



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)



دانشکده مهندسی کامپیوتر
و فناوری اطلاعات

دستور کار آزمایشگاه شبکه‌های کامپیوتری

مسئول آزمایشگاه:

دکتر مسعود صبایی

پاییز ۹۷

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ
حَمْدُ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ

فهرست مطالب

۱	فصل ۱ : مقدمه
۲	۱- آشنایی با تجهیزات شبکه و کابل کشی.
۲	۲- هدف آزمایش.
۲	۳- مطالب مقدماتی
۲	۴- ۱- تجهیزات شبکه
۱۲	۵- ۲- کابل کشی
۱۷	۶- ۳- قطعات و ابزارهای موردنیاز
۱۸	۷- ۴- شرح آزمایش
۲۱	۸- ابزارهای مدیریت شبکه‌های کامپیووتری
۲۱	۹- ۱- هدف آزمایش
۲۱	۱۰- ۲- شرح آزمایش
۲۱	۱۱- ۱- مشاهده تنظیمات آدرس IP واسطه‌های شبکه
۲۲	۱۲- ۲- استفاده از برنامه‌های خط فرمان
۲۳	۱۳- ۳- ارزیابی ارتباط با سیستم‌های دیگر با استفاده از ابزارهای Ping و Tracert
۲۵	۱۴- ۴- استفاده از ابزار Ping Plotter
۲۸	۱۵- آشنایی با نرمافزار Wireshark
۲۸	۱۶- ۱- هدف آزمایش
۲۸	۱۷- ۲- مطالب مقدماتی
۳۱	۱۸- ۳- قطعات و ابزارهای موردنیاز
۳۱	۱۹- ۴- شرح آزمایش
۳۱	۲۰- ۱- لایه‌بندی پروتکل‌ها
۳۲	۲۱- ۲- کار با فیلتر کننده بسته‌ها
۳۶	۲۲- فصل ۲ : لایه کاربرد
۳۷	۲۳- ۱- راهاندازی سرویس‌های Web و FTP
۳۷	۲۴- ۱- هدف آزمایش
۳۷	۲۵- ۲- قطعات و ابزارهای موردنیاز

۳۷ ۱-۳-۱- شرح آزمایش
۳۸ ۱-۳-۱- تنظیمات سرور Web
۴۴ ۱-۳-۲- تنظیمات سرور FTP
۴۸ ۱-۳-۳- پروتکل HTTP
۴۸ ۱-۳-۴- پروتکل FTP
۵۰	۲- کار با کاربردهای Web، سوکت و پویش سرویس‌ها
۵۰	۲- ۱- هدف آزمایش
۵۰	۲- ۲- فعالیت‌های قبل از آزمایش
۵۰	۲- ۳- قطعات و ابزارهای موردنیاز
۵۰	۲- ۴- شرح آزمایش
۵۰	۲- ۴- ۱- کارکرد DNS
۵۲	۲- ۴- ۲- مشاهده و تخصیص پورت‌های لایه انتقال با استفاده از ابزار Netstat
۵۳	۳- ۴- ۲- کارکرد Web
۵۴	۴- ۴- ۲- پویش سرویس‌ها
۵۶	فصل ۳: لایه انتقال
۵۷	۱- تحلیل TCP با استفاده از Wireshark
۵۷	۱- ۱- هدف آزمایش
۵۷	۱- ۲- فعالیت‌های قبل از آزمایش
۵۷	۱- ۳- شرح آزمایش
۶۴	فصل ۴: لایه شبکه
۶۵	۱- آشنایی با شبیه‌ساز Boson Netsim
۶۵	۱- ۱- هدف آزمایش
۶۵	۱- ۲- مطالب مقدماتی
۶۷	۱- ۲- ۱- انواع حافظه در تجهیزات سیسکو
۶۹	۱- ۲- ۲- اتصال از طریق کابل سریال
۷۰	۱- ۳- ۲- پروتکل CDP
۷۰	۱- ۳- ۳- قطعات و ابزارهای موردنیاز

۷۰ ۴-۱- شرح آزمایش
۷۰ ۴-۱-۱- تنظیمات مقدماتی
۷۴ ۴-۱-۲- اختصاص آدرس IP به واسطه‌های شبکه
۷۷ ۴-۱-۳- اتصال به مسیریاب از طریق Telnet
۷۸ ۴-۱-۴- تنظیمات پروتکل CDP
۷۹ ۲- آشنایی با مکانیسم NAT و پروتکل DHCP
۷۹ ۱-۲- هدف آزمایش
۷۹ ۲-۲- مطالب مقدماتی
۸۲ ۳-۲- شرح آزمایش
۸۲ ۱-۳-۲- مکانیسم NAT
۸۵ ۲-۳-۲- پروتکل DHCP
۸۸ ۳- آشنایی با شبیه‌ساز GNS3
۸۸ ۱-۳- هدف آزمایش
۸۸ ۲-۳- مطالب مقدماتی
۸۸ ۱-۲-۳- معرفی GNS3
۹۷ ۲-۲-۳- مسیریابی
۹۹ ۳-۳- قطعات و ابزارهای موردنیاز
۹۹ ۴- فعالیت‌های قبل از آزمایش
۱۰۰ ۵-۳- شرح آزمایش
۱۰۰ ۱-۵-۳- مسیریابی ایستا
۱۰۱ ۲-۵-۳- مسیریابی RIPv2
۱۰۴ ۴- آشنایی با پروتکل مسیریابی OSPF
۱۰۴ ۱-۴- هدف آزمایش
۱۰۴ ۲-۴- مطالب مقدماتی
۱۰۷ ۳-۴- فعالیت‌های قبل از آزمایش
۱۰۷ ۴-۴- قطعات و ابزارهای موردنیاز
۱۰۸ ۵-۴- شرح آزمایش

۱۰۸	۱-۵-۴	- دستور کار اول
۱۱۰	۲-۵-۴	- دستور کار دوم
۱۱۵	۵	- کار با شبیه‌سازی GNS3
۱۱۵	۱-۵	- هدف آزمایش
۱۱۵	۲-۵	- فعالیت‌های قبل از آزمایش
۱۱۵	۳-۵	- قطعات و ابزارهای موردنیاز
۱۱۵	۴-۵	- شرح آزمایش

فصل ۱: مقدمه

۱- آشنایی با تجهیزات شبکه و کابل‌کشی

۱-۱- هدف آزمایش

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

۱-۲- مطالب مقدماتی

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

۱-۲-۱- تجهیزات شبکه

۱-۲-۱-۱- کابل‌های افقی

بر اساس استاندارد ANSI/TIA-568-C.2 زوج سیم به هم تابیده‌ی بدون محافظ^۱ (UTP) ۱۰۰ اهمی که از جنس مس هستند استفاده می‌شود. طبق این استاندارد امکان پیاده‌سازی کابل‌های افقی با استفاده از فیبر نوری چندحالته‌ی ۶۲.۵/۱۲۵ میکرون یا ۵۰/۱۲۵ میکرون نیز وجود دارد. برای انتقال داده و صوت بر بستر شبکه، استفاده از

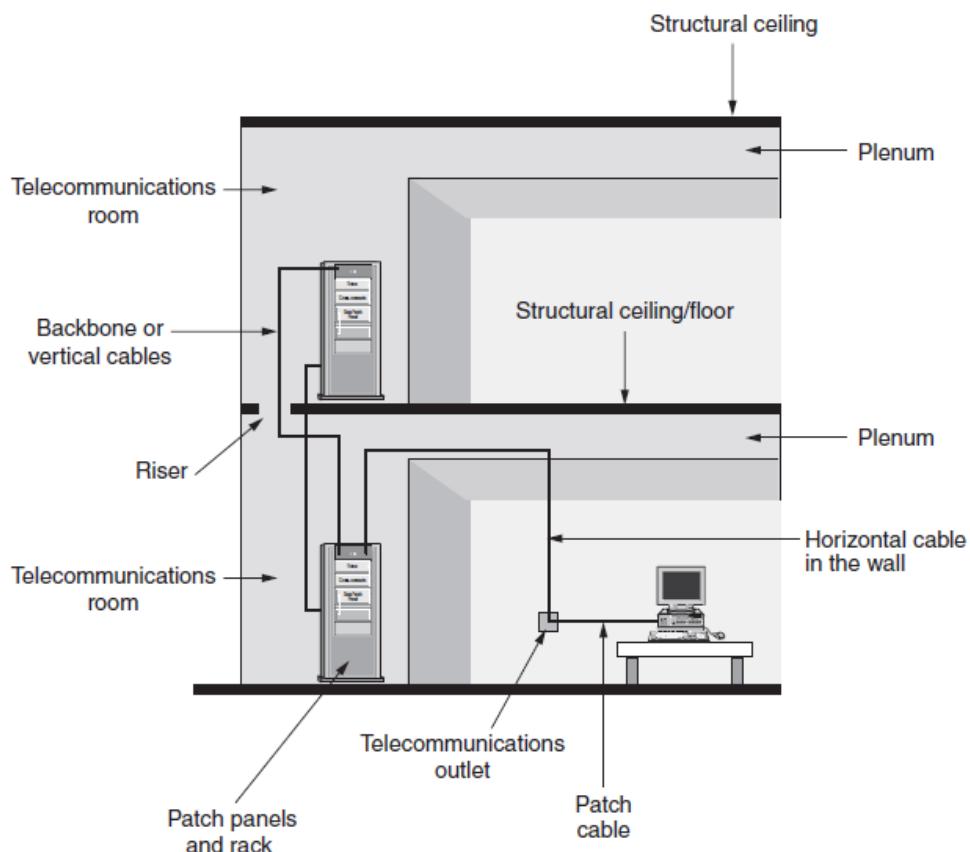
^۱ Four-Pair Unshielded Twisted Pair (UTP)

کابل‌های هم محور^۲ (Coaxial) به عنوان کابل افقی مناسب نیست.

۲-۱-۲-۱- کابل‌های Backbone

برای پیاده‌سازی کابل‌های Backbone می‌توان از زوج سیم به هم تابیده‌ی محافظ دار^۳ ۱۰۰ Screened Twisted Pair (ScTP) یا UTP (STP) یا فیبر نوری تک‌حالته‌ی ۸.۳/۱۲۵ میکرون نیز چند‌حالته‌ی ۶۲.۵/۱۲۵ میکرون یا فیبر نوری تک‌حالته‌ی ۵۰/۱۲۵ میکرون و یا فیبر نوری تک‌حالته‌ی ۱۵۰ هم‌محور استفاده کرد. برای ارتباطات Backbone استفاده از کابل‌های STP و هم‌محور ۱۵۰ اهمیت دارد. برای دلیل محدودیت مسافت در کابل‌های مسی (STP, UTP, ScTP)، استفاده از فیبر نوری به عنوان رسانه‌ی انتقال در Backbone ترجیح داده می‌شود.

شکل (۱-۱) مؤلفه‌های معمول یک محیط کابل‌کشی ساختاریافته را نشان می‌دهد.



شکل (۱-۱) مؤلفه‌های 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 عموماً یک فضای ایجاد شده بین طبقات

² Coaxial Cable

³ Shielded Twisted Pair (STP)

مختلف است که می‌توان کابل‌ها را از یک طبقه به طبقه دیگر انتقال داد.

Patch Panel - ۳-۱-۲-۱

وظیفه اصلی Patch Panel این است که بین نقاط انتهایی کابل‌های شبکه و تجهیزات شبکه-ای (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 Cord و Patch Panel به سوئیچ، 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 به کار رفته در سیستم انتخاب شود، زیرا در صورت عدم تطابق، سیگنال حامل داده را تضعیف خواهد کرد. شکل (۲-۱) Patch Panel با ۴۸ پورت را نشان می‌دهد.



شکل (۲-۱) یک Patch Panel

Patch Cord - ۴-۱-۲-۱

کابل‌هایی هستند که برای برقراری ارتباط بین نقاط انتهایی کابل‌های افقی و تجهیزات شبکه (مانند سوئیچ و هاب) در Patch Panel و یا برقراری ارتباط بین دستگاه‌های انتهایی (مانند رایانه و پرینتر) و پریز ارتباطی^۴ 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.

^۴ Outlet

۱-۲-۵- مجرای سیم

مجرای سیم^۵ 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 زمان بر 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 ۴۰٪ تا ۶۰٪ 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 کابل‌کشی‌های Backbone) استفاده کرد. شکل (۱-۳) و شکل (۱-۴) نمونه‌هایی از مجرای سیم هستند.



شکل (۱-۳) نمونه‌ای از مجرای سیم



شکل (۱-۴) نمونه‌ای دیگر از مجرای سیم

^۵ Conduit

۱-۲-۶- سینی کابل

به عنوان جایگزینی برای مجرای سیم، می‌توان از سینی کابل^۶ 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 (۱-۵) یک نمونه سینی کابل به همراه کابل‌های داخلی را نشان می‌دهد.

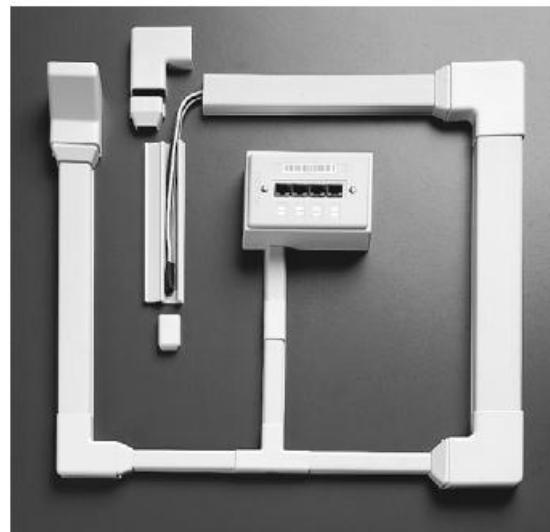


شکل (۱-۵) نمونه‌ای از سینی کابل

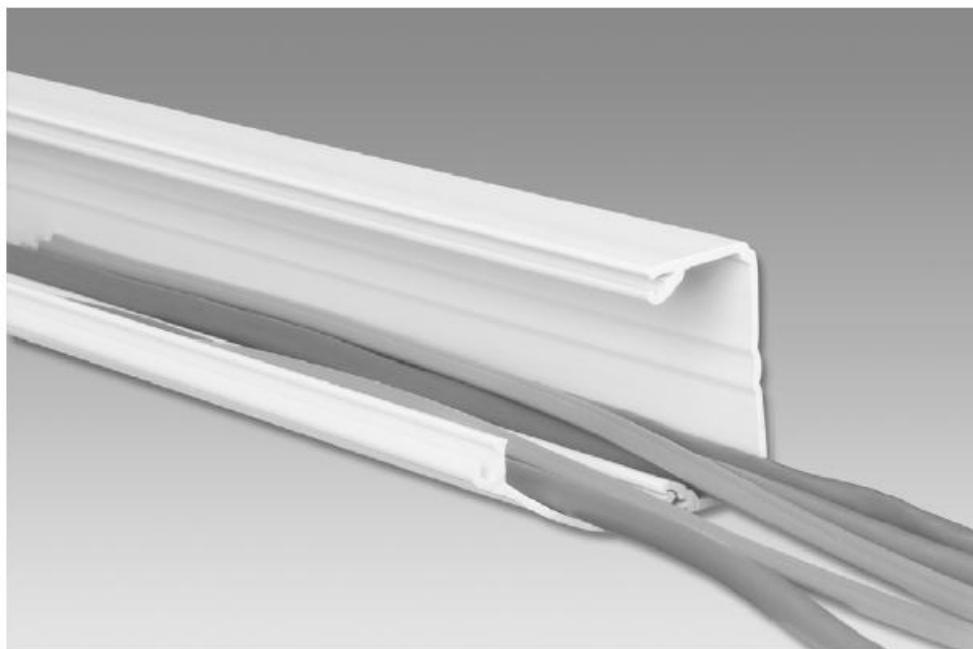
۱-۲-۷- داکت

داکت نوع خاصی از مجرای سیم است که برای کابل‌کشی افقی روی سطوح استفاده می‌شود. داکت‌ها معمولاً به صورت مازولار ساخته می‌شوند. از داکت برای کابل‌کشی روی سطوح دیوارهایی که امکان هدایت کابل از داخل آن‌ها وجود ندارد استفاده می‌شود. شکل (۱-۶) و شکل (۱-۷) نشان دهنده‌ی سیستم داکت‌کشی است.

⁶ Cable Tray



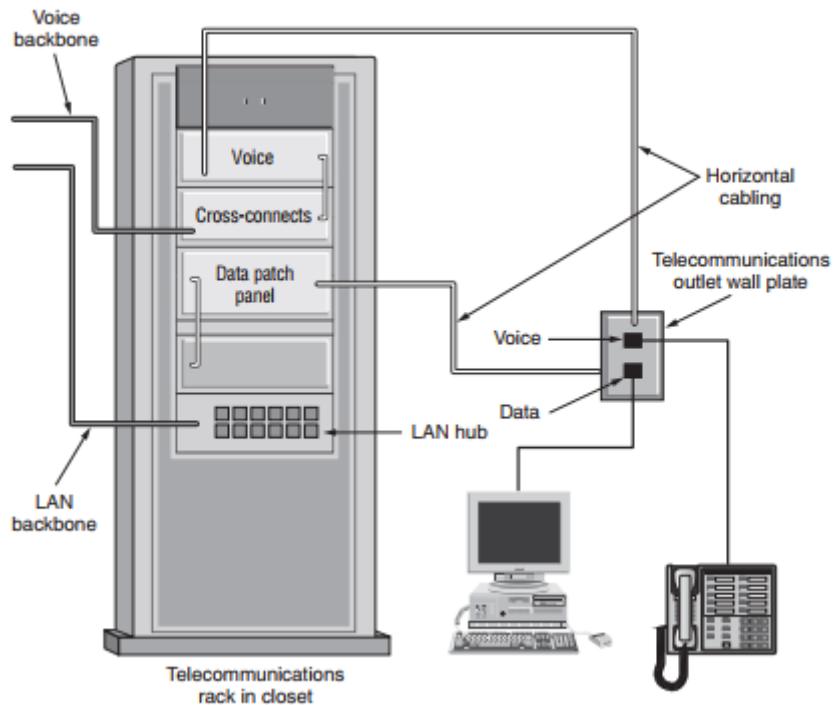
شکل (۶-۱) یک سیستم ماذولار داکت کشی



شکل (۷-۱) داکت عبوری از یک سطح با تعدادی کابل

۸-۱-۲-۱- پریز ارتباطی

پریز ارتباطی ارتباط بین تجهیزات انتهایی و رک‌ها را تسهیل می‌کند. طراح شبکه، پریزها را به رک‌ها متصل می‌کند و تجهیزات انتهایی صرفاً به پریز متصل می‌شوند. یک نمونه از پریزهای ارتباطی در شکل (۸-۱) و شکل (۹-۱) آورده شده است.



شکل (۸-۱) ارتباط تجهیز انتهایی به رک از طریق پریز



شکل (۹-۱) یک نمونه پریز ارتباطی

۹-۱-۲-۱ رک

رک^۷ ها به شما کمک می کنند تا زیرساخت کابل کشی خود را نظم دهید. ارتفاع آن معمولاً می تواند بین ۳۹ اینچ تا ۸۴ اینچ و پهنای آن ۱۹ تا ۲۳ اینچ باشد. در ۶۰ سال اخیر، رک ها با پهنای ۱۹ اینچ بسیار مورد استفاده قرار گرفته اند. این رک ها، رک ۱۹ اینچی یا رک EIA^۸ نامیده می شوند.

به طور کلی سه نوع رک وجود دارد:

⁷ Rack

⁸ Electronic Industries Association

- رک‌های دیواری^۹
- رک‌های فریم اسکلتی^{۱۰}
- کابینت‌های کاملاً تجهیز شده^{۱۱}

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 (۱۰-۱) یک رک دیواری را نشان می‌دهد.



شکل (۱۰-۱) نمونه‌ای از رک دیواری

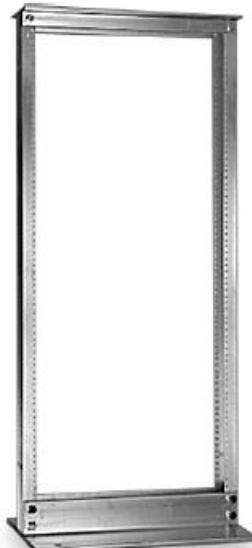
رک‌های فریم اسکلتی (یا رک‌های ۱۹ اینچی یا EIA) متداول‌ترین نوع رک‌های مورد استفاده هستند. این رک‌ها بر اساس استاندارد EIA/ECA-310-E (مربوط به سال ۲۰۰۵) طراحی و ساخته شده‌اند. این رک‌ها بین ۳۹ اینچ تا ۸۴ اینچ ارتفاع دارند. طراحی رک‌های ایستاده به گونه‌ای است که امکان کار کردن با قسمت جلویی و پشتی تجهیزات نصب شده وجود دارد. هنگام نصب رک فریم اسکلتی، باید بین دیوار و رک، فضای کافی برای جاسازی تجهیزات وجود داشته باشد (عمق تجهیزات معمولاً بین ۶ اینچ تا ۱۸ اینچ است). همچنین باید فضای کافی برای فردی که با تجهیزات کار خواهد کرد، در پشت رک در نظر گرفته شود (حداقل ۱۲ اینچ تا ۱۸ اینچ). همچنین باید از استحکام رک روی زمین برای جلوگیری از سقوط آن اطمینان حاصل کرد. در این رک‌ها می‌توان از ابزار مدیریت کابل^{۱۲}، خصوصاً زمانی که تعداد کابل‌ها زیاد است استفاده کرد. شکل (۱۱-۱) و شکل (۱۲-۱) نمونه‌هایی از رک‌های اسکلتی را نشان می‌دهند.

⁹ Wall-Mounted Brackets

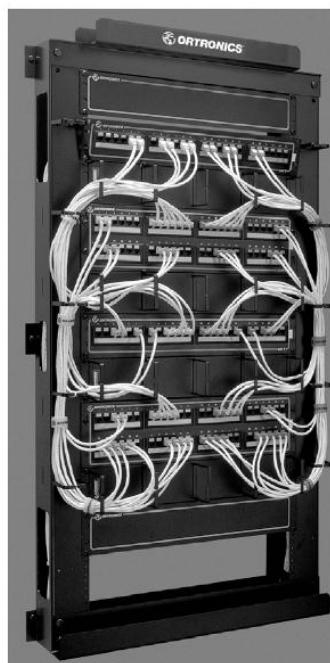
¹⁰ Skeletal frames

¹¹ Full Equipment Cabinets

¹² Cable Management



شکل (۱۱-۱) یک فریم اسکلتی ۱۹ اینچی



شکل (۱۲-۱) رک فریم اسکلتی The Ortronics Mighty Mo II با مدیریت کابل، نصب شده روی دیوار

تجهیزات داخل رک محدود به Patch Panel و تجهیزات ارتباطی (سوییچ و مسیریاب) نمی‌شوند. سروورها از جمله تجهیزات رایج نصب شده در رک هستند. قفسه‌های ابزار، قفسه‌ی مانیتور و قفسه‌ی کیبورد هم از جمله سایر تجهیزات قابل نصب در رک هستند. شکل (۱۳-۱) نمونه‌ای از این قفسه‌ها است.



شکل (۱۳-۱) نمونه‌هایی از قفسه برای رک‌های ۱۹ اینچی

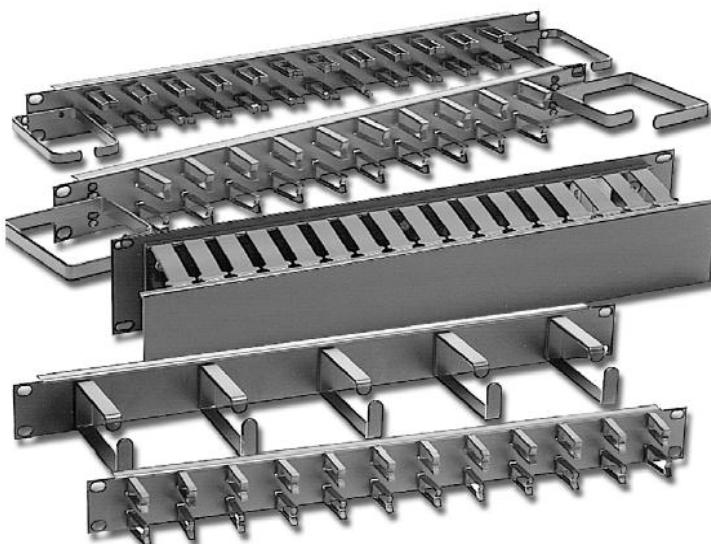
کابینت‌های کاملاً تجهیز شده، گران‌ترین گزینه برای انتخاب است. این کابینت‌ها امکان قفل درهای کابینت و فراهم کردن امنیت تجهیزات داخلی را دارند. این رک‌ها می‌توانند بسیار ساده و یا بسیار تجهیز شده (مثل سیستم خنک‌کننده‌ی داخلی و سیستم حفاظت از تداخل الکترومغناطیسی) باشند. شکل (۱۴-۱) یک کابینت را نشان می‌دهد.



شکل (۱۴-۱) یک کابینت کاملاً تجهیز شده

۱۰-۱-۲-۱- لوازم جانبی مدیریت کابل

این لوازم به مدیریت و نظم بخشی به کابل های ارتباطی، خصوصاً در رک هایی که قادر ابزار مدیریت سیم هستند، کمک می کنند. از جمله این ابزار می توان به آویزهای کابل^{۱۳} در قسمت جلو و یا پشت تجهیزات نصب شده در رک اشاره کرد. شکل (۱۵-۱) ابزار مدیریت کابل را نشان می دهد.



شکل (۱۵-۱) ابزار مدیریت کابل محصول MilesTek

۲-۲-۱- کابل کشی

۱-۲-۲-۱- قوانین

در کابل کشی قوانینی وجود دارد که برخی از آن ها را مرور می کنیم:

- برای کابل کشی افقی حداقل طول کابل ۹۰ متر باشد به علاوه اینکه طول Patch Cord های مورد استفاده در داخل قفسه های مخابراتی^{۱۴} باید بیشتر از ۵ متر شود.
- کابل های حامل داده را هرگز نباید به هم پیوند زد، اگر کابلی در نقطه ای دچار مشکل شد با کابل جدید جایگزین شود. اگر سیم های کابل آسیب دیده اند کابل را تعویض کنید.
- کابل ها را مستقیما روی سقف قرار ندهید، از سینی کابل، قلاب J^{۱۵}، نرده بان افقی^{۱۶} و یا روش های دیگر استفاده کنید.
- زمانی که در سیستم کابل کشی از داده و صدا پشتیبانی می شود برای خطوط صوتی از

¹³ Cable Hangers

¹⁴ Telecommunications Closet

¹⁵ J Hook

¹⁶ Horizontal Ladder

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.

۲-۲-۲-۱ - استاندارد کابل‌کشی ANSI/TIA-568-C

در اواسط دهه ۸۰ 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 غالباً تک منظوره انجام می‌شده است. انجمن صنعت ارتباطات کامپیوتر (CCIA) از اتحادیه صنعت الکترونیک^{۱۷} (EIA) درخواست توسعه یک استاندارد کابل‌کشی و ساخت‌یافته را کرد که در سال ۱۹۹۱، EIA و انجمن صنعت مخابرات^{۱۸} (TIA) اولین نسخه‌ی استاندارد کابل‌کشی مخابراتی ساختمان‌های تجاری را تحت عنوان ۵۶۸ ANSI/TIA/EIA به چاپ رساند. این استاندارد چندین بار بازنگری و بهروزرسانی شده است. در سال ۱۹۹۵ 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 ۲۰۰۱ یک بروزرسانی از استاندارد تحت عنوان ANSI/TIA/EIA-568-B منتشر شد. سرانجام در سال ۲۰۰۹ 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^{۱۹} های (RJ-45 و RJ-11) است. این استاندارد ترتیب سیم‌های کابل UTP را برای اتصال به پین^{۲۰} های سوکت بیان می‌کند که با T568A و T568B شناخته می‌شوند. در جدول (۱-۱) جزئیات این دو استاندارد بیان شده است.

¹⁷ Electronic Industries Alliance

¹⁸ Telecommunications Industry Association

¹⁹ Socket, Plug, Jack

²⁰ Pin

جدول (۱-۱) استانداردهای T568A و T568B

T568B		T568A	
شماره پین	رنگ	شماره پین	رنگ
۱	سفید-نارنجی	۱	سفید-سبز
۲	نارنجی	۲	سبز
۳	سفید-سبز	۳	سفید-نارنجی
۴	آبی	۴	آبی
۵	سفید-آبی	۵	سفید-آبی
۶	سبز	۶	نارنجی
۷	سفید-قهوه‌ای	۷	سفید-قهوه‌ای
۸	قهوه‌ای	۸	قهوه‌ای

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 به جز جفت ۲ و ۳ که جایه‌جا 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 (۲-۱) برخی از کاربردهای رایج و پین‌های استفاده شده در آن‌ها را نشان می‌دهد.

شكل (۱۶-۱) نحوه اتصال سیم‌های کابل UTP را طبق استانداردهای T568A و T568B بر روی پین‌های سوکت نشان می‌دهد. شکل (۱۷-۱) به صورت واضح سیم‌های رنگی متناسب با هر پین را نمایش داده است.

۱-۲-۲-۳- تفاوت سوکت‌های RJ-45 و RJ-11

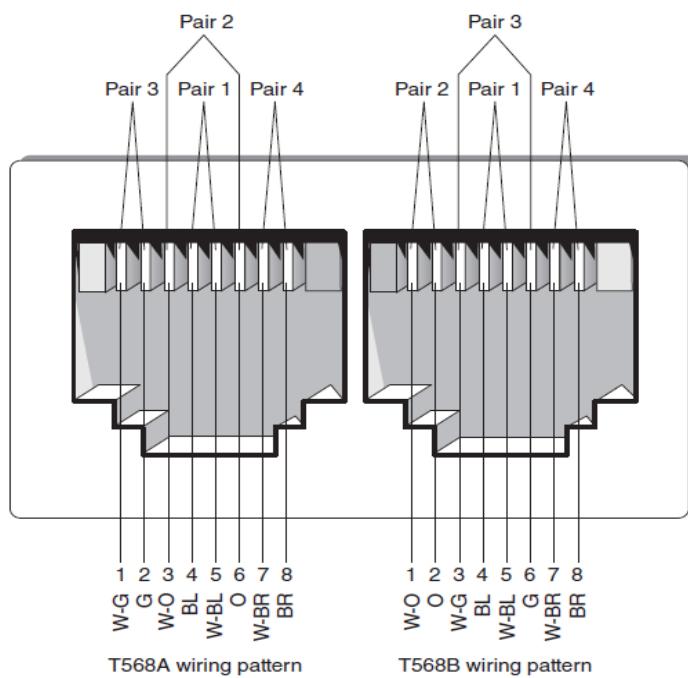
دودسته اصلی از سوکت^{۲۱} ها (نام دیگر آن‌ها پلاگ هست) برای اتصال به کابل‌های زوج سیم به هم تابیده استفاده می‌شود: RJ-45 و RJ-11

این دو سوکت اساساً مشابه هستند به جز آن که 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 (۱-۱۸) نشان داده شده‌اند. سوکت‌های RJ-11 position دارند اما به جای شش سطح تماس فلزی با دو سطح تماس فلزی پیکربندی شده‌اند دلیل این کار صرفه‌جویی در هزینه برای کاربردهای تلفنی است که تنها نیاز داریم دو سیم تماس داشته باشند.

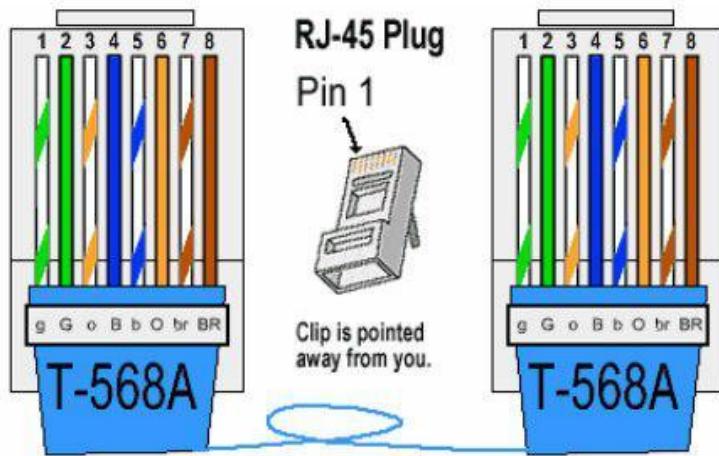
²¹ Socket, Plug, Jack

جدول (۲-۱) جفت کردن کابل‌های UTP متناسب با کاربردها

کاربرد	پین ۱ و ۲	پین ۳ و ۶	پین ۴ و ۵	پین ۷ و ۸
Analog voice	-	-	ارسال/دریافت	-
ISDN	Power	ارسال	دریافت	Power
10Base-T (802.3)	ارسال	دریافت	-	-
Token Ring (802.5)	-	ارسال	دریافت	-
100Base-TX (802.3u)	ارسال	دریافت	-	-
100Base-T4 (802.3u)	ارسال	دریافت	دوطرفه	دوطرفه
100Base-VG (802.12)	دوطرفه	دوطرفه	دوطرفه	دوطرفه
FDDI (TP-PMD)	ارسال	Optional	Optional	دریافت
ATM User Device	ارسال	Optional	Optional	دریافت
ATM Network Equipment	دریافت	Optional	Optional	ارسال
1000Base-T (802.3ab)	دوطرفه	دوطرفه	دوطرفه	دوطرفه
10GBase-T (802.3an)	دوطرفه	دوطرفه	دوطرفه	دوطرفه

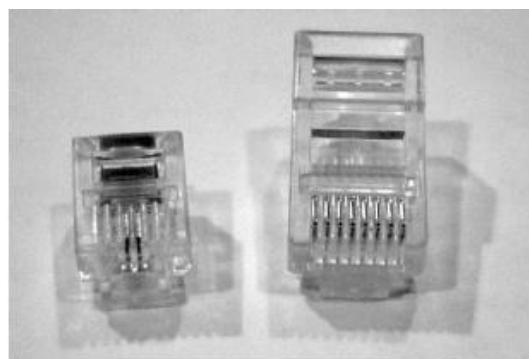


شکل (۱۶-۱) نحوه اختصاص سیم‌ها به پین‌های سوکت



شکل (۱۷-۱) 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.



شکل (۱۸-۱) به ترتیب از راست سوکت RJ-45 و RJ-11

نکته: دو سر انتهایی Patch Cord های مستقیم^{۲۲} با استانداردهای مشابه سیم‌کشی می‌شوند به عبارت دیگر برای هر دو سر انتهایی یا از استاندارد T568-B یا T568-A استفاده می‌شود. Patch Cord را به پریز ارتباطی و Patch Panel را به تجهیزات شبکه مانند هاب، سوئیچ و روتور متصل می‌کند. برای Patch Cord های متقطع^{۲۳} یکسر انتهایی با استاندارد T568-A و سر دیگر با استاندارد T568-B سیم‌کشی می‌شود. برای شبکه‌های Ethernet Patch Cord های متقطع مستقیماً PC ها را بدون واسطه هیچ تجهیز شبکه‌ای به هم متصل می‌کند. برای اتصال هاب‌ها، سوئیچ‌ها و

²² Straight Patch Cord

²³ Crossover Patch Cord

روترها به یکدیگر، متناسب به نوع تجهیزات در طرفین یا یک کابل مستقیم یا یک کابل متقطعه موردنیاز است.

۱-۳- قطعات و ابزارهای موردنیاز

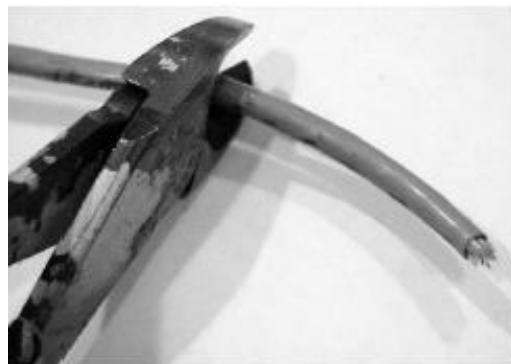
تجهیزات موردنیاز برای انجام این آزمایش به همراه عکس آنها در جدول (۱-۳) نشان داده شده است.

جدول (۱-۳) تجهیزات موردنیاز

نام تجهیز	مقدار موردنیاز	عکس
CAT5 رشته کابل	مقدار لازم	
RJ-45 سوکت	برای هر کابل دو عدد	
آچار Crimp یا آچار پرس	یک عدد	
شبکه Tester	یک عدد	
سیم چین	یک عدد	
کابل لخت کن	یک عدد	

۴-۱- شرح آزمایش

- با استفاده از سیمچین کابل را به اندازه دلخواه برش دهید، دقت کنید که کابل را باید ۳ اینچ (۷.۶۲ سانتی‌متر) بیشتر از طول کابل پچ نهایی برش بزنید (شکل (۱۹-۱)).



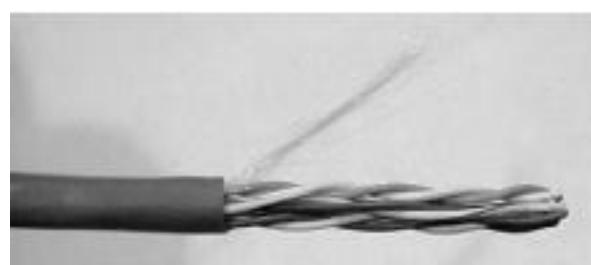
شکل (۱۹-۱) برش کابل

- با استفاده از کابل لخت کن پوسته‌ی کابل را جدا می‌کنید به این صورت که کابل لخت کن را حدود ۱.۵ اینچ (۳.۸۱ سانتی‌متر) از انتهای کابل قرار دهید و کابل لخت کن را دو بار دور کابل بچرخانید (شکل (۲۰-۱)).



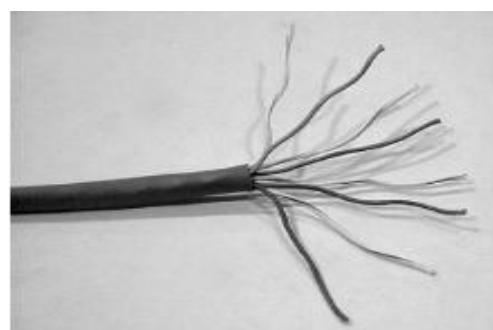
شکل (۲۰-۱) لخت کردن کابل

- 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 (۲۱-۱)).



شکل (۲۱-۱) کابل لخت شده

۴. تمامی سیم‌های داخلی را صاف کنید و آن‌ها را کاملاً از هم جدا کنید به صورتی که بتوان تمامی آن‌ها مانند شکل (۲۲-۱) را مشاهده کرد.



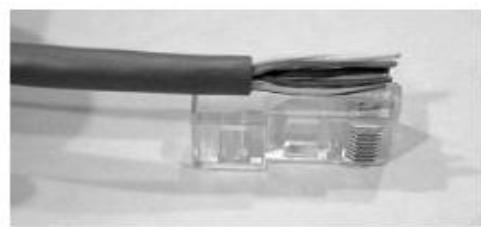
شکل (۲۲-۱) جداسازی سیم‌های داخلی

۵. هر کدام از سیم‌ها را مطابق با یکی از استانداردهای گفته شده در جدول (۲-۱) مانند شکل (۱-۱) مرتب کنید.



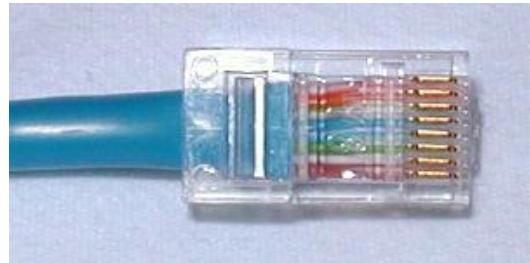
شکل (۱-۱) مرتب‌سازی رنگ‌ها بر اساس استاندارد T568B

۶. سیم‌های داخلی را مرتب کنید به صورتی که انتهای همگی آن‌ها در یک خط قرار بگیرند، اطمینان حاصل کنید که مانند شکل (۲۴-۱) پوسته‌ی کابل داخل سوکت RJ-45 قرار گیرد.



شکل (۲۴-۱) مرتب کردن سیم‌های داخلی

۷. 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 این که این مرحله آخرین گام قبل از پرس کردن با آچار Crimp هست، در انجام این مرحله دقت کنید (شکل (۲۵-۱)).



شکل (۲۵-۱) نحوه قرارگیری صحیح سیم‌های داخلی در سوکت

۸. طبق شکل (۲۶-۱) سوکت و کابل را داخل آچار Crimp قرار دهید، دسته آچار را محکم فشار دهید تا به انتهای برسد و در حدود سه ثانیه با فشار نگهدارید.



شکل (۲۶-۱) پرس کردن سوکت

۹. پس از آنکه پرس را انجام دادید، سوکت را از آچار Crimp جدا کنید. بررسی کنید تا همه سیم‌ها با پین‌های متناظر خود به درستی پرس شده‌اند. اگر سوکت به درستی پرس نشده باشد باید آن را برش دهید و تمامی مراحل را از ابتدا انجام شود.

۲- ابزارهای مدیریت شبکه‌های کامپیووتری

۱-۲- هدف آزمایش

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

مطالبی که در این آزمایش پوشش داده می‌شود عبارت‌اند از:

- مشاهده تنظیمات آدرس IP واسطه‌های شبکه
- استفاده از برنامه‌های خط فرمان شامل Tracert، Ping
- استفاده از ابزار Ping plotter

۲-۲- شرح آزمایش

۱-۲-۲- مشاهده تنظیمات آدرس IP واسطه‌های شبکه

با استفاده از دستور ipconfig /all اطلاعات مربوط به تنظیمات پروتکل IP واسطه‌های سیستم شما لیست خواهند شد. این اطلاعات شامل آدرس IP سیستم، ماسک شبکه، آدرس دروازه^{۲۴} شبکه، آدرس فیزیکی واسطه‌ها و آدرس سرور DNS است و به تفکیک واسطه‌ها نمایش داده خواهد شد. این دستور را می‌توانید در محیط CMD اجرا کنید. نمونه‌ای از خروجی این دستور در شکل (۲۷-۱) نمایش داده شده است.

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : ceit.local
Description . . . . . : Marvell Yukon 88E8040 PCI-E Fast Ethernet Controller
Physical Address. . . . . : 00-24-BE-7E-88-88
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::218b:a522:11f5:ac9e%16(Preferred)
IPv4 Address. . . . . : 172.23.154.77(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : Monday, November 6, 2017 4:24:42 AM
Lease Expires . . . . . : Friday, November 10, 2017 4:24:43 AM
Default Gateway . . . . . : 172.23.152.1
DHCP Server . . . . . : 172.23.128.25
DHCPv6 IAID . . . . . : 50341054
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-70-46-BB-00-24-BE-7E-88-88
DNS Servers . . . . . : 172.23.128.23
                                         172.23.128.22
NetBIOS over Tcpip. . . . . : Enabled
```

شکل (۲۷-۱) خروجی دستور ipconfig /all

²⁴ Gateway

توضیحات بخش‌های مهم شکل (۱-۲۷) در جدول (۴-۱) 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 169.169 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.

جدول (١-٤) 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 ۴ واسط شبکه
IPv6 Address	آدرس IP نسخه ۶ 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 شبکه‌ای شما در آن قرار دارد را مشخص می‌کند.

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

برنامه‌های خط فرمان مانند Ping، Tracert و Netstat 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 (۱-۲۸) در خط فرمان چاپ می‌شود.

سوال ۱: به نظر شما سوییچ ۱-چیست و چگونه عمل می‌کند؟

```

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -t             Ping the specified host until stopped.
                 To see statistics and continue - type Control-Break;
                 To stop - type Control-C.
  -a             Resolve addresses to hostnames.
  -n count       Number of echo requests to send.
  -l size        Send buffer size.
  -f             Set Don't Fragment flag in packet <IPv4-only>.
  -i TTL         Time To Live.
  -v TOS         Type Of Service <IPv4-only>. This setting has been deprecated
                 and has no effect on the type of service field in the IP Header.
  -r count       Record route for count hops <IPv4-only>.
  -s count       Timestamp for count hops <IPv4-only>.
  -j host-list   Loose source route along host-list <IPv4-only>.
  -k host-list   Strict source route along host-list <IPv4-only>.
  -w timeout     Timeout in milliseconds to wait for each reply.
  -R             Use routing header to test reverse route also <IPv6-only>.
  -S srcaddr    Source address to use.
  -4             Force using IPv4.
  -6             Force using IPv6.

```

شکل (۲۸-۱) خروجی دستور ping/?

۲-۳-۲-۲ ارزیابی ارتباط با سیستم‌های دیگر با استفاده از ابزارهای Tracert و Ping

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 (۲۹-۱) 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، ۷۹ میلی‌ثانیه است که نسبتاً مناسب است. این تاخیر معمولاً باید زیر ۱ ثانیه باشد. همچنین تمام بسته‌ها باید دریافت شده باشند. در شکل (۲۹-۱) مشاهده می‌کنید که هر چهار بسته ارسالی، دریافت شده‌اند. دریافت نکردن هر یک از بسته‌ها می‌تواند نشان از وجود مشکل در شبکه باشد.

```

ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=82ms TTL=48
Reply from 8.8.8.8: bytes=32 time=80ms TTL=48
Reply from 8.8.8.8: bytes=32 time=78ms TTL=48
Reply from 8.8.8.8: bytes=32 time=79ms TTL=48

Ping statistics for 8.8.8.8:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 82ms, Average = 79ms

```

شکل (۲۹-۱) خروجی دستور ping 8.8.8.8

سوال ۲: 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.

سوال ۳: 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 (۱-۳۰) داده شده است.

```
Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
```

```
1      2 ms      1 ms      6 ms  172.23.152.1
2      <1 ms      <1 ms      <1 ms  172.23.128.2
3      1 ms      <1 ms      <1 ms  172.16.4.4
4      1 ms      <1 ms      1 ms   172.29.1.3
5      *          *          *      Request timed out.
6      *          *          *      Request timed out.
7      *          *          *      Request timed out.
8      *          *          *      Request timed out.
9      *          *          *      Request timed out.
10     *          *          *      Request timed out.
11     *          *          *      Request timed out.
12     *          *          *      Request timed out.
13     8 ms       6 ms       6 ms   10.201.177.41
14     7 ms       6 ms       6 ms   10.10.53.190
15     14 ms      11 ms      12 ms  85.132.90.189
16     *          *          *      Request timed out.
17     84 ms      81 ms      80 ms  72.14.212.229
18     *          *          *      Request timed out.
19     126 ms     94 ms      164 ms 108.170.236.83
20     84 ms      83 ms      85 ms  google-public-dns-a.google.com [8.8.8.8]
```

Trace complete.

شکل (۱-۳۰) خروجی دستور tracert

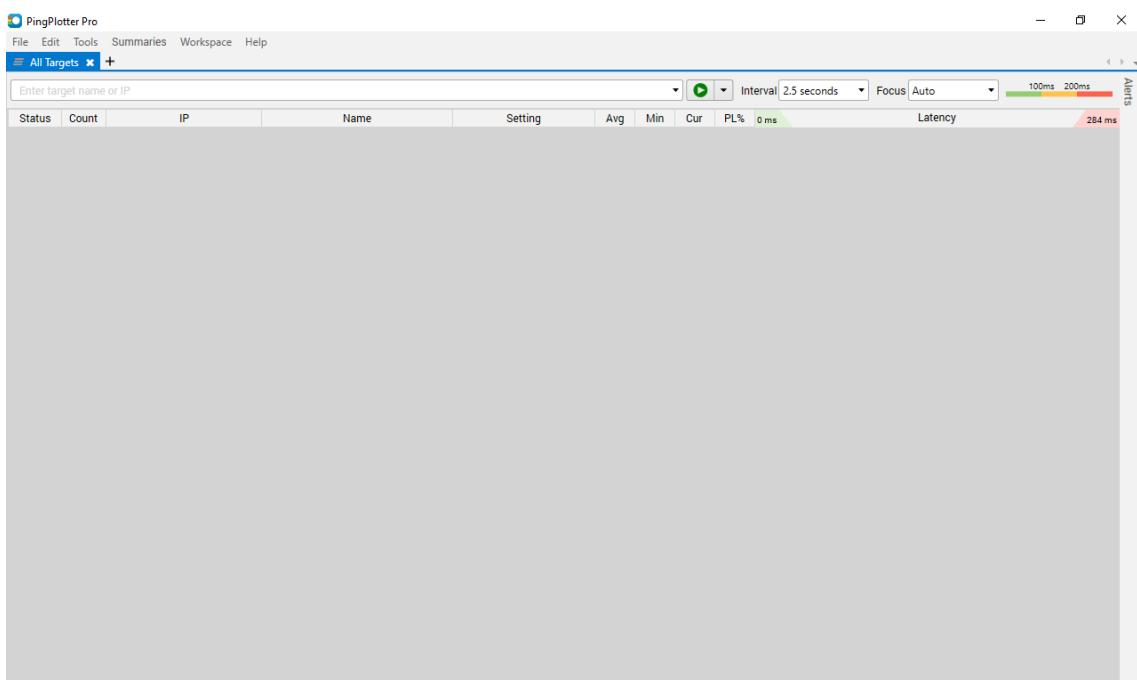
همان‌گونه که در این شکل مشاهده می‌شود، ستون اول از سمت چپ، بیانگر گام‌های عبور بسته است. هر گام بیانگر یک مسیریاب است. سه ستون بعدی بیانگر زمانی است که بین ارسال و دریافت بسته طول کشیده است. درنهایت ستون اول از سمت راست بیانگر آدرس IP مسیریاب در آن گام است.

سوال ۴: دستور tracert aut.ac.ir و tracert facebook.com و tracert google.com 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 Request timeout قرار facebook.com در بعضی از گامها به جای آدرس IP مسیریاب‌ها، گرفته است؟ آخرین آدرس IP در خروجی مربوط به facebook چه ارتباطی با دارد.

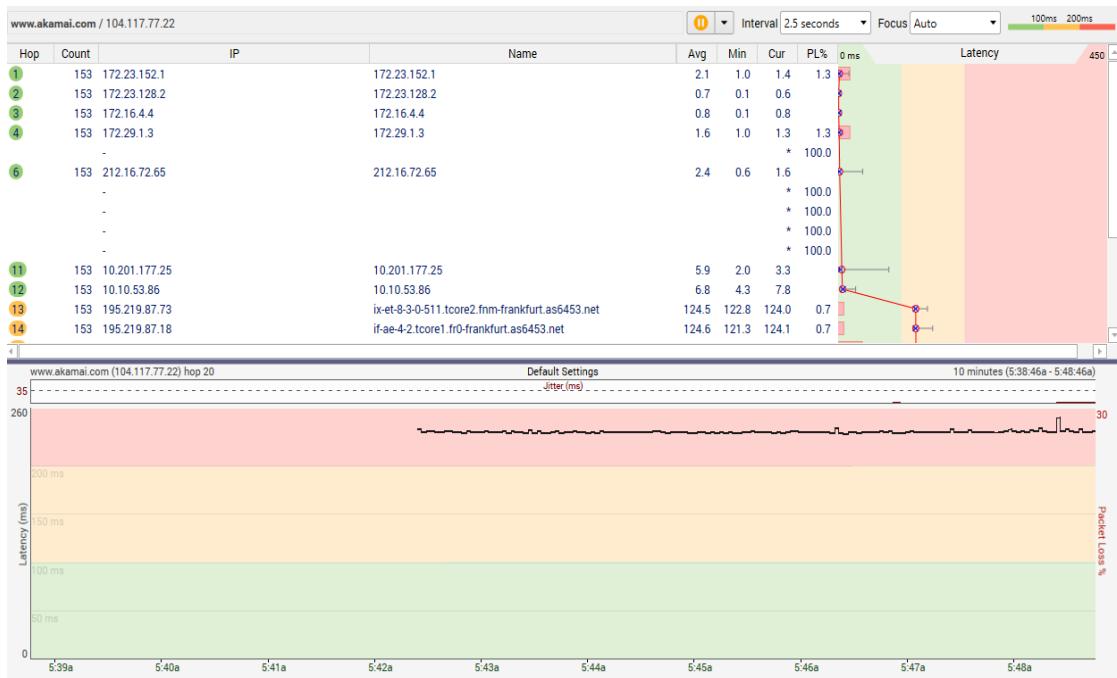
۴-۲-۲- استفاده از ابزار Ping Plotter

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 (۳۱-۱) نمایش داده شده است.



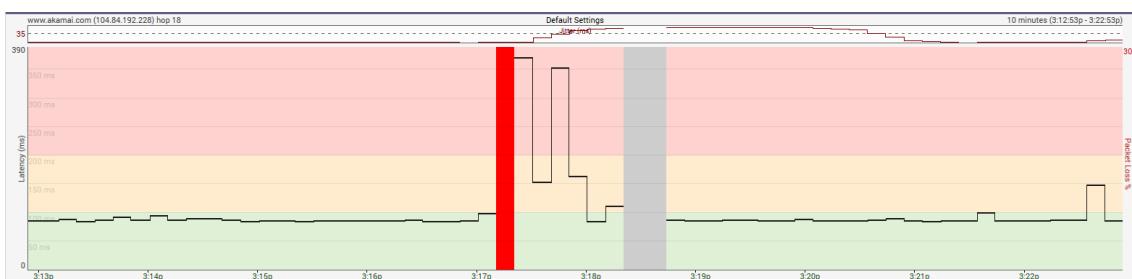
شکل (۳۱-۱) نمایی از ابزار Ping Plotter

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 (۳۲-۱) مشاهده می‌شود برنامه Ping Plotter با Ping کردن دائم مقصد، وضعیت تاخیر بسته‌های دریافتی را نظارت می‌کند.



شکل (۳۲-۱) صفحه کلی

همان گونه که در شکل بالا مشاهده می‌شود، تعداد گام‌های بسته‌ها 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 (۳۳-۱) نمایش داده شده است.



شکل (۳۳-۱) نمودار تاخیر بسته‌های دریافتی

مشاهده می‌شود که تاخیر بسته‌ها در ساعت ۳:۱۷ 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 (۳۴-۱) نمایش داده شده است.

IP	MAC Address	MAC Vendor	Hostname	Ping	Protocols	Description
172.23.152.131	6c:f0:49:70:2f:2e	GIGA-BYTE TECHNOLOGY CO.,LTD.	Montajab		UPnP ARP	MONTAJAB:bahman; MONTAJAB:montjab1983@hotmail.com; MONTAJAB:OMNeTpp; MONTAJAB
172.23.152.142	00:22:15:fa:fe:39	ASUSTek COMPUTER INC.	DESKTOP-2V91QVF		UPnP ARP	DESKTOP-2V91QVF
172.23.154.0	70:4d:7b:46:4c:45	ASUSTek COMPUTER INC.			UPnP ARP	Windows/10.0.14393 UPnP/1.1 BitTorrent(client)(native)/7100
172.23.152.182	f0:de:f1:e2:7e:eb	Wistron Infocomm (Zhongshan) Corporation	Armin-PC		UPnP ARP	ARMIN-PC
172.23.154.46	00:1f:d0:93:d9:5b	GIGA-BYTE TECHNOLOGY CO.,LTD.	roshanfekr-PC		UPnP ARP	ROSHANFEKR-PC:roshanfekr; Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
192.168.19.254	00:50:56:f5:a7:74	VMware, Inc.			ARP	
192.168.83.254	00:50:56:f8:f8:0c	VMware, Inc.			ARP	
172.23.152.1	04:6c:9d:27:9e:d8	Cisco Systems, Inc			ARP	
172.23.154.61	b8:70:f4:83:c4:82	COMPAL INFORMATION (KUNSHAN) CO., LTD.	MAHDI		ARP UPnP	mahdi
192.168.170.6					mDNS	Professor
172.23.152.112	d4:85:64:1a:aa:9a	Hewlett Packard			mDNS ARP	HP LaserJet P2035n
172.23.152.126	78:24:af:42:f2:6f	ASUSTek COMPUTER INC.	DESKTOP-3PU37OR		UPnP ARP	DESKTOP-3PU37OR
172.23.153.28	74:d0:2b:c5:c2:e7	ASUSTek COMPUTER INC.			mDNS ARP	570323970
172.23.152.209	e0:cb:4e:89:c3:f2	ASUSTek COMPUTER INC.			mDNS ARP	227356191
172.23.152.132	40:8d:5c:71:79:53	GIGA-BYTE TECHNOLOGY CO.,LTD.			mDNS ARP	944109430
172.23.152.224	1c:1b:0d:39:42:c5	GIGA-BYTE TECHNOLOGY CO.,LTD.	DESKTOP-L3ALBT3		mDNS ARP	769263051

شکل (۱-۳۴) 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.

سوال ۵: با استفاده از ping و ipconfig آدرس فیزیکی دروازه شبکه و یکی از دوستان خود را پیدا کنید.

۳- آشنایی با نرم افزار Wireshark

۱-۳- هدف آزمایش

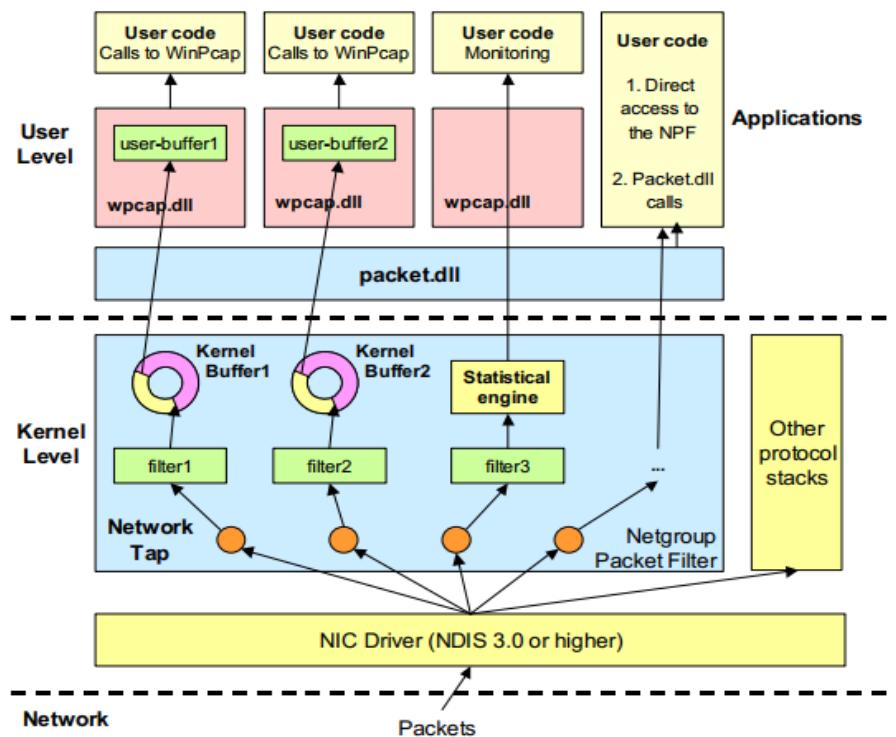
هدف از این آزمایش آشنایی با نرم افزار Wireshark و بررسی پروتکل‌ها در لایه مختلف سیستم عامل‌های خانواده ویندوز و لینوکس است که به شما اجازه می‌دهید ترافیک شبکه خود را تحلیل کنید. پروژه‌ی Wireshark در سال ۱۹۹۸ با نام Ethereal توسط Gerald Combs آغاز شد. این پروژه در سال ۲۰۰۶ به Wireshark تغییر نام داد. این نرم افزار توسط چهارچوب Qt و با زبان C/C++ نوشته شده است. این برنامه قادر به تحلیل برخط بیش از ۱۰۰۰ پروتکل در نسخه ۱.۱۰.۶ است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه‌های شنود و تحلیل دیگر مانند Microsoft Network Monitor، TCPdump

برنامه Wireshark تحلیل کننده پروتکل و شنود کننده ارتباط متن باز بر روی سیستم عامل‌های 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 نرم افزار توسط چهارچوب Qt و با زبان C/C++ نوشته شده است. این برنامه قادر به تحلیل برخط بیش از ۱۰۰۰ پروتکل در نسخه ۱.۱۰.۶ است. همچنین قادر به خواندن اطلاعات خروجی انواع برنامه‌های شنود و تحلیل دیگر مانند Microsoft Network Monitor، TCPdump

Plaintext، PostScript، CSV، XML

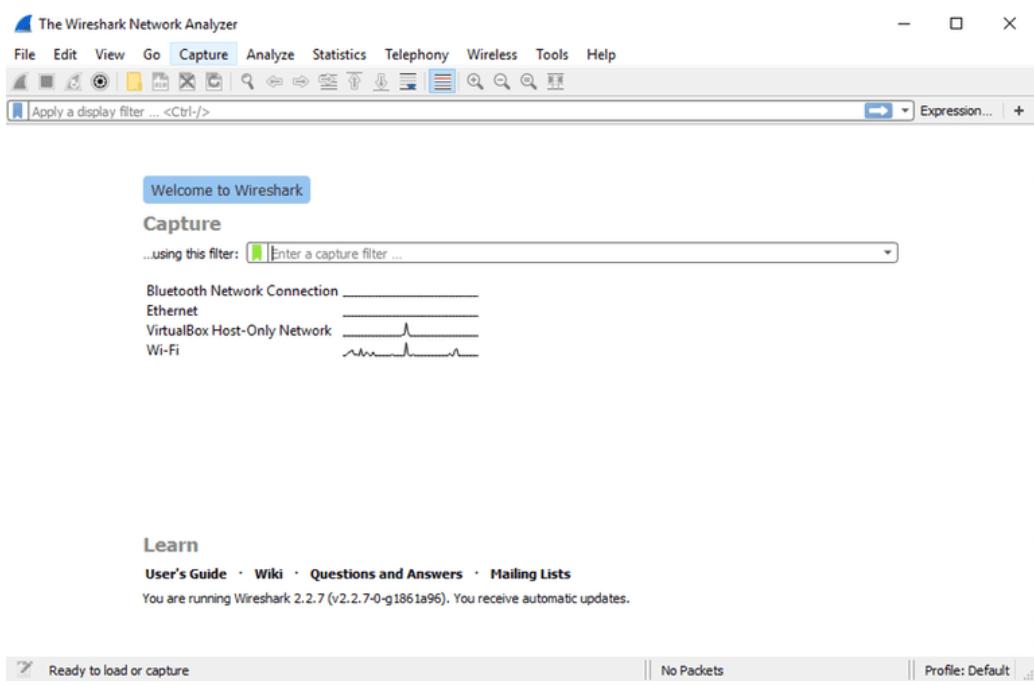
در سیستم عامل خانواده ویندوز، برنامه Wireshark شنود بسته‌ها با استفاده از کتابخانه Winpcap انجام می‌دهد. معماری نرم افزار Winpcap در شکل (۳-۵-۱) نمایش داده شده است. همان‌گونه که در این شکل مشخص است، برنامه Winpcap از دو بافر یکی در سطح کرنل و دیگری در سطح کاربر، یک ماشین فیلتر کننده که فیلترهایی را به بسته‌ها اعمال می‌کند و همچنین دو فایل packet.dll و wpcap.dll که این‌ترفیس‌های 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 «صرفًا بسته‌های پروتکل UDP دریافت شوند» تعریف کند. بسته‌ها پس از اینکه توسط گرداننده شبکه، از واسطه شبکه خوانده شدند جمع‌آوری می‌شوند؛ بنابراین کارایی Winpcap وابسته به گرداننده شبکه است. همچنین مشخص است که صرفاً یک کپی از بسته‌ها توسط Winpcap دریافت می‌شود و بسته‌ها هم‌زمان می‌توانند پسته پروتکلی سیستم عامل که در شکل با نام Other protocol stack مشخص شده است را طی کنند.



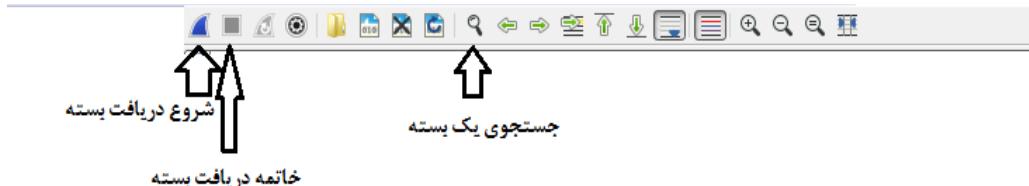
شکل (۳۵-۱) معماری نرم‌افزار Wireshark

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 (۳۶-۱) نمایش داده می‌شود.



شکل (۳۶-۱) صفحه اول برنامه

واسط شبکه‌ای که به اینترنت متصل است را انتخاب کنید. در ادامه برنامه شروع به دریافت بسته‌ها از کارت شبکه می‌کند. معمولاً 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 (۱-۳۷) نمایش داده شده است.



شکل (۱-۳۷) 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 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 در شکل (۱-۳۸) نمایش داده شده است.

The screenshot displays the Wireshark interface with several annotations:

- Annotations above the packet list:**
 - شمارشگر بسته‌ها (Packet number): Points to the first column of the packet list.
 - زمان دریافت بسته (Time): Points to the second column of the packet list.
 - آدرس مبدأ (Source): Points to the third column of the packet list.
 - آدرس مقصد (Destination): Points to the fourth column of the packet list.
- Annotations below the packet list:**
 - سرآیند پروتکل‌ها در لایه‌های مختلف یک بسته (Protocols in different layers of a single packet): A callout box pointing to the bottom of the list pane, containing the text '(در صورت وجود، به همراه داده لایه کاربرد)'.
 - نمایش Hex یک بسته (Hex view of a packet): A callout box pointing to the bottom of the details pane.

No.	Time	Source	Destination	Protocol	Length	Info
319	13.155301	172.24.72.86	172.24.72.11	HTTP	251	251 GET /WFADevice.xml HTTP/1.1
320	13.155969	172.24.72.15	172.24.72.86	TCP	62	1990 + 16600 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
321	13.156037	172.24.72.86	172.24.72.15	TCP	54	16600 + 1990 [ACK] Seq=1 Ack=1 Win=64240 Len=0
322	13.156276	172.24.72.86	172.24.72.15	HTTP	251	GET /WFADevice.xml HTTP/1.1
323	13.156966	172.24.72.17	172.24.72.86	TCP	60	1990 + 16597 [ACK] Seq=1 Ack=198 Win=6432 Len=0
324	13.157388	172.24.72.86	172.24.72.240	TCP	62	16602 + 50142 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
325	13.157966	172.24.72.17	172.24.72.86	TCP	156	1990 + 16597 [PSH, ACK] Seq=1 Ack=198 Win=6432 Len=102 [TCP segment of a reassembled PDU]
326	13.159462	172.24.72.86	172.24.72.18	TCP	62	16603 + 49152 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
327	13.160375	172.24.72.86	172.24.72.16	TCP	62	16604 + 1990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
328	13.167780	172.24.72.86	172.24.72.13	TCP	62	16605 + 1990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
329	13.172968	172.24.72.17	172.24.72.86	HTTP/XML	1054	HTTP/1.1 200 OK
330	13.173048	172.24.72.86	172.24.72.17	TCP	54	16597 + 1990 [ACK] Seq=198 Ack=1104 Win=63138 Len=0

Frame 326: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_11:b1:f6 (90:fc:52:11:b1:f6), Dst: BelkinIn_63:a8:2c (b4:75:0e:63:a8:2c)
 Internet Protocol Version 4, Src: 172.24.72.86, Dst: 172.24.72.18
 Transmission Control Protocol, Src Port: 16603, Dst Port: 49152, Seq: 0, Len: 0

شکل (۱-۳۸) بخش‌های مهم نرم‌افزار wireshark

۳-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- برنامه Wireshark نسخه ۲ به بعد
- یک کامپیوتر با سیستم‌عامل ویندوز ۷ به بعد با دسترسی به اینترنت

۴-۴- شرح آزمایش

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

۱-۴-۱- 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.

سوال ۱: به یک بخش دلخواه از بسته‌های شنود شده مراجعه کنید. چه پروتکل‌هایی را مشاهده می‌کنید. لیست آن‌ها را یادداشت کنید.

سوال ۲: یک بسته را به دلخواه 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 ۳ چقدر است؟

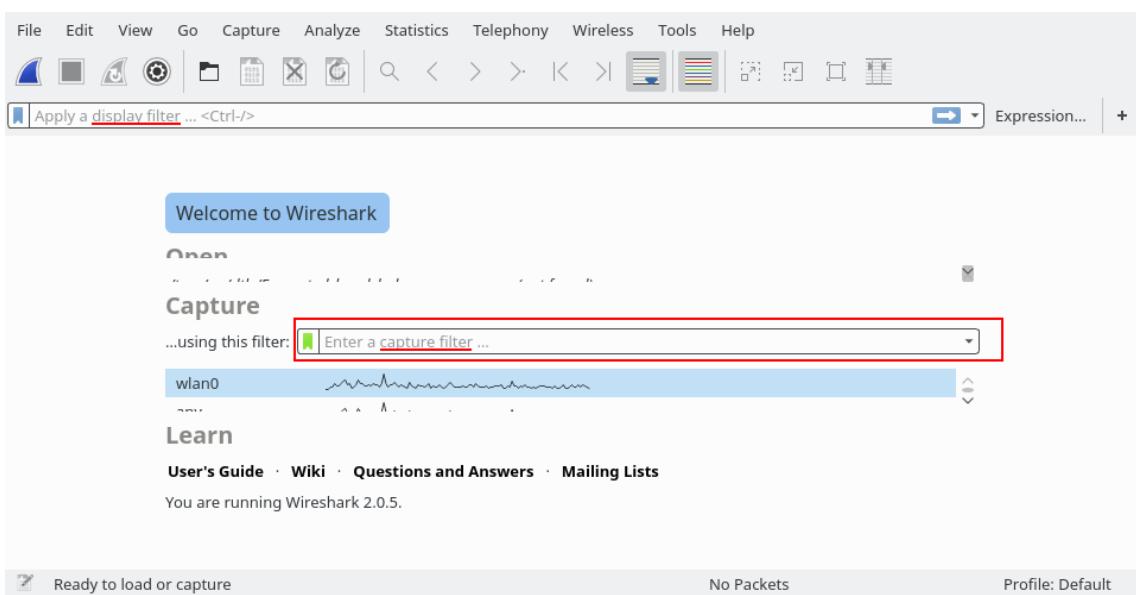
سوال ۳: آیا می‌توانید بسته‌هایی را پیدا کنید که بدون پروتکل‌های لایه‌های Application و Transport Network باشند؟ این بسته‌ها از چه پروتکلی استفاده کرده‌اند؟

سوال ۴: 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.

سوال ۵: 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 مبدأ و مقصد را یادداشت کنید. به نظر شما این اعداد در مبدأ و مقصد چه چیزی را مشخص می‌کند؟ Checksum مربوط به پروتکل‌های TCP و UDP را مشخص کنید.

۳-۴-۲- کار با فیلتر کننده بسته‌ها

برنامه Wireshark دو نوع فیلتر کننده بسته دارد. یک نوع Capture Filter است و نوع دیگر Capture Filter .Display 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 صرفاً مربوط به فیلتر کردن بسته‌های جمع‌آوری شده است. با استفاده از Display Filter می‌توان تعدادی از بسته‌های جمع‌آوری شده را مشخص کرد که در پنجه Wireshark نمایش داده شوند. این تفاوت در شکل (۱-۳۹) نیز نمایش داده شده است.



شکل (۱-۳۹) انواع فیلتر بسته

۳-۴-۲-۱- کار با Capture Filter

۱. به صفحه اول برنامه بروید و در قسمت Capture Filter، مقدار port 53
۲. را وارد کنید. درنهایت اینترفیسی که به اینترنت دسترسی دارد را انتخاب کنید.
۳. 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 صرفاً بسته‌های پروتکل DNS را در Wireshark مشاهده کنید.

سوال ۶: 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.

سوال ۷: کدامیک از آدرس‌های پیدا کرده در بخش قبل را می‌توانید در خروجی دستور /all ipconfig مشاهده کنید؟

سوال ۸: 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؟

سوال ۹: 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؟

سوال ۱۰: به نظر شما چه type های دیگری ممکن است وجود داشته باشد؟ سه مورد را یادداشت کنید.

۴-۳-۲-۲-۲- کار با Display Filter

۱. دوباره به صفحه اول برنامه بروید. این بار اینترفیس را بدون هیچ Capture Filter ای انتخاب کنید.

۲. در CMD دستور زیر را وارد کنید.

tracert p30download.com

منتظر بمانید تا کار دستور به اتمام برسد.

۳. بدون اینکه شنود بسته را متوقف کنید در قسمت display filter مقدار dns را تایپ کنید و اینتر را بزنید. مشاهده می‌کنید که صرفاً بسته‌های مربوط به پروتکل DNS انتخاب شدند در حالی که سایر بسته‌ها نیز در حال دریافت شدن از گرداننده کارت شبکه هستند.

۴. از قسمت سمت راست Display Filter، بر روی Expression کلیک کنید. صفحه مطابق شکل (۴۰-۱) باز می‌شود. IP را جستجو کنید و IPv4 را از ستون سمت چپ انتخاب کنید.

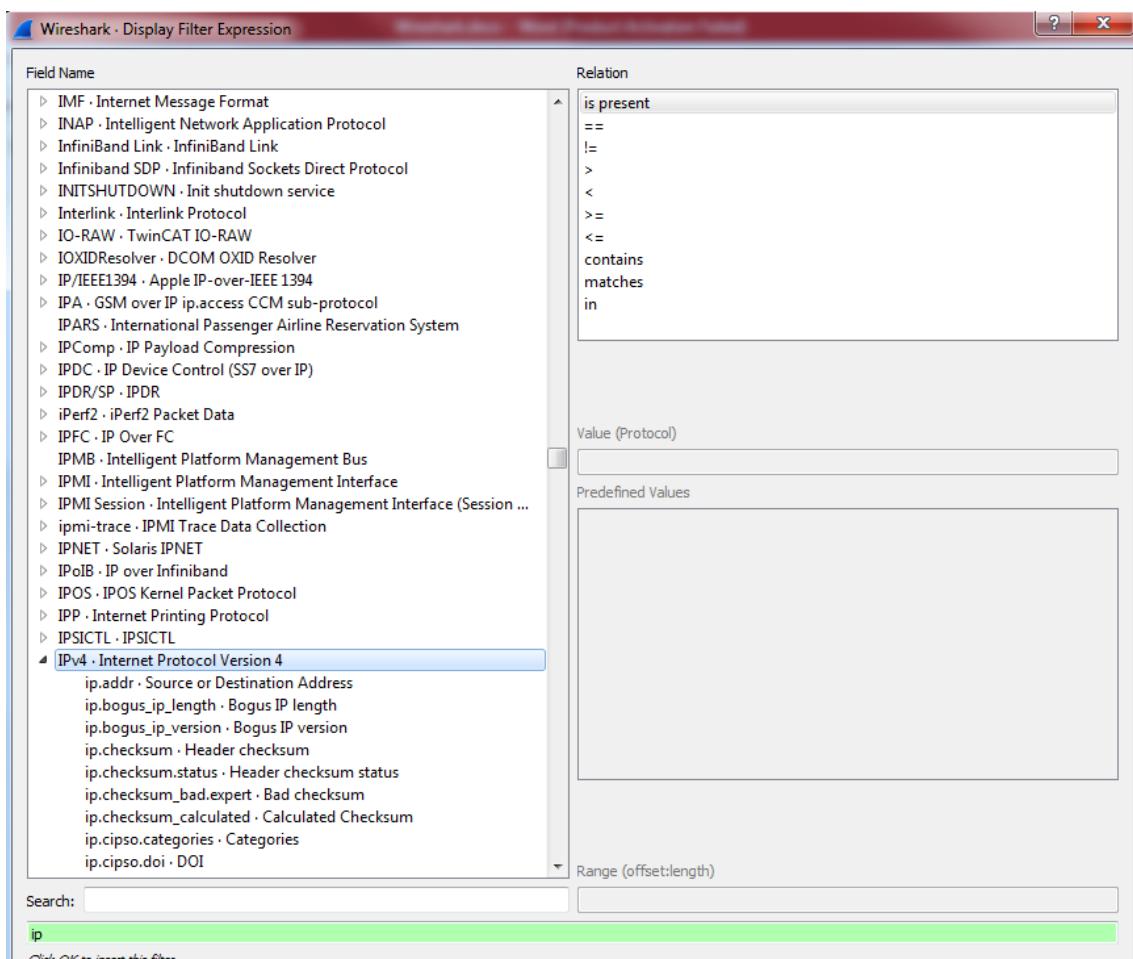
۵. از زیر بخش‌های IPv4، بخش ip.addr را انتخاب کنید. سپس از بخش relation، مقدار == را انتخاب کرده و در بخش Value آدرس IP که از دستور tracert به شما گزارش شده است را وارد کنید. به عنوان مثال برای آدرس p30download.com مشابه شکل (۴۱-۱) است.

سوال ۱۱: بعد از کلیک کردن بر روی OK چه اتفاقی می‌افتد؟ در بسته‌هایی که مشخص شده‌اند چه پروتکل‌هایی را مشاهده می‌کنید؟

سوال ۱۲: 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.

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

سوال ۱۳: به نظر شما هدف از تغییر این مقدار چیست؟ می‌توانید با مراجعه به هدف دستور tracert آن را شرح دهید.



شكل (۱۰-۱) انتخاب Display Filter

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

سوال ۱۴: این فیلتر چه کاری انجام می‌دهد؟

Field Name	Relation
<ul style="list-style-type: none"> ▷ ipmi-trace - IPMI Trace Data Collection ▷ IPNET - Solaris IPNET ▷ IPoIB - IP over Infiniband ▷ IPOS - IPOS Kernel Packet Protocol ▷ IPP - Internet Printing Protocol ▷ IPSICTL - IPSICTL ▷ IPv4 - Internet Protocol Version 4 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ip.addr - Source or Destination Address ip.bogus_ip_length - Bogus IP length ip.bogus_ip_version - Bogus IP version ip.checksum - Header checksum ip.checksum.status - Header checksum status ip.checksum._bad.expert - Bad checksum ip.checksum_calculated - Calculated Checksum ip.cipso.categories - Categories ip.cipso.doi - DOI ip.cipso.malformed - Malformed CIPSO tag ip.cipso.sensitivity_level - Sensitivity Level ip.cipso.tag_data - Tag data ip.cipso.tag_type - Tag Type ip.cur_rt - Current Route ip.cur_rt_host - Current Route Host ip.dsfield - Differentiated Services Field ip.dsfield.dsdp - Differentiated Services Codepoint ip.dsfield.ecn - Explicit Congestion Notification ip.dst - Destination ip.dst_host - Destination Host ip.empty_rt - Empty Route ip.empty_rt_host - Empty Route Host ip.evil_packet - Packet has evil intent ip.flags - Flags ip.flags.df - Don't fragment ip.flags.mf - More fragments ip.flags.rb - Reserved bit ip.flags.sf - Security flag 	is present == != > < >= <=br/> in
	Value (IPv4 address) 5.144.130.116 Predefined Values
Search:	Range (offset:length)
ip.addr == 5.144.130.116 Click OK to insert this filter	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

شکل (٤١-١) مقدار برای p30download.com

فصل ۲: لایه کاربرد

۱- راهاندازی سرویس‌های Web و FTP

۱-۱- هدف آزمایش

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

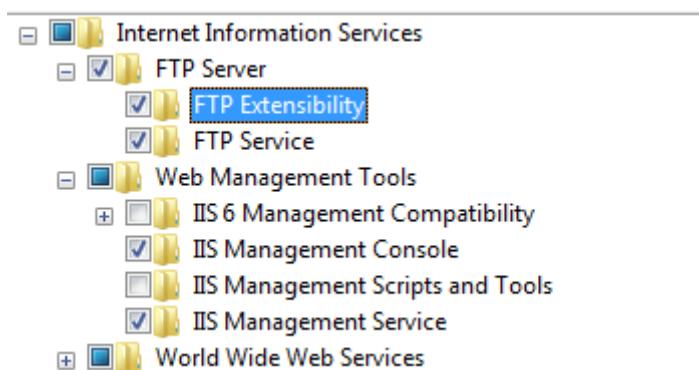
۱-۲- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم‌عامل ویندوز ۷ برای هر گروه
- برنامه Filezilla نسخه ۳.۱۷.۰.۱

۱-۳- شرح آزمایش

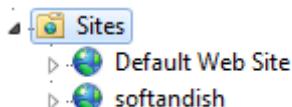
ابتدا تنظیمات مربوط به سرور Web را انجام می‌دهیم. سپس تنظیمات FTP Server را بررسی می‌کنیم. برای این منظور ابتدا عبارت Turn windows features on or off را در قسمت جستجوی ویندوز ۷، جستجو کنید. سپس بخش‌های زیر را از پنجره نمایش داده شده، انتخاب نمایید و بر روی OK کلیک کنید. دقت کنید هر سه بخش FTP Server، Web Management Tools و Web Management Tools FTP Server مانند شکل (۱-۲) تیک خورده باشند.



شکل (۱-۲) پیش تنظیمات

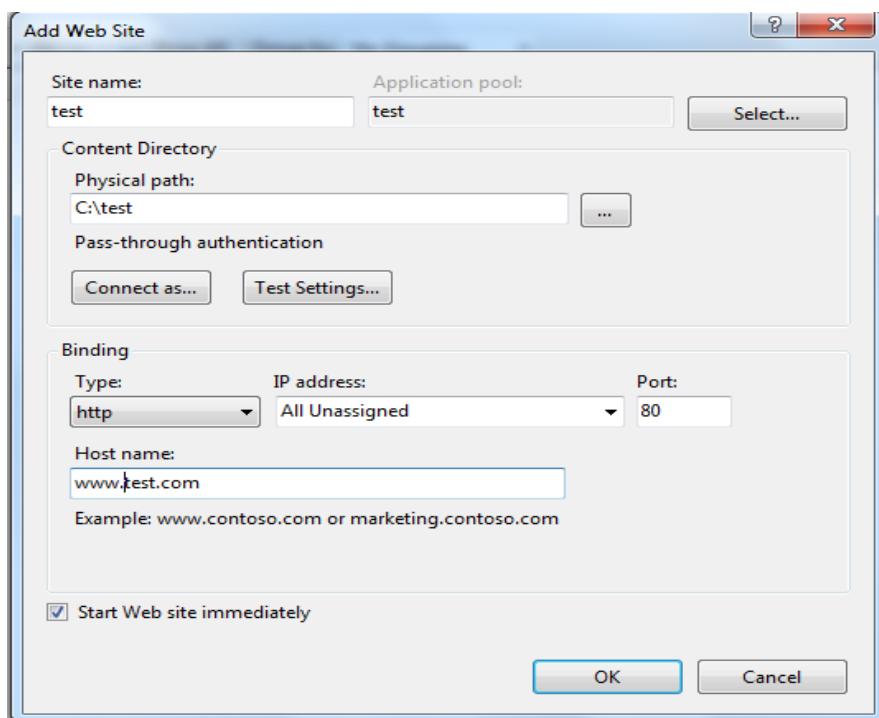
۱-۳-۱- تنظیمات سرور Web

۱. 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.



شکل (۲-۲) مرحله اول

۲. 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.



شکل (۳-۲) مرحله دوم

۳. مشاهده می‌کنید که به صورت پیشفرض سایت بر روی تمام آدرس‌های IP دستگاه و بر روی پورت ۸۰ bind می‌شود. با زدن دکمه OK سایت ایجاد می‌شود.
۴. 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.

```

index.html
1 <html>
2   <head>
3     <title>
4       Hello
5     </title>
6   </head>
7   <body>
8     Hello World!
9   </body>
10  </html>

```

شکل (۴-۲) مرحله سوم

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

سوال ۱: سایتی که ایجاد کرده‌اید نمایش داده نمی‌شود، چرا؟

۶. به آدرس C:\Windows\System32\drivers\etc hosts در سیستم بروید و فایل را با یک ویرایشگر مانند Notepad++ باز کنید. خط زیر را به آن اضافه کنید. دقت کنید که Host name خود را به جای www.test.com قرار دهید.

127.0.0.1 www.test.com

شکل (۵-۲) مرحله چهارم

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

سوال ۲: 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؟

۸. 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.

۹. در محیط cmd به محل فایل rawcap.exe بروید. آن را با دستور نشان داده شده در شکل (۶-۲) اجرا کنید

```

C:\test>RawCap.exe 127.0.0.1 test.pcap
Sniffing IP : 127.0.0.1
File        : test.pcap
Packets    : 10

```

شکل (۶-۲) دستورات اجرایی در cmd

۱۰. 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.

۱۱. فایل ذخیره شده 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. شکل مشابه شکل (۷-۲) نمایش داده خواهد شد.

No.	Time	Source	Destination	Protocol	Length	Info
58	5.996343	127.0.0.1	127.0.0.1	TCP	48	7391 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 SACK_PERM=1
59	5.996343	127.0.0.1	127.0.0.1	TCP	48	80 → 7391 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65495 SACK_PERM=1
60	5.996343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
61	5.996343	127.0.0.1	127.0.0.1	HTTP	580	GET / HTTP/1.1
62	5.996343	127.0.0.1	127.0.0.1	TCP	40	80 → 7391 [ACK] Seq=1 Ack=541 Win=7652 Len=0
63	5.998343	127.0.0.1	127.0.0.1	HTTP	337	HTTP/1.1 200 OK (text/html)
64	5.998343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=541 Ack=298 Win=7895 Len=0

شکل (۷-۲) نمونه‌ای از خروجی Follow HTTP Stream

سوال ۳: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

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

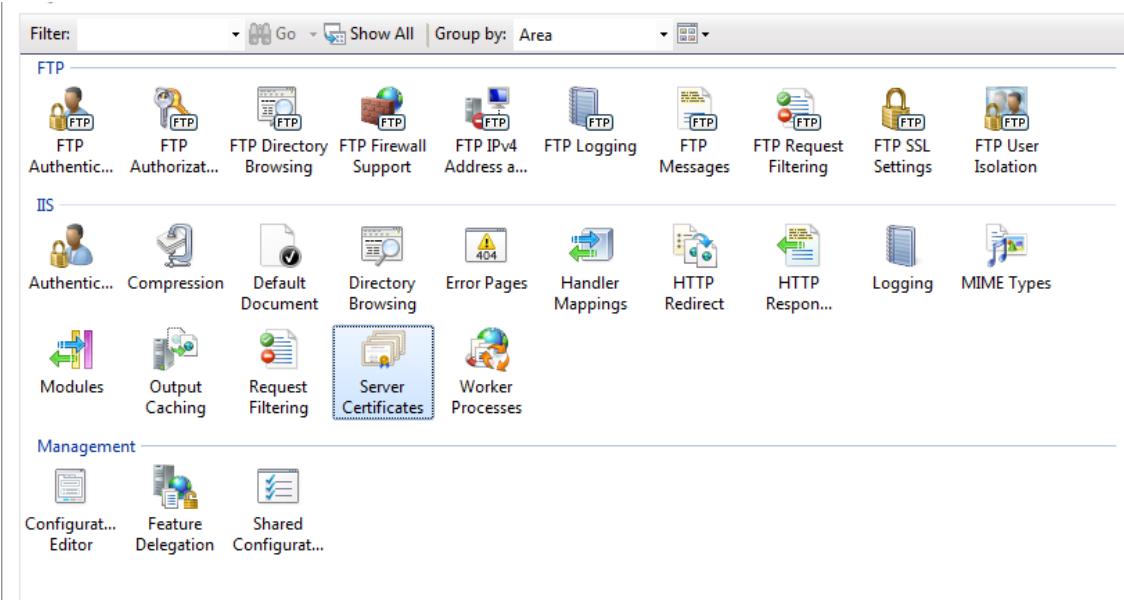
سوال ۴: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟

سوال ۵: 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؟

سوال ۶: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

سوال ۷: در مرورگر آدرس 127.0.0.1 را تایپ کنید. چرا هیچ‌کدام از سایت‌ها نمایش داده نمی‌شوند؟

۱۳. دوباره به محیط IIS Manager بروید. این بار در ستون سمت چپ بر روی نام کامپیوتر کلیک کنید. صفحه نمایش داده شده در شکل (۸-۲) باز می‌شود.



شکل (۸-۲) صفحه نمایش داده شده بعد از انتخاب نام کامپیوتر

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

Name	Issued To	Issued By	Expiration Date	Certificate Hash
softandish.com		Let's Encrypt Authority X3	6/7/2017 12:31:00 ...	5694FF79696224530AA463F5E227A5355DEA3F3

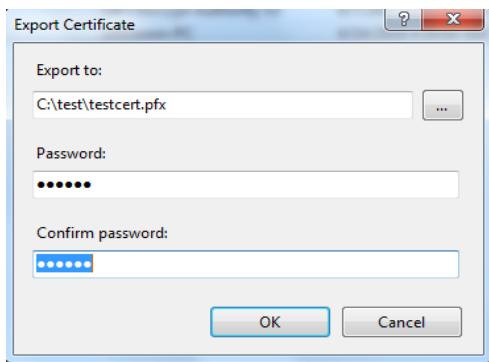
شکل (۹-۲) انتخاب Create Self-Signed Certificate

۱۵. یک نام برای آن انتخاب کنید و بر روی OK کلیک کنید. بهتر است نام انتخابی مطابق نام سایت باشد؛ مثلاً *.test.com مطابق شکل (۱۰-۲) ساخته می‌شود.

*.test.com PC PC 4/14/2018 4:30:00 AM B9408697274CA8457F474603DC.

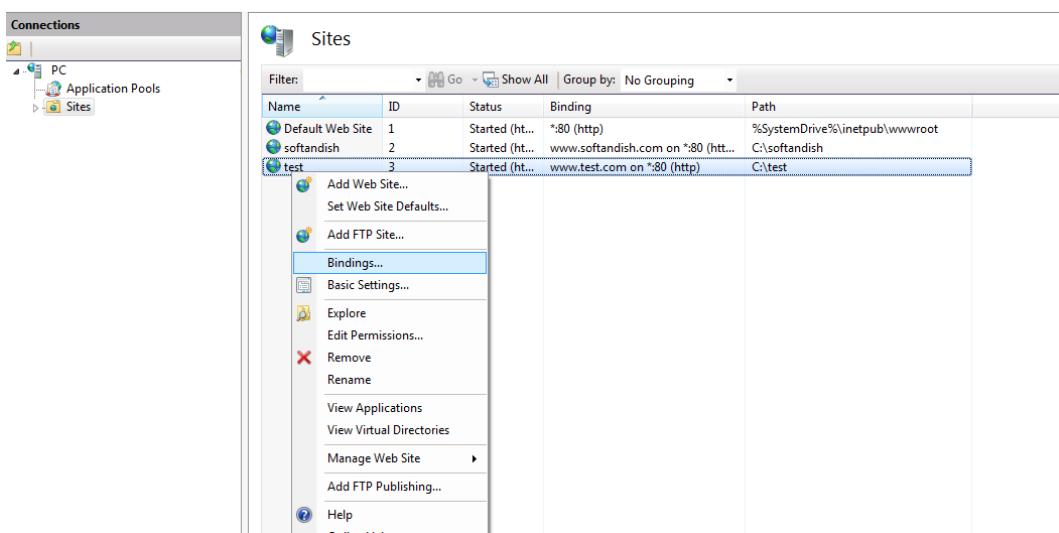
شکل (۱۰-۲) نمونه گواهی ساخته شده

۱۶. اگر بر روی گواهی ساخته شده کلیک راست کرده و export را کلیک کنید صفحه نشان داده شده در شکل (۱۱-۲) نمایش داده می‌شود. آن را کامل کرده و گواهی را export کنید. هر پسورد دلخواهی که می‌خواهید در بخش Password قرار دهید.



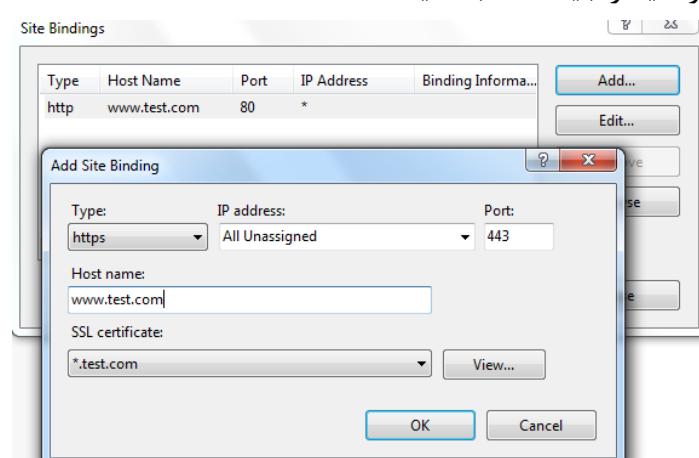
شکل (۱۱-۲) نحوه export گواهی

۱۷. 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.



شکل (۱۲-۲)- مرحله اول Binding

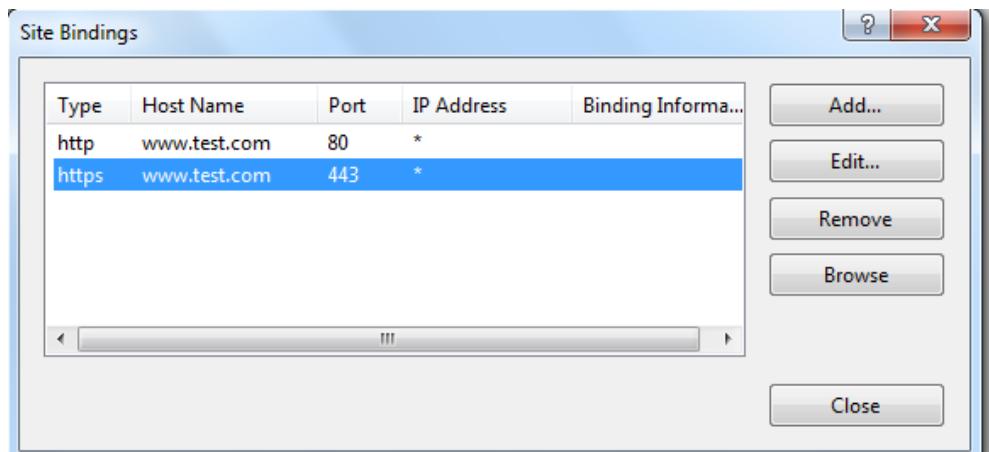
۱۸. بر روی Add کلیک کنید و مطابق شکل (۱۳-۲) آن را تکمیل کنید. دقت کنید که گواهی که خودتان ایجاد کردہاید را باید انتخاب کنید.



شکل (۱۳-۲)- مرحله دوم Binding

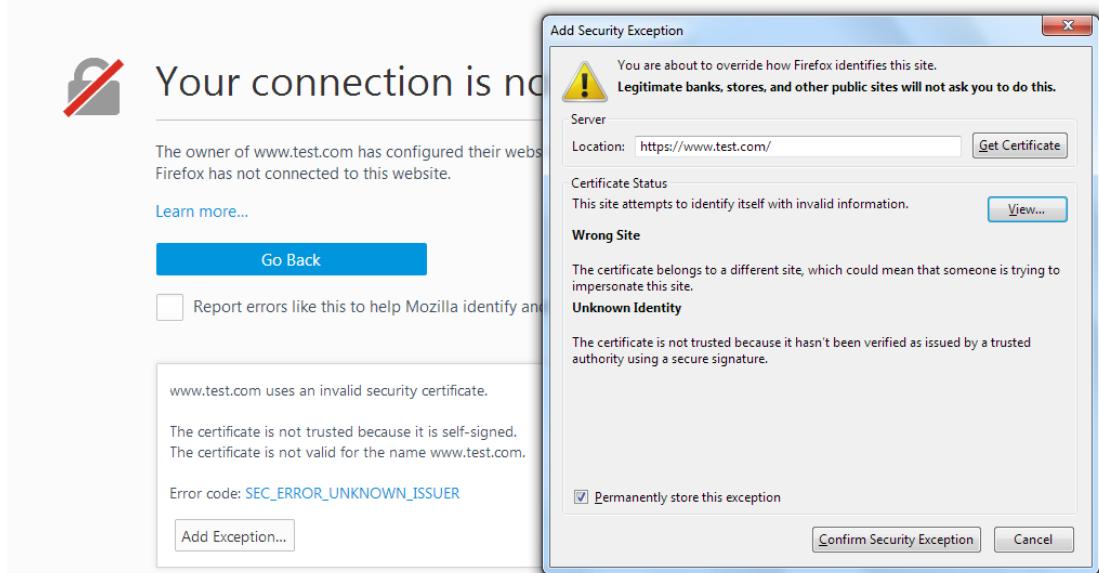
۱۹. بر روی OK کلیک کنید. حالا Binding های نشان داده شده در شکل (۱۴-۲) را دارید.
۲۰. حال آدرس [/https://www.test.com](https://www.test.com) را در مرورگر خود باز کنید. دقت کنید که به جای آدرس سایت خود را قرار دهید.

سوال ۸: آیا با مشکلی مواجه شدید؟ اگر با مشکل مواجه شدهاید با استفاده از rawcap مشخص کنید که چه مشکلی وجود دارد.



شکل (۱۴-۲)- مرحله سوم-Binding

۲۱. سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل (۱۵-۲) نمایش داده می‌شود.



شکل (۱۵-۲) خطای نمایش داده شده

۲۲. بر روی Add exception کلیک کرده و دکمه View را فشار دهید.
- سوال ۹: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه

الگوریتم‌هایی انجام شده است.

۲۳. 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 (۱۶-۲) نمایش داده می‌شود.

سوال ۱۰: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟

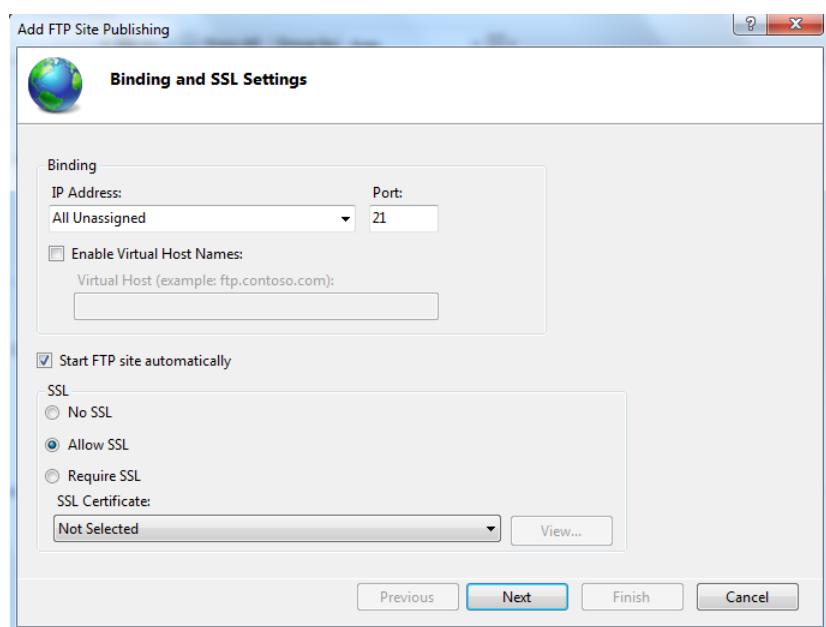
۲۰ ۲.۰۵۴۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 1593 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 SACK_PERM=1
۲۱ ۲.۰۵۴۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 443 → 1593 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=65495 SACK_PERM=1
۲۲ ۲.۰۵۴۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 1593 → 443 [ACK] Seq=1 Ack=1 Win=8192 Len=0
۲۴ ۲.۰۵۴۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 443 → 1593 [ACK] Seq=1 Ack=230 Win=7963 Len=0
۳۰ ۲.۰۵۶۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 1593 → 443 [ACK] Seq=230 Ack=146 Win=8047 Len=0
۳۲ ۲.۰۵۶۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 443 → 1593 [ACK] Seq=146 Ack=289 Win=7904 Len=0
۳۴ ۲.۰۵۶۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 443 → 1593 [ACK] Seq=146 Ack=971 Win=7222 Len=0
۳۶ ۲.۰۵۸۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TCP	48 1593 → 443 [ACK] Seq=971 Ack=375 Win=7818 Len=0
۲۳ ۲.۰۵۴۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TLSv1	269 Client Hello
۲۹ ۲.۰۵۵۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TLSv1	185 Server Hello, Change Cipher Spec, Encrypted Handshake Message
۳۱ ۲.۰۵۶۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TLSv1	99 Change Cipher Spec, Encrypted Handshake Message
۳۳ ۲.۰۵۶۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TLSv1	722 Application Data, Application Data
۳۵ ۲.۰۵۸۱۱۸	۱۲۷.۰.۰.۱	۱۲۷.۰.۰.۱	TLSv1	269 Application Data

شکل (۱۶-۲) نمونه خروجی Follow SSL Stream

سوال ۱۱: به یک سایت مانند <https://google.com> وصل شده، گواهی آن را بررسی کنید.
گواهی آن سایت با گواهی سایت شما چه تفاوت‌هایی دارد؟

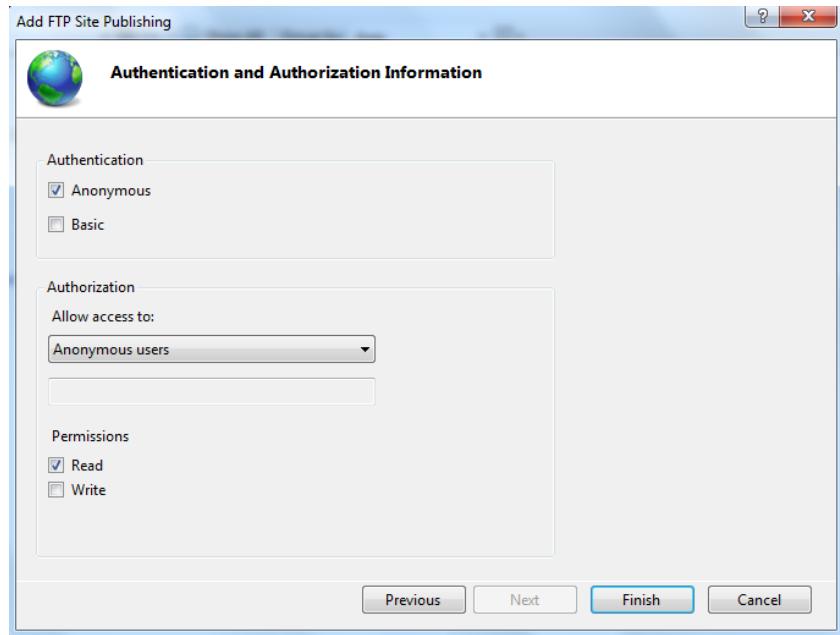
۲-۳-۱- تنظیمات سرور FTP

۱. 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 (۱۷-۲) انجام دهید. به جای Test.com اسم سایت خود را قرار دهید.



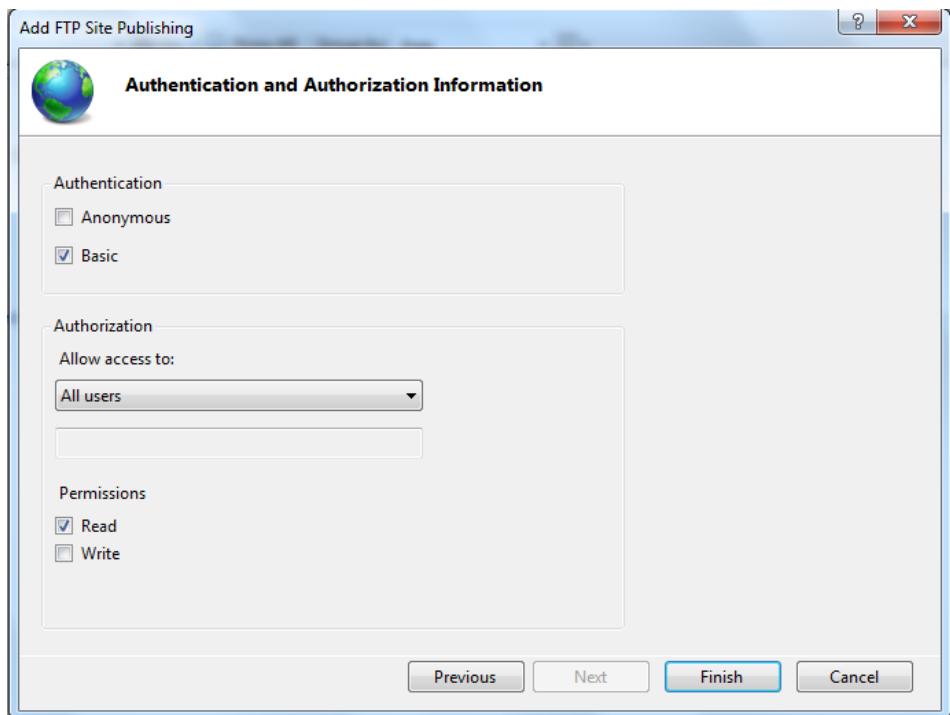
شکل (۱۷-۲) FTP Site Publishing

۲. دکمه Next را بزنید و صفحه بعد را مطابق شکل (۱۸-۲) کامل کنید.



شکل (۱۸-۲) تکمیل Binding

۳. بر روی دکمه Finish کلیک کنید. درنهایت Binding هم ساخته می شود.
 ۴. به آدرس <ftp://www.test.com> بروید. ارتباط را با Rawcap شنود کنید.
- سوال ۱۲: 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 مبدأ و مقصد ارتباط را مشخص کنید.
۵. 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 (۱۹-۲) تکمیل کنید.
 ۶. 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.
- سوال ۱۳: آیا نام کاربری و پسورد قابل خواندن است؟
۷. اگر از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید، صفحه نشان داده شده در شکل (۲-۲۰) نمایش داده می شود.

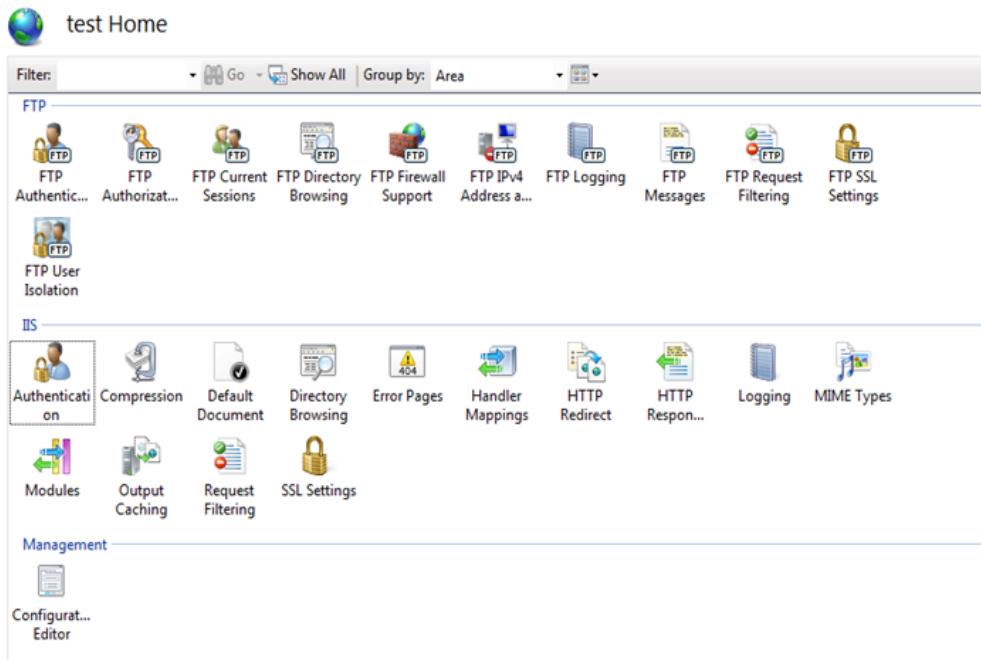


شکل (۱۹-۲) تنظیمات Authentication

	Default Web Site	1	Started (ht...)	*:80 (http)	%SystemDrive%\inetpub\wwwroot
	test	3	Started (ht...)	www.test.com on *:80 (http),ww...	C:\test

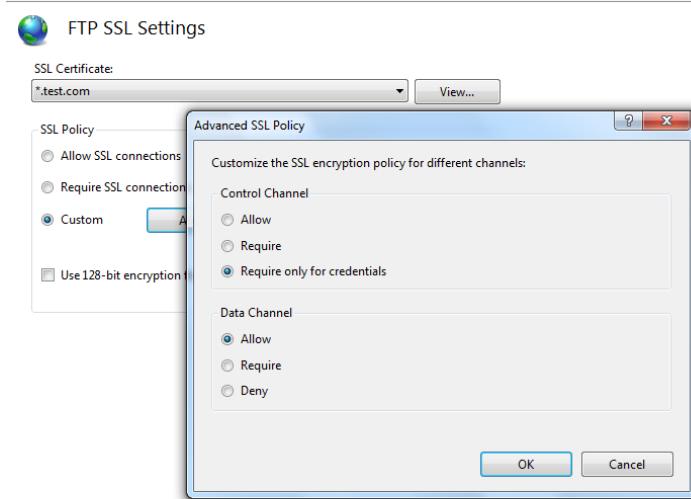
شکل (۲۰-۲) صفحه نمایش داده شده بعد از انتخاب Sites

۸. با انتخاب سایت خود، صفحه نشان داده شده در شکل (۲۱-۲) نمایش داده می‌شود. تنظیمات نامهای کاربری و دسترسی‌ها در این بخش مشخص است
- سوال ۱۴: به FTP Authentication و FTP Authorization وارد شوید و مشخص کنید چه سطح دسترسی برای چه کاربرانی تعریف شده است.



شکل (۲۱-۲) صفحه نمایش داده شده بعد از انتخاب نام سایت خود

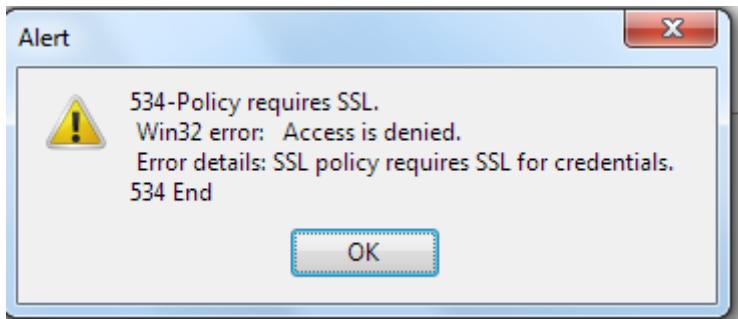
۹. دوباره از منوی سمت چپ، ابتدا بر روی Sites کلیک کنید و سپس سایت خود را انتخاب کنید. به بخش FTP SSL Settings بروید. یک گواهی انتخاب کنید. سپس بر روی Custom کلیک کنید و آن را مطابق شکل (۲۲-۲) تکمیل کنید. پس از آن دکمه Apply را فشار دهید.



شکل (۲۲-۲) تنظیمات SSL Policy

سوال ۱۵: سعی کنید دوباره سایت را از مرورگر باز کنید. آیا می‌توانید به سایت وارد شوید؟

سوال ۱۶: در مرورگر فایرفاکس خطای نمایش داده شده در شکل (۲۳-۲) نشان داده می‌شود. معنی این خطا چیست؟



شکل (۲۳-۲) خطای نمایش داده شده

۱. برنامه Filezilla را از آدرس <https://filezilla-project.org/> دانلود کنید. پس از نصب، در قسمت loopback Host 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 قابل خواندن است؟

HTTP - ۳-۳-۱ پروتکل

۱. 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.
۲. بر روی یکی از بسته‌های پروتکل HTTP کلیک راست کرده و انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.
۳. 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؟
۴. در پنجره باز شده، بسته‌هایی 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؟

FTP - ۴-۳-۱ پروتکل

۱. 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.
۲. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدأ و مقصد ارتباط را مشخص کنید.

۳. در یکی از بسته ها مقدار Username و در بسته دیگر مقدار Password به سمت سرور ارسال شده است. این مقادیر را مشخص کنید.

۲- کار با کاربردهای Web، DNS، سوکت و پویش سرویس‌ها

۱-۱- هدف آزمایش

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

۱-۲- فعالیت‌های قبل از آزمایش

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

۱-۳- قطعات و ابزارهای مورد نیاز

ابزارهای مورد نیاز برای انجام این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم‌عامل ویندوز ۷ یا بالاتر برای هر گروه
- برنامه Nmap نسخه ۷.۷ به بالا
- برنامه Wireshark نسخه ۲.۴ به بالا

۱-۴- شرح آزمایش

۱-۴-۱- کارکرد DNS

در ابتدا با ابزارهای برخط^{۲۵} 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 (۲۴-۲) نمایش داده شده است.

²⁵ Online

The screenshot shows the homepage of Viewdns.info. At the top, there are tabs for Tools, API, Research, and Data. Below the tabs are several tool boxes arranged in a grid:

- Reverse IP Lookup**: Find all sites hosted on a given server. Input: Domain / IP, GO.
- Reverse Whois Lookup**: Find domain names owned by an individual or company. Input: Registrant Name or Email Address, GO.
- IP History**: Show historical IP addresses for a domain. Input: Domain (e.g. domain.com), GO.
- DNS Report**: Provides a complete report on your DNS settings. Input: Domain (e.g. domain.com), GO.
- Reverse MX Lookup [NEW]**: Find all sites that use a given mail server. Input: Mail server (e.g. mail.google.com), GO.
- Reverse NS Lookup**: Find all sites that use a given nameserver. Input: Nameserver (e.g. ns1.example.com), GO.
- IP Location Finder**: Find the geographic location of an IP Address. Input: IP, GO.
- Chinese Firewall Test**: Checks whether a site is accessible from China. Input: URL / Domain, GO.
- DNS Propagation Checker**: Check whether recent DNS changes have propagated. Input: Domain (e.g. domain.com), GO.
- Is My Site Down**: Check whether a site is actually down or not. Input: Domain (e.g. domain.com), GO.
- Iran Firewall Test**: Check whether a site is accessible in Iran. Input: Site URL / Domain, GO.
- Domain / IP Whois**: Lookup information on a Domain or IP address. Input: Domain / IP soft98.ir, GO.
- Get HTTP Headers**: View the HTTP headers returned by a domain. Input: Domain, GO.
- DNS Record Lookup**: View all DNS records for a specified domain. Input: Domain (e.g. domain.com), GO.
- Port Scanner**: Check if common ports are open on a server. Input: Domain / IP, GO.
- Traceroute**: Trace the servers between ViewDNS and a remote host. Input: Domain / IP, GO.
- Spam Database Lookup**: Determine if your mail server is on any spam lists. Input: IP, GO.
- Reverse DNS Lookup**: View the reverse DNS entry for an IP address. Input: IP, GO.
- ASN Lookup**: Lookup information on an ASN. Input: Autonomous System Number (e.g. 3456), GO.
- Ping**: Test the latency of a remote system from ViewDNS. Input: Domain / IP, GO.
- DNSSEC Test**: Test if any domain name is configured for DNSSEC. Input: Domain (e.g. domain.com), GO.
- URL / String Decode**: Convert a URL with "%#%" values to a readable format. Input: URL / String, GO.
- Abuse Contact Lookup**: Find the abuse contact address for a domain name. Input: Domain, GO.
- MAC Address Lookup**: Determine the manufacturer of a network device. Input: MAC Address (e.g. 00-22-11-22-33), GO.
- Free Email Lookup**: Determine if a domain provides free email addresses. Input: Domain (e.g. gmail.com), GO.

شکل (۲۴-۲) وبسایت Viewdns

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

سوال ۱: نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟

سوال ۲: آدرس name server آن چیست؟

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

سوال ۳: رکوردهای A، NS و MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می‌کنند؟

سوال ۴: در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir) آیا آدرس IP آن را می‌توانید مشخص کنید؟

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

سوال ۵: چه وبسایتها دیگری بر روی همین سرور قرار دارند (آدرس IP آنها را با آدرس IP سایت farsnews.com مقایسه کنید)؟

سوال ۶: به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

۴. به وبسایت زیر بروید:

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

۵. در این وبسایت آدرس aut.ac.ir وارد کرده و درخواست‌ها و پاسخ‌های دریافت شده را بررسی کنید.

۲-۴-۲- مشاهده و تشخیص 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 (۲۵-۲) مشاهده می‌شود.

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1395	www:1396	ESTABLISHED
TCP	127.0.0.1:1396	www:1395	ESTABLISHED
TCP	127.0.0.1:2681	www:19872	ESTABLISHED
TCP	127.0.0.1:6070	www:8580	CLOSE_WAIT
TCP	127.0.0.1:6128	www:8580	TIME_WAIT
TCP	127.0.0.1:6129	www:8580	TIME_WAIT
TCP	127.0.0.1:6130	www:8580	TIME_WAIT
TCP	127.0.0.1:6131	www:8580	TIME_WAIT
TCP	127.0.0.1:6133	www:8580	TIME_WAIT
TCP	127.0.0.1:6144	www:8580	TIME_WAIT
TCP	127.0.0.1:6148	www:8580	TIME_WAIT
TCP	127.0.0.1:6150	www:8580	TIME_WAIT
TCP	127.0.0.1:6155	www:8580	TIME_WAIT
TCP	127.0.0.1:6162	www:8580	TIME_WAIT
TCP	127.0.0.1:6164	www:8580	TIME_WAIT
TCP	127.0.0.1:6165	www:8580	TIME_WAIT
TCP	127.0.0.1:6166	www:8580	TIME_WAIT
TCP	127.0.0.1:6167	www:8580	TIME_WAIT
TCP	127.0.0.1:6169	www:8580	TIME_WAIT
TCP	127.0.0.1:6170	www:8580	TIME_WAIT
TCP	127.0.0.1:6171	www:8580	TIME_WAIT
TCP	127.0.0.1:6172	www:8580	TIME_WAIT
TCP	127.0.0.1:6174	www:8580	TIME_WAIT
TCP	127.0.0.1:6176	www:8580	TIME_WAIT
TCP	127.0.0.1:6177	www:8580	TIME_WAIT
TCP	127.0.0.1:6179	www:8580	TIME_WAIT
TCP	127.0.0.1:6180	www:8580	TIME_WAIT
TCP	127.0.0.1:6182	www:8580	TIME_WAIT
TCP	127.0.0.1:6187	www:8580	TIME_WAIT
TCP	127.0.0.1:6188	www:8580	TIME_WAIT
TCP	127.0.0.1:6190	www:8580	TIME_WAIT
TCP	127.0.0.1:6191	www:8580	TIME_WAIT
TCP	127.0.0.1:6192	www:8580	TIME_WAIT

شکل (۲۵-۲) نمونه‌ای از خروجی دستور netstat

بسیاری از موقع، 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.

سوال ۷: برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

سوال ۸: دستوری را پیدا کنید که به وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.

Web - ۳-۴-۲ کارکرد

۱. 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
```

۲. 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

سوال ۹: دلیل وارد کردن دو enter پشت سر هم چیست؟

سوال ۱۰: 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.

سوال ۱۱: آیا این ارتباط persistent است؟

۳. 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

۴. 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.

سوال ۱۲: 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.

۵. 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
```

۶. برای اینکه مطمئن شوید، با استفاده از دستور ipconfig تایید کنید که در سیستم دوستان هستید. ارتباط را با دستور CTRL+C ارتباط قبلی را خاتمه دهید.

۷. 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 تحويل می‌دهد.

```
ncat -l -p 4444 < index.html
```

۸. برای فایل index.html می‌توانید از محتوای زیر استفاده کنید:

HTTP/1.1 200 OK

```
<html>
<head>
<title>Hello</title>
<body> Salam!</body>
</head>
</html>
```

سوال ۱۳: 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.

۴-۴-۲- پویش سرویس‌ها

برنامه‌ی NMAP به منظور پویش شبکه و سرویس‌های سیستم‌های انتهایی مورد استفاده 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.

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

سوال ۱۴: سیستم‌عامل دوست شما چیست؟

سوال ۱۵: چه پورت‌هایی روی سیستم دوست شما باز است؟

سوال ۱۶: سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

سوال ۱۷: مراحل بالا را برای سایت aut.ac.ir انجام دهید. سیستم‌عامل این وبسایت چیست؟

سوال ۱۸: 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

Ping را asg.aut.ac.ir کنید. به نظر شما نتیجه اسکن به چه دلیلی تغییر کرده است؟ این ماشین چه نقشی در دانشگاه دارد؟

فصل ۳: لایه انتقال

۱- تحلیل TCP با استفاده از Wireshark

۱-۱- هدف آزمایش

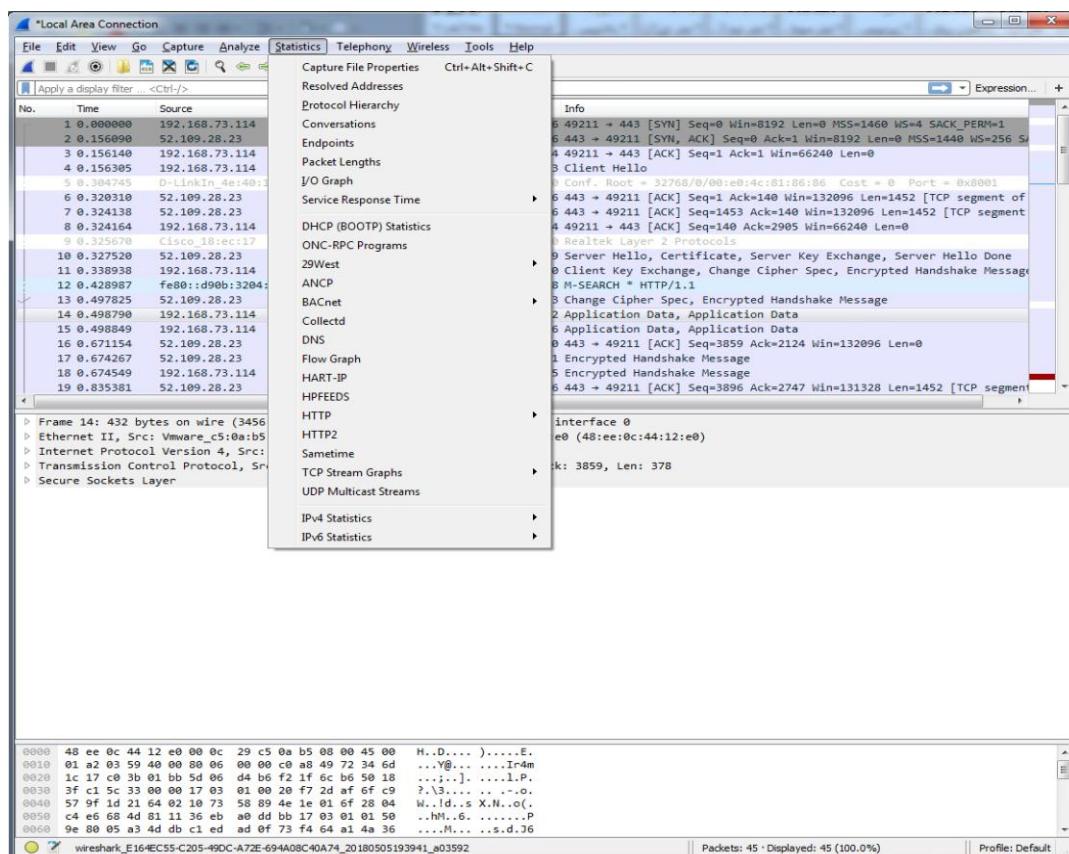
در این آزمایش قصد داریم آشنایی بیشتری با نرمافزار Wireshark و منوی Statistics در آن پیدا کنیم و از امکانات آن برای تحلیل بسته‌های جم‌آوری شده استفاده نماییم.

۱-۲- فعالیت‌های قبل از آزمایش

دستور کار جلسه‌ی آشنایی با wireshark را مرور کنید.

۱-۳- شرح آزمایش

نرمافزار wireshark را باز کرده، چند دقیقه به وب گردی بپردازید و بسته‌ها را جم‌آوری کنید. سپس مطابق جم‌آوری 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.



شكل (۱-۳) زبانه Statistics

۱. بر روی گزینه‌ی Resolved Addresses کلیک کنید.

سوال ۱: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

سوال ۲: آیا می‌توانید سه بایت اولی که برای آدرس فیزیکی کارت‌های شبکه Cisco می‌باشد را مشخص کنید؟

۲. بر روی گزینه‌ی protocol hierarchy کلیک کنید.

سوال ۳: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

سوال ۴: چند درصد بسته‌های شما به یک ارتباط TCP بر روی بستر IPv4 تعلق دارند؟

۳. بر روی گزینه‌ی Conversations کلیک کنید.

سوال ۵: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

۴. یک نشست TCP را مشخص کنید. (برای مشخص کردن یک نشست TCP نیاز است که آدرس و پورت مبدأ و مقصد را مشخص کنید). توجه داشته باشید مفهومی که Wireshark از نشست برداشت می‌کند با مفهومی که در کلاس آموخته‌اید تفاوت دارد.

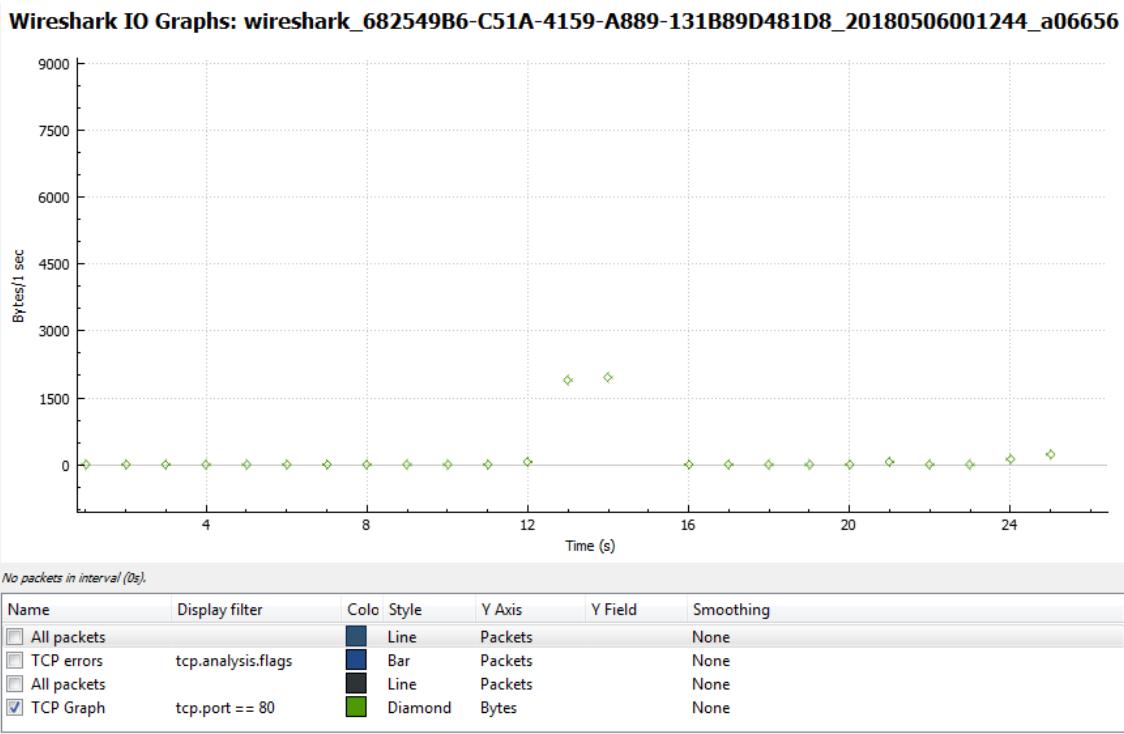
۵. بر روی گزینه‌ی endpoints کلیک کنید.

سوال ۶: در پنجره‌ای که باز می‌شود چه چیزی را مشاهده می‌کنید؟

سوال ۷: چه مقصد‌هایی برای ارتباط‌های TCP در سیستم شما استفاده شده‌اند؟

سوال ۸: آیا می‌توانید از زبانه Ethernet و از روی تعداد بسته‌های مبادله شده، Default Gateway شبکه خود را تشخیص دهید؟

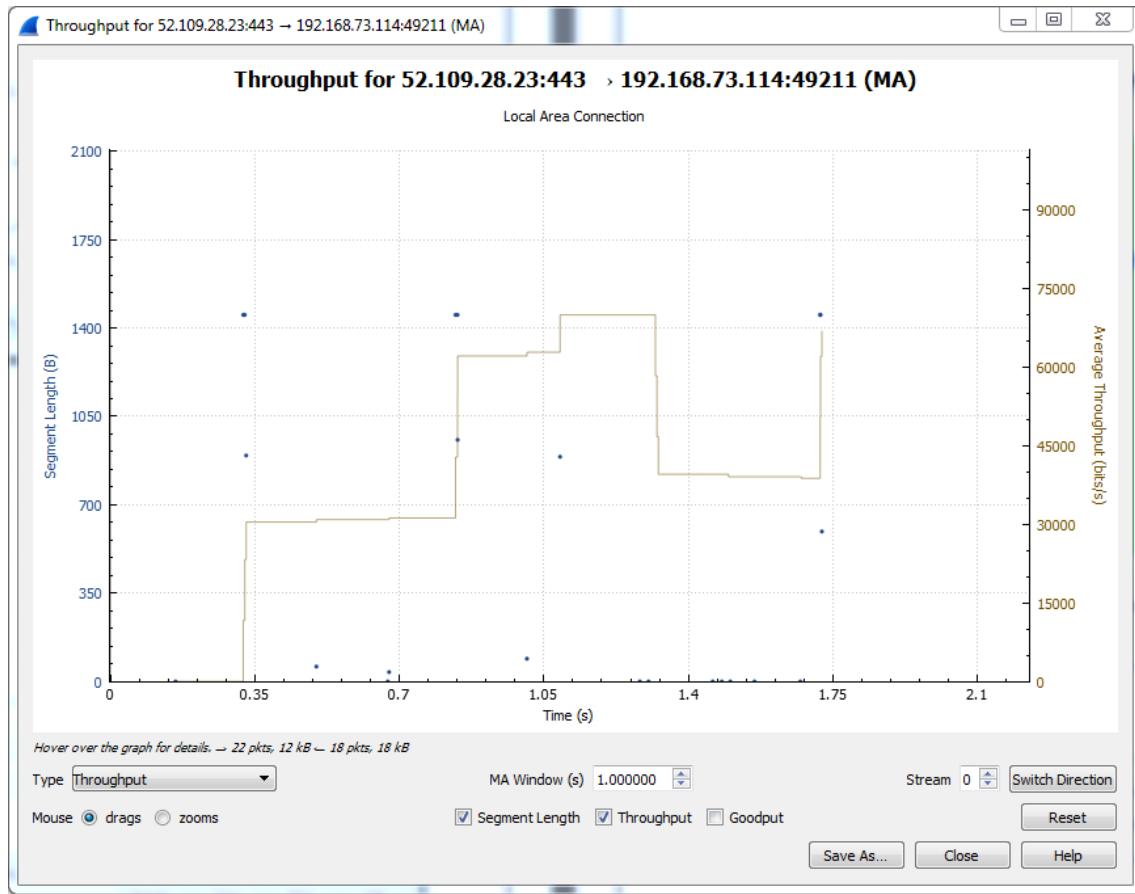
۶. بر روی گزینه‌ی I/O Graph کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید نرخ I/O را مشاهده کنید. شما می‌توانید در این صفحه نمودارهای مختلفی بسازید. بر روی دکمه + در پایین پنجره باز شده کلیک کنید، سپس یک فیلتر به آن اضافه کنید تا نمودار تعداد بسته‌ها در ثانیه را مشاهده کنید. مشاهده می‌کنید که با کلیک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



شکل (۲-۳)

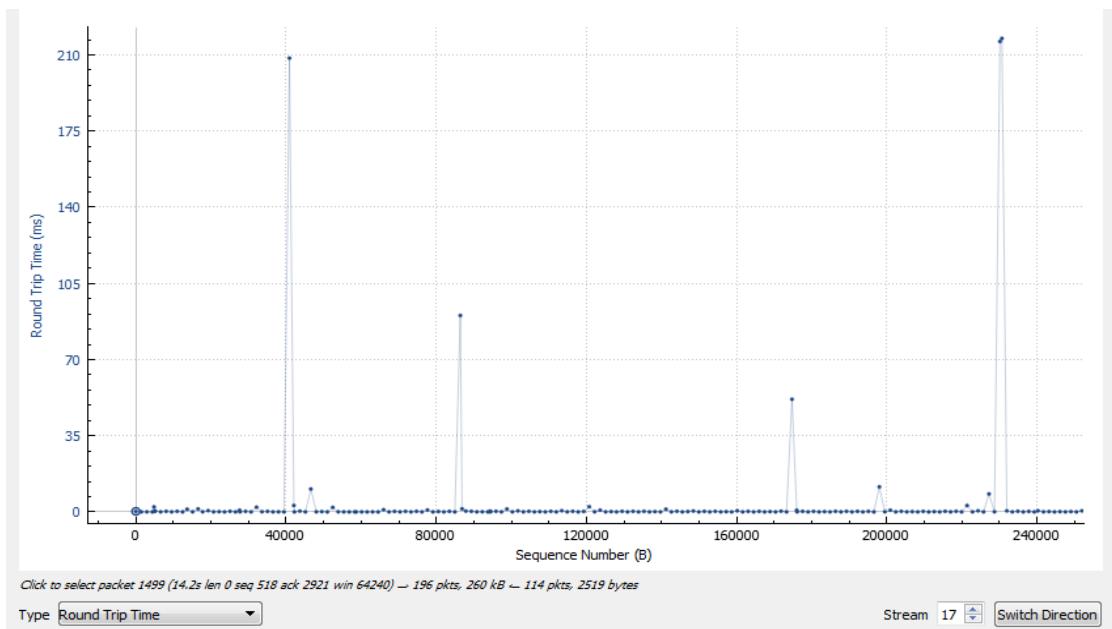
۷. بسته‌های مربوط به ارتباط با یک سایت را فیلتر کنید (با استفاده از Follow TCP Stream) و سپس بر روی گزینه‌ی Flow Graph کلیک کنید. از منوی پایین، در بخش Show packets را انتخاب کنید. به صورت کامل جزئیات مربوط به Ack و SeqNum و شماره پنجره را دنبال کنید.

۸. 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 (۳-۳) 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 segment های 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.



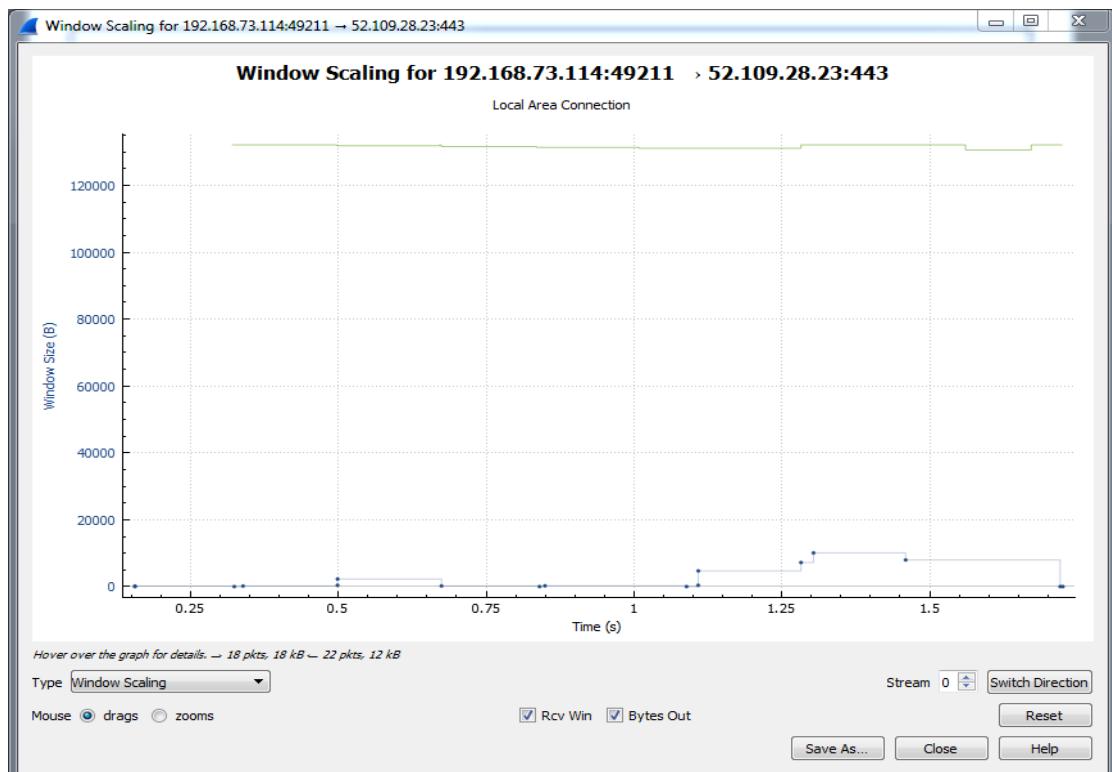
شکل (۳-۳) نمودار گذردهی

۹. 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 (۴-۳)). گزینه‌های این پنجره نیز مانند قسمت ۸ است. می‌توانید با انتخاب گزینه‌ی RTT By Sequence Number در گوشه پایین سمت راست را به شماره Stream مربوط 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.



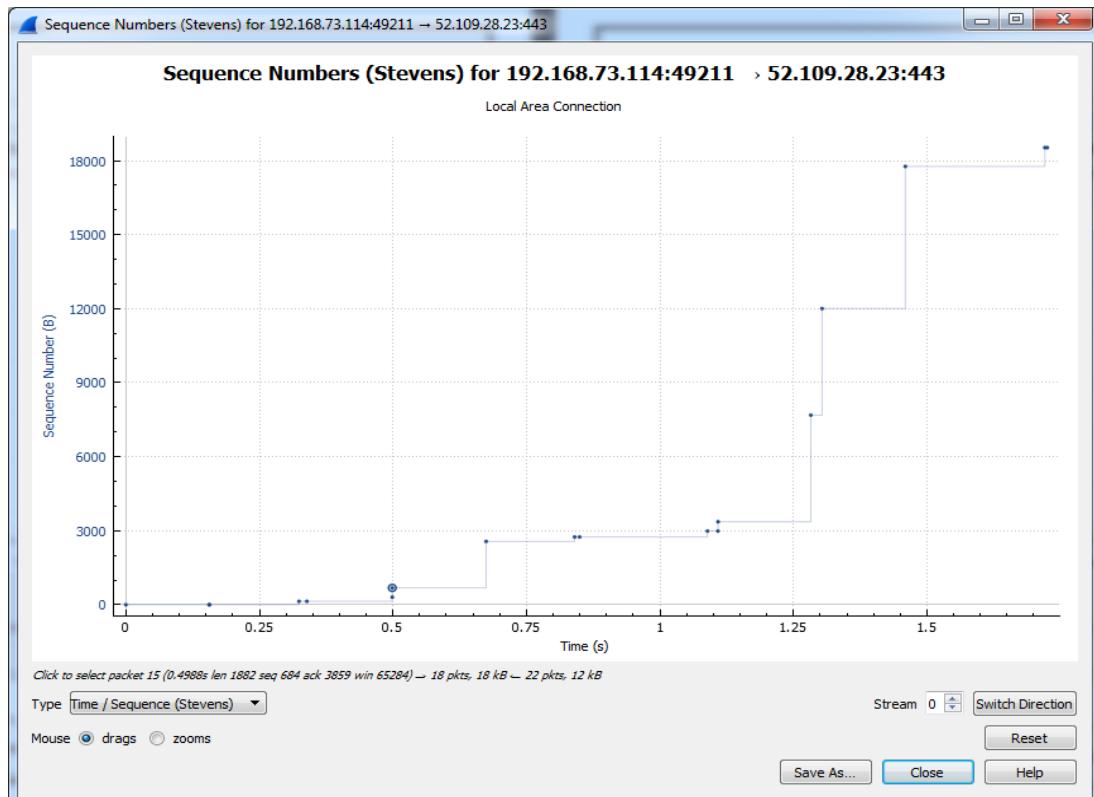
شکل (۴-۳) نمودار RTT

۱۰. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Window Scaling کلیک کنید. پنجره‌ای مانند شکل (۵-۳) باز می‌شود که می‌توانید اندازه‌ی پنجه‌ی 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.



شکل (۵-۳) نمودار Window Scaling

۱۱. بر روی گزینه‌ی TCP Stream Graph کلیک کنید، در منوی جدیدی که باز می‌شود بر روی Sequence Time / Sequence (Stevens) کلیک کنید. در پنجره‌ای که باز می‌شود می‌توانید 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.



شکل (۳-۶) نمودار Sequence Numbers

سوال ۹: به سایت دانلود دانشگاه مراجعه کنید

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

به صورت 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 IP Conversation سایت دانشگاه را مشخص کنید. سپس می‌توانید آن را به عنوان یک فیلتر اعمال کنید و نمودارهای Throughput و Windows scaling، 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 به صورت 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 ۴ 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 باز کنید. Wireshark

فصل ۴: لایه شبکه

۱- آشنایی با شبیه‌ساز Boson NetSim

۱-۱- 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.

۱-۲- 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 کامپیوتوری 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 ۱۰ از ۴۲ نوع مسیریاب و ۷ نوع سوییچ پشتیبانی می‌کند. همچنین در هر سناریو قادر است تا ۲۰۰ دستگاه را شبیه‌سازی کند. این نرمافزار گواهینامه‌های ICND1 و ICND2 را پوشش می‌دهد که در ROUTE، SWITCH و TSHOOT را به آزمایش‌ها می‌پوشاند. چندین دسته تقسیم می‌شوند از جمله: Stand-Alone Labs، Scenario Labs، Sequential Labs و Supplemental Labs که آزمایش‌های Standalone می‌باشند و باستگی به آزمایش‌های قبلی اجرا می‌شوند و آزمایش Sequential نیاز به اطلاعاتی دارند که در آزمایش‌های قبلی، گفته شده 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.

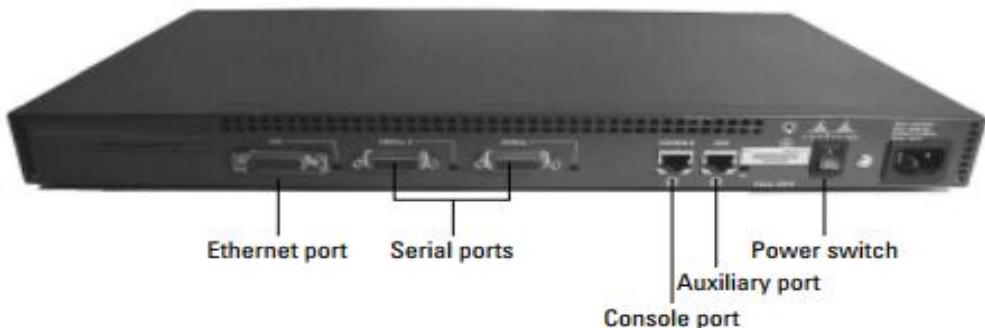
برای دسترسی به محیط Cisco IOS می‌توان از CLI استفاده کرد. محیط CLI شامل چندین سطح دسترسی است و دستورات قابل اجرا در هر سطح صرفاً وابسته به سطح دسترسی‌ای که در آن قرار دارید است. با وارد کردن علامت سوال (?) در CLI می‌توانید لیستی از دستورات موجود برای سطح دسترسی که در آن قرار دارید را به دست آورید. در 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 (۱-۴) نحوه دسترسی و خروج از سطح دسترسی‌های دستوری رایج را نشان می‌دهد.

جدول (۱-۴) نحوه دسترسی و خروج از سطح دسترسی‌های دستوری رایج

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

انواع مختلفی از پورت‌ها در تجهیزات ارتباطی وجود دارد که نمونه‌ای از آن‌ها در شکل (۱-۴) نشان داده شده است. در ادامه در مورد برخی از این راههای ارتباطی به اختصار توضیحاتی ارائه می‌شود.



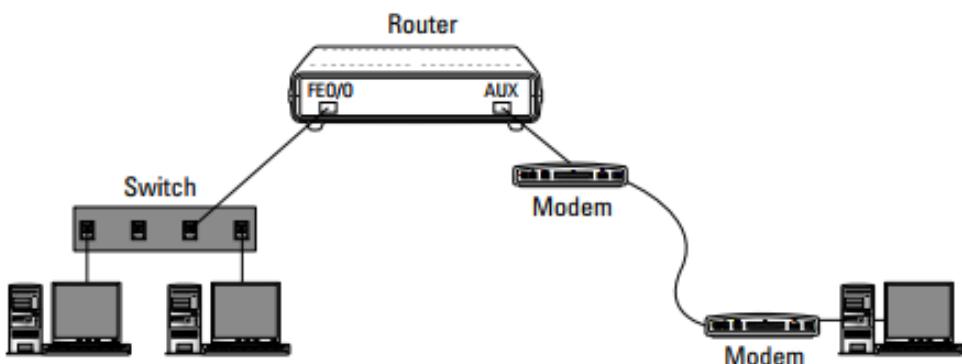
شکل (۱-۴) انواع مختلف پورت‌ها

- پورت کنسول: پورت کنسول^{۲۶} 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 به صورت فیزیکی با روتر در ارتباط بود. هنگام اتصال محلی به روتر، کابل کنسول معمولاً از پورت سریال

²⁶ Console port

کامپیوتر به پورت کنسول در دستگاه متصل می‌شود. تمام پورت‌های دستگاه با یک شناسه منحصر به فرد^{۲۷} 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 0 console یا به طور مختصر con 0 اشاره دارد، زیرا آن اولین پورت کنسول در روترا است.

- پورت auxiliary: پورت auxiliary دقیقاً به عنوان یک پورت کنسول استفاده می‌شود به این معنی که به صورت 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 ۴-۲). در این صورت برای مدیریت روترا دیگر نیازی به حضور فیزیکی در کنار روترا نیست.



شکل (۴-۲) نحوه اتصال از طریق پورت auxiliary

- VTY: از VTY^{۲۸} 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.

۱-۲-۱- 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 مورد استفاده در دستگاه‌های سیسکو توضیح داده می‌شود.

²⁷ Unique ID

²⁸ Virtual terminal

ROM - ۱-۱-۲-۱

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 که در ROM ذخیره می‌شوند عبارت‌اند از:

- POST^{۲۹} مجموعه‌ای از رویه‌ها که در هنگام راهاندازی برای چک کردن سختافزارهای دستگاه اجرا می‌شوند.
- برنامه Bootstrap: برنامه Boot Loader یا Bootstrap 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 معمولاً به این صورت استفاده می‌شود که با استفاده از آن می‌توان اینترفیس‌ها را تنظیم کرد تا این 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.

Flash - ۲-۱-۲-۱

سیستم‌عامل IOS در آن ذخیره می‌شود. دلیل اینکه IOS در حافظه flash ذخیره می‌شود نه در ROM این است که به طور پیوسته در زمان ارتقا می‌باید 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 (۳-۴) نمایش داده شده است.

VRAM - ۳-۱-۲-۱

VRAM^{۳۰} 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 می‌شود running configuration است که شامل تنظیمات کنونی و در حال اجرای سیستم است. به عنوان مثال: اگر نام روترا تغییر دهیم این تغییر نام روت در VRAM ذخیره می‌شود و اگر دستگاه را راهاندازی مجدد کنیم نام

²⁹ Power-On Self-Test

³⁰ Volatile RAM

جدیدی که اعمال کرده بودیم حذف می‌گردد. برای اینکه این اتفاق نیفتد باید running configuration را در nonvolatile RAM ذخیره کرد. علاوه بر اطلاعات running configuration دیگری شامل کش ARP، جدول مسیریابی و جدول آدرس MAC نیز در آن ذخیره می‌شوند.



شکل (۳-۴) کارت حافظه Flash

NVRAM - ۴-۱-۲-۱

NVRAM^{۳۱} اطلاعات را به صورت دائمی ذخیره می‌کند حتی اگر برق قطع شود اطلاعات داخل آن از بین نمی‌رود. اصلی‌ترین اطلاعاتی که در آن ذخیره می‌شود config Startup است. این تنظیمات به عنوان پیکربندی راهانداز شناخته می‌شود و در هر بار راهاندازی، به دستگاه اعمال می‌شود.

۲-۲-۱ اتصال از طریق کابل سریال

دستگاه‌هایی که به واسطه کابل سریال با یکدیگر ارتباط برقرار می‌کنند به دو دسته DCE^{۳۲} و DTE^{۳۳} تقسیم می‌شوند. دستگاه DCE نرخ clock برای 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.

³¹ Nonvolatile RAM

³² Data Communication Equipment

³³ Data Terminal Equipment

۳-۲-۱ پروتکل CDP

پروتکل (CDP) در لایه دوم مدل هفت لایه‌ای OSI، Cisco Discovery Protocol (CDP) نام 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 802.1 می‌سازد.

یک تجهیز به صورت 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.

۳-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

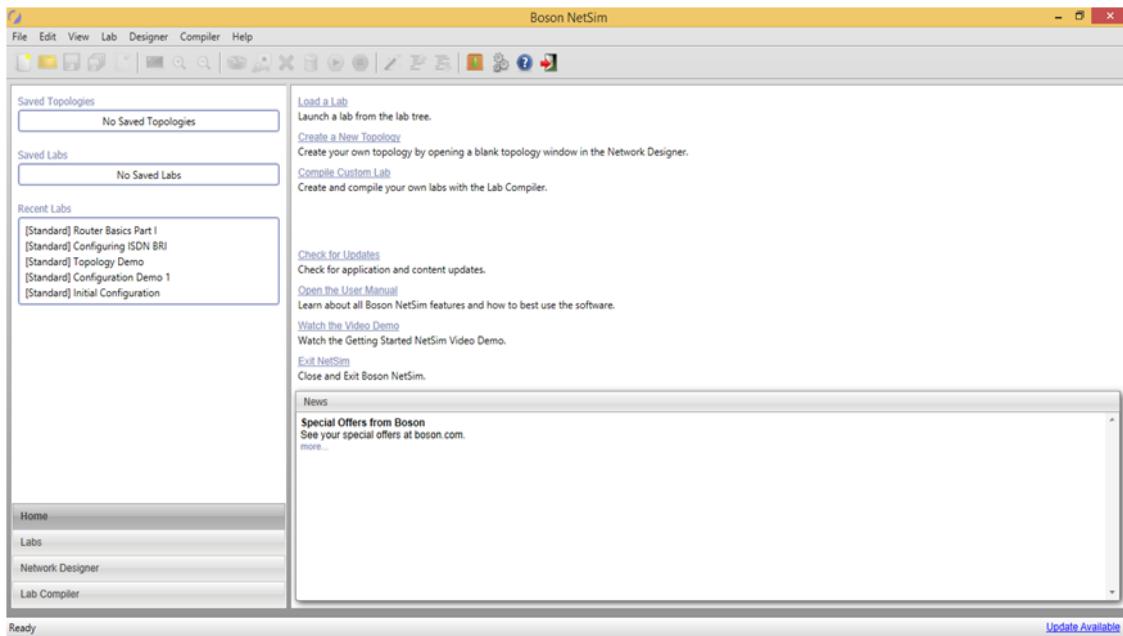
- کامپیوتر شخصی با سیستم‌عامل ویندوز برای هر گروه
- شبیه‌ساز Boson نسخه ۱۰ یا سایر شبیه‌سازهای سیستم‌عامل IOS

۴-۱- 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 منحصر به فرد، نگاشت می‌کنید. در ادامه با استفاده از Telnet به یک مسیریاب متصل خواهید شد و به تنظیمات اولیه پروتکل CDP خواهید پرداخت.

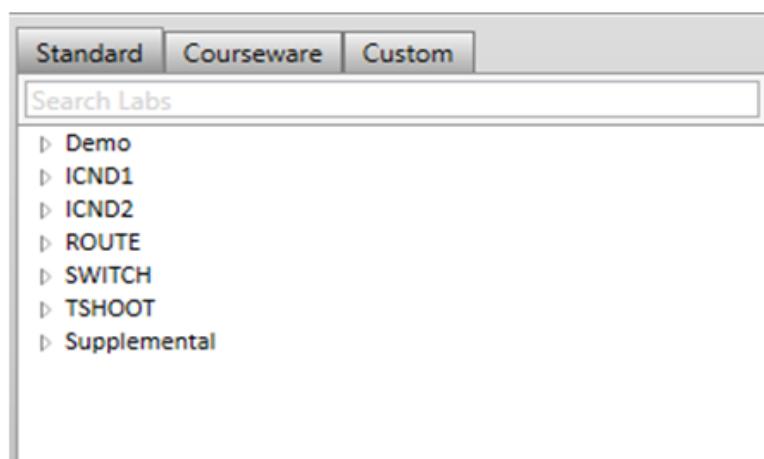
۴-۱-۱- تنظیمات مقدماتی

۱. در ابتدا برای شروع کار برنامه BOSON را باز کنید. صفحه‌ای مطابق شکل (۴-۴) را مشاهده می‌شود:



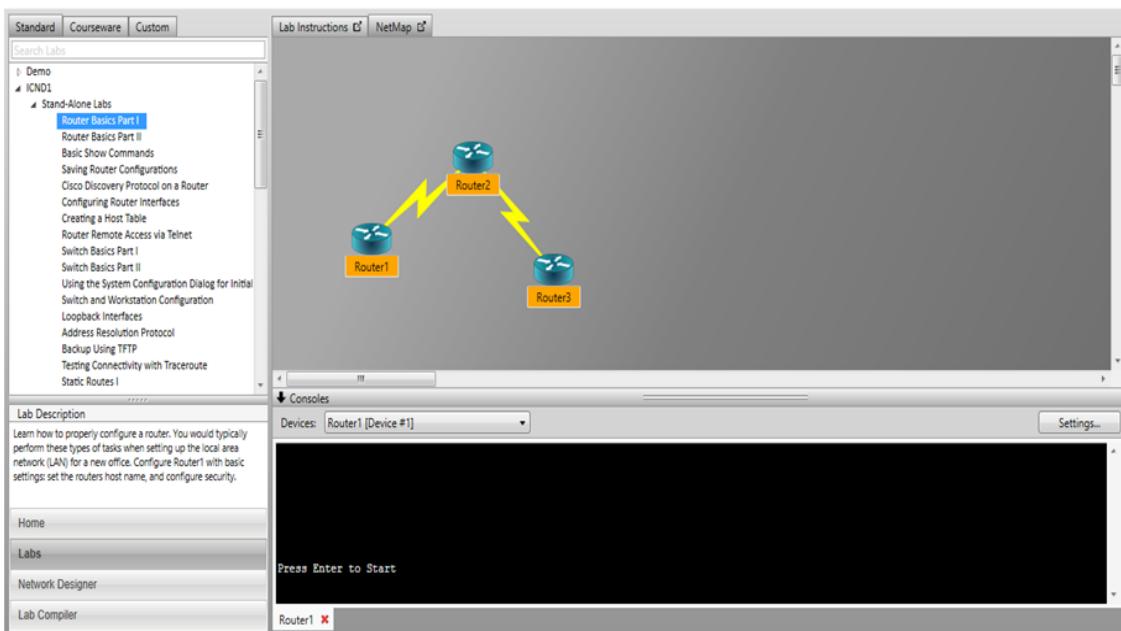
شکل (۴-۴) صفحه نخست Boson

۲. سپس از قسمت چپ و پایین گزینه Labs را انتخاب کنید تا آزمایش‌های موجود در نرم‌افزار را مشاهده کنید. سه نوع دسته‌بندی طبق شکل (۵-۴) 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).



شکل (۵-۴) انواع دسته‌بندی آزمایش‌های موجود

۳. 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 (۶-۴) مشاهده می‌شود.



شکل (۶-۴) 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 console 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.

۴. 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 فعلی عبارت exit یا logout استفاده کنید.
۵. با نوشتن یک علامت سوال (?) می‌توانید به همه دستورات قابل استفاده دسترسی پیدا کنید و با زدن کلید فاصله (space) لیست را به طور کامل تر مشاهده کنید.
۶. 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.

سوال ۱: دستورات show زیر را اجرا کنید و خروجی هر کدام را در گزارش کار توضیح

دهید:

```
show flash
show history
show terminal
show protocols
show version
```

show clock
show interfaces
show ip interface brief

٧. با نوشتن `configure terminal` به حالت پیکربندی عمومی یک مسیریاب وارد شوید.
٨. 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.
٩. با نوشتن دستور `enable password CISCO` برای ورود به سطح دسترسی `Privileged EXEC` می‌توانید گذرواژه^{۳۴} CISCO را تنظیم کنید.
١٠. 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 کردۀاید را وارد کنید تا بتوانید به سیستم ورود کنید.
١١. با دستور `enable secret` نیز می‌توان برای ورود به سطح دسترسی گذرواژه گذاشت.

سوال ۲: تفاوت این دو روش (مرحله ۹ و ۱۱) در چیست؟

١٢. با استفاده از دستور `show running-config` تنظیمات سیستم را مرور کنید و گذرواژه‌های رمز شده را مشاهده کنید.
١٣. 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.
١٤. با دستور `show history` می‌توانید آخرین دستورات وارد شده در ترمینال را که در حافظه روتر ذخیره شده است مشاهده کنید. با دستور `terminal show` تعداد دستوراتی را که به صورت پیش‌فرض ذخیره می‌کند را پیدا کنید. وارد محیط تنظیم Global شوید سپس با دستور `line 0 console 0` وارد تنظیمات کنسول شوید. با استفاده از دستور `history size 100` تاریخچه مسیریاب را تنظیم کنید که ۱۰۰ دستور را در خود نگهداری کند.

سوال ۳: حداقل تعدادی که برای ذخیره دستورات می‌توان تعریف نمود چند است؟

١٥. 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 `BOSON password` 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.

³⁴ Password

۱۶. 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.

۱۷. 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.

۱۸. 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.

۱۹. 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 mypassword** یک نام کاربری با رمز عبور برای ورود به سیستم تعریف کنید.

۲۰. تنظیماتی که با دستور show running-config قابل مشاهده هستند به طور خودکار در روتر ذخیره نمی‌شوند و با قطع برق از بین می‌روند. به منظور ذخیره این تنظیمات در روتر از دستور show startup-config copy running-config startup-config نیز می‌توان تنظیمات ذخیره شده در NVRAM را مشاهده کرد.

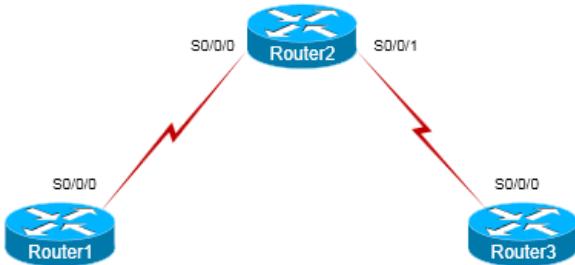
سوال ۴: چگونه می‌توان اطلاعات ذخیره شده در NVRAM را حذف کرد؟

۲۱. 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.

سوال ۵: یک کاربر به نام lab3 تعریف کرده و سپس رمز ۱۵۳۷۵۹ را برای این کاربر تعریف کنید سپس تاریخچه دستورات ترمینال را به ۵۰ 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.

۲-۴-۱- اختصاص آدرس IP به واسطه‌های شبکه

در این آزمایش، به واسطه‌های مسیریاب آدرس IP اختصاص خواهد یافت. ابتدا توپولوژی مطابق با شکل (۴-۷) ایجاد کنید. تمام واسطه‌ها از نوع Serial هستند.



شکل (۷-۴) توپولوژی آزمایش

جدول (۲-۴) آدرس‌های شبکه

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

۱. با استفاده از دستور enable و سپس configure terminal وارد محیط تنظیم Global مسیریاب شوید. سپس نام مسیریاب‌ها را مطابق با جدول (۲-۴) تغییر دهید.
۲. در مسیریاب اول، از محیط کانفیگ خارج شوید و با استفاده از دستور show ip interface brief وضعیت واسطه‌های مختلف را یادداشت نمایید.
۳. در مسیریاب اول، وارد محیط کانفیگ شده و با استفاده از دستور interface serial 0/0/0 وارد تنظیمات واسط سریال شوید.

سوال ۶: چه دستوراتی در این مرحله قابل اجرا است؟ آن‌ها را شرح دهید.

۴. دستور no shutdown را اجرا کنید. سپس با استفاده از دستور on Serial interface توضیحات نوشته شده در مقابل دستور descrirption Router1 show interface serial 0/0/0 را به این واسط اضافه کنید. با استفاده از دستور Router1 می‌توانید توضیحات اضافه شده را مشاهده کنید.

۵. 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.

سوال ۷: با استفاده از دستور show ip interface brief توضیح دهید که چرا واسط ابتدا

up می‌شود و سپس down می‌شود.

۶. با استفاده از دستور show interfaces serial 0/0/0 توضیحات اضافه شده به این واسط را مشاهده کنید.
۷. به ترمینال مسیریاب Router2 بروید. مراحل ۳ و ۴ (فقط دستور no shutdown را اجرا کنید) را تکرار کنید.

۸. با استفاده از دستور `end` از محیط تنظیمات خارج شوید.

سوال ۸: با استفاده از دستور `show ip interface brief` توضیح دهید چرا برای مسیریاب

Line و `administrator status` در حالت `up` است ولی Router1

در حالت `down` Protocol است.

۹. مراحل ۳ و ۴ (فقط دستور `no shutdown` را برای واسط دوم Router2 نیز اجرا کنید).

۱۰. مراحل ۳ و ۴ (فقط دستور `no shutdown` را اجرا کنید) را برای مسیریاب Router3 نیز اجرا کنید.

سوال ۹: 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

می آید؟

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

سوال ۱۰: 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.

سوال ۱۱: توضیح دهید که چرا همیشه نیاز به اجرای دستور `clock rate` نداریم و صرفا دستور `no shutdown` کافی است؟

۱۲. 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.

۱۳. با استفاده از دستور `ip address 10.1.1.1 255.255.255.0` به این واسط اختصاص دهید.

۱۴. مرحله ۱۲ را برای مسیریاب Router2 تکرار کنید.

۱۵. با استفاده از دستور `ip address 10.1.1.2 255.255.255.0` به واسط اول این مسیریاب آدرس IP اختصاص دهید.

۱۶. 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.

۱۷. مرحله ۱۲ 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.

۱۸. از محیط تنظیمات هر سه ترمینال با استفاده از دستور end خارج شوید.

سوال ۱۲: در ۱ Router با استفاده از دستور ping آدرس 10.1.1.2 را ping کنید. چه

اتفاقی می‌افتد؟

سوال ۱۳: در ۲ Router با استفاده از دستور ping آدرس 172.16.10.1 را ping کنید. چه

اتفاقی می‌افتد؟

۱۹. دستور show ip interface brief را بر روی مسیریاب Router2 اجرا کنید و خروجی را یادداشت کنید.

۲۰. 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.

۲۱. 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 اسمی نگاشته می‌شوند. در این صورت، به جای مشخص کردن آدرس IP، صرفاً به کار بردن اسم متناظر با آدرس، کافی خواهد بود.

۲۲. با استفاده از دستور end از محیط تنظیمات خارج شوید. سپس با استفاده از دستور ping router1، مسیریاب router1 را ping کنید.

۲۳. خروجی دستور show hosts بر مسیریاب router2 را یادداشت کنید.

۱-۴-۳- اتصال به مسیریاب از طریق Telnet

۱. با استفاده از دستور configure terminal به محیط تنظیمات عمومی مسیریاب Router1 بروید.

۲. با استفاده از دستور line vty 0 4 وارد تنظیمات ترمینال مجازی بشوید.

۳. دستور login و سپس دستور password test را اجرا کنید. با استفاده از دستور end از محیط تنظیمات خارج شوید.

۴. در مسیریاب Router2 دستور telnet 10.1.1.1 را اجرا کنید. پسورد تنظیم شده را وارد کنید.

۵. 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.

۶. 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.

۴-۴-۱ تنظیمات پروتکل CDP

۱. در مسیریاب Router2 دستور show cdp interface را اجرا کنید. زمان ارسال بسته‌های CDP چقدر است؟
 ۲. دستور show cdp neighbors را بر روی مسیریاب Router2 اجرا کنید. در خروجی، ستون Hold time به معنی زمانی است که اگر به روزرسانی دریافت نشود آن سطر پاک خواهد شد.
سوال ۱۴: سایر ستون‌های خروجی را شرح دهید.
 ۳. با استفاده از دستور show cdp neighbors detail جزیيات پروتکل CDP را مشاهده کنید.
- سوال ۱۵:** چه اطلاعاتی توسط پروتکل CDP منتقل شده است؟
۴. بر روی مسیریاب Router3 دستور show cdp neighbors را اجرا کنید. خروجی را یادداشت کنید.
 ۵. 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 ۴۵ ثانیه تغییر دهید.
 ۶. با استفاده از دستور cdp holdtime 60 زمان hold time را به ۶۰ ثانیه تغییر دهید.
 ۷. با استفاده از دستور end از محیط تنظیمات کلی خارج شود. سپس دستور show cdp را اجرا کنید و خروجی را یادداشت نمایید.
 ۸. 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 (با استفاده از دستور cdp enable می‌توان cdp را دوباره فعال کرد).
 ۹. با استفاده از دستور end از محیط تنظیمات خارج شوید.
 ۱۰. پس از گذشت چند دقیقه بر روی مسیریاب Router3 دستور show cdp neighbors را اجرا کنید. خروجی را تفسیر کنید.

۲- آشنایی با مکانیسم NAT و پروتکل DHCP

۱-۲- هدف آزمایش

هدف از انجام این آزمایش آشنایی با آدرس دهی شبکه برای استفاده از سرویس های اینترنت است. بدین منظور عملکرد و پیکربندی مکانیسم NAT، PAT و پروتکل DHCP بررسی می شود.

۲-۲- مطالب مقدماتی

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

در NAT آشنایی با مفاهیم آدرس IP خصوصی^{۳۵} یا غیر معتبر^{۳۶} و آدرس IP عمومی یا معتبر از اهمیت ویژه ای برخوردار است. طبق RFC 1918، آدرس های IP خصوصی، آدرس هایی هستند که به وسیله شبکه هایی که مستقیماً به اینترنت متصل نیستند، استفاده می شوند. در RFC6890 لیستی از آدرس های IP خصوصی و نحوه برخورد با آنها ارائه شده است. به منظور اینکه سیستم ها با آدرس شبکه های خصوصی به اینترنت متصل شوند می بایست از NAT استفاده شود. آدرس های IP خصوصی در اینترنت قابل مسیریابی نیستند و معمولاً توسط ISP^{۳۷} ها فیلتر می شوند. یک آدرس IP عمومی در اینترنت قابل مسیریابی است. سازمان IANA^{۳۸} مسئول اختصاص آدرس IP عمومی در اینترنت است. سازمان IANA نیز این مسئولیت را به سازمان های محلی واگذار می کند، به عنوان مثال ARIN^{۳۹} مسئول تخصیص آدرس های IP عمومی در آمریکای شمالی است.

مکانیسم NAT، یک آدرس (معمولًا آدرس مبدا) در سرآیند بسته ها با یک آدرس دیگر (معمولًا آدرس عمومی) جایگزین می کند. این مکانیسم معمولًا در دیواره آتش شبکه پیاده سازی می شود. در حالت کلی، سه روش برای پیاده سازی NAT وجود دارد.

- در این حالت یک نگاشت یک به یک و ثابت بین آدرس های اصلی و مپ شده وجود دارد. در این حالت اگر ده آدرس خصوصی داشته باشد، نیاز به ده آدرس

³⁵ private

³⁶ invalid

³⁷ Internet Service Provider

³⁸ Internet Address Numbers Authority

³⁹ Ameriacan Registry for Internet Numbers

عمومی خواهید داشت.

- Dynamic: در این حالت دستگاهها در شبکه داخلی، به صورت خودکار از یک pool آدرس عمومی، آدرس دریافت می‌کنند.

- Overload: 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.

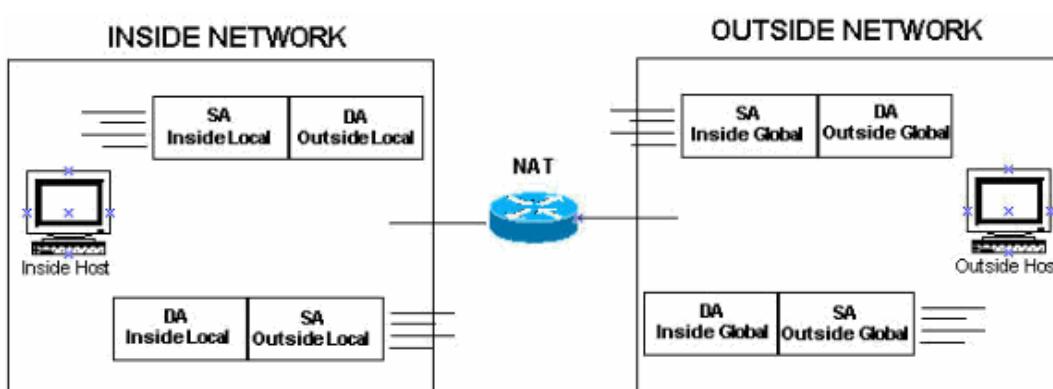
در مکانیسم NAT آدرس‌های مختلفی ممکن است به دستگاهها تعلق بگیرد که عبارت‌اند از:

- آدرس IP خصوصی یک دستگاه در شبکه داخلی: Inside Local
- آدرس IP عمومی یک دستگاه در شبکه داخلی. این آدرس، می‌تواند آدرسی باشد که آدرس خصوصی به آن مپ شده است.

- آدرس IP یک دستگاه در شبکه خارجی که برای شبکه داخلی قابل رویت است. این آدرس الزاماً یک آدرس عمومی نیست ولی لزوماً 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.

- آدرس IP عمومی یک دستگاه در شبکه خارجی.

رونده کلی تغییر آدرس‌ها را در شکل (۸-۴) مشاهده می‌کنید.



شکل (۸-۴) روند کلی تغییر آدرس‌ها

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

مراحل تنظیم NAT به صورت پویا عبارت است از:

۱. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
۲. ایجاد یک pool آدرس عمومی که می‌تواند به صورت پویا به آدرس‌های شبکه خصوصی اختصاص یابد.
۳. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۴. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۵. 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:

۱. به صورت ایستا، برای هر آدرس داخلی یک آدرس خارجی تعریف کنید.
۲. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۳. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.

در این حالت از آنجایی که 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 بتوانند 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 یکتاپورت 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 صرفاً یک آدرس local global داشته باشند و با استفاده از پورت از یکدیگر تشخیص داده شوند.

مراحل تنظیم PAT عبارت است از:

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

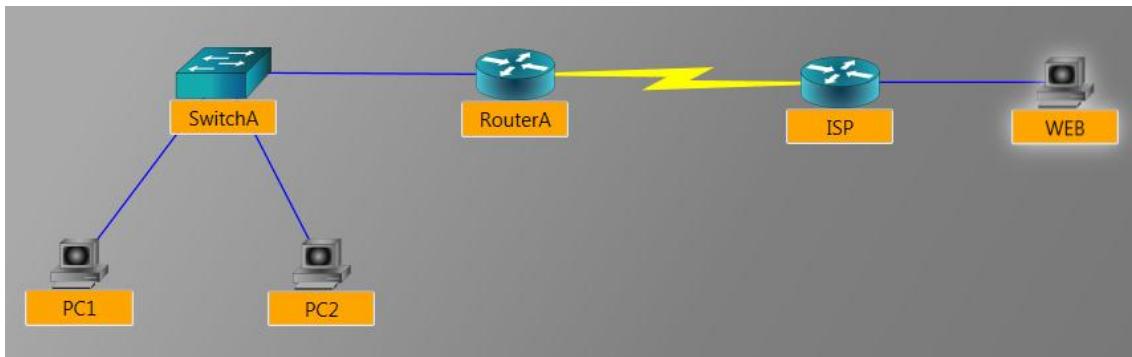
به عنوان یک مثال کلی، هنگامی که بسته SYN به سمت دروازه شبکه فرستاده می‌شود، دستگاه NAT آدرس IP و شماره پورت در سرآیند TCP را با آدرس IP عمومی و یک شماره پورت یکتا عوض می‌کند و بسته را به سمت شبکه عمومی ارسال می‌کند. در جواب اگر آدرس پورت مقصد بسته در جدول دستگاه NAT وجود داشته باشد، تبدیل آدرس دوباره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

۳-۲- 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

۱-۳-۱- مکانیسم NAT

توبولوژی که در این آزمایش بررسی می‌شود در شکل (۹-۴) نشان داده است. آدرس‌های IP واسطه‌ها در این آزمایش در جدول (۳-۴) آمده است.



شکل (۹-۴) توپولوژی آزمایش NAT

جدول (۳-۴) آدرس‌های موردنیاز آزمایش NAT

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

۱-۱-۳-۲ مکانیسم NAT است

۱. واسطه‌ای دستگاه‌ها مطابق آدرس‌های داده شده در جدول (۳-۴) تنظیم شده است. آیا PC1 و PC2 قادر به Ping کردن یکدیگر هستند؟ چرا؟ آیا از PC1 می‌توانید ISP را Ping کنید؟ چرا؟
۲. 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.
۳. در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفاً آدرس IP مبدأ در بسته خروجی از شبکه تغییر می‌کند.

ip nat inside source static 192.168.100.2 200.152.200.1

سوال ۱: از PC1 و PC2 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

سوال ۲: با استفاده از دستور

show ip nat translations

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

۲-۱-۳-۲- مکانیسم NAT پویا

۱. 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

۲. یک لیست دسترسی ایجاد کنید.

سوال ۳: این لیست چه کاری انجام می‌دهد.

۳. 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

سوال ۴: این دستور چه کاری انجام می‌دهد؟

۴. از محیط تنظیم عمومی وارد تنظیمات اینترفیس ۰/۰ fastethernet شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس ۰/۰ serial شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

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

ip nat inside source list 1 pool pool1

سوال ۵: از PC1 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟

۶. با استفاده از دستور

show ip nat translations

سوال ۶: جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

۳-۱-۳-۲- مکانیسم PAT

۷. 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 192.168.100.0 0.0.0.255

یک لیست دسترسی ایجاد کنید.

سوال ۷: این لیست چه کاری انجام می‌دهد؟

۸. 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.

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

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

سوال ۸: از مسیریاب ISP را Ping PC1 و PC2 کنید. چه اتفاقی می‌افتد؟

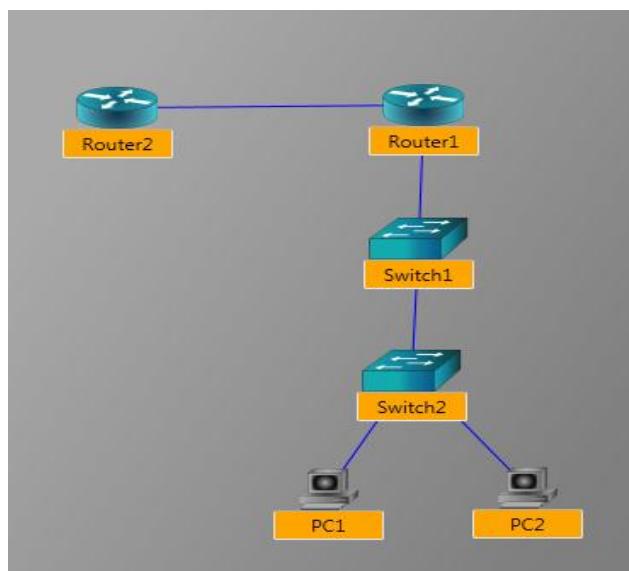
سوال ۹: با استفاده از دستور

show ip nat translations

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

۲-۳-۲ پروتکل DHCP

توپولوژی که در این آزمایش بررسی می‌شود در شکل (۱۰-۴) نشان داده است.



شکل (۱۰-۴) توپولوژی آزمایش DHCP

آدرس‌های IP واسطه‌های مسیریاب Router1 در این آزمایش در جدول (۴-۴) آمده است

جدول (۴-۴) آدرس‌های موردنیاز آزمایش DHCP

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

۱. واسطه‌ای مسیریاب Router1 را مطابق اطلاعات آدرس‌های داده شده تنظیم کنید.

۲. در محیط تنظیم عمومی مسیریاب Router1 با استفاده از دستور
service dhcp

서ویس 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.

۳. 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 اختصاص یافته را مشخص کنید. در مقابل دستور lease ابتدا روز، سپس ساعت و دقیقه می‌تواند قرار بگیرد؛ بنابراین 4 2 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.

۴. بر روی سیستم PC1 دستور

ipconfig /ip dhcp

را وارد کنید. خروجی دستور

ipconfig /all

را مشاهده کنید.

۵. بر روی مسیریاب Router1 دستور

show ip dhcp binding

را اجرا کنید و خروجی را مشاهده کنید.

۶. بر روی مسیریاب Router1 دستور

show ip dhcp server statistics

را اجرا کنید و خروجی را مشاهده کنید.

۷. 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
```

۸. دومین pool را نیز تنظیم کنید.

۹. 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.

سوال ۱۰: در مسیریاب Router2 از محیط تنظیمات خارج شوید. با استفاده از دستور

Show dhcp lease

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

۳- آشنایی با شبیه‌ساز GNS3

۱-۳- هدف آزمایش

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

۲-۳- مطالب مقدماتی

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

۱-۲-۳- معرفی GNS3

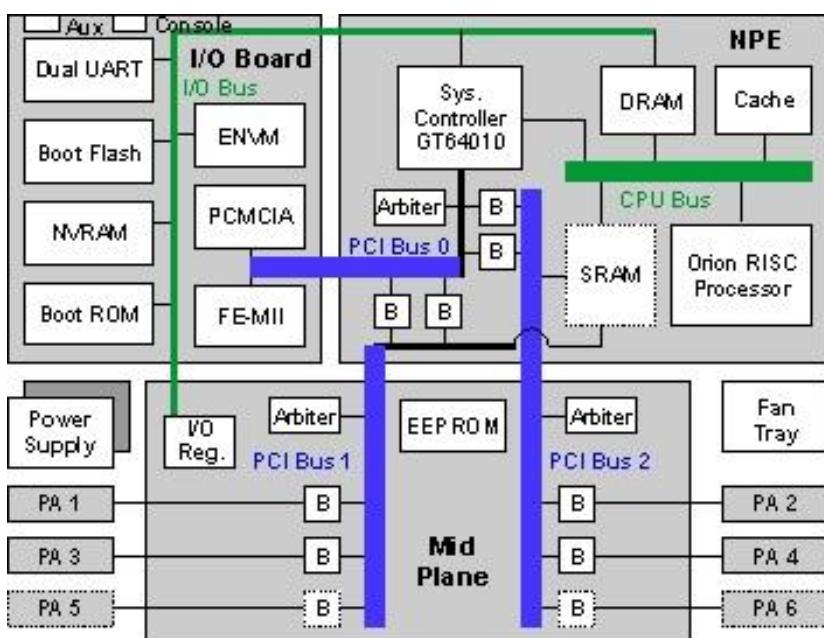
GNS3 برنامه‌ای متن‌باز همراه با محیطی گرافیکی برای شبیه‌سازی واقعی شبکه‌های پیچیده است. این نرم‌افزار با استفاده از Dynamips می‌تواند سیستم‌عامل IOS (سیستم‌عامل مخصوص مسیریاب‌ها و سوئیچ‌های CISCO) را اجرا کند. همچنین از Dynagen به عنوان یک واسط کاربری مبتنی بر متن برای ارتباط با Dynamips استفاده می‌شود.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

هر لینک را به یک پورت UDP نگاشت می‌کند. آدرس 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. آدرس Base Console شروع پورت‌های TCP است که کنسول‌های هر کدام از دستگاه‌های شبکه به آن نگاشت می‌شوند.

از آنجایی که در این آزمایش در Image مربوط به مسیریاب‌های سری ۷۲۰۰ سیسکو استفاده می‌شود لازم است در مورد معماری کلی آن اطلاعاتی داشته باشد. از مسیریاب‌های سری ۷۲۰۰، صرفاً از مسیریاب 7206VXR پشتیبانی می‌کند. معماری کلی سری ۷۲۰۰ در شکل (۱۱-۴) مشاهده می‌شود.

مهم‌ترین بخش‌های این معماری، NPE، I/O Board، 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 کلک، مدل‌های مختلفی برای NPE وجود دارد. از GNS3

NPE400 به صورت پیشفرض پشتیبانی می‌کند که نرخ کلک آن ۳۵۰ MHz است. اگر به بخش‌های مختلف I/O Board که در تنظیمات مسیریاب در Slot0 GNS3 با در هر مسیریاب شناخته می‌شود، در شکل بالا نگاه کنید، مولفه‌های Boot ROM، Boot Flash 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 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.



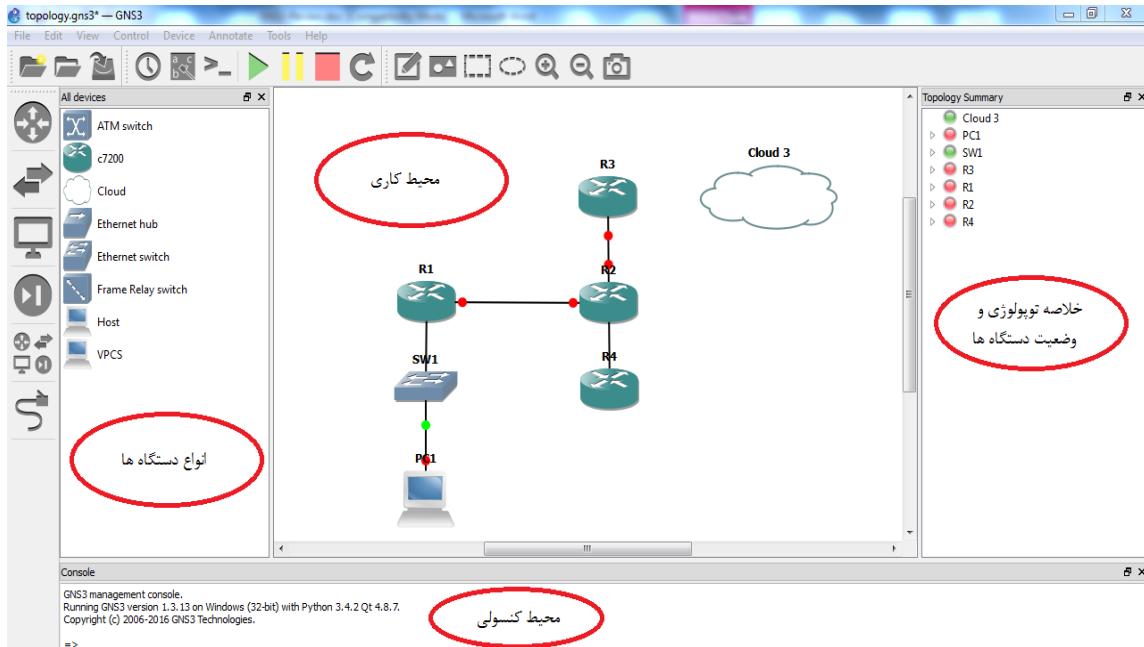
شکل (۱۱-۴) معماری کلی سری ۷۲۰۰

شکل (۱۲-۴) نمایی از واسط گرافیکی نرمافزار GNS3 است. واسط کاربری ۳ 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،

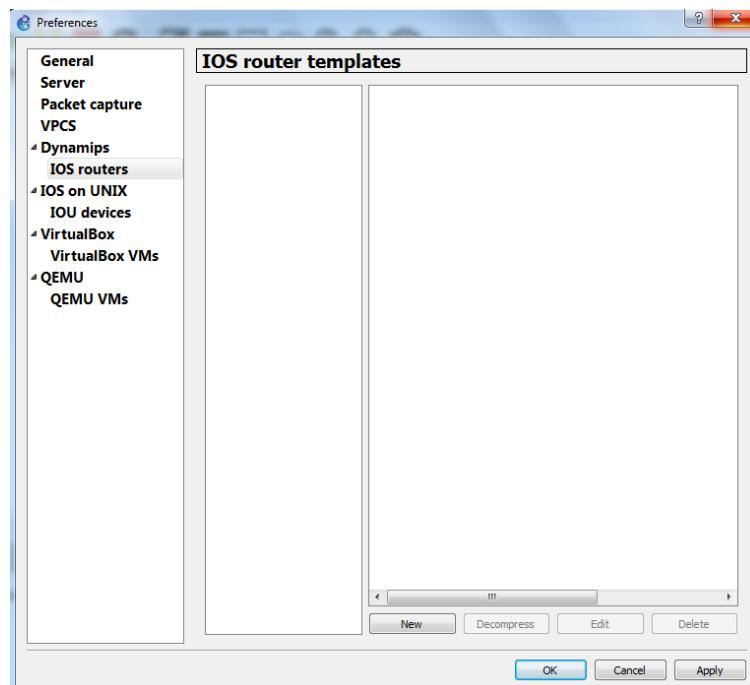
وضعیت خاموش، روشن بودن آن‌ها و همچنین نحوه اتصال این دستگاه‌ها به یکدیگر را مشاهده نمود.

- 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.



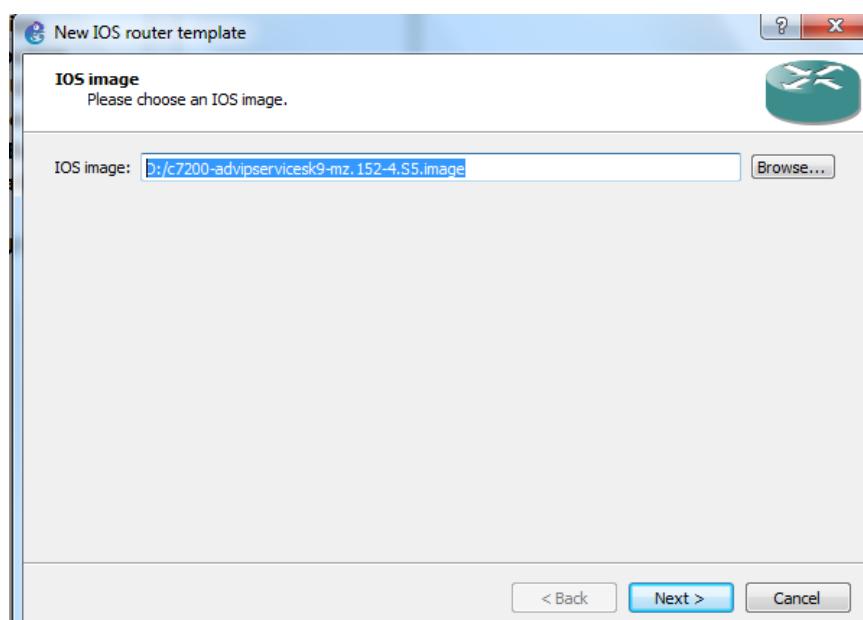
شکل (۱۲-۴) نمایی از واسط گرافیکی نرم‌افزار GNS3

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 (۱۳-۴) از بخش Zیر بخش IOS Routers Dynamips



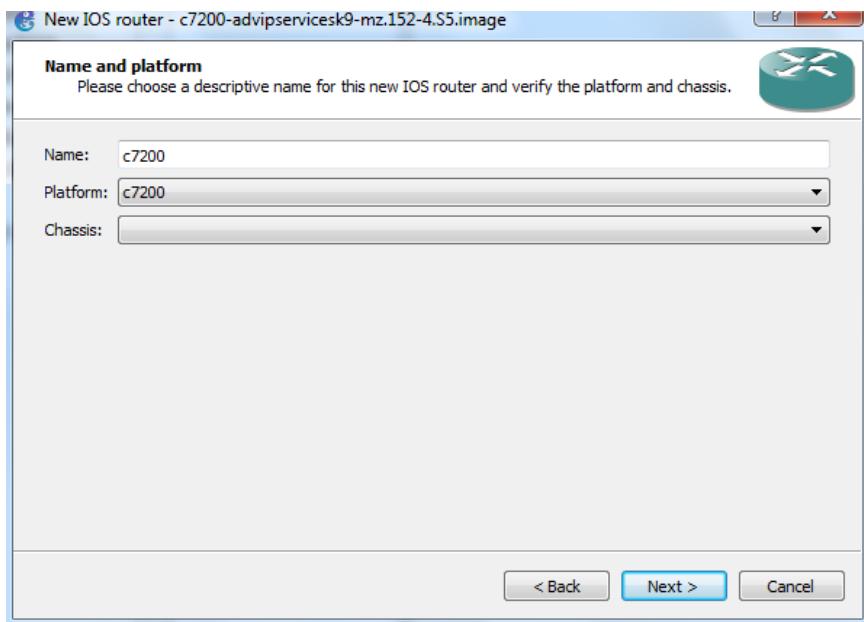
شکل (۱۳-۴) صفحه تنظیمات GNS3

سپس بر روی گزینه New کلیک کرده و مانند شکل (۱۴-۴) آدرس Image مربوطه را به برنامه بدهید.



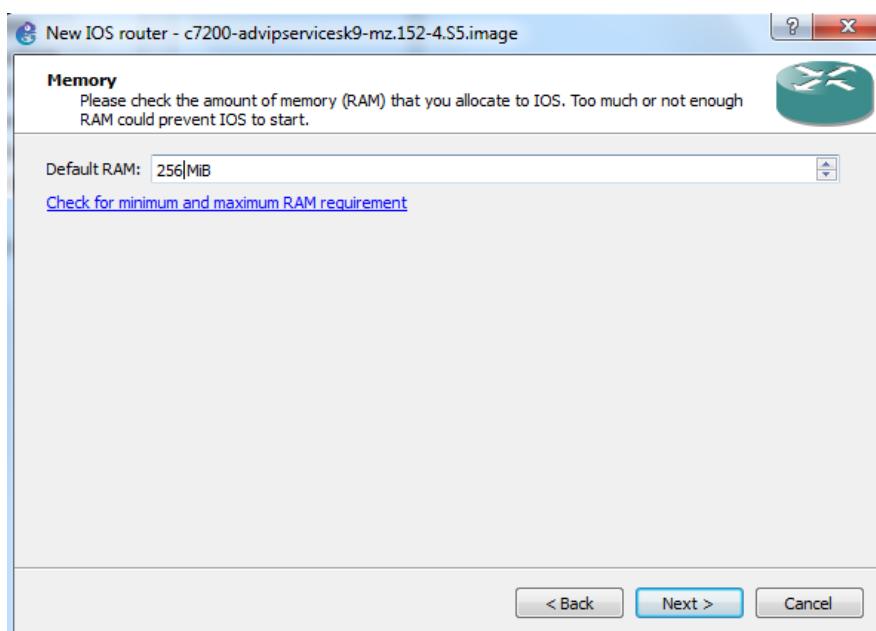
شکل (۱۴-۴) وارد کردن آدرس Image مربوطه

بر روی دکمه Next کلیک کنید. مرحله بعدی در شکل (۱۵-۴) نشان داده شده است. از آنجایی که Image اضافه شده مربوط به سری ۷۲۰۰ مسیریاب‌های سیسکو بوده است، این گزینه به صورت پیش‌فرض انتخاب شده است. بر روی دکمه Next کلیک کنید.



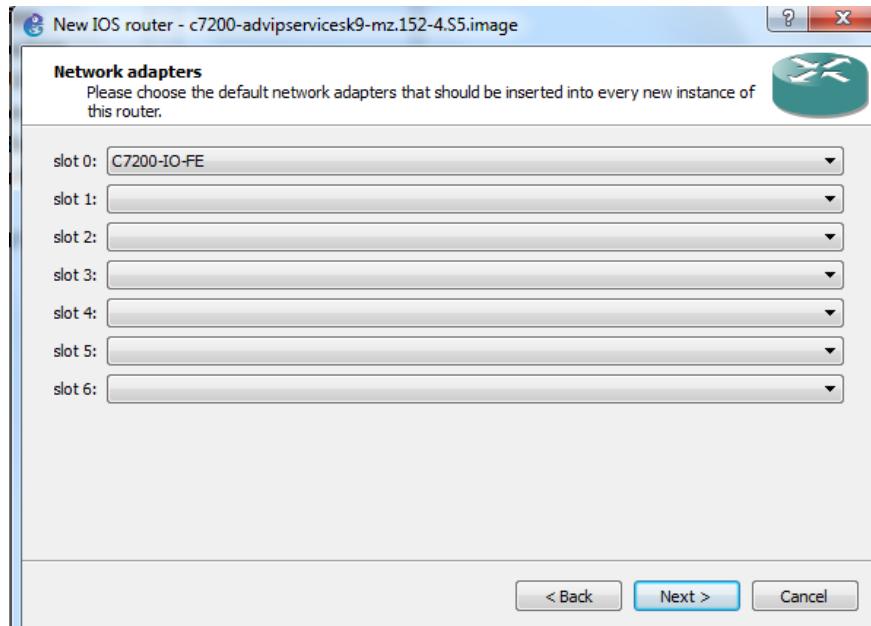
شکل (۱۵-۴) انتخاب نام Image

مطابق شکل (۱۶-۴) مقدار رم موردنیاز برای هر نمونه IOS را برابر ۲۵۶ مگابایت قرار دهید.



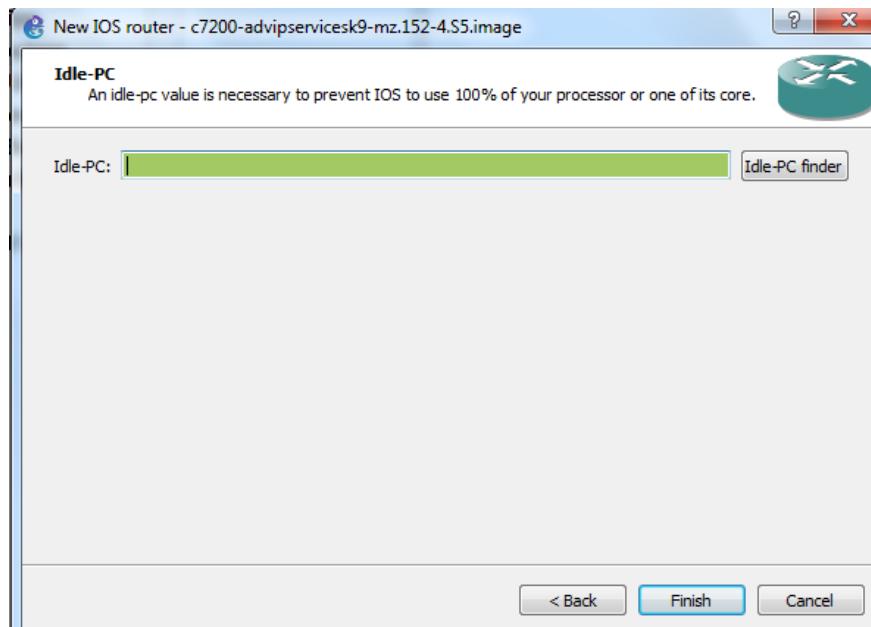
شکل (۱۶-۴) مشخص کردن میزان RAM موردنیاز برای هر نمونه IOS

برای هر مسیریابی، باید مشخص کنید که IO Controller آنچه واسطه‌ایی دارد. به طور مثال در شکل (۱۷-۴) انتخاب شده است که به هر مسیریاب یک IO Controller که دارای یک پورت Fast Ethernet است اضافه شود. انتخاب گزینه C7200-IO-2FE منجر به اضافه شدن دو پورت Ethernet می‌شود.



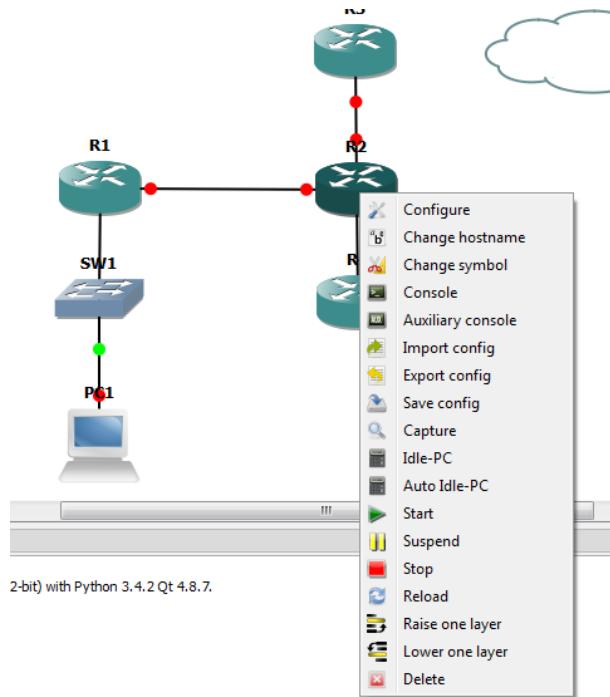
شکل (۱۷-۴) مشخص کردن واسطه‌های IO Controller مسیریاب

سپس باید مقدار Idle-PC finder انتخاب شود. مطابق شکل (۱۸-۴) بر روی کلیک کنید و پس از یافتن مقدار مناسب بر روی Finish کلیک نمایید.



شکل (۱۸-۴) 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 تopolوژی شبکه اضافه کنید. اگر بر روی هر مسیریاب، راست کلیک کنید منوی مانند آنچه در شکل (۱۹-۴) نشان داده شده است را مشاهده می‌کنید.



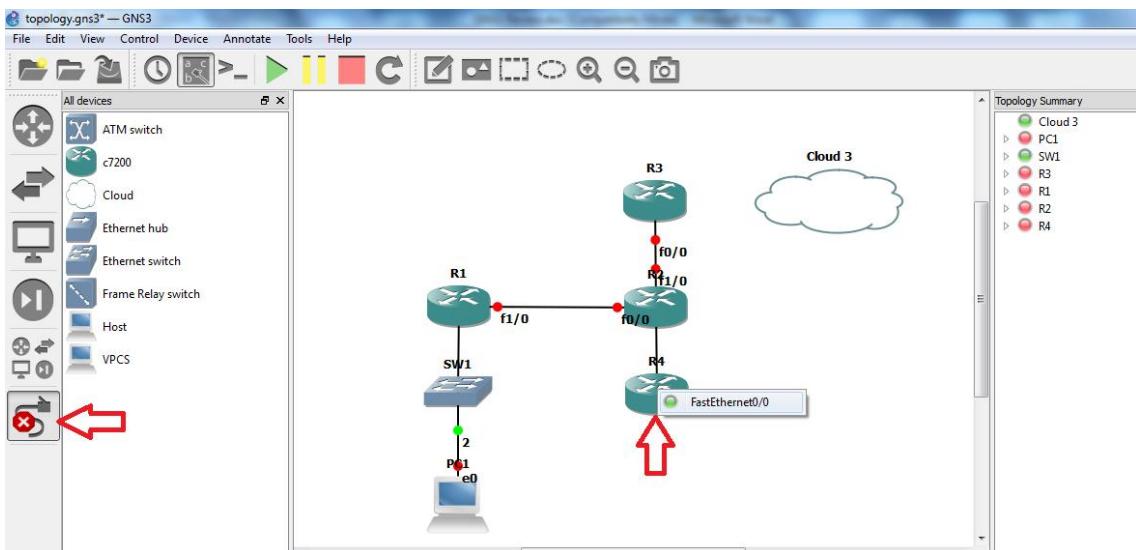
شکل (۱۹-۴) منوی در دسترس هر دستگاه

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.
- **Reload, Suspend, Stop, Start**: برای راهاندازی مسیریاب، روشن، خاموش، غیرفعال کردن دستگاه و راهاندازی دوباره مورداستفاده قرار می‌گیرند.
- **Idle PC**: 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 هنگامی که 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

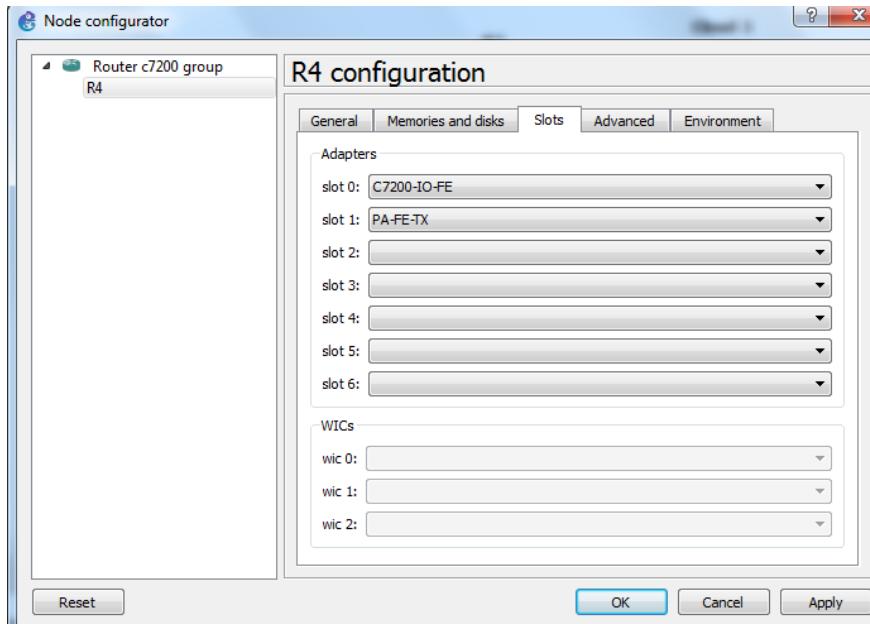
شود.

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 صرفاً 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 (۲۰-۴) می‌خواهیم از مسیریاب R4 یک لینک به سوییج اضافه کنیم. با انتخاب گزینه Add a Link از منوی دستگاه‌های GNS3 و کلیک کردن بر روی مسیریاب R4 مشاهده می‌شود که این مسیریاب صرفاً یک پورت دارد (رنگ سبز نشان‌دهنده اشغال بودن است) که آن هم قبلاً اشغال شده است.



شکل (۲۰-۴) 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 (۲۱-۴) نمایش داده شده است.



شکل (۲۱-۴) صفحه تنظیمات مربوط به مسیریاب چهارم

واسط جدید در محیط کنسول مسیریاب R4 با نام Fastethernet1/0 مشخص شده است

.(شکل (۲۲-۴)).

```

Router>en
Router#show ip int br
Router#show ip int brief
Interface          IP-Address      OK? Method Status           Protocol
FastEthernet0/0    unassigned      YES unset administratively down down
FastEthernet1/0    unassigned      YES unset administratively down down
Router#

```

شکل (۲۲-۴) واسطهای مسیریاب چهارم

اگر یک واسط دیگر از نوع PA-2FE-TX به این مسیریاب اضافه کنیم، اینترفیس‌های مسیریاب مطابق شکل (۲۳-۴) تغییر می‌کند.

```

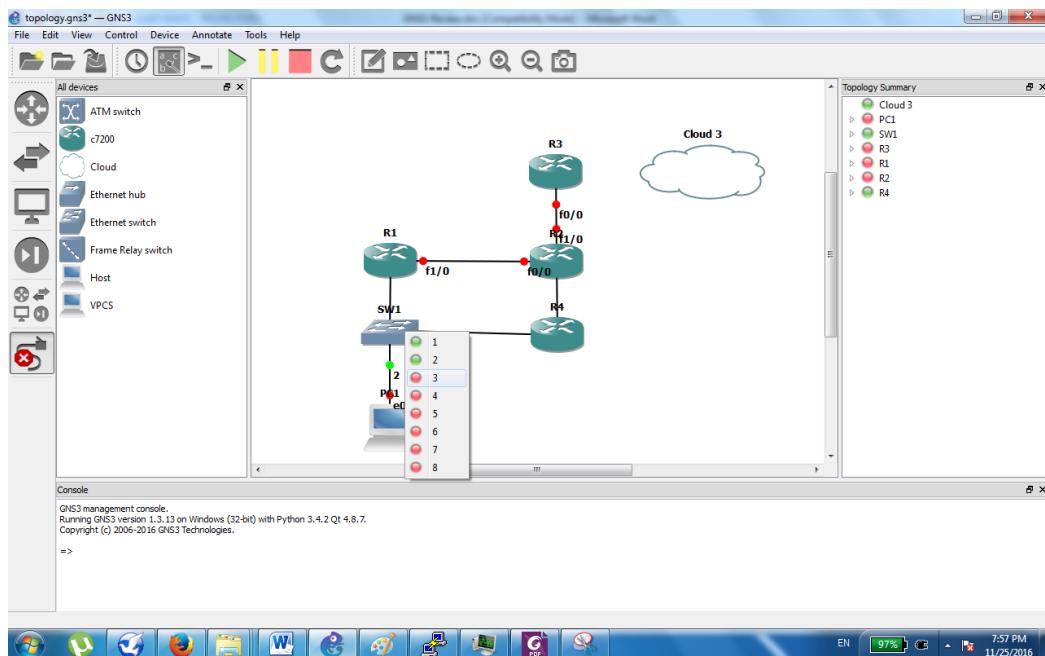
Router#show ip int brief
Interface          IP-Address      OK? Method Status           Protocol
FastEthernet0/0    unassigned      YES unset administratively down down
FastEthernet1/0    unassigned      YES unset administratively down down
Router#
*Nov 25 19:51:50.391: %OIR-6-INSCARD: Card inserted in slot 2, interfaces administratively shut down
*Nov 25 19:51:54.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to down
*Nov 25 19:51:54.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to down
Router#
Router#show ip int brief
Interface          IP-Address      OK? Method Status           Protocol
FastEthernet0/0    unassigned      YES unset administratively down down
FastEthernet1/0    unassigned      YES unset administratively down down
FastEthernet2/0    unassigned      YES unset administratively down down
FastEthernet2/1    unassigned      YES unset administratively down down
Router#

```

شکل (۲۳-۴) 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 دهد تا به سوییچ برسید و بر روی آن کلیک کنید. شکلی مطابق شکل (۲۴-۴) نمایش داده می‌شود. بر روی یکی از پورت‌های قرمز رنگ سوییچ کلیک کنید تا لینک ایجاد شود.



شکل (۲۴-۴) ایجاد لینک بین مسیریاب چهارم و پورت سوم سوییچ

به منظور 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.

۲-۲-۳ - مسیریابی

طبق مدل لایه‌ای OSI مسیریابی جزو وظایف لایه ۳ است. مسیریابی می‌تواند ایستا یا پویا باشد. در مسیریابی ایستا، جداول مسیریابی بدون استفاده از پروتکل‌های مسیریابی در هر مسیریاب ایجاد می‌شود. معمولاً در شبکه‌هایی که تغییرات توپولوژی به ندرت 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 به وسیله 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^{۴۰} (LS) و بردار فاصله^{۴۱} (DS) تقسیم نمود.

⁴⁰ Link State

در پروتکل‌های مسیریابی DV هر گره کل جدول مسیریابی خود را صرفاً 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^{۴۱} 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 متتمرکز کوتاه‌ترین مسیر (نظیر Dijkstra) کم‌هزینه‌ترین مسیر به تمام گره‌های شبکه را محاسبه کرده و جدول مسیریابی خود را به روز 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 راه حل‌های 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 صرفاً با توجه به کلاس‌های IP، در مورد بسته‌های به روزرسانی 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 (۵-۴) مشاهده می‌شود. آدرس شبکه 127.0.0.0 رزرو شده است. کلاس D برای Multicasting و کلاس E برای اهداف تحقیقاتی استفاده می‌شود.

⁴¹ Distance Vector

⁴² LSDB

جدول (۴-۵) کلاس‌های مختلف IP

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

۳-۳- قطعات و ابزارهای موردنیاز

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

عبارت‌اند از:

- یک کامپیوچر با سیستم‌عامل ویندوز
- نرم‌افزار GNS3 نسخه ۱.۳.۱۳ یا بالاتر
- Cisco IOS 7200 Image •

۴-۴- فعالیت‌های قبل از آزمایش

به سوالات زیر پاسخ دهید:

سوال ۱: فواید و معایب استفاده از مسیریابی ایستا را شرح دهید.

سوال ۲: در چه مواردی از مسیریابی ایستا استفاده خواهیم کرد؟

سوال ۳: از چه الگوریتم‌های دیگری به غیر از بلمن فورد می‌توان در پروتکل‌های مسیریابی استفاده کرد. نحوه کار آن‌ها را توضیح دهید.

سوال ۴: فرمت پیام‌های مسیریابی RFC2453 را از RIPv2 به دست آورده و رسم نمایید و همچنین فیلدهای آن را توضیح دهید.

سوال ۵: آدرس‌دهی سلسله مرتبی را با ذکر مزایا و معایب آن شرح دهید.

۳-۵- شرح آزمایش

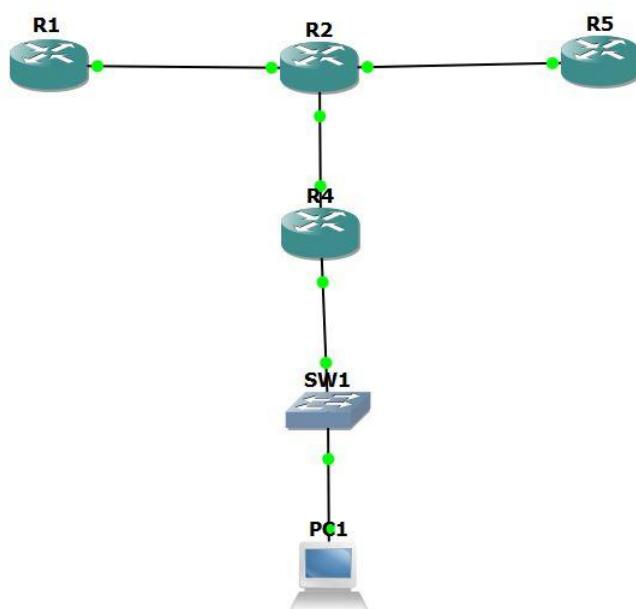
همان‌طور که ذکر شد یکی از هدف‌های انجام این آزمایش آشنایی با پروتکل‌های مسیریابی شبکه اینترنت است. به این منظور این آزمایش به دو بخش زیر تقسیم می‌شود:

- مسیریابی ایستا (Static Routing)
- پروتکل مسیریابی RIP

۳-۱-۵- 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 می‌توانند توسط مدیر شبکه به صورت دستی وارد شده یا توسط نرم‌افزار از قبل محاسبه شده و در مسیریاب‌ها وارد شده باشد.

۱. شبکه نشان داده شده در شکل (۲۵-۴) را در محیط شبیه‌ساز ایجاد کنید.



شکل (۲۵-۴) توپولوژی شبکه آزمایش مسیریابی ایستا

۲. آدرس‌های IP زیر را به واسطه‌های مسیریاب‌ها اختصاص دهید و نام آن‌ها را مطابق جدول (۶-۴)، تغییر دهید.

جدول (۴-۶) آدرس‌های IP دستگاه‌های شبکه

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

سوال ۶: چرا واسطه‌ایی که با FastEthernet به یکدیگر وصل شده‌اند، نیازی به تنظیم clock rate ندارند؟

۳. از مسیریاب شماره ۱ مسیریاب شماره ۴ را Ping کنید.

سوال ۷: نتیجه Ping را تحلیل نمایید.

سوال ۸: برای آنکه از مسیریاب ۱ مسیریاب ۴ Ping شود (و برعکس) بر روی چه مسیریاب‌هایی باید جدول جلوهای ایجاد گردد؟

۴. بهمنظور ایجاد مسیر از مسیریاب ۱ به مسیریاب ۴، با استفاده از دستور ip route جداول جلوهای 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

۵. از محیط تنظیمات خارج شده و از مسیریاب شماره ۱ مسیریاب شماره ۴ را Ping کنید.

سوال ۹: نتیجه Ping را تحلیل نمایید.

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

۷. با استفاده از دستور

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

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

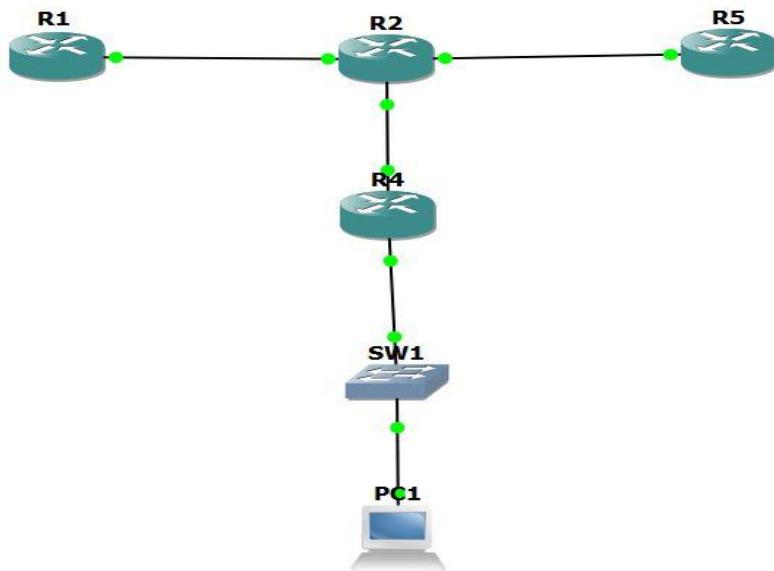
۳-۵-۲- مسیریابی RIPv2

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 ۳۰ ثانیه یکبار به گره‌های همسایه ارسال می‌کند و بر اساس جدول‌های رسیده، جدول مسیریابی هر مسیریاب با استفاده از الگوریتم بلمن فورد به روزرسانی شده و مسیر با حداقل هزینه انتخاب می‌شود. فاصله بیشتر از ۱۶ گام به عنوان مقصد غیرقابل دسترس برای این پروتکل شناخته می‌شود. در صورت

پیدا کردن مسیرهای یکسان، پروتکل از حداقل ۴ 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.

۱. شبکه نشان داده شده در شکل (۲۶-۴) را در محیط شبیه‌ساز ایجاد کنید.



شکل (۲۶-۴) توپولوژی شبکه آزمایش مسیریابی RIPv2

۲. دستگاه‌ها را مطابق جدول (۷-۴) آدرس‌دهی نمایید. همچنین نام مسیریاب‌ها را نیز مطابق جدول زیر تغییر دهید.

جدول (۷-۴) آدرس‌های IP دستگاه‌های شبکه

Device	Interface	IP Address	Subnet Mask
Router2	FastEthernet 0/0	10.1.1.1	255.255.255.0
	FastEthernet 1/0	92.168.1.1	255.255.255.0
	FastEthernet 0/1	172.16.1.1	255.255.255.0
Router1	FastEthernet 0/0	10.1.1.2	255.255.255.0
Router4	FastEthernet 0/0	192.168.1	255.255.255.0
	Loopback 0	2.10.1.2.1	255.255.255.0
Router5	FastEthernet 0/0	172.16.1.2	255.255.255.0
	Loopback 0	10.1.3.1	255.255.255.0

۳. 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
```

۴. با استفاده از دستور Ping مطمئن شوید آدرس‌دهی‌ها درست بوده است.
۵. ابتدا وارد محیط تنظیم عمومی شوید. سپس با استفاده از دستور rip و سپس با دستور 2 version 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 ۱، ۲، ۴ و ۵ انجام دهید.

سوال ۱۰: چه گزینه‌های دیگری برای دستور router وجود دارد؟

۶. برای هر مسیریاب شبکه‌هایی که به آن متصل هستند را با استفاده از دستور network وارد کنید. به عنوان مثال برای مسیریاب شماره ۱ دستور به صورت 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 (۸-۴) است. دقت کنید آدرس‌های Loopback نیز باید تنظیم شوند.

جدول (۸-۴) آدرس‌های شبکه

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

۷. از محیط تنظیمات خارج شوید. سپس با دستور show ip protocols پروتکل‌های مسیریابی فعال بر روی مسیریاب Router1 را بررسی کنید.
۸. با استفاده از دستور show ip route جدول مسیریابی مسیریاب شماره ۲ را بررسی کنید. بررسی کنید که مسیریاب، به چه شبکه‌هایی دسترسی دارد و تفاوت شبکه‌های مشخص شده با شبکه‌های کانفیگ شده در چیست؟
۹. از محیط تنظیمات خارج شوید و سعی کنید که از مسیریاب شماره ۱ آدرس Loopback مسیریاب شماره ۴ Ping را کنید
- سوال ۱۱: چرا Ping موفقیت‌آمیز بود؟

۴- آشنایی با پروتکل مسیریابی OSPF

۱-۴- هدف آزمایش

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

۲-۴- 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 تopoلوزی شبکه را در خود ذخیره کرده و در صورت هرگونه تغییر در حالت پیوندها، تغییرات را به صورت سیل‌آسا اطلاع‌رسانی می‌کند که به آن^{۴۳} 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^{۴۴} تعیین کنیم. در پروتکل‌های مسیریابی از نوع LS هر مسیریاب حداقل سه جدول جداگانه را نگهداری می‌کند. یکی از این جداول وضعیت همسایگانی را که مستقیماً به مسیریاب متصل شده‌اند نگهداری می‌کند. در جدول دیگر، تopoلوزی شبکه 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 کاهش سربار عملیات مسیریابی، افزایش سرعت همگرایی و محدود کردن اعلام تغییرات شبکه در یک ناحیه و عدم انتشار آن به سایر نواحی شبکه می‌شود. با به کارگیری ویژگی فوق می‌توان شبکه‌ای بزرگ را به چندین شبکه کوچک‌تر که به آن‌ها ناحیه^{۴۵} گفته می‌شود، تقسیم نمود. در صورتی که ابعاد یک شبکه بسیار بزرگ باشد، یک گزینه مناسب پروتکل OSPF است. این پروتکل سرعت همگرایی بالائی دارد و توانایی توزیع بار بین چندین مسیر با هزینه یکسان به یک مقصد را دارد.

در پروتکل OSPF، هر کدام از ناحیه‌های شبکه یک ID منحصر به فرد ۳۲ بیتی دارند. به ناحیه مرکزی، Backbone گفته می‌شود و آن ۰ است. تمامی نواحی دیگر باید به این ناحیه مرکزی متصل باشند. انواع مختلف مسیریاب در پروتکل OSPF در جدول (۹-۴) آمده است.

⁴³ Link-State Advertisement

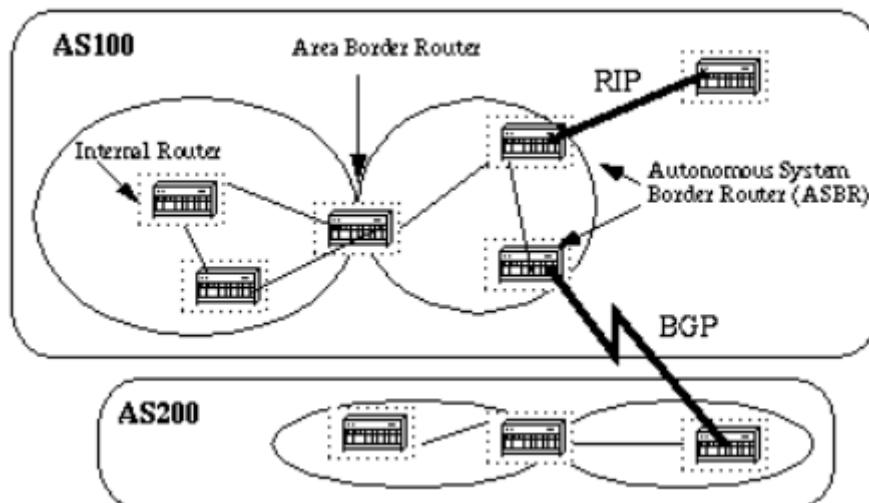
⁴⁴ Process ID

⁴⁵ Area

جدول (۹-۴) انواع مسیریاب در پروتکل OSPF

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

مثالی از این مسیریاب‌ها در شکل (۲۷-۴) مشاهده می‌شود.



شکل (۲۷-۴) 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.
- در یک لینک با دسترسی چندگانه، توسط یک Designated Router منتشر می‌شود و بیانگر مسیریاب‌هایی هستند که به آن لینک دسترسی دارد.

- LSA هایی که توسط ASBR منتشر می شود بیانگر شبکه خارج AS یا آدرس default route برای شبکه خارجی است.

عملکرد کلی پروتکل به شرحی است که در ادامه می آید. هر مسیریاب در بازه های Hello پیغام های Hello را بر روی واسطه های خود ارسال می کند. هر مسیریاب که پیغام Hello مسیریاب دیگر را دریافت کند، آن را به عنوان neighbor خود انتخاب می کند. مادامی که دو مسیریاب فعال هستند پیغام های Hello منتشر خواهد شد. هر مسیریاب به اندازه زمان Dead Interval منتظر دریافت پیغام Hello می ماند. اگر در این مدت هیچ پیام HELLO از مسیریاب همسایه دریافت نشود، فرض بر این گذاشته می شود که مسیریاب همسایه غیرقابل دسترس است. همچنین شرط زیر نیز علاوه بر دریافت پیغام Hello باید برقرار باشد تا دو مسیریاب همسایه یکدیگر شوند:

- شماره Area و نوع آن باید در همه آن ها یکسان باشد.
- مدت زمان بین ارسال پیام های Hello و همچنین Dead Interval باید در همه آن ها یکسان باشند. زمان پیش فرض به ترتیب ۱۰ و ۴۰ ثانیه است.
- در صورت فعال کردن احراز هویت، مسیریاب ها 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 ۳۲ بیتی دارد که بی ارتباط به آدرس IP است ولی می تواند یکی از آدرس های IP مسیریاب نیز باشد. سه راه برای انتخاب شناسه مسیریاب^{۴۶} 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 اختصاص یافته تغییر نخواهد کرد. در صورت تغییر باید تنظیمات پروتکل OSPF از ابتدا انجام شود. این شناسه در پیغام های منتشر شده در پروتکل قرار خواهد گرفت.

پس از اینکه مسیریاب همسایه های خود را شناسایی کرد، رابطه مجاورت^{۴۷} را با آن ها برقرار می کند. در این مرحله مسیریاب ها، پایگاه های داده خود را با یکدیگر مبادله می کنند. برای مسیریاب هایی که به یک واسط مشترک دسترسی دارند یک Router Designate انتخاب می شود و

⁴⁶ Router-id

⁴⁷ Adjacency

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. پس از این حالت، مسیریاب‌ها وارد مرحله Loading خواهند شد و اطلاعات گم شده 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 سیل آسا فقط داخل یک Area منتشر خواهد شد و ABR مسئولیت انتقال اطلاعات شبکه به سایر ABR‌ها 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 واسطه مربوطه است. همچنین برای هر Area یک جدول وجود دارد.

- آدرس‌هایی که در Area فعلی وجود دارد. Router Link state
- تعداد اینترفیس‌های مسیریاب مشخص شده با ADV Router در آن Area است.
- معمولاً توسط Designate Router ایجاد می‌شود Net link state
- واسط Designate Router در آن بخش است.
- این جدول بیانگر آدرس‌های خارج از Area فعلی است که توسط ABR‌ها منتشر شده است. Summary Net link state
- توسط ADV Router ها همه ABR‌ها هستند

۳-۴- فعالیت‌های قبل از آزمایش

به سوالات زیر پاسخ دهید:

- سوال ۱: تفاوت‌های پروتکل‌های مسیریابی OSPF و RIPv2 را بیان کنید.
- سوال ۲: فرمت پیام‌های مسیریابی OSPF را از RFC 2178 به دست آورده و رسم نمایید و همچنین فیلدهای آن را توضیح دهید.

۴- قطعات و ابزارهای موردنیاز

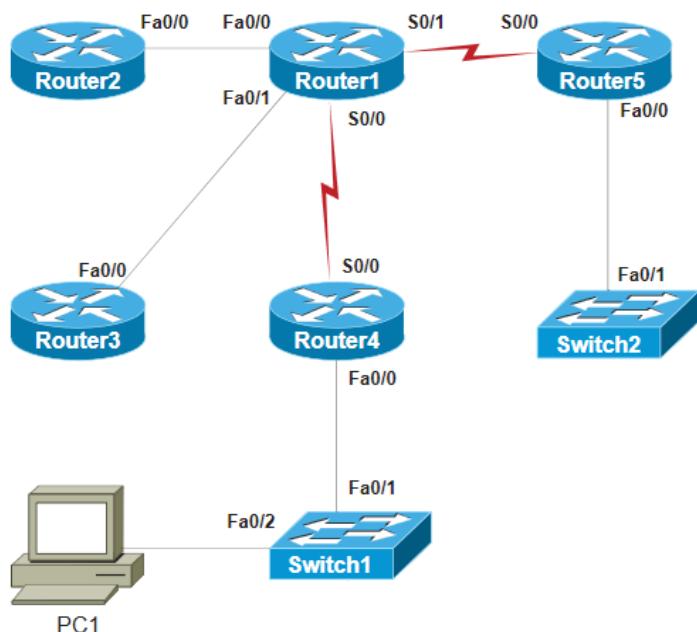
فهرست قطعات، تجهیزات و ابزارهای (سختافزاری و نرمافزاری) لازم برای انجام این آزمایش عبارت‌اند از:

- یک کامپیوتر با سیستم‌عامل ویندوز
- نرمافزار GNS3 نسخه ۱.۳.۱۳ یا بالاتر

۴-۵- شرح آزمایش

۱-۵- دستور کار اول

شبکه شکل (۲۸-۴) را در محیط شبیه‌ساز ایجاد کنید.



شکل (۲۸-۴) توپولوژی شبکه آزمایش اول OSPF

واسطه‌های مسیریاب‌ها را مطابق جدول (۱۰-۴) آدرس‌دهی نمایید. نرخ Clock را برابر ۶۴۰۰۰ تنظیم نمایید.

جدول (۱۰-۴) آدرس‌های IP در آزمایش اول OSPF

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

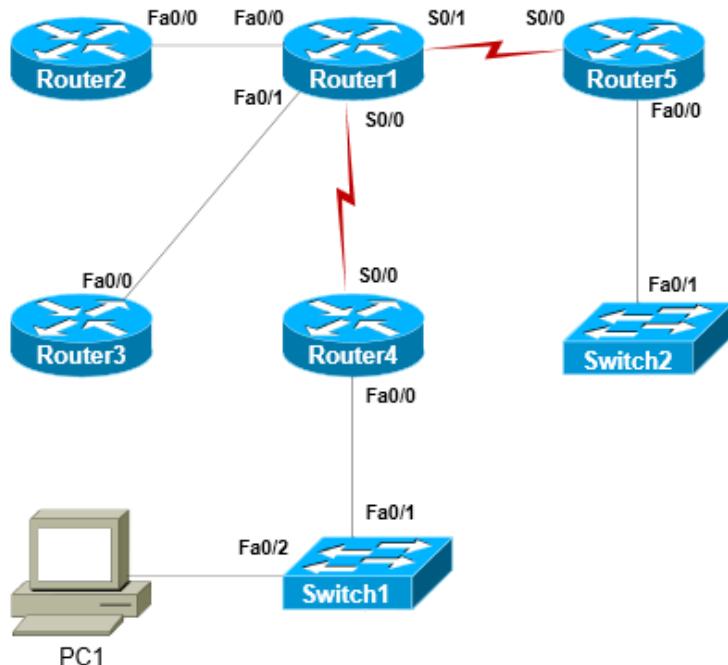
۱. هر مسیریاب می‌تواند همزمان چندین نمونه از پروتکل مسیریابی، با تنظیمات متفاوت را اجرا کند. در حالی که برای سایر پروتکلهای مسیریابی چنین قابلیتی وجود ندارد. برای این منظور، باید یک شماره فرآیند به نمونه پروتکل مسیریابی اجرا شده اختصاص یابد؛ بنابراین بر روی مسیریاب ۱، وارد محیط تنظیمات عمومی شوید و با دستور

router ospf 100

- یک نمونه از فرآیند مسیریاب برای پروتکل OSPF با شناسه 100 ایجاد نمایید.
۲. بر روی مسیریاب ۱، شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه ۰ اضافه کنید.
network 10.1.1.0 0.0.0.255 area 0
 ۳. بر روی مسیریاب ۱، شبکه 172.16.10.0 را با wildcard 0.0.0.255 و شناسه ناحیه ۰ اضافه کنید.
network 172.16.10.0 0.0.0.255 area 0
 ۴. بر روی مسیریاب ۲، وارد محیط تنظیمات عمومی شوید. یک فرآیند OSPF را اجرا و از شناسه فرآیند ۱۰۰ استفاده کنید. سپس بر روی آن شبکه 10.1.1.0 را با wildcard 0.0.0.255 و شناسه ناحیه ۰ اضافه کنید.
 ۵. بر روی مسیریاب ۴، وارد مسیریاب فرآیند ۱۰۰ را اجرا و از شناسه 172.16.10.0 را با wildcard 0.0.0.255 و شناسه ناحیه ۰ اضافه کنید.
 ۶. همان‌طور که می‌بینید مسیریاب‌های ۲ و ۴ به‌طور مستقیم به یکدیگر متصل نیستند. از هر یک از این مسیریاب‌ها، دیگری را ping کنید و نتایج را تحلیل کنید.
 ۷. با دستور Show ip route جدول مسیریابی مسیریاب‌های ۱، ۲ و ۴ را مشاهده کنید.
 ۸. با استفاده از دستور show ip protocols اطلاعات پروتکل‌های مسیریابی را در مسیریاب ۱ مشاهده نمایید.
 ۹. با دستور Show ip ospf پایگاه داده مربوط به پروتکل OSPF مسیریاب‌های ۱، ۲ و ۴ را مشاهده کنید. ID هر یک از مسیریاب‌ها را یادداشت نمایید.
 ۱۰. با دستور Show ip ospf neighbor همسایه‌های مسیریاب‌های ۱، ۲ و ۴ را مشاهده کنید. همچنین، ID مسیریاب‌ها، Address و Dead Time آن‌ها را یادداشت نمایید.
- سوال ۳: آیا ID با Address فرق دارد؟
۱۱. بر روی مسیریاب ۱، وارد تنظیمات واسط ۰/۰ Fastethernet شده و زمان ارسال بسته‌های Hello را به ۲۰ ثانیه افزایش دهید (درصورتی که از شبیه‌ساز BOSON استفاده می‌کنید، دستور زیر پیاده‌سازی نشده‌اند).
ip ospf hello-interval 20
 ۱۲. بر روی مسیریاب ۱، زمان Dead Interval Time را به ۸۰ ثانیه تغییر دهید (درصورتی که از شبیه‌ساز BOSON استفاده می‌کنید، دستور زیر پیاده‌سازی نشده‌اند).
ip ospf dead-interval 80
- سوال ۴: توضیح دهید چرا ارتباط مسیریاب ۱ با مسیریاب ۲ برقرار نیست؟

۴-۵-۲- دستور کار دوم

شبکه نشان داده شده در شکل (۲۹-۴) را در محیط شبیه‌ساز ایجاد کنید.



شکل (۲۹-۴) توپولوژی شبکه آزمایش دوم

واسطه‌های مسیریاب‌ها را مطابق جدول (۱۱-۴) آدرس‌دهی نمایید. نرخ Clock را برابر ۶۴۰۰۰ تنظیم نمایید.

جدول (۱۱-۴) آدرس‌های IP در آزمایش دوم OSPF

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

۱. در محیط تنظیم عمومی مسیریاب Router1 با دستور

router ospf 100

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

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

network 10.1.1.0 0.0.0.255 area 0

۳. 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.
۴. 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.

۵. در محیط تنظیم عمومی مسیریاب Router2 با دستور

router ospf 10

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

۶. 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

۷. 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
در حالی که مسیریاب Router1 و Router2 مستقیماً به یکدیگر متصل هستند.

سوال ۵: توضیح دهید چه اتفاقی رخ داده است؟

۸. 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.

۹. از محیط تنظیمات مسیریاب Router2 خارج شوید. دستور

show ip ospf neighbor

را بر روی مسیریاب Router1 اجرا کنید.

سوال ۶: توضیح دهید چه اتفاقی رخ داده است؟

۱۰. 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 به جای # شماره فرآیند قرار می‌گیرد، وارد تنظیمات فرایند شوید.
۱۱. با استفاده از دستور

router-id 60.60.60.60

۱۲. شناسه مسیریاب را تغییر دهید.

سوال ۷: مسیریاب چه پیغامی را نمایش می‌دهد؟

۱۳. 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.

سوال ۸: به مسیریاب Router1 بروید. چه پیغام‌هایی برای مسیریاب با شماره 10.1.1.2 مشاهده می‌کنید؟

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

show ip ospf

ID مسیریاب را مشاهده نمایید.

سوال ۹: چه تغییری رخ داده است؟

۱۵. دستور

show ip ospf neighbor

را بر روی مسیریاب Router1 اجرا کنید.

سوال ۱۰: خروجی چه تفاوتی با مرحله ۹ دارد؟

۱۶. 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.

سوال ۱۱: آیا نیازی به پاک کردن فرآیند OSPF وجود دارد؟ چرا؟

۱۷. با استفاده از دستور

router ospf 100

وارد تنظیمات فرآیند OSPF در 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.

۱۸. از محیط تنظیمات خارج شده و دستور

show ip ospf neighbor

را اجرا کنید.

سوال ۱۲: چرا آدرس Loopback اضافه شده جز همسایه‌های مسیریاب Router1 نیست؟

۱۹. دستور

show ip ospf database

را بر روی مسیریاب Router1 اجرا کنید.

سوال ۱۳: آیا آدرس Loopback اضافه شده را آنجا مشاهده می‌کنید؟

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

سوال ۱۴: چرا ping موفقیت‌آمیز است؟

۲۱. واسط سریال مسیریاب‌های Router4 و Router1 را نیز کانفیگ کرده و واسطه‌ای آن‌ها را مطابق جدول (۱۱-۴) در area های مربوطه قرار دهید.

۲۲. در مسیریاب Router4، دستور

show ip route

را اجرا کنید.

سوال ۱۵: در مقابل ردیف مربوط به آدرس 50.50.50 عبارت‌های O و IA نوشته شده است. این‌ها چه معنی دارند؟

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

show ip ospf route

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

۲۴. در مسیریاب Router1 دستور

show ip ospf

را اجرا کنید.

سوال ۱۶: این مسیریاب از چه نوع از مسیریاب‌های گفته شده در OSPF است؟

۵- کار با شبیه‌سازی GNS3

۱-۵- هدف آزمایش

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

۲-۵- فعالیت‌های قبل از آزمایش

آزمایش آشنایی با شبیه‌سازی GNS3 را مرور کنید.

۳-۵- قطعات و ابزارهای مورد نیاز

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

- یک کامپیوتر با سیستم‌عامل ویندوز
- نرم‌افزار GNS3 نسخه ۱.۳.۱۳ یا بالاتر
- Cisco IOS 7200 Image
- برنامه Wireshark

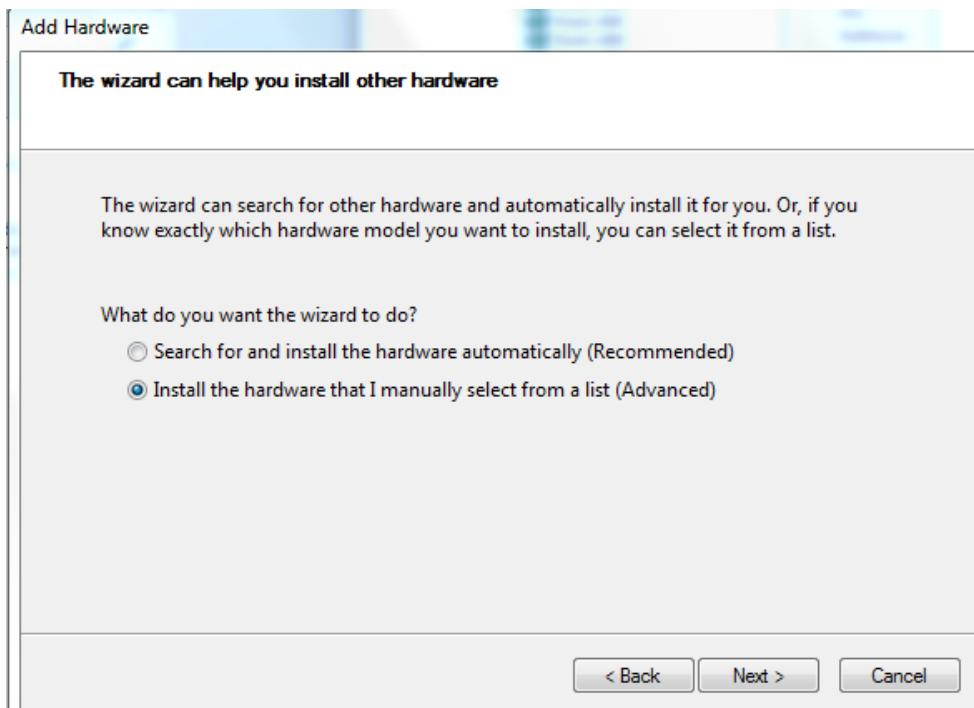
۴-۵- شرح آزمایش

ابتدا باید یک Loopback Adaptor را به سیستم اضافه کنید. برای این کار با فشردن دکمه استارت ویندوز ۷، hdwwiz.exe را جستجو کنید. پس از باز کردن برنامه دکمه Next را زده و مطابق شکل (۳۰-۴) گزینه دوم را انتخاب کنید.

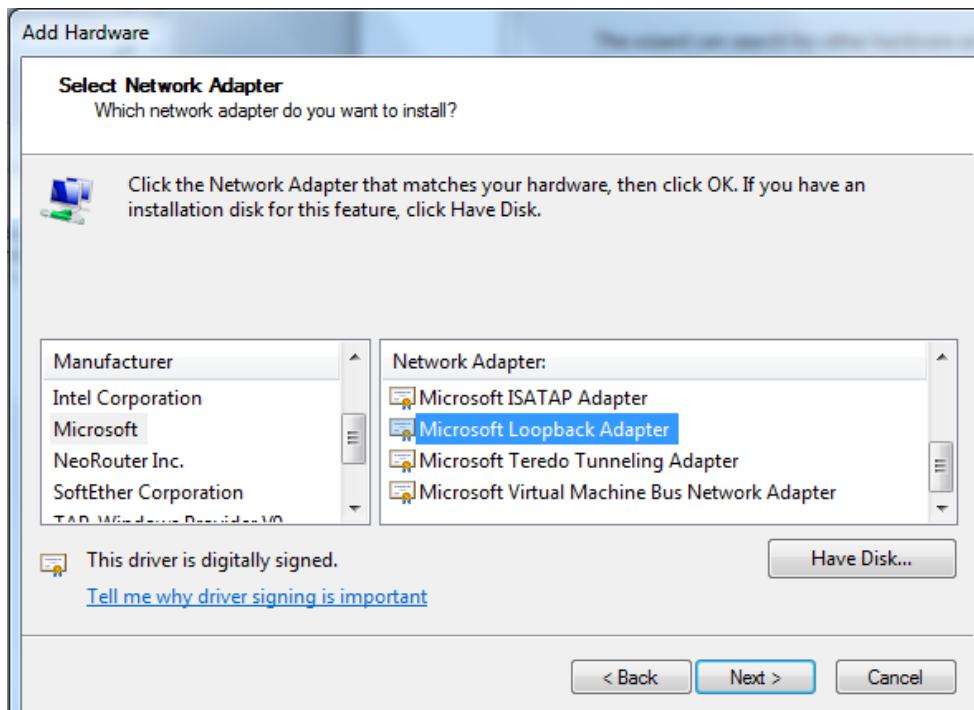
در صفحه بعد، Network Adaptors را انتخاب کرده و Next را بزنید. از بین دستگاه‌های نمایش داده شده، مطابق شکل (۳۱-۴)، Microsoft Loopback adaptor را انتخاب کنید. پس از زدن دکمه Next و نصب Loopback Adaptor، سیستم را ری استارت کنید.

پس از ورود به محیط ویندوز، از محیط کنترل پنل ویندوز ۷ عبارت Network را جستجو کنید و Network and Sharing Center را انتخاب کنید. سپس از ستون سمت چپ، change 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 (۳۲-۴)

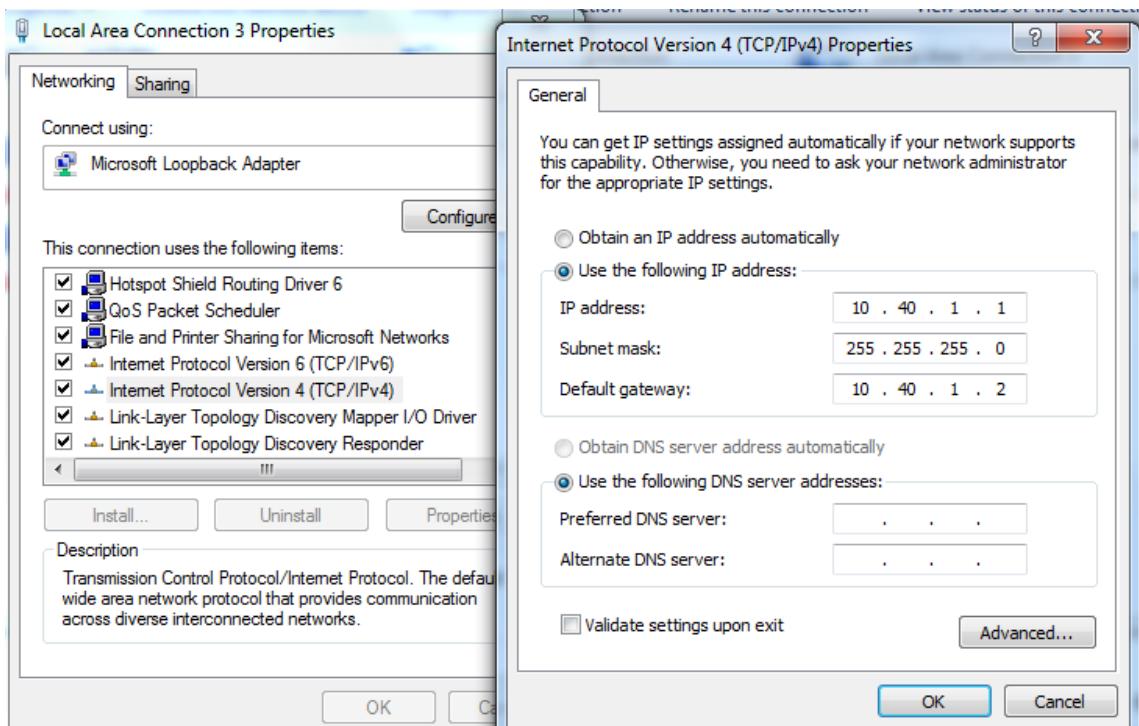
انجام دهید.



شكل (٣٠-٤) ایجاد Loopback Adaptor - مرحله اول

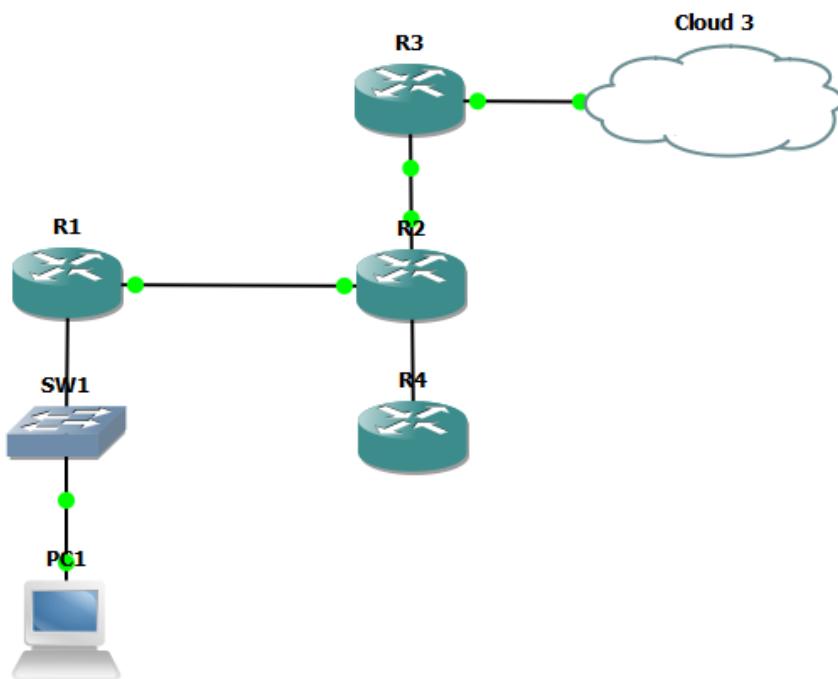


شكل (٣١-٤) ایجاد Loopback Adaptor - مرحله دوم



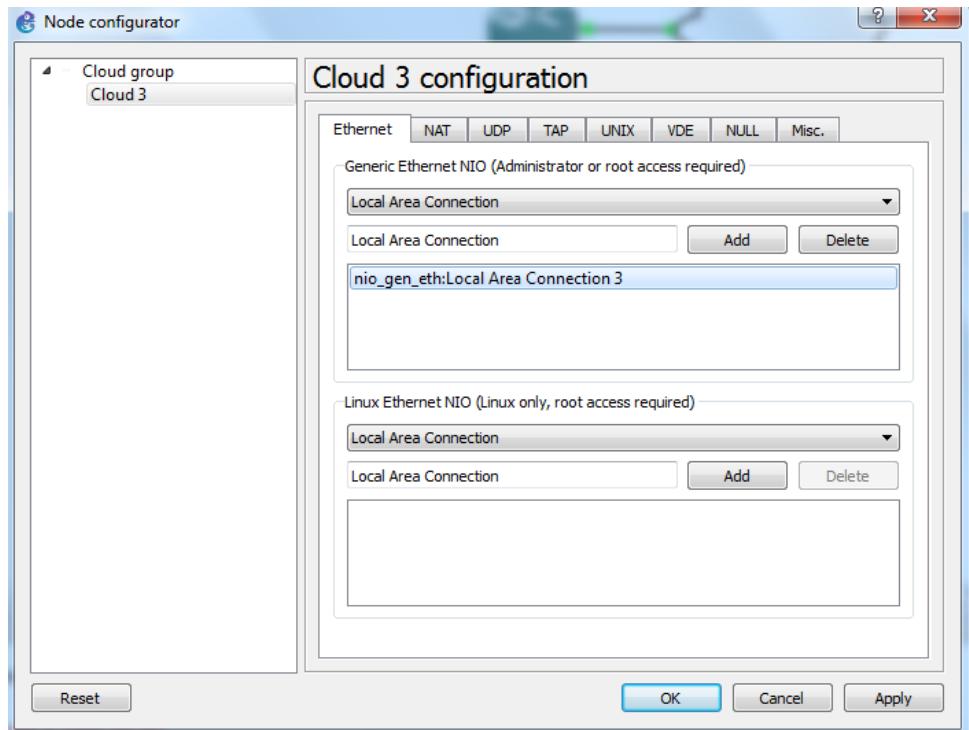
شکل (۳۲-۴) ایجاد Loopback Adaptor مرحله سوم

۱. شبکه نشان داده شده در شکل (۳۳-۴) را در محیط شبیه‌ساز ایجاد کنید.



شکل (۳۳-۴) توپولوژی شبکه

۲. در محیط شبیه‌ساز بر روی ابر کلیک راست کنید و گزینه Configure را انتخاب کنید. سپس در بخش Ethernet، مطابق شکل (۳۴-۴) Local Area Connection ایجاد شده را به عنوان دستگاهی که این ابر به آن متصل است انتخاب کرده و دکمه Add را فشار دهید.



شکل (۳۴-۴) پیکربندی ابر

۳. پس از انجام این کار، ابر را به مسیریاب R3 متصل کنید.
۴. آدرس‌های IP را طبق جدول (۱۲-۴) به دستگاهها اختصاص دهید.

جدول (۱۲-۴) آدرس IP دستگاهها

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

۵. همه آدرس‌های IP داده شده را بر روی همه مسیریاب‌ها تنظیم کنید.

۶. 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 مقصد بسته در هیچ یک از شبکه‌های تنظیم شده بر روی مسیریاب قرار نداشت، بسته به آدرس 10.40.1.1 ارسال شود.

۷. بر روی واسط 1/0 در مسیریاب R1 با استفاده از wireshark بسته‌های ارسال شده را شنود کنید و تا پایان آزمایش آن را خاتمه ندهید.

۸. تمام مسیریاب‌ها باید قادر به Ping یکدیگر باشند. با استفاده از پروتکل‌های مسیریابی که تا به حال بررسی کرده‌اید، تنظیمات لازم را انجام دهید.

۹. 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.

۱۰. 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.

۱۱. 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 ping google.com را انجام دهید. حال آدرس google.com را ping کنید.

۱۲. با استفاده از پروتکل DHCP به PC1 آدرس IP اختصاص دهید. 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.

۱۳. 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.

۱۴. بسته‌های دریافت شده در Wireshark را ذخیره کنید.

سوال ۱: ترتیب اجرای پروتکل‌های مختلف و بسته‌های رد و بدل شده را بررسی کنید.