۱-۱ توضیحاتی بیشتر در مورد Mac Address

همانطور که اشاره شد، یکی از وظایف لایه ۲ مدل OSIتخصیص آدرس دهی فیزیکی است که به آن MAC Address هم گفته می‌شود.

از وظایف دیگر لایه ۲ می توان از کنترل نوبت دسترسی[۱] نام برد. مکانیزمی که کنترل می کند که به صورت صحیح و منصفانه، رسانه ارتباطی در اختیار ماشین‌های مختلف در گره قرار گیرد. مهمترین مثال‌ها در این مورد را بررسی کردیم. روش CSMA/CD در توپولوژی‌های گذرگاه و ستاره‌ای و همچنین استفاده از Token در توپولوژی حلقه. وظیفه مهم دیگر در لایه ۲، تشخیص خطا است و همچنین کپسوله کردن و باز کردن داده‌ها.

اما در مورد آدرس فیزیکییا MAC Address بیشتر صحبت می‌کنیم. هر آداپتور شبکه ای که در یک شبکه استفاده می‌شود، دارای یک آدرس به شکل یک عدد ۴۸ بیتی است. این آدرس توسط کارخانه سازنده به آن سخت‌افزار نسبت داده می‌شود. به همین دلیل است که به این آدرس، آدرس فیزیکی گفته می‌شود. به دلیل یکتا بودن این آدرس به آن، آدرس مدیریت شده جهانی[۲] یا به اختصار UAA نیز گفته می‌شود. برای اینکه این شماره منحصر به فرد بماند، این آدرس تحت نظارت و استانداردهای انجمن مهندسان الکتریک و الکترونیک[۳] (IEEE) تولید می‌شود. به این ترتیب که این آدرس ۴۸ بیتی به دو قسمت ۲۴ بیتی تقسیم می‌گردد.

۱.Arbitration

۲.Universally Administrated Address

۳.Institute of Electrical and Electronical Engineers

به ۲۴ بیت سمت چپ آدرس شناسه یکتای سازمانی[۱] یا به اختصار OUI گفته می‌شود. هر تولید کننده‌ای که بخواهد آداپتور شبکه تولید کند باید از IEEE یک OUI دریافت کند و به عنوان ۲۴ بیت اول آدرس سخت‌افزارهای شبکه خود بایستی از آن OUI استفاده کند. به این ترتیب آن تولید کننده با تغییر اعداد در ۲۴ بیت دوم آدرس می تواند تا 2^{24} آداپتور شبکه تولید نماید. در صورتی که یک کارخانه آنقدر بزرگ باشد که تعداد محصولاتش از 2^{24} که بیش از ۱۶ میلیون عدد می‌شود، فراتر رود. بایستی مجددا یک OUI جدید از IEEE دریافت نماید.

آدرس های ۴۸ بیتی فیزیکی، معمولا در مبنای ۱۶ نوشته می شود. برای مثال یک آدرس در محیط سیستم عامل ویندوز می‌تواند به شکل 30-85-A9-90-DF-54باشد. همین آدرس در دستگاه‌های سیسکو معمولا به شکل 3085-A990-DF54 نمایش داده می‌شود.

می‌توانید با جستجوی عبارت «MAC Address and OUI Lookup» در گوگل، سایت‌هایی را بیابید که با ورود ۲۴ بیت اول آدرس فیزیکی نام کارخانه سازنده آداپتور شبکه را اعلامی می کنند.

برای دیدن MAC Address در کامپیوتر شخصی می توان در محیط Command از دستور getmac استفاده نمود. برای این منظور می توانیم این اعمال را انجام دهید:

Windows+R → cmd → getmac

در این دستور شما تنها شماره آدرس‌ها را می‌بینید و مشخص نیست که این آدرس‌ها متعلق به کدام دستگاه از ماشین هستند. اما استفاده از دستور زیر اطلاعات بیشتری به ما می‌دهد:

---

۱. Organizationally Unique Identifier

Windows+R → cmd → ipconfig/all

برای اینکه اطلاعات آدرس‌های فیزیکی در یک فایل متن ذخیره گردد، می توان از دستور زیر استفاده نمود:

Windows+R → cmd → ipconfig/all>c:\file.txt

البته نام و مسیر فایل می‌تواند دلخواه باشد.

برای دسترسی به تنظیمات کارت‌های شبکه می‌توان از این دستور استفاده نمود:

Windows+R → ncpa.cpl

و یا از قسمت شبکه در کنترل پنل به آن دسترسی پیدا کرد.

۲-۱ نگاهی به یک فریم در لایه ۲

در لایه پیوند داده‌ها فریمی استفاده می‌شود که با وجود اینکه در استانداردهای مختلف تفاوت‌هایی دارد، اما در استاندارد شماره 802.3 از IEEE که به آن فریم اترنت هم گفته می‌شود، به شکل زیر است:

Preamble 7	SFD 1	Destination 6	Source 6	Length 2	Data and Pad 46-1500	FCS 4

اعداد در هر فیلد، اندازه آن فیلد بر حسب بایت است.

Preamble برای همگام (Sync) شدن مبدا و مقصد تعدادی بیت از سمت مبدا ارسال می‌گردد. تا مقصد خود را با نرخ ارسال داده ها در فرستنده همگام کند. اندازه این داده ها ۷ بایت است. درون هر بایت از این بخش داده 01010101 ارسال می‌گردد. به دلیل اینکه نمی‌تواند ممکن است در عملیات همگام سازی بیتی‌هایی عقب و جلو شوند. روش شمارش بیت‌ها از طرف گیرنده برای فهمیدن پایان این فیلد، ممکن است با مشکل موجه شود.این است که بایت بعدی که SFD[۱] نام دارد، برای پایان دادن به بخش همگام‌سازی و نشان آغاز فریم اصلی است.این فیلد دارای یک ساختار ثابت 01010111 است. که در ۷ بیت قبلی این قالب وجود ندارد. گیرنده با دریافت این قالب متوجه می‌شود که بخش همگام سازی به پایان رسیده است. پس از آن دو فیلد ۶ بایتی هست که Mac Address مقصد و مبدا در آن‌ها وجود دارد. فیلد ۲ بایتی بعدی Length نام دارد کهبه معنای طول داده فریم می‌باشد.

در اترنت اولیه این فیلدType یا PTF[۲]نام داشت که مشخص می‌کرد که در لایه بالایی چه پروتکلی وجود دارد. هر پروتکل دارای یک کد در مبنای ۱۶ است. برای مثال کد مربوط به پروتکل IP عدد 0800 و کد پروتکل ARP عدد 0806 می‌باشد. برای اینکهگاهی PTF و گاهی طول فریم مد نظر بود، قرار بر این شد که هر گاه در این فریم عددی کمتر از 0600 (در مبنای ۱۶) قرار داشته باشد. این عدد به معنای طول داده در فریم است. اما اعداد بیشتر به معنای PTF هستند.

---

۱. Start Frame Delimiter

۲. Protocol Type Field

تا اینجا سرآیند فریم بود. پس از آن داده اصلی قرار دارد. در انتهای فریم یک فیلد چهار بایتی به نام FCS[1] وجود دارد که کد تشخیص خطا است. این فیلد که در حقیقت پی‌آیند فریم است، به این ترتیب محاسبه می‌گردد که پس از تولید فریم در مبدا و پیش از ارسال آن، از بخش سرآیند با الگوریتمی تحت عنوان CRC[2] یک عدد چهار بایتی تولید می کند (همان FCS) و آن را در انتخای فریم ارسال می نماید. گیرنده با دریافت بسته، مجددا سرآیند را تحت محاسبه با الگوریتم CRC قرار می‌دهد و FCS را مجددا تولید می‌کند. اگر FCS ارسالی از سوی مبدا و FCS تولید شده در مقصد – که می تواند یک سوییچ یا مقصد نهایی باشد – یکی نبود، یعنی داده‌ها در مسیر انتقال با خطا مواجه شده‌اند. یعنی برخی از صفرها و یک‌ها تغییر یافته اند. این حالت خطا می‌تواند به خاطر رخ دادن حالت برخورد ایجاد شود یا القای بار جانبی یا اصطلاحا Cross Talk وجود داشته باشد. القای بار جانبیدر حالتی رخ می‌دهد که یک منبع تولید نویز مانند یک کابل برق یا یک دستگاه تلفن همراه در نزدیکی رسانه انتقال باشد و روی داده‌های ارسالی از آن، خطا ایجاد کند. در زوج سیم‌های به هم تابیده، اثر القای بار جانبی تا حد زیادی محدود می‌گردد. به هم تابیده شدن سیم‌ها باعث ایجاد سپری در برابر القای بار جانبی می‌شود. اما اگر منبع القا، قوی باشد، باز هم احتمال ایجاد خطا وجود دارد.

در استاندارد بعدی که برای تکمیل این فریم توسط IEEE که با شماره 802.2 مشخص گردید، به سرآیند فیلدهایی اضافه شد.

---

[1]. Frame CheckSum

[2]. Cyclic Redundancy Check

Preamble 7	SFD 1	Destination 6	Source 6	Length 2	DSAP 1	SSAP 1	CTL 1	OUI 3	Type 2	Data and Pad 46-1500	FCS 4

فیلدهای DSAP[1]، SSAP[2] و CTL یا Control در مجموع به نام سرآیند LLC[3] نام گرفتند و دو فیلد OUI و Type هم سرآیند SNAP[4] نامیده شدند. هر چند سرآیند LLC گسترش چبدا نکرد و در حد نشانه‌ای برای این شد که مشخص شود که سرآیند از کدام استاندارد است. به این ترتیب که اگر مقدار AA در DSAP و SSAP و مقدار 03 در CTRL قرار داشته باشد. مشخص می‌شود که بعد از آن سرآیند SNAP وجود دارد که در آن، همان‌گونه که گفته شد، OUI نام کارخانه سازنده و Type پروتکل لایه بالایی را مشخص می‌سازد.

[1].Destination Service Access Point

[2].Source Service Access Point

[3].Logical Link Control Header

[4].Sub Network Access Protocol Header

در این فصل به لایه های شبکه و بحث بیشتری درباره لایه ۲ یعنی لایه پیوند داده ها پرداختیم. در فصل بعدی به سراغ لایه شبکه که می توان گفت مهمترین لایه در شبکه های کامپیوتری است خواهیم رفت.

۲ فصل دوم: لایه شبکه

در فصل قبل مفاهیم اولیه شبکه و لایه ها را مرور کردیم و درباره لایه پیوند داده ها صحبت نمودیم. در این فصل به سرغ لایه مهم شبکه، لایه شماره ۳ از مدل استاندارد OSI می‌رویم. در لایه ۳ آدرس‌دهی منطقی[۱]، مسیریابی[۲]، تشخیص خطا و کپسوله‌سازی انجام می‌پذیرد. مفهوم کپسوله سازی مانند لایه ۲ است. به این معنی که قطعه داده دریافتی از لایه بالاتر را در قالب بسته یا Packet کپسوله می‌کند. این عمل با افزودن سرآیند انجام می‌پذیرد. بسته لایه شبکه برخلاف فریم لایه ۲ پی‌آیند ندارد.

تشخیص خطا نیز مانند لایه ۲ است. اما کد تشخیص خطا در سرآیند قرار دارد نه در پی‌آیند. زیرا همانطور که گفتیم در بسته لایه شبکه، پی‌آیند نداریم. اما دو مورد دیگر یعنی آدرس‌دهی منطقی و مسیریابی، مهمترین اعمال در لایه شبکه هستند که به آن‌ها خواهیم پرداخت.

۲-۱ آدرس‌دهی منطقی

در این بخش ابتدا مشخص می‌کنیم که به چه دلیل به آدرس دهی منطقی نیاز داریم و آدرس دهی فیزیکی در لایه ۲ کافی نیست.

---

[۱].Logical Addressing

[۲].Routing

همانطور که در فصل قبلی دیدیم، هر آداپتور شبکه دارای یک آدرس فیزیکی منحصر به فرد می‌باشد. اما این آدرس معمولا در محدوده شبکه‌های محلی یا LANبه کار می‌رود. در بسیاری از موارد در شبکه محلی آدرس‌های MAC به صورت مجازی برای دستگاه‌هایی که فاقد آدرس فیزیکی هستند ساخته می‌شود تا قابل دسترسی باشند. این عمل چون در محدوده شبکه‌های محلی انجام می‌پذیرد، دیگر تضمین کننده یکتا بودن آدرس‌های MAC نیست. به عبارت دیگر ممکن است در دو شبکه محلی مختلف آدرس MAC یکسان وجود داشته باشند. تا زمانی که هر شبکه محلی مستقل برای خود کار کند. مشکلی پدید نمی‌آید. اما زمانی که چند شبکه محلی به هم متصل می‌شوند و شبکه سراسری[1] یا WAN به وجود می‌آید، دیگر آدرس‌های MAC نمی‌توانند مرجع مناسبی برای آدرس دهی باشند. به همین دلیل در لایه سوم که محدوده کاریش از شبکه محلی فراتر رفته است، آدرس‌دهی دیگری به عنوان آدرس‌دهی منطقی مورد استفاده قرار می‌گیرد. یکی از مهم‌ترین و بزرگترین شبکه‌های سراسری، اینترنت است. اینترنت بزرگترین نوع موجود اتصال تعداد زیادی شبکه محلی و سراسری است. در اینترنت و اکثر شبکه‌های دیگر برای آدرس‌های‌دهی منطقی از پروتکل اینترنت[2] یا IP استفاده می‌شود. به همین دلیل در بسیاری از موارد به جای آدرس منطقی، از واژه آدرس IP استفاده می‌شود.

در حال حاضر دو نسخه ۴ و ۶ از IP مورد استفاده قرار می‌گیرد. IPV4 دارای طول ۴ بایت و IPV6 دارای ۱۶ بایت طول است. بین این دو نسخه،

---

[1].Wide Area Network

[2].Internet Protocol

نسخه ۵ به وجود آمد که در مدت کوتاهی به دلیل اشکالاتی که داشت، منسوخ شد. در حال حاضر نسخه ۴ به صورت وسیعی توسط کاربران نهایی مورد استفاده قرار می‌گیرد. ولی نسخه ۶ در مراکز ارتباطی و سرویس دهی اینترنت مانندISP[1]ها مورد استفاده قرار می‌گیرد.

نسخه ۴ IP معمولا به شکل ۴ عدد پشت سر هم به نشانه ۴ بایت آن، نمایش داده می شود. مانند: 192.168.200.21

به دلیل اینکه هر عدد نماینده هشت بیت است اصطلاحا گفته می‌شود که IPV4 از ۴ هشت تایی یا Octet تشکیل شده است. معمولا این آدرس ۳۲ بیتی به دو قسمت اصلی تقسیم می‌شود. تعدادی از بیت‌های سمت چپ (پر ارزش) این آدرس به عنوان شناسه شبکه (Net ID) و بقیه بیت‌ها به عنوان شناسه میزبان (Host ID) شناخته می‌شود. میزبان، یک ماشین در شبکه است که دارای یک آدرس مجزا باشد. ممکن است یک کامپیوتر تنها باشد یا ماشینی که به یک شبکه محلی متصل است و از طریق آن کل ماشین‌های درون آن شبکه محلی به اینترنت متصل می‌شوند.

برای اینکه مشخص شود که چه میزان از آدرس IP مربوط به شبکه و چقدر مربوط به میزبان یا ماشین‌های کاربر انتهایی هستند، دو روش وجود دارد:

- نماد پیشوندی[2]: به این ترتیب مورد استفاده قرار می‌گیرد که با یک عدد در انتهای آدرس، تعداد بیتهای بخش پیشوند که همان شناسه شبکه است را مشخص می‌نماید. برای نمونه، آدرس

[1].Internet Service Provider

[2].Prefix Notation

192.168.200.21/24 مشخص می‌نماید که در این آدرس ۲۴ بیت به شناسه شبکه و ۸ بیت به شناسه میزبان تعلق دارد.

- ماسک زیر شبکه[۱]: در کنار آدرس ۳۲ بیتی اصلی، یک آدرس ۳۲ بیتی دیگر به عنوان ماسک در نظر گرفته می‌شود. در این ماسک به جای بیت‌های بخش شناسه شبکه، یک و به جای بیت‌های بخش شناسه میزبان، صفر قرار می گیرد. مثلا ماسک زیرشبکه 255.255.255.0 نشان می دهد که ۲۴ بیت یکو ۸ بیت صفر است (عدد ۲۵۵ در مبنای۲ برابر ۸ رقم ۱ است). بنابر این ۲۴ بیت شناسه شبکه و ۸ بیت شناسه میزبان وجود دارد.

در آدرس دهی شناسه میزبان، قرار دادی وجود دارد که زمانی یک آدرس معتبر[۲] ، بیت‌های این شناسه همگی صفر یا همگی یک نبایند باشند.برای نمونه اگر در یک شبکه، شناسه شبکه 193.169.200 باشد. آدرس‌های معتبر از 193.169.200.1 تا 193.169.200.254 خواهند بود. آدرسهای 193.169.200.0 و 193.169.200.255 به آدرس‌های نامعتبر[۳] برای میزبان‌های آن شبکه خواهند بود. آدرس 193.169.200.0 به آدرس شبکه معروف است و شبکه با آن شناخته می‌شود. و آدرس 193.169.200.255 به آدرس پخش همگانی[۴]

---

۱. Subnet Mask

۲. Valid

۳. Invalid

۴. Broadcast

معروف است و زمانی به کار می‌رود که بسته‌ای به مقصد همه میزبان‌های آن شبکه ارسال گردد.

در ابتدا برای آدرسهای IP چند کلاس در نظر گرفته شد:

- کلاس A: برای شناسایی این کلاس، اولین بایت آدرس بین ۱ و ۱۲۶ می‌تواند باشد. در آدرس‌های متعلق به این کلاس، شناسه شبکه آن ۸ بیت و شناسه میزبان ۲۴ بیت است.
- کلاس B: اولین بایت آدرس در این کلاس،بین ۱۲۸ و ۱۹۱است و شناسه شبکه آن ۱۶ بیت و شناسه میزبان ۱۶ بیت است.
- کلاس C: اولین بایت آدرس در این کلاس، بین ۱۹۲ و ۲۲۳ است و شناسه شبکه آن ۲۴ بیت و شناسه میزبان ۸ بیت است.
- کلاس D: اولین بایت آدرس در این کلاس، بین ۲۲۴ و ۲۳۹ است. این کلاس برای ارتباطات گروهی[۱] رزرو شد.
- کلاس E: اولین بایت آدرس در این کلاس، بین ۲۴۰ و ۲۵۴ است.این کلاس برای مصارف تحقیقاتی و آزمایشی رزرو شد.

البته در حال حاضر این کلاس‌ها به شکل کامل استفاده نمی شود. به این دلیل که در بسیاری از شبکه ها به ویژه در کلاسهای A و B تعدادی از آدرس‌های رزرو شده برای میزبانها، بلا استفاده می‌ماند. برای مثال فرض کنید که یک موسسه یک شبکه در کلاس B خریداری کند. در کلاس B

[۱]. Multicasting

که شناسه میزبان آن ۱۶ بیت است، می تواند حدود 2^{16}میزبان در این شبکه داشته باشد. این یعنی بیش از ۶۵هزار میزبان؛ که ممکن است این تعداد میزبان در آن شبکه نباشد.

به این ترتیب یک شبکه به چندین زیر شبکه تقسیم شد و در اختیار کاربران متفاوت قرار داده شد و کم کم آدرس‌های بدون کلاس شکل گرفت.

یک آدرس IP می تواند عمومی[۱] یا خصوصی[۲] باشد. یک آدرس خصوصی درون یک شبکه استفاده می‌شود و از فضای خارج یک شبکه مانند اینترنت قابل دسترسی نیست. اما آدرس عمومی یک آدرس منحصر به فرد است که از خارج شبکه هم در دسترس است. با این آدرس از هرجای اینترنت با آن میزبان می توان تماس برقرار نمود.برای اینکه منحصر به فرد بودن آدرس‌های عمومی مراجعی وجود دارند که استفاده کنندگان اینترنت مانند ISP ها از این مراجع تعدادی آدرس عمومی دریافت می‌کنند و در اختیار کاربرانشان قرار می‌دهند. این مراجع با این نامها شناخته می‌شوند: IETF[۳]، ICANN[۴] و IANA[۵]

آدرس‌های خصوصی که در یک شبکه قرار می گیرند، در دامنه خاصی قرار دارند. سه دامنه برای آدرس‌های خصوصی متناظر با سه کلاس عمومی A، B و C داریم که به شرح زیر است:

- 10.0.0.0/8 به این معنی که حوزه آدرس‌های مورد استفاده آن از 10.0.0.0 تا 10.255.255.255 است.

---

۱. Public

۲. Private

۳. Internet Engineering Task Force

۴. Internet Corporation for Assigned Names and Numbers

۵. Internet Assigned Numbers Authority

- 172.16.0.0/12 به این معنی که حوزه آدرس‌های مورد استفاده آن از 172.16.0.0 تا 172.31.255.255 است.
- 192.168.0.0/24 به این معنی که حوزه آدرس‌های مورد استفاده آن از 192.168.0.0 تا 192.168.255.255 است.

دقت کنید که در گفتار عمومی معمولا از واژه آدرس معتبراشتباها به جای آدرس عمومی استفاده می‌شود.

در حال حاضر زمانی که یک آدرس شبکه از یکی از مراجعی که گفته شد گرفته می‌شود، می‌تواند به چند زیر کلاس تقسیم شود تا از آن استفاده بهتری گردد. به این عمل CIDR[1] گفته می‌شود که به دو روش انجام می‌گردد. روش اول SLSM[2] است که در آن شبکه به چند زیرشبکه مساوی تقسیم می‌گردد و روش دوم VLSM[3]نام دارد که در آن دامنه‌هایی که به زیرشبکه‌ها اختصاص می‌یابد، اندازه های متفاوت دارند. مدل اول معمولا زمانی استفاده می‌گردد که تعداد میزبان‌ها در زیر شبکه ها نزدیک به هم باشند و مدل دوم در زمانی استفاده می‌شود که تعداد کاربران در زیر شبکه ها با هم اختلاف داشته باشند و می‌خواهیم از آدرس‌های IP موجود، استفاده بهینه بکنیم.
برای نمونه فرض کنید که شبکه دارای آدرس 193.170.32.0/24 است که در آن ۸ بیت برای شناسه میزبان درنظر گرفته شده است. می

[1]. Classless Inter Domain Routing

[2]. Same Length Subnet Mask

[3]. Variable Length Subnet Mask

خواهیم با روش SLSM آن را به چهار زیر شبکه تقسیم نماییم. در این حالت آدرس جدیددرون شبکه به193.170.32.0/26 تبدیل می گردد و ماسک زیرشبکه آن 255.255.255.192 خواهد بود. به عبارت دیگر تعداد بیت‌های اختصاص یافته به شنایه میزبان ۶ بیت می‌باشد. کل IP ها درشبکه اصلی $۲^{۸}$ یا ۲۵۶ بود که از آنها ۲۵۴ تایش معتبر بود. در این حالت که چهار زیرشبکه مساوی داریم، در هر یک از چهار دامنه زیر شبکه $۲^{۶}$ یا ۶۴ آدرس IP خواهیم داشت که ۶۲ تا از آن‌ها معتبر است. محدوده IP های معتبر در این چهار دامنه به شرح زیر خواهد بود:

Range 1: 193.170.32.1 – 193.170.32.62
Range 2: 193.170.32.65 – 193.170.32.126
Range 3: 193.170.32.129 – 193.170.32.190
Range 4: 193.170.32.193 – 193.170.32.254

در این حالت گفته می‌شود که پرش‌ها در این زیر شبکه ۶۴ تایی است. به این معنی که آغاز آدرس‌های میزبان در هر زیر شبکه با زیر شبکه بعدی ۶۴ عدد تفاوت دارد.

حال فرض کنید که می خواهیم در همین شبکه به آدرس 193.170.32.0/24 سه زیر شبکه داشته باشیم که در هر کدام ۱۰۰، ۵۰ و ۱۵ میزبان وجود داشته باشد. واضح است که با روش SLSM نمی توان این کار را کرد. در اینجا به سراغ روش VLSM می‌رویم که در آن تعداد میزبان‌ها در زیر شبکه‌ها می‌توانند متفاوت باشند. در این روش، طراح شبکه، برای هر زیر شبکه، دامنه‌ای با محدوده جداگانه محاسبه می کند. در اینجا این محاسبات را می‌بینیم.

Range 1:

Hosts: 100 → IP Required: 100+2=102 → 64>102>128 →2^6>102>2^7→ Host ID bits: 7 bit
Subnet Address: 192.170.32.0/25, Subnet Mask: 255.255.255.128
Hop: 128
Range 1 Valid IPs: 192.170.32.1 – 192.170.32.127
Range2:
Hosts: 50 → IP Required: 50+2=52 → 32>52>64 →2^5>52>2^6→ Host ID bits: 6 bit
Subnet Address: 192.170.32.0/26, Subnet Mask: 255.255.255.192
Hop: 64
Range 2 Valid IPs: 192.170.32.129 – 192.170.32.190
Range3:
Hosts: 15 → IP Required: 15+2=17 → 16>17>32 →2^4>52>2^5→ Host ID bits: 5 bit
Subnet Address: 192.170.32.0/27, Subnet Mask: 255.255.255.224
Hop: 32
Range 3 Valid IPs: 192.170.32.193 – 192.170.32.222

مشخص است که هنوز IP ها به پایان نرسیده و هنوز هم می توان زیر شبکه‌دیگری هم ساخت. دیده می‌شود که در این روش محاسبات کمی پیچیده‌تر است. اما از دامنه‌های آدرس IP بهتر استفاده می‌شود.

۲-۲ پروتکل ARP[1]

[1]. Address Resolution Protocol

همانطور که گفته شد، در لایه ۳ آدرس‌های مبدا و مقصد بر اساس آدرسهای IP شناخته می‌شوند. اما در لایه ۲ این آدرس‌های MAC هستند که مبدا و مقصد را مشخص می کنند. اگر فرستنده یک بسته اطلاعاتی آدرس IP مقصد را داشته باشد. لزوما آدرس MAC آن را نخواهد داشت. دقت کنید که دیگر لزومی ندارد که فرستنده و گیرنده در یک شبکه محلی باشند و بینشان یک سوییچ باشد که هدایتشان کند. ممکن است مبدا و مقصد در دو شبکه جداگانه اما متصل به هم باشند و بینشان چندین سوییچ و مسیریاب قرار داشته باشد. بنابر این به روش یا پروتکلی نیاز است که بوسیله آن بتوان به آدرس MAC مربوط به یک آدرس IP رسید. پروتکل ARP در اینترنت و اکثر شبکه های سراسری دیگر به همین منظور استفاده می‌گردد.

بسته از مبدا به کمک آدرس IP و توسط مسیریاب‌ها به سمت شبکه مقصد هدایت می‌شود (چون از آدرس IP آدرس شبکه مشخص می‌گردد). بسته به جایی می رسد که درون شبکه مقصد است و باید به میزبان نهایی برسد. در اینجا سویچهای درون شبکه باید بسته را به مقصد برسانند و آن‌ها هم از طریق آدرس MAC این‌کار را انجام می‌دهند. در این حالت اگر آدرس Mac مقصد موجود نباشد، بسته اصلی نگاه داشته می‌شود و پروتکل ARP اجرا می‌گردد.

پروتکل ARP یک پروتکل لایه ۳ است. زمانی که پیام ARP به لایه ۲ می رسد، فریم ارسالی در آدرس مبدأ، آدرس MAC فرستنده را دارد اما در آدرس مقصد از ۴۸ بیت ۱ یا به عبارتی از عدد FF:FF:FF:FF:FF:FF

استفاده می کند. این آدرس، نشانه پخش همگانی[1] است. سوییچی که این بسته را دریافت می‌کند متوجه می‌شود که این بسته باید به همه ارسال شود. به دلیل اینکه در قسمت Type از فریم کد ARP قرار دارد. هر ماشین گیرنده متوجه می‌شود که باید بررسی کند که اگر این آدرس به مقصد او بود، پاسخ دهد. این است که به داده لایه ۳ مراجعه می‌شود و آدرس IP مقصد را استخراج می‌کند. اگر آدرس خودش بود، بسته را به همان شکل باز می‌گرداند، تنها آدرس MAC مبدا را به جای مقصد قرار داده و آدرس مبدا را با آدرس MAC خودش پر می کند. بسته باز می‌گردد و اینبار مبدا آدرس MAC مقصد را دارد و می‌تواند بسته اصلی را ارسال نماید. ضمنا این آدرس MAC مرتبط با آدرس IP در یک حافظه موقت به نام ARP Cache برای ارتباطات بعدی استفاده می‌شود. و تا زمانی که داده‌های این حافظه پاک یا نامعتبر نشوند، دیگر در آن مقصد خاص نیازی به استفاده از پروتکل ARP نیست. انتقال بسته های ARP علاوه بر پر شدن ARP Cache در ماشین‌ها، باعث پر شدن MAC Address Table در سوییچ‌ها نیز می‌گردد.

برای دیدن ARP Cache در کامپیوتر می‌توان در محیط Command از دستور arp –a و برای پاک کردن آن می‌توان از دستور arp –d استفاده نمود.

برای مشاهده MAC Address Table در یک سوییچ می‌توان از دستور زیر استفاده نمود.

```
Switch#show mac-address-table
```

[1]. Broadcast

۲-۳ پروتکل DHCP[۱]

این پروتکل به شکل یک سرویس در لایه ۳ استفاده می‌شود. با استفاده از این سرویس دیگر لازم نیست که برای ماشین‌ها در یک شبکه به صورت دستی آدرس IP تنظیم نمود. هر ماشین با آغاز اتصال به شبکه، با درخواست از سرور DHCP یک آدرس منحصر به فرد در آن شبکه دریافت می‌کند. برای اینکه در یک شبکه، کامپیوتر بتواند از یک سرور DHCP آدرس دریافت کند، بایستی در تنظیمات شبکه در قسمت

Network Connections → (Selected Network) → Properties → IPV4 → Properties

گزینه Obtain an IP Address Automatically انتخاب شده باشد.

در این حالت کامپیوتر در آغاز اتصال به شبکه آغاز به کشف DHCP[۲] می‌کنند. در این حالت پیام درخواست آدرس را به آدرس 255.255.255.255 می‌فرستد. این آدرس، مربوط به پخش همگانی است. پس همه دستگاه‌ها در شبکه آن را دریافت می‌کنند. از جمله مسیریابی در شبکه که سرور DHCP هم هست. در این حالت DHCP یک DHCP Offer باز می‌گرداند. به دلیل این‌که گیرنده هنوز آدرس IP معتبر ندارد. پیام ارسالی از طرف DHCP هم پخش همگانی می‌شود و به دست همه ماشین‌ها می‌رسد. حال ماشین یا ماشین‌هایی که نیاز به آدرس دارند، یک DHCP Request می‌فرستند.

---

۱. Dynamic Host Configuration Protocol

۲. DHCP Discovery

در هنگام تعریفDHCP توسط مدیر شبکه، یک آدرس زیر شبکه برایش تعریف می‌شود. برای نمونه 192.168.1.0/24 در این حالت اصطلاحا یک حوضچه[1] از آدرس‌های IP های معتبر برای این DHCP به وجود می‌آید.DHCP از این حوضچه در پاسخ هر DHCP Requestیک آدرس بر می‌دارد و در قالب یک DHCP Acknowledgment ارسال می‌کند. در این پیام مشخص می‌کند که برای کدام آدرس MAC، کدام آدرس IP در نظر گرفته شده است. DHCP به نحوی این عمل را انجام می‌دهد که درون شبکه آدرس تکراری ایجاد نشود.

[1]. Pool