۲-۳ آدرس‌دهی بدون کلاس (CIDR): Classless InterDomain Routing

در این شیوه‌ی آدرس‌دهی IP، مرز بین NetID و HostID از پیش تعین شده نیست (برخلاف کلاس‌های IP) بلکه یک عدد ۳۲ بیتی دیگری به نام الگوی زیر شبکه یا Subnet Mask وجود دارد که مشخص می‌کند چه بخشی از آدرس IP مربوط به NetID و چه بخشی مربوط به HostID است.

برای به دست آوردن آدرس شبکه، آدرس IP و Subnet Mask با هم and منطقی می‌شوند.(Boolean and) حاصل آدرس شبکه است.

∞ نکته: بیت‌های ۱ در Subnet Mask مشخص‌کننده‌ی بیت‌های مربوط به NetID هستند و بیت‌های صفر در آن مشخص‌کننده‌ی بیت‌های مربوط به HostID در آدرس IP هستند.

∞ نکته:

0 and y = 0

1 and y = y

مثال:

IP : 68.101.29.4

Subnet Mask : 255.0.0.0

NetID : 68.0.0.0

و به صورت باینری:

01000100 . 01100101 . 00011101 . 00000100

11111111 . 00000000 . 00000000 . 00000000

01000100 . 00000000 . 00000000 . 00000000

∞ نکته: اگر تعداد بیت‌های ۱ در **subnet mask** بعد از علامت / جلوی آدرس **IP** نوشته شود، این فرمت نمایش را فرمت پیشوندی یا **Prefix** گویند. بعنوان نمونه، آدرس **IP** و ماسک زیرشبکه آنرا در مثال قبل، می‌توان بصورت **68.101.29.4/8** می‌توان نمایش داد.

۲-۳-۱ کاربردهای عمده‌ی CIDR

- تقسیم یک شبکه به چند زیرشبکه (Subnetting)
- ترکیب چند شبکه و تشکیل یک شبکه‌ی واحد (Supernetting)

۲-۳-۱-۱ Subnetting

مثال برای Subnetting: می‌خواهیم شبکه‌ی زیر را به ۸ زیرشبکه تقسیم کنیم: 172.31.0.0/16

الف) محاسبه کنید Subnet Maskای را که این شبکه را به ۸ زیرشبکه تقسیم کند.

ب) آدرس ۸ زیر شبکه را به دست آورید.

ج) آدرس‌های Broad Cast آن‌ها را به دست آورید.

د) محدوده‌ی مجاز آدرس‌های هر زیر شبکه را به دست آورید.

جواب:

الف) برای ایجاد ۸ ادرس زیر شبکه به ۳ بیت نیاز داریم یعنی باید ۳ بیت از HostID کم کنیم و به NetID اضافه نماییم.

$2^3 = 8$ 3 bit

16+3=19

172.31.0.0/19

Subnet Mask: 255.255.224.0 11100000=224

ب و ج)

172.31.00000000.00000000	172.31.0.0	172.31.31.255
172.31.00100000.00000000	172.31.32.0	172.31.63.255
172.31.01000000.00000000	172.31.64.0	172.31.95.255
172.31.01100000.00000000	172.31.96.0	172.31.127.255
172.31.10000000.00000000	172.31.128.0	172.31.159.255
172.31.10100000.00000000	172.31.160.0	172.31.191.255
172.31.11000000.00000000	172.31.192.0	172.31.223.255
172.31.11100000.00000000	172.31.224.0	172.31.255.255

د)

172.31.0.1 تا 172.31.31.254

172.31.32.1 تا 172.31.63.254

172.31.64.1 تا 172.31.95.254

172.31.96.1 تا 172.31.127.254

172.31.128.1 تا 172.31.159.254

172.31.160.1 تا 172.31.191.254

172.31.192.1 تا 172.31.223.254

172.31.224.1 تا 172.31.255.254

۲-۱-۳-۲ Supernetting

مثال برای Super netting: ۴ آدرس در زیر داده شده است بزرگترین Subnet Mask را پیدا کنید که این چهار آدرس را به یک شبکه‌ی واحد تبدیل کند.

192.168.160.0/24

192.168.176.0/24

192.168.180.0/24

192.168.191.0/24

جواب: باید یک Subnet Mask طراحی کنیم که با هرکدام از آن‌ها and شود یک جواب واحد بدست آید. قسمت‌های مشترک همه‌ی آدرس‌ها را یکسان در نظر می‌گیریم، یعنی در مثال بالا فقط ۸ بیت سوم است که با هم متفاوتند. پس آن‌ها را به مبنای ۲ برده و همین عمل اشتراک را در مبنای ۲ انجام می‌دهیم یعنی از هر ۴ عدد در مبنای ۲ مشترک‌ها را برای Subnet انتخاب می‌کنیم. به این صورت که قسمت‌های مشترک آدرس‌ها را یک و قسمت‌هایی که مشترک نیستند را صفر می‌گذاریم.

160	10100000
176	10110000
180	10110100
191	10111111

11100000 = 224

Subnet Mask: 255.255.224.0

آدرس شبکه: 192.168.160.0/19

NetID:

- مشخص شدن محدوده‌ی آدرس‌های IP شبکه (تخصیص آدرس‌ها را ساده‌تر می‌کند.)
- خلاصه‌سازی جداول مسیریابی در مسیریاب‌های میانی و بین راه
- می‌توان تشخیص داد که دو میزبان (فرستنده و گیرنده) در یک شبکه هستند یا در دو شبکه‌ی مجزا

۲-۳-۲ Default Gateway (دروازه‌ی پیش‌فرض)

کار مسیریابی را انجام می‌دهد به این صورت که اگر یک میزبان بخواهد به یک میزبان دیگر داده ارسال کند به طوری که فرستنده و گیرنده در دو شبکه‌ی مجزا قرار داشته باشند(یعنی NetID آن‌ها با هم متفاوت باشد)، فرستنده داده را به دروازه‌ی پیش‌فرض ارسال می‌کند (یعنی آدرس MAC دروازه‌ی پیش‌فرض را روی فریم ارسالی خود قرار می‌دهد ولی آدرس **IP** مقصد نهایی بر روی بسته درج می‌شود) و دروازه‌ی پیش‌فرض آن را به سمت گیرنده (مقصد) هدایت می‌کند.

نکته: وقتی پروتکل IP می‌خواهد یک بسته‌ی اطلاعاتی را روی شبکه بفرستد باید به نحوی آدرس فیزیکی اولین ماشینی که با آن باید ارتباط برقرار کند را بداند، که این ماشین می‌تواند مسیریاب پیش‌فرض یا آدرس فیزیکی مقصد روی همان شبکه‌ی محلی باشد.

نکته:

آدرس IP گیرنده در کل مسیر ثابت است ولی آدرس MAC گیرنده، گام به گام (**Hop by Hop**) تغییر می‌کند.

۲-۳-۳ آدرس‌های معتبر (Valid IP) و آدرس‌های شخصی (Private IP)

آدرس‌های معتبر IP آدرس‌هایی هستند که در کل شبکه اینترنت شناخته شده هستند و در مراجع مربوطه مالکیت IP ثبت شده است و مسیریاب‌ها می‌توانند میسر مناسب به آدرس‌های معتبر را پیدا کنند.

آدرس‌های Private IP آدرس‌هایی هستند که تنها در شبکه محلی معتبر هستند و در اینترنت اعتبار ندارند. این آدرس‌ها برای شبکه‌هایی طراحی شده که نمی‌خواهند بطور مستقیم به اینترنت متصل باشند (اتصال این شبکه‌ها به

اینترنت از طریق Gateway و ترجمه آدرس و یا از طریق پروکسی صورت می‌گیرد). هرگاه بسته با آدرس مقصد یک IP نامعتبر به یک مسیریاب در اینترنت برسد، دور ریخته می‌شود و به مقصد نمی‌رسد.

محدوده آدرس‌های شخصی که در استاندارد تعریف شده است عبارتند از:

10.0.0.0/ 8

176.16.0.0/ 12 (یعنی 176.16.0.0 تا 176.31.255.255)

192.168.0.0/ 16

نکته:

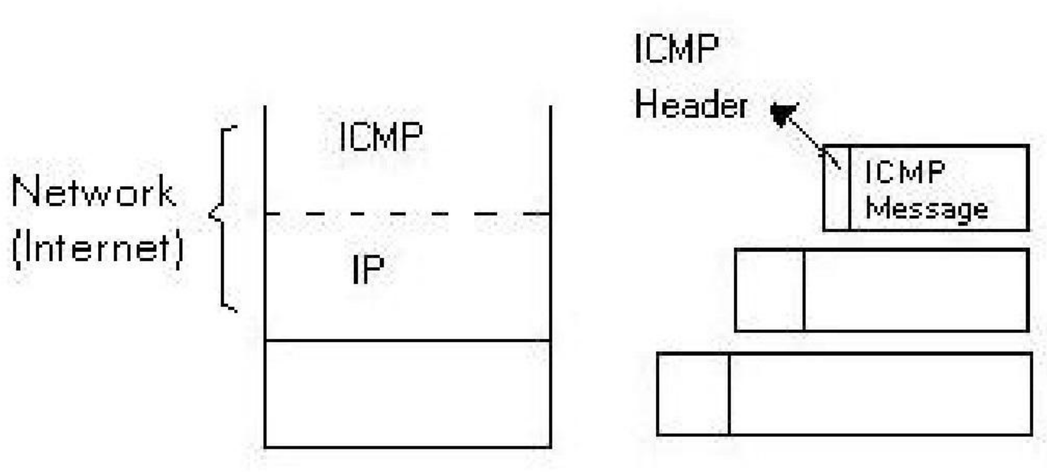
- پروتکل IP یک پروتکل بدون اتصال و نامطمئن است و در هنگام بروز هرگونه خطا، پروتکل IP هیچ گونه اطلاعاتی به فرستنده و در مورد سرنوشت بسته نخواهد داد.
- عدم گزارش خطا به تولیدکننده یک بسته، منجر به تکرار خطا و حمل بیهوده‌ی بسته‌ها می‌شود.

۲-۴ پروتکل ICMP:

Internet Control Message Protocol

پروتکل مدیریتی (کنترلی) لایه‌ی IP است و در کنار پروتکل IP ، برای گزارش انواع خطا و ارسال پیام به مبدا بسته در هنگام بروز مشکلات، استفاده می‌شود. در حقیقت ICMP یک سیستم گزارش خطاست که بر روی پروتکل IP نصب می‌شود تا در صورت بروز خطا به فرستنده پیام مناسب بدهد. در واقع مانع از ادامه یافتن خطا می‌شود ولی خطا تصحیح نمی‌کند.

این پروتکل اشکالات موجود را در قالب یک سری پیام گزارش می‌کند. هر پیام در داخل یک بسته‌ی IP حمل می‌شود.



ساختار کلی پیام ICMP:

Type	Code	Checksum
Parameters		
Data (Payload)		

شکل ۲-۲: ساختار پیام ICMP

Type:

داخل این فیلد یک عدد قرار می‌گیرد که نوع پیام را مشخص می‌کند و ساختار فیلدهای پارامتر و دیتا به این فیلد بستگی دارد. به طور مثال ممکن است نوع پیام Destination Unreachable باشد.

Code: هر نوع پیام ممکن است چند زیرگروه داشته باشد. مثلا در مثال بالا ممکن است شبکه غیرقابل دسترس باشد و یا Host مورد نظر در دسترس نباشد.

Checksum: همانند IP عمل می‌کند. برای کنترل خطا.

Parameters: گاه در یک سری از پیام‌ها استفاده می‌شود و گاه ممکن است هیچ نوع کاربردی نداشته باشد و خالی بماند.

Data: داده‌ای که قرار است ارسال شود.

انواع پیام‌های ICMP:

- Destination Unreachable: مقصد غیر قابل دسترس است.
- Time Exceed: یعنی در زمان پیش‌بینی شده‌ی TTL به مقصد نمی‌رسد پس دور ریخته می‌شود و در نتیجه یک پیام ICMP فرستاده می‌شود.
- Source Quench: با دریافت این پیام مبدا یا مسیریاب باید حجم و سرعت ارسال بسته‌ها را پایین بیاورد.
- Redirect: زمانی ارسال می‌شود که یکی از مسیریاب‌های شبکه بسته‌ی دریافتی‌اش را باز باید به همان مسیریاب یا گره‌ای که بسته را از آن دریافت کرده است بازگرداند.

- Echo Request & Echo Reply: در Ping استفاده می‌شود، یعنی فرستنده این پیام را می‌فرستد(Echo Request) و گیرنده همان پیام را بازمی‌گرداند(Echo Reply)
- Timestamp Request & Timestamp Reply: علاوه بر مورد بالا زمان دریافت و ارسال مجدد بسته را نیز درج می‌کند.

در دستورات Echo Request ,Echo Reply , Timestamp Request, Timestamp Reply برای هرکدام یک شماره ترتیب در یک فیلد جداگانه قرار می‌دهند تا بفهمند که کدام پاسخ به کدام سوال و درخواست مربوط می‌شود.

۲-۵ پروتکل ARP:

Address Resolution Protocol

هرگاه بخواهیم آدرس MAC یک کامپیوتر را از روی آدرس IP آن به دست آوریم از پروتکل ARP استفاده می‌کنیم برای این‌کار کامپیوتر فرستنده یک ARP Request تولید کرده و داخل آن پیامی به این مضمون (چه کسی آدرس MAC کامپیوتری با آدرس IP ... را دارد؟) را در شبکه Broad Cast می‌نماید. (یعنی آدرس MAC آن را ۱ می‌گذارد.) تمام کامپیوترهای شبکه این پیام را دریافت کرده و تنها کامپیوتری به آن پاسخ می‌دهد که صاحب آدرس IP فوق است. و گیرنده یک پیام ARP Reply تولید می‌کند و آدرس MAC خود را در آن قرار می‌دهد و آن را به تولید کننده‌ی پیام ARP Request ارسال می‌کند.

در هنگام به کارگیری پروتکل ARP وقتی آدرس فیزیکی مربوط به ایستگاهی روی شبکه سوال می‌شود، ممکن است آن ایستگاه روی شبکه‌ی محلی دیگری باشد و بالطبع پاسخی نمی‌رسد. در چنین حالتی دو راه حل وجود دارد:

الف) وقتی مسیریابی که به آن شبکه متصل است می‌بیند آدرس مقصدی که توسط ARP سوال شده روی یک شبکه‌ی محلی دیگر واقع است در پاسخ به آن، آدرس فیزیکی خودش را به ایستگاه فرستنده ارسال می‌کند به این روش **Proxy ARP** گفته می‌شود.

ب) ایستگاه‌ها خود موظفند که محلی یا خارجی بودن ماشین مقصد را با توجه به الگوی زیر شبکه تشخیص داده و در صورت خارجی بودن آدرس فیزیکی یک مسیریاب مناسب را انتخاب کنند.

ARP Table:

آدرس‌های به دست آمده از طریق پروتکل‌های ARP در این جدول ذخیره می‌شوند تا در دفعات بعدی برای به دست آوردن MAC نیاز به عملیات ARP نداشته باشیم (ARP cache) که باعث بالارفتن سرعت پروتکل ARP می‌شود

ARP cache هر دقیقه یک بار Update می‌شود.

IP	MAC	Expire
192.168.1.18	EF-FB-AB-00-AA	...
192.168.1.31	ED-99-09-33-00-09	...

۲-۶ پروتکل DHCP:

Dynamic Host Configuration Protocol

- پروتکلی است جهت تخصیص دادن آدرس‌های IP و سایر تنظیمات شبکه (نظیر دروازه‌ی پیش‌فرض، الگوی زیرشبکه، آدرس سرور DNS، آدرس سرور WINS و ...) به تجهیزات شبکه به صورت خودکار(Automatic) و پویا.
- آدرس IP می‌تواند به صورت دائمی تخصیص بیابد یا برای مدت زمانی معین در اختیار Client قرار بگیرد (Lease)
- این پروتکل بر پایه‌ی پروتکل قدیمی‌تر Bootp ، ایجاد شده و از پروتکل UDP جهت انتقال پیام‌های خود استفاده می‌کند.
- این پروتکل نیز ماهیت Client/Serverای دارد، سرور روی پورت UDP Port 67 و Client بر روی UDP Port 68 ، این پروتکل را اجرا می‌کند.

۱-۶-۲ مکانیزم کاری DHCP

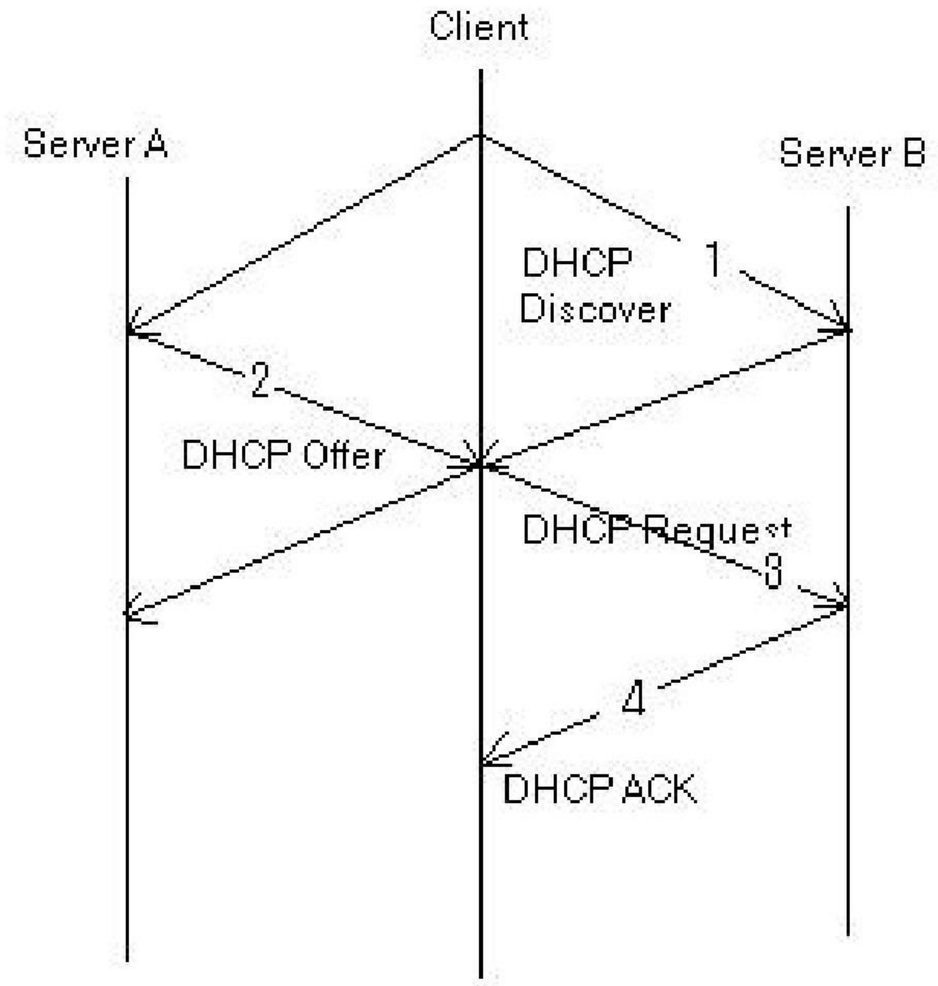
۱- Client در هنگام بوت شدن، یک پیغام DHCP Discover تولید کرده و آن را در شبکه Broad Cast می‌کند.(فاز شناسایی تمام DHCP Serverهای شبکه)

۲- سپس تمام DHCP Serverهای شبکه، آدرس پیشنهادی خود را درون یک پیام به Client ارسال می‌کنند.

۳- Client پس از جمع‌آوری تمام پیشنهادها، یکی را انتخاب کرده و یک پیام DHCP Request تولید می‌کند و آدرس را از سرور درخواست می‌نماید. این پیام در شبکه Broad Cast می‌شود(جهت اطلاع تمام سرورها)

۴- سروری که Client به آن درخواست داده، با دادن پیام DHCP ACK به صورت Uni Cast ، IP را به Client تخصیص می‌دهد. در اینجا مراحل تخصیص آدرس کامل شده است.

۵- Client می‌تواند با دادن درخواست DHCP Release به سرور، IP گرفته شده را آزاد کند.



شکل ۲-۳: فرایند تخصیص IP در DHCP

۲-۶-۲ مکانیزم تمدید IP در DHCP

زمان **T**: حداکثر زمان تعیین شده برای اجاره‌ی IP

زمان $\mathbf{T_1}$: معمولا 1/2 زمان T است.

زمان $\mathbf{T_2}$: معمولا 7/8 زمان T است.

- پس از زمان T_1 ، Client سعی می‌کند تا با ارسال پیام DHCP Request به سروری که IP را از آن اجاره کرده، مدت زمان اجاره را تمدید کند. اگر سرور در پاسخ به این درخواست DHCP ACK بفرستد، IP برای مدت زمان معین تعیین شده، دوباره در اختیار Client باقی می‌ماند.
- در صورتی که زمان T_2 سپری شود، Client موفق به تمدید اجاره‌ی IP از سرور نشود، یک پیام به تمام سرورها به صورت Broad Cast ارسال می‌کند تا IP جدیدی دریافت کند.
- در صورتی که مدت تعیین شده پایان یابد، IP از Client پس گرفته می‌شود.

۲-۶-۳ DHCP Relay

معمولا مسیریاب‌ها به پیام‌های Broad Cast اجازه عبور نمی‌دهند (از جمله پیام‌های DHCP). بنابراین اگر لازم بود که به nodeهای یک شبکه که توسط Routerها به چندین زیرشبکه تقسیم شده است، توسط DHCP ، آدرس IP به صورت خودکار تخصیص داده شود مسیریاب‌ها باید پیام‌های DHCP را به سمت DHCP Server عبور دهند. به این کار DHCP Relay گویند.(مسیریاب پیام DHCP را به صورت Uni Cast به سرور می‌فرستد.)

تنظیمات DHCP Relay در مسیریاب‌های CISCO با دستور IP Helper صورت می‌گیرد.

نکته:

پروتکل RARP برعکس پروتکل ARP ، MAC Address را به IP تبدیل می‌کند.