره Wireshark نمایش داده شوند. این تفاوت در ‏شکل (1-39) نیز نمایش داده شده است.



انواع فیلتر بسته

* + - * 1. کار با Capture Filter

1. به صفحه اول برنامه بروید و در قسمت Capture Filter، مقدار

port 53

1. را وارد کنید. درنهایت اینترفیسی که به اینترنت دسترسی دارد را انتخاب کنید.
2. CMD را باز کرده و دستور

ping google.com

را وارد کنید. سپس دستور

nslookup 1.1.1.1

را نیز وارد کنید. اکنون شنود بسته‌ها را متوقف کنید. شما باید صرفا بسته‌های پروتکل DNS را در Wireshark مشاهده کنید.

یکی از بسته‌ها که از سیستم شما ارسال شده است را انتخاب کنید. پروتکل لایه Transport چیست؟ آدرس IP مقصد چیست؟ سرایند لایه دوم را انتخاب کنید. آدرس مبدا و مقصد را یادداشت کنید.

کدام‌یک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور/all ipconfig مشاهده کنید؟

یک بسته مربوط به دستور Ping را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه کاری استفاده شده است؟

یک بسته مربوط به دستور nslookup را انتخاب کنید و به بخش مربوط به پروتکل DNS در آن بروید. به بخش Queries بروید. چه type ای انتخاب شده است؟ به نظر شما این درخواست DNS برای چه ‌کاری استفاده شده است؟

به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

* + - * 1. کار با Display Filter

1. دوباره به صفحه اول برنامه بروید. این بار اینترفیس را بدون هیچ Capture Filter ای انتخاب کنید.
2. در CMD دستور زیر را وارد کنید.

tracert p30download.com

منتظر بمانید تا کار دستور به اتمام برسد.

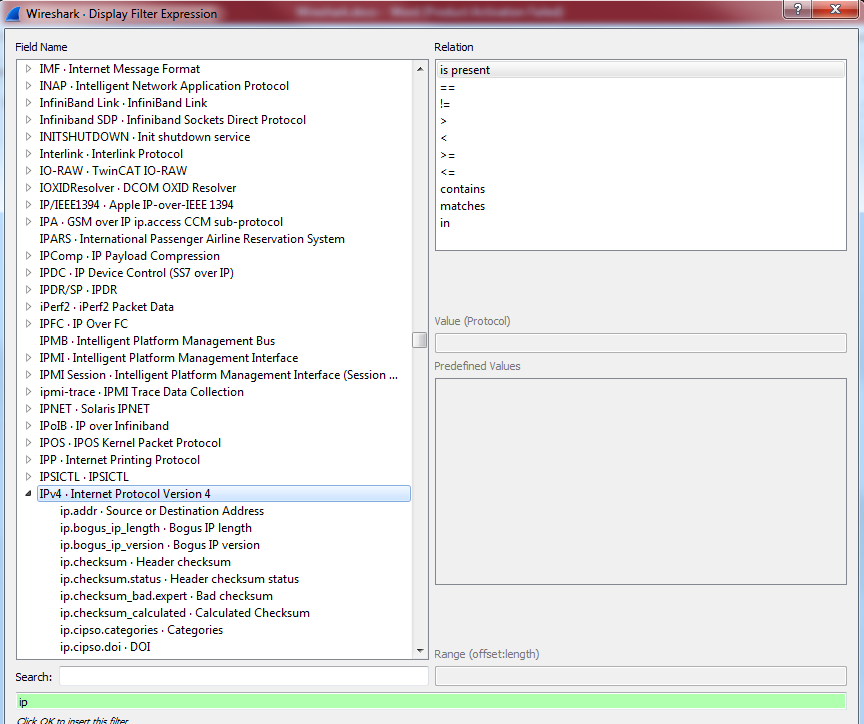
1. بدون اینکه شنود بسته را متوقف کنید در قسمت display filter مقدار dns را تایپ کنید و اینتر را بزنید. مشاهده می‌کنید که صرفا بسته‌های مربوط به پروتکل DNS انتخاب شدند در حالی که سایر بسته‌ها نیز در حال دریافت شدن از گرداننده کارت شبکه هستند.
2. از قسمت سمت راست Display Filter، بر روی Expression کلیک کنید. صفحه مطابق ‏شکل (1-40) باز می‌شود. IP را جستجو کنید و IPv4 را از ستون سمت چپ انتخاب کنید.
3. از زیر بخش‌های IPv4، بخش ip.addr را انتخاب کنید. سپس از بخش relation، مقدار == را انتخاب کرده و در بخش Value آدرس IP که از دستور tracert به شما گزارش شده است را وارد کنید. به عنوان مثال برای آدرس p30download.com مشابه ‏شکل (1-41) است.

بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

اولین بسته را انتخاب کنید. به بخش پروتکل Internet Control Message Protocol بروید. مقدار type را مشخص کنید. به بخش مربوط به پروتکل IP بروید و مقدار TTL را یادداشت کنید.

1. برای بسته‌هایی که مبدا آن‌ها ماشین شماست مقدار TTL را یادداشت کنید. این مقدار در حال تغییر است.

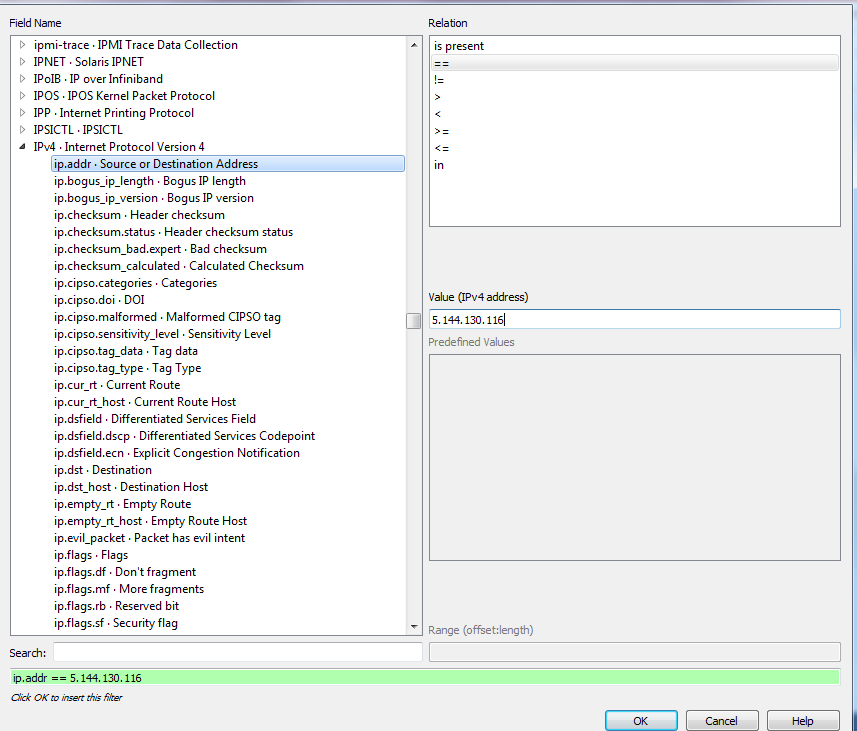
به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.



انتخاب Display Filter

1. از بخش فیلتر، مقدار فیلتر را به دستور ip.proto == 6 تغییر دهید.

این فیلتر چه کاری انجام می‌دهد؟



مقادیر برای p30download.com

1. لایه کاربرد
   1. راه‌اندازی سرویس‌های Web و FTP
      1. هدف آزمایش

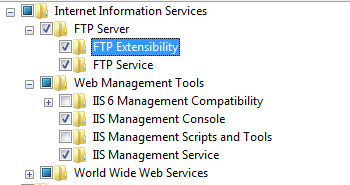
هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط به راه‌اندازی سرویس‌های Web و FTP و تحلیل بسته‌های HTTP و FTP است.

* + 1. قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

* کامپیوتر شخصی با سیستم‌عامل ویندوز 7 برای هر گروه
* برنامه Filezila نسخه 3.17.0.1
  + 1. شرح آزمایش

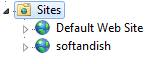
ابتدا تنظیمات مربوط به سرور Web را انجام می‌دهیم. سپس تنظیمات FTP Server را بررسی می‌کنیم. برای این منظور ابتدا عبارت Turn windows features on or off را در قسمت جستجوی ویندوز 7، جستجو کنید. سپس بخش‌های زیر را از پنجره نمایش داده شده، انتخاب نمایید و بر روی OK کلیک کنید. دقت کنید هر سه بخش FTP Server، Web Management Tools و World Wide Web Services مانند ‏شکل (2-1) تیک خورده باشند.



پیش تنظیمات

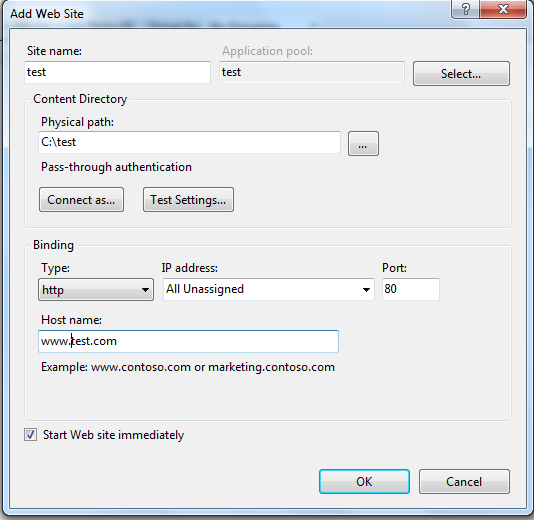
* + - 1. تنظیمات سرور Web

1. از بخش start عبارت iis را جستجو کرده و Internet information service manager را انتخاب کنید. در پنجره باز شده از ستون سمت چپ بر روی Sites کلیک راست کنید و Add Website را انتخاب کنید.



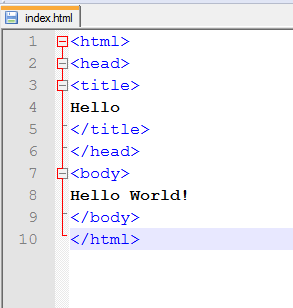
مرحله اول

1. در پنجره باز شده، یک نام و یک Host name برای سایت انتخاب کنید. همچنین باید یک مسیر بر روی سیستم خود مشخص کنید که اطلاعات مربوط به سایت در آنجا نگهداری می‌شوند.



مرحله دوم

1. مشاهده می‌کنید که به صورت پیش‌فرض سایت بر روی تمام آدرس‌های IP دستگاه و بر روی پورت 80 bind می‌شود. با زدن دکمه OK سایت ایجاد می‌شود.
2. یک صفحه ساده مانند شکل زیر ایجاد کنید و آن را در مسیر مشخص شده برای سایت قرار دهید. نام آن را index.html بگذارید.



مرحله سوم

1. حال در مرورگر خود آدرس Host نوشته شده برای سایت را وارد کنید.

سایتی که ایجاد کرده‌اید نمایش داده نمی‌شود، چرا؟

1. به آدرس C:\Windows\System32\drivers\etc در سیستم بروید و فایل hosts را با یک ویرایشگر مانند Notepad++ باز کنید. خط زیر را به آن اضافه کنید. دقت کنید که Host name خود را به‌جای [www.test.com](http://www.test.com) قرار دهید.

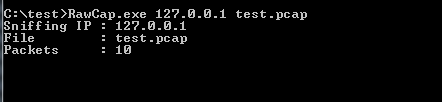


مرحله چهارم

1. حال در cmd دستور زیر را وارد کنید. ipconfig /flushdns این دستور باعث پاک شدن کش DNS سیستم شما خواهد شد.

آدرس سایت خود را در مرورگر وارد کنید و ارتباط خود را با استفاده از wireshark شنود کنید. آیا می‌توانید مشخص کنید کدام بسته مربوط به سایت شما است؟ چه اتفاقی افتاده است؟

1. Wireshark نمی‌تواند ترافیک مربوط به آدرس‌های Loopback را شنود کند؛ بنابراین از برنامه Rawcap استفاده می‌کنیم. از آدرس <http://www.netresec.com/?page=RawCap> آن را دانلود کنید.
2. در محیط cmd به محل فایل rawcap.exe بروید. آن را با دستور نشان داده شده در ‏شکل (2-6) اجرا کنید



دستورات اجرایی در cmd

1. حالا سایت را باز کنید. پس از اتمام باز شدن، با ctrl+c می‌توانید از rawcap خارج شوید. فایل در محل اجرای برنامه ذخیره می‌شود. دقت کنید قبل از باز کردن سایت، کش مرورگر خود را پاک کنید.
2. فایل ذخیره‌شده را با wireshark باز کنید. بسته‌های مربوط به سایت را پیدا کنید. بر روی یکی از آن‌ها کلیک راست کرده و follow HTTP Stream را انتخاب کنید. شکلی مشابه ‏شکل (2-7) نمایش داده خواهد شد.



نمونه‌ای از خروجی Follow HTTP Stream

آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

1. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکل HTTP را مشاهده کنید.

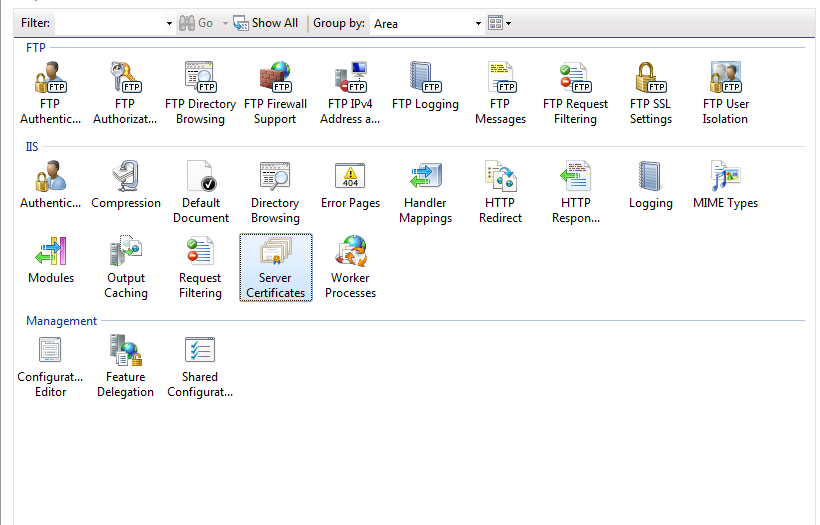
مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم‌ شده است؟

یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

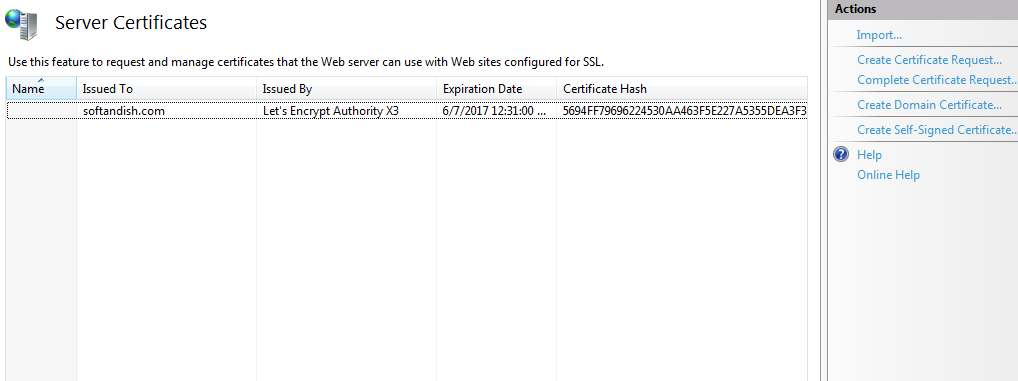
در مرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچ‌کدام از سایت‌ها نمایش داده نمی‌شوند؟

1. دوباره به محیط IIS Manager بروید. این بار در ستون سمت چپ بر روی نام کامپیوتر کلیک کنید. صفحه نمایش داده شده در ‏شکل (2-8) باز می‌شود.



صفحه نمایش داده شده بعد از انتخاب نام کامپیوتر

1. بر روی Server Certificate کلیک کنید. از ستون سمت راست بر روی Create Self-Signed Certificate کلیک کنید.



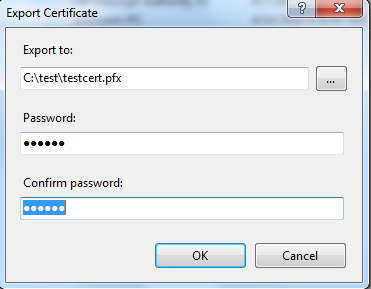
انتخاب Create Self-Signed Certificate

1. یک نام برای آن انتخاب کنید و بر روی OK کلیک کنید. بهتر است نام انتخابی مطابق نام سایت باشد؛ مثلا\*.test.com گواهی مطابق ‏شکل (2-10) ساخته می‌شود.



نمونه گواهی ساخته شده

1. اگر بر روی گواهی ساخته شده کلیک راست کرده و export را کلیک کنید صفحه نشان داده شده در ‏شکل (2-11) نمایش داده می‌شود. آن را کامل کرده و گواهی را export کنید. هر پسورد دلخواهی که می­خواهید در بخش Password قرار دهید.



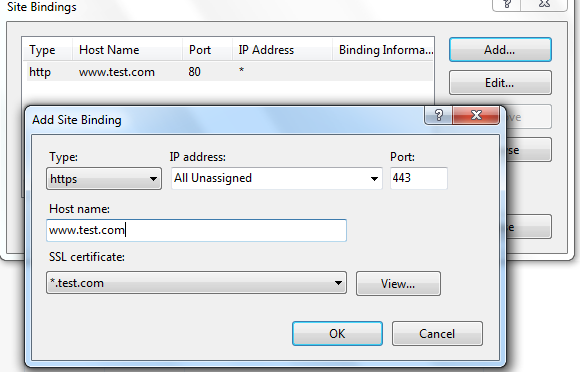
نحوه export گواهی

1. حال دوباره از ستون سمت چپ بر روی Sites کلیک کنید. سپس سایت خود را انتخاب کرده و بر روی آن کلیک راست کرده و Binding را انتخاب کنید.



Binding- مرحله اول

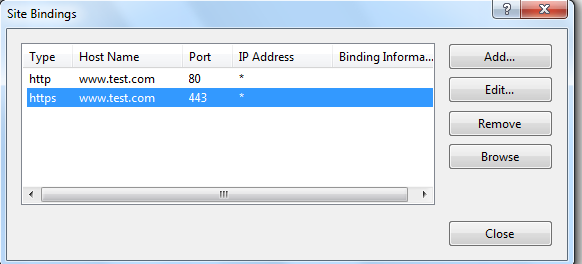
1. بر روی Add کلیک کنید و مطابق ‏شکل (2-13) آن را تکمیل کنید. دقت کنید که گواهی که خودتان ایجاد کرده‌اید را باید انتخاب کنید.



Binding- مرحله دوم

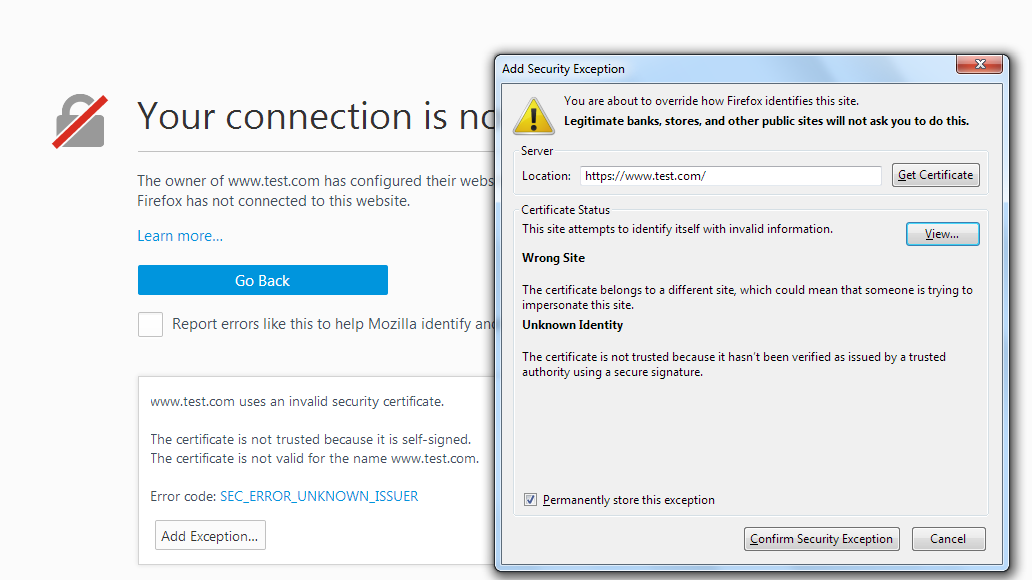
1. بر روی OK کلیک کنید. حالا Binding های نشان داده شده در ‏شکل (2-14) را دارید.
2. حال آدرس <https://www.test.com/> را در مرورگر خود باز کنید. دقت کنید که به‌جای test.com آدرس سایت خود را قرار دهید.

آیا با مشکلی مواجه شدید؟ اگر با مشکل مواجه شده‌اید با استفاده از rawcap، مشخص کنید که چه مشکلی وجود دارد.



Binding- مرحله سوم

1. سایت را در مرورگر باز کنید. خطای نشان داده شده در ‏شکل (2-15) نمایش داده می‌شود.



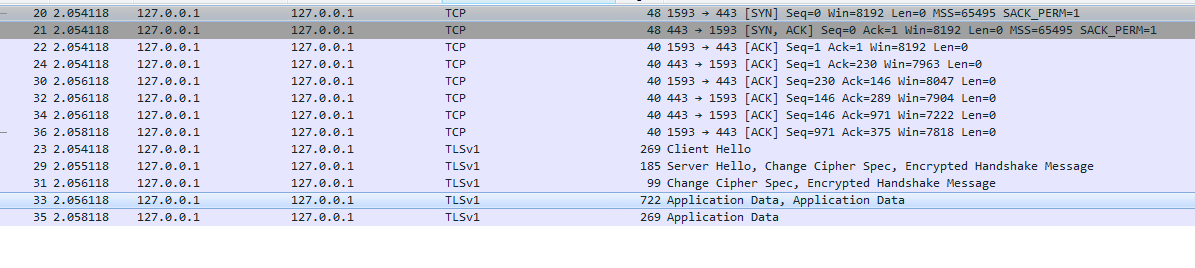
خطای نمایش داده شده

1. بر روی Add exception کلیک کرده و دکمه View را فشار دهید.

مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت‌زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.

1. حال ارتباط را با Rawcap شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. صفحه‌ای مطابق ‏شکل (2-16) نمایش داده می‌شود.

آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

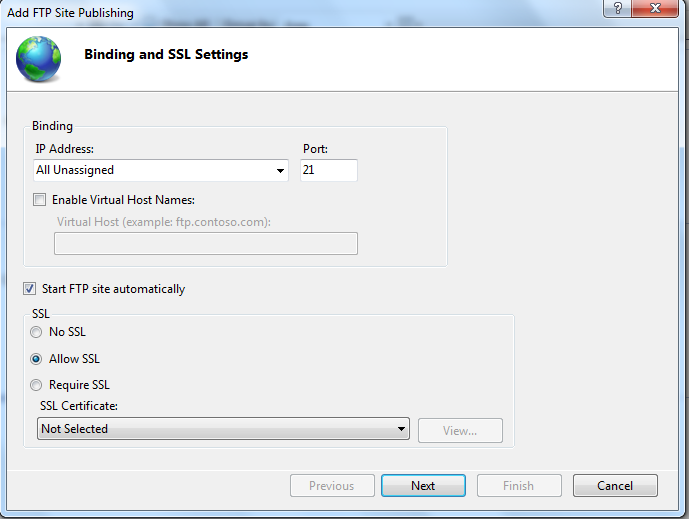


نمونه خروجی Follow SSL Stream

به یک سایت مانند https://google.com وصل شده، گواهی آن را بررسی کنید. گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

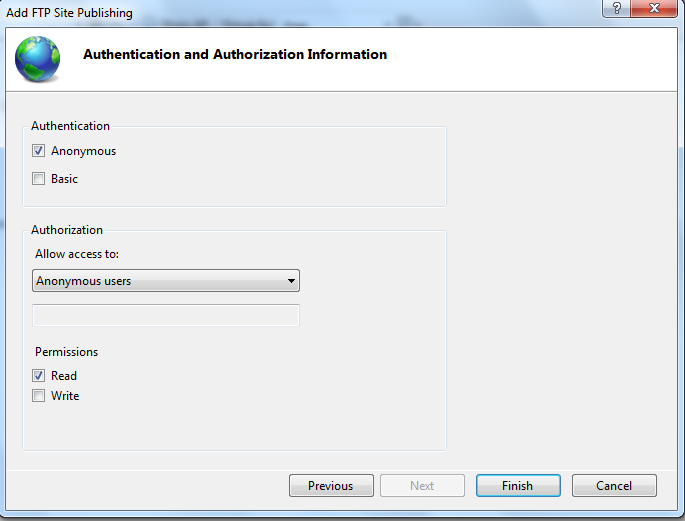
* + - 1. تنظیمات سرور FTP

1. دوباره به صفحه اصلی IIS Manager بروید. بر روی نام سایت ساخته شده خودتان در ستون سمت چپ کلیک راست کرده و Add FTP Publishing را انتخاب کنید. تنظیمات را مطابق ‏شکل (2-17) انجام دهید. به‌جای Test.com اسم سایت خود را قرار دهید.



FTP Site Publishing

1. دکمه Next را بزنید و صفحه بعد را مطابق ‏شکل (2-18) کامل کنید.



تکمیل Binding

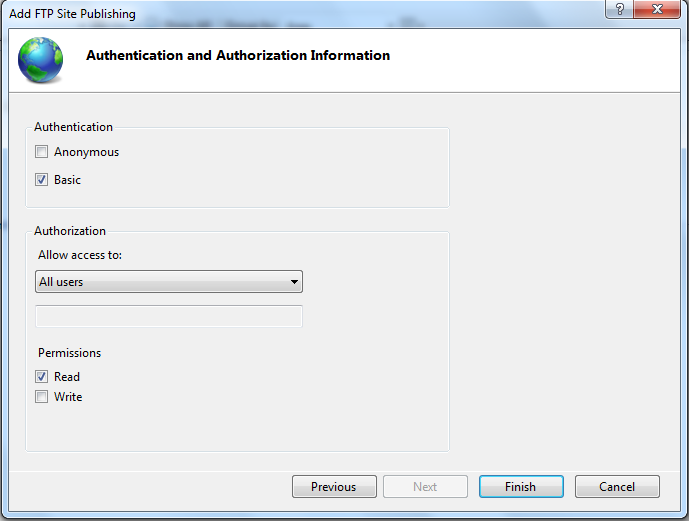
1. بر روی دکمه Finish کلیک کنید. درنهایت Binding هم ساخته می‌شود.
2. به آدرس <ftp://www.test.com/> بروید. ارتباط را با Rawcap شنود کنید.

مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

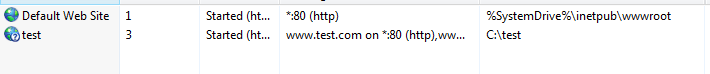
1. اکنون با کلیک راست کردن بر روی سایت خود و انتخاب گزینه Remove FTP Publishing، تنظیمات قبلی را حذف کنید. حال دوباره Binding جدیدی ایجاد کنید و این بار بخش Authentication را مطابق ‏شکل (2-19) تکمیل کنید.
2. دوباره به آدرس <ftp://www.test.com/> بروید. این بار باید نام کاربری و پسورد سیستم خود را وارد کنید تا اجازه دسترسی به شما داده شود. ارتباط را با Raw cap شنود کنید.

آیا نام کاربری و پسورد قابل خواندن است؟

1. اگر از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید، صفحه نشان داده شده در ‏شکل (2-20) نمایش داده می‌شود.



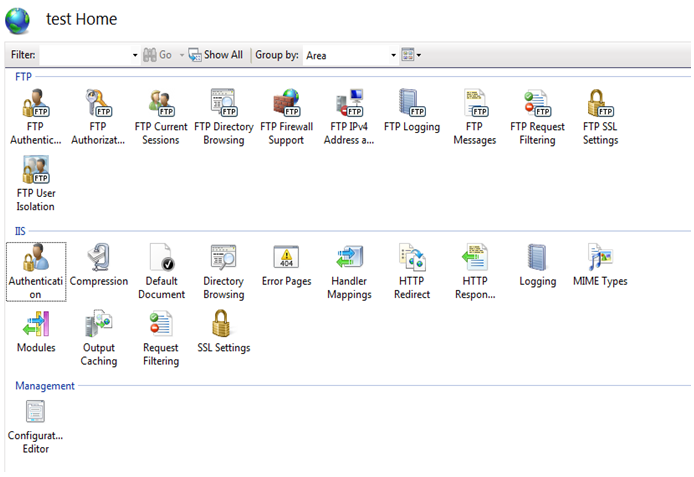
تنظیمات Authentication



صفحه نمایش داده شده بعد از انتخاب Sites

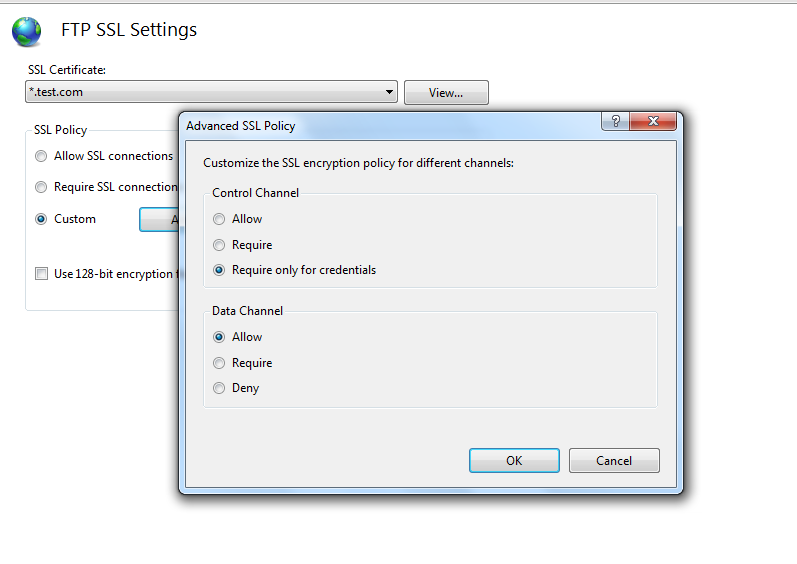
1. با انتخاب سایت خود، صفحه نشان داده شده در ‏شکل (2-21) نمایش داده می‌شود. تنظیمات نام‌های کاربری و دسترسی‌ها در این بخش مشخص است

به FTP Authentication و FTP Authorization وارد شوید و مشخص کنید چه سطح دسترسی برای چه کاربرانی تعریف شده است.



صفحه نمایش داده شده بعد از انتخاب نام سایت خود

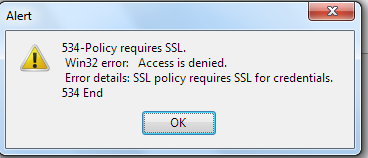
1. دوباره از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید و سپس سایت خود را انتخاب کنید. به بخش FTP SSL Settings بروید. یک گواهی انتخاب کنید. سپس بر روی Custom کلیک کنید و آن را مطابق ‏شکل (2-22) تکمیل کنید. پس از آن دکمه Apply را فشار دهید.



تنظیمات SSL Policy

سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟

در مرورگر فایرفاکس خطای نمایش داده شده در ‏شکل (2-23) نشان داده می‌شود. معنی این خطا چیست؟



خطای نمایش داده شده

1. برنامه Filezilla را از آدرس <https://filezilla-project.org/> دانلود کنید. پس از نصب، در قسمت Host، loopback را بنویسید. نام کاربری و پسورد ویندوز خود را وارد کنید و بر روی Quickconnect کلیک کنید. ارتباط را با Rawcap شنود کنید. آیا نام کاربری و پسورد قابل‌خواندن است؟
   * + 1. پروتکل HTTP
2. عمل شنود را آغاز کنید، مرورگر را باز کرده و به آدرس <http://aut.ac.ir> بروید. شنود را متوقف کرده و بسته‌ها را بررسی کنید:
3. بر روی یکی از بسته‌های پروتکل HTTP کلیک راست کرده و Follow HTTP Stream را انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.
4. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش های مختلف پروتکل HTTP را مشاهده کنید. مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟
5. در پنجره باز شده، بسته هایی با پروتکل TCP هم مشخص شده است. اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟
   * + 1. پروتکل FTP
6. عمل شنود را آغاز کرده و مرورگر را باز کرده و به آدرس <ftp://ftp.lip6.fr/> بروید. شنود را متوقف کنید. یک بسته مربوط به پروتکل FTP را انتخاب کرده، بر روی آن کلیک راست کنید و Follow TCP Stream را انتخاب کنید.
7. پروتکل لایه Transport استفاده شده برای این بسته ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.
8. در یکی از بسته ها مقدار Username و در بسته دیگر مقدار Password به سمت سرور ارسال شده است. این مقادیر را مشخص کنید.
   1. کار با کاربردهای Web، DNS، سوکت و پویش سرویس‌ها
      1. هدف آزمایش

در این آزمایش قصد داریم با تعدادی از ابزارهای شبکه که به‌وسیله آن‌ها می‌توانیم در کاربردهای Web و DNS به‌عنوان سرویس‌گیرنده استفاده شوند، آشنا شویم.

* + 1. فعالیت‌های قبل از آزمایش

پروتکل‌های HTTP، TCP، UDP و DNS را یک‌بار مرور کنید.

* + 1. قطعات و ابزارهای موردنیاز

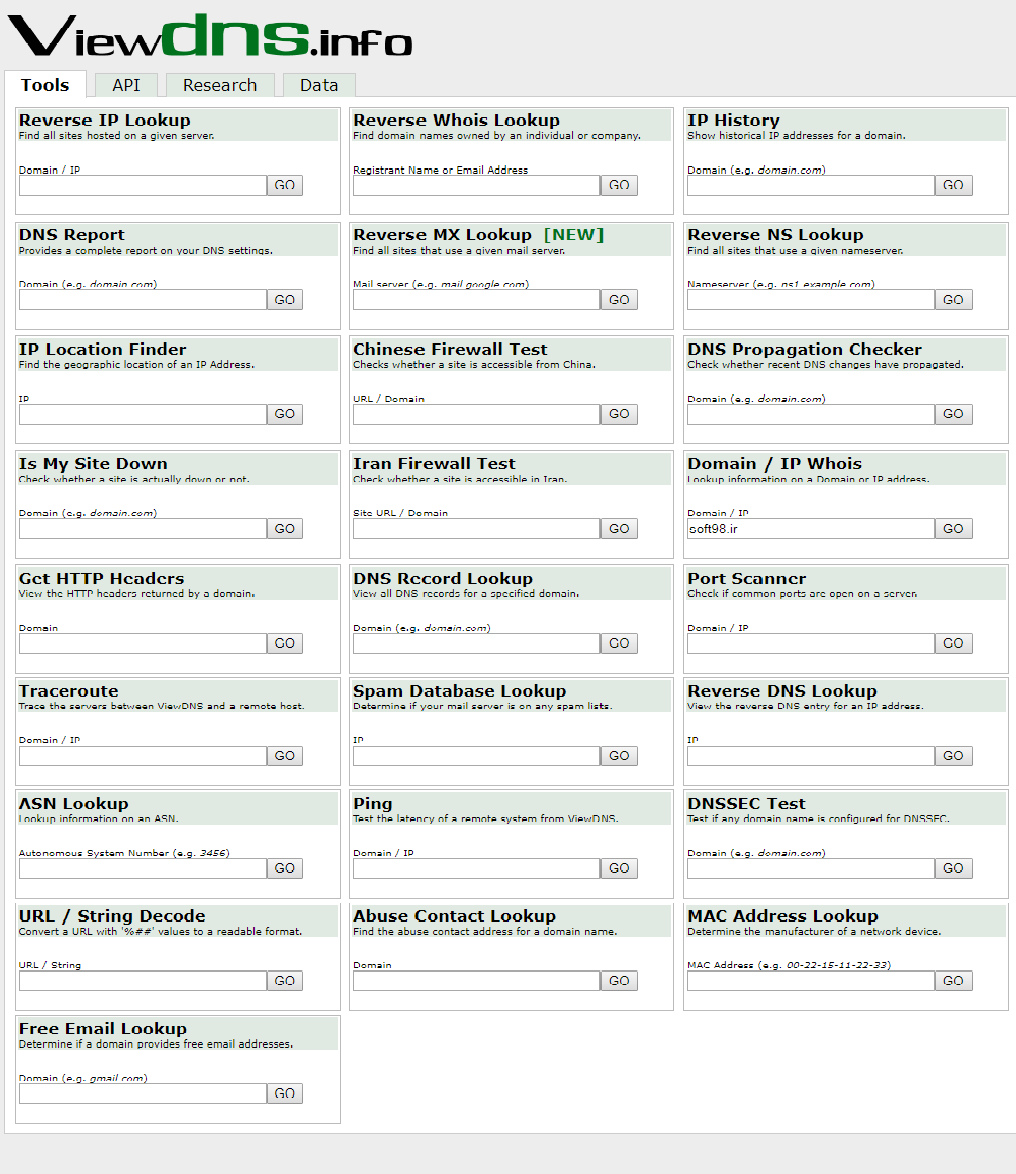
ابزارهای موردنیاز برای انجام این آزمایش عبارت‌اند از:

* کامپیوتر شخصی با سیستم‌عامل ویندوز 7 یا بالاتر برای هر گروه
* برنامه Nmap نسخه 7.7 به بالا
* برنامه Wireshark نسخه 2.4 به بالا
  + 1. شرح آزمایش
       1. کارکرد DNS

در ابتدا با ابزارهای برخط[[25]](#footnote-25) کارکرد DNS آشنا می‌شویم. یکی از این ابزارها، وب‌سایت ViewDNS است. در گام اول با آدرس زیر وارد این و‌ب‌سایت شوید:

<http://viewdns.info/>

صفحه اول این وب‌سایت در ‏شکل (2-24) نمایش داده شده است.



وب‌سایت Viewdns

1. در قسمت Domain / IP Whois رفته و آدرس soft98.ir را وارد نمایید.

نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟

آدرس name server آن چیست؟

1. در وب‌سایت به قسمت DNS Report رفته و آدرس soft98.ir را وارد نمایید.

رکوردهای NS، A، TXT و MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می‌کنند؟

در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir)، mail server دانشگاه را مشخص کنید. آیا آدرس IP آن را می‌توانید مشخص کنید؟

1. در قسمت Reverse IP Lookup آدرس farsnews.com را وارد کنید.

چه وب‌سایت‌های دیگری بر روی همین سرور قرار دارند (آدرس IP آن‌ها را با آدرس IP سایت farsnews.com مقایسه کنید)؟

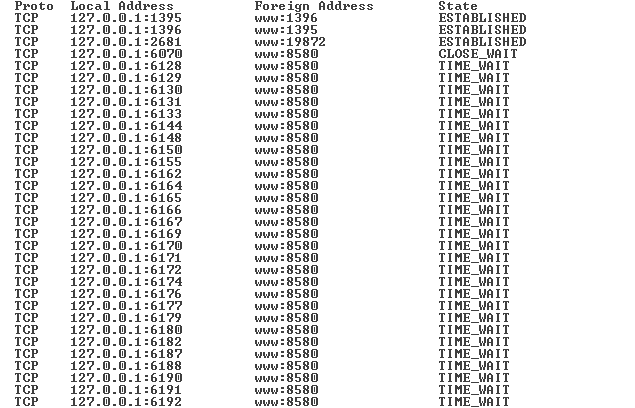
به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

1. به وب‌سایت زیر بروید:

<https://simpledns.com/lookup-dg>

1. در این وب‌سایت آدرس aut.ac.ir وارد کرده و درخواست‌ها و پاسخ‌های دریافت شده را بررسی کنید.
   * + 1. مشاهده و تخصیص پورت‌های لایه انتقال با استفاده از ابزار Netstat

با استفاده از ابزار netstat می‌توان وضعیت پورت‌های لایه انتقال سیستم را مشاهده کرد. به صورت دقیق‌تر می‌توان مشاهده نمود که چه سوکت‌هایی در سیستم وجود دارند و وضعیت آن‌ها چیست. نمونه‌ای از خروجی این دستور در ‏شکل (2-25) مشاهده می‌شود.



نمونه‌ای از خروجی دستور netstat

بسیاری از مواقع، برنامه‌هایی نیاز به گوش دادن به یک پورت خاص در سیستم هستند. حال اگر برنامه دیگری قبل از آن‌ها، به آن پورت خاص گوش بدهد برنامه جدید قادر به گوش دادن به آن پورت نخواهد بود. در این حالت با استفاده از این دستور می‌توانید مشاهده کنید چه پورت‌هایی توسط چه برنامه‌هایی استفاده می‌شود.

برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم بازکرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

دستوری را پیدا کنید که به‌وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به‌صورت عددی لیست شوند.

* + - 1. کارکرد Web

1. در این بخش می‌خواهیم با استفاده از ابزار ncat و پروتکل HTTP یک ارتباط با وب سرور دانشگاه ایجاد کنیم. CMD را باز کرده و با استفاده از دستور زیر ابتدا یک ارتباط TCP با aut.ac.ir روی پورت ۸۰ ایجاد کنید.

ncat –v aut.ac.ir 80

1. در ادامه پیام HTTP مربوط به دریافت آدرس / را مطابق دستورات زیر وارد کنید. پس از فشردن دکمه enter در خط دوم یک‌بار دیگر enter را وارد کنید.

GET / HTTP/1.1

Host: aut.ac.ir

دلیل وارد کردن دو enter پشت سر هم چیست؟

پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه‌ی اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام‌ها با استفاده از wireshark اثبات کنید.

آیا این ارتباط persistent است؟

1. با فشردن CTRL+C ارتباط قبلی را خاتمه دهید و دستور زیر را وارد کنید:

ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe

1. این دستور یک سوکت TCP ایجاد می‌کند که بر روی پورت 16000 گوش فرا می‌دهد، این موضوع را با استفاده از netstat –abn مشاهده کنید.

این پورت بر روی کدام آدرس IP، bind شده است؟ بعد از برقراری ارتباط با این سوکت، برنامه CMD نیز اجرا می‌شود. در ادامه دستوراتی که فرستنده ارسال کند به این برنامه داده می‌شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.

1. آدرس آی‌پی سیستم دوست خود را یادداشت کنید، دستور زیر را اجرا کرده تا به پورت 16000 سیستم دوست خود متصل شوید:

ncat friend\_ip 16000

1. برای اینکه مطمئن شوید، با استفاده از دستور ipconfig تایید کنید که در سیستم دوستتان هستید. ارتباط را با دستور CTRL+C ارتباط قبلی را خاتمه دهید.
2. با استفاده از دستور زیر می‌توانید یک web server ساده ایجاد کنید. این سرور تنها فایل index.html را که به آن داده‌اید میزبانی می‌کند و به کاربر تحویل می‌دهد.

ncat -l –p 4444 < index.html

1. برای فایل index.htnl می‌توانید از محتوای زیر استفاده کنید:

HTTP/1.1 200 OK

<html>

<head>

<title>Hello</title>

<body> Salam!</body>

</head>

</html>

دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول این فایل بسازید و نتیجه را امتحان کنید.

* + - 1. پویش سرویس‌ها

برنامه‌ی NMAP به‌منظور پویش شبکه و سرویس‌های سیستم‌های انتهایی مورداستفاده قرار می‌گیرد. با استفاده از این برنامه می‌توانید تشخیص دهید بر روی هر سیستم چه سرویس‌هایی قرار دارد و آیا آن سرویس‌ها در دسترس هستند و یا خیر. رابط کاربری گرافیکی این ابزار Zenmap نام دارد.

1. برنامه Zenmap را اجرا کرده و با استفاده از آن آدرس آی پی سیستم دوست خود را اسکن کنید.

سیستم‌عامل دوست شما چیست؟

چه پورت‌هایی روی سیستم دوست شما باز است؟

سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

مراحل بالا را برای سایت aut.ac.ir انجام دهید. سیستم‌عامل این وب‌سایت چیست؟

این بار آدرس asg.aut.ac.ir را پویش کنید. با انتخاب پروفایل Intense scan، نتیجه چیست؟ پروفایل Intense scan, No ping را انتخاب کنید. نتیجه چیست؟ آدرس asg.aut.ac.ir را Ping کنید. به نظر شما نتیجه اسکن به چه دلیلی تغییر کرده است؟ این ماشین چه نقشی در دانشگاه دارد؟

1. لایه انتقال
   1. تحلیل TCP با استفاده از Wireshark
      1. هدف آزمایش

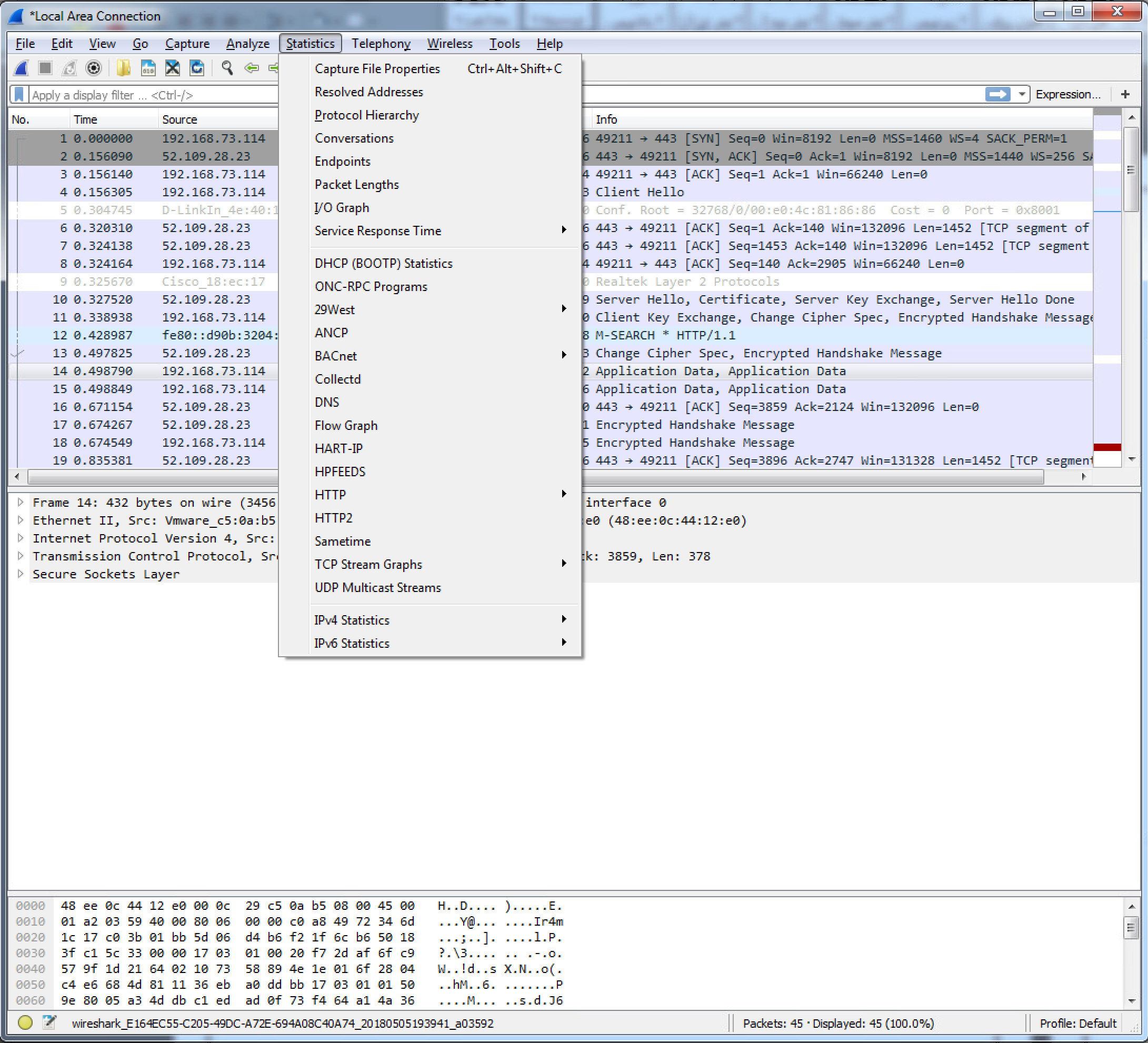
در این آزمایش قصد داریم آشنایی بیشتری با نرم‌افزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته‌های جمع‌آوری‌شده استفاده نماییم.

* + 1. فعالیت‌های قبل از آزمایش

دستور کار جلسه‌ی آشنایی با wireshark را مرور کنید.

* + 1. شرح آزمایش

نرم‌افزار wireshark را باز کرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جمع‌آوری کنید. سپس مطابق جمع‌آوری بسته را متوقف کرده و از منوی بالا بر روی گزینه‌ی Statistics کلیک کنید. در ادامه قصد داریم مواردی که در این زبانه وجود دارند را بررسی کنیم.



زبانه Statistics

1. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

آیا می‌توانید سه بایت اولی که برای آدرس فیزیکی کارت‌های شبکه Cisco می‌باشند را مشخص کنید؟

1. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟

1. بر روی گزینه‌ی Conversations کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

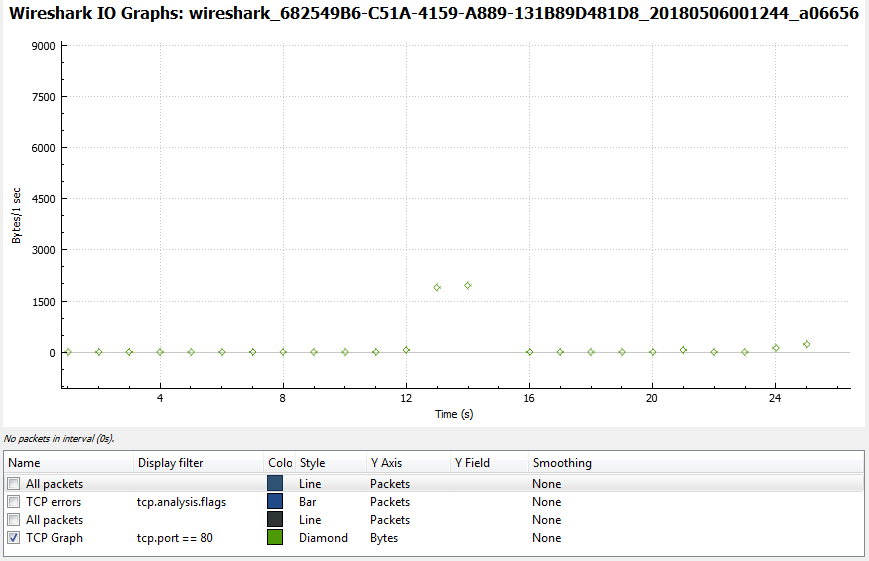
1. یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدا و مقصد را مشخص کنید.) توجه داشته باشید مفهومی که Wireshark از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.
2. بر روی گزینه‌ی endpoints کلیک کنید.

در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

چه مقصدهایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟

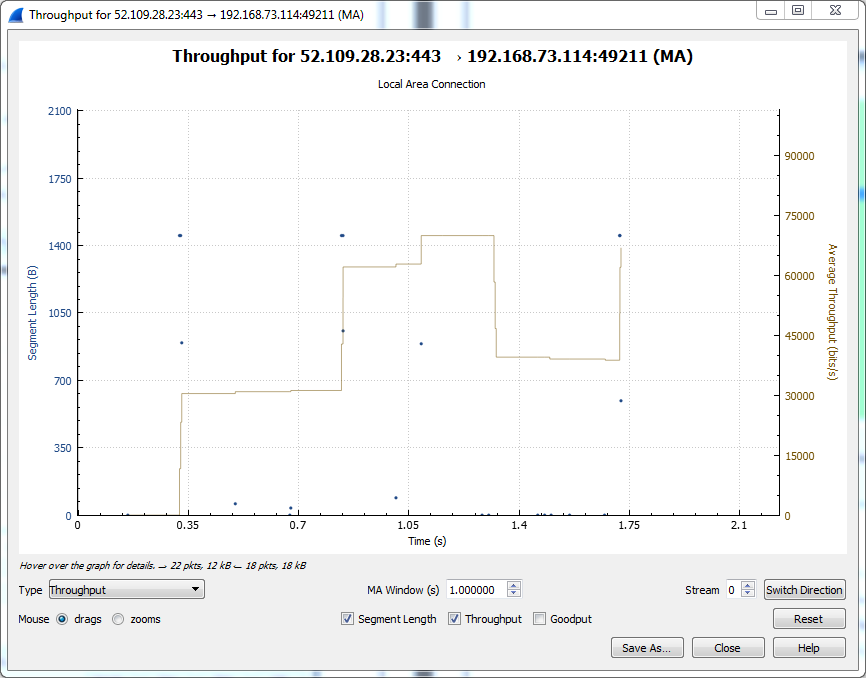
آیا می‌توانید از زبانه Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید؟

1. بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O‌ را مشاهده کنید. شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک بر روی نمودار، بسته‌ها در پنجره اصلی مشخص خواهند شد.



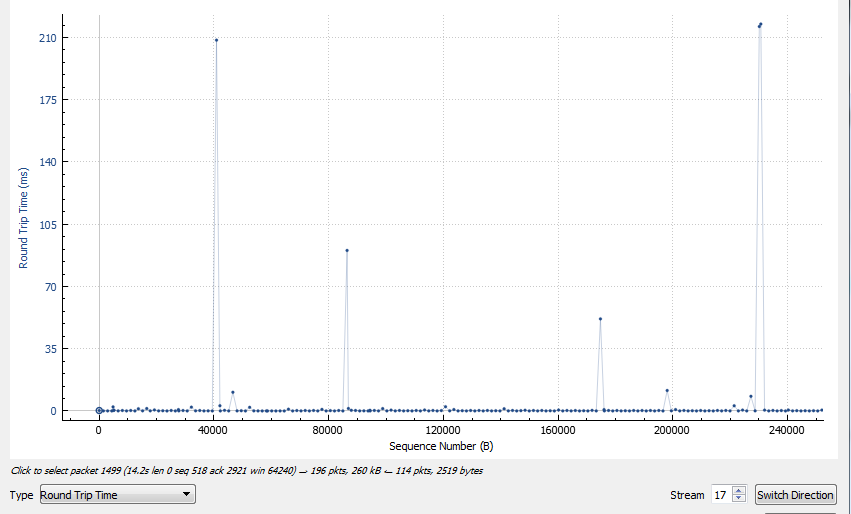
IO Graphs

1. بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید (با استفاده از Follow TCP Stream). سپس بر روی گزینه‌ی Flow Graph کلیک کنید. از منوی پایین، در بخش Show، Displayed packets را انتخاب کنید. به‌صورت کامل جزئیات مربوط به SeqNum و Ack و شماره پنجره را دنبال کنید.
2. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Throughput کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید گذردهی میانگین با واحد بیت در ثانیه در طول زمان برای یک ارتباط TCP را مانند ‏شکل (3-3) مشاهده کنید. با گزینه‌ی Switch Direction می‌توانید ارتباط در جهت برعکس را بررسی کنید. بر روی نمودار نقاط آبی رنگی قرار دارند، این نقاط طول segmentهای ارسال شده برحسب بایت در ارتباط TCP را در آن زمان نمایش می‌دهد. با افزایش شمارنده‌ای که در پایین پنجره با نام Stream قرار دارد می‌توانید ارتباط TCP خود را عوض کنید. منظور از Goodput نرخی است که کاربرد داده خود را دریافت می‌کند و در آن Retransmission ها در نظر گرفته نمی‌شوند.



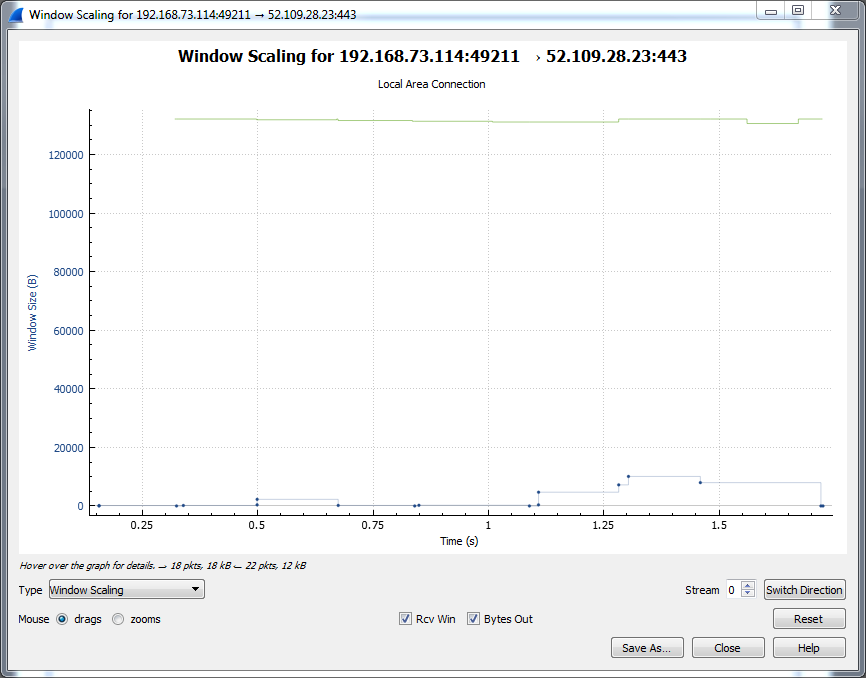
نمودار گذردهی

1. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Round Trip Time کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید زمان یک رفت و برگشت را برای یک ارتباط TCP مشاهده کنید (‏شکل (3-4)). گزینه‌های این پنجره نیز مانند قسمت 8 است. می‌توانید با انتخاب گزینه‌ی RTT By Sequence Number این نمودار را برحسب شماره‌ی بسته‌ها داشته باشید. شمارنده Stream در گوشه پایین سمت راست را به شماره Stream مربوط به اتصال TCP با یکی از سایت‌هایی که داشتید تنظیم کنید.



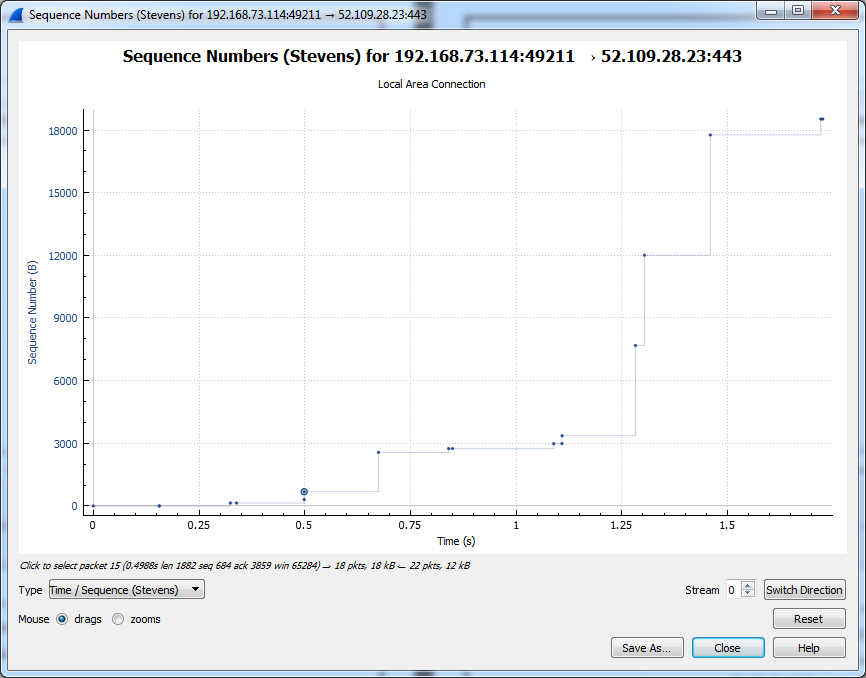
نمودار RTT

1. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. پنجره‌ای مانند ‏شکل (3-5) باز می‌شود که می‌توانید اندازه‌ی پنجره‌ی دریافت (با خط سبز رنگ) و بایت‌های ارسالی (با خط آبی رنگ) را برای یک ارتباط TCP مشاهده نمایید. تمامی تنظیمات این پنجره مانند قسمت ۸ است.



نمودار Window Scaling

1. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Time / Sequence (Stevens) کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید Sequence number در طی زمان را برای یک ارتباط TCP مشاهده نمایید. تمامی تنظیمات این پنجره مانند قسمت ۸ است. با استفاده از این نمودار می‌توانید تاخیر، از دست رفتن و تداخلات در ارتباط را پیدا کنید. این نمودار توسط W. Richard Stevens پیشنهاد شده است. دقت کنید که نمودار مربوط به اندازه پنجره دریافتی است.



نمودار Sequence Numbers

به سایت دانلود دانشگاه مراجعه کنید

<http://download.aut.ac.ir/>

به‌صورت هم‌زمان دو فایل با اندازه بزرگ را دانلود کنید و در Wireshark بسته‌ها را به مدت یک دقیقه شنود کنید. به ‌عنوان مثال می‌توانید دو نسخه ویندوز

<http://download.aut.ac.ir/prg/Utility/7.iso>

<http://download.aut.ac.ir/prg/Utility/Windows.8.Enterprise.x64.iso>

را دانلود کنید. شرایط ازدحام در شبکه رخ می‌دهد. ابتدا از طریق Conversation آدرس IP سایت دانشگاه را مشخص کنید. سپس می‌توانید آن را به‌عنوان یک فیلتر اعمال کنید و نمودارهای Throughput، Windows scaling و RTT را بررسی کنید و مشخص کنید در شرایط ازدحام چه اتفاقی برای موارد بیان شده رخ می‌دهد. تغییرات را برای ده بسته قبل و بعد یک بسته دلخواه به‌صورت دقیق بررسی کنید.

از آنجایی که محیط گرافیکی ممکن است قادر به نمایش همه بسته‌ها نباشد، Wireshark را در محیط خط فرمان از طریق دستور زیر اجرا کنید. ابتدا به محل نصب Wireshark بروید و برنامه tshark که مخصوص خط فرمان است را اجرا کنید:

tshark –D

با اجرای این دستور مشاهده می‌کنید که اینترفیس‌های شما لیست می‌شوند. عدد اینترفیسی که می‌خواهید بر روی آن شنود کنید را یادداشت کنید. به فرض اینترفریس شماره 4 را انتخاب کرده‌اید. دستور زیر را اجرا کنید:

tshark –i 4 –p –w output.pcap

پس از آن بسته‌ها شنود می‌شوند. درنهایت Ctrl + C را فشار دهید و فایل output.pcap را با Wireshark باز کنید.

1. لایه شبکه
   1. آشنایی با شبیه‌ساز Boson Netsim
      1. هدف آزمایش

هدف از این آزمایش آشنایی با انجام پیکربندی اولیه مسیریاب‌ها، آدرس‌دهی پروتکل IP، تنظیمات سوییچ، آشنایی با پروتکل CDP و نحوه اتصال از راه دور به مسیریاب با استفاده از Telnet در شبیه‌ساز Boson NetSim است.

* + 1. مطالب مقدماتی

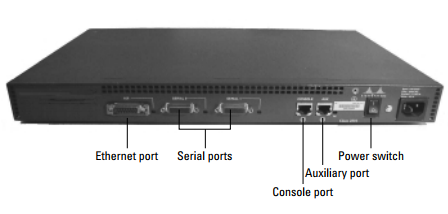
نرم‌افزار BOSON NetSim توسط شرکت BOSON ساخته شده است. مدل تجهیزات تولیدشده توسط شرکت CISCO در کتابخانه این نرم‌افزار وجود دارد. از این نرم‌افزار می‌توان برای شبیه‌سازی شبکه‌های کامپیوتری تجهیز شده توسط محصولات شرکت CISCO، استفاده کرد. همچنین می‌توان برای آموزش طراحی شبکه و پیکربندی تجهیزات CISCO از این نرم‌افزار بهره برد. این نرم‌افزار در نسخه 10 از 42 نوع مسیریاب و 7 نوع سوییچ پشتیبانی می‌کند. همچنین در هر سناریو قادر است تا 200 دستگاه را شبیه‌سازی کند. این نرم‌افزار گواهینامه‌های ICND1, ICND2, ROUTE, SWITCH, TSHOOT را پوشش می‌دهد که در ICND1 و ICND2 آزمایش‌ها به چندین دسته تقسیم می‌شوند از جمله: Stand-Alone Labs, Sequential Labs, Scenario Labs, Supplemental Labs که آزمایش‌های Standalone بدون وابستگی به آزمایش‌های قبلی اجرا می‌شوند و آزمایش Sequential نیاز به اطلاعاتی دارند که در آزمایش‌های قبلی، گفته‌شده است. با استفاده از این برنامه قادر خواهید بود علاوه بر استفاده از آزمایش‌های Standalone و Sequential به طراحی آزمایش‌های متنوع دیگر نیز بپردازید و دستورات سیستم‌عامل IOS را تمرین کنید.

برای دسترسی به محیط Cisco IOS می‌توان از CLI استفاده کرد. محیط CLI شامل چندین سطح دسترسی است و دستورات قابل اجرا در هر سطح صرفا وابسته به بستگی به سطح دسترسی‌ای که در آن قرار دارید است. با وارد کردن علامت سوال (؟) در CLI می‌توانید لیستی از دستورات موجود برای سطح دسترسی که در آن قرار دارید را به دست آورید. در ابتدا هنگام ورود به CLI، در سطح دسترسی user EXEC قرار دارید. سطح دسترسی user EXEC تنها حاوی یک زیرمجموعه محدود از دستورات است. برای دسترسی به تمام دستورات، باید به سطح دسترسی privileged EXEC وارد شوید. از سطح دسترسی privileged EXEC می‌توان وارد سطح دسترسی تنظیم Global شد. در این سطح دسترسی به عنوان مثال می‌توانید اسم دستگاه را تغییر دهید. همچنین در صورتی که بخواهید تنظیماتی برای اجزای تجهیز انجام دهید، به عنوان مثال یک آدرس IP به یک واسط اختصاص دهید، باید وارد سطح دسترسی تنظیم Interface شوید. ‏جدول (4-1) نحوه دسترسی و خروج از سطح دسترسی‌های دستوری رایج را نشان می‌دهد.

نحوه دسترسی و خروج از سطح دسترسی‌های دستوری رایج

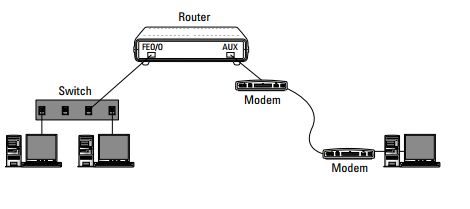
|  |  |  |
| --- | --- | --- |
| سطح دسترسی | روش ورود | نماد خط فرمان |
| User EXEC | Log in | Router> |
| Privileged EXEC | در سطح دسترسی user، از دستور enable  استفاده می‌شود | Router# |
| تنظیم Global | در سطح دسترسی privileged EXEC از دستور configure terminal استفاده می‌شود | Router(config)# |
| تنظیم Interface | در سطح دسترسی تنظیم Global، با استفاده از دستور interface  یک واسط خاص را مشخص کنید. | Router(config-if)# |

انواع مختلفی از پورت‌ها در تجهیزات ارتباطی وجود دارد که نمونه‌ای از آن‌ها در ‏شکل (4-1) نشان داده شده است. در ادامه در مورد برخی از این راه‌های ارتباطی به‌اختصار توضیحاتی ارائه می‌شود.



انواع مختلف پورت‌ها

* پورت کنسول: پورت کنسول[[26]](#footnote-26) این امکان را فراهم می‌کند که به روتر متصل شده، آن را مدیریت کرده و پیکربندی آن را تغییر دهید. برای متصل شدن به روتر از طریق پورت کنسول باید از یک کابل کنسول استفاده کرد. اتصال به پورت کنسول برای تغییر تنظیمات دستگاه، اتصال محلی به روتر نامیده می‌شود زیرا باید به‌صورت فیزیکی با روتر در ارتباط بود. هنگام اتصال محلی به روتر، کابل کنسول معمولاً از پورت سریال کامپیوتر به پورت کنسول در دستگاه متصل می‌شود. تمام پورت‌های دستگاه با یک شناسه منحصربه‌فرد[[27]](#footnote-27) که از نوع پورت و یک شاخص شماره‌گذاری ساخته شده که مشخص می‌کند به کدام پورت از آن نوع اشاره می‌شود. به عنوان مثال، پورت کنسول به عنوان console 0 یا به‌طور مختصر con 0 اشاره دارد، زیرا آن اولین پورت کنسول در روتر است.
* پورت Auxiliary: پورت auxiliary دقیقاً به عنوان یک پورت کنسول استفاده می‌شود به این معنی که به‌صورت محلی به پورت auxiliary با استفاده از کابل کنسول متصل می‌شویم. دلیل اصلی ایجاد پورت auxiliary این بود که بتوان یک مودم را به پورت auxiliary وصل کرد و سپس از راه دور به مودم متصل شده و کارهای مدیریتی را انجام داد (مانند ‏شکل (4-2)). در این صورت برای مدیریت روتر دیگر نیازی به حضور فیزیکی در کنار روتر نیست.



نحوه اتصال از طریق پورت auxiliary

* VTY: از vty[[28]](#footnote-28) برای ارتباط از راه دور از طریق پروتکل‌های SSH و TELNET استفاده می‌شود که برای کاربری که از راه دور متصل می‌شود یک ترمینال مجازی در اختیارش قرار می‌دهد.
  + - 1. انواع حافظه در تجهیزات سیسکو

یکی از مهم‌ترین جنبه‌هایی که در تجهیزات سیسکو باید درک شود بحث انواع حافظه‌ها است زیرا هر نوع حافظه یک هدف خاص را دنبال می‌کند. در ادامه این بخش انواع حافظه‌های مورداستفاده در دستگاه‌های سیسکو توضیح داده می‌شود.

* + - * 1. ROM

این نوع حافظه فقط خواندنی است که شبیه حافظه‌های ROM در کامپیوتر عمل می‌کند. این حافظه شامل کد سطح پایین مسئول راه‌اندازی دستگاه است. اجزایی هستند که در ROM ذخیره می‌شوند عبارت‌اند از:

* POST[[29]](#footnote-29) مجموعه‌ای از رویه‌ها که در هنگام راه‌اندازی برای چک کردن سخت‌افزارهای دستگاه اجرا می‌شوند.
* Bootstrap: برنامه Bootstrap یا Boot Loader بعد از POST اجرا می‌شود. هدف از برنامه Bootstrap این است که سیستم‌عامل IOS را از حافظه Flash خوانده و سپس آن را در حافظه بارگذاری کند.
* RX-boot: اگر هیچ IOS ای در حافظه Flash نباشد می‌توان از یک IOS کوچک که در ROM قرار دارد استفاده کرد. این IOS کوچک عملکرد محدودی دارد و معمولا به این صورت استفاده می‌شود که با استفاده از آن می‌توان اینترفیس‌ها را تنظیم کرد تا IOS اصلی از یک سرور TFTP در شبکه دانلود شود.
* ROM Monitor: برای رفع مشکلات مربوط به تنظیمات دستگاه استفاده می‌شود. به عنوان مثال اگر رمز عبور دستگاه را فراموش کنید می‌توانید به ROMMON بوت کنید تا پسورد را Reset کنید.
  + - * 1. Flash

سیستم‌عامل IOS در آن ذخیره می‌شود. دلیل اینک IOS در حافظه flash ذخیره می‌شود نه در ROM این است که IOSبه طور پیوسته در زمان ارتقا می‌یابد و لازم است که بتوان آن را تغییر داد. می‌توان حافظه flash را بر روی برد سیستم نصب کرد یا اینکه از یک کارت حافظه flash استفاده کرد همان‌طوری که در ‏شکل (4-3) نمایش داده شده است.

* + - * 1. VRAM

VRAM[[30]](#footnote-30) که به عنوان حافظه RAM نیز شناخته می‌شود و با قطع برق اطلاعات داخلش نیز از بین می‌رود. اصلی‌ترین اطلاعاتی که در این حافظه نگهداری می‌شودrunning configuration است که شامل تنظیمات کنونی و در حال اجرای سیستم است. به عنوان مثال: اگر نام روتر را تغییر دهیم این تغییر نام روتر در VRAM ذخیره می‌شود و اگر دستگاه را راه‌اندازی مجدد کنیم نام جدیدی که اعمال کرده بودیم حذف می‌گردد. برای اینکه این اتفاق نیفتد باید running configuration را در nonvolatile RAM ذخیره کرد. علاوه بر running configuration اطلاعات دیگری شامل کش ARP، جدول مسیریابی و جدول آدرس MAC نیز در آن ذخیره می‌شوند.



کارت حافظه Flash

* + - * 1. NVRAM

NVRAM[[31]](#footnote-31) اطلاعات را به‌صورت دائمی ذخیره می‌کند حتی اگر برق قطع شود اطلاعات داخل آن از بین نمی‌رود. اصلی‌ترین اطلاعاتی که در آن ذخیره می‌شود Startup config است. این تنظیمات به‌عنوان پیکره‌بندی راه‌انداز شناخته می‌شود و در هر بار راه‌اندازی، به دستگاه اعمال می‌شود.

* + - 1. اتصال از طریق کابل سریال

دستگاه‌هایی که به واسطه کابل سریال با یکدیگر ارتباط برقرار می‌کنند به دو دسته DCE [[32]](#footnote-32)و DTE [[33]](#footnote-33)تقسیم می‌شوند. دستگاه DCE نرخ clockبرای ارسال اطلاعات بر روی کابل را مشخص می‌کند. زمانی که یک دستگاه خارجی، مانند مودم، به یک مسیریاب متصل می‌شود، دستگاه خارجی DCE محسوب می‌شود. زمانی که از این کابل برای اتصال دو مسیریاب به یکدیگر استفاده می‌شود، هر یک از دو مسیریاب می‌تواند DCE باشد. در این صورت، بر روی کابل سمت DCE مشخص شده است و یا اگر مشخص نشده باشد می‌توان با استفاده از دستورات سیستم‌عامل IOS، سمت DCE را مشخص کرد و نرخ clock را تنظیم نمود. نرخ clock در سیستم‌عامل IOS بر اساس بیت بر ثانیه تنظیم می‌شود و بیانگر نرخ انتقال اطلاعات بر روی لینک است.

* + - 1. پروتکل CDP

پروتکل Cisco Discovery Protocol (CDP) در لایه دوم مدل هفت لایه‌ای OSI، Data Link، قرار دارد. این پروتکل توسط شرکت Cisco طراحی شده است و با استفاده از آن دستگاه‌ها بدون نیاز به داشتن آدرس IP، قادر به شناسایی همسایگان خود و به اشتراک‌گذاری اطلاعات پایه‌ای مانند نسخه سیستم‌عامل و آدرس‌های IP خواهند بود. پروتکل‌های مشابه دیگری توسط سایر سازندگان نیز پیشنهاد شده است. پروتکل LLDP، پروتکل دیگری است که بدون وابستگی به سازنده خاصی دستگاه‌ها را قادر به اشتراک‌گذاری اطلاعاتی از جمله لیست همسایگان و مشخصات در یک شبکه محلی مطابق با IEEE 802 می‌سازد.

یک تجهیز به‌صورت پیش‌فرض هر ۶۰ ثانیه پیام CDP Advertisement را ارسال می‌کند. این پیام‌ها هرگز forward نمی‌شوند و اگر سه بار به یک تجهیز پیام ارسال شده باشد و سایر تجهیزات پیامی از آن دریافت نکنند، آن تجهیز را از جدول خود حذف می‌کنند.

* + 1. قطعات و ابزارهای موردنیاز

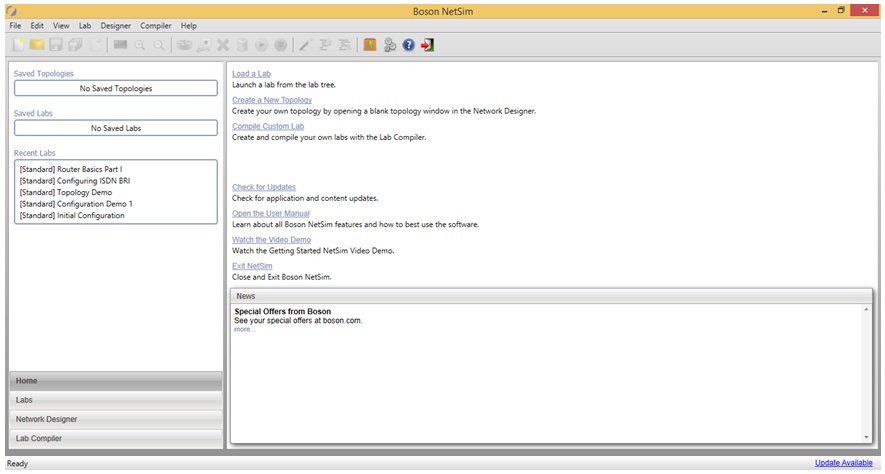
ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

* کامپیوتر شخصی با سیستم‌عامل ویندوز برای هر گروه
* شبیه‌ساز Boson نسخه 10 یا سایر شبیه‌سازهای سیستم‌عامل IOS
  + 1. شرح آزمایش

در این آزمایش ابتدا با دستورات کلی سیستم‌عامل IOS کار می‌کنید سپس نرخ clock واسط‌های سریال مسیریاب‌ها را تنظیم می‌کنید. در ادامه به واسط‌های مسیریاب‌ها آدرس IP اختصاص می‌دهید و با استفاده از جدول Host، آدرس‌های IP را به یک نام منحصربه‌فرد، نگاشت می‌کنید. در ادامه با استفاده از Telnet به یک مسیریاب متصل خواهید شد و به تنظیمات اولیه پروتکل CDP خواهید پرداخت.

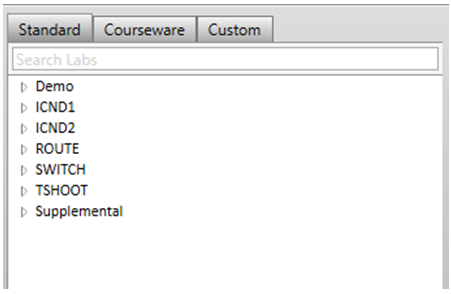
* + - 1. تنظیمات مقدماتی

1. در ابتدا برای شروع کار برنامه BOSON را باز کنید. صفحه‌ای مطابق ‏شکل (4-4) را مشاهده می‌شود:



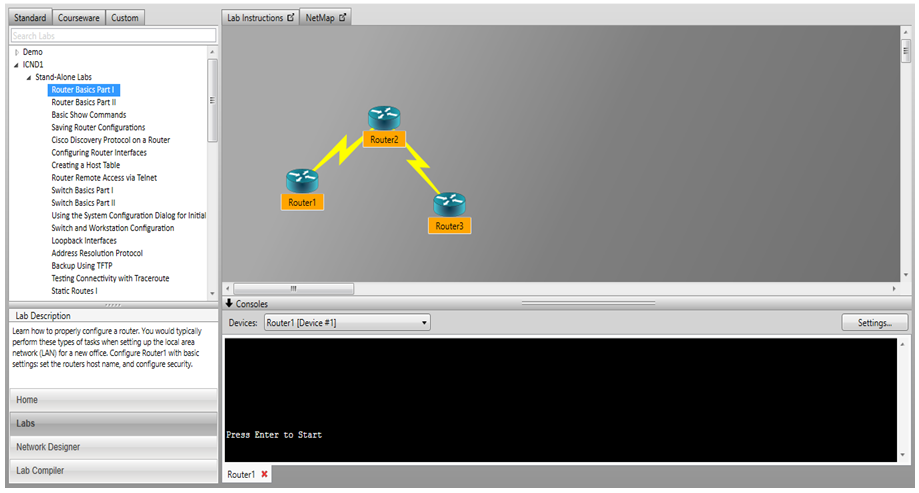
صفحه نخست Boson

1. سپس از قسمت چپ و پایین گزینه Labs را انتخاب کنید تا آزمایش‌های موجود در نرم‌افزار را مشاهده کنید. سه نوع دسته‌بندی طبق ‏شکل (4-5) برای آزمایش‌های موجود وجود دارد. دسته‌بندی Standard را انتخاب کنید که آزمایش‌ها را طبق گواهینامه‌های سیسکو مرتب می‌کند (البته Demo و Supplemental جزء گواهینامه‌ها نیست).



انواع دسته‌بندی آزمایش‌های موجود

1. در آزمایش اول برای نمونه از دسته ICND1 و از آزمایش‌های Stand-Alone، آزمایش اول یعنی Router Basics Part 1 را انتخاب کنید. بعد از انتخاب صفحه‌ای مانند ‏شکل (4-6) مشاهده می‌شود.



آزمایش اول

با انتخاب Lab Instructions دستور کار آزمایش مربوطه و توضیحات لازم نشان داده می‌شود و با انتخاب NetMap توپولوژی نمایش داده می‌شود. در قسمت پایین نیز concole ارتباطی با تجهیزات قرار دارد و از بخش Devices نیز می‌توان انتخاب کرد که کنسول کدام تجهیز باز شود. در قسمت Lab Description نیز توضیحاتی کلی در مورد آزمایش انتخاب شده نشان داده می‌شود.

1. در ابتدا ترمینال یک مسیریاب را باز کنید. سپس با نوشتن دستور enable به سطح دسترسی Privileged EXEC ورود کنید. برای خروج از این محیط می‌توانید از دستور disable استفاده کنید. برای بستن صفحه فعال از عبارتexit یا logout استفاده کنید.
2. با نوشتن یک علامت سوال (؟) می­توانید به همه­ی دستورات قابل‌استفاده دسترسی پیدا کنید و با زدن کلید فاصله (space) لیست را به طور کامل­تر مشاهده کنید.
3. با مراجعه به حالت اجرایی دارای امتیاز می‌توانید با نوشتن علامت سوال لیست دستورات را مشاهده کنید. برای مثال با تایپ دستور show ? می‌توان تمام دستوراتی را که ابتدایشان دستور show است را مشاهده کنید.

دستورات show زیر را اجرا کنید و خروجی هرکدام را در گزارش کار توضیح دهید:

show flash

show history

show terminal

show protocols

show version

show clock

show interfaces

show ip interface brief

1. با نوشتن configure terminal به حالت پیکربندی عمومی یک مسیریاب وارد شوید.
2. با استفاده از دستور host می‌توانید نام مسیریاب را تغییر بدهید. به عنوان مثال با دستور hostname Router1 اسم مسیریاب را به Router1 تغییر دهید.
3. با نوشتن دستور enable password CISCO برای ورود به سطح دسترسی Privileged EXEC، می‌توانید گذرواژه[[34]](#footnote-34) CISCO را تنظیم کنید.
4. برای آزمودن گذرواژه قرار داده شده با دستور exit خروج کرده و با دستور enable به حالت اجرایی ورود کنید؛ خواهید دید باید گذرواژه‌ای که در دستور بالا تنظیم کرده­اید را وارد کنید تا بتوانید به سیستم ورود کنید.
5. با دستور enable secret نیز می‌توان برای ورود به سطح دسترسی Privileged EXEC گذرواژه گذاشت.

تفاوت این دو روش (مرحله 9 و 11) در چیست؟

1. با استفاده از دستور show running-config تنظیمات سیستم را مرور کنید و گذرواژه‌های رمز شده را مشاهده کنید.
2. حال با استفاده از دستور service password-encryption تمام گذرواژه‌های سیستم رمز می‌شود. این دستور را اجرا کنید. سپس دستور show running-config را اجرا کرده و با خروجی قبلی مقایسه کنید.
3. با دستور show history می‌توانید آخرین دستورات وارد شده در ترمینال را که در حافظه روتر ذخیره شده است مشاهده کنید. با دستور show terminal تعداد دستوراتی را که به صورت پیش‌فرض ذخیره می‌کند را پیدا کنید سپس با استفاده از دستور history size 100 تاریخچه مسیریاب را تنظیم کنید که 100 دستور را در خود نگهداری کند.

حداکثر تعدادی که برای ذخیره دستورات می‌توان تعریف نمود چند است؟

1. می‌توانید از محیط تنظیمات عمومی با دستور line console 0 وارد تنظیمات کنسول شوید. سپس با استفاده از دستور login امکان قرار دادن پسورد بر روی محیط ورود به کنسول را فعال کنید. سپس با استفاده از دستور password BOSON گذرواژه BOSON را برای ورود به سیستم تنظیم کنید. با استفاده از دستور end و سپس دستور exit نشست فعلی شما به صورت کامل خاتمه می‌یابد. حال به سیستم ورود کنید و گذرواژه تنظیم‌شده را ارزیابی کنید.
2. وارد محیط تنظیم عمومی شوید. برای این کار ابتدا باید با استفاده از دستور enable وارد سطح دسترسی Privileged EXEC شوید، سپس با استفاده از دستور config terminal وارد محیط تنظیم Global شوید.
3. در محیط تنظیم Global با استفاده از دستور line vty 0 4 وارد محیط تنظیم ترمینال‌های مجازی شوید. سپس مانند تنظیمات کنسول، تنظیمات گذرواژه را انجام دهید.
4. با استفاده از دستور clock set hh:mm:ss day month year می‌توانید ساعت و تاریخ فعلی مسیریاب را تنظیم کنید. همچنین می­توانید پیامی را به صورت روزانه تنظیم کرد تا هر بار پس از ورود نمایش داده شود. برای این کار در محیط تنظیم عمومی دستور

banner motd #YOUR BANNER#

را اجرا کنید.

1. وارد محیط تنظیم Global شوید و سپس با دستور line console 0 وارد تنظیمات کنسول شوید و سپس با دستور login local را وارد کرده و سپس به محیط تنظیم Global برگردید و با دستور username MyName password mypasswor یک نام کاربری با رمز عبور برای ورود به سیستم تعریف کنید.
2. تنظیماتی که با دستور show running-config قابل مشاهده هستند به طور خودکار در روتر ذخیره نمی‌شوند و با قطع برق از بین می‌رود. به‌منظور ذخیره این تنظیمات در روتر از دستور copy running-config startup-config استفاده می‌شود. با دستور show startup-config نیز می‌توان تنظیمات ذخیره شده در NVRAM را مشاهده کرد.

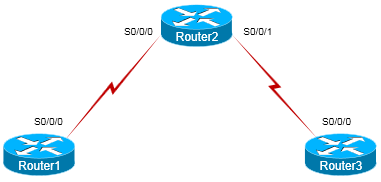
چگونه می‌توان اطلاعات ذخیره شده در NVRAM را حذف کرد؟

1. با دستور reload نیز بارگذاری مجدد می‌شود و در حین بارگذاری پیغامی مبنی برای کانفیگ مجدد نشان داده می‌شود که در صورت تایپ “yes” باید تنظیمات اولیه روتر را در این بخش وارد کنیم و در صورت وارد کردن “no” تنظیمات ذخیره شده در NVRAM بارگذاری می‌شود.

یک کاربر به نام lab3 تعریف کرده و سپس رمز 153759 را برای این کاربر تعریف کنید سپس تاریخچه دستورات ترمینال را به 50 افزایش داده و سپس ساعت روتر را به ساعت انجام آزمایش تنظیم کرده و تنظیمات جاری را در NVRAM ذخیره کرده و در پایان نیز تنظیمات اعمال شده را نمایش دهید.

* + - 1. اختصاص آدرس IP به واسط‌های شبکه

در این آزمایش، به واسط‌های مسیریاب آدرس IP اختصاص خواهد یافت. ابتدا توپولوژی مطابق با ‏شکل (4-7) ایجاد کنید. تمام واسط‌ها از نوع Serial هستند.



توپولوژی آزمایش

آدرس‌های شبکه

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Mask | IP Address | Interface | Device |
| 255.255.255.0 | 10.1.1.1 | Serial 0/0/0 | Myrouter1 |
| 255.255.255.0  255.255.255.0 | 10.1.1.2  172.16.10.2 | Serial 0/0/0  Serial 0/0/1 | Myrouter2 |
| 255.255.255.0 | 172.16.10.1 | Serial 0/0/0 | Myrouter3 |

1. با استفاده از دستور enable و سپس configure terminal وارد محیط تنظیم Global مسیریاب شوید. سپس نام مسیریاب‌ها را مطابق با ‏جدول (4-1) تغییر دهید.
2. در مسیریاب اول، از محیط کانفیگ خارج شوید و با استفاده از دستور show ip interface brief وضعیت واسط‌های مختلف را یادداشت نمایید.
3. در مسیریاب اول، وارد محیط کانفیگ شده و با استفاده از دستور interface serial 0/0/0 وارد تنظیمات واسط سریال شوید.

چه دستوراتی در این مرحله قابل اجرا است؟ آن‌ها را شرح دهید.

1. دستور no shutdown را اجرا کنید. سپس با استفاده از دستورdescription Serial interface on Router1 توضیحات نوشته شده در مقابل دستور descrirption یعنی Serial interface on Router1 را به این واسط اضافه کنید. با استفاده از دستورshow interface serial 0/0/0 می‌توانید توضیحات اضافه شده را مشاهده کنید.
2. در مسیریاب اول با استفاده از دستور end از محیط تنظیمات خارج شوید. دو پیغام پشت سر هم نمایش داده می‌شود که در یکی up شدن واسط و در دیگری down شدن آن عنوان شده است.

با استفاده از دستور show ip interface brief توضیح دهید که چرا واسط ابتدا up می‌شود و سپس down می‌شود.

1. با استفاده از دستور show interfaces serial 0/0/0 توضیحات اضافه شده به این واسط را مشاهده کنید.
2. به ترمینال مسیریاب Router2 بروید. مراحل 24 و 25 را تکرار کنید.
3. با استفاده از دستور end از محیط تنظیمات خارج شوید.

با استفاده از دستورshow ip interface brief توضیح دهید چرا برای مسیریاب Router1 وRouter2 وضعیت administrator status در حالت up است ولی Line Protocol در حالت down است.

1. مراحل 24 و 25 را برای واسط دوم Router2 نیز اجرا کنید.
2. مراحل 24 و 25 را برای مسیریاب Router3 نیز اجرا کنید.

بر روی مسیریاب Router2 دستور show controller را اجرا کنید. در توضیحات نمایش داده شده DCE cable را جستجو کنید. آیا Router2 سمت DCE به حساب می‌آید؟

1. پس از مشخص شدن سمت DCE کابل سریال، با استفاده از دستور configure terminal و سپس interface serial 0/0/0 به تنظیم واسط مسیریاب بروید. سپس با استفاده از دستورclock rate 1000000 نرخ کلاک را تنظیم کنید. سپس DCE دوم را انتخاب کنید و دوباره با دستور clock rate 1000000 نرخ کلاک را تنظیم کنید.

حال بر روی مسیریاب Router1 و Router3 دستور show ip interface brief را اجرا کنید و توضیح دهید که چرا Line Protocol در حالت up است.

توضیح دهید که چرا همیشه نیاز به اجرای دستور clock rate نداریم و صرفا دستور no shutdown کافی است؟

1. در مسیریاب Router1 با استفاده از دستورات enable و configure terminal وارد محیط تنظیم عمومی شوید. سپس با استفاده از دستور interface serial 0/0/0 وارد تنظیمات واسط شبکه شوید.
2. با استفاده از دستور ip address 10.1.1.1 255.255.255.0 آدرس IP به این واسط اختصاص دهید.
3. مرحله 33 را برای مسیریاب Router2 تکرار کنید.
4. با استفاده از دستور ip address 10.1.1.2 255.255.255.0 به واسط اول این مسیریاب آدرس IP اختصاص دهید.
5. با استفاده از دستور interface serial 0/0/1 به تنظیم واسط دوم Router2 بروید و سپس با استفاده از دستور ip address 172.16.10.2 255.255.255.0 به آن آدرس IP اختصاص دهید.
6. مرحله 33 را برای مسیریاب سوم تکرار کنید. سپس با استفاده از دستور ip address 172.16.10.1 255.255.255.0 به آن آدرس IP اختصاص دهید.
7. از محیط تنظیمات هر سه ترمینال با استفاده از دستور end خارج شوید.

در Router 1 با استفاده از دستور ping آدرس 10.1.1.2 را ping کنید. چه اتفاقی می‌افتد؟

در Router 2 با استفاده از دستور ping آدرس 172.16.10.1 را ping کنید. چه اتفاقی می‌افتد؟

1. دستور show ip interface brief را بر روی مسیریاب Router2 اجرا کنید و خروجی را یادداشت کنید.
2. در مسیریاب Router2 از محیط تنظیمات با استفاده از دستور end خارج شوید. سپس با استفاده از دستور configure terminal وارد محیط تنظیمات عمومی شوید.
3. با استفاده از دستور ip host router1 10.1.1.1 آدرس router1 را به جدول Host مسیریاب اضافه کنید. به خاطر سپردن آدرس‌های IP کار سختی است؛ بنابراین از جدول Host استفاده می‌کنیم که در آن آدرس‌های IP به اسامی نگاشته می‌شوند. در این صورت، به‌جای مشخص کردن آدرس IP، صرفا به کار بردن اسم متناظر با آدرس، کافی خواهد بود.
4. با استفاده از دستور end از محیط تنظیمات خارج شوید. سپس با استفاده از دستور ping router1، مسیریاب router1 را ping کنید.
5. خروجی دستور show hosts بر مسیریاب router2 را یادداشت کنید.
   * + 1. اتصال به مسیریاب از طریق Telnet
6. با استفاده از دستور configure terminal به محیط تنظیمات عمومی مسیریاب Router1 بروید.
7. با استفاده از دستور line vty 0 4 وارد تنظیمات ترمینال مجازی بشوید.
8. دستور login و سپس دستور password test را اجرا کنید. با استفاده از دستور end از محیط تنظیمات خارج شوید.
9. در مسیریاب router2 دستور 10.1.1.1 telnet را اجرا کنید. پسورد تنظیم شده را وارد کنید.
10. هر زمان که خواستید نشست فعلی را متوقف کنید، کلیدهای Ctrl+Shift+6 را هم‌زمان فشار دهید سپس رها کرده و بلافاصله X را فشار دهید.
11. در مسیریاب Router2 با استفاده از دستور show sessions لیست نشست‌های فعلی را مشاهده کنید. با استفاده از دستور resume 1 که عدد 1 بیانگر شماره نشست در خروجی دستور show sessions است، نشست را ادامه دهید. با دستور disconnect 1 هم می‌توان نشست را خاتمه داد.
    * + 1. تنظیمات پروتکل CDP
12. در مسیریاب Router2 دستور show cdp interface را اجرا کنید. زمان ارسال بسته‌های CDP چقدر است؟
13. دستور show cdp neighbors را بر روی مسیریاب Router2 اجرا کنید. در خروجی، ستون Hold time به معنی زمانی است که اگر به‌روزرسانی دریافت نشود آن سطر پاک خواهد شد.

سایر ستون‌های خروجی را شرح دهید.

1. با استفاده از دستور show cdp neighbors detail جزییات پروتکل CDP را مشاهده کنید.

چه اطلاعاتی توسط پروتکل CDP منتقل شده است؟

1. بر روی مسیریاب Router3 دستور show cdp neighbors را اجرا کنید. خروجی را یادداشت کنید.
2. در مسیریاب router2 با استفاده از دستور configure terminal وارد محیط تنظیمات کلی شوید. سپس با استفاده از دستور cdp timer 45 زمان ارسال بسته‌های cdp را به 45 ثانیه تغییر دهید.
3. با استفاده از دستور cdp holdtime 60 زمان hold time را به 60 ثانیه تغییر دهید.
4. با استفاده از دستور end از محیط تنظیمات کلی خارج شود. سپس دستور show cdp را اجرا کنید و خروجی را یادداشت نمایید.
5. با استفاده از دستور configure terminal و سپس interface serial 0/0/1 وارد تنظیمات واسط سریال بر روی مسیریاب Router2 شوید. سپس با استفاده از دستور no cdp enable پروتکل cdp را بر روی این واسط غیرفعال کنید (ا استفاده از دستور cdp enable می‌توان cdp را دوباره فعال کرد).
6. با استفاده از دستور end از محیط تنظیمات خارج شوید.
7. پس از گذشت چند دقیقه بر روی مسیریاب Router3 دستور show cdp neighbors را اجرا کنید. خروجی را تفسیر کنید.
   1. آشنایی با مکانیسم NAT و پروتکل DHCP
      1. هدف آزمایش

هدف از انجام این آزمایش آشنایی با آدرس‌دهی شبکه برای استفاده از سرویس‌های اینترنت است. بدین منظور عملکرد و پیکربندی مکانیسم NAT، PAT و پروتکل DHCP بررسی می‌شود.

* + 1. مطالب مقدماتی

مکانیسم NAT برای تبدیل یک فضای آدرس IP به یک فضای آدرس دیگر انجام می‌شود. یکی از کاربردهای مهم این مکانیسم در تبدیل آدرس خصوصی و عمومی به یکدیگر است که برای دسترسی سیستم‌های با آدرس IP خصوصی به شبکه اینترنت ضروری است.

در NAT آشنایی با مفاهیم آدرس IP خصوصی[[35]](#footnote-35) یا غیر معتبر[[36]](#footnote-36) و آدرس IP عمومی یا معتبر از اهمیت ویژه‌ای برخوردار است. طبق RFC 1918، آدرس‌های IP خصوصی، آدرس‌هایی هستند که به‌وسیله شبکه‌هایی که مستقیما به اینترنت متصل نیستند، استفاده می‌شوند. در RFC6890 لیستی از آدرس‌های IP خصوصی و نحوه برخورد با آن‌ها ارائه شده است. به منظور اینکه سیستم‌ها با آدرس شبکه‌های خصوصی به اینترنت متصل شوند می‌بایست از NAT استفاده شود. آدرس‌های IP خصوصی در اینترنت قابل مسیریابی نیستند و معمولا توسط ISP[[37]](#footnote-37) ها فیلتر می‌شوند. یک آدرس IP عمومی در اینترنت قابل مسیریابی است. سازمان IANA[[38]](#footnote-38) مسئول اختصاص آدرس IP عمومی در اینترنت است. سازمان IANA نیز این مسئولیت را به سازمان‌های محلی واگذار می‌کند، به عنوان مثال ARIN[[39]](#footnote-39) مسئول تخصیص آدرس‌های IP عمومی در آمریکای شمالی است.

مکانیسم NAT، یک آدرس (معمولا آدرس مبدا) در سرآیند بسته‌ها با یک آدرس دیگر (معمولا آدرس عمومی) جایگزین می‌کند. این مکانیسم معمولا در دیواره آتش شبکه پیاده‌سازی می‌شود. در حالت کلی، سه روش برای پیاده‌سازی NAT وجود دارد.

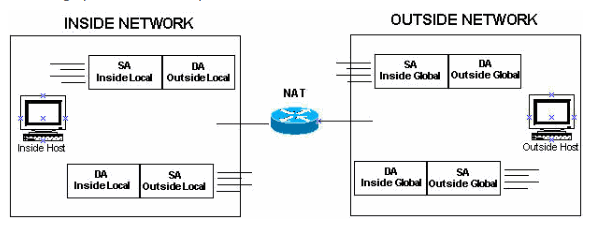
* Static: در این حالت یک نگاشت یک‌به‌یک و ثابت بین آدرس‌های اصلی و مپ شده وجود دارد. در این حالت اگر ده آدرس خصوصی داشته باشید، نیاز به ده آدرس عمومی خواهید داشت.
* Dynamic: در این حالت دستگاه‌ها در شبکه داخلی، به‌صورت خودکار از یک pool آدرس عمومی، آدرس دریافت می‌کنند.
* Oveload: در این حالت، یک بازه از آدرس‌های خصوصی، به یک آدرس عمومی مپ می‌شوند. در این حالت برای اینکه مسیریاب قادر به تفکیک درخواست‌ها باشد، شماره پورت موجود دربسته‌ها را نیز با یک شماره پورت دیگر عوض کرده و نگاشتی از این تعویض پورت نگهداری می‌کند.

در کتب درسی، هر سه این مکانیسم‌ها به صورت یکپارچه با نام NAT شناخته می‌شود.

در مکانیسم NAT آدرس‌های مختلفی ممکن است به دستگاه‌ها تعلق بگیرد که عبارت‌اند از:

* Inside Local: آدرس IP خصوصی یک دستگاه در شبکه داخلی.
* Inside Global: آدرس IP عمومی یک دستگاه در شبکه داخلی. این آدرس، می‌تواند آدرسی باشد که آدرس خصوصی به آن مپ شده است.
* Outside Local: آدرس IP یک دستگاه در شبکه خارجی که برای شبکه داخلی قابل رویت است. این آدرس الزاما یک آدرس عمومی نیست ولی لزوما باید قابل مسیریابی در شبکه داخلی باشد. در حالتی که از NAT برای آدرس‌های مقصد استفاده شود این آدرس می‌تواند با آدرس Outside Global متفاوت باشد. در غیر این صورت مقدار آن برابر Outside Global است.
* Outside Global: آدرس IPعمومی یک دستگاه در شبکه خارجی.

روند کلی تغییر آدرس‌ها را در ‏شکل (4-8) مشاهده می‌کنید.



روند کلی تغییر آدرس‌ها

در این حالت مسیریاب هم‌زمان آدرس مبدا و آدرس مقصد بسته را ترجمه می‌کند. در این آزمایش صرفا به تغییر آدرس مبدا بسته خواهیم پرداخت.

مراحل تنظیم NAT به صورت پویا عبارت است از:

1. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
2. ایجاد یک pool آدرس عمومی که می‌تواند به صورت پویا به آدرس‌های شبکه خصوصی اختصاص یابد.
3. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
4. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
5. تنظیم دسترسی ACL برای استفاده از NAT و pool ایجاد شده.

در این حالت به راحتی می‌توان مشاهده کرد که آدرس‌های Inside local به چه آدرس Inside global مپ شده و به چه آدرس outside global متصل شده است.

برای تنظیم مپ کردن به صورت ایستا نیازی به تعریف ACL ندارید. مراحل تنظیم NAT ایستا عبارت است از:

1. به‌صورت ایستا، برای هر آدرس داخلی یک آدرس خارجی تعریف کنید.
2. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
3. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.

در این حالت ازآنجایی‌که نشست‌ها به صورت پویا برقرار نمی‌شوند، اطلاعات نشست شامل اینکه آدرس داخلی به چه آدرس outside global متصل شده است وجود نخواهد داشت.

همان‌گونه که توضیح داده شد، مکانیسم‌های NAT توضیح داده شده نیاز به تعداد زیادی آدرس عمومی دارند تا بتواند تبدیل آدرس را انجام دهد. با توجه به محدودیت آدرس‌های IPv4، نیاز به مکانیسم دیگری احتیاج می‌شود که آدرس‌های خصوصی را به تعداد محدودی آدرس عمومی نگاشت کند. این مکانیسم که بخش دیگری از مکانیسم NAT است از تبدیل پورت مبدا در سرآیند بسته استفاده می‌کند و با نام PAT نیز شناخته می‌شود. همان‌طور که میدانید، در سرآیند TCP و UDP آدرس پورت مبدا و مقصد نیز وجود دارد. در این مکانیسم علاوه بر تبدیل آدرس در سرآیند IP، آدرس پورت مبدا نیز در سرآیند TCP و UDP نیز با یک مقدار یکتای دیگر جایگزین می‌شود. این مقدار، به یک پورت بر روی دستگاهی که مکانیسم PAT را پیاده‌سازی کرده اشاره می‌کند؛ بنابراین همه دستگاه‌های شبکه داخلی می‌توانند صرفا یک آدرس global local داشته باشند و با استفاده از پورت از یکدیگر تشخیص داده شوند.

مراحل تنظیم PAT عبارت است از:

1. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
2. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
3. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
4. تنظیم دسترسی ACL برای استفاده از PAT: به این صورت که یک اینترفیس باید به صورت overload مشخص شود.

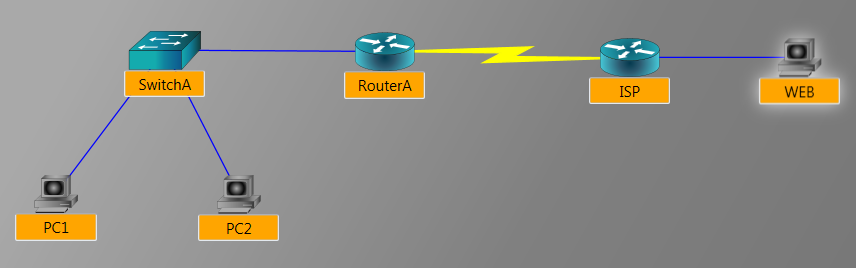
به عنوان یک مثال کلی، هنگامی‌که بسته SYN به سمت دروازه شبکه فرستاده می‌شود، دستگاه NAT آدرس IP و شماره پورت در سرآیند TCP را با آدرس IP عمومی و یک شماره پورت یکتا عوض می‌کند و بسته را به سمت شبکه عمومی ارسال می‌کند. در جواب اگر آدرس پورت مقصد بسته در جدول دستگاه NAT وجود داشته باشد، تبدیل آدرس دوباره انجام می‌شود و بسته به شبکه داخلی ارسال می‌شود.

* + 1. شرح آزمایش

در ابتدا به بررسی مکانیسم NAT می‌پردازیم و با تنظیمات NAT پویا، NAT ایستا و PAT آشنا خواهیم شد. سپس پروتکل DHCP را موردبررسی قرار خواهیم داد

* + - 1. مکانیسم NAT

توپولوژی که در این آزمایش بررسی می‌شود در ‏شکل (4-9) نشان داده است. آدرس‌های IP واسط‌ها در این آزمایش در ‏جدول (4-3) آمده است.



توپولوژی آزمایش NAT

آدرس‌های موردنیاز آزمایش NAT

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| RouterA | FastEthernet 0/0  Serial 0/0 | 192.168.100.1  200.152.200.2 | 255.255.255.0  255.255.255.252 |
| ISP | FastEthernet 0/0  Serial 0/0 | 25.16.59.1  200.152.200.1 | 255.255.255.252  255.255.255.252 |
| Device | IP Address | Subnet Mask | Default Gateway |
| PC1 | 192.168.100.2 | 255.255.255.0 | 192.168.100.1 |
| PC2 | 192.168.100.129 | 255.255.255.0 | 192.168.100.1 |
| Web | 25.16.59.2 | 255.255.255.252 | 25.16.59.1 |

* + - * 1. مکانیسم NAT ایستا

1. واسط‌های دستگاه‌ها مطابق آدرس‌های داده شده در ‏جدول (4-3) تنظیم شده است. آیا PC1 و PC2 قادر به Ping کردن یکدیگر هستند؟ چرا؟ آیا از PC1 می‌توانید ISP را Ping کنید؟ چرا؟
2. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار، ابتدا از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet 0/0 شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial 0/0 شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

1. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفا آدرس IP مبدا در بسته خروجی از شبکه تغییر می‌کند.

ip nat inside source static 192.168.100.2 200.152.200.1

از PC1 و PC2 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

با استفاده از دستور

show ip nat translations

جدول NAT در RouterA را مشاهده کنید و آن را شرح دهید.

* + - * 1. مکانیسم NAT پویا

1. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار ابتدا وارد محیط تنظیمات عمومی شوید. سپس با استفاده از دستور

access-list 1 permit 192.168.100.0 0.0.0.255

1. یک لیست دسترسی ایجاد کنید.

این لیست چه کاری انجام می‌دهد.

1. در ادامه یک pool آدرس تعریف کنید. دستور زیر را وارد کنید.

ip nat pool pool1 200.152.100.65 200.152.100.70 netmask 255.255.255.248

این دستور چه کاری انجام می‌دهد؟

1. از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet 0/0 شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial 0/0 شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

1. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید.

ip nat inside source list 1 pool pool1

از PC2 , PC1 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

1. با استفاده از دستور

show ip nat translations

جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

* + - * 1. مکانیسم PAT

1. بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار ابتدا وارد محیط تنظیمات عمومی شوید. سپس با استفاده از دستور

access-list 2 permit 192.168.1.0 0.0.0.255

یک لیست دسترسی ایجاد کنید.

این لیست چه کاری انجام می‌دهد؟

1. از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet 0/0 شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial 0/0 شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

1. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید.

ip nat inside source list 2 interface serial 0/0 overload

از PC1 و PC2 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

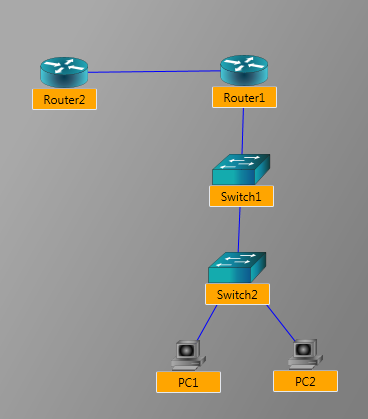
با استفاده از دستور

show ip nat translations

جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

* + - 1. پروتکل DHCP

توپولوژی که در این آزمایش بررسی می‌شود در ‏شکل (4-10) نشان داده است.



توپولوژی آزمایش DHCP

آدرس‌های IP واسط‌های مسیریاب Router1 در این آزمایش در ‏جدول (4-4) آمده است

آدرس‌های موردنیاز آزمایش DHCP

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| Router1 | Fastethernet 0/1  Fastethernet 0/0 | 180.10.1.2  192.168.1.1 | 255.255.255.0  255.255.255.0 |

1. واسط‌های مسیریاب Router1 را مطابق اطلاعات آدرس‌های داده شده تنظیم کنید.
2. در محیط تنظیم عمومی مسیریاب Router1 با استفاده از دستور

service dhcp

سرویس DHCP را فعال کنید. سپس با استفاده از دستورهای

ip dhcp excluded-address 180.10.1.2

ip dhcp excluded-address 192.168.1.1

آدرس‌های مربوط به اینترفیس‌های فعلی مسیریاب را از لیست اختصاص آدرس‌های DHCP خارج کنید.

1. در محیط تنظیم عمومی، با استفاده از دستور

ip dhcp pool pool1

وارد تنظیم DHCP شوید. سپس با استفاده از دستور

network 192.168.1.0 255.255.255.0

lease 2

آدرس شبکه و زمان رهاسازی آدرس اختصاص‌یافته را مشخص کنید. در مقابل دستور lease ابتدا روز، سپس ساعت و دقیقه می‌تواند قرار بگیرد؛ بنابراین lease 2 4 به معنی دو روز و چهار ساعت است.

در ادامه با استفاده از دستور

default-router 192.168.1.1

آدرس دروازه پیش‌فرض برای کسانی که از این سرور DHCP استفاده می‌کنند را مشخص کنید.

1. بر روی سیستم PC1 دستور

ipconfig /ip dhcp

را وارد کنید. خروجی دستور

ipconfig /all

را مشاهده کنید.

1. بر روی مسیریاب Router1 دستور

show ip dhcp binding

را اجرا کنید و خروجی را مشاهده کنید.

1. بر روی مسیریاب Router1 دستور

show ip dhcp server statistics

را اجرا کنید و خروجی را مشاهده کنید.

1. بر روی مسیریاب Router1 دومین Pool را نیز تنظیم کنید. در محیط تنظیم عمومی، با استفاده از دستور

ip dhcp pool pool2

وارد تنظیم DHCP شوید. سپس با استفاده از دستور

network 180.10.1.2 255.255.255.0

lease 2

1. دومین pool را نیز تنظیم کنید.
2. در مسیریاب Router2، وارد محیط تنظیم واسط fastethernet0/0 شوید. ابتدا با دستور

no shut

واسط را فعال کنید. سپس با دستور

ip dhcp client lease 1

تنظیم کنید که مسیریاب، آدرس DHCP را با مقدار lease 1 درخواست کند. سپس با دستور

ip address dhcp

تنظیم آدرس واسط مسیریاب را در حالت DHCP قرار دهید.

در مسیریاب Router2 از محیط تنظیمات خارج شوید. با استفاده از دستور

Show dhcp lease

مشخص کنید زمان‌های lease، Renewal و Rebind چقدر هستند و چه ارتباطی با یکدیگر دارند.

* 1. آشنایی با شبیه‌ساز GNS3
     1. هدف آزمایش

هدف از انجام این آزمایش آشنایی با شبیه‌ساز GNS3 به‌منظور شبیه‌سازی عملکرد مسیریاب‌ها و سوییچ‌های سیسکو و آشنایی با مسیریابی ایستا و نحوه کار پروتکل مسیریابی RIPv2 است.

* + 1. مطالب مقدماتی

در این بخش ابتدا به معرفی کلی برنامه GNS3 پرداخته می‌شود.

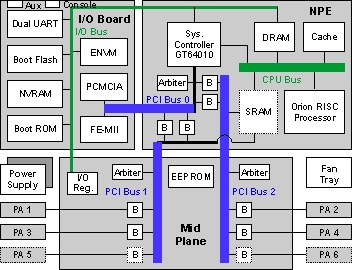
* + - 1. معرفی GNS3

GNS3 برنامه‌ای متن‌باز همراه با محیطی گرافیکی برای شبیه‌سازی واقعی شبکه‌های پیچیده است. این نرم‌افزار با استفاده از Dynamips می‌تواند سیستم‌عامل IOS (سیستم‌عامل مخصوص مسیریاب‌ها و سوئیچ‌های cisco) را اجرا کند. همچنین از Dynagen به‌عنوان یک واسط کاربری مبتنی بر متن برای ارتباط با Dynamips استفاده می‌شود. برای سهولت در شبیه‌سازی یک شبکه واقعی در GNS3 مدل‌های زیادی از تجهیزات شبکه در کتابخانه این نرم‌افزار موجود است.

Dynamips هر لینک را به یک پورت UDP نگاشت می‌کند. BaseUDPآدرس شروع پورت‌های UDP ای است که لینک‌های شبکه ساخته شده در محیط GNS3 به آن‌ها نگاشت می‌شوند. کنسول هر یک از دستگاه‌ها به یک پورت TCP نگاشته می‌شود. Base Console آدرس شروع پورت‌های TCP است که کنسول‌های هرکدام از دستگاه‌های شبکه به آن نگاشت می‌شوند.

ازآنجایی‌که در این آزمایش در Image مربوط به مسیریاب‌های سری 7200 سیسکو استفاده می‌شود لازم است در مورد معماری کلی آن اطلاعاتی داشته باشید. از مسیریاب‌های سری 7200، GNS3 صرفا از مسیریاب 7206VXR پشتیبانی می‌کند. معماری کلی سری 7200 در ‏شکل (4-11) مشاهده می‌شود.

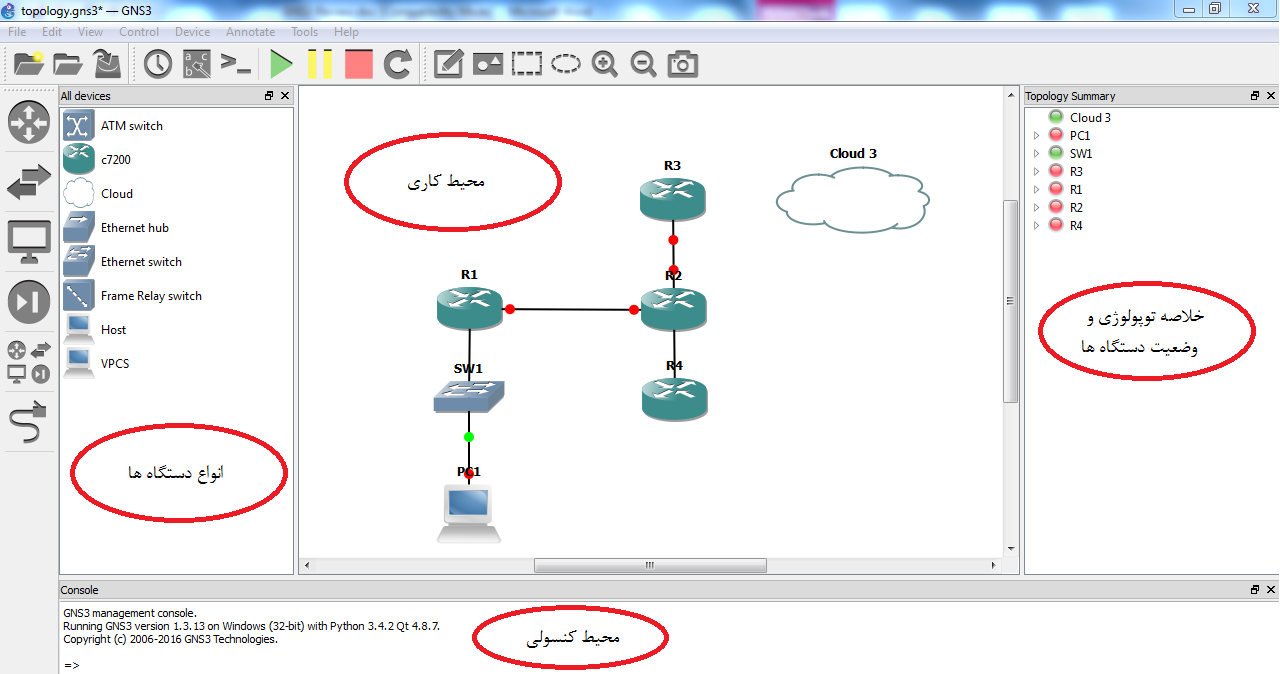
مهم‌ترین بخش‌های این معماری، NPE، I/O Board، اسلات‌های Port Adapter که با PA مشخص شده‌اند هستند. NPE وظیفه پردازش بسته‌ها را بر عهده دارد و شامل پردازنده و حافظه اصلی است. وابسته به امکانات و نرخ کلاک، مدل‌های مختلفی برای NPE وجود دارد. GNS3 از NPE400 به صورت پیش‌فرض پشتیبانی می‌کند که نرخ کلاک آن MHz350 است. اگر به بخش‌های مختلف I/O Board که در تنظیمات مسیریاب در GNS3 با Slot0 در هر مسیریاب شناخته می‌شود، در شکل بالا نگاه کنید، مولفه‌های NVRAM، Boot Flash، Boot ROM و پورت‌های کنسول و AUX را مشاهده خواهید کرد. اگرچه I/O Board می‌تواند هیچ پورتی برای ارتباط با صفحه داده نداشته باشد ولی می‌توان تا دو پورت Fast Ethernet و یا یک پورت Gigabit Ethernet نیز به آن اضافه کرد که در تنظیمات GNS3 اجباری است. درنهایت Port Adapter ها اینترفیس کنترلر هستند و می‌توانند تعداد دلخواهی پورت به مسیریاب اضافه کنند. PA ها را در زمان کارکرد مسیریاب جایگزین کرد و Hot Swappable هستند.



معماری کلی سری 7200

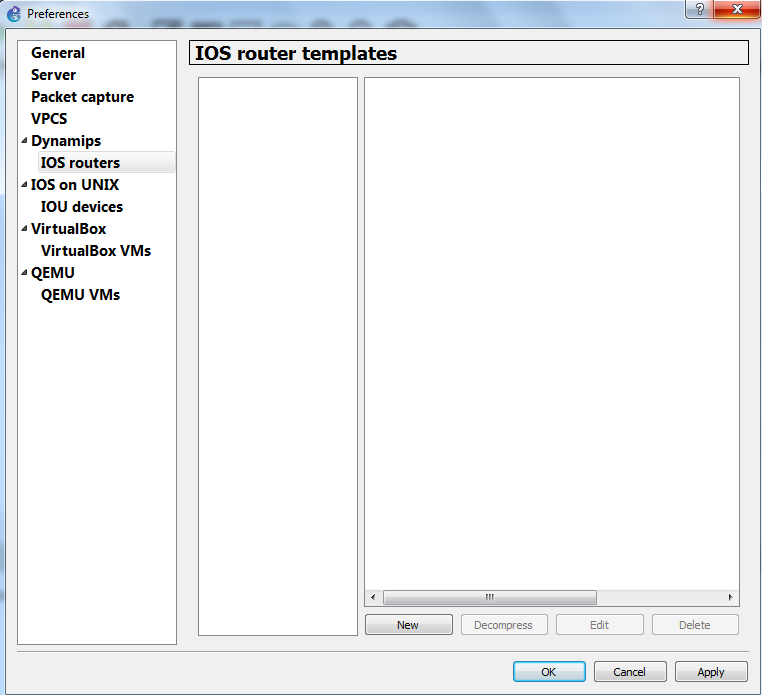
‏شکل (4-12) نمایی از واسط گرافیکی نرم‌افزار GNS3 است. واسط کاربری GNS3 از قسمت‌های زیر تشکیل شده است:

* محیط کاربری**:** در این قسمت می‌توان با اضافه کردن انواع سوییچ‌ها و مسیریاب‌ها، شبکه موردنظر خود را طراحی نمود.
* انواع دستگاه‌ها: در این بخش انواع دستگاه‌های شبکه که توسط GNS3 پشتیبانی و مدل شده‌اند را می‌توان مشاهده نمود. برای انتخاب هر دستگاه، ابتدا سیستم‌عامل مخصوص آن باید به محیط GNS3 اضافه شده باشد. سپس با عمل کشیدن و رها کردن می‌توان دستگاه موردنظر را به محیط کاربری اضافه نمود.
* خلاصه توپولوژی شبکه: در این بخش می‌توان خلاصه دستگاه‌های موجود در شبکه، وضعیت خاموش، روشن بودن آن‌ها و همچنین نحوه اتصال این دستگاه‌ها به یکدیگر را مشاهده نمود.
* محیط کنسولی: در این قسمت می‌توان از طریق کنسول و دستورات Dynagen با Dynamips ارتباط داشت و کارهایی از قبیل توقف شبیه‌سازی، اجرای دوباره شبیه‌سازی، عیب‌یابی و ... توسط این بخش انجام می‌شود.



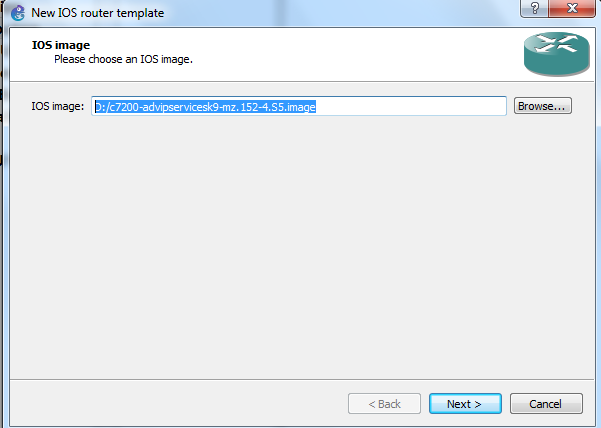
نمایی از واسط گرافیکی نرم‌افزار GNS3

برای استفاده از این نرم‌افزار باید پس از نصب، تنظیمات لازم انجام شوند. این تنظیمات شامل اضافه کردن یک Image مربوط به سیستم‌عامل IOS است. بدین منظور پس از نصب از منوی Edit، گزینه Preference را انتخاب کنید. سپس از صفحه باز شده، مطابق با ‏شکل (4-13) از بخش Dynamips زیر بخش IOS Routers را انتخاب کنید.



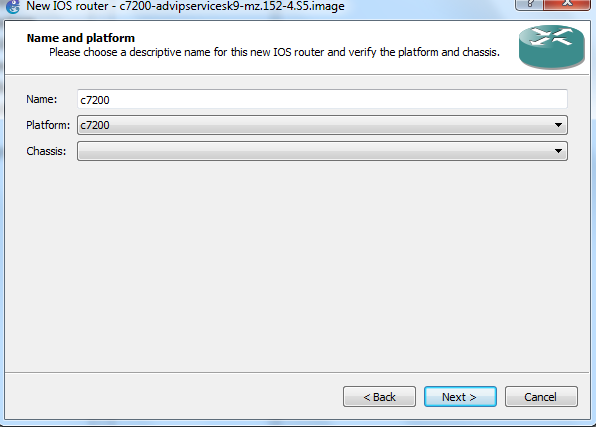
صفحه تنظیمات GNS3

سپس بر روی گزینه New کلیک کرده و مانند ‏شکل (4-14) آدرس Image مربوطه را به برنامه بدهید.



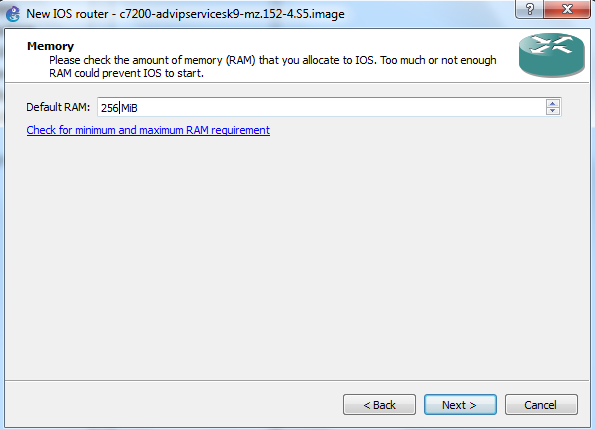
وارد کردن آدرس Image مربوطه

بر روی دکمه Next کلیک کنید. مرحله بعدی در ‏شکل (4-15) نشان داده شده است. ازآنجایی‌که Image اضافه شده مربوط به سری 7200 مسیریاب‌های سیسکو بوده است، این گزینه به‌صورت پیش‌فرض انتخاب شده است. بر روی دکمه Next کلیک کنید.



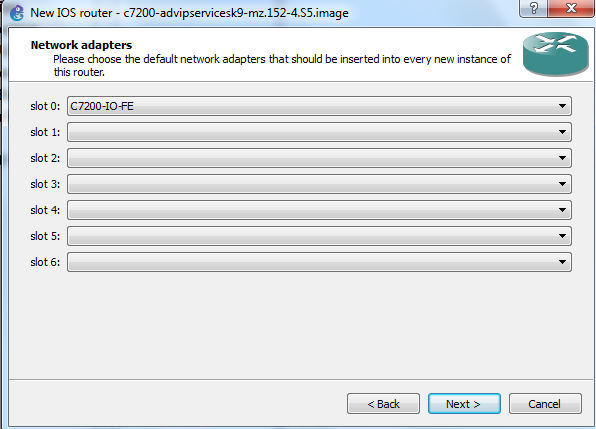
انتخاب نام Image

مطابق ‏شکل (4-16) مقدار رم موردنیاز برای هر نمونه IOS را برابر 256 مگابایت قرار دهید.



مشخص کردن میزان RAM موردنیاز برای هر نمونه IOS

برای هر مسیریابی، باید مشخص کنید که IO Controller آنچه واسط‌هایی دارد. به طور مثال در ‏شکل (4-17) انتخاب شده است که به هر مسیریاب یک IO Controller که دارای یک پورت Ethernet Fast است اضافه شود. انتخاب گزینه C7200-IO-2FE منجر به اضافه شدن دو پورت Fast Ethernet می‌شود.



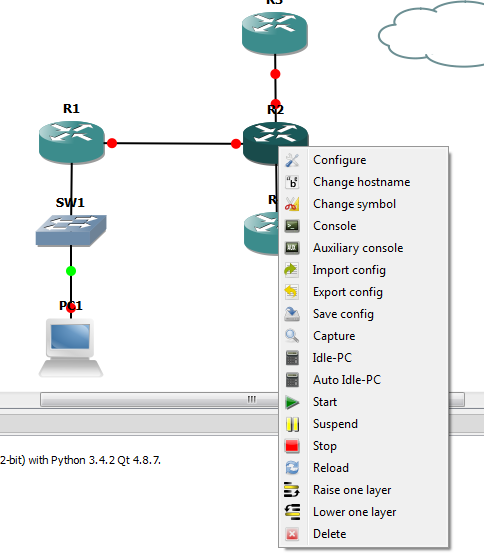
مشخص کردن واسط‌های IO Controller مسیریاب

سپس باید مقدار Idle-PC انتخاب شود. مطابق ‏شکل (4-18) بر روی finder Idle-PC کلیک کنید و پس از یافتن مقدار مناسب بر روی Finish کلیک نمایید.



مشخص کردن میزان Idle-PC

پس از اتمام تنظیمات می‌توانید با استفاده از ستون سمت چپ در شبیه‌ساز (قسمت انواع دستگاه­ها) مسیریاب‌ها و سوییچ‌های موردنیاز را با استفاده از کشیدن و رها کردن به توپولوژی شبکه اضافه کنید. اگر بر روی هر مسیریاب، راست کلیک کنید منوی مانند آنچه در ‏شکل (4-19) نشان داده شده است را مشاهده می‌کنید.

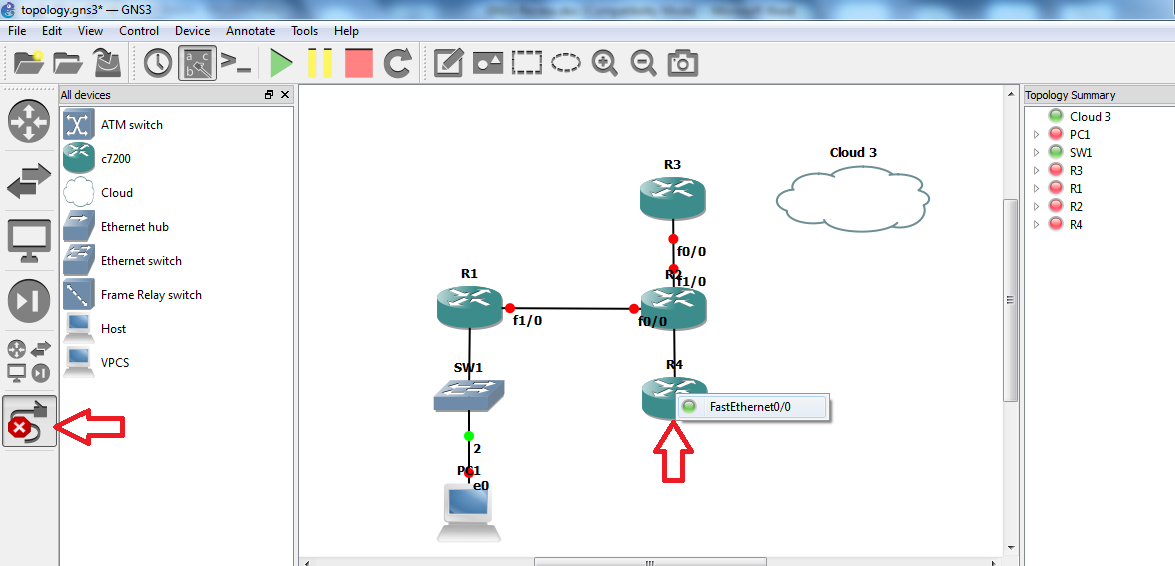


منوی در دسترس هر دستگاه

نکات مهمی که در این منو وجود دارد به شرح زیر است:

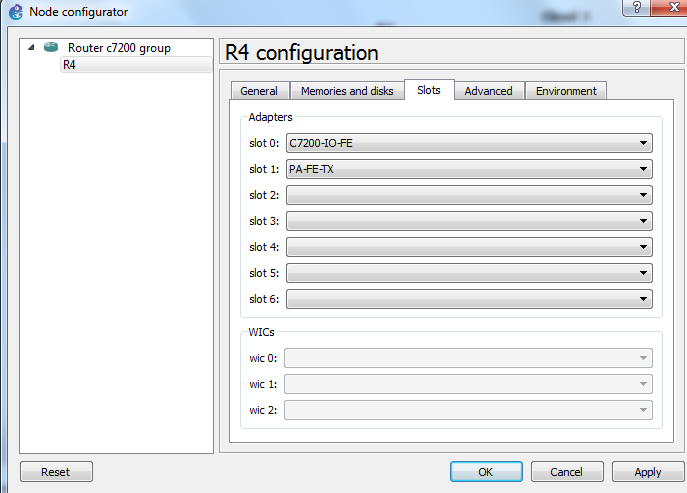
* Configure: با استفاده از این قسمت قادر خواهید بود مشخصات سخت­افزاری دستگاه (مقدار رم مصرفی، تعداد اسلات‌ها، تعداد کارت‌های شبکه و ...) را تغییر دهید.
* Console: با استفاده از console می‌توانید به محیط خط فرمان دستگاه دسترسی پیدا کنید. این همان محیط خط فرمانی است که در شبیه‌سازهای دیگر نیز مشاهده می­کنید.
* Capture: با مشخص کردن واسط و مقصد بسته‌ها، می‌توان بسته‌هایی که از دستگاه عبور می‌کند را شنود کرده و با استفاده از Wireshark، مشاهده نمود.
* Start**،** Stop**،**Suspend**،** Reload: برای راه‌اندازی مسیریاب، روشن، خاموش، غیرفعال کردن دستگاه و راه‌اندازی دوباره مورداستفاده قرار می‌گیرند.
* IdlePC: مقداری است که حدس زده می‌شود برابر idle loop دستگاه است؛ یعنی قسمتی از کد که دستگاه در صورت بیکار بودن در داخل آن loop قرار می‌گیرد و کاری را انجام نمی‌دهد. GNS3 با حدس زدن مقادیر مختلف سعی در پیدا کردن این مقدار در image داده شده می‌کند و با استفاده از آن هنگامی‌که یک دستگاه در این قسمت قرار گرفت دستگاه را در حالت sleep قرار می‌دهد. این کار سبب کاهش مقدار حافظه مصرفی و CPU بر روی دستگاهی که GNS3 بر روی آن در حال اجرا است، می‌شود؛ بنابراین به ما اجازه می‌دهد تعداد بیشتری دستگاه به محیط شبیه‌سازی اضافه شود.

برای اتصال بین دستگاه‌های مختلف چندین واسط در GNS3 وجود دارد که متناسب با اینترفیس هر دستگاه به صورت خودکار انتخاب می‌شود. برای ایجاد لینک بین دو دستگاه صرفا کافی است که یکی از پورت‌های خالی یک دستگاه را انتخاب کرده و به پورت خالی دستگاه دیگر متصل نمایید. به عنوان مثال در ‏شکل (4-20) می‌خواهیم از مسیریاب R4یک لینک به سوییچ اضافه کنیم. با انتخاب گزینه Add a Link از منوی دستگاه‌های GNS3 و کلیک کردن بر روی مسیریاب R4، مشاهده می‌شود که این مسیریاب صرفا یک پورت دارد (رنگ سبز نشان‌دهنده اشغال بودن است) که آن هم قبلا اشغال شده است.



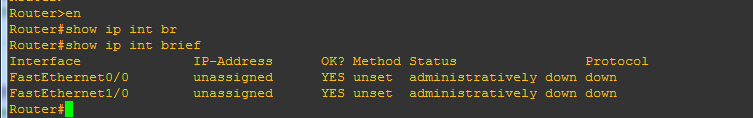
نحوه ایجاد لینک بین مسیریاب چهارم و سوئیچ

بنابراین بر روی مسیریاب R4 کلیک راست کرده و گزینه Configure را انتخاب کنید. در صفحه باز شده، گزینه PA-FE-TX را انتخاب کنید تا یک اینترفیس از نوع Fast Ethernet به آن اضافه شود. اضافه شدن واسط جدید در ‏شکل (4-21) نمایش داده شده است.



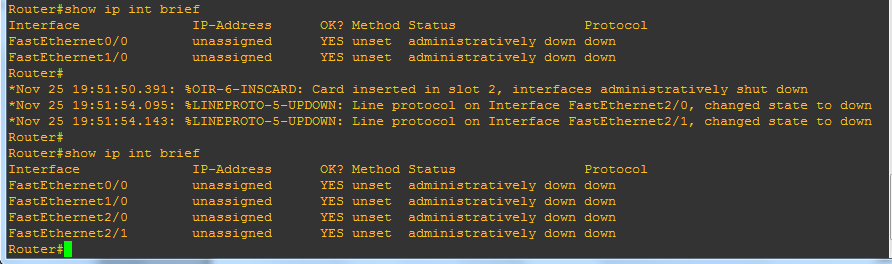
صفحه تنظیمات مربوط به مسیریاب چهارم

واسط جدید در محیط کنسول مسیریاب R4 با نام Fastethernet1/0 مشخص شده است (‏شکل (4-22)).



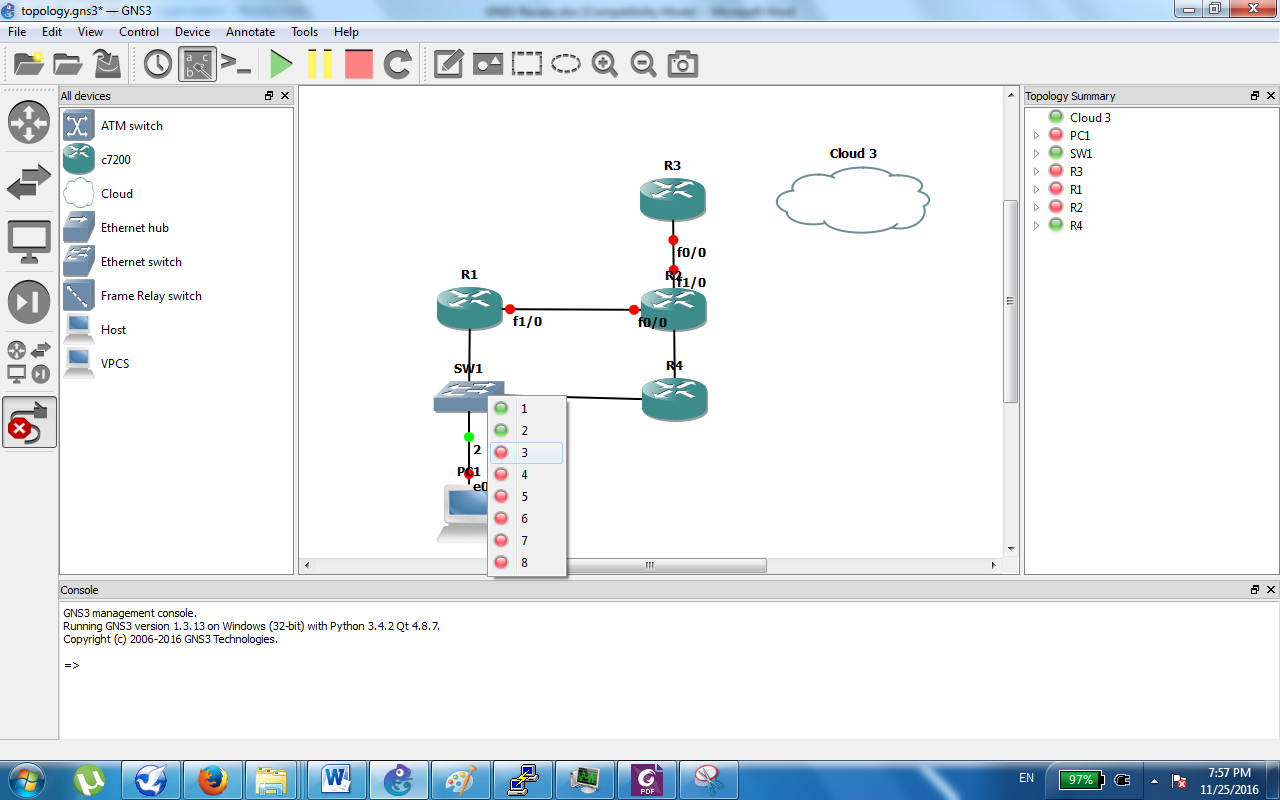
واسط‌های مسیریاب چهارم

اگر یک واسط دیگر از نوع PA-2FE-TX به این مسیریاب اضافه کنیم، اینترفیس‌های مسیریاب مطابق ‏شکل (4-23) تغییر می‌کند.



واسط‌های مسیریاب چهارم بعد از اضافه کردن واسط‌های جدید

حال می‌توان لینک را ایجاد کرد. دوباره گزینه Add a Link را انتخاب کنید و بر روی مسیریاب کلیک کنید و یکی از اینترفیس‌هایی که قرمز هستند را مشخص کنید. سپس لینک را تا سوییچ ادامه دهید تا به سوییچ برسید و بر روی آن کلیک کنید. شکلی مطابق ‏شکل (4-24) نمایش داده می‌شود. بر روی یکی از پورت‌های قرمز رنگ سوییچ کلیک کنید تا لینک ایجاد شود.



ایجاد لینک بین مسیریاب چهارم و پورت سوم سوئیچ

به‌منظور ارتباط محیط GNS3 با شبکه بیرونی، می‌توان از یک Cloud استفاده کرد. در هنگام کار کردن با GNS3 همواره Idle-PC را انتخاب کنید تا سربار استفاده از CPU دستگاه کاهش یابد.

* + - 1. مسیریابی

طبق مدل لایه‌ای OSI مسیریابی جزو وظایف لایه 3 است. مسیریابی می‌تواند ایستا یا پویا باشد. در مسیریابی ایستا، جداول مسیریابی بدون استفاده از پروتکل­های مسیریابی در هر مسیریاب ایجاد می‌شود. معمولا در شبکه‌هایی که تغییرات توپولوژی به‌ندرت اتفاق می‌افتد، از مسیریابی ایستا استفاده می‌شود، به این معنی که مدیر شبکه مسیرها را تعیین نموده و بر اساس آن جداول مسیریابی را در هر مسیریاب ایجاد می‌کند.

ساخت جداول مسیریابی در مسیریابی پویا به‌وسیله پروتکل‌های مسیریابی صورت می‌گیرد، به این صورت که بر اساس اطلاعات مسیریابی مبادله شده بین مسیریاب­های شبکه و اجرای یک الگوریتم مسیریابی، جداول مسیریابی ایجاد می‌شود. الگوریتم‌های مسیریابی را می‌توان به دو دسته حالت لینک[[40]](#footnote-40)(LS) و بردار فاصله[[41]](#footnote-41) (DS) تقسیم نمود.

در پروتکل‌های مسیریابی DV هر گره کل جدول مسیریابی خود را صرفا به همسایه‌های خود ارسال می‌کند. با دریافت این جدول، هر گره جدول مسیریابی خود را اصلاح می‌کند و مسیر با هزینه کمتر را انتخاب می‌کند. از مشکلات این پروتکل‌ها می‌توان به مشکلات همگرایی جداول مسیریابی اشاره کرد. برای رفع این مشکلات می‌توان از پروتکل‌های LS استفاده کرد.

در پروتکل‌های مسیریابی LS، هر مسیریاب تمام شبکه‌هایی که به آن‌ها متصل است را به روش سیل‌آسا به اطلاع کلیه گره‌های شبکه می‌رساند. هر مسیریاب یک پایگاه داده حالت لینک[[42]](#footnote-42) دارد که بیان‌کننده کل توپولوژی شبکه است و با استفاده از اطلاعات منتشرشده توسط همه گره‌ها در شبکه ساخته می‌شود. حالت یک لینک را می‌توان به عنوان توصیف لینک (شامل آدرس IP، آدرس ماسک شبکه و ...) و نحوه ارتباط آن لینک با همسایه‌های مسیریاب در نظر گرفت. هر مسیریاب بر اساس هزینه لینک‌ها، با اجرای یک الگوریتم مسیریابی متمرکز کوتاه‌ترین مسیر (نظیر Dijkstra) کم‌هزینه‌ترین مسیر به تمام گره‌های شبکه را محاسبه کرده و جدول مسیریابی خود را به‌روز می‌کند؛ بنابراین در این پروتکل‌ها، همه مسیریاب‌ها یک جدول بیان‌کننده کل توپولوژی شبکه در اختیار خواهند داشت. از مشکلات این پروتکل‌ها می‌توان به حجم بالای انتشار اطلاعات در شبکه اشاره کرد. برای رفع این مشکل راه‌حل‌های مختلفی پیشنهاد شده است. به عنوان مثال در پروتکل OSPF، انتشار اطلاعات به ناحیه‌های مشخصی محدود می‌شود.

یک تفاوت دیگر پروتکل‌های مسیریابی، توجه آن‌ها به کلاس‌های آدرس IP است. پروتکل‌های مسیریابی می‌توانند صرفا با توجه به کلاس‌های IP، در مورد بسته‌های به‌روزرسانی اطلاعات رفتار کنند (پروتکل‌های Classful) و یا اینکه به صورت Classless عمل کرده و به ماسک شبکه نیز توجه کنند. پروتکل RIPv1 نمونه یک پروتکل مسیریابی Classful و پروتکل RIPv2 یک پروتکل Classless است. کلاس‌های مختلف IP در ‏جدول (4-5) مشاهده می‌شود. آدرس شبکه 127.0.0.0 رزرو شده است. کلاس D برای Multicasting و کلاس E برای اهداف تحقیقاتی استفاده می‌شود.

کلاس‌های مختلف IP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Address Range | Default Subnet Mask | 1st Octet High Order Bits | 1st Octet Decimal Range | Class |
| 1.0.0.1 to 126.255.255.254 | 255.0.0.0 | 0 | 1 – 126 | Class A |
| 128.1.0.1 to 191.255.255.254 | 255.255.0.0 | 10 | 128 – 191 | Class B |
| 192.0.1.1 to 223.255.254.254 | 255.255.255.0 | 110 | 192 – 223 | Class C |
| 224.0.0.0 to 239.255.255.255 | - | 1110 | 224 – 239 | Class D |
| 240.0.0.0 to 254.255.255.254 | - | 1111 | 240 – 254 | Class E |

* + 1. قطعات و ابزارهای موردنیاز

فهرست قطعات، تجهیزات و ابزارهای (سخت‌افزاری و نرم‌افزاری) لازم برای انجام این آزمایش عبارت‌اند از:

* یک کامپیوتر با سیستم‌عامل ویندوز
* نرم‌افزار GNS3 نسخه 1.3.13 یا بالاتر
* Image Cisco IOS 7200
  + 1. فعالیت‌های قبل از آزمایش

به سوالات زیر پاسخ دهید:

فواید و معایب استفاده از مسیریابی ایستا را شرح دهید.

در چه مواردی از مسیریابی ایستا استفاده خواهیم کرد؟

از چه الگوریتم‌های دیگری به غیر از بلمن فورد می‌توان در پروتکل‌‌های مسیریابی Distance Vector استفاده کرد. نحوه کار آن‌ها را توضیح دهید.

فرمت پیام‌های مسیریابی RIPv2 را از RFC2453 به دست آورده و رسم نمایید و همچنین فیلدهای آن را توضیح دهید.

آدرس‌دهی سلسله مراتبی را با ذکر مزایا و معایب آن شرح دهید.

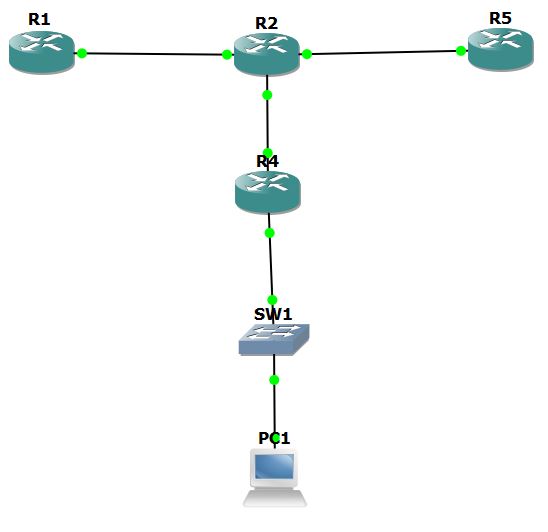
* + 1. شرح آزمایش

همان‌طور که ذکر شد یکی از هدف‌های انجام این آزمایش آشنایی با پروتکل‌های مسیریابی شبکه اینترنت است. به این منظور این آزمایش به دو بخش زیر تقسیم می‌شود:

* مسیریابی ایستا (Static Routing)
* پروتکل مسیریابی RIP
  + - 1. مسیریابی ایستا

در این قسمت با مسیریابی ایستا آشنا خواهید شد و نحوه ایجاد جدول مسیریابی به صورت دستی در مسیریاب‌ها را فرا خواهید گرفت. به صورت خلاصه در این نوع مسیریابی، در هر مسیریاب باید اطلاعات شبکه مقصد و لینک خروجی که بسته از آن لینک باید خارج شود، در مسیریاب به صورت صریح ذکر گردد. این اطلاعات می‌تواند توسط مدیر شبکه به صورت دستی وارد شده یا توسط نرم‌افزار از قبل محاسبه شده و در مسیریاب‌ها وارد شده باشد.

1. شبکه نشان داده شده در ‏شکل (4-25) را در محیط شبیه‌ساز ایجاد کنید.



توپولوژی شبکه آزمایش مسیریابی ایستا

1. آدرس­های IP زیر را به واسط‌های مسیریاب‌ها اختصاص دهید و نام آن‌ها را مطابق ‏جدول (4-6)، تغییر دهید.

آدرس‌های IP دستگاه‌های شبکه

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Mask | IP Address | Interface | Device |
| 255.255.255.0  255.255.255.0 | 10.1.1.1  12.5.10.1 | FastEthernet 0/0  Serial 0/0 | Router1 |
| 255.255.255.0 | 10.1.1.2 | FastEthernrt 0/0 | Router2 |
| 255.255.255.0 | 12.5.10.2 | Serial 0/0 | Router4 |

چرا واسط‌هایی که با FastEthernet به یکدیگر وصل شده‌اند، نیازی به تنظیم clock rate ندارند؟

1. از مسیریاب شماره 1 مسیریاب شماره 4 را Ping کنید.

نتیجه Ping را تحلیل نمایید.

برای آنکه از مسیریاب 1 مسیریاب 4 Ping شود (و برعکس) بر روی چه مسیریاب‌هایی باید جدول جلورانی ایجاد گردد؟

1. به‌منظور ایجاد مسیر از مسیریاب 1 به مسیریاب 4، با استفاده از دستور ip route جداول جلورانی موردنیاز را ایجاد کنید. برای این منظور ابتدا وارد محیط تنظیمات عمومی شوید. شکل کلی دستور به صورت زیر است:

ip route destination-network subnet-mask next-hop-ip

1. از محیط تنظیمات خارج شده و از مسیریاب شماره 1 مسیریاب شماره 4 را Ping کنید.

نتیجه Ping را تحلیل نمایید.

1. با استفاده از دستور show ip route، جداول مسیریابی در مسیریاب اول را لیست کنید.
2. با استفاده از دستور

no ip route destination-network subnet-mask next-hop-ip

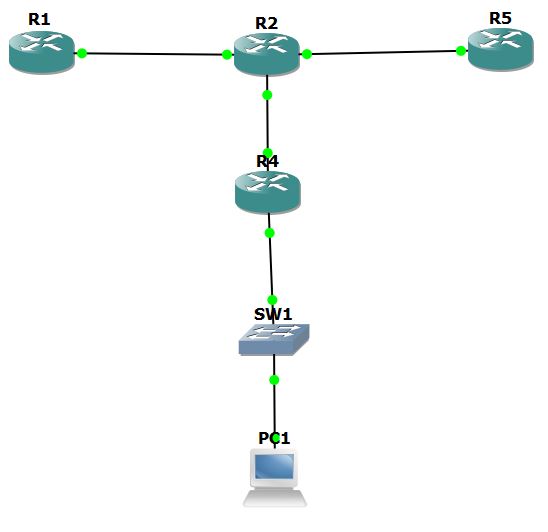
در محیط تنظیم عمومی، سطر ایجاد شده در جدول جلورانی را پاک کنید.

* + - 1. مسیریابی RIPv2

RIPv2 یک پروتکل مسیریابی DV و Classless است. RIPv1 یک پروتکل Classful بوده است. در جداول مسیریابی RIPv2 برخلاف RIPv1 به همراه آدرس شبکه، ماسک شبکه نیز به گره‌های همسایه ارسال می‌شود. پروتکل RIP از Hopcount به عنوان هزینه مسیر استفاده می‌کند؛ به عبارت دیگر هزینه هر لینک یک در نظر گرفته می‌شود. هر مسیریاب جدول مسیریابی خود را هر 30 ثانیه یک‌بار به گره‌های همسایه ارسال می‌کند و بر اساس جدول‌های رسیده، جدول مسیریابی هر مسیریاب با استفاده از الگوریتم بلمن فورد به‌روزرسانی شده و مسیر با حداقل هزینه انتخاب می‌شود. فاصله بیشتر از 16 گام به عنوان مقصد غیرقابل دسترس برای این پروتکل شناخته می‌شود. در صورت پیدا کردن مسیرهای یکسان، پروتکل از حداکثر 4 مسیر برای توزیع بسته‌ها استفاده می‌کند.

واسط Loopback یک واسط مجازی در مسیریاب است که می‌توان آن را مانند سایر واسط‌ها تنظیم کرد. این واسط همیشه up است حتی اگر تمام واسط‌های فیزیکی down باشند. از موارد استفاده این واسط می‌توان به عنوان Router ID در پروتکل OSPF نام برد.

1. شبکه نشان داده شده در ‏شکل (4-26) را در محیط شبیه‌ساز ایجاد کنید.



توپولوژی شبکه آزمایش مسیریابی RIPv2

1. دستگاه‌ها را مطابق ‏جدول (4-7) آدرس‌دهی نمایید. همچنین نام مسیریاب‌ها را نیز مطابق جدول زیر تغییر دهید.

آدرس‌های IP دستگاه‌های شبکه

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Mask | IP Address | Interface | Device |
| 255.255.255.0  255.255.255.0  255.255.255.0 | 10.1.1.1 1  92.168.1.1  172.16.1.1 | FastEthernet 0/0  FastEthernet 1/0  FastEthernet 0/1 | Router2 |
| 255.255.255.0 | 10.1.1.2 | FastEthernet 0/0 | Router1 |
| 255.255.255.0  255.255.255.0 | 192.168.1  2 10.1.2.1 | FastEthernet 0/0  Loopback 0 | Router4 |
| 255.255.255.0  255.255.255.0 | 172.16.1.2  10.1.3.1 | FastEthernet 0/0  Loopback 0 | Router5 |

1. واسط‌های Loopback را می‌توان با دستور interface loopback # در محیط تنظیم عمومی ایجاد کرد. سپس در ادامه به آن آدرس IP اختصاص داد. به عنوان مثال دستورات می‌تواند شبیه زیر باشند.

Router5(config-if)#interface loopback 0

Router5(config-if)#ip address 10.1.3.1 255.255.255.0

1. با استفاده از دستور Ping مطمئن شوید آدرس‌دهی‌ها درست بوده است.
2. ابتدا وارد محیط تنظیم عمومی شوید. سپس با استفاده از دستور router rip و سپس با دستورversion 2 پروتکل مسیریابی RIPv2 را فعال کنید. سپس دستور no auto-summary را نیز اجرا کنید تا آدرس‌های زیر شبکه نیز انتشار پیدا کنند. این کار را برای مسیریاب‌های 1، 2، 4 و 5 انجام دهید.

چه گزینه‌های دیگری برای دستور router وجود دارد؟

1. برای هر مسیریاب شبکه‌هایی که به آن متصل هستند را با استفاده از دستور network وارد کنید. به‌عنوان مثال برای مسیریاب شماره 1 دستور به صورت network 10.1.1.0 خواهد بود. آدرس شبکه بدون در نظر گرفتن زیر شبکه‌ها و بدون در نظر گرفتن ماسک شبکه وارد می‌شود؛ بنابراین آدرس شبکه‌ها مطابق ‏جدول (4-8) است. دقت کنید آدرس‌های Loopback نیز باید تنظیم شوند.

آدرس‌های شبکه

|  |  |
| --- | --- |
| Network address | Device |
| 10.1.1.0  192.168.1.0  172.16.1.0 | Router2 |
| 10.1.1.0 | Router1 |
| 10.1.2.0  192.168.1.0 | Router4 |
| 10.1.3.0  172.16.1.0 | Router5 |

1. از محیط تنظیمات خارج شوید. سپس با دستور show ip protocols پروتکل‌های مسیریابی فعال بر روی مسیریاب Router1 را بررسی کنید.
2. با استفاده از دستور show ip route جدول مسیریابی مسیریاب شماره 2 را بررسی کنید. بررسی کنید که مسیریاب، به چه شبکه‌هایی دسترسی دارد و تفاوت شبکه‌های مشخص شده با شبکه‌های کانفیگ شده در چیست؟
3. از محیط تنظیمات خارج شوید و سعی کنید که از مسیریاب شماره 1 آدرس Loopback مسیریاب شماره 4 را Ping کنید

چرا Ping موفقیت‌آمیز بود؟

* 1. آشنایی با پروتکل مسیریابی OSPF
     1. هدف آزمایش

هدف از انجام این آزمایش آشنایی با نحوه عملکرد پروتکل مسیریابی OSPF است.

* + 1. مطالب مقدماتی

پروتکل OSPF یک پروتکل مسیریابی از نوع LS و Classless است که از الگوریتم Djikstra برای پیدا کردن کوتاه‌ترین مسیر بین شبکه‌ها استفاده می‌کند. این پروتکل برای مسیریابی داخل AS به کار می‌رود. در این پروتکل، گره‌ها توپولوژی شبکه را در خود ذخیره کرده و در صورت هرگونه تغییر در حالت پیوندها، تغییرات را به صورت سیل‌آسا اطلاع‌رسانی می‌کند که به آن [[43]](#footnote-43)LSA می‌گویند. پروتکل OSPF از پروتکل RIP پیچیده‌تر است و برای پیکربندی به فرمان‌های متفاوتی نیاز دارد. به عنوان مثال برای فعال کردن OSPF باید یک شناسه فرایند[[44]](#footnote-44) تعیین کنیم. در پروتکل‌های مسیریابی از نوع LS هر مسیریاب حداقل سه جدول جداگانه را نگهداری می‌کند. يكی از اين جداول وضعيت همسايگانی را كه مستقيما به مسیریاب متصل شده‌اند نگهداری می‌کند. در جدول ديگر، توپولوژی شبكه نگهداری می‌شود و از جدول سوم برای نگهداری اطلاعات مسیریابی استفاده می‌شود.

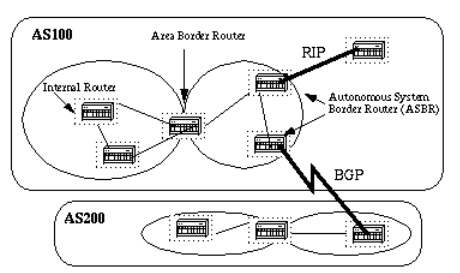
در پروتکل OSPF تقسیم‌بندی یک شبکه بزرگ به شبکه‌های مستقل از هم، باعث مزایایی از قبیل كاهش سربار عمليات مسیریابی، افزايش سرعت همگرایی و محدود كردن اعلام تغییرات شبكه در يك ناحيه و عدم انتشار آن به ساير نواحی شبكه می‌شود. با به‌کارگیری ويژگی فوق می‌توان شبکه‌ای بزرگ را به چندين شبكه کوچک‌تر كه به آن‌ها ناحيه[[45]](#footnote-45) گفته می‌شود، تقسيم نمود. درصورتی‌که ابعاد يك شبكه بسيار بزرگ باشد، یک گزينه مناسب پروتكل OSPF است. اين پروتكل سرعت همگرایی بالائی دارد و توانایی توزیع بار بین چندين مسير با هزینه يكسان به یک مقصد را دارد.

در پروتکل OSPF، هرکدام از ناحیه‌های شبکه یک ID منحصربه‌فرد 32 بیتی دارند. به ناحیه مرکزی، Backbone گفته می‌شود و ID آن0 است. تمامی نواحی دیگر باید به این ناحیه مرکزی متصل باشند. انواع مختلف مسیریاب در پروتکل OSPF در ‏جدول (4-9) آمده است.

انواع مسیریاب در پروتکل OSPF

|  |  |
| --- | --- |
| توضیح | مسیریاب |
| تمام اینترفیس‌های آن متعلق به یک ناحیه است. | Internal Router |
| حداقل یک اینترفیس متصل بهArea 0 دارد. | Backbone Router |
| حداقل یک اینترفیس متصل به Area 0 و حداقل یک اینترفیس متصل به یک ناحیه دیگر دارد. | Area Border Router |
| از یک منبع دیگر Redistribution آدرس‌ها را انجام می‌دهد. به عنوان مثال می‌تواند به یک AS دیگر متصل باشد. | Autonomous System Boundry Router |

مثالی از این مسیریاب‌ها در ‏شکل (4-27) مشاهده می‌شود.



مثالی از مسیریاب‌های مختلف در OSPF

پروتکل OSPF فعالیت خود را به‌وسیله انتشار دادن اطلاعات مربوط به مسیریاب‌های شبکه با کمک پیام‌های LSA انجام می‌دهد. در صورت تغییر در حالت لینک نیز پیغام LSA منتشر خواهد شد. این LSA ها شامل اطلاعاتی راجع به تمام اینترفیس‌های مسیریاب خواهد بود. انواع مختلفی از LSA ها وجود دارد:

* LSA منتشر شده توسط مسیریاب‌های داخل یک Area بیانگر هزینه و حالت لینک‌های مسیریاب است.
* LSA منتشر شده توسط ABR برای هر Area بیانگر اطلاعات خلاصه شده شبکه خارج آن Area است.
* LSA در یک لینک با دسترسی چندگانه، توسط یک Router Designated منتشر می‌شود و بیانگر مسیریاب‌هایی هستند که به آن لینک دسترسی دارد.
* LSA هایی که توسط ASBR منتشر می‌شود بیانگر شبکه خارج AS یا آدرس default route برای شبکه خارجی است.

عملکرد کلی پروتکل به شرحی است که در ادامه می‌آید. هر مسیریاب در بازه‌های Hello Interval پیغام‌های Hello را بر روی واسط‌های خود ارسال می‌کند. هر مسیریاب که پیغام Hello مسیریاب دیگر را دریافت کند، آن را به عنوان neighbor خود انتخاب می‌کند. مادامی‌که دو مسیریاب فعال هستند پیغام‌های Hello منتشر خواهد شد. هر مسیریاب به‌اندازه زمان Dead Interval منتظر دریافت پیغام Hello می‌ماند. اگر در این مدت هیچ پیام HELLO از مسیریاب همسایه دریافت نشود، فرض بر این گذاشته می‌شود که مسیریاب همسایه غیرقابل‌دسترس است. همچنین شروط زیر نیز علاوه بر دریافت پیغام Hello باید برقرار باشد تا دو مسیریاب همسایه یکدیگر شوند:

* شماره Area و نوع آن باید در همه آن‌ها یکسان باشد.
* مدت‌زمان بین ارسال پیام‌های Hello و همچنین Dead Interval باید در همه آن‌ها یکسان باشند. زمان پیش‌فرض به ترتیب 10 و 40 ثانیه است.
* در صورت فعال کردن احراز هویت، مسیریاب‌ها باید قادر به احراز هویت بر روی لینک بین خود باشند؛ بنابراین باید همگی کلید یکسانی داشته باشند.

در این پروتکل، هر مسیریاب نیاز به یک شناسه 32 بیتی دارد که بی‌ارتباط به آدرس IP است ولی می‌تواند یکی از آدرس‌های IP مسیریاب نیز باشد. سه راه برای انتخاب شناسه مسیریاب[[46]](#footnote-46) به ترتیب اولویت وجود دارد:

* انتخاب توسط مدیر شبکه
* بالاترین آدرس ip برای loopback interface ها
* بالاترین آدرس ip برای non-loopback interface ها

پس از اینکه فرآیند مربوط به پروتکل مسیریابی اجرا شد، شناسه مسیریاب اختصاص‌یافته تغییر نخواهد کرد. در صورت تغییر باید تنظیمات پروتکل OSPF از ابتدا انجام شود. این شناسه در پیغام‌های منتشرشده در پروتکل قرار خواهد گرفت.

پس از اینکه مسیریاب همسایه‌های خود را شناسایی کرد، رابطه مجاورت[[47]](#footnote-47) را با آن‌ها برقرار می‌کند. در این مرحله مسیریاب‌ها، پایگاه‌های داده خود را با یکدیگر مبادله می‌کنند. برای مسیریاب‌هایی که به یک واسط مشترک دسترسی دارند یک Designate Router انتخاب می‌شود و این مسیریاب مسئولیت ارسال پایگاه‌های داده به مسیریاب‌ها را بر عهده دارد. در مرحله ایجاد مجاورت، مسیریاب‌ها پایگاه داده خود را برای یکدیگر ارسال می‌کنند و پایگاه داده‌ها در کل شبکه منتشر خواهد شد. این حالت Exchange نام دارد. پس‌ازاین حالت، مسیریاب‌ها وارد مرحله Loading خواهند شد و اطلاعات گم‌شده یا قدیمی را دوباره درخواست می‌کنند. درنهایت در مرحله Full همه مسیریاب‌ها یک پایگاه داده یکسان خواهند داشت و قادر به اجرای پروتکل Dijkstra خواهند بود. LSA به صورت سیل‌آسا فقط داخل یک Area منتشر خواهد شد و ABR مسئولیت انتقال اطلاعات شبکه به سایر ABR ها را دارد.

پایگاه داده پروتکل OSPF در یک مسیریاب شامل سه بخش است. در همه این بخش‌ها ADV Router مسیریابی است که آن آدرس را منتشر کرده و Link ID آدرس IP واسط مربوطه است. همچنین برای هر Area یک جدول وجود دارد.

* Router Link state: آدرس‌هایی که در Area فعلی وجود دارد. Link count برابر تعداد اینترفیس‌های مسیریاب مشخص شده با ADV Router در آن Area است.
* Net link state: معمولا توسط Designate Router ایجاد می‌شود Link ID بیانگر واسط Designate Router در آن بخش است.
* Summary Net link state: این جدول بیانگر آدرس‌های خارج از Area فعلی است که توسط ABR ها منتشر شده است. ADV Routerها همه ABR هستند
  + 1. فعالیت‌های قبل از آزمایش

به سوالات زیر پاسخ دهید:

تفاوت‌های پروتکل‌های مسیریابی OSPF و RIPv2 را بیان کنید.

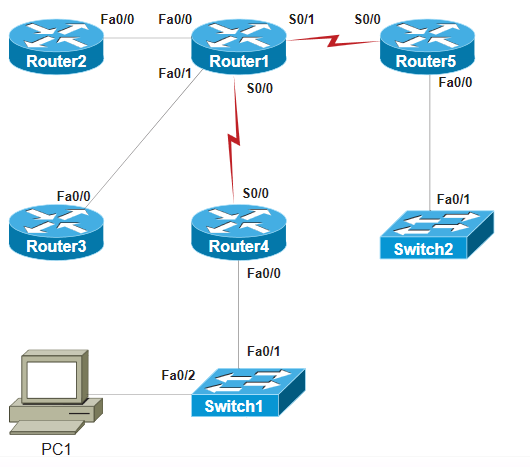
فرمت پیام‌های مسیریابی OSPF را از RFC 2178 به دست آورده و رسم نمایید و همچنین فیلدهای آن را توضیح دهید.

* + 1. قطعات و ابزارهای موردنیاز

فهرست قطعات، تجهیزات و ابزارهای (سخت‌افزاری و نرم‌افزاری) لازم برای انجام این آزمایش عبارت‌اند از:

* یک کامپیوتر با سیستم‌عامل ویندوز
* نرم‌افزار GNS3 نسخه 1.3.13 یا بالاتر
* Image Cisco IOS 7200
  + 1. شرح آزمایش
       1. دستور کار اول

شبکه ‏شکل (4-28) را در محیط شبیه‌ساز ایجاد کنید.



توپولوژی شبکه آزمایش اول OSPF

واسط‌های مسیریاب‌ها را مطابق ‏جدول (4-10) آدرس‌دهی نمایید. نرخ Clock را برابر 64000 تنظیم نمایید.

آدرس‌های IP در آزمایش اول OSPF

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Mask | IP Address | Interface | Device |
| 255.255.255.0  255.255.255.0 | 10.1.1.1  172.16.10.1 | FastEthernet 0/0  Serial 0/0 | Router1 |
| 255.255.255.0 | 10.1.1.2 | FastEthernet 0/0 | Router2 |
| 255.255.255.0 | 172.16.10.2 | Serial 0/0 | Router4 |

1. هر مسیریاب می‌تواند هم‌زمان چندین نمونه از پروتکل مسیریابی، با تنظیمات متفاوت را اجرا کند. درحالی‌که برای سایر پروتکل‌های مسیریابی چنین قابلیتی وجود ندارد. برای این منظور، باید یک شماره فرآیند به نمونه پروتکل مسیریابی اجرا شده اختصاص یابد؛ بنابراین بر روی مسیریاب 1، وارد محیط تنظیمات عمومی شوید و با دستور

router ospf 100

یک نمونه از فرآیند مسیریاب برای پروتکل OSPF با شناسه 100 ایجاد نمایید.

1. بر روی مسیریاب 1، شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 10.1.1.0 0.0.0.255 area 0

1. بر روی مسیریاب 1، شبکه 172.16.10.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 172.16.10.0 0.0.0.255 area 0

1. بر روی مسیریاب 2، وارد محیط تنظیمات عمومی شوید. یک فرآیند OSPF را اجرا و از شناسه فرآیند 100 استفاده کنید. سپس بر روی آن شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 10.1.1.0 0.0.0.255 area 0

1. بر روی مسیریاب 4، OSPF را اجرا و از شناسه فرآیند 100 استفاده کنید. سپس بر روی آن شبکه 172.16.10.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 172.16.10.0 0.0.0.255 area 0

1. همان‌طور که می‌بینید مسیریاب‌های 2 و 4 به‌طور مستقیم به یکدیگر متصل نیستند. از هر یک از این مسیریاب‌ها، دیگری را ping کنید و نتایج را تحلیل کنید.
2. با دستور Show ip route جدول مسیریابی مسیریاب‌های 1، 2 و 4 را مشاهده کنید.
3. با استفاده از دستور show ip protocols اطلاعات پروتکل‌های مسیریابی را در مسیریاب 1 مشاهده نمایید.
4. با دستور Show ip ospf پایگاه داده مربوط به پروتکل OSPF مسیریاب‌های 1، 2 و 4 را مشاهده کنید. ID هر یک از مسیریاب‌ها را یادداشت نمایید.
5. با دستور Show ip ospf neighbor همسایه‌های مسیریاب‌های 1، 2 و 4 را مشاهده کنید. همچنین، ID مسیریاب‌ها، Address و Dead Time آن‌ها را یادداشت نمایید.

آیا ID با Address فرق دارد؟

1. بر روی مسیریاب 1، وارد تنظیمات واسط Fastethernet 0/0 شده و زمان ارسال بسته‌های Hello را به 20 ثانیه افزایش دهید (درصورتی‌که از شبیه‌ساز BOSON استفاده می‌کنید، دستور زیر پیاده‌سازی نشده‌اند.)

ip ospf hello-interval 20

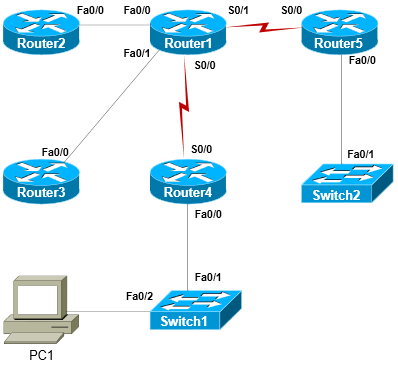
1. بر روی مسیریاب1، زمان Dead Interval Time را به 80 ثانیه تغییر دهید (درصورتی‌که از شبیه‌ساز BOSON استفاده می‌کنید، دستور زیر پیاده‌سازی نشده‌اند).

ip ospf dead-interval 80

توضیح دهید چرا ارتباط مسیریاب 1 با مسیریاب 2 برقرار نیست؟

* + - 1. دستور کار دوم

شبکه نشان داده شده در ‏شکل (4-29) را در محیط شبیه‌ساز ایجاد کنید.



توپولوژی شبکه آزمایش دوم OSPF

واسط‌های مسیریاب‌ها را مطابق ‏جدول (4-11) آدرس‌دهی نمایید. نرخClock را برابر 64000 تنظیم نمایید.

آدرس‌های IP در آزمایش دوم OSPF

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Area ID | Subnet Mask | IP Address | Interface | Device |
| 0  2 | 255.255.255.0  255.255.255.0 | 10.1.1.1  172.16.10.1 | FastEthernet 0/0  Serial 0/0 | Router1 |
| 0 | 255.255.255.0 | 10.1.1.2 | FastEthernet 0/0 | Router2 |
| 2 | 255.255.255.0 | 172.16.10.2 | Serial 0/0 | Router4 |

1. در محیط تنظیم عمومی مسیریاب Router1 با دستور

router ospf 100

یک نمونه از فرآیند اجراکننده پروتکل OSPF با شناسه 100 ایجاد نمایید.

1. بر روی مسیریاب Router1، شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 10.1.1.0 0.0.0.255 area 0

1. از محیط تنظیم ospf خارج شده و وارد محیط تنظیم عمومی شوید. سپس با استفاده از دستور

interface f0/0

وارد محیط تنظیم واسط fast Ethernet 0/0 بر روی مسیریاب Router 1 شوید.

1. با دستور

ip ospf authentication

احراز هویت به صورت plain text بر روی این اینترفیس را فعال کرده، سپس با استفاده از دستور

ip ospf authentication-key r1r2key

کلید r1r2key را به عنوان کلید احراز هویت تنظیم کنید.

1. در محیط تنظیم عمومی مسیریاب Router2 با دستور

router ospf 10

یک نمونه از فرآیند اجراکننده پروتکل OSPF با شناسه 10 ایجاد نمایید.

1. بر روی مسیریاب Router2، شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه 0 اضافه کنید.

network 10.1.1.0 0.0.0.255 area 0

1. از محیط تنظیمات خارج شوید. دستور

show ip ospf neighbor

را بر روی مسیریاب Router1 اجرا کنید. هیچ مسیریابی به عنوان همسایه لیست نشده است درحالی‌که مسیریاب Router1 و Router2 مستقیما به یکدیگر متصل هستند.

توضیح دهید چه اتفاقی رخ داده است؟

1. در محیط تنظیم عمومی مسیریاب Router2 وارد تنظیم واسط fast Ethernet 0/0 شوید. سپس با استفاده از دستور

ip ospf authentication

احراز هویت به صورت plain text بر روی این اینترفیس را فعال کرده، سپس با استفاده از دستور

ip ospf authentication-key r1r2key

کلید r1r2key را به عنوان کلید احراز هویت تنظیم کنید.

1. از محیط تنظیمات مسیریاب Router2 خارج شوید. دستور

show ip ospf neighbor

را بر روی مسیریاب Router1 اجرا کنید.

توضیح دهید چه اتفاقی رخ داده است؟

1. با استفاده از دستور

show ip ospf

بر روی مسیریاب Router2، شماره فرآیند اجراکننده پروتکل OSPF و ID مسیریاب را مشاهده کنید. سپس با استفاده از دستور

conf t

وارد محیط تنظیم عمومی شده و با استفاده از دستور

router ospf #

که به‌جای # شماره فرآیند قرار می‌گیرد، وارد تنظیمات فرایند شوید.

1. با استفاده از دستور

router-id 60.60.60.60

1. شناسه مسیریاب را تغییر دهید.

مسیریاب چه پیغامی را نمایش می‌دهد؟

1. در مسیریاب Router2، بدون اینکه وارد هیچ محیط تنظیمی شوید دستور

clear ip ospf process

را اجرا کنید. در جواب حرف y را وارد نمایید.

به مسیریاب Router1 بروید. چه پیغام‌هایی برای مسیریاب با شماره 10.1.1.2 مشاهده می‌کنید؟

1. در مسیریاب Router2 از محیط تنظیمات خارج شوید. با استفاده از دستور

show ip ospf

ID مسیریاب را مشاهده نمایید.

چه تغییری رخ داده است؟

1. دستور

show ip ospf neighbor

را بر روی مسیریاب Router1 اجرا کنید.

خروجی چه تفاوتی با مرحله 9 دارد؟

1. در مسیریاب Router1 وارد محیط تنظیم عمومی شوید. سپس یک اینترفیس loopback با شماره 1 با استفاده از دستورات

interface loopback 1

ip address 50.50.50.50 255.255.255.0

ایجاد کرده و به آن آدرس IP اختصاص دهید. از محیط تنظیمات اینترفیس خارج شده و وارد محیط تنظیمات عمومی شوید.

آیا نیازی به پاک کردن فرآیند OSPF وجود دارد؟ چرا؟

1. با استفاده از دستور

router ospf 100

وارد تنظیمات فرآیند OSPFدر مسیریاب Router1 شده و با استفاده از دستور زیر یک شبکه به آن اضافه کنید.

network 50.50.50.0 0.0.0.255 area 1

دقت کنید که شماره فرآیندها را اشتباه وارد نکنید. در صورت نیاز شماره فرآیند را به دست آورده و در صورت اشتباه وارد کردن دستورات، با اضافه کردن کلمه no به ابتدای دستور اشتباه، دستور پاک خواهد شد.

1. از محیط تنظیمات خارج شده و دستور

show ip ospf neighbor

را اجرا کنید.

چرا آدرس Loopback اضافه شده جز همسایه‌های مسیریاب Router1 نیست؟

1. دستور

show ip ospf database

را بر روی مسیریاب Router1 اجرا کنید.

آیا آدرس Loopback اضافه شده را آنجا مشاهده می‌کنید؟

1. بر روی مسیریاب Router2، آدرس 50.50.50.50 را Ping کنید.

چرا ping موفقیت‌آمیز است؟

1. واسط سریال مسیریاب‌های Router4 و Router1 را نیز کانفیگ کرده و واسط‌های آن‌ها را مطابق ‏جدول (4-11) در area های مربوطه قرار دهید.
2. در مسیریاب Router4، دستور

show ip route

را اجرا کنید.

در مقابل ردیف مربوط به آدرس 50.50.50.50 عبارت‌های O و IA نوشته شده است. این‌ها چه معنی دارند؟

1. از مسیریاب Router4، مسیریاب Router2 را ping کنید. Ping موفقیت‌آمیز است. با استفاده از دستور

show ip ospf route

مشخص کنید که مسیر ارسالی برای این بسته، از چه واسط‌ها و چه Area هایی عبور می‌کند.

1. در مسیریاب Router1 دستور

show ip ospf

را اجرا کنید.

این مسیریاب از چه نوع از مسیریاب‌های گفته شده در OSPF است؟

* 1. کار با شبیه‌سازی GNS3
     1. هدف آزمایش

هدف این آزمایش آشنایی بیشتر و کار با شبیه‌ساز GNS3 به‌منظور شبیه‌سازی عملکرد مسیریاب‌ها و سوییچ‌های سیسکو است.

* + 1. فعالیت‌های قبل از آزمایش

آزمایش آشنایی با شبیه‌سازی GNS3 را مرور کنید.

* + 1. قطعات و ابزارهای موردنیاز

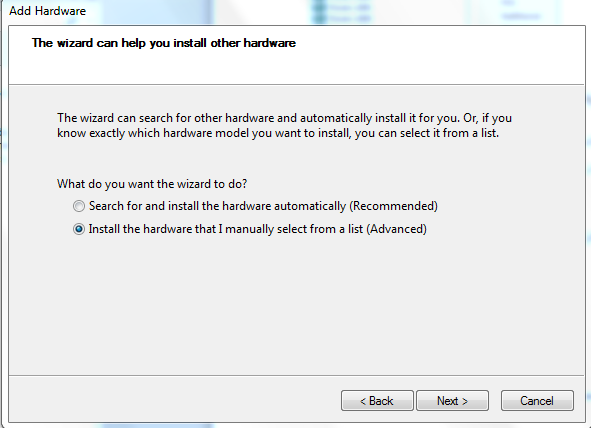
فهرست قطعات، تجهیزات و ابزارهای لازم (سخت‌افزاری و نرم‌افزاری) برای انجام این آزمایش عبارت‌اند از:

* یک کامپیوتر با سیستم‌عامل ویندوز
* نرم‌افزار GNS3 نسخه 1.3.13 یا بالاتر
* Image Cisco IOS 7200
* برنامه Wireshark
  + 1. شرح آزمایش

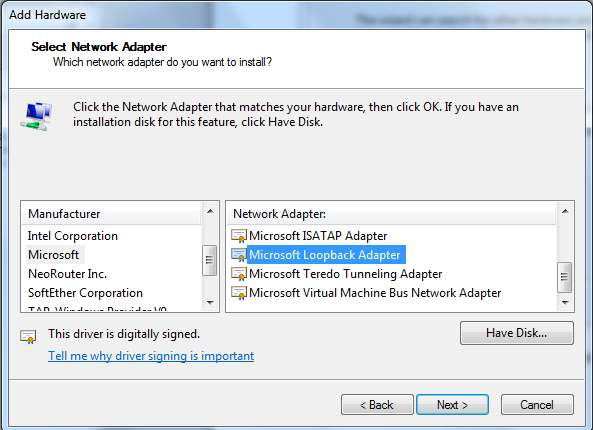
ابتدا باید یک Loopback Adaptor را به سیستم اضافه کنید. برای این کار با فشردن دکمه استارت ویندوز 7، hdwwiz.exe را جستجو کنید. پس از باز کردن برنامه دکمه Next را زده و مطابق ‏شکل (4-30) گزینه دوم را انتخاب کنید.

در صفحه بعد، Network Adaptors را انتخاب کرده و Next را بزنید. از بین دستگاه‌های نمایش داده شده، مطابق ‏شکل (4-31)، Microsoft Loopback adaptor را انتخاب کنید. پس از زدن دکمه Next و نصب Loopback Adaptor، سیستم را ری استارت کنید.

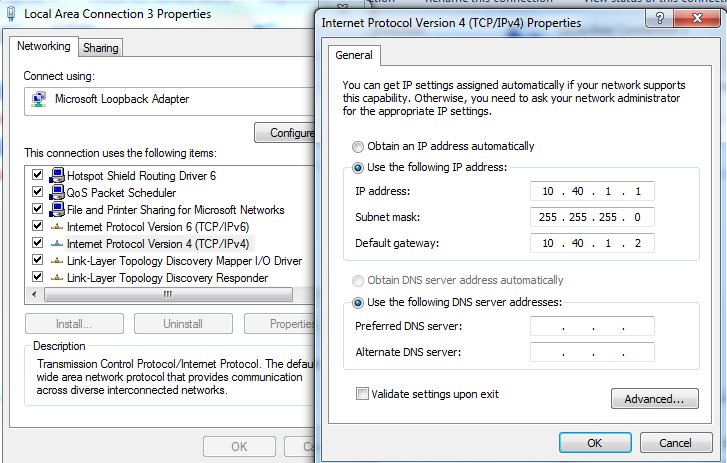
پس از ورود به محیط ویندوز، از محیط کنترل پنل ویندوز 7 عبارت Network را جستجو کنید و Network and Sharing Center را انتخاب کنید. سپس از ستون سمت چپ، change adaptor settings را انتخاب کرده و Local Area Connection جدیدی که ساخته‌اید را پیدا کنید. بر روی آن کلیک راست کنید و Properties را انتخاب کنید. تنظیمات IPv4 را مطابق ‏شکل (4-32) انجام دهید.



ایجاد Loopback Adaptor- مرحله اول

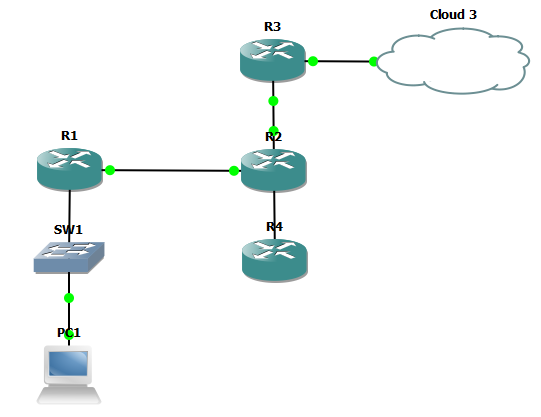


ایجاد Loopback Adaptor- مرحله دوم



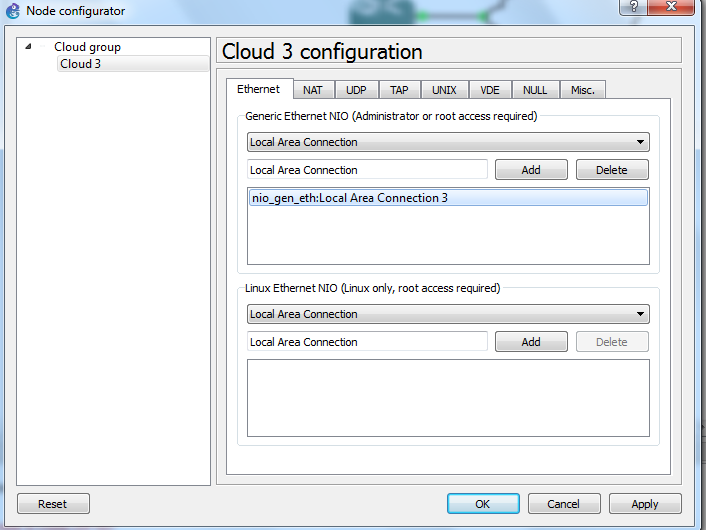
ایجاد Loopback Adaptor مرحله سوم

1. شبکه نشان داده شده در ‏شکل (4-33) را در محیط شبیه‌ساز ایجاد کنید.



توپولوژی شبکه

1. در محیط شبیه‌ساز بر روی ابر کلیک راست کنید و گزینه Configure را انتخاب کنید. سپس در بخش Ethernet، مطابق ‏شکل (4-34) Local Area Connection ایجاد شده را به عنوان دستگاهی که این ابر به آن متصل است انتخاب کرده و دکمه Add را فشار دهید.



پیکربندی ابر

1. پس از انجام این کار، ابر را به مسیریاب R3 متصل کنید.
2. آدرس­های IP را طبق ‏جدول (4-12) به دستگاه‌ها اختصاص دهید.

آدرس IP دستگاه‌ها

|  |  |
| --- | --- |
| IP | Device |
| 10.10.1.1/24  10.1.1.1/24 | R1 |
| 10.10.1.100/24  10.20.1.100/24  10.30.1.100/24 | R2 |
| 10.40.1.2/24  10.30.1.1/24 | R3 |
| 10.20.1.1/24 | R4 |
| DHCP | PC1 |

1. همه آدرس‌های IP داده شده را بر روی همه مسیریاب‌ها تنظیم کنید.
2. بر روی مسیریاب R1 آدرس مسیر پیش‌فرض را تنظیم کنید. برای این کار وارد تنظیمات عمومی شوید، سپس با استفاده از دستور

ip route 0.0.0.0 0.0.0.0 10.40.1.1

تنظیم کنید که درصورتی‌که مقصد بسته در هیچ‌یک از شبکه‌های تنظیم شده بر روی مسیریاب قرار نداشت، بسته به آدرس 10.40.1.1 ارسال شود.

1. بر روی واسط fastethernet 1/0 در مسیریاب R1 با استفاده از wireshark بسته‌های ارسال شده را شنود کنید و تا پایان آزمایش آن را خاتمه ندهید.
2. تمام مسیریاب‌ها باید قادر به Ping یکدیگر باشند. با استفاده از پروتکل‌های مسیریابی که تا به حال بررسی کرده‌اید، تنظیمات لازم را انجام دهید.
3. از تمام مسیریاب‌ها باید قادر به Ping کردن آدرس 10.40.1.1 باشید. نیاز به چه تنظیمی بر روی چه مسیریابی وجود دارد؟ چرا؟ تنظیمات لازم را برای این کار انجام دهید.
4. از تمام مسیریاب‌ها باید قادر به Ping کردن آدرس 8.8.8.8 باشید. برای این منظور باید آدرس default route تنظیم شده در مسیریاب R3 به مسیریاب‌های دیگر منتشر شود. برای این کار در مسیریاب R3 وارد تنظیمات پروتکل مربوطه شوید سپس با استفاده از دستور

default-information originate

آدرس مسیر پیش‌فرض انتشار خواهد یافت.

1. بر روی مسیریاب R1 وارد محیط تنظیم عمومی شوید. با استفاده از دستورات

ip domain-lookup

ip name-server 8.8.8.8 8.8.4.4

تنظیمات مربوط به سرور DNS را انجام دهید. حال آدرس google.com را ping کنید.

1. با استفاده از پروتکل DHCP به PC1 آدرس IP اختصاص دهید.PC1 باید قادر به Ping کردن آدرس google.com باشد. برای این منظور در تنظیم سرور DHCP و در Pool ای که تعریف کرده‌اید با استفاده از دستور

dns-server 8.8.8.8

آدرس سرور DNS را تنظیم کنید.

1. در PC1 با استفاده از دستور

ip dhcp

آدرس DHCP به دست بیاورید. با استفاده از دستور

show ip

تنظیم آدرس IP مربوط به PC1 نمایش داده می‌شود.

1. بسته‌های دریافت شده در Wireshark را ذخیره کنید.

ترتیب اجرای پروتکل‌های مختلف و بسته‌های رد و بدل شده را بررسی کنید.

1. Four-Pair Unshielded Twisted Pair (UTP) [↑](#footnote-ref-1)
2. Coaxial Cable [↑](#footnote-ref-2)
3. Shielded Twisted Pair (STP) [↑](#footnote-ref-3)
4. Outlet [↑](#footnote-ref-4)
5. Conduit [↑](#footnote-ref-5)
6. Cable Tray [↑](#footnote-ref-6)
7. Rack [↑](#footnote-ref-7)
8. Electronic Industries Association [↑](#footnote-ref-8)
9. Wall-Mounted Brackets [↑](#footnote-ref-9)
10. Skeletal frames [↑](#footnote-ref-10)
11. Full Equipment Cabinets [↑](#footnote-ref-11)
12. Cable Management [↑](#footnote-ref-12)
13. Cable Hangers [↑](#footnote-ref-13)
14. Telecommunications Closet [↑](#footnote-ref-14)
15. J Hook [↑](#footnote-ref-15)
16. Horizontal Ladder [↑](#footnote-ref-16)
17. Electronic Industries Alliance [↑](#footnote-ref-17)
18. Telecommunications Industry Association [↑](#footnote-ref-18)
19. Socket, Plug, Jack [↑](#footnote-ref-19)
20. Pin [↑](#footnote-ref-20)
21. Socket, Plug, Jack [↑](#footnote-ref-21)
22. Straight Patch Cord [↑](#footnote-ref-22)
23. Crossover Patch Cord [↑](#footnote-ref-23)
24. Gateway [↑](#footnote-ref-24)
25. Online [↑](#footnote-ref-25)
26. Console port [↑](#footnote-ref-26)
27. Unique ID [↑](#footnote-ref-27)
28. Virtual terminal [↑](#footnote-ref-28)
29. Power-On Self-Test [↑](#footnote-ref-29)
30. Volatile RAM [↑](#footnote-ref-30)
31. Nonvolatile RAM [↑](#footnote-ref-31)
32. Data Communication Equipment [↑](#footnote-ref-32)
33. Data Terminal Equipment [↑](#footnote-ref-33)
34. Password [↑](#footnote-ref-34)
35. private [↑](#footnote-ref-35)
36. invalid [↑](#footnote-ref-36)
37. Internet Service Provider [↑](#footnote-ref-37)
38. Internet Address Numbers Authority [↑](#footnote-ref-38)
39. Ameriacan Registry for Internet Numbers [↑](#footnote-ref-39)
40. Link State [↑](#footnote-ref-40)
41. Distance Vector [↑](#footnote-ref-41)
42. LSDB [↑](#footnote-ref-42)
43. Link-State Advertisement [↑](#footnote-ref-43)
44. Process ID [↑](#footnote-ref-44)
45. Area [↑](#footnote-ref-45)
46. Router-id [↑](#footnote-ref-46)
47. Adjacency [↑](#footnote-ref-47)