



در حال حاضر دو نوع آدرس آی پی وجود دارد IPv4 و IPv6. در ادامه مطلب توضیحات کامل درباره این دو نوع آدرس آی پی (ip address) و آدرس مک MAC Address ارائه می‌شود.

این مطلب بخشی از [سری آموزش‌های نتورک پلاس](#) است که بیشتر در سایت شبکه منتشر شده است. برای مشاهده فهرست و خرید کتاب Network+ راهنمای شبکه‌ها [اینجا](#) کلیک کنید.

آدرس مک لایه پیوند داده

یک آدرس مک درون هر کارت واسط شبکه به شکل توکار قرار گرفته است. آدرسی که انتظار می‌تواند منحصر به فرد و مخصوص همان کارت واسط شبکه باشد. آدرس مک یک مقدار 48 بیتی است که به صورت اعداد هگزا که با دو نقطه از یکدیگر جدا می‌شوند نوشته می‌شود. مثال زیر نمونه‌ای از یک آدرس مک است.

00:60:8C:00:54:99

گره‌ها روی یک شبکه محلی با استفاده از آدرس‌های مک یکدیگر را پیدا می‌کنند.

آدرس آی پی در لایه شبکه

یک آدرس آی پی تقریباً به هر رابط یا به عبارت دقیق‌تر به هر گره متصل به شبکه تخصیص داده می‌شود. هر کامپیوتر یا دستگاهی برای آن‌که بتواند به اینترنت متصل شود به آدرس آی پی نیاز دارد. آدرس آی پی کمک می‌کند تا دستگاه‌های متصل به اینترنت را شناسایی کنیم. برنامه‌های کاربردی همچون مرورگرهای وب می‌توانند آدرس‌های آی پی را بازیابی و ذخیره کنند، اما در زمان مسیریابی، یک آدرس آی پی تنها در لایه شبکه استفاده می‌شود.

انواع آدرس‌های آی پی

در حال حاضر دو نوع آدرس آی پی به شرح زیر وجود دارد:

IPv4: نسخه چهارم پروتکل اینترنت (IPv4) سرنام (Internet Protocol version 4) دارای آدرس‌های 32 بیتی است که در قالب چهار مقدار اعشاری که در گروه‌های هشت‌بیتی شبیه به 92.106.50.200 قرار دارند نوشته می‌شوند. هر گروه هشت‌تایی در مبنای دودویی نوشته می‌شود که دقیقاً 8 بیت است. به‌طور مثال مقدار 92 در

فرمت دودویی برابر با 1100 0101 است.

نکته: یک مقدار باینری به سیستمی اشاره دارد که بر مبنای صفرها و یکها کار می‌کند. این سیستم که به مبنای دودویی شهرت دارد پایه و اساس هر محاسبه‌ای بوده و شما به عنوان یک کارشناس شبکه مجبور هستید اطلاعات دقیقی در ارتباط با آن به دست آورید.

IPv6: در نسخه ششم پروتکل اینترنت (IPv6) سرنام Internet Protocol version 6 مقادیر 128 بیتی هستند و در بلوک‌های هشت‌گانه با اعداد هگزا نوشته می‌شوند. مثال زیر نمونه‌ای از یک آدرس مبتنی بر پروتکل نسل ششم است.

2001:0DB8:0B80:0000:0000:00D3:9C5A:00CC

نکته: یک مقدار هگزادسیمال (عدد هگزا خوانده می‌شود) که به آن مبنای شانزده گفته می‌شود، اعداد را به شکل متفاوتی نشان می‌دهد. در مبنای 16 اعداد از مقدار 0 تا 9 به شکل عادی نوشته شده اما از مقدار 10 به بعد از کاراکترهای A تا F برای نمایش آن‌ها استفاده می‌شود.

A, B, C, D, E, F, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0

دقت کنید مبنای هگزا نیز یکی دیگر از مبناهای مهمی است که باید اطلاعات جامعی در ارتباط با آن به دست آورید.

درگاه‌ها در لایه انتقال

یک درگاه (در اصطلاح عام یک پورت) شماره‌ای است که لایه انتقال برای پیدا کردن یک برنامه کاربردی از آن استفاده می‌کند. این شماره یک برنامه را در میان برنامه‌های مختلفی که روی میزبان اجرا می‌شوند شناسایی می‌کند. به‌طور مثال یک برنامه وب‌سرور به‌طور معمول به‌گونه‌ای پیکربندی شده است که همواره در حال گوش دادن به درخواست‌هایی است که از درگاه 80 وارد می‌شوند.

لایه کاربرد- نام کامپیوتر و نام میزبان

هر هاست (میزبان) روی یک شبکه دارای کاراکترهای منحصر به فردی است که نام میزبان را شکل می‌دهند. به این کاراکترها نام دامنه کاملاً واجد شرایط (FQDN) سرنام fully qualified domain name گفته می‌شود. www.mycompany.com، ftp.mycompany.com و susan.mycompany.com همگی نام‌های دامنه معتبر در یک شبکه هستند. به‌طور جمعی به دو بخش آخر نام میزبان (به‌طور مثال mycompany.com) نام دامنه می‌گویم که در حالت کلی اشاره به دامنه یا شبکه یک سازمان دارند. در مثال ما، بخش ابتدایی این آدرس‌ها ([susan, ftp](http://susan.ftp)) و www نام میزبان هستند که مشخص کننده یک کامپیوتر منحصر به فرد روی یک شبکه هستند. ftp اشاره به نام میزبانی دارد که به یک سرور FTP اختصاص داده می‌شود (از پروتکل ftp استفاده می‌کند) و www نیز در حالت کلی به نام میزبانی اختصاص داده می‌شود که کامپیوتری است که روی یک وب‌سرور در حال اجرا است. (از پروتکل انتقال ابرمتن ایمن استفاده می‌کند).

نکته: سازمانی که مسئولیت پیگیری و اختصاص آدرس‌های آی‌پی، شماره پورت‌ها و نام دامنه‌ها بر عهده او است، آیانا (IANA) سرنام Internet Assigned Numbers Authority نام دارد. آیانا یکی از دپارتمان‌های آیکان (ICANN) سرنام Internet Corporation for Assigned Names and Numbers است که یک سازمان غیرانتفاعی بوده که مسئولیت وضع خط‌مشی‌هایی که کمک می‌کنند اینترنت بدون مشکل کار کند را عهده‌دار است. برای دریافت اطلاعات بیشتر در ارتباط با این دو سازمان به آدرس‌های www.iana.org و www.icann.org مراجعه کنید. در این آدرس‌ها اطلاعات مفیدی وجود دارد که نشان می‌دهند اینترنت چگونه کار می‌کند.

اکنون که تصویری بزرگ از فرآیند آدرس‌دهی هر لایه در مدل OSI به دست آورید، زمان آن رسیده است که جزئیات بیشتری در این ارتباط به دست آورده و ببینید این‌کار چگونه انجام می‌شود. کار را با آدرس‌های مک که در پایین مدل OSI قرار دارند آغاز می‌کنیم.

آدرس‌های مک

مک آدرس کارت‌های شبکه به شکل مستقیم روی مدار چاپی این قطعات یا به شکل برجسب روی آن‌ها درج شده است. شکل زیر نمونه‌ای از یک مک آدرس درج شده روی یک کارت شبکه را نشان می‌دهد. (اگر موفق نشدید مک آدرس کارت شبکه را مشاهده کنید، راهکارهایی برای مشاهده مک آدرس وجود دارد که در شماره‌های آینده به آن‌ها خواهیم پرداخت).



مک آدرس متعلق به کارت شبکه شرکت Dlink

مک آدرس‌ها از دو قسمت تشکیل شده که 48 بیت طول داشته، در مبنای هگزادسیمال نوشته می‌شوند و با دو نقطه از یکدیگر جدا شده‌اند. مثال زیر نمونه‌ای از یک مک آدرس را نشان می‌دهد.

00:60:8C:00:54:99

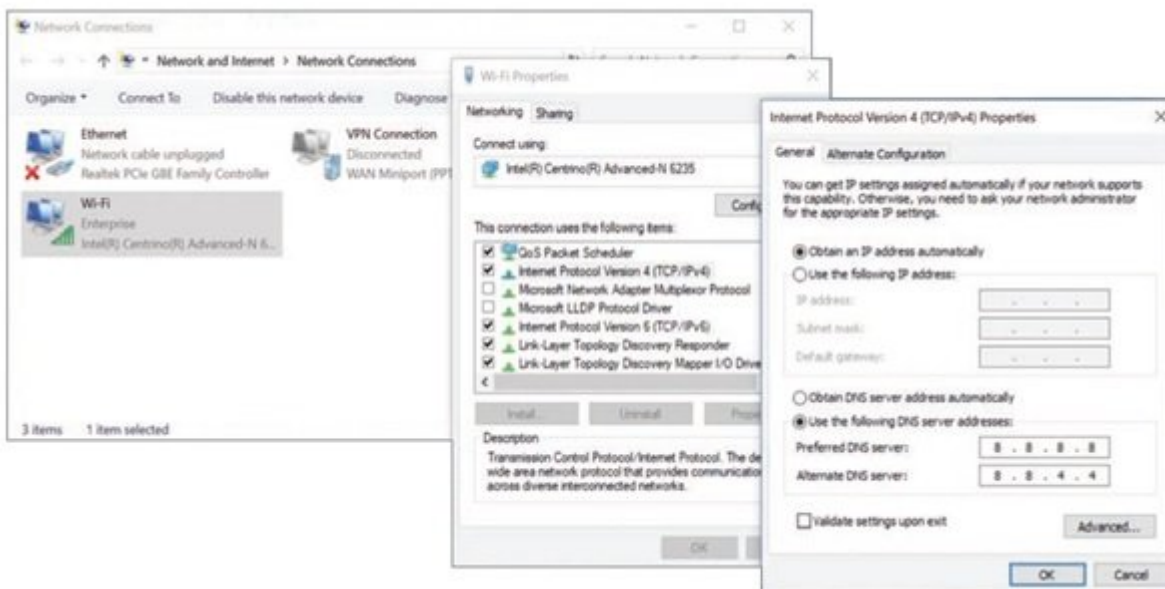
24 بیت اول (شش کاراکتر هگزا 00:60:8C) شناسه منحصر به فرد سازمانی (OUI) سرنام Organizationally Unique Identifier هستند که سازنده کارت شبکه را توصیف می‌کنند. این شناسه از سوی موسسه مهندسان برق و الکترونیک (IEEE) به سازنده یک کارت شبکه تخصیص داده می‌شود. اگر مک آدرس یک کامپیوتر را در اختیار داشته باشید، در ادامه می‌توانید با یک جست‌وجوی اینترنتی سازنده کارت شبکه را پیدا کنید. IEEE بانک اطلاعاتی نسبتاً مفصلی ایجاد کرده که درون این بانک اطلاعاتی شناسه منحصر به فرد سازمانی هر تولیدکننده در آن نگهداری شده و از طریق وب در معرض دید همگان قرار دارد. در زمان نگارش این مقاله دسترسی به بانک اطلاعاتی فوق از طریق آدرس [OUI Index](#) امکان‌پذیر است.

24 بیت دوم شناسه منحصر به فرد دستگاه (Device ID) است که برای شناسایی خود دستگاه استفاده می‌شود. تولیدکنندگان به هر کارت شبکه یک شناسه توصیف‌کننده منحصر به فرد اختصاص می‌دهند که این شناسه بر مبنای مدل کارت شبکه، زمان ساخت کارت شبکه و... ایجاد می‌شود. در نتیجه به لحاظ تئوری هیچ دو کارت شبکه‌ای مک آدرس یکسانی نخواهند داشت.

آدرس‌های آی‌پی

در مدل OSI زمانی که به لایه سوم می‌رسیم با آدرس‌های آی‌پی منحصر به فرد گره‌ها روی لایه شبکه (Network Layer) سروکار خواهیم داشت. در حالی که مک‌آدرس برای ارتباطات درون شبکه‌ای استفاده می‌شود، در مقابل یک آدرس آی‌پی برای اتصال یک دستگاه درون شبکه‌ای به یک دستگاه گیت‌وی شبیه به روتر استفاده می‌شود. شما می‌توانید یک آدرس آی‌پی ایستای ثابت برای یک دستگاه در نظر بگیرید یا می‌توانید دستگاه را به شکلی پیکربندی کنید که یک آدرس آی‌پی پویا را به شکل متغیر از یک سرور DHCP در هر بار که به شبکه متصل می‌شود دریافت کند. یک سرور پروتکل پیکربندی پویای میزبان (DHCP) سرنام Dynamic Host Configuration Protocol نحوه تخصیص پویای آدرس‌های آی‌پی به دستگاه‌های شبکه را مدیریت می‌کند. در مقاله‌های آتی اطلاعات بیشتری در ارتباط با DHCP به دست خواهید آورد. اکنون اجازه دهید به تنظیمات TCP/IP روی یک کامپیوتر ویندوز 10 نگاهی داشته باشیم.

1. در کادر جست‌وجوی ویندوز 10 عبارت Control Panel را تایپ کرده و روی گزینه پیدا شده کلیک کنید. در Control Panel روی گزینه Network and Internet کلیک کرده و سپس روی گزینه Network and Sharing Center کلیک کنید. در ادامه روی گزینه Change adapter settings در سمت چپ پنجره کلیک کنید.
2. روی آیکن مربوط به ارتباط شبکه کلیک راست کرده و گزینه Properties را انتخاب کنید. در پنجره باز شده، گزینه Internet Protocol Version 4 را کلیک کرده و سپس روی گزینه Properties کلیک کنید.



3. در پنجره ظاهر شده گزینه Obtain an IP address automatically for dynamic IP به شما اجازه می‌دهد از سرور DHCP برای تخصیص پویای آدرس‌های آی‌پی استفاده کنید. گزینه Use the following address به شما اجازه می‌دهد یک آدرس آی‌پی ایستا، زیرشبکه و گیت‌وی پیش‌فرض را انتخاب کنید. البته به این نکته توجه داشته باشید که شما با پیکربندی TCP/IP نیز می‌توانید آدرس سرور سامانه نام دامنه (DNS) را از یک سرور DHCP به دست آورده یا به شکل دستی آدرس سرور سامانه نام دامنه را مشخص کنید.

توضیح هر یک از مقادیر شکل بالا به شرح زیر است:

Gateway: یک کامپیوتر، روتر یا دستگاهی است که میزبان برای دسترسی به شبکه از آن استفاده می‌کند. دروازه پیش‌فرض/گیت‌وی پیش‌فرض (default gateway) دستگاهی است که گره‌های شبکه برای اولین بار برای دسترسی به دنیای خارج از آن استفاده می‌کنند.

Subnet mask: زیرشبکه که برخی منابع به آن netmask می‌گویند (البته درست نیست!) یک مقدار 32 بیتی است که به یک کامپیوتر کمک می‌کند کامپیوتر دیگری را پیدا کند. این مقدار 32 بیتی نشان می‌دهد چه بخش از یک آدرس آی‌پی جزئی از شبکه بوده که شناسه شبکه (network ID) یا آدرس شبکه (network address) نامیده می‌شود و چه بخش جزئی از میزبان بوده و شناسه منحصر به فرد میزبان (host ID) یا شناسه منحصر به فرد گره

(node ID) نامیده می‌شود. زیرشبکه به دستگاه‌هایی که درون زیرشبکه قرار دارند، کمک می‌کند به شکل مستقیم با یکدیگر ارتباط برقرار کنند. با استفاده از این اطلاعات، یک کامپیوتر می‌تواند تعیین کند که آیا کامپیوتر دیگری با یک آدرس آی‌پی تخصیص داده شده به آن درون زیرشبکه وجود دارد یا خیر.

نکته: بیشتر منابع subnet mask و netmask را دو مفهوم یکسان می‌دانند، اما به لحاظ فنی تفاوت ظریفی میان این دو اصطلاح وجود دارد. subnet شبکه کوچکی است که درون یک شبکه بزرگ قرار دارد. یک netmask مشتمل بر بیت‌های یک آدرس آی‌پی است که شبکه‌ای بزرگ‌تر را نشان می‌دهند، در حالی که subnet mask بیت‌های یک آدرس آی‌پی را نشان می‌دهد که توصیف‌کننده یک زیرشبکه کوچک‌تری هستند که درون یک شبکه بزرگ‌تر قرار دارد. در بیشتر مواقع این دو واژه به جای یکدیگر استفاده می‌شوند. ما در شماره‌های آینده اطلاعاتی بیشتری در ارتباط با زیرشبکه (subnet) ارائه خواهیم کرد.

سرور سامانه نام دامنه DNS Server: سروری است که مسئولیت ردیابی نام کامپیوترها و آدرس‌های آی‌پی را عهده‌دار است. در دنیای شبکه انواع مختلفی از سرورهای سامانه نام دامنه وجود دارد که با نحوه کار آن‌ها بیشتر آشنا خواهید شد.

شما می‌توانید در پنجره خط فرمان از ابزار ipconfig برای پیدا کردن تنظیمات جاری TCP/IP استفاده کنید. این ابزار به ویژه زمانی مفید است که قصد استفاده از DHCP را دارید، زیرا تخصیص خودکار آدرس‌های آی‌پی در پنجره ویژگی‌های IPv4 نشان داده نمی‌شود.

آدرس‌های IPv4

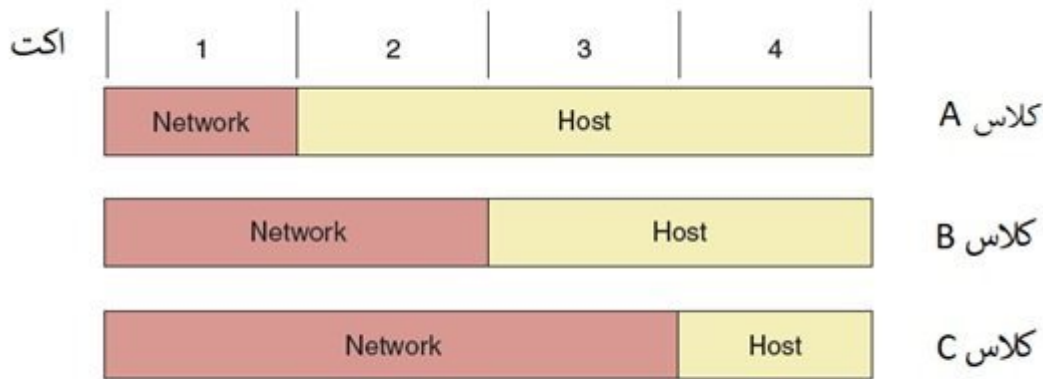
یک آدرس آی‌پی 32 بیتی به چهار گروه هشت بیتی تقسیم شده که به صورت چهار عدد اعشاری جدا از هم همچون 72.56.105.12 نشان داده می‌شوند. هر یک از این چهار گروه اکت (octet) نامیده می‌شوند. بزرگ‌ترین عدد 8 بیتی برابر با مقدار 11111111 بوده که معادل 255 در سیستم دهدهی است. بنابر این، بزرگ‌ترین آدرس آی‌پی می‌تواند برابر با 255.255.255.255 در سیستم دهدهی و برابر با 11111111.11111111.11111111.11111111 در سیستم باینری (دودویی) باشد. هر کدام از این چهار اکت می‌توانند هر مقداری در محدوده 0 تا 255 را داشته باشند که در مجموع 4.3 میلیارد آدرس (256x256x256x256) در نسخه چهارم پروتکل IPv4 را شامل می‌شوند. البته از این تعداد، برخی از آدرس‌های آی‌پی رزرو شده هستند، بنابراین مقدار فوق یک عدد تقریبی است.

قالب آدرس‌های IPv4

بخش اول یک آدرس آی‌پی برای شناسایی یک شبکه و بخش دوم برای شناسایی میزبان استفاده می‌شود. زمانی که تصمیم می‌گیرید از آدرس‌های طبقه‌بندی شده استفاده کنید که در اصل روش سنتی مدیریت محدوده آدرس‌های آی‌پی هستند، خط تقسیم بخش شبکه و بخش میزبان با محدوده‌های اعدادی که اشاره به آدرس‌های آی‌پی دارند ممکن است کمی مشکل است. آدرس‌های IPv4 به پنج کلاس A، B، C، D و E تقسیم می‌شوند. جدول زیر محدوده آدرس‌های آی‌پی عمومی نسل چهارم هر یک از این کلاس‌ها را نشان می‌دهد.

کلاس‌های آدرس آی‌پی			
کلاس	اکت شبکه	تعداد تقریبی شبکه‌های ممکن	تعداد تقریبی آدرس‌های آی‌پی در دسترس در هر شبکه
A	x.y.z to 126.x.y.z.1	126	16 میلیون
B	x.y to 191.255.x.y.128.0	16,000	65,000
C	192.0.0.x to 223.255.255.x	2 میلیارد	65,000

x، y و z در یک آدرس آی‌پی بیان‌گر اکتی است که برای شناسایی میزبان‌ها روی یک شبکه از آن استفاده می‌شود. شکل زیر نشان می‌دهد که چگونه کلاس‌های A، B و C در بخش شبکه و میزبان تقسیم می‌شوند.



بخش شبکه و بخش میزبان برای هر کلاس آدرس IP

نکته: [آزمون نتورک پلاس](#) از شما انتظار دارد که بتوانید کلاس هر آدرس آی پی را تشخیص دهید. به همین دلیل لازم است که جدول بالا را حفظ کنید. شما با نگاه کردن به یک آدرس آی پی باید بتوانید بگویید که یک آدرس به چه کلاسی تعلق دارد.

کلاس B، A، و C آدرس‌های آی پی مجاز در دسترسی هستند که روی بستر اینترنت استفاده شده و به همین دلیل به آن‌ها آدرس‌های آی پی عمومی گفته می‌شود. برای حفظ آدرس‌های آی پی عمومی به شکلی که هم اکنون از آن‌ها استفاده می‌شود، یک شرکت می‌تواند از آدرس‌های آی پی خصوصی روی شبکه خصوصی خودش استفاده کند. شبکه‌ای که قرار نیست به شکل مستقیم به اینترنت متصل شود. آیانا پیشنهاد می‌کند که سازمان‌ها از آدرس‌های آی پی زیر در شبکه‌های خصوصی خود استفاده کنند.

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

آدرس‌های آی پی کلاس‌های E و D برای استفاده عمومی در دسترس نیستند. آدرس‌های کلاس D از اکت 224 آغاز شده و به اکت 239 ختم می‌شوند و برای انتقال چندبخشی (multicast) که در آن یک میزبان پیامی را برای چند میزبان دیگر ارسال می‌کند استفاده می‌شوند. یک مثال در این زمینه موقعی است که میزبانی یک کنفرانس ویدئویی را از طریق اینترنت با چند شرکت دیگر برگزار می‌کند. آدرس‌های کلاس E که از اکت 240 آغاز شده و تا اکت 254 ادامه پیدا می‌کنند برای جست‌وجو اختصاص یافته‌اند. علاوه بر این، آدرس‌های آی پی که در جدول زیر مشاهده می‌کنید برای استفاده‌های خاص پروتکل TCP/IP در نظر گرفته شده‌اند و نباید به دستگاهی روی شبکه تخصیص داده شوند.

آدرس‌های آی پی	عملکرد
255.255.255.255	از سوی پردازنده‌های پس‌زمینه TCP/IP برای ارسال پیام‌ها به شکل همه پخش (broadcast) استفاده می‌شود. همه پخش به معنای آن است که در یک شبکه یک دستگاه برای همه کامپیوترهای عضو شبکه اطلاعات را ارسال کرده که در اصلاح تخصصی به آن همه پخش می‌گویند.
255.255.255.255	در حال حاضر تخصیص پیدا نکرده است.
through 127.0.0.1 127.255.255.254	برای جست‌وجو یا نشان دادن کامپیوتر شما استفاده شده که در این حالت به آدرس loopback معروف است.
through 169.254.0.1 169.254.255.254	برای ساخت یک آدرس آی پی خصوصی خودکار (APIPA) زمانی استفاده می‌شود که یک کامپیوتر برای DHCP پیکربندی شده و برای اتصال به شبکه قادر نیست از آدرس IPv4 که سرور DHCP ارائه می‌کند استفاده کند.

نکته: یک شبکه محلی به گروهی از کامپیوترها و دستگاه‌های مختلف اشاره دارد که می‌توانند بدون نیاز به یک روتر و از طریق یک آدرس به شکل مستقیم با یکدیگر در ارتباط باشند. به لحاظ فنی، به یک شبکه محلی که شامل گره‌هایی است که اطلاعات را به شکل همه‌پخشی ارسال می‌کنند دامنه همه‌پخشی (broadcast domain) می‌گویند. در یک چنین شبکه‌هایی روترها پیام‌های همه‌پخشی را فوراً نکرده و بنابراین مرز مشخصی برای یک شبکه محلی ایجاد می‌شود.

نکته: در حالت کلی در آزمون‌های نتورک‌پلاس به APIPA اشاره می‌شود.

آدرس‌های IPv6

استاندارد IPv6 برای بهبود قابلیت مسیریابی، سرعت بخشیدن به ارتباطات استاندارد IPv4 و ارائه آدرس‌های آی‌پی عمومی بیشتری روی بستر اینترنت طراحی شد. اما نحوه نوشتن و خواندن آدرس‌های IPv6 چگونه بوده و چه ویژگی‌هایی دارند؟

- آدرس‌های IPv6 همگی 128 بیتی هستند که در قالب یک بلوک هشت‌تایی و در مبنای هگزادسیمال نوشته می‌شوند که با کاراکتر دو نقطه از یکدیگر جدا می‌شوند. مقدار زیر بیان‌گر یک آدرس آی‌پی نسل ششم است:

```
2001:0000:0B80:0000:0000:00D3:9C5A:00CC
```

- در این آدرس هر بلوک 16 بیتی است. به‌طور مثال، اولین بلوک در آدرس آی‌پی قبلی 2001 یک مقدار هگزا است که مبنای باینری آن به شرح زیر است:

```
0010 0000 0000 0001
```

- صفرهایی که در قالب بلوک‌های چهارگانه در آدرس قرار دارند قابل حذف شدن هستند. با حذف این صفرها آدرس آی‌پی ما به صورت زیر نوشته می‌شود:

```
2001:0000:B80:0000:0000:D3:9C5A:CC
```

- اگر بلوک‌هایی همگی شامل صفر باشند، امکان حذف بلوک‌ها و جایگزینی کاراکتر دو نقطه :: وجود دارد. برای اجتناب از اشتباه، فقط یک مجموعه از کاراکترهای دو نقطه‌ای در یک آدرس آی‌پی استفاده می‌شوند. این حرف به این معنا است که آدرس آی‌پی ساده ما می‌تواند به یکی از دو حالت زیر نوشته شود.

```
2001::B80:0000:0000:D3:9C5A:CC
```

```
2001:0000:B80::D3:9C5A:CC
```

ما در [سری از آموزش‌های نتورک‌پلاس](#) از متد دوم برای نمایش آدرس‌ها استفاده می‌کنیم، زیرا صفرهای کمتری دارد. روشی که کامپیوترها برای برقراری ارتباط بر مبنای IPv6 از آن استفاده می‌کنند باعث شده است تا اصطلاحاتی که برای توصیف ارتباطات TCP/IP استفاده می‌شوند با تغییراتی همراه شود. در اینجا به چند مورد از این اصطلاحاتی اشاره می‌کنیم که در استاندارد IPv6 از آن‌ها استفاده می‌شود.

- یک لینک (پیوند) که در اغلب موارد لینک محلی (local link) نامیده می‌شود در هر شبکه محلی محدود شده با روترها استفاده می‌شود.
- یک رابط/واسط ضمیمه الصاق شده به گرهی در یک لینک است. این ضمیمه می‌تواند فیزیکی و یک آداپتور شبکه مرتبط با وای‌فای باشد یا می‌تواند منطقی و یک ماشین مجازی باشد.
- شبکه‌هایی که به شکلی پیکربندی شده‌اند که از هر دو پروتکل IPv4 و IPv6 استفاده کنند شبکه‌های دو پشته نامیده می‌شوند. با این حال، اگر بسته‌های یک شبکه مجبور شوند از شبکه‌های دیگری عبور کنند که از الگوی دو پشته بهره نمی‌برند، برای حل این مشکل از تکنیک تونل‌زنی استفاده می‌شود تا بسته‌های IPv6 بدون مشکل انتقال پیدا کنند. از آنجایی که اینترنت به‌طور کامل دو پشته نیست، تکنیک تونل‌زنی همیشه برای انتقال بسته‌های IPv6 روی اینترنت استفاده می‌شود.

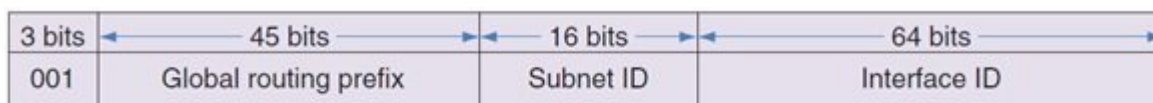
- 64 بیت آخر یا بلوک چهارم یک آدرس IPv6 برای شناسایی رابط استفاده شده و interface ID یا interface identifier نامیده می‌شود. این 64 بیت منحصر به فرد برای شناسایی یک رابط روی یک لینک محلی استفاده می‌شود.
- Neighbors یا در اصطلاح عام همسایگان به دو یا چند گرهی که روی یک لینک هستند اشاره دارد.

انواع آدرس‌های IPv6

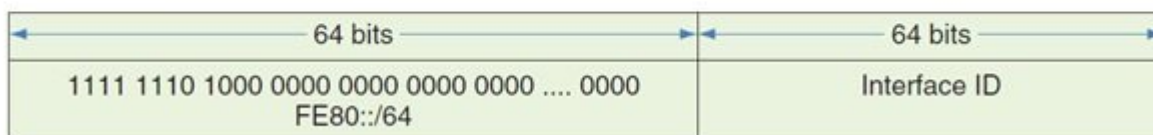
نوع کلاس‌بندی آدرس‌های IPv6 متفاوت از IPv4 است. IPv6 از سه نوع آدرس آی‌پی پشتیبانی می‌کند که به شرح زیر هستند:

آدرس تک‌یاب (unicast address): یک گره منفرد در یک شبکه را نشان می‌دهد. در شکل زیر دو نوع آدرس تک‌یاب را مشاهده می‌کنید.

آدرس‌های جهانی



آدرس محلی



2 مدل آدرس در پروتکل IPv6

global address: آدرس جهانی می‌تواند روی اینترنت مسیریابی شده و عملکردی شبیه به آدرس‌های عمومی IPv4 دارد. این آدرس‌ها در بیشتر موارد با پیشوند 2000::3 شروع می‌شوند هرچند پیشنهادهای دیگری نیز معرفی شده و استفاده می‌شوند. در پیشوند فوق 3/ نشان می‌دهد که سه بیت ابتدایی ثابت بوده و همیشه برابر با 001 هستند. اگر در شکل بالا دقت کنید مشاهده می‌کنید که 16 بیت برای شناسه زیرشبکه رزرو شده‌اند که برای شناسایی یک زیرشبکه در یک شبکه بزرگ سازمانی استفاده می‌شوند.

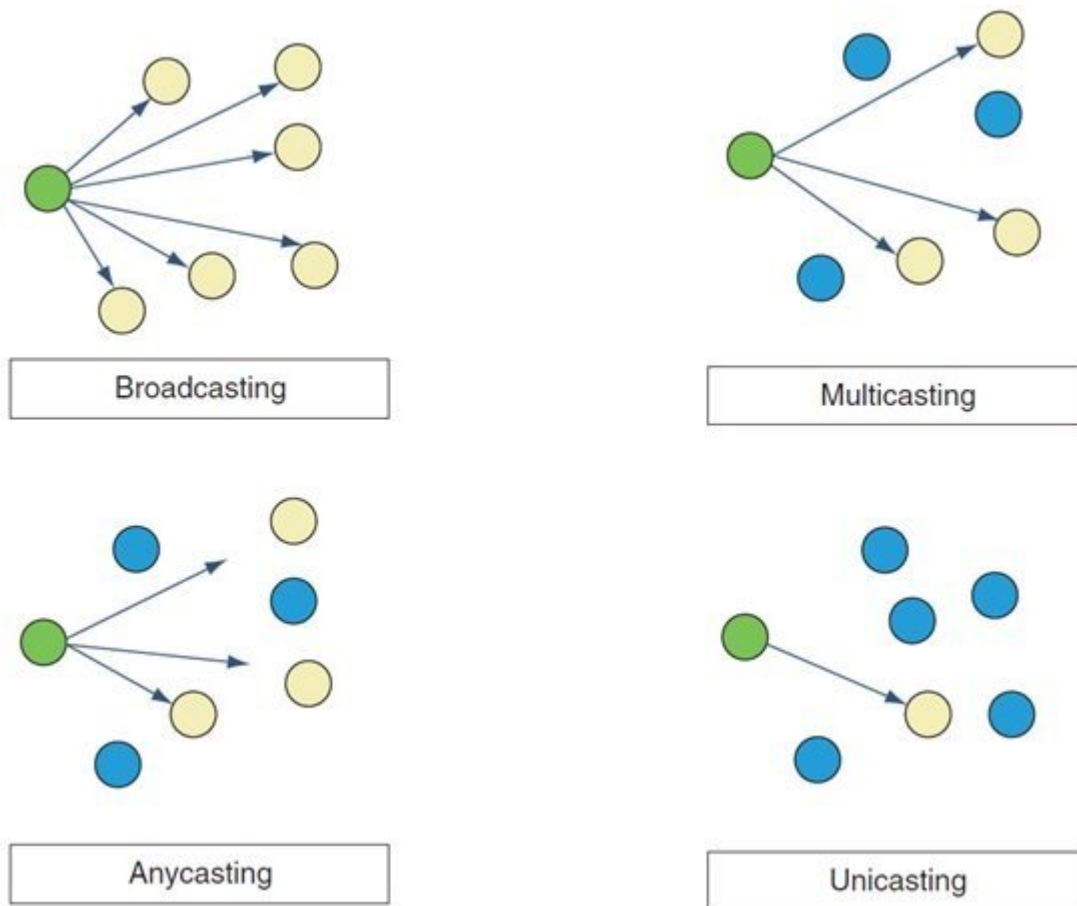
link local address: آدرس لینک محلی می‌تواند برای برقراری ارتباط میان گره‌هایی که درون لینک یکسانی قرار دارند استفاده شده و شبیه به آدرس APIPA در IPv4 به شکل خودکار پیکربندی می‌شود. آدرس فوق با FE90::/10 آغاز می‌شود. 10 بیت اول رزرو شده پیشوند ثابت بوده (10 1110 1111) و 54 بیت باقی‌مانده در پیشوند 64 بیتی همگی صفر هستند. از این‌رو یک پیشوند آدرس لینک محلی همان‌گونه که در تصویر بالا مشاهده می‌کنید در اغلب موارد به صورت FE80::/64 نوشته می‌شود. شما نباید از آدرس‌های لینک محلی روی بستر اینترنت استفاده کنید.

multicast address: این آدرس‌ها بسته‌ها را به همه گره‌ها یا گروهی از گره‌ها در مقصد تحویل می‌دهند.

anycast address: این آدرس‌ها برای شناسایی مقصدهای چندگانه استفاده شده و بسته‌ها را به نزدیک‌ترین مقصد تحویل می‌دهند. به‌طور مثال، یک سرور سامانه نام دامنه ممکن است یک درخواست سامانه نام دامنه را برای یک گروه از سرورهای سامانه نام دامنه که همه آن‌ها دارای آدرس پیش‌فرض هستند ارسال کند. یک روتر که در حال پردازش درخواست‌ها است، مسیریابی منتهی به همه سرورهای سامانه نام دامنه که درون یک گروه قرار دارند را آزمایش کرده و درخواست را به نزدیک‌ترین سرور هدایت می‌کند.

به شما گفتیم در پروتکل IPv4 زمانی که عمل همه‌پخش (broadcasting) انجام می‌شود، پیام‌ها برای هر گره‌ای روی شبکه ارسال می‌شود. اما در پروتکل IPv6 برای کاهش ترافیک شبکه همه‌پخش حذف شده است. در شکل زیر مفاهیم چندپخش، همه‌پخش، تک‌یابی، هریابی و نحوه اتصال گره‌ها به یکدیگر نشان داده شده است. در شکل زیر

هر نقطه سبز رنگ بیانگر یک گره ارسال کننده است. نقاط زرد رنگ گره‌هایی هستند که دریافت کننده بوده و نقاط آبی رنگ سایر گره‌های شبکه هستند که در فرآیند انتقال هیچ بسته‌ای دریافت نمی‌کنند.



در جدول زیر فهرستی از پیشوندهای مربوط به آدرس‌های فعلی IPv6 را مشاهده می‌کنید. دقت کنید در جدول زیر آدرس‌های یونیکست محلی که با لینک‌های محلی کار می‌کنند به آدرس‌های آی‌پی خصوصی در پروتکل IPv4 شباهت زیادی دارند. شما می‌توانید از فرمان ipconfig برای مشاهده آدرس‌های IPv4 و IPv6 که به همه ارتباطات روی کامپیوتر تخصیص داده شده‌اند استفاده کنید.

پیشوند آدرس‌های پروتکل IPv6

نوع آدرس آی‌پی	پیشوند آدرس	توضیحات
Global unicast	3::2000	First 3 bits are always 001
Link local unicast	FE80::/64	First 64 bits are always 1111 1110 1000 0000 0000 0000 0000
Unique local unicast	FC00::/7	First 7 bits are always 1111 110
	FD00::/8	First 8 bits are always 1111 1101
Multicast	FF00::/8	First 8 bits are always 1111 1111

در مثال زیر چهار آدرس آی‌پی به یک ارتباط فیزیکی روی یک لپ‌تاپ تخصیص داده شده است.

```

C:\Users\MikeandJill>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::64d2:bd2e:fa62:b91138
    IPv4 Address. . . . . : 192.168.2.163
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Wireless LAN adapter Local Area Connection* 15:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::28c5:6548:7ba0:b92c57
    IPv4 Address. . . . . : 192.168.2.115
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Tunnel adapter Local Area Connection* 14:

    Connection-specific DNS Suffix . : 
    IPv6 Address. . . . . : 2001:0:9d38:6ab8:382e:faf3:e768:3ac1
    Link-local IPv6 Address . . . . . : fe80::302e:faf3:e768:3ac1310
    Default Gateway . . . . . : ::

C:\Users\MikeandJill>

```

آدرس IPv6 تخصیص داده شده به یک رابط اترنت

آدرس IPv4 تخصیص داده شده به یک رابط اترنت

آدرس IPv6 تخصیص داده شده به یک رابط وای فای

آدرس آی پی IPv4 تخصیص داده شده به یک رابط بی سیم

فرمان ipconfig آدرس های آی پی IPv4 و IPv6 تخصیص داده شده به یک کامپیوتر را نشان می دهند.

پیکربندی خودکار IPv6

مکانیزم آدرس دهی IPv6 به این شکل طراحی شده است تا یک کامپیوتر بتواند به شکل خودکار آدرس آی پی پیوند محلی خود را بدون آن که نیازی به کمک سرور DHCPv6 داشته باشد تنظیم کند. این رویکرد شبیه حالتی است که IPv4 از APIPA استفاده می کند. در مکانیزم پیکربندی خودکار زمانی که یک کامپیوتر از IPv6 استفاده می کند در ابتدا یک ارتباط شبکه ای را به شرح زیر ایجاد می کند.

گام 1: کامپیوتر آدرس IPv6 خودش را ایجاد می کند. از FE80::/64 به عنوان 64 بیت اول استفاده کرده که پیشنهاد نامیده می شوند. بسته به نحوه پیکربندی سیستم عامل، 64 بیت آخر که شناسه رابط نام دارند می توانند به یکی از دو روش زیر ایجاد شوند:

- 64 بیت به شکل تصادفی تولید می شوند. در این حالت یک آدرس آی پی به نام آدرس آی پی موقت شناخته شده و هرگز در سامانه نام دامنه ثبت نشده یا برای تولید آدرس های جهانی برای اتصال به اینترنت استفاده نخواهد شد. این آدرس آی پی در اغلب موارد برای اجتناب از شناسایی و هک شدن کامپیوتر تغییر پیدا می کند. این روش پیش فرضی است که ویندوز 10 از آن استفاده می کند.
- 64 بیت از سوی مک آدرس آداپتور شبکه تولید می شود. مک آدرس ها 48 بیتی هستند و باید به استاندارد 64 بیتی که به آن EUI-64 (64 به آن) بیت توسعه یافته منحصر به فرد) می گویند تبدیل شوند. برای تولید یک شناسه واسط، سیستم عامل 48 بیت آدرس مک یک دستگاه را دریافت کرده و 16 بیت به میانه این 48 بیت اضافه کرده و مقدار بیت هفتم را معکوس می کند.

گام 2: کامپیوتر مطمئن می شود یک آدرس آی پی منحصر به فرد در شبکه در اختیار دارد.

گام 3: کامپیوتر این سوال را مطرح می کند که آیا روتری در شبکه وجود دارد تا اطلاعات پیکربندی را ارائه کند. این پیام به نام درخواست از روتر (RS) نامیده می شود. اگر روتر پاسخی که شامل اطلاعات پروتکل پیکربندی پویا میزبان بوده و RA نامیده می شود را ارائه کند، کامپیوتر از هرگونه اطلاعاتی همچون آدرس های آی پی سرور سامانه نامه دامنه یا پیشنهادهای شبکه استفاده می کند. این فرآیند، کشف پیشنهادهای نام داشته و به کامپیوتر اجازه می دهد از

پیشوند برای تولید لینک محلی خودش استفاده کرده یا از آدرس IPv6 جهانی با اضافه کردن شناسه واسط (interface ID) خودش به پیشوند استفاده کند. از آنجایی که یک کامپیوتر می‌تواند لینک محلی خود یا آدرس آی‌پی جهانی را استفاده کند، سرور DHCPV6 به‌طور معمول فقط به آدرس‌های IPv6 که میزبان‌ها برای دریافت آدرس ثابت به آن نیاز دارند رسیدگی کرده و این آدرس‌ها را در اختیارشان قرار می‌دهد. به‌طور مثال، وب‌سرور و سرورهای سامانه نام دامنه می‌توانند آدرس‌های IPv6 ایستا خودشان را از سرور DHCPV6 دریافت کنند.

نکته: در شبکه‌های بزرگ، فرآیند تخصیص آدرس آی‌پی و همچنین زیرساخت آدرس آی‌پی به سرعت می‌توانند به یک موجودیت پیچیده و خارج از کنترل تبدیل شوند. یک سامانه مدیریت آدرس آی‌پی (IPAM) سرنام IP address management system به عنوان یک محصول مستقل یا جایگذاری شده درون محصولاتی دیگری همچون ویندوز سرور می‌تواند فرآیند برنامه‌ریزی، استقرار و نظارت بر محدوده آدرس‌دهی آی‌پی درون یک شبکه را عهده‌دار شود. ابزارهای IPAM می‌توانند به شکل خودکار محدوده آدرس آی‌پی را تشخیص داده، رزرو کرده، تفکیک کرده، موارد استثنا را مشخص کرده و اطلاعات را با رکوردهای سامانه نام دامنه یکپارچه کرده و در نهایت یک نظارت مستمر بر مباحث امنیتی، بزرگ شدن شبکه و اشکال‌زدایی ارائه کنند.

این سند به‌عنوان یک راهنمای کلی برای درک مفاهیم و روش‌های مدیریت آدرس آی‌پی در شبکه‌های بزرگ ارائه شده است. برای اطلاعات بیشتر، لطفاً به منابع زیر مراجعه کنید.

تاریخ انتشار:

28 مهر 1398

نشانی منبع:

<https://www.shabakeh-mag.com/networking-technology/14593/%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%DA%A9%D8%A7%D9%85%D9%84-%D8%A8%D8%A7-%D8%A7%D9%86%D9%88%D8%A7%D8%B9-%D8%A2%D8%AF%D8%B1%D8%B3%E2%80%8C-%D8%A2%DB%8C%E2%80%8C%D9%BE%DB%8C-ipv4-%D9%88-ipv6>