IPv4 چیست؟

پروتکل اینترنت نسخه ۴ یا به اختصارIPv4 ، چهارمین بازبینی پروتکل اینترنت (IP) و نخستین نسخه‌ایست که به گستردگی به کارگرفته شد. این نسخه از پروتکل در هستهٔ روش‌های شبکه بندی بر پایهٔ استانداردها در اینترنت است. هرچند به کارگیری نسخه ششم پروتکل اینترنت (IPv6)تا تاریخ ۲۰۱۰ آغاز شده‌است، IPv4پراستفاده‌ترین پروتکل اینترنت است.

IPv4 در "RFC 791" ازانتشارات گروه ویژه مهندسی اینترنت (IETF) در سپتامبر ۱۹۸۱ - که جایگزین تعریف قدیمی تر آن در سال ۱۹۸۰ در "RFC 760" شد تشریح شده‌است.

IPv4 پروتکلی بدون اتصال برای استفاده در شبکه‌های راهگزینی بسته لایه پیوند (مانند اترنت) است. این پروتکل بر مبنای مدل بیشترین تلاش برای تحویل کار می‌کند بدین معنی که هیچ تضمینی برای رساندن بسته‌ها به مقصد، پشت سر هم رسیدن و حفظ توالی بسته هاو یا عدم تکراری بودن بسته‌ها ارائه نمی‌دهد. این جنبه‌های مربوط به جامعیت داده‌ها در لایه بالایی یعنی لایه انتقال درنظرگرفته شده‌اند(مانند پروتکل کنترل انتقال (TCP)).

نشانی دهی

هر آدرس IPv4 شامل 32 بیت می‌شود که از 4 بخش 8 بیتی تشکیل شده‌است. در نتیجه فضای نشانی را به ۴٬۲۹۴٬۹۶۷٬۲۹۶ ($۲^{۳۲}$) نشانی یکتای ممکن محدود می‌سازد. اما قسمتی از این نشانی‌ها برای مقاصد خاصی مانند شبکه‌های خصوصی (تقریباً ۱۸ میلیون نشانی) وچند پخشی(تقریباً ۲۷۰ میلیون نشانی) رزرو شده‌است و شمار نشانی‌های قابل استفاده برای مسیریابی روی شبکه عمومی اینترنت کمتر می‌شود. همچنانکه نشانی‌های بیشتری به کاربران تخصیص می‌یابد به اتمام آدرسهای IP نزدیک تر می‌شویم، هرچند که طراحی‌های مجدد ساختار نشانی دهی شبکه از راه شبکه‌های باکلاس(Classful network)، مسیریابی میان دامنه بدون کلاس (CIDR)و ترجمه نشانی شبکه (NAT) از عواملی هستند که این امر را به تعویق انداختند.

محدودیت IPv4 در شمار نشانی‌ها انگیزه‌ای برای ایجاد IPv6 شد که هنوز در مراحل اولیه به‌کارگیری قرار داردو تنها راه حل بلند مدت برای کمبود نشانی هاست.

نمایش نشانی

نشانی‌های پروتکل اینترنت نسخه ۴ به شکل دهدهی نقطه دار نمایش داده می‌شوند. هر نشانی از چهار هشت تایی(octet) تشکیل می‌شود که در مبنای ده نوشته و با نقطه از هم جدا می‌شوند.

نماد	مقدار	تبدیل از دهدهی
نمایش دهدهی نقطه دار	۱۹۲٫۰٫۲٫۲۳۵	N/A
نقطه دارمبنای ۱۶	0xC0.0x00.0x02.0xEB	هر هشت تایی (octet) جداگانه به مبنای ۱۶ تبدیل می‌شود
نقطه دار مبنای ۸	۰۳۰۰۰۰۰۰۰۰۲۰۳۵۳	هر هشت تایی (octet) به صورت جداگانه‌ای به مبنای ۸ تبدیل می‌شود
دستگاه پایه ۱۶	0xC00002EB	بهم چسباندن هشت تایی‌ها در پایه ۱۶
دهدهی		عدد ۳۲ بیتی بیان شده در پایه ۱۰

بیشتر این قالب‌های نمایش را همه مرورگرهای اینترنت می‌فهمند. علاوه بر آن اگر از نمایش نقطه دار استفاده شود، هر هشت تایی را می‌توان در مبنایی متفاوت نوشت. مثلاً نشانی فوق را می‌توان به شکل x00.0002.235192.0 نیز نشان داد.

تخصیص

نشانی دهی باکلاس(Classful Addressing)

درسیستم نشانی دهی اولیه یک نشانی آی پی به دوقسمت تقسیم می‌شد، *شناسه شبکه* که توسط باارزش‌ترین هشت تایی (بالاترین مرتبه) نشانی مشخص می‌گردید و شناسه میزبان که توسط ۳ هشت تایی باقی‌مانده مشخص می‌گردید و از این رو به "فیلد باقیمانده" مشهور بود. این روش امکان نشانی دهی تا حداکثر ۲۵۶ شبکه را فراهم می‌کرد که به زودی معلوم شد که این تعداد ناکافی است.

برای غلبه بر این محدودیت، در سیستمی که بعدها به نام شبکه بندی باکلاس خوانده شد، باارزشترین هشت تایی در تعریفی جدید به کلاسهایی از شبکه‌ها تقسیم شد. این سیستم پنج کلاس نشانی تعریف می‌کند A,B,C,D:و .E کلاس‌های A,B,C تعداد بیتهای متفاوتی برای مشخص کردن شبکه دارندو باقی نشانی مانند قبل برای مشخص کردن یک میزبان درون شبکه به کار می‌رود. بدین ترتیب کلاس‌های شبکه ظرفیت‌های متفاوتی برای نشانی دهی به میزبان‌ها دارند. کلاس D برای نشانی‌های چندپخشی و کلاس E برای کاربردهای آینده رزرو شدند.

کلاس :A در این کلاس ۸ بیت اول آن netID و ۲۴ بیت آخر hostID است و بیت اول netID صفر است. در نتیجه از ۱ تا ۱۲۶ را در بر میگیرد.

کلاس :B در این کلاس ۱۶ بیت اول آن netID و ۱۶ بیت آخر hostID است و بیت اول netID یک و بیت دوم صفر است. در نتیجه از ۱۲۸ تا ۱۹۱ را در بر میگیرد.

کلاس :C در این کلاس ۲۴ بیت اول آن netID و ۸ بیت آخر hostID است و دو بیت netID آن یک و بیت سوم صفر است. در نتیجه از ۱۹۲ تا ۲۲۳ را در بر میگیرد.

کلاس :D در این کلاس سه بیت netID آن یک و بیت چهارم صفر است. در نتیجه از ۲۲۴ تا ۲۳۹ را در بر میگیرد.

کلاس :E در این کلاس چهار بیت netID آن یک است. در نتیجه از ۲۴۰ تا ۲۵۵ را در بر میگیرد.

نشانی دهی بدون کلاس (Classless Addressing)

زیرشبکه بندی

در سال ۱۹۸۵ زیرشبکه‌ها معرفی شدند که امکان تقسیم شبکه‌های باکلاس را ایجاد کرد.

پوشش زیرشبکه با طول متغیر(Variable Length SUBnet Mask)

در سال ۱۹۸۷ پوشش زیرشبکه با طول متغیر (VLSM)معرفی شد که برای ایجاد زیر شبکه‌هایی با اندازه‌های متفاوت به کار می‌رود.

مسیریابی میان دامنه‌ای بدون کلاس (CIDR) و ابرشبکه بندی (Supernetting)

درحوالی سال ۱۹۹۳ مسیریابی میان دامنه بدون کلاس (Classless Inter-Domain Routing) معرفی شد. CIDR برای پیاده‌سازی ابرشبکه بندی به کار می‌رود. ابر شبکه بندی انبوهش مسیر را ممکن می‌سازد. CIDR نشان‌گذاری پیشوندی را معرفی کرد که به نام نشان‌گذاری سی آی دی آر (CIDR) نیز شناخته می‌شود. این نشان‌گذاری اکنون در هر سه مورد نشانی دهی بدون کلاس به کار می‌رود: زیرشبکه بندی (subnetting) ، پوشش زیرشبکه با طول متغیر (VLSM) و ابرشبکه بندی (supernetting).

abfile.ir

CIDR جانشین سیستم ابتدایی کلاس‌های آی پی شد و سیستم قدیم به دلیل طراحی مبتنی بر کلاس، در مقابله با واژه (بدون کلاس)Classless به نام (باکلاس)classful خوانده شد. مزیت اصلی استفاده از CIDR این است که می‌توان هر فضای نشانی را تقسیم نمود تا امکان تخصیص بلوک‌های کوچکتر یا بزرگتر به کاربران به وجود آید.

ساختار سلسله مراتبی CIDR تحت نظارت سازمان مرجع شماره‌های تخصیص داده شده (Internet Assigned Numbers Authority یا IANA) و دفاتر ثبت منطقه‌ای اینترنت (Regional Internet Registry یا RIR) تخصیص نشانی‌ها در جهان را مدیریت می‌کند. هر RIR یک پایگاه داده WHOIS دارد که برای جستجوی عموم در دسترس است و حاوی اطلاعات مربوط به تخصیص آی پی هاست. اطلاعات این پایگاه داده در بسیاری از ابزارهایی که مکان جغرافیایی یک نشانی آی پی را مشخص می‌کنند نقش مرکزی دارد.

نشانی‌های ویژه

بلوک‌های نشانی رزرو شده

بلوک آدرس CIDR	توضیح	منبع
۸/۰٫۰٫۰٫۰	شبکه جاری (تنها به عنوان نشانی مبدأ معتبر است)	RFC 1700
۸/۱۰٫۰٫۰٫۰	شبکه خصوصی	RFC 1918
۸/۱۲۷٫۰٫۰٫۰	آدرس بازگشت(Loopback)	RFC 5735
۱۶/۱۶۹٫۲۵۴٫۰٫۰	Link-Local	RFC 3927
۱۲/۱۷۲٫۱۶٫۰٫۰	شبکه خصوصی	RFC 1918
۲۴/۱۹۲٫۰٫۰٫۰	پیکربندی خودکار نشانی برای لایه پیوند (IANA)	RFC 5735
۲۴/۱۹۲٫۰٫۲٫۰	TEST-NET-1، مستندسازی و نمونه کد	RFC 5735
۲۴/۱۹۲٫۸۸٫۹۹٫۰	رله IPv6 به IPv4	RFC 3068
۱۶/۱۹۲٫۱۶۸٫۰٫۰	شبکه خصوصی	RFC 1918
۱۵/۱۹۸٫۱۸٫۰٫۰	آزمایش‌های محک زدن شبکه	RFC 2544
۲۴/۱۹۸٫۵۱٫۱۰۰٫۰	TEST-NET-2، مستندسازی و مثال‌ها	RFC 5737
۲۴/۲۰۳٫۰٫۱۱۳٫۰	TEST-NET-3، مستندسازی و مثال‌ها	RFC 5737
۴/۲۲۴٫۰٫۰٫۰	چند پخشیها شبکه کلاس D سابق	RFC 3171
۴/۲۴۰٫۰٫۰٫۰	رزرو شبکه کلاس E سابق	RFC 1700
۲۵۵٫۲۵۵٫۲۵۵٫۲۵۵	پخش گسترده(Broadcast)	RFC 919

شبکه‌های خصوصی

از تقریباً ۴ میلیارد نشانی آی پی، سه دامنه از آن برای شبکه بندی خصوصی رزرو شده‌اند. این دامنه نشانی‌ها خارج از شبکه‌های خصوصی قابل مسیر یابی نیستند و ماشین‌های خصوصی نمی‌توانند مستقیماً با شبکه‌های عمومی ارتباط داشته باشند، اما می‌توانند از طریق ترجمه نشانی شبکه (NAT) این کار را انجام دهند.

دامنه‌های زیر سه دامنه‌ای هستند که برای شبکه‌های خصوصی رزرو شده‌اند (RFC 1918).

نام	دامنه نشانی	شمار نشانی‌ها	توصیف در شکل باکلاس(Classful)	بزرگترین بلوک CIDR
بلوک ۲۴-بیتی	۱۰،۰،۰،۰– ۱۰،۲۵۵،۲۵۵،۲۵۵	۱۶،۷۷۷،۲۱۶	یک کلاسA	۸/۱۰،۰،۰،۰
بلوک ۲۰-بیتی	۱۷۲،۱۶،۰،۰– ۱۷۲،۳۱،۲۵۵،۲۵۵	۱،۰۴۸،۵۷۶	دامنه شامل ۱۶ کلاس B همجوار	۱۲/۱۷۲،۱۶،۰،۰
بلوک ۱۶-بیتی	۱۹۲،۱۶۸،۰،۰– ۱۹۲،۱۶۸،۲۵۵،۲۵۵	۶۵،۵۳۶	دامنه شامل ۲۵۶ کلاس Cهمجوار	۱۶/۱۹۲،۱۶۸،۰،۰

شبکه خصوصی مجازی

بسته‌هایی که نشانی خصوصی داشته باشند، عمداً توسط مسیریاب‌ها نادیده گرفته می‌شوند. بنابراین برقراری ارتباط بین دو شبکه خصوصی بدون داشتن امکانات اضافی امکانپذیر نیست. برای انجام این کار می‌توان از شبکه خصوصی مجازی (VPN) استفاده کرد.

VPNها یک تونل ارتباطی بین دوشبکه و از طریق شبکه عمومی درست می‌کنند که دو سر انتهایی آن به عنوان مسیریابهایی برای بسته‌های شبکه‌های خصوصی عمل می‌کنند. این مسیریاب‌ها بسته‌ای را که نشانی خصوصی دارد پوشش می‌دهند و سرآیندهایی با نشانی قابل مسیر یابی در شبکه عمومی به بسته اضافه می‌کنند تا بتوانند آن را از راه شبکه عمومی به مسیریاب مقابل در انتهای دیگر تونل تحویل دهند و در آنجا سرآیندهای نشانی عمومی بسته حذف می‌شود و بسته اولیه به ماشین محلی مقصد تحویل داده می‌شود.

به صورت اختیاری می‌توان بسته‌های کپسول شده(پوشش داده شده) را برای حفظ امنیت داده درهنگام عبور از شبکه عمومی، رمزگذاری نمود

نشانی دهی پیوند-محلی (Link-Local Addressing)

RFC 5735 یک بلوک نشانی - ۱۶/۱۶۹،۲۵۴،۰،۰ - برای استفاده ویژه در نشانی دهی پیوند-محلی تعریف می‌کند. این نشانی‌ها تنها در پیوند(مثل یک قطعه شبکه محلی ویا ارتباط نقطه به نقطه) معتبر هستند. این نشانی‌ها قابل مسیر یابی نیستند و نمی‌توانند نشانی مبدأ یا مقصد بسته‌ای باشند که از اینترنت عبور می‌کند. نشانی‌های پیوند-محلی برای پیکربندی خودکار (Autoconfiguration) میزبانهایی که قادر نیستند از طریق DHCP یا تنظیمات داخلی خود، نشانی بگیرند.

وقتی که این بلوک نشانی رزرو شد، هیچ ساز وکار استانداردی برای پیکربندی خودکارنشانی وجود نداشت. برای پر کردن این خلا مایکروسافت یک پیاده‌سازی از آن با عنوان نشانی دهی آی پی خصوصی خودکار Automatic Private IP Addressing یا APIPA به دلیل قدرت مایکروسافت در بازار، APIPA در میلیون‌ها ماشین به کار رفت و تبدیل به یک استاندارد عملی (غیر رسمی) شد. چندین سال بعد IETF یک استاندارد رسمی برای این کارکرد بانام پیکربندی پویای نشانی‌های آی پی پیوند-محلی به وجود آورد (RFC 3927).

میزبان خانگی(Localhost)

دامنه نشانی ۱۲۷،۰،۰،۱ تا ۱۲۷،۲۵۵،۲۵۵،۲۵۵ (۸/۱۲۷،۰،۰،۱) برای ارتباط میزبان خانگی نشانی‌های درون این دامنه هرگز خارج از رایانه میزبان ظاهر نمی‌شوند و بسته‌هایی که به این نشانی فرستاده شوند به همان دستگاه مجازی شبکه بازمی‌گردند.

نشانی‌هایی که به ۰ یا ۲۵۵ ختم می‌شوند

این تنهایک اشتباه عمومی است که گمان می‌رود هرگز نمی‌توان نشانی‌هایی که به ۰ یا ۲۵۵ ختم می‌شوند را به ماشینی تخصیص داد. این موضوع تنها در صورتی که پوشش زیرشبکه ۲۴ بیت یا بیشتر باشد صادق است. - شبکه‌های کلاس C یا مطابق نمادگذاری CIDR پوشش‌های زیرشبکه ۲۴/ تا ۳۲/ (۲۵۵٫۲۵۵٫۲۵۵٫۰ تا 255.255.255.255)

در نشانی دهی با کلاس تنها سه پوشش زیر شبکه (Subnet Mask)ممکن است: کلاس255.0.0.0 - A ، کلاس 255.255.0.0 - B و کلاس 255.255.255.0 - C مثلاً در زیرشبک۱۹۲٫۱۶۸٫۵٫۰/۲۵۵٫۲۵۵٫۲۵۵٫۰ شناسه ۱۹۲٫۱۶۸٫۵٫۰ به کل زیرشبکه اشاره می‌کند و نمی‌تواند به یک ماشین تنها در آن زیر شبکه تخصیص داده شود.

یک نشانی پخشی (broadcast address) به نشانی گفته می‌شود که اجازه می‌دهد اطلاعات به تمام ماشین‌های یک زیر شبکه فرستاده شود. آدرس پخشی یک زیر شبکه طی یک عملیات "یا" ی بیتی بین مکمل بیتی پوشش زیر شبکه و شناسه شبکه به دست می‌آید. در مورد مثال بالا نشانی پخشی ۱۹۲٫۱۶۸٫۵٫۲۵۵ خواهد بود. برای جلوگیری از اشتباه این نشانی نیز قابل تخصیص دادن به ماشین‌ها نمی‌باشد. در یک شبکه کلاس A یا B یا C نشانی پخشی همیشه به ۲۵۵ ختم می‌شود.

با اختراع CIDR آدرس‌های پخشی الزاماً به ۲۵۵ ختم نمی‌شوند.

به‌طور کلی اولین آدرس هر زیرشبکه، نشانی شبکه و آخرین آدرس نشانی پخشی آن شبکه هستند و بقیه نشانی‌ها را می‌توان برای ماشین‌های شبکه استفاده کرد.

ترجمه نشانی

میزبان‌های روی اینترنت معمولاً به جای نشانی آی پی با نام دامنه شناخته می‌شوند مانندfa.wikipedia.com ، iran.ir، google.com اما مسیریابی در اینترنت بر اساس نام نیست و با استفاده از نشانی آی پی که به این نام‌های دامنه تعلق می‌گیرد، بسته‌ها مسیریابی می‌شوند. پس لازم است که نام‌های دامنه به نشانی‌های آی پی ترجمه شوند.

سامانه نام دامنه (DNS) کار تبدیل نام‌ها به نشانی‌ها و نشانی‌ها به نام‌ها را انجام می‌دهد .DNS ساختار سلسله مراتبی دارد و می‌تواند ترجمه یک فضای نام را به کارساز(سرور)های DNS دیگر بسپارد.

سامانه نام دامنه قابل قیاس با راهنمای تلفن است که نام‌ها را به شماره تلفن تبدیل می‌کند.

پایان یافتن نشانی‌ها

به دلیل رشد سریع اینترنت. نشانی‌های تخصیص نیافته پروتکل اینترنت رو به اتمام است. عوامل زیر باعث سرعت بخشیدن به اتمام نشانی هاست:

- دستگاه‌های موبایل - مانند لپ‌تاپ و دستیار دیجیتال شخصی(PDA)
- دستگاه‌های همیشه روشن - مانند مودم ADSLو مودم کابلی
- افزایش شمار کاربران اینترنت

راه حل استاندارد مهاجرت به پروتکل اینترنت نسخه ۶ است. اما روش‌های زیر نیز باعث کندترشدن اتمام نشانی هاست:

- ترجمه نشانی شبکه(NAT)

- استفاده از شبکه‌های خصوصی
- میزبانی مجازی بر پایه نام

تا تاریخ آوریل ۲۰۰۸ پیش‌بینی‌ها حاکی از این است که نشانی‌های تخصیص نیافته بین فوریه ۲۰۱۰ و مه ۲۰۱۱ تمام خواهد شد

ترجمه نشانی شبکه(NAT)

کمبود نشانی‌های آی پی از دهه ۱۹۹۰ باعث پیدایش روش‌های استفاده کارآمد تر از نشانی‌ها شد. یکی از این روش‌ها ترجمه نشانی شبکه است. دستگاه‌های NAT کل شبکه خصوصی را پشت یک نشانی آی پی عمومی پنهان می‌کنند. بسیاری از ارائه دهندگان اینترنت از این روش استفاده می‌کنند.

ساختاربسته

یک بسته آی پی از دو بخش سرآیند و داده تشکیل می‌شود

سرآیند

سرآیند بسته آی پی نسخه ۴ از ۱۳ فیلد تشکیل می‌شود که ۱۲ تای آن‌ها اجباری هستند. فیلد سیزدهم اختیاری است. این فیلدها به گونه‌ای در سرآیند بسته‌بندی می‌شوند که پرارزش‌ترین بایت در ابتدا بیاید.

<table dir="rtl">
<tr><td>شروع بیت</td><td>۳–۰</td><td>۷–۴</td><td>۱۵–۸</td><td>۱۸–۱۶</td><td>۳۱–۱۹</td></tr>
<tr><td>۰</td><td>نسخه</td><td>اندازه سرآیند</td><td>سرویس‌های متمایز</td><td colspan="2">اندازه کل</td></tr>
<tr><td>۳۲</td><td colspan="2">شناسایی</td><td>پرچم‌ها</td><td colspan="2">افست قطعه</td></tr>
<tr><td>۶۴</td><td>عمرباقیمانده بسته</td><td colspan="2">پروتکل</td><td colspan="2">مجموع مقابله‌ای سرآیند</td></tr>
<tr><td>۹۶</td><td colspan="5">نشانی مبدا</td></tr>
<tr><td>۱۲۸</td><td colspan="5">نشانی مقصد</td></tr>
<tr><td>۱۶۰</td><td colspan="5">انتخاب‌ها (اگر طول سرآیند> ۵)</td></tr>
<tr><td>۱۶۰</td><td colspan="5"></td></tr>
</table>

- نسخه: اولین فیلد در سرآیند یک بسته آی پی، فیلد ۴ بیتی نسخه‌است. مقدار این فیلد برای بسته آی پی نسخه چهار، ۴ می‌باشد.
- اندازه سرآیند :(IHL) این فیلد طول سرآیند بسته را بر حسب تعداد کلمههای ۳۲ بیتی (Word) مشخص می‌کند. از آنجا که در یک بسته آی پی نسخه ۴ طول فیلد اختیاری ثابت نیست، اندازه سرآیند در این فیلد ذخیره می‌شود (که برابر با محل شروع فیلد داده نیز هست). کمترین مقدار مجاز برای این فیلد ۵ است (RFC 791)که برابر با 160=32×5 بیت می‌باشد. و از آنجا که این فیلد ۴ بیتی است بیشترین مقدار آن ۱۵ کلمه یا 480=۳۲×۱۵ بیت است.
- سرویس‌های متمایز:در ابتدا این فیلد به عنوان نوع سرویس (TOS) تعریف شد. اکنون این فیلد در RFC 2474 برای سرویسهای متمایز (DiffServ) و در RFC 3168برای هشدارصریح ازدحام Explicit Congestion Notification یا ECN تعریف می‌شود. فناوری‌های جدیدی در حال پدید آمدن هستند که نیاز به جریان بی‌درنگ داده‌ها دارند و از این فیلد استفاده می‌کنند. نمونه این فناوری‌ها صداروی پروتکل اینترنت (VoIP) است که برای مبادله داده‌های صوتی دو طرفه به کار می‌رود.

هدف اولیه از فیلد نوع سرویس (TOS) این بود که فرستنده بسته ترجیح خود را در مورد نوع برخورد بابسته در اینترنت مشخص کند. مثلاً فرستنده می‌تواند با قرار دادن مقادیری در این فیلد ترجیح خودرا برای تاخیر کمتر یا قابلیت اطمینان بیشتر اعلام کند. اما در عمل این فیلد

زیاد که کارگرفته نشد و توسط اکثر مسیریابهای تجاری نادیده گرفته می‌شد. در نتیجه پژوهش‌ها و آزمایش‌ها برای ایجاد کاربردی برای این فیلد، تعریف فیلد سرویسهای متمایز (DS)برای آن ارائه شد.

بنابه تعریف RFC 791این فیلد از ۸ بیت برای مشخص کردن نوع سرویس به شرح زیر استفاده می‌کند:

- بیتهای ۰ تا ۲ :تقدم
- بیت 3: 0= تأخیر معمولی 1=تاخیر کم
- بیت 4: 0=عملکرد معمولی 1=عملکرد بالا
- بیت 5: 0= قابلیت اطمینان معمولی 1=قابلیت اطمینان بالا
- بیت 6: 0=هزینه معمولی 1=کمینه کردن هزینه‌های مالی تعریف شده در RFC 1349
- بیت ۷: هرگز تعریف نشده‌است.
- اندازه کل بسته: این فیلد ۱۶ بیتی اندازه کل بسته شامل سرآیند + داده را بر حسب بایت مشخص می‌کند. کمترین اندازه بسته ۲۰ بایت است (۲۰بایت سرآیند + ۰ بایت داده). اندازه بیشینه بسته ۶۵۵۳۵ (مقدار بیشینه یک کلمه۱۶ بیتی) بایت می‌باشد. هر میزبان لازم است که بسته‌های با طول حداقل ۵۷۶ بایت را پردازش کند اگرچه میزبان‌های امروزی بسته‌های بسیاز بزرگتر را پردازش می‌کنند. در برخی از شبکه‌ها محدودیت‌هایی برای اندازه بسته‌ها گذاشته می‌شود که در این مورد باید بسته‌ها چندپاره (fragment) شوند.
- شناسایی: این فیلد یک فیلد شناسایی است و برای شناسه‌گذاری یکتا بر روی قطعات مختلف یک بسته چند پاره شده بکار می‌روند.
؛ پرچم‌ها: یک فیلد ۳ بیتی است که برای کنترل وشناسایی قطعات یک بسته چندپاره شده به کار می‌رود:
- بیت ۰: رزرو شده. باید همیشه ۰ باشد
- بیت ۱: چندپاره نکن(DF)
- بیت ۲: قطعات بیشتر(MF)

اگر بیت DF یک (روشن) باشد و برای مسیریابی بسته نیاز به چندپاره کردن آن باشد، به ناچار بسته حذف می‌شود.

وقتی که یک بسته پند پاره می‌شود همه قطعات آن به استثنای قطعه آخر باید پرچم MF را مقدار ۱ (روشن) بدهند.

- افست قطعه: فیلدی ۱۳ بیتی است که شماره یک قطعه را بر حسب واحدهای ۸ بیتی، تسبت به نقطه شروع بسته اولیه چندپاره نشده نشان می‌دهد. افست اولین قطعه صفر است.
- عمر باقی‌مانده بسته :(TTL) این فیلد ۸ بیتی از باقی ماندن بسته‌های سرگردان آی پی در شبکه جلوگیری می‌کند. مقدار این بسته توسط پیش‌فرض سیستم تعیین می‌شود و پس از عبور از هر مسیریاب یک شماره از این فیلد کم می‌شود. اگر این مقدار صفر شود مسیریاب بسته را حذف می‌کند و یک پیام ICMPبه فرستنده بسته می‌فرستد و فرستنده متوجه می‌شود که عمر بسته پایان یافته‌است. برنامه‌های traceroute بر اساس همین پیام ICMP کار می‌کنند.
- مجموع مقابله‌ای سرآیند :(Header Checksum) این فیلد ۱۶ بیتی برای کشف خطا به کار می‌رود. در هر جهش (hop)باید مجموع مقابله‌ای سرآیند محاسبه و با مقدار این فیلد مقایسه شود. اگر این دو مقدار برابر نباشند به معنی بروز خطای انتقال است و

بسته حذف می‌شود. این شیوه تنها برای کشف خطا در سرآیند است و در مورد خطای داده‌ها پروتکلی که در بسته آی پی بسته‌بندی (encapsulate)شده(پروتکل لایه بالاتر) مسوول است. هر دو پروتکل UDPو TCPنیز فیلد مجموع مقابله‌ای دارند.

- پروتکل: این فیلد پروتکلی را که در بخش داده بسته استفاده شده معرفی می‌کند IANA .لیستی از پروتکل‌ها وشماره آن‌ها را ارائه می‌دهد که ابتدا در RFC 790 تعریف شد. از آنجا که در هر جهش (hop) فیلد TTL تغییر کرده و کاهش می‌یابد و ممکن است چندپارگی (fragmentation) نیز انجام شود باید در هر جهش (مثلاً در هر مسیریاب) مجموع مقابله‌ای سرآیند از نو محاسبه شود. روش محاسبه مجموع مقابله‌ای در RFC 1071بیان شده‌است.

- نشانی مبدا: هر نشانی IPv4 از چهار بایت تشکیل شده. در این فیلد مقدار باینری هر هشت تایی (octet) از نشانی در بایت مربوطه قرار می‌گیرد. این نشانی فرستنده بسته‌است. اگر از ترجمه نشانی شبکه (NAT) استفاده شده باشد در این صورت این فیلد نشانی واقعی مبدأ را مشخص نمی‌کند. بلکه ماشینی که عمل NAT را انجام می‌دهد آدرس خود را در این فیلد می‌گذارد و پاسخ بسته نیز به ماشین NAT فرستاده می‌شود که در آنجا به نشانی واقعی میزبان ترجمه می‌گردد.

- نشانی مقصد: مشابه فیلد قبلی است با این تفاوت که نشانی گیرنده بسته را مشخص می‌کند.

- انتخاب‌ها: این فیلد اختیاری است و غالباً مورد استفاده قرار نمی‌گیرد. در صورت استفاده از این فیلد، فیلد IHL باید به گونه‌ای مقداردهی شود که اندازه انتخاب‌های اضافه شده را نیز شامل شود. اگر پایان این انتخاب‌ها الزاماً بر پایان سرآیند منطبق نباشد می‌توان از نشان EOL (پایان لیست انتخابها) برای مشخص نمودن پایان انتخابهااستفاده نمود. مقادیری که می‌توانند در این فیلد قرار بگیرند عبارتند از:

فیلد	اندازه (بیت)	توضیح
کپی	۱	در صورتی‌که نیاز باشد که انتخاب‌ها در تمام قطعه‌های یک بسته چندپاره شده کپی شوند باید این مقدار یک باشد.
رده انتخاب	۲	طبقه‌بندی عمومی انتخاب. ۰ برای انتخاب‌های "کنترلی"، و ۲ برای اشکال زدایی و سنجش. ۱و۳ رزرو شده‌اند.
شماره انتخاب	۵	یک انتخاب را مشخص می‌کند.
طول انتخاب	۸	اندازه کل انتخاب را نشان می‌دهد(که شامل این فیلد هم می‌شود). این فیلد ممکن است برای انتخاب‌های ساده وجود نداشته باشد.
داده انتخاب	متغیر	داده‌های ویژه انتخاب. این فیلد ممکن است برای انتخاب‌های ساده وجود نداشته باشد.

- نکته: اگر طول سرآیند بیشتر از ۵ باشد به این معنی است که فیلد انتخاب‌ها وجود دارد و باید مورد توجه قرار گیرد.

- نکته: گاهی فیلدهای کپی، رده انتخاب، شماره انتخاب را با هم به عنوان فیلد نوع انتخاب بیان می‌کنند.

داده

آخرین فیلد بسته جزو سرآیند نیست و در محاسبه مجموع مقابله‌ای استفاده نمی‌شود. محتویات فیلد داده در فیلد پروتکل سرآیند مشخص می‌شود و می‌تواند هر یک از پروتکل‌های لایه انتقال باشد.

برخی از مهم‌ترین پروتکل‌ها به همراه شماره پروتکل به قرار زیر است:

- 1 پروتکل پیام کنترلی اینترنت(ICMP)
- 2 پروتکل مدیریت گروه اینترنت(IGMP)

- 6 پروتکل کنترل انتقال(TCP)
- 17 پروتکل داده نگار کاربر(UDP)
- 89 نخست کوتاه‌ترین مسیر باز(OSPF)
- 132 پروتکل انتقال کنترل جریان(SCTP)

برای مشاهده لیست کامل، لیست شماره پروتکلهای آی پی را ببینید.

پروتکلهای کمکی

آی پی پروتکلی است که میان شبکه بندی را در لایه اینترنت امکانپذیر می‌کند و از این رو اینترنت را می‌سازد. آی پی از یک سیستم نشانی دهی منطقی استفاده می‌کند. نشانی‌های آی پی به سخت افزار گره نخورده‌اند و یک واسط شبکه می‌تواند چندین نشانی آی پی داشته باشد. میزبان‌ها و مسیریاب‌ها نیاز دارند که ارتباط بین واسطهای دستگاه و نشانه‌های آی پی را بفهمند تا بتوانند به درستی یک بسته آی پی را روی لینک به مقصد تحویل دهند .پروتکل ترجمه نشانی (ARP) ترجمه ازنشانی‌های آی پی به نشانی‌های فیزیکی (MAC Address) را انجام می‌دهد .پروتکل پیکربندی پویای میزبان (DHCP) برای تخصیص خودکار نشانی به میزبان‌ها به کار می‌رود.

منابع

- Planning Classless Routing: TCP/IP
- ↑ Understanding IP Addressing
- ↑ Planning Supernetting and Classless Interdomain Routing (CIDR): TCP/IP
- ↑ Hain, Tony. "IPv4 Address Pool, quarterly generated" (PDF). Archived from the original (PDF) on 3 July 2007. Retrieved 2007-07-01.
- ↑ Huston, Geoff. "IPv4 Address Report, daily generated". Retrieved 2007-09-30.

abfile.ir