تمرین ششم شبکه های کامپیوتری - دکتر صبایی

سوال اول)

الف) لایه شبکه ۴ وظیفه اصلی دارد:

- Routing) در شبکه تعداد زیادی مبدا و مقصد وجود دارد. یکی از وظایف اصلی لایه شبکه انتخاب ریشه های صحیح برای برقراری ارتباط است. الگوریتم های متعددی برای تعیین مبدا و مقصد و همچنین مسیر وجود دارد.
- Packetizing) بسته های Packet از لایه Transport به لایه شبکه منتقل میشود و طی فرایندی این بسته ها به بسته های جدیدی از نوع Datagram تبدیل می شوند که هدر های متعددی از جمله IP دارد.
- Addressing) از دیگر وظایف این لایه تخصیص دادن یک شناسه منحصر به فرد به هر دستگاه است که با آن شناخته شود.

به طور کلی وظیفه این لایه (برای گیرنده) دریافت بسته ها از لایه انتقال و ساخت نوعی بسته کامل تر با مشخصات بیشتر و انتخاب مسیر ارسال در نهایت و ارسال آنها به لایه پایین تر است که به دو وظیفه Data Plane و Control Plane تقسیم می شود. پروتکل های متعددی در این راستا درگیر هستند.

ب) تفاوت اصلی این دو روش آن است که در Traditional Networking وظایف سخت افزاری تعریف شده (و معمولا تغییر یا ارتقا آنها دشوار و پر هزینه است) که در Data Plane تعیین میشوند اما در روش SDN وظایف نرم افزاری تعریف شده و قابلیت تغییر آسان تری دارند که از طریق Control Plane تعیین میشود. به واسطه این طراحی روش Traditional Networking به صورت غیر متمرکز بوده در صورتی که SDN یک سامانه متمرکز است. از طرفی مشکل یابی و نگهداری SDN بسیار آسان تر از Traditional Networking است.

ج) مزیت ها:

- قابلیت Programmable بودن شبکه نرم افزاری تغییر یا بهبود آنها را آسان تر می کند.
- هزینه Maintenance کمتری داشته و عیب یابی آنها راحت تر است.
- به صورت متمرکز بوده و الگوریتم های مسیریابی آن در برخی ویژگی ها بهتر عمل میکند.
- طراحی آسان تری نسبت به Traditional Networking دارند

سوال دوم)

الف) در Datagram Packet Switching با هر بسته دیتاگرام به صورت یک ماژول جدا رفتار میشود به طوری که هر ماژول به خود به تنهایی روی شبکه ارسال و مدیریت می شود. از طرفی یک سرویسی است که در آن نیاز به connection نداریم و در نتیجه نیازی به تخصیص منابع و رزرو کردن آنها نداریم. این درصورتی است که در Virtual Packet Switching یک مسیر بین مبدا

و مقصد برقرار شده است که بسته ها از طریق آن منتقل می شوند. به همین دلیل اتصال زنده (live connection) نیاز داشته و جریان بنظر یک جریان فیزیکی می آید.

ب) مقایسه این دو طراحی:

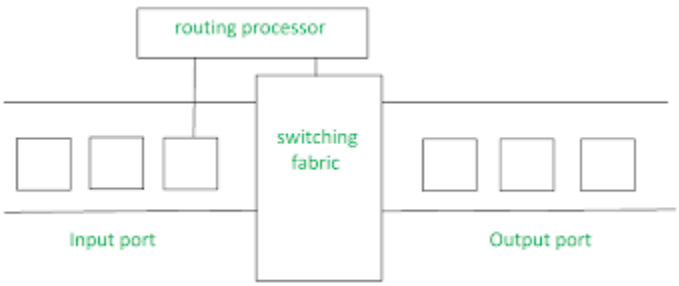
- اتصال زنده: طراحی DPS به جریان زنده نیاز ندارد یا به عبارتی هیچ مسیر خاصی به اتصال تخصیص داده نشده. اما طراحی VPS یک مسیر برای انتقال تخصیص داده شده. به عبارتی روش دوم نیاز به منابع بیشتر و ثابت تری دارد.
- مسیر انتقال: در طراحی DPS هر بسته اختیار در انتقال از هر مسیری که Routing Algorithm برای آن تعیین بکند را دارد. به عبارتی هر بسته میتواند (در حالت تئوری) از مسیر مختلفی عبور کند اما در روش VPS یک مسیر تعیین شده و تمامی بسته ها از آن عبور می کنند.
- ترتیب دریافت: در طراحی DPS بسته ها لزوما با ترتیب ارسال شده دریافت نمی شوند زیرا از مسیر ها ی مختلفی عبور کرده که تاخیر های متفاوتی دارند. اما در طراحی VPS همه بسته ها لزوما ترتیب یکسان دارند.
- قابل اطمینان بودن: طراحی DPS برخلاف VPS قابل اطمینان نیست به دلایل متعددی از جمله دلایل بالا.
- در طراحی DPS ما Efficiency بالا و تاخیر بالا داریم اما در طراحی VPS هر دو معیار کم هستند.

ج) اگر مسیریاب ها به سرعت از کار می افتند بهتر است از DPS استفاده کنیم زیرا در VPS یک مسیر در ابتدا تخصیص داده میشود که تعداد زیادی مسیریاب دارد و از کار افتادن هر یک منجر به از بین رفتن کل مسیر میشود.

ذ) در این حالت مسیریاب ها ظرفیت کمتری داشته و منطقی است که ما هم فشار کمتری روی مسیریاب ها بگذاریم. پس انتخاب DPS به دلیل نیاز نداشتن به تخصیص منابع انتخاب بهتری است.

سوال سوم)

الف)



در هر مسیریاب تعدادی پورت ورودی و خروجی داریم که توسط جدولی به یکدیگر map می شوند. از طرفی routing processor الگوریتم مسیریابی را اجرا کرده و مسیر بعدی را مشخص می کند. از طرفی map کردن پورت های ورودی به خروجی نیز از مسئولیت های routing processor است.

تمرین ششم شبکه های کامپیوتری - دکتر صبایی

ب) بار اصلی آن است که برای هر بسته ورودی باید الگوریتم مسیریابی صورت بگیرد و این سربار زیادی دارد. کار های زیادی می توان انجام داد از جمله بهبود الگوریتم مسیریابی و افزایش قدرت پردازنده از نظر سخت افزاری و نرم افزاری. همچنین طراحی کلی بهتر برای اینکه کمتر دچار packet loss شویم. زیرا packet loss منجر به دوباره درگیر شدن پردازنده می شود.

ج) در VPS هر فریم دریافتی دو بار کپی می شود که خود سربار است. دفعه اول از Network Adapter به بافر موقت و بعد از بافر موقت به بافر برنامه. از طرفی تخصیص منابع باعث می شود کارآمدی و عملکرد مسیریاب کاهش یابد. برای حل این مشکلات میتوان پردازنده قوی تری طراحی کرد و I/O throughput را بهبود داد. همچنین بهبود الگوریتم مسیریابی نیز کمک کننده است.

سوال چهارم)

الف) ۱) در روش classless هیچ محدودیت و سقفی بر روی network ID و host ID نداریم. ۲) فرایند تخصیص IP رو روش classless طراحی شده تا rapid exhaustion را کاهش دهد. ۳) در روش classless تعداد iP بیشتری می توانیم اختصاص دهیم. ۴) روش classless داینامیک تر است.

ب) این روش برعکس subnetting بوده که یک IP Address بزرگ را به subnetwork های کوچیک تر تقسیم میکرد. در عوض این روش شبکه های متعددی را به یکدیگر پیوند زده تا شبکه حتی بزرگتری داشته باشیم.

سوال پنجم)

الف)

- Inside Local Address) به Ip Address های اختصاص داده شده به دستگاه های داخل شبکه گوییم.
- Inside Global Address) یک Host که به طور فیزیکی داخل شبکه موجود است اما به آدرس آن از زاویه یک gateway به خارج از شبکه نگاه میکنیم.
- Outside Local Address) آدرس دستگاه های درون یک شبکه است که نوعی private شده و به طور مستقیم قابل دسترسی و اتصال مستقیم نیستیم.
- Outside Global Address) یک public address بوده که خارج از شبکه ما است و شامل تعداد زیادی outside local address (از نگاه ما) است.

ب) ماژول ۱۷۲.۱۶۸.۲۰.۱۰ قصد برقراری ارتباط با ماژول ۱۹۲.۱۰۰.۲۰.۲ داشته که روی یک شبکه نیستند. پس برای ارتباط ابتدا بسته را به Gateway Router ارسال کرده که توسط NAT پس از بررسی امکان ترجمه داشتن ترجمه می شود. اگر شرایط مهیا بود Inside Local Address به Inside Global Address تبدیل شده و پس از ذخیره شدن ارسال می شود. بعد از پاسخ دادن سرور آدرس دوباره به ۱۹۲.۱۰۰.۱۰.۲۵ بازگشته که در NAT به ۱۷۲.۱۶۸.۲۰.۱۰ ترجمه میشود که Inside Local Address است.

سوال هفتم)

تمرین ششم شبکه های کامپیوتری - دکتر صبایی

الف) کافی است کوچکترین آدرس و همچنین بزرگترین آدرس را مرتبا شنود کرده و ذخیره کنیم. در نهایت تعداد کل آدرس ها برابر: *(آخرین آدرس - اولین آدرس)* + *1* خواهد بود.

ب) خیر نمی تواند. در عوض باید تک تک آدرس ها را شنود کرده و اگر تکرار نشده بودند به لیستی اضافه کنیم.

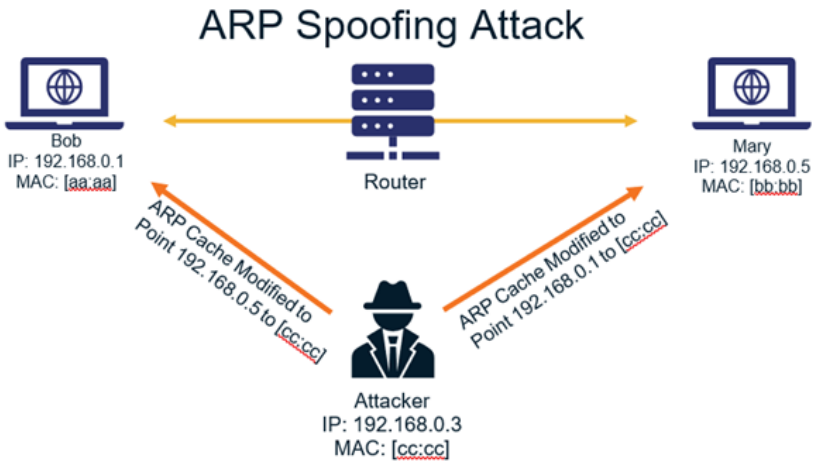
سوال هشتم)

بله زیرا برای آدرس های استاتیک NAT چک میکند که آدرس ها از پیش موجود نباشند. اما برای آدرس های محلی نیازی نیست و کافی است اگر آدرس از قبل استفاده نشده بود آن را در جدول NAT بروزرسانی کنیم. (اضافه کنیم)

سوال نهم)

الف) این پروتکل به زبان ساده Ip Address را به Physical Address ترجمه می کند زیرا در اصل انتقال و ارتباطات بر اساس MAC Address است و نه Ip Address. روش کار به این صورت است که ARP یک بسته ی درخواستی را برای همه دستگاه های موجود در شبکه پخش می کند که آیا هر یک از ماشین ها از همان IP Address خاص استفاده می کنند یا خیر. هنگامی که یک ماشین IP Address را متعلق به خود می‌شناسد، یک پاسخ ارسال می‌کند تا ARP بتواند حافظه را برای مراجعات بعدی آن دستگاه را به روز کند و ارتباط را ادامه دهد.

ب) در ARP Spoofing یک حمله کننده پیام ARP روی شبکه محلی ارسال می کند که باعث می شود MAC Address حمله کننده به IP Address یک دستگاه موجود در شبکه متصل شود و به آن ارتباط برقرار کند.



سوال یازدهم)

الف) انگیزه اصلی نیاز جهانی به IP Address های منحصر به فرد بوده زیرا IPv4 در حال اتمام بود. حال با IPv6 میتوان به تعداد خیلی بیشتری IP داشت و حالا حالا ها تمام نمی شود (:

ب) مزایا IPv6 نسبت به IPv4:

- در IPv6 بر خلاف Ipv4 که تنها ۳۲ بیت برای ساخت IP داشتیم حال ۱۲۸ بیت داریم!

- هدرهای IPv6 بسیار بهینه سازی شده به طوری که برخی هدر هایی اضافه حذف شده است.
- از طرفی IPv6 امکان هدر های اضافه را دارد.
- امنیت پروتکل جدید نسبت به قدیمی افزایش پیدا کرده است.
- دارا بودن Header Checksum که میتوان با استفاده از آن بسته را دوباره ارسال کرد.
- دارا بودن Options که در قسمت payload می آید.
- قابلیت Fragmentation و Reassembly که فقط در مبدا و مقصد صورت میگیرد. افزایش امنیت!

ج) اجزا و شرط وظایف:

- Version) این فیلد IP Version Number را مشخص میکند که در پروتکل جدید ۶ بیت دارد. نکته ای که وجود دارد آن است که گذاشتن ۴ رو این فیلد منجر به پروتکل Ipv4 نمیشود!
- Traffic Class) این فیلد ۸ بیت دارد که این امکان را میدهد که برای بسته های دیتاگرام اولویت تعیین کنیم.
- Flow Label) این فیلد ۲۰ بیت گرفته که جریان دیتاگرام ها را مشخص می کند.
- Payload Length) این فیلد ۱۶ بیتی اندازه payload را مشخص می کند که همان data است. در ادامه آن ۴۰ بیت هدر داریم.
- Next Header) این هدر مانند نسخه قبلی مشخص می کند چه پروتکلی برای انجام عملیات استفاده می شود. برای مثال UDP و TCP
- Hop Limit) مشخص می کند چند با دیتاگرام ارسالی می تواند فرستاده شود. به عبارتی مقدار این فیلد با هر بار ارسال یکی کم شده و زمانی که معادل صفر شود بسته دیتاگرام loss می شود. نوعی فیلد کنترلی و صحت سنجی است.
- Source and Destination Addresses) آدرس های مبدا و مقصد برا بسته است.
- Data) همان payload بوده و دیتا های مورد انتقال

د) در این حالت مبدا تلاش میکند تا کوچک ترین MTU را با استفاده از فرایند MTU Discovery پیدا کند. به این صورت که مبدا یک بسته با اندازه مشخص می فرستد و اگر پیام Too Big دریافت کرد اندازه آن را کاهش می دهد. این کار تا جایی تکرار می شود که پیغام Too Big دریافت نشود. این پیام در بخش option مقدار Don't Fragment دارد.

همچنین بیت M Flag مشخص می کند که آیا بسته آخرین Fragment بوده یا خیر. پس ماژول انتهایی به سادگی می تواند آن را تشخیص دهد.

سوال دوازدهم)

در این پروتکل ۴ مرحله وجود دارد: اول Server Discovery بوده که در آن این پروتکل به دنبال دستگاه های تازه متصل به شبکه است. بعد از یافتن آنها و در مرحله دوم IP Lease Offer داریم که به این دستگاه ها پیشنهاد IP Address می شود تا

راحت تر به شبکه متصل شده. این تنها یک پیشنهاد است که به همه میرود و میزبان میتواند آن را قبول نکند (ولی میکند ^_^). بعد میزبان هایی که این پیشنهاد را قبول میکنند با ارسال IP Lease Request آن را درخواست می کنند. در مرحله بعد IP Lease Acknowledge از طرف سرور DHCP به میزبان ارسال شده که به آن IP تخصیص می دهد.

این پروتکل در لایه Application بوده و برای پروتکل های UDP و TCP کارکرد دارد و بر روی سرور DHCP قرار می گیرد. هدف از استفاده این پروتکل ساده سازی فرایند تخصیص IP است.

سوال سیزدهم)

الف) این الگوریتم که دو نوع متمرکز و غیر متمرکز دارد یک مسیر بین دو مبدا و مقصد برای ارسال بسته های داده مشخص می کند. هدف این الگوریتم کاهش ترافیک و سرعت بخشیدن ارتباطات است.

ب) در این الگوریتم هر مسیریاب اطلاعات مسیریاب های اطراف خود را با بقیه مسیریاب ها به اشتراک میگذارد. به طور دقیق تر این الگوریتم از Dijkstra استفاده میکند و به دلیل متمرکز بودن این الگوریتم سریع تر Converge می شود.

ج) این الگوریتم غیر متمرکز و iterative و async بوده که در آن هر مسیریاب اطلاعات مسیریاب های دیگر که به طور مستقیم به آنها وصل شده را فقط دیده و بر اساس آن بخشی از مسیر را بهینه می کند. (الگوریتم Bellman Ford)

د) تفاوت ها:

- در Distance Vector نیاز به bandwidth پایین دارد زیرا بسته ها به صورت محلی به اشتراک گذاشته می شوند اما در Links State برعکس این حالت است.
- در Distance Vector بر اساس دانش محلی تصمیمی گیری میشود اما در Link State بر اساس دانش کلی شبکه
- در Distance Vector از Bellman Ford استفاده شده ولی در دیگری از Dijkstra
- ترافیک Distance Vector بسیار کمتر از Link State است
- الگوریتم Distance Vector غیر متمرکز است اما Link State متمرکز است. میتوان گفت به این دلیل الگوریتم اولی کمی سریع تر باشد.
- الگوریتم Distance Vector بسیار دیرتر از Link State میتواند Converge کند.
- در Distance Vector شاهد Persistent Looping هستیم اما در دیگر نه - زیرا اطلاعات همه node ها را داریم!

سوال چهاردهم)

الف) این الگوریتم non-adaptive بر این اساس کار می کند که زمانی که یک بسته از به یک router می رسد آن بسته به تمام مسیر های دیگر بجز مسیری که از آن آمده ارسال می شود. این الگوریتم به چند دسته تقسیم می شود:

ب) الگوریتم بسیار ساده ای است که حتما کوتاه ترین مسیر را انتخاب می کند.

ج) معایب:

- تعداد زیادی بسته بدون استفاده (duplicate) ساخته می شود.
- الگوریتمی است که به تمام مقصد ها بسته را می فرستد در صورتی که فقط یک مقصد به آن نیاز دارد.
- باعث افزایش ترافیک شبکه و تاخیر ارسال بسته ها میشود.

د) راه حل ها:

- ساختن ورژن های مختلف این الگوریتم که باعث بهبود آن میشود:
  - Uncontrolled Flooding) بسته به تمام همسایه ها ارسال می شود.
  - Controlled Flooding) بسته به الگوریتم های مختلف بسته ارسال می شود.
  - Selective Flooding) بسته فقط به مسیر هایی ارسال می شود که بنظر میرسد به سمت مقصد هدایت می شوند و نه به تمام مسیر ها
- افزودن hop counter و فیلد hop برای حذف duplicate ها

سوال پانزدهم)

Step	N’	D(t), P(t)	D(u), P(u)	D(v), P(v)	D(w), P(w)	D(y), P(y)	D(z), P(z)
0	x	infinite	infinite	3, x	6, x	6, x	8, x
1	xv	7, v	6, v	3, x	6, x	6, x	8, x
2	xvu	7, v	6, v	3, x	6, x	6, x	8, x
3	xvuw	7, v	6, v	3, x	6, x	6, x	8, x
4	xvuwy	7, v	6, v	3, x	6, x	6, x	8, x
5	xvuwyt	7, v	6, v	3, x	6, x	6, x	8, x
6	xvuwytz	7, v	6, v	3, x	6, x	6, x	8, x

سوال شانزدهم)

الف) این روش نوعی Loop Avoidance Method است که در آن یک مسیر را Poison می کنیم تا از اهمیت آن بکاهیم. برای مثال اگر مقدار هزینه مسیر ها بین صفر تا ده باشد ما هزینه یک مسیر را عمدا یازدهم گذاشته تا بی نهایت تلقی شود.

سوال هفدهم)

تمرین ششم شبکه های کامپیوتری - دکتر صبایی

الف) یک سیستم مستقل به مجموعه ای از Prefix IP Address ها گفته می شود که متعلق به یک شبکه بوده که توسط یک نهاد مرکزی کنترل می شوند.

ب) انوع آن:

- Multihomed) یک سیستم مستقل که با دو یا چند سیستم مستقل دیگر در ارتباط است.
- Transit) یک سیستم مستقل که به عنوان رابط بین دو یا چند سیستم مستقل خارجی عمل می کند.
- Single-homed (stub)) یک سیستم مستقل که با فقط با یک سیستم مستقل دیگر در ارتباط است.

ج) به دلیل آن است که Inter-Domain Routing تمام اینترنت خارج یک سیستم مستقل را نادیده می گیرد در صورتی که یک Intra-Domain Routing فرض می کند اینترنت شامل تعداد زیادی سیستم های مستقل غیر مرتبط (disconnected) است.

هدف ساده سازی فرایند Routing برای سیستم های مستقل است. به این صورت که یک Inter-Domain Routing نیاز به دانش خارج از سیستم مستقل خودش ندارد و بدیهی است سریعتر و با منابع کمتر به عملکرد خود میرسد. از طرفی امنیت را بسیار افزایش می دهد.

د) برای افزایش امنیت هر سیستم به طوری که ماژول های کوچک تر داخل این سیستم ها با خیال راحت تری امنیت را برقرار می کند.

سوال هجدهم)

الف) همیشه مسیری که کمترین تعداد hop را دارد به عنوان مسیر بهینه انتخاب می شود. پروتکل RIP با محدود کردن تعداد hop بین مبدا و مقصد باعث می شود تا از بوجود آمدن حلقه در مسیر جلوگیری کنیم و از طرفی مسیر بهتری انتخاب کنیم.

الگوریتم مورد استفاده در این روش Distance-Vector است و در لایه Application استفاده می شود.

ب) UDP

ج) حداکثر تعداد hop که می توانیم استفاده کنیم ۱۵ است. پس اندازه شبکه نمیتواند دلخواه و بزرگتر از ۱۵ hop باشد.

د) هر پیام RIP می تواند نهایتا 512 byte دیتا را منتقل کند و شامل Version، IP Address، Subnet Mask، Next Hop، Version و فیلد های دیگر است.

سوال نوزدهم)

از آنجایی که z میخواهد ترافیک y را منتقل کند، به y درخواست میفرستد. حال y دیتاگرامی دارد که باید به آدرسی در z برود. ولی اگر z به y پیامی فرستاد، y فقط می تواند از طریق x آن را re-advertise کند و چاره ای نیست.

سوال بیستم)

با استفاده از فیلد AS_PATH و بررسی آن می توان به وجود حلقه پی برد. اگر شماره سیستم مستقل محلی در این فیلد نبود یعنی در حلقه گیر کرده ایم.

تمرین ششم شبکه های کامپیوتری - دکتر صبایی

سوال بیست و یکم)

الف) این پروتکل بین دستگاه های محلی یک شبکه مورد استفاده قرار میگیرد تا ارور ها و مشکلات موجود را با یکدیگر به اشتراک بگذارند. به گونه ای یک report protocol است. این پروتکل در لایه شبکه وجود دارد.

ب) این برنامه با فرستادن پیام ICMP به یک interface روی یک شبکه و منتظر بودن برای جواب کار میکند.

ج) این برنامه با مپ کردن اینکه چطور دیتا از مبدا به مقصد بر روی اینترنت منتقل می شود به ما کمک میکند. به طوری که ماژول های میانی را میبینیم و میتوانیم آن را تحلیل کنیم. همچنین اطلاعاتی برای تاخیر و زمان این انتقالات به ما می دهد.

سوال بیست و دوم)

الف) دسته ها:

- CSMA/CA) این پروتکل برای carrier transmission استفاده شده و با حس کردن مشغول بودن چنل آن broadcast را متوقف کرده تا زمانی که چنل دوباره آزاد باشد. همچنین در هنگام collision detection ارسال را متوقف می کند به طور موقت. برای مثال در یک شبکه دو دستگاه می توانند به طور همزمان ارسال داشته باشند که می تواند باعث بوجود آمدن collision شود. برای حل این مشکل این پروتکل برخی از دستگاه ها را مجبور میکند بخشی از ارسال خود را متوقف کرده تا collision برطرف شود.
- CSMA/CD) مانند بالا برای carrier transmission استفاده شده ولی عملکرد آن قبل از اتفاق افتادن collision است. مثال این پروتکل مانند پروتکل قبلی است اما قبل این رویداد سیستم متوجه شده و عملیات لازم را انجام میدهد.

ب) برای وای فای از CSMA/CA و CSMA/CD استفاده می کنیم.

سوال بیست و چهارم)

الف) و **ب)**

A: 192.168.1.001 / 00-00-00-00-00-00

B: 192.168.1.003 / 11-11-11-11-11-11

Left-LAN: 192.168.0.002 / 22-22-22-22-22-22

Router1: 192.168.2.002 / 33-33-33-33-33-33

C: 192.168.2.001 / 44-44-44-44-44-44

Middle-LAN: 192.168.2.003 / 55-55-55-55-55-55

D: 192.168.2.004 / 66-66-66-66-66-66

E: 192.168.3.001 / 77-77-77-77-77-77

Right-LAN: 192.168.3.002 / 88-88-88-88-88-88

تمرین ششم شبکه های کامپیوتری - دکتر صبایی

F: 192.168.3.003 / 99-99-99-99-99-99