



تفاوت ورژن های IPV4 & IPV6

پروژه پنجم درس شبکه های کامپیوتری

دانشجو: سارا حیدری

استاد درس: دکتر علی زارع

IP چیست؟



Internet Protocol Address

- (Internet Protocol) IP یکی از مهم‌ترین پروتکل‌های شبکه‌ای است که مسئول انتقال داده‌ها در بستر اینترنت و شبکه‌های محلی است.

- این پروتکل آدرس‌دهی را برای دستگاه‌های متصل به شبکه فراهم می‌کند و به دو نسخه اصلی تقسیم می‌شود: IPv4 و IPv6

تفاوت های IPv4 و IPv6

پشتیبانی از ویژگی ها جدید

05

آدرس دهی

01

Header

02

روش انتقال (Routing)

03

امنیت

04



آدرس دهی

IPv6

- آدرس‌های ۱۲۸ بیتی (هر آدرس IPv6 شامل هشت گروه از چهار رقم هگزادسیمال است.)
- فرمت کلی آدرس‌های IPv6 به صورت زیر است که با **کولون** (**:**) از هم جدا می‌شوند.
- IPv6 قادر به پشتیبانی از حدود ۳۴۰ سکتیلیون (یعنی ۳۴۰ ضرب در ۱۰ به توان ۳۶) آدرس (برای مدت‌های طولانی نیازی به نسخه‌های جدید یا تغییرات در سیستم آدرس‌دهی نخواهیم داشت).

IPv4

- آدرس‌های ۳۲ بیتی (هر آدرس IPv4 شامل چهار بخش عددی است که هر بخش می‌تواند مقداری بین ۰ تا ۲۵۵ داشته باشد.)
- فرمت کلی آدرس‌های IPv4 به صورت چهار عدد جدا شده با **نقطه** است؛ مثلاً: ۱۹۲.۱۶۸.۱.۱
- تعداد کل آدرس‌های ممکن در حدود **۴.۳ میلیارد** (این مقدار در ابتدای اینترنت کافی به نظر می‌رسید، اما با رشد سریع دستگاه‌های متصل به اینترنت نیاز به یک نسخه جدید به وجود آمد.)

Header

IPV6

- Header ساده‌تر

- اندازه ثابت و برابر با ۴۰ بایت

- حذف یا ساده‌سازی بسیاری از فیلدهای غیرضروری جهت

- پردازش سریع‌تر بسته‌ها

- مثال، فیلد Fragmentation (تکه‌تکه کردن بسته‌ها) در IPv6 به کلی حذف شده و این وظیفه به پروتکل‌های سطح بالاتر یا خود شبکه‌های انتقال داده واگذار شده است.

IPV4

- پیچیدگی بیشتری نسبت به IPv6 دارد.

- اندازه Header ثابت نیست و می‌تواند با استفاده از گزینه‌های اضافی تغییر کند.

- برخی از فیلدهای مهم در IPv4 Header شامل طول کل بسته، آدرس مبدأ و مقصد، نسخه پروتکل و TTL است.

روش انتقال (Routing)

IPV6

- به دلیل وجود تعداد زیادی آدرس، نیازی به NAT نیست و هر دستگاه می‌تواند یک آدرس عمومی منحصر به فرد داشته باشد.
- ساختار مسیریابی بهینه‌تر شده و از تکنیک‌هایی مانند Aggregation استفاده می‌شود (که باعث کاهش پیچیدگی جداول مسیریابی و بهبود کارایی شبکه می‌شود).

IPV4

- استفاده از پروتکل‌های مختلف مسیریابی مانند OSPF، BGP و RIP
- به دلیل محدودیت در تعداد آدرس‌ها و ساختار مسیریابی، شبکه‌ها مجبور به استفاده از تکنیک‌هایی مثل NAT* شده‌اند (تا بتوانند تعداد بیشتری از دستگاه‌ها را با استفاده از یک آدرس IP عمومی به اینترنت متصل کنند).
- این تکنیک‌ها می‌توانند منجر به مشکلاتی در مسیریابی و امنیت شوند.

امنیت

IPV6

- پروتکل IPv6 به صورت پیش‌فرض از IPsec برای تأمین امنیت استفاده می‌کند. (این به این معناست که داده‌های انتقالی در IPv6 به طور خودکار رمزگذاری و تأیید صحت می‌شوند، که باعث افزایش امنیت کلی شبکه می‌شود.)

IPV4

- پروتکل IPv4 به صورت ذاتی امنیت خاصی ندارد.

- برای افزودن ویژگی‌های امنیتی به شبکه‌هایی که از IPv4 استفاده می‌کنند، نیاز به استفاده از پروتکل‌های امنیتی اضافی مثل IPsec است. (این پروتکل‌ها معمولاً به صورت اختیاری استفاده می‌شوند.)

پشتیبانی از ویژگی‌های جدید

IPv6

- IPv6 با توجه به نیازهای مدرن طراحی شده است و از ویژگی‌هایی مثل

Auto-configuration (پیکربندی خودکار آدرس‌ها)، بهبود مسیریابی و پشتیبانی بهتر از شبکه‌های سیار برخوردار است.

- IPv6 به طور پیش‌فرض از multicast برای ارسال داده‌ها به گروه‌های خاصی از گیرندگان پشتیبانی می‌کند.

IPv4

- بسیاری از نیازهای جدید اینترنت، مثل IoT یا موبایل‌های هوشمند، را به خوبی پوشش نمی‌دهد.

- مدیریت شبکه‌ها به دلیل کمبود آدرس‌ها و پیچیدگی‌های مسیریابی چالش‌برانگیز است.



Thanks!