

معرفی IPv6 قسمت دوم - معرفی ساختار (نسخه PDF)



به آدرس IP نسخه 6 آدرس IP نسل آینده یا Next Generation IP Address نیز گفته می شود. اگرچه تاکنون تقریباً ده سال است که بر روی ویژگی ها و استانداردهای پروتکل IPv6 کار شده، اما اخیراً نهایی شده است. علاوه بر این برخی از جنبه های آن هنوز توسط گروه های کاری سازمان IETF در حال کار و بررسی است. همانطور که در مقاله قبلی اشاره شد آدرس های صادر شده توسط IPv6 برای راهکارهای جامع ناکافی بود. این مسئله طراحان را مجبور کرد تا بر روی نسخه جدید این پروتکل کار کنند و این موضوع را به گونه ای انجام دهند که دوباره با مسائل مشابه روبرو نشوند. اعضای انجمن اینترنت که مسئولیت توسعه پروتکل را بر عهده دارند، هر پروتکل جدیدی را که تحت RFC توسعه یافته به دقت موشکافی و بررسی می کنند.

RFCها پرونده هایی هستند که جزئیات و ویژگی های پروتکل ها را ارائه می دهند. بنابراین سازندگان نرم افزار و سخت افزار از این طریق نحوه اعمال پروتکل در استانداردها را خواهند دانست. این استاندارد سازی باعث می شود که ارائه دهندگان نرم افزار و سخت افزار جدا از توسعه تخصص یک پروتکل از یک طرح و برنامه یکسان تبعیت کنند. همانگونه که درک ساختار و نحوه عملکرد IPv6 بسیار حیاتی است برای آدرس دهی IPv6 و بهره گرفتن از آن به نحو مطلوب باید مفهوم و مکانیزم عمل آن را به طور دقیق درک نمود. آدرسهای IPv6 به طول 128 بیت بوده که فضای بسیار زیادی را در اختیار ما قرار داده اند. طول آدرسهای IPv6 بسیار بزرگتر از IPv4 می باشد. اما چه ویژگی دیگری نسبت به نسخه قبلی پروتکل IP متفاوت است؟

- در ابتدا باید گفت که به جای 4 گروه، 8 گروه از اعداد و برای جداسازی آنها، به جای علامت های نقطه، از ":" استفاده شده است. اما به وضوح می توان حروفی را نیز در بین اعداد مشاهده نمود.
- افزایش اندازه آدرس IP، در IP نسخه 6، 128 بیت برای آدرس دهی در دسترس قرار دارد. 128 بیت فضای آدرس به معنی این است که شما بتوانید 2 به توان 128 عدد آدرس متفاوت در اختیار داشته باشید.

این یعنی 340,282,366,920,938,000,000,000,000,000,000 یعنی آدرس توسط IPv6 ارائه میشود

با این حساب اگر هر IPv6 یک گرم وزن داشته باشد مجموع کل IPv6 مساوی با 56 برابر وزن کره زمین میشود.

ICMPv6 یا پروتکل پیغام کنترل اینترنت نسخه 6

(Internet Control Message Protocol, version 6): یک بخش کلیدی از معماری IPv6 است. ICMPv6، وظایف اجرایی و کنترل پیغامهای برگشتی (پیغامهای اطلاعاتی و خطا (شامل PingV6)) لازم را برای تضمین درست و هموار عمل کردن فرایند IPv6 را برعهده دارد. این وظایف شامل:

- گزارش خطای پردازش پکت
- تشخیص و عیب یابی
- کشف همسایه
- گزارش عضویت multicast (کشف multicast Listener همانند IGMP برای IPv6)
- DHCPv6 نسخه جدید DHCP برای IPv6 می باشد. کاملاً از نو طراحی شده است فقط از لحاظ مفهومی شبیه به DHCP است. DHCPv6 شامل عملکرد جدید مثل Authentication است.
- پروتکل های مسیریابی برای IPv6 شامل OSPFv3، RIPv6



پروتکل IPv6 برای اهداف امنیتی طراحی نشد. بدلیل اینکه بحث امنیت جزء وظایف لایه های بالایی در مدل OSI محسوب می شود، IPv6 امنیت را با هدف رمزنگاری و تصدیق هویت، پشتیبانی می کند. Routerهایی که با IPv6 کار می کنند، قادر به تکه تکه کردن پکت ها نمی باشند. اگرچه در IPv4 روترها قادر به تکه تکه کردن پکتها بوده اند اما در IPv6 تنها زمانی این اجازه را به شما می دهد که تکه تکه شدن پکت ها در مبدا صورت گیرد. آدرسهای IPv6 مانند آدرسهای MAC در مبنای 16 بیان می شوند. در هنگام برقراری ارتباط HTTP با یک دستگاه IPv6، آدرس آن را در مرورگر وب خود باید با علامتهای "[]" محصور نمایید. دلیل این کار نیز بسیار ساده است. زیرا مرورگرها برای شناسایی شماره پورتها از علامتهای ":" بهره گرفته و در صورت محصور نکردن آدرس IPv6 با "[]"، هیچ راهی برای مشخص نمودن شماره

۱۲۸ بیت IPv۶ از دو ۶۴ بیت تشکیل شده است. مثالی از ساختار یک آدرس IPv۶ :



۶۴ بیت مربوط به Interface ID و کارت شبکه دستگاه است. از این شناسه برای مشخص کردن آدرس منحصر بفرد هر اینترفیس شبکه استفاده می شود. ۶۴ بیت بعدی به صورت زیر است :

- **FP (Former Prefix)** : به ۳ بیت اول آدرس FP می گویند. نوع آدرس را مشخص می کند. آدرس global است یا private ، به عنوان مثال در آدرسهای Global Unicast معادل ۰۰۱ است.
- **TLA_ID (Top Level Aggregator Identifier)** : به ۱۳ بیت بعدی TLA می گویند. محل جغرافیایی یک IP Address را مشخص می کند. برای تشخیص اینکه مبدا یک مسیر چه بوده و از کجا می آید. اگر بلوک های بزرگتر به ISPها و ارائه گردند و پس از آن به نوبت به مشتریها، تشخیص اینکه مسیرهای طی شده مربوط به کدام شبکه بوده است، بسیار راحت تر خواهد بود. با IPv۴ بسیاری از آدرسها قابل انتقال هستند. همچنین تعداد سازمانهایی که بلوک های آدرس را به سازمانهای تجاری و دیگر مشتریان پایین دست ارائه می کنند بسیار زیاد است بنابراین دانستن اینکه یک مسیر از کجا ناشی شده و شروع می شود، بدون پیگیری رو به عقب مبدا یک پکت (Trace)، غیر ممکن است. اکنون به وسیله IPv۶ ، تعیین مبدا یک مسیر، بسیار عملی تر و امکانپذیرتر شده است.

فرض کنید که اینترنت شامل ۵۰۰ تامین کننده ردیف اول باشد، در این صورت توسط جستجو در یک مدت بسیار کم، بر مبنای شناسه TLA مربوط به طولانی ترین مسیر، می توان فهمید که مسیر از کجا آغاز شده است. حتی می توان نرم افزاری را تولید کرد که این وظیفه را در داخل خود جای داده و انجام دهد. (البته اگر آن نرم افزار قابلیت به روز رسانی لیست آدرسهای اختصاص داده شده را داشته باشد). TLAها در اصل به NAP اشاره می کند.

NAP (Network Access Point) : در سطح دنیای اینترنت ۱۲ تا NAP وجود دارد. توجه کنید که این Access Point به معنی AP شبکه های وایرلس نیست. Back-Bone های اینترنت NAP هستند. شاهراه های اینترنتی به NAP ختم می شوند. تا Backbone اصلی در دنیای اینترنت وجود دارد که اکثراً هم در آمریکا هستند. مثل AT&T یک NAP است. در ساختار اینترنتی بایستی مشخص شود که به کدام یک از NAPها متصل می شویم . این قسمت (TLA) توسط سازمان بین المللی تخصیص آدرسهای اینترنتی IANA اختصاص داده می شود.

پس اول بایستی معلوم شود که آدرس ما چیست ؟ Global است یا Private ، بعد با فرض اینکه Global باشد حالا باید مشخص شود که این آدرس Global به کدام NAP اینترنتی ختم می شود. تا اینجا از ۶۴ بیت، ۳ بیت FP و ۱۳ بیت TLA مشخص شد. همانند پروتکل IPv۴ ، در پروتکل IPv۶ نیز گروهی از آدرسها برای مقاصد خاص رزرو شده اند. پروتکل IP نسخه ۶، ۸ بیت رزرو شده دارد که اگر به این NAPها در آینده اضافه شود و آدرس های NAP کم بیاد می تواند از این رزروها استفاده کند. مثل ۰:۰:۰:۰:۰:۰:۰:۰ که معادل " :: " بوده و شبیه به آدرس ۰.۰.۰.۰ در IPv۴ عمل می کند. این آدرس به مفهوم آدرس فرستنده یک پیام در برخی از پیکربندی ها می باشد.

- **NLA_ID (Next Level Aggregator Identifier)** : به ۲۴ بیت بعدی NLA می گویند. شناسه ۲۴ بیتی برای حوزه های کوچکتر از TLA است. شامل مجموعه ای از آدرس هاست که به واسطه بلوک TLA و پس از آن به سیستمهای زیر مجموعه اختصاص داده می شود. به AS مربوطه اشاره می کند. مثلاً شماره AS مخابرات ایران. NLA ما می شود یعنی NLA مخابرات ایران.
- **SLA_ID (Site Level Aggregator Identifier)** : به ۱۶ بیت بعدی SLA می گویند. مشخص کردن حوزه های کوچکتر از NLA. به عنوان مثال مشخص کردن شرکت ها و سازمانهای دولتی در داخل یک کشور. شماره AS ISP ما را مشخص می کند. برای نمایش ساده تر IPv۶ می توان قسمتهایی از آن را که تماماً صفر است، فقط با یک صفر نمایش داد و یا تمام صفرها را به همراه کولن بعد از آن حذف کرد.

فشرده سازی IPv۶



چند نکته :

- IPv۶ نمی تواند با " :: " شروع شود.
- در هر قسمت ۱۶ بیتی می توان حداکثر از عدد DDDD و حداقل از ۰۰۰۰ استفاده کرد.
- در IPv۶ چیزی به نام Subnet Mask وجود ندارد اما به جای آن Prefix (بیشوند) وجود دارد.

به طور مثال IP آدرس ۳::۲۰۰۱ با پیشوند ۶۴ بیت به صورت ۶۴/۳::۲۰۰۱ نوشته می شود، مفهوم این است که ۶۴ بیت از سمت چپ ثابت و نشان دهنده آدرس شبکه (subnet ID) است و مابقی می تواند برای کامپیوترهای داخل شبکه تغییر کند.

- می توان برای هر کامپیوتر چندین Subnet ID تعریف کرد که به این تکنیک **Multinetting** می گویند.
- اگر پیشوند IP آدرسی مشخص نشود ، به طور پیش فرض، ۶۴ بیت در نظر گرفته می شود.



انواع آدرس دهی در IPv6

۱. Unicast
۲. Multicast
۳. Anycast

چند نوع مختلف آدرس دهی Unicast

۱. Global Unicast
۲. Link-Local Unicast
۳. Unique-Local Unicast



- **Global Unicast**: به مفهوم آدرسهای unicast قابل انتقال در اینترنت بوده (قابلیت آدرس دهی در اینترنت را بر عهده دارند) و شبیه به نوع متناظر آن در IPv4 می باشند ، به این نوع آدرسها **Aggregatable Address** نیز می گویند. این ساختار از قسمتهای زیر تشکیل شده است :



- **Link-Local Unicast**: شبیه به آدرسهای Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرسها را می توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند را تخصیص داد. این آدرسها که در غیاب DHCP Server ایجاد می شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس ، در کادر **Properties** کارت شبکه گزینه **obtain IPv6 address automatically** را انتخاب کنیم. سیستم عامل به طور خودکار براساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می دهد.



- **Unique-Local Unicast**: این آدرسها را با نام **Site-Local unicast** هم می شناسند. نیز قابلیت انتقال در اینترنت را نداشته اما در هر جا که مورد استفاده قرار گیرند ، در بین تمامی دیگر آدرسهای اینترنت منحصر به فرد می باشند. عملکرد این نوع آدرسها دقیقا شبیه به آدرسهای private در IPv4 بوده و امکان برقراری ارتباط بین دستگاههای یک سازمان محلی را با واسطه روترها ممکن می سازند. این آدرسها با ۱۶ بیت ثابت (fec0) شروع می شوند و به دنبال آن ۳۲ بیت صفر و سپس ۱۶ بیت مربوط به Subnet ID است که معمولا آن را هم صفر در نظر می گیرند. ۶۴ بیت پایانی هم که **Interface ID** است که برای هر کامپیوتر منحصر به فرد است.*



- **آدرسهای Multicast**: شبیه به IPv4، پیامهای ارسال شده به مقصد این آدرسها، توسط گروهی از دستگاههای دارای آدرس مزبور دریافت می شود. این آدرسها در برخی از مواقع با نام **One-to-Many** نیز نامیده می شوند. در IPv6 آدرسهایی که با FF شروع می شوند، در گروه آدرسهای multicast قرار خواهند گرفت.



- **آدرس های Anycast**: در ارتباط با آدرسهای Anycast در مقاله قبل توضیح دادم اما برای تکمیل توضیحات عرض میکنم که ، برای ساختن یک آدرس Anycast و اختصاص دادن آن به یک router باید ابتدا بخش NET ID مربوط به IPv6 Address شبکه را ثابت و قسمت Subnet ID را صفر قرار دهیم. در واقع می توان گفت که برای ساخت چنین آدرسی نیاز به داشتن IP Perfix شبکه داریم. به طور مثال برای شبکه ۶۴/۱:۱:۱:۱::۲۰۰۱ آدرس Anycast برابر با ۰:۰:۰:۰:۱:۱:۱:۱::۲۰۰۱ یا در حالت فشرده ۱:۱:۱:۱::۲۰۰۱ خواهد بود. حال

اگر بسته ای به آدرس Anycast ارسال شود ، به دست نزدیکترین آدرس Anycastی که روی روتر تنظیم شده است می رسد. این عمل با استفاده از ساختارهای مسیریابی آدرسهای Anycast و Routing Metric های مسیریابی اتفاق می افتد و زمانیکه یک packet با آدرس Anycast ارسال شود بعد از اینکه به دست اولین و نزدیکترین دستگاه برسد، دیگر به دنبال دستگاههای دیگر نمی گردد و مسیریابی به اتمام می رسد.

نویسنده : عاطفه حسین زاده

منبع : جزیره شبکه و زیرساخت وب سایت توسینسو

هرگونه نشر و کپی برداری بدون ذکر منبع دارای اشکال اخلاقی می باشد

زهرا مرشدی

با تشکر از مقاله ی خوبتون. استفاده از ipv6 توی امنیت شبکه تاثیری داره؟

عاطفه حسین زاده

بله...با توجه به اینکه در IPv6 از پروتکل IPsec به عنوان یه بخش الزامی مطرح شده که باعث ایجاد یک زیرساخت امنیتی مناسب به منظور ارائه سرویس های امنیتی میشه.

ظرفیت عملیاتی IPsec طوری هست که سازمانها به کمک اون بتونن وضعیت مدل امنیتی و سیاستهای امنیتی خودشون و توسعه بدن. البته یه نقطه ضعفهایی هم داره که به دلیل اجرای اون در شبکه باید به عنوان بخشی از تدابیر امنیتی از این نقاط ضعف پروتکل آگاه باشیم.

یک نکته : اگه شبکه شما از IPv6 استفاده نمیکنه بهتره پروتکل رو غیرفعال کنید، چون در غیر اینصورت زمینه اجرای حمله های امنیتی رو برای مهاجمان فراهم می کنید.

موفق باشید

رضا ایرانی

واقعا عالی بود

فک کنم تو این سایت تنها سیسکو کار شما هستین؟؟؟

محمد نصیری

خیلی جامع و کامل بود ، ممنونم از شما ، برام شکل سوکت در آدرس IP ورژن ۶ خیلی جالب بود چون ما در آدرس IP ورژن ۴ خیلی راحت قالب سوکت رو یا : مشخص می کردیم اما در نسخه ۶ : خودش جزئی از آدرس هست ، قابلیت احراز هویت یا Authentication ای که فرمودید DHCP انجام میده هم برام جالب بود که خودش میتونه ضریب امنیتی بسیار خوبی رو ایجاد کنه ، معرفی NAP ها هم از نظرم جالب بود که براحتی امکان شناسایی مکانی و موقعیت های IP رو به ما میدن ، اما چند نکته برام هنوز مبهم مونده :

۱. اولیش اینکه در NLA-ID و SLA-ID شما گفتید که ۲۴ بیت بعد از NLA رو میگن NLA-ID و ۱۶ بیت بعد از NLA رو میگن SLA-ID یعنی ایندو در هم تداخل دارند ؟ درون هم هستند ؟

۲. و ابهام بعدی هم در خصوص این هست که در قسمتی از مقاله اشاره شده که در هر قسمت ۱۶ بیتی حداکثر می توان از DDDD و حداقل می توان از ۰۰۰۰ استفاده کرد ، اینجا کمی ابهام داره برام ، به این نمونه آدرس IP ورژن ۶ دقت کنید
fe8۰::۴۹c۳:c۹db:dbdf:a۸۷۹%۱۹ حرف F رو داره !!!

عاطفه حسین زاده

یک موسسه جهانی هست که ثبت AS میکنه. یعنی هر کسی که بخواد AS ثبت کنه باید در این موسسه ثبت کنه. مثلا AS مخابرات ایران.

NLA و SLA به نوعی برای مشخص کردن حوزه ها استفاده می شوند. مثلا اگه بیان ایران و طوری تقسیم بندی کنند که هر استان NLA خودش و داشته باشه NLA شما در تهران میشه NLA مخابرات تهران. پس کسانی که توی تهران با هم کار دارن با توجه به اینکه NLAهاشون شبیه به هم هست ترافیکشون از تهران بیرون نمیره.

و به همین ترتیب از ایران.

SLA به حوزه های کوچکتر اشاره میکنه. مثلا ISPها.

رضا ایرانی

موسسه IANA هست که زیر مجموعه اش هم RIPE که وظیفه تخصیص IP و AS و ... رو میده آدرسش هم هست:

ripe.net

سعید فتحی

فقط در تکمیل این موضوع باید بگم که TLA و NLA از ساختار IPv6 حذف شده اند و SLA هم تغییر نام پیدا کرده است ... این هم قسمتی از آخرین ورژن کتاب Network + که توسط مایکروسافت به چاپ رسیده ...

These original field descriptions still appear in many IPv6 descriptions, but the standard was actually modified in ۲۰۰۳ to eliminate the separate TLA and NLA fields and rename the SLA field. The current official format for global unicast addresses, consists of the following elements:

Global routing prefix: A ۴۸-bit field beginning with the ۰۰۱ FP value, the hierarchical structure of which is left up to the RIR

Subnet ID: Formerly known as the SLA, a ۱۶-bit field that organization can use to create an internal hierarchy of sites or subnets

Interface ID: A ۶۴-bit field identifying a specific interface on the network

Theoretically, the global routing prefix and subnet ID field can be any size.

Eskali

سلام

با تشکر جامع بود

سعید کمندری

سلام

با تشکر ، خوب بود.

Mahdi hajipour

تو کاربرد INTERFACE ID چیه ؟

فقط همون ۶۴ بیتی که برای مشخص کردن آدرس منحصر بفرد هر اینترفیس شبکه استفاده می شود؟

تو کاربرد IPV6 کاربرد INTERFACE ID چیه ؟

فقط همون ۶۴ بیتی که برای مشخص کردن آدرس منحصر بفرد هر اینترفیس شبکه استفاده می شود؟

مطلب اصلی