فصل هفتم

معماری TCP/IP

۷-۱- تاریخچه TCP/IP

برای اولین بار درسال ۱۹۶۲ فردی به نام J.C.R. Licklider از دانشگاه MIT آمریکا، ایده ایجاد یک شبکه جهانی از کامپیوتر ها را مطرح نمود و آنرا برای توسعه بیشتر به آژانس پروژه تحقیقاتی پیشرفته دفاعی آمریکا (DARPA[1]) ، منتقل کرد. به دنبال آن، دانشمند دیگری به نام Leonard Kleinrock از دانشگاه MIT آمریکا وبا همکاری با دانشگاه UCLA تئوری سوئیچینگ بسته ای را که پایه و اساس عملکرد شبکه جهانی اینترنت شد، ارائه نمود. درسال ۱۹۶۵ آقای Lawrence Roberts از دانشگاه MIT اقدام به اتصال کامپیوتری در Massachusetts آمریکا به کامپیوتردیگری درایالت کالیفرنیا این کشور و از طریق خطوط تلفنی نمود. درسال ۱۹۶۶ این شخص تجربه عملی فوق را به DARPA منتقل نمود. در سال ۱۹۶۸ DARPA قرارداد همکاری با شرکت BBN برای پیاده‌سازی نرم‌افزار شبکه آرپانت که از قدیمیترین شبکه‌های سوئیچینگ بسته‌ای می‌باشد، منعقد ساخت. بسیاری از مراکز تحقیقاتی و دانشگاه‌ها و پایگاه‌های نظامی از شبکه آرپانت برای پیاده‌سازی و آزمایش پروژه‌های تحقیقاتی خود استفاده کردند.

درسال ۱۹۶۹ با استفاده از شبکه فوق، چهار دانشگاه اصلی آمریکا به نام های دانشگاه UCLA، انیستیتوی تحقیقاتی Stanford، دانشگاه UCSB و دانشگاه Utah به یکدیگر متصل شدند. درسال ۱۹۷۰ مراکز دیگری شامل دانشگاه MIT، دانشگاه Harvard ، شرکت های BBN و SDC به شبکه فوق اضافه شدند. به دنبال آن درسال ۱۹۷۱، آزمایشگاه هایLincoln دانشگاه MIT و دانشگاه های Carnegie-Mellon وCase-Western Reserve به شبکه فوق اتصال یافتند. در سال ۱۹۷۵ کنترل شبکه آرپانت از DARPA گرفته شد و به آژانس ارتباطات دفاعی آمریکا (DCA) منتقل گردید. این آژانس نظامی، از آرپانت به‌عنوان بخشی از شبکه دفاعی ملی (DNN) استفاده کرد.

دردهه ۷۰، معماری TCP/IP توسط فردی به نام Bob Kahn درشرکت BBN ارائه گردید و بعدها توسط Vint Cerf دردانشگاه Stanford و دیگران توسعه یافت. درسال ۱۹۸۰ وزارت دفاع آمریکا معماری فوق را جایگزین پروتکل قدیمی NCP[2] درشبکه خود نمود. این معماری درسال ۱۹۸۳ به صورت جهانی مورد پذیرش قرار گرفت.

در سال ۱۹۸۳، شبکه آرپانت به دو شبکه تجزیه گردید. حاصل تجزیه این شبکه، دو شبکه مستقل دیگر به نام‌های میلنت و آرپانت شد. شبکه آرپانت به‌عنوان یک شبکه تحقیقاتی و آزمایشگاهی باقی ماند و میلنت برای کاربردهای نظامی و انتقال داده‌های محرمانه استفاده گردید. هر دو شبکه از بستر سخت‌افزاری یکسانی برای تبادل اطلاعات استفاده می‌کردند و امکان تبادل اطلاعات بین این دو شبکه وجود داشت. از شبکه آرپانت به‌عنوان یک شبکه پایه و اساسی برای پیاده‌سازی شبکه جهانی اینترنت استفاده شد. شبکه آرپانت دارای ۵۰ مینی‌رایانه مدل C30 و C300 ساخت شرکت BBN بود که از آن به‌عنوان سوئیچ‌های شبکه استفاده می‌شد. شبکه آرپانت دارای وسعت زیادی بود و تقریباً سراسر آمریکا و اروپای غربی را گسترش می داد. در ابتدای راه‌اندازی شبکه آرپانت اغلب ازکانال‌های خطوط اجاره‌ای با سرعت ۵۶ کیلوبیت برثانیه استفاده می‌گردید، ولی امروزه از کانال‌های با سرعت بالاتر برای اتصال نودهای شبکه اینترنت استفاده می‌شود. با گسترش اینترنت، شبکه آرپانت از میان برداشته شد و جای خود را به شبکه گسترده و جهانی اینترنت داد. البته شبکه نظامی میلنت همچنان

[1] Deffence Advance Research Project Agency
[2] Network Control Protocol

به کار خود ادامه می‌دهد. درسال ۱۹۸۶ شبکه NSFNET[1] با استفاده از کانال های ۵۶ کیلوبیت برثانیه درایالت متحده آمریکا توسعه یافت.

در شکل (۷-۱) مدل لایه‌ای و معماری TCP/IP که از آن به‌عنوان معماری شبکه جهانی اینترنت استفاده می‌شود، نشان داده شده است. یکی از قابلیت‌های عمده TCP/IP ، امکان استفاده از آن در اتصال شبکه‌ها به یکدیگر جهت ایجاد یک شبکه وسیعتر می‌باشد. با استفاده از معماری TCP/IP امکان اتصال چندین شبکه محلی و ایجاد یک شبکه وسیعتر فراهم می‌آید. معماری TCP/IP قبل از مدل لایه‌ای مرجع OSI به‌وجود آمد و بنابراین لایه‌های TCP/IP به‌طور کامل با لایه‌های OSI مطابقت ندارند.

همان‌طور که در شکل (۷-۱) نیز مشاهده می‌شود، در معماری TCP/IP از پنج لایه فیزیکی، پیوند داده، شبکه، حمل و لایه کاربرد استفاده می‌شود. می‌توان گفت که لایه کاربرد در TCP/IP معادل سه لایه جلسه، ارائه و کاربرد در مدل OSI می‌باشد. در سطح لایه حمل در مدل TCP/IP از دو پروتکل TCP[2] و UDP[3] و در سطح لایه شبکه از پروتکل اینترنت (IP[4])استفاده می‌شود. یکی از مزایای بسیار عمده معماری TCP/IP که باعث گسترش و محبوبیت آن شده است، این است که در این معماری هیچ استاندارد و پروتکل خاصی برای لایه‌های اول و دوم وضع نشده است. این امر باعث می‌شود که به‌راحتی بتوان از TCP/IP برروی فن‌آوری‌های مختلف لایه فیزیکی استفاده کرد. در سطح لایه کاربرد، از پروتکل‌های کاربردی مانند FTP،SNMP[5]،DNS[6]،TELNET و SMTP[7] استفاده می‌شود.

<table>
<tr><td>لایه کاربرد</td><td colspan="6">Trace Route</td><td>SNMP</td><td colspan="2">SMTP</td><td colspan="2">FTP</td><td colspan="2">telnet & rlogin</td><td>ping</td></tr>
<tr><td></td><td colspan="6">….</td><td>OSPF</td><td colspan="2">RIP</td><td colspan="2">BOOTP</td><td colspan="2">TFTP</td><td>DNS</td></tr>
<tr><td>لایه حمل</td><td colspan="5">ICMP</td><td colspan="4">UDP</td><td colspan="4">TCP</td></tr>
<tr><td>لایه شبکه</td><td colspan="13">IP</td></tr>
<tr><td>لایه پیونددداده</td><td colspan="3">PPP</td><td colspan="2">HDLC</td><td colspan="4">LLC</td><td colspan="3"></td></tr>
<tr><td></td><td>…</td><td>SMDS</td><td>ATM</td><td colspan="3">frame relay</td><td colspan="2">حلقه نشانه</td><td>X.25</td><td>802.3</td><td>اترنت</td></tr>
<tr><td>لایه فیزیکی</td><td>ماهواره</td><td colspan="2">مایکروویو</td><td colspan="3">کابل هم محور</td><td>UTP</td><td colspan="3">فیبرنوری</td></tr>
</table>

شکل (۷-۱): معماری TCP/IP

۷-۲- نیاز به آدرس‌های IP

درشبکه های کامپیوتری، با اتصال چند شبکه به یکدیگر، شبکه اینترنت ایجاد می شود. باید توجه نمودکه شبکه جهانی اینترنت که درآن میلیون ها کامپیوتر از طریق هزاران شبکه مختلف به یکدیگر متصل شده اند، نوع خاصی از شبکه اینترنت است. یکی از کارهای اصلی در ساختن یک شبکه TCP/IP،اختصاص دادن آدرسهای اینترنت به نود های شبکه می باشد.

[1] National Science Foundation Network
[۲] Transmission Control Protocol
[۳] User Datagram Protocol
[٤] Internet Protocol
[٥] Simple Network Management Protocol
[٦] Domain Name System
[۷] Simple Mail Transfer Protocol

آدرسهای اینترنت در شبکه های TCP/IP آدرسهای IP نامیده می شوند. هنگام تخصیص آدرسهایIP، لازم است که چند عامل را در نظر بگیریم. اولین عامل که باید در نظر گرفته شود این است که هر آدرس شبکه IP یکتا باشد. آدرسهای IP دارای یک ساختار معین هستند. نمی توان فقط یک نود را به شبکه IP متصل کرد و به آن یک آدرس IP واحد اختصاص داد بلکه علاوه برآن باید مراقب بود که آدرس IP با آدرسهای IP نود های دیگر آن بخش شبکه سازگار باشد. هنگام پیاده سازی معماری TCP/IP برروی یک شبکه، یکی از کارهایی که باید انجام شود انتخاب و پیکره بندی درست آدرسهای IP است. دو نسخه فعلی از پروتکلIP موجود است که عبارتند از: IP نسخه ۴(IPV4) و IP نسخه ۶ (IPV6). IP نسخه ۴ که هنوز پروتکل مهم اینترنت است از آدرسهای ۳۲ بیتی استفاده می کند. پروتکلIP نسخه۶ که پروتکل نسل بعدی است، برای جایگزینی IP نسخه ۴ طراحی شده است. پروتکلIP نسخه ۶ از آدرسهای ۱۲۸ بیتی استفاده می نماید.

برای اتصال نود ها به اینترنتی که شامل بیش از یک شبکه می باشد، باید از یک مدل آدرس دهی منطقی سازگار در شبکه استفاده شود. آدرسهای منطقی مشخص کننده های یکتایی می باشند. می توان برای تعیین این آدرسها ازمقادیرعددی یا اسمی استفاده نمود. آدرسهای شبکه مشخص کننده های نقطه دسترسی به سرویس[1]در لایه شبکه مدل مرجع هستند. این آدرسها، آدرسهای SAP شبکه(NSAP[2]) نام دارند ومی بایست برای همه پروتکل هایی که در لایه شبکه مدل مرجع ارتباط برقرارمی کنند، یکتا باشند.

در سطح لایه شبکه مدل مرجعTCP/IP، معمولاً از یک مقدار عددی به جای مقدار اسمی برای آدرسهای NSAP استفاده می شود. این انتخاب به خاطر آن است که برای پروتکل های لایه های پایین مدل مرجع، کار با مقادیر عددی به جای اسم های نمادین مفیدتر است. آدرس IP باید ساختاری داشته باشد تا مسیریابی را به طور کارآمد محاسبه کند. محاسبات مسیریابی با اعداد دودویی به جای اسامی نمادین کارآمدتر است و این دلیل دیگری است که چرا مقادیر عددی برای آدرسهای شبکه مناسبتر از اسامی نمادین هستند. به طور کلی لایه های بالاتر مدل مرجعTCP/IP مایل به استفاده ازآدرسهای اسمی می باشند، درحالیکه لایه های پایین تر از آدرسهای عددی استفاده می کنند.

آدرسهای NSAP برای هر اتصال به شبکه فیزیکی مورد نیاز است. اگرN اتصال شبکه از یک میزبان موجود باشد، بایستی N آدرس NSAP به آنها نسبت داد. سخت افزار شبکه مانند یک بورد شبکه برای ایجاد اتصال به شبکه استفاده می شود و آدرسهای سخت افزاری شبکه مقادیر عددی هستند. طراحان اینترنت از یک مدل آدرس دهی منطقی شبکه برای آدرسهای IP استفاده نموده اند که از هر آدرس لایه فیزیکی مستقل می باشد.

معماری TCP/IPروی انواع مختلف سخت افزار شبکه قابل اجرا می باشد. برای مثال اترنت، شبکه حلقوی و FDDI از آدرسهای فیزیکی ۴۸ بیتی استفاده می کنند. بقیه انواع سخت افزار شبکه ممکن است از آدرس های ۸ بیتی، ۱۶ بیتی و یا ۳۲ بیتی استفاده کنند. با استفاده از آدرس های منطقی به جای آدرس های فیزیکی، پروتکل اینترنت مجبور نیست به صفات سخت افزاری شبکه زیرین ربط داده شود. از آنجا که آدرس های IP به آدرس های سخت افزاری وابسته نیستند، می توان سخت افزار زیرین را با سخت افزار جدیدتر بدون نیاز به تغییر آدرس منطقی جایگزین کرد. به بیان دیگر می توان شبکه را با تکنولوژیهای سریع تر و کارآمدتر ارتقاء داد بدون اینکه نیازی به تغییر آدرس های منطقی باشد.

۷-۳- ساختار آدرس های IP

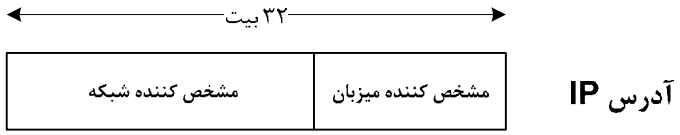
برای مسیریابی بسته های IP، مسیریابها باید قادر به تمایز بین شبکه های منطقی مختلف باشند. طراحان شبکه تصمیم گرفتند تا آدرس IP را طوری ساختار دهی کنند که قادر باشند فرق بین شبکه های منطقی مختلف را تشخیص دهند. با

[1] Service Access Point (SAP)
[2] Network SAP

اندازه ۳۲ بیتی آدرس NSAP ، حداکثر تعداد اتصالاتی که در یک زمان می توان در شبکه داشت 2^{32} است که برابر با ۴,۲۹۴,۹۶۷,۲۹۶ یا در حدود ۴ میلیارد می باشد. بعضی از آدرسهای IP برای اهداف خاصی رزرو شده اند و نمی توانند به اتصالات شخصی شبکه اختصاص داده شوند. شکل(۷-۲) تقسیم آدرس IP را نشان می دهد.

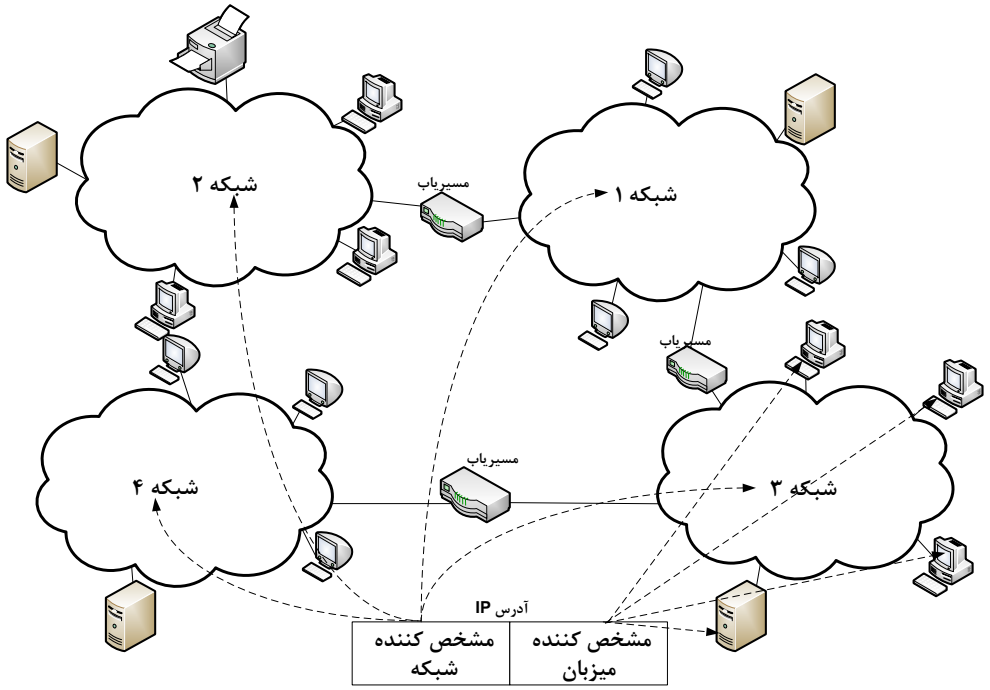
همانطور که درشکل (۷-۲) دیده می شود، آدرس IP دارای طول کلی چهار بایت می‌باشد که از دو قسمت عمده تشکیل شده است و عبارتند از:

- بخش مشخص‌کننده شبکه (netid[1])
- بخش مشخص‌کننده میزبان (hostid[2])



شکل (۷-۲): استفاده از آدرس IP برای شناسایی شبکه و میزبان

آدرس IP را بطور منطقی می توان به وسیله زوج (مشخص کننده میزبان، مشخص کننده شبکه) توصیف کرد. قسمت مشخص کننده شبکه، آدرس شبکه متصل را توصیف کرده و مشخص کننده میزبان کاربر را درون شبکه نشان می دهد. شکل(۷-۳) نشان دهنده این است که چگونه می توان از مشخص کننده های شبکه یکتا برای تشخیص شبکه های متصل استفاده کرد.



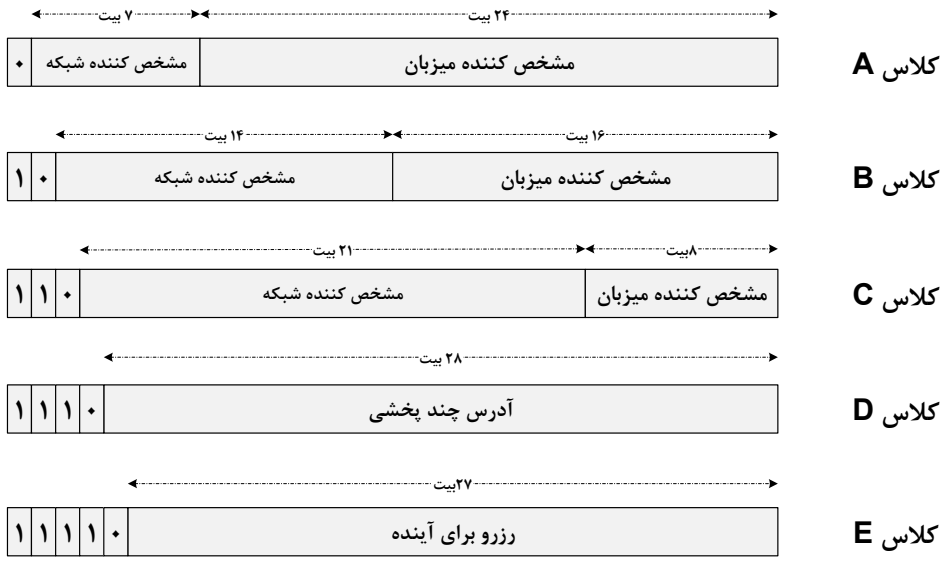
شکل(۷-۳): مثالی از شبکه نشان دهنده مقادیر مشخص کننده شبکه برای تشخیص شبکه

[1] Network identifier
[2] Host identifier

تقسیم آدرس IP به یک مشخص کننده شبکه و یک مشخص کننده میزبان، یک مدل آدرس دهی "سلسله مراتبی" است. آدرس دهی سلسله مراتبی برای مسیریابی کارآمدتر طراحی شده است. نگرانی اصلی مسیریابها رساندن بسته IP به شبکه مقصد است. برای این منظور مسیریابها باید اطلاعاتی درباره مشخص کننده های شبکه و نه مشخص کننده های میزبان ذخیره کنند. مشخص کننده های شبکه از مشخص کننده های میزبان کوتاهتر بوده وباعث می شود مقدار اطلاعاتی که مسیریابها باید بدانند مدیریت پذیرتر باشند. اگر تفاوتی بین شماره شبکه و شماره میزبان وجود نداشت و یک مدل آدرس دهی متوالی بجای یک مدل آدرس دهی سلسله مراتبی استفاده می شد، مسیریابها می بایست توانایی ذخیره همه ۴ میلیارد آدرس های IP را داشته باشند.

همه میزبانهای متصل به یک شبکه دارای یک مشخص کننده شبکه یکسان بوده و مشخص کننده میزبان آنها متفاوت است. برای اینکه مسیریابی به طور صحیح انجام شود، شبکه های متصل باید مشخص کننده شبکه یکتا داشته باشند. شبکه هایی که مشخص کننده شبکه یکسان دارند، دارای یک پیشوند عمومی می باشند که آدرس های IP میزبان های درون شبکه را نشان می دهد.

با تقسیم مشخص کننده شبکه و مشخص کننده میزبان، ۳ کلاس آدرس اولیه ایجاد گردید. در کنار ۳ کلاس A و B و C دو کلاس آدرس دیگر D و E نیز تعریف شده اندکه درشکل (۷-۴) نشان داده شده است. کلاسD برای عملیات چندپخشی رزرو شده است. این کلاس از آدرسهای IP، توسط پروتکلهای مخصوصی برای انتقال پیامها به یک گروه انتخابی از نودها استفاده می شود. کلاس E برای استفاده های آینده رزرو شده است. جدول(۷-۱) تعداد شبکه هاوتعداد میزبانهایی که درهر کلاس آدرس IP قابل دسترسی هستند را نشان می دهد.



شکل (۷-۴): کلاسهای تعریف شده آدرس IP

کلاس A برای شبکه های خیلی بزرگ مناسب است اما چون فیلد مشخص کننده شبکه آن فقط ۷ بیت است، تنها ۱۲۷ تا از چنین شبکه هایی قابل ایجاد می باشد. آرپانت اصلی مثالی از یک شبکه کلاس A است. شبکه های کلاس B شبکه هایی با اندازه متوسط هستند که برای سازمانهای متوسط وبزرگ مناسبند. شبکه های کلاس C برای سازمان های کوچک مناسبند. درشبکه های کلاس C، هر شبکه نمی تواند بیشتر از ۲۵۴ میزبان داشته باشد.

جدول (۷-۱): تعداد شبکه ها و میزبان ها در هر کلاس آدرس

نوع کلاس	محدوده تغییرات مشخص کننده شبکه	تعداد شبکه	تعداد میزبان
کلاس A	۰ تا ۱۲۷	۱۲۷	۱۶۷۷۷۲۱۴
کلاس B	۱۲۸ تا ۱۹۱	۱۶۳۸۳	۶۵۵۳۴
کلاس C	۱۹۲ تا ۲۲۳	۲۰۹۷۱۵۱	۲۵۴
کلاس D	۲۲۴ تا ۲۳۹	-	-
کلاس E	۲۴۰ تا ۲۴۷	-	-

برای راحتی بیشتر، آدرس های IP ۳۲ بیتی با ۴ عدد دهدهی نمایش داده می شوند. اعداد دهدهی بوسیله نقطه از هم جدا می شوند. این نوع نمایش آدرس، نشانه گذاری دهدهی نقطه دار نامیده می شود. در زیر یک آدرس IP در شکل دودویی و نشانه گذاری دهدهی نقطه دار آن نشان داده شده است.

آدرس IP = ۱۰۰۱۰۰۰۰ ۰۰۰۱۰۰۱۱ ۰۱۰۰۱۰۱۰ ۱۱۰۰۱۰۰۱

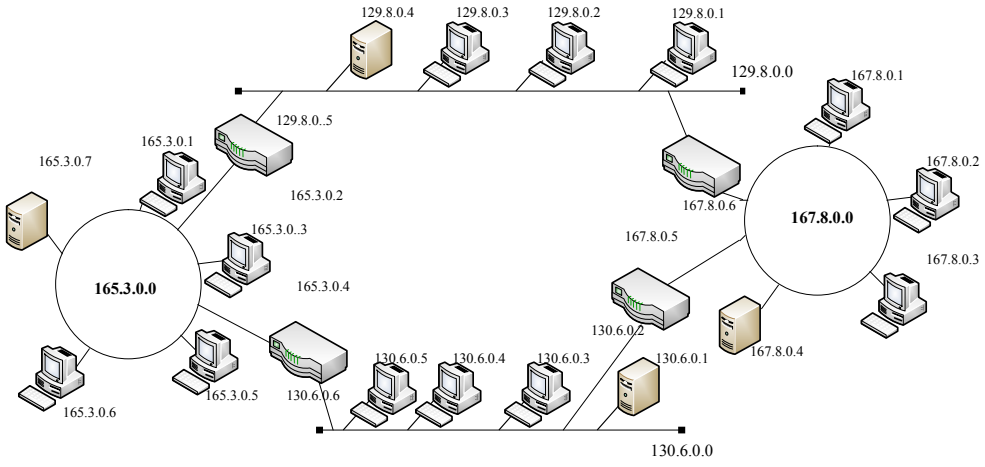
آدرس IP = 144.19.74.201

جدول(۷-۲)، بازه مقادیر اولین عدد دهدهی یک آدرس IP را در نشانه گذاری دهدهی نقطه دار نشان می دهد. با استفاده از این جدول کلاس آدرس IP را به آسانی با بررسی اولین عدد دهدهی آدرس IP می توان مشخص کرد.

جدول(۷-۲): تشخیص کلاس آدرس IP از اولین عدد دهدهی

کلاس آدرس	حداقل مقدار اولین بایت آدرس	حداکثر مقدار اولین بایت آدرس
A	۰	۱۲۶
B	۱۲۷	۱۹۱
C	۱۹۲	۲۲۳
D	۲۲۴	۲۳۹
E	۲۴۰	۲۴۷

درشکل (۷-۵) مثالی از تخصیص آدرس های IP دریک شبکه اینترنت نشان داده شده است.



شکل (۷-۵) : مثالی از آدرس‌های IP در یک شبکه اینترنت

۷-۴- آدرسهای IP خاص

برخی از آدرسهای IP دارای مفهوم خاصی بوده و برای کاربردهای خاصی رزرو شده اند. این آدرسهای خاص به شرح زیر می باشند:

۷-۴-۱- آدرس 0.0.0.0

دراین آدرس، فیلدشماره شبکه صفر است که به معنی "این شبکه" می باشد . فیلد شماره میزبان نیز صفر است، که به معنی"این نود" در شبکه است . این آدرس معمولا زمانی استفاده می شودکه یک نود شبکه سعی می کند تا آدرس IP خود را مشخص کند. به عنوان مثال، نود های شبکه برای انتساب یک آدرس IP از یک سرویس دهنده مرکزی BOOTP استفاده می کنند. هنگامی که نود IP یک تقاضای ابتدایی را به سرویس دهنده BOOTP می فرستد، نود IP فرستنده که فاقد آدرس IP است ازمقدار 0.0.0.0 در فیلد آدرس IP مبدا استفاده می کند تا نشان دهد که "این نود" (شماره میزبان صفر) در "این شبکه" (شماره شبکه صفر) است. هنگامی که نود، آدرسIP خود را از پاسخ BOOTP بدست آورد دیگرازآدرس 0.0.0.0 استفاده نمی کند. آدرس 0.0.0.0 در جداول مسیریابی نیز استفاده می شود تا ورودیهای شبکه را برای آدرسIP مسیریاب پیش فرض نشان دهد. باید توجه نمود که آدرس IP 0.0.0.0 را فقط می توان به عنوان آدرس IP مبدا استفاده کرد و هرگز به عنوان آدرسIP مقصد استفاده نمی شود.

۷-۴-۲- آدرس 0.hostid

این آدرس به معنی شماره میزبان در "این شبکه" است. اگر یک نود در شبکه ای بسته ای را دریافت کند که شماره شبکه در آدرس IP مقصد صفر باشداما شماره میزبان موجود درآدرس مقصد با آن نود مطابقت داشته باشد، نود بسته را خواهد پذیرفت. گیرنده مقدار صفر را در شماره شبکه به معنی این شبکه تفسیر می کند.

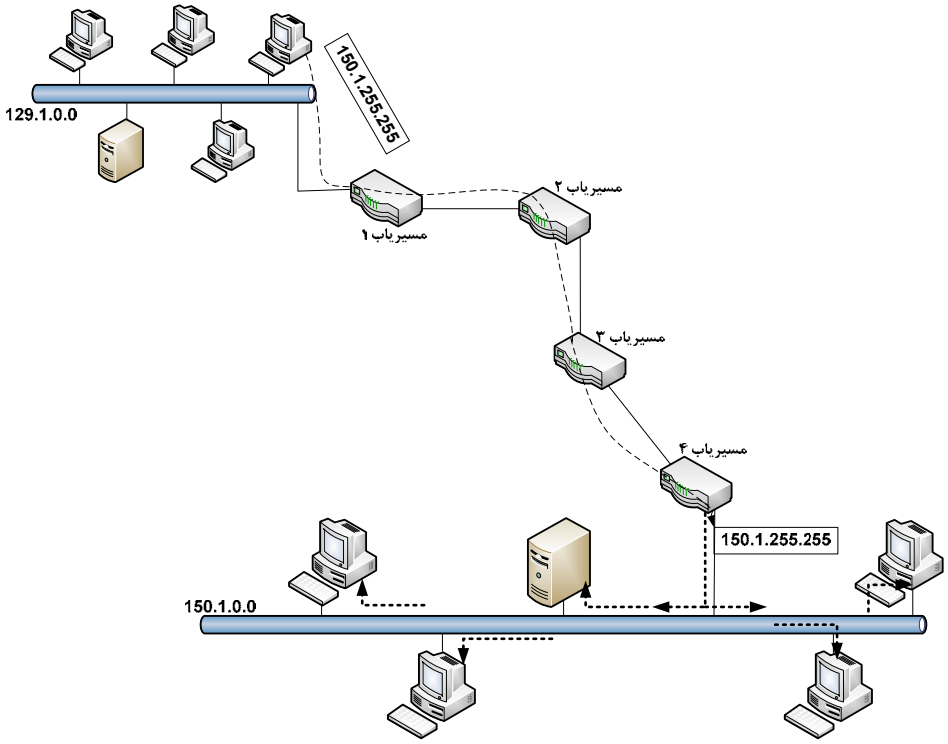
۷-۴-۳-آدرس netid.255

این آدرس همه پخشی مستقیم[1]بوده و به معنی ارسال بسته به همه نود ها در یک شبکه خاص است. این آدرس می تواند بعنوان آدرس IP مقصد یک بسته IP استفاده شده و هرگز نمی تواند به عنوان آدرس مبدأ باشد. یک آدرس همه پخشی مستقیم توسط همه نود های شبکه دیده می شود. بنابراین به عنوان مثال برای شماره شبکه 137.53، آدرس همه پخشی 137.53.255.255 خواهد بود.

پیام های همه پخشی مستقیم به یک شبکه خاص فرستاده می شوند که شماره آن شبکه در فیلد شماره شبکه آدرسIP مقصد مشخص می شود. مسیریابهای شبکه، قادر به پیش بردن بسته های همه پخشی مستقیم می باشند و بسته IP را به مسیریاب نهایی که به شبکه مقصد متصل است، می فرستند. مسیریاب شبکه مقصد مجبور خواهد بود که بسته IP را به همه نود های شبکه بفرستد. همانطور که درشکل (۷-۶) دیده می شود، آدرس های همه پخشی مستقیم از مسیریاب های میانی شبکه عبور کرده و در شبکه مقصد به همه میزبان ها به صورت همه پخشی ارسال می شوند. دراین مثال، ایستگاهی درشبکه بالا به آدرس شبکه 129.1.0.0 بسته همه پخشی مستقیم به آدرس 150.1.255.255 ارسال می دارد. این بسته از تمام مسیریاب های میانی عبور کرده تا به مسیریاب متصل به شبکه مقصد برسد(مسیریاب ۴). این مسیریاب متوجه می

[1] Directed broadcast

شود که آدرس مقصد به صورت همه پخشی مستقیم است. بنابراین با استفاده از قابلیت همه پخشی لایه ۲، بسته دریافتی را به همه میزبان های شبکه ارسال می دارد.



شکل (۷-۶): مثالی از یک همه پخشی مستقیم

البته می توان با پیکره بندی مناسب مسیریاب های شبکه، از پیش بردن بسته های همه پخشی مستقیم توسط مسیریاب های شبکه جلوگیری نمود.

۷-۴-۴- آدرس 255.255.255.255

این آدرس خاص، نشان دهنده یک آدرس همه پخشی محدود است که از جانب مبدا به همه نود های آن شبکه ارسال می شود. همه پخشی محدود در شبکه های محلی قابل استفاده است و هرگز از مرز یک مسیریاب عبور نمی کند. در یک همه پخشی مستقیم، فرستنده باید مقدار شماره شبکه را دربخش خاص آدرس مقصد قراردهد. اگر همه پخشی در یک شبکه محلی مورد نظرباشد، می توان از همه پخشی محدود استفاده کرد که نیازی به داشتن شماره شبکه ندارد. یک آدرس همه پخشی محدود هرگز به عنوان یک آدرس IP مبدا استفاده نمی شود، بلکه فقط می تواند به عنوان یک آدرس IP مقصد استفاده گردد.

۷-۴-۵- آدرس netid.0

این آدرس که همه بیتهای مشخص کننده میزبان در آن صفر است، هرگز به یک میزبان خاص انتساب داده نمی شود و نشان دهنده خود شبکه است. به عنوان مثال، آدرس IP 137.53.0.0 را در نظر بگیرید. این یک آدرس شبکه کلاس B است که به شبکه کلاس B 137.53 اشاره می کند.

۷-۴-۶- آدرس 127.x.x.x

با بررسی جدول (۷-۲)، می توان متوجه شدکه عدد ۱۲۷ که باید دربازه مقادیر کلاسA باشد، درمجموعه آدرس های کلاس A استفاده نمی شود. این عدد برای قابلیت برگشت حلقه رزرو شده است. آدرس برگشت حلقه یک آدرس مخصوص است. درخیلی از کاربردهای شبکه، تمایل به بررسی و تست نرم افزار وسیستم عامل شبکه می باشد. نتایج موجود در هر بسته ای که توسط یک برنامه کاربردی به آدرس 127.X.X.X ارسال شود، بدون دستیابی به واسطه شبکه به برنامه کاربردی برمی گردد. بسته از بافر انتقال به بافر دریافت در همان کامپیوتر کپی می شود. به این دلیل است که آدرس 127.X.X.X آدرس برگشت حلقه نامیده می گردد. آدرس برگشت حلقه نرم افزاری را می توان برای تشخیص پیکره بندی صحیح TCP/IP استفاده کرد . برای مثال می توان از این خاصیت همراه با ابزار Ping استفاده نمود تا از کار کردن نرم افزار لایه IP اطمینان حاصل کرد . ابزارPing یک بسته ICMP را به یک آدرسIP مقصد می فرستد و لایه IP در آن آدرس به آن پاسخ می دهد. درفصل بعد، با عملکرد پروتکل ICMP آشنا خواهیم شد.

۷-۴-۷- آدرس های تک پخشی ، همه پخشی و چند پخشی

هنگامیکه یک بسته IP به یک آدرس IP انفرادی فرستاده می شود، یک بسته IP تک پخش نامیده می شود و فرآیند ارسال بسته، تک پخشی نام دارد. ازتک پخشی برای برقراری ارتباط بین دو نود IP استفاده می شود. هنگامیکه یک بسته IP به همه نود های یک شبکه خاص فرستاده می شود، همه پخشی نام دارد. در چند پخشی یک آدرس کلاس D به عنوان آدرس مقصد استفاده می گردد. بسته IP به گروهی ازنودها تحویل داده می شود که توسط یک آدرس کلاس D مشخص می شوند. سیستم هایی که آدرس چندپخشی یکسان دارند به یک گروه چندپخشی متعلق هستند. به اعضای یک گروه چندپخشی همانطور که یک آدرس کلاس D انتساب داده می شود، می بایست یک آدرس IP از گروه آدرس کلاس C,B,A نیز انتساب گردد. گروه چندپخشی به دو طریق می تواند یک بسته IP را دریافت کند:

- بسته های IP مستقیما به آدرس IP خصوصیشان فرستاده شود (کلاس C,B,A)
- بسته های IP به آدرس چندپخشی آنها ارسال شود (کلاس D)

آدرسهای کلاس D با عددی دربازه ۲۲۴ تا ۲۳۹ شروع می شوند. برای انجام چندپخشی، یک میزبان باید توانایی پیوستن به یک گروه چندپخشی یا بیرون رفتن از گروه چند پخشی را داشته باشد. این توانایی معمولا با یک خط دستور و سیستم عامل خاص پیاده سازی می شود. نرم افزار لایه IP باید توانایی شناسایی آدرسهای چند پخشی بسته های IP ورودی و خروجی را داشته باشد. پیاده سازیهای قدیمی IP ، قادر به شناسایی آدرسهای چندپخشی نبودند. هر میزبان در شبکه IP توانایی پیوستن به یک گروه چندپخشی را دارد. لازم نیست میزبانها در یک شبکه محلی منفرد باشند بلکه این امکان وجود دارد که هر میزبان دریک شبکه مختلف و دور از یکدیگر وجود داشته باشند. این شبکه ها بوسیله مسیریابها از هم جدا می شوند. در نتیجه مسیریابها باید بدانند که چگونه بسته های چند پخشی را در شبکه پیش ببرند. برای انجام اینکار بطور کارآمدتر مسیریابها باید بدانند که آیا میزبانهای موجود در یک شبکه متصل محلی بخشی از یک گروه چند پخشی هستند یا خیر؟ بدین منظور مسیریابها اطلاعاتی را بین یکدیگر مبادله می کنند و کشف می کنند که آیا اعضای گروه در شبکه های دور وجود دارندیا خیر؟ میزبانهایی که به یک گروه چندپخشی می پیوندند یا آن را ترک می کنند از پروتکل مدیریت گروه اینترنت[1](IGMP) برای گزارش عضویتشان در گروه به مسیریابهای همسایه استفاده می کنند. مسیریابهای همسایه این

[1] Internet Group Management Protocol(IGMP)

گزارش را دریافت نموده و جداول داخلی خود را درباره میزبانهایی که اعضای یک گروه چند پخشی هستند را به روز می رسانند. مسیریابها توانایی سرشماری میزبانها را بوسیله پرس وجو درباره عضویت جاریشان در فواصل معین نیزدارند. این سرشماریها با استفاده از آدرس چندپخشی مخصوص 224.0.0.1 به همه سیستمها در این زیر شبکه فرستاده می شود. هنگامی که یک چند پخشی به یک شبکه محلی فرستاده می شود، ازتوانایی سخت افزاری چند پخشی شبکه های محلی استفاده می شود.

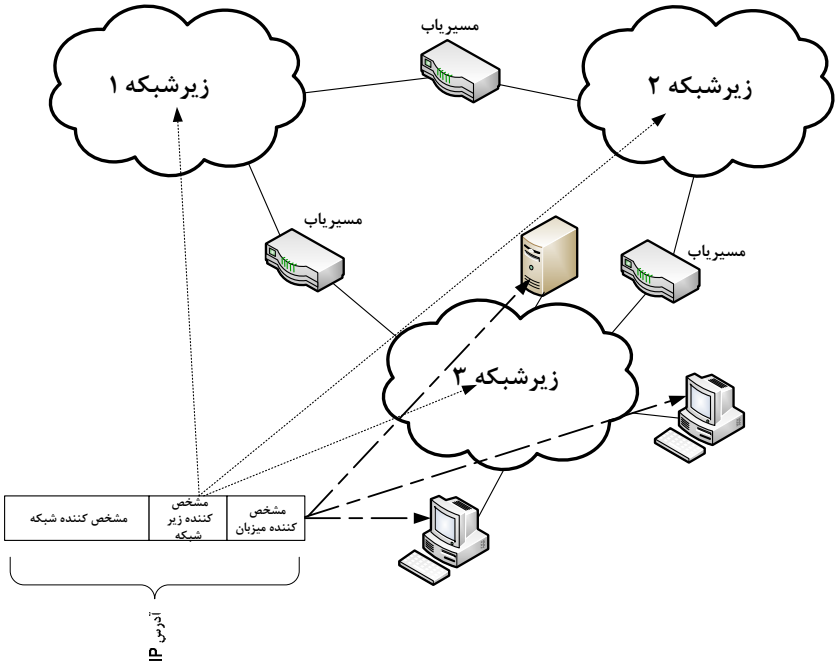
۷-۵- زیر شبکه سازی

آدرس هایIPV4 برای تخصیص به شبکه های مختلف با ابعاد متفاوت طراحی شده اند. این قالب های آدرس در مراحل آغازین اینترنت به خوبی کار می کردند، اما با رشد و گسترش اینترنت و افزایش تعداد میزبان های شبکه، به تدریج ضعف قالب های آدرس IP نمایان گردید. این ضعف، عدم استفاده بهینه از فضای آدرس های IP و وجود اتلاف درآنها بود. برای حل مشکل اتلاف فضای آدرس IP، مفهوم زیر شبکه سازی درسال ۱۹۸۵ مطرح گردید.

زیر شبکه ها با استفاده از یک شماره شبکه، امکان اتصال چندین شبکه را به یکدیگرممکن می سازند. همانطور که قبلا ذکر شد، آدرس شبکه برای همه میزبان های داخل یک شبکه یکسان است. معمولا طراحان شبکه، یک آدرس شبکه یکتا را به یک شبکه داده شده انتساب می دهند و سپس به میزبانها، مقادیر قسمت میزبان آدرس IP انتساب داده می شود. این تنظیم منتج به این امر می شود که همه میزبانهای داخل یک شبکه یک پیشوند آدرس شبکه یکسان داشته باشند. تعداد بیتهای استفاده شده در پیشوند آدرس شبکه به قالب آدرس IP بستگی دارد. برای قالب آدرس کلاس A، ۸ بیت برای آدرس شبکه و ۲۴بیت برای آدرس میزبان استفاده می شود. برای آدرس کلاس B ، ۱۶ بیت برای آدرس شبکه و ۱۶ بیت برای آدرس میزبان استفاده می شود. برای قالب آدرس کلاس C،۲۴ بیت برای آدرس شبکه و ۸ بیت برای آدرس میزبان استفاده می گردد. مزیت استفاده از مدل دو بخشی آدرس شبکه و آدرس میزبان برای آدرس های IP ، کمینه کردن تعداد ورودی ها در جدول مسیر یابی است. به جای اینکه برای هر میزبان در یک شبکه یک رکورد درجدول مسیریابی داشته باشیم، میتوان با استفاده از یک رکورد مجرد جدول مسیریابی همه میزبان های در یک شبکه را خلاصه کرد. این رکوردجدول مسیریابی فقط شامل قسمت آدرس شبکه است که پیشوند مشترک برای همه میزبان های شبکه می باشد. مسیریابها، پیشوند مشترک شبکه های مقصد را در جدول مسیریابی خود با پیشوند آدرسIP مقصد موجود دربسته انطباق می دهند. یک انطباق منجر به انتخاب مسیر خاص برای مسیریابی بسته می شود. هنگامی که یک مسیر یاب یک بسته را به یک شبکه می فرستد ، مسیر یاب تنها قسمت شبکه آدرس IP مقصد بسته را بررسی میکند و قسمت میزبان آدرس IP مقصد را بررسی نمی نماید.

به عنوان مثال یک شبکه IP را با شماره شبکه 149.108.0.0 در نظر بگیرید که ۱۶ بیت قابل انتساب دارد. این ۱۶ بیت کلا $۲^{۱۶}$ ترکیب شماره میزبان را که برابر با ۶۵۵۳۶ است ممکن می سازد. از ۶۵۵۳۶ ترکیب نمی توان الگوی متشکل از بیتهای ۱(همه بیتها ۱) را استفاده کرد. چون این الگو برای آدرس همه پخشی رزرو شده است. همچنین نمیتوان الگوی متشکل از بیت های صفر (همه بیتها صفر) را برای انتساب شماره میزبان استفاده کرد، زیرا این الگو برای خود شبکه رزرو شده است. بنابراین از کل۶۵۵۳۶ شماره میزبان ممکن، تنها از دو شماره میزبان نمی توان استفاده کرد. بنابراین درکل۶۵۳۵۴ میزبان باقی می ماند.

استفاده ازقابلیت زیر شبکه سازی، شبکه را قادر می سازد تا بدون اینکه بقیه شبکه متصل شده از تغییرات در شبکه داخلی مطلع شوند، به طور داخلی ساختاردهی گردند. شکل(۷-۷) ارتباط بین فیلدهای یک آدرس IP و زیر شبکه را نشان می دهد.



شکل(۷-۷): زیر شبکه و شماره های زیر شبکه

مسیریاب های موجود بین زیرشبکه ها، باید از تعداد بیت تخصیص داده شده به زیر شبکه سازی، مطلع باشند.
مزایای زیر شبکه سازی شامل موارد زیر است:

- کاهش ترافیک شبکه
- افزایش کارآیی شبکه
- ساده سازی مدیریت
- ساختار دهی مجدد یک شبکه داخلی بدون اثر گذاشتن شبکه های خارجی
- بهبود بخشیدن امنیت

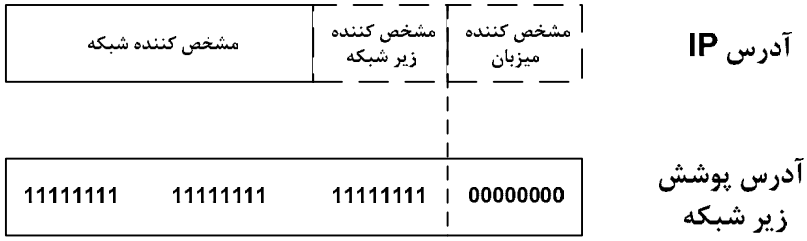
۷-۵-۱- پوشش زیر شبکه[1]

پوشش زیر شبکه بوسیله مسیریابها و میزبانهای زیر شبکه به منظورتشخیص و جداسازی فضای کامپیوتر میزبان از فضای زیر شبکه استفاده می شود. پوشش زیر شبکه فیلد مشخص کننده میزبان را به شماره زیر شبکه و شماره میزبان تقسیم می کند. پوشش زیر شبکه یک عدد ۳۲ بیتی است که مقدار آن با استفاده از قوانین زیر شکل می گیرد:

- ۱ها در پوشش زیر شبکه متعلق به قسمت مشخص کننده شبکه و شماره زیر شبکه در آدرس IP است.
- صفر ها در پوشش زیر شبکه متعلق به قسمت شماره میزبان در آدرس IP است.

شکل(۷-۸) مثالی از نحوه کاربرد این قوانین را نشان می دهد. این شکل یک شماره شبکه کلاس B را نشان می دهدکه برابر 255.255.255.0 می باشد.

[1] Subnet mask



شکل (۷-۸): نمایش پوشش زیر شبکه

از آنجاییکه درقالب بسته های IP کلاس B فضای مشخص کننده میزبان برابر با ۱۶ بیت می باشد، بنابراین درحالت عادی و بدون استفاده از زیر شبکه سازی، مقدار آدرس پوشش برای کلاس B برابر با 255.255.0.0 است. اگر مقدار پوشش زیر شبکه 255.255.255.0 برای یک شبکه کلاس B استفاده شود، این مقدار نشان میدهد که از زیر شبکه سازی استفاده شده است. با توجه به تعداد۱های موجود درآدرس پوشش زیرشبکه فوق، می توان دریافت که فضای مشخص کننده میزبان درآدرس کلاس B فوق برابر با ۸ بیت می باشد.

۷-۵-۲- انتساب کارآمد شماره های زیر شبکه

در زیر شبکه سازی، قسمت میزبان آدرس IP به دو فیلد تقسیم می شود که عبارتند از شماره زیر شبکه و شماره میزبان. با این تقسیم بندی، آدرسIP دارای سلسله مراتب سه سطحی می شود. این عمل منجر به صرفه جویی در مسیریابی و استفاده مجدد از یک پیشوند شماره شبکه مشترک برای زیر شبکه ها می شود.

۷-۶- آدرسهای شبکه های خصوصی (اینترانت ها)

درسال ۱۹۹۴، برای کاهش نیاز به آدرس های IP جدید، RFC1597 راجع به اختصاص آدرس به شبکه های خصوصی ارائه شد. نویسندگان این RFC، مدلی را برای انتساب آدرس های IP در شبکه های خصوصی پیشنهاد کردند. شبکه های خصوصی اتصال محدودی به اینترنت دارند. میزبان های موجود دراین شبکه ها را می توان به گروه های زیر کلاس بندی کرد:

- میزبانهایی که نیاز به دستیابی به میزبانهایی درسازمانهای تجاری دیگر یا اینترنت ندارند.
- میزبانهایی که نیاز به دستیابی به سرویسهای خارجی محدودی مانند FTP،e-mail , remote login Netnews و غیره دارند که می توان با استفاده از دروازه لایه کاربرد این دستیابی رافراهم نمود.
- میزبانهایی که نیاز به دستیابی درسطح لایه شبکه به شبکه خارج از سازمان تجاری دارند. این نیازمندی ازطریق اختصاص اتصال های IP با آدرس های معتبر، رفع می شود.

برای تخصیص آدرس به میزبان های نوع اول، می توان از آدرس های IP غیر معتبر استفاده نمود. این آدرسها فقط درهمان شبکه خصوصی اعتبار داشته و ازدنیای خارج قابل دسترسی نمی باشند. چون با این میزبان ها هیچ مبادله بسته خارج از شبکه خصوصی رخ نمی دهد، مشکل آدرس IP تکراری هرگز دیده نخواهد شد. میزبان های دسته دوم که به وسیله دروازه سطح کاربرد از اینترنت خارجی ایزوله شده اند، نیازی به آدرس های IP یکتا در اینترنت ندارند. به این دلیل که دروازه سطح کاربرد، آدرس های IP این میزبانها را از شبکه خارجی مخفی می سازند. بنا به دلایل امنیتی، خیلی از سازمانهای

تجاری برای اتصال به شبکه داخلی خود به اینترنت از دروازه های لایه کاربرد (مانند دیواره آتش[1]) استفاده می کنند. شبکه داخلی معمولا بطور مستقیم به اینترنت دسترسی ندارند و فقط یک یا چند میزبان دیوار آتش از اینترنت قابل رویت هستند. در این حالت، شبکه داخلی می تواند از شماره های IP غیر یکتا استفاده کند.

توسط نهاد IANA[2] آدرس های IP تخصیص داده می شود. نهاد IANA توسط ICANN[3]اداره می شود.ICANN یک شرکت غیرانتفاعی کالیفرنیای آمریکا می باشد که درسال ۱۹۹۸ تاسیس گردید و وظیفه عمده آن مدیریت تخصیص نام ها و آدرس های IP می باشد.

IANA سه بلوک از فضای آدرس IP را برای شبکه های خصوصی رزرو کرده است تا به میزبان های گروه یک و دو انتساب داده شود. این سه بلوک آدرس عبارتند از:

- ۱ شبکه کلاس A از آدرس 10.255.255.255 تا 10.0.0.0
- ۱۶ شبکه کلاسB از آدرس172.31.255.255 تا 172.16.0.0
- ۲۵۶ شبکه کلاس C از آدرس 192.168.255.255 تا 192.168.0.0

چنانچه یک سازمان تجاری تصمیم بگیرد تا از آدرس های IP خارج از فضای آدرس فهرست شده فوق استفاده کند، این کار را می تواند بدون هیچ هماهنگی با IANA انجام دهد. این فضای آدرس می تواند توسط خیلی از سازمانهای تجاری استفاده شود و نیاز به انتساب شماره شبکه های جدید نمی باشد. آدرسهای فوق در فضای آدرس خصوصی سازمان تجاری، یکتا هستند اما در شبکه یکتا نمی باشند. اگر یک سازمان تجاری برای کاربردها ووسایل متصل به شبکه خود نیاز به فضای آدرس یکتای سرتاسری داشته باشند، چنین آدرسهایی را از سرویس دهنده اینترنت بدست خواهند آورد. از آنجاییکه آدرس های خصوصی معنی سرتاسری ندارند، اطلاعات مسیریابی درباره شبکه های خصوصی نباید خارج از سازمان تجاری منتشر شوند.

۷-۶-۱- سیستم ترجمه آدرس های شبکه (NAT[4])

سیستم NAT آدرس های IP شبکه محلی را به آدرسهای یکتا برای استفاده بر روی اینترنت تبدیل می کند. هرچنداین روش برای ایجاد آدرس های بیشتر برای استفاده در شبکه داخلی ابداع شده است، ولی می توان از آن برای مخفی کردن اطلاعات مربوط به سیستمهای داخلی نیز استفاده کرد. NAT می تواند تمام اطلاعات مربوط به پروتکلهایTCP/IP شبکه داخلی را مخفی کرده طوری که از دید کاربران خارجی چنین به نظر برسد که تمام ترافیک از یک آدرس خاص منتشر می شود. سیستم NAT همچنین این امکان را فراهم می کند که هر محدوده آدرسی را بتوان برای سیستمهای داخلی استفاده کرد، بدون اینکه کوچکترین مشکلی برای شبکه پیش بیاید.

عملکرد NAT به این صورت است که یک دستگاه (مثل کامپیوتر یا مسیریاب) به عنوان دروازه ورود به اینترنت عمل می کند و با این کار آدرس های ایستگاه های کاری را به آدرس دستگاهی که NAT روی آن فعال است ترجمه می کند. به بیان دیگر NAT روی دستگاهی که به اینترنت وصل شده فعال می شود و ایستگاه های کاری و به طور کلی شبکه داخلی را ازدید اینترنت پنهان می دارد. از سوی دیگر اینترنت، کل شبکه را به صورت یک دستگاه ساده می بیند که به اینترنت متصل می باشد.

---

[1] Firewall
[2] Internet Assigned Numbers Authority
[3] Internet Corporation for Assigned Names and Numbers
[4] Network Address Translation

NAT روی شبکه تغییری ایجاد نمی کند و نیازی به تنظیمات دوباره روی ایستگاه های کاری نیست. فقط ایستگاه های کاری می بایست آدرس دروازه خروجی از شبکه را که همان آدرس دستگاهی است که NAT روی آن فعال شده را بدانند.

چهار عملکرد اصلی NAT به ترتیب میزان استفاده در زیر آمده است:

- ترجمه ایستا : حالتی است که یک سیستم خاص(مثلا یک سرویس دهنده) همیشه دارای ترجمه آدرس ثابتی است که امکان برقراری ارتباط از طرف سیستمهای خارجی با آن را فراهم می کند.
- ترجمه پویا (اتوماتیک): حالتی است که یک عده از سیستمهای داخلی از یک یا چند آدرس برای ارتباط با شبکه خارجی استفاده می کنند. این روش برای مخفی کردن مشخصات سیستمهای داخلی یا گسترش محدوده آدرسهای مورد استفاده در شبکه داخلی استفاده می شود.
- توزیع بار : در این حالت یک آدرس ثابت به یک سری آدرس دیگر ترجمه می شود که همه سرویس دهنده هایی هستند که به یک درخواست خاص پاسخ می دهند. این روش برای توزیع بار یک سرویس دهنده پرترافیک برروی یک سری سرویس دهنده استفاده می شود.
- افزونگی : در حالتی که یک شبکه از چند روش برای اتصال به اینترنت استفاده می کند، از این روش استفاده می شود تا در صورت قطع شدن هرکدام از مسیرها از مسیر دیگر استفاده شود.

NAT دارای برخی مشکلات نیز می باشد. بعضی پروتکلها از طریق NAT قابل استفاده نمی باشند، از جمله این پروتکل ها عبارتند از:

- پروتکلهایی که نیاز به برقراری ارتباط مجدد با سرویسگیر دارند : هیچ مسیر مشخصی به سمت سرویسگیر وجود ندارد پروتکلهای H.323 ، RSH و IRC از این دسته اند.
- پروتکلهایی که آدرسهای TCP/IP را داخل اطلاعات بسته قرار می دهند.
- پروتکلهایی که اطلاعات سرآیند TCP/IP را رمز می کنند. پروتکلPPTP از این دسته پروتکل هاست.
- پروتکلهایی که از آدرس فرستنده برای چک کردن مسائل امنیتی استفاده می کنند.
- علاوه بر موارد فوق، پروتکل ICMP نیز با NAT مشکل دارد. نرم افزار ICMP بعضی وقتها قسمت اول بسته اصلی را که شامل آدرسهای ترجمه نشده می باشد، داخل پیام ICMP قرار می دهد. البته از لحاظ امنیتی هیچ لزومی ندارد که بسته های ICMP بتوانند از دیواره آتش عبور کنند.

استفاده از NAT یک سری مشکلات امنیتی نیز دارد که به مواردی از آنها در اینجا اشاره می شود:

- ترجمه ایستا = عدم امنیت: استفاده از ترجمه ایستا سیستمهای داخلی را محافظت نمی کند. استفاده از ترجمه ایستا، فقط آدرس و شماره درگاه سرویسگیر را بصورت یک به یک عوض می کند و هیچ مکانیزم امنیتی روی ارتباط ایجاد شده برقرار نمی کند. برای محافظت از یک سرویس داخل شبکه باید از پراکسی استفاده کرد.

- یک ارتباط همیشه دوطرفه است: وقتی یک سرویسگیر با یک سرویس دهنده ارتباط برقرار می کند، یک ارتباط از سرویس دهنده به سمت سرویسگیر نیز ایجاد می شود. برقراری ارتباط با بعضی سرویس دهندهها، مثلاً یک وب سایت ، ممکن است منجر به بروز مشکلات امنیتی در شبکه شود. ازآنجا که روی تمام ارتباطات ایجاد شده از طرف شبکه داخلی نمی توان کنترل داشت بهتر است برای هر سرویس از پراکسی استفاده کرد تا محتویات بسته هایی که وارد شبکه می شوند کنترل شود.

۷-۷- ابر شبکه سازی

تکنیک زیر شبکه سازی در سال ۱۹۸۵ برای استفاده کار امد تر از اختصاص آدرسهای IP برای شبکه های بزرگ مطرح شد. زیر شبکه سازی برای شبکه هایی با فضای آدرس بزرگ مانند کلاس A و کلاسB کاملا خوب کار می کند، اما این قالب های آدرس شبکه خیلی عمومی بوده و به سرعت درحال پرشدن می باشند. همچنین می توان از زیر شبکه سازی برای آدرس های کلاس C استفاده کرد. اما یک آدرس کلاس C فقط ۲۵۴ میزبان را پشتیبانی می کند. در بسیاری از شبکه ها ممکن است تقسیم شبکه کلاسC عملی نباشد. مخصوصا هنگامیکه لازم است تعداد میزبانهای پشتیبانی شده در هر زیر شبکه بیشتر از ۱۲۶ تا باشد.

آدرس های کلاس A و کلاس B به سرعت درحال استفاده و روبه اتمام می باشند. این پدیده که نشان دهنده اتمام فضای آدرس می باشد، پدیده ROADS[1] خوانده می شود. با وجود اینکه آدرسهای کلاس A و کلاس B روبه اتمام می باشند، ولی هنوزتعداد کافی از آدرسهای کلاس C موجود می باشد. سازمانهای بزرگ که نیاز به پشتیبانی بیشتر از ۲۵۴ میزبان دارند مجبورند از چندین آدرسهای شبکه کلاس C استفاده کنند.

فرض کنید که یک سازمان برای پشتیبانی ۶۵۵۳۴ میزبان نیاز به یک آدرس کلاس B دارد. اگر این سازمان نتواند یک آدرس کلاس B به شبکه خود اختصاص دهد، می تواند این کاررا با استفاده از چندین آدرس کلاس C انجام دهد. سوال این است که چند آدرس کلاس C برای پشتیبانی ۶۵۵۳۴ لازم است؟جواب در حدود ۲۵۶ است. این ۲۵۶ آدرس کلاس C را می توان به عنوان یک بلوک اختصاص داد. به عنوان مثال مجموعه آدرس های کلاس C زیرقادر به تامین یک آدرس کلاس B می باشند:

202.100.0.0 تا 202.100.255.255

این تکنیک، ابرشبکه سازی نام دارد. درحقیقت ابرشبکه سازی این قابلیت را به مدیران شبکه می دهد که با استفاده از چند بلوک آدرس کلاس C، بتوان یک آدرس کلاس B بدست آورد.

مزیت این تنظیم بهره وری بهتر ازفضای آدرس است. برای مثال اگر یک سازمان نیاز به شبکه ای با ۸۰۰۰ میزبان دارد بهتر است بجای انتساب یک آدرس کلاس B مجرد از یک بلوک ۳۲تایی آدرس کلاس C استفاده کنند.یک شبکه کلاس B تا ۶۵۵۳۴ میزبان را پشتیبانی می کند اما در این مثال ۵۷۵۳۵= ۸۰۰۰-۶۵۵۳۴ آدرس بکار نخواهد رفت. بنابراین با تخصیص بهینه تعداد آدرس های مورد نیاز با استفاده از روش ابرشبکه سازی، امکان استفاده بهینه از فضای آدرس های IP فراهم شده و از هرگونه اتلاف درفضای آدرس های IP جلوگیری می شود.

تکنیک ابر شبکه سازی برای استفاده ارائه دهندگان سرویس اینترنت(ISP[2]) برای تداوم اتصال اینترنت طراحی شده است. معمولا فقط ISP ها اجازه دارند تا بلوک های بزرگ آدرس از آدرس ها کلاس C را فراهم کنند. ISP ها می توانند بلوک های کوچکتر این آدرس های کلاس C را به سازمانهای دیگر که می خواهند تعداد زیادی از کامپیوتر های خود را به اینترنت متصل کند اختصاص بدهند. بعلاوه بسیاری ازسازمانهای تجاری که به آنها بلوک های آدرس کلاس C انتساب داده شده است از ابرشبکه سازی استفاده می کنند. ابرشبکه سازی اندازه جداول مسیریابی را نیز کاهش می دهد.

۷-۷-۱- مسیر یابی درون ناحیه ای بدون کلاس اینترنت (CIDR[3])

اختصاص بلوک های آدرس کلاس C از اتمام از اتمام سریع آدرس های کلاس B جلوگیری می کند. اما ازطرف دیگر، این اختصاص کلاس C به ذخیره شدن ورودی های اضافی در جدول مسیریابی مسیریابها نیاز دارد. همانطور که اشاره شد، برای

[1] Running Out of ADderss Space
[2] Internet Service Provider
[3] Classless Inter Domain Routing

تامین یک آدرس کلاس B نیاز به یک بلوک ۲۵۶تایی از آدرس های کلاس C می باشد. بنابراین مسیریاب های شبکه، درجدول مسیریابی خود به جای استفاده از یک رکورد، از ۲۵۶ رکورد استفاده می نمایند. این امر افزایشی را در تعداد ورودی های جدول مسیر یابی با با ظرفیت ۲۵۶ نشان می دهد. به عنوان مثال اگر یک مسیر یاب که از آدرسهای کلاس B استفاده می کند ۲ مگابایت حافظه برای جدول مسیریابی خود نیازداشته باشد، با عوض کردن این آدرسها با آدرسهای کلاس C به حافظه ای برابر با ۵۱۲=۲۵۶*۲ مگابایت نیاز دارد.

برای رفع مشکل فوق، از تکنیک مسیر یابی درون ناحیه ای بدون کلاس اینترنت (CIDR) استفاده می شود. تکنیک CIDR برای خلاصه کردن یک بلوک از آدرس های کلاس C به یک ورودی جدول مسیریابی مجرد استفاده می شود. این ترکیب منجر به کاهش تعداد ورودی های جداگانه جدول مسیریابی می شود. بلوک آدرس های کلاس C بوسیله یک ورودی جدول مسیریابی که به صورت زیر است ترکیب می شوند:

(پوشش ابر شبکه ، پایین ترین آدرس در بلوک)

پایین ترین آدرس در بلوک، آغاز بلوک آدرس است و پوشش ابر شبکه، تعداد آدرس های کلاس C در بلوک را مشخص می کند. پوشش ابرشبکه، برای پیشوند یکسان همه آدرس های کلاس C شامل۱است و برای قسمتهایی از آدرس های کلاس C که مقادیر متفاوت دارند صفر می باشد. به عنوان مثال، ورودی جدول مسیریابی CIDR زیر را در نظر بگیرید :

(200.1.160.0, 255.255.224.0)

نمایش بیتی 200.1.260.0 و 255.255.224.0 که پوشش CIDR است به صورت زیر است:

110010000 00000001 10100000 00000000
111111111 11111111 11100000 00000000

با بررسی CIDR ، قسمت مشترک درفضای آدرس های کلاس C به صورت زیر می باشد:

11001000 00000001 101

صفر ها در پوشش CIDR به قسمت متغیر بلوک آدرسهای بلوک آدرسهای کلاس C تعلق دارند. بنابراین بازه آدرسهای C بین آدرسهای کلاس C پایین و بالای زیر است:

11001000 00000001 10111111 111111111=200.1.191.255

نشانه گذاری دیگری که می توان برای بلوک های CIDR استفاده به شرح زیر است:

تعداد بیتهای پیشوند مشترک / پایین ترین آدرس در بلوک

تعداد بیتهای پیشوند مشترک، بیانگر تعداد ۱های پوشش ابر شبکه است. بنابراین مثال های زیر نمایشهای هم ارز بلوک CIDR هستند:

(200.1.160.0 , 255.255.224.0)=200.1.160.0/19

۷-۸- آدرسهای IP نسخه ۶

همانطور که قبلا در این فصل اشاره شد، با بزرگ شدن اینترنت، فضای آدرس ۳۲ بیتی برای آدرس های IP نسخه ۴، رو به اتمام می باشد. هر اتصال شبکه IP در اینترنت نیاز به یک آدرسIP یکتا دارد. بعضی از تجهیزات شبکه، بیشتر از یک اتصال شبکه دارند که نتیجه آن مصرف سریع آدرسهای IP قابل انتساب است. تخمین زده شده است که آدرسهای IP ۳۲ بیتی، می توانند بیشتر از ۲/۱۰۰/۰۰ شبکه و چیزی حدود ۳۷۲۰ میلیون میزبان را مهیا سازد. با این وجود ، مدل اختصاصی فضای آدرس IP نسخه ۴زیاد کارآمد نیست. حتی با وجود تکنیک های زیرشبکه سازی و ابرشبکه سازی که امکان استفاده بهینه از فضای آدرس های IP را فراهم می کند، همچنان مشکل کمبود آدرس های IP نسخه ۴ حس می گردد.

برای رفع مشکل فوق، موسسه استانداردگذاری اینترنت (IETF[1]) تصمیم به طراحی پروتکل اینترنت نسل بعدی گرفت که به عنوانIPng یا IP نسخه ۶ (IPV6) شناخته می شود. یکی ازاهداف طراحی IPV6 استفاده ازآدرسهای ۱۲۸ بیتی می باشدکه چهار برابر اندازه بیتی آدرسهای IPV4 است. IPV6 نیز از مفهوم شماره های شبکه و شماره های میزبان استفاده می کند، اما این مفهوم را به چند سطح توسعه داده است. آدرس دهی سلسله مراتبی در IPV6 مسیریابی کارآمدتری را پشتیبانی می کند. آدرس IPV6 با استفاده ۳۲ بیت آدرسهای IPV4 در بیتهای پائین مرتبه فضای آدرس و اضافه کردن یک پیشوند ثابت ۹۶ بیتی می تواند شامل یک آدرس IPV4 باشد. پیشوند ۹۶ بیتی شامل ۸ بیت صفر است که با ۱۶ بیت صفر یا ۱۶ بیت ۱ دنبال می شود. IPV6 با هدف امکان تعامل وارتباط با سیستمهای IPV4 طراحی شده است که یک دوره همزیستی را برای دو سیستم IP سبب می شود. هدف این است که سیستمهای IPV4 جاری را عاقبت با سیستمهای IPV6 جایگزین کرد.

پروتکلIPV6 سیستمهای قابل حمل متحرک را پشتیبانی می کند. این خاصیت به کاربران کامپیوترهای قابل حمل و وسایل دیگر اجازه می دهد تا بدون انجام پیکره بندی دستی از هر جایی به شبکه متصل شوند. همچنین IPV6 قابلیت رمزنگاری را در لایه اینترنت پشتیبانی می کند و پشتیبانی بهتری را برای ترافیک بلادرنگ مهیا می سازد. ترافیک داده های بلادرنگ تضمینی را برای حداکثر تاخیر بسته های ارسالی در شبکه نیاز دارد.

چون آدرس های IPV6 ۱۲۸ بیت طول دارند، استفاده از نشانه گذاری دهدهی نقطه دار یک نشانه گذاری مناسب برای نوشتن آدرس های IPV6 نیست. اگر برای نوشتن آدرسهای IPV6 از نشانه گذاری دهدهی نقطه دار استفاده شود، می بایست یک رشته را شامل ۱۶ عدد دهدهی که با نقطه از هم جدا شده اند نوشت. طراحانIPV6 استفاده از نشانه گذاری شانزده شانزدهی دو نقطه دار را برای نوشتن الگوی بیتی انتخاب کردند. هریک از مقادیر شانزده شانزدهی به عنوان ۱۶ بیت نوشته شده اند که بوسیله کاراکتردونقطه (:) از هم جدا شده اند. به عنوان مثال یک آدرس IPV6 می تواند به صورت زیر نوشته شود:

5800:00C3:E3C3:F1AA:48E3:D923:D495:AAFE

با استفاده از نشانه گذاری شانزده شانزدهی دو نقطه دار ارقام و کاراکتر های جدا سازی کمتری مورد نیاز است. دوتکنیک مختلف برای کاهش نمایش آدرس های IPV6 ارائه شده است. تکنیک اول این است که می توان صفرهای موجود درآدرس را حذف نمود. به عنوان مثال، آدرس IPV6 زیر را در نظر بگیرید:

48A6:0000:0000:0000:0000:0DA3:003F:0001

با پرش از صفر های اضافی این آدرس را می توانید به صورت آدرس ساده شده زیر بنویسید:

48A6:0:0:0:0:DA3:3F:1

تکنیک دوم از فشرده سازی صفر استفاده می کند. به این صورت که یک رشته از صفرهای تکراری درآدرس های IPv6 را می توان حذف نمود وبه جای آن "::" جایگزین کرد. بنابراین آدرس IPV6 پیش را می توان به صورت زیر نوشت :

48A6::DA3:3F: 1

نمایش IPV6 آدرس IPV4 170.1.1.1 به صورت زیر می باشد:

0:0:0:0:0:0:AA01:101

همچنین می توان این آدرس را به صورت زیر نیز نمایش داد:

::AA01:101

[1] Internet Engineering Task Force

پرسش های فصل

۱. دو مزیت اصلی معماری TCP/IP را شرح دهید.
۲. رابطه بین تعداد اتصال های یک میزبان به شبکه با تعداد آدرسهای IP مورد نیاز آن میزبان را توضیح دهید.
۳. مستقل بودن آدرس IP از آدرس فیزیکی چه مزایا و چه معایبی به دنبال خواهد داشت.
۴. مزیت استفاده از یک مقدار آدرس منطقی برای آدرسهای IP چیست؟
۵. کاربرد هریک از کلاس های آدرس IP را توصیف نمایید.
۶. مفهوم آدرس دهی تک پخشی، چند پخشی و همه پخشی را توضیح دهید.
۷. برای عملیات تک پخشی، چند پخشی و همه پخشی درمدل آدرس دهی IP چه تمهیداتی دیده شده است؟
۸. مزایا و عیب های تقسیم آدرس IP به یک netid و یک hostid چیست ؟
۹. تفاوت بین یک آدرس همه پخشی مستقیم و یک آدرس همه پخشی محدود را باذکر مثال مناسب توضیح دهید.
۱۰. یک آدرس برگشت حلقه نرم افزاری چیست ؟ قالب آن را توصیف کنید . چند نمایش آدرس برگشت حلقه وجود دارد ؟
۱۱. کاربردهای آدرس IP 0.0.0.0 و 255.255.255.255 را بنویسید.
۱۲. یک شبکه کلاس C با آدرس 194.34.56.0 داده شده است چند میزبان برای این شبکه امکان دارد ؟ برای آدرس کلاس B 166.23.0.0 چه طور؟
۱۳. مفهوم و کاربرد آدرس های خصوصی را نوشته و توضیح دهید که تحت چه شرایطی یک سازمان خواستار استفاده از آدرس های خصوصی است ؟
۱۴. دریک شبکه اینترنت ، به چه نوع میزبان هایی می توان یک آدرس IP خصوصی انتساب داد ؟ آیا می توان یک آدرس IP خصوصی به یک میزبان یا مسیریابی که برای دنیای خارج قابل رویت است، اختصاص داد؟
۱۵. نوع کلاس IP آدرس های زیر را بدست آورید:

23.1.3.5	198.34.54.23	233.12.3.4
45.2.3.67	178.11.23.5	254.12.34.5

۱۶. مفهوم و کاربرد زیر شبکه سازی را با ذکر یک مثال مناسب توصیف نمایید.
۱۷. مزایای زیرشبکه سازی را بنویسید.
۱۸. عملکرد پروتکل NAT را با ذکر یک مثال توضیح دهید.
۱۹. مفهوم و کاربرد ابر شبکه سازی را با ذکر یک مثال مناسب توصیف نمایید.
۲۰. پدیده ROADS را توضیح دهید.